Liaison Statement to IEEE

Document Title	Liaison Statement to IEEE 802.11 – WBA Industrial IoT Deliverable	Page 1 of 1

Date	11th January 2022	**Meeting Time**	Tuesday 8am PT, 4pm GMT
WG / Project	WBA Wi-Fi 6/6E for Industrial IoT		
To	IEEE		
Project chaired by	Malcolm Smith (Cisco), Bryan Wills (Deutsche Telekom)		
Topic	New Deliverable – Enabling Wi-Fi determinism in an IOT world		

Dear IEEE 802.11 Chair, Dorothy Stanley,

The WBA Members have formed and approved a technical activity during 2021 called Wi-Fi 6/6E for Industrial IoT, focused on understanding and recommending latest Wi-Fi technology to the IIoT use cases and requirements.

The group has recently finished a whitepaper that addresses:

- Industrial IoT market drivers
- Emerging IIoT Use Cases
- Evolution of Wi-Fi 6/6E technology
- RF and Network Deployment Guidelines

In light of this, the group leadership would like to formally liaise with the IEEE the final draft, and confidential version of the document that will be published later to the WBA Members end-January 2022.

The program meetings will carry on now with live trials, where the technology is tested and applied to real practical scenarios of industrial IoT.

Specific requests:

- WBA invites IEEE members to provide opportune feedback on the document, as well as any other areas that WBA should also consider in the industrial IoT domain
- WBA invites IEEE members with a technical or business interest in this sector to be involved in the ongoing trials that will take place during 2022
- WBA would like to present this work at the upcoming IEEE plenary

Yours sincerely,
The WBA Wi-Fi 6/6E for Industrial IoT Chairs

Upcoming WBA events:

- Wireless Global Congress & Working Sessions Dubai 25-27 January 2022
- For more information, consult https://www.wirelessglobalcongress.com/

[Confidential for IEEE only]

Wi-Fi 6/6E for Industrial IOT

Enabling Wi-Fi determinism in an IOT world

Source: Wireless Broadband Alliance
Author(s): WBA Wi-Fi 6/6E for IIOT
Issue date: January 2022
Version: 1.0.0
Document status: Draft

WIRELESS BROADBAND ALLIANCE
DRIVING NEXT WIRELESS EXPERIENCE

ABOUT THE WIRELESS BROADBAND ALLIANCE

Wireless Broadband Alliance (WBA) is the global organization that connects people with the latest Wi-Fi initiatives. Founded in 2003, the vision of the Wireless Broadband Alliance (WBA) is to drive seamless, interoperable service experiences via Wi-Fi within the global wireless ecosystem. WBA's mission is to enable collaboration between service providers, technology companies, cities, regulators and organizations to achieve that vision. WBA's membership is comprised of major operators, identity providers and leading technology companies across the Wi-Fi ecosystem with the shared vision.

WBA undertakes programs and activities to address business and technical issues, as well as opportunities, for member companies. WBA work areas include standards development, industry guidelines, trials, certification and advocacy. Its key programs include NextGen Wi-Fi, OpenRoaming, 5G, IoT, Testing & Interoperability and Policy & Regulatory Affairs, with member-led Work Groups dedicated to resolving standards and technical issues to promote end-to-end services and accelerate business opportunities.

The WBA Board includes Airties, AT&T, Boingo Wireless, Broadcom, BT, Cisco Systems, Comcast, Deutsche Telekom AG, Google, Intel and Viasat. For the complete list of current WBA members, **click here**.

Follow Wireless Broadband Alliance:

www.twitter.com/wballiance

http://www.facebook.com/WirelessBroadbandAlliance

https://www.linkedin.com/company/wireless-broadband-alliance

CONFIDENTIALITY

Privileged/confidential information may be contained in this document and any files attached in it ('WBA Documentation').

Only WBA member companies who have signed the new WBA IPR Policy (Located at: **WBA Extranet** and are the intended recipient are entitled to receive, review or comment on this WBA Documentation.

If you are not the intended recipient (or have received this WBA Documentation in error), please notify the sender and WBA (**pmo@wballiance.com**) immediately and delete this WBA Documentation. Any unauthorized copying, disclosure, use or distribution of this WBA Documentation is strictly forbidden.

UNDERTAKINGS AND LIMITATION OF LIABILITY

This Document and all the information contained in this Document is provided on an 'as is' basis without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for particular purpose, or non-infringement.

In addition, the WBA (and all other organizations who may have contributed to this document) makes no representations or warranties about the accuracy, completeness, or suitability for any purpose of the information. The information may contain technical inaccuracies or typographical errors. All liabilities of the WBA (and all other organizations who may have contributed to this document) howsoever arising for any such inaccuracies, errors, incompleteness, suitability, merchantability, fitness, and non-infringement are expressly excluded to the fullest extent permitted by law. None of the contributors make any representation or offer to license any of their intellectual property rights to the other, or to any third party. Nothing in this information or communication shall be relied on by any recipient.

The WBA also disclaims any responsibility for identifying the existence of or for evaluating the applicability of any claimed copyrights, patents, patent applications, or other intellectual property rights, and will take no position on the validity or scope of any such rights. The WBA takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any effort to identify any such rights.

Neither the WBA nor any of the other organizations who may have contributed to this document will be liable for loss or damage arising out of or in connection with the use of this information. This is a comprehensive limitation of liability that applies to all damages of any kind, including (without limitation) compensatory, direct, indirect, or consequential damages, loss of data, income or profit, loss of or damage to property and claims of third parties.

CONTENTS

1 Wireless IIOT market 3

1.1 Scope of Industrial IoT for this Whitepaper 3

1.2 Relevant market drivers 3

1.2.1 Improve quality 3

1.2.2 Improve yield 4

1.2.3 Improve safety 4

1.2.4 Improve security 5

1.2.5 Reduce downtime 5

1.2.6 Reduce cost of goods 6

1.3 Emerging IIoT use cases 7

1.3.1 AMR/AGV 8

1.3.2 Sensors 11

1.3.3 Safety controls 13

1.3.4 Video-AMR Fusion 14

1.3.5 AR/VR/XR 17

1.3.6 Industrial automotive 18

1.3.7 Wireless Time-sensitive-networking (WTSN) 20

Wi-Fi location-based services 23

1.4 Security considerations 24

2 Wi-Fi 6/6E 27

2.1 Evolution to determinism (OFDMA) 27

2.2 Wi-Fi 6/6E MU-MIMO 28

2.3 Power savings 29

2.4 BSS Color & spatial reuse (SR) 30

2.5 Quality-of-Service (QoS) architecture 32

2.6 Wi-Fi security 33

3 RF/network Deployment guidelines 34

3.1 Factory/Warehouse/Logistics 34

3.2 Automotive 35

3.3 Wi-Fi TSN 37

FIGURES

Figure 1 WiFi6/6E IIOT use-cases 7
Figure 2 AMR/AGV 8
Figure 3 AMR movement KPIs 9
Figure 4 Sensors 11
Figure 5 Safety controls 13
Figure 6 Video-AMR fusion 14
Figure 7 AMR Video Fusion process 15
Figure 8 AR/VR/MR 17
Figure 9 Wireless TSN Architecture options 20
Figure 10 WTSN Architecture 22
Figure 11 IEC 62443-4-2 26
Figure 12 OFDMA 27
Figure 13 MU-MIMO 28
Figure 14 TWT 29
Figure 15 BSS Color 31
Figure 16 OBSS PD 32
Figure 17 Automotive coverage 36

1 Wireless IIOT market

1.1 Scope of Industrial IoT for this Whitepaper

This whitepaper examines Industrial IoT encompasses solutions that employed by multiple industries to understand and improve their economic value by connecting machines, materials, people, processes, products, and services to improve visibility and understanding, increase quality and efficiency and create greater value for their respective customers.

Typical industries employing IIoT include manufacturing industries, process industries (such as chemical and pharmaceutical but also oil and gas and mining industries) as well as food and agriculture industries. Moreover, logistics, health and retail environments are known to utilize Industrial IoT to improve business outcomes.

1.2 Relevant market drivers

At a very high level, those working in the production of goods and services are primarily concerned with the continuing ability to profitably provide a reliable and timely product to their customers. This is how production plays a part in getting, growing, and keeping customers. It is not surprising, therefore, that the traditional drivers for adoption of wireless industrial IoT is colored by a set of traditional drivers that center on their ability to enhance certain manufacturing practices that support this overall cause and that do not get in the way of any of the other practices supporting the same overall cause.

Smart manufacturing adoption is reliant upon systems that focus on interoperability, scalability, reusability, and security. Together, these attributes combine into what is typically referred to as resiliency. In the past, designing a resilient system with wireless networks was a major challenge. Dropping data from a sensor on a production line, as an example, could not be tolerated. Thanks to technological advances in wireless, wireless systems are now implemented in industrial environments that match the resilience of wired systems.

The following sections briefly introduce several relevant market drivers to be considered in the potential adoption of wireless systems in industrial applications.

1.2.1 Improve quality

Providing a consistently good product or service is of primary concern for most manufacturers. When a customer can depend on the manufacturer’s product, reputation increases as does customer loyalty.

Improvements in quality mark one of the top reasons industries is making a move to Industry 4.0, a transformation of traditional manufacturing and industrial practices with inclusion of the

latest smart technologies. Since retrofitting a plant with sensors and actuators is expensive, it is natural to consider Wi-Fi based devices for upgrades.

With more information about the process, one can improve the operations and improve quality. For instance, the steel industry is adopting cameras to monitor the precise thickness of products leaving rolling machines. With the additional information, adjustments can be made real time to ensure proper control of the resulting product.

1.2.2 Improve yield

Yield, more specifically known as first-pass yield or throughput yield, is the number of acceptable units divided by the total number of units produced. The ability to meet customer demand, then, is highly dependent on yield and becomes a primary driver for most industries.

With more information from sensors and monitors, one can employ new analytics to improve yields. Manual inspection can be replaced with AI-enhanced visual systems to reduce manufacturing errors and improve yield. Problems can be identified earlier in the process, lessening the cost of repair. Rework becomes less frequent and lessens the cost of producing the resulting goods.

It should be noted that if a company is stamping out inexpensive plastic toys, yield might be more of a concern than quality. In such a case, the top two drivers in this list may be reversed. However, for a pharmaceutical company, quality will be more important than yield since a poor-quality product could be detrimental to an individual's health.

1.2.3 Improve safety

Processes that include blades, high temperatures, high pressures, and robotics are just a few of the areas of greatest concern for the safety of the engineers and technicians in the facility.

Here, reliability and availability are paramount concerns for systems which protect life and limb. As a result, traditionally most safety systems are wired. However, there are cases in which the ease of installation of wireless systems can enhance monitoring processes for safety. For instance, wireless cameras might be used to alert operators of someone entering an unauthorized area. Locking mechanisms may be installed which use wireless means to unlock them and log their use.

Such monitoring systems can improve the overall safety of a plant. For timely action, they must not fail in notifying operators or in logging actions. As a result, it is common to see fail-safe systems in place which test the communications link periodically on such systems. The scheduling features of Wi-Fi 6/6E can greatly aide in this capacity.

1.2.4 Improve security

Security is a driver that takes a position just under improving quality, yield, and safety. Traditionally, security in an industrial plant has been focused on physical security, e.g., entry control. As a result, many plants have cameras, entry keypads, automated locks, and other controls to ensure only those with the proper authority have access to the facilities. The ease of installation of wireless systems for physical security is resulting in a growing use of Wi-Fi devices for such purposes.

Looking beyond the growing use of physical security, it must also be noted that cyber-attacks on industrial facilities are at an all-time high [Sec1]. As of the time of this whitepaper, there are 230,000 new malware infections detected every day [Sec2]. In April 2020, the Computer Emergency Response Team of India (CERT-In) reported a substantial increase in cyber-attacks on Virtual Private Networks (VPN) used by industry to communicate with employees at remote locations, just as many are working from home.

It is widely considered that most cyber-attacks are on wired systems. However, a third of all recorded attacks are from unknown origins [Sec3], so wireless attacks could be occurring, as well. Additionally, as wired security improves, one can expect that wireless attacks will increase.

Cyber-attacks can happen on any connectivity route and on any part of the industrial system. One of the most elusive types of attack on legacy wireless security is perpetrated by an individual who is near the industrial plant and passively sniffs or actively attacks Wi-Fi security exchanges – such as offline dictionary attacks on WPA2-Personal passwords, or rogue AP attacks on WPA2-Enterprise RADIUS credentials with client devices that do not perform proper network validation. Once captured, the perpetrator can mimic a client device (such as a sensor or actuator) and open a channel of communication with the network, appearing as a normal, connected edge device. Once a perpetrator is in the network, a great amount of damage can be done.

In addition, the industry will likely have simple IoT devices installed, like temperature sensors or limit switches, which have limited computing power and/or battery power. Such devices may require alternative security measures to fully integrate with a system employing Wi-Fi 6 or 6E utilizing WPA3.

1.2.5 Reduce downtime

Predictive maintenance has long been studied to reduce downtime of a production line by identifying problems that could eventually result in equipment failure. With early detection, repairs can be scheduled and made without disrupting the production flow.

Sensors deployed for such use include vibration sensors and acoustic sensors for bearing wear, differential pressure gauges for hydraulics, gas and humidity sensors for air quality, and temperature sensors to prevent overheating. These IIoT devices provide valuable data on the operating conditions of equipment in the processes. They can alert operators to conditions that suggest equipment inspection and possible removal and replacement during the next scheduled down time.

As more equipment is monitored, wiring becomes prohibitive. Industry is moving towards the inclusion of wireless technologies to lessen the cost of obtaining more information about their processes. In one recent case in the oil and gas industry, moving to a wireless installation resulted in a 75% cost reduction in installation [Ind1].

During the trial, speeds of 700 Mbps using 80 MHz channels were achieved and low latency applications, like video calling and video streaming, performed well with results below 6ms [Ind2].

1.2.6 Reduce cost of goods

With the growing cost of storage comes the need for more accurate control over inventory. Indoor global positioning systems (GPS) and radio frequency identification (RFID) tags offer means to locate parts and provide inventory remotely. Tracking personnel and equipment is done through Bluetooth Low Energy (BLE) and Ultra-Wide Band (UWB) technology. Mobile devices are useful in checking in deliveries and monitoring shipping. Some advanced manufacturing facilities automate the delivery of needed parts to production lines via pick-and-place robots and conveyors.

The entire process can be described as Work-in-Process (WIP) Acceleration. An average 2.5% savings in Cost of Goods has been reported by implementing processes that minimize excess inventory [Ind3]. These include inventory optimization, Manufacturing Execution Systems (MES), electronic Kanban (tracking systems often employing bar codes) and advanced supply chain planning. These systems are heavily dependent on timely information being available throughout the process, suggesting the addition of sensors and monitors for this purpose.

Supply chain optimization can also be enhanced by employing wireless systems. Already discussed are aspects that lower inventory holding costs, but there are many other aspects that impact supply chain management [Ind4]. Safety-stock can be prioritized based on electronic transfer of information on customer service requests. Advanced methods of cross-docking, merge-in-transit and vendor-managed inventory can be integrated into production schedules.

1.3 Emerging IIoT use cases

Ubiquitous connectivity is a key requirement for *Cyber Physical Systems* which provide the foundation for initiatives such as Industry 4.0 or Smart Factory. It enables the transition from a hierarchical architecture, typically consisting of 5 layers according to the *Purdue Model*, to such *Cyber Physical Systems* for industrial automation. A converged network, with Wi-Fi as an essential part of it, provides the communication platform. It allows reliable access to data, physically represented as sensors and actors, from anywhere, as well as data exchange between these devices but also between machines and people. Protocols such as OPC UA (especially OPC UA FX: *from the sensor to the cloud*) will be used to connect field devices with applications running in a cloud environment. Wi-Fi represents one important option to implement this. Wi-Fi is typically deployed in combination with other technologies such as Ethernet to implement the end-to-end connectivity needed. This link enables a more efficient production process based on visibility and enhanced decision making including the enablement of mass customization. In this context, Wi-Fi is especially important to allow more dynamic factory scenarios where cable-based connections are difficult to adapt.

While IIOT spans a myriad of applications, the focus of this whitepaper will be on the following emerging use-cases:

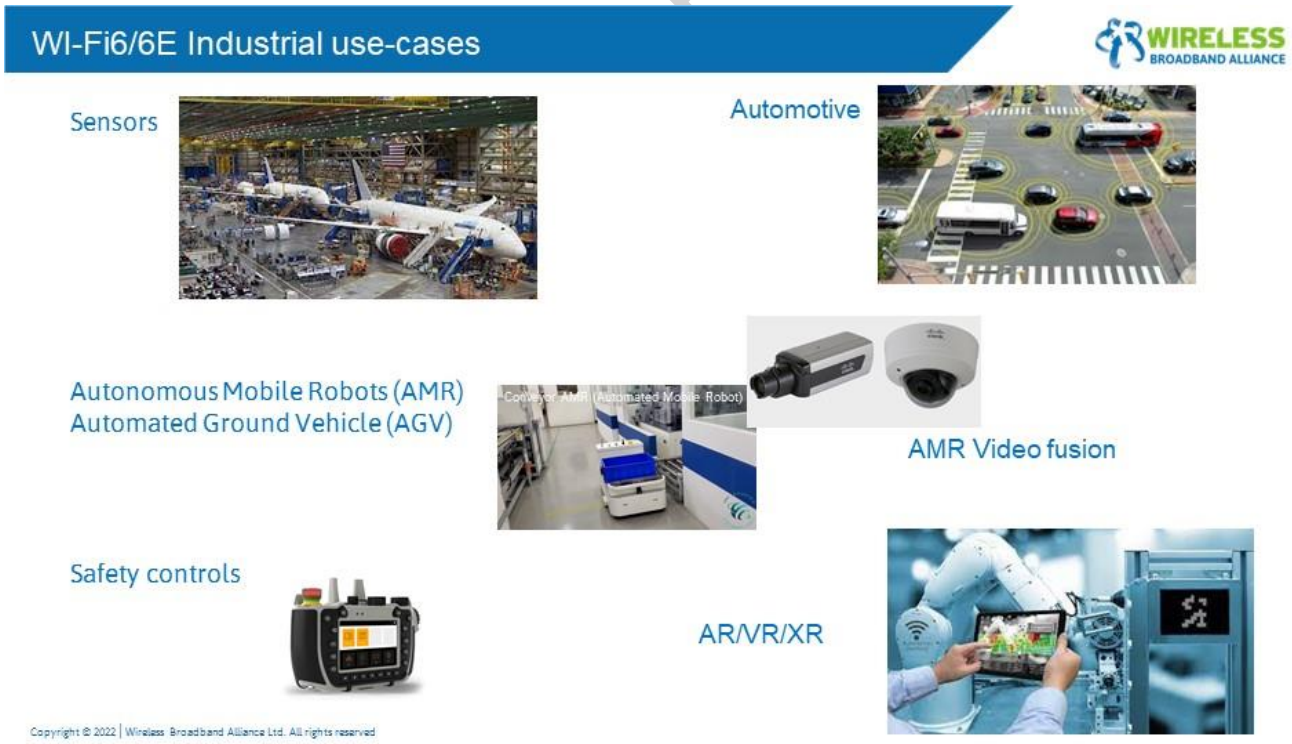


Figure 1 WiFi6/6E IIOT use-cases

1.3.1 AMR/AGV

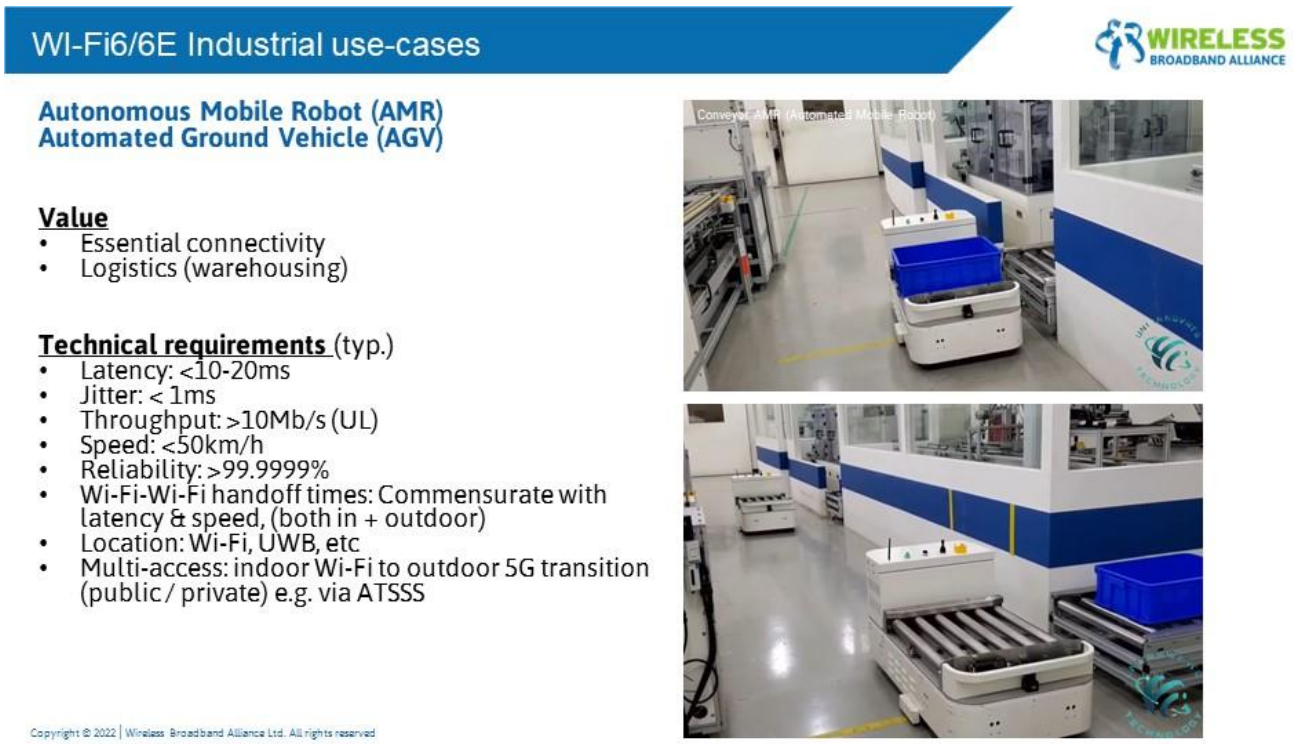


Figure 2 AMR/AGV

Manufacturing and process industries increasingly find themselves confronted with the conflicting requirements of providing ever more customized and individualized products while at the same time increasing production efficiency which historically requires producing larger batches.

The requirement is thus to industrialize customization. To do so requires the ability to flexibly and automatically link production processes (and assets) that add value in the overall production process, and to do so in a scalable manner.

While linking the information flows is a comparable straightforward task, the flexible linking of the physical logistics between processes and assets is still a nascent area. This is true for the classical view on inbound, outbound, and reverse logistics. This becomes even more obvious for the newer domain of intralogistics, most relevant for the flexibilization challenges observed.

Autonomous Mobile Robot (AMR) and Automated Ground Vehicle (AGV) platforms are utilized by factories, warehouses, and logistics businesses. Used to carry and deliver parts, products, and materials from a variety of sources and destinations be it inside a building or outside on a loading dock.

AGVs have a long tradition in increasing efficiency in various industries, including manufacturing and process industries and logistics hubs. Typically, most AGV implementations

are limited to pre-defined transportation tasks or routes. This static approach cannot deliver on the flexibility requirements modern production and logistics require, however.

On the other hand, AMRs are robots built with the capability to autonomously move and perform tasks. They come in many different shapes and sizes and with many different sets of capabilities as well as different types of navigation. As they are capable of fully autonomous mobility, they typically do not require modifications of the facilities to become operational. They can be up and running almost immediately. These robots will acquire a localization map, and many come with simultaneous location and mapping (SLAM) technology that allows them to continuously understand their operational environment.

Both types of robots are increasingly equipped with onboard sensors (radar, lidar, optical, etc.) to detect the platform's environment in real-time and using actuators (arms, conveyor, etc.) to assist in moving materials to/from the platform itself. In addition, some platforms may also have explicit onboard location/positioning technology based on either the Wi-Fi network, UWB or even outdoor GPS networks.

Depending on the degree of autonomy, some AMRs may only require cyclic task planning/guidance information from the control system. More advanced AMR set-ups might also place localization, navigation and even motion control onto a control system edge platform suitable for an entire fleet of AMRs. The relevance of latency for the transport scenario is best presented by observing the distance travelled at certain speeds during certain latency periods:

cm travelled during x ms at speed y km/h							
		x ms					
		1	5	10	20	50	100
y km/h	5	0.1	0.7	1.4	2.8	6.9	13.9
	10	0.3	1.4	2.8	5.6	13.9	27.8
	20	0.6	2.8	5.6	11.1	27.8	55.6
	30	0.8	4.2	8.3	16.7	41.7	83.3
	35	1.0	4.9	9.7	19.4	48.6	97.2

Figure 3 AMR movement KPIs

As an example, if the AMR is travelling at 20 kph and the two-way (round-trip) latency for reporting an event (e.g., position) and receiving a command from the system is 50ms, then the AMR would move ~1ft in that time. In some scenarios, this distance may be sufficient but in others a timelier response may be needed to affect route re-planning. For example, if 10ms 2-way latency was possible then the AMR would have only travelled 3" allowing for a much larger safety margin. To provide those kinds of latency assurances in dense AMR environments (i.e.,

with simultaneous upload of video, sensor data, position, etc.), scheduling enhancements such as UL-OFDMA and wireless TSN (WTSN) are key to enabling this technology.

AMR/AGV platforms contain many sensors to provide ranging/depth measurements to enable digital mapping or generation of a real-time digital-twin and 3D Vision. Sensor data including optical (stereo/3D), radar, LIDAR, are amongst a few. Images are typically reported periodically either in raw or compressed (processed) formats. When connected via Wi-Fi, this data can place a high load (e.g., 50-250Mb/s) on the uplink. AMR/AGVs are typically deployed in numbers at a given site so a single AP may need to support 10+ platforms simultaneously driving perhaps 2.5Gb/s throughput. Meeting these demands requires increased bandwidth, efficiency, and higher data-rates. Wi-Fi 6/6E provide up to 160MHz channel width for multi-Gbps, 1024 QAM data rates, and increased efficiency with UL/DL OFDMA. Wi-Fi 6E provides additional spectrum capacity and eliminates backyard compatibility and contention from legacy devices all together.

Finally, given AMR/AGV platforms can roam both inside and outside a facility (e.g., warehouse to port) it is important that the mobility between the indoor micro (e.g., Wi-Fi) and outdoor macro networks (e.g., 5G) operates in real-time and that latency bounds are preserved without noticeable packet loss. To achieve this outcome, the handoff process must be optimized at a system-level (AP, STA, gateways, etc) via mobility management techniques that leverage relevant standards (e.g., 802.11k/v/r).

1.3.2 Sensors

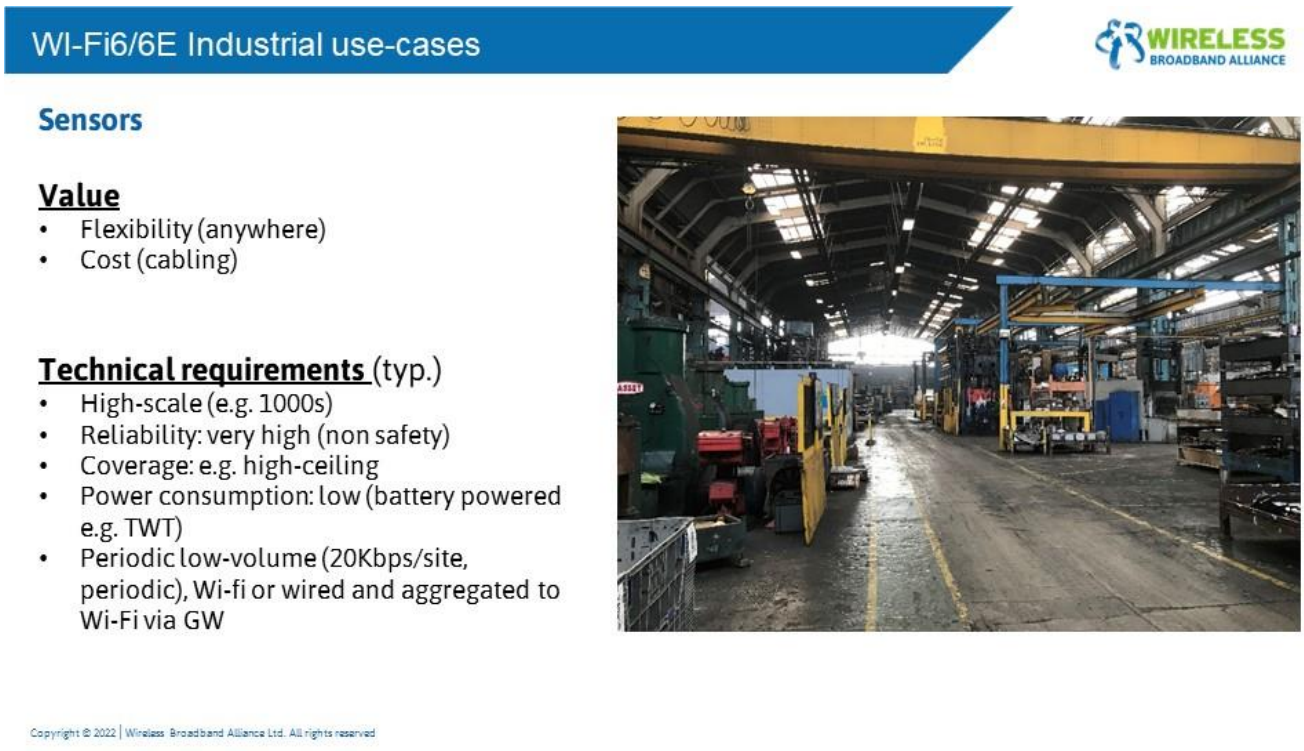


Figure 4 Sensors

Sensors will play a critical part in the industry 4.0 revolution. With the aim to data enable all key equipment in the manufacturing process, a typical site may require 20,000 sensors at high-density (e.g., 1 sensor / sq. ft).

The types of sensors used for applications such as process control and discrete manufacturing include vibration (e.g., rotating machines), temperature, rotation, volts/amps, pressure, valve state, relay(open/closed). Sensors will be connected to the network in a variety of ways:

- Hardwired standalone units
- Wi-Fi standalone units
- Groups of sensors connected to a central control unit which is then presented to the network via hardwire or Wi-Fi
- 5G connected sensors

In some applications, the sensors can be hard-wired (mains powered) and simply need to periodically report information to the control system which monitors/controls it's status. However, in many emerging applications either the cost of powering and connecting these devices is prohibitive (at scale) or the form-factor of the device permits only battery-power operation. It is these most challenging sensors we will consider here due to a) their stringent power consumption needs and b) large scale impacts on AP performance.

While the per-sensor traffic load is small, the aggregate load is significant. If we take a sensor with 10 data tags as an example. Each tag will be around 30 bytes of information. Let's assume a 1 second cycle, so 10 x 30bytes = 1.46kB of data per second. Scaling up to 20,000 sensor tags and we have: 20,000 x 30bytes = 586kB of data per second.

That's 35MB per minute and 16.9GB of data per 8-hour shift if all sensors are transmitting every second. In practice, not all sensors will require per second readings, some will only require transmit on change readings while others may need less than 1 second readings, however the impact on data transport and storage is significant.

The massive amounts of data collected by all the methods listed above will end up in a central repository such as an edge or cloud compute platform where the analytics and machine learning (ML) value of the system will be realised. Many systems will access the data to provide various views depending on the required application. For maintenance applications, the data can be used to predict machine performance degradation or failure enabling them to act before either situation is realised. Proactive maintenance results in consistent product quality and predictable machine uptime. This same predictive analysis data can be then relayed back operations staff via tablets and laptops via the Wi-Fi network. While latency is not critical for this application, it is important that all devices receiving the data receive the same readings at the same time. Inconsistent timings could lead to two engineers having different views of the same machine states. Wi-Fi will be key in delivering machine health information to operators and maintenance staff. Environmental sensors will utilise TWT to enable small battery powered devices in hard-to-reach areas. Data will be relayed back to the ERP system, enabling high levels of data capture against every manufacturing batch.

1.3.3 Safety controls

Figure 5 Safety controls

Safety control systems such as remote controls/HMI for industrial machines serve to allow the user direct control over the operation of what may be dangerous machinery. As such, responsiveness to controls, especially STOP buttons, needs to be near instantaneous (<1m) and as reliable as a wire (which effectively Wi-Fi replaces).

In accordance with its safety function, these controllers also may need to know the position (or range) with respect to the machine it controls to ensure the user has not “wandered off” and is no longer considered to be operating the machine. In such cases, the machine might initiate an auto shutdown, if the controller is >10m from it with an uncertainty of <1m. This requirement drives a new level of positioning accuracy that can be driven today with ranging techniques from Wi-Fi like FTM (802.11mc) and/or UWB.

1.3.4 Video-AMR Fusion

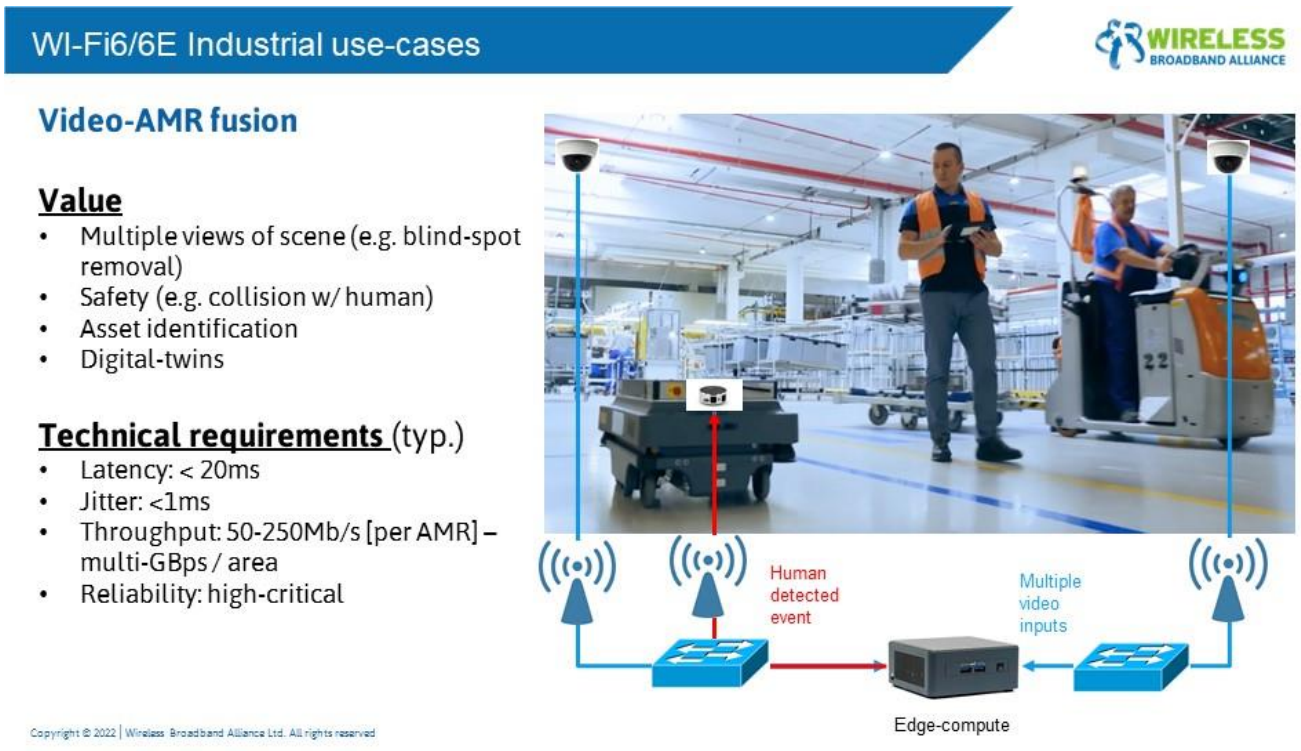


Figure 6 Video-AMR fusion

Video Fusion is the basis of the real-time digital twin concept. The digital twin provides a means to control and steer processes of the physical plant while simultaneously providing a safe environment to gather data. This can be used model and test and prove process changes and improvements prior to undertaking process re-engineering. It also enables new business models by enabling clients to engage and experience the production processes.

This capability can enable a range of use-cases that benefit the AMR system such as:

- Blind-spot removal
- Collision avoidance
- Co-bot (N x N collaboration)
- Route re-planning:
- Asset/people identification & tracking
- Real time 3D Mapping
- Safety alerts

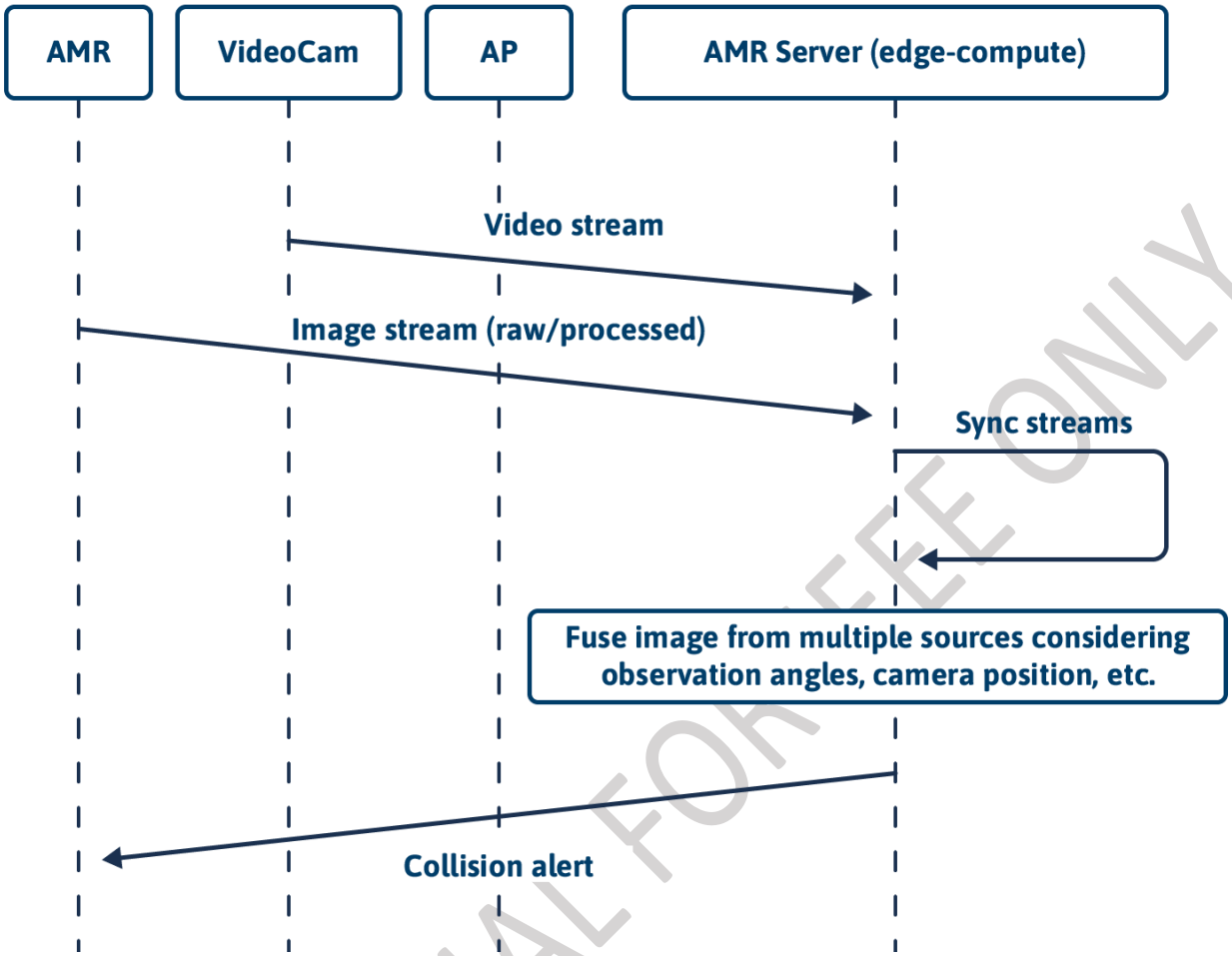


Figure 7 AMR Video Fusion process

In an exemplary fusion control loop above, images are periodically transmitted by both the mobile AMR and fixed cameras and delivered with predictable low latency to the AMR server. The server is typically running on an edge-compute platform collocated with the AP/WLAN.

The server synchronizes the streams in time (using e.g., in-built timestamps) allowing a frame-by-frame fusion of the image streams. Then, knowing the accurate position and orientation of each camera, advanced fusion processes such as object identification and collision detection can be applied. Alerts based on collision detection events can then be generated towards the AMR which can take appropriate evasive action to avoid said collision.

This process (input, sync, process, alert) is executed as part of a real-time control loop with tight bounds on latency and jitter (to affect a timely sync) and (as noted) also needs timely and accurate location information.

Like the underlying AMR and Video use-cases, tight bounds around packet delivery KPIs such as latency (e.g., 20ms) and jitter (e.g., 5ms) are a given. However, when applied to real-time

sensor fusion we need to consider additional benefits such as the ability to synchronize delivery of frames from multiple sources (i.e., delivery schedule) and/or accurately timestamp the frames such that they can be successfully fused without incurring unnecessary synchronization delays at the server.

These types of process synchronization requirements can only be met if each of the cameras and AMRs in the facility have access to wireless TSN (WTSN) capabilities. The ability to precisely scheduled delivery with bounded latency can only be provided with a common high-resolution clock signal.

More fundamentally, successful fusion requires that each sensor position (e.g., ceiling camera, AMR) and orientation be available to the system accurately and in real-time. While the fixed assets positions may be obtained via site survey means, the AMRs position is constantly changing and needs to be determined in real-time (i.e., order of the fusion loop e.g., 40ms). This positioning could be provided by GPS in outdoor environments, but indoor GPS is more challenging. Fortunately, a high-speed Wi-Fi based location technology such as FTM is available and part of a WTSN solution (i.e., for time-sync) and thus provided for an optimal solution.

1.3.5 AR/VR/XR

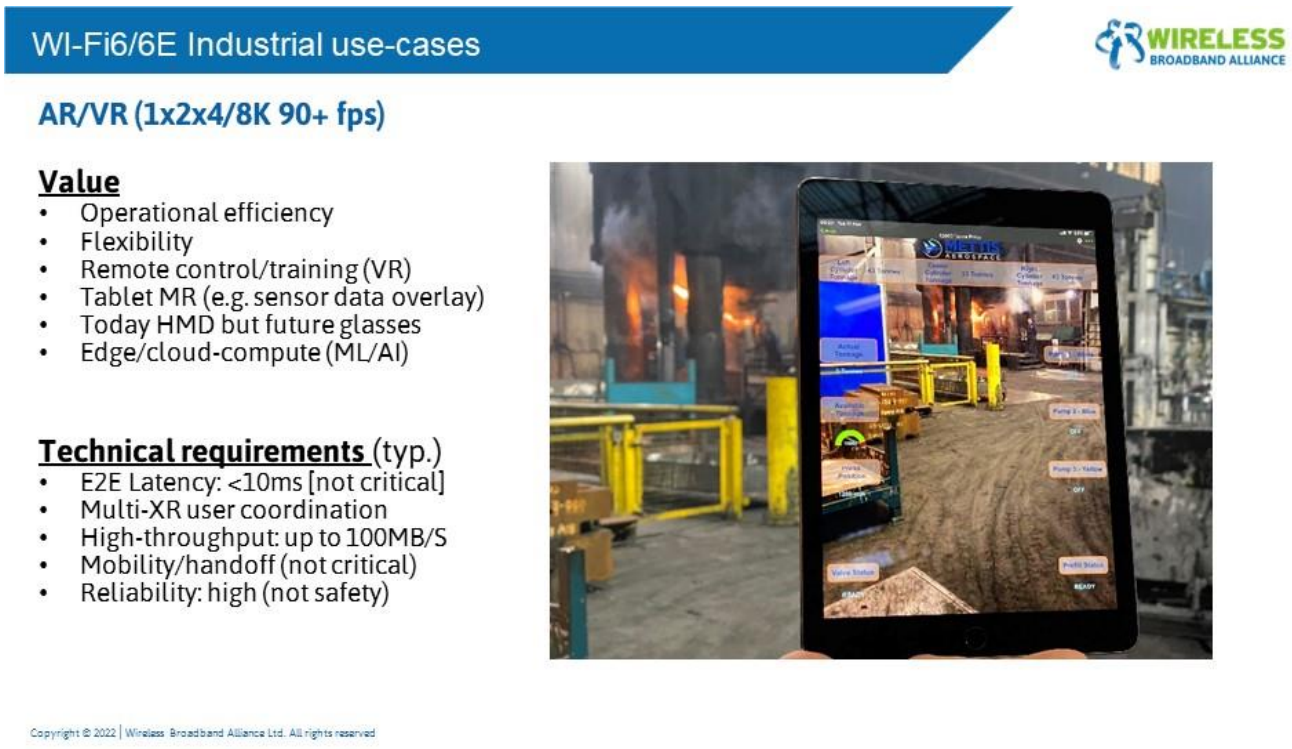


Figure 8 AR/VR/XR

Augmented Reality/Virtual Reality/Mixed Reality (XR) can be utilised to enable applications such as walk-by health monitoring combining an on-screen video feed with overlaid contextual machine information on a tablet. This would provide the operator with real-time sensor and control information (see Figure 8 AR/VR/XR). This could be extended to allow operators to receive process instructions via AR enabled safety glasses. Although AR/MR is not as data intensive as full VR, latency must be low to allow the user experience to be fluid (typically <100ms). An emerging application is virtual reality (VR) based machine remote control over Wi-Fi. This needs to be seamless and require high levels of resilience (e.g., AP failure, channel outage, etc) to meet safety critical requirements.

1.3.6 Industrial automotive

WIFi6/6E Industrial use-cases

Automotive

Value
- Telemetrics
- Logistics

Technical requirements (typ.)
- High-capacity (40GB/min)
- High-density (e.g. parking lot, charging station, storage lot)
- Low-interference (<<-60dBm)
- Reliability: Non-critical

Exemplary outdoor automotive use-case

Figure 9 Industrial Automotive

Automation in the manufacturing process improves efficiency and reduces error. A continuous learning model requires that the outcomes be known in order to provide feedback to the manufacturing automation processes. The automobile today is a rolling sensor array processing and correlating massive amounts of data on board and increasingly offloading more and more telemetry. The autonomous driving sensors alone generate data upwards of 4TB per day much of which needs to be uploaded for further processing and analysis. Use cases including the local network connectivity, wireless sensor data collection, continuous data uploads, charging efficiency and performance for Electric Vehicles (EV), firmware updates, GPS Map information and traffic updates. Over-the-air and Advanced Driver Assisted Systems (ADAS) have all gone mainstream. If not today, in the near future, every vehicle parked in a garage or in a driveway will have some amount of data that it still needs to address while out of service. One vehicle manufacturer is using 40 GB of offline data transfer as a target for telemetry upload and maintenance updates alone. Offload of this type of data is not particularly time sensitive, and can happen during non-operational times (for an EV, it could happen at the same time it's being charged). Even if this data is collected while the vehicle is essentially parked, this means that every vehicle in the parking garage could be looking to exchange up to 40 GB of data with the available Wi-Fi network.

Data to and from a vehicle is important, but it's also important to the ecosystem growing to support EV's. Charging an EV presently takes 75 amp service. Consider a parking lot filled with charging stations that will need to optimize the energy transfer from electric power grid to vehicles while also providing a convenient payment system which can be handled with Wi-Fi 6

onboard in automobiles. In addition to the high data requirements from vehicles, there is also a significant growth of mobile video traffic from 63% at 38 exabytes per month in 2019 to a projected 75% of data traffic with 160 Exabytes per month in 2025 [Auto1]

Cellular macro networks (4G/5G) shall certainly boost broadband IoT performance and micro/pico-cells will support ultra-reliable low latency communication (URLLC) for critical IoT [Auto2] in venues such as automotive manufacturing plants. Wi-Fi 6 is fully capable of complementing 5G networks by delivering the services in automotive connectivity. While, cellular and 5G operates on licensed bands and is typically deployed ubiquitously outdoor (at a large capital cost), Wi-Fi utilizes unlicensed spectrum and is typically deployed indoor to cost-effectively cover Enterprise buildings, homes or high-density public venues (HotSpots). Wi-Fi 6 has already offloaded 50% of the total mobile traffic from cellular networks [Auto3]. The integration of Wi-Fi 6 by the 5G operators in their deployment plans has projected increased offload to 60% or more by 2022. Interesting to note – HD Maps and Telematics is classified as “less than best effort”.

The Automotive industry is expected to be one of the top four data producing industries by 2030. In order to meet the requirements of the IoT and Industry 4.0 use cases more is needed to meet the expected demands. Wi-Fi 6 can provide a consistent high speed low latency data path today.

The use of IoT doesn’t stop once product is shipped from the point of manufacture to the retail dealership/store. Through the shipping process it is quite common to track the journey of every product to its final retail destination. Each stage of the journey from manufacturing to the dealership is managed by inventory tags or GPS freight tracking systems all relying on wireless connections to provide updates seamlessly throughout the journey.

Once delivered to the final retail destination, the vehicles on board systems tele metrics will be associated with an owners account and will then track the vital systems for the remainder of the vehicles service life.

Here again, onboard sensors for pressure, temperature, motion, vibrations, all work together to provide information regarding preventative maintenance or even failure diagnosis before the issue becomes a problem. Tele metrics information once collected is then used back at the manufacturing process to improve results achieved in the final products lifespan.

The information flow to the point of manufacture provides crucial operational insights under a widely ranging user environments and use cases. These learnings are used to develop software updates to adjust or improve the function over the lifecycle of the product. Thus the control loop initially established at the manufacturing level to improve processes, can be leveraged across the products lifecycle to provide the continuous improvement vital to the manufacturing and development efforts.

1.3.7 Wireless Time-sensitive-networking (WTSN)

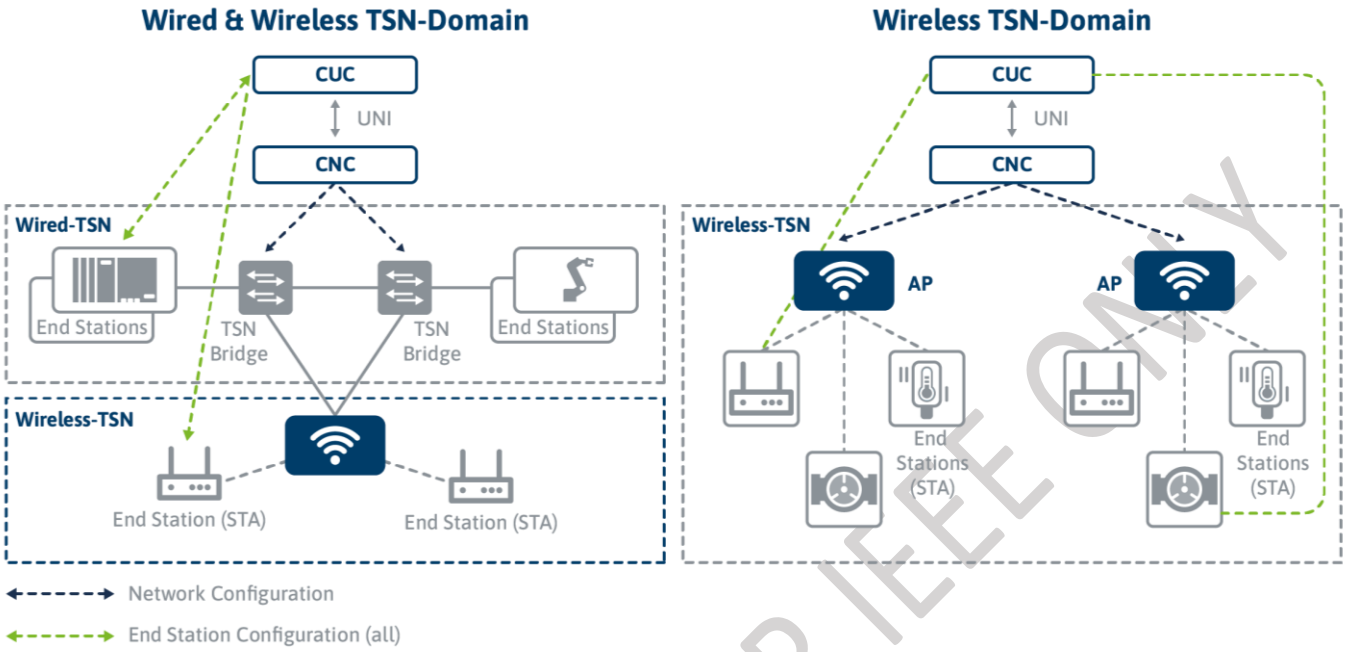


Figure 10 Wireless TSN Architecture options

New and emerging use cases in factory and process automation require increased reliability, greater throughput, reduced and bounded latency as well as flexibility and agility in deployments. TSN is an essential technology to enable deterministic behavior in networking with objectives to support real-time applications and to achieve network convergence.

The term TSN (Time-Sensitive Networking) stems from a set of standards, currently more than a dozen, specified by the IEEE 802.1 TSN Task Group. These standards define tools and mechanisms to facilitate capabilities such as precise time synchronization, traffic shaping, transmission scheduling, path control, filtering, and redundancy. Based on these tools, key characteristics of determinism in networking such as bounded latency and jitter as well as low packed loss are achievable in an interoperable way. TSN-Profiles are means to combine a selection of features, default parameters, protocols, and procedures for specific domains and industries such as industrial automation (e.g.: IEC/IEEE 60802: TSN-Profiles for Industrial Automation) or entertainment (e.g.: IEEE 802.1BA: Audio/Video Bridging). Based on profiles, the complexity is much better manageable, and certifications are feasible using a fixed set of tools and predefined features.

With Wi-Fi 6, deterministic QoS capabilities are available. This comprises especially the following characteristics and features:

1. Precise Time Synchronization as defined in IEEE 802.1AS -2020 for Wi-Fi, this especially pertains to Timing Measurement (TM), Fine Timing Measurement (FTM), both specified in IEEE 802.1AS-2020 in the scope of supporting extended physical layer options. Typically, Industrial automation applications require synchronized time that is traceable to a known source (i.e. to Global Time). It is needed to coordinate and align actions, perhaps in the scope of a control loop application, and to align, order and record actions and events based on precise time stamping.
2. Traffic prioritization: Natively not a TSN-feature, traffic prioritization is often used in combination with other TSN-tools to address the criticality of traffic types. It defines the Strict Priority Selection algorithm used to select the next frame to be transmitted from multiple queues on an egress port. The initial mechanism uses the Priority Code Point (PCP) field to map traffic classes to queues.
3. Low and bounded latency following the definitions in IEEE 802.1be (low latency) and IEEE 802.11ax. For deployments in combination with Deterministic Ethernet (TSN), an overall scheduling can be realized using 802.1Qbv (bounded latency). Scheduled Traffic (IEEE 802.1Qbv) introduces transmission gates for time-based control of queues. The scheduling concepts in Wi-Fi 6 are described in detail in clause 2.1
4. High reliability is needed wherever application does not tolerate any packet loss. With Wi-Fi, it is based on IEEE 802.11be multi-link. With Multi-link operation (MLO), access points (AP) and stations (STA) are enabled to transmit and receive data from the same traffic flow over multiple radio interfaces using link aggregation at the MAC layer where a link is mapped to a channel and band. This feature provides the capabilities to meet the high reliability objective with frame duplication over multiple links, like FRER as specified in IEEE 802.1CB.
5. Resource management: is required to configure and manage the features mentioned above. Using the definitions in IEEE 802.1Qcc, a controller-based approach, applying the Centralized Network Configuration (CNC) / Centralized User Configuration (CUC) architecture, enables schedule and path computing as well as network and device configuration based on user requests (represented by the CUC). The User Network Interface (UNI) exists between CNC and CUC.

In combination, the underlying mechanisms provide a toolset, similar and interoperable with the definitions in IEEE 802.1TSN. It always depends on the use cases and the requirements what tools are applied and in which order. These definitions are the outcome of the engineering process.

Because of a strictly standardized approach aligned with the tools and features specified in IEEE 802.1, a combination with wired TSN-mechanism is doable in an end-to-end way. This will be an essential precondition for initiatives such as Industry 4.0 and Digital Factory, supporting the vision of lean and agile manufacturing. Technically, it is achievable using a hybrid configuration and management process to enable resource reservation along the entire path from the sender (talker) to the receiver (listener) as well precise time synchronization. This hybrid model (see figure 0815) is based on the approach to make the configuration and management entity (CNC) wireless aware, but to hide the short-term Wi-Fi related configuration and scheduling mechanisms.

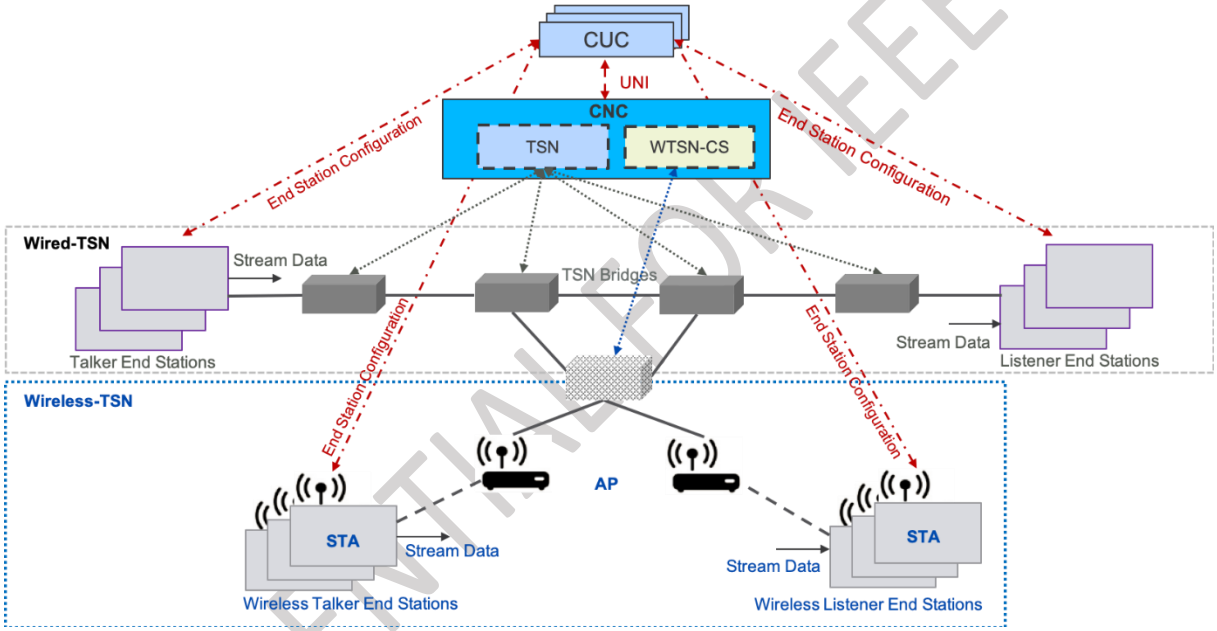
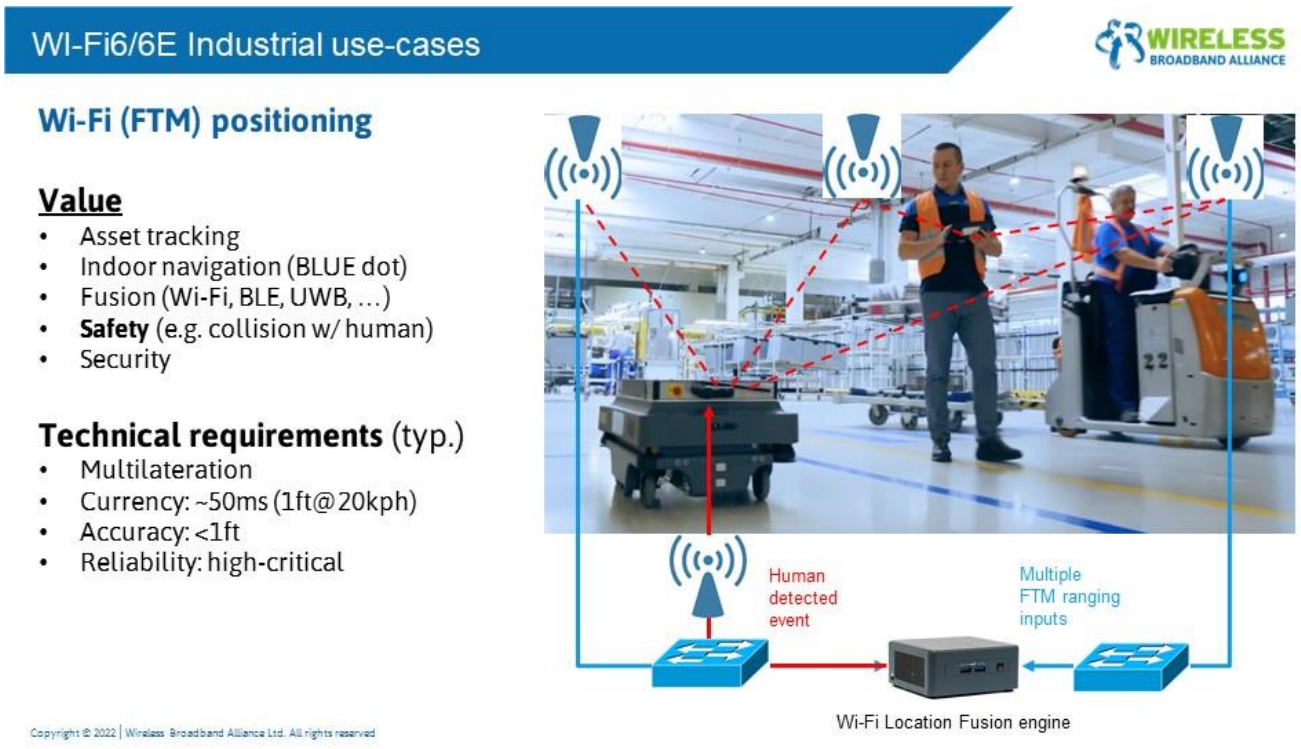


Figure 11 WTSN Architecture

In addition to the capabilities to meet deterministic requirements, increased usability is another benefit of Wireless-TSN. The controller-based concepts (CNC/CUC) as well as designated protocols and interfaces for network configuration in combination with industry-specific engineering tools allow application driven configuration of networks and devices. The use of application data derived from engineering tools leads to network configuration based on intent and avoids manual and error-prone configuration. A tight integration between CNC and CUC hides complexity of network configuration.

The Wireless-TSN capabilities as described in this clause does not represent a use case itself, they serve as a framework to provide the deterministic capacities and related features for the use cases listed in this whitepaper. A concrete use case, say AR/VR or Safety Controls, might only require a subset of the TSN-features available with Wi-Fi 6.

Wi-Fi location-based services



Wi-Fi allows precise indoor range and position/location determination based on inherent mechanisms using the Fine Timing Measurement (FTM) protocol as specified in IEEE 802.11-2016. Since it does not require additional Wi-Fi infrastructure, it all works on the existing wireless network already providing connectivity. Indoor location services offer the capabilities to enable new use cases and to enrich existing scenarios. The subsequent bullets list essential capabilities provided by precise location information:

- Indoor Navigation – as a prerequisite for mobility and related applications and systems such as Autonomous Mobile Robots (AMR) and Automated Ground Vehicles (AGV) such as forklifts, delivery platforms, etc. Precise location determination allows secure indoor navigation for these vehicles on the factory floor or in a warehouse environment. This includes route planning, exception handling and safety related aspects such as collision avoidance based on proximity.
- Asset Tracking – as an enabler for managing devices, tools, or other apparatuses indoors to support workflows where mobile assets are involved. It allows exception management to locate faults or lost devices. Furthermore, it can encompass employee location tracking for safety reasons (in adherence to legal regulation and law).
- Smart Manufacturing – precise location information can help to enrich digital work orders to allow agile and optimized manufacturing processes. Integration into ERP systems allows correlation with other information to streamline automation and production.

- Security and Alarm Handing – predefined zones, policies and alerts can help to tighten physical security regarding access control and to support theft protection.
- Network Management and Planning – with location-based services, network planning, troubleshooting and network design can be performed more efficiently.

Technically, Wi-Fi location determination is based on radio transmission ranging between an access point (AP) and the end station (asset). This requires precise time-synchronization to a reference clock such as that provided by 802.1AS. In principle, the mechanism uses a round trip measurement and timestamping of frames on both sides to calculate the transmission time and to derive the range from each other. Measurement bursts are a means to perform averaging across several measurements with the outcome of a more accurate range. Depending on the mobility, periodic measurements are necessary (e.g.: every few seconds).

To determine the location, a mapping into a coordinate system is needed. This requires measurements between multiple pairs of endpoints of Access Points, at least three for 2-dimensional position, and at least four for a 3-dimensional position. At this point, the WLAN knows the geo-location of the end-station since the APs fixed positions are well-known. In applications where location reciprocity is required, the APs share their geo-location with the end station (asset). Based on this, the end station is able to calculate its position on a map (w.r.t other assets). It requires diligent configuration and management to enable location services in a Wi-Fi network including installation of access points (e.g.: location, height-above-floor). Any configuration towards location determination should address security and privacy aspects to protect user's personal data protection.

1.4 Security considerations

Network convergence and increased connectivity comes with a price, the attack surface increases as well. Security must be addressed from the very beginning of designing and developing such networks. Network and protocol security are essential requirements of robust operational technology networks employed in industrial environments. This is especially a concern if wireless communication is involved. In many deployments, systems and networks are part of the critical infrastructure such as Industrial Automation and Control Systems (IACS). A widely used series of security standards for IACS is ISA/IEC 62443 (Industrial communication networks - IT security for networks and systems). Part 3-3 of ISA/IEC 62443 explicitly defines requirements for wireless communication because of its specific nature regarding physical security controls with implications regarding risk analysis and assessment. The specification suggests that to meet the requirements of a given industrial sector, a "Defence in Depth" methodology is the recommended approach. It consists of six high-level steps, including creating a security plan, separating networks, providing perimeter protection, segmenting networks, hardening devices, and continuously monitoring and patching.

Secure network segmenting [Seg1] needs to be considered especially in the context of IOT devices since these devices often require access to specific manufacturers cloud services (e.g., device SW updates) and IT on-boarding systems (e.g., EasyConnect access to an Enterprise certificate authority). A general recommended approach is to implement a secure segment (or virtual network) for these distinct network uses and device types (e.g., by manufacturer) that restricts access only to the necessary IOT or onboarding systems.

Where wireless security is concerned, an implementation with Wi-Fi 6 or Wi-Fi 6E would particularly address device hardening by including a WPA3 security protocol. While WPA3-Personal is supported in every Wi-Fi 6/6E device, support for WPA3-Enterprise might depend on device support, device management and onboarding considerations. For client devices that do not have a rich UI or other mechanisms for credential provisioning, secure onboarding mechanisms such as Wi-Fi Easy Connect might be considered in combination with secure network segmentation, where trust bootstrapping is based on scanning a QR code scan, or other out-of-band mechanisms such as BT, NFC and 802.1X certificates. Wi-Fi Easy Connect can be used to securely provision WPA3-Personal or WPA3-Enterprise credentials, or to provision DPP Connectors for use with DPP enabled APs [Sec4]. For some use cases, other frameworks such as CSA Matter might also be used to onboard devices with Wi-Fi credentials [Sec5].

In contrast to IT systems, availability and data integrity are often very important attributes, followed by confidentiality and data privacy. Robust implementations using means of redundancy are required to accomplish the objective of high availability. Redundancy can be achieved by, for example, making use of multiple radios simultaneously operating in different channels. Figure 9 illustrates the four security levels defined as part of IEC 62443-4-2.

Sample Requirements

IEC 62443-4-2 Component Identification and Authentication Control

Feature	SL1	SL2	SL3	SL4
Identify and authenticate human users	X	X	X	X
Component shall enable the management of accounts	X	X	X	X
Component shall support the management of identifiers	X	X	X	X
Component shall support authenticator management	X	X	X	X
Password based authentication with defined password strength	X	X	X	X
Obscure authentication feedback during authentication process	X	X	X	X
Enforce unsuccessful login attempt limit, lock account	X	X	X	X
Provide warning message to individuals attempting to access the system	X	X	X	X
Uniquely identify and authenticate all human users		X	X	X
Software process and device identification and authentication		X	X	X
When PKI is used, the component shall integrate with PKI infrastructure		X	X	X
When PKI is used, the component shall check validity of certificates		X	X	X
Support for symmetric key based authentication		X	X	X
Unique software process and device identification and authentication			X	X
Authenticators shall be protected by hardware mechanisms			X	X
Prevent password reuse for configurable number of generations human users			X	X
Protection of public key via hardware			X	X
Protection of symmetric key data via hardware			X	X
Multifactor authentication for all interfaces				X
Prevent password reuse for configurable number of generations software process or device				X

ISASecure 11 ISA Security Compliance Institute

Figure 12 IEC 62443-4-2

2 Wi-Fi 6/6E

2.1 Evolution to determinism (OFDMA)

Prior to Wi-Fi 6, each Wi-Fi endpoint (or STA) associated with an AP was responsible for deciding when it should transmit data packets in the uplink (UL) to its AP. This scheme termed carrier-sense-multiple-access with collision avoidance (CSMA/CA) allows a STA (or AP) to detect channel state (busy or not) via carrier-sensing (CS) and if the channel is free after a monitoring period, can transmit its queued data packet. This is thus effectively a random access (RA) scheme. All such schemes are simple (not requiring AP coordination) and give good performance and low latency under lightly loaded conditions. However, as the load increases, so to do on-air collisions since the STA are essentially uncoordinated relying only on Carrier Sense (CS) and a random back-off. Under such loaded conditions, both performance and latency can degrade quickly. This can lead to real-time sessions (e.g., voice, video) experiencing poor performance which, in the IIOT realm could be catastrophic!

Enter scheduled access (SA) or trigger-based (TB) uplink (UL) orthogonal frequency domain multiple access (OFDMA) as it is termed in Wi-Fi 6. With SA, STA transmissions can be coordinated by the AP to avoid collisions among STAs. Unlike CSMA/CA, there may be coordination overhead in certain scenarios, but with typical loads, the net gains in latency are significant. In particular, the strict 99% latency (critical for all real-time and IIOT applications) is very low and relatively well bounded compared to Wi-Fi5.

Wi-Fi 6 OFDMA also operates in both uplink and downlink directions. The channel bandwidth is split into several slices called resource units (RU) and each RU is potentially assigned to different devices. Parallel access to the channel optimizes the utilization and reduces the contention between stations. This increases AP and STAs transmit opportunities and reduces latency. Figure 10 illustrates an example of single user (left) and OFDMA (right) access in Wi-Fi 6/6E.

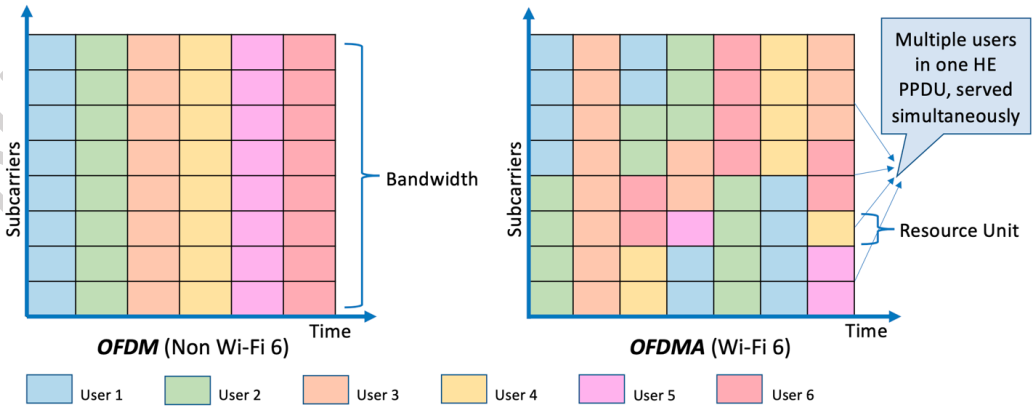


Figure 13 OFDMA

2.2 Wi-Fi 6/6E MU-MIMO

MU-MIMO was first introduced in Wi-Fi 5; however, it took the efficiency of OFDMA in Wi-Fi 6 to make it practical. MU-MIMO increases the system throughput by using multiple spatial streams to simultaneously communicate with multiples of clients simultaneously. In Wi-Fi 5 the overhead of channel information required offset any real gains that could be made. As a result, STA support was poor in the market. Wi-Fi 5 was also limited to a maximum of 4 spatial streams and only benefited downlink traffic. A maximum of 4 clients could operate in parallel in any downlink transmission. In contrast, Wi-Fi 6 MU-MIMO can manage up to 8 spatial streams (unique devices) and supports both uplink and downlink transmission in 2.4GHz, 5GHz, and the 6 GHz bands (Wi-Fi 6E). Wi-Fi 6 is presently operating with as many as 8 spatial streams supporting up to 8 client devices simultaneously. Wi-Fi 6 OFDMA and MU-MIMO can quadruple the amount of data being served to clients while dramatically reducing the airtime consumed.

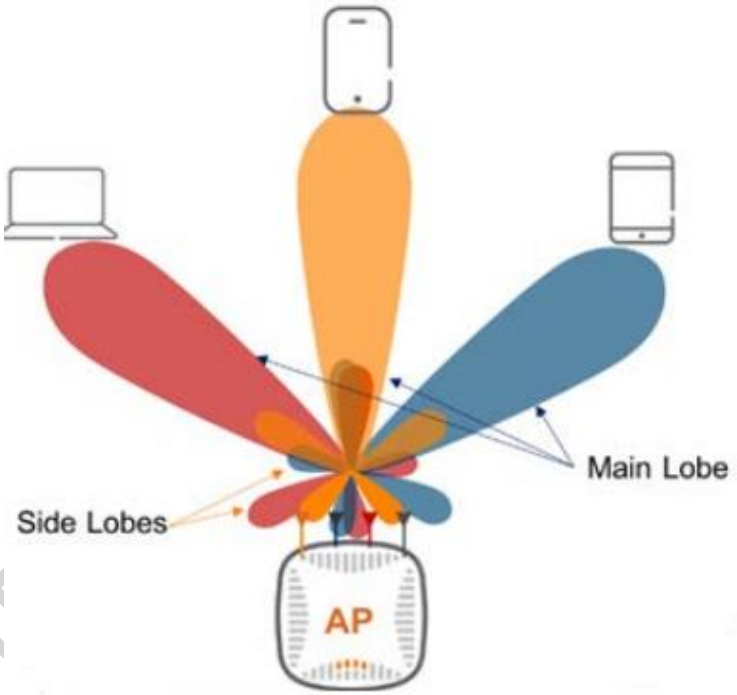


Figure 14 MU-MIMO

2.3 Power savings

Several power savings techniques have been used in prior Wi-Fi generations (Wi-Fi 5, 4, …) to minimize power draw such as Unscheduled-Automatic Power Save Delivery (U-APSD). However, this method has been optimized for applications such as voice and still relies on the client receiving periodic control traffic from the AP.

A more efficient power-save & scheduling enhancement was added to Wi-Fi 6 termed target-wake-time (TWT). This capability allows a STA to access a scheduled transmit opportunity (TXOP) at an agreed time between the AP and STA. For example, a STA might negotiate a pre-scheduled TXOP or service period (SP) every 1000ms as this is the period of a voice session it is transporting. This then allows the STA to go to sleep and wake-up only when it expects its TXOP (i.e., every 1000ms). Thus, a power savings can be realized by the STA since it can turn off its Wi-Fi receiver and transmitter for the majority of the TWT SP (e.g., 999 out of 1000ms). As a bonus, like UL TB scheduled access, TWT-based scheduled access can also result in a collision free environment and thus the related benefits of better performance & latency @ scale.

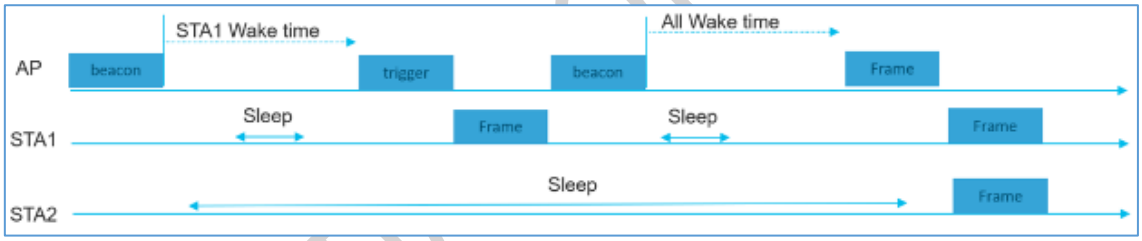


Figure 15 TWT

Implemented along with appropriate connection management enhancements (BSS Max Idle Period) allows an effective sleep time of up to 65535*1000*1024us or ~18.5 hours! For complex (multiple spatial-steam) devices, the additional benefits of dynamic multi-user spatial multiplexing power save (MU-SMPS) allows the IIOT sensor to only activate multiple receivers when a high-speed burst)

In Wi-Fi 6, TWT provides for three flavors which are suited to various use-cases as follows:

- Individual: a STA wishes to sleep then wake-up and transmit in accordance with a well-known application service period (SP). This may be a suitable option for IIOT devices such as battery powered sensors that only need to report information infrequently (e.g., minutely temp sensor). In such cases, the communications cost (i.e., Wi-Fi modem) may be a significant portion of the devices power budget

- Broadcast: a set of STA wish to wake-up at the same time to receive periodic information from a server. This may be a suitable option for IIOT devices such as AMR/AGVs that receive periodic map and order updates from the robotic control system,
- Dynamic (TWT Information): a STA supports applications with a dynamic variety of service periods or TXOP durations. This may be a suitable option for IIOT devices with on-demand periodic flows such as voice and video whereby the session starts and stops at unpredictable times (e.g., video capture is enabled by an operator in order to diagnose a problem).

2.4 BSS Color & spatial reuse (SR)

In an industrial Wi-Fi deployment, expecting densities of 3-4 devices /m^2 requires dense AP placement/coverage. BSS Coloring with Wi-Fi 6/6E allows the assignment of unique color code to each BSS operating on a given channel. BSS Color allows Stations and APs to understand the difference between a transmission to or from the AP they are connected to (Intra BSS) and a conversation that is intended for another BSS (AP) entirely (Inter BSS). A station hearing a transmission that's part of different BSS can simply ignore it without wasting time or energy to demodulate it. BSS Coloring also makes it possible to identify spatial reuse opportunities, that is, an opportunity for more stations to transmit at the same time. BSS Coloring allows Stations to know when another station is a source of interference, or when both could potentially transmit at the same time without interfering with one another. This improves the contention mechanisms available in previous Wi-Fi generations by adding an efficient mechanism to allow selective spatial re-use. This will increase the operating density of Wi-Fi networks, while simultaneously reducing interference and improving spectral efficiency.

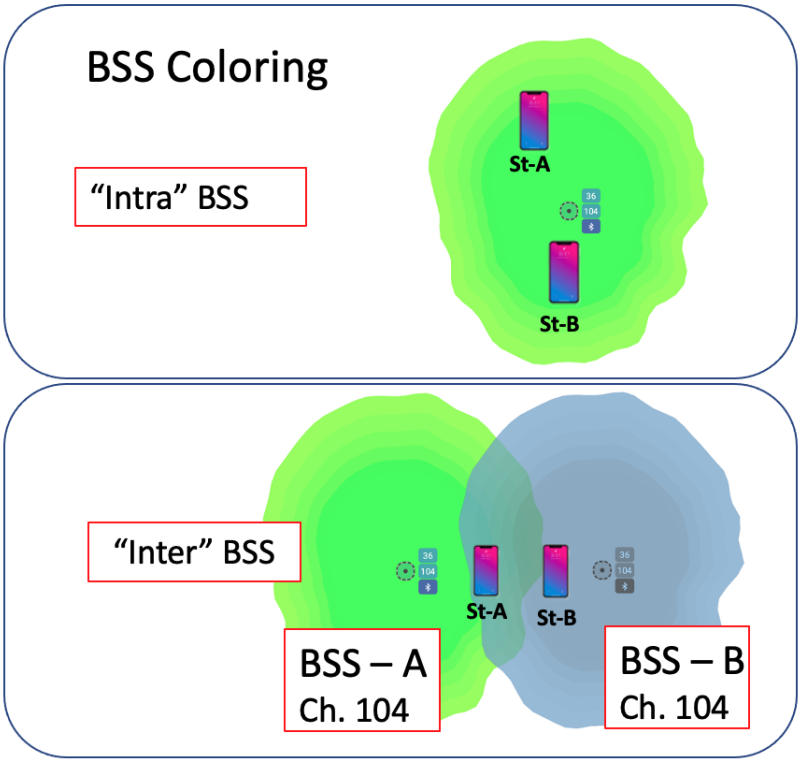


Figure 16 BSS Color

Wi-Fi 6 OBSS PD based Spatial Reuse (SR) Operation: High Density Wi-Fi deployments are often hindered by the inefficiency of the contention mechanism. BSS Color adds intelligence that can be used to identify Spatial Reuse opportunities. OBSS PD based SR (Spatial Reuse) can optimize the efficient reutilization of spectrum in dense networks. To increase the number of parallel transmissions possible, the clear channel assessment/carrier sense (CCA/CS) threshold is adjusted to a new value called OBSS Preamble Detect (PD) which reduces contention and improves access to the channel by raising the default CCA/CS threshold under specific conditions. By optimally selecting the PD, interfering APs can transmit to their corresponding stations [4].

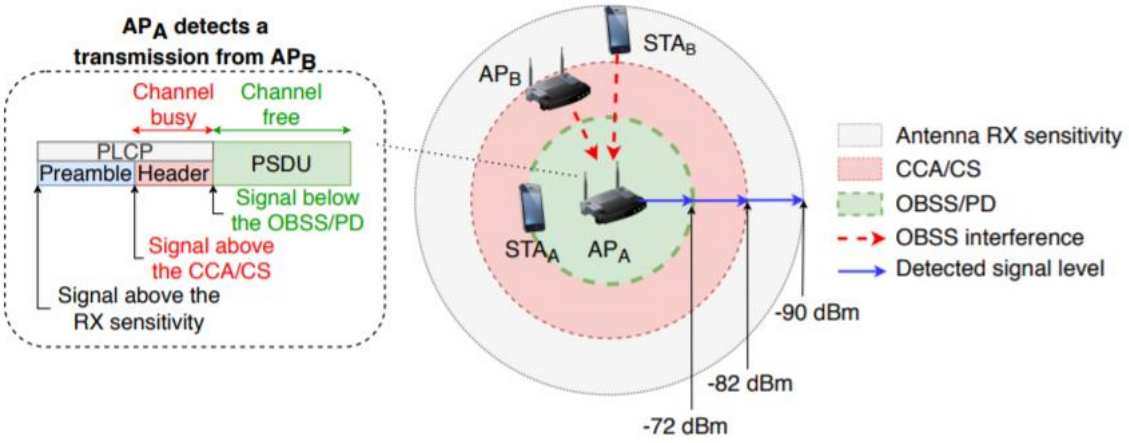


Figure 17 OBSS PD

A Wi-Fi 6 device can differentiate between the Intra and Inter BSS by the BSS color field inspection. Intra BSS frames must use the default PD threshold of -82dBm to avoid interference. However, an Inter BSS frame can use a more aggressive PD threshold for more parallel transmissions depending on its proximity to other BSS stations. A Wi-Fi 6 device may also simply drop the inter BSS frame without demodulating the entire frame which saves radio power and time as well.

2.5 Quality-of-Service (QoS) architecture

Packet-level Quality-of-service (QoS) in a Wi-Fi 6 environment involves the following:

- Traffic flow classification, marking and treatment
    - IP Differentiated Services Code Point (DSCP) or Type-of-service (TOS)
- Enhanced distributed Channel Access (EDCA)
    - User Priority (UP) and/or traffic-identifier (TID)
- Multi-user (MU)-EDCA

Application of legacy DSCP-based QoS and EDCA with UP/TID mapping has been well covered in previous Wi-Fi generations. In Wi-Fi 6, a new QoS mechanism known as MU-EDCA had been added to address the challenge of prioritization of uplink (UL) traffic in a scheduled trigger-based (TB) access regime. Under MU-EDCA, a device (STA) that accepts an uplink trigger from the AP (i.e., agrees to be scheduled by it) must accept the terms of the MU-EDCA parameters and ignore the existing EDCA parameters.

The most important MU-EDCA parameter is the per Access Category (AC) timer value which dictates when the STA can revert to EDCA and perform legacy un-scheduled contention-based access. Within this scheduled access period (i.e., within the timeout period), the MU-EDCA

parameters such as CW min, CW max and AIFSN can be set in a way that allows controlled contention between the devices (STA). However, for time-sensitive industrial applications such as described within it is recommended this be disabled (AIFSN=0) and rather the per-AC time be set to the maximum to prevent unscheduled transmissions.

2.6 Wi-Fi security

To address the kinds of attack vectors identified in 1.2.4, Wi-Fi Alliance launched WPA3 in 2018 [Sec6]. Additional features and improvements have subsequently been added to WPA3, notably in the December 2019 and December 2020 updates [Sec7]. WPA3-Personal uses the SAE protocol to provide resistance to offline dictionary attacks on the password. The Hash-to-Element (H2E) variant of this protocol provides additional protection against side-channel attacks [Sec8]. The (optional) SAE-PK (SAE Public Key) mode [Sec9] protects against evil-twin AP attacks when password-based authentication is used in public networks, or in networks where there is risk of the password being compromised. WPA3-Enterprise requires client devices to perform server certificate validation to protect against rogue AP attacks. The (optional) WPA3-Enterprise 192-bit mode requires use of stronger CNSA approved encryption and authentication methods, targeting networks carrying highly sensitive data [Sec10]. WPA3 devices are required to support Transition Disable signaling to protect against downgrade attacks when transition modes (for interoperability with WPA2 devices) are used. Additional (optional) features include Beacon Protection to protect against active attacks that manipulate the contents of Beacon frames, and Operating Channel Validation to provide additional protection against multi-channel man-in-the-middle attacks [Sec11]. WPA3 certification also includes testing for the so-called FragAttacks vulnerabilities [Sec12]. More information on these features is available in the WPA3 Technology Overview [Sec13]. Wi-Fi Alliance has also launched Enhanced Open as a replacement for legacy open networks, which provides link encryption but does not provide mutual authentication [Sec14]. In addition, Wi-Fi Alliance launched Easy Connect, which provides a mechanism for securely onboarding headless client devices to networks using WPA3 or DPP security [Sec15].

One aspect that separates industrial IoT security applications from others is the fact that devices for industrial control and monitoring are designed for 20-year lifetimes. This means that every plant will have both old and new technology co-existing, a challenge called out in more detail in Security considerations. The 2019 Global ICS and IIoT Risk Report [Sec16], released November of 2020, states that 53% of industrial plants surveyed operate systems with Windows XP machines, for instance, which is a technology introduced in the year 2001. Thus, an industrial control systems engineer should always consider legacy devices when structuring security solutions

3 RF/network Deployment guidelines

3.1 Factory/Warehouse/Logistics

Factory environments are often a collection of large (e.g., 100K+ sq. ft) buildings with tall ceilings (e.g., 30+ft/ 10+m) and large metal obstructions. Factory automation equipment is either stationary (e.g., metal pressing machinery) or mobile (e.g., moving automotive assembly line, AMR/AGV). Both types of applications require reliable (e.g., 99.999%), low-latency (e.g., 10-100ms) and deterministic communications between the controller and robot in order to avoid unintended movement including collisions with other pieces of expensive equipment and humans (e.g., sensed by the robots or other sensors). Factories can also be equipped with 1000s of sensors placed on equipment for the purposes of diagnostic monitoring and operations optimization. These sensors can be affixed to stationary assets (e.g., large rotating machines) or mobile assets (e.g., AMR/AGV) and can report everything from pressure, temperate or real-time LIDAR mapping data. Like the automation control systems, these sensors also require reliable and deterministic communications with their monitoring systems to ensure accuracy and timely response to events. Finally, emerging factory systems desire augmented, virtual or mixed reality (AR/VR/MR) to visualize and perhaps control factory systems (e.g., remote grabber with a built-in camera presented in MR to the operator located in the on-site control room). The requirements for these types of applications not only need deterministic low latency but also high throughout due to the use of live 4/8K stereo video feeds.

To meet the physical structure challenges (high ceilings with lots of metallic obstructions), it is common to deploy Wi-Fi with high-gain directional antennas (e.g., 10-15 dBi, 25–60-degree beamwidth) to contain the radiation pattern of the AP and counter RF degradation and fading affects at the floor level of the factory. The need for antenna's is not limited to high ceiling use cases, but also to provide cell isolation in increasingly dense environments. Co-Channel interference is the most common contributor to sub optimal Wi-Fi installations. Wi-Fi itself may be Ubiquitous around the world, but regulatory rules often change the number of channels (bandwidth) that can be used in each region effectively. In regions relying on lower channel space, using directional antennas can allows for increasing channel re-use rates without adding additional co-channel interference into the performance concerns.

Addressing low latency and determinism from a deployment POV typically relies on a three-pronged approach:

- Maximizing the devices data rate at the edge, reduces contention and increases the effective number of stations that can be managed
- Minimizing co-channel interference (CCI) between APs, ensures full and interference free bandwidth is available maximizing the available spectrum

- Leveraging 802.11ax/Wi-Fi 6 Scheduling capabilities to optimize the traffic patterns and manage critical QoS requirements

A shipping yard or port facility typically contain several challenges for coverage with Wi-Fi due to sheer physical space. Many can be covered just fine by mounting suitable outdoor class APs high on light posts or other high points if available across the facility. With such mounting points Wi-Fi can be deployed today using Wi-Fi Mesh even if the wired infrastructure is not in place to support it. This Mesh network nodes contain multiple radios now capable of providing wide area coverage while simultaneously providing full or half-duplex backhaul links. In extremely large area coverage, it may be wise to rely on 4g/5g Macro network coverage and relying on an Open Roaming architecture to allow hybrid network coverage model to manage the transitions seamlessly.

3.2 Automotive

Along with the steady increase in the number of automobiles that will require connectivity, and the amounts of data they will need to accommodate, where they access the network from for telematics and maintenance upgrades will also change. For vehicle owners, data uploads will need to be processed regularly and at times when the vehicle is out of service. This means either while parked at work, or overnight. Wi-Fi 6 is an attractive option for this task because of its cost and wide availability. Most of the Wi-Fi deployed in automobiles today is of the mobile broadband variety – providing hotspot for the vehicle occupants. With the increased need for network access, could this Wi-Fi also be used to connect the vehicle to its data infrastructure?

Because Wi-Fi is contention based, understanding how Wi-Fi propagates externally from a Wi-Fi radio located inside the vehicle is important. First, some assumptions were validated with industry experts. In Car Wi-Fi is largely implemented on 2.4 GHz using 802.11n which is suitable for a low density mobile broadband use case. In a parking garage with 100's of other vehicles, becomes a very high density use case. Wi-Fi 6 capable radios are scheduled to start rolling into production in the 2022/23 model years according to at least one manufacturer.

1. Wi-Fi is installed as part of the infotainment system, most often located inside the dashboard, either as part of the control unit or a module plugged into it.
2. Wi-Fi antennas are integrated into the module/components and are usually low gain Omni Directional
3. Tx power levels used are variable, it doesn't take a lot of power to have a great experience from within the vehicle. This is changing as more use cases require connectivity outside of the vehicle.

To test a Wi-Fi 6 2x2 2 AP placed underneath the dashboard. The resulting signal propagation was mapped to understand the potential for reaching an external Wi-Fi network, as well as interference to potential to other vehicles. The resulting plot shows that with a 4 dBm Tx signal, propagation was quite good outside of the vehicle. At 21 ft/6.5 m the measured RSSI was at measured - 54 dBm.

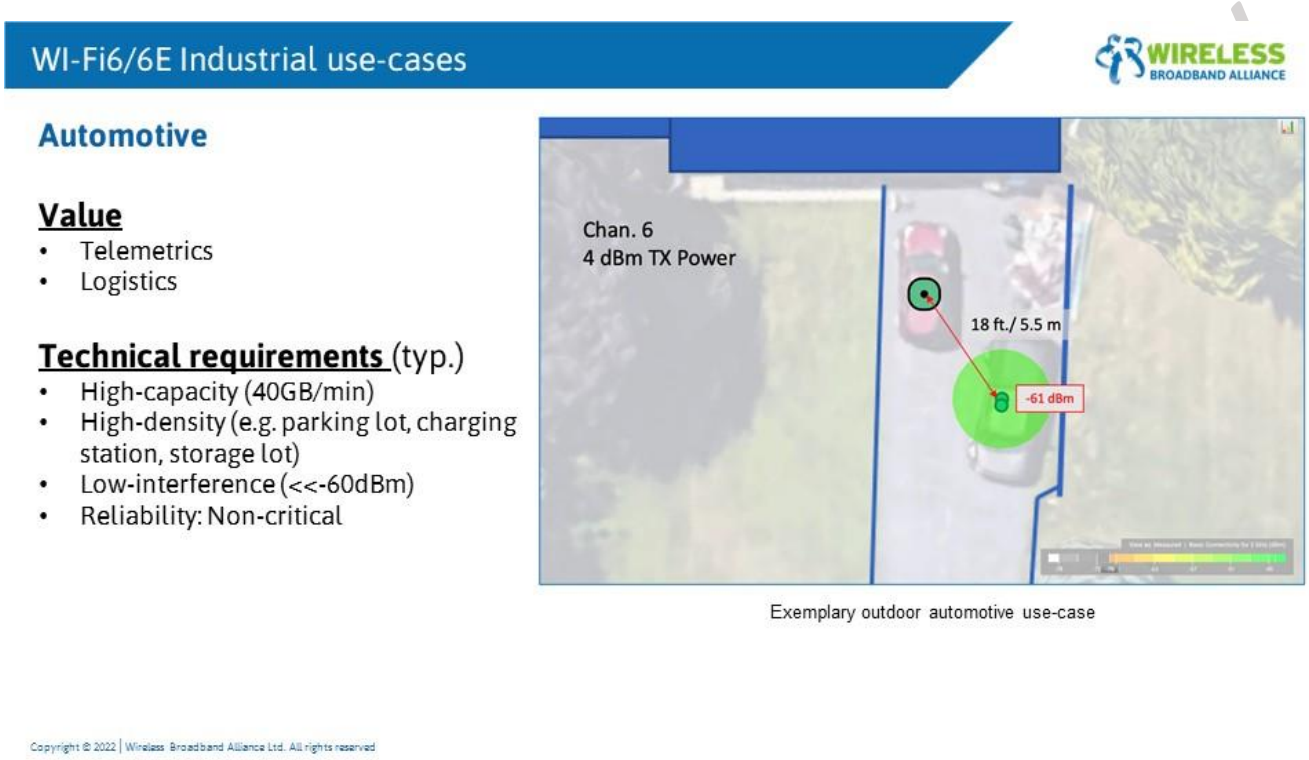


Figure 18 Automotive coverage

In the driveway of a suburban home with only two vehicles, providing an interference-free Wi-Fi connection isn't very complicated. However, in a metropolitan parking garage filled with several hundred vehicles this becomes more complex. Wi-Fi 6 and Wi-Fi 6E in the 5 and 6 GHz spectrum can ensure capacity and provide more than enough separation to provide stable, low latency/high throughput connections.

Wi-Fi has been part of the planning in the Automotive industry for some time. Wireless Access in Vehicular Environments (WAVE) is defined in the amendment IEEE 802.11p to support Intelligent Transportation Systems (ITS) applications. It broadly includes the information exchange between high-speed passenger vehicles, ambulances, and roadside infrastructure in the licensed ITS band of 5.9GHz. With DSRC applications now moving partly to cellular technologies some of the previously reserved channel in 5.9 GHz have been re-designated to unlicensed use by Wi-Fi in the US as the UNii-4 band further expanding the bandwidth available to Wi-Fi.

3.3 Wi-Fi TSN

Network convergence is essential to meet the requirements of new and evolving use cases in the scope of IIoT and OT. This encompasses an integration with Time-Sensitive Networking (TSN) to achieve end-to-end deterministic transmissions over wired and wireless links. Precise time synchronization is crucial to enable the deterministic behaviour of all network components and end-devices including applications in case of isochronous behaviour. This comprises the profile specific aspects as well as clock domain definitions (e.g.: global clock, working clock). Furthermore, the definitions of TSN-domains need to be considered because of administrative constraints. To accomplish network convergence over a hybrid infrastructure (wired, wireless), network management needs to work end-to-end with great usability. The fully centralized model for TSN as specified in IEEE 802.1Qcc provides the entities (CUC, CNC), procedures and interfaces (UNI) to enable this for the Ethernet and Wi-Fi links combined. Based on the definitions of IEC/IEEE 60802 (TSN-Profiles for Industrial Automation), the objective of Plug and Produce is achievable. From a system perspective, a single common multi-vendor converged network provides a scalable platform for OPC UA (FX / FLC) which is a designated protocol for Industry 4.0.

Conclusion

Throughout this whitepaper, WBA explored how Wi-Fi 6/6E can be used to address key Industry 4.0 use-cases that connect machines, material, people, processes, products, and services to improve visibility and understanding, increase quality and efficiency and ultimately create greater value for manufacturers and their customers.

Whether the application is a mobile autonomous mobile robot (AMR) with heterogenous cellular access or a Wi-Fi safety control unit, industry can integrate these wireless technologies today into their logistics, control and manufacturing processes and achieve the desired operational outcomes.

These outcomes are enabled by the new characteristics of Wi-Fi 6/6E such as scheduled & triggered access that provides more deterministic performance akin to 5G and provides:

- Bounded low packet latency
- Controlled packet jitter
- Improved reliability
- Wi-Fi Time-sensitive-network (WTSN) capability

And for use cases that require both determinism AND ultra-high-speed, up to 1.2GHz of spectrum is now accessible with Wi-Fi 6E. This provides multi-Gb/s data rates that key applications such as industrial AR/VR/MR, on-board video and sensor fusion require to be scalable.

So, whether it's operating a fleet of high-tech robots or the more mundane task of collecting TBs of factory floor analytics, Wi-Fi 6 clearly has a prominent place in the future of industrial automation, logistics and by extension mission-critical Enterprise.

The WBA Wi-Fi 6/6E for Industrial IoT group will now carry on and perform real live proof of concepts of the multiple use cases represented above.

The IIoT trials will be kicked-off during 2022, make sure to be involved to benefit from the testing and partnerships to leverage improved competitiveness within the sector.

For more information, do not hesitate in contacting **pmo@wballiance.com**.

REFERENCES

- [Sec 1] Blackhat USA June 2020 Attendee Survey, Cyber Threats in Turbulent Times. **https://i.blackhat.com/docs/usa/2020/P3_28203_BH20_Report.pdf**
- [Sec 2] European Union's cybersecurity agency ENISA statistic reported in the 2021 Europol Serious and Organised Crime Threat Assessment Report.
- [Sec3] United States National Cybersecurity and Communications Integration Center (NCCIC) Industrial Control Systems Cyber Emergency Response Team's (ICS-CERT) 2016 Annual Assessment Report
- [Sec4] Wi-Fi Alliance Easy Connect™ Specification **https://www.wi-fi.org/download.php?file=/sites/default/files/private/Wi-Fi_Easy_Connect_Specification_v2.0.pdf**
- [Sec5] Matter is the foundation for connected things **https://buildwithmatter.com**
- [Sec6] Wi-Fi Alliance WPA3™ Specification **https://www.wi-fi.org/file/wpa3-specification**
- [Sec7] Wi-Fi Alliance® Wi-Fi® Security Roadmap and WPA3™ Updates **https://www.wi-fi.org/download.php?file=/sites/default/files/private/202012_Wi-Fi_Security_Roadmap_and_WPA3_Updates.pdf**
- [Sec8] Analysing WPA3's Dragonfly Handshake **https://wpa3.mathyvanhoef.com**
- [Sec9] Consumer expectations for home Wi-Fi®: The year everything changed **https://www.wi-fi.org/beacon/thomas-derham-nehru-bhandaru/Wi-Fi certified-wpa3-december-2020-update-brings-new-0**
- [Sec10] Wi-Fi Alliance – Discover Wi-Fi **https://www.wi-fi.org/discover-wi-fi/security**
- [Sec11] Consumer expectations for home Wi-Fi®: The year everything changed **https://www.wi-fi.org/beacon/thomas-derham-nehru-bhandaru/Wi-Fi certified-wpa3-december-2020-update-brings-new-protections**
- [Sec12] Wi-Fi Alliance® Security Update **https://www.wi-fi.org/security-update-fragmentation**
- [Sec13] Wi-Fi CERTIFIED WPA3™ Technology Overview (2021) **https://www.wi-fi.org/downloads-registered-guest/Wi-Fi_CERTIFIED_WPA3_Technology_Overview_202101.pdf/35521**
- [Sec14] Wi-Fi Alliance Wi-Fi CERTIFIED Enhanced Open Technology Overview **https://www.wi-fi.org/downloads-registered-guest/Wi-Fi_CERTIFIED_Enhanced_Open_Technology_Overview.pdf/**

- [Sec15] Wi-Fi Alliance Easy ConnectTM Specification **https://www.wi-fi.org/discover-wi-fi/Wi-Fi-easy-connect**
- [Sec16] CyberX Global ICS and IIoT Risk Report, 2019. **https://cdn2.hubspot.net/hubfs/2479124/CyberX%20Global%20ICS%20%2F%20IIoT%20Risk%20Report.pdf**
- [Seg1] Cisco Live – Designing IoT Aware Enterprise **https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2020/pdf/DGTL_BRKENS-1200.pdf**
- [Ind1] BP Carson: Accutech Wireless Instrumentation in Oil Refinery Safety Application," Schneider Electric, Doc. No. TBULM01012-54, November 2011, **https://download.schneider-electric.com/files?p_enDocType=Customer+references&p_File_Name=BP+Carson.pdf&p_Doc_Ref=BP+Carson**
- [Ind2] WBA Wi-Fi 6 Trial – Industrial Manufacturing **https://www.wballiance.com/wp-content/uploads/2020/11/Wi-Fi 6-Trial-Report-Industrial-Manufacturing.pdf**
- [Ind3] W. Duncan, "Top 5 Ways Manufacturers Reduce Materials Cost," LinkedIn, July 11, 2016, **https://www.linkedin.com/pulse/top-5-ways-manufacturers-reduce-material-costs-william-duncan/**
- [Ind4] R. Cox, "25 Ways to Lower Supply Chain Inventory Costs," SupplyChain247, July 28, 2013, **https://www.linkedin.com/pulse/top-5-ways-manufacturers-reduce-material-costs-william-duncan/**
- [Auto1] Ericsson Mobility Report **https://www.ericsson.com/4acd7e/assets/local/mobility-report/documents/2019/emr-november-2019.pdf**
- [Auto2] Ericsson Review – Transforming Transportation with 5G **https://www.ericsson.com/4a61e3/assets/local/reports-papers/ericsson-technology-review/docs/2019/etr-transforming-transportation-with-5g.pdf**
- [Auto3] NXP – 6 reasons why automotive OEMs are upgrading to Wi-Fi 6 **https://www.nxp.com/company/blog/6-reasons-why-automotive-oems-are-upgrading-to-wi-fi-6:BL-6-REASONS-TO-UPGRADE-TO-WI-FI-6**
- [Auto3] EDN - Wi-Fi 6 will streamline automotive connectivity **https://www.edn.com/Wi-Fi-6-will-streamline-automotive-connectivity/**
- [Auto4] Spatial Reuse in IEEE 802.11ax WLANs **https://arxiv.org/pdf/1907.04141.pdf**

- [Auto5] LTE and IEEE 802.11p for vehicular networking: a performance evaluation **https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/1687-1499-2014-89**
- [Auto6] What is IEEE 802.11p? **https://www.everythingrf.com/community/what-is-ieee-802-11p**

ACRONYMS AND ABBREVIATIONS

ACRONYM / ABBREVIATION	DEFINITION
FTM	Fine Timing Measurement
BLE	Bluetooth Low Energy
UWB	Ultra-Wideband
AR	Augmented Reality
VR	Virtual Reality
XR	Extended Reality
MIMO	Multiple-Input-Multiple-Output
MU-MIMO	Multi-user MIMO
BSS	Basic Service Set
SR	Spatial Reuse
QoS	Quality-of-Service
AMR	Autonomous Mobile Robot
AGV	Automated Ground Vehicle
TSN	Time Sensitive Network
IOT	Internet-of-Things
IIOT	Industrial IOT
VPN	Virtual Private Network
CERT	Computer Emergency Response Team
CERT-In	CERT India

WPA	Wi-Fi Protected Access
CCI	Co-channel-interference
WAVE	Wireless Access in Vehicular Environments
ITS	Intelligent Transportation Systems
DSRC	Dedicated Short Range Communications
DPP	Device Provisioning Protocol
UL	Uplink
DL	Downlink
ATSSS	Access Traffic Steering, Switching & Splitting
SLAM	Simultaneous location and mapping
GPS	Global Positioning System
AP	Access Point
GB	Gigabyte
KB	Kilobyte
TWT	Target Wakeup Time
ERP	Enterprise Resource Planning
Mb/s	Megabits per second
GBps	Gigabytes per second
MR	Mixed Reality
E2E	End-to-end
MB/s	Megabytes per second
ML	Machine Learning

STA	Station (endpoint)
ADAS	Advanced Driver Assisted Systems
EV	Electric Vehicle
URLLC	ultra-reliable low latency communication
MLO	Multi-link-operation
FRER	Frame replication and re-assembly
CUC	Centralized User Configuration
CNC	Centralized Network Configuration
SA	Scheduled Access
TB	Trigger-based
CSMA	Carrier sense multiple access
CS	Carrier Sense
RU	Resource Unit
PPDU	Physical layer Protocol Data Unit
U-APSD	Unscheduled-Automatic Power Save Delivery
TXOP	Transmit Opportunity
SP	Service Period
MU-SMPS	multi-user spatial multiplexing power save
CCA	Clear Channel Assessment
PD	Preamble Detect
OBSS	Overlapping BSS
RX	Receive

TX	Transmit
PSDU	Physical Layer Service Data Unit
PLCP	Physical Layer Convergence Protocol
SRG	Spatial Reuse Group
TOS	Type of service
IP	Internet Protocol
DSCP	Differentiated Services Code Point
UP	User Priority
EDCA	Enhanced distributed Channel Access
TID	traffic-identifier
CW	Contention Window
AIFSN	Arbitrated Inter Frame Space Number
HE	High efficiency (802.11ax)
RA	Random access
SAE	Simultaneous Authentication of Equals
HD	High-density/definition
WIP	Work In Progress
MES	Manufacturing Execution Systems
OPC UA	Open Process Control - Unified Architecture
OFDMA	Orthogonal Frequency Division Multiple Access
WBA	Wireless Broadband Alliance
WTSN	Wi-Fi Time Sensitive Network

PARTICIPANT LIST (INCOMPLETE)

NAME	COMPANY	ROLE
Malcolm Smith	Cisco Systems Inc.	Project Leader & Chief Editor
Bryan Wills	Deutsche Telekom	Project Co-Lead
Bahar Sadeghi	Intel Inc.	Project Co-Lead
Dave Green	METTIS Aerospace	Editorial Team
Page Heller	Endpoint Security	Editorial Team
Youssef Abdelilah	American Tower	Editorial Team
Jim Florwick	Cisco Systems Inc.	Editorial Team
Maik Seewald	Cisco Systems Inc.	Editorial Team
Page Heller	Endpoint Security	Editorial Team
A R Balalakshmi	C-DOT	Editorial Team
Gourav Jain	C-DOT	Editorial Team
Carlos Cordeiro	Intel Inc.	Editorial Team
Thomas Derham	Broadcom	Editorial Team
Thomas Steven	American Tower	Project Participant
Fernando Garces	American Tower	Project Participant
Peter Thornycroft	Aruba HPE	Project Participant
Jim Sturges	AT&T	Project Participant
Kevin Franzen	AT&T	Project Participant
Lawrence Masike	BOFINET	Project Participant
Rob McLaughlin	Boingo Wireless	Project Participant
Peter Barany	Boingo Wireless	Project Participant
Kevin Hartle	BT	Project Participant

Steve Dyett	BT	Project Participant
Luther Smith	CableLabs	Project Participant
Loay Kreishan	Charter Communications	Project Participant
Matt MacPherson	Cisco	Project Participant
Mark Grayson	Cisco	Project Participant
Flavio Correa	Cisco	Project Participant
Aravind Balakrishnan	Cisco	Project Participant
Mir Alami	Cisco	Project Participant
Tim O'Brien	Comcast	Project Participant
Jason D. Hintersteiner	Comcast	Project Participant
John Brzozowski	Comcast	Project Participant
Sami Susiaho	Comcast	Project Participant
Deepak Tripathi	CommScope	Project Participant
Jesus Barrios	CommScope	Project Participant
Angelos Mavridis	Deutsche Telekom	Project Participant
Jay Labhart	Endpoint Security	Project Participant
Nataliia Ermakova	ER-Telecom	Project Participant
Djamel Ramoul	iBwave	Project Participant
Karl Ingolf	Intel Corporation	Project Participant
Binita Gupta	Intel Corporation	Project Participant
Necati Canpolat	Intel Corporation	Project Participant
Souma Badombena	Intel Corporation	Project Participant
Azad Singh	Jio	Project Participant
Edward Wincott	Jisc	Project Participant
Mike Richardson	Jisc	Project Participant

Michael Murray	Jisc	Project Participant
Lola Harre	Jisc	Project Participant
Michelle Havard	Keysight Technologies Inc	Project Participant
Ashley Beckford	Keysight Technologies Inc	Project Participant
Jonas Trunk	Linktel	Project Participant
Henrique Gomes	Linktel	Project Participant
Justin Eichenlaub	m3connect	Project Participant
Sergey Gorkov	Maxima Telecom	Project Participant
Livia Rosu	MaxLinear	Project Participant
Satish Mudugere	MaxLinear	Project Participant
Gabor Bajko	MediaTek	Project Participant
Max Riegel	Nokia	Project Participant
Scott Tan	onsemi	Project Participant
Finbarr Coghlan	Orange	Project Participant
Paul Schomburg	Panasonic Avionics	Project Participant
Rolf De Vegt	Qualcomm	Project Participant
Bikas Kar	Rakuten Mobile	Project Participant
George Hart	Rogers	Project Participant
Wael Guibene	Samsung	Project Participant
Sarwar Iqbal	Shaw Communications	Project Participant
Ravi Jain	STL	Project Participant
Les Goldman	Syniverse	Project Participant
Abdullah Caldir	Turk Telekom	Project Participant
Jim Koutras	Viasat	Project Participant
Bruno Tomás	WBA	Project Participant

Tiago Rodrisgues	WBA	Project Participant
Steve Namaseevayum	WBA	Project Participant
Pedro Mouta	WBA	Project Participant