The Municipal Internet of Things (IoT) Blueprint

A publication of the Wireless SuperCluster of the Global City Teams Challenge
https://pages.nist.gov/GCTC/super-clusters/
July 10, 2019

Authors
(in alphabetical order):

Will Barkis, Orange Silicon Valley, Section 7
Tony Batalla, City of San Leandro CA, Sections 2-4
Benson Chan, Strategy of Things, Section 5
Lan Jenson, Adaptable Security, Section 6
Renil Paramel, Strategy of Things, Section 5
Bill Pugh, Smart Connections Consulting, Section 6
Jon Walton, County of San Mateo CA, Section 1
Ruwan Welaratna, Evo, Inc., Section 6
Tom Williams, Palo Alto Networks, Section 2 [Security Considerations]
Steve Wimsatt, CommScope (Ruckus), Section 7

Editors:

Tony Batalla, City of San Leandro, CA
David Witkowski, Joint Venture Silicon Valley

GLOBAL CITY TEAMS CHALLENGE

Acknowledgments

The Wireless SuperCluster would like to acknowledge the following people for their support, encouragement, and contributions both to this Blueprint and to the entire Global City Teams Challenge community:

Sokwoo Rhee of the National Institute of Standards and Technology (NIST) for his tireless dedication to the GCTC program and concept;

Jean Rice of the National Telecommunications and Information Administration (NTIA) for her immense support of the Wireless SuperCluster (previously the Public Wi-Fi SuperCluster);

Our fellow SuperClusters and the Cybersecurity and Privacy Advisory Committee (CPAC), along with associated Action Clusters;

Our Advisory Team (in alphabetical order): John Coluccio; Gary Dennis; Daniel Herb; Zack Huhn; Bob Iannucci; Benny Lee; Jack Mulqueeny; Cef Ramirez; Alexandra Reams; Vijay Sammeta; Kim Sanchez; Jeffrey Tackes; Mo Shakouri; and Rebecca Wise;

Additional Contributors to our IoT Blueprint Workshop (in alphabetical order), held in May 2018 Orrick, Herrington & Sutcliffe LLP in Menlo Park, CA: Geoffrey Arnold; Rick Goetz; Damon Kachur; Lloyd Jobe; Jeff Lewis; Mrinal Wadhwa; and Ed Walker;

We also extend our sincere gratitude to the staff - and by extension the elected officials - of the following local governments for contributing their experiences and stories for this Blueprint so that other government agencies can learn from their trailblazing efforts:

- **City of Calgary, AB Canada:** Colin Adderley, IT Engineer; Sylvain Mayer, IT Manager; Nathalie Tacail, Communication Planner; and Nan Xie, IT Leader;
- **City of San Diego, CA:** Lorie Cosio-Azar, Formerly with Environmental Services; Cody Hooven, Director/Chief Substantiality Officer; and Arwa Sayed, Project Officer;
- **City of San Leandro, CA:** Michael Hamer, Assistant IT Manager; Debbie Pollart, Public Works Director;
- **County of San Mateo, CA:** Ulysses Vinson, Chief Smart Communities Officer.

Finally, we'd like to affirmatively state that this work serves as a testament to the success of the GCTC program and its overarching goal of bringing together an international community of government practitioners and officials, working at all levels (i.e., national, state/provincial, local) with academics, non-profits, and the private sector to share our individual experiences, expertise, challenges, and achievements so that collectively, we can learn from one another, develop communities of practice, and thereby accelerate successful adoption of cutting-edge cyber-physical systems and innovations by government agencies throughout the world.

Preamble

If you are a local government official or employed by a municipality, chances are by now you have heard the term “Smart City.” Perhaps you have even wondered what it means for your agency and, possibly, your constituents. However, while it is not difficult to find articles explicating the *promise* of smart cities it is, in fact, much harder to find examples of *actual* smart cities.[1]

While this revelation may be surprising, it actually makes sense; a universally accepted definition of “smart city” does not exist because cities, counties, states and their equivalents throughout the world are tremendously varied. The issues that Jaipur, India are trying to understand and improve are likely to be different from those in Madrid, Spain – which are both different from Tampa, Florida. This is to be expected and, for smart communities to evolve, this variance must be embraced. Rather than seek a one-size-fits-all definition, government agencies should define their own meaning for what constitutes “smart” in terms that serve their goals and specific needs.

However, what smart communities *will* share is an underlying relationship with information and communications technology (ICT). Put another way, all smart communities will utilize, in some form or another, a varied collection of devices, networks, data and analytics. As a *collective system*, these pieces are often abstracted as one grand concept: the “Internet of Things” (IoT).[2]

The evolution of smart communities and IoT are tightly interwoven; practitioners often speak of them as synonyms for each other. For example, the term “connected city,” which some use in place of “smart city,” explicitly implies IoT; hence, the “connected” part of the equation. However, this can all be exhausting for government decision makers to keep up with, particularly for those who are not IT professionals and technologists.

Thus, the purpose of this Blueprint is to provide state and local government leaders, technology practitioners and researchers, and industry partners with a practical overview of the Internet of Things and how it will affect government agencies in the future.

[1] The authors of this Blueprint often use the term “Smart Community” in place of “Smart City” to be inclusive of counties, special districts, and states that are within the scope of the Smart City Movement and related technology.
[2] The term “Internet of Things” - like Smart Cities - has no singular definition and is in fact comprised of several forms of technologies and complementary components and systems.

Table of Contents

Acknowledgments i
Preamble ii
Scope of This Blueprint iv
1. Impacts to Municipal Governments of IoT Networks 1
2. Considerations for Deploying Municipal IoT 4
Deployment Considerations 4
Security Considerations 6
Regionalization and Interoperability 7
Civic Engagement & Privacy 8
Smart Communities Framework 8
3. The Current State of Municipal IoT Deployments 10
4. Case Study Summary Findings & Discussion 14
5. Practical Guide: Deploying an IoT Network 17
Introduction 17
Decision Process 17
Important Considerations 18
Connectivity Option Selection Process 27
Examples 34
Template - Connectivity Selection 38
6. Practical Guide: IoT Cybersecurity & Privacy 41
I. IoT: Cybersecurity and Privacy Risks 41
II. IoT: Trustworthy and Resilient through Risk Management 42
III. Best Practices and Considerations 43
Section Appendixes 52
7. Full Case Study Reports 59
City of Calgary, AB Canada 60
City of San Diego, CA 65
City of San Leandro, CA 69
County of San Mateo, CA 74

Scope of This Blueprint

The scope of this Blueprint will be on the IoT networks themselves – the physical and logical layers, not necessarily the software applications and data generated therefrom. To this end, this Blueprint employs the following nomenclature:

Municipal IoT Network: Network-connected devices, installed in a networked system of protocols, wired and/or wireless communications technologies, computer servers and software, used by governmental entities.

Network-connected Devices: Sensors, actuators, connected vehicles; energy usage monitoring sensors; physical access control security systems and lighting; utility control and metering systems; intelligent traffic monitoring and management; public safety sensors (gunshot detection, cameras, bike lane monitoring); street light sensors; etc.

Figure 1 below provides a mental map for understanding the basic outline of a Municipal IoT network. These networks are, essentially, cyber-physical systems that underpin the various domain-specific applications and outcomes that Smart Communities hope to achieve, such as improved Public Safety, Transportation, Broadband, Economic Development, etc.

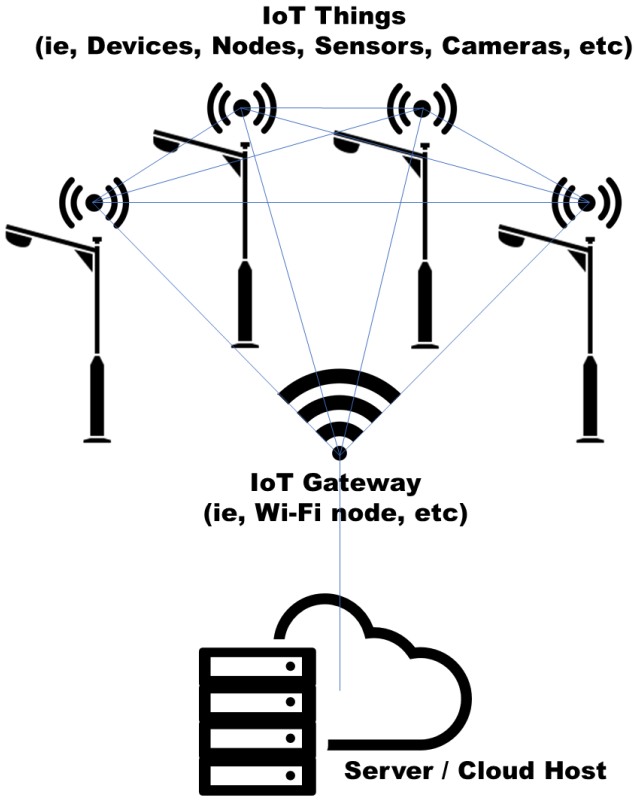


Figure 1 - Mental Map of a Municipal IoT Network consisting of: IoT Devices, a Wi-Fi Gateway, Communications Lines (i.e., fiber optics and/or the Internet itself), and a Server or Cloud Hosted Controller

Section 1: Impacts of IoT to Municipal Government and is a generalized discussion of six ways IoT networks will change government operations in the future. Areas as diverse and varies as governmental service delivery, government operating costs, outcomes in local economies, environmental sustainability, and digital and social equity all may be affected by improvements in technology that will stem from IoT and Smart Communities. This section attempts to answer the fundamental questions: *Why should government officials care about IoT and why does this matter?*

Section 2: Considerations for Deploying Municipal IoT Networks examines the models that local governments have considered for IoT networks deployments. These models generally fall into one of two categories: 1) government agencies build and maintain their own IoT networks and services; and 2) cellular and telecommunications firms build and maintain networks that government agencies can subscribe to as-a-service (in a manner similar to how we subscribe to cellular phone service). We explore these as well as additional models, such as public-private partnerships. Security, the concept of "regionalization", interoperability, and civic engagement are additional considerations discussed.

Section 3: The Current State of Municipal IoT presents research findings developed for this report, derived from an online survey conducted in January 2019. A key takeaway from the survey is support for the notion that the Municipal IoT is still in the "early adopter" stage and some years out from reaching maturity.

Section 4: Case Study Summary Findings & Discussion also presents firsthand research developed for this report: case studies of local government leaders who have deployed IoT networks in their communities, from the cities of San Diego, CA; San Leandro, CA; Calgary, AB Canada; and the County of San Mateo, CA. These structured interviews provide a rich source of qualitative data and uncover important lessons for all Municipal IoT deployments.[3]

The next two sections are comprised of in-depth technical, hands-on guides intended to inform and guide local government decision makers, officials, staff, and others with an interest in municipal IoT networks.

Section 5: A Practical Guide to Deploying Municipal IoT Networks is a hands-on, systematic walkthrough to assess IoT networks for government agencies and contains a wealth of managerial and technical information.

Section 6: A Practical Guide to IoT Cybersecurity and Privacy guides decision makers through the complex but critical areas of cybersecurity and privacy.

Section 7: Full Case Study Reports provides the full case study reports, written for this Blueprint, covering each city and project in detail.

[3] All interviewees have graciously agreed to share their stories on record.

1. Impacts to Municipal Governments of IoT Networks

The Municipal IoT will probably have numerous impacts to state and local government agencies and their operations. In a sense, this is the heart of this Blueprint paper, and the essential reason for its existence. IoT networks have the potential to improve greatly the way we deliver services, reduce operating costs, improve the economy and commerce, promote better environmental stewardship, and provide opportunities for digital equity and access – leading to developments in tourism, breakthroughs in transportation and transit, and so much more. While this list of potential use cases is by no means exhaustive, it provides an introduction for government leaders as to what they should start looking for when it comes to the potential impacts of IoT networks.

Impact #1: Enhanced Service Delivery

Many civil service problems have been around so long, they are considered more like facts of life than actual problems. *Of course,* there is traffic at rush hour. *Of course,* parking downtown is a pain. *Of course,* the trashcans on Main Street overflow on weekends. IoT technology and smart city systems are not a magic wand to make these challenges disappear – but they can certainly help. Emerging technologies can utilize GPS systems, cameras, electronic road signs, and traffic light coordination (all connected via IoT) to keep traffic flowing. Parking spot sensors can alert the public when and where parking is available – an impact especially appreciated by handicapped visitors and owners of electric vehicles in need of a charge. Meanwhile, streetlights connected into citywide wireless networks, controlled remotely and activated via mobile apps, will reduce staff time for maintenance and provide greatly improved energy efficiency.

Municipalities can also collect vast amounts of data on how long it takes citizens to get from place to place or how long they spend waiting for public transit, and then alter routes or times accordingly based on documented needs. Smart waste bins can now send alerts when they need to be emptied, allowing municipalities to both prevent them from overflowing on busy days, and prevent unnecessary pickups on slow days.

Impact #2: Reduced Operating Costs

The prevention of unnecessary waste pickups referenced above is more than just a convenience; it also saves money and reduces greenhouse gas emissions. Despite a public perception of government bloat, many local agencies operate on a shoestring budget. Installing IoT technology to transform a city into a *smart city* obviously requires an initial investment, but the savings can add up quickly. IoT sensors installed in a water supply system can track water pressure, chemical composition, and flow. When numbers veer outside the expected range, the system can automatically alert local authorities to address the situation – and provide real-time data to back up their decisions. Sensors can turn streetlights on or off – or even adjust their brightness – depending on ambient light levels or detected motion. Smart technology can increase energy efficiency to reduce energy bills, increase irrigation efficiency to reduce water bills, and increase resource efficiency to reduce resource costs. Asset management systems can track physical resources throughout a space—ladders or forklifts in a government building, for example—so staff

can locate them easily. This not only saves time and headache for workers but also prevents the purchasing of unnecessary resources to replace “lost” ones.

Impact #3: Improved Economy and Commerce

IoT technology encourages cooperation between multiple public and private organizations to collect, analyze, and actualize real-time information. Businesses can use data collected through IoT to improve their services, understand pain points, and better target potential customers. Smart kiosks installed on downtown street corners can provide wayfinding services to help guide people wherever they’re trying to go; concierge services, to help people find the nearest movie theater, clothing store, or Indian restaurant; or even display advertisements, to generate extra revenue for local government and exposure for local businesses. Data even shows smart cities enhance competitiveness in attracting new residents and businesses.

Impact #4: Environmental Sustainability

Energy and water efficiency have already been mentioned but deserve to be highlighted here as well. Citizens are increasingly expecting their governments to act on such issues, and smart technology can allow agencies to make truly intelligent choices. Something as simple as installing solar panels can save both money and the environment. Deploying air quality sensors can allow municipalities to monitor air quality changes throughout the day and identify areas or times of particularly heavy pollution. This data can be critical to sensitive populations, such as those suffering from respiratory ailments, but can also be used by authorities to reveal businesses that may be polluters and create action plans aimed at reducing emissions.

Impact #5: Equitable Access

IoT technology contains an important keyword buried in the acronym: *internet*. Many rural, coastal, underserved, or unincorporated communities struggle with fiber, wireless, and cellular connectivity. This means many residents and visitors miss out on the benefits the internet can bring, including innovation and free-flowing communication, economic development, educational opportunity, and democratic access. During emergencies, when traditional landlines and other services fail, internet access can be a literal lifesaver, providing critical local information. However, making a commitment to smart technology also means making a commitment to ensure internet access – “oT” isn’t very helpful without the “I.” Obviously, many municipalities cannot afford to create wired internet connections throughout their territory, but there is no need to. Other innovative technologies exist to help provide access in remote or difficult-to-reach areas, such as microwave technology. Becoming a smart city can be a great reason to begin providing much-needed internet access to a community.

Impact #6: Everything Else

The possibilities with smart technology are nearly limitless. Sensors can track which streets have been plowed after a blizzard and which streets still need to be plowed. They can monitor the structural integrity of bridges and buildings to prevent full or partial collapses, saving money and lives. From bots to sensors, the use of smart technology can free up staff to focus on strategic initiatives rather than manual drudgery.

Regardless of geographic location, population, economic size and might, governments working with the Internet of Things are hoping to improve the lives of the residents and visitors in their communities. This core value binds us all together on the journey to becoming “smart.” Ultimately, it all comes down to public service—using technology to best serve the public by making the best use of resources available to us.

Having discussed the positive impacts of the Municipal IoT and why you, dear reader, should care, the Blueprint will now provide an overview of the current state of The Municipal IoT, including findings from our research and a thorough discussion of how Municipal IoT will become ubiquitous and highly available in the future, which is not today.

Figure 2 - Impacts of Municipal IoT

2. Considerations for Deploying Municipal IoT

Deployment Considerations

Perhaps the most fundamental decision government agencies will make regarding IoT networks is how the IoT network will be built and what the business model and ownership structure will be. The current consensus is that there will likely be two primary paths for IoT network deployments, with a third, less ubiquitous option serving as a "catch-all" classification for anything that does not squarely fit within the first two.

Build and Own Model

This first model would occur when a government agency develops specific requirements for an IoT network and then enters into a contract with a firm to build a network to those specifications (likely following some form of competitive bidding process). This generally happens as a capital improvement/public works project, though it could take on another form. It could be funded by general funds, reserves, bonds, monies from tax revenues, a loan, or other revenue sources available to the agency. The key distinguishing factor in this arrangement is that the government agency would pay for the entire cost of construction and installation of the network and would then own the whole system once it was completed.

In the Blueprint we refer to this model as "Build and Own Model" – a government would pay to have a network built and would own the system after it was installed. There are several advantages to the Build model. Namely, the ongoing operating expense would presumably be lower, and the government would not be constrained on how it could use the network. For instance, if it decided to lease access to other providers, it could. On the other hand, if it decided to deploy a new service on the network, such as a parking application in addition to an existing street light application, there would be no associated new service costs to do so, beyond the costs to develop said new application. However, the tradeoffs are the high capital costs, the ongoing operating costs, and the engineering skills required to maintain and further develop the network and related services (although in many cases, the operations and maintenance of the network may end up contracted out).

Subscription / 5G Model

The next model is more straightforward. Soon, it is widely assumed that regional and national cellular firms, such as AT&T, Verizon, and T-Mobile, will introduce IoT network services, such as Cat-M, NB-IoT and LTE-M. In fact, research data from Ericsson in April 2018 suggests that 70% of cellular providers will focus on "Cellular IoT" (i.e., IoT delivered over cellular networks).[4]

This strategy is closely tied to the rollout of 5G networks, which are believed to deliver many benefits over traditional 4G networks, including gigabit speed, low latency, and better indoor

[4] https://www.sdxcentral.com/articles/news/ericsson-70-of-service-providers-will-focus-on-cellular-iot/2018/04/

coverage.[5] Furthermore, new capabilities in 5G such as network slicing, automation, and software-defined networking are presumed to enable the business model for cost-effective IoT subscription plans.[6]

From a deployment standpoint, 5G is widely expected to be deployed using "small cell" technology; that is, small radios that will provide higher speeds than 4G cell towers, but most be closer and in greater quantity to achieve the same coverage levels.[7] In many cases, cellular service and infrastructure providers are working with municipalities to develop agreements to deploy small cell technology.[8]

Meanwhile, cable companies such as Comcast as working on their own IoT network services, such as MachineQ (based on LoRaWAN).[9] Hence, it follows that at some point in the near future government agencies will be able to subscribe to these IoT network services in the same manner that they do cellular plans for mobile devices today. The cellular companies would construct and own the IoT networks and government agencies would procure services from whomever they preferred to on the open market.

In the Blueprint, we refer to this as the "Subscription / 5G Model" – a government would buy IoT network service from a company and pay a subscription fee on a recurring basis (this is conceptually identical to how LTE cellular data service is sold today). The advantages of this model are the sheer ease of deployment, elimination of any upfront capital costs, and lack of need for ongoing maintenance and engineering teams. However, the trade-offs are that the recurring subscription costs would presumably continue to increase over time, while subscribers to the network would be restricted to whatever terms cellular firms allowed under their contracts. For example, deploying a new service might require an additional contract and/or set of fees, while collaborating with a local agency or another firm might be barred altogether.

Other Models

Another model, for lack of a better term, is "Other" – this is a model that does not align well with the Build and Own or Subscription / 5G models. Although this sounds broad, in practicality, the form it would likely take on would be some sort of a Public-Private Partnership. One example of this model would be a private sector firm agreeing to provide some or all of the capital costs to build the network in exchange for the ability to monetize the network somehow; perhaps the government agency would become an anchor tenant. However, this would be a hybrid approach in which the agency would have far greater say over the technical specifications and design of

[5] https://www.ericsson.com/en/about-us/india/authored-articles/5g-and-iot-ushering-in-a-new-era
[6] https://www.networkworld.com/article/3268668/5g-to-become-the-catalyst-for-innovation-in-iot.html
[7] https://www.pwc.com/us/en/industries/tmt/library/5g-small-cell-revolution.html
[8] It should also be noted that a 2018 FCC order that limits local control over deployment of small cells within municipalities is, as of July 2019, the subject of a lawsuit in the Ninth Circuit Court of Appeals. Policies for small cell deployments and agreements are outside the scope of this Blueprint.
[9] https://corporate.comcast.com/press/releases/comcasts-machineq-enterprise-iot-service-announces-next-wave-of-customers

the network, as well as the engineering and development of new services and applications in the future. In this way, the agency would have a custom IoT network, but would not own it.

Another model could be where a government agency designs, develops, and has constructed a network but then develops a revenue model to lease service to local firms in an IoT economy. Because it is impossible to know, a priori, what models might emerge in the future this model, which we refer to as the "Exotic Model", is used as a catchall for anything that does not fit squarely into the others.

Regardless of which model a government agency decides on, there will be many considerations that should factor into the decision. There is no right or wrong answer and this Blueprint does not proclaim to make a determination of superiority; these decisions are fully a matter of local control. What the Blueprint does stress is the importance of making the decision with clear eyes and a good grasp of the trade-offs inherent with the decision.

This should in no way be considered an exhaustive list of possible models. There are likely many other things that municipal leaders will have to contend will face before, during, and after their IoT networks are deployed. A primary takeaway of this Blueprint is that it is crucial to have the right mix of staff at the table right from the start to ensure every aspect is covered. Cross-functional teams, including key decision makers from public works, information technology and innovation, planning, legal, executive management, technical commissions, citizen's advisory committees, and elected officials should be created to manage these deployments to increase the odds of success.

Security Considerations

Security was an afterthought in much of the early IoT system designs. However, recent events have awakened the industry to the critical need for multiple levels of protection across the entire IoT value chain. By 2020, it is expected that 25 percent of cyberattacks will target IoT.

IoT devices pose unique security challenges to municipalities (who assume the role of a service provider in some cases) in order to operate their networks. The low-cost, low-complexity model of most IoT devices means manufacturers have little incentive to add security functions, and the devices are unlikely to have sufficient processing capability to support any endpoint security application. Most IoT devices are intended to minimize human interaction, or are deployed in remote or inaccessible locations, so they are physically less secure and not under direct observation. This means that any misbehavior may go unnoticed for some time. With the millions of lightly secured devices expected, municipality networks are vulnerable to signaling attacks and other DDoS attacks targeting network elements. Preventing, identifying and remediating infections of IoT systems and devices has become critical to network availability and the goals of IoT cost-reduction/service-enhancement.

Fully protecting IoT requires multiple levels of protection across the entire IoT value chain. Instantly detecting malicious activity and blocking suspicious traffic, as well as enforcing other safeguards are the fundamental security requirements. Continually monitoring command & control (CC) traffic traversing the network for device-to-controller conversations is critical; determining which are permitted and which are outside the allowed or expected. Automatic containment is a necessity, since an infected device or controller can quickly infect the entire system. Often the goal of the attack is not the location of the penetration; it just happens to be the easiest point of entry. Therefore, monitoring and automatically prohibiting any non-sanctioned lateral movement among IoT systems is paramount to stopping the spread of an attack toward the intended goal.

Additionally, defining a baseline of IoT expected behavior (protocols, ports, communication frequency, common endpoints, etc.) is critical to understanding when the IoT infrastructure is not behaving as expected and has been compromised. Behavioral network analytics are the norm for the human user, and just as important for IoT devices. As IoT solutions spread and grow, automated identification and protection against malware, often driven by automated attacks, is the best defense.

These principles are encompassed within the Zero Trust model of security. Zero Trust promotes "never trust, always verify" as its guiding principle. With Zero Trust there is no default trust for any entity — including users, devices, applications, and packets — regardless of what it is and its location on, or relative to, the service network. By establishing Zero Trust boundaries that effectively compartmentalize different segments of the network, one can protect critical intellectual property from unauthorized applications or users, reduce the exposure of vulnerable systems, and prevent the lateral movement of malware throughout the network.

Editor's Note: The topic is expanded in the Cybersecurity & Privacy Section

Regionalization and Interoperability

Another important consideration, which was touched upon in the Smart City framework discussed above, is the idea of regionalization. A regional, collaborative approach can be immensely helpful when first entering the smart technology space. Bringing other municipalities into the conversation to share resources not only helps lower costs, but also ensures innovation does not stop at city borders. Housing, traffic, mobility, and environmental issues do not stop at lines on a map. Regional problems thus require borderless solutions. This approach can also provide an area with a competitive edge. In many communities, people may work, shop, and live in different cities; ubiquitous technology access and solutions need to travel with residents and visitors as they move about throughout their days. Who would not want to shop in the area with a smart parking app to make parking easier? With smart trashcans that are emptied when needed and will never overflow? With air quality sensors providing the knowledge needed to prevent a child's asthma attack? Municipalities should work together on solving these challenges, if not out of the goodness of their hearts, then simply to prevent residents and visitors from taking their tax dollars elsewhere.

However, like any multi-jurisdictional approach, such regional efforts could be fraught with challenge. Some agencies may not buy into the model or may disagree with a technical or operational decision; procurement and maintenance agreements would need to be drafted among multiple agencies, requiring significant amounts of staff and legal time. These delicate negotiations would need to be driven with buy-ins from the very highest levels of local and regional leadership.

If such an effort failed to materialize, in the very least agencies could develop data-sharing agreements and interoperability standards. In this approach, agencies might use different vendors and solutions, but the applications and services operating on the underlying IoT networks could be developed in such a way that data users and devices could roam seamlessly between the different networks. This may not be practical, in which case basic data sharing agreements would allow the data – decoupled from the IoT network itself – to be shared between agencies. Of course, this would require data frameworks to ensure that unprocessed (i.e., raw) could be processed and interpreted by other agencies.

Civic Engagement & Privacy

As agencies embark on IoT network efforts, there are still yet other factors to consider. For one, there is the matter of resident reaction and engagement. Residents may have a number of concerns ranging from privacy, security, and possibly even health concerns over the radio signals emitting from wireless devices. Agencies must be prepared to deal with these. Related to this is a matter of aesthetics and neighborhood character. Agencies may want to consider adopting aesthetics guidelines to ensure that IoT networks and devices are consistent with the look and feel of their communities and do not contribute to urban blight. For agencies with open data policies, it will be important to think through how the data generated by IoT networks will be made available to the public. This is extremely useful for communities where citizen engagement through technology has become an influencing trend.

Smart Communities Framework

While this Blueprint, by and large, focuses on IoT networks, it goes without saying that the outcomes Smart Communities hope to achieve such as: improved public safety, transportation, broadband connectivity and bridging the digital divide, economic development, sustainability and energy management, and delivery more and better digital services to their residents are, ultimately, what matter most. As such, this Blueprint provides a framework for Smart Communities in Figure 1 below with the IoT and connectivity networks underpinning it.

This framework starts with upper “horizontal” bands, which sit atop various “vertical” domains, themselves typically managed by separate divisions and departments within the organization. These horizontal bands introduce a focus on **Regionalization** (more fully delineated above) and the **Organization** itself, specifically the leadership and management decisions regarding how it structured and develops the *capacities* of innovation, resilience, efficiency, and sustainability.

The last upper horizontal band is **Data and Analysis**. This is, arguably, the most critical aspect of the framework. IoT networks will generate data on many elements of civic life previously unavailable. Thus, how these data are managed are critical to the promise of Smart Communities being fully realized. *Who owns the data? Who can analyze it? Is the data transferrable and stored in industry standard formats? It is proprietary? How is privacy protected and managed? How is the data secured?* These are questions of substance, which carry important policy considerations.

These upper horizontal bands are followed by "vertical" bands; the domains spoken of previously, such as: **public safety, transportation, broadband, inclusion, engagement, economic development, energy and waste management, environmental sustainability, and digital services**. These represent the most common domains, though there are doubtless many others. Software applications typically reside *within* these vertical bands and it is here that improved outcomes are achieved; hence, they are the most visible. *However, the premise of this framework is that those outcomes are not possible or, in the very least, are far less probable in a context where the horizontal elements are not aligned with the goals within the domains*.

Finally, underpinning these are the lower horizontal bands, **Connectivity Networks** themselves, which must be **Secure and Resilient**.[10] (This Blueprint is focused on these lower two bands.) Wrapping everything is **Vision & Execution and Knowledge & Insight**, which create a cycle so that the entire framework can continuously improve and deliver results.

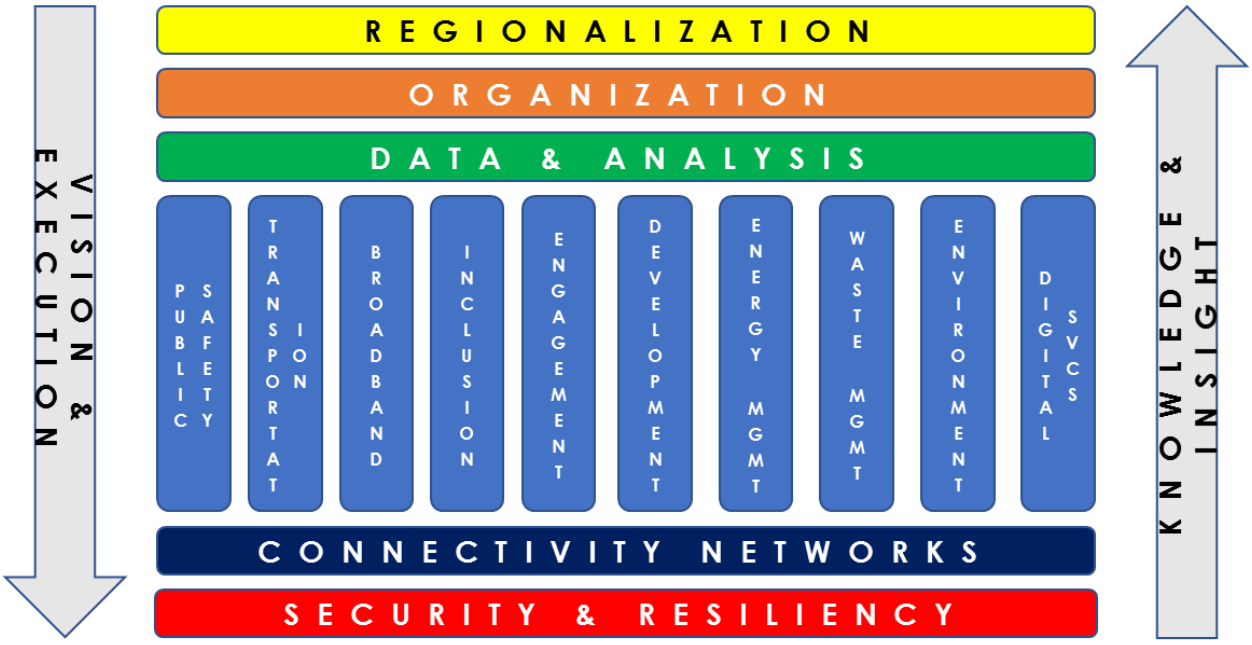


Figure 3 - Smart Community Conceptual Framework

[10] Connectivity networks can include, but are not limited to: fiber optics, wireless and cellular networks, Ethernet, etc.

3. The Current State of Municipal IoT Deployments

The authors of this Blueprint conducted an online survey of municipal government officials in January 2019 with the goal of finding out information regarding the current state of the municipal IoT deployments.[11]

The results support the notion that government officials believe municipal IoT will be extremely impactful; **an overwhelming majority of respondents (89.2%) agreed, "municipal IoT will have a significant impact on your organization now or in the future."**

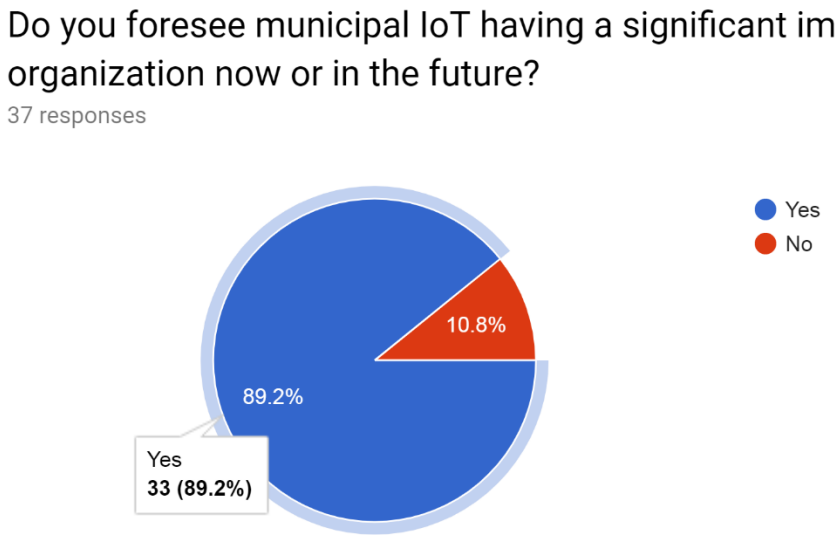


Figure 4 - Will IoT have a significant impact?

Further backing up this finding, the Center for Digital Government, in an article published on November 9th, 2018 presenting data from its 2018 Digital Cities survey, cited that 92% of respondents of their survey stated that the "IoT is impacting city strategic plans," representing a 50.81% increase from 2016 when the number was 61%.[12]

Regarding which functional domains/areas respondents felt will be impacted by municipal IoT, with the optional to select all that apply, the top four domains were, in order:

1. Street Lights (78.8%)	2. Utilities (75.8%)
3. Transportation (72.7%)	4. Public Safety (72.7%)

Notable from the survey was that many other domains also broke the 50% mark. This finding is consistent with the broad impacts of IoT laid out by the authors of this Blueprint in Section 1,

[11] The survey was conducted online and received 37 responses from verified government officials with a breakdown as follows: 73% City/Town; 13.5% Special District; 10.8% County; 2.7% State
[12] https://www.govtech.com/biz/data/Cities-Are-Rapidly-Taking-on-Internet-of-Things-Technology.html

suggesting that government operations across the board will be transformed when IoT networks and related systems become commonplace in government agencies.

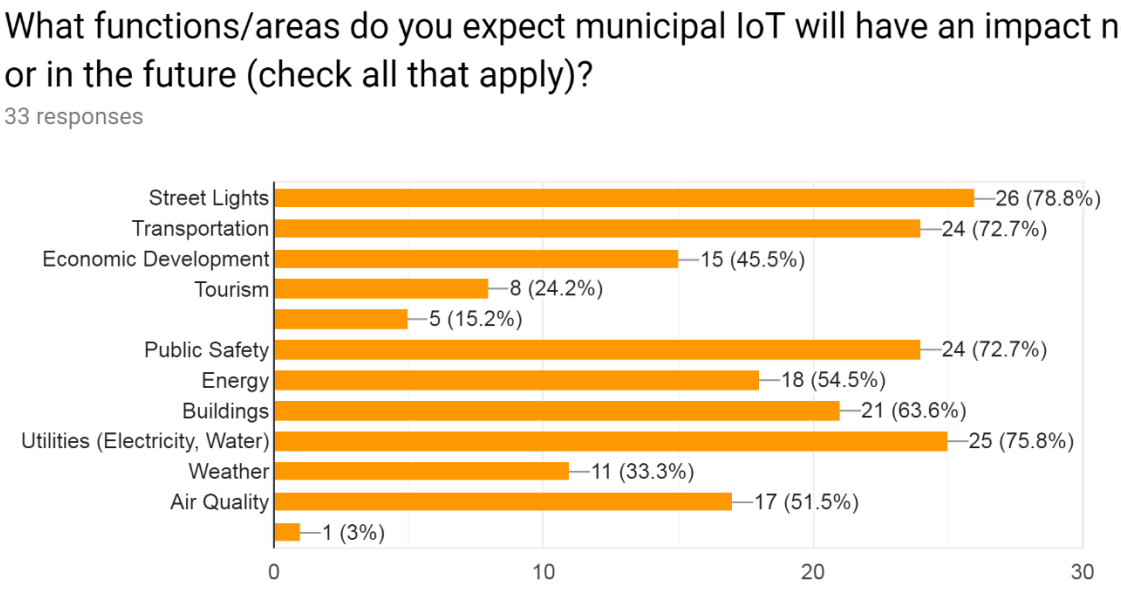


Figure 5 - Which functional areas will be impacted?

However, the data also suggest that IoT deployments at the state and local level are still far from reaching maturity, and as a market, are still in the emerging / early stages of the adoption curve. Regarding the current phase of IoT deployments, 63.6% of respondents of our survey stated their deployment was in the Consideration/Planning phase; 18.2% stated in the Pilot phase; and only 9.1% in the Project Phase.

Put another way, the vast majority of respondents, 81.2%, stated that they were only in the planning or pilot phases. ***This strongly supports the notion that Municipal IoT networks are not widely deployed at this time***.

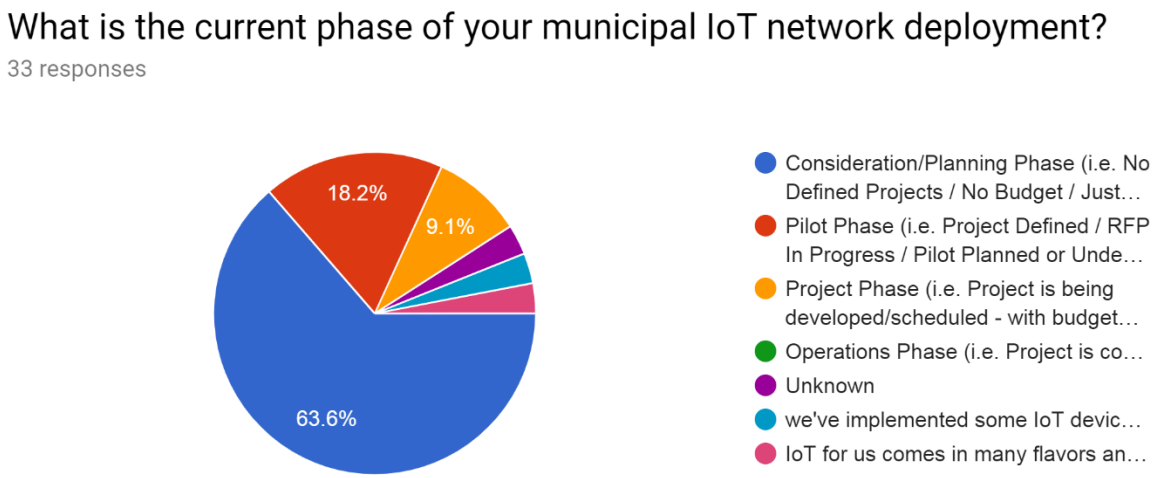


Figure 6 - Current phase of IoT Deployment

Finally, in terms of the timeline for deployment, the majority of respondents, a combined 84.9%, said **their deployments will take place in 2020 or later (i.e., 2020, 2021, or 2022 and beyond)**. This supports the theory that the adoption curve for Municipal IoT will be long and drawn out, lasting for several more years – possibly a decade or more – before reaching maturity and mainstream adoption.

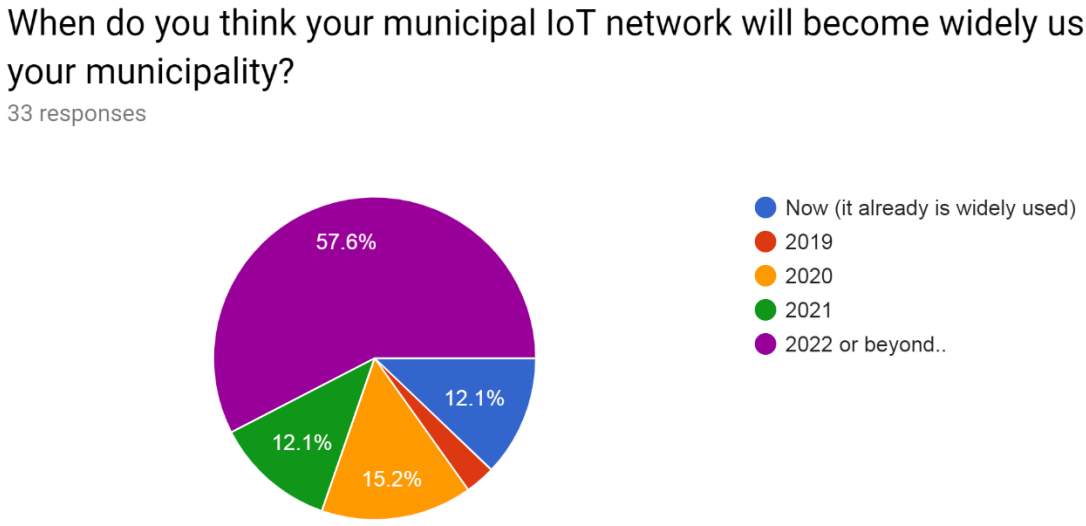


Figure 7 - When will IoT be widely used?

For readers familiar with Everett Rogers' theory of innovation diffusion, which classifies five distinct phases of adoption, these survey results (though the sample size is low), give support to the notion that the Municipal IoT industry is still in the Innovators / Early Adopters phase.[13]

Geoffrey Moore later wrote about the concept of "crossing the chasm" from the Innovators & Early Adopters to the Early & Late Majority, where a technology innovation is considered mature; it is fair to say for Municipal IoT we have not yet reached that milestone.[14] **Figure 8 below depicts these concepts and is a key contribution from this research**.

It should be said that is a process of innovation – governments, researchers, and their private sector partners are working independently, yet as part of an informal, collective system where knowledge is being created, shared, refined, and rewritten. While this research demonstrates that it will take many more years to fully realize the transformative potential of Municipal IoT, learning is undoubtedly occurring already, as the next section will discuss.

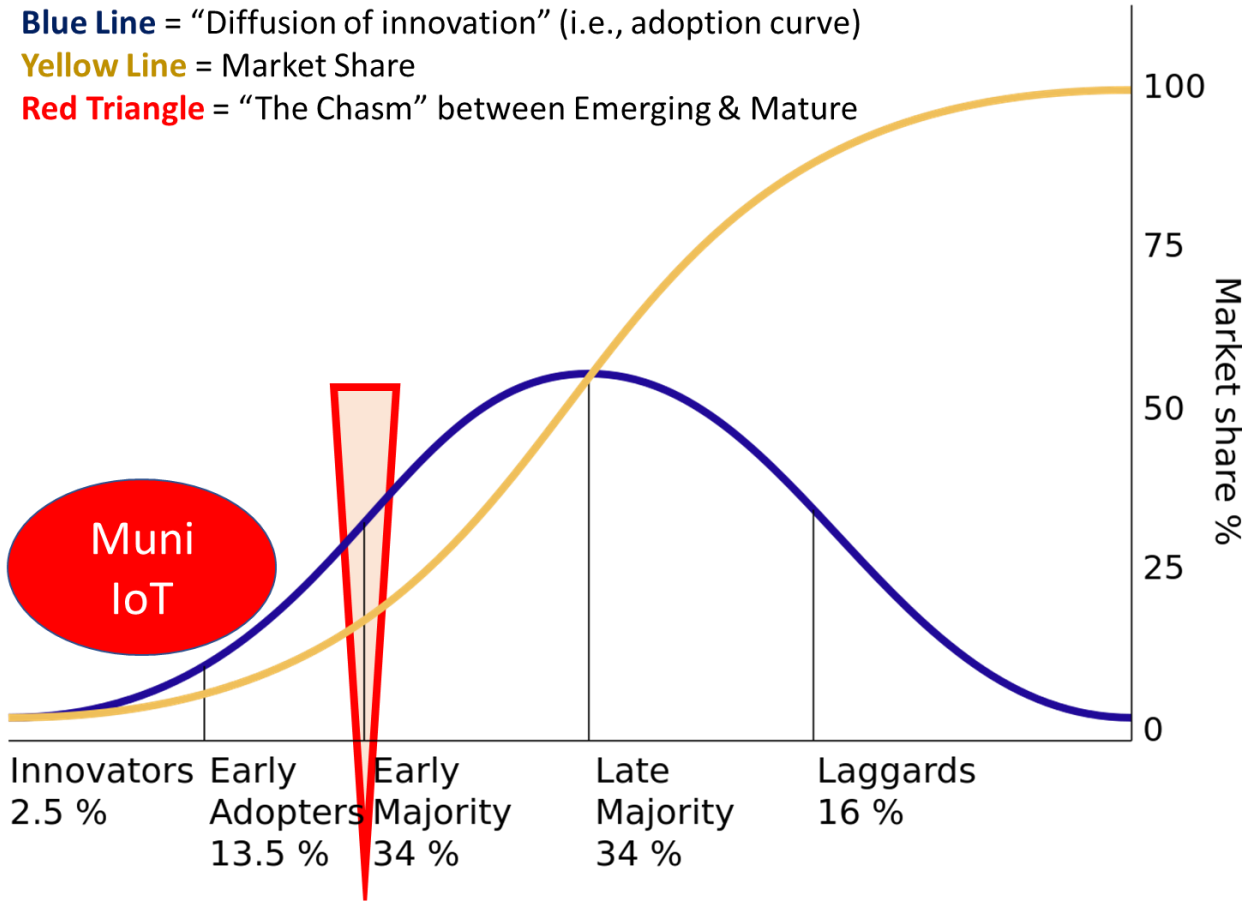


Figure 8 – Municipal IoT in relation to Rogers' Innovation Curve & Moore's "Chasm"

[13] https://en.wikipedia.org/wiki/Diffusion_of_innovations
[14] https://en.wikipedia.org/wiki/Crossing_the_Chasm

4. Case Study Summary Findings & Discussion

Introduction & Methodology

During the development of this Blueprint, the authorship team conducted a series of case study interviews of local government agencies in the United States and Canada known to have deployed IoT networks. The team spoke with the cities of San Diego; San Leandro, CA; Calgary, AB Canada; and the County of San Mateo, CA. Below is a summary of the key findings from these case studies.

Project Structure

The structure of these IoT projects falls into two primary buckets: a) Pilot Projects and b) Production Projects. To illustrate, San Diego and San Leandro both implemented full-scale, citywide production IoT networks initially built for a one use-case, while Calgary and San Mateo County deployed test networks to evaluate pilot solutions across various use-cases.[15]

Pilot Networks

The pilot networks were designed to cover large areas at low costs with no pre-defined solutions in mind. Both projects were developed by the respective Information Technology Departments. These open innovation projects, which involved external partners creating and testing new software on these networks, shared similar goals of **iterative learning, exploration, and experimentation.**

San Mateo County staff developed a test environment it called “SMC Labs” and collaborated with multiple private sector partners to test many IoT network technologies, including LoRaWAN, NB-IoT, and cellular IoT. County agencies were included in an effort to co-create solutions with private sector firms using IoT sensors and networks. For example, SMC Labs has developed and tested solutions for parking, irrigation, air quality, and more.

Meanwhile, Calgary staff deployed a geographically large LoRaWAN system at a very low cost. It’s IT Department began by working with city departments (“business units”) to identify needs and then worked to develop small proof-of-concept projects around those areas. The IT team minimized risk by starting small and iterating. This was deployed with an agile methodology, setting clear milestones, realistic and working to achieve them. They benefited from an existing partnership between the City of Calgary and the University of Calgary, called the “Urban Alliance,” which brought researchers into the program.[16] This led to a successful “smart agriculture” project at the Devonian Gardens, a City-run botanical garden in their downtown core. Through the process of iteration, experimentation, and learning they eventually developed a low-cost sensor for measuring various plant care metrics.

[15] We define “production deployment” as being fully implemented and used day-to-day government operations. This is contrasted with “pilot” or “test” networks, which have no actual government services using them for operations.
[16] https://ucalgary.ca/urbanalliance/

Production Networks

Cities in our research that built citywide production IoT networks found innovative ways to reduce the normally intense capital costs of constructing a production IoT network. San Diego, CA and San Leandro, CA both employed a similar strategy by leveraging an LED street light retrofit project, expected to save their respective cities millions of dollars in energy costs, to "bundle" the construction work with building an IoT network using the same streetlights as mounting locations for the IoT sensors.

Both cities reported that this approach **saved huge amounts of time and money in construction and related costs.** San Diego's project was led by its Sustainability Department, while San Leandro's project was led by its Public Works Department.

In terms of technologies used, San Leandro deployed "smart" street light technology built on a 6LoWPAN IPv6 network, developed by Paradox Engineering (installed by Climatec, a Bosch subsidiary)[17]. San Diego installed IoT sensors developed by AT&T/GE Current, which also use 6LoWPAN over IPv6.[18]

There were some similar lessons learned throughout each project. For example, San Diego identified that it can be worthwhile to have technical staff on-hand during the deployment to test the sensors and tweak them, as needed, and ensure the sensors are working and have proper electrical and communication connections, etc. This can eliminate needing to have crews revisit IoT sensors to perform such tweaks after the installation (thus reducing extra time and cost). Staff also found that using cellular service to connect IoT sensors can be convenient but is also expensive in a large-scale network so, as a result, they are looking for alternative communications methods that do not require monthly service costs. San Diego staff is also engaging with the public over privacy concerns, but this has benefited in having a robust policy drafted that puts these concerns at the fore.

Meanwhile, San Leandro staff discussed the importance of involving technical staff early on to ensure the IoT network design is consistent with a given agency's current IT infrastructure, competencies, and resources. In their example, the 6LoWPAN network required installing IoT nodes on the street lights, along with some 30+ IoT Wi-Fi gateways located throughout the city, all connecting to the city's fiber optic network, by way of traffic controller cabinets where the Wi-Fi gateways connected to Ethernet switches. This connected approximately 4,800 streetlights to a virtual server hosted at the city's data center. As it turned out, this was a major technical undertaking that required several networking components and decisions along the way; as such, having IT involved turned out to be an important factor in the success of the project.

At the same time, the roles of Operational Technology ("OT" – which in San Leandro's case remained with Public Works) and Information Technology ("IT" – which for San Leandro stayed with the IT Department) should also be discussed early on. For San Leandro, the IoT Wi-Fi

[17] https://smartcitysl.com/tag/climatec/
[18] https://about.att.com/story/ge_current_intelligent_lighting.html

gateways became a natural demark where IT transitioned to OT; this provided a framework for support and ongoing maintenance after the network went live. For San Leandro, cross-functional collaboration and informal social networks among staff led to a good working relationship between IT and OT. However, in the absence of strong inter-departmental relationships and trust among teams, operational boundaries should be formally discussed as early in the project as possible.

Conclusion

IoT technologies are still emerging and extremely new ground for local governments. For those who decide to forge ahead and build their own, our case studies outline two distinct paths: a) low cost pilot networks that evaluate applications in partnership with private sector firms; and b) production networks with a single focus such as street lights that can be bundled into larger construction projects that have organizational and political momentum and backing.

For pilot networks, it is important to start small, build the right partnerships (both internally and externally), set the right expectations among stakeholders and learn from each trial. Meanwhile, for production networks, there are huge economies of scale in bundling IoT with other construction projects. However, it is critical to have the right teams involved and develop a "big picture" strategy for how the IoT network can be leveraged for use-cases in the future. *Within* each path, it is important to engage the public and address their concerns as part of the deployment and policy process.

Editor's Note: Full case study reports can be found in Section 7.

5. Practical Guide: Deploying an IoT Network

Introduction

Today's IoT market is already crowded; there is a confusing multitude of IoT connectivity options. However, there are some important ways to distinguish them. For example, some connectivity options operate in the licensed (or regulated) frequency bands, while others operate in the unlicensed or unregulated spectrum. Some options are capable of supporting large amounts of data such as video traffic while others can only transmit very small amounts of data. Meanwhile, some are capable of transmitting over several miles while others are good for a few dozen feet.
While many options in the market today will narrow to a more manageable few in the future (as winner and loser inevitably emerge), the reality remains that there is no "one size fits all" or universal connectivity option that will work for all the different use cases a municipal government will face. In many cases, you will need to have multiple connectivity options operating concurrently.

The purpose of this section of the Blueprint is to provide decision-makers with an understanding of the consideration parameters and a roadmap to guide them through the IoT selection process.

Decision Process

Process overview

Figure Eight shows the high-level view of the key decision steps involved in determining the most appropriate IoT connectivity options. The selection of the connectivity option is based on a number of parameters and considerations, which will differ across municipalities. What may be a feasible option for one may not be appropriate or available for another. As an example, urban centers have more options to work with than in rural areas - mostly due to geographic and topographic reasons. At the same time, rural areas have very specific requirements and applications that require a connectivity option that may not be appropriate for most urban areas.

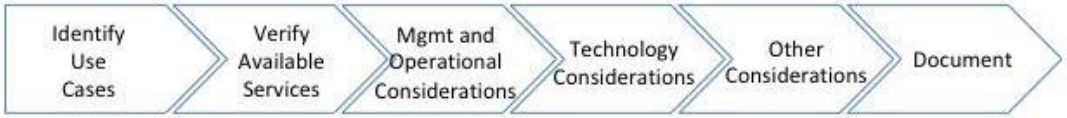


Figure 9 - Six steps involved in selecting the IoT connectivity option

Key assumptions

The IoT connectivity selection process is based on a number of assumptions. These include:

- **Each case is unique**: There is no “one size fits all” connectivity option that works across all different use cases and municipalities. In many cases, the “best fit” option may be two or three options operating concurrently;
- **The “best fit” options are a point in time decision**: What works today may not work tomorrow and, as connectivity options come and go, and the underlying technologies improve, the decision considerations may change;
- **There is no perfect option for any one situation**: The selection process is an exercise in trading off multiple pros and cons of the various considerations; and
- **Not all selection choices are available to all decision-makers**: Sometimes those decisions are made for you. For example, a telecommunications provider may not serve your geographic area, leaving the “Lease Model” described above as a non-starter.

Key outcomes

The connectivity selection process helps planners and decision-makers navigate a complex set of considerations and options. Some key outcomes include:

- **Simplifying options**: One major goal of the process is to filter out quickly the unfeasible or unrealistic options immediately. This helps to efficiently focus resources and attention on the few remaining options;
- **Holistic decision-making**: Even after the filtering process, there may still be multiple options available. The best-fit option is not always about technology and performance. Factors such as ownership, availability, financial, operations, risk, and obsolescence are major considerations that affect which option is selected;
- **Decision-making consistency**: While the IoT drivers, technology, and management considerations will vary, this process provides a fundamental framework that is relevant today and in the future; and
- **Supports the business case**: No matter what option is ultimately decided upon, a justification or business value case is needed. This process provides the inputs and support that can be used in the development of a business case.

Important Considerations

Use case

The IoT use cases, or applications, drive the initial selection of compatible connectivity options. This initial selection is based on four parameters:

1. **Indoor use, outdoor use, or both**? Different connectivity technologies are required for indoor and outdoor applications. There is some overlap in which indoor technology, such as Wi-Fi, can be used for outdoor applications, but only in very limited situations.

2. **How much data is being transmitted and how frequently**? Continuous video feeds required the most bandwidth while messaging data require the least. Device firmware updates fall somewhere in the middle.
3. **How far is the data transmitted?** This can range from a few feet to tens of miles. As an example, air quality sensors in remote locations send data to a base station miles away, while an indoor thermostat only needs to send data to a wireless access point <20 feet away.
4. **Do the devices have continuous access to power?** The more data being transmitted, the more power is required for the device. Devices without access to continuous power, or lacking the ability to recharge internal batteries, are limited to the type of data they can transmit and connectivity options they support.

Connectivity Coverage

Once a candidate set of connectivity options are determined, municipal planners are faced with a couple of questions. These include:

1. Which of these connectivity services are available in the areas or concern?
2. Should I buy these services from a third party telecommunications services provider (i.e., Subscription / 5G Model) or should I build my own (i.e., Build and Own Model) or is there some other option available to me altogether (i.e., Exotic Model)?

In the current IoT market, the geographic coverage offered by service providers is limited at best. While telecommunications service providers are actively rolling out IoT connectivity, they often prioritize highly density, metropolitan cores over less populated rural areas. This is unfortunate, but a reality with which we must content. In addition, not all metropolitan areas are served with the full set of IoT connectivity options. Some areas will only have one option, while other markets may have multiple options, such as NB-IoT and LoRaWAN. Finally, even if IoT connectivity service is available in those areas, there may still be coverage gaps *within* the service area, as service providers may choose for operational or economic reasons not to cover certain areas.

Although the Subscription / 5G Model of utilizing telecommunications operator services will likely be the expedient option for many municipalities, there are situations where the Build and Own Model of designing, procuring, building, and maintaining their own connectivity network may ultimately be a better long-term option. These situations include:

1. The desired IoT connectivity service is not provided by any service provider, or the use case devices (or “things”) are not compatible with the service;
2. Telecommunications service provider offers partial coverage over the geographic area of interest. A municipality will likely want or require full coverage for the areas not served by the operator;
3. Or, a municipality may want indoor coverage for IoT application and find that building a network is better for that purpose;

4. Municipal connectivity requirements such as mission critical infrastructure, service levels, resiliency requirements, etc. may not met by a telecommunications operator;
5. A municipality may wish to own and operate its own IoT connectivity network for strategic, policy, or economic reasons (e.g., mission critical infrastructure, reduced or eliminated ongoing subscription costs, ability to deploy new services without friction, privacy requirement in place by the municipality, the desire to own and control their own data, etc.);

A very important aspect of the consideration to "subscribe or buy" network coverage, mentioned above, is financial. Municipal leaders and decision-makers must look at the total costs over the lifetime of the network. The total costs comprise the initial equipment and capital costs, the maintenance and operational costs (including people), as well as the projected connectivity costs (associated with provisioning devices onto the network) and in some cases, even the decommissioning costs. Often times, while the capital costs will be much higher, the lifetime costs of building and owning a network can be much lower than leasing service from a provider.

Technology

When deciding between connectivity options, there are a number of technical considerations that must be reviewed. These considerations have alignment to the desired use case, frequency spectrum, security, device support and open versus proprietary networks.

Alignment to Use Case.

For every use case or application, there are multiple connectivity options available. Take the example of selecting IoT connectivity for a municipal outdoor air quality sensor network deployed around the community. The amount of information that is transmitted is small (bits) and relatively infrequent (every 15 minutes). There are several feasible connectivity options for this application - NB-IoT, LoRaWAN, and SigFox. However, these options are not the same and have different implications for other (and future) applications that want to use this same connectivity network.
These options have different data throughputs, upload/download speeds, range or distance coverage in urban environments, and so on. For example, SigFox has a different throughput up from and down to the device. This asymmetric throughput means that it is not ideal for those cases where the device requires a signal, nor is it possible to update firmware on a device. While the other options have higher data throughputs, they suffer from other constraints. The point here is that there is no "right" or "wrong", and no "one size fits all" option. The main consideration here is to look deeper at a few of the parameters that matter to understand what the performance capabilities are between the different connectivity options, even if they are initially feasible for a particular set of use cases.

Licensed and unlicensed spectrum operation

IoT connectivity options operate in either the licensed or unlicensed frequency bands. Federal agencies, such as the FCC and NTIA in the United States, specify what frequency spectrums

licensed and unlicensed connectivity options in which to operate. Telecommunications companies offering connectivity in the licensed bands must apply and pay to use part of the frequency spectrum over a specific geographic area. In contrast, the unlicensed frequency bands are open to everyone, and no application and no payment is required to operate. For example, if a municipality wishes to operate their own network, they can do so in the unlicensed spectrum without having to apply to the FCC and pay for the right to operate in this spectrum. Note that service providers (including municipal operators) and equipment designed for use in the unlicensed bands must still adhere to government regulations on frequency and transmission power. Table 1 lists some of connectivity options that operate in the licensed and unlicensed bands.

Licensed Spectrum	Unlicensed Spectrum
Cellular 2G/3G/4G Cellular 5G CBRS (Priority Access Licenses - PAL) LTE Cat M1 NB-IoT	Wi-Fi Bluetooth ZigBee Z-Wave LoRaWAN SigFox CBRS (General Authorized Access - GAA) 6LoWPAN

Table 1 - IoT connectivity options in the licensed and licensed spectrums.

The main advantage licensed band connectivity has over unlicensed band connectivity is that potential interference is greatly minimized, and in cases where interference occurs the licensee has the ability to assert claims against the sources of interference. As licensed operators in the same coverage area are operating on different frequencies, there is little likelihood of their networks interfering with one another. This is important for applications that are mission critical, latency or time sensitive, as well as those requiring high uptime or availability, such a broadband network service being sold in subscription models (i.e., retail cellular plans). However, in order to have such reliability, the licensed band carries a steep cost in fees to the FCC for the right to order to operate in these bands. For example, a 2017 Federal Communications Commission auction raised nearly $20 billion from commercial entities seeking leases of licensed spectrum.[19]

In contrast, the unlicensed band is open to anyone and everyone, with no consideration for aligning frequency occupancy, and future interference is a possibility. For example, Wi-Fi, microwave ovens, Bluetooth headsets, baby monitors, and smart meters all operate in the same 2.4 GHz spectrum. Each new device added increases the likelihood of interference, which could cause signal degradation and possibly result in some devices failing to connect altogether. This interference, then, can clearly impact the operation of the applications utilizing the connectivity service and require more network tuning and controls to operate together.

[19] https://www.reuters.com/article/us-usa-wireless-auction/fcc-spectrum-auction-bidding-ends-at-19-6-billion-idUSKBN15P2QF

Thus, despite the higher risk of interference and greater need for network maintenance, municipalities wishing to operate their own IoT connectivity networks are more likely to look at unlicensed options, solely because of the financial viability of them over licensed spectrum.

Security

All connectivity options incorporate security measures in one form or another, such as encryption, key management and authentication. The specific approaches to security may vary. For example, some IoT connectivity options build on top of the open standards (e.g. LoRaWAN) their own protocols to create their own "proprietary" version with security that is more robust. While it is beyond the scope of this section to compare and contrast the security approaches of each connectivity option, the security consideration is one that must be examined at both the connectivity level, as well as "end to end" (device to gateway to cloud). This is particularly important for mission critical and other applications where availability of services is important. One common approach is to have multiple IoT networks with mission critical applications on a more secure connectivity option, while general purpose and non-critical applications are transmitted through another option.

Editor's Note: This Blueprint goes into far more detail on this topic in the Cybersecurity & Privacy section.

Device support

While there are multitudes of IoT connectivity options in the marketplace, not all devices can support these options. Some devices have been designed to support a specific connectivity option, while others are more agnostic and support multiple options through changeable radio modules or availability in a number of different connectivity models.

IoT based controllers for the remote monitoring and management of streetlights are examples of devices that are designed with a single connectivity option. While different controller manufacturers use different connectivity options, most of these solutions do not yet offer multi-connectivity options. In this case, buying from one manufacturer locks you into a particular connectivity option.

In the ideal situation, the connectivity option selected should support as many different devices and use cases as possible (and reasonable) in order to maximize the use of the network. However, it is not always practical to do so. There will be instances when you have a specific connectivity option and limit access to that network. These instances include:

- Municipal IoT applications (parking sensors, air quality, etc.)
- Mission critical municipal IoT applications
- Pilot and experimental, non-production ready IoT applications

Open versus proprietary connectivity

Connectivity options can be based on open standards or proprietary technology. Open standards are those defined by key participants within the industry. Each has its own set of advantages and disadvantages. The needs of each municipality are different and will determine what is most appropriate (and available) at that particular point in time. Planners should not look at open versus proprietary consideration as a “right” or “wrong,” but rather from a “more right” or “less right” perspective.

Options based on industry standards provide a measure of flexibility, ensure maximum interoperability with compatible devices, and do not lock you into a particular solution vendor for service and hardware. Often, community-based development structure, such as open source software, provides continuous updates, innovative capabilities and enhancements faster than any one vendor can do on its own. In addition, free access to the technology increases the pool of experts, developers and support resources that you can potentially tap into when the need arises. However, open standard based options may not work in every situation. You may have IoT applications that have very specific or unique requirements, such as security, that are or have not been incorporated into the standard. You may have mission critical applications in which require robust and dedicated engineering support that you cannot get from a consortium. There may be a proprietary technology that comes packaged with vendor or third-party support, giving you lower risk and liability. At the same time, your municipality may not have the expertise to support an open standard and thus may prefer a proprietary, vendor-backed alternative.

Proprietary connectivity may incorporate approaches that may work better than the current open standard based technologies for security, latency and throughput. Solution creators of these technologies may provide a more robust level of customer and technical support. Depending on the technology, some proprietary connectivity solutions have an ecosystem of third-party devices and applications that support their technology. In other cases, municipalities may have limited options if they want to use a particular device (e.g. smart water meters) that only works with a particular connectivity technology.

Maturity

There is a wide variety of IoT connectivity options in the marketplace today; however, they are evolving, with some more mature than others. The technology will continue to evolve as IoT evolves, new use cases and applications emerge, and more and more devices connect to IoT networks. While there is not a single “one size fits all” connectivity option, there is likely to be some consolidation around a smaller set of connectivity options in the future. For example, LoRaWAN may gain widespread adoption in the future, pushing aside other IoT connectivity protocols. IoT connectivity options will lose out due to a lack of market adoption, while some will be regulated to niche use cases and applications, while still others will be superseded or consumed into others through mergers and acquisitions. Given how early on we are in the marketplace today, it is not in the scope of this document to predict winners or losers. Rather, this document advises decision makers to consider the technology maturity of these options, as well

as to devise a future-proofing strategy to mitigate the risks associated with incorporating some of these IoT connectivity networks into municipal operations.

Management and Operations.

Network management is an important consideration for municipalities. This consideration is somewhat simplified for municipalities that elect to use the Subscription / 5G Model (i.e., connectivity services provided by telecommunications operators).

For municipalities that are deploying all or part of their own network in some form of the Build Model, the management and operation of this network will be an important consideration. There are three emerging management models:

- Network is owned and managed by the county, or by a regional agency, with connectivity services are provided to the municipality
- Network is owned and managed by municipality
- Network is owned by the municipality, but management is outsourced to a third-party operator on behalf of the municipality

Many municipalities own and manage their own public safety communications networks. They own communications infrastructure, including radio towers, fiber optics, wireless and antenna infrastructure. They have an internal organization and resources to manage this infrastructure. Municipalities that have this capability should assess the feasibility of incorporating IoT connectivity management into their organization, which may mean training existing Information Technology Staff on new IoT systems, thus adding IoT support to the existing IT Department's roles and responsibilities.

Many smaller municipalities do not own much infrastructure. In this case, their options are to either develop this capability internally, which may pose a difficult challenge, or to contract with a third party (private or public) to manage and operate their network. In some cases, such municipalities may be able to contract with their county or other regional agencies who have this existing capability.

Other Considerations

Beyond the considerations listed, municipal decision-makers need to examine a variety of contributing factors.

Risk

There are a variety of risk factors that should be considered when evaluating IoT connectivity options. These risks include the following:

- **Technology maturity risk**: IoT connectivity technologies are still evolving, and there is a risk that the technology may not evolve, or not be able to adequately overcome technical challenges
- **Market adoption risk**: There is a multitude of connectivity options in the market today. Some of these technologies may not be in the market a few years from now because the technology may not be able to adapt to new use cases, or the market has shifted to other adoptions.
- **Lock in risk**: The IoT applications and devices are locked into a specific connectivity method. This prevents migration to other options in the future, as well as binds the municipality to higher costs and operational risks
- **Financial risk**: Whether you build or buy the IoT network, there is a risk where the costs have not been fully quantified and could exceed initial projections. In addition, there are potential costs associated with switching connectivity options in the future.
- **Operational risk**: Are the right structures, processes and skills in place to support and manage the connectivity option?

Due to the nascent nature of the IoT market, the level of risk undertaken by municipalities today is necessarily higher than the risks will be five years from now when the IoT market is more mature. Municipalities must understand the risks associated with today's IoT connectivity technologies, as well as take an inward look at how much, and where risk can be taken. Once that is known, then one can incorporate this into the final selection.

Financial

There are different costs associated not only with each connectivity option, but also with each of the various management/ownership models. These are detailed in Table 2.

Management Model	**Cost areas**
"Subscription Model" (Use telecom operator provided connectivity services)	● Recurring monthly fees based on # of devices, connectivity time, taxes ● Other fees - integration fees, setup, special service as requested ● Fee may increase each year
"Build Model" (Own and manage IoT network)	● Capital Costs ○ IoT connectivity equipment - gateways, etc. ○ IoT infrastructure - towers, broadband backhaul, etc. ○ Deployment and testing ● Maintenance and management ○ Devices management, provisioning, and upgrades ○ Systems upgrades

	● Operations support ● Personnel ● Decommissioning
“Exotic Model” (Own network, outsource management, etc.)	● Capital Costs ○ IoT connectivity equipment - gateways, etc. ○ IoT infrastructure - towers, broadband backhaul, etc. ● Program management ● Recurring Costs ○ Contractor or vendor fees for deploying, maintenance and device mgmt, support

Table 2 - Management models for procuring IoT network connectivity.

Skills and resources

If using an IoT connectivity service provider (Subscriber / 5G model) is not an option, one major consideration to study is what skills and resources are needed to construct an IoT network on your own. For example, IoT connectivity management requires a variety of skill sets, including; networking, wireless communications, systems and device administration, and security. These skills are not necessarily within the scope and capabilities of existing Information Technology Departments, who are responsible for infrastructure within the city or internal use. However, it is not a far leap to imagine a well-run IT Department with adequate staffing levels successfully absorbing these duties into their current responsibilities. However, additional budget allocations may be required for training, external support, and vendor maintenance to complement IT staff.

For municipalities without a strong or adequately staffed IT department, outsourcing to IoT connectivity management vendors or systems integrators for deployment, testing and management of the network is an option.

A third option, in line with the recommendation of this Blueprint to focus on regional solutions, is to collaborate with either the county, neighboring cities, or other regional agencies to create a multi-agency function that is responsible for managing IoT networks. This shared services center model can be deployed to support multiple jurisdictions. In some cases, the county and regional agencies may have some existing capability that this additional role can be added and funded.

It must also be mentioned that the burden of IoT network management will not fall solely on existing IT Departments. In fact, there will need to be thought given to the Operational Technology (OT) teams and how they collaborate with IT. In many cases, OT will be handled in Public Works Departments, by technicians and engineers responsible for functions such as streetlights, electricity, transportation and traffic, and roads. For public safety systems, there may be OT staff working within the Public Safety Units. For example, OT teams may be responsible for connectivity and performance of edge devices, while IT manages gateways and servers. This

relationship between IT and OT will be critical for the success of IoT networks and should be expressed in formal operational guidelines.

Connectivity Option Selection Process

Step One: Initial connectivity selection

A major part of the connectivity selection occurs in the initial use case classification. By properly identifying and classifying the use cases against four parameters, a majority of the connectivity options can be eliminated immediately from consideration. This allows a majority of the effort to be spent on evaluating the remaining options.

This is a straightforward four-step process. You start with the full set of available connectivity options. After each step, the candidate list of potential connectivity options narrows. The list that remains is discussed in the next section.

- Step 1: Determine if applications are indoor, outdoor, or both (Table 3)
- Step 2: Determine whether the applications require high bandwidth or not (Table 4)
- Step 3: Determine how far the devices must communicate are from the transmitter (Table 3)

Range	Indoor	Outdoor
Short (30 ft.)	BT, BTLE	
Medium (300 ft.)	Wi-Fi, ZWave, ZigBee	Wi-Fi, ZigBee, AMI
Long (miles)		Cellular - 2G, 3G, 4G LTE Cellular LPWAN - NB-IoT, Cat M1 Unlicensed LPWAN - LoRaWAN, SigFox, etc.

Table 3 - IoT network connectivity options for indoor and outdoor applications.

Application	**Examples**	**Characteristics /bandwidth**	**Indoor**	**Outdoor**
High bandwidth	Video		Wi-Fi	2G, 3G, 4G LTE Wi-Fi
Medium bandwidth	Audio/Voice		Wi-Fi, ZigBee, ZWave, BT	Wi-Fi ZigBee
Low Bandwidth	Sensors		BT, BLE	NB-IoT LTE Cat M1

				SigFox LoRaWAN

Table 4 - Suitability of IoT network connectivity options for IoT applications.

Step Two: Verify Available Connectivity Services

With the list of options generated from Step One, we now proceed to the next set of decisions. This step is concerned with making a decision on whether to use the Subscription Model (i.e., third party telecommunications operator provider IoT connectivity services), or the Build Model (i.e., provide your own network). For this, we refer the reader to earlier sections that discussed the pros and cons of each model.

Table 5 (below) is used to determine what service is available from a commercial service provider. While this is more applicable to outdoor use cases, in some cases IoT connectivity services can cover indoor uses. Contact the service providers to see what providers are operating in your area. Service can be offered by the traditional telecommunications carriers, broadband internet service providers, and a new generation of IoT connectivity providers. Complete Table 5.

Provider name	IoT connectivity service provided	How much of your service area is currently covered (view coverage map)	If no or limited coverage, when will coverage be available?

Table 5 - Template table for documenting availability third party IoT connectivity in your area.

Note that in your area, you may have one or more service providers offering coverage. Conversely, you may have none. However, based on the information collected, this will allow you to begin to answer the following questions:

- Of the list of the IoT connectivity options pared down from Step One, which ones do a third-party service provider offer?
- How much of the connectivity service is covered in the areas that you are concerned with?
- If not covered, or fully covered, what are their plans to provide the coverage that you need to operationalize your use cases?
- Will the IoT connectivity solution and the service provider meet your use case requirements (see considerations in the Connectivity Coverage considerations?

If the questions are answered satisfactorily, then the option to use telecommunications operator provided services is available to you. While the decision is made to use operator provided services may further simplify the choice of connectivity options, you may still be left with some additional choices to make. In some areas, you may only have one operator for IoT service, and if that is the choice you have, then you have just selected your connectivity option. In other markets, you may have two or three different operators, each providing a different connectivity option. In this case, while you have narrowed down your options from Step One, you must still look at the next steps, including the technical considerations to further narrow down your options.

If the option of using carrier provided services is not available, you still have to have to provide your own coverage and service. However, you will have to continue to select your options based on other parameters in the following steps.

Step Three: Management Considerations

In arriving at this step, we know the following:

- The list of compatible connectivity options based on classifying the use cases to be considered
- Whether the option of using third party provided connectivity services is available to you or not

This step is concerned with:

- If the option to use connectivity services are available to you - should you use it?
- If the option to use connectivity services is not available, how should you deploy and operate this network? In-house or outsource?

If the option to use third party connectivity services is a possibility, planners should answer the following questions:

- Is the connectivity coverage provided sufficient for my use cases now and in the near future?
- If there are gaps in the coverage area in the areas that concern me; does the operator have plans to close those gaps? Are they willing to close those gaps?
- Can the operator provide the level of service, availability, performance and security that I need for my use cases and applications?
- Do my applications or use cases have any special considerations that keep me from using a third-party connectivity network or doing business with these providers? This includes municipal policies, regulations, privacy, etc.
- If I were to not use a third-party network, do I have the budget, capability, resources and management commitment to build my own?

If there is no option (or desire) to use third party connectivity services, or the option is not available (see Step 2), then the municipality will need to build, deploy and manage their own network. In

this case, planners must determine whether the city will do this themselves internally, or to outsource some or all of this to a network systems integrator.

- Does the municipality have the skills and resources to deploy the network?
- If this skill set and resource exists, which department/agency is it in? Is it within their charter to take this on? Are they willing to take it on?
- If the skillset and resources do not exist, or the agency is not willing to take it on, are there network systems integrators that can be contracted to do this work?
- Of the design, build, deploy, operate and maintain, which parts does the municipality want to outsource, and which parts it wants to do itself?
- Does the city have the budget commitment for maintenance and operations moving forward to keep this network going?

Step Four: Technology Considerations

In arriving at this step, we know the following:

- The list of compatible connectivity options based on classifying the use cases to be considered.
- Whether the option of using third party provided connectivity services is available to you or not. If the decision was made to use the connectivity services of a third party such as a telecommunications operator, the list of the original compatible connectivity options from step three is narrowed down even more.
- If the option is not available, we still have the list of options from Step Two.

Not all remaining connectivity options are the same. There are now a number of technical considerations to examine in order to narrow this list down more (in the case that there are still multiple compatible options remaining). This is done by examining a few technical parameters and mapping the fit of the connectivity options against it.

First, complete Table 6 below (leave the weighting column blank for now). A description of the parameters was discussed earlier in a previous section. Some of the parameters are easily determined (e.g. licensed or unlicensed, open standard or proprietary, alignment to use case, device support) by looking at the specifications, while others need a deeper analysis (e.g. security, maturity).

Parameter	Weight (0 to 10)	Connectivity Option One	Connectivity Option Two	Connectivity Option Three
Alignment to Use Case (Throughput/Directionality)				
Licensed or Unlicensed				
Open or proprietary				
Device Support				
Security				
Maturity				
Ranking				

Table 6 - Table Template - Scoring of IoT connectivity options.

With the table just completed, now examine and analyze this table as a whole. This step is about understanding the tradeoffs between the remaining options to see what works best for your individual municipality. One option may have certain parameters that align with your preferences or use cases better than others do, but the remaining parameters may not align as well. For example, you may like the idea of using a connectivity based on open standards, but it operates on the unlicensed spectrum and its security capabilities may not meet your needs as you have a mission critical application. In contrast, another option may operate on the licensed spectrum, but the technology is relatively immature and unproven at scale.

Once the table is completed, the next step is to assign a value to the considerations and to the connectivity options that correspond to each consideration. This is to quantify the differentiation between the options. The underlying principle is that not all considerations are equal. For example, the alignment to the use case may be more important than the licensed or unlicensed consideration, which is more important that the open vs proprietary consideration. Each of these considerations must be assigned a weighting from 0 to 100% with 0 being the least important. The sum of all the weightings (across all the technology considerations) must equal 100%.

Once the considerations are given a weighting, the connectivity options (considerations) must now be given a value. Starting with the “Alignment to use case” consideration row, review each connectivity option against it. Assign a value of between 1 and 5 (with 5 being the best) to each option, taking into consideration how well that option meets your needs for “Alignment to use case.”

Parameter	Weight (0 to 10)	Connectivity Option One	Connectivity Option Two	Connectivity Option Three
Alignment to Use Case (Throughput/Directionality)	W1	C1W1	C2W1	C3W1
Licensed or Unlicensed	W2	C1W2	C2W2	C3W2
Open or proprietary	W3	C1W3	C2W3	C3W3
Device Support	W4	C1W4	C2W4	C3W4
Security	W5	C1W5	C2W5	C3W5
Maturity	W6	C1W6	C2W6	C3W6
Ranking				

Table 7 - Weighting and scoring for IoT connectivity options.

Once each consideration is assigned a weighting (between 0 and 100%), and each connectivity option corresponding to each consideration is assigned a value (between 1 and 5, with 5 being the best), it is now time to score and rank the options. The score of Connectivity options are can be calculated as follows:

- Connectivity Option One Score = W1*C1W1 + W2*C1W2 + W3*C1W3 + W4*C1W4 + W5*C1W5 + W6*C1W6
- Connectivity Option Two Score = W1*C2W1 + W2*C2W2 + W3*C2W3 + W4*C2W4 + W5*C2W5 + W6*C2W6
- Connectivity Option Three Score = W1*C3W1 + W2*C3W2 + W3*C3W3 + W4*C3W4 + W5*C3W5 + W6*C3W6

The Connectivity Option with the highest score then becomes the highest-ranking option, and the one with the lowest is the lowest-ranking option. Note that this is just a score to differentiate between the connectivity options and is used to generate discussion and inform on a preferred option. The final selection is still based on the discretion of the municipality.

Note in evaluating and scoring each consideration and option that there is no one “right” answer - this step is more of an iterative process and making tradeoffs among the remaining options in whole. Each municipality will weigh these parameters differently based on their individual situations, use cases and preferences. What is right for one municipality may not be appropriate for another.

Step Five: Other considerations

In arriving at this stage, you now have an understanding of the various options from a use case fit and technology perspective. You would have ranked the remaining options and may have a preference that will work for your municipality.

This step is to further refine that ranking by examining non-technical parameters, which will create some separation in your rankings.

These other considerations were discussed previously in another section. Similar to the exercise with step four, complete Table 8 below, and update your rankings based on that.

For best results, this exercise should be completed with feedback from various municipal organizations. Unlike the technical considerations in Step Four, these parameters cut across organizational boundaries.

Parameter	**Weight (0-100%)**	**Connectivity Option One**	**Connectivity Option Two**	**Connectivity Option Three**
Risk				
Financial				
Skills and resources				
Procurement				
Ranking				

Table 8 - Weighting and scoring of management considerations.

The ranking and scoring of these options for this table is similar to what was discussed in Step Four.

Step Six: Documentation

Upon completion of Step Five, you would have a ranked list of compatible connectivity options. Some municipalities will be ready to take action, while other municipalities may not yet be ready. Given the very dynamic state of the current IoT connectivity market, some of the decisions made through this exercise may be invalidated over time.

Therefore, it is important that each of the steps will be documented. This includes the key drivers, assumptions, requirements, context be documented so that these can be revisited at a later point in time, when the municipality is ready to act.

If things have changed, it is important to understand the original thinking and context for a particular set of choices, and to confirm those are still valid. If things have changed, on either the connectivity side, or the municipality side, the planner does not have to start all over again.

Examples

Example: IoT sensor network to be deployed in a Large Metropolitan Area

A county is planning to deploy a network of low bandwidth non-mission critical IoT sensors, from air quality, flood monitoring, and asset tracking, in order to increase responsiveness and provide better service to its residents, businesses, agencies and visitors. The county comprises both an urban center, as well as a large rural area. The county is serviced by several network connectivity providers, which offer NB-IoT, LoRaWAN and SigFox.

Step One. Initial Classification

- Indoor/Outdoor Category - The sensor network will be deployed outdoors.
- Bandwidth - sensors use very little bandwidth with each sensor transmitting a very small amount of data every hour.
- Range - The sensors are placed throughout the county, from urban areas to remote rural areas. The location of the sensor can be far away from a gateway or base station.
- Power - some of the sensors are placed out in the field and are remote with no power while others may be connected to a power source. The sensors are that are battery powered and in remote locations that require a relatively long service life of 5 to 10 years.

In this initial classification, using Table 3, we can narrow down the initial connectivity options to those that are long range and outdoor use. This yields cellular connectivity options (2G, 3G, 4G/LTE) as well as LPWAN options (both licensed and unlicensed such as NB-IoT, LoRaWAN, etc.).

Most IoT sensors, such as air quality, asset tracking, etc. are low bandwidth as they are only transmitting a very small set of data. With this understanding, we further narrow the connectivity options down to the low bandwidth options. This yields the LPWAN options such as NB-IoT, LTE Cat M1, LoRaWAN, SigFox, etc.

Step Two Verify connectivity services.

In this step, we want to find out what third party services providers have set up networks that cover this area and document the results in Table 5. If these network services are available, and if it makes sense for the county to use these services instead of setting up a county owned/managed connectivity network, then the connectivity selection process is greatly simplified.

In this example, we know that a few service providers already provide coverage in the county. The example states that NB-IoT, LoRaWAN and SigFox cover the county. A different provider supplies each type of service.

Step Three. Management considerations.

In this step, since connectivity service is available, the planner has to decide whether to use a third party or to build their own.

In this case, while the IoT sensor network is used for county operations, it is not mission critical (on the same level as disaster management or public safety), nor does it contain any sensitive data. In addition, because the sensors are dispersed over wide areas within the county, it would require the county to deploy many gateways to fully cover the areas in which the sensors operate. The services providers already have coverage in the area the county sensors will be. In this case, it makes sense to use telecommunication operator provided services.

Step Four. Technology considerations.

There are still three options available - NB-IoT, LoRaWAN, and SigFox. Now we need to look a little closer and rank the choices. Each of the options will have their own pros and cons, and ranking is a method to normalize between the various options.

We start with completing Table 6 as follows. The security and maturity fields are left blank in this example, as it is left to the reader to investigate and complete. Security is a complex topic, and each option has a different approach to security. Each approach was designed to work specifically with the connectivity service. It is not the intention of this document to appear to endorse one approach over another.

Parameter	**Weight 0 - 100**	**Connectivity Option One - NB-IoT from service provider**	**Connectivity Option Two - SigFox connectivity service**	**Connectivity Option Three - LoRaWAN service from service provider**
Alignment to Use Case (Throughput/Directionality)		• 250 kbps (up and down)	• 100 bps • 140 messages up max per day @ 12 bytes • 4 messages down max per day @ 8 bytes	• 50 kbps (up and down)
Licensed or Unlicensed		Licensed	Unlicensed	Unlicensed
Open or		Based on 3GPP	Proprietary	Open

proprietary		standards		
Device Support		Verify ability to support	Verify ability to support	Verify ability to support
Security				
Maturity				
Ranking				

Table 9 - Example of Technology Considerations table completed.

Upon completion of this table (and the subsequent investigation to complete the boxes), it is time to review and create some separation in the connectivity choices.

The first thing to look at is the alignment to the use case in a deeper level of detail. In this case, we start with the data rates offered by each option, as that is relevant parameter here. IoT sensors are simple devices sending back a very small amount of data on a regular basis (e.g. once or twice an hour). All three connectivity options can certainly support the operation of these sensors, but there are some differences. The SigFox option allows for a very small amount of data to be uploaded and a max number message uploaded per day (140). However, it only allows for a very small downlink. This means that if there is any embedded firmware that needs to be updated via Over the Air (OTA) methods, it would be difficult to do it this way and firmware updates may not be feasible.

For the other two options, the data transmission rate is a couple of orders of magnitude higher than SigFox. This higher data rate may be a bit of an overkill for some sensors, but these other connectivity options provide future proofing and flexibility for other use cases.

The next option to consider is the licensed or unlicensed spectrum operation. The licensed option is designed to mitigate any effects of interference. In a dense urban environment, interference is a major issue than in a rural area. In contrast, the other two options operate in the unlicensed ISM band, and over time as more and more IoT devices go to market, the potential for interference increases.

Finally, we consider the case of open versus proprietary. The real issue in this case is vendor lock in and you can only use vendors that have connectivity that supports this option. This may preclude the deployment of other types of use cases or devices in the future.

Finally, one important thing to consider is whether the devices can support the three options. Some devices will support multiple options, while others will support only one. Look at the sensors and see what networks they can support. If they only support one option, it may be possible to find another vendor that may support the other two options. If not, and if this application is critical, you may have to choose a network option based on this sensor. Beyond the initial set of sensors,

what other sensors and things are planned in the future? This ability to support future sensors and applications are an important consideration for selecting a network option.

Note that not all considerations are equal. In this example, the county planner decides (in collaboration with other appropriate county personnel) that alignment to use case is most important and assigns it a value of 10. The team also decides that device support and licensed/unlicensed spectrum operation are critical and assigns it a value of 9 and 8 respectively. (Note: the weighting in this example are just assumptions the authors made up. In actuality, the planner can assign it whatever number they wish based on internal conversations of what is most important).

Based on the brief discussion, we arrive at the following weightings and rankings below. The score for each option was then calculated

- Option One = 0.35*4 + 0.15*3 + 0.05*2 + 0.20*3 + 0.20*3 + 0.05*4 = 3.30
- Option Two = 0.35*2 + 0.15*1 + 0.05*2 + 0.20*2 + 0.20*3 + 0.05*3 = 2.10
- Option Three = 0.35*3 + 0.15*1 + 0.05*4 + 0.20*4 + 0.20*2 + 0.05*3 = 2.75

Parameter	**Weight 0 - 100%**	**Connectivity Option One - NB-IoT from service provider**	**Connectivity Option Two - SigFox connectivity service**	**Connectivity Option Three - LoRaWAN service from service provider**
Alignment to Use Case (Throughput/Directionality)	35%	4	2	3
Licensed or Unlicensed	15%	3	1	1
Open or proprietary	5%	2	2	4
Device Support	20%	3	2	4
Security	20%	3	3	2
Maturity	5%	4	3	3
Ranking		3.30 (#1)	2.10 (#3)	2.75 (#2)

Table 10 - Example of technology considerations scoring.

In going through this exercise, the goal is to identify which of the technology considerations are most important in the selection of the connectivity option, then use to create separation in the

remaining connectivity options so that you can rank them, and then pick the best one based on that. Based on this, we have the rankings of each option through Step Four.

We did not look at the management considerations for the purposes of this example. These are very subjective, based on needs, experiences, etc. We leave that to the reader. However, this example should give the reader a walkthrough of the connectivity selection process.

Template - Connectivity Selection

Step One: Initial connectivity selection

- Step 1: Determine if applications are indoor, outdoor, or both (Table 3)
- Step 2: Determine whether the applications use a lot of bandwidth or not (Table 4)
- Step 3: Determine how far the devices are from the transmitter (Table 3)

List all connectivity options that are applicable after answering the questions.

Step Two: Verify Available Connectivity Services

With the list of options generated from Step One, we now proceed to the next set of decisions. This step is concerned with making a decision on whether to use third-party telecommunications operator for IoT connectivity services or provide your own.

Complete the form below by contacting telecommunications providers.

Provider name	**IoT connectivity service provided**	**How much of your service area is currently covered (view coverage map)**	**If no or limited coverage, when will coverage be available?**

Table 11 - Contacting telecommunications providers.

Step Three: Management Considerations

If the option to use third party connectivity services is a possibility, planners should answer the following questions:

- Is the connectivity coverage provided sufficient for my use cases now and in the near future?

- If there are gaps in the coverage area in the areas that concern me, does the operator have plans to close those gaps? Are they willing to close those gaps?
- Can the operator provide the level of service, availability, performance and security that I need for my use cases and applications?
- Do my applications or use cases have any special considerations that keep me from using a third-party connectivity network or doing business with these providers? This includes municipal policies, regulations, privacy, etc.
- If I do not use a third-party network, do I have the budget, capability, resources and management commitment to build my own?

If there is no option to use third party connectivity services, or the option is not available (see Step 2), then the municipality will need to build, deploy and manage their own network. Please answer the following questions:

- Does the municipality have the skills and resources to deploy the network?
- If this skill set and resource exists, which department/agency is it in? Is it within their charter to take this on? Are they willing to take it on?
- If the skill set and resources do not exist, or the agency is not willing to take it on; then are there network systems integrators that can be contracted to do this work?
- Of the design, build, deploy, operate and maintain, which parts does the municipality want to outsource, and which parts it wants to do itself?
- Does the city have the budget commitment for maintenance and operations moving forward to keep this network going?

Step Four. Technology considerations.

The four main tasks are:

- Complete the table
- Establish a weighting for each consideration (row)
- Establish a relative rank for each connectivity option
- Calculate the weighted score of each option

Parameter	**Weight (0 to 100)**	**Connectivity Option One**	**Connectivity Option Two**	**Connectivity Option Three**
Alignment to Use Case (Throughput/Directionality)				
Licensed or Unlicensed				

Open or proprietary				
Device Support				
Security				
Maturity				
Ranking				

Table 12 - IoT Technology Considerations.

Step Five: Other considerations

The four steps:

- Complete the table
- Establish a weighting for each consideration (row)
- Establish a relative rank for each connectivity option
- Calculate the weighted score of each option

Parameter	**Weight (0-100%)**	**Connectivity Option One**	**Connectivity Option Two**	**Connectivity Option Three**
Risk				
Financial				
Skills and resources				
Procurement				
Ranking				

Table 13 - Ranking other considerations.

6. Practical Guide: IoT Cybersecurity & Privacy

Chapter Summary

The purpose of the chapter
With the advent of IoT devices and their rapid and wide adoption in Smart Cities, municipalities face an urgent necessity to ensure the IoT-related ecosystems are trustworthy by design. New regulations will no doubt be enacted by the federal and local regulatory bodies in due time, but municipalities face an urgent need for practical guidance for built-in security and privacy protection.

Whom is it intended for
The audiences are municipality policy makers, department heads, innovation officers and strategists as well as technology implementers tasked with building IoT capabilities. Policy makers and administrators can expect to gain a good understanding of big-picture considerations and relevant legal considerations to aid their planning while technology implementers can leverage a set of tools to facilitate their implementation.

What the reader should expect to take away
The readers can take away an easy-to-adopt and one-size-does-not-fit-all approach for municipalities to plan on cybersecurity and privacy needs for IoT capabilities.

Collaboration with other chapters
This chapter may cross-reference the other chapters where appropriate for a seamless reading experience. Convention and general cybersecurity and privacy considerations are available in Global City Teams Challenge: Cybersecurity and Privacy Advisory Committee Guidebook.

I. IoT: Cybersecurity and Privacy Risks

The infamous Mirai botnet pushed IoT security risks on the world stage on October 21, 2016. Initially as a money-making project of three college students, the distributed denial of service (DDoS) stunned the world with its powerful impact: it made high-profile companies such as GitHub, Twitter, Reddit, Netflix, Airbnb inaccessible for hours as well as the backbone of the Internet DNS service provider Dyn.[20]

This IoT devices-centered DDoS was neither the first, nor the last of attacks. In fact, IoT systems can be leveraged to cause damage to all three pillars of information security: confidentiality, integrity and availability.

Another attack at a Las Vegas Casino significantly dented the high rollers' trust and confidential information. [More description: here, here and here]

[20] https://en.wikipedia.org/wiki/Mirai_(malware)

Municipalities suffer more severe setbacks or impacts when security is ignored at even an inconspicuous seemingly unimportant component. The primary cause of the 2003 Northeast blackout was a software bug in the alarm system in an energy company's control room that led to a catastrophic shutdown of the electrical grid, affecting 55 million people.[21] Appendix A offers more types of risks of which all IoT project personnel should be aware.

Similarly, the ubiquity of IoT devices and constantly evolving laws leave much to be desired for privacy protection. The fact that IoT devices are identifiable across more networks further exacerbates the need to protect against unintended sharing of information. Many data points can be correlated about citizens and their households to create profiles of people and places in order to make decisions about them. Since municipalities are expected to serve their stakeholders' best interest, they bear more responsibilities to protect all stakeholders' privacy and do it right the first time. Municipalities with Smart City ambitions and IoT enablement vision ignore privacy considerations at their own peril.

II. IoT: Trustworthy and Resilient through Risk Management

With unprecedented potentials come unforeseeable risks. It is paramount to maintain people's trust and ensure resilient IoT systems. Such a goal is only feasible through risk management, especially in cybersecurity and privacy.

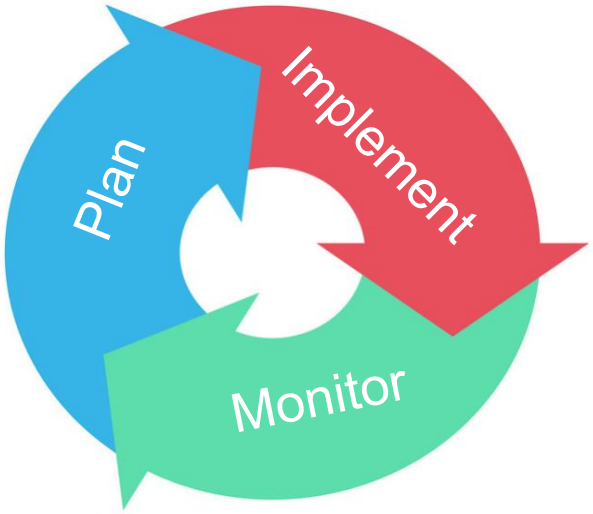
Cybersecurity and privacy risk management is far from an undue burden; on the contrary, any IoT capabilities without designed-in risk management will prove to be costly, prone to disruptions by cyber threats and unsustainable.

[21] http://www.govtech.com/security/Security-Privacy-Governance-Concerns-About-Smart-City-Technologies-Grow.html

Risk management is a mature discipline that ensures the most cost-beneficial outcome for IoT deployment. The Cybersecurity and Privacy Advisory Committee (CPAC) under NIST's Global City Teams Challenge and the Smart Secure Cities and Communities Challenge, has summarized the following lifecycle after combining three disciplines, namely risk management, information security and project management:

1. Plan
2. Implement
3. Monitor

These iterative phases have integrated NIST Risk Management Framework and Cyber Security Framework. The table below depicts the key activities in each phase, as well as the corresponding activities in RMF and CSF. More details are available in CPAC's Guidebook.



Cybersecurity and Privacy Risk Management Cycle

III. Best Practices and Considerations

Best Practices:

- Empower an individual with accountability and resources in early planning
  - This individual will be motivated to adopt best practices wherever available.
- Establish a cybersecurity framework and privacy framework
  - Such frameworks allow the teams to realize fully the benefit of a consistent lexicon and methodologies. Data Privacy is the guiding directive by which we are able to preserve our freedoms, including the freedom to be informed and the freedom to choose.
- Ensure collaboration and transparency whenever possible
  - Approaches that do not integrate across organizational silos have proven not only limiting in capabilities, but also costly. Seek assessment and validation by independent third parties to avoid blind spots.

Technical and IoT-Specific Considerations

- ***Technological diversity and limitations*** – Given the diverse array of technologies in the smart city environment (e.g., IoT devices), selected controls – including common controls – may not be able to be implemented as intended. Factors restricting implementation may include limitations in built-in functionality, processing power, battery life, etc. This may

necessitate significant effort in terms of tailoring security and privacy controls, determining compensating controls, or assessing risk acceptance. Organizations and system owners will need to document how controls are actually implemented and configured and determine whether the residual risk is acceptable.[22]

Wireless Industry Announces New Cybersecurity Certification Program for Cellular-Connected IoT Devices.[23]

NIST teams together with industry leaders have proposed MUD.[24]

- ***Common control challenges and opportunities*** – Collaboration across government departments and agencies can lead to increased efficiency, for example, with the identification and implementation of common controls. However, diversity of technologies, architectures, and infrastructures could limit the feasibility of common controls. Collaboration from policy, governance, budget, and infrastructure perspectives may be needed to maximize the effective implementation of common controls. Establishing, implementing, and maintaining common controls can be enabled by some of the other considerations identified in this document (e.g., leveraging the procurement process, external communications).

- ***Continuous monitoring in highly dynamic smart environment*** – Smart city environments are highly dynamic with frequent changes to the technology environment. Corresponding cybersecurity and privacy requirements and controls will undoubtedly need to be revised, updated, reconfigured, etc. Organizations and systems owners will need to determine the appropriate minimum frequency at which necessary risk management processes will be conducted. This frequency may vary by system security category and impact level, mission, information type(s), and other organization risk factors. That said, the long-term risk management objective is to continue to move towards increased automation and truly continuous (i.e., real-time) monitoring of risk.[25]

---

[22] Additional discussion of IoT and associated cybersecurity and privacy risks and considerations can be found in the following resources: *Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* and *NIST Cybersecurity White Paper: Internet of Things (IoT) Trust Concerns*.

[23] https://www.ctia.org/news/wireless-industry-announces-internet-of-things-cybersecurity-certification-program, August 21, 2018

[24] NIST MUD: https://csrc.nist.gov/publications/detail/sp/1800-15/draft

[25] Indeed, NIST 800-37 Rev. 2 recommends that "Organizations should maximize the use of automation, wherever possible, to increase the speed, effectiveness, and efficiency of executing the steps in the Risk Management Framework (RMF). Automation is particularly useful in the assessment and continuous monitoring of controls, the preparation of authorization packages for timely decision-making, and the implementation of ongoing authorization approaches—together facilitating a real-time or near real-time risk-based decision-making process for senior leaders. Organizations have significant flexibility in deciding when, where, and how to use automation or automated support tools for their security and privacy programs. In some situations, automated assessments and monitoring of controls may not be possible or feasible."

Legal and Liability Considerations

- ***Understand new and/or additional regulatory exposure*** – Depending on the organization(s) and on the types of data being processed by the IoT system, various regulatory requirements may come into effect. For instance, if a system includes healthcare data (e.g., vital sign information from wearable sensors worn by first responders), HIPAA may apply. Alternatively, if a system includes data that allows members of the public to be identified (e.g., video recordings), various privacy regimes may apply, such as GDPR or California data privacy laws.

- ***Risk mitigation through cybersecurity insurance*** – Smart cities can consider cybersecurity insurance as a risk mitigation measure (i.e., risk transfer). Cybersecurity insurance is an expanding and open area of business support/development, and can reduce potential financial loss (i.e., consequence) and thereby reduce total risk. However, insurance would only be suitable for mitigating certain risks (i.e., those that can directly translate into monetary loss). A recent Wall Street Journal survey suggested that a majority of the 25 largest U.S. cities have, or are considering, cyber insurance.[26]

- ***Cautious use of non-disclosure agreements -*** The use of non-disclosure agreements (NDA) should be carefully considered. The municipality may need to share vendor information with external regulatory bodies or even other vendors (e.g., data formats sent by an IoT device may need to be known by packet inspection engines). NDAs should provide enough latitude to enforce the municipality's chosen cybersecurity and privacy risk posture while also respecting vendors' intellectual property and proprietary information. The municipality will benefit from periodic technology audit/risk review assessments, similar to those carried out for financial audits and reviews of banks, financial, and other complex organizations.

US Federal level agencies[27]

Many laws at the US federal level require that information systems protect sensitive data they store or process. Failure to comply with these laws may incur various consequences including stiff fines. In worst cases, data breaches and business interruption are common consequences after a successful attack as in Atlanta City in March 2018.[28]

- Summary of impacts of major laws, regulations and standards; with the list in Appendix D

The Risk Assessment section of the Blueprint provides guidance on the types of risks that might arise when deploying IoT projects in Agency contexts. Risks might be technical, operational,

[26] https://www.wsj.com/articles/more-cities-brace-for-inevitable-cyberattack-1536053401
[27] Eric A. Fischer, Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation, https://fas.org/sgp/crs/natsec/R42114.pdf, December 12, 2014.
[28] FBI investigating cyberattack on Atlanta that involves ransom note, http://thehill.com/policy/cybersecurity/379846-fbi-investigating-cyberattack-on-atlanta-that-involves-ransom-note, BY BRETT SAMUELS - 03/22/18 06:14 PM EDT

contractual, or legal. Mitigations, when available, can take various forms just as the risks can. Everyone involved in deploying IoT projects should be familiar with the contents of the Risk Assessment section.

Risks associated with IoT projects can be thought of as all of the risks of any IT project, and a new set of risks brought on by:

- The presence of networked computing devices at the edge of the network
- New network transports
- Rich data sets traversing the network and being stored in data repositories
- The introduction or expansion of cloud-based IT solutions in the Agency's technology ecosystem

Beyond the technical risks brought on by IoT, there may be operational and organizational challenges related to systems that were previously the exclusive purview of Operational Technology departments or roles now interacting much more closely with Information Technology departments or roles. Departmental communication and training may be advantageous to leverage the potential benefits and address the new risks of such integration.

Risks should be assessed using a combination of evaluating the likelihood of the risk being exploited and the costs resulting from any exploitation.

This section attempts to call out specific risks related to IoT deployments and is not intended to prescribe a complete risk management framework. The Agency should consult a document such as NIST 800-30r1 for an overview of a complete risk management framework.[29]

The appendix to this document includes a Risk Assessment Questionnaire that may be useful in working through the risk discovery process during the system design process.

Considerations – Risk Gaps

IoT projects introduce devices with connectivity and computational power at the network edge. Previously, devices with these capabilities were generally contained within data centers, or other network segments that could be configured for limited ingress/egress and monitored. The deployment of these edge devices might also introduce new network technologies at several layers of the OSI network model. The Agency's existing threat model and risk assessment framework may need to be extended to cover these new system components. Additionally, IoT projects may be leveraging unvetted, or at least immature, technologies or systems with inadequate documentation (examples include the Heartbleed flaw in TLS, KRACK in Wi-Fi, and 802.11R flaws in WPA roaming). This is in addition to the classic risks of IT projects like data stewards, failure to adhere to the principle of least responsibility, improper configuration of data center resources, etc.

[29] NIST 800-30-R1: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Considerations – Costs to Recover

In the event of a breach, remediation might include technical, contractual, and legal effort. The breach should be understood so that future similar breaches can be prevented. Any theft or loss resulting from the breach might require reporting to relevant regulators as well as affected residents and enterprises. The costs associated with such actions should be considered in evaluation the potential impact of a breach.

Considerations – Costs to Implement

Risk mitigations must be considered as part of the overall budget of any IoT project. Some costs may be up-front (e.g., system design reviews, pre-deployment comprehensive penetration testing) and others might be ongoing (e.g., active network traffic monitoring, insurance).

Considerations - Regulatory Requirements

Depending on the Agency and on the type of data being processed by the IoT system, various regulatory requirements may come into effect. For instance, if the system includes healthcare data (vital sign information from wearable sensors worn by first responders, say), HIPAA may apply. Alternatively, if the system includes data that allows members of the public to be identified (video recordings for instance) various privacy regimes may apply (GDPR or California privacy law).

Considerations – System Implementation Insource vs Outsource

As IoT products become more mature, vendors are increasingly able to provide risk documentation and mitigation strategies. Agencies are encouraged to involve vendors in the Risk Assessment process, both for the components the Agency is procuring from the vendor, and to help evaluate risks at touchpoints between components that may come from different vendors, or already exist in the Agency's infrastructure. Use of standard authentication technologies like server certificate verification as part of TLS connections, network mapping and monitoring, and device whitelists for network access will require vendor support and should be built in to system specifications, with attendant contractual terms.

Considerations – Risk Evaluation Insource vs Outsource

Conversely, vendors may not have adequate familiarity with the particular risks and especially their associated costs faced by the Agency. In such cases, it would be prudent for the Agency to take the lead on risk evaluation. Vendors may have information on vulnerabilities in system components that are discovered as time goes on. The Agency may wish to require that vendors keep the Agency informed as vulnerabilities are discovered. The Agency may also wish to require that vendors disclose standard software components that are used in system components so that the Agency can independently be aware of vulnerabilities. For instance, the CERT CVE database of vulnerabilities can be useful.

The use of Non-Disclosure Agreements should be carefully considered. The Agency may need to share vendor information with external regulatory bodies, or even other vendors (for instance,

data formats sent by an IoT device may need to be known by packet inspection engines). The Agency should ensure that any NDAs provide enough latitude to enforce the Agency's security posture.

The Agency may benefit from periodic technology audit/risk review assessments, similar to those carried out for Agency finances. Banks and financial institutions are held to a technology audit/risk review assessment that results in finding reports, so considerations that apply to banks should be considered for the Agency.[30]

Approach – Areas of Risk – Risk Gaps

Special attention should be paid to:

- Interfaces between system components
- Services that may be driven by the data from the system

As an example, consider the BigBelly trash collection system. If someone hacks the BigBelly communications channel and causes unneeded collection truck trips, who is liable for the costs associated with those trips? BigBelly, for making it possible for the trashcans to be impersonated? The telecoms provider for making a channel that an attacker could hack? The garbage service for rolling a truck without verifying the need?

As another example, suppose an eavesdropper is able to listen in on public safety dispatch communications and commit crimes in places far away from current police presence. Encryption can be provided by both the device and the telecoms channel. In general, a philosophy of defense in depth suggests both layers of encryption should be applied. If the two channels are provided by two vendors, and somehow the combination is cracked, who is responsible?

Approach – Technical Attack Vectors

Consideration should be given to encryption of data in transit and at rest. Standard technologies like TLS for sockets over the internet help with both authentication and encryption. Configuration errors can cause these protections to be ignored or not present, though, so verification of correct performance should be included. The transport technology may offer its own layer of encryption (Wi-Fi WPA2 for instance), which should be used. Encryption within encryption is encouraged, and encryption implementations using standard libraries is encouraged. Library versions should be cataloged and tracked with device firmware versions so that if a library flaw is discovered, it can be known which devices are at risk and need to be updated or withdrawn from service.

Unauthorized access to devices is a huge risk. If an attacker can log in to the device, which is higher risk with IoT devices, they can use it for their own purposes, whether that is launching Denial of Service attacks on third parties, mining cryptocurrencies, or accessing the Agency's other IT resources. Network services on the device should be disabled if not needed for the

[30] For more information see, *Bank Secrecy Act*: https://www.occ.treas.gov/topics/compliance-bsa/bsa/index-bsa.html

designated task of the device, all authentication methods should be unique, and any default authentication methods should be changed by the end user at installation/commissioning time.

Network whitelists should be considered. Devices should have unique identifiers like MAC addresses that can be used at the network transport layer to ensure this communication is expected. Whitelists can be applied at multiple touchpoints and will depend on the particular network architecture.

Backend attacks on databases and cloud infrastructure should be addressed through the techniques common to all such IT projects.

System components will almost certainly use standard software components like OpenSSL for TLS and cryptography algorithm implementations, TCP/IP stacks, and Linux, BSD, or real time operating systems. Vulnerabilities in standard software components are often tracked in the CERT CVE database. A list of components used across the system, including version information, is invaluable because it can be compared to the CERT CVE database to ascertain quickly the technical risks.

Approach - Technical Attack Consequences

Any breach of the system, whether at the edge, the datacenter, or somewhere in between, can have a wide range of consequences. Data may be exfiltrated, Agency services may be compromised, Agency resources (included the IoT devices) may be leveraged by an attacker for their own purposes. Telecom or datacenter usage limits may be breached, leading to financial consequences.

Risk Assessment Outcomes

The risk assessment process should leave the Agency with a set of documents outlining the solution architecture, an awareness of the risk vectors for each component in the solution, an awareness of how the solution interacts with other Agency IT assets, and a quantified set of costs to implement the system including risk mitigation, and a quantified set of costs to recover from breaches. The technical documentation (including risk vectors for each component) should be maintained as system components are updated (including firmware updates) or replaced, and as vulnerabilities are discovered in the deployed components. The documentation should include locations of vulnerability listings, like the CERT CVE vulnerability database.

Key Smart City Risk Management Considerations

Operationalizing and standardizing risk management across the organization is critical for minimizing cybersecurity and privacy risks during the development and operation of smart city capabilities and solutions. It will be up to cities and their partners to determine the appropriate risk management policies and processes to adopt and implement based on their current risk management practices, risk posture, and their risk management strategy. While aspects of risk management may seem daunting and challenging, there are certainly opportunities that cities can leverage to their advantage. The following considerations are things that smart city

organizations should keep in mind as they pursue the development and maturation of their risk management programs.

- ***Risk management as a smart city enabler –*** Proper risk management practices and communication of those risk management practices can actually help enable the development, deployment, and operation of smart city capabilities. Risk management should not be viewed as an encumbrance. Proper cybersecurity and privacy controls can help gain public trust and buy-in and promote requisite participation in smart city functions.
- ***Intra-governmental coordination and collaboration –*** Given the interconnectedness and multi-stakeholder nature of smart city capabilities and solutions, successful risk management will require significant communication, collaboration, and coordination between city departments and agencies. This necessitates the development of consensus, modification of existing structures and processes, and consideration of new shared resource and service models.
- ***Public-Private and intergovernmental coordination –*** Smart city systems often involve a mix of assets (e.g., city-owned and operated; regional; commercially-owned and operated). Successful risk management will require sharing of information (including potentially business-sensitive information), coordination of risk management and governance practices, and alignment of organizational and system boundaries.
- ***External communication of risk management strategy and policies –*** It is important for organizations to adequately communicate risk management strategies, policies, and guidance not only to internal departments and agencies but also to existing and prospective external partners, service providers, vendors, and constituents. This enables external parties to understand the risk management environment in which they are expected to participate and also enables capability providers to develop capabilities based on well-established risk management practices (e.g., security and privacy control baselines).
- ***Leverage acquisition and procurement mechanisms –*** Risk management needs to include acquisition and procurement offices and personnel – both in the establishment and implementation of risk management practices. Smart city solutions' dependence on external services and COTS products provides an opportunity for smart city buyers to dictate risk management requirements in contractual agreements, service level agreements, product certifications, etc. This is a means for smart cities to have some level of control over the security and privacy of systems and products that would otherwise be out of their control and ultimately assist in mitigating enterprise risk.
- ***Management of risk from external services, systems, and products –*** Smart cities' reliance on external services, contractor-owned systems, and COTS products necessitates mechanisms to ensure the risks associated with external services, systems, and products are properly managed. This includes all aspects of the risk management process, including the prioritization of systems and assets; the selection and implementation of controls; and the independent assessment and continuous monitoring

of systems. This may require contractual agreements, service level agreements, or participation in independent, third-party certification programs.

- ***Identifying, understanding, and assessing interdependencies –*** Smart city functionality may introduce new dependencies (e.g., data dependencies), and risk management decisions will need to consider the nature of these interdependencies. While an information system or an information type may be low impact for some stakeholders, the system or data may be high impact in another stakeholder's context.
- ***Technological diversity and limitations –*** Given the diverse array of technologies in the smart city environment, selected controls – including common controls – may not be able to be implemented as intended. Factors restricting implementation may include limitations in built-in functionality, processing power, battery life, etc. This may necessitate significant effort in terms of tailoring security and privacy controls, determining compensating controls, or assessing risk acceptance. Organizations and system owners will need to document how controls are actually implemented and configured and determine whether the residual risk is acceptable.
- ***Common control challenges and opportunities –*** Collaboration across government departments and agencies can lead to increased efficiency, for example, with the identification and implementation of common controls. However, diversity of technologies, architectures, and infrastructures could limit the feasibility of common controls. Collaboration from policy, governance, budget, and infrastructure perspectives may be needed to maximize the effective implementation of common controls.
- ***Risk mitigation through cybersecurity insurance –*** Smart cities can consider cybersecurity insurance as a risk mitigation measure (i.e., risk transfer). Cybersecurity insurance could reduce potential financial loss (i.e., consequence) and thereby reduce total risk. However, insurance would only be suitable for mitigating certain risks (i.e., those that can directly translate into monetary loss).
- ***Leverage existing IT/system assessment and auditing functions –*** If a city already has an independent assessor or auditor (whether a government organization or a contractor) for their enterprise IT systems, the scope of work could be expanded to include smart city systems. However, the city will need to consider whether the assessor or auditor has the requisite, specialized expertise to evaluate the diverse set of smart city technologies and systems.
- ***Continuous monitoring in highly dynamic smart environment –*** Smart city environments are highly dynamic with frequent changes to the technology environment. Organizations and systems owners will need to determine the appropriate minimum frequency at which necessary risk management processes will be conducted. This frequency may vary by system security category and impact level, mission, information type(s), and other organization risk factors. That said, the long-term risk management objective is to continue to move towards increased automation and truly continuous monitoring of risk.

Section Appendixes

Appendix A: IoT Threat Examples

Device Hijack - Confidentiality & Integrity
There are three main threats if a networked device can be accessed by unauthorized agents: direct misuse, exploiting connections for further unauthorized access, and misuse of Agency resources. Direct misuse might include a smart lock being actuated or surveillance cameras being watched. Exploiting connections means the attacker uses the device's privileged position in the Agency's network to access further networked assets. Resource misuse includes using the networked device to mine cryptocurrencies or attack internet-based assets outside the Agency's control. Recent occurrences of these attacks are (Jan 2019 Nest camera access, aquarium thermostat, Mirai botnet). The first two threats directly open the Agency to liability concerns due to data privacy breach and operational risk due to unauthorized access, while the third may consume limited Agency resources like power or bandwidth.
Device can be compromised to spy on owners: IOT device that has Audio/Video capability can be compromised to listen the surrounding area or capture video footage that otherwise should not be available publicly. There are reported cases of Baby Monitors being used to spy on the inside of the house due to default or weak passwords.

Device can be compromised and used to attack other systems within the same network: As a connected device inside the network, connected device can be compromised and used as a hoping point to access more sensitive areas of the network. This threat becomes more severe on IIOT environments where simple networked cameras can be used as a gateway to access control systems.

Device can be compromised to attack other networks: There are multiple scenarios where the device can be used to attack other external devices on the Internet. Mirai is one of the best examples of what is possible thru this attack scenario.

- DDOS can be performed on website/services on the Internet (i.e. Mirai)
- Device can be leveraged to compromise other vulnerable devices on the Internet by running vulnerability scanning on vast amount of IP addresses and ranges.
- Device can be hijacked to send spam emails for financial gain
- Device can be hijacked to perform targeted phishing attacks on individuals that "trusts" the network which device belongs to for circumventing certain controls

Device can be compromised to cause physical damage: Smart cars can be hijacked to cause physical damage to the driver and passengers. There have already been reported cases of cars turning off during normal driving conditions at high speeds. Another example is HVAC systems being turned off during winter causing physical damage to the building unit. In the cases of IIOT applications, simple turning off a production machine can cause millions of dollars in damage as

uncontrolled pause in production causes materials and time to be wasted (i.e. microchip production plants).

Information Disclosure or Modification - Confidentiality & Integrity
Information about the user or the infrastructure could leak to attackers: Widespread deployment of IOT devices turn our cities into data generation warehouses where great deal of information is being captured and shared between different services and service providers. Improperly secured communication protocols/devices can be eavesdropped to capture information about the environment as well as the users of the service.

Information processed and shared by the device can be modified: In certain cases, information modification can result in more serious outcomes then information disclosure. This is certainly the case in the medical field where data being received from an IOT device is used to provide health and safety services to individuals. In the simple case of an insulin pump, pump's remote sensor can be tricked to send a signal to the pump to release high levels of insulin to the bloodstream

Service Disruption - Availability
Device can become non-functional disrupting the service: in the case of "Smart Homes" or buildings, lights can be turned off disrupting the lighting for the unit. In more serious attack scenario, all lights and smart devices in a specific region can be turned on drawing large amount of power from the GRID disrupting the electric grid. In the case of ransomware, device and the data it contains can be encrypted for demanding ransom before turning on the service.

Appendix B: Use Cases

Application	User Story	Connectivity	Typical Security	Threat Vector	Risk Management Proposal	Business Risk	City deployed and Status
Smart Waste	As a city operator I would like to know when to dispatch garbage collection in order to reduce the unnecessary routes contributing to pollution and improving efficiency	Wi-Fi LoRa	Radius 802.1X AES 128	Man in the middle DDOS			
Connected Lighting	As a city operator I would like to have adaptive controls for my LED lighting in both the street and area environment to improve safety and energy efficiency	Wi-Fi LoRa Cellular	Radius 802.1X AES 128 SHA, ECC, PKI, Network authentication				

Traffic Monitoring	As a city operator I would like to reduce traffic congestion within the city by deploying cameras and edge gateways	Wi-Fi LoRa Cellular Fiber	Radius 802.1X AES 128 SHA, ECC, PKI, Network authentication				
Environmental Monitoring	As a city operator, I would like to understand certain conditions and pollutants in the city environment. I would like the gasses and particulates to be reported based on threshold events	Wi-Fi LoRa Cellular					
Smart Parking	As a city operator I would like to provide the citizens with open parking space indication that is presented either by a digital sign or delivered via a mobile application	Wi-Fi LoRa Cellular Fiber					
Digital Kiosk	As a city operator, I would like to provide an element of citizen engagement via the use of digital kiosks that will deliver city information such as nearby restaurants, parking, heat maps for where events are	- Wi-Fi - LoRa - Cellular - Fiber					

Appendix C: Municipal Roles and Responsibilities

Personnel and Management Models

- Privacy Officer - manages policies, coordinates audits
- Data Owner/Custodian - determines required controls
    - should not be contractor
    - avoid conflict of interest
- Auditor (could be third party) - determines effectiveness of controls

- Administrator/Engineer - applies the controls

Incident management

- Chief IoT Officer. Dictates strategy and manages IT governance and security
- Software engineer. Manages software and program code.
- Developer. Goes beyond software and manages hardware.
- Networking engineer. Provides networking and connectivity capability.
- Designer. Ensures user interface that controls sensors and examines data.
- Data scientist. Works with sensor data to apply analytics.
- Coordinator. Supervises the manufacturing floor to address robot breakdown and disaster recovery.

Appendix D: IoT-related Standards and Laws

Many laws at the US federal level require that information systems protect sensitive data they store or process temporarily. Failure to comply with them may incur various consequences including stiff fines. In worst cases, data breaches and business interruption are common consequences after a successful attack as in Atlanta City in March 2018.[31]

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- NIST Cyber Security Framework (CSF)
- NISTIR 8200 (International Cybersecurity Standardization for IoT)
- Center for Internet Security (CIS) (20 critical controls)
- National Response Framework (NRF)
- National Incident Management System (NIMS)
- General Data Protection Regulation (GDPR)
- Information Technology Infrastructure Library (ITIL)
- ISO 27001/2
- FEDRamp
- State /Local Laws
- NIST White Paper (10/17/2018), "Internet of Things (IoT) Trust Concerns" NIST IR 8200, "Status of International Cybersecurity Standardization for the Internet of Things"
- NIST IR 8196 (DRAFT), "Security Analysis of First Responder Mobile Devices and Wearable Devices" goes into the Use Cases, Attack categories, Threat Analysis, Security Objectives and IoT Security Concerns"
- NIST IR 8228 (DRAFT), "Considerations for Managing Internet of Things (IoT)

[31] FBI investigating cyberattack on Atlanta that involves ransom note, http://thehill.com/policy/cybersecurity/379846-fbi-investigating-cyberattack-on-atlanta-that-involves-ransom-note, BY BRETT SAMUELS - 03/22/18 06:14 PM EDT

Cybersecurity and Privacy Risks". The purpose of this IR 8228 is to help federal agencies and other organizations better understand and manage cybersecurity and privacy risks associated with their own IoT devices throughout their life cycles, this publication is the introductory document providing the FOUNDATION for a planned series of publications on more specific aspects of this IoT topic.

- NIST White Paper Draft (comments due March 18, 2019, "Security for IoT Sensor Networks: Building Management Case Study"
- NIST Privacy Framework
- New York City's IoT Guidelines (35 cities have adopted), https://iot.cityofnewyork.us/

Conventions	Law/ Regulation/ Standards	Applicable to Municipalities' IoT Projects?	Consequences of noncompliance	Covered Data	Security	Privacy	Case Studies
HIPAA	Health Insurance Portability and Accountability Act of 1996	Yes If IoT projects handles people's protected health information (PHI) or e-PHI	compliance or corrective action through other informal means, including a resolution agreement, civil money penalties (CMPs) may be imposed for noncompliance against a covered entity.	• the individual's past, present or future physical or mental health or condition, • the provision of health care to the individual • the past, present, or future payment for the provision of health care to the individual	The Security Rule establishes a national set of security standards for protecting certain health information that is held or transferred in electronic form.	The HIPAA Privacy Rule, or Standards for Privacy of Individually Identifiable Health Information, establishes national standards for the protection of certain health information.	No Business Associate Agreement? $31K Mistake – April 20, 2017

For reference: contained in CPAC Guidebook[32]
Appendix Conventions

1. **Information systems**
   The term information systems are defined in 44 U.S.C. §3502 as "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information," where information resources are "information and related resources, such as personnel, equipment, funds, and information technology."

2. **Cybersecurity**
   Thus cybersecurity, a broad and arguably somewhat fuzzy concept for which there is no consensus definition, might best be described as measures intended to protect information systems—including technology (such as devices, networks, and software), information, and associated personnel—from diverse forms of attack. The concept has, however, been characterized in various ways. For example, the interagency Committee on National Security Systems has defined it as "the ability to protect or defend the use of cyberspace from cyberattacks," where cyberspace is defined as "a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded

[32] GCTC Cybersecurity and Privacy Advisory Committee (CPAC) can be found here: https://pages.nist.gov/GCTC/super-clusters/

processors and controllers".[33]

In contrast, cybersecurity has also been defined as synonymous with information security (see, for example, S. 773, the Cybersecurity Act of 2010, in the 111th Congress), which is defined in current law (44 U.S.C. §3532(b)(1)) as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide— (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; (C) availability, which means ensuring timely and reliable access to and use of information; and (D) authentication, which means utilizing digital credentials to assure the identity of users and validate their access.

3. Information security
Synonymous with cybersecurity

[33] Committee on National Security Systems, National Information Assurance (IA) Glossary, April 2010, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf. Information security.

7. Full Case Study Reports

The following section contains full case study reports written for this Blueprint. The authors conducted telephone interviews of a period of several months between January and May 2019. The following municipalities contributed:

- City of San Leandro, CA
- City of Calgary, AB Canada
- County of San Mateo, CA
- City of San Diego, CA

Staff interviewed for these case studies were directly involved in the IoT projects described herein and have graciously agreed to share the details of their projects for others to learn from.

Editor's Note: Full Case Studies Begin on Next Page

City of Calgary, AB Canada

Highlights

- The City of Calgary IT was seeing more and more requirements from business units to "connect things, get the data and do something with it";
- They selected LoRaWAN as a very low cost IoT networking solution that can support the majority of new use cases and has good built-in security;
- Collaboration through formal and informal processes allows them to identify, test and evaluate new Smart City IoT solutions at low cost;
- The IT team emphasizes agile, iterative, flexible approaches to maximize learning and minimize risk;
- The City is working with the University of Calgary's Urban Alliance Initiative to recruit specific technical and application experts to support new IoT solutions.

City Background

Calgary, a city of 1.3 million people, is located about 50 miles east of the Canadian Rockies in the Canadian province of Alberta. It is Canada's third largest city and in addition to being home to many large energy companies has a diverse economy, including financial services, film and television, transportation and logistics, technology, and manufacturing. Calgary has consistently been recognized for its high quality of life. In 2018, The Economist magazine ranked Calgary the fourth most livable city in the world in their Global Livability Ranking.[34]

The City has a history of innovation and began building city-owned telecom assets over 20 years ago. It now has over 450 km of dark fiber, 200+ connected buildings and fiber-linked intersections, as well as a seven ring MPLS network. Its Field Mobility group has deployed a number of radio towers and provides wireless services to support SCADA, police communications, public works crews and other mobile use cases.

Project Overview

Calgary IT account managers, who work with the city's 32 different departments ("business units"), began learning about potential IoT use cases to improve decision making, while reducing operational costs. After initial efforts to add IoT sensors to vehicles using existing communications and build a Business Intelligence infrastructure, the City realized it needed a new network that could connect IoT sensors to collect even more data to drive improvements across city functions.

After researching several options, Calgary decided to deploy a LoRaWAN network to support new IoT use cases. LoRaWAN operates in unlicensed spectrum and each LoRa gateway on a 30-meter-tall tower has a coverage radius of at least 10 kilometers. Given that the City already had fiber-connected telecom towers, it was remarkably easy and low cost to deploy a LoRa

[34] https://www.economist.com/graphic-detail/2018/08/14/vienna-overtakes-melbourne-as-the-worlds-most-liveable-city

network that covers the majority of Calgary. This provided an IoT network solution so that they could begin to test and evaluate use cases and applications.

“LoRa seemed too good to be true,” said Sylvain Mayer, Manager of IT Innovation and Collaboration. “Our business goal was to understand the risk profile – how reliable is the network, how accurate is the data, what could break the sensors? We really focus on re-use and reliability.”
With a solid network in place, the City also reached out to the Urban Alliance at the University of Calgary to help identify specific IoT sensor solutions and develop, if needed, applications to apply new data to City challenges. Whenever the City identifies a new challenge, it is posted to the Urban Alliance and they solicit proposals to work on it.

Devonian Gardens - Smart Ag

One early standout was a ‘Smart Agriculture’ use case in downtown. The Calgary Parks department manages “Devonian Gardens,” an indoor 2.5-acre park and botanical garden on the 4th floor of the downtown shopping centre. The gardens include a living wall, koi ponds, fountains, a children's play area, and over 550 trees. As a major attraction, the Parks department closely managed irrigation and other conditions at Devonian Gardens; however, it was costly to maintain as it entailed quite a bit of guesswork as to what the plants really needed. Calgary reached out to the Urban Alliance and found a student to lead the project and paired them with a horticulturist and a SCADA expert to research IoT sensors and solutions.

They started small, spending around CAN$5,000 to buy sensors for a single garden bed to measure moisture, humidity, light and other conditions. The initial solution ran into issues, however, with programming, reliability, lifespan and unexpected costs. They tried working with a local company, but that approach also failed. Finally, they found a Swiss company with expertise developing robust outdoor solutions in the agriculture/photosynthesis space. This solution worked well and was less than half the cost of their original selection.

This project, even with the initial failures, is viewed as quite successful for several reasons. First, the City found a multi-sensor solution at a reasonable price point. And so far, this appears to provide the reliability that is needed for a larger scale deployment – where the largest cost will be placing the sensors and writing the software to drive the use case. Second, they also learned that lighting and ‘vapor deficit’ were the critical metrics to enable effective plant care. Finally, since they set clear expectations up front that this was a trial, so they could test multiple options,

they were able to show their early results and solicit their feedback on what was working and not working without fear of the project being cancelled as a failure.

Other Use Cases

Map showing where Calgary's snowplows are and what streets are cleared (City of Calgary)

As a major city that gets over 50 inches of snow each winter, Calgary works hard to ensure its snowplows keep streets as clear as possible.

However, after any large snowfall, the City inevitably gets a number of calls from people who can't get to work, or businesses whose trucks can't make deliveries, etc. There were already radios in the plows with GPS capabilities, so the city simply added IoT sensors to indicate when the plow was actually being used so they could map plowing activity and better assign plowing routes, as well as immediately answer questions about if or when a street would be plowed.

Calgary also deployed sensors at city-owned golf courses to monitor the pace of play. By putting sensors in six carts, the starter could see the actual pace of play and develop trend analyses to better understand when to stretch out starting times or skip some foursomes to maintain an acceptable pace. They could also see problems on the course more quickly and send out a Marshall to speed things up.

Calgary is also working on an acoustic sensor that could provide the height and location of different sounds. This has been shared with the police department and University of Calgary to explore potential use cases.

A final near-term application is to help drive economic development by making the network available for students, incubators and local entrepreneurs to test new IoT solutions. Calgary does not want to be in the "Network-as-a-Service" business, so it is not offering to support non-City deployments. Instead, it is allowing people to test new product solutions on a live network, so they can more rapidly introduce well-designed IoT solutions to sell to other cities or campuses.

Findings and Best Practices

Calgary is still by its own estimation in the early stages of defining and implementing full IoT solutions. However, they have proven infrastructure in place and have a successful process to work with end-users and evaluate potential applications. Moving forward, Calgary is planning to expand their efforts from 5-6 use cases up to as many as 10 use cases.

While they are still in the process of refining requirements, evaluating solutions and proving business cases, Calgary has established some clear best practices for the entire IoT project lifecycle.

- **Understand the application and use case.** Calgary IT has account managers working with each of their end-user departments, as well as with each other, to identify and scope out potential IoT solution needs. End-users are engaged in Proof of Concept projects (POCs) in order to help evaluate results and refine requirements.
- **Understand the risks to achieving your goal.** A lot can go wrong, especially with entirely new use cases, outdoor deployments and new or untested vendors. Since sensor placement can be the most expensive driver of overall deployment cost, it is critical to ensure they will provide the needed data, can be easily calibrated or recalibrated, support your security policies and will last the intended lifetime in your local climate conditions.
- **Start small and iterate.** Starting small allows you to move quickly, consider and evaluate multiple options, and keep end users engaged by showing early milestone results. Seeking bids for a full deployment would require an 8-12-month process and a lot of documentation on requirements that are uncertain or not well understood and there is a risk of getting locked into a vendor and solution that may or may not meet the project needs. Since it already has a citywide LoRa network in place and is working with the University of Calgary Urban Alliance, Calgary IT is able to rapidly deploy proof of concept projects to refine their needs and evaluate specific hardware and applications.
- **Do not try to overbuild**. Focus on what is needed to deliver the expected results to the target end user. You might not need a comprehensive platform that integrates every application.
- **Set expectations.** Not every project is going to work or deliver as many benefits as needed for a business case. Sometimes learning what can't be delivered is very useful to focus the organization on new or more relevant objectives. So long as you maintain active communications with your end user, keep them engaged in the process, and set expectations that the goal of initial tests is to understand the use case and potential solution, then you reduce the risk of failure.

To date, Calgary has not completed any large-scale deployments, though the network provides near city-wide coverage. But Calgary is the first Canadian city to build and own this new type of wireless network and the project recently won the 2018 Alberta Minister's Award for Municipal Excellence. Finally, the City has a strong vision and approach for how they want to use it: learning how sensors, data and connectivity can help residents. "There is no substitute for learning except for doing, just to be clear," said Mayer.

Urban Alliance

The Urban Alliance is a **research partnership** between the City of Calgary and University of Calgary, created in 2007 to encourage and coordinate the seamless transfer of cutting-edge research between the University and the City - for the benefit of all our communities. The senior administrations of both organizations are deeply committed to the success of the Alliance. The Urban Alliance is a prime example and vehicle for one of the three foundational commitments of the *Eyes High* vision, to fully integrate the University with the community. The City sees the Alliance as playing a key role in realizing its long-term priorities and the imagineCALGARY vision.

Through the Alliance, both organizations **pursue common interests in research, development and education** relating to:

- Finding excellent solutions to complex problems facing Calgary
- Fostering world class research and innovation
- Developing highly qualified personnel
- Establishing flexible, cross discipline approaches
- Energizing the relationship between University and City staff
- Facilitating continuity of corporate memory, wisdom and experience
- Realizing Calgary's long-term priorities and vision
- Nurturing a long-term partnership between the City and University

Vision:

To win recognition as a "world class" university in a "world class" city ... through collaboration in municipal innovation, research and education that positions Calgary well for long term.

Visit the Urban Alliance website.

City of San Diego, CA

Highlights

- San Diego has completed one of the largest City IoT deployments
- The City leveraged an LED street light transition, and savings generated from it, to fund 3,200 IoT sensor nodes
- The results are promising, but several important lessons have been learned

City Background

San Diego, with an estimated population of 1,419,516 as of July 1, 2017, is the eighth-largest city in the United States and the second-largest in California. It has been called "the birthplace of California" since it was the first site visited by Europeans on the West Coast of the U.S., and is known for its mild year-round climate, extensive beaches, many military facilities, and recent emergence as a healthcare and biotechnology development center.

Project Overview

San Diego has emerged as a global leader in City IoT deployments. Working with key partners including GE, AT&T, Genetec and Xaqt, the city has deployed 3,200 sensor nodes on street lights throughout the City, which it is using for a variety of use cases, including: advanced parking management solutions to identify highest density parking areas and streamline enforcement. It is also looking at Vision Zero initiatives to eliminate traffic fatalities and severe injuries. The deployed nodes also include sensors such as temperature and humidity which are available and being utilized for new use cases.

In addition to City Council vision and support, San Diego's deployment was enabled by the savings from their LED streetlight transition. This transition was accurately estimated to deliver $2.4 million/year in savings from energy and operations and maintenance (O&M), and the city's sustainability department was able to leverage this to identify and pursue new 'smart city' opportunities.

Their overall project is already viewed as a success, and additional benefits that can be delivered as more city departments leverage the available sensors and data will only add to this success. However, as an early adopter and innovator, San Diego has learned quite a bit about the unique challenges of IoT projects.

Project Planning and Approval

This project was conceived and planned by the Sustainability Department based on the substantial expected savings from their LED streetlight transition project. After a successful initial pilot with 25 sensors in 2015, they were able to move forward and implement their LED and IoT sensor project since it showed very clear payback.

However, the Sustainability Dept did, and continues to, reach out to other departments to promote this effort and highlight additional opportunities. The San Diego Police Department quickly bought into the project as they saw a compelling use case for video sensors to support efficiency in violent crime investigations.

Installation

The physical installation of the lights and sensor nodes went quite smoothly. The single truck roll approach (i.e., installing LED light fixtures and IoT sensors at the same time) significantly reduced

the incremental cost of deploying the sensors, as expected. However, they encountered some unexpected challenges related to the sensors that could be minimized or avoided now that they have a better understanding of these new technologies.

One issue arose from needing to better plan the rollout and understand the voltage requirements and light capabilities. The streetlights may support multi-voltage or single voltage, and this varies across the city, therefore utilities should be aware of their streetlight infrastructure prior to ordering sensors to ensure they are ordered with the proper voltage that matches the streetlight they are installed on. Also, the sensors tended to require significantly more lead time to order, and required technical review before being deployed, so cities should plan accordingly.

Another lesson learned is to have the installation crews turn on and validate the sensor nodes (in this case they were GE systems) as they are being deployed. This helps identify some issues and eliminate rework later if some sensors need calibration or alignment. This is easy to do while the installation crew is still on the pole, and if there is a trained technical crew available to evaluate nodes as they are installed. Otherwise, the lag time between the installation by the crew and the commissioning by the vendor requires the crews to go back to the location again to ensure proper activation.

Finally, the City opted to use 3G/4G connectivity to backhaul the sensor traffic. This was easy to implement, and benefits from the ubiquitous and reliable existing LTE networks but is expensive to operate. Currently the City is looking for opportunities to move to fiber or Ethernet backhaul options as lower cost options.

Engagement with Other City Departments

Cross-department engagement was a goal from the beginning, and in some cases, especially with the Police Department, San Diego achieved very positive results. The Police Department was engaged from the beginning and is already experiencing significant benefits from using the system to support violent crime investigations. The system is helping to reduce many hours of investigative work, while increasing the quality of evidence, which saves a lot of money. The Police Department is also collaborating with the Sustainability department to find innovative Vision Zero solutions that can reduce and ultimately eliminate traffic deaths.

While there has been outreach to other City departments from the beginning, the results have been slower. In San Diego's case, it would have been helpful to have an actual solution or analytics dashboard upfront to help some of the other departments visualize and understand the potential benefit from this new data. "It is a little like selling Grandma a smartphone," said Cody Hooven, Director/Chief Sustainability Officer. "Until they see actual new data it's hard to understand how useful it can be." Helping departments across the city visualize and better understand the new capabilities upfront will help increase adoption of the system.

Given that engaging other City users is likely to be an ongoing need, San Diego's Sustainability Dept is working to identify a designated point person in each city department who can be fully educated on current and future IoT capabilities so that unique department requirements from across the City can be captured up front.

In general, the team found that engaging people from the get-go - as opposed to later in the process - can be incredibly beneficial. Staff in other departments as well as people throughout

the community can provide extensive and unique insight into a wider range of challenges and can help focus the project on the most critical solutions.

Benefits Achieved from the IoT Project

The primary focus and benefit from San Diego's IoT project were always the LED lighting transition, and this seems to be delivering benefits as planned, with the expected $2.4 million/year savings in energy and operations and maintenance.

The additional benefits from the IoT sensor nodes are also becoming clear, although they are still more anecdotal in terms of measured savings. On the cost side, since the sensor nodes were deployed as part of the LED streetlight transition, their incremental deployment costs were reduced dramatically vs. a stand-alone deployment that would have required another full set of truck rolls.

From a benefit perspective, the most significant benefit so far beyond the energy savings is the reported major time savings in serious crime investigations. The availability of high-quality video from across the City is an invaluable asset and it is strictly accessible to police officials as approved by the Chief of Police. Other use cases, including the Vision Zero initiative and use of the temperature and humidity sensors, are still being evaluated, but will only enhance the value proposition for the sensors.

Note that the financial arrangement within the City is the departments using the sensor data must cover the ongoing O&M costs, and the sensors have a planned 7-year life before a refresh cycle. So, the cost of the incremental IoT data is extremely low.

As a best practice, the team felt that project management, including scoping, budgeting, identifying resources is particularly important, and complex, since IoT is such a new and dynamic category. Teams need to be sure they know what they are getting into, have adequate funding, both upfront and sustaining, and are aligned to the broader community to maximize success.

Data Policy Challenges and Decisions

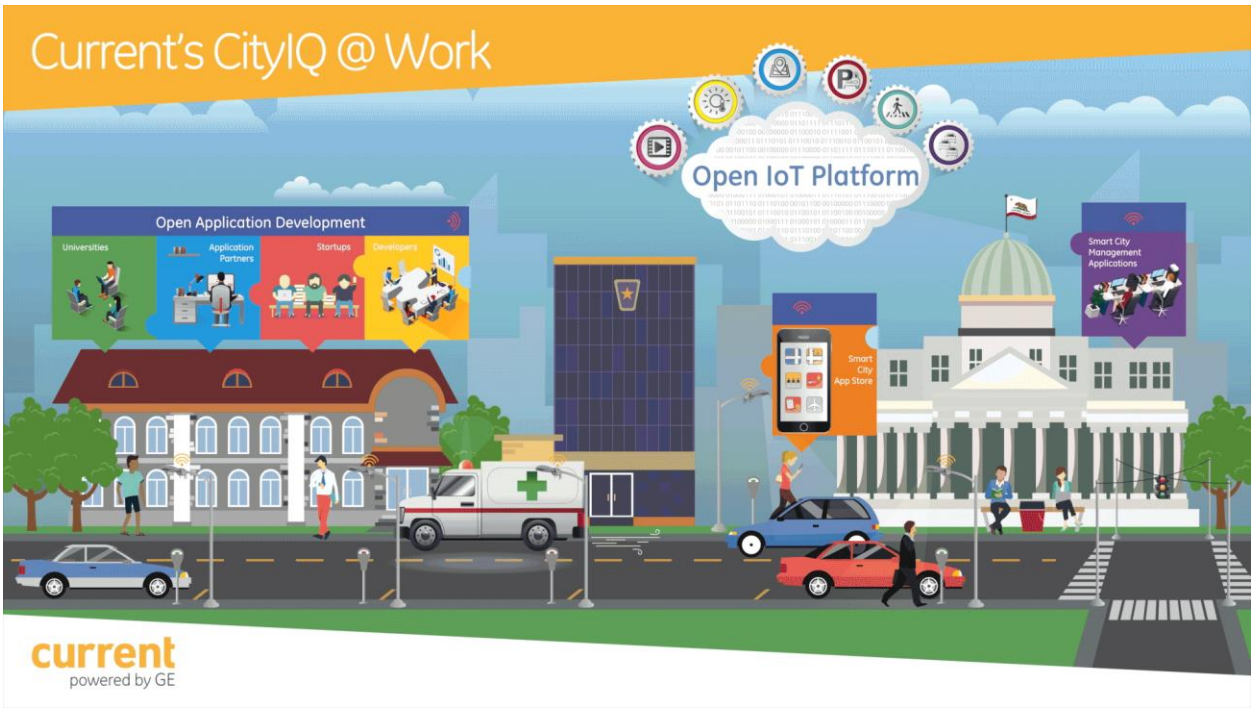
The wave of new data collected by City IoT devices and sensors, while delivering extremely valuable information to cities, has raised concerns among the public about data privacy and security. San Diego is no exception, and the City is being careful to avoid any mishaps. They have clear ownership of any data generated from their IoT systems and can control access and provide audit trails for any actual data access or usage. Video data, for instance, can be used by Police Department officials for very specific requests to support violent and serious crime investigations. It cannot be used for petty crimes or other minor enforcement activities.

The City also developed a working data policy for this effort. A benefit of this policy is that new data sources that are generated can be used in ways that both improve city operations and provide benefits to the community. In San Diego, for instance, there is a large cluster of data analytics companies that have requested access to the new data to test and validate new solutions. This will be another source of new benefits to the City once the IoT information can be appropriately shared.

Next Steps

San Diego has successfully rolled out one of the largest municipal IoT programs in the world and is seeing the benefits that they were initially looking for. This is quite an achievement and shows that it is possible to innovate and deliver impressive new capabilities even in local governments, which are very risk averse given their requirement to operate 24 x 7 to meet a wide range of diverse citizen, business and visitor needs.

But San Diego is not finished yet. The City plans to continue to augment the data they have and search for new use cases by working with additional city departments, local data analytics firms and partners such as GE. They also see great opportunities to leverage their work regionally by working more closely with other nearby cities and towns.



City of San Leandro, CA

Highlights

- In 2017, San Leandro completed one of the first citywide IoT networks, a $5.2 million project consisting of over 4,700 LED retrofit streetlights, water control infrastructure for city parks, and city facilities upgrades including HVAC, furnaces, and lighting controls.
- San Leandro's Public Works Department led the project with support from the IT Department. The contract was won by a subsidiary of Bosch called Climatec, who used technology developed by Paradox Engineering to build the connected street light system.
- The project required the network to provide alerts about the status of streetlights and to control lights remotely, which meant that this was essentially a "Smart Cities" project from the onset.
- ***Key recommendation: "IoT projects utilize complex technology. Having your Information Technology team (IT) working closely with your Operations Teams (OT) in Public Works and together with your Vendors to develop the architecture, implementation, maintenance, and management plans will ensure the project is successful."***

City Background

San Leandro is a mid-sized suburban town of 90,465 people located on the eastern shore of the San Francisco Bay, just to the south of Oakland. It is part of Alameda County whose county seat is Oakland and stretches from Berkeley in the north to Fremont in the south and Pleasanton and Livermore in the east, making it the seventh-most populous county in the state. San Leandro has a diverse population, with Asians forming a plurality at roughly 30% of the population, Whites and Hispanics each at around 27%, African-Americans at 12%, and one of the lower 48 States' larger Pacific Islander populations forming about 1% of the city's population.

Founded in 1872, San Leandro is one of the oldest cities in California. Historically a town with dozens of cherry farms and a Spanish missionary ranch, San Leandro's economy has evolved over the last century and a half from agriculture to manufacturing to distribution to most recently adopting the goal of "becoming a new center of innovation in the San Francisco Bay Area."

From 2016-2018, the Public Works Department led the completion of a $5.2 million project to convert the City's 4,800+ streetlights to LEDs. The project required a system with the ability to send alerts and be controlled remotely, effectively requiring the City to build an IoT network in the process. Thus, San Leandro completed one of the first citywide IoT networks in the world.

Project Overview

The project began with San Leandro Public Works Department's need to upgrade city infrastructure in a number of areas. This included facilities upgrades such as HVAC, furnaces, and lighting controls. It also included irrigation systems (smart clocks) for all of the several city parks to control water usage. Many of the upgrades were deferred maintenance on a number of

old systems that were a long time in coming. The streetlights needed to be upgraded to LEDs to use less energy for the City's climate goals as well as energy cost savings.

Public Works Director Debbie Pollart had the vision to integrate the different infrastructure upgrades into one project that would be paid for by the cost savings from the energy efficiency gains of the LED retrofit. She did not want to touch the General Fund, so the $5.2 million project was paid for with low-interest bank loan financing. Public Works had planned the project for years and generated buy-in among city leaders for the system upgrades.

The project's primary goals were focused on climate impact and energy management and efficiency. At the time, the City did not have any formal IoT Strategic Plan or Smart Cities Plan. The City did have a Climate Action Plan (2009) and the positive climate impact of the project was an important component of the project. Climatec, who eventually won the bid, guaranteed a certain level of energy savings of over a 15-year period, in effect, promising to write the City a check if those energy savings were not met. This significantly reduced the financial risk to the City to take on the loan funding.

One of the requirements originally built into the product project was the ability to receive alerts when the streetlights went out so Public Works crews could take proactive more timely corrective actions. This effectively made the project a Smart City RFP because streetlights would not normally do that on their own. The streetlights required a network to make the lights smart so the construction of the IoT network was a by-product of this requirement.

> *"The joke was, that when I had the first meeting with [Public Works Director] Debbie Pollart and said that this thing is like a big 'smart city' network, she said, 'No, no, that's what you and [then Chief Innovation Officer] Debbie [Acosta] do.' She may have said that a little tongue in cheek - she was very innovative and forward-thinking to bundle smart street light technology with an LED retrofit project." -- Tony Batalla, CTO, City of San Leandro*

Installation and Operation

In 2013, the City's Public Works Department began studying the energy efficiency opportunities of converting its streetlights from traditional bulbs to LEDs. With Energy Efficiency & Conservation Block Grant monies, they did a small LED retrofit of approximately 5% of the city streetlights to measure the efficiency gains and prove out the cost savings. The larger project for a citywide audit of possible energy and water efficiencies was approved by the City Council in 2014; the Request for Proposals for the full deployment went out in 2015 and the contract was awarded to a Bosch subsidiary called Climatec, in partnership with Swiss engineering firm Paradox Engineering to design the system. This was by far the largest deployment that Climatec had ever done with Paradox in terms of scale. The project went into full construction in late 2016 with a one-year timeline and was complete in 2017-2018. Some of the technical portions are still a work in progress as of 2019 but it is functionally up and running.

From a technical perspective, the streetlights are mesh-connected in a Low-Power Wireless Personal Area Network (6LoWPAN) operating in the 900 MHz ISM Band. These nodes backhaul on approximately 35 strategically- placed Wi-Fi gateways that, in turn, connect to the city's fiber-optic network at designated traffic signal intersections. The data transports on the fiber network to City Hall, where it reaches a virtual Control Management System (CMS). Using a web interface to access the CMS, city staff can individually control every light, set policies for when the lights turn off and on, monitor functionality and even get alerts and email alerts when a light bulb fails to do proactive maintenance (thus meeting that early RFP requirement).

There were some technical challenges, but the IT team recognized immediately the scale of the project and the team felt that the challenge "was actually fun." One of the first things they did with Paradox was use GIS to refine the locations of planned Wi-Fi gateways. The original plans were done without insight into the actual landscape; IT was able to provide much more input into what locations would be ideal for coverage and signal strength.

From there, they had to figure out how to get gateway signals back to City Hall. The IT team was able to utilize traffic signal controllers, located within traffic cabinets at each intersection, to connect the Wi-Fi gateways to the fiber network. However, data had never been passed from the traffic network to the City network where the IoT CMS would reside, so a network architecture needed to be developed, including the implementation of a new firewall to allow traffic to securely pass between those two networks. With the help of City traffic signal engineers' electricians, who had fortunately upgraded the switches inside their traffic cabinets in 2011 to managed systems, a field test was conducted to prove that Wi-Fi gateway data could be sent through the traffic signal controllers, along the City fiber network, through firewalls, and into a virtual server in the City Hall data center. And it worked!

As the construction was went into full gear, there was still no formal operational plan for who would manage the network after it was built. However, informally it became agreeable that the best arrangement would be for Public Works (OT) to manage the edge - the street lights and 6LoWPAN sensors on the street lights themselves, receiving alerts from the CMS for those devices, while IT would be responsible for all the connectivity from the data center and servers to the Wi-Fi gateways and everything in between, including the fiber and traffic connections. This included putting in a place a maintenance contract in place with Paradox Engineering, managed by IT, for ongoing support and upgrades of the CMS.

Security in the solution includes frequency-hopping, network segmentation, firewalls, and application controls (i.e., account passwords) on the CMS. However, it was not a focus during the design or construction. Looking at it in retrospect, San Leandro decided to partner with a cybersecurity firm called CryptoMove to investigate how vulnerable the system is to attack. This research is still ongoing.

Engagement with City Departments

The Public Works Department led this major capital project and IT was brought in later in the process, after the construction was underway. These projects have a lot of moving parts and need to involve the right people at the right time. To some extent this kind of collaboration is informal and unstructured almost by nature. In particular, it can be hard to engage IT before you realize you need their support. However, from the IT team's perspective, it is always good to get IT involved at the kickoff of the project. Often there is an IT component and involving IT early on can enable them to understand future requirements and plan accordingly, creating a cohesive technology strategy for the organization.

Benefits Achieved from the IoT Project

San Leandro is currently on target to achieve its energy efficiency goals, saving about $447,000 per year with a planned 15- year lifecycle. This, combined with other energy and water savings, is saving an estimated 1,977,391 kilowatt-hours of energy per year, which is the equivalent of removing 2,103 annual metric tons of CO2 greenhouse gas emissions from the environment.

The functionality of the system, including the generation of data about city systems, is working at a base level as intended. The success in achieving some of the secondary goals of the project, such as proactive maintenance of the streetlights, is less clear. For instance, Public Works may not be using the alerts or setting policies to handle them. Another goal of collecting the data was to create a dashboard that could be shared with the public to show the savings with great transparency but due to technical and security considerations, the dashboard is only being used internally so those public trust benefits have not yet been fully realized.

The IoT network won a Smart 50 Award from the Smart Cities Council in 2018 and places San Leandro among the very first cities in the United States to deploy a citywide IoT network. It is meeting its financial targets, and in that regard has been very successful. It is actively exploring how to utilize the IoT network for additional use cases in the future.

Lessons Learned

1. The involvement of the technical people the earlier, the better.
2. IT vs OT: learning where that ends. They learned it organically but didn't have formal plan going in. What is your operational plan? Who is responsible for the maintenance? Do we have a maintenance contract with a vendor? How will ongoing maintenance and vendor support be funded?
3. It might be a missed opportunity not to recognize the full gravity of the project earlier on. If San Leandro had recognized the full opportunity earlier on, they might have been able to do this with a broader vision. It was designed as a single- use case. However, it may have been able to be leveraged, from the beginning, for parking, public safety, and emergency response to name a few. This may still happen, and it does not detract from the financial success of the street lights project; however, if they had looked at it with a bigger vision for an IoT wireless network they may have considered things such as

regional uses, interoperability with other networks, open data, analytics, and security. You don't get a second chance to build a multi-million-dollar IoT network.

Next Steps

San Leandro is exploring how to utilize its IoT network for additional use cases. This has been dubbed the "City as a Platform" concept. One pilot they did was for sensors in trashcans to understand the state of the bin. In the summer of 2017, students from Harvey Mudd College, including a San Leandro High School graduate, interned with Pilot City, a nonprofit San Leandro education incubator, to develop a Smart Waste Monitoring pilot solution for measuring the fill level of street trashcans that connected to the City's platform. The pilot ended up requiring significant engineering resources from Paradox Engineering as they needed to redevelop a lot of their backend database system to make it work.

However, Paradox is introducing an API and development kit that may hasten future application development. San Leandro is also working on the aforementioned security project with CryptoMove to demonstrate an IoT security solution.

In the future, there is always the possibility that the network may support additional use cases. But there is also a possibility future use cases will require their own IoT networks that are better-suited to those specific use cases. This is not unique to San Leandro and many municipalities in the future may end with several, co-existing IoT networks all utilizing various aspects of the core communications networks in place. San Leandro predicts that if this happens, it will place a greater emphasis on the data generated from these systems, rather than the systems themselves. The data can easily traverse disparate network boundaries and ultimately will be what drive insights and improved outcomes. However, public agencies will need to ensure they own and can freely access these datasets and are not restricted by the IoT solutions they implement.

County of San Mateo, CA

Highlights

- San Mateo County launched SMC Labs in 2018 to lead the county's "Smart Region" efforts with a vision beyond cities and borders to solve challenges for all residents, utilizing shared fiber and public Wi-Fi networks.
- SMC Labs is a "co-creation" innovation center relying on partnerships with private-sector companies to showcase numerous connectivity technologies, including: LoRaWAN, Wi-Fi, NB-IoT, and cellular IoT.
- The primary goal of SMC Labs is to experiment and learn about how to make the Internet of Things useful for communities.
- **Key Takeaways: The Lab environment has been good for experimenting and learning about multiple technologies from multiple solution providers. "We tested some things that didn't work at all." Numerous early pilots are helping to identify use cases of importance as well as challenges in implementation**.

County Background

The County of San Mateo is one of the nine counties of the San Francisco Bay Area. It is located immediately south of the consolidated City and County of San Francisco and its 448 square miles cover most of the San Francisco Peninsula, extending from the Pacific on the west to the San Francisco Bay on the east and south to Menlo Park, just north of Palo Alto and Stanford University. San Francisco International Airport (SFO) is located at the northern end of the county. The county population of 764,000 is spread across 22 cities and large unincorporated areas as well as rural areas. The County's built environment spans a wide range from highly urban to exceptionally rural, though most of the populated areas are suburban. Its economy is driven by IT and biotech companies and San Mateo County hosts the headquarters of Facebook, Oracle, Visa, Sony Interactive Entertainment, Electronic Arts, YouTube, Genentech, and Gilead Sciences, as well as a hub of venture capital firms on Sand Hill Road in Menlo Park.

Project Overview

SMC Labs leads the County's "Smart Region" efforts, which includes experimentation and learning about the Internet of Things as it relates to communities. SMC Labs is working in partnership with cities across the county as well as with private-sector firms to deploy IoT wireless connectivity solutions to experiment with connected devices and sensors. They are testing several different IoT wireless connectivity services as well as a number of different sensors. Their main focus has been how to make government more efficient and how to achieve better quality of life for residents.

Early use cases include:

- Parking availability for disability-accessible parking spots and electric vehicles;
- Irrigation water conservation with smart moisture sensors;
- Localized air quality and environmental monitoring;

- Real time tracking and monitoring of mobile assets;
- Pedestrian and outdoor space utilization;
- Optimized and predictive waste collection.

Project Origin, Planning and Approval

In May 2018, San Mateo County's Information Services Department (ISD) launched SMC Labs, a "smart solutions" innovation center, with the goal of bringing together diverse stakeholders including city operators, residents, universities, domain experts and private sector solutions providers to co-create solutions to problems facing communities and residents throughout the county.

"Housing, traffic, mobility, and environmental issues don't stop at city borders. Regional problems require a borderless approach, and the County of San Mateo is uniquely positioned to address these issues. We laid the groundwork [in 2017] when we started deploying a countywide fiber and public Wi-Fi network as the first step towards a Digital San Mateo County. SMC Labs is the next step of this journey," said County of San Mateo Chief Information Officer Jon Walton in a statement at the time of the launch.

Equity and inclusion were major concerns as well. "Despite being located in the heart of Silicon Valley, there are two very different populations in San Mateo County. One is technology-savvy and lives in the larger, resource rich cities. The other includes smaller suburban and underserved rural communities with limited digital infrastructure. My goal is to bring innovative solutions from SMC Labs to serve all San Mateo County residents, leaving no one behind," said Ulysses Vinson, Director of SMC Labs and Chief Smart Communities Officer for San Mateo County.

The county's efforts to bridge the digital divide led it to provide free high-speed internet access to underserved communities through fiber and Wi-Fi deployments. People understand what public Wi-Fi means and how to connect to the internet, so these efforts naturally evolved to focus on how to put innovation to use not just for connecting people but also devices. The approach is focused on catalyzing the useful application of the Internet of Things and that is largely the framework they are using for their Smart Region program. SMC Labs' approach is to pilot a number of connectivity technologies as well as connected devices that send data over those networks.

Installation and Operation

To start, SMC Labs has created two innovation zones for testing solutions to local issues: one on the San Mateo County Center Campus in Redwood City and a second at East Palo Alto City Hall. The program is run out of the Information Services Department, which leads the IT operations for the county government.

From the launch in 2018, the program has been a collaboration with industry and SMC Labs' approach has been to foster a healthy ecosystem rather than to choose any single technology or vendor. SMC Labs launched with an inaugural set of innovation partners that included:

- T-Mobile for NB-IoT wireless connectivity;
- Helium for a decentralized IoT connectivity network;
- Fybr for a Smart Cities parking platform based on LoRa;
- RoamBee for asset tracking;
- Ntropy for resident engagement;
- Strategy of Things for innovation strategy and management.

New partners have been added as well. DISH Network is now working with SMC Labs on an NB-IoT deployment and the initial use case will focus on air quality measurement using sensors that will send data over their network. One sensor partner is a Bay Area startup called Clarity, which is currently using LTE to get the data from their devices.

LoRaWAN is a connectivity platform that SMC Labs is also exploring and is partnering with Comcast's MachineQ unit, which is deploying LoRaWAN in the area. In this partnership, SMC Labs will own and operate four wireless access points and MachineQ will oversee the device management on the network. Similar to a public Wi-Fi network, the LoRaWAN service uses open, global LoRa standards and is interoperable with compatible sensors. For one of the parking pilots, SMC Labs is using Fybr's IoT platform that uses LoRa gateways (though they use proprietary software so are not necessarily interoperable with other sensors). Another company is doing smart parking to evaluate how many spots are available at a given time.

The partnership model - and who pays for what - is flexible. Currently, the projects have been about 50/50 where SMC Labs buys the sensors and/or equipment vs the company providing them for free. In some cases, the companies need to work with a city or the County to help strengthen product-market fit or even develop effective use cases from their infrastructure. In general, the approach is to co-create and establish pilots in a no-cost agreement with the goal of learning what works and what does not work. With that knowledge, SMC Labs and the companies can make the business case to city departments who will lead the procurement of deploying the solution at scale.

Engagement with City Departments

When the project began, the innovation and IT teams started talking to County agencies and generally found there was little to no understanding of IoT technologies and how they would relate to use cases that might address their needs. That led in some way to the function of the lab as a knowledge resource for cities governments and County agencies across the region. The problems that many of their cities face are similar so they wanted to experiment and share information across the "smart region."

CSO Ulysses Vinson's approach is straightforward: "After SMC Labs has it tried out, we can then engage with a County agency or city and see if this is something they want. They are the business owner."

Benefits Achieved from SMC Labs

To date, SMC Labs has led five different IoT-related pilots with varying degrees of completion:

1. Parking availability for disability parking spots and EV parking spots in the San Mateo County parking garage in Redwood City. Drivers with disabilities or those with electric vehicles (EVs) may voluntarily limit their mobility to certain areas because they are not sure if they can park their car near where they need to go. Using Fybr's Smart Cities platform, parking sensors, a mobile app and Alexa integration, SMC Labs ran a pilot to understand if there were technological solutions to these challenges. Questions to be answered: Where are these spaces? How often are they utilized? How long is each space occupied? Which days and times are busiest? Which times are least? What is the best way to communicate parking space availability? How will parking space utilization change with if we can share this information with drivers? The pilot has been running since June 1, 2018 and a preliminary detailed report is available on SMC Labs' website.

- Key learnings to date:
    - Current parking capacity for EV and disabled drivers is sufficient to meet current demand levels.
    - EV parking spaces are underutilized outside of core hours and on weekends.
    - County employee electric vehicles are parked an hour longer (on average) than their public counterparts.
    - Using voice commands to find available parking shows promise as long as the commands are short and simple.

2. Localized Air Quality and Environmental Monitoring: Air quality varies from location to location, even within blocks of each other. People who are very sensitive to air quality may be affected negatively as they go from one area to another. The current air quality monitoring system provided by the Bay Area Air Quality Management District is spaced too far apart to give highly localized information. So, SMC Labs piloted air quality and environmental sensors and a notification system to understand a set of questions: How do air quality levels change from location to location? How large are the differences? What causes the differences in local air quality? How do the various air quality sensors compare (e.g., consumer grade air quality sensors, low cost pro-grade intermediate sensors and high-end sensors, etc.)? Where do they all fit within this air quality monitoring ecosystem? The pilot began in May 2018 with three initial sets of low-cost sensors in San Mateo and East Palo Alto and integrated on the Fybr platform. The results indicated that the sensors were inadequate to answer the questions proposed by the pilot. A second set of 10 sensors is being deployed in 2019 by a startup named Clarity. SMC Labs is also exploring three different vendors for data integration.

- Initial learnings:
    - The sensors were mounted on building rooftops, when they should have been mounted lower; only 12 to 15 ft above the ground.

    - There was no pre-installation calibration against a known sensor (I.e. Compared and calibrated against one of the air quality district sensors).
    - The sensors did not provide the level of accuracy required (which was evident when the Camp Fire wildfire smoke covered the region)

- Next steps based on these learnings are to update the pilot as follows:
    - Deploy 10 Clarity air quality sensors throughout the county. Sensors are expected to be installed in February of 2019.
    - Locations will be selected based on a set of considerations – proximity to sensitive receptors, geographic and terrain diversity, construction and traffic activity.
    - Evaluate and understand the range of air quality sensors available – from low cost consumer grade to high reliability, mission critical sensors. Identify use cases for each type.
    - Potentially incorporate this range of sensors into this second pilot.

3. People and Mobility Patterns Analysis: Urban planners have limited awareness of how pedestrians, visitors and commuters move around within a city and selected areas. This lack of understanding results in services that do not match expectations, suboptimal resident engagement and experiences. In 2019, SMC Labs will be piloting a people and mobility analytics project. This project will use RadioLocus mobility analytics service and utilize San Mateo County's public wi-fi network to understand visitor mobility patterns. Questions to be answered: How many people are visiting in a particular area? How long do they stay? How often do they come back? When do they come? Where are they coming from? Where do they go next? What services should we create in those areas that best serve the needs of visitors? The results of this pilot will be used to help urban planners, economic development organizations and transportation agencies develop new services. No results yet reported.

4. Optimized Waste Collection: With no data on waste bin fill status, bins can overflow, and waste collectors spend resources serving trash bins that are not at capacity. This results in inefficient collection of trash and unnecessary driving and vehicle emissions. SMC Labs plans to pilot waste bin sensors and collection analytics to see if improvements can be made. Questions to be answered: Are we collecting trash at the right intervals and times? When should we do it? Which areas require additional collection frequency, and which require larger and more bins? Do we need to modify existing collection routes? No results yet reported.

5. Real time tracking and monitoring of mobile assets: City departments lack the ability to track in real-time equipment and assets that move from location to location. This results in lost assets, as well as inability to productively deploy assets to where they are most needed. SMC Labs is piloting a solution with Roambee asset tracking sensors and beacons and a location monitoring dashboard. Questions to be answered: What items need to be tracked? How will this affect asset productivity? How will this affect operational efficiency? How accurate is the tracking? Are there differences in performance and accuracy due to different connectivity methods? How accurate are these in real time or near real time? The project is starting in early 2019. An initial

pre-pilot test of the RoamBee asset tracking solution, using cellular as the connectivity method, was reasonably accurate. However, battery life was shorter than expected. The actual pilot will be conducted using NB-IoT connected tracking devices with the NB-IoT connectivity provided by T-Mobile.

- The Department of Public Works has identified two use cases for the pilot:
    - Tracking of mechanized equipment (forklifts) that are deployed and move across county facilities and projects
    - Tracking of ladders that are located in and around county facilities. These may be inside buildings as well as outside the buildings.

In addition to testing the ability to track assets, SMC Labs will also be testing and understanding the feasibility of NB-IoT as a connectivity option for asset tracking. If the asset tracking solution supports LoRaWAN, they will also be evaluating asset tracking performance against this as well. No results yet reported.

Lessons Learned

The SMC Labs approach emphasizes experimentation and learning. For example, one company using LoRaWAN said that their battery life was three years and it did not even last three weeks. It turned out that they were reporting data every few minutes that did not need to be reported that frequently. It was a learning experience for both the County and the technology company. They shifted their whole business model because of that. “We are here to test this stuff because it is all new,” said Vinson.

Smart Cities and Smart Regions are complicated and require collaboration, including between government agencies and through open innovation efforts with the private sector. SMC Labs’ approach is to co-create with diverse stakeholders and enable collaboration to solve complex challenges. Vinson again: “Building this Smart Region ecosystem is a significant undertaking composed of many layers and moving parts, including the underlying network, security, data, applications, and partners to leverage these applications.”

Next Steps

SMC Labs is part of a broader smart region initiative by the County of San Mateo to use modern innovation methodologies and “smart technologies,” such as the Internet of Things, machine learning, “big data,” and blockchain, to address regional issues. These non-IoT pilots are not discussed in detail here but include a drone detection pilot around sensitive areas such as correctional facilities or the San Francisco International Airport, an affordable housing portal that uses digital services to improve access to affordable housing through a partnership with Exygy, and more. SMC Labs is directed by Ulysses Vinson. SMC Labs reports directly to the county’s Chief Information Officer, Jon Walton. The program is assisted by a strategic innovation partner, Strategy of Things.[35]

[35] Renil and Benson of Strategy of Things are contributing authors of this Blueprint.

To understand the extent that IoT will be useful in achieving their communities' goals, SMC Labs is going to continue to experiment with multiple connectivity networks. Questions to be answered: What connectivity technologies are available to support basic and smart city applications? Do we build and operate our own networks, or should we use a vendor provided connectivity service? How do these different connectivity options compare? What use cases work best with which connectivity technologies? They have identified two driving problems:

> Problem #1: There are multiple IoT and smart city connectivity technologies such as Wi-Fi, LoRaWAN, SigFox, NB-IoT, Helium and other proprietary like Fybr-Link. These are still maturing, and there is no one size fits all connectivity strategy that will work for all use cases.
>
> Problem #2: There exists a "digital divide" within San Mateo County. Select areas, such as rural areas, unincorporated areas, and certain areas do not have connectivity, or sufficient connectivity for basic applications.

SMC Labs will be setting up a Wi-Fiber long-range wireless transport (millimeter wave) network to provide broadband connectivity to underserved areas by Q2-2019. SMC Labs will be setting up three MachineQ (Comcast) LoRaWAN gateways at select locations within San Mateo County in Q1-2019. Within the zones covered by these gateways, SMC Labs will be providing LPWAN service and testing a variety of use cases. SMC Labs will be testing a variety of use cases, including Asset Tracking that will be running on T-Mobile's NB-IoT connectivity service in Q1 2019. A review of T-Mobile's coverage maps has shown that there is countywide coverage. When available, SMC Labs will be one of the first testers of Helium's blockchain based community connectivity network. Helium gateways will be available for deployment in Q2-2019. SMC Labs will work with Helium to identify select use cases that will run on Helium's network.

More broadly, SMC Labs will continue to build out their knowledge and expertise in sensors, connectivity and data as they move beyond celebrating their one-year anniversary in May 2019. They plan to continue building out new Innovation Zones to cover downtown corridors and eventually expand countywide. They will continue working with public and private partners in Silicon Valley and beyond. They will also continue experimenting with important use cases for their communities, finding appropriate business units within cities for those ready to scale and addressing their mission: "to protect and enhance the health, safety, welfare and natural resources of the community, and provide quality services that benefit and enrich the lives of the people of this community. We are committed to: The highest standards of public service; A common vision of responsiveness; The highest standards of ethical conduct; Treating people with respect and dignity.