Industrial Automation Wireless Networks Update – Ever More Relevant for CIP Communications

David Brandt, Paul Didier Bob Voss
Principal Engineer, Solution Architect, Distinguished Engineer
Rockwell Automation, Cisco, Panduit

Presented at the ODVA
2023 Industry Conference & 22nd Annual Meeting
October 18, 2023
El Vendrell, Spain

Abstract

Wireless is no longer just an extension of the Enterprise Wi-Fi. Industrial wireless use cases are increasing in industrial operations: AR/VR assistance for personnel, location services, highspeed SW downloads to products and mobile machinery and assets. The wireless technology choices are also growing: Wi-Fi, 5G/Private 5G, sensor networks, Bluetooth, ultra-wideband and other reliable wireless technologies. The technologies are making enhancements for industrial use cases. All offer opportunities to enhance safety, security, and efficiency. This session will explore the wireless options providing key considerations around Use Case, Spectrum, Distance, Reliability, Speed, Latency, Management and Total Cost of Ownership. Additionally, the session will consider how ODVA may be able to help users and vendors integrate wireless technologies for use in CIP communications.

Keywords

Wi-Fi, Private 5G, Industrial Wireless

Use Cases

Industrial Wireless technologies are ever improving and evermore utilized in industrial operations. The technology improvements are meeting more and more of the industrial requirements, including:

- High-Bandwidth and throughput to bandwidth intensive applications such as video streaming, Augmented/virtual reality and tele-remote support
- Low latency to support tighter Industrial Automation and Control applications, including CIP Safety.
- High-availability via improved interference avoidance, faster roaming and lower packet-loss rates

Key use cases where industrial wireless play key roles include:

- Smart devices – such as smart phones and tablets
- Automated Guided Vehicles – autonomous robots and vehicles moving product and parts around production facilities
- Surveillance Cameras – streaming video for surveillance and vision control
- Human Machine Interface – mobile HMIs keep operational personnel connected
- Remote Expert – integrated remote engineers and support for deployment and problem resolution
- Augmented Reality/Virtual Reality – mobile AR/VR headsets to improve personnel effectiveness
- Sensors, Actuators – wireless sensors and actuators where wired connectivity is challenging
- Wireless Tooling – More effectiveness and efficient tooling when not tethered
- Mobile Work-Cell – flexible, nomadic production equipment and assets
- Product Downloads – download Software and data to intelligent products.

Technologies – Current State

This section will provide an overview of key standard wireless technologies: Wi-Fi (a.k.a. IEEE 802.11) and Cellular 5G (managed by the 3GPP standards organization).

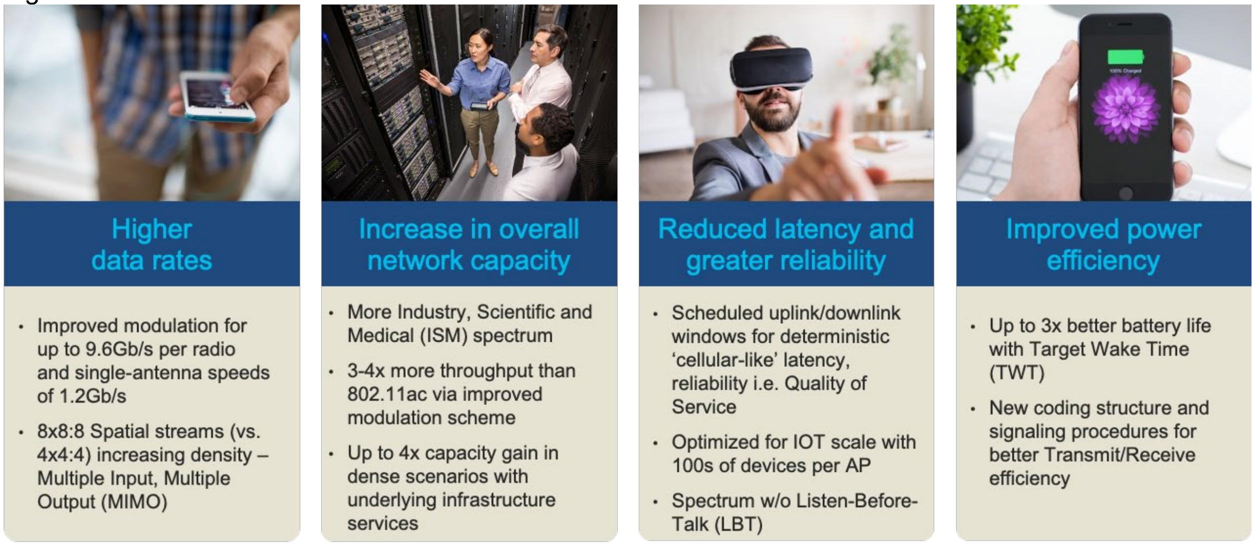
Wi-Fi – Current State

Currently, the most recent available Wi-Fi technology is based on Wi-Fi 6/6E technology. Wi-Fi 6 technology (IEEE 802.11ax) is currently shipping where much of the infrastructure is ready to support the additional spectrum allocation referred to as Wi-Fi 6E. As of the writing of this paper, Wi-Fi 6E is available in a number of countries, including the US, although only a limited set of devices support it yet. Specifically, low-power indoor (LPI) devices support 6E. Most industrial Wi-Fi 6 devices must disable support for 6E because they do not have integral antennas and/or have enclosures that could be used outdoors (even if they are intended to be used indoors, but must withstand washdown).

Wi-Fi 6/6E - Update

The following summarizes the key enhancements in Wi-Fi 6/6E:

Figure 1 – Wi-Fi 6/6E enhancements



Higher data rates

- Improved modulation for up to 9.6Gb/s per radio and single-antenna speeds of 1.2Gb/s
- 8x8:8 Spatial streams (vs. 4x4:4) increasing density – Multiple Input, Multiple Output (MIMO)

Increase in overall network capacity

- More Industry, Scientific and Medical (ISM) spectrum
- 3-4x more throughput than 802.11ac via improved modulation scheme
- Up to 4x capacity gain in dense scenarios with underlying infrastructure services

Reduced latency and greater reliability

- Scheduled uplink/downlink windows for deterministic 'cellular-like' latency, reliability i.e. Quality of Service
- Optimized for IOT scale with 100s of devices per AP
- Spectrum w/o Listen-Before-Talk (LBT)

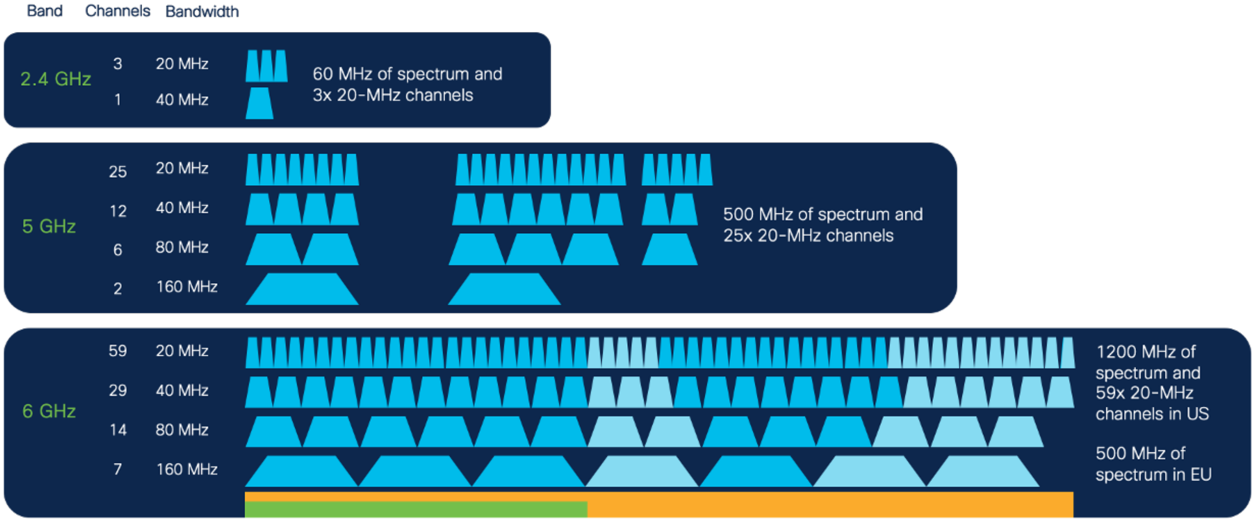
Improved power efficiency

- Up to 3x better battery life with Target Wake Time (TWT)
- New coding structure and signaling procedures for better Transmit/Receive efficiency

For more information see: https://www.cisco.com/c/en/us/products/collateral/wireless/white-paper-c11-740788.html.

In addition to these features, Wi-Fi 6E grants additional access to 1200 MHz of relatively clean spectrum in the newly-opened unlicensed 6 GHz band that significantly increases the available spectrum (roughly @200% increase in the US, @100% increase in EU) , improving data rates, lowering interference and supporting more applications.

Figure 2 – Wi-Fi 6/6E available spectrum diagram

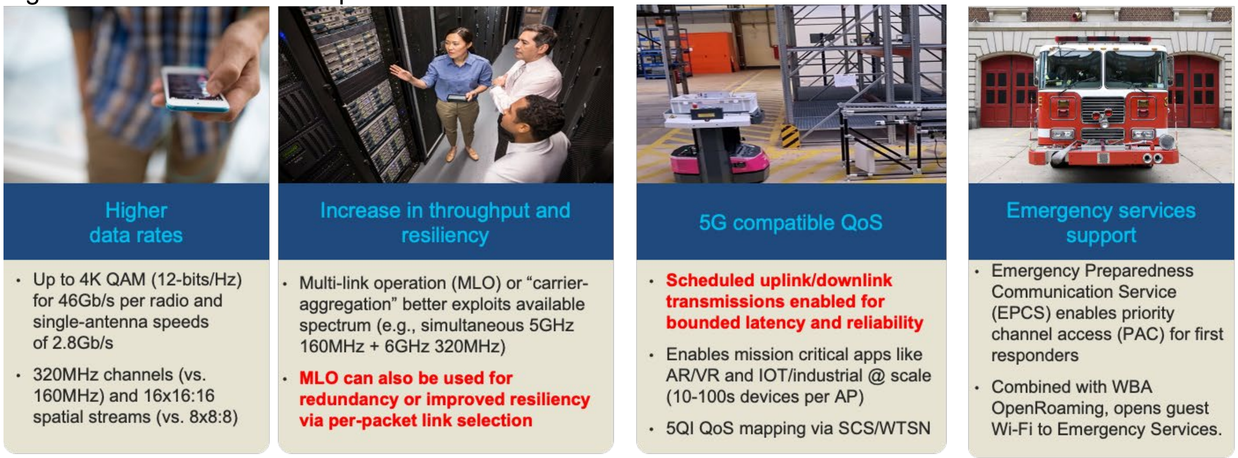


Wi-Fi 7 - Update

As of the writing of this paper, the Wi-Fi Alliance is working on Wi-Fi 7 and is expected to be ratified in 2024. The IEEE IEEE is still working on IEEE 802.11be.

Wi-Fi 7 continues the improvements in resiliency, bandwidth and denser deployments of devices. Wi-Fi 7 currently includes enhancements for industrial applications around resiliency and priority.

Figure 3 - Enhancements expected in Wi-Fi 7



Higher data rates

- Up to 4K QAM (12-bits/Hz) for 46Gb/s per radio and single-antenna speeds of 2.8Gb/s
- 320MHz channels (vs. 160MHz) and 16x16:16 spatial streams (vs. 8x8:8)

Increase in throughput and resiliency

- Multi-link operation (MLO) or “carrier-aggregation” better exploits available spectrum (e.g., simultaneous 5GHz 160MHz + 6GHz 320MHz)
- **MLO can also be used for redundancy or improved resiliency via per-packet link selection**

5G compatible QoS

- **Scheduled uplink/downlink transmissions enabled for bounded latency and reliability**
- Enables mission critical apps like AR/VR and IOT/industrial @ scale (10-100s devices per AP)
- 5QI QoS mapping via SCS/WTSN

Emergency services support

- Emergency Preparedness Communication Service (EPCS) enables priority channel access (PAC) for first responders
- Combined with WBA OpenRoaming, opens guest Wi-Fi to Emergency Services.

For more information see: https://wballiance.com/road-to-wi-fi-7/

5G - Update

3GPP is the organization that creates 5G standards. The standards cover the complete 5G architecture – UE (User Equipment) end-devices, RAN (Radio-Access Network) and Mobile Packet Core. The standards are delivered in releases. Here are some considerations about 3GPP standards:

- Feature release for telecom providers remains 5G vendor priority
- There is *significant lag* between 3GPP specification release and commercial availability (particularly of "industrial" features not needed by telecom)
  - Release 16 completed in 2020
  - No infrastructure supporting Release 16 features (e.g., time sync support) until end of 2023 / early 2024
- 5G modems more closely follow 3GPP releases
  - Some updates are via firmware, but many require new silicon
  - More likely to see 5G modems advertised as "Release 16-compliant"
- Infrastructure adds features from future 3GPP releases *incrementally*
  - Typically via software update
  - Follows vendor internal roadmaps
  - Features from lower-numbered 3GPP releases are generally added first
  - Some features (e.g., localization) may require special hardware support in basebands
- Even though the standards are released groups, UE, RAN and MPC vendors can pick and choose what features and functions to deliver.

Below is a table of features relevant to industrial communications and the release that they were included.

Table 1: 5G Feature Release

Feature	Release 15 (2018/2019)	Release 16 (2020)	Release 17 (2022)
URLLC (Ultra-Reliable Low-Latency Communication)	All basic features (for IMT-2020 compliance)	Adds redundant transmissions, QoS monitoring	No new features
Ethernet PDU	No	Yes	Yes
Time Sync Support	None	IEEE 802.1AS gPTP only	IEEE 1588 PTP (CIP Sync)
Positioning	< 50 m	< 3 m	< 1 m
Network Slicing	Basic slicing features (similar to VLAN)	Adds network slice-based authentication (NSSAA)	Adds slice groups (NSSRG), enhanced RAN support
IIoT	Relies on LTE	5G core support for NB-IoT	NR RedCap (replacement for LTE Cat 1)

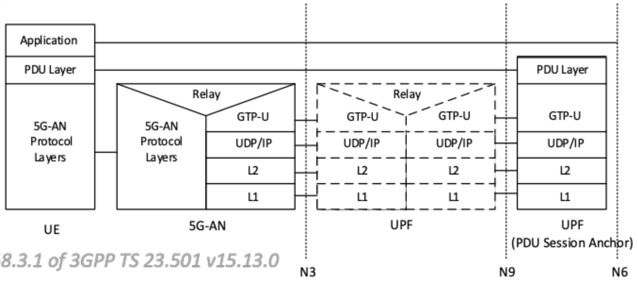
5G and CIP

The good news is that 5G natively carries EtherNet/IP traffic, as it is based on TCP/IP. A few other notes about 5G and industrial networks:

- Support for Ethernet frames was added in 3GPP Release 16, specifically Ethernet protocol data unit (PDU) sessions
  - Most existing 5G equipment on the market today does not support Ethernet PDU
- EtherNet/IP is carried by TCP and UDP, so **EtherNet/IP can run on any 5G!**
  - Most industrial protocols need special tunneling (e.g., VXLAN) or Ethernet PDU support
- Special support is needed for:
  - Time synchronization (motion)
  - Multiple devices behind a UE
- 5G typically requires UEs to request a schedule to send data uplink which may disrupt low-latency communications, which can be mitigated via Grant-Free Scheduling
- Along these lines, typical 5G systems are configured to prioritize downlink data (e.g., video streaming) over uplink, whereas industrial communication creates nearly symmetric uplink and downlink traffic. This can be mitigated with 1:1 slot ratios.

Each of the above are covered below.

Figure 4 – 3GPP 5G support stack in Releases 15 through 17.



§8.3.1 of 3GPP TS 23.501 v15.13.0

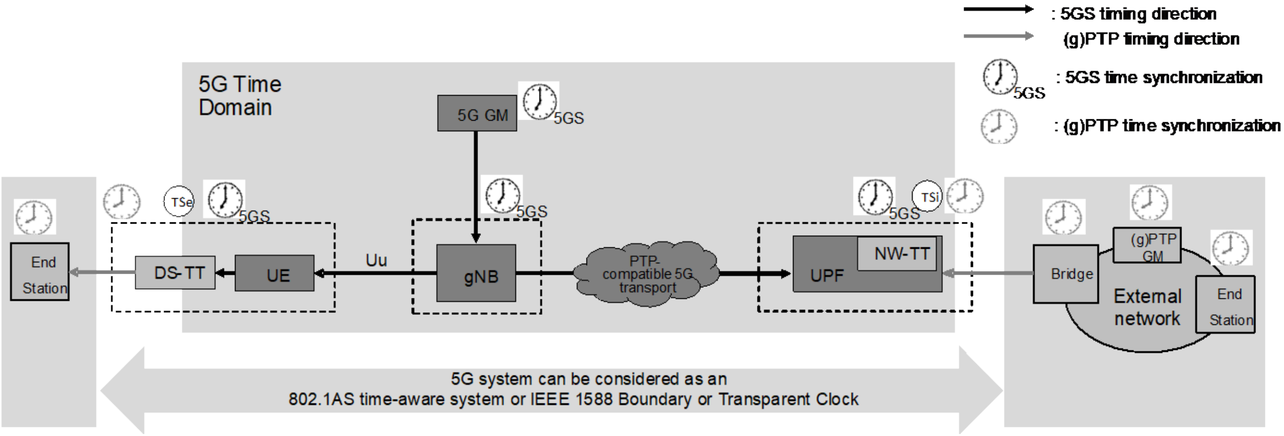
- PDU layer: PDU = protocol data unit. This layer corresponds to the PDU carried between the user equipment (UE) and the data network (DN) over the PDU Session.
  - When the PDU Session Type is IPv4 or IPv6 or IPv4v6, it corresponds to IPv4 packets or IPv6 packets or both of them.
  - When the PDU Session Type is Ethernet, it corresponds to Ethernet frames.
- 5G-AN: 5G access network
- GTP-U: GPRS Tunnelling Protocol for the user plane

5G and Precision Time Protocol (PTP)

5G base stations must be synchronized to a GPS-derived clock to avoid interference with neighboring cells. GPS time is distributed to UEs via a system information block (SIB), specifically SIB 9 for standalone networks and SIB 16 for non-standalone networks that rely on LTE. The distribution of GPS clock data, combined with a method such as timing advance (TA) to correct for signal time of flight, allows all elements of the 5G system to remain synchronized.

3GPP has added features to support industrial PTP protocols (IEEE 802.1AS gPTP in Release 16 and standard PTP / CIP Sync in Release 17) as depicted below.

Figure 5 – 3GPP PTP support as of Release 17


: 5GS timing direction
(g)PTP timing direction
: 5GS time synchronization
5GS
: (g)PTP time synchronization
5G Time Domain
5G GM
5GS
TSe
5GS
5GS
5GS
TSi
End Station
DS-TT
UE
Uu
gNB
PTP-compatible 5G transport
UPF
NW-TT
Bridge
(g)PTP GM
External network
End Station
5G system can be considered as an
802.1AS time-aware system or IEEE 1588 Boundary or Transparent Clock

While details may be vendor-specific, the basic mechanism to support PTP works as follows:

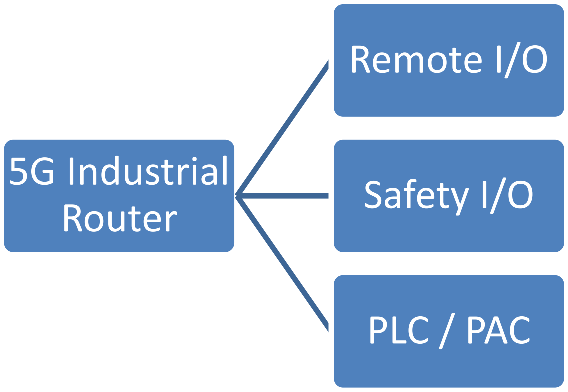
- A 5G system (5GS) supporting Release 16+ will correct residence time via **TSN Translators (TTs)**
- There are two types of TTs: device-side TT (DS-TT; TSN master), and network-side TT (NW-TT)
- Ingress traffic into the 5G system is timestamped; on egress, the TTs subtract the current time from the ingress timestamp to compute residence time, which is added to a correction field
- In essence, the 5G system acts like a single switch implementing a PTP transparent clock
- The PTP Grandmaster may be internal or external to the 5G system; at most one NW-TT can be a TSN slave

Support for Multiple Devices Behind Single UE

Cellular was originally designed for phone and eventually smart phone use, where all traffic was to/from a single end device. As such, it is still developing "bridging" functions similar to Work-Group Bridges found in Wi-Fi networks.

Figure 6 – Industrial Use Case – multiple devices behind a UE connection

https://www.industrialnetworking.com/pdf/HMS-anybus-wireless-bolt.pdf



A few points about support for multiple devices behind a single 5G user equipment (UE):

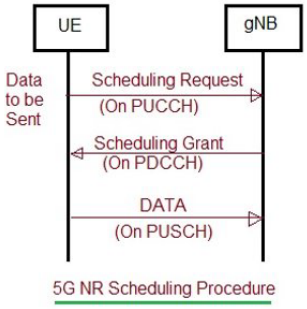
- It is advantageous if a single UE can support multiple automation devices
  - 5G UEs (modules or routers) are expensive
  - Many automation devices are located in metal cabinets that block RF, so it often doesn't make sense to integrate 5G radios in these devices
- Tunneling / VXLAN can be used to support multiple devices behind a single UE
  - May need an "extra box" behind UE to act as a tunnel endpoint

    - Some UEs have tunneling support or can run containers (e.g., with OpenVPN)
- 5G also supports “framed routing” (3GPP TS 23.501 §5.6.14)
    - Originally developed as part of RADIUS (RFC 2865)
    - 5G vendors may call this feature “Routing Behind Mobile Station” or “Routing Behind UE”, but it is typically implemented using framed routing
- Example of how framed routing works:
    - Allocate small subnet (/27 or smaller) behind UE
    - This subnet is associated with a user name and password, stored in the 5G core
    - When a 5G UE initially connects (attaches) to a network, it authenticates using SIM credentials (primary authentication)
    - A 5G UE may also authenticate to a specific data network using EAP (typically via PAP or CHAP) with a user name and password; this is called secondary authentication
    - When the UE performs secondary authentication, a route is created in the core to the subnet associated with the secondary authentication credentials

Grant-Free Scheduling

5G UEs typically must request permission (a grant) to send uplink data. This adds delay and increases inter-packet delay variation (colloquially called jitter), both of which are problematic for CIP protocols. The added delay from this scheduling procedure also generally precludes very low-latency applications.

Figure 7 – 5G Scheduling Procedure



https://www.rfwireless-world.com/5G/5G-NR-Scheduling-Request-Procedure.html

Grant-free scheduling (also called transmission without grant, TWG) avoids the added delay and packet delay variation caused by uplink scheduling. It works as follows:

- The 5G base station reserves resources for uplink for each UE; the UE can transmit on these reserved uplink resources at any time
- The periodicity of the grant-free uplink resources is adjustable; ideally this period would be the same as the CIP packet interval, but synchronization may not be possible
- In general, grant-free schedule reduces latency at the expense of throughput since reserved uplink resources may not be used

1:1 Slot Ratios

EtherNet/IP typically has approximately equal traffic in each direction. Typical cellular use cases are downlink heavy (e.g., streaming video). In fact, most 5G equipment initially only supported a few fixed downlink to uplink ratios with at best a 4:1 downlink to uplink ratio.

This downlink uplink asymmetry creates several problems for EtherNet/IP traffic. First, it creates a bottleneck in the uplink direction, which may cause extra queuing delay for CIP connections in this direction. A second, less-obvious effect is that it also increases the time required for physical-layer retries when the uplink slots are fewer and farther apart. This adds delay and increases inter-packet delay variation.

Therefore, usage of slot ratios as close to 1:1 as possible is advantageous for EtherNet/IP traffic. A few points about 1:1 slot ratios:

- 5G divides resources in time into frames, subframes, slots, then symbols
  - Individual symbols can be allocated for downlink, uplink, or flexible
- With time-division duplexing, slots (each containing 14 symbols) are typically allocated as downlink (D), uplink (U), or special (S; mix of symbols)
    - It takes time to switch radios between transmitting and receiving, so blocks of downlink or uplinks slots allows higher throughput
- Slot patterns sets ratio of uplink to downlink traffic, as well as retry delay
  - 5G base stations and UEs initially offered only a few fixed slot ratios
  - Closest to symmetric was 4:1 downlink to uplink, such as DDDSUUDDDD
  - Current 5G equipment may offer nearly 1:1 slot ratio, e.g., DDSUU
- Even with an exactly 1:1 slot ratio, downlink throughput is typically better due to MCS differences, such as higher-order QAM in downlink

Key Industrial Considerations

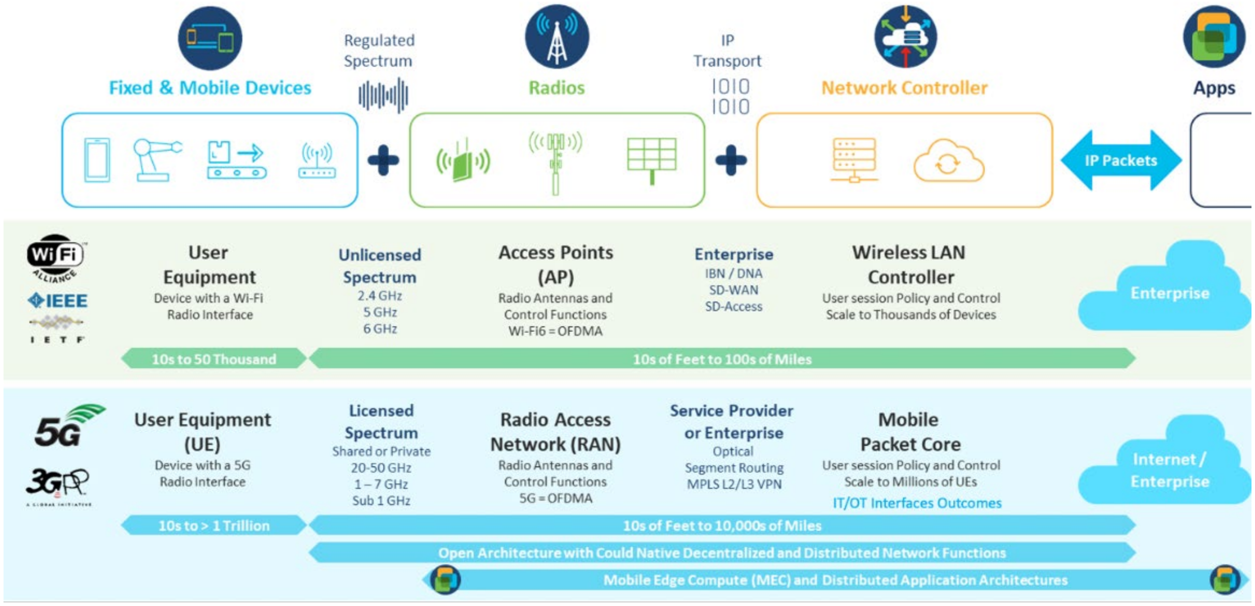
The key considerations when choosing wireless communications include:

1. What are the devices to connect? Cranes, AGVs, tablets, sensors etc.
2. What are the applications requirements? Latency, reliability, nomadic/stationary, etc.
3. What are the deployment Scenarios? Regional regulations, spectrum, indoor/outdoor, access/backhaul
4. What are the potential technology options?
   - **Wired:** Ethernet, serial, DSL
   - **Wireless:** Wi-Fi and Ultra-Reliable Wireless Backhaul, 5G Cellular, Wi-SUN, LoRaWAN,
   - **Spectrum:** Unlicensed, Licensed: Private, Public, Shared
5. What are the CapEx and OpEx Implication?

Wireless Architectures

Below is a depiction of wireless architectures for WiFi and 5G:

Figure 7 – Wi-Fi and 5G architectures


Fixed & Mobile Devices
Regulated Spectrum
Radios
IP Transport
1010
1010
Network Controller
Apps
IP Packets
User Equipment
Device with a Wi-Fi Radio Interface
Unlicensed Spectrum
2.4 GHz
5 GHz
6 GHz
Access Points (AP)
Radio Antennas and Control Functions
WI-FI6 = OFDMA
Enterprise
IBN / DNA
SD-WAN
SD-Access
Wireless LAN Controller
User session Policy and Control
Scale to Thousands of Devices
Enterprise
10s to 50 Thousand
10s of Feet to 100s of Miles
User Equipment (UE)
Device with a 5G Radio Interface
Licensed Spectrum
Shared or Private
20-50 GHz
1 – 7 GHz
Sub 1 GHz
Radio Access Network (RAN)
Radio Antennas and Control Functions
5G = OFDMA
Service Provider or Enterprise
Optical
Segment Routing
MPLS L2/L3 VPN
Mobile Packet Core
User session Policy and Control
Scale to Millions of UEs
IT/OT Interfaces Outcomes
Internet / Enterprise
10s to > 1 Trillion
10s of Feet to 10,000s of Miles
Open Architecture with Could Native Decentralized and Distributed Network Functions
Mobile Edge Compute (MEC) and Distributed Application Architectures

ODVA Impact

As stated above, CIP and EIP are already well suited for both Wi-Fi and 5G communications with a few noted caveats, especially around time synchronization and motion applications. Both technologies are designing improvements for industrial control applications.

****

The ideas, opinions, and recommendations expressed herein are intended to describe concepts of the author(s) for the possible use of ODVA technologies and do not reflect the ideas, opinions, and recommendation of ODVA per se. Because ODVA technologies may be applied in many diverse situations and in conjunction with products and systems from multiple vendors, the reader and those responsible for specifying ODVA networks must determine for themselves the suitability and the suitability of ideas, opinions, and recommendations expressed herein for intended use. Copyright ©2023 ODVA, Inc. All rights reserved. For permission to reproduce excerpts of this material, with appropriate attribution to the author(s), please contact ODVA on: TEL +1 734-975-8840 FAX +1 734-922-0027 EMAIL odva@odva.org WEB www.odva.org. CIP, Common Industrial Protocol, CIP Energy, CIP Motion, CIP Safety, CIP Sync, CIP Security, CompoNet, ControlNet, DeviceNet, and EtherNet/IP are trademarks of ODVA, Inc. All other trademarks are property of their respective owners.