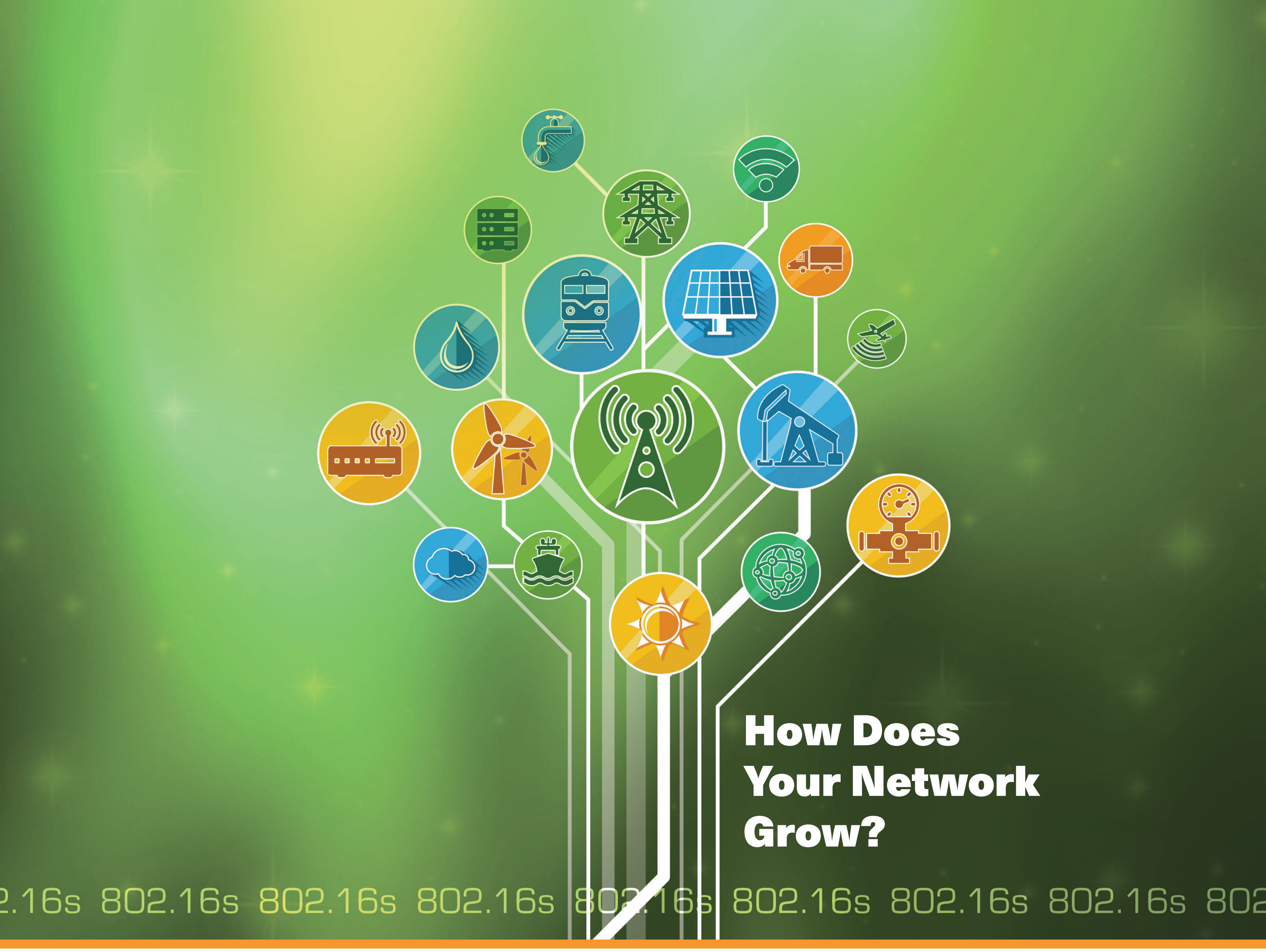

How Does
Your Network
Grow?
802.16s 802.16s 802.16s 802.16s 802.16s 802.16s 802.16s 802.16s 802

The Case For Private, Standard Technology Wireless Mission Critical Communications Networks

Kathy Nelson, P.E.

ONDAS NETWORKS
Connectivity solutions for
MISSION CRITICAL IoT

Private vs. Public Networks

For several decades, critical infrastructure entities, such as oil and gas, utilities, rail, and first responders, among others, have relied on their own telecommunications networks. These privately owned, privately maintained networks have been used to manage day-to-day operations and to coordinate emergency services in times of crisis.

Many of these networks need to be mission-critical and have used portions of the wireless spectrum that were either unavailable to other users or unwanted by other industries. Historically the FCC has made some narrowband spectrum available through spectrum coordinators to allow for a geographic reuse without interference. Increasingly these low data capacity networks are struggling to keep up with the new technology. Additionally, the use of private, uncrowded portions of the spectrum was employed because mission-critical tasks like providing power, producing and providing energy to the public, protecting citizens, and responding to disasters needed clear, reliable channels of communication to be effective.

In recent years, however, as these mission-critical networks have evolved, the deployment of new services has caused an exponential increase in data communications and has strained the capacity of many in-place infrastructures. At the same time, the ongoing need to implement and maintain security, both cyber and physical, has added to the data requirements of mission-critical networks.

More Modernization, Less Interference

Many of today's mission-critical networks face a two-fold challenge. First, there is the need to modernize. The present-day requirements for real-time data, sophisticated control and monitoring functions which continue to move farther to the network edge, and high-level security place new demands on the underlying infrastructure and are often more than existing narrowband networks can support.

Second, there is the need to ensure the quality of communications. Some portions of the licensed spectrum – those used by first responders, for example – remain dedicated solely to their use and are therefore clear from interference, but others are much more congested due to changes in allocation. Many of the portions of the spectrum where mission-critical services have traditionally operated are either being reallocated to commercial providers or made accessible to other users and, as a result, experience increased interference.

Do Public Cellular Networks Meet the Need?

As mission-critical services address the challenges of modernization and are forced by the spectrum crunch to seek alternatives with less signal interference, there is pressure to make use of public cellular networks simply because these public networks are available. Using a commercial network for mission-critical services can lower capital cost, since the initial capital expenditure is lower, but all the other decisions involved in running a network are left up to the service provider. That is, someone else decides how spectrum is allocated, the schedule for technology upgrades and maintenance, how to ensure availability, and so on.

While commercial network providers may be eager to gain the business of mission-critical services, and may make some accommodations to structure their offerings to suit their needs, the long-standing commitments these providers have to consumers influence their policies. For example, cellular technology supports prioritization, which lets network operators give priority to mission-critical communications, but today's commercial providers don't make use of the capability. That means consumer-driven demand, for things like streaming media, takes bandwidth away from mission-critical services when it's needed most.

The other consideration when working with a public cellular provider, beyond losing control of how the network is managed and the lack of prioritization, is the fact that commercial networks don't typically provide the level of performance necessary to support mission-critical applications.

Stringent Requirements

Critical infrastructure industries simply cannot compromise when it comes to connectivity, which is why organizations have relied on their own networks for so long – they deal with operating requirements that are more stringent than in other industries and their business continuity drivers require a committed network that is highly stable and predictable.

By running their own networks, mission-critical services can be certain they have the four things needed to remain responsive and effective in times of emergency: reliability, availability, latency, and security.

RELIABILITY | Communication with personnel and devices needs to go through, without interference, even if transmission and reception take place in rural or remote areas.

AVAILABILITY | These critical networks cannot afford down time. The goal of 100% network availability may only be attainable in theory, but a standard for today's mission-critical networks is 99.999% availability, which equates to five minutes of downtime per year. Few, if any commercial networks offer this level of availability. Even 99.99% availability, which equates to 52 minutes of downtime per year, is not a level of service commercial carriers and their publicly available, consumer focused network products are willing to provide.

LATENCY | Control and signaling communications sent to and from remote devices must be delivered without delay, at extremely low latency rates. When performing tasks such as remotely controlling oil or gas flow and equipment, switching a power line, controlling a circuit breaker, or sending a stop command to an out-of-control train, the signal needs to be transmitted in a fraction of a second, but commercial networks can never guarantee latency rates this low.

SECURITY | Safety and protection are of primary importance, for employees as well as the public, since extreme harm can result if a mission-critical infrastructure is hacked in any way. Access to the network needs to be restricted to ensure only authorized personnel can get into the network, and data transmissions need to be encrypted, to prevent tampering, theft, or, worse yet, acts of sabotage or terrorism.

Commercial Cellular Falls Short

Commercial public cellular networks simply don't offer the levels of reliability, availability, latency, and security that mission-critical services require. Designed primarily for the consumer market, commercial cellular networks tend to focus the majority of their resources on urban, more populated areas, where consumers use high-bandwidth connections.

While these public cellular networks are usually equipped to deal with short-term blackouts and other service interruptions, they're not typically prepared to the same extent that mission-critical networks are. Where a commercial base station might have backup batteries onsite that provide four to eight hours of operation, or might be able to connect to a backup power source, such as a generator, mission-critical networks tend to have onsite generators that are fueled and ready to run for days at a time, if not a week or more, without a service call. Many sites also have redundant backhaul paths or rings, to improve data accessibility to the site during emergencies, and put redundant radio hardware in place to ensure continuity.

Real-World Failures

The very real impact of natural disasters has made clear, in recent years, the risks of relying on public cellular networks for mission-critical services. In August 2017, when Tropical Storm Harvey made landfall in Texas, 55 counties were declared disaster areas. The impact report published by the Federal Communication Commission (available at fcc.gov), shows that heavy rain and high-speed winds led to cellular outages scattered throughout the area, with some counties experiencing coverage losses as high as 94.7%.

The local utility, however, that owns, operates, and maintains a private land mobile radio system, as well as a private network for mission-critical communications for monitoring and controlling devices (SCADA), maintained 100% communication availability during the entirety of Harvey. They had only one outage, caused by extensive flooding, at a single substation.

The situation was similar in October 2018, when Hurricane Michael impacted the U.S. Gulf Coast. There were cellular outages throughout the 100 counties in Alabama, Florida, and Georgia impacted by the storm, with the FCC reporting that some counties lost up to 88.9% percent of coverage. Cellular service continued to be spotty well after the storm made landfall, with the FCC reporting significant outages in some areas even two weeks later.

It's important to note that cell site outages are often due to power outages. Any critical infrastructure service that relies on a public cellular network for communications will fail to respond during blackouts and other emergencies, because having a cell site go down means communication with personnel and devices in the field goes dark. That is, any communication network intended for use during power outages simply has to have a reliable source of backup power.

The Private Licensed Alternative

Discouraged by the prospect of sharing spectrum with the general public, on a commercial cellular network that is unlikely to meet their needs for continuity and security, mission-critical services are expanding and enhancing their private networks to gain the connectivity and coverage they need.

These private networks operate in FCC protected licensed spectrum. Licensing ensures that wireless operators don't interfere with each other's transmissions and gives mission-critical services an operating environment that is virtually free of the interference associated with unlicensed channels. As a result, for mission-critical entities to have their own private networks, they need access to licensed private spectrum.

The Need for Standard Technology

While private networks are critical to mission critical industries, most critical infrastructure entities do not typically have access to enough spectrum to deploy standard technologies, such as LTE or IEEE 802.16, the two most common wireless technologies. Additionally, standards such as LTE, were designed for the consumer industry, not mission critical industries. This means that critical industry companies are forced to install communications networks that are proprietary, which puts them at risk if the manufacturer goes out of business or discontinues their product line.

However, in the fall of 2017, a new narrower channel standard technology was ratified and published by the IEEE.

IEEE 802.16s effort was a grass roots effort launched because electric utilities looking for a standard technology that could be used in the narrow channel bands they have access to, typically purchased on the secondary market such as the 700 MHz A band, 217 – 219 MHz, 1.4 GHz, etc. These spectrum bands do not have enough bandwidth to support other standard technologies. LTE requires a minimum of 1.4 MHz and IEEE 802.16 a minimum of 1.25 MHz of bandwidth.

Public broadband wireless technologies are evolving towards higher speeds and smaller cell sizes and are focused on consumer applications. The public Internet of Things (IoT) services such as Narrowband LTE (NB-LTE) are being deployed with a focus on consumer market applications and are not well suited for mission critical IoT applications.

The IEEE 802.16s standard is designed for the mission critical private broadband wireless market. It provides multimegabit throughput using relatively narrow channel size (between 100 kHz to 1.20 MHz) and long range (e.g., 25 miles and beyond) to minimize spectrum acquisition and network infrastructure cost.

IEEE 802.16s is optimized for mission critical remote control applications, not the consumer market. Many mission critical applications such as Supervisory Control and Data Acquisition (SCADA) require more data to go from the remote devices, such as a substation, to a master device. This is a reverse asymmetrical data flow and is nearly opposite to the consumer market which is heavily driven by data that goes from the network to the remote device, such as in streaming Netflix videos, etc. IEEE 802.16s addresses this by adopting Time Division Duplex (TDD) with a downlink to uplink traffic ratio up to 1:10.

Frequency Division Duplex (FDD) vs. Time Division Duplex (TDD)

LTE and several proprietary technologies are based on FDD due to the fact that spectrum has historically been paired. To understand the difference between FDD and TDD, think of FDD as a freeway where there are the same number of traffic lanes going into and out of a city. During morning rush hour, all the traffic lanes going into the city are clogged and traffic is moving slower due to congestion, while the traffic lanes going out of the city are mostly empty. It would be more effective if some of those lanes could be configured so that more of them could go into the city because there is more traffic. TDD allows for that "traffic lane" configuration. The number of "lanes" moving traffic in each direction is configurable, making more efficient use of the RF spectrum. This is very important when RF spectrum is limited and is the basis of IEEE 802.16 and IEEE 802.16s.

IEEE 802.16s Highlights

While IEEE 802.16 is a good base for an efficient wireless technology, changes were needed to adapt it and make it even more efficient in narrower channels, namely reducing the overhead so more user data could be transmitted. The standard is designed so it can be reverse asymmetrical, more throughput for upstream than downstream, which is how most mission critical systems function although it can be symmetrical or asymmetrical, depending on system requirements. The next several paragraphs compare the differences between IEEE 802.16 and IEEE 802.16s to show how the overhead is reduced in order to make the standard more efficient.

IEEE 802.16s Air Interface Protocol Highlights

IEEE 802.16s supports channel sizes between 100 kHz and 1.20 MHz. The standard specifies the air interface protocol parameters in 50 kHz increments, starting at 100 kHz. IEEE 802.16s is based on the 128 Fast Fourier Transform (FFT) flavor of the IEEE 802.16 as they are applied to a 1.25 MHz wide channel and has a 10.94 kHz subcarrier spacing. IEEE 802.16s fits the waveform bandwidth to the narrower channels as follows:

- The sampling clock is reduced to accommodate narrower channel bandwidth resulting in a reduction in subcarrier spacing.
- The number of sub-channels is reduced to avoid excessive subcarrier spacing reduction.

IEEE 802.16s uses the following subcarrier allocation schemes:

- Use of adjacent subcarrier per sub-channel allocations scheme known as Band Adaptive Modulation and Coding (AMC).
- Three mandatory Band AMC subcarrier allocations schemes are defined in the standard:
  - Band AMC 2 X 3 (Optional in IEEE 802.16)
  - Band AMC 1 X 6 (Optional in IEEE 802.16)
  - Band AMC 1 X 3 (A new subcarrier allocation scheme for IEEE 802.16s)

The IEEE 802.16 standard preamble for 128 FFT employs 36 subcarriers interleaved every third carrier. IEEE 802.16s standard specifies two new preamble schemes to fit into 54 and 27 subcarriers respectively. The new preamble sequences maintain the IEEE 802.16 autocorrelation to cross correlation ratio performance. The IEEE 802.16 ranging Code Division

Multiple Access (CDMA) code for 128 FFT employ 96 subcarriers, whereas IEEE 802.16s specifies 2 additional CDMA code schemes to fit into 54 and 27 subcarriers respectively.

IEEE 802.16s uses a total of 128 subcarriers. 108 of these are active subcarriers, 19 are guard subcarriers, 12 are pilots, and one is a DC subcarrier (see figure 1).

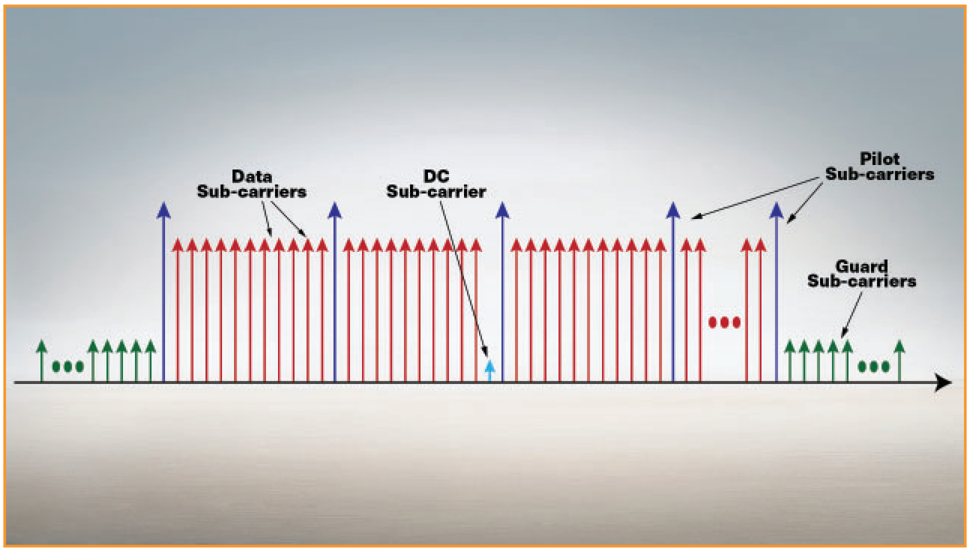


Figure 1

Additional Air Interface Protocol Changes for Better Frequency Utilization

The following air interface protocol changes were made in IEEE 802.16s to make better use of spectrum:

- Convolutional Turbo Coding (CTC) is mandatory. This lowers the Forward Error Correction (FEC) Code thresholds relative to Convolutional Coding (CC).
- Make 64 QAM 5/6 a mandatory scheme to enable higher frequency utilization (30 bytes per slot) if conditions allow.
- Use single zone with band AMC in both downlink and uplink directions to avoid the overhead of multiple zones scheme.
- Support new frame durations of 10 ms, 12.5 ms, 20 ms, 25 ms, 40 ms, and 50 ms to reduce per frame overhead for narrower channels while maintaining the IEEE 802.16 standard 5 ms frame duration for use at higher ends of the channel bandwidth.
- Support of Cyclic Prefix values of 1/8, 1/16 and 1/32 to reduce overhead if multipath conditions allow.
- Supports DL:UL ratio in the range 10:1 to 1:10 to support asymmetrical and reverse asymmetrical applications.

IEEE 802.16s TDD Frame Structure

IEEE 802.16s has a configurable TDD frame structure which includes a frame duration between 5 ms and 50 ms. It includes a downlink to uplink ratio between 1:10 and 10:1 with gaps that can be configured to accommodate a very long range. The new standard allows up to 12 subchannels with Band AMC 1X6 or Band AMC 1X3 and downlink bursts do not need to be rectangular as with IEEE 802.16, meaning more data can be packed into the frames, resulting in less overhead. Uplink allocations may be limited to a number of subchannels as needed to make the link, for example, limiting to a single subchannel maximizes Transmit Power Density (TPD) (see figure 2).

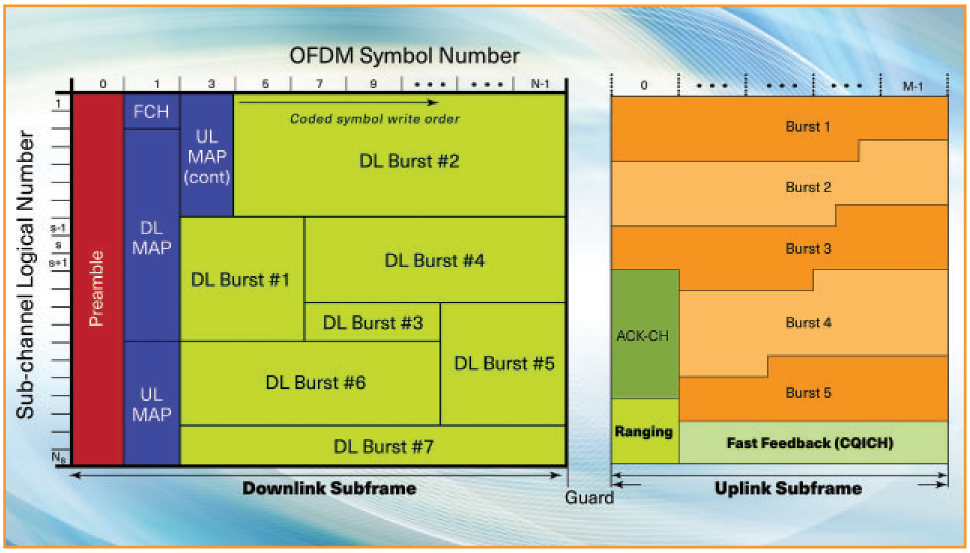


Figure 2

Partial Use of Sub-Channels (PUSC) vs Band AMC Subcarrier Allocation Schemes

In the IEEE 802.16 standard, Partial Use of Sub-Channels (PUSC) is mandatory in the first zone in both the Uplink (UL) and the Downlink (DL). The use of multiple zones introduces extra overhead and is not a good fit within relatively narrow channels. A DL PUSC slot consists of one sub-channel by two Orthogonal Frequency-Division Multiple Access (OFDMA) symbols. A slot is the smallest entity allocated by the MAC layer. The downlink allocation is done frequency before time. In the DL PUSC PHY Layer, there are 72 data subcarriers per symbols, 12 pilot subcarriers per symbol and one DC subcarrier, which results in the utilization relative to preamble bandwidth allocation of 72 /108 = 66.7% for DL and the utilization relative to bandwidth allocation of 72/96 = 75%. For UL, the utilization relative to preamble bandwidth allocation of 8/12 or 67% and the utilization relative to bandwidth allocation of 67% * 96/108 = 59.55%.

With PUSC, there are a large number of guard subcarriers. This impact can be offset by adjusting the symbol rate. Additionally, there are a large number of pilots and each section of the TDD frame employs a different number of subcarriers:

- Preamble: 108 subcarriers
- DL PUSC: 84 subcarriers
- UL PUSC: 96 subcarriers
- Ranging CDMA codes: 96 sub-carriers

Bandwidth consumption is determined by the preamble but is not fully utilized by other sections of the TDD frame. Subcarriers for each sub-channel are interleaved across the entire channel however sub-channels cannot be used for narrower channels. The number of DL subchannels is different from the number of UL subchannels which creates a re-use problem as there are a small number of subchannels.

The preamble is used for remote station phase and frequency synchronization and employs three sets of 36 subcarriers out of 108 subcarriers. Each subcarrier is Binary Phase Shift Keying (BPSK) modulated with a pseudorandom code. Each set employs every third subcarrier with each set extending over 108 subcarriers. Additionally, the preamble power is boosted by 9 dB relative to the data power level.

Band AMC Sub-Carrier Allocation Principles

Band AMC, on the other hand, uses continuous sub-carrier mapping with the same allocation in the downlink and the uplink. The full channel allocation is aligned with the preamble. There are nine subcarriers which are collected in a bin (8 data + 1 pilot) and the bins are collected in sub-channels of 1x6, 2x3 or 3x2 (see figure 3).

Band AMC 2 X 3

- Total Number of bins per sub-channel in 2x3 AMC = 6
- Total Number of sub-carriers/Bin = Pilot-1 + Data-8 = 9
- Total Number of sub-carriers/sub-channel = 9 * 6 = 54 (6 Pilot + 48 Data) = 1 Slot
- Total Number of sub-channels = 6
- PHY Layer utilization:
  - » 288 data sub-carriers
  - » 36 pilot sub-carriers
  - » PHY Layer Utilization for AMC = 288/(288+36) = 88.88 %

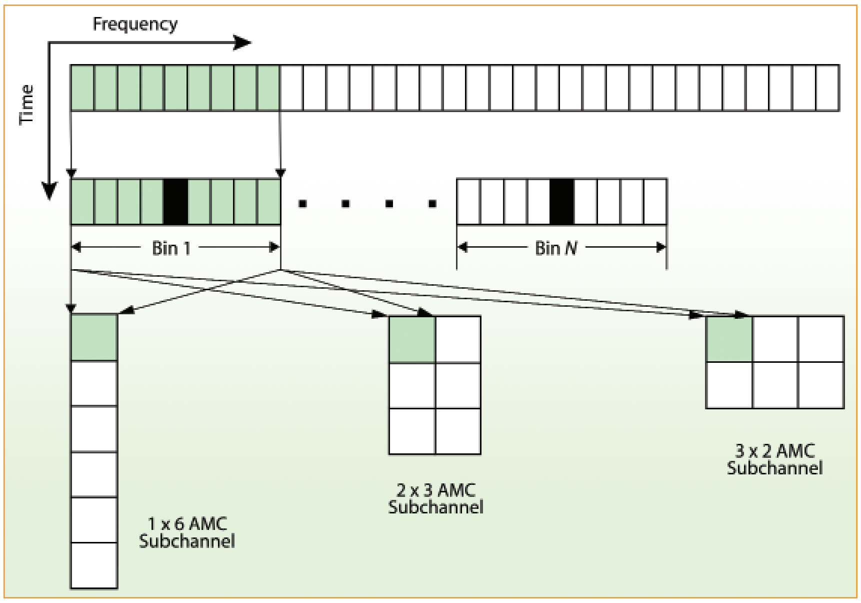


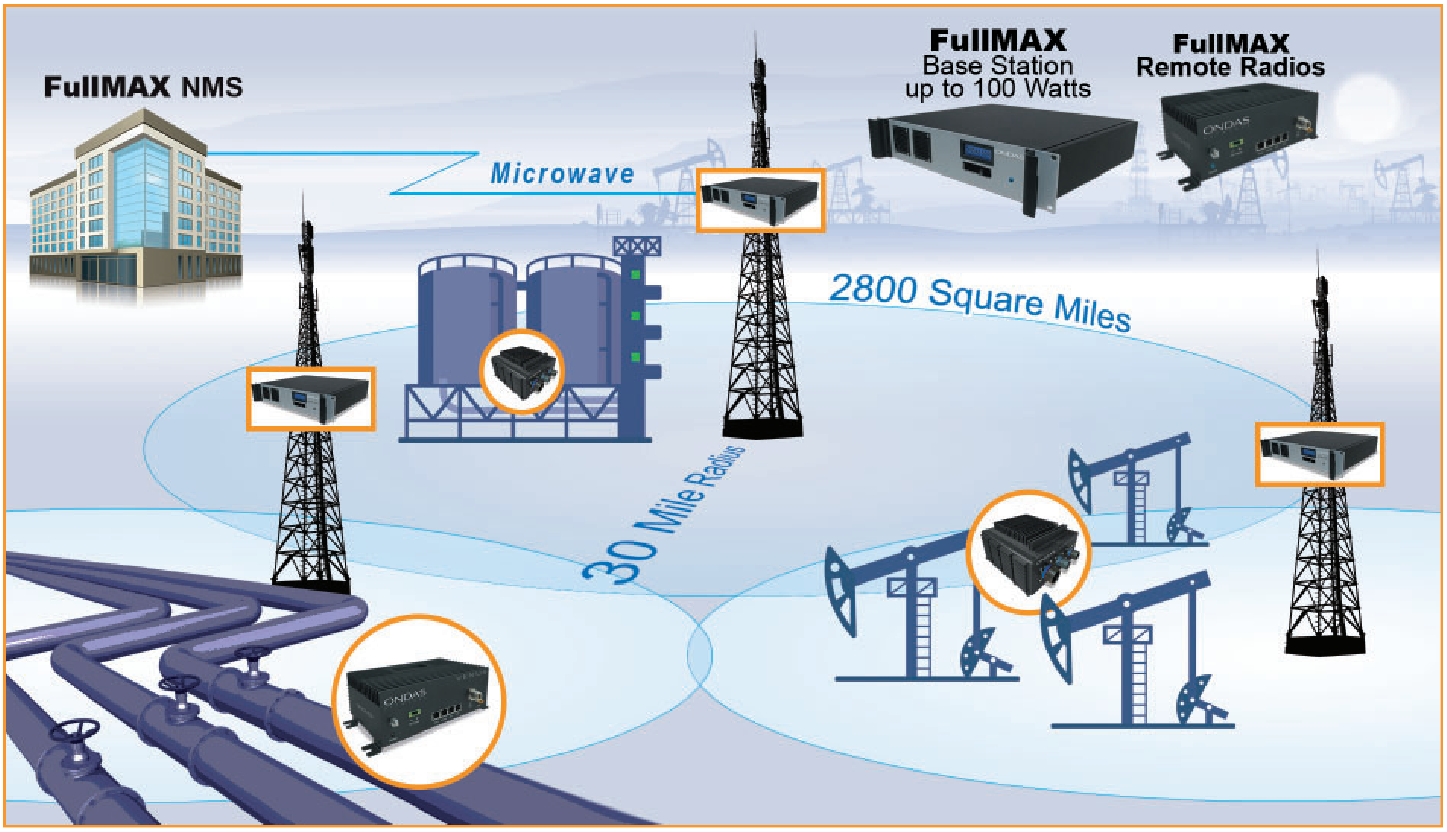
Figure 3

In order to further reduce overhead, the DL MAP Cyclic Redundancy Check (CRC) was reduced from 32 bits to 8 bits and uses non-rectangular DL bursts to reduce wastage. Reduction of Packet Data Unit (PDU) overhead with small of Service Data Unit (SDU)s belonging to different service flows is allowed in IEEE 802.16s whereas it is not allowed in IEEE 802.16. On the uplink side, the MAP CRC is reduced from 32 to 8 bits. Because of the greater efficiency of Band AMC is used in IEEE 802.16s and PUSC is not. PUSC, however is allowed in IEEE 802.16.

What does this mean and how is this beneficial for mission critical applications?

As more data is required and more intelligence and processing for mission critical networks moves to the edge, capability of communications networks need to increase. This newly developed, highly efficient, narrower channel standard enables critical industries to deploy mission critical applications on private, licensed, secure wireless communications networks.

These communications networks can be used to manage a variety of mission critical applications, including wide area intelligent networks for smart grids, smart pipes, smart fields and any other mission critical network that needs internet protocol connectivity. These networks can provide real-time monitoring and information on the condition of assets, identifying and minimizing potential equipment failure from wear and tear or communication disruptions. As a result, operators are able to improve productivity in the field and reduce waste and machine wear and tear.



> *"As we look to the next generation of 1.4 GHz gear, the prospects of having an industry standard as an option are exciting, particularly when that new standard infuses a lot of new technology that allows for more efficient use of the spectrum,"* says Fredrick Smith, an Infrastructure Architect at Chevron.

The Better Choice for Safety and Resilience

The private, licensed, standard technology approach to network operation offers greater control over the availability and security of critical services and provides a foundation for the new, smart applications that today's critical infrastructure entities demand.

Perhaps even more important, though, is the fact that private licensed networks let critical infrastructure entities' mission-critical services deliver the benefits that millions of people rely on every day. After all, it's one thing for people to go without their smartphones or media centers for a few hours, but it's another thing entirely if power isn't restored, furnaces don't function, or clean water isn't available. By running mission-critical services on private licensed networks, communities can remain safer and more resilient in difficult times.

Kathy Nelson is the Director of Technical Product Marketing and Industry Relations at Ondas Networks, formerly Full Spectrum, where she leads Ondas' industry relations and product marketing across all industrial verticals including electric utilities, oil & gas, water, transportation and government. Ms. Nelson has 25 years of experience as a telecommunications engineer in the utility industry focusing primarily on SCADA and Land Mobile Radio telecommunications systems. Ms. Nelson served as UTC Chairwoman of the Board in 2017 – 2018, ending a tenure of nearly ten years on UTC's board of directors, four of those years as Public Policy Division Chair. Ms. Nelson is a strong advocate for private networks for utilities and other critical infrastructure entities. Ms. Nelson has a B.S. in Electrical Engineering from North Dakota State University and is a registered professional engineering in Minnesota, Wisconsin, and North Dakota.

Ondas Networks Inc. (formerly Full Spectrum Inc.) is a wireless networking company that designs and manufactures its multi-patented, Software Defined Radio (SDR) platform for Mission Critical IoT (MC-IoT) applications. Ondas' markets include Electric Utilities, Oil & Gas, Water, Rail, Transportation and Government. Customers use our SDR technology to deploy their own private licensed broadband wireless networks. Ondas Networks provides a frequency agnostic radio platform from 70 MHz to 6 GHz and beyond. We also offer mission-critical entities the option of a managed network service. Ondas' SDR technology supports IEEE 802.16s, the new worldwide standard for private licensed wide area industrial networks. Our radios enable wide area intelligent networks for smart grids, smart pipes, smart fields and any other mission critical network that needs internet protocol connectivity. Ondas' technology supports secure wireless data communications using industry standards for AAA as well as customer selectable link-layer encryption up to AES 256.