Wireless Universal Serial Bus (Wireless USB)

A Wireless USB (WUSB) is a Universal Serial Bus (USB) built on ultra-wideband (UWB) technology, which uses a radio frequency (RF) link, rather than cables, to transfer information between compatible USB devices.

The USB Implementers Forum, Inc. (USB-IF) discourages the WUSB abbreviation and prefers to reference the term as Certified Wireless USB.

WUSB enables 127-point connections with compatible devices and has a signal radius of three to 10 meters, with signal strength ranging from 480 to 110 Mbps. Security is ensured via transmission encryption.

Key WUSB features include:

- Plug and Play (PnP) compatibility and hot swapping with other devices
- Compatibility with earlier USB versions. However, a Device Wire Adapter (DWA) or WUSB hub is used to to facilitate the wired to wireless transition, enabling the wireless use of USB 2.0 devices and WUSB host connectivity.
- Host capability, which may be used with a PC through a Host Wire Adapter (HWA) that connects to a USB port or the MiniCard Interface
- Support of a dual-role device (DRD), which works as a WUSB device, as well as a host with several features
- Like any successful standard, USB, Universal Serial Bus has kept pace with technology and the standard has been updated seeing USB 1, USB 1.1, USB2, USB3 and then USB 3.1, USB 3.2 and then USB 4.
- Each successive USB standard has added more to the technology, improving and refining the performance.
- With the use of USB being so widespread, backwards compatibility as far as is possible is very important, along with a future upgrade path.

- It is sometimes useful to compare USB1, vs USB 2, or USB2 vs USB3 etc looking at the different capabilities and specifications of each USB version.

USB Implementers Forum

- In order to ensure that USB is an industry standard and not one that is a standard for a particular manufacturer, the USB standard is developed and maintained by the USB Implementers Forum, USB-IF.
- This is a non-profit corporation that has been founded by the companies that developed the USB standard and now want to use and develop it.
- Some of the member companies for the USB-IF include companies such as Hewlett Packard, Intel, LSI Corporation, Renesas, Microsoft, etc..
- The USB Implementers Forum develops and maintains the USB standards, including Wireless USB and runs a compliance programme to maintain the quality of USB products and ensure compatibility between devices.

ZIGBEE

Zigbee is a wireless technology developed as an open global standard to address the unique needs of low-cost, low-power wireless IoT networks. The Zigbee standard operates on the IEEE 802.15.4 physical radio specification and operates in unlicensed bands including 2.4 GHz, 900 MHz and 868 MHz.

The 802.15.4 specification upon which the Zigbee stack operates gained ratification by the Institute of Electrical and Electronics Engineers (IEEE) in 2003. The specification is a packet-based radio protocol intended for low-cost, battery-operated devices. The protocol

allows devices to communicate in a variety of network topologies and can have battery life lasting several years.

The Zigbee 3.0 Protocol

The Zigbee protocol has been created and ratified by member companies of the Zigbee Alliance.Over 300 leading semiconductor manufacturers, technology firms, OEMs and service companies comprise the Zigbee Alliance membership. The Zigbee protocol was designed to provide an easy-to-use wireless data solution characterized by secure, reliable wireless network architectures.

ZIGBEE ADVANTAGE

The Zigbee 3.0 protocol is designed to communicate data through noisy RF environments that are common in commercial and industrial applications. Version 3.0 builds on the existing Zigbee standard but unifies the market-specific application profiles to allow all devices to be wirelessly connected in the same network, irrespective of their market designation and function. Furthermore, a Zigbee 3.0 certification scheme ensures the interoperability of products from different manufacturers. Connecting Zigbee 3.0 networks to the IP domain opens up monitoring and control from devices such as smartphones and tablets on a LAN or WAN, including the Internet, and brings the true Internet of Things to fruition.

Zigbee protocol features include:

- Support for multiple network topologies such as point-to-point, point-to-multipoint and mesh networks
- Low duty cycle – provides long battery life
- Low latency
- Direct Sequence Spread Spectrum (DSSS)
- Up to 65,000 nodes per network

- 128-bit AES encryption for secure data connections
- Collision avoidance, retries and acknowledgements

The Zigbee 3.0 software stack incorporates a 'base device' that provides consistent behavior for commissioning nodes into a network. A common set of commissioning methods is provided, including Touchlink, a method of proximity commissioning.

Zigbee 3.0 provides enhanced network security. There are two methods of security that give rise to two types of network:

- Centralized security: This method employs a coordinator/trust center that forms the network and manages the allocation of network and link security keys to joining nodes.
- Distributed security: This method has no coordinator/trust center and is formed by a router. Any Zigbee router node can subsequently provide the network key to joining nodes.

Nodes adopt whichever security method is used by the network they join. Zigbee 3.0 supports the increasing scale and complexity of wireless networks, and copes with large local networks of greater than 250 nodes. Zigbee also handles the dynamic behavior of these networks (with nodes appearing, disappearing and re-appearing in the network) and allows orphaned nodes, which result from the loss of a parent, to re-join the network via a different parent. The self-healing nature of Zigbee Mesh networks also allows nodes to drop out of the network without any disruption to internal routing.

The backward compatibility of Zigbee 3.0 means that applications already developed under the Zigbee Light Link 1.0 or Home Automation 1.2 profile are ready for Zigbee 3.0. The Smart Energy profile is also compatible with Zigbee 3.0 at the functional level, but Smart Energy has additional security requirements that are only addressed within the profile.

Zigbee's Over-The-Air (OTA) upgrade feature for software updates during device operation ensures that applications on devices already deployed in the field can be seamlessly migrated to Zigbee 3.0. OTA upgrade is an optional functionality that manufacturers are encouraged to support in their Zigbee products.

Mesh Networks

A key component of the Zigbee protocol is the ability to support mesh networking. In a mesh network, nodes are interconnected with other nodes so that multiple pathways connect each node. Connections between nodes are dynamically updated and optimized through sophisticated, built-in mesh routing table.

Mesh networks are decentralized in nature; each node is capable of self-discovery on the network. Also, as nodes leave the network, the mesh topology allows the nodes to reconfigure routing paths based on the new network structure. The characteristics of mesh topology and ad-hoc routing provide greater stability in changing conditions or failure at single nodes.

Zigbee Applications

Zigbee enables broad-based deployment of wireless networks with low-cost, low-power solutions. It provides the ability to run for years on inexpensive batteries for a host of monitoring and control applications. Smart energy/smart grid, AMR (Automatic Meter Reading), lighting controls, building automation systems, tank monitoring, HVAC control, medical devices and fleet applications are just some of the many spaces where Zigbee technology is making significant advancements.

6LoWPAN

The 6LoWPAN system is used for a variety of applications including wireless sensor networks. This form of wireless sensor network sends data as packets and using IPv6 - providing the basis for the name - IPv6 over Low power Wireless Personal Area Networks.

6LoWPAN provides a means of carrying packet data in the form of IPv6 over IEEE 802.15.4 and other networks. It provides end-to-end IPv6 and as such it is able to provide direct connectivity to a huge variety of networks including direct connectivity to the Internet.

In this way, 6LoWPAN adopts a different approach to the other low power wireless sensor network solutions.

6LoWPAN and IETF

6LoWPAN is an open standard defined by the Internet Engineering Task Force, IETF in their document RFC 6282. The IETF is the standards body that defines many of the open standards used in the Internet including HTTP, TCP, UDP and many others.

Whilst 6LoWPAN was originally conceived to build on top of IEEE 802.15.4, a standard that set out the lower layers for a 2.4 GHz low power wireless system, it is now being developed and adapted to work with many other wireless bearers including Bluetooth Smart; power line control, PLC, and low power Wi-Fi.

The 6LoWPAN group have then defined the encapsulation and compression mechanisms that enable the IPv6 data to be carried of the wireless network.

The development of the 6LoWPAN system was not as easy as might be thought as the basic natures of the two systems are very different. However it was believed that using packet data over a low power wireless sensor network would offer significant advantages in terms of data handling and management.

6LoWPAN application areas

With many low power wireless sensor networks and other forms of ad hoc wireless networks, it is necessary that any new wireless system or technology has a defined area which it addresses. While there are many forms of wireless networks including wireless sensor networks, 6LoWPAN addresses an area that is currently not addressed by any other system, i.e. that of using IP, and in particular IPv6 to carry the data.

The overall system is aimed at providing wireless internet connectivity at low data rates and with a low duty cycle. However there are many applications where 6LoWPAN is being used:

- ***General Automation:*** There are enormous opportunities for 6LoWPAN to be used in many different areas of automation.
- ***Home automation:*** There is a large market for home automation. By connecting using IPv6, it is possible to gain distinct advantages over other IoT systems. The Thread initiative has been set up to standardize on a protocol running over 6LoWPAN to enable home automation.
- ***Smart Grid:*** Smart grids enable smart meters and other devices to build a micro mesh network and they are able to send the data back to the grid operator's monitoring and billing system using the IPv6 backbone.
- ***Industrial monitoring:*** Automated factories and industrial plants provide a great opportunity for 6LoWPAN and using automation, can enable major savings to be made. The ability of 6LoWPAN to connect to the cloud opens up many different areas for data monitoring and analysis.

6LoWPAN basics

The 6LoWPAN technology utilises IEEE 802.15.4 to provide the lower layers for this low power wireless network system. While this seems a straightforward approach to the development of an packet data wireless network or wireless sensor network, there are incompatibilities between IPv6 format and the formats allowed by IEEE 802.15.4. This differences are overcome within 6LoWPAN and this allows the system to be used as a layer

over the basic 802.15.4.

In order to send packet data, IPv6 over 6LowPAN, it is necessary to have a method of converting the packet data into a format that can be handled by the IEEE 802.15.4 lower layer system.

IPv6 requires the maximum transmission unit (MTU) to be at least 1280 bytes in length. This is considerably longer than the IEEE802.15.4's standard packet size of 127 octets which was set to keep transmissions short and thereby reduce power consumption.

To overcome the address resolution issue, IPv6 nodes are given 128 bit addresses in a hierarchical manner. The IEEE 802.15.4 devices may use either of IEEE 64 bit extended addresses or 16 bit addresses that are unique within a PAN after devices have associated. There is also a PAN-ID for a group of physically co-located IEEE802.15.4 devices.

6LoWPAN security

It is anticipated that the Internet of Things, IoT will offer hackers a huge opportunity to take control of poorly secured devices and also use them to help attack other networks and devices.

Accordingly security is a major issue for any standard like 6LoWPAN, and it uses AES-128 link layer security which is defined in IEEE 802.15.4. This provides link authentication and encryption.

Further security is provided by the transport layer security mechanisms that are also included. This is defined in RFC 5246 and runs over TCP.

For systems where UDP is used the transport layer protocol defined under RFC 6347 can be used, although this may require some specific hardware requirements.

6LoWPAN interoperability

One key issue of any standard is that of interoperability. It is vital that equipment from

different manufacturers operates together.

When testing for interoperability, it is necessary to ensure that all layers of the OSI stack are compatible. To ensure that this can be achieved there several different specifications that are applicable.

Any item can be checked to conform it meets the standard, and also directly tested for interoperability.

6LoWPAN is a wireless / IoT style standard that has quietly gained significant ground. Although initially aimed at usage with IEEE 802.15.4, it is equally able to operate with other wireless standards making it an ideal choice for many applications.

6LoWPAN uses IPv6 and this alone has to set it aside from the others with a distinct advantage. With the world migrating towards IPv6 packet data, a system such 6LoWPAN offers many advantages for low power wireless sensor networks and other forms of low power wireless networks.

Wireless HART

WirelessHART uses a **2.4 GHz band**—license-free and used worldwide—as a transfer medium for several radio technologies, including WLAN, Bluetooth, and ZigBee. But, **WirelessHART** is much more than a WLAN variant.

WirelessHART uses a **flat mesh network** where all radio stations (field devices) form a network. Every participating station serves simultaneously as a **signal source** and a **repeater**. The original transmitter sends a message to its nearest neighbor, which passes the message on until the message reaches the base station and the actual receiver. In addition, **alternative routes** are set up in the initialization phase. If the message cannot be transmitted on a particular path, due to an obstacle or a defective receiver, the message is automatically passed to an alternative route. So, in addition to extending the range of the

network, the **flat mesh network** provides redundant communication routes to increase reliability.

The communication in the **Wireless Network** is coordinated with TDMA (Time Division Multiple Access), which synchronizes the network participants in 10 ms timeframes. This enables a very reliable (collision-free) network, and reduces the lead and lag times during which a station must be active.

To avoid jamming, **WirelessHART** uses also FHSS (Frequency Hopping Spread Spectrum). All 15 channels as defined in IEEE802.15.4 are used in parallel; **WirelessHART** uses FHSS to "hop" across these channels. Channels that are already in use are blacked out to avoid collisions with other wireless communication systems.

The combination of 10s synchronization and 15 channels allows 1500 communications per second.

WirelessHART is a wireless communications protocol for process automation applications. It adds wireless capabilities to HART technology while maintaining compatibility with existing HART devices, commands, and tools. WirelessHART uses mesh networking technology. Each device in a mesh network can serve as a router for messages from other devices. In other words, a device doesn't have to communicate directly to a gateway, but just forward its message to the next closest device. This extends the range of the network and provides redundant communication routes to increase reliability, particulalry in the difficult radio environment found in process facilities.

Each WirelessHART network includes three main elements:

- Wireless field devices connected to process or plant equipment. This device could be a device with WirelessHART built in or an existing installed HART-enabled device with a WirelessHART adapter attached to it.

- Gateways enable communication between these devices and host applications connected to a high-speed backbone or other existing plant communications network.
- A Network Manager is responsible for configuring the network, scheduling communications between devices, managing message routes, and monitoring network health. The Network Manager can be integrated into the gateway, host application, or process automation controller.