SCTE CABLE-TEC EXPO 22
SEPTEMBER 19-22 • PHILADELPHIA, PA

2022 Fall Technical Forum
SCTE • CABLELABS • NCTA

Requirements for the IoT Infrastructure in the Customer Premises

A Technical Paper prepared for SCTE by

Rajesh Abbi
Principal Consultant
Duke Tech Solutions, Inc.
111 Fieldbrook Ct. Cary, NC 27519
+1 919 455 4787
rajesh.abbi@duketechsolutions.com

Charles Chapman
Manager of Customer Training and Loyalty
Enersys
3767 Alpha Way
Bellingham, WA. 98226
+1 941 228 5102
chuck.chapman@enersys.com

Sudheer Dharanikota
Managing Director
Duke Tech Solutions, Inc.
111 Fieldbrook Ct. Cary NC 27519
+1 919 961 6175
sudheer@duketechsolutions.com

Kyle Haefner
Lead Security Architect
CableLabs
858 Coal Creek Cir, Louisville, CO 80027
+1 303 661 9100
k.haefner@cablelabs.com

Clarke Stevens
Principal Architect, Emerging Technologies
Shaw Communications, Inc.
1801 N. Broadway, Suite 501
Denver, CO 80202
+1 720 723 2316
clarke.stevens@sjrb.ca

Table of Contents

List of Figures

List of Tables

1. Executive summary

Customer premises networks have been evolving since the early days of POTS (Plain Old Telephone Service). The introduction of new services like Cable TV, Broadband, and later VoIP, has driven numerous changes in the premises networking requirements. It is therefore no surprise that with the emergence of a vast array of new Internet of Things (IoT) applications and other revenue-generating applications, the premises networking requirements will change yet again. Also, with the advent of these new service offerings such as Telecom for Wellness (T4W) [3], [4], [5] and Smart Cities [12] applications, even the definition of the term "customer premises" itself needs to be realigned.

To better understand these changes in the customer premises networks - as well as plan for them in advance - the SCTE has launched a new initiative under its IoT Working Group called the Wiring Closet Drafting Group (WCDG) [13]. This is a cross-functional team comprising members from the IoT, Smart Cities, Telehealth, and Aging in Place (AIP) working groups. The expectation is to gather and consolidate customer premises networking requirements from all these various classes of IoT applications and make recommendations for future customer premises networks that can be built in a modular fashion using the recommendations from the WCDG.

In this paper, we explore the special needs arising from these recent developments in the customer premises network and outline a framework of requirements that are being compiled by the SCTE WCDG. We highlight key service and business considerations for various application use cases including managed Wi-Fi, home security, home automation, telehealth, aging-in-place, hospital-at-home, smart cities, and their associated security, installation, and support services. We believe this framework can greatly enhance the serviceability and adoption of these new services and can enable significant future revenue opportunities for communications service providers (CSP).

2. Evolution of cable customer premises

Home networks have come a long way over the past few years. They are no longer the domain of technology enthusiasts who cobbled up connectivity between various devices in the home. Today – especially in the wake of the ongoing pandemic – home networks have taken center stage in the life of most people. In addition to the need for ubiquitous Wi-Fi service being the critical driver for these networks – a host of home automation IoT services including sensors, video communications, interactive devices, as well as other next-generation service offerings such as aging-in-place and telehealth are beginning to drive significant complexity in the home network.

From the cable customer perspective, the scope of cable services has also evolved from primarily video services to mainly residential subscribers to now a much broader set of video, voice, and data services to subscribers spanning residential, businesses (offices, retail, hospitality), airports, parks, stadium, hospitals, and even governments (municipal, city infrastructure) etc.

The recent emergence of IoT applications has dramatically expanded the type of services cable networks can deliver. At the same time, the needs of all these disparate services have brought with it significantly increased complexity in the network infrastructure in the customer premises. The future of in-home networking is dependent on the modular deployment of revenue-generating services that not only offer services in a tiered fashion but also are manageable from installation and service assurance points of view. To better understand the needs of the emerging IoT applications and services, and to better prepare for them, the SCTE IoT working group has launched the Wiring Closet Drafting Group (WCDG). This group is a cross-functional team from the IoT, Smart Cities, Telehealth, and Aging in Place (AIP) working groups. The fundamental Premises of WCDG is that by deploying relevant solutions where the

services are deployed a priori, the cable operator can (1) turn up the service faster, (2) customize services to the needs, and (3) can have a competitive advantage in delivering end-to-end services. In this work, we evaluate different needs that arise from such enhancements to the in-home (SFU, MDU), common area (MDUs and planned communities), and smart cities network. We propose a step-by-step upgrade to the Telecom closet, a general-purpose term used for an aggregating unit of the Telecom services offered by the operators. These factors are further explored in this paper.

3. Emerging IoT applications

No new technology in recent history has had the dramatic scope of impact as IoT. This is a technology that touches just about everything we deal with and has the potential to revolutionize life in unforeseen ways. Many ecosystems (such as Telehealth, AIP, smart cities, etc.) are being developed using these IoT devices. Let's take a quick look at some of the more popular IoT applications and services being deployed today.

Home Automation and Security Applications: Some of the most popular IoT applications deployed in homes today are for home automation and security. Home automation enables homeowners to control various elements in their home remotely. These include lights, door locks, thermostats, sprinkler systems etc. While home security has been deployed for many years, most applications in the past involve professionally installed and monitored systems using proprietary technologies. IoT has opened the door to self-installed security systems and devices including sensors and cameras for monitoring the home remotely. These have brought not only significant convenience to homeowners, but they can literally be lifesaving at times.

	Aging in Place	Telehealth
Users	Older adults (65+), caregivers	Individuals, providers
Stakeholders	Family members, care givers, doctors, service personnel etc.	All family members, providers, (payors)
Needs	Communicating, monitoring, service, support, integration	Communicating, monitoring, integrating with provider systems
Challenges	Ease of use, provider network integration, problem solving	Ease of use, device and EMR integration, remote monitoring,
Telecom opportunity	End to end solution, managed services, provider integration	End to end solution, managed services, provider integration

Figure 1 - Telecom for Wellness Opportunity and Challenges Summary

Telecom for Wellness (T4W) applications: The wellness industry is going through a major transformation to modernize the infrastructure, reduce the cost and increase the quality of care. In a series of articles, we have suggested how the Telecom industry can assist the wellness industry[5], [6], [7], [8], [9]. We call this inter-industry collaboration Telecom for Wellness (T4W). Even though the T4W

opportunity is not limited to these two major intersection points, we focus on AIP and Telehealth use cases to illustrate our requirements on the WCDG architecture. (Refer to [1] for six different opportunities that a Telecom operator can address through the T4W.) The SCTE Data Standards Subcommittee, of which two of the authors are members, is actively working on T4W solutions for the AIP and Telehealth areas in working groups three [10] and four [11].

Figure 1 provides a quick summary of the T4W opportunity and challenges from AIP and Telehealth points of view. Many of the needs, challenges, and Telecom opportunities of both markets are similar (refer to the SCTE working group analysis at [10], [11]). Some of the high-level use cases that need to be supported for these two markets include:

- Providing basic communication between the users and the providers/caregivers
- Providing seamless communication between the users and the stakeholders
- Monitoring the users for health, mobility, fall detection, etc.
- Analyzing the data collected from the users and properly notifying the stakeholders
- Assisting the T4W service providers with claims by documenting accountability
- Offering managed services to support installations, product support, and other services to improve adoption and retain customers

The goal of this paper is not to elaborate on these use cases, but to use them to motivate the WCDG modular architectures. For additional information refer to the working group documents.

Retail Business Applications: Retailers have been on the forefront of the IoT revolution trying to exploit the troves of valuable information made available by IoT-enabled devices. From managing the store security, environment, lighting, to monitoring customer traffic and store inventory on a real-time basis – IoT is finding uses in almost every facet of their business today.

Factory/Industrial Automation: Factories and the manufacturing industry has been at the forefront of automation for a long time. Most factories deploy purpose-built machines, tools, robots etc. to automate repetitive tasks. IoT has brought a whole new dimension to this automation. Machines do not just automate their workflow – they can even coordinate seamlessly with other machines and systems on the shop floor, and perhaps even with others across the world.

Inventory/Fleet Management: IoT enables convenient and precise tracking of the location of enabled devices. This has found many applications in the shipping and logistics business for managing product inventory as well as for vehicle and material tracking within a building to all the way across continents.

Smart City Applications: IoT is finding many applications in municipal governance from automated utilities monitoring to smart streetlights, traffic and parking management, energy, and waste management to public transportation applications. Cable operators are uniquely positioned to assist in accelerating many of these applications (refer to Smart City working group at [12]).

Some of these applications intersect in terms of service offerings. For example, smart communities can provide wellness applications along with smart city applications on the managed public Wi-Fi infrastructure.

All the above evolving solutions can provide a huge differentiator for cable operators if they are ahead with their infrastructure to monetize them through flexible and managed offerings at the service delivering locations.

4. Special needs of IoT applications

The vast array of new IoT applications – some of which we outlined above - bring with them many special needs. Let's explore some of the key needs of these IoT applications across various dimensions.

4.1. Location needs

The first dimension we will look at is location. The location where a service is delivered has a major impact on many other requirements across many other dimensions as well. The location determines the scope of the service, and hence the prebuilt modular components that can be deployed in that location are determined. Table 1 gives a high-level view of the typical location where certain types of IoT services are delivered.

Table 1 - Location where services are being offered by current and some future applications

Service	In single-family homes	In multi-dwelling homes	In business premises	In common areas	In public places
Traditional quad-play	x	x	x		
Residential IoT	x	x		x	
Business IoT			x		x
Smart city applications			x	x	x
Telehealth applications	x	x	x		
AIP applications	x	x		x	x

4.2. Security needs

The second dimension we look at is security. Security is another dimension that has broad implications across many areas of an IoT application. IoT devices and applications can expose sensitive data and details about subscribers. Modern networks must be architected to protect and isolate these devices. The network should be capable of identifying the devices that run on it, and where possible, implement security controls based on this device's identity. Devices should be explicitly and securely onboarded on to the network using standards such as Wi-Fi Alliance's Easy Connect protocol, which gives devices unique credentials on the network that can be easily updated on a per-device basis and does not require re-credentialing of all the devices on the network.

In addition to device identity, the network architecture should allow devices to be isolated and segmented based on several factors including device type, function, or risk. For example, medical devices may be put on a network that is separate from other smart home devices. This would allow for access controls scoped to the medical device and prevent generic smart home devices from connecting to the medical device.

Finally, future networks should be able to recognize if the behavior of a device is acting outside of established bounds. This could be accomplished deterministically using a device's Manufacturer Usage Description (MUD) which gives explicit ports and protocols that the device is allowed to communicate with over the network, or probabilistically using heuristics or machine learning.

4.3. Reliability needs

As we move from entertainment services to many more mission critical services in the customer premises, the need for system reliability increases significantly. Telehealth services in the home, industrial IoT and connected vehicle support applications will require high availability.

4.4. Timing/Latency needs

Many real-time applications like industrial IoT and connected vehicle support applications that will require stringent network timing and latency control. Since not all applications have the same level of need, it is best to architect the wiring closet based on the needs of the applications being served.

4.5. Power needs

Once again, the applications requiring high reliability will also require reliable power. Backup power will commonly be needed in many cases. The location of the wiring closet will determine the powering options. Battery backup will commonly be needed in many cases. The type of applications being supported by the wiring closet and the location will determine the battery backup options

Power has many considerations in this infrastructure. There are power sources, power demands and power distribution which must work in concert.

4.5.1. Power sources

Let's look at some of the typical power sources that can be used for these applications.

4.5.1.1. Utility power

Utility power is the most abundant of the power source which is available at all but a few potential deployment sites. The North American power grid is delivered to customer premises using a 120V/240VAC single split phase deployment. The same grid can deliver this 120/240VAC service to businesses, but 3 phase utility power is also delivered to businesses. These 3 phase deliverables can be modified using a transformer to deliver the common 120/240VAC used elsewhere, so this utility power standard will be referenced throughout this document. The frequency of the utility AC waveform is constant throughout North America using a 60Hz standard.

Most electronic devices considered for this IoT infrastructure deployment support utility power using a universal utility AC power supply or power pack which can directly connect to the utility grid for powering. These packs are reliable, cost effective and energy efficient. The packs come in a wide range of capacity to drive both the direct device needs as well as those that may be hosted by these devices.

Though the utility grid is ubiquitous and capable there can be issues with its delivery. A utility or grid outage is a common term for these delivery issues. In most cases these outages are of a short duration and more of a nuisance for the end user, but the electronics and services supported by this IoT infrastructure system could provide "Lifeline" services, so any interruption of their operation can create a bad scenario. The following steps should be taken to improve resiliency and reduce trouble calls:

- Limiting user intervention to the power source of the IoT infrastructure.
- Avoiding a "switched" outlet and have a dedicated power circuit, if possible, with a clearly marked circuit breaker in the panel.

4.5.1.2. HFC plant power

HFC plant powering is one of the oldest methods of proving CPE power in a cable network. eMTAs and ATAs are also commonly powered by the cable HFC plant. HFC plants typically power the copper network and associated actives using 63VAC or 89VAC power supplies. This power can be routed anywhere the hardline plant is deployed and extended to the customer though the use of power passing taps. The older HFC CPE power passing taps could only support about 300mA, but newer power passing taps can support 2+ Amps of HFC power to the CPE devices.

There are some considerations while using HFC plant powering:

- The load on the HFC plant must be considered in larger, high current deployments. The typical HFC power supply has a capability of delivering 15A @ 90VAC routinely; but if the IOT infrastructure demanded 2 Amps for each site this would quickly exhaust the available power.
- HFC plant powering could be used as a primary or backup source of power, but once again, a high demand would exhaust the HFC powering batteries quickly; additional batteries might have to be added to the HFC powering location to address this additional power demand. The HFC plant is very efficient at propagating RF signals, but slightly less efficient at conveying the HFC powering. Losses occur through the hardline, actives, passives and largely in the customer drop. The end of line voltage range would need to accommodate a volage range from 45 to 90VAC.

4.5.1.3. Hybrid fiber power

The Hybrid Fiber Power solutions have been deployed in cellular tower deployments as well as similar high voltage low current powering of DSLAMs. PON architectures could provide centralized powering sources and hybrid power cable with converters in the IoT infrastructure cabinet to provide the needed power for the supported electronics. The basic designs leverage several 24 AWG to 12 AWG conductors to allow a high voltage low current transmission, some touting distances of up to10kM. The hybrid fiber powering could be delivered as a primary or backup source of power and communications.

4.5.1.4. Local renewable power

Consumers and businesses are deploying renewable energy resources at their sites and these sources can be leveraged to power our IoT infrastructure hardware. Solar, Wind, Micro-Hydro are the main sources of these renewable energy systems and there are several modes of operation of these systems: Grid Direct, Off grid, and Hybrid. Grid direct and Hybrid are most likely what would be used in concert with our IoT infrastructure; but our connection considerations are very different in those two deployments. Grid Direct systems rely on the utility grid for operation, and the loss of the utility grid causes these systems to shut down for safety reasons. The IoT infrastructure would be connected to a panel as it would in a utility deployment, the major difference is that during renewable production the IoT infrastructure would be powered from the renewable energy source. The Hybrid renewable system includes storage and handles grid loss a bit differently by disconnecting itself and its loads from the Grid to assure safety, but a "Backup Loads Panel" would be powered by the Hybrid system and its storage. In this case all the IoT infrastructure should be tied to the backup loads panel to assure operation through utility outage events.

4.5.2. Backup power considerations

The IoT infrastructure will likely support lifeline services and will require resilient powering. There are several ways of providing resilient backup power. We will look at some of the most commonly available options below. The amount of backup time these systems provide can vary, so the right option should be used depending on the application.

4.5.2.1. Interdevice batteries

One of the longest deployed backup powering scenarios in cable is the use of a backup battery in an eMTA. A similar method could be used to maintain the IoT infrastructure powering. The battery could be placed in the device itself or located externally. The device can be used to charge the battery. The size of the battery should be sufficient to meet the needs of the application.

Battery based backup is very efficient from both a cost and round-trip power utilization point of view. However, it can prove to be an extra burden when the batteries reach their end of life and must be replaced. Most of these battery backup solutions include battery monitoring for run time and battery health.

4.5.2.2. External UPS

External UPS devices are probably the second widest deployment of backup power for cable user equipment deployments. These are external units that are plugged into the utility and then the supported cable hardware is plugged into them. These systems are largely not monitored, which can create a "delayed outage" scenario where the system runs for a time during a utility event, but when the battery is exhausted in these external UPS devices the hosted IoT infrastructure system goes dark. There are both consumer and industrial grades of UPS devices, with the industrial scale devices providing longer runtime better monitoring options and survivability.

4.5.2.3. Whole house backup

Behind the meter storage and other large scale backup solutions are similar hybrid renewable system that can leverage renewable sources. The idea is that a large battery bank is hooked to an inverter/charger which can provide a backup power source for many powered devices in the premises. The system will disconnect from the grid during a power outage and through a backup loads panel can provide service during the utility outage. The IoT infrastructure electronics would need to be connected to the backup loads panel for power.

4.6. Interoperability needs

With the evolution of IoT technology, a broad range of devices, applications, and services have been deployed in the customer premises networks today. The IoT framework of the future must provide some means of integrating all these devices and applications in a consistent manner.

5. Opportunities for cable operators

So why should cable operators care about these emerging new services in their customer premises networks – especially given all the complexity they bring with them?

It is precisely the complexity that has stymied the widespread deployment of these IoT services in the market. Numerous technology vendors are vying to capture the market – but, at best, most have only succeeded in delivering point solutions to one specific application they control.

We believe that cable operators are ideally placed to take full advantage of their central role in the customer premises network to pull all the pieces of the puzzle together and thereby unlock a lot of potential value in their customer's IoT environment.

It is also clear that many proprietary solutions currently being deployed will only find limited success in the marketplace. For any widespread deployment, a standards-based approach will be needed.

6. Wiring closet concept

The traditional infrastructure cable operators placed in the customer premises was simple and compact. All that was needed was a small enclosure or a closet to house it all. This was commonly known as the Wiring Closet or Telecom Closet. As we outlined above, the needs of the customer premises – and even the customers themselves – have evolved significantly. So, what is the new "Wiring Closet" of the future?

It is clear the needs of customers will vary a lot from a single-family home subscribing to basic cable to a municipality supporting various smart-city applications. Obviously, we cannot have a one-size-fits-all solution for all these applications. It is also clear the customer premises infrastructure of the future will not necessarily even be a closet. The idea is to develop a customer premises framework that provides a standard and modular way of scaling from a simple wiring enclosure to a distributed set of resources where necessary.

The following are the three basic characteristics of a Wiring Closet:

- Expandable to current and future IoT applications
- Address the spectrum of needs from in-home to public areas
- Serviceable unit for the cable operators

7. Wiring closet requirements

What are the requirements for such a broad framework to support IoT services in the customer premises network? That is one of the main questions the WCDG group is trying to address at the SCTE. While this is still a work in progress, we highlight a few key requirements in this section that the group feels are necessary for any such framework.

7.1. Customer premises location requirements

As we noted above, various IoT applications need to be supported in different locations in a customer premises. Following locations must be supported by the customer premises framework.

- Single Family Units: Support in indoor and outdoor locations.
- Multi-Dwelling Units: Support in unit indoor and outdoor locations as well as common area indoor and outdoor locations.
- Commercial Units: Support in indoor as well as common area indoor and outdoor locations.
- Public Spaces: Support in a cabinet as well as pole mounted locations.

7.2. Networking requirements

Customer premises framework needs to support both wired and wireless networking infrastructure.

- Wired infrastructure should preferably be supported for premises distribution where wireless distribution is challenging and for fixed devices.
- Wireless infrastructure should be supported for mobile devices. Adequate signal coverage throughout the customer premises should be ensured.

7.3. Security requirements

As noted above, security is critical for many IoT applications. As such, the customer premises framework shall support comprehensive security capabilities including following:

- All communication links shall support authentication, authorization, and encryption capabilities.
- Wireless Access Points shall support authentication and encryption capabilities.
- Gateway devices shall support secure boot and secure upgrade capabilities.
- No default login credentials should be supported. In addition, security infrastructure should be upgraded to the latest available standards.
- Any test/diagnostic access ports shall be disabled by default or require secure login.

7.4. Powering requirements

Many IoT applications have special powering needs. As such, the premises infrastructure should support following powering requirements.

- The premises infrastructure shall support following options as power sources:
  - AC utility mains
  - HFC 60V/90V
  - Power over Coax
  - Power over Ethernet (PoE)

7.5. Environmental requirements

Since the premises infrastructure will have to support a wide range of premises locations, it needs to meet a broad range of environmental needs. Following are some of the key environmental requirements the premises infrastructure will need to support.

- The premises equipment shall support installation in indoor enclosure, outdoor enclosure, outdoor cabinet installation, and outdoor pole mount enclosure.
- The equipment shall meet all necessary environmental and safety requirements per ETL, UL, and NEMA.
- The equipment shall meet all local building and environmental codes.

7.6. Installation and support requirements

Due to the broad range of potential IoT applications that could be installed in the customer premises and the resulting complexity, the premises framework will need to meet numerous installation and support requirements.

- All serviceable equipment must be located in an area offering easy access for service personnel

- Basic infrastructure should be pre-installed in any new building construction
- Auto-configuration processes should be used where possible to minimize user intervention
- Installer should ensure adequate signal coverage throughout the premise (e.g., Wi-Fi signal coverage)
- All installed equipment and infrastructure should be well labeled and documented
- Support responsibilities should be clearly outlined along with contact information for responsible party
- Maintenance responsibility for any backup batteries should be clearly specified along with necessary maintenance schedule
- Installation should support notification of low/failed/missing backup battery condition to service personnel
- Equipment installations should support easy hardware upgrade.
- Devices deploying software should preferably support automatic online software upgrades.

7.7. Reliability requirements

Many IoT applications will potentially support critical healthcare or business support services that will have high reliability expectations. Following are some of the reliability requirements the premises infrastructure needs to meet:

- Power Reliability: Backup power should be made available depending on the type of application and location needs.
- Communication Reliability: A backup communication link may be necessary in case of failure of primary communication link.
- Device Reliability: Devices providing critical services such as healthcare support should have built-in redundancy or a spare available.
- Service Reliability: Critical services must be supported by a highly reliable support infrastructure including a 24x7 support team.

7.8. Interoperability requirements

It is not enough for IoT applications to function by themselves. To minimize complexity for the user as well as to make applications easier to use, the customer premises framework should provide a common infrastructure for applications to interface with each other. Following are some of the interoperability requirements the premises infrastructure needs to meet:

- The customer premises framework should support a common infrastructure for applications to interface with each other.
- The framework should support a consistent way of managing all the applications and devices in the customer premises.

8. Conclusions and next steps

In this paper we have clearly outlined the need for developing a comprehensive framework for supporting the vast array of IoT applications and services in customer premises networks from simple single-family homes to large city-wide smart-city networks. Such a framework will enable widespread deployment of a multitude of value-added services in the near future and place the cable operator in a pivotal role in this vast ecosystem.

The first step in getting to such a framework is to develop a comprehensive set of requirements to be supported by this framework. We have highlighted a number of key requirements in this paper, but much more work must be done. The WCDG group is looking for subject matter experts from a broad range of areas to come and contribute to this work.

Abbreviations

AIP	aging in place
ETL	Electrical Testing Laboratories
HFC	hybrid fiber coax
IoT	internet of things
MDU	multi dwelling unit
NEMA	National Electrical Manufacturers Association
PoE	power over ethernet
POTS	plain old telephone service
SCTE	Society of Cable Telecommunications Engineers
SFU	single family unit
T4W	telecom for wellness
UL	Underwriters Laboratories
VoIP	voice over internet protocol
WCDG	wiring closet drafting group

Bibliography & References

[1] SCTE 266-2021: *IoT Recommended Premises Network Infrastructure Practices for Cable Operators*
[2] Rajesh Abbi, Changing Landscape with IoT, Dec 2021, available here
[3] Duke Tech Solutions market research, *Telehealth market report – A Telecom based opportunity analysis*, available here
[4] Sudheer Dharanikota, *Summary of Telecom for Wellness interviews*, Oct 2021, available here
[5] Clarke Stevens, Sudheer Dharanikota, *Aging in Place and Telehealth Use Cases from the Cable Operator Perspective*, SCTE Journal, March 2022, available here
[6] Sudheer Dharanikota, Ayarah Dharanikota, *Why are cable operators natural fit to support Telehealth – An inter-industry perspective*, 2020 SCTE Expo, available here
[7] Sudheer Dharanikota, Ayarah Dharanikota, Dennis Edens, Bruce McLeod, *Aging in Place business case for cable operators*, SCTE Journal, June 2021, available here
[8] Sudheer Dharanikota, Ayarah Dharanikota, Dennis Edens, Bruce McLeod, *Telehealth business case for cable operators*, SCTE Journal, September 2021, available here
[9] Sudheer Dharanikota, Clarke Stevens, *End to end Telecom for Healthcare architecture – a cable operator perspective*, 2021 SCTE Expo, available here
[10] SCTE Data Standards Subcommittee, Working Group 3, Aging in Place, available here
[11] SCTE Data Standards Subcommittee, Working Group 4, Telemedicine, available here
[12] SCTE Data Standards Subcommittee, Working Group 1, Smart Cities DG, available here
[13] SCTE Data Standards Subcommittee, Working Group 1, Wiring Closet DG, available here

