ELECTRIC POWER RESEARCH INSTITUTE

Utility Telecom Taxonomy and Architecture for Field Area Networks

3002009786

Utility Telecom Taxonomy and Architecture for Field Area Networks

3002009786

Technical Update, May 2017

EPRI Project Manager

T. Godfrey

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THE FOLLOWING ORGANIZATIONS PREPARED THIS REPORT:

CDKnudsen & Associates

Drucker Associates

Electric Power Research Institute (EPRI)

This is an EPRI Technical Update report. A Technical Update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ACKNOWLEDGMENTS

The following organizations prepared this report:

CDKnudsen & Associates
41 Blaine Cir
Moraga, Ca. 94556

Principal Investigator
C. Knudsen

Drucker Associates
12124 NE 144th St.
Kirkland, Washington 98034

Principal Investigator
E. Drucker

Electric Power Research Institute (EPRI)
3420 Hillview Avenue
Palo Alto, California 94304

Principal Investigators
T. Godfrey
J. Herman
B. Ealey

This report describes research sponsored by EPRI.

This publication is a corporate document that should be cited in the literature in the following manner:

Utility Telecom Taxonomy and Architecture for Field Area Networks. EPRI, Palo Alto, CA: 2017. 3002009786.

ABSTRACT

A utility communications network is a highly complex system composed of wired and wireless systems, firewalls, routers, data centers, and security mechanisms that span a large and diverse geographic area. Technology and architectural options can be applied in varied combinations to develop a communications system. The process, however, is compounded by the diversity of non-standard and standard technologies as well as the complex and fast moving pace of new technologies. The purpose of this document is to help utilities define their distribution system and grid modernization wireless communication needs. Consideration is given to the overall architecture and its implications for the wireless components.

Approaches will be mapped out for creating specific baseline utility communication architectures and determining technology choices, including the following:

- A list of specific technologies mapped to a taxonomy organized into a structure with graphical relationship diagram(s) to show categories and interdependencies
- An architecture decision tree to help determine possible sets of technologies that can best be applied in light of utility needs and constraints

Complex factors contribute to making a communications system decision. This decision is compounded by the fact that the system will need to be in place for the next 20 years, and once deployed, it will be very difficult or impossible to change. It is therefore critical that this process focus on quantified metrics to help make such decisions under specific conditions.

Keywords
Wireless taxonomy
Distribution automation
Telemetry
Control
Communications network
Architecture decision tree

ACRONYMS

AMI	Advanced Metering Infrastructure
ARRA	American Recovery and Reinvestment Act of 2009
bps	bits per second
BRS	Broadband Radio Service
CapEx	Capital Expenditure
CBRS	Citizens Broadband Radio Service
CPE	Customer Premise Equipment
CTS	Clear to Send
DER	Distributed Energy Resource
DSP	Digital Signal Processor
EBS	Educational Broadband Service
eMTC	enhanced Machine Type Communication (aka LTE-M)
EPC	Evolved Packet Core
FAD	FAN Aggregation Devices
FAN	Field Area Network
FCC	Federal Communications Commission
FirstNet	First Responder Network Authority
FLISR	Fault Location Isolation and Service Restoration
FNPRM	Further Notice of Proposed Rulemaking
4G	Fourth Generation (cellular technology)
GAA	General Authorized Access
GHz	gigahertz
GMS	Grid Management System
IED	Intelligent Electronic Device
IP	Internet Protocol
ISM	Industrial, Scientific, and Medical (radio band)
ITFS	Instructional Television Fixed Service
kbps	kilobits per second
kHz	kilohertz
LAN	Local Area Network
LMR	Land Mobile Radio
LMS	Location and Monitoring Service
LPWAN	Low-Power Wide-Area Network
MAC	Media Access Control
Mbps	megabits per second
MDS	Multipoint Distribution Service

MHz	megahertz
M-LMS	Multilateration Location Monitoring Service
ms	millisecond(s)
M2M	Machine to Machine
MVNO	Mobile Virtual Network Operator
NIST	National Institute of Standards and Technology
NPRM	Notice of Proposed Rulemaking (FCC)
NTIA	National Telecommunications and Information Administration
OEM	Original Equipment Manufacturer
OFDM	Orthogonal Frequency-Division Multiplexing
OpEx	Operating Expenditure
OTA	Over-the-Air
PAL	Priority Access Licensee
PDN	Packet Data Network
PER	Packet Error Ratio
PHY	Physical Layer
PSCR	Public Safety Communications Research
PtMP	Point-to-Multipoint
PTP	Point-to-Point
PV	Photovoltaic
PVNO	Private Virtual Network Operator
QoS	Quality of Service
PAL	Priority Access Licensee
RAN	Radio Access Network
REAG	Regional Economic Area Group
RF	Radio Frequency
RTS	Request to Send
s	second(s)
SAS	Spectrum Access System
SCADA	Supervisory Control and Data Acquisition
SCE	Southern California Edison
SDARS	Satellite Digital Audio Radio Service
SDG&E	San Diego Gas & Electric
SIM	Subscriber Identification Module
SNR	Signal-to-Noise Ratio
TBD	To Be Determined
3GPP	3rd Generation Partnership Project
UE	User Equipment

ULS	Universal Licensing System
U-NII	Unlicensed National Information Infrastructure
USD	U.S. dollars
UTC	Utilities Telecom Council
UVNO	Utility Virtual Network Operator
VPN	Virtual Private Network
WAN	Wide Area Network
WCS	Wireless Communications Service
WID	WAN Interface Device
WiMAX	Worldwide Interoperability for Microwave Access
WRC	World Radio Conference

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1
PURPOSE

The energy industry agrees that there is a need to improve the performance, reliability, and security of utility communications systems used for distribution automation, telemetry, and control. Such a communications network is a highly complex system composed of wired and wireless systems, firewalls, routers, data centers, and security mechanisms that span a large and diverse geographic area. This update focuses on the wireless aspects of such a system, but gives consideration to the overall architecture and its implications for the wireless components.

Technology and architectural options can be applied in varied combinations to develop a communications system architecture. The process, however, is compounded by the diversity of non-standard and standard technologies as well as the complex and fast moving pace of new technologies. **The purpose of this document is to help utilities define their distribution system communication needs, understand the hierarchy of technology options, and determine how to best approach the process of choosing an architecture and technologies that will meet their needs.**

Figure 1-1 helps to define how the wireless taxonomy integrates within the EPRI Telecom Initiative.

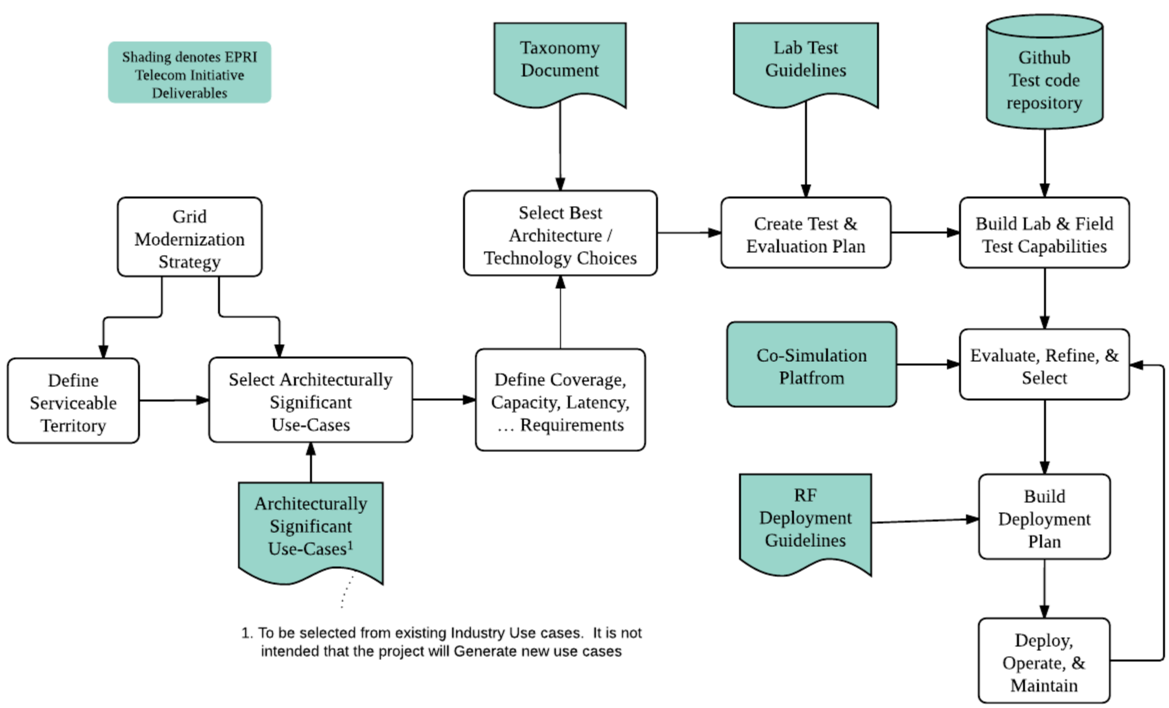

Figure 1-1
Integration of Wireless Taxonomy Within the EPRI Telecom Initiative

2 SCOPE

The scope of this update will be to identify ways to define and characterize utility grid modernization wireless communication needs. Approaches will be mapped out for creating specific baseline utility communication architectures and determining technology choices, including the following:

- A list of specific technologies mapped to a taxonomy organized into a structure with graphical relationship diagram(s) to show categories and interdependencies
- An architecture decision tree to help determine possible sets of technologies that can best be applied in light of utility needs and constraints

Testing, deployment guidelines, operations practices, and maintenance guidelines will be covered in subsequent sections of EPRI's Telecom Initiative. A large body of work has also been completed consisting of available industry use cases and requirements. The scope of this effort will not focus on the development of any use case but rather will leverage existing knowledge and information.

For the purposes of this effort, the communications system does not extend into the data center but rather defines clearly dimensioned interfaces to the data center. Intra-data center communications are out of scope for this document, and the expectation is that data center communications will be designed to support the necessary interface requirements.

3
APPROACH

The communications system is the fabric that spans the entire utility. In concept, the system is agnostic in terms of technology and only requires a certain level of performance, reliability, and security between a defined set of nodes on the network. Such a system can be segmented into an extensible set of tiers, where each tier will provide a particular level of service. Specific technologies can then be mapped to each tier, and different applications can be mapped to one or more of the tiers depending on their needs as defined by business requirements. Technologies and tiers can overlap as any single technology could support multiple tiers. Similarly, applications can use more than one tier or different tiers depending on the application demands.

The focus of this document, depicted by the shaded area of Figure 3-1, will be to map technology sets to logical tiers of service defined by known requirements and the natural break points of current and emerging technologies. This segmentation will then be used to help clarify and define specific communication architectures.

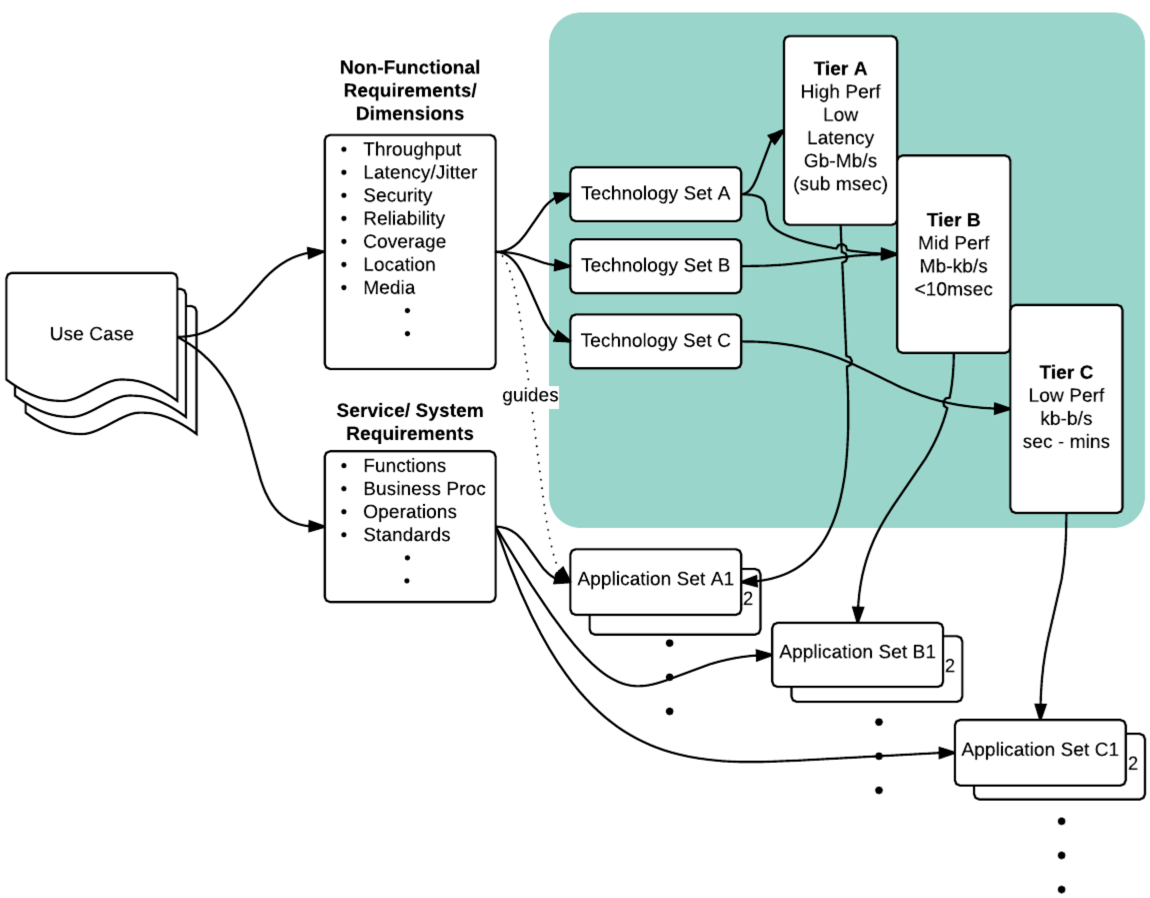

Figure 3-1
Communication System

Technology choices can be mapped into domains defined as centralized, distributed, and edge, as shown in Figure 3-2. These domains have been defined within Southern California Edison's *Grid Modernization Initiative: Grid Management Architecture* document[1].

The ***centralized*** domain is the data center environment operated by the utility or on the utility's behalf in the Cloud.

The ***distributed*** domain is provided by infrastructure in the middle of the communications and electrical systems. This includes equipment in substations, poles, and underground vaults. The distributed domains are larger in number (thousands), require medium levels of effort to update, have intermediate infrastructure lifetimes (5–15 years), offer intermediate levels of processing power, and have bandwidth that varies from a fiber optic link to the equivalent of a cellular data connection.

The ***edge*** domain is provided by infrastructure at the edge of the network. This includes transformers, reclosers, cap-bank controllers, meters, and the like. The edge domain is not segmented by element ownership. Any device that can be controlled by the grid management system (GMS) is assumed to be within the boundary of the system. For example, a residential photovoltaic (PV) system may be owned by the customer, but the interface to the GMS allows the device to be controlled to effect distributed energy resources (DERs) load balancing. The edge environments are multitudinous in number (millions), require high levels of effort to update, have extended equipment lifetimes (15 years or more), may offer very low levels of processing power, and may have bandwidth equivalent to a dial-up modem link.

These can typically be mapped to well-known boundaries such as the core utility network (central), substations (distributed), and intelligent electronic devices (IEDs) or meters (edge). There are also many cases in which these boundaries are blurred, for example, an IED with distributed computing resources that can gather local data, communicate with peers, and take action based on a local algorithm. In this case, the IED is within both the edge domain and the distributed domain depending on the task it is performing.

---

[1] "DISTRIBUTECH 2016: INTRODUCING THE NEXT-GENERATION GRID-MANAGEMENT SYSTEM AT SCE," Edison International, accessed 28 April 2017. http://www.edison.com/home/innovation/grid-modernization.html.

Grid Modernization Initiative: Grid Management Architecture. Southern California Edison: 2016. http://www.edison.com/content/dam/eix/documents/innovation/SCE%20Grid%20Management%20System%20Architecture%202.1.16b.pdf.

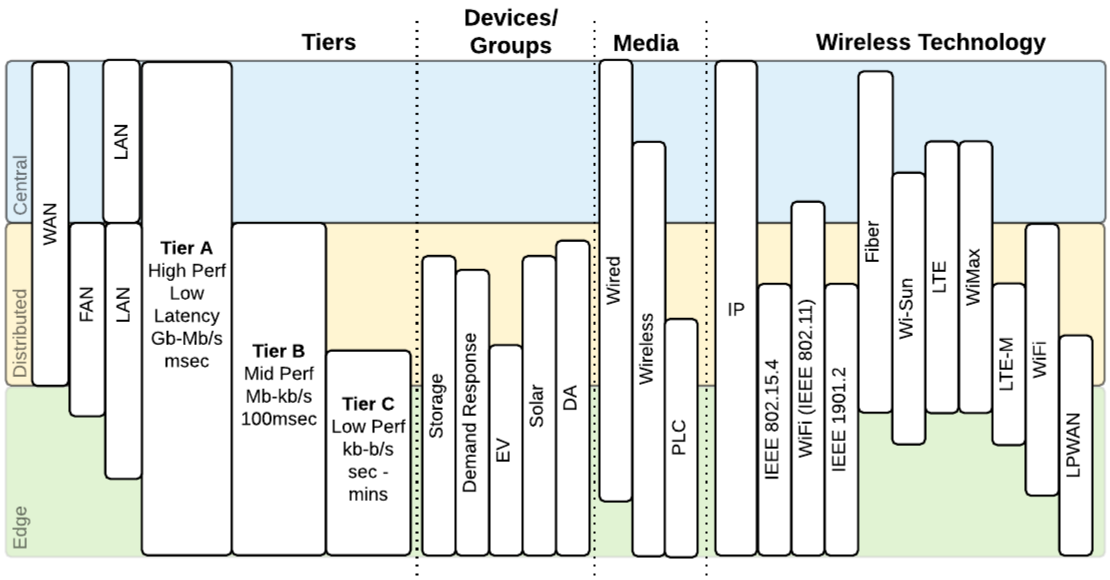

Figure 3-2
Groups of Applications and Performance Segmentation

Using these concepts, a utility can identify the groups of applications and performance segmentation it needs across its serviceable territory and the domains within that territory. There is no single right answer, and the choices of technology and architecture will be highly dependent on legacy applications, size, budget, and regulatory constraints. Some will be greenfield and some will need to migrate gracefully over time. Some will need at least a mid-tier network nearly everywhere with pockets of high-tier performance for specific applications, while others will have the ability to extend fiber broadly and have little need for the lower tiers. These concepts allow a utility to confidently select an architectural framework for a communications system that can then be used to define a more specific technology selection and plan for integration and deployment.

An example framework employing a superset of tiers and technology choices is depicted in Figure 3-3. In this example, it is clear that the communication fabric is actually a system of systems. Field area network (FAN)1 provides the majority of coverage, while FAN2 and FAN3 are used for fill-in and hard to reach locations. Wide area network (WAN)2 is a fiber core, while WAN1 provides high-performance tiers to specific locations in the distributed and edge domains.

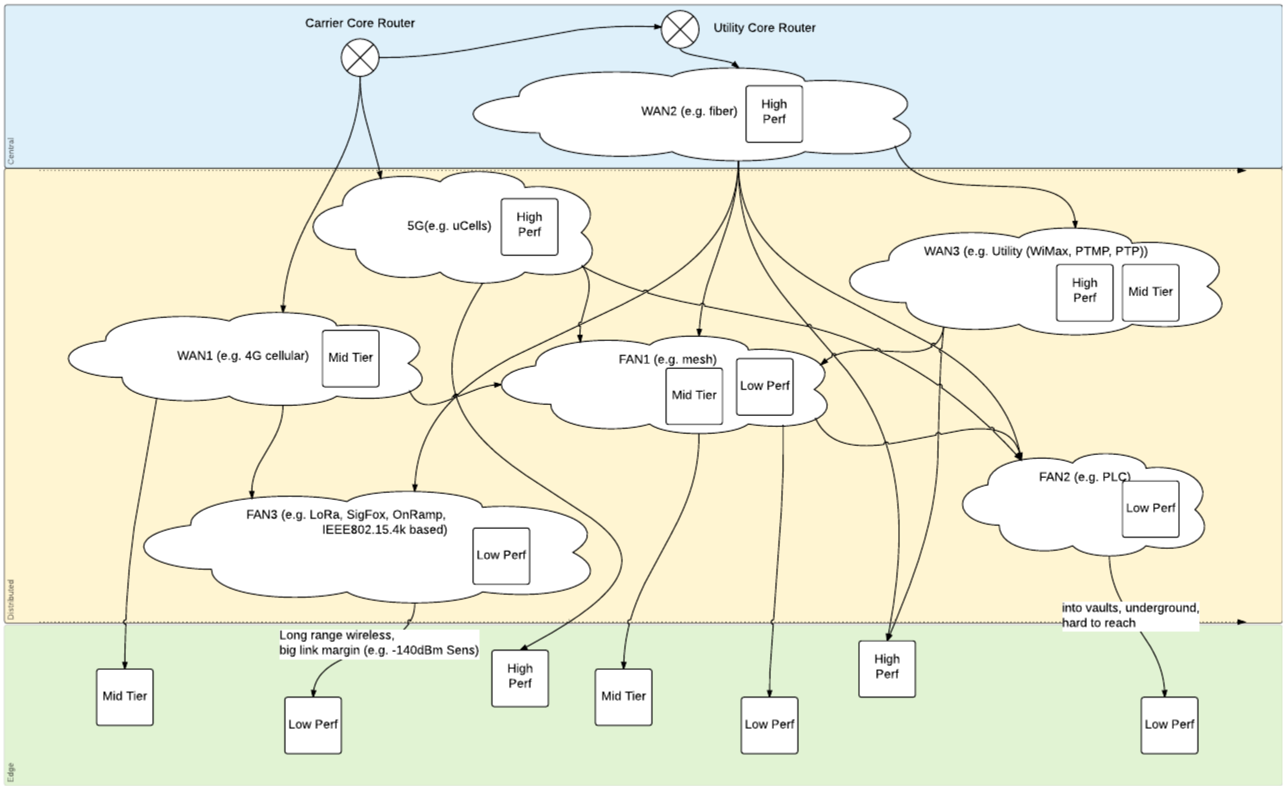

Figure 3-3
Example Framework with a Superset of Tiers and Technology Choices

Wherever possible, the definition of specific technologies will be based on industry standards. The use of standards-based technology has many benefits including multi-vendor sourcing, multi-vendor interoperability, backwards compatibility, extensibility, and graceful migration to future technologies. In the absence of industry standards for a specific needed technology, minimal non-standard optionality will be employed. For these cases, detailed profiles will be defined such that internal compliance can be maintained across vendors and can create the artifacts necessary to move the industry to a more formal industry-alliance-supported interoperability model. This is an important concept as the alternative is to accept proprietary systems, vendor lock-in, and a limited or impractical path for technologies to evolve and extend over time. Interoperability, backwards compatibility, and extensibility are key tenets of the communications fabric. Maintaining compatibility through standards allows for older systems to migrate gracefully to newer technologies and provides a path for future technologies to be added over time without service disruption or “forklift upgrades.”

Ultimately, there is a minimal set of “best architectures” that can be derived from the taxonomy of technology choices. Utility-specific business and regulatory drivers, specific topology and morphologies, and architecturally significant use cases will define boundary conditions for each utility. A decision tree tool and a graphical representation of the taxonomy will be developed to assist in the architecture selection process.

4 TECHNOLOGY HIERARCHY

A technology hierarchy will be defined consisting of the areas listed below. Each technology will be defined as it applies to the utility industry. A relative comparison across a set of common metrics will be created to help with the architecture decision process. It is important to note that it is easy to get too complex and deep in technology details. The goal of this effort will be to keep the scope such that the output can be practically applied to real-world architectures and deployments.

4.1 Technology Summary Format

The technology definition will be broken down into the following summary structure:

- Description of the technology
- Current state of the art in the industry as applicable to utilities
- High-level comparative metric table and summary
- Links to other documents and resources throughout the report

4.2 Technologies

This section presents an overview of the set of technologies available to utilities that can provide FAN communications for distribution systems. The technologies vary greatly in performance, cost, and complexities. It is also very difficult to absolutely quantify the performance metrics because they are highly dependent on many variable parameters (for example, deployment density, antenna height, configurations, applications, and traffic densities). The list of technology types includes mesh systems in the industrial, scientific, and medical (ISM) unlicensed bands, Wi-Fi, WiMAX, and Long Term Evolution (LTE) technologies. Table 4-1 provides a subjective comparison of criteria for some of the features, performance metrics, and trade-offs for each category, while Table 4-2 provides metric definitions for Table 4-1. The table is keyed to low, medium, and high values, with red being low, medium being yellow, and green being high in terms of the metric being evaluated. These metrics are meant to be high-level system performance measures that allow a subjective comparison of the technologies. NISTR 7761[2] provides a deeper definition of very specific performance parameters and metrics for wireless systems.

[2]U.S. Department of Commerce. National Institute of Standards and Technology (NIST). *NIST Priority Action Plan 2: Guidelines for Assessing Wireless Standards for Smart Grid Applications*, February 2011. NISTR 7761. http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/PAP02Wireless/NISTIR7761.pdf

Table 4-1
Subjective Comparison of Criteria

	WiSUN (Mesh)	LPWAN	Wi-Fi (Mesh)	Wi-Fi (PtMP)	WiMAX (3.6)	WiMAX (700)	LTE 4G (Com)	LTE 4G (MVNO/ PVNO)	LTE 4G Leased	LTE-M (aka eMTC
Throughput—Core	Hundreds of kbps	bps—Tens of kbps	Mbps	Mbps	Mbps	Hundreds of kbps	Mbps	Mbps	Mbps	Hundreds of kbps
Latency Core3	<100 ms	s	<10 ms	<10 ms	<100 ms	100 ms	<100 ms	<100 ms	<100 ms	TBD
Throughput—Peer-to-Peer	>100 kbps	N/A	Mbps	Mbps		Hundreds of kbps				TBD
Latency—Peer-to-Peer	<100 ms	N/A	<10 ms	<10 ms		<200 ms	<200 ms	<200 ms	<200 ms	TBD
Coverage Probability										
Capital Expenditure (CapEx)										
Operating Expenditure (OpEx										
Extensibility										
Scalability										
RF Coverage										
Spectrum Complexity	unlic	Unlic Sub-1 GHz ISM	unlic	unlic	"Lightly" lic/shared	lic	lic	lic	leased	lic
Interoperability										
Tier	mid	low	high	high	high	mid	mid	mid	mid	mid-low

[3] In evaluating any packet data radio communications technology for use in applications such as supervisory control and data acquisition (SCADA), it is important to examine both transmission latency and connection latency. Transmission latency is the end-to-end delay of packets through the communications network on *existing connections*. Connection latency is the time required to establish the connection through the network in the first place.

Table 4-2
Metric Definitions

Metric	Definition
Throughput—Core	The maximum throughput that can be achieved from the edge devices to the core systems.
Latency—Core	The lowest latency that can be achieved from the edge devices to the core systems. Note: Internet of things (IoT) optimized systems may be theoretically capable of low latency, but often do not enable it due to low duty cycle (long sleep time) system settings intended to reduce endpoint power consumption.
Throughput—Peer-to-Peer	Typical peer-to-peer throughput for devices in near proximity on a lightly loaded network, for example, fault location isolation and service restoration (FLISR) teams.
Latency—Peer-to-Peer	Typical peer-to-peer latency for devices in near proximity on a lightly loaded network (for example, FLISR teams). Note: cellular architecture does not support direct peer-to-peer. Depending on the system, the best case involves forwarding through the base station, while the worst case involves a round trip to and from the network core.
Coverage Probability	For a typical deployment, this is the probability of coverage for any device. This represents taking 100 devices randomly distributed across the defined serviceable territory and measuring how many meet a defined level of performance.
CapEx	Relative cost of infrastructure—does not include core systems.
OpEx	Relative operating costs—includes any recurring service fees.
Extensibility	How easy the system is to extend both in coverage and added capacity as the system needs increase and expand.
Scalability	How scalable the system is to readily handle 1 million nodes.
Radio Frequency (RF) Coverage	Relative coverage metric
Spectrum Complexity	Defines how complex or limiting the need for spectrum is to the system; for example, “unlic” (unlicensed) is simple, while “leased” or “purchased” is complex.
Interoperability	The ability to interoperate with other vendor systems—must have an industry compliance program for true interoperability. Simple implementation to a standard is not sufficient.

In summary, the mesh systems are relatively easy to deploy and can provide good coverage and adequate performance—trading off peak capacities for lower cost and greater flexibility. The table above includes two types of mesh systems. The first category is based on IEEE 802.15.4 technology (Wi-SUN), with data rates in the tens of kbps using frequency-shift keying (FSK) modulation and data rates in the hundreds of kbps using orthogonal frequency-division multiplexing (OFDM) modulation. The sub-1 GHz spectrum provides longer range and better coverage. The second mesh category is based on IEEE 802.11 (Wi-Fi) in the 2.4 GHz (and in some cases 5 GHz) bands, with data rates into the Mbps and <10 ms latency per hop. Due to the shorter range at 2.4 GHz, a larger number of mesh router nodes are required for full coverage, increasing cost.

In some applications, the ability of commodity Wi-Fi devices to connect is a benefit. The recently released 802.11ah amendment enables operation in the 915 MHz ISM band and could potentially improve range. Products based on 802.11ah are not yet commercially available. The lower data rate of IoT type LPWAN systems such as LoRa, provide good coverage but have very limited capacity and latency; these systems are more of a niche, hard-to-reach, telemetry, or slow control enhancement system. Wi-Fi point-to-multipoint (PtMP) systems can have good performance for the links that are enabled but can be very difficult to manage and scale. These products are often built around Wi-Fi technology but in practice are not interoperable. WiMAX systems can provide high capacity but are coverage-limited in the higher frequency bands. Spectrum has become available in the sub-GHz bands (such as the 700 MHz Upper A Block), but the bandwidth is limited making capacity over an area a challenge. Development of standards for this band is currently underway to adapt the mature 802.16 WiMAX technology to the smaller spectrum allocation. LTE is a very mature technology, and if utilities had access to the sub-GHz spectrum, this would be the obvious best choice for distribution control. As that is not the case, utilities employing LTE must manage through complex sharing agreements or as an overlay on top of other networks making reliability, long-term viability, and quality of service (QoS) challenging to manage. LTE-M for machine to machine (M2M) communication is still evolving and may provide a better solution than standard LTE.

As readers can see, there is no good clear answer as to what is the best choice for a utility distribution FAN. In fact, the right answer is more likely an integration of one or more of these choices into an overall communication fabric to support distribution system needs. The following sections will discuss each technology grouping in greater detail to help frame them such that the best choice can be made based on a particular utility requirements.

4.2.1 Wi-SUN

In most cases, utilities have very little or no private spectrum available to deploy and operate a communications network. This leaves them few choices other than capacity-limited land mobile radio (LMR), other narrowband solutions, commercial cellular, or unlicensed solutions employing wireless mesh technologies. In these instances, mesh solutions in the unlicensed ISM bands, while not delivering multi Mbps rates, can deliver good performance adequate to meet many, if not all, modernized distribution automation requirements.

This section will discuss technologies that employ a wireless mesh architecture using unlicensed spectrum in the 900 MHz and 2.4 GHz bands. Most employ IEEE 802.15.4g[4] with modifications or proprietary extensions. The Wi-SUN Alliance is working to align a common set of standards for utility FANs into an interoperable, certified set of profiles. Many of the leading Advanced Metering Infrastructure (AMI) vendors (for example, Silver Spring Networks, Landis+Gyr, Cisco, and Itron) are also members of the Wi-SUN Alliance[5] and include the following listed at this link: https://www.wi-sun.org/index.php/en/about-us/member-companies.

One of the biggest challenges today is that while the Wi-SUN Alliance is targeting interoperability—and all of the vendors will state that they are standards-compliant—no one single technology will interoperate across vendors. The Alliance profile contains many optional features and is working to define a common set of mandatory features. There are challenges as vendors do not desire mandatory features or are not able to agree upon a common set of features. In addition, there is a lack of utility participation and alignment around a unified set of requirements and insistence on vendor interoperability. Great opportunity exists for creating a unified interoperable profile around grid modernization requirements if utilities will engage and serve as arbitrator to drive vendor consensus. If utilities do not engage in this effort, the technologies will be relegated to vendor-proprietary, non-interoperable systems.

Figure 4-1 below depicts how this process might work. In the simplest sense, the Telecom Initiative utilities would align around a common set of requirements that could be represented by one or two individuals within the Alliance. Each utility would not have to contribute greatly to the standards effort other than to ratify the requirements and the need for a common set of interoperable mandatory features by all vendors. In addition, an EPRI reference design and an open source test repository based on work performed at Southern California Edison (SCE) would provide a basis for testing and developing products.

---

[4] "IEEE 802.15 WPAN™ Task Group 4g (TG4g) Smart Utility Networks," IEEE 802.15, accessed 28 April 2017. http://www.ieee802.org/15/pub/TG4g.html.

[5] Wi-SUN Alliance, accessed 28 April 2017. https://www.wi-sun.org/index.php/en/.

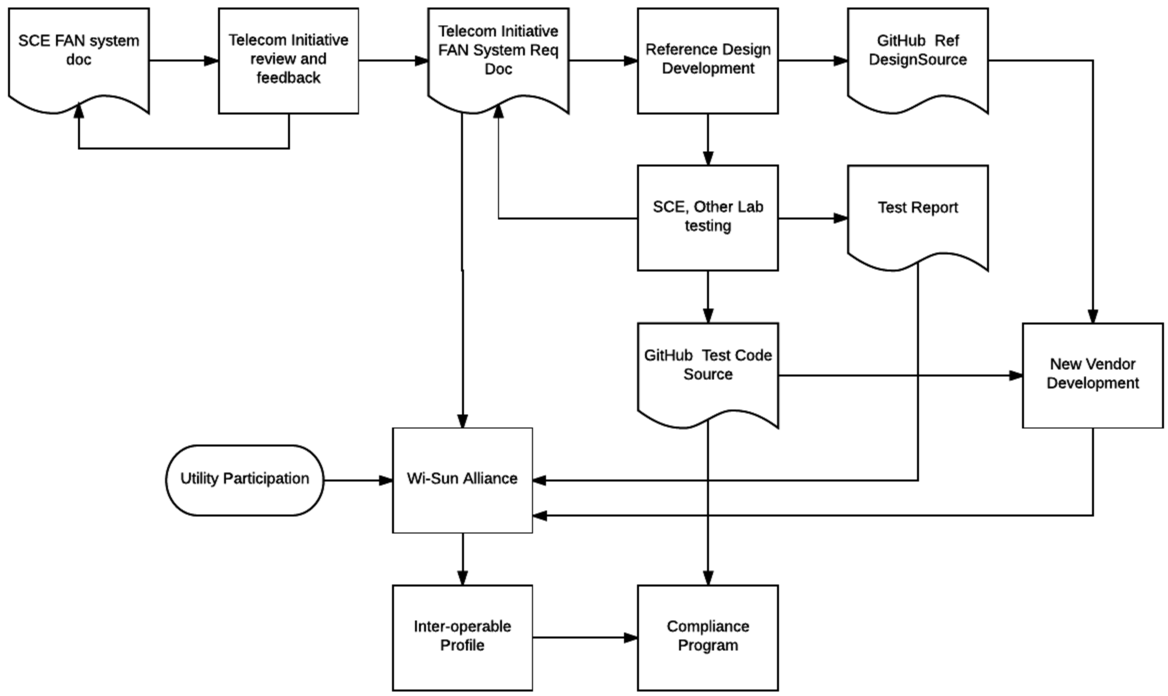

Figure 4-1
Standards Interoperability Trajectory Flow Diagram

4.2.1.1 Technology Overview

The new generation of unlicensed meshed technologies typically offer goodput rates of up to 1 Mbps and best case latencies of a 10–20 ms for a single hop. These technologies are comprised of many nodes that can route traffic to multiple neighbors and dynamically adjust the routes to accommodate traffic loading and interference. Aggregation node devices will have high capacity connectivity to a fiber core network and will be the egress point for communications from the FAN to core networks. Peer-to-peer routing within the mesh is also supported to allow local devices to communicate directly to a neighbor without having to route information to a central router. This is a key benefit of these systems in that relatively low latencies can be realized for peer-to-peer distributed computer applications. A typical system would be deployed having less than five hops 95% or more of the time and would provide latencies of better than 100 ms between regionally located field devices.

Architecturally, a mesh network, as shown in Figure 4-2, is comprised of FAN aggregation devices (FADs) and field devices. FADs are typically located at a point of high-capacity network connectivity such as a substation fiber, fiber extensions on a distribution line, a high-capacity overlay, or a PtMP link. Field devices mesh over wireless links. Today’s next generation mesh nodes employ multiple adaptive modulations with raw physical layer (PHY) rates exceeding 1 Mbps and single-hop, one-way latencies on the order of 10 ms. Early mesh systems were very application-specific and did not route alternative device traffic without cumbersome static routing and configurations, if at all. Current next generation systems should be able to route from any point on the network to any other point on the network with both Internet Protocol version 4 (IPv4) and IPv6 addressing. Typical specifications for a deployed system are <100 ms one-way latency for any devices routing under a common FAD and <500 ms for any cross-WAN communications. Use cases for grid-modernized distribution automation applications not only require substation-to-device communications but also significant amounts of low-latency peer-to-peer communications between field devices.

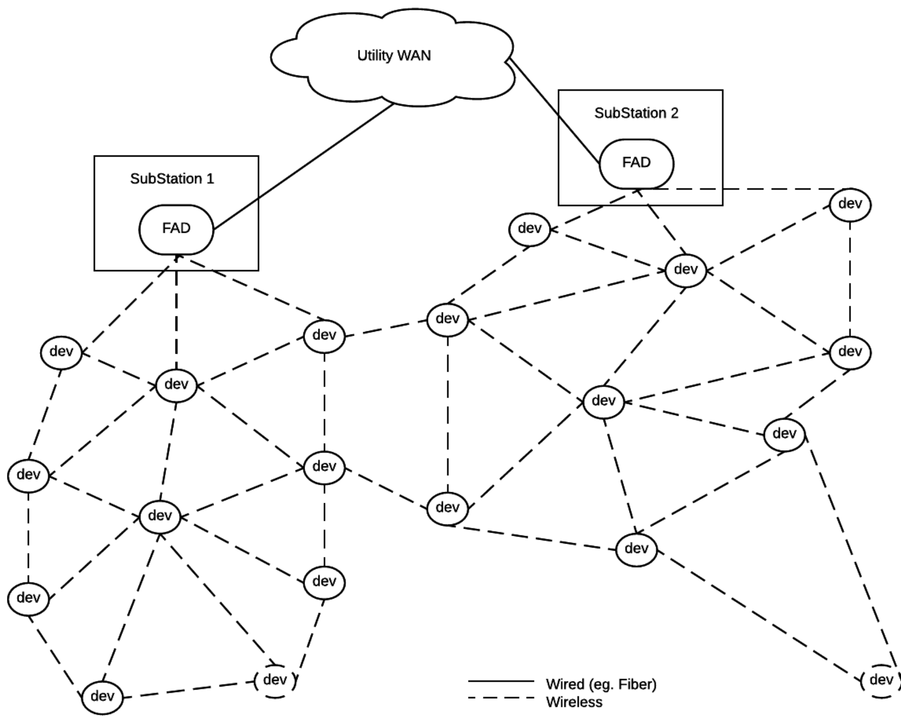

Figure 4-2
Mesh Network

From a capacity perspective, the FADs tend to be the serialization point of the network. In other words, the loaded capacity of a FAD is the limit of the amount of capacity that can flow from the devices in the field to the core applications. Another good rule of thumb is that every time the hops double, capacity decreases by more than half and latency is doubled. (Appendix C provides a more detailed discussion on the latency of these systems.) Contention at nodes in the network is mitigated through the use of backoff mechanisms such as increasing time to retry clear to send (CTS) with a degree of randomization. It is also important to understand that these types of networks function best when lightly loaded. Performance limits relative to traffic capacity and latency requirements need to be taken into consideration when defining deployment plans and system densities. Understanding how QoS mechanisms are implemented within the vendor systems is also important. QoS is something that many vendors support. Some use simple queue prioritizations, while others use more sophisticated media access control (MAC) layer mechanisms. In designing a system deployment model, it is critical to understand how QoS improves critical message performance as capacity increases. When designing a deployment, it is good to keep these factors in mind as the density of devices and FADs/field device ratios can dramatically affect system performance. Typically, as explained previously, system deployment having less than five hops 95% or more of the time and latencies of better than 100 ms between regionally located FADs are good metrics to start with.

One benefit of these systems is that infrastructure size and cost are small, which allows for highly flexible incremental improvements and network optimization. Operation metric trending and monitoring can identify capacity issues before they become critical, and steps can be taken to enhance coverage and capacity to mitigate issues.

4.2.1.2 Unlicensed Mesh Technology History

Wireless mesh technologies have their roots in ALOHAnet[6]. The network was pioneered at the University of Hawaii in June 1971. In many ways, similar to the challenges faced by today's FAN utility networks, there was no easy way to connect campuses across various islands. The random access methods developed were later the basis for Ethernet and Wi-Fi standards. In the early 1980s, amateur radio operators began developing packet radio and dubbed it AMateur Packet Radio Network (AMPRNet) with designated IP addresses in the 44.0.0.0 network for worldwide use. Over the years, packet radio[7] evolved across North America. In 1985, Metricom was founded with the goal of developing these technologies to sell to electric, gas, oil, and water industrial customers. UtiliNet was one of the products developed by Metricom[8] and is still in use today by many utilities. There was very little evolution of the technology until recent regulatory acceptance of AMI rate cases and American Recovery and Reinvestment Act of 2009 (ARRA) funding provided a business opportunity for vendors to invest in development of newer systems. Currently, grid modernization is further expanding the business opportunity for these mesh systems not only with less dense networks but also with higher performance requirements. Among the challenges faced with this evolution is the need to turn what has been an application-focused system into a true Layer 3 network that can support Ipv4, IPv6, and peer-to-peer routing of external devices from any point to any other point on the network.

4.2.2 Wi-Fi

Wi-Fi is an important wireless technology because it is able to provide very high data rates and operates effectively in the unlicensed spectrum. The 802.11 Wi-Fi standard was designed as a wireless local area network (LAN). Wi-Fi is widely used in the utility industry for its primary use as a short-range link to computers, tablets, and other mobile devices. The use of Wi-Fi networks in offices and control centers is widespread, and Wi-Fi is increasingly deployed in the field at substations and in vehicles (mobile hotspots) to serve the mobile workforce.

The use of Wi-Fi in utility field networks is more specialized and falls into two general categories: PtMP links and mesh systems.

---

[6] https://en.wikipedia.org/wiki/ALOHAnet

[7] https://en.wikipedia.org/wiki/Packet_radio

[8] https://en.wikipedia.org/wiki/Ricochet_(Internet_service)

4.2.2.1 Point-to-Multipoint (PtMP) Links

Long-range outdoor operation was not anticipated as a primary use case. The challenges to achieving long-range Wi-Fi links result are threefold:

1. Power limits that apply to unlicensed ISM operation
2. RF propagation and penetration limitations resulting from the predominant use of the 2.4 GHz and 5.8 GHz ISM bands
3. In-band interference resulting from the widespread use of Wi-Fi in homes and businesses

Nevertheless, many products are available to utilities that use Wi-Fi for relatively long distance links. The limitations can be overcome by carefully engineered links taking advantage of line-of-sight paths and high-gain (directional) antennas. The achievable range is typically on the order of a few kilometers.

4.2.2.2 Wi-Fi Mesh Networks

A number of vendors—including ABB/Tropos Networks, Aruba Networks (HP), Firetide®, and Cisco—offer metropolitan-scale broadband mesh networks based on Wi-Fi technology. These mesh networks can provide multi-Mbps data throughput across a broad area. The spacing between mesh routing nodes is limited due to propagation, power, and interference. The relatively high density of routing node deployment often results in a higher system infrastructure cost.

Although the mesh nodes provide access to end (client) devices using standard Wi-Fi, the inter-router mesh itself is proprietary. One challenge that arises with these systems when deployed over a large area is mitigation of self-interference. Because there are a limited number of Wi-Fi channels, each group of radios must be on a common frequency. Close attention must be paid concerning how particular vendors manage channel coordination. Use of smaller channels and centralized coordination are some of the mechanisms being employed. Despite the approval of the 802.11s amendment for mesh networking in 2011, none of the vendors have adopted it to date.

Some Wi-Fi mesh networks use a combination of the 2.4 GHz band and the 5 GHz bands. If range and propagation permit operation in the 5 GHz band, the inter-router mesh backhaul traffic can be separated from the device access at 2.4 GHz, increasing system throughput.

Mesh requires careful design of the backhaul, or gateway takeout points. If too many routers and endpoints use a single gateway to the WAN backhaul, system throughput will be significantly reduced. The recently approved 802.11ah standard specifies Wi-Fi operation in the 915 MHz ISM band. This development could improve range and Wi-Fi mesh economics, when and if the standard is supported in products.

4.2.3 WiMAX

4.2.3.1 Wideband

The broadest use of IEEE 802.16 (WiMAX) in utility applications has been in the 3.65–3.70 GHz band. More than 100 utility networks have been deployed in that spectrum. The band was first designated as a “lightly licensed” land mobile service under Part 90, under rules first established in 2007. These rules required that users obtain a nonexclusive license from the

Federal Communications Commission (FCC) and register each base and fixed station by location. The spectrum is not owned, and licensees are expected to coordinate with others to prevent interference. In reality, unregistered users have been found operating in the band.

During 2014, the 3.65 GHz band was in the news due to an FCC Notice of Proposed Rulemaking (NPRM) that changed the rules for the band. The FCC NPRM grew out of the National Broadband Plan, which includes directives to make 500 MHz of spectrum available for mobile wireless use and to incorporate "innovative spectrum access models" to manage the spectrum. The FCC first proposed the Citizens Broadband Radio Service (CBRS) in 2012 to enable sharing of spectrum at 3.5 GHz between federal and non-federal users. This 150 MHz band (3.50–3.65 GHz) is below and adjacent to the existing 50 MHz band at 3.65–3.70 GHz. The NPRM was followed by a Further Notice of Proposed Rulemaking (FNPRM), FCC 15-47, in April 2014. The FNPRM was adopted April 17, 2015, as GN Docket No. 12-354. The ruling introduces a three-tiered licensing structure. Federal users retain the highest priority, but such use continues to be primarily located along the coasts and a few other specific sites. The next tier is Priority Access Licensees (PALs). The lowest priority is General Authorized Access (GAA) for the use of any remaining locations and frequencies.

The FCC 15-47 ruling represents a significant change for utilities already using the 3.65 GHz band. The rules include the mandatory coordination of spectrum sharing database services called the Spectrum Access System (SAS). The concept is similar to the spectrum sharing system adopted for TV white space. The FCC did not accept the suggestion of the WiMAX Forum and comments filed by utilities to leave the rules for the upper part of the band unchanged. However, the outcome is not all bad news. The incumbency provision protects existing networks for at least five years. Even after that, operating in the upper part of the band as a GAA user is effectively no different than the previous "lightly licensed" rules. In some ways, this arrangement is better because the SAS mandates sharing and coordination, whereas there was no obligation for coordination under the previous rules.

4.2.3.2 Narrowband

Due to the high value of spectrum to commercial cellular operators, any spectrum able to support LTE commands a very high price at auction or on the secondary market. However, many utility applications can be served by narrower bands that offer proportionally lower data rates. One example that has been offered for sale is the 700 MHz Upper A Block. This spectrum consists of two 1 MHz wide channels at 757 MHz and 787 MHz. The channel width is too narrow to be supported by either LTE or 802.16 (WiMAX) standards. As a result, equipment that is able to support operation in this spectrum is currently entirely proprietary. The IEEE 802.16 working group is developing the 802.16s amendment to enable the standard to specify operation in channel widths below 1.25 MHz. The 700 MHz spectrum is the impetus for the project, but the standard itself is frequency agnostic. When complete, the amendment will support operation in narrower channels at any frequency that becomes available.

The 1 MHz channel provides a unique set of characteristics. On one hand, the narrower channel cannot be considered for commercial cellular, making the spectrum more affordable. On the other hand, the width (and resulting data rate) are considerably expanded compared to radio systems designed to operate in legacy licensed spectrum sized for analog voice, with bandwidths of tens of kHz. In addition, the 802.16 standard provides the benefits of a cellular architecture, including frequency re-use, seamless handover of mobile devices between base stations, and the ability to increase throughput over an area by increasing base station density.

4.2.4 LTE

LTE is the popular name for the most current, fourth generation (4G) global standard for commercial cellular telecommunications technology. LTE is essentially a universal standard since it is deployed, or will be deployed, throughout the world and comprises a significantly large share of the total market. This is significant because in each previous generation of cellular evolutionary development, there were at least two incompatible standards deployed throughout the world.

LTE is a so-called "all IP" technology in that it is intended for transport of Internet Protocol packet data on both the "user plane" (user traffic conveyed to and from user devices) and the "control plane" (control data that supports network and user device operation and control). Published LTE standards govern packet data communications on the air interface between network radio base stations and user devices as well as on interfaces between various standardized functional elements in the LTE network. As a result, user devices and network components are available from a large number of manufacturers at highly competitive prices. In addition, because LTE networks are widely deployed, there is a very large body of expertise in all aspects of the technology, including network design and optimization, network deployment, network operation, user device design and manufacturing, user device provisioning, technical testing, and applications development. LTE user devices in particular are manufactured in very large volumes, resulting in high levels of design and manufacturing efficiencies that keep product costs very low.

4.2.4.1 LTE Network Architecture

LTE networks utilize a standardized architecture comprising a number of different functional elements that intercommunicate using standardized operational protocols, as shown in Figure 4-3. The network is generally divided between the Radio Access Network (RAN) (comprising a plurality of radio base stations called eNodeBs) and the Evolved Packet Core (EPC) (comprising a number of elements that support network operation, traffic routing, management of user devices, and interconnection to external packet data networks such as the public Internet). The EPC connects to the eNodeBs of the RAN through a standardized IP interface called S1. External networks such as the public Internet connect to the EPC using industry standard Internet Protocols on an SGi interface. In general, the EPC may connect to multiple RANs through parallel S1 interfaces and to multiple external IP networks through parallel SGi interfaces.

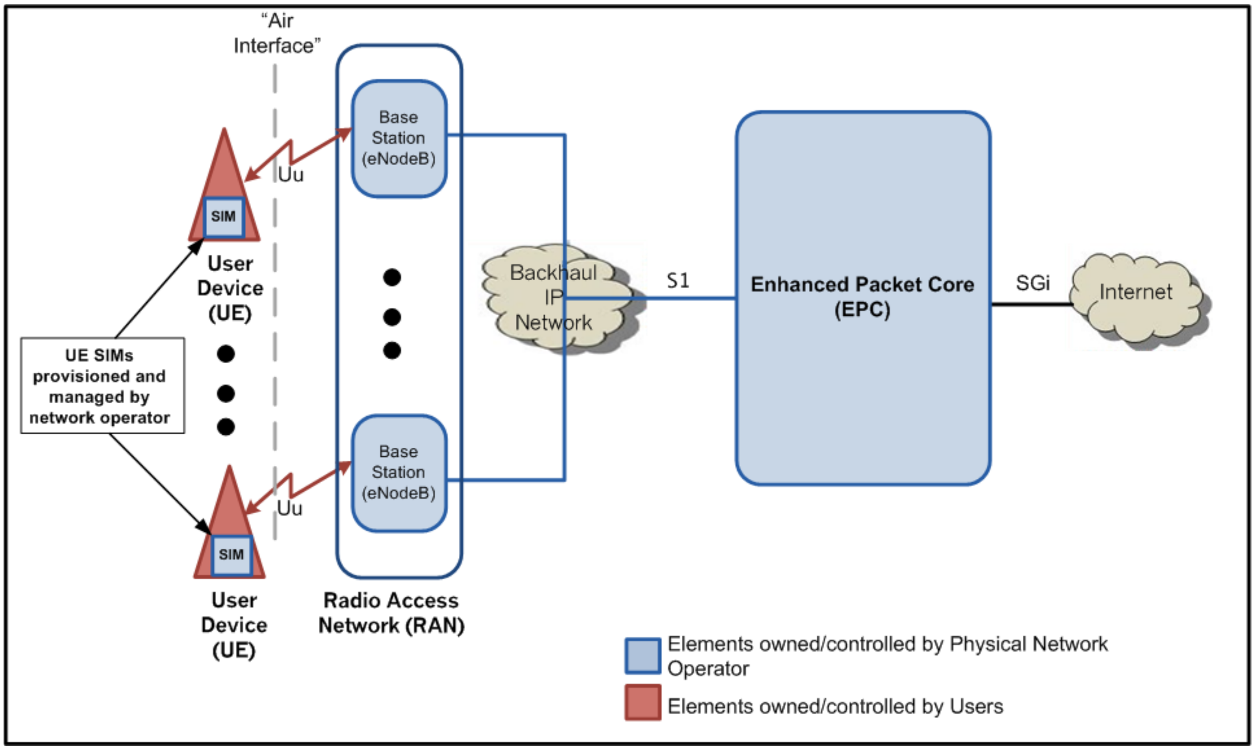

Figure 4-3
Basic LTE Network Architecture

The LTE RAN provides wireless connections and data communications services to an essentially unlimited number of discrete user devices singly referred to as user equipment (UE). Each UE carries a subscriber identification module (SIM), which is provisioned with various means of centrally administered identification to ensure unique and secure identification by the serving LTE network. The LTE air interface (U_u) comprises both downlink (base station transmit/user device receive) and uplink (user device transmit/base station receive) radio channels. From the standpoint of LTE standards, the UE consists only of the device that communicates with the LTE network and provides a user plane data interface to an integrated or connected device. That user-side interface is not subject to published standards and can be physically and logically formatted to suit specific applications. For example, in some grid data communications applications, the UE may take the form of a modem that connects to a remote IED (for example, a SCADA device) through a USB or Ethernet port.

4.2.4.2 4G LTE Technology

As currently deployed commercially, LTE is a fourth generation (4G) cellular telecommunications standard. In common usage, the terms "LTE" and "4G" are often used interchangeably. However, it is anticipated that LTE standards will evolve to encompass future generations of cellular technology.

In many respects, 4G LTE is ideally suited to the requirements of data communications for the modernized grid. Most critically, as a cellular system, 4G LTE is a true FAN providing geographically ubiquitous wireless service over a broad area, which greatly reduces the cost and logistics associated with provisioning new communications capabilities in the grid. Its control functionality is specifically designed to handle "bursty" transmissions of small to moderate amounts of data, to or from a virtually unlimited number of different user devices, with a minimum of control “overhead” and low latency. The air interface incorporates multiple levels of error detection and correction for highly robust connectivity. The radio channel automatically adjusts modulation and coding schemes to efficiently accommodate a wide range of signal-to-noise ratios (SNRs). Since it is specifically intended for IP connectivity at both the user device and connection to external networks, 4G LTE will efficiently support migration of grid communications from various serial data schemes to packet data format. Furthermore, while in commercial LTE networks, user plane traffic generally involves connection to the public Internet from the LTE network’s Packet Data Network (PDN) Gateway element, connections can also be made to a private IP network or through a virtual private network (VPN) carried on the Internet.

EPRI report 3002009792, *Public Networking and Shared Networks – Architecture and Operation*, will provide further discussion of LTE technology and its potential use for grid data communications.

The challenge of LTE as a solution for a utility FAN is primarily based on the spectrum. LTE is designed for operation in the exclusively licensed spectrum. Virtually all new and expanding commercial cellular networks operate using LTE standards, and demand for the mobile packet data communications services—particularly for connection to the Internet—is growing rapidly. As a result, where spectrum access is based purely on economic factors (for example, through competitive bidding), the purchase or lease cost will be at a premium for spectrum “chunks” that are of sufficient width for a minimal LTE channel (~1.4 MHz) and in a band that is practical for use in commercial cellular systems (generally between 500 MHz and 3 GHz). This high cost and the general scarcity of suitable spectrum may make it impractical for a utility to deploy and operate its own dedicated LTE network.

As an alternative to a dedicated network, utilities may investigate the feasibility of sharing a “critical infrastructure” LTE network that is deployed for, and restricted for use by, certain entities such as police, fire departments, and so forth. The practical implications of such an arrangement are discussed in Section 4.4.1 – 4.4.4.

A second alternative is to utilize commercial LTE networks for grid data communications. While operators are delighted to have utilities as customers, the commercial networks are first and foremost oriented toward serving the traditional individual retail user. The mismatch is seen in multiple dimensions, the first of which is cost. Many utilities can capitalize investment in their infrastructure, but operational expenses such as cellular charges go right to the bottom line. Reliability and availability are other concerns, including unplanned service outages, time of restoration of service after storms, and loss of connectivity during times of peak use by retail customers. Finally, coverage is sometimes an issue. If particular regions or sites lack adequate coverage, utilities have little leverage to cause the operation to upgrade their network infrastructure. However, these concerns can be mitigated to a significant extent through the use of specialized interface and administrative relationships offered by a number of major commercial LTE network operators.

4.2.4.3 5G Technology

Cellular communications technology is constantly evolving, with refinements and new features periodically implemented in the governing standards to ensure backwards and forwards compatibility. However, even as such incremental changes are being made to cellular technologies that are already operational, work is typically underway on the next generation cellular technology, which generally incorporates significant changes to the air interface. While backwards and forwards compatibility is not assured between technologies of different generations, user devices are commonly designed and provisioned for compatibility with not only current generation networks but also at least some previous generation networks.

As discussed in Section 4.2.4.2, LTE, the latest globally operational cellular standard, is considered a fourth generation (4G) technology. Currently, various manufacturers, industry groups, academic researchers, as well as 3rd Generation Partnership Project (3GPP) (see Section 4.2.4.4 and Section 4.2.4.5) have begun developmental work on what will become the fifth generation (5G) cellular technology. At present, there is no consensus on what form 5G technology will take, but it is generally assumed that it will be intended as a packet data network that will provide very high levels of throughput capacity in areas of dense traffic concentration. Accordingly, 5G will most likely provide very high capacity in specific locations, with ubiquitous coverage provided only in dense urban areas. Indeed, most 5G proposals envision operation on the spectrum above 3 GHz, which is probably impractical for providing ubiquitous service over wide geographic regions. Because of this limitation, 5G will most likely not be a replacement for 4G LTE but rather a separate but fully integrated enhancement. It is therefore reasonable to expect that further development and eventual deployment of 5G cellular networks will not move 4G LTE technology into the "legacy" category any time within the foreseeable future.

4.2.4.4 LTE-M

Within the wireless industry a rapidly growing market segment is so-called machine to machine (M2M) communications. From a channel-loading standpoint, the overwhelming majority of user plane traffic on wireless data networks consists of data to or from devices with a human user interface, for example, smartphones. Most of these data represent information that is or will be communicated through that user interface. By contrast, M2M communications involve conveyance of data that are neither originated by nor intended (at least directly) for human users. For example, one currently popular M2M application is asset tracking. A shipping container or railcar can be equipped with a device composed of a GPS receiver and LTE modem. The device can be programmed to report (to a server) its position, either periodically when it has moved a certain distance from its last reported position or when polled by the server.

An important attribute of most M2M communications is that they involve the transfer of relatively small amounts of user plane data. For example, a report of position down to the best resolution obtainable from GPS requires just a few bytes of data if predefined protocols are used. By contrast, transmission of human-oriented user plane information such as voice, video, and even text require vastly higher quantities of data, which must often be delivered at high speeds in order to provide satisfactory performance.

M2M is part of a broader category of communications that is generally called the Internet of things (IoT). The driving force behind IoT is that many aspects of modern life can be enhanced by communications-enabled control of the various "things" that make up the man-made environment. A commonly cited IoT application is the connected home, wherein all manner of devices—from lights to hot water heaters to rooftop solar panels—are centrally controlled and monitored to provide optimal performance and efficiency.

With the rapidly growing interest in M2M and IoT, 3GPP (the standards body that develops and maintains LTE standards) has published a set of standards for operation of a special functionality within LTE networks. These standards, known as LTE-M, are aimed specifically at M2M and IoT applications. A key characteristic of LTE-M is the ability to define, within a broader LTE channel, a relatively narrow LTE-M channel for the air interface between special LTE-M UE and serving base stations. LTE-M also imposes limits on maximum data speeds and maximum packet sizes and introduces a scheme that allows for unique identification of a vastly larger number of devices. It is anticipated that these and other features will allow LTE-M UE to be manufactured at scale and at substantially lower per-unit costs, being able to operate for long periods on inexpensive primary batteries.

Most of the benefits of LTE-M will be lost if compatible UE must also be compatible with conventional LTE networks. Thus, widespread commercial use will only be practical when LTE-M functionality is introduced in most LTE networks, or alternatively when substantial geographic coverage is provided by stand-alone LTE-M networks. This appears to be, at best, several years in the future.

4.2.4.5 LTE Standards

Comprehensive standards that fully define the LTE air interface and interfaces between the various defined elements of the LTE network are promulgated and maintained by 3GPP, a global collaboration between groups of telecommunications associations, manufacturers, and commercial network operators. Published LTE standards are public domain documents.

As is traditional in cellular telecommunications, LTE standards are both backward- and forward-compatible. This means that, with rare exceptions, user devices and network elements designed for compatibility with a particular revision level of the standards will continue to interoperate properly with devices and elements designed to any future revision level and vice versa. This assured future compatibility is of particular importance in grid communications, where equipment life cycles tend to be very long compared to the speed of cellular standards evolution.

Additional life-cycle protection is provided to LTE user devices by standardized over-the-air (OTA) provisioning, activation, and software updating. This means that all programmable functionality, as well as most relevant standards enhancements, can be incorporated into user devices in the field without a requirement for physical retrieval or even in-person maintenance.

LTE standards comprise specialized protocols that enable networks to limit access to user devices with specific programmed “access class” codes. An additional standardized feature allows networks to prioritize specific categories of user plane data communications over others. Together, these standardized features should allow commercial networks to be able to guarantee specified QoS metrics (access reliability, throughput speeds, and latency) for critical grid communications, even when network loading in a particular geographic area or a specific eNodeB is at saturation levels.

4.3 Spectrum

One of the first questions that must be asked when planning a FAN communication system is, “What spectrum will be used?” Most utilities do not have access to a licensed spectrum or if they do, it is limited in capacity, coverage, or both. The availability of a spectrum will be an early decision point when defining a FAN architecture. There are many choices ranging from licensed to unlicensed and from leased to shared. This section will provide a brief summary of the possible available spectrum applicable for utility distribution FAN systems. A more detailed analysis is presented in EPRI's *Assessment of Licensed Communication Spectrum for Electric Utility Applications*[9].

The range of electromagnetic frequencies that radio waves are able to operate on are collectively referred to as the RF spectrum and is regulated by the FCC. Beginning in 1934, there has existed a growing set of regulations that govern the emission of signals in the RF spectrum. In parallel with the FCC, the National Telecommunications and Information Administration (NTIA) manages the use of RF spectrum for federal and U.S. military users. The primary method that the FCC uses to regulate the spectrum is the issuance of licenses. These licenses provide the holder with certain rights and responsibilities. Historically, they were issued on a first-come, first-served basis and required only nominal administrative fees. However, when cellular telephony usage experienced exponential growth, the FCC embarked on a path of auctioning spectrum to the highest bidder. This has been primarily used for broadband rather than narrowband spectrum; however, to date, the FCC has held ~100 auctions for spectrum of all types throughout the usable band of frequencies.

The most common metric used to measure and compare the value of different spectrums is the price paid in dollars in the numerator with the product of the bandwidth of the spectrum multiplied by the population density within the area covered by the license in the denominator. The shorthand expression for this is $/MHz-PoP. For the most part, there has been a steady and rapid increase in the value of spectrum with each auction.

As is often the case in dynamic commercial markets, there are bankruptcies, mergers, and other types of reorganization that often require the transfer of assets. While the FCC regulations have always covered successors and assigns, in the 2003/2004 timeframe, the FCC clarified and expanded its rules to support and even encourage a secondary market for spectrum licenses. Another method used by the FCC is "type acceptance" of equipment produced by manufacturers for operation in unlicensed bands. This has expanded greatly, with a major revision of the FCC rules in 1989 and the establishment of the IEEE 802.11 standards along with the creation of the Wi-Fi alliance that certifies interoperability of equipment and standards compliance. Other technologies and protocols that operate in unlicensed bands and that are of interest to utilities are covered in Section 4.3.5.

Due to high spectrum costs, most, if not all, frequencies with mature technologies such as LTE and high capacity are beyond the price range of utilities. This leaves unlicensed or less than optimal spectrum choices with varied levels of technology maturity and availability for utility use. As with technology metrics, it is difficult to precisely quantify the differences between the various available spectrums. Table 4-3 provides a subjective comparison of some of the spectrums being explored for use in modern utility FANs.

---

[9] *Assessment of Licensed Communication Spectrum for Electric Utility Applications*. EPRI, Palo Alto, CA: 2015. 3002005851.

Table 4-3
Subjective Spectrum Comparison

	406 MHz	700 MHz	ISM & U-NII (915 MHz 2.4 GHz 5.8 GHz)	2.3 GHz (WCS)	2.5 GHz (BRS/EBS)	3.65 GHz (CBRS)	4.9 GHz
Ownership	lic	lic	unlic	leased	leased	lic + shared	lic + shared
Bandwidth	14 MHz, channel and bandwidth TBD	2 x 1 MHz	26 + 83 MHz	2 x 5 MHz	2 x 6 MHz 12 x 5.5 MHz	150 MHz varied tiers of use	50 MHz (1, 5, 10, 15, or 20 MHz channels)
Coverage	good	good	good (<1GHz) poor (>1 GHz)	poor	poor	poor	poor
Capacity	low	low	low	moderate	high	high	high
Maturity	pre/not defined	low	moderate	moderate	good	moderate	good
Technology Availability	NA	few	many	few	some	some	many

Each of these spectrum areas is discussed in greater detail below.

4.3.1 406 MHz

The EPRI Spectrum Assessment identified an underutilized block of spectrum in the range of 406–420 MHz. This is a government spectrum allocation managed by the NTIA. This spectrum is relatively low in frequency and less attractive to commercial cellular. The closest cellular spectrum is LTE Band 31 at 450 MHz. The 14 MHz band is wide enough to support an LTE network with frequency reuse. EPRI and the Utilities Telecom Council (UTC) are continuing to seek permission from the NTIA to perform testing and demonstration of successful sharing of this spectrum between a utility and an incumbent government user. In contrast to the dynamic spectrum sharing promoted by the FCC, where frequencies and rights to use can change daily or hourly, this spectrum sharing will likely be more static. For example, the utility would use the upper 6 MHz, and the government user would use the lower 8 Mhz. This spectrum is much lower in frequency and will have significantly greater range but will also be harder to effectively reuse if higher capacity is needed; it may be best used for more rural applications.

4.3.2 700 MHz

The 700 MHz spectrum was previously used for analog television broadcasting, specifically UHF channels 52–69. The FCC ruled that the digital television transition would make these frequencies no longer necessary for broadcasters because of the improved spectral efficiency of digital broadcasts, allowing for broadcasts on first-adjacent channels instead of having to leave empty TV channels as guard bands between analog stations. Thus, all broadcasters were required to move to channels 2–51 as part of the digital TV transition. Much of this spectrum has been purchased through auction by cellular carriers and is currently providing commercial LTE services. More recently the upper A block, 2 x 1 MHz paired, was auctioned of by the FCC and is available for utility FAN communications. This spectrum has been acquired by a group of utilities, including SRP, Great River Energy, Portland General Electric, and others. The spectrum for all of California was purchased by the High Speed Rail Authority. Any utility usage in the state would have to be sub-licensed from the existing licensee. The channels are limited to a 2 x 1 MHz pair, making it a gray area in terms of whether it is considered wideband or narrowband. Compared to the types of channel bandwidths typically used by 802.16 and LTE, it is narrowband. Those standards do not specify operation in a channel narrower than 1.4 MHz as currently defined. Compared to voice channels, however, the spectrum is wideband. A few vendors offer variations of 4G standards that can operate in relatively narrow channels (hundreds of kHz) and provide commensurate bandwidth (hundreds of kbps). These data rates are usable for many FAN applications. Work is underway in the IEEE to amend the 802.16 standard to support narrower channel widths. The IEEE 802.16s amendment project began in mid-2016, and the amendment is slated for completion in 2017.

If the technology matures and industry standards such as 802.16 evolve, this could be a very good choice for high coverage with a moderate amount of capacity for FAN applications.

4.3.3 Leased

4.3.3.1 2.3 GHz

The Wireless Communications Service (WCS) and the Satellite Digital Audio Radio Service (SDARS) occupy 55 MHz of RF spectrum, frequently referred to as the “2.3 GHz band,” from 2305–2360 MHz. The SDARS occupies 25 MHz in the center portion of the 2.3 GHz band at 2320–2345 MHz. The WCS occupies frequency bands on either side of the SDARS allocation and consists of four blocks in the 2305–2320 and 2345–2360 MHz bands: two 10 MHz blocks (paired 5 MHz blocks) and two unpaired 5 MHz blocks (see Figure 4-4).

Spectrum space in the 2.3 GHz band was first designated in 1997, but it has not been fully utilized by mobile networks because of the potential for interference to satellite communications at nearby frequencies. In June 2012, AT&T and Sirius XM filed a proposal with the U.S. FCC that would protect adjacent satellite communications bands from interference and allow the WCS band to be fully exploited for mobile Internet service. The C and D blocks adjacent to the SDARS bands are licensed by AT&T and were of the greatest concern to Sirius XM. The proposal, which was accepted by the FCC in October 2012, was designed to minimize interference with SDARS.

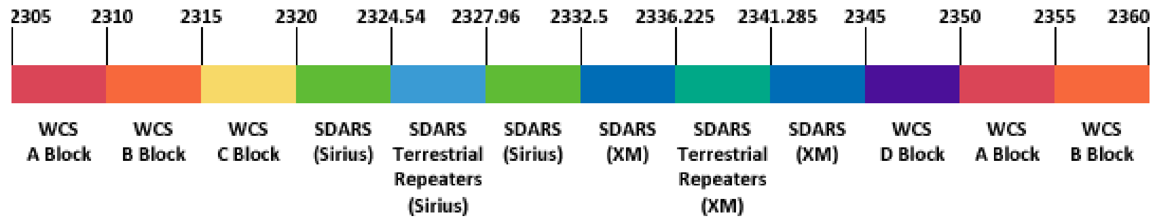

Figure 4-4
Wireless Communication Services Spectrum Space

The FCC's rules for the 2.3 GHz WCS band are contained in 47 CFR Parts 27.50 through 27.73. Prior to the AT&T and Sirius XM proposal, the C and D blocks had a prohibition on mobile and portable operation. Fixed customer premise equipment (CPE) stations were also prohibited from use of outdoor antennas. There were also severe restrictions on transmit power and duty cycles for the C and D blocks as well as a portion of the A and B blocks closest to the SDARS frequencies.

Under the revised rules adopted after the agreement, the entire A and B blocks were relieved of the power and duty cycle restrictions, and these restrictions were modified somewhat for the C and D blocks. The prohibition on outside antennas was removed for the C and D blocks with the condition that they be professionally installed. Most importantly, the concept of "harmful interference" was clearly defined from a technical perspective. Information sharing and coordination procedures were also codified in the regulations.

Almost immediately following the issuance of the new rules, AT&T executed transactions with the other WCS spectrum licensees that held the remaining geographic areas that AT&T did not possess. Primarily, these other licenses were held by Comcast, while SDG&E held licenses for the C and D block for metropolitan San Diego.

In February 2016 at the DistribuTECH show in Orlando, AT&T and Nokia presented a proposal for U.S. utilities to lease the C and D blocks for Smart Grid communications. The basic terms of the proposal were that AT&T would offer a 15-year lease on the spectrum and Nokia would provide both the network equipment (LTE eNodeBs and the EPC) as well as the UE.

The AT&T/Nokia proposal is attractive to utilities in that it is for two 5 MHz blocks and is able to provide broadband service with standards-based LTE equipment. Additional benefits discussed were that the UE would be dual band/dual SIM so that the utility would have immediate service via the AT&T commercial network while the utilities' WCS band RAN is being built out. AT&T has also stated that it is interested in utility infrastructure such as poles, towers, and fiber optics to support the buildout of its commercial A and B block RAN. The utility contribution of these assets could be used in exchange to reduce or eliminate the spectrum lease fees. Current status on this offer is that several utilities have agreed to test or pilot the spectrum, but there have been no announced deals to date.

On January 18, 2017, the FCC issued an order in response to AT&T request for an extension on construction deadlines for the C and D blocks of the WCS band. The order (WT Docket No. 16-181) does grant relief from previous deadlines but imposes additional interim milestones to ensure progress is being made towards deployment. To understand these conditions, it is helpful to understand the geographic boundaries for the WCS licenses. The FCC uses regional economic area groups (REAGs) as the boundaries. Figure 4-5 shows six REAGs for the continental United States.

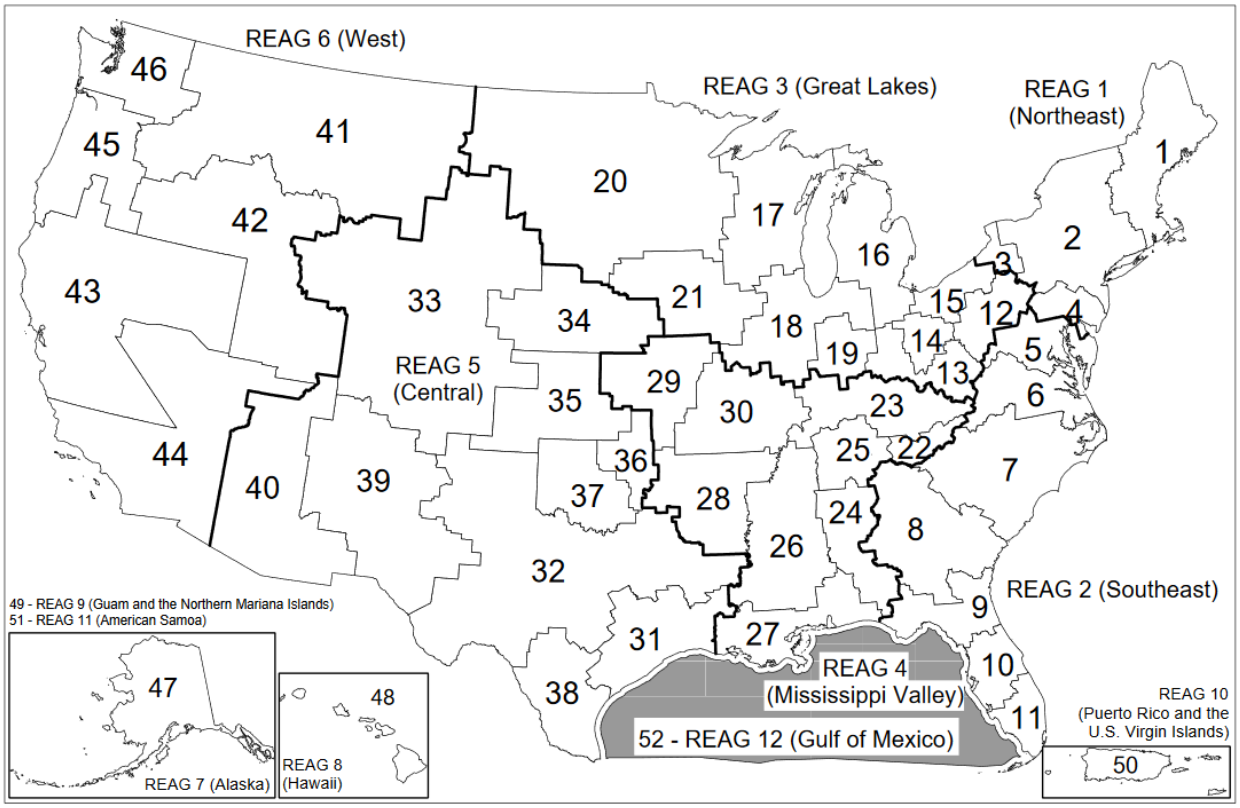

Figure 4-5
Geographic Boundaries for the WCS Licenses

The interim and final milestones from the FCC for C and D block deployment are as follows:

- September 13, 2017—AT&T must report to the FCC on the utility customers, for which AT&T has agreed to provide its Smart Grid service and the timeframes for deployment with respect to those customers. The report must also provide the results of any equipment testing and trial/initial deployments.
- September 13, 2019—AT&T must have contracts for commercial deployment with at least 10 utilities, file a report in Universal Licensing System (ULS) demonstrating that it has such contracts, and provide supporting documentation to the FCC. AT&T must also have begun operation in two of the six continental REAGs and provide documentation showing that it has done so. The report filed on this date must also update the FCC on the status of AT&T's build-out and the status of AT&T's contracts with other utilities.
- September 13, 2020—AT&T must have begun operation in four of the six continental REAGS (that is, an additional two REAGs), and file a report in ULS with documentation showing that this obligation has been satisfied. The report must again update the FCC on the status of AT&T's build-out and the utilities for which AT&T is providing service.

- September 13, 2021—AT&T must file a report in the ULS demonstrating its compliance with the modified final performance benchmark.

In summary, the 2.3 GHz WCS band spectrum is technically capable of providing broadband, low-latency, standards-based LTE coverage for fixed utility Smart Grid and distribution automation communications needs. In light of the recent FCC conditions on AT&T for interim deployment milestones, it is likely that attractive commercial terms could be reached in negotiations with AT&T/Nokia. The FCC document reaffirms their "keep what you use" philosophy in regard to spectrum licenses. Therefore, if progress is not made, it appears to be somewhat possible that AT&T would lose these C and D licenses in locations where they are not deployed. To better understand the apparent exhaustion of patience in the recent FCC order, it should be noted that this spectrum was originally issued under the FCC Auction No. 14 in 1997.

4.3.3.2 2.5 GHz Frequency

This frequency was first used from 1963–1972 to transmit analog instructional televisions programs. In 1972, the FCC granted permission for commercial operators to use the frequency for over-the-air pay TV known as Multipoint Distribution Service (MDS). The FCC reallocated eight of the Instructional Television Fixed Service (ITFS) channels for use by commercial operations in 1983. In 1995, the FCC auctioned many of these channels with new designations of Educational Broadband Service (EBS) and Broadband Radio Service (BRS). Over the years, through many different licensing and leasing agreements, Sprint became the majority owner of the MDS spectrum.

Even if Sprint decides to allow a utility usage model for some of its spectrum, coverage will always be a challenge at higher frequencies, and deployment costs will be high. The best use may be for high-speed backhaul or very targeted coverage for specific low-latency, high-performance devices.

4.3.4 Shared Spectrum

4.3.4.1 3.65 GHz

The 3.65 GHz CBRS was recently allocated by the FCC to a multi-tiered usage model with three tiers of users. The highest tier is for incumbent federal and satellite users. The second tier is licensed in regional areas and must give protection to the higher tier. The third and lowest tier will be able to operate using FCC approved devices without a license but must accept all interference from the higher tiers. The FCC will employ SAS—a highly automated frequency coordinator—to assign frequencies in the 3.5 GHz band. The SAS will also authorize and manage use of the CBRS spectrum, protect higher tier operations from interference, and maximize frequency capacity for all CBRS operators. SAS administrators will be permitted to charge CBRS operator fees for registration and frequency coordination services.

As with the 2 GHz spectrum, coverage will always be a challenge at these higher frequencies, and deployment costs will be high. The best use may be for high-speed backhaul or very targeted coverage for specific low-latency, high-performance devices.

4.3.4.2 4.9 GHz

The FCC allocated the 4940–4990 MHz band for use in support of public safety in 2002. The rules governing this allocation are found in 47 CFR Parts 1201–1217. A broad range of usage types is allowed:

- Fixed or mobile
- Voice, video, or data
- Unattended and continuous operation
- Point-to-point (PTP) or PtMP
- Mesh
- Temporary or permanent stations

There is a prohibition on aeronautical mobile operation. There are also requirements to coordinate with other licensees to avoid interference as well as a requirement to protect astronomy operations. These licenses are noted as shared and non-exclusive. The rules allow flexibility in channel bandwidth, with 1, 5, 10, 15, and 20 MHz wide channels allowed. The main obstacle for utility use is that the band is “limited to operations in support of public safety.” It would be necessary for the utility to convince the local governmental or state public safety entities that utility use meets the mission statement and obtain their support before filing an application. It has been past experience that even in regions where public safety entities have not yet deployed 4.9 GHz systems, they are hesitant to support utility use in the band in order to reserve the spectrum for their own potential future use.

4.3.5 Unlicensed

Unlicensed spectrum in the United States is broadly used. These bands were first established at the International Telecommunications Conference of the ITU in Atlantic City, 1947. The American delegation specifically proposed several bands, including the now commonplace 2.4 GHz ISM band, primarily to accommodate microwave heating. Currently Wi-Fi, Bluetooth, ZigBee, cordless phones, and other wireless systems all share this band. Such low power communication devices must accept any interference received, and the Part 15 device must not cause harmful interference. Radio communication services operating within these bands must also accept harmful interference that may be caused by these applications.

The 5 GHz band is important for unlicensed use not only in the United States but also worldwide. The World Radio Conference (WRC), an ITU body, meets every four years in an effort to harmonize spectrum usage internationally. A variety of channels in several different allocations from 4.9–5.925 GHz are designated as Unlicensed National Information Infrastructure (U-NII). In the United States, parts of the U-NII spectrum are used for versions of Wi-Fi under IEEE 802.11a and 802.11n, whereas in Europe and Japan, different segments are used for 802.11h and 802.11j, respectively.

Electric utility industry usage of the 915 MHz ISM band has significantly increased in the last 5–10 years with the wide-scale deployment of AMI systems, the majority of which are based on mesh technology and use this band. These AMI systems operate under Part 15 rules and use either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS) technology. Overlapping with the 915 MHz unlicensed band are two other licensed allocations (both secondary to federal government use). As shown in Figure 4-6, the first non-federal licensed allocation is the Multilateration Location Monitoring Service (M-LMS), and the second allocation is amateur radio.

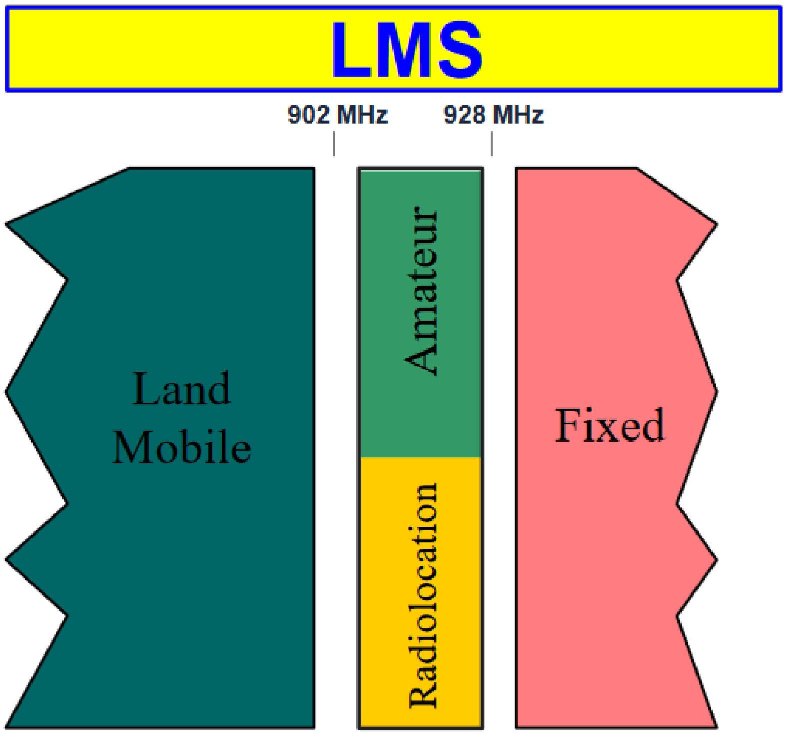

Figure 4-6
Multilateration Location Monitoring Service (M-LMS)

Amateur radio usage of the band pre-dated the AMI deployments and used narrow-band FM modulation; co-existence between the two was found to be acceptable.

The FCC permitted radiolocation, or Location and Monitoring Service (LMS) in 1995, and a nationwide auction (No. 21) was held in 1999. The auction only raised approximately $3.4M for 289 economic area (EA) licenses. Out of the four winning bidders, Progeny LMS, LLC acquired the vast majority of the licenses.

Progeny LMS and the other LMS license holders have filed multiple waiver requests over the years with the FCC for extension of the construction deadlines. These have been granted each time. This has resulted in the creation of a general perception in the wireless industry that LMS was a failed service and would never be deployed. However, the Progeny LMS business model changed in 2015 when the FCC issued new regulations for E911 location accuracy for the cellular telephone industry. The FCC order contains a phased approach where increasing accuracy is required on a prescribed timeline. This timeline includes vertical location requirements beginning in 2018. Progeny LMS has been working with the cellular carriers and original equipment manufacturer (OEM) vendors to develop a solution for the E911 indoor location requirement; this was a key factor in Progeny LMS obtaining the most recent construction extension in January 2017. The FCC granted this despite objections from IEEE 802, Itron, and Landis+Gyr, all of which disputed results of field testing that had been conducted for the purpose of determining M-LMS interference potential to unlicensed devices.

4.3.5.1 Wi-SUN Types

Wi-SUN type mesh systems operate in the 902–928 MHz and 2.4 GHz portions of the unlicensed ISM bands designated for radio communications under part 15 of FCC regulations. Wi-SUN systems use IEEE 802.15.4g PHY standards requiring relatively narrow channels on the order of 100 kHz and contention-based media access mechanisms. While there is significant use and proliferation of Wi-Fi Bluetooth, within the band, the Wi-SUN physical and media access protocols tend to be fairly robust in the face of interference—although they do this at the expense of capacity and spectral efficiency.

4.3.5.2 PTP/PtMP Systems

A variety of PTP and PtMP systems are available for operation in both licensed and unlicensed spectrums. Those systems operating in the licensed spectrum tend to be narrowband solutions, operating in channel bandwidths up to tens of kHz. This type of spectrum was originally allocated for analog voice communication. Those systems operating in the unlicensed spectrum typically employ spread spectrum modulation, which can be a direct sequence of frequency hopping. The unlicensed system takes advantage of the wider spectrum in the ISM bands and can deliver data rates in the low Mbps. These systems are sometimes based on standardized underlying technology but are proprietary in practice.

4.4 Utilizing Commercial LTE Public and Shared Networks

Commercial wireless data networks have been in operation globally for several years, demonstrating the ability to provide packet data connectivity over large areas with essentially ubiquitous service coverage. Of course, the levels of performance, service reliability, and resiliency to natural and man-made disasters vary from one commercial network to another. In general (and with the notable exception of disaster situations), however, the service provided by the latest generation of technology, LTE, offers levels of performance and reliability that may be attractive for at least some utility data communications applications. This may be of particular importance for utilities that are unable to, or choose not to, deploy their own ubiquitous coverage FAN.

The following discussion will consider various general architectural alternatives that might be used by a utility for obtaining data communications services on commercial LTE networks. These alternatives reflect specialized technical and administrative relationships between the utility and the wireless network operator, which contrast with the typical customer/service provider relationship that most are familiar with as cellular service consumers. While it is possible for utilities to obtain data communications services from a commercial network operator as would any other customer, the unique performance, reliability, and security needs of utility data communications strongly suggest consideration of one or more of these specialized relationships, examples of which are discussed below. Some of the more important features of these specialized relationships are summarized in Table 4-4.

Table 4-4
Features of Specialized Relations for Utility Data Communications

Feature	Conventional Customer	Enterprise Customer (See 4.4.1)	Commercial MVNO (See 4.4.2)	Dedicated UVNO (See 4.4.3)	PVNO (See 4.4.4)
Potential for direct technical staff interface for problem resolution		x			x
Potential for obtaining special higher access priority and QoS treatment		x		x	x
Potential for utilizing redundant physical networks (without redundant remote device UE)		x		x	x
Potential for network interface via private IP network or VPN		x		x	x
Utility may retain control over remote device (LTE UE) provisioning and maintenance					x
Potential for emulation of "peer" RAN to allow utility data communications to bypass commercial network EPC				x	x
Potential for peer-to-peer relationship and interface between commercial wireless network and utility data communications network					x
Potential for obtaining special M2M (IoT) features		x	x	x	x

4.4.1 Commercial Network “Enterprise Customer”

Most major commercial wireless network operators are prepared to expend substantial marketing and engineering resources to accommodate unique requirements of large enterprises when doing so results in a commensurate level of revenue. An operator’s interest in attracting such “enterprise customers” will likely be particularly strong when such a revenue stream is judged to be reliable and of reasonable duration, both of which can be satisfied by provision of services contracts.

In the context of the basic LTE network architecture shown in Figure 4-3, the traditional network “customer” is the user of one or a small number of individual pieces of UE, which are commonly smartphones or portable computers with integral LTE modems. In a basic form, the enterprise customer configuration may be very little changed from this arrangement, except that the number of individual UEs “owned” by the enterprise customer might be substantial. For example, a utility could contract with a commercial wireless network operator to simply provide their standard level of data communications services to a large amount of UE connected to (or integrated within) remote IEDs placed within the transport and/or distribution infrastructure. In this very basic “enterprise customer” arrangement, such remote device UE would be treated by the network as any other UE, with user plane connectivity provided over the public Internet. Thus a utility’s data communications server would communicate with remote IEDs through the Internet and the commercial wireless network and would be subject to the same service and security limitations as conventional customers (for example, increased connection latency at times of peak wireless data traffic demand).

Fortunately, as noted above most major network operators are prepared to provide special accommodation for the unique needs of enterprises that represent lucrative revenue opportunities, so long as the core provision of services to ordinary customers is not significantly impacted. As one might expect, the range of possible accommodations, both technical and administrative, is virtually unlimited. However, it is reasonable to suggest an architectural model for an “enterprise customer” relationship between a power utility and a commercial LTE network, as shown in Figure 4-7. As depicted here, several primary accommodations have been introduced relative to the basic LTE network architecture shown in Figure 4-3. First, special configuration may be provided to some elements of the network’s EPC. For example, UE—identified as equipment associated with utility remote devices that require high levels of access reliability and/or low connection latency—may be assigned a special access priority code. EPC provisioning may be introduced that ascribes high service quality parameters to data communications to and from the utility’s data communications server. While the network operator still manages provisioning of the SIMs in the utility’s remote device UE, the provisioning may introduce special characteristics (such as an access priority code) unique to such UE. Finally, and of particular importance for security of utility data communications, the wireless network EPC can be connected to the utility data communications server by either a private IP network or a virtual private network (VPN) on the public Internet. These measures can effectively prevent both the utility’s server and its remote devices from being accessed conventionally over the Internet.

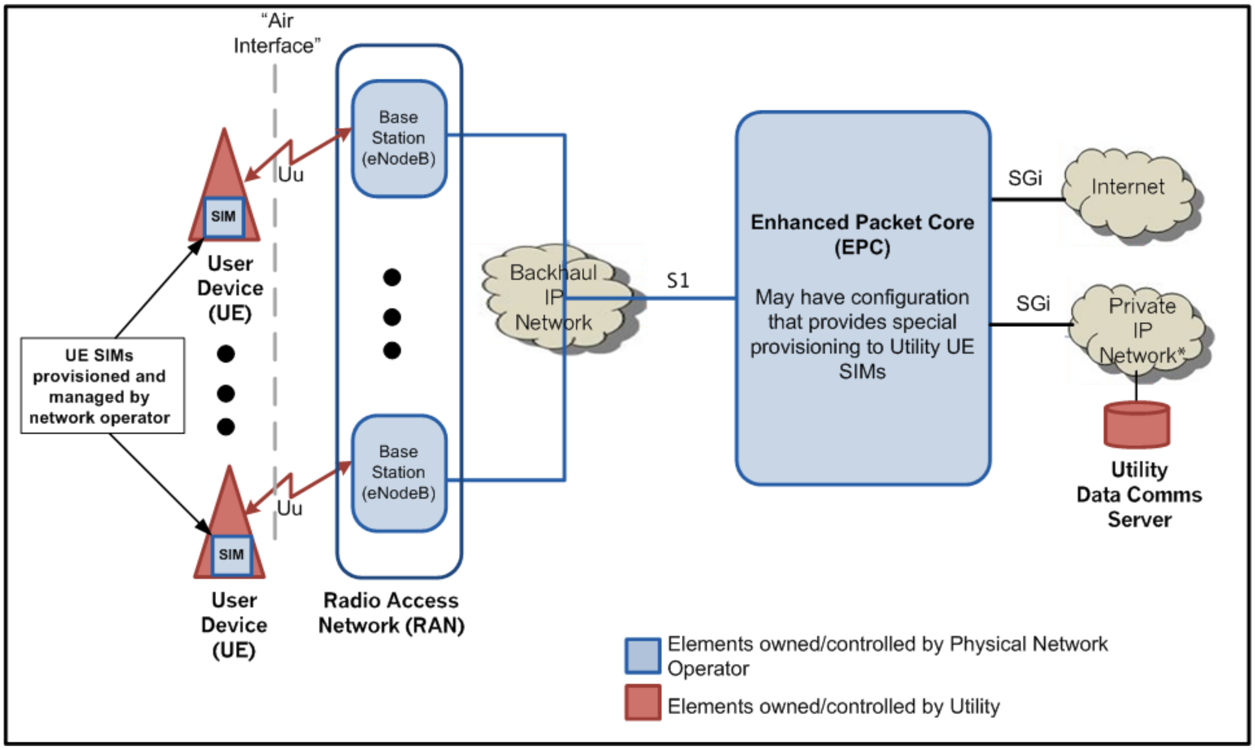

Figure 4-7
Enterprise Customer

In addition to addressing some important performance and security issues that might otherwise make use of a commercial wireless data network impractical for critical utility data communications functions, a contractual "enterprise customer" relationship may yield very important administrative benefits. In particular, a provision of services contract may obligate the network operator to provide staff and other resources to quickly address and resolve technical issues as they arise.

4.4.2 Commercial MVNO

Mobile virtual network operators (MVNOs) are generally commercial entities that resell mobile telecommunications services to consumers (or less frequently to businesses and/or governmental agencies). As the name implies, MVNOs do not themselves operate physical wireless networks but rather purchase services from such operators at bulk or wholesale prices and then resell these services to their customers. MVNOs must provide a commercially acceptable extent of geographic coverage (often nationwide, but in some cases regionally limited) by cobbling together agreements with one or more physical network operators that collectively provide that coverage.

In many cases, MVNOs handle most or all of the "back office" functions associated with wireless services, such as billing, marketing, and customer service. This relieves physical network operators of the associated costs, which they would otherwise have to bear (as they do for their own direct customers). Because MVNOs do not have to undertake the very high capitalization associated with building a physical wireless network—or the operating expenses of maintaining one—they can operate at very thin margin levels between retail and wholesale costs of the services they sell.

Like physical network operators, MVNOs may offer voice telephone services, packet data (generally Internet) services, or both. For purposes of this discussion, the focus here will be limited to the type of packet data services that would likely be employed by utilities for communications to and from remote devices placed in the transmission and distribution infrastructure and/or to and from AMI devices.

A typical architectural relationship between a commercial MVNO and a physical 4G LTE network from which it draws services is shown in Figure 4-8. It should be noted that the precise operational relationship will generally be governed by contract; thus, in some cases, the architectural relationship may vary somewhat from that depicted in this figure and described below.

In Figure 4-8, the MVNO server, which manages administration of mobile devices used by the MVNO customers, is connected to the physical LTE network through the public Internet. MVNO customer devices may be physically provisioned with SIMs programmed by or for the MVNO. Most critically, an MVNO device's list of preferred networks, governing which networks the MNVO will operate on in various geographic regions, is controlled by the MVNO and is informed by the service agreements that exist between the MVNO and the collection of physical network operators with which it contracts. Standardized over-the-air provisioning can be executed by the physical network in accordance with parameters defined by the MVNO. This allows the MVNO to make and execute changes to its service agreements without a requirement for recalling the devices for a physical SIM change (for example, changing the physical network operator that will provide service to its customers in a certain area).

The MVNO server is the main database for the identities and other profile data for the remote devices (UE) associated with the MVNO. These data are provided to the LTE network, typically using standardized protocols. User plane data, on the other hand, do not flow through the MVNO server, but rather are handled in the same way as user plane data to and from other UE operating on the network, which is typically over the public Internet. Thus, as depicted in Figure 4-8, user plane data between a utility data communications server and the various remote devices with which it communicates will be carried on the Internet.

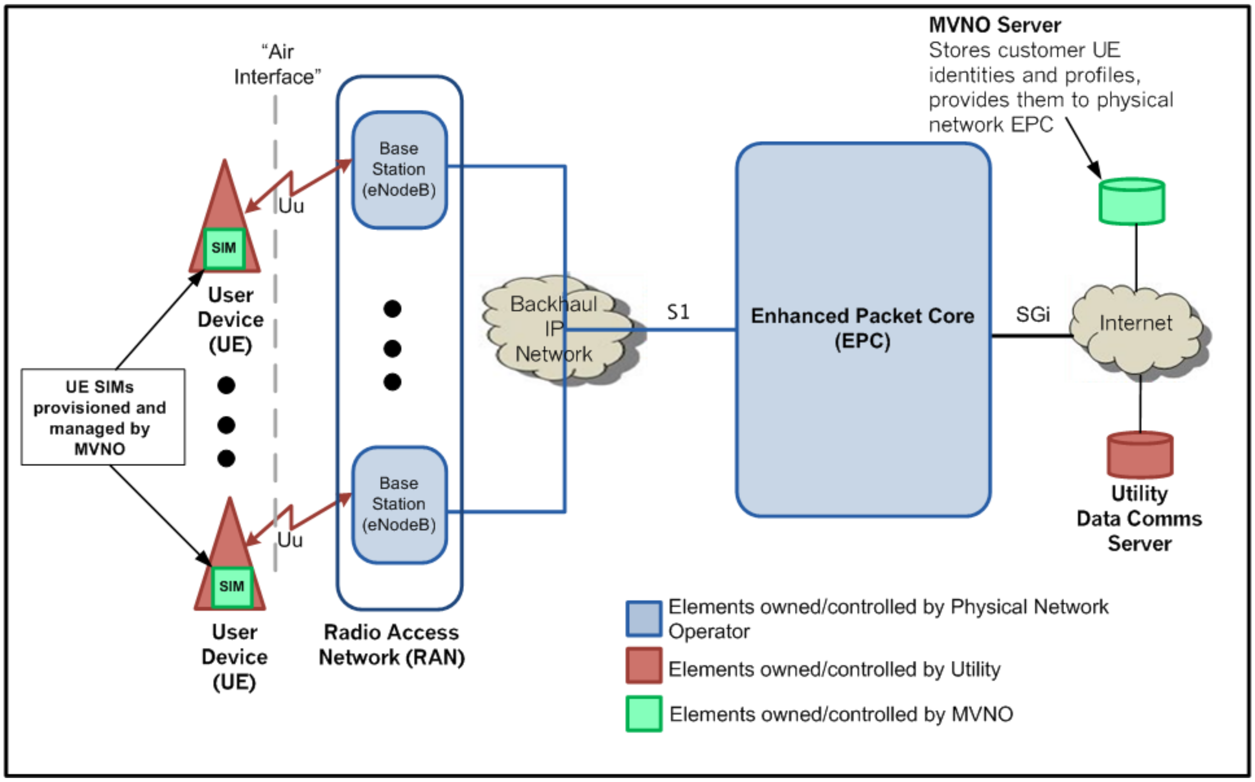

Figure 4-8
Commercial MVNO

Recent years have seen the emergence of MVNOs dedicated to providing M2M communications services. These services were initially developed primarily for applications such as wide range asset or vehicle tracking. In such cases, use of an MVNO (as opposed to a single physical network operator) can ensure consistency of operation over multiple physical networks and even over different communications technologies (for example, by integrating mobile satellite with LTE cellular to provide seamless global coverage). In some cases, M2M service providers may utilize their own data gateways, allowing user plane data to flow through their servers. Some M2M service providers actually offer value-added products such as asset management services and/or software.

From an administrative perspective, use of a commercial MVNO for utility data communications offers some attractions. For example, where the geographic reach of a utility's transmission and distribution network extends across multiple urban and rural areas served by several different physical network operators, an MVNO could provide a single administrative "point of contact" for provisioning and management of data communications. There are, however, a number of limitations to MVNO-provided services that might make them impractical for communications to and from at least the more critical remote devices in the utility infrastructure. In particular, quality, reliability, and resiliency of data communications services provided through MVNOs will usually be, at best, the same as the connected physical network operators provide to their general customer base. That means, for example, establishing a connection between the utility's data communications server and a remote device at a particular location may be unacceptably slow if the serving physical network is experiencing high traffic in and around the same location. Additionally, MVNOs generally will provide services on only one physical network in any particular area, eliminating the prospect of providing redundancy through utilization of multiple networks. Finally, obtaining services through a commercial MVNO introduces a layer of isolation between those responsible for management of utility data communications and the personnel within the physical network operation that could help resolve any service quality or security issues.

The architecture of MVNO-provided data communications services, as shown in Figure 4-8, would likely introduce significant issues of communications security, with user plane data being carried on the public Internet through an administratively isolated third party (the physical network EPC). Tools that might otherwise be used to enhance cyber-security—for example, use of a private IP network rather than the public Internet—may not be available.

4.4.3 Dedicated UVNO

What might be called a utility virtual network operator (UVNO) is a variation on the more established MVNO. Its organization and technical relationships with physical wireless networks are configured specifically to address a number of the shortcomings in MVNO-provided data communications services as they relate to the needs of utilities, particularly for connection to mission-critical remote devices.

Likely architectural relationships between a physical LTE network, a UVNO, and utility data communications devices and server are shown in Figure 4-9. (It should be noted that as UVNO implementations evolve, some details of these architectural relationships might change.) Comparing Figure 4-9 to the architecture for conventional commercial MVNOs shown in Figure 4-8, a number of significant differences can be seen.

As suggested in Figure 4-9, the contractual relationship between the UVNO and the operator of the physical network may include provision of standardized (or even proprietary) features that ensure adequate access priority and QoS treatment for communications between a utility's data communications server and its remote devices. Additionally, the provisioning and programming of SIMs within the utility's remote devices are managed by the UVNO, which is crucial to ensuring proper operation of the specialized functionality the UVNO provides.

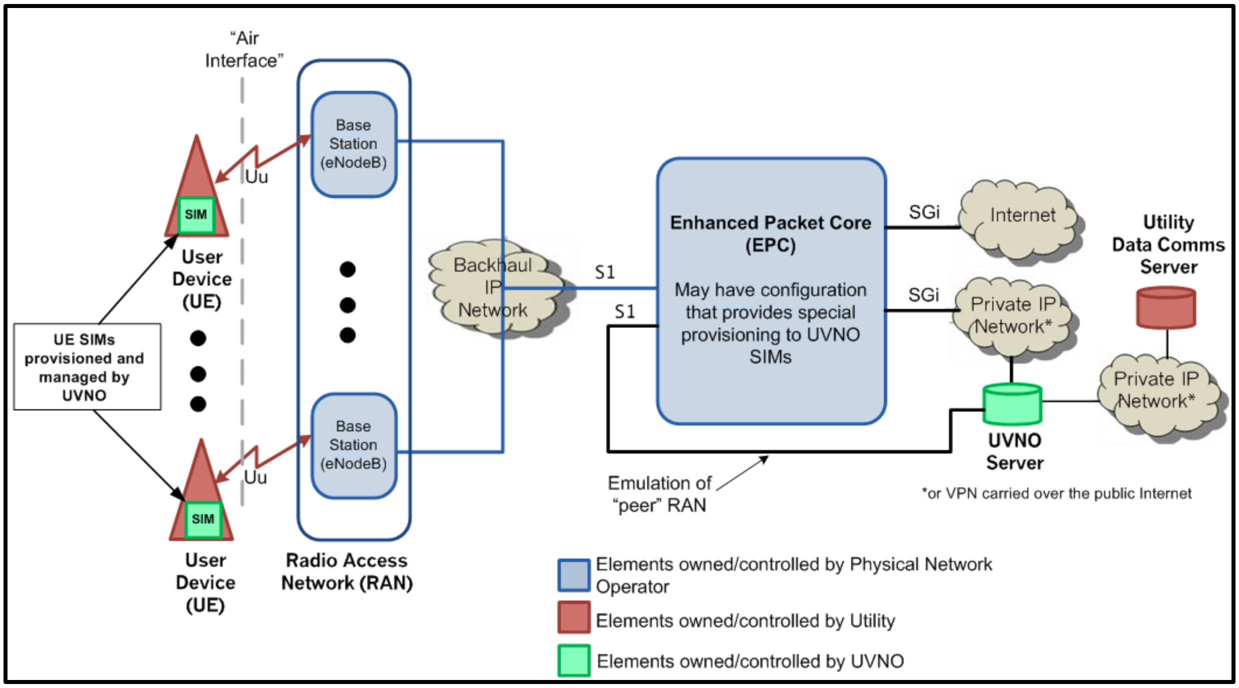

Figure 4-9
Dedicated UVNO

For enhanced security, the UVNO can connect to the physical network over a private IP network or a virtual private network (VPN) carried over the public Internet. Because it is specifically dedicated to serving the highly security-sensitive needs of utilities, the UVNO server itself can be provisioned with enhanced security features typically employed for such applications.

The UVNO server may also be provisioned such that all user plane data between the utility's data communications server and its remote devices will pass through the UVNO server on dedicated private IP networks or VPNs. This connectivity architecture provides a significant enhancement to protections against cyber attacks since both the utility's data communications server and its remote devices can be shielded from access via the Internet.

Reliability and resiliency of data communications through the UVNO can be substantially enhanced through use of redundant physical networks. To achieve this, the UVNO server is connected to the EPCs of two different physical LTE networks that serve the same geographical area. At remote locations where data communications are required, enablement of this network redundancy can be achieved in two ways. In one, the SIMs in each UE are programmed to access the "secondary" network in the event service in the "primary" network is disrupted. An even more robust redundancy can be achieved by providing independent UEs at the remote location, one provisioned for operation on "Network A" and the other on "Network B." Thus configured, protection is established against a failure or disruption of service on one of the networks and a failure of the remote location's UE.

Finally, as suggested in Figure 4-9, the UVNO server can interface with the commercial network EPC through an S1 interface as well as an SG1 interface. The S1 interface will allow the UVNO server to emulate a RAN parallel to the physical RAN. With this configuration, user plane packet data connections can bypass the physical network EPC entirely, allowing the UVNO to exert better control on latencies and cyber security.

As with a commercial MVNO, from a business and administrative perspective, reliance on a UVNO introduces a layer of isolation between those responsible for management of utility data communications and the physical network operator. However, since a UVNO is dedicated to providing critical communications services to utilities, it is reasonable to expect that they would be prepared to negotiate with physical network operators so as to address and resolve technical issues that impinge on such services. For example, in a case where the local physical LTE network does not provide reliable coverage to a particular location where one of their utility customers needs data connectivity, the UVNO could negotiate with the physical network operator to improve that coverage. Alternatively, the UVNO might be able to resolve the problem by, for example, installing an RF "booster" to improve coverage at that location.

4.4.4 Connection as a PVNO

A utility may contract with one or more physical network operators to connect to physical networks as a private virtual network operator (PVNO). To realize all of the operational and security benefits of such an arrangement, the utility would have to employ (or have employed on its behalf) a server (PVNO server) that would provide at least some of the provisioning, control, and administration of its remote devices. A likely architecture for PVNO connectivity with a physical LTE network is shown in Figure 4-10.

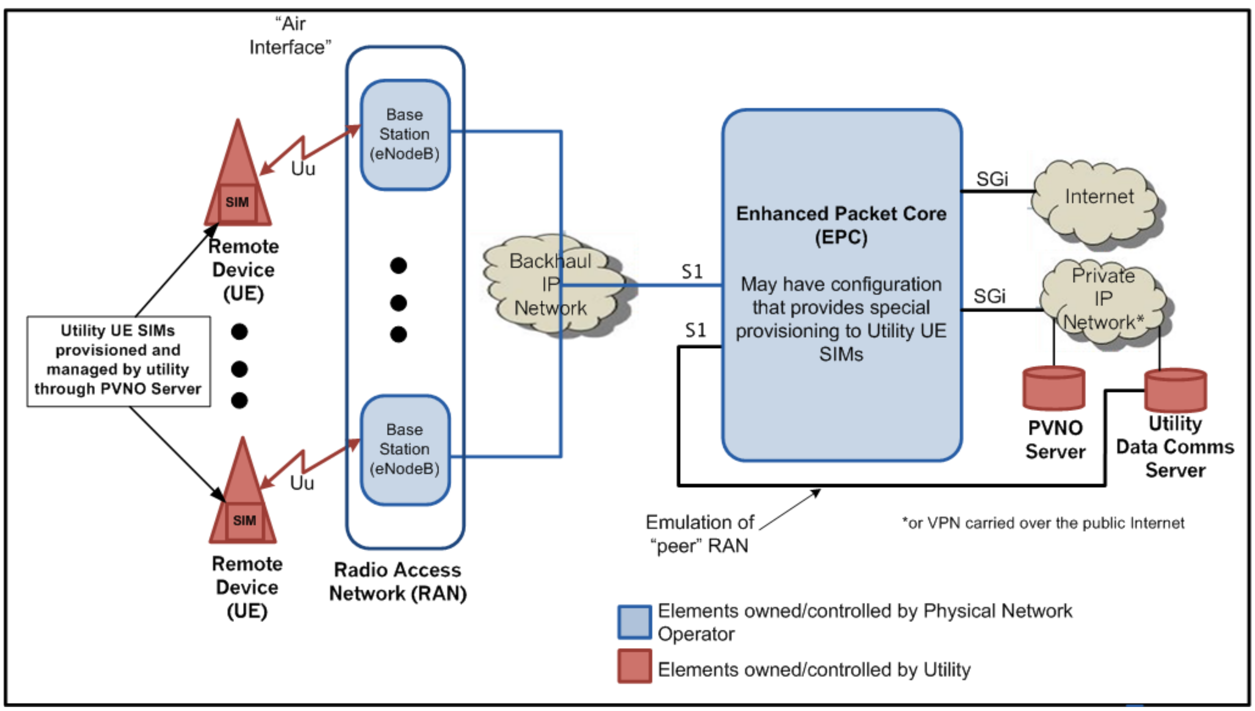

Figure 4-10
PVNO

While it could be housed in the same physical computing entity, the PVNO server is a separate functional entity from the utility data communications server that is the endpoint for user plane data communications with remote devices.[10] The PVNO server provides control plane information to the physical LTE network's EPC and serves to, among other tasks, manage the provisioning and programming of the SIMs in the utility's remote devices. This control plane functionality may also provide at least some of the provisioning for the physical network EPC that relates to the access priority and QoS treatment for utility data remote devices and communications.

As suggested in Figure 4-10, both user plane and control plane data transported to or from the physical network could be carried on a private IP network or a VPN carried on the public Internet. This connectivity would allow effective isolation of such communications, and the devices involved, from the Internet. Additionally, as in the UVNO case (see Section 4.4.3), the utility data communications server can interface with the commercial network EPC through an S1 interface as well as an SG1 interface, allowing user plane packet data connections to bypass the physical network EPC entirely for better control of latencies.

As discussed for the UVNO case, the PVNO server and utility data communications server could be provisioned to connect (by private IP network or VPN) to multiple physical networks, whether to achieve required geographical coverage or to provide redundancy of service over a particular area. At the remote devices network, redundancy could be enabled by appropriate programming and provisioning of remote device SIMS or by deploying redundant UE.

In utilizing the PVNO architecture for data communications over commercial wireless networks, the utility will be contracting directly with the network operator. This should allow direct interaction between those responsible for management of utility data communications and the appropriate network operator personnel, which could serve to expedite the addressing and resolution of technical issues. However, it should be noted that with respect to resource allocation, operations management of a commercial wireless network would be primarily focused on its core commercial services to its mass customer base. It might be prudent for utility communications management to be prepared to address certain technical issues on their own, for example, by deploying RF "boosters" to enhance coverage from the commercial network in an area where the coverage would otherwise be inadequate or unreliable and where the utility has deployed, or wishes to deploy, a remote device.

4.4.5 Sharing a Network with Public Safety Entities

4.4.5.1 700 MHz FirstNet

The First Responder Network Authority (FirstNet) was created by Congress in 2012 to establish a nationwide broadband network for public safety. FirstNet owns the license for 20 MHz of spectrum in the 700 MHz band that is allocated for public safety. FirstNet is chartered to build out a national, interoperable broadband public safety network, but it must accomplish that on a state-by-state basis. The network is expected to be funded by $7 billion (USD) in proceeds from other wireless spectrum auctions. Testing of the FirstNet broadband network is done by the Public Safety Communications Research (PSCR) laboratory, which is jointly operated by the

---

[10]Presumably, some utility user plane data communications may be directly between two or more remote devices, which would then not require connection to the data communications server.

National Institute of Standards and Technology (NIST) and the National Telecommunications and Information Administration (NTIA) in Boulder, Colorado. PSCR is funded by NIST, NTIA, FirstNet, and the U.S. Department of Homeland Security to conduct research and testing on public safety broadband networks. PSCR is working with vendors who contribute equipment, and they have a fully functional 700 MHz LTE network at their laboratory in Boulder.

From the beginning, these agencies have considered sharing the public safety broadband network with utilities. The ongoing operations and maintenance cost for the FirstNet network is estimated to be around $2 billion (USD) per year. Some of that funding is expected to come from secondary users. A great deal of synergy exists in the requirements for high-reliability public safety networks and utility FANs. Utilities could share towers and other structures for cell sites as well as their existing fiber for backhaul in exchange for access to the public safety spectrum. The law requires that entities sharing the spectrum have secondary status to public safety, but there has been no formal definition of what *secondary* means. Under FirstNet's current perspective, all secondary users, whether they are commercial Internet service providers or utilities, are treated the same. If FirstNet feels that they require the full capacity of their network, the secondary users would not receive any access. Secondary users would be removed from the network through the LTE preemption mechanism. Utilities would have little interest in investing in a network if they would be denied access to it during a scenario involving first responders. Utilities would be interested in sharing a network under terms that allow a certain percentage of the capacity to be guaranteed for critical monitoring and control purposes and a larger "upside" in everyday operation. For example, critical SCADA would be guaranteed no matter what, but AMI backhaul could be throttled or preempted in an emergency situation that taxes the network to capacity with public safety users. If FirstNet were willing to guarantee access on the network with a defined level of performance, utilities might be very interested in partnering. Without having guaranteed access on the network, utilities will most likely not partner with FirstNet or state governments to help build out the network.

FirstNet had intended to announce the recipient of the contract award in November 2016 after a 10 month request for proposals (RFP) process. Legal issues delayed the process. In March 2017, AT&T was selected as the deployment vendor to build and manage the network. FirstNet's position on utilities as network partners is expected to become clearer now that the deployment vendor has been selected.

5
TECHNOLOGY DECISION PROCESS

A process will be developed to help define a "best-fit" architecture for a specific utility. In many cases, there will be more than one possible choice. The process will include five major progressions depicted in Figure 5-1. Tools, methods, and metrics will be created to streamline each step in the process. The first step will clearly define bounding conditions for the communications system. This includes a specific serviceable territory definition, legacy system constraints, current traffic and communications needs, projected traffic and communications needs, available spectrum, and other factors. Steps 2 and 3 will define the system needs based on the bounding conditions and then organize needs across system tiers. Steps 4 and 5 will then provide a mechanism to compare and select architectures and technology choices that best fit the system needs.

The technology hierarchy will define tiers for the communication system based on quantitative dimensions (latency, throughput, security, and QoS). Technologies can then be mapped to the tiers, and adjustments can be made or tiers added as it is determined how technologies, applications, and tiers all map to each other. This would be defined through a "binning" based on knowledge of available technology and experience. Groups of nodes can then be mapped to required tiers of service, constrained by bounding conditions relative to the location of the interface. For example, fiber cannot be installed to every distribution sensor, and such devices will probably employ forms of wireless connectivity. The end result is a definition for a system segmented by tiers and technology and mapped across utility bounding conditions.

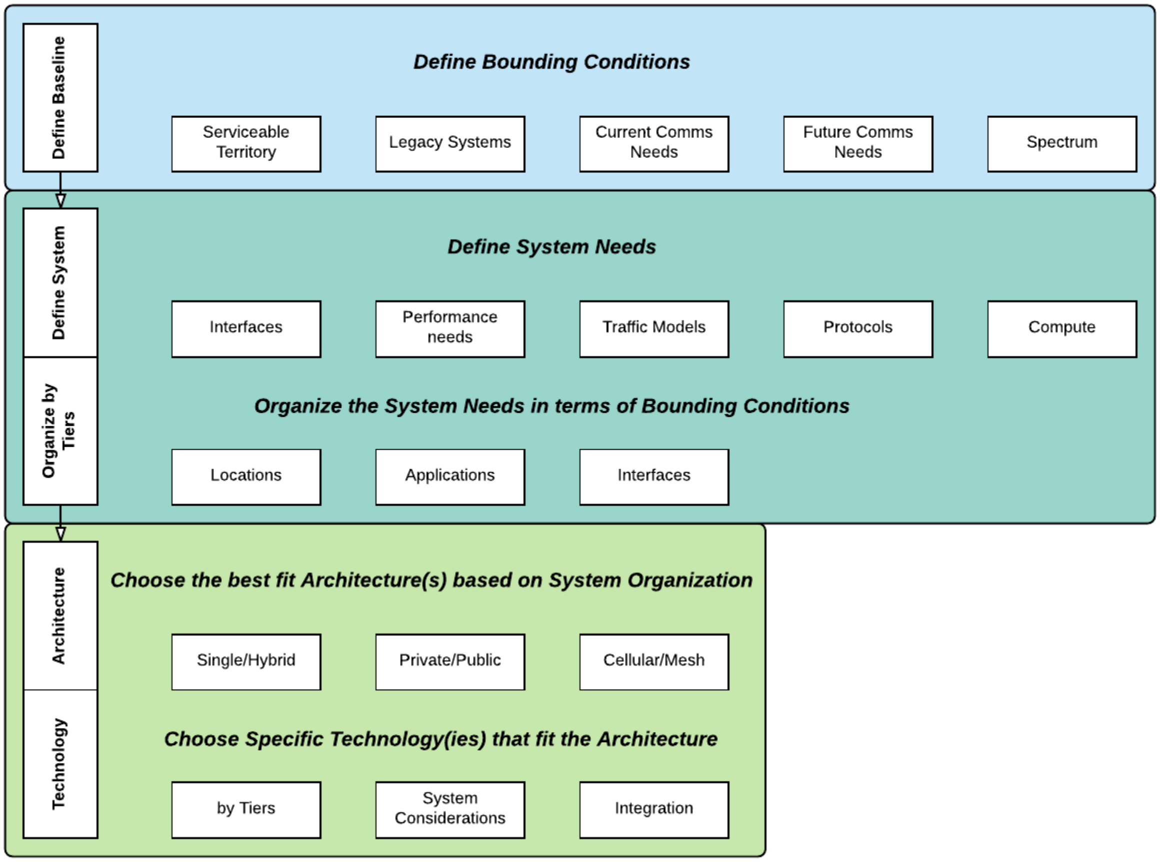

Figure 5-1
Technology Decision Process: Five Major Progressions

Complex factors contribute to making a communications system decision. This decision is also compounded by the fact the system will need to be in place for the next 20 years, and once deployed, it will be very difficult or impossible to change. It is therefore critical that this process focus on quantified metrics to help make decisions under specific conditions (such as capacity per square kilometer or cost per square mile per capacity). Such metrics will help utilities to make the best selections while weighing business costs and regulatory constraints.

A

DEFINITIONS AND GLOSSARY

Coverage Probability	For a typical deployment, this is the probability of coverage for any device. This represents taking 100 devices randomly distributed across the defined serviceable territory and measuring how many meet a defined level of performance.
Goodput	Defined as the application-level throughput (that is, the number of useful information bits delivered by the network to a certain destination per unit of time). The amount of data considered excludes protocol overhead bits as well as retransmitted data packets.
Raw PHY Rate	Defined as the physical layer bit rate or the total number of physically transferred bits per second over a communication link.
Territory	The entire area in which a utility is responsible to provide service.
Serviceable Territory	The area of coverage necessary to cover all current and projected devices within the territory, for example, a one-quarter mile buffer around all distribution lines.
Morphology	In RF planning, morphology describes the density and height of man-made or natural obstructions and can be classified into areas such as urban, suburban, and rural.
Capacity	For a specific node within a network, the maximum goodput that can be delivered to the node measured in bits per second.
Latency	The one-way delay between two nodes of a communication system for a 256-bit User Datagram Protocol (UDP) packet.
Packet Error Ratio (PER)	The ratio of numbers packets received without error divided by the total number of packets sent over a long time interval, expressed in percentage.
Reliability	A metric expressed in nines (9s) (%), with an equivalent time per year: 3 - 9s = 8.76 hours outage per year 4 - 9s = 52.56 minutes outage per year 5 - 9s = 5.256 minutes outage per year 6 - 9s = 31.54 seconds outage per year 7 - 9s = 3.15 seconds outage per year
WAN Interface Device (WID)	The boundary wireless router or microwave radio between the FAN network and high speed (for example, fiber) core network.

Availability	The percentage of time within a 30-day study period that PER <99.9% traffic flows from ingress to egress of the FAN network
Back Office	Information technology (IT) infrastructure connected to a core high speed network.
Device	Devices deployed in the field as part of the FAN system including both field devices and FAN aggregation devices
FAN Aggregation Device (FAD)	The boundary router into the FAN network, which may be the same as the WAN interface device. A FAN aggregation device may also be a field device when it is directly connected to a grid control or sensing device.
Field Device (FD)	All edge node communication devices (for example, wireless routers and end nodes) that make up the FAN, defined as being directly connected to grid control or sensing devices.
FAN network	Ingress of messages or signals from mesh end nodes to the egress of those messages at the WID or field aggregation device located at a substation.
Intelligent Electronic Device (IED)	Microprocessor-based controllers of power system equipment such as circuit breakers, transformers, and capacitor banks.
Mobile Virtual Network Operator (MVNO)	A MVNO, or mobile other licensed operator (MOLO), is a wireless communications services provider that does not own the wireless network infrastructure over which the MVNO provides services to its customers. An MVNO enters into a business agreement with a mobile network operator to obtain bulk access to network services at wholesale rates, then sets retail prices independently.[1] The MVNO may use its own customer service, billing support systems, marketing, and sales personnel, or it could employ the services of a mobile virtual network enabler (MVNE).
Private Virtual Network Operator (PVNO)	A PVNO is an entity such as a utility that contracts with one or more commercial wireless network operators to provide it with radio access network (RAN) services through a dedicated peer-to-peer network connection.
Field Area Network (FAN)	A utility communications network that is deployed to support the distribution system. The boundary of the FAN is usually defined as any components of the overall communications system that extend beyond wired high-speed core networks.
Wide Area Network (WAN)	WAN covers a large area and provides high speed backhaul to a utility FAN (for example, core fiber WAN or cellular WAN).
ISM	Industrial, scientific, and medical frequency bands
MAC	Media access control layer of a communication system
PHY	Physical layer of a communication system

B

SAMPLE METRIC TEMPLATE DEFINITIONS

Defining specific values for technology metrics is a non-trivial effort as many assumptions are dependent upon the service territory morphology, spectrum choice, endpoint/remote radio quantity/density, utility internal capabilities, outsourced labor rates, cost of capital, and numerous other items. As such, it is not possible to give specific numbers for the technologies within this document. Table B-1 provides a suggested set of metrics for utility use and for possible inclusion as part of RFPs, while Table B-2 presents succinct loading definitions.

Table B-1
Sample Metric Template

Metric	Description
Peer-to-peer capacity	For lite, moderate, full, and saturated, measure the aggregate capacity between two peer devices.
Capacity per FAD	For lite, moderate, full, and saturated, measure the aggregate capacity at a FAD device.
$/km^2	For the total estimated cost of the field-deployed devices (including all extraneous hardware, installation costs, and operational costs over the 15-year life of the system), divide by the area supported by the system. This does not include back office system components.
kbps/km^2, from field to core	For lite, moderate, and full loaded networks, define the average data flows from the devices to the core routers, normalized to square kilometers.
$/kbps/km^2, from field to core	Normalized cost per capacity per area
Hop distribution to core	This is the estimated histogram of the hop count distribution for the modeled deployment areas, which does not include WAN backhaul as a hop. For mesh systems, include each hop from the FAN aggregation device to the field device. For cellular systems, count repeaters as hops. Provide the 90th percentile of distribution as a fixed metric.
Average latency distribution to core	For lite, moderate, and full loaded networks as well as the data flows from the devices to the core routers, this represents a distribution of the average latency over a statistically relevant number of packets. Provide the 90th percentile of distribution as a fixed metric.
Average latency distribution to field	For lite, moderate, and full loaded networks as well as the data flows from the core routers to devices, this represents a distribution of the average latency over a statistically relevant number of packets. Provide the 90th percentile of distribution as a fixed metric.
Average latency peer to peer	Latency between two peers in the network

Table B-2
Loading Definitions

Loading	**Definition**
Lite	This is a very lightly loaded network with little or no contention, representing near ideal lab conditions for good link connectivity and low interference.
Moderate	The serialization point of the network is at 50% full loading capacity (for example, a base station or mesh access point).
Full	The serialization point of the network is at 100% capacity (for example, base station/FAN aggregation device). At this point, the output rate is 90% of the input rate.
Saturated	The serialization point of the network is at 125% full loading capacity (for example, base station or mesh access point).

C
EXAMPLE OF WI-SUN LATENCY

To understand how the media access protocols function in these systems one can imagine each device as a rotary switch with multiple positions. Each position represents a direct peer mesh node. At any time, a switch can only be in one position and it can typically only receive or transmit. As a result, the routing and lower layer MAC protocols must manage how to best optimize the communications between devices. Each device must keep track of its "neighbors" and best routes to other peers. Once the best route is determined, the device must "decide" based on link quality how to best send a packet. The highest speed modulation possible should be used on a per packet basis if possible. Some solutions will employ a digital signal processor (DSP) that can perform link management on a packet-by packet basis, while others will negotiate a link speed and only change at a slow rate. Once the target and mode is determined, a typical data link transaction may flow as depicted in Figure C-1 below.

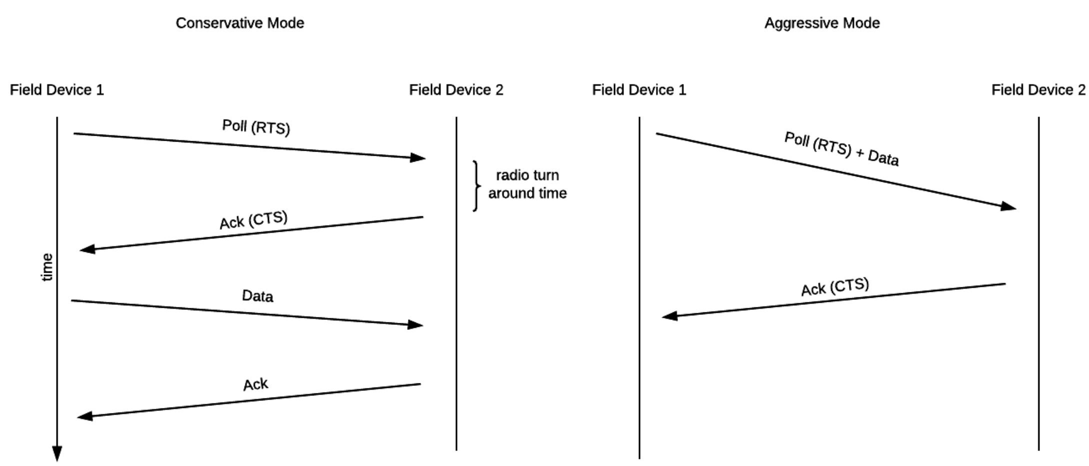

Figure C-1
Generic Data Link Mechanisms

This is a generic representation of how the link between each meshed node sends data. In a congested environment, a small poll or request to send (RTS) packet will be sent to sound the channel. Once acknowledged, the larger data packet is sent. In less congested environments, the system may dynamically use a more aggressive mechanism and simply send the data, resulting in lower latency communications. For example, with a 256-byte payload and very conservative overhead estimates:

- RTS: 64 bytes
- CTS: 32 bytes
- Data header: 64 bytes
- Data: 256 bytes

A state-of-the-art radio should achieve a turnaround time of better than a few hundred microseconds; some of the older systems achieve turnaround times on the order of 1–3 ms.

For a conservative mode, the following equation is used:

$$[(64B + 32B + 64B + 256B) * 8\ bits/B]/800\ kbps\ + 3 * 1\ ms\ =\ 7.16\ ms$$

For a more aggressive mode, the following equation is used:

$$[(32B + 64B + 256B) * 8\ bits/B]/800\ kbps\ + 2 * 1\ ms\ =\ 5.52\ s$$

Adding another 1–2 ms for upper layer processing and queuing allows for a best case theoretical one-way single hop latency on the order of 10 ms.

Export Control Restrictions

Access to and use of EPRI Intellectual Property is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or permanent U.S. resident is permitted access under applicable U.S. and foreign export laws and regulations. In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI Intellectual Property, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case-by-case basis an informal assessment of the applicable U.S. export classification for specific EPRI Intellectual Property, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes. You and your company acknowledge that it is still the obligation of you and your company to make your own assessment of the applicable U.S. export classification and ensure compliance accordingly. You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of EPRI Intellectual Property hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI members represent 90% of the electric utility revenue in the United States with international participation in 35 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together…Shaping the Future of Electricity

3002009786

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com