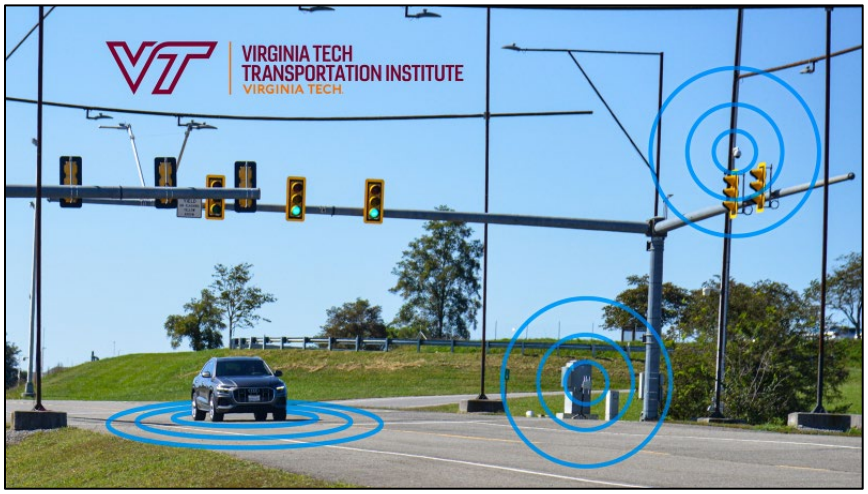
Introduction to Communications in Transportation

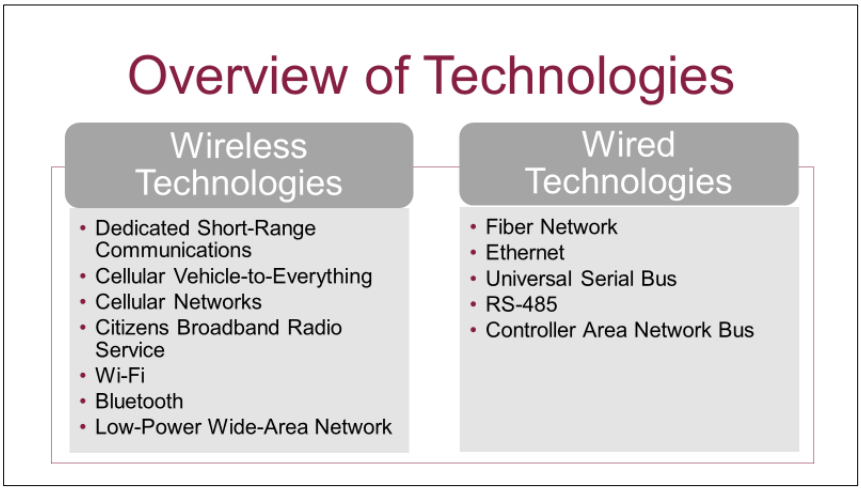


UNIT 1 – Introduction

MODULE 1 – Introduction to ITS

Overview

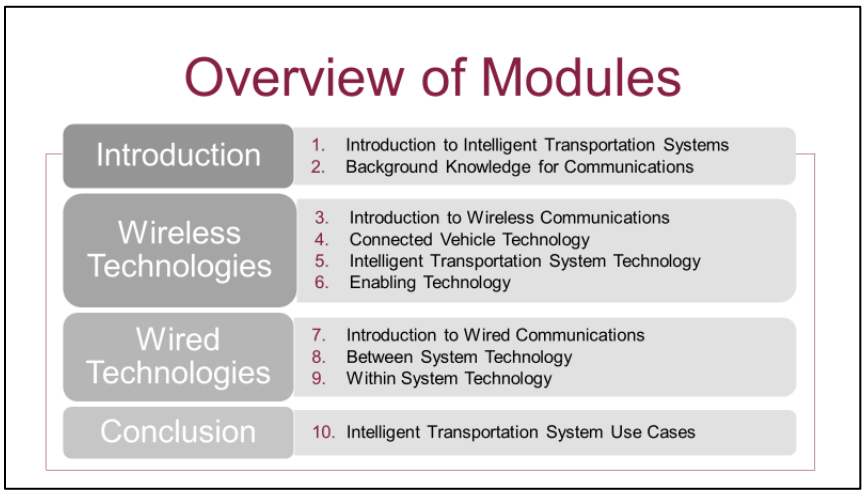
Overview of Technologies



Welcome to the Introduction to Communications in Transportation Training Program. This training provides a high-level overview of the types of communications that support intelligent transportation systems, traffic management, and connected vehicle environments. Some real-world applications of each type of communication are also discussed.

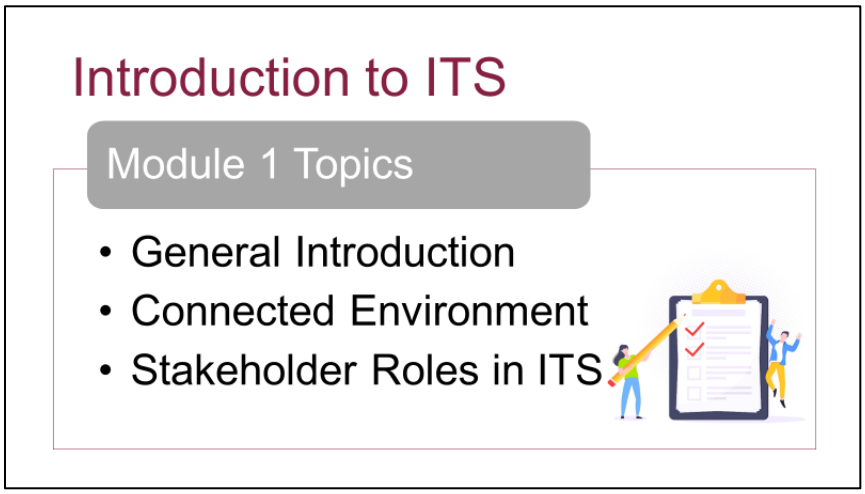
In the coming segments, we will review the most relevant wireless and wired technologies that can support information exchange in the connected transportation environment. This content was compiled in early 2022, and some information may have since changed in this rapidly evolving market. For wireless technologies, we will discuss Dedicated Short-Range Communications (known as DSRC), Cellular Vehicle-to-Everything (known as C-V2X), Cellular Networks, Citizens Broadband Radio Service (known as CBRS), Wi-Fi, Bluetooth, and Low-Power Wide-Area Network (known as LPWAN). For wired technologies, we will discuss Fiber Networks, Ethernet, Universal Serial Bus (known as USB), RS-485, and Controller Area Network Bus (known as CAN Bus).

Overview of Modules



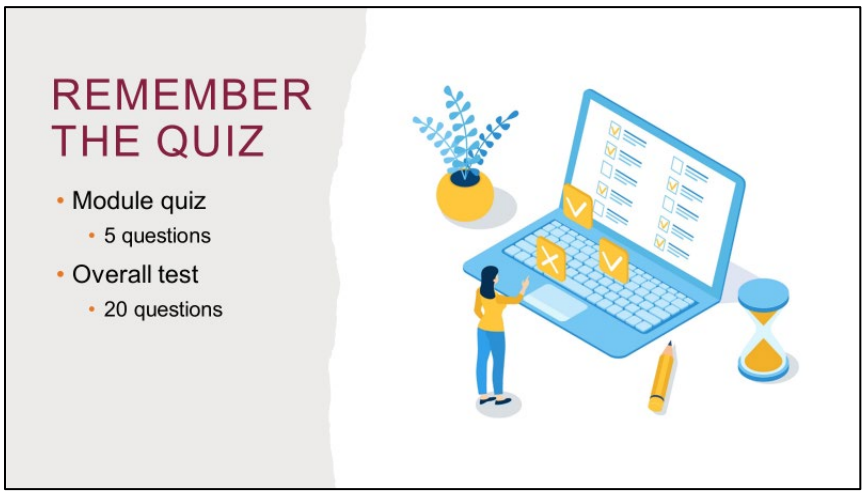
These technologies will be covered in a series of module units that include an Introduction followed by Wireless Technologies, Wired Technologies, and a Conclusion.

Introduction to ITS



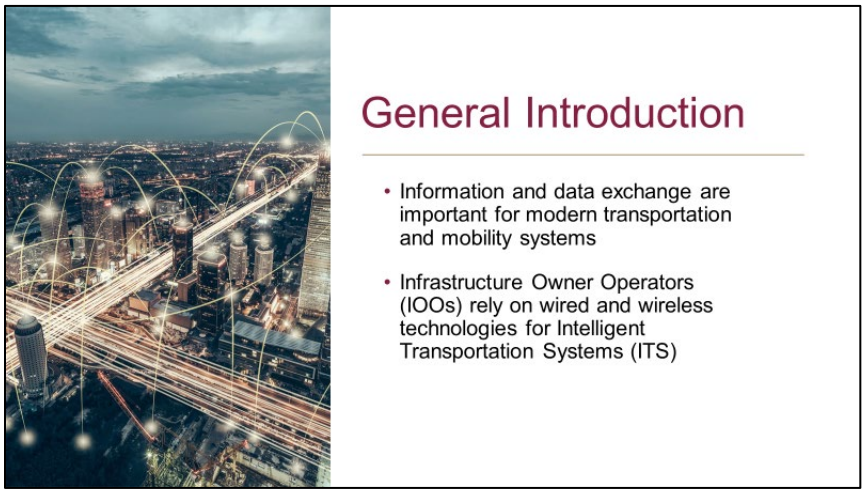
In Module 1 - Introduction to ITS, we will cover a general introduction to wired and wireless technology and the benefits of Intelligent Transportation Systems (known as ITS). We will then discuss what a connected environment is and the types of communications that occur between various actors. Lastly, we will touch on the roles of stakeholders in ITS.

Remember the Quiz



Remember, there is a quiz at the end of each module with five questions for you to answer. At the end of the training, there will be an overall test with 20 questions.

General Introduction

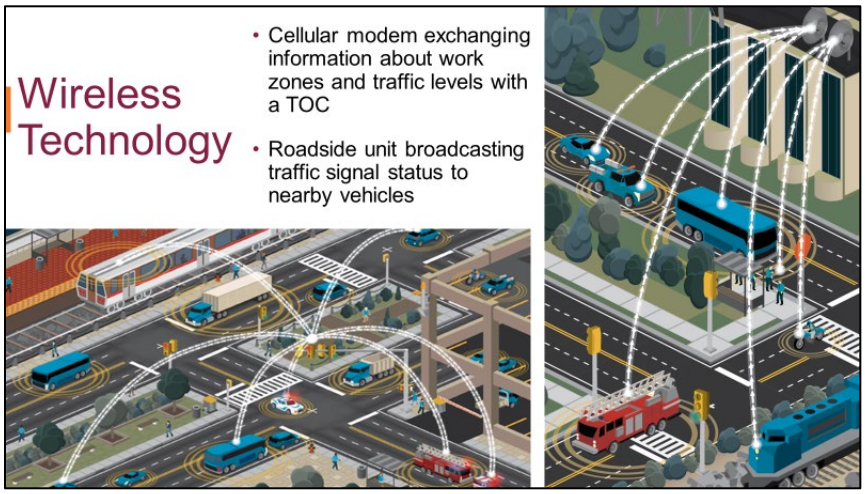


Information and data exchange are becoming increasingly important for improving the quality of operations and safety in modern transportation and mobility systems. Infrastructure Owner Operators (or IOOs) such as Departments of Transportation, as well as metropolitan areas and local communities rely more and more on these technologies to control and monitor their Intelligent Transportation Systems (or ITS). Today's intelligent transportation systems can utilize a combination of these communication technologies in their deployments.

Wired Technology

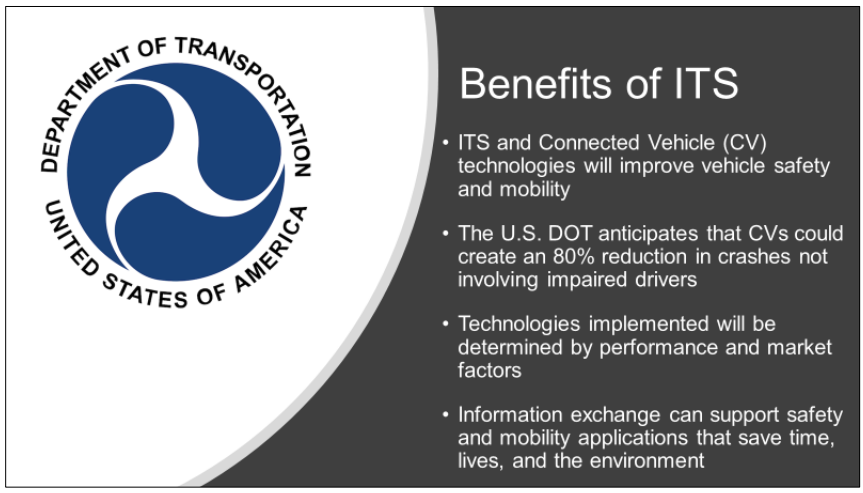
Examples of wired communication technology include a fiberoptic cable providing connectivity between a traffic signal controller at an intersection and a central traffic signal control system in a Traffic Operations Center (also known as a TOC). Another example is an ethernet cable that connects a camera at an intersection to a video processing unit located in an intersection cabinet.

Wireless Technology



Examples of wireless communications technology include a cellular modem exchanging real-time information about work zones and traffic levels with a TOC and a roadside radio unit broadcasting the traffic signal status from an intersection to nearby vehicles.

Benefits of ITS



Current research suggests that Intelligent Transportation Systems and Connected Vehicle (or CV) technologies will improve safety and mobility. For example, the United States Department of Transportation (or DOT) anticipates that connected vehicle technologies could create an 80% reduction in crashes not involving impaired drivers (1). However, connected vehicle technologies largely remain in research and early deployment stages. The technologies broadly implemented in the future will be determined by technical performance and market factors such as cost, user acceptance, and regulation.

The advent of both connected and automated vehicle technologies has facilitated information exchange between vehicles and other connected devices, including vehicles, infrastructure elements such as traffic signals, and even pedestrians. This information exchange can support an even broader range of safety and mobility applications that have the potential to save time, lives, and the environment.

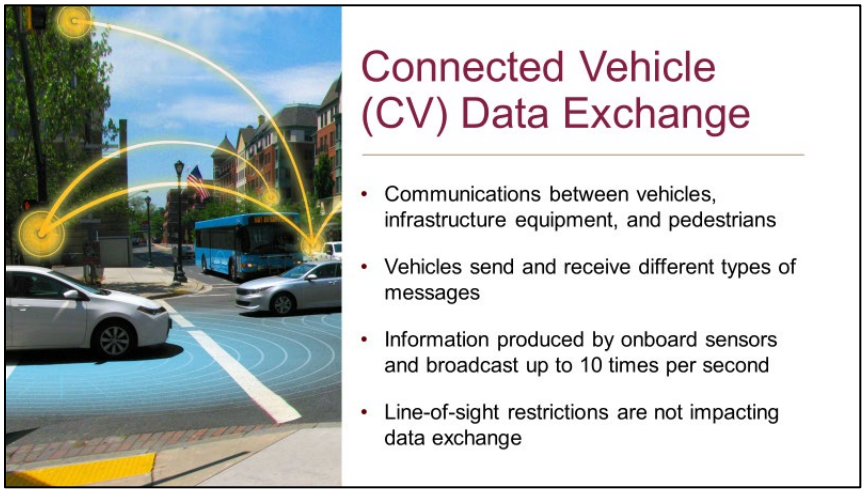
Connected Environment

Developing a Driving Environment

Traditionally, vehicles have relied on the driver to sense and interpret the driving environment. The effectiveness of the driver in this role varies widely based on human factors such as age, experience, drowsiness, distraction, and physical traits, in addition to environmental factors such as weather, lighting, and the density of the surrounding traffic. Drivers can misjudge or misinterpret cues that influence decision-making at critical moments, which may lead to crashes. Additionally, when the driver perceives these cues quickly and accurately, there can still be variability in the driver's cognitive decision-making process and evasive maneuver execution.

Over the last decade, vehicles have increasingly been equipped with Advanced Driver Assistance Systems (ADAS) that utilize sensors such as cameras, radar, and ultrasonic sensors to interpret the environment and notify the driver of potential collisions. In more advanced vehicles, the systems may automatically respond by applying steering and/or braking on behalf of the driver to avoid collision or reduce severity. While these onboard sensing systems are often more reliable and effective than a human driver, their accuracy may also be affected by line-of-sight restrictions or sensor range limitations.

Connected Vehicle (CV) Data Exchange

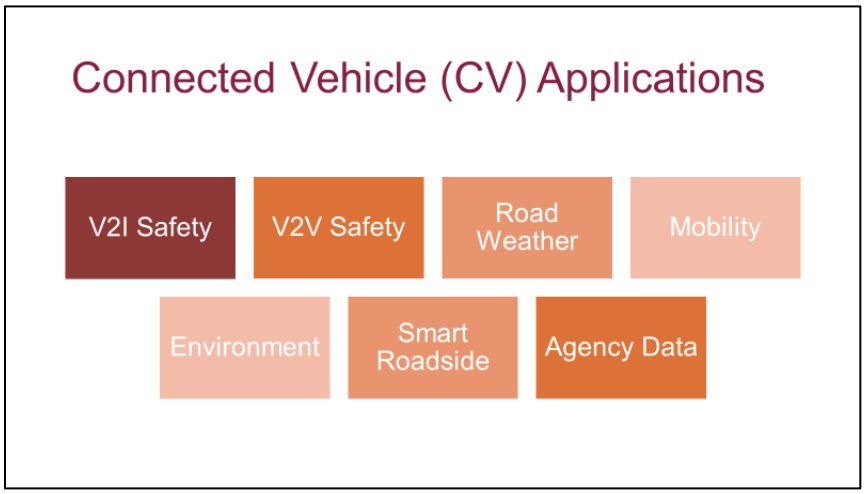


In a connected environment, vehicles are equipped with special radios allowing them to communicate with other vehicles, infrastructure equipment, and pedestrians when those actors are also similarly equipped. This

information is produced by highly accurate onboard sensors, and the radios are used to exchange information about vehicle characteristics, location, and path. In this environment, vehicles send and receive different types of messages that can be categorized according to the type of actor the vehicle is exchanging information with.

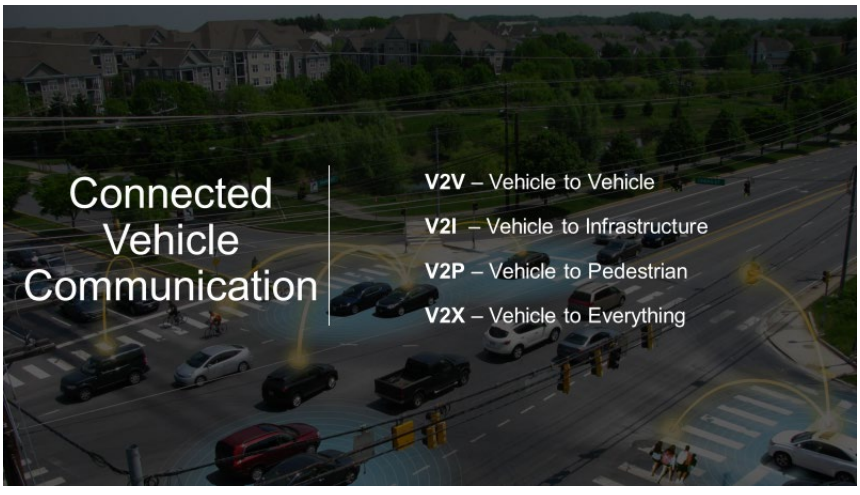
These messages are broadcast to other actors up to 10 times per second. These systems can exchange messages with many nearby vehicles without being affected by line-of-sight restrictions. This allows the vehicle's system to effectively detect presence or "see through" other vehicles and around corners, enabling it to better anticipate collisions and enact automatic measures to intervene.

Connected Vehicle (CV) Applications



A variety of applications can use the information transmitted between connected vehicles and connected devices to improve safety and traffic flow. Applications include those we have already mentioned plus a wide range of applications that address safety, mobility, and environmental issues. The frequency and accuracy of the exchanged data allows the connected applications to achieve significantly better outcomes than what can be achieved by unaided human drivers or through vehicle systems that only use their own onboard sensors.

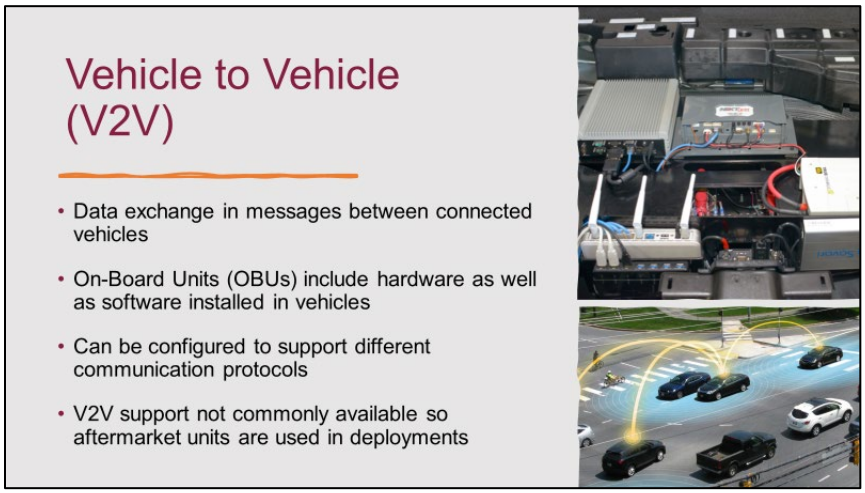
Connected Vehicle Communication



Some acronyms reflecting communications between vehicles and different actors are now commonly used. Vehicle-involved communications in a connected environment include V2V for Vehicle to Vehicle, V2I for Vehicle to Infrastructure, V2P for Vehicle to Pedestrian, and V2X for Vehicle to Everything. It's worth noting

that in the future, automated vehicles will also benefit from these information exchanges as they seek to interpret the status and intent of other nearby road users and infrastructure beyond the range of their own sensors. Next, we will discuss the communication modalities in more detail.

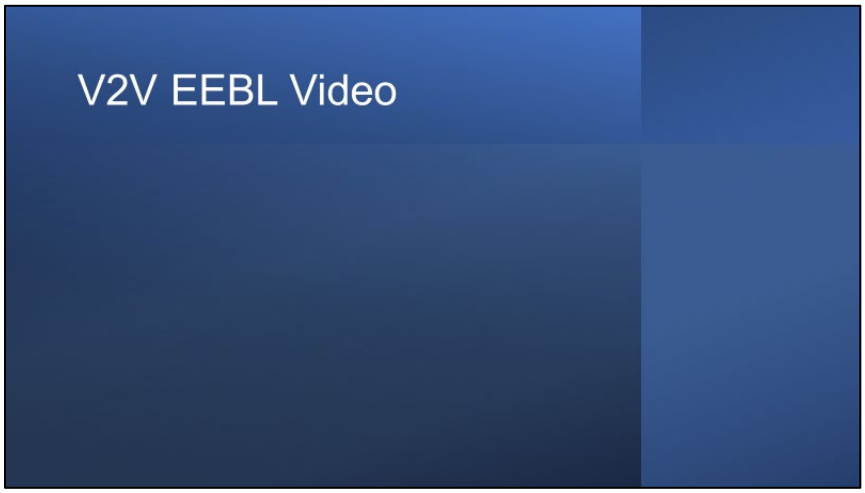
Vehicle to Vehicle



When data is exchanged in messages directly from one connected vehicle to another, the communication is referred to as Vehicle to Vehicle (or V2V, for short).

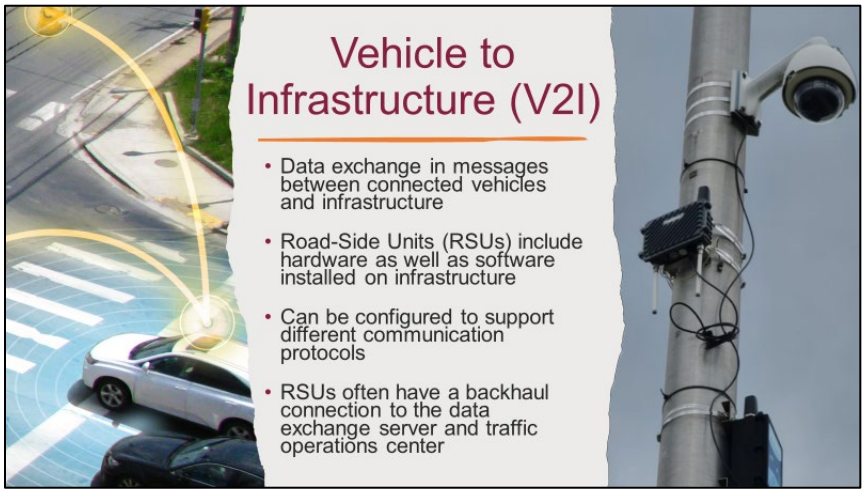
V2V communications are made possible by what is commonly known an On-Board Unit (or OBU) installed in the vehicle. The term On-Board Equipment (or OBE) refers to the physical radio hardware, antenna, and accompanying software that enables the transfer of information between vehicles to support connected vehicle applications. However, since the term OBU is more commonly used, we will refer to the equipment using that terminology. OBUs can be configured to support many types of wireless communication protocols, and each has its own unique strengths and weakness. These protocols will be defined and contrasted in more detail later in this training in Modules 4 and 5. OBUs that support V2V are not commonly available in production vehicles yet, so current deployments utilize aftermarket OBUs, which results in systems that are not always fully integrated into the vehicle's instrument panel or advanced driver assist systems.

V2V EEBL Video



One V2V application enabled by communication between connected vehicles is called Emergency Electronic Brake Lights (EEBL). In this scenario, lead Vehicle A is travelling ahead of semitruck Vehicle B with following Vehicle C. When Vehicle A begins to rapidly decelerate, the EEBL application broadcasts a hard braking event in its Basic Safety Message (or BSM) along with standard details such as speed, location, and brake status. The surrounding vehicle OBUs that receive BSMs from Vehicle A determine the relevance to their paths of travel and provide an in-vehicle warning to the driver, if applicable.

Vehicle to Infrastructure

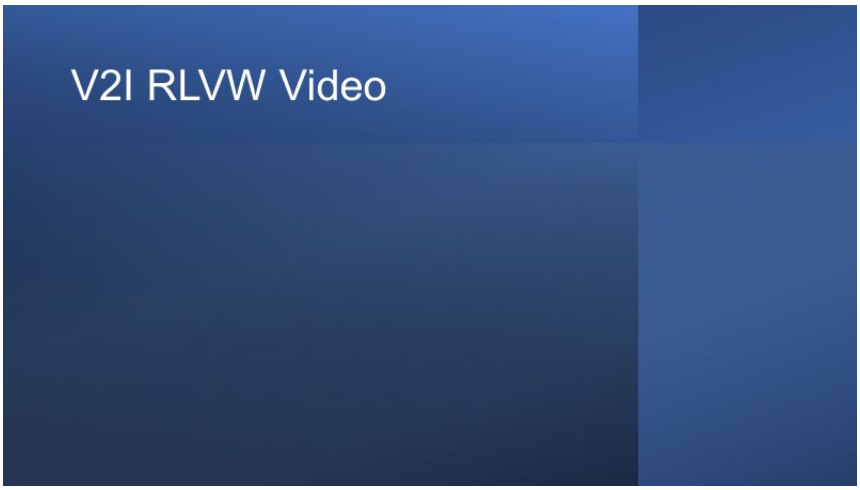


Messages passed between connected vehicles and connected infrastructure elements are referred to as vehicle to infrastructure (or V2I, for short).

V2I communications are made possible by Road-Side Units (known as an RSU), which are hardware and accompanying software installed on roadside infrastructure such as traffic light poles or mast arms with enough elevation to avoid line-of-sight interference. The term Road-Side Equipment (or RSE) refers to the physical radio hardware, antenna, and accompanying software that enables the transfer of information to support connected applications. However, since RSU is more commonly used, we will refer to the equipment using that terminology.

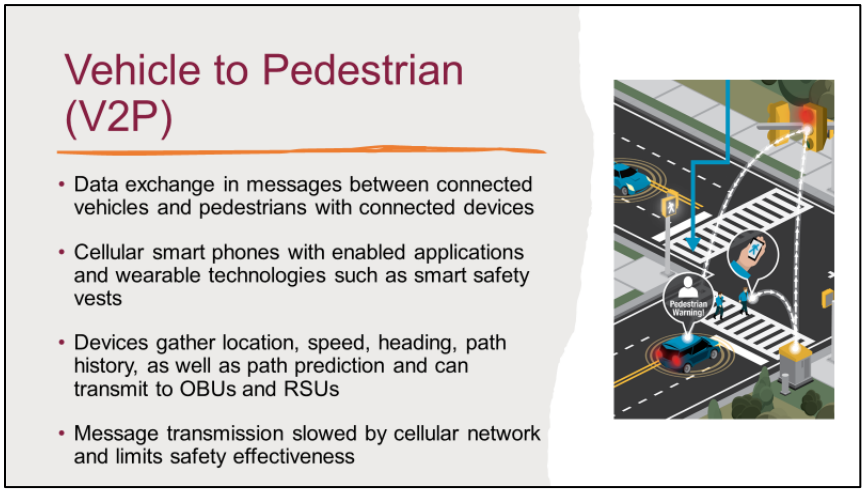
In some cases, such as along a section of freeway, RSUs may be installed on custom poles, gantries, or other infrastructure. On arterials and urban streets, RSUs would typically be deployed on street light poles or mast arms. RSUs may be powered using a Power over Ethernet (PoE) interface that allows data and power to be transmitted simultaneously via an ethernet cable. Like the OBU, an RSU can also be configured to support a variety of communications protocols. These protocols will be further defined and contrasted later in this training in Modules 4 and 5. RSUs are often connected to other equipment located in a roadside cabinet and typically include a backhaul connection to a data exchange server and TOC.

V2I RLVW Video



A V2I application enabled by connected technology is Red Light Violation Warning (RLVW). In this scenario, RSUs at an intersection broadcast signal status data to approaching vehicles through Signal Phasing and Timing (SPaT) messages. The OBU on the vehicle receives the SPaT messages which provide information about when the lights will change status. The OBU can provide a warning to the driver if they are approaching a light that is about to turn red or if they are not reacting to stop when the light has already turned red. At the same time, BSMs transmitted to the RSU at the intersection and can be used to extend a red-light phase at opposing approaches if a vehicle is not going to stop for a red light.

Vehicle to Pedestrian



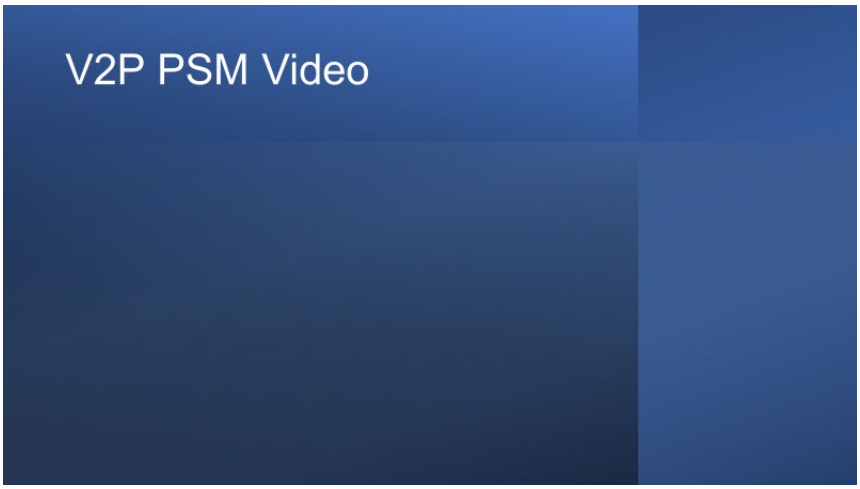
Data can also be exchanged between connected vehicles and pedestrians who are equipped with a connected device such as a smart phone. This data exchange is called vehicle to pedestrian (known as V2P). At this time, V2P data exchange is less mature and widespread than V2V and V2I, but as connected vehicle technologies continue to evolve, it is anticipated that V2P will be more broadly implemented.

V2P communications are enabled by mobile devices carried by vulnerable road users such as pedestrians, cyclists, and construction workers. These devices include cellular smart phones equipped with applications to communicate in a connected environment and wearable technologies such as smart safety vests designed for roadside workers. The cost, weight, and power requirements of V2P technologies have limited their

application thus far but as technology advance, it is anticipated that pedestrian devices that can support V2P communication will become mainstream.

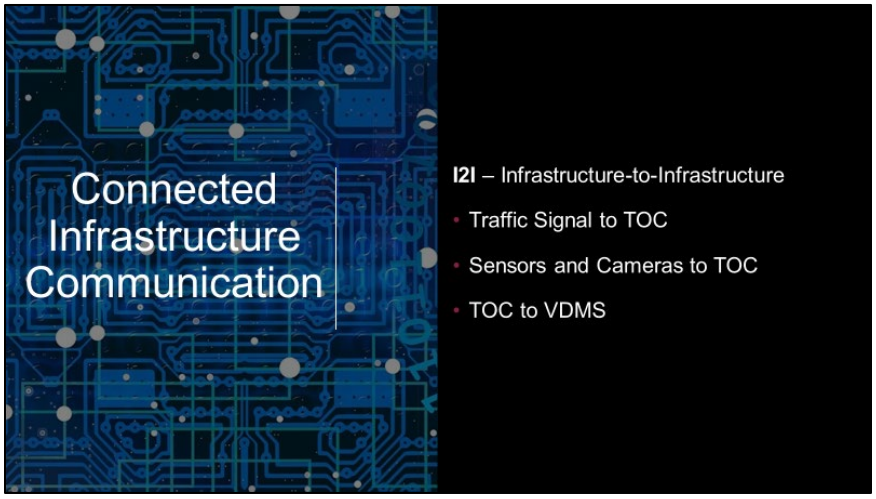
Mobile devices can gather information such as location, speed, heading, path history, and path prediction for the pedestrian and can transmit this information to OBUs and RSUs. However, mobile devices must use the cellular network, which means the data will be transmitted through a cell tower to a mobile network carrier. While the commercial networks have significantly improved their coverage, speed, and reliability, routing the message traffic through their networks causes message transmission to be slower, which can limit the effectiveness of safety-related applications that are extremely time-critical. Messaging under this type of exchange, referred to as Personal Safety Messages (or PSMs), are included in the current automotive engineering standards but require further development and testing.

V2P PSM Video



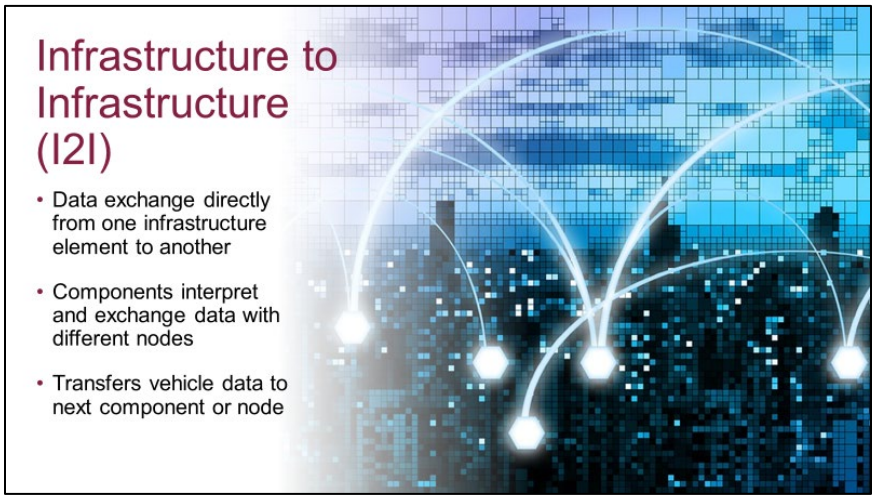
A future V2P application enabled by connectivity is a Pedestrian Warning Message (or PSM). In this scenario, as a connected vehicle travels down the roadway, it transmits it's BSM to RSUs at nearby intersections. A pedestrian waiting to cross at a signalized intersection broadcasts a PSM to the nearby RSU. The RSU transmits details of the PSM to the vehicle OBU which can be used to alert the driver. The pedestrian can also receive an indication that it's safe to cross the intersection through their smart phone device.

Connected Infrastructure Communication



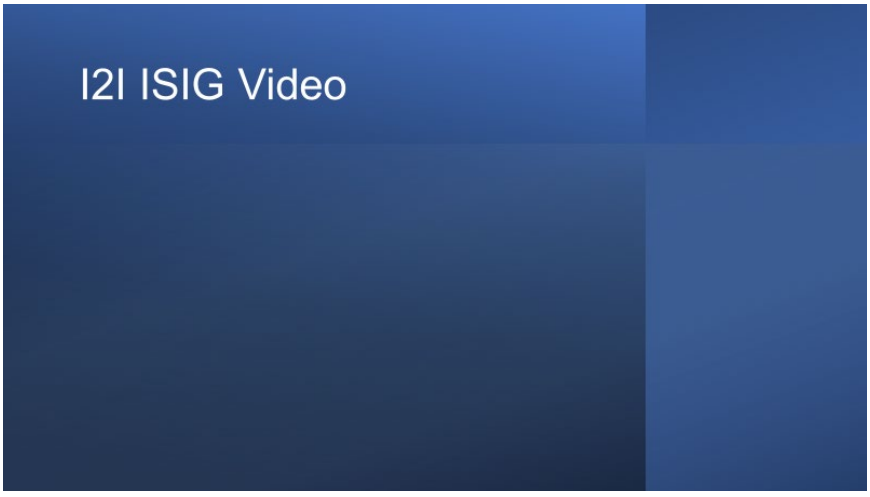
Communications between different infrastructure components and nodes in a connected environment is known as I2I for Infrastructure-to-Infrastructure. This communication includes ITS systems such as traffic signal controllers communicating with TOCs via a fiber network or via a wireless connection such as mesh or 4G. Additionally, applications within a TOC receive information from deployed technologies such as environmental sensors, work zones, side-fire radar, and CCTV for roadway monitoring. Infrastructure connections also allow for information to be distributed from a TOC to road users via a Virtual Dynamic Message Sign (VDMS).

Infrastructure to Infrastructure



I2I communication allows infrastructure components including sensors, cameras, and RSUs to interpret and exchange data with other nodes so information can be relayed across the network. These infrastructure components receive data from passing motor vehicles and the environment to effectively transfer the information to the next infrastructure component or node. Not every infrastructure end point can be easily or reasonably accessed with a wired connection so wireless solutions can supplement this by extending the range and functionality of the overall communication network.

I2I ISIG Video



An example I2I application is the Intelligent Traffic Signal System (ISIG). This uses vehicle location and movement data transmitted to RSUs via BSMs. RSUs installed at intersections along a stretch of arterial roadway also share their Signal Phase and Timing (SPaT) information with each other. The information allows

for signal timing to be adjusted allowing for improved traffic flow at a single intersection or series of intersections.

Stakeholder Roles in ITS

Intelligent transportation systems are enabled by three main stakeholder groups, Infrastructure Owner Operators (IOOs), Original Equipment Manufacturers (OEMs), and Third-Party Navigation Application Providers. These groups are intertwined and increasingly reliant on wired and wireless technologies to operate their telematics and intelligent transportation systems. The technology required to fully implement a connected vehicle ecosystem has been available and proven for more than a decade. However, widespread deployment has yet to materialize due to a number of factors including cost of equipment, competing radio technologies, and regulatory uncertainty. Let's explore how these factors affect each of the stakeholders.

Infrastructure Owner Operators (IOOs)

Infrastructure Owner Operators (commonly DOTs, local municipalities, or tribal governments) are responsible for providing safe and efficient transportation infrastructure and services for their citizens. Currently, most IOOs use both wireless and wired communications to control and monitor their deployed infrastructure technology such as traffic signals, traffic management, and traffic surveillance systems through TOCs. These same infrastructure components can be used to generate and exchange transportation-related data between their connected roadside infrastructure and vehicles equipped with the necessary technologies to improve safety and the quality of their operations. For these reasons, most IOOs are interested in using connected

infrastructure systems and have made some investment in the deployment of connected vehicle testbeds or pilot environments to learn about what it takes to deploy and maintain the technology. However, until there are significant numbers of connected vehicles on the road to communicate with, it will be difficult to justify the cost of further implementation.

Original Equipment Manufacturers (OEMs)

Original equipment manufacturers (OEMs) are private automobile manufacturers that design and produce vehicles with advanced driver assistance systems, connected vehicle applications, and fully or partially automated driving capabilities that may rely on connected infrastructure sometime in the future.

OEMs have been testing and validating connected vehicle equipment and applications for years, and they acknowledge the potential safety benefits those technologies can provide. However, most OEMs struggle to justify the addition of connected technology to the vehicle at this initial phase as there are not enough other equipped vehicles, infrastructure, or pedestrians to interact with. Consumers will not recognize the potential benefits until there is sufficient market penetration of these solutions. The average age of a vehicle on the road in the US is 12 years (2). If the federal government mandated connected vehicle systems on all new production vehicles, it would take 12 years to realize the benefits and almost 25 years for the entire vehicle fleet to be equipped.

In addition, IOOs such as state DOTs are a broad and fragmented sector, and not all of them are planning to implement connected vehicle solutions at the same time, for the same purposes, or in the same way. Therefore, the lack of standardization and commonality of approach has left OEMs unable to count on IOOs to have infrastructure-based solutions deployed that will be interoperable and behave in the same way from jurisdiction to jurisdiction. The result is that OEMs have been reluctant to incorporate advanced infrastructure supported connected technologies into their vehicles unless those applications can be broadly deployed without additional customization to allow interoperability across all environments.

Third-Party Navigation Application Providers

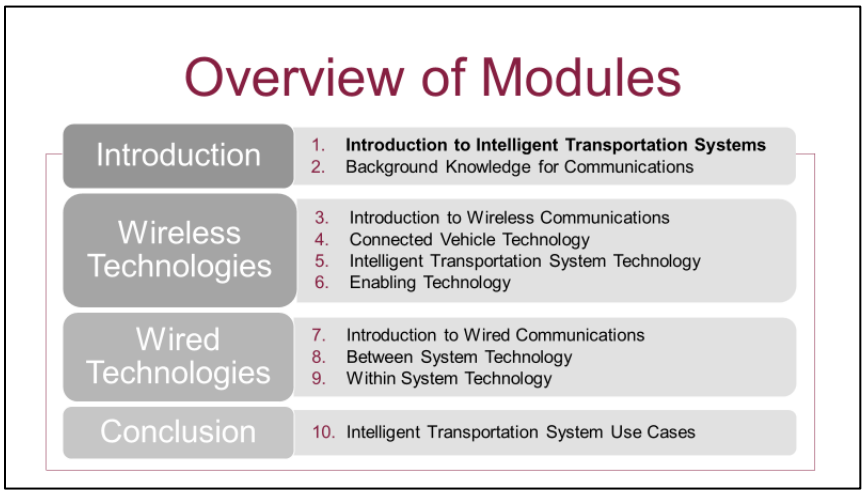
One connected transportation solution that has been widely adopted and gained significant market penetration is the third-party navigation application. Third-party mobile navigation applications are installed in users' cellular handset devices and are used to provide navigation and trip-related information to the user as they drive.

In general, these applications gather GPS information including location, speed, and heading while the application is running. The data is sent from the handset to a central system through a cellular connection to determine travel speeds and times for various segments of a driving route. This information is aggregated from many vehicles in the central system and used to provide optimal routing alternatives for users. In addition, the location of law enforcement, travel hazards, weather events, or traffic incidents may also be provided to the user, including re-routing instructions if a faster alternative exists.

This type of crowdsourced data collection is currently a low-cost way to deliver system-wide information to the provider, which allows for a more effective navigation solution for drivers. Application providers such as Waze and Google Maps will continue to see additional data sources as they are standardized. The Federal Highway Administration (FHWA) is leading efforts to establish new data management formats and distribution solutions such as the Work Zone Data Exchange. These systems will support standardization of the data, which will make it more efficient for application providers and OEMs to access data from a wide variety of providers without needing to customize their solutions.

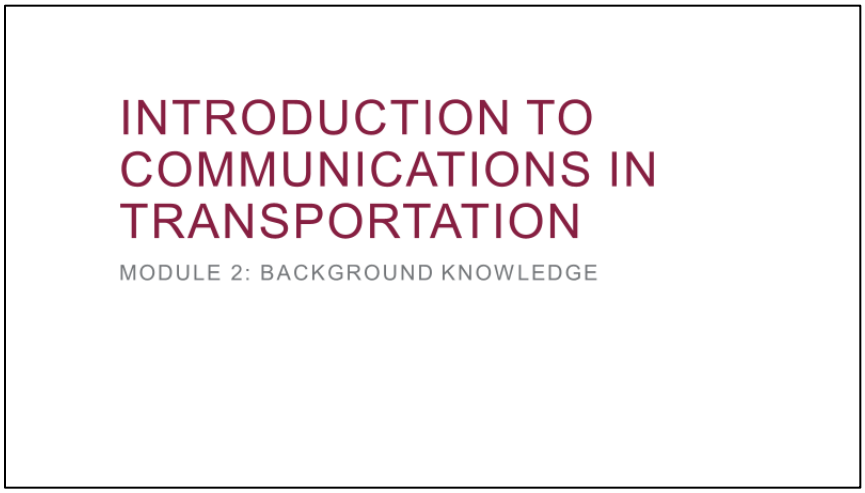
Next

Overview of Modules



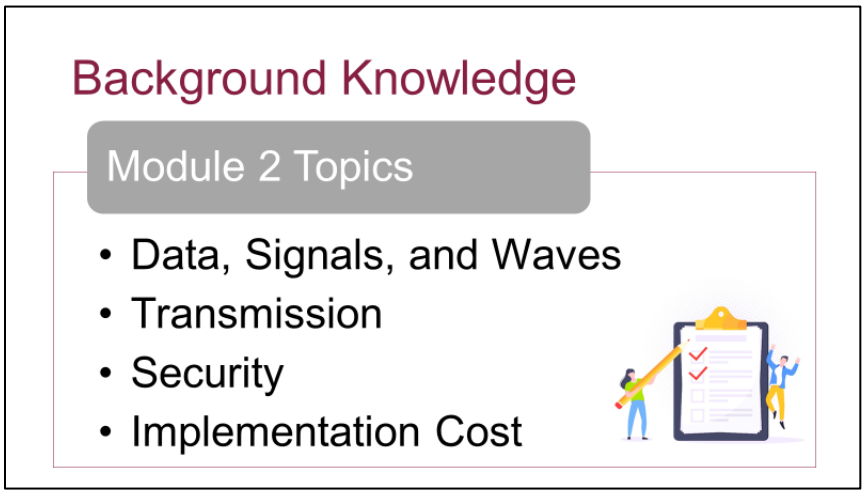
This concludes Module 1 – Introduction to ITS learning materials. In the next module, we will review Background Knowledge for Communications, but first, let's finish off with a quiz.

MODULE 2 – Background Knowledge



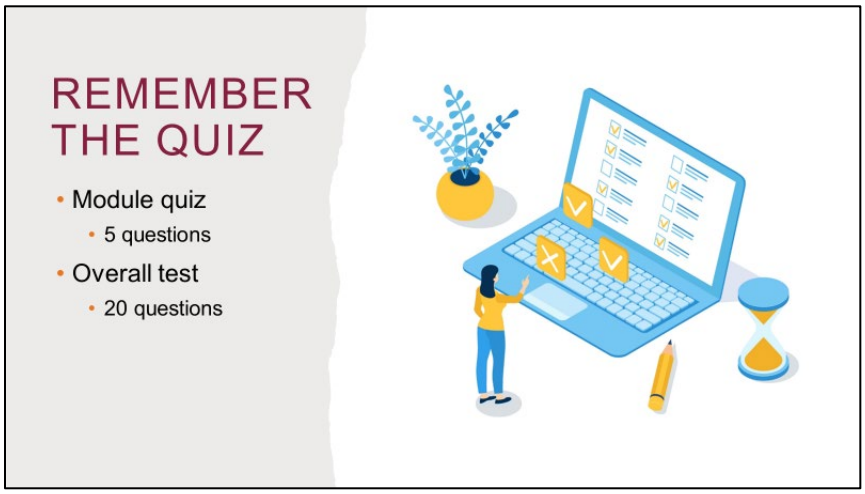
Overview

Background Knowledge



In Module 2 – Background Knowledge, we will discuss the building blocks of data, the types of signals, and electromagnetic waves. We will then discuss transmission factors, transmission limitations, and radio frequency. Elements of data security including terminology related to data access, verification, and protection will be included as well as some considerations for implementation cost. The underlying terminology and concepts related to these technologies are important to understand when comparing communication capabilities and planning future implementations.

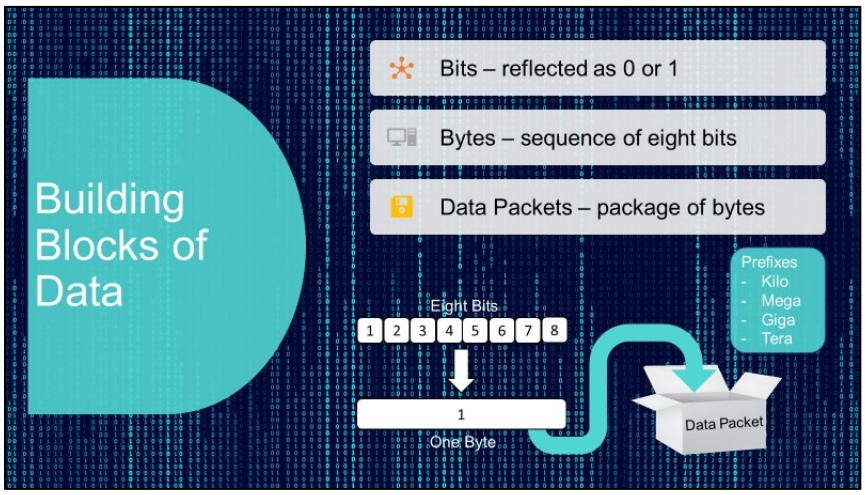
Remember the Quiz



Remember, there is a quiz at the end of each module with five questions for you to answer. At the end of the training, there will be an overall test with 20 questions.

Data, Signals, and Waves

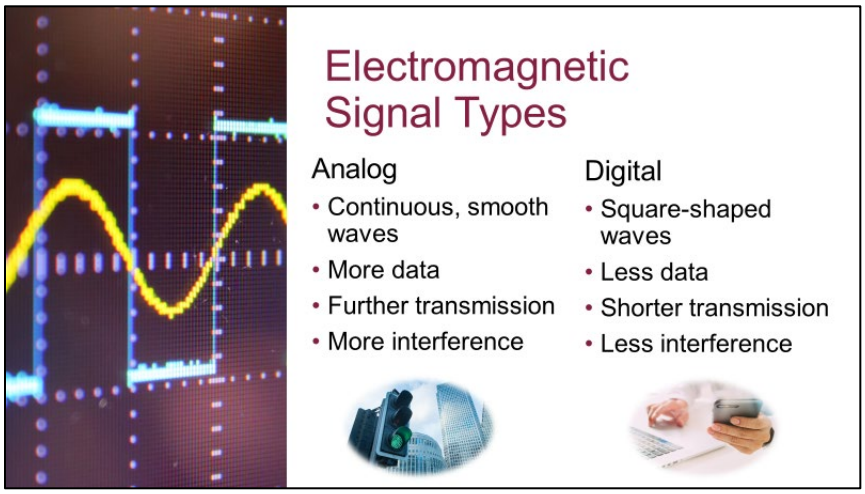
Building Blocks of Data



Bits are reflected as a binary 1 or 0, and bytes are a sequence of eight bits. These comprise the smallest amount of information that can be processed, and by stringing them together the information can be stored and communicated via an electromagnetic signal. The terms bits and bytes are often preceded by prefixes such as “kilo,” “mega,” “giga,” and “tera” to denote a thousand, million, billion, and trillion bytes, respectively.

A data packet is a unit of data comprised of bytes made into a single package that travels along network paths. Multiple data packets are often required to fully transmit information, and thus transmission details such as the sender, intended receiver, number of packets, and packet order are also included. For example, to transmit a high-quality image, the sender breaks it down into smaller pieces and compiles it into packets. The receiver will then confirm all packets have been obtained and use the packet order to rebuild the image.

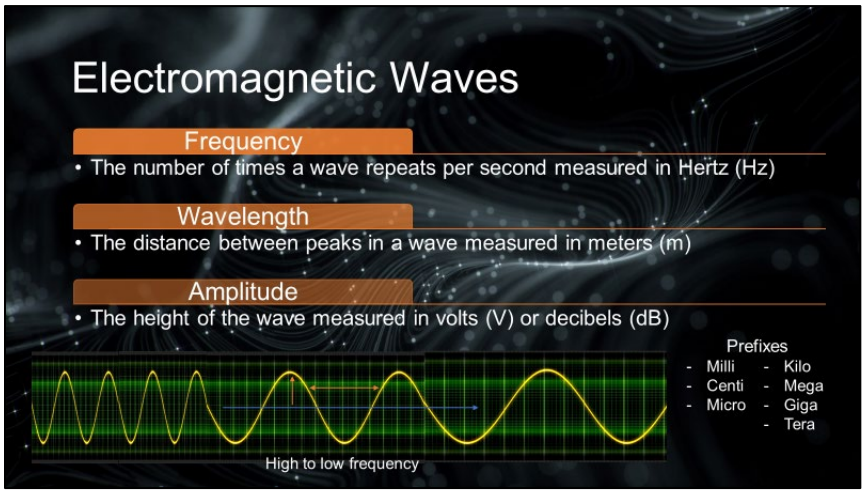
Analog vs. Digital Signals



There are two types of electromagnetic signals: analog and digital. Both signal types can be transmitted through wired and wireless technology, but they vary in their applications. Analog signals are used in applications such as traffic signals or older cameras. They are continuous, smooth waves that can contain more bits of information compared to digital signals. Additionally, analog signals can be transmitted further than digital signals, meaning they have an increased range using the same amount of power. However, analog signals are more susceptible to external influences such as noise and interference.

Digital signals are used more frequently in today's technology applications than analog signals. They are square-shaped waves that assume discrete values with very short rise times. Digital signals store data in the form of binary bits and are encrypted. Digital signals can be propagated using points of constant voltage that are directly encoded; therefore, digital signals do not need post processing when received. Analog signals can be converted to digital signals using a process called "digitizing." However, this process requires the use of additional hardware for sampling, quantization, and encoding. Digitizing also increases latency and can cause data loss.

Electromagnetic Waves



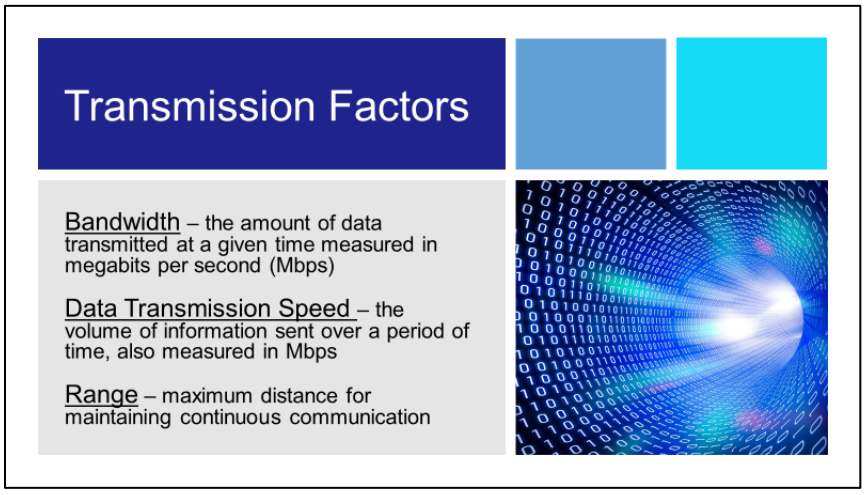
Electromagnetic waves are defined by two main characteristics: frequency and amplitude. Frequency is the number of times a wave repeats itself per second and is measured in Hertz (Hz). The inverse of frequency is wavelength, which measures the distance between peaks in a wave in meters (m). Amplitude is the

instantaneous power of the signal represented by the height of the wave and is generally measured in volts (V) or decibels (dB) for communication purposes.

These wave characteristics affect how the wave will perform and how effective the signal will be in different environments. Wireless signals with lower frequencies degrade less when they pass through objects such as walls or foliage compared to higher frequency signals. The choice of transmit power level is a design tradeoff between range and energy consumption. A lower frequency signal can travel further with the same amount of power but has a lower data transmission speed, while a higher frequency signal requires more power to travel the same distance. The higher the power transmission, the longer the effective range, making it more likely that the signal can be received at longer distances.

Transmission

Transmission Factors

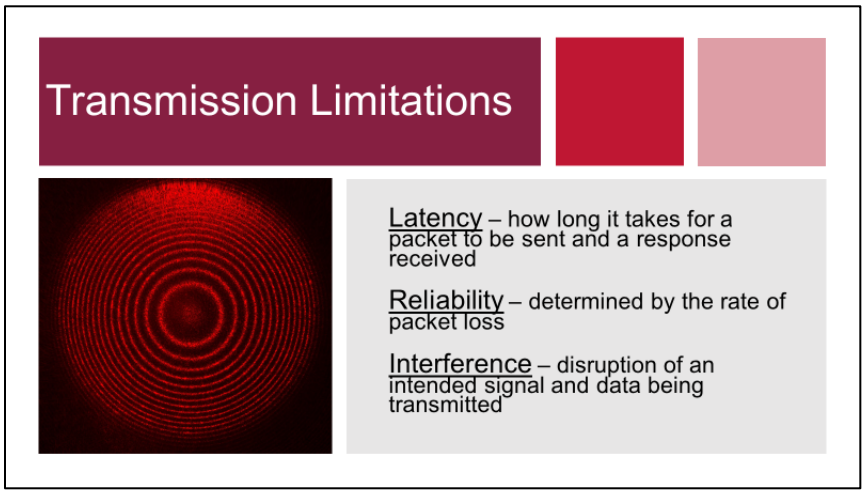


Bandwidth reflects the amount of data that can be transmitted at a given time through a single connection to one or multiple devices and is generally measured in megabits per second, or Mbps. Data transmission speed reflects the volume of information that can be sent through a connection over a period of time and is also measured in Mbps. To illustrate this concept, imagine your home Wi-Fi has a bandwidth of 100 Mbps. If four smartphones were connected to the Wi-Fi at the same time, each cell phone could have one fourth of the total bandwidth, with data transmission speeds of 25 Mbps.

For reference, the average internet download or transmission speed ranges from 12 to 25 Mbps, so for a household with three or four people, a bandwidth of 100 Mbps is typical. Modern LTE cell phones are capable of data transmission speeds over 100 Mbps, but a reasonable expectation in typical cellular network conditions is 20 to 30 Mbps.

Range is the maximum distance possible between a transmitting and receiving device for maintaining continuous communication. This is typically measured in meters, feet, or miles. Range is mainly influenced by amplitude or the power of the data transmission as well as the line of sight available for the signal to propagate without obstruction.

Transmission Limitations

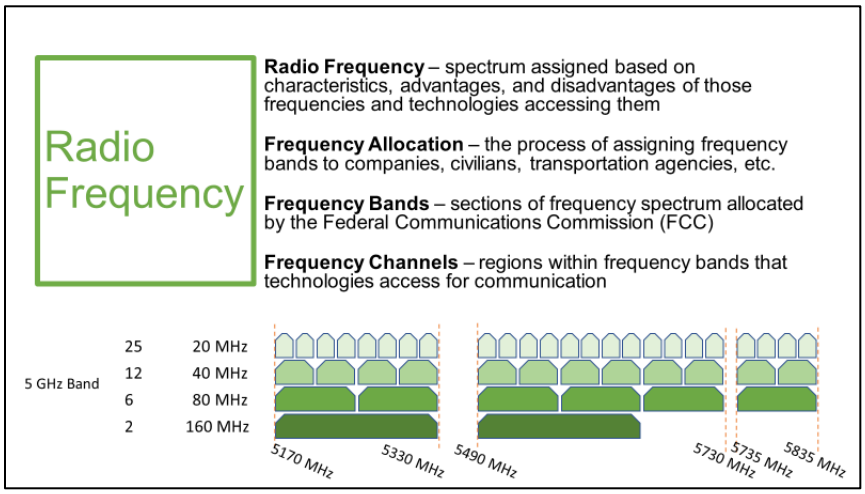


Latency is a measure of how long it takes for a packet of information to be sent and a response received. Higher latency corresponds to longer delays in sending and receiving information. Practically speaking, latency depends on a variety of factors such as transmission speed, bandwidth, processing speed, and interference. Latency is a critical factor in how effective safety-related applications will be as added latency results in less time for a driver or system to respond.

Reliability can be measured in a few ways but is generally determined by the rate of packet loss. Packet loss is experienced when the entire data packet is not completely communicated between the sender and receiver. Wired communications typically have a packet loss rate of 0, meaning that all data transmitted is received. Wireless communications can experience packet loss due to variations in signal strength or interference. Some technologies require an unobstructed Line of Sight (LOS) due to a sharp decrease in reliability when obstructions such as buildings are in its signal path. Wireless transmissions at lower frequencies using higher power are less affected by their environment, making them more immune to noise and more reliable.

Interference is the addition of unwanted signals, commonly referred to as noise, that disrupt an intended signal and data being transmitted. Interference generally affects wireless communication but can also affect unshielded wires transmitting in close proximity. Interference can be intentional, as in the form of jammers; unintentional, such as being too close to a different transmitter; or a product of natural phenomena such a solar eruption. Interference causes the data transmitted to not match the data received by changing the frequency, amplitude, or other characteristics of the signal. Interference can generally be avoided in wireless communications through proper usage of the spectrum allocated by the Federal Communications Commission, which will be discussed next.

Radio Frequency

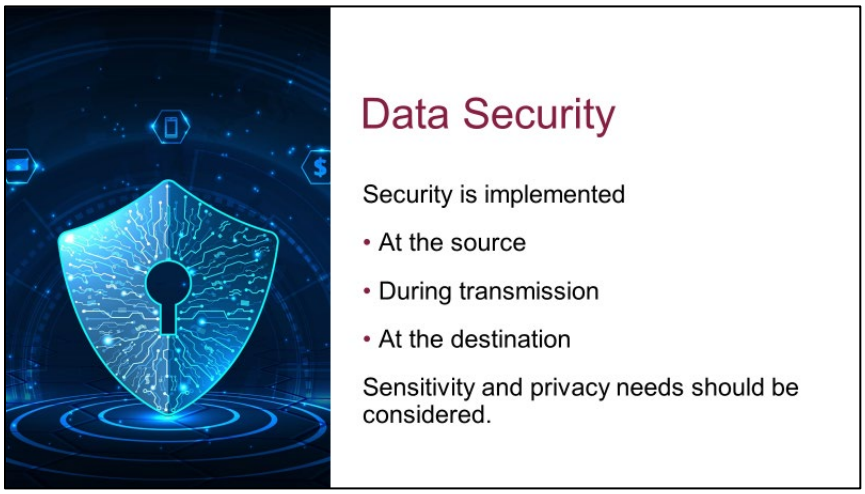


To avoid interference, different technologies are assigned radio frequencies on the spectrum based on the characteristics, advantages, and disadvantages of those frequencies and the technologies accessing them. These assigned frequencies, called bands, are allocated by the Federal Communications Commission (also known as the FCC) to companies, civilians, transportation agencies, and more. Frequency channels are within the bands and are what technologies are accessing specifically when communicating via the radio frequency.

While the use of some radio spectrum bands requires licensing, individuals or companies may intentionally or inadvertently use unlicensed spectra when operating very high frequency or ultrahigh frequency two-way radios. When establishing wireless communications systems, it may be necessary to acquire the proper permits to ensure regulatory compliance and reliability by preventing interference from other spectrum users.

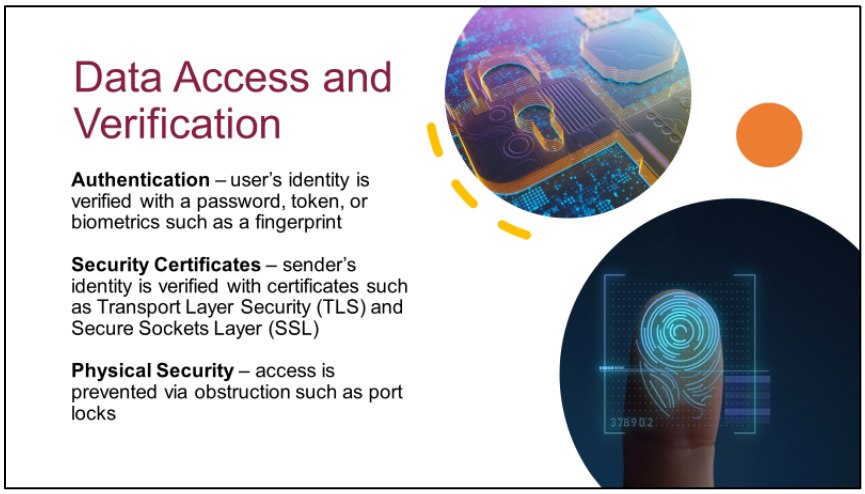
Security

Data Security



Considerations should be made for the security framework necessary when constructing wired and wireless networks. Security should be implemented at the source, during transmission, and at the destination of a data transfer. The sensitivity of the data and privacy required should also be factored in when determining security needs. For example, higher security measures may be needed when transmitting sensitive or proprietary data.

Data Access and Verification

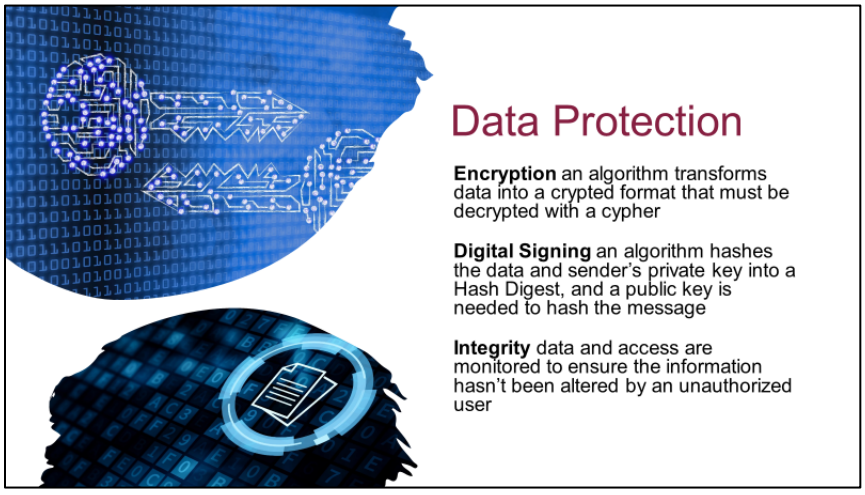


Authentication is a process where the user's identity is verified to provide them access to transmitted data. This commonly occurs with a password but also includes tokens and biometrics such as a fingerprint.

Security certificates standards are used to verify the identity of a sender. In a connected environment, security certificates are transmitted along with safety messages to ensure they are from a trusted source. Common certificates are Transport Layer Security (referred to as TLS) and Secure Sockets Layer (referred to as SSL).

Physical security refers to preventing access via obstruction. Applicable to wired technologies, examples can include port locks preventing connections and other physical deterrents.

Data Protection



Encryption is a process by which an algorithm transforms data into an indecipherable format that must be decrypted with a cypher. Encryption standards for federal computer systems are referred to as Federal Information Processing Standards (or FIPS). Encryption can be asymmetric when data is encrypted using a private key, often held by the creator, and decrypted with the

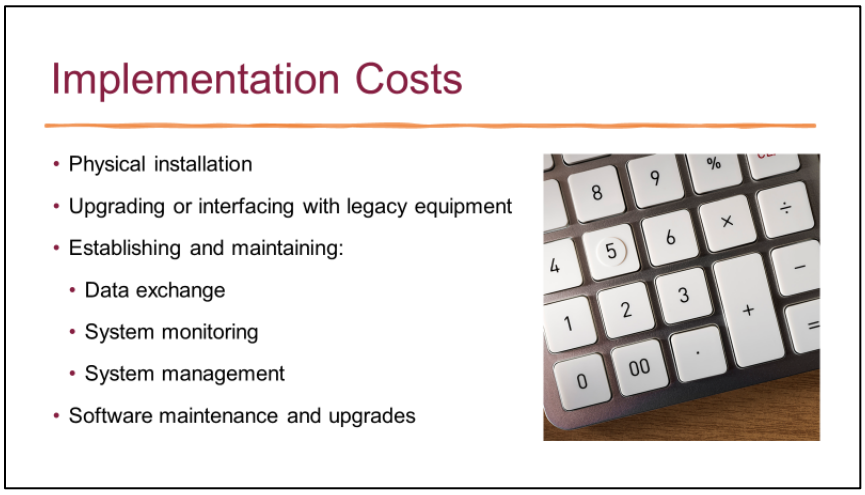
public key. It can also be symmetric when using only one key for both encryption and decryption. A common method used is Advanced Encryption Standard (AES).

Digital signing is a process by which an algorithm hashes both the data and the sender's private key into what is referred to as a hash digest. The recipient receives the data, hash digest, and public key and uses the public key to then hash the message. The hash digests from the transmitter and receiver are compared and, if consistent, then the sender is confirmed, and the data has not been changed. This does not account for potential interception.

Integrity refers to a process of monitoring data and access to ensure the information has not been altered by an unauthorized user. This method commonly uses Message Authentication Code (MAC) or an Authenticated Encryption with Associated Data (AEAD).

Implementation

Implementation Costs



There are a number of factors that need to be considered when estimating the cost of connected vehicle technology and infrastructure-based implementations.

The first is the cost of physical installation, this includes labor to run wires between a traffic signal cabinet and an RSU on a mast arm, temporary traffic control while the work is being done, and reconfiguration of the traffic signal cabinet to accommodate the equipment.

The second is the cost of upgrading or interfacing with existing legacy equipment that may not be capable of supporting the necessary information exchange. An example includes traffic signal controllers that were not designed to support the broadcast of SPaT data. These systems would require upgrades or replacements to support interfaces to RSUs that support SPaT broadcast.

Next is the cost of establishing and maintaining a data exchange, system monitoring, and system management. Mission critical systems will need to be interfaced to a system that IOOs can use to monitor their status to verify maximum reliability and availability.

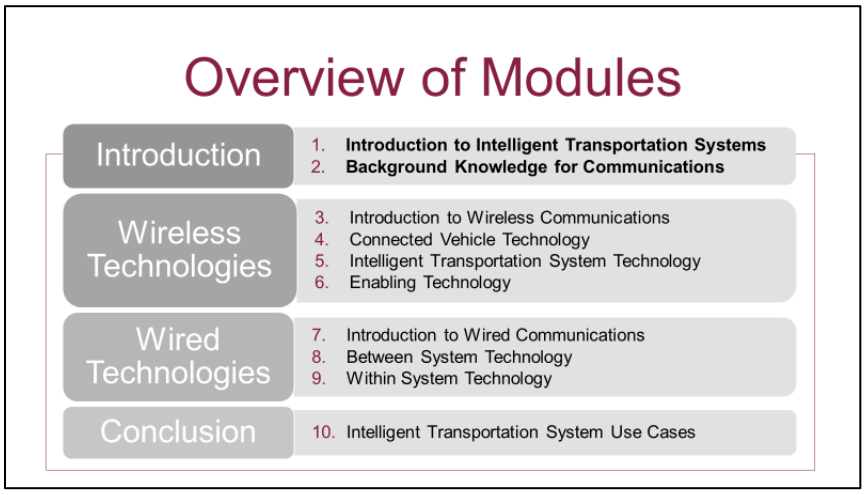
Finally, there is the cost of software maintenance and upgrades. Connected vehicle software, both operating systems and applications, must be upgraded regularly to maintain a secure and fully functional environment.

Implementation Variability

Determining the cost for deploying a connected technology can vary widely based on supplier and model. Additional costs for implementation can be influenced by factors such as the current network infrastructure or other regional limitations.

Next

Overview of Modules



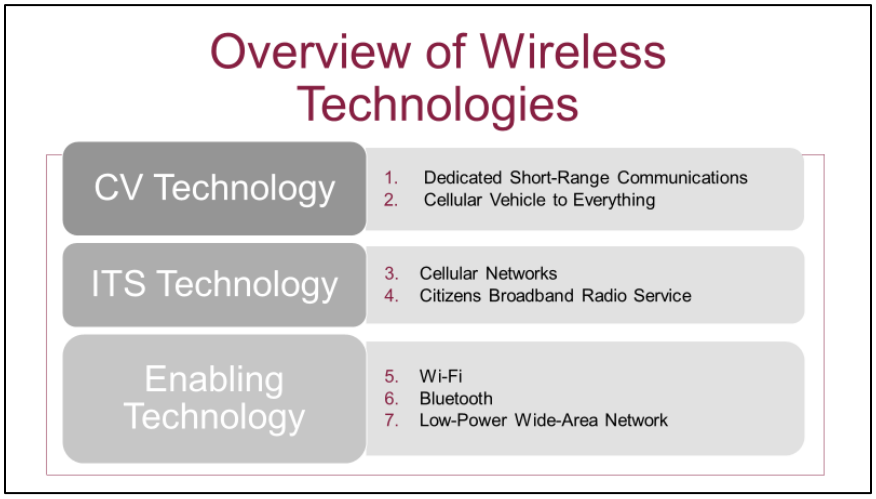
This concludes Module 2 – Background Knowledge for Communications learning materials. In the next module, we will begin reviewing wireless technologies starting with an introduction to wireless communications, but first, let's finish off with a quiz.

UNIT 2 – Wireless Communications

MODULE 3 – Introduction to Wireless Communications

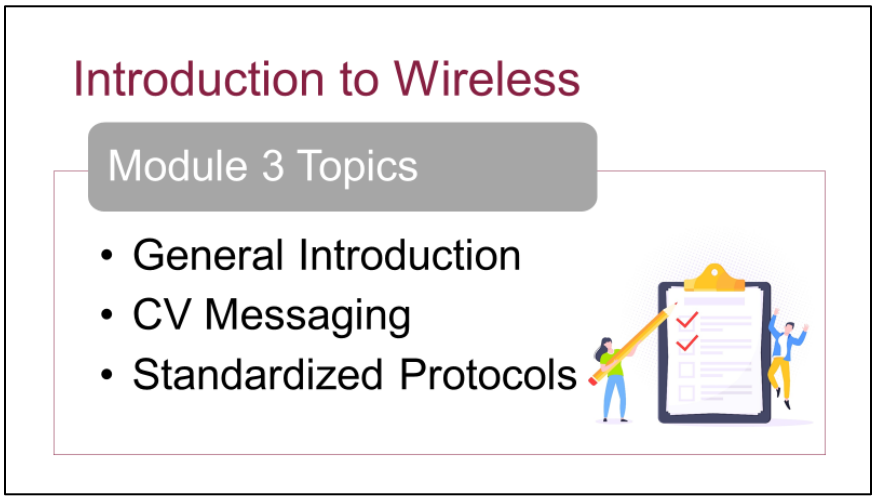
Overview

Overview of Wireless Technologies



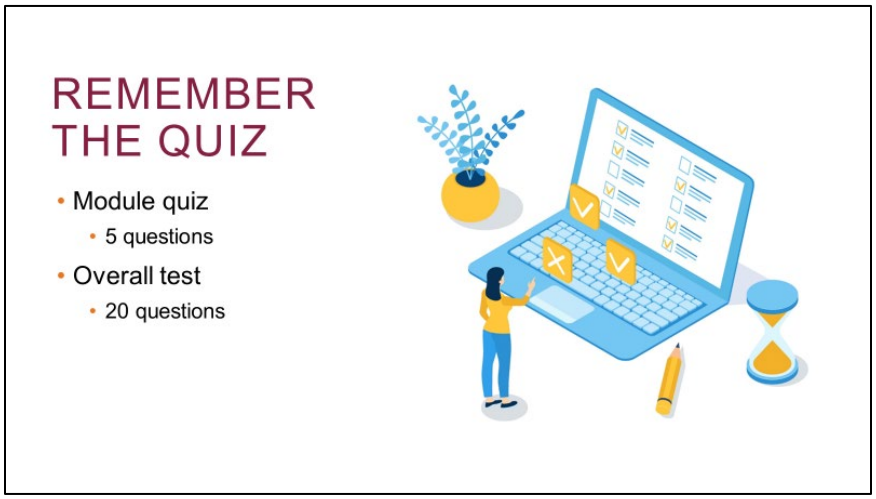
In this series of modules, we will discuss wireless technologies involved in connected vehicle technology, intelligent transportation system technology, and enabling technology. Within those, we will review the listed technologies and discuss Dedicated Short-Range Communications (DSRC), Cellular Vehicle-to-Everything (C-V2X), Cellular Networks, Citizens Broadband Radio Service (CBRS), Wi-Fi, Bluetooth, and Low-Power Wide-Area Network (LPWAN).

Introduction to Wireless



In Module 3 – Introduction to Wireless, we will cover a general introduction, followed by connected vehicle messaging applications and exchange rates. Then we will discuss security credential management as well as standardized protocols for communication.

Remember the Quiz

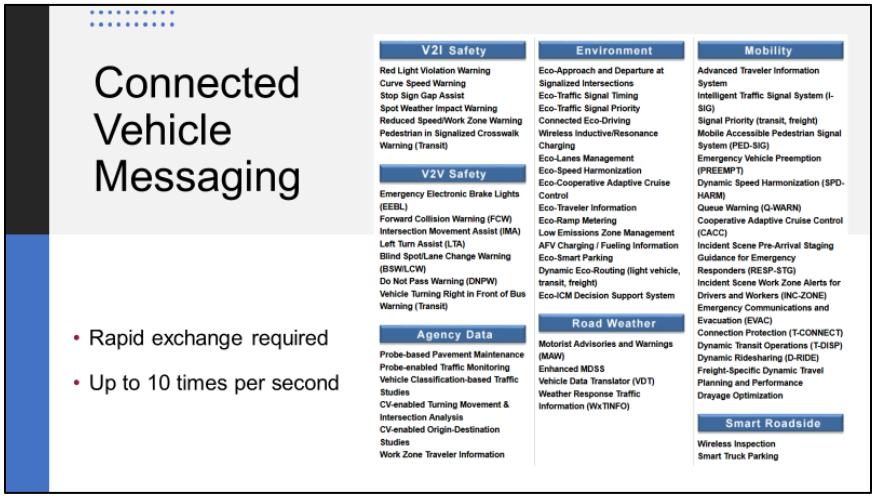


Remember, there is a quiz at the end of each module with five questions for you to answer. At the end of the training, there will be an overall test with 20 questions.

General Introduction

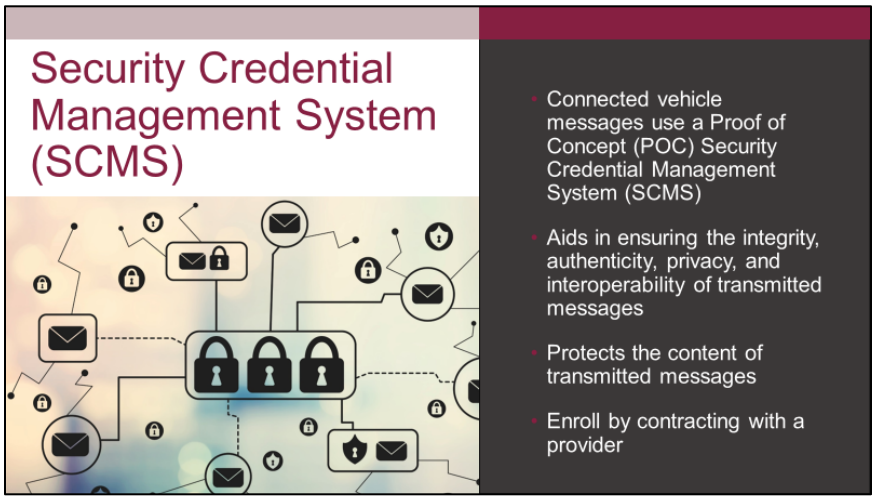
Wireless communications have many advantages over wired communications in connected vehicle applications, including increased mobility and reduced cost of implementation as physical wires do not have to be buried or connected between end points. Wireless communications use the environment such as air, water, and solids as the travel medium rather than a dedicated wire. However, as a result, wireless communications are less consistent than wired communications due to the potential for interference in dynamic operational environments. As discussed in Modules 1 and 2, interference can have a significant impact on connected vehicle applications using transmitted messages in safety applications.

CV Messaging



There are a variety of connected vehicle applications that use wireless technology to exchange associated messages that enable the successful operation of those applications. In most cases, safety applications require high reliability and rapid data exchange as the applications support collision avoidance, for which the timing of response is critical. Most connected vehicle data exchange standards require information to be sent at a rate of up to 10 times per second.

Security Credential Management System (SCMS)



Connected vehicle messages use a Security Credential Management System (SCMS), which is a Proof of Concept (POC) security system that helps ensure the integrity, authenticity, privacy, and interoperability of transmitted messages. The SCMS POC uses a Public Key Infrastructure (PKI) to encrypt messages and manage security certificates. Anonymized digital security certificates are issued by the SCMS POC and are the key to authenticating and ensuring the integrity of transmitted safety and mobility messages. The system protects the content of transmitted messages by screening, identifying, and removing misbehaving devices. Vehicle to Vehicle (or V2V) and Vehicle to Infrastructure (or V2I) devices enroll into an SCMS by contracting with a provider. Security certificates are obtained from Certificate Authorities (CAs) and are attached to messages to prove the transmitting device is a trusted actor in the system. Next, we will discuss some communications protocols and message standards currently used in a connected environment.

Standardized Protocols

Standardized protocols and message sets have been developed by the International Society of Automotive Engineers (known as SAE International) in standards J2735 Vehicle to Everything (V2X) Communications Message Set Dictionary (formerly titled Dedicated Short-Range Communications (DSRC) Message Set Dictionary) and J2945 On-Board System Requirements for V2V Safety Communications to assure interoperability between connected vehicle systems and applications in a connected environment. The

messages provide a standardized data format and organization that helps assure that dissimilar systems can speak the same language.

J2735

SAE standard J2735 V2X Communications Message Set Dictionary is a data dictionary that specifies data frames and elements required for certain standardized message sets in a connected vehicle environment. In addition to these message types, J2735 also provides information on message priority, which is heavily influenced by the urgency of the message. For example, a message related to a safety-critical warning would take priority over traffic information. The following are examples of messages in this standard:

Basic Safety Messages (or BSMs) are typically broadcast from vehicles and include details such as current GPS location, speed, heading, dimensions, brake status, and accelerations. A second optional part can also provide the status of other vehicle systems such as the wipers, lights, and temperature, if equipped to do so.

Personal Safety Messages (or PSMs) contain similar information as the BSM but are meant for pedestrians and other vulnerable road users such as construction workers. They contain information such as current location, velocity, and heading as well as optional details including path history, path prediction, public safety, and road worker activity.

Signal Phase and Timing (or SPaT) Messages provide the current traffic signal status, what the next status will be, and when the signal will change. The SPaT message works in concert with the MAP message, which defines the geographic layout of the intersection and what traffic signal phases correspond to the phases in the SPaT message.

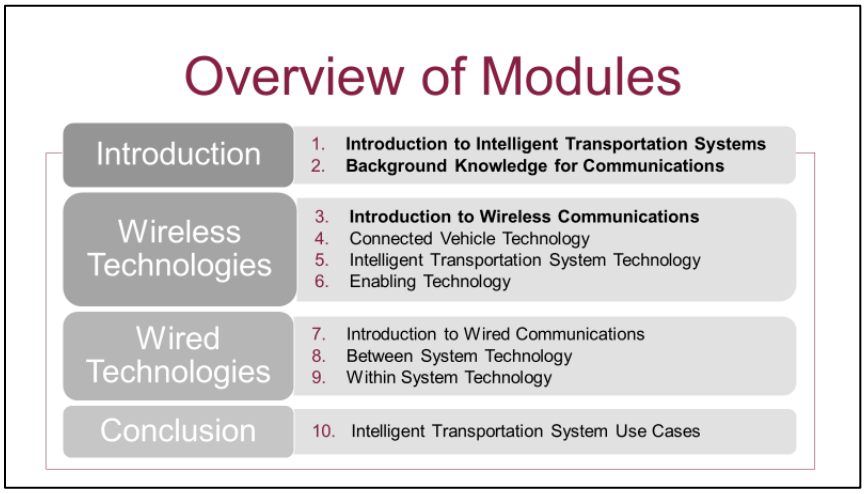
Traveler Information Messages (or TIMs) are used to convey information about traffic incidents, weather events, work zones, and other traffic information to drivers. The TIM includes a location, description of the condition, and when the information is valid.

J2945

SAE standard J2945 titled On-Board System Requirements for V2V Safety Communications provides guidance and information applicable to subsequent J2945/x standards that specify applications operable under the J2945 standard. For example, J2945/3 contains interface requirements for weather application interoperability. J2945/4, which has yet to be released as of early 2022, will rework some of the standards outlined in the J2735 message set dictionary to improve functionality for reduced speed zones such as work zones and emergency vehicle operations.

Next

Overview of Modules

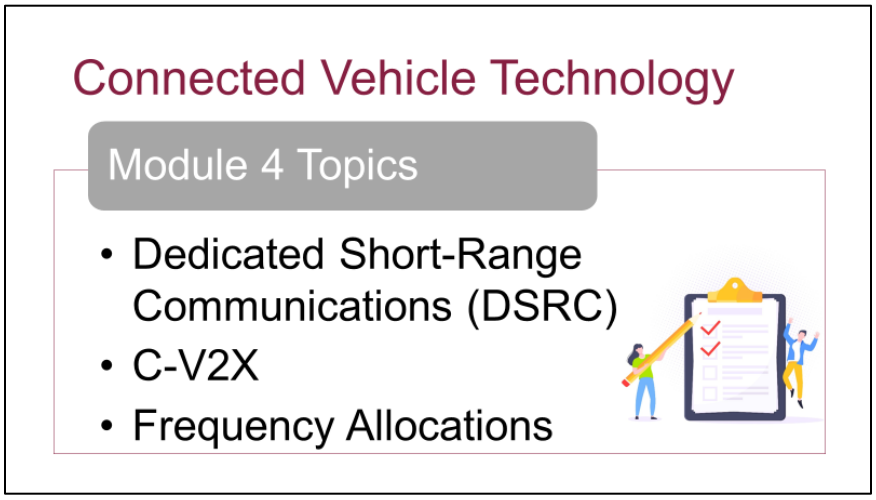


This concludes Module 3 – Introduction to Wireless Communications learning materials. In the next module, we will begin reviewing wireless technologies including Dedicated Short-Range Communications (also known as DSRC) and Cellular Vehicle to Everything (referred to as C-V2X), but first, let's finish off with a quiz.

MODULE 4 – Connected Vehicle Technology

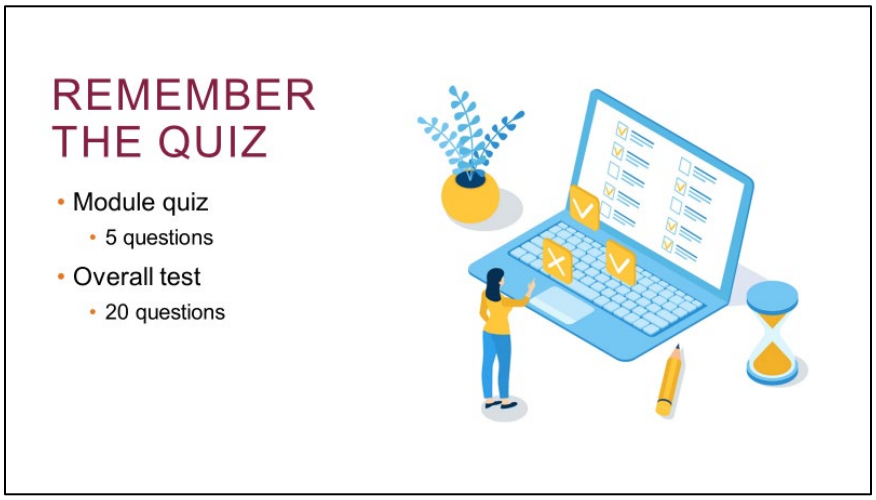
Overview

Connected Vehicle Technology



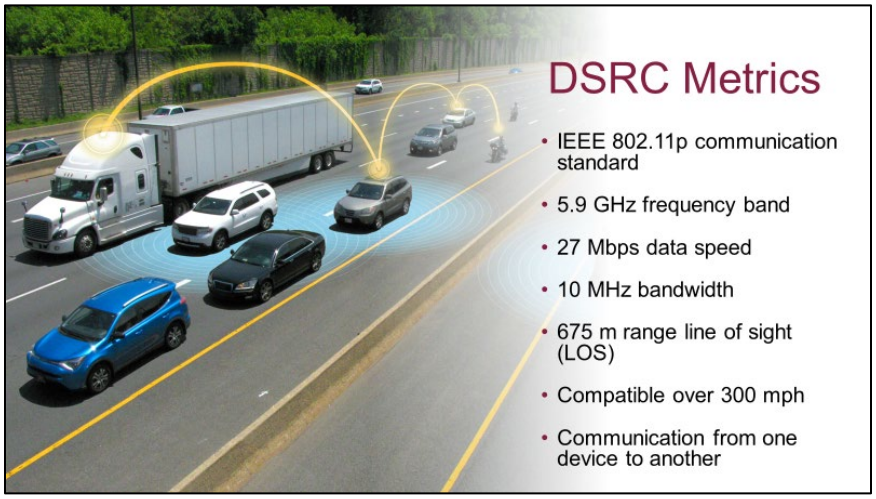
In Module 4 – Connected Vehicle Technology, we will cover metrics, implementation, and security for Dedicated Short-Range Communications (also known as DSRC) and Cellular Vehicle to Everything (referred to as C-V2X). After that we will discuss connected vehicle security and frequency allocations for the transportation sector. These communication technologies are used in vehicle-involved wireless communications in an Intelligent Transportation System environment.

Remember the Quiz



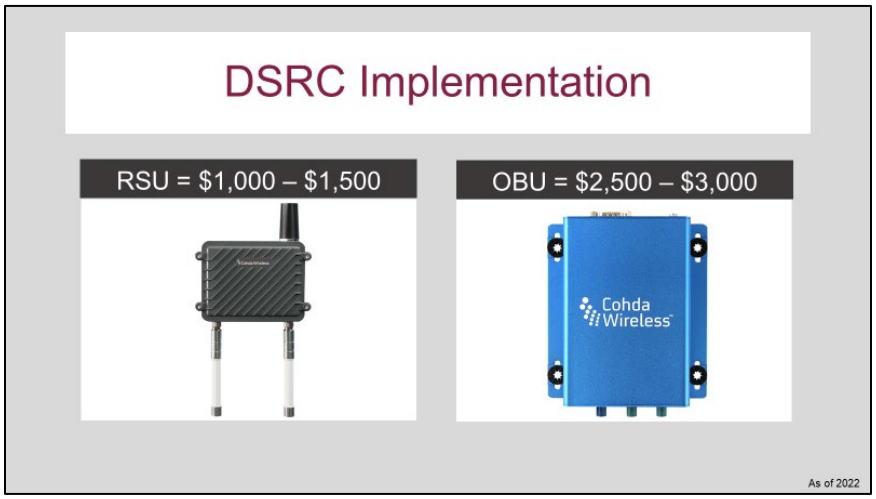
Remember, there is a quiz at the end of each module with five questions for you to answer. At the end of the training, there will be an overall test with 20 questions.

DSRC Metrics



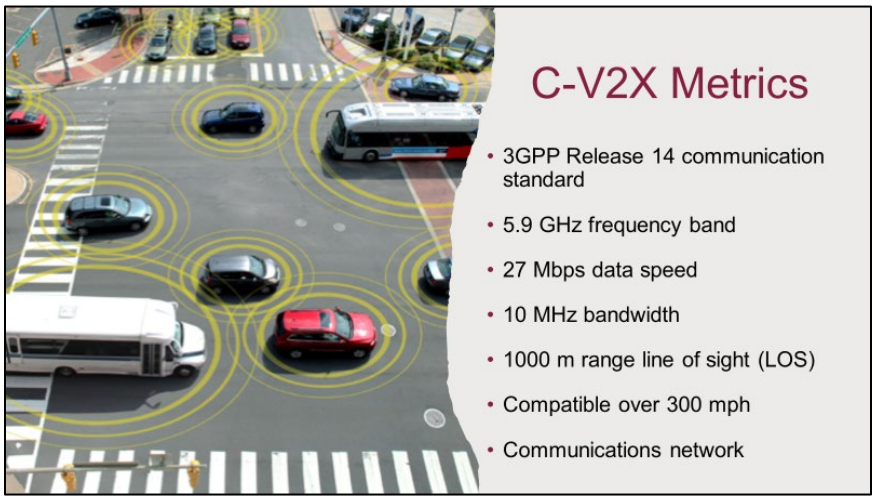
Connected vehicle communication strategies have been around for approximately two decades, truly beginning with Dedicated Short-Range Communications (or DSRC for short) in 2003. DSRC uses the Institute of Electrical and Electronics Engineers (IEEE) 802.11p protocol standard and was developed to exchange data rapidly, reliably, and securely between vehicles and systems for a variety of safety applications. It uses the 5.9 GHz frequency band and is capable of data speeds up to 27 Mbps, with a 10 MHz bandwidth, and up to 675 meters of range with a clear Line of Sight (LOS). These metrics allow for a larger volume of messages to be transmitted quickly. Additionally, communications are compatible with vehicles moving at relative speeds of over 300 mph, but communication is only from one device to another rather than among a wider area network.

DSRC Implementation



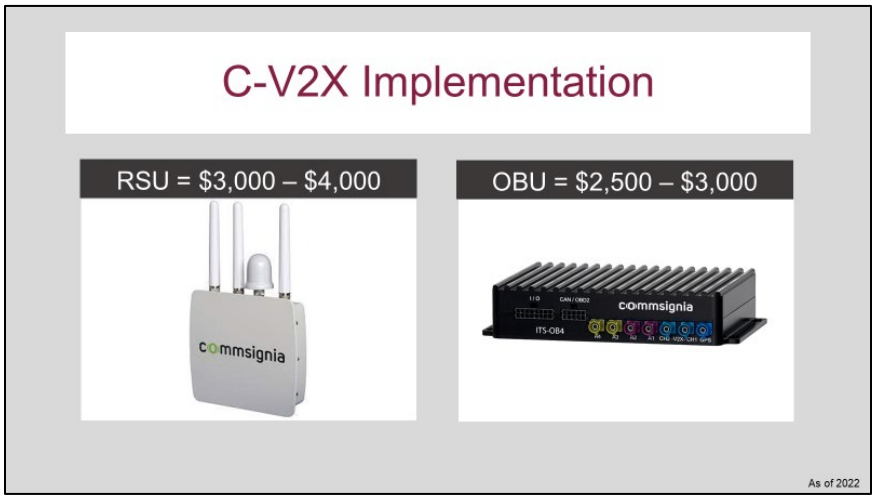
Practically speaking, to maintain continuous coverage in a Vehicle to Infrastructure (V2I) usage scenario, DSRC Road-Side Units (also call an RSUs) would need to be installed approximately every kilometer or so. As of 2022, an example DSRC On-Board Unit (also called an OBU) costs around $2,500 to $3,000 and an RSU costs around $1,000 to $1,500 in low-volume purchases. The lack of wider area networking capability limits DSRC's potential in a connected transportation environment.

C-V2X Metrics



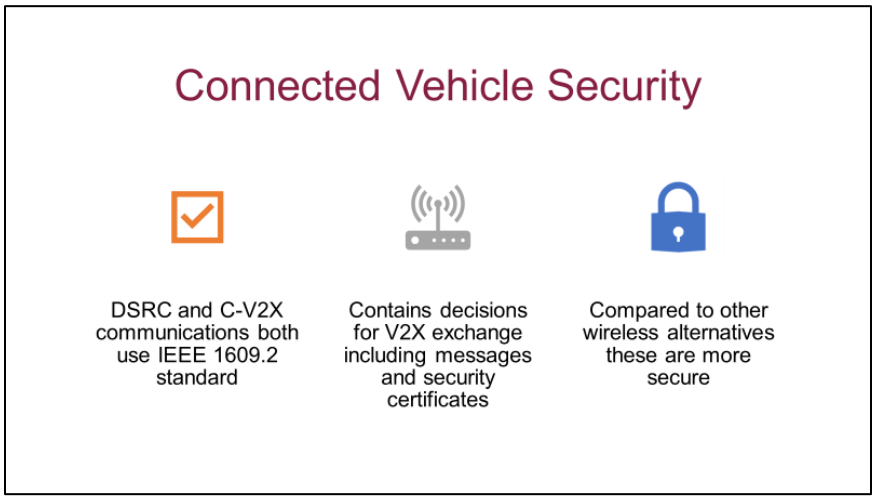
In recent years, a new communication technology has emerged—cellular-vehicle to everything (or C-V2X)—that effectively combined the low-latency, high-reliability communications of DSRC with the wide area coverage of a cellular network. C-V2X uses the 3GPP Release 14 communication standard and will serve as the foundation for vehicles to communicate with each other and everything around them, providing 360-degree non-line-of-sight awareness and a higher level of predictability for enhanced road safety and autonomous driving. A plethora of new use cases have been made possible due to C-V2X's high reliability and near-real-time latency. Like DSRC, C-V2X also uses the 5.9 GHz frequency band and provides data speeds up to 27 Mbps and a 10 MHz bandwidth. It also features up to 1,000 meters of range when there is a clear Line of Sight (LOS) and can establish connections with vehicles traveling over 300 mph.

C-V2X Implementation



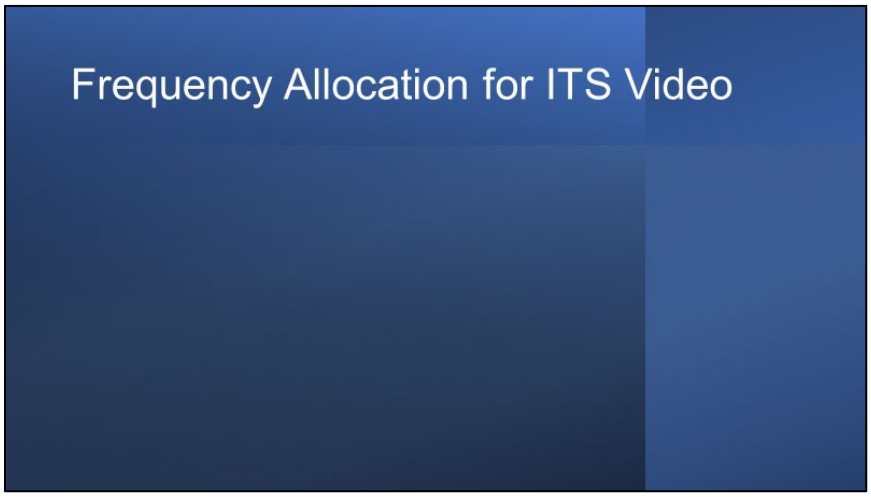
As with DSRC, to maintain continuous coverage when implemented, RSUs need to be installed approximately every kilometer. An example C-V2X RSU costs around $3,000 to $4,000 in low-volume purchases, and an OBU costs around $2,500 to $3,000.

Connected Vehicle Security



DSRC and C-V2X communications both use the IEEE 1609.2 standard, which contains several crypto and protocol decisions for V2X packet exchange, including messages for connected applications in a vehicle environment and security certificates. Compared to other wireless alternatives, these are more secure and support various security measures, including encryption and mutual authentication. The safety messages are used to support the safety applications and the certificate exchange messages discussed in Modules 1 and 3.

Frequency Allocation for ITS Video



Question 1 - Connected vehicle tech such as DSRC has been around for a while. Why don't we see much deployment of it?

DSRC has been around for about 20 years. About that time, the FCC allocated a full 75 megahertz of that spectrum around the 5.9 gigahertz band to be able to support applications for connected vehicles, including vehicles, talking to other vehicles, vehicles talking to infrastructure. Upon that you can build safety applications that really have a potential to benefit by reducing crashes and injuries. A lot of pilot testing programs have been conducted, those applications have been developed, and we found it to be a very, very effective technology and something that could really save a lot of lives.

Unfortunately, there was at one point a notice of proposed rulemaking that was going to make it mandatory for all new production vehicles to have these radios on them when they come off the production floor. Unfortunately, that rule did not ever become a final rule and therefore that mandate was taken away.

In the meantime, a new technology called Cellular V2X was introduced and has been undergoing rapid development and testing as well. Cellular V2X allows two radios to talk to each other, point to point communications, but also to be able to talk through a traditional cellular network, which of course greatly expands the amount of deployment area that you would have coverage in.

Question 2 - What's the current status of the connected vehicle landscape? Have there been any developments that will help accelerate the deployment?

Well, a lot of good development has been completed on looking at these applications, how they can improve and support safety. States have made significant investments in developing test beds and environments where they can try out these technologies for the first time. And I think largely the world is ready to move forward with some kind of connected vehicle deployment. Unfortunately, there's still a little bit of uncertainty with respect to what the right technology will be. As I mentioned before, Cellular V2X is emerged, and it provides some advantages in terms of its areas of coverage that can be handled. And then but DSRC has been around for a long time and has proven itself to be quite capable.

Recently, the FCC has made a decision to reallocate some of the original 75 megahertz of spectrum to unlicensed users, such as Wi-Fi. There's a huge demand for Wi-Fi bandwidth out there, and it really helps drive our economy in a lot of ways. If we think about it. And so, the FCC is responding to that demand, taking some of the allocation away from the connected vehicle usage allocation and making it available to the others. At the same time, it is effectively making a decision moving forward that Cellular V2X will be the solution in the future.

All right. So, these diagrams can help us see how the spectrum has been allocated around the 5.9 gigahertz band. So, within the 75 megahertz that were available to the safety band, it was divided up into 10 megahertz, effectively channels. So, they had seven channels and they were all allocated to DSRC. As of this new rulemaking that the FCC has put forth, the bottom four channels will be assigned to unlicensed Wi-Fi, while the top three channels will be split between DSRC and C-V2X with C-V2X having two of the channels. A year after the rule goes into effect, effectively, all the channels will be allocated to C-V2X at the top end of that band for doing the safety applications and DSRC will be decommissioned.

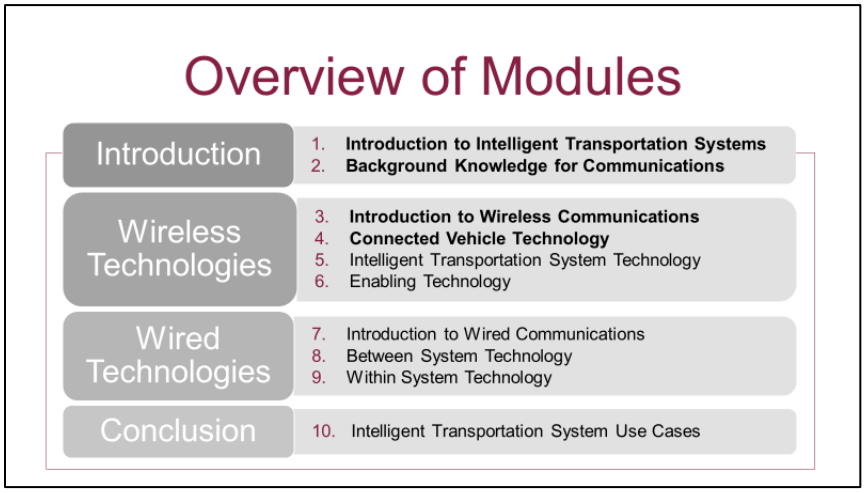
Question 3 - What do you see for the future?

Yeah. As far as the future goes for Connected Vehicle, a variety of things could happen. I think there's still some uncertainty, even with the FCC creating this rule to reallocate the spectrum. There are some pending lawsuits that have concerns over where the technology is sourced that may still have some impact on the outcome of what is ultimately adopted. I believe that will move forward thinking that Cellular V2X is going to be the right solution and probably a lot of the testing and development will be done on that platform.

However, in the meantime, mobile network operators like AT&T, Verizon, and Sprint, they have their own new concepts for how this might move forward as well. So, they can use a technology called Multi-access Edge Computing (MEC) to effectively steer network traffic through their existing cell tower systems to be very high reliability and low latency. And so, they're going to compete for that business model on their own as well. So depending upon how fast that technology moves along, that may also ultimately impact how these communications will come forward.

Next

Overview of Modules

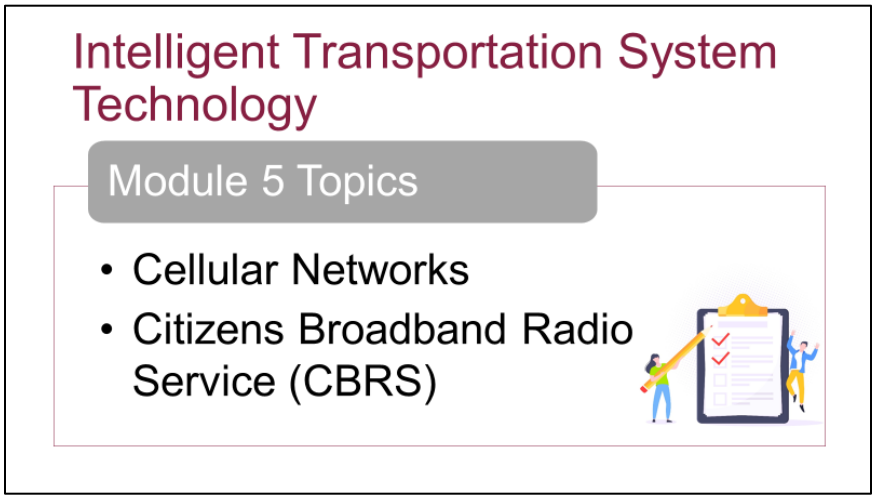


This concludes Module 4 – Connected Vehicle Technology learning materials. In the next module, we will continue reviewing wireless technologies including Cellular Networks and Citizens Broadband Radio Service (known as CBRS), but first, let’s finish off with a quiz.

MODULE 5 – Intelligent Transportation Systems Technology

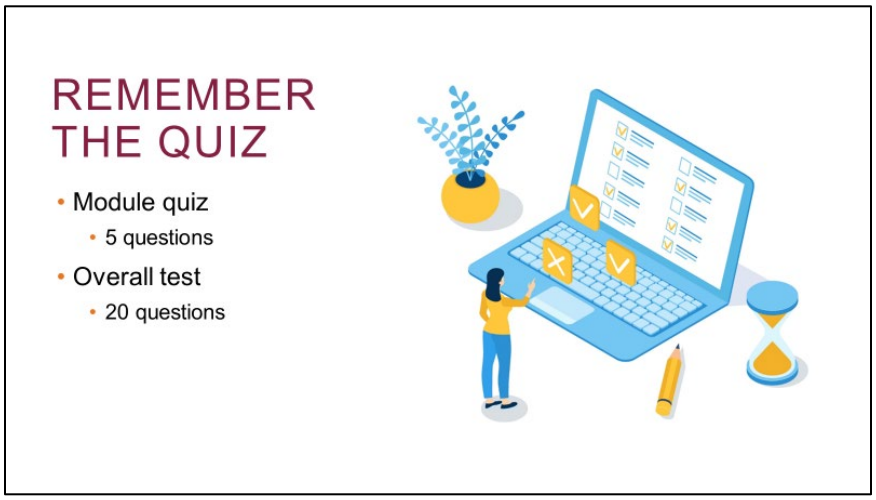
Overview

Intelligent Transportation Systems



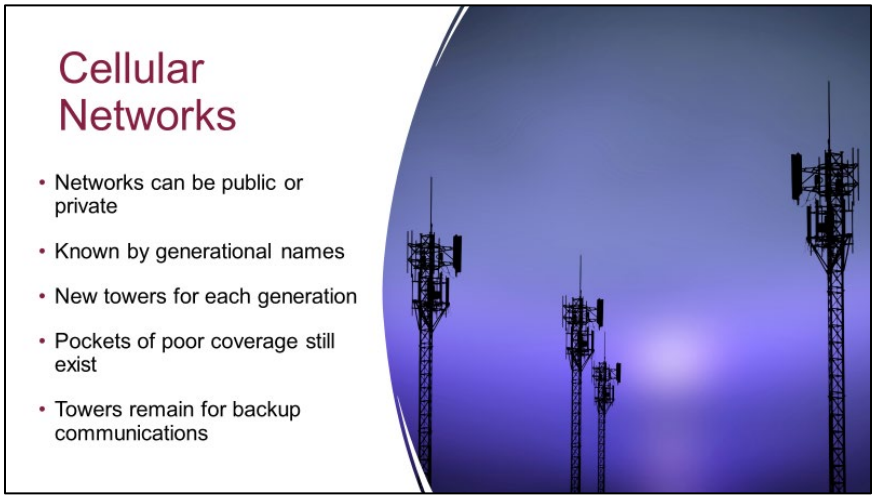
In Module 5 – Intelligent Transportation Systems (ITS), we will cover metrics, implementation, and security for Cellular Networks including previous generations and current generation bands. We will then discuss metrics and implementation for Citizens Broadband Radio Service (known as CBRS). ITS environments use these wireless communication technologies, and they require significant infrastructure installations for sustained network operation.

Remember the Quiz



Remember, there is a quiz at the end of each module with five questions for you to answer. At the end of the training, there will be an overall test with 20 questions.

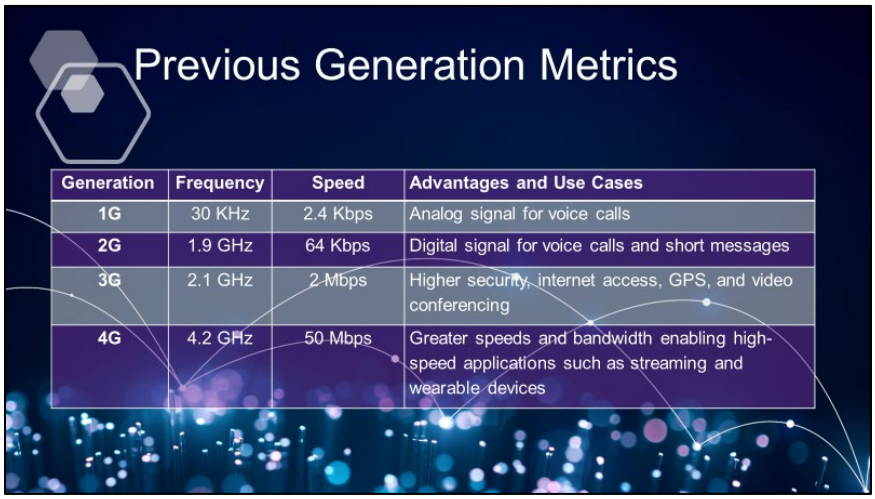
Cellular Networks



Cellular networks use the same broadband network as consumer cell phones, but its communication protocols have other uses for intelligent transportation systems. The networks can be public or private with public networks serving to connect individual users to cellular and internet services. Private networks are where a company, organization, or community might be given dedicated priority or access to use the network for their own purposes. Mobile network operators, may dedicate “slices” of their networks for private use, further expanding their ability to charge for access. It is expected that 5G network deployment will expand the implementation of private 5G networks enabling greater connectivity, security, and bandwidth for a wide variety of uses.

Cellular communications are commonly known by generational names, such as 4G or 5G, and new towers must be built with each generation for network conversion. While cellular networks are currently ubiquitous across the United States, pockets of poor coverage still exist in some regions. Although early generations such as 2G and 3G have been broadly discontinued, the towers often remain where they can be used as back-up for low-power voice or text-only communications.

Previous Generation Metrics

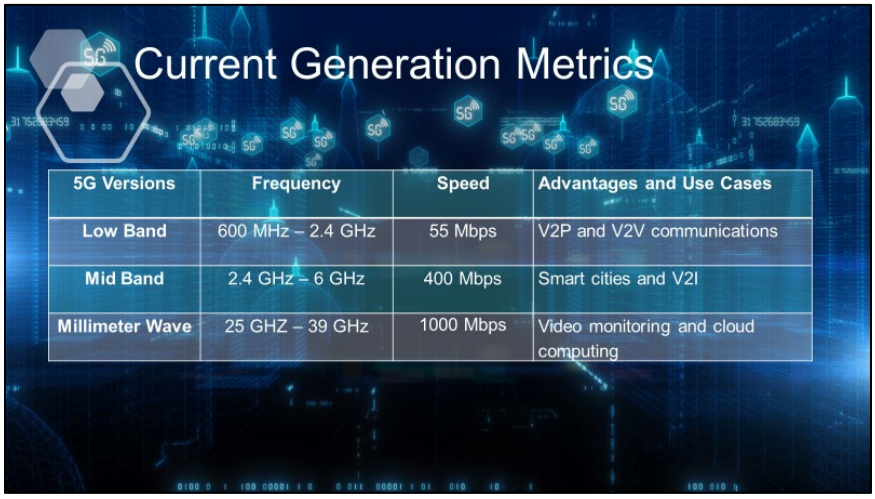


Initial generations of cellular networks such as 1G and 2G provided connectivity via analog and digital signals, respectively. 1G operated at a 30 KHz frequency with speeds of 2.4 Kbps and provided analog voice calling. The second generation operated at the 1.9 GHz frequency and offered speeds up to 64 Kbps, allowing for digital voice calls and short message transmission.

3G brought about the first era in which data connections and internet access became possible. Operating at a 2.1 GHz frequency with data speeds around 2 Mbps, this generation provided additional security, GPS navigation, and video conferencing capabilities.

The introduction of 4G required towers that were smaller and allowed for private networks to be constructed at a much lower cost. With this generation, greater bandwidth could be used, and data speeds significantly increased to approximately 50 Mbps. This allowed for a larger volume of data to be transmitted more quickly and led to additional use cases such as streaming and wearable devices. Like 3G, the range of 4G for reliable transmission and reception is less than 10 miles but can be as low as 1 mile in dense urban environments. Companies such as OnStar and some original equipment manufacturers have even used 4G to broadcast telematics data from equipped vehicles, providing a substantial benefit to fleet management services and public safety personnel.

Current Generation Metrics



The capabilities of 5G present many exciting new use cases, but 5G is not a direct replacement of 4G and offers its own unique drawbacks and advantages. 5G is an umbrella term for three versions: 5G low band, 5G mid band, and 5G millimeter wave. Cellular providers have different names that refer to these three flavors, which each operate on different frequencies thus influencing data speeds.

The low band version of 5G uses some of the same frequency bands as prior generations, ranging between 600 MHz and 2.4 GHz. The speed of this flavor is comparable to 4G at around 55 Mbps, but the claimed benefit is reduced latency and more sophisticated security. The lower frequency leads to decreased speed but increased range, making it less susceptible to interference compared to other 5G flavors. This version can be used for Vehicle-to-Pedestrian (or V2P) and Vehicle-to-Vehicle (V2V) communications.

The mid band version uses a higher frequency of 2.4 GHz to 6 GHz with data speeds around 400 Mbps. This provides faster speeds compared to low band with more range and less interference than millimeter wave. This version can be used for smart cities and Vehicle-to-Infrastructure (V2I) applications.

Millimeter wave operates in the range of 25 GHz to 39 GHz, making it more susceptible to interference and limiting its range. This is ideal for use in line-of-sight applications where the signal is not obstructed. This version of 5G can achieve speeds up to 1000 Mbps and higher, potentially replacing Wi-Fi. This band of 5G can be used for HD video monitoring as well as the transfer or raw sensor data into cloud computing for processing.

The most promising use cases for 5G are where high-bandwidth and near-real-time latency are required, such as for offline sensing. In this example, raw video or LiDAR sensor data is sent to an offline server and then processed for object identification and classification; the results are returned to a vehicle or system that can use the data for safety applications. Offloading this processing burden may significantly lower energy consumption and cost of deployment of advanced automated vehicles.

Cellular Network Implementation

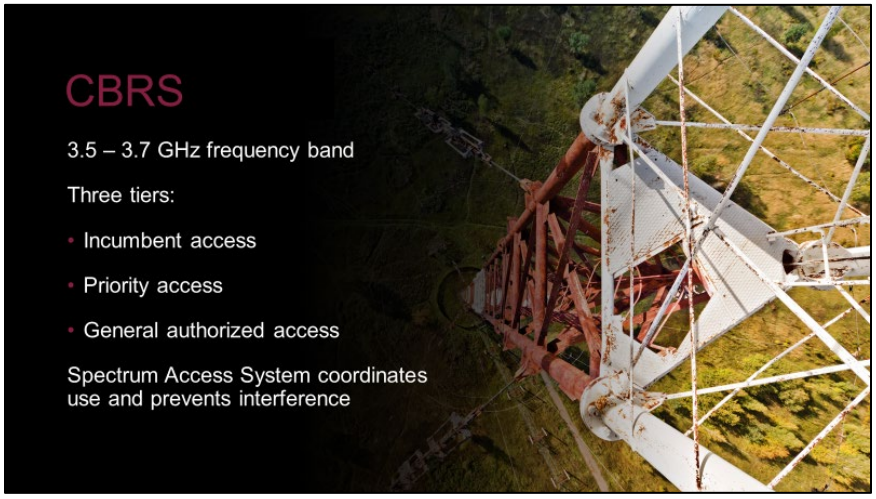
The current cost of 5G hardware is higher than 4G, and the shorter range requires more towers to be constructed. Small cells are used to extend the network coverage and are significantly smaller than 4G towers, allowing for installation on buildings, telephone poles, and other existing infrastructure. A variety of options have been used to conceal small cells in cities, such as mounting to existing light poles, on top of buildings and even on the underside of manhole covers.

Cellular data plans cost around $35 to $65 per month per device for a typical “unlimited” data quantity. However, most carriers use a variety of techniques to limit their unlimited plan, such as reducing

transmission speed after certain data milestones are achieved, referred to as “throttling”. Small cells can be installed to extend the 5G network coverage and cost approximately $14,000 per unit.

Additionally, cellular networks that use 4G/LTE and 5G wireless technologies should establish protection for connections between the User Equipment (UE), Mobility Management Entity (MME), and elements in the wireline networks and mobile stations. To satisfy these requirements, the security is significantly improved by adding advanced key hierarchy, including Key Management Authentication, Encryption, and Integrity Protection (IP).

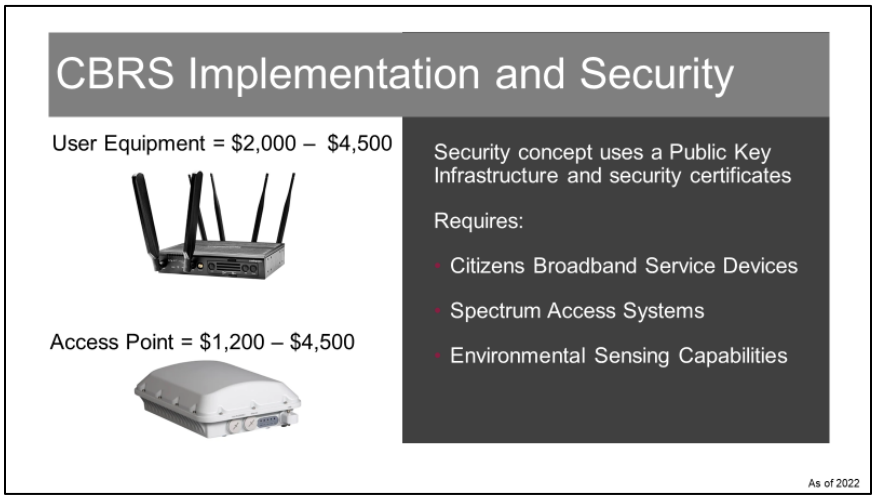
CBRS Metrics



Citizens Broadband Radio Service (or CBRS) is designated for sharing among three tiers and operates within the 3.5 to 3.7 GHz band. The three tiers of users include incumbents, priority access license, and general authorized access users. The incumbents tier holds priority over the other tiers and is used by United States military radars, fixed-station satellites, and wireless internet service providers. The priority access license tier uses contracts to allocate channel access, which are obtained through competitive bidding on a regional basis. The lowest tier (general authorized access) allows transmission over any available portion of the CBRS band without a license. The CBRS band has been dubbed the innovation band by the FCC because of this unique, tiered sharing concept. Additionally, a cloud-based service called the Spectrum Access System is used to coordinate spectrum use and prevent interference by ensuring the lower tier users switch channels based on the utilization by higher-tier users.

CBRS offers the opportunity to create private networks to communicate with deployed equipment, such as smart intersection applications that process their sensor data on a server or in the cloud and require high bandwidth, very low latency, and high reliability. The downside of CBRS is that the priority access license (PAL) is required to maintain high reliability and must be purchased in each jurisdiction of use. For this reason, CBRS is seen as more of a research and development option and not as a platform for broad deployment.

CBRS Implementation and Security

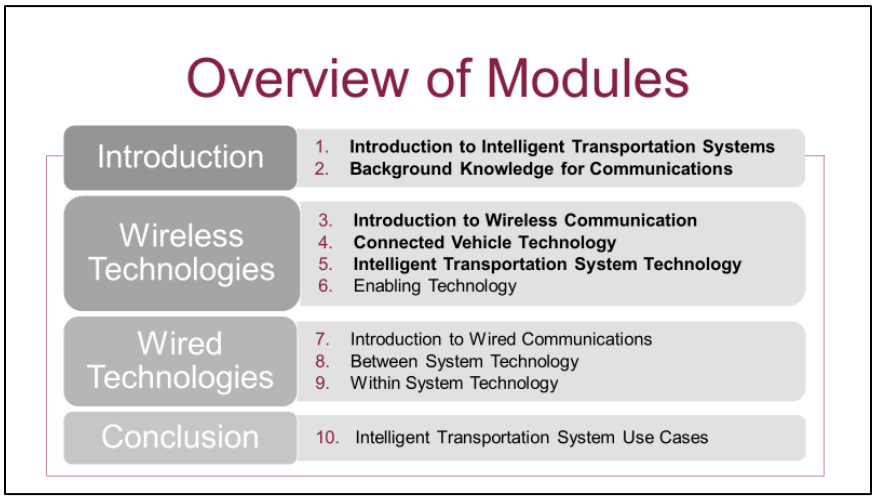


The security concept for CBRS uses a Public Key Infrastructure (PKI) that governs CBRS communications and requires Citizens Broadband Service Devices (known as CBSDs), Spectrum Access System (referred to as SAS), and Environmental Sensing Capabilities (or ESCs). The SAS uses a PKI to authenticate and authorize users based on a Root of Trust (RoT) that provides reliable functions the Certificate Authority (CA) can use to ensure security. The ESC network was completed in 2019 and ensures that transmissions are free from interference by both detecting an incumbent and reducing its interference.

Access Point cost can range from $1,200 to $4,500 and could be used in outdoor environments such as intersections. The user equipment cost ranges from $2,000 to $5,000 and can be used in-vehicle with specific SIM Cards.

Next

Overview of Modules

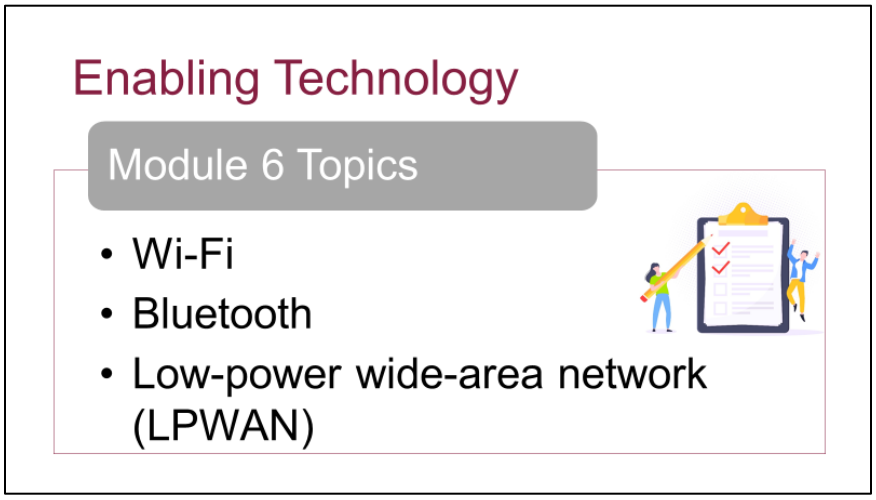


This concludes Module 5 – Intelligent Transportation System Technology learning materials. In the next module, we will continue reviewing wireless technologies including Wi-Fi, Bluetooth, and Low-Power Wide-Area Network (or LPWAN), but first, let's finish off with a quiz.

MODULE 6 – Enabling Technology

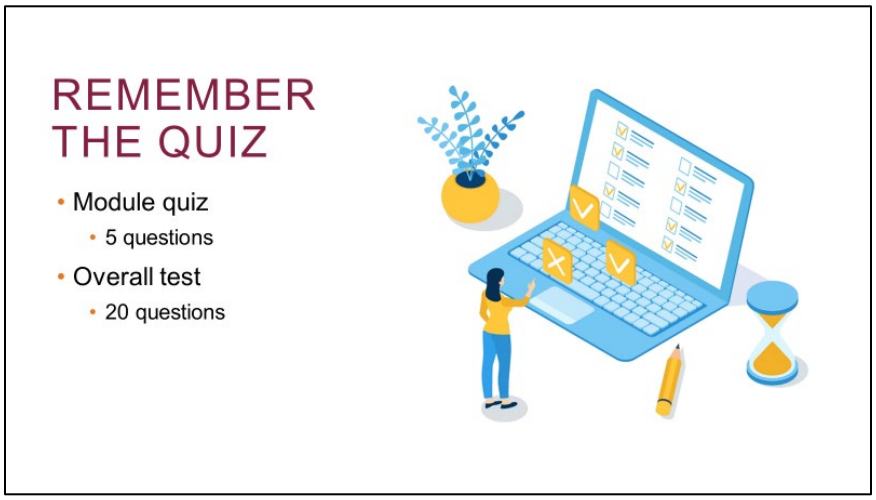
Overview

Enabling Technology



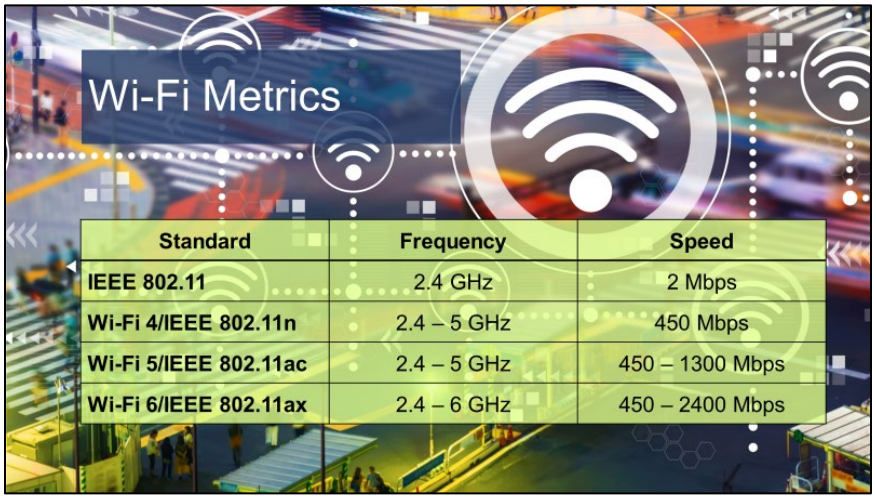
In Module 6 – Enabling Technology, we will cover metrics, implementation, and security for Wi-Fi, Bluetooth, and Low-Power Wide-Area Network (or LPWAN). These technologies are used to enable and facilitate communications within local area networks.

Remember the Quiz



Remember, there is a quiz at the end of each module with five questions for you to answer. At the end of the training, there will be an overall test with 20 questions.

Wi-Fi Metrics



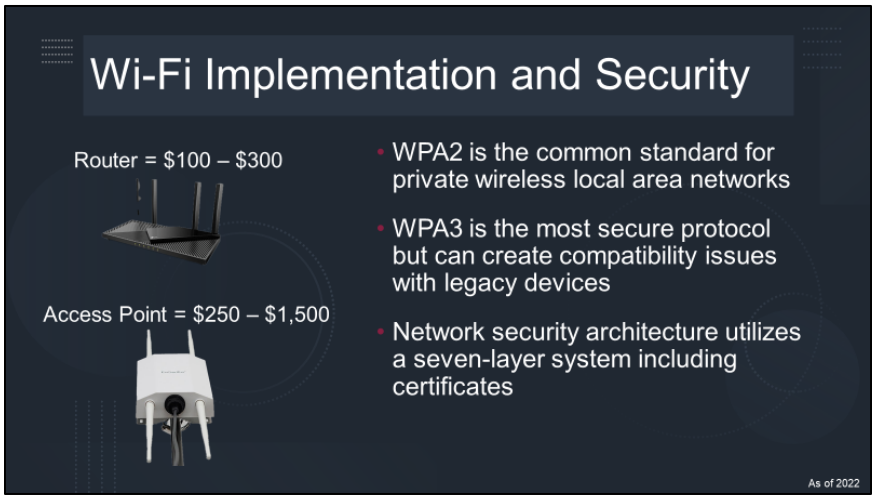
Wi-Fi is an umbrella term that refers to the most common form of short-range, high-speed wireless communication for internet traffic. Wi-Fi's standard has been updated as technology advanced, with each iteration denoted as a different protocol. Originally called Institute of Electrical and Electronics Engineers (or IEEE) 802.11 when released in 1997, this early standard operated in the 2.4 GHz frequency band with data speeds of 2 Mbps.

Most modern Wi-Fi connections are now "dual band," meaning they can operate in the 2.4 or 5 GHz range. The 5 GHz frequency uses new devices for close-range communication, while the 2.4 GHz frequency uses older devices adapted to prior standards. Newer devices can also be used at 2.4 GHz frequency in cases where the signal must travel further, travel through more obstacles, and/or travel through high-traffic environments where interference is present.

The Wi-Fi 4 standard IEEE 802.11n was released in 2009. This standard is noteworthy because it offered dual-band connectivity, which significantly increased data speeds to 600 Mbps with a range of over 70 meters indoors and 250 meters outdoors. The currently implemented standard is Wi-Fi 5, IEEE 802.11ac, which

provides speeds up to 1,300 Mbps at the 5 GHz frequency and 450 Mbps at the 2.4 GHz frequency. The latest standard, Wi-Fi 6, IEEE 802.11ax, has adopted a third frequency band of 6 GHz to provide even faster speeds but is more susceptible to interference from obstructions between the transmitter and receiver. It's worth noting that the data speeds listed are theoretical maximums and are heavily dependent on hardware.

Wi-Fi Implementation and Security



The security of Wi-Fi varies depending on the protocol implemented because some are more secure than others. WPA2 (which refers to Wi-Fi Protected Access Two) is the most common and has been the standard for private wireless local area networks. WPA3 was introduced in 2019 and is the most secure protocol in use as of 2022, but it can create compatibility issues with legacy devices. The network security architecture uses a seven-layer system that includes built-in protocol features such as firewalls, Virtual Private Networks (called VPNs), and anti-virus software. Authentication and encryption are implemented at the MAC (or Message Authentication Code) layer, and security certificates are implemented at additional layers.

An example Dual Band Wi-Fi 6 Router costs approximately $100 to $300 per unit. An example Wi-Fi 6 Access point suited for outdoor environments is approximately $250 to $1,500 and can be mounted discretely to infrastructure in a manner similar to 5G small cells.

Bluetooth Metrics and Implementation

Next, we will discuss Bluetooth technology. Similar to Wi-Fi, Bluetooth is a short-range technology that operates in the 2.4 GHz frequency band but has a lower bandwidth and transmission speed. The most recent iteration, Bluetooth 5.0, increased transmission speed to 2 Mbps and extended the range to 800 ft. Bluetooth 5.0 also introduced slot masking, which reduces interference by avoiding similar frequencies that are detected nearby. Bluetooth to USB adapters are fairly inexpensive, with models ranging from $10 to $30.

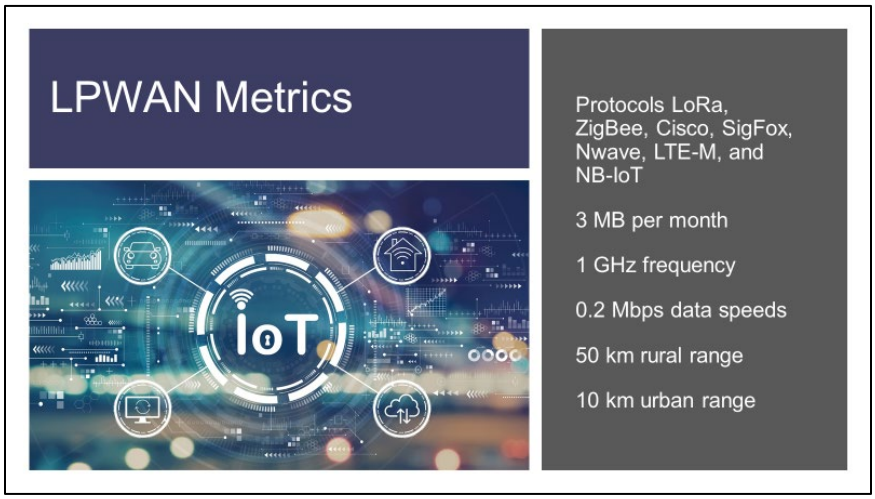
Bluetooth Security

Bluetooth can be considered slightly more secure than Wi-Fi due to its device pairing architecture and its lower range, which requires proximity to intercept data. There are two main security modes: LE Security Mode 1, in which security is enforced by encryption, and LE Security Mode 2, in which security is enforced by signing of data. We will first discuss the security levels within those security modes.

Security Mode 1 has four levels of security numbered 1 through 4 from least to most secure. Security Level 1 supports any Bluetooth communication without security and therefore does not require authentication or encryption. Increasing in complexity, Security Level 2 supports Federal Information Processing Standards (FIPS)-compliant encryption during unauthenticated pairing, while Security Level 3 supports encryption and pairing authentication. Finally, Security Level 4 supports encrypted pairing authentication as well as encryption for transmissions. Security Mode 2 has two levels of security that include Security Level 1 with unauthenticated pairing and data signing and Security Level 2 with pairing authentication and data signing.

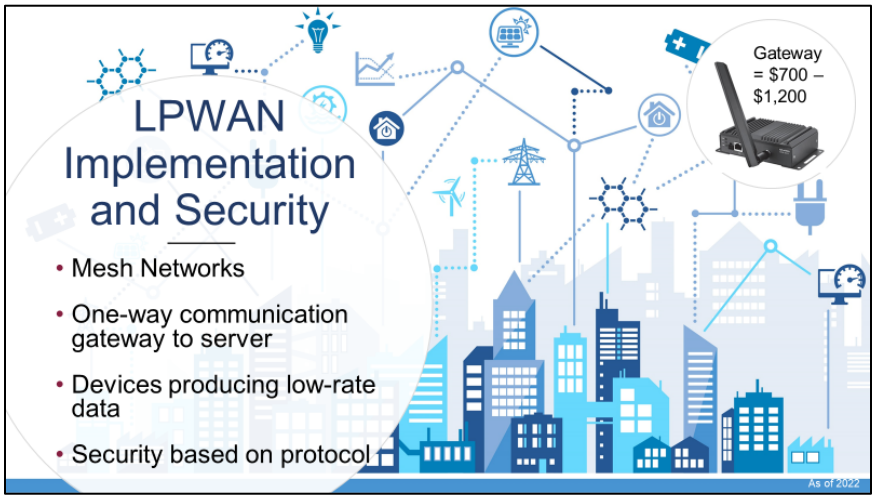
There are two additional security modes that combine elements from Modes 1 and 2 and their respective levels. The first is Mixed Security Mode, which is used when a device requires support for Security Modes 1 and 2, meaning it needs to utilize encrypted data as well as signed data. The second is Secure Connection Only Mode, which uses only Security Mode 1 with its Security Level 4, meaning it only supports authenticated connections and encryption.

LPWAN Metrics



Low-power wide-area network (or LPWAN) refers to a variety of communication protocols such as, ZigBee, SigFox, Nwave, LTE-M, NB-IoT, and LoRaWAN by Cisco. LPWAN is the primary form of communication for devices transmitting and receiving less than 3 MB of data per month, which account for almost 90% of deployed Internet of Things (IoT) devices. The protocols are generally low frequency, below 1 GHz, limiting data speeds at low power to up to 200 Kbps (0.2 Mbps). However, this low frequency also allows for a longer range of 50 km in rural environments and 10 km in urban settings.

LPWAN Implementation and Security



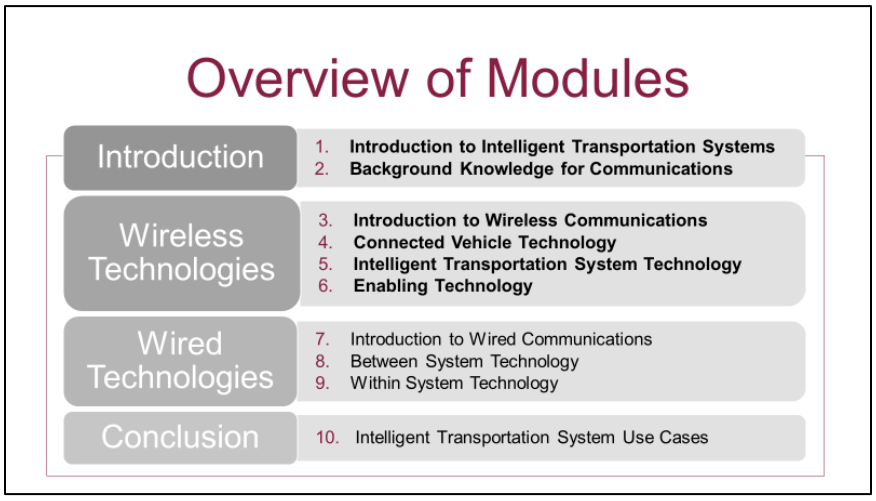
Most LPWAN technologies are one-way communication from the radio, or Gateway, to the server, which reduces the complexity, cost, and power consumption. However, LPWAN technology as well as other technology protocols can benefit from utilizing a mesh network structure. Mesh Networking is a unique local area network topology that operates dynamically through non-hierarchical and direct connections. This network configuration minimizes coverage gaps and enables effective workload distribution by allowing nodes to self-organize and transmit signals. Individual nodes receive signals from other nodes and forward them to the server or to other nodes which increases range and reliability. Additional power is required for operation, but because the network can maintain function if nodes are broken, maintenance costs can be reduced overall.

LPWANs can assume a variety of architectures and can run through public cellular, private cellular, Wi-Fi, Bluetooth, Fiber, and Ethernet depending on the application. These characteristics make LPWAN ideal for distributed devices producing low-rate data from sensors, such as a vibration detector for bridge monitoring, a water level sensor for flood detection, parking occupancy sensors, and emissions sensors for air quality monitoring. These technologies are specifically designed for very low power, enabling communication with tiny batteries that can last decades. Devices vary in price depending on several factors, including the protocol and sensing objectives, but they are typically low-cost ranging from under $100 to a couple hundred per device. An example Gateway (or radio) with Ethernet Interface costs $700 to $1,200. Mesh networks can be a cost-effective solution, as demonstrated with the implementation of 400 radios across 350 intersections and 130 data networks in Northern Virginia that potentially saved $600,000 on installation and operations.

Security for LPWAN is dependent on the specific protocol being used. For example, LoRaWAN security uses an Advanced Encryption Standard (AES) encryption method, while Sigfox uses a systematic process to maintain security. Sigfox broadcasts a radio message that is received by base stations and then transmitted to the core network before being routed to the receiving IoT devices. NB-IoT uses a three-layer system that includes the perceptron layer, transmission layer, and application layer that manages data access and control through integrity and authentication.

Next

Overview of Modules



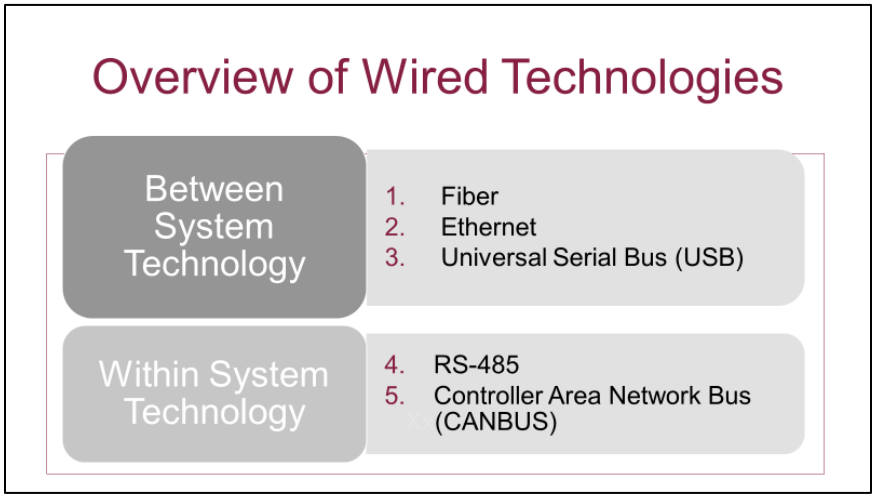
This concludes Module 6 – Enabling Technology learning materials. In the next module, we will discuss wired technology, its advantages, and its disadvantages, but first, let's finish off with a quiz.

UNIT 3 – Wired Communications

MODULE 7 – Introduction to Wired Communications

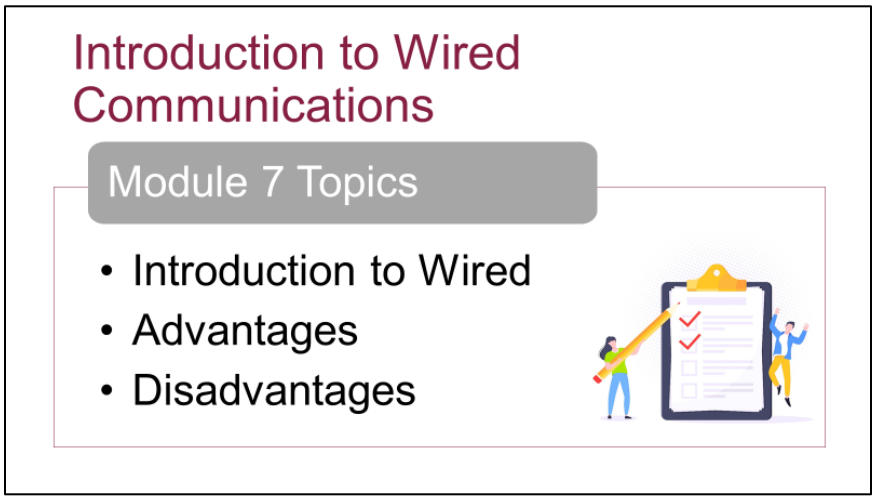
Overview

Overview of Wired Technologies



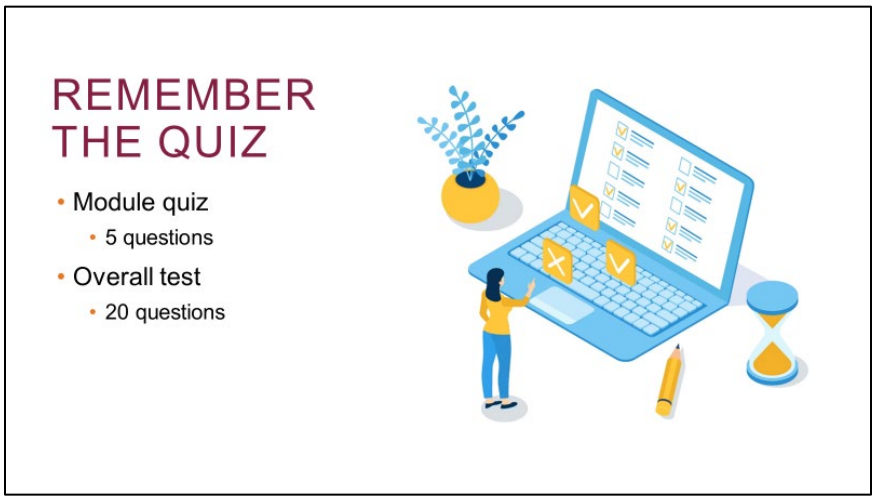
In this series of modules, we will discuss wired technologies used in between system technology and within system technology. Within those categories, we will review the listed technologies and discuss Fiber, Ethernet, Universal Serial Bus (USB), RS-485, and Controller Area Network (CAN) Bus.

Introduction to Wired Communications



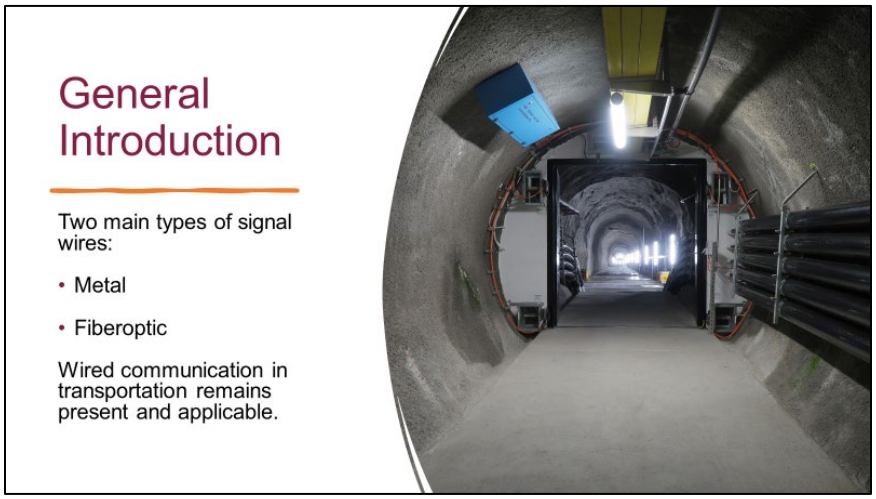
In Module 7 – Introduction to Wired Communications, we will cover a general introduction, advantages, and disadvantages of wired technology.

Remember the Quiz



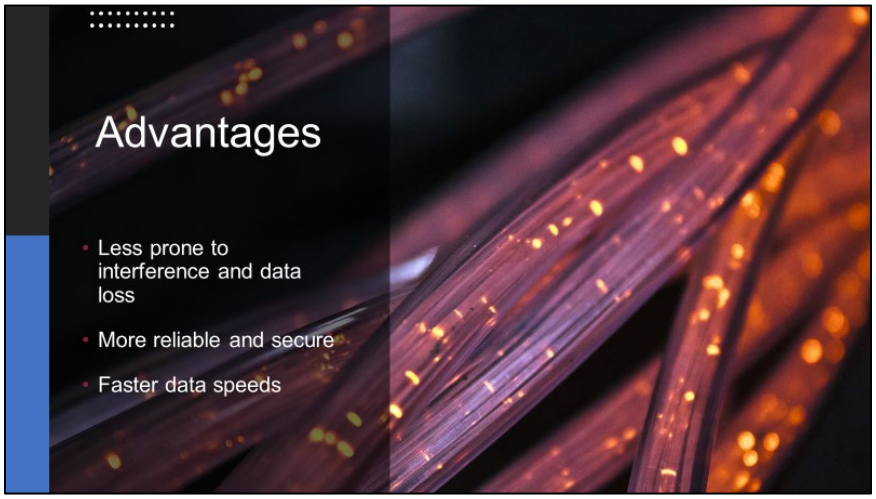
Remember, there is a quiz at the end of each module with five questions for you to answer. At the end of the training, there will be an overall test with 20 questions.

General Introduction



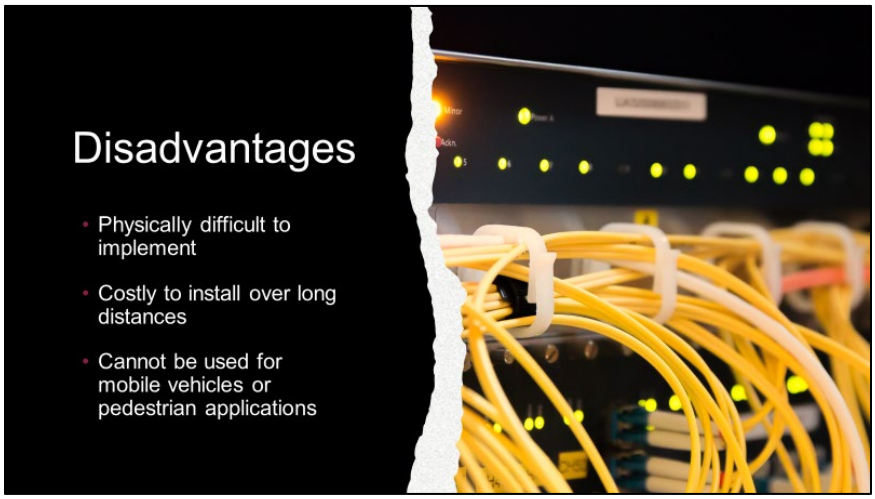
Wired communication signals are sent through two main types of signal wires: metal and fiberoptic. The use of wired communication in transportation remains present and applicable, especially when combined with wireless technologies to provide a total solution. For example, wired technology can also provide power, as is seen with Power over Ethernet (PoE), which is used when connecting a wireless device such as an access point to a power source.

Advantages



Compared to wireless communication, wired communication is less prone to interference and data loss, making it a more reliable communication method. Additionally, wired communications are inherently more secure because the wire must be physically accessed for the transmission to be intercepted. Wired communication data speeds are also typically faster than wireless.

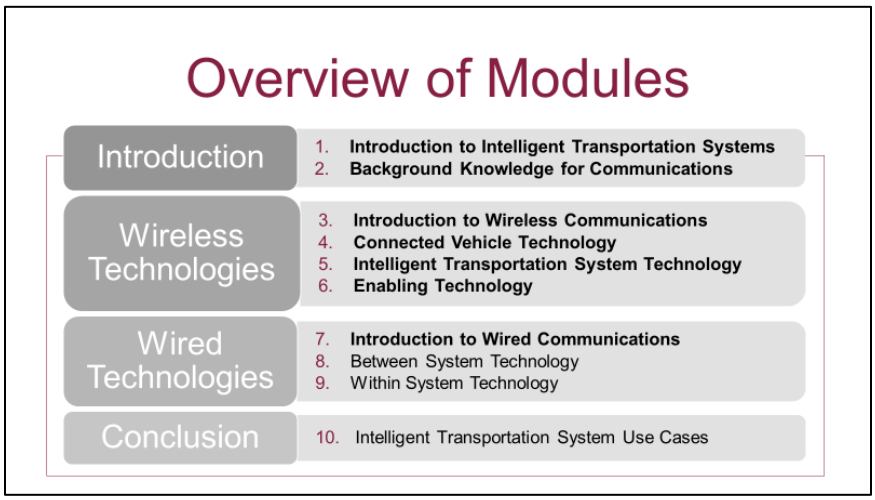
Disadvantages



However, wired communication can be physically difficult implement and costly to install over long distances when burying cable is required. They also cannot be used on mobile devices or vehicles for external communications with other connected vehicles or infrastructure elements.

Next

Overview of Modules

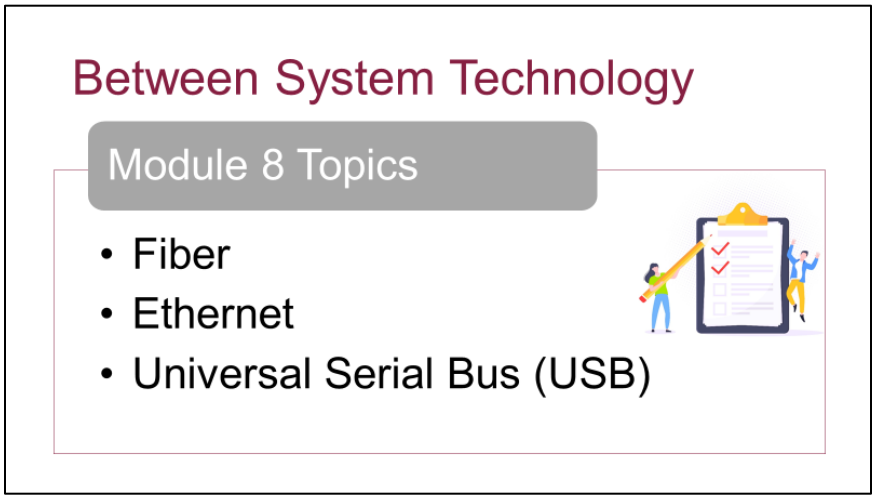


This concludes Module 7 – Introduction to Wired Communications learning materials. In the next module, we will discuss fiber, ethernet and USB, but first, let's finish off with a quiz.

MODULE 8 – Between System Technology

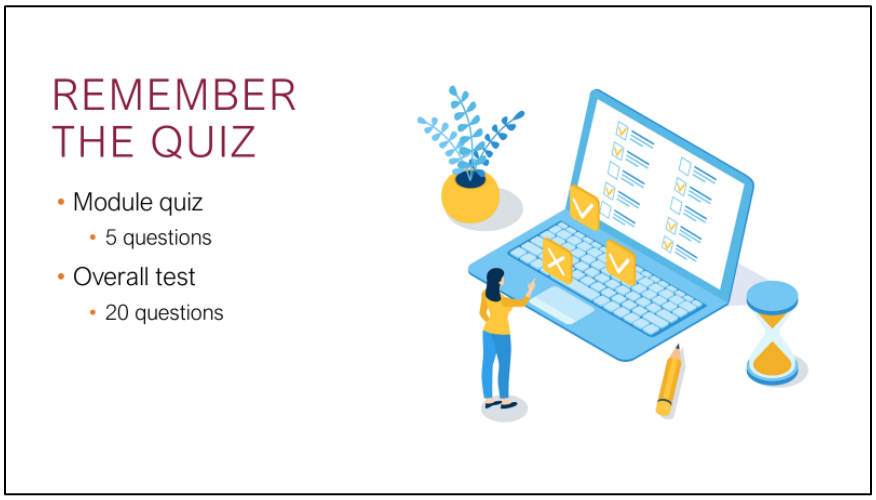
Overview

Between System Technology



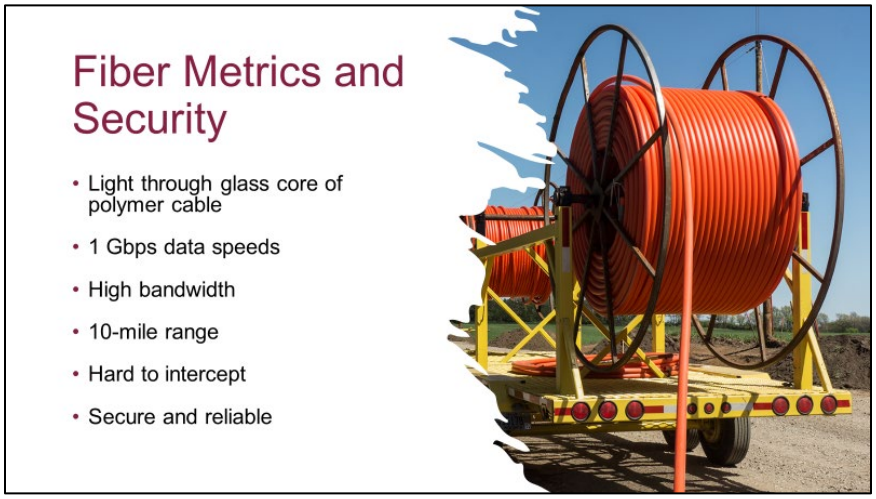
In Module 8 – Between System Technology, we will discuss metrics, implementation, and security for Fiber, Ethernet, and USB.

Remember the Quiz



Remember, there is a quiz at the end of each module with five questions for you to answer. At the end of the training, there will be an overall test with 20 questions.

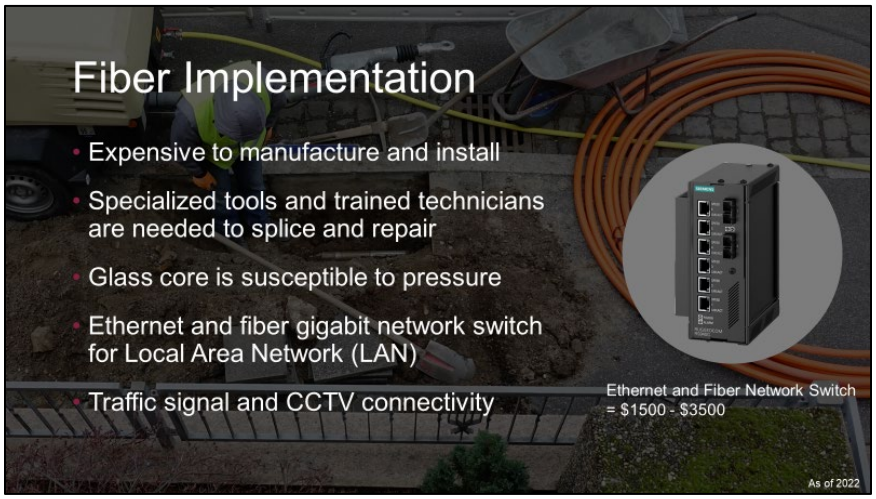
Fiber Metrics and Security



Fiberoptic cable, often referred to simply as fiber, delivers light through the glass core of a polymer cable instead of an electric current through a copper or aluminum cable. This method presents significant advantages over traditional cabling since light travels much faster than electrical signals and can be sent as a digital signal with light intensity being directly encoded into bits. This translates to high transmission speeds of over 1000 Mbps with extremely low latency and very high bandwidth. In addition, well-constructed fiber cables can achieve ranges exceeding 10 miles.

Fiber is very hard to intercept and difficult to tap because the wires used do not radiate electromagnetic frequencies like other technologies. From a physical perspective, this is the most secure and reliable form of wired communication technology.

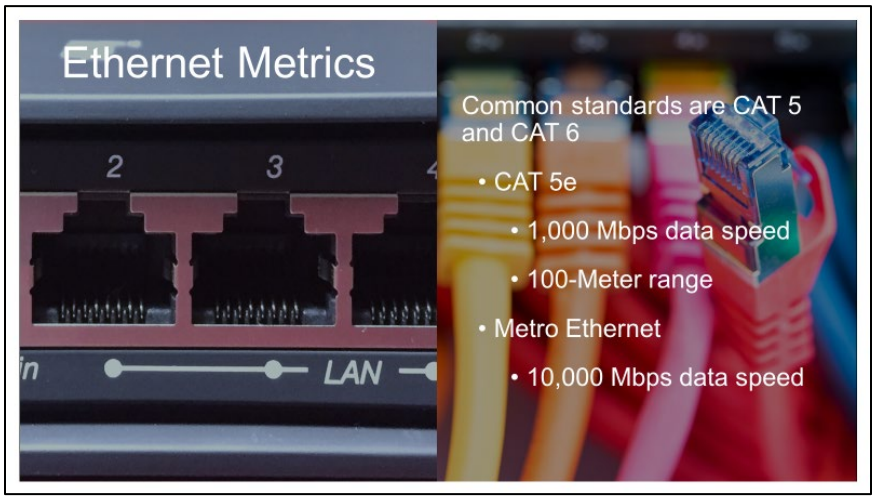
Fiber Implementation



However, like most of the technologies discussed in this training, fiber has its drawbacks. The cable and hardware are much more expensive to manufacture and install (5 to 10 times the cost of copper cable). Fiber also has some physical limitations not encountered with metal cabling. For instance, it is extremely difficult to splice and repair fiber in the field, requiring specialized tools and trained technicians. Fiber is less flexible relative to copper cable so it cannot be bent or put under significant pressure when buried without breaking the glass core.

Traffic management operations can utilize fiber to provide connectivity between distributed traffic signal equipment and a central traffic operations center (TOC). In addition to the costs associated with installing fiber cables, an ethernet and fiber gigabit network switch is also required. For connected intersections, these switches are installed within the traffic signal cabinet, and the cost can range from $1,500 to $3,500. Because fiber is ideal for higher bandwidth applications, it is often used to connect high-resolution CCTV cameras to a central TOC to support real-time surveillance and incident management.

Ethernet Metrics

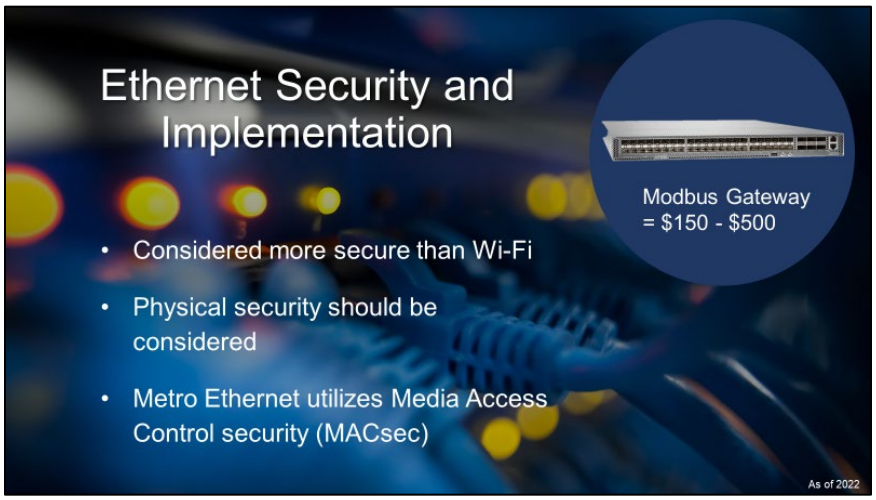


Ethernet is a wired network technology that provides high rates of data speed and power. Many different standards of ethernet have evolved from CAT 1 to CAT 8, the most common being CAT 5 and CAT 6. CAT 3 was the first to carry any substantial amount of data to establish local area networks, while CAT 5 was the first to accommodate Power over Ethernet (PoE), allowing for over 2.5 W of power transmission alongside

data. While the range and data speed can vary, CAT 5e offers data speeds of up to 1,000 Mbps with a cable range of up to 100 meters, or 328 feet. CAT 8 is currently used in smart mobility deployments to connect smart sensors to EDGE computing which requires the high bandwidth provided by this standard.

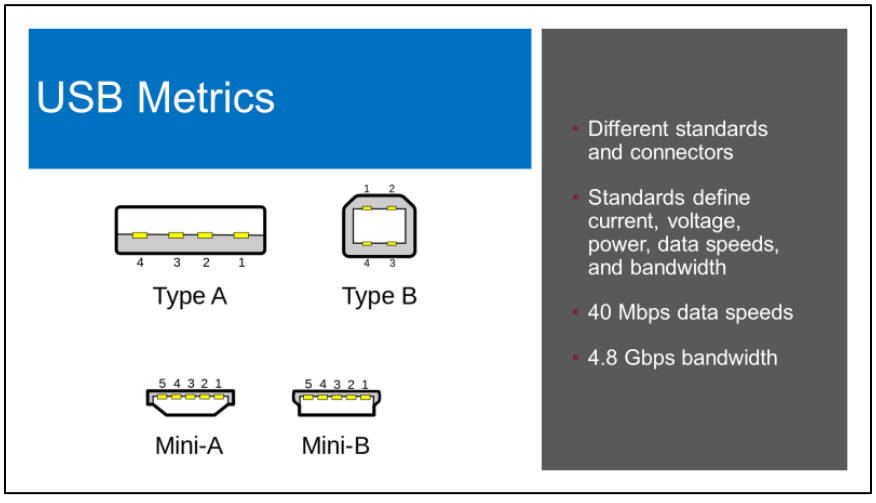
Due to ethernet's advantages such as its excellent durability and easy integration with Wi-Fi networks, it is the most common wired technology for internet traffic. Metro ethernet connections use metropolitan area network (MAN) technology and are utilized in transportation systems with data speeds up to 10,000 Mbps.

Ethernet Security and Implementation



Compared to Wi-Fi networks, an ethernet connection is considered more secure. In addition, like other wired technologies, physical security should be considered to prevent access to transferred data obtained through various tapping techniques. Metro ethernet utilizes Media Access Control security (MACsec) to detect and prevent threats from accessing and tampering with the network. An example router for Metro ethernet costs $45,000 to $55,000.

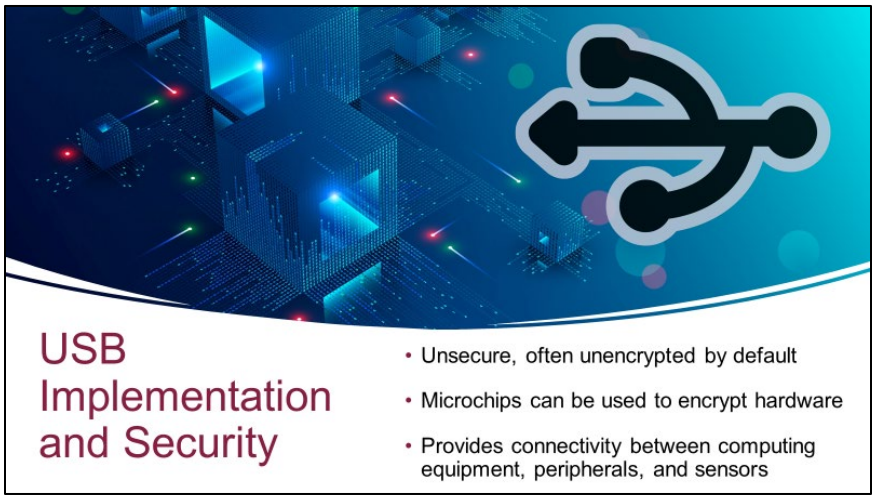
USB Metrics



Universal Serial Bus (or USB) offers reliable data transmission and can supply a significant amount of power. There are different USB standards and connectors currently utilized in a variety of combinations. For example, the standard USB 3.1 is operational with connector types USB-A, USB-B, USB Micro B, and USB-C. The USB standards are defined by different amounts of voltage, and power capabilities as well as the

maximum data transmission speed and bandwidth. The latest standard USB4 has a maximum data transmission speed of 40 Mbps with a bandwidth of 4.8 gigabytes per second. Additionally, USB4 can provide 20 volts producing 100 watts of power using a USB-C to USB-C connecting cable. The current bandwidth of most USB standards is larger than that of RS-485 (discussed next).

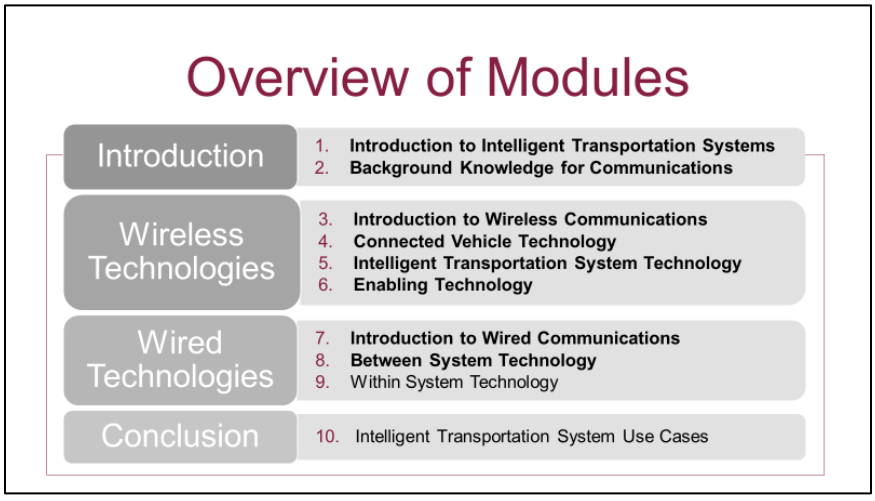
USB Implementation and Security



Most USB communications are unsecure, and storage drives are often unencrypted by default. However, microchips can be used in USB drives to encrypt the hardware, requiring a password for connectivity. USB connectivity can be used in a variety of transportation applications but is typically used to provide connectivity between computing equipment and a wide variety of peripherals and sensors. For example, an aftermarket infotainment system installed in a vehicle can be connected to and thus controlled by the driver's smart phone via USB.

Next

Overview of Modules

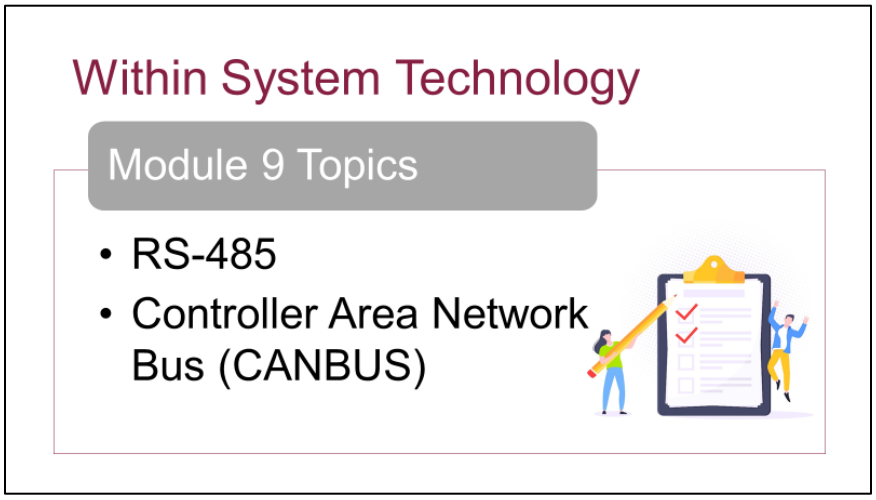


This concludes Module 8 – Between System Technology learning materials. In the next module, we will discuss RS-485 and Controller Area Network (CAN) Bus, but first, let's finish off with a quiz.

MODULE 9 – Within System Technology

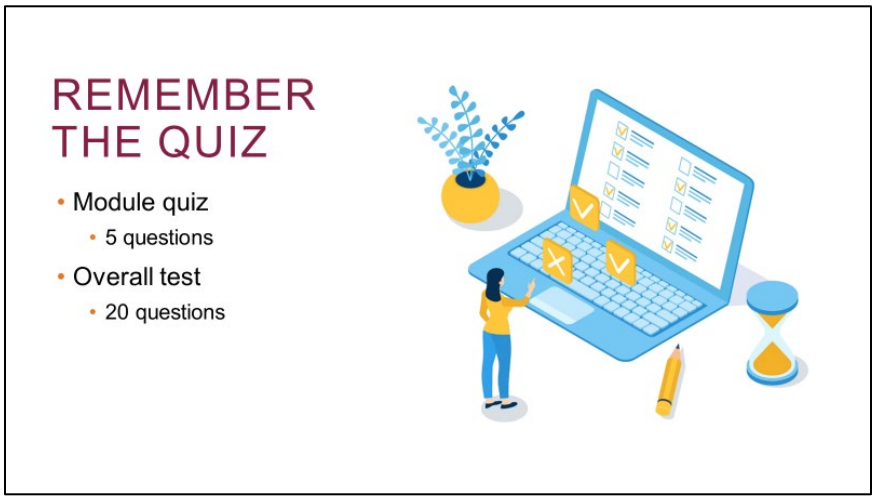
Overview

Within System Technology



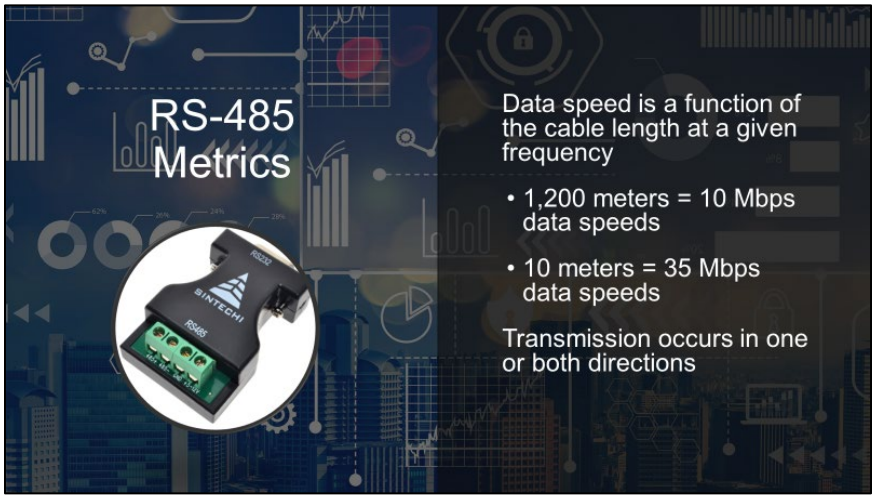
In Module 9 - Within System Technology, we will cover metrics, implementation, and security for RS-485, Ethernet, and Controller Area Network (CAN) Bus.

Remember the Quiz



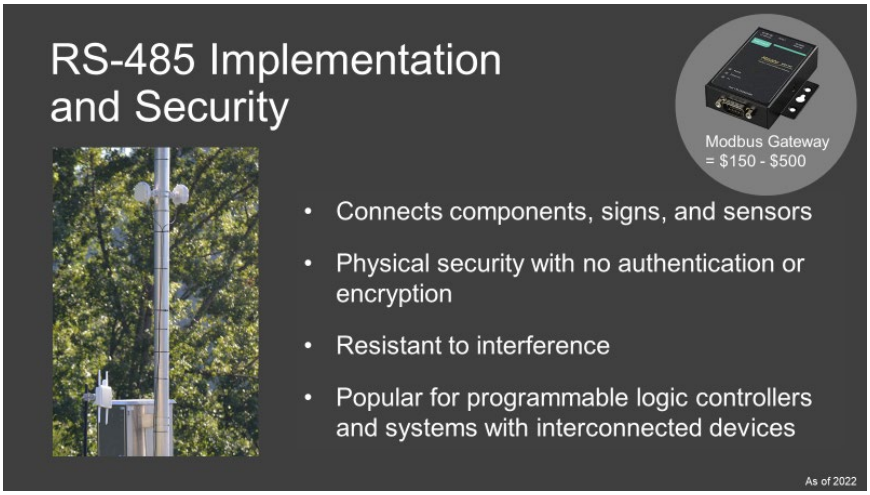
Remember, there is a quiz at the end of each module with five questions for you to answer. At the end of the training, there will be an overall test with 20 questions.

RS-485 Metrics



RS-485 stands for Recommended Standard 485 used in serial communications and is an older yet still reliable method of wired data transmission. RS-485 replaced RS-232 as a low-power alternative to point-to-point communication, and USB will soon entirely replace RS-232 as the high-voltage option. The data speed of RS-485 is a function of the cable length at a given frequency. The maximum cable length is 1,200 meters (or 4,000 feet), which would offer speeds of 10 megabits per second. Similarly, if the cable length is up to 10 meters or 32.8 feet, data speeds would be 35 megabits per second. RS-485 can be configured for use in two-way communications using a half-duplex system, where data is transmitted in only one direction at a time, or in a full-duplex system, allowing for transmission in both directions.

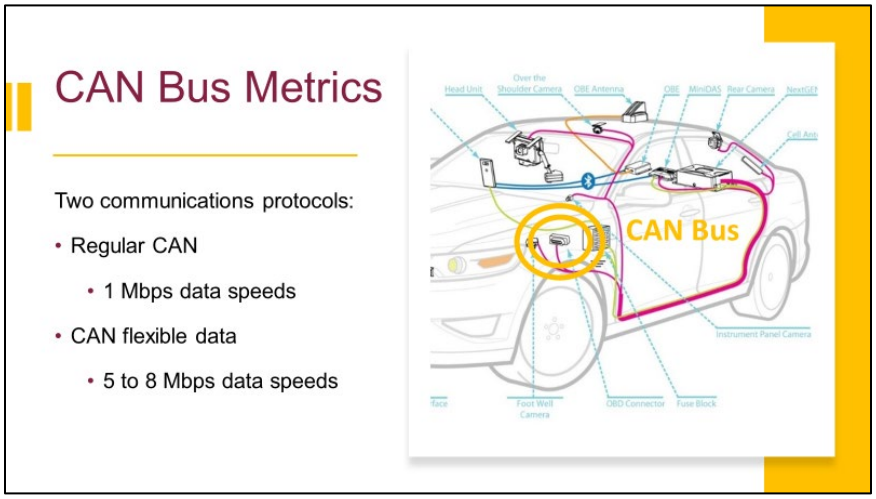
RS-485 Implementation and Security



The technology is still used in transportation to connect various traffic signal control components, signs, and sensors together, such as a fixed-speed sensor that measures the speed of passing vehicles. It is commonly used in computers to transmit data between the controller and a disk drive as well as in video surveillance and base stations. An example gateway costs approximately $150 to $500.

In addition, RS-485 requires physical security to prevent unauthorized access and also does not offer any authentication or encryption methods. Its resistance to electrical interference due to differential signaling along with its capacity for 32 controllers make RS-485 popular for use in programmable logic controllers and systems in which multiple devices need to be interconnected.

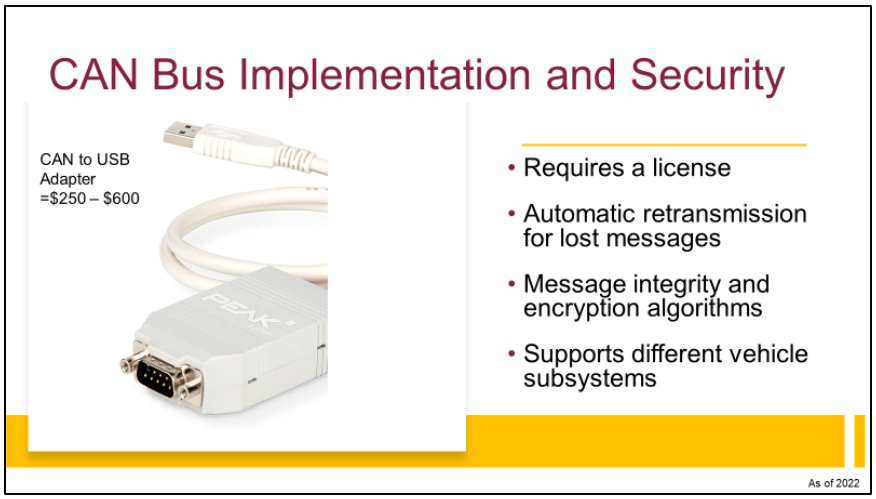
CAN Bus Metrics



Controller Area Network (CAN) bus technology is mostly found in cars and allows multiple controllers and sensors to communicate over the same network without a host. This reduces latency and decreases the amount of physical wiring, making CAN bus technology well suited for vehicle applications for which real-time processing as well as lightweight and compact packaging are required. CAN bus technology includes two communications protocols: regular CAN and CAN flexible data, with the main difference being the ability of CAN flexible data to switch between data rates based on the transmission size. Typically, CAN flexible data is used for broadcasting sensor data and to control information between connected instrumentation.

CAN bus offers data speeds up to 1 Mbps for cable lengths less than 40 meters or 131 feet. Similar to RS-485, the data speed is a function of the cable length; thus, a length of 500 meters or 1,640 feet provides data speeds of 125 Kbps. These are commonly referred to as high-speed CAN and low-speed CAN, respectively. The flexible data rate provided by CAN flexible data offers transmission speeds of 5 to 8 Mbps.

CAN Bus Implementation and Security

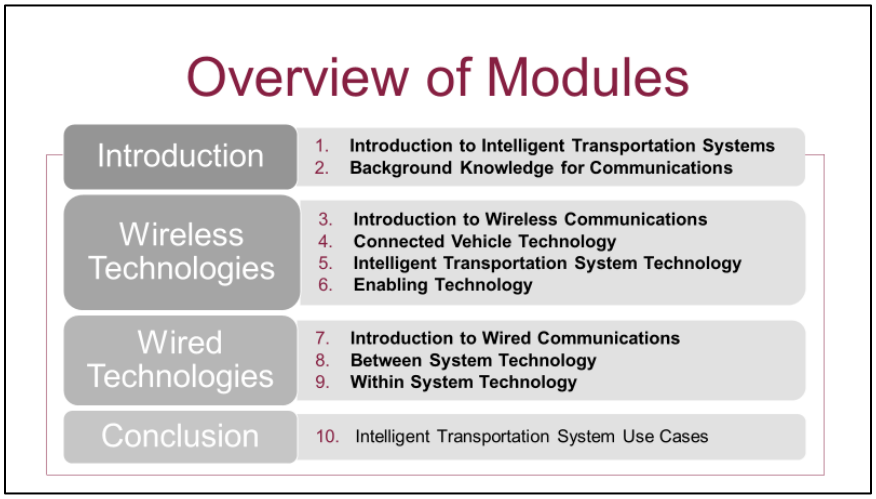


Compared to RS-485, CAN uses about 90% less power but is more costly. The use of CAN flexible data requires a license due to the high cost of software development and maintenance. It supports automatic retransmission for lost messages, but there is potential for signal integrity issues. However, CAN bus itself does not have any built-in authentication mechanisms but can ensure message integrity and use encryption algorithms. Due to the increase in message size caused by encryption, CAN bus will operate at an even slower transmission speed if utilized in this way. Message integrity, however, can be ensured using a Message Authentication Code (MAC) or an Authenticated Encryption with Associated Data (AEAD).

Many newer vehicles have multiple CAN Busses that each support different operational subsystems such as steering control, collision warning, and power management while providing varying levels of security. An example unit costs $250 to $600.

Next

Overview of Modules



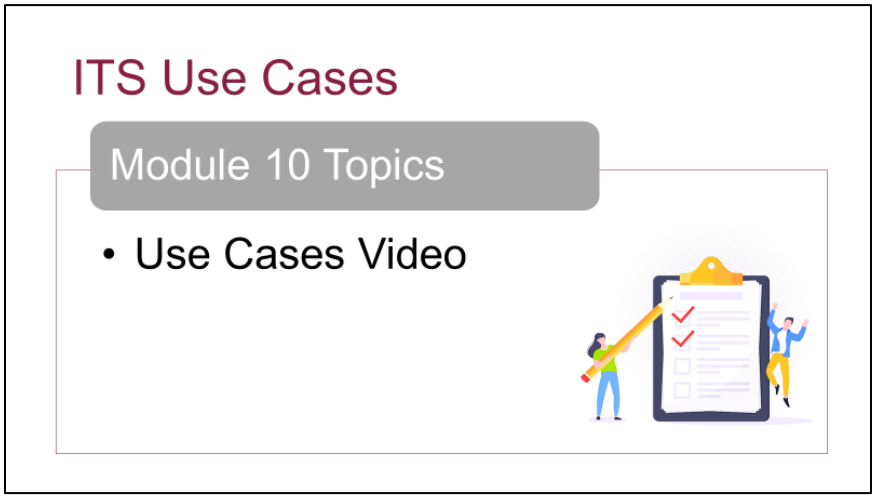
This concludes Module 9 – Within System Technology learning materials. In the next module, we will conclude this training by discussing use cases that showcase different connected environments applicable to Intelligent Transportation Systems.

UNIT 4 - Conclusion

MODULE 10 – ITS Use Cases

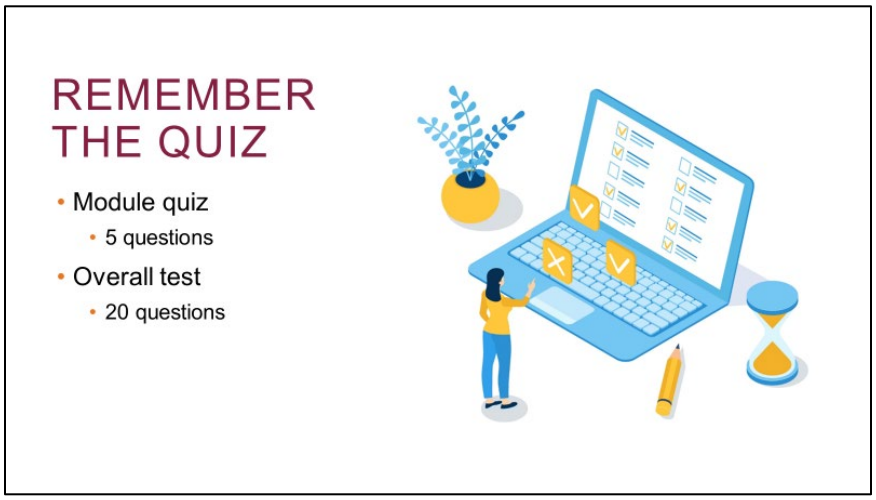
Overview

ITS Use Cases



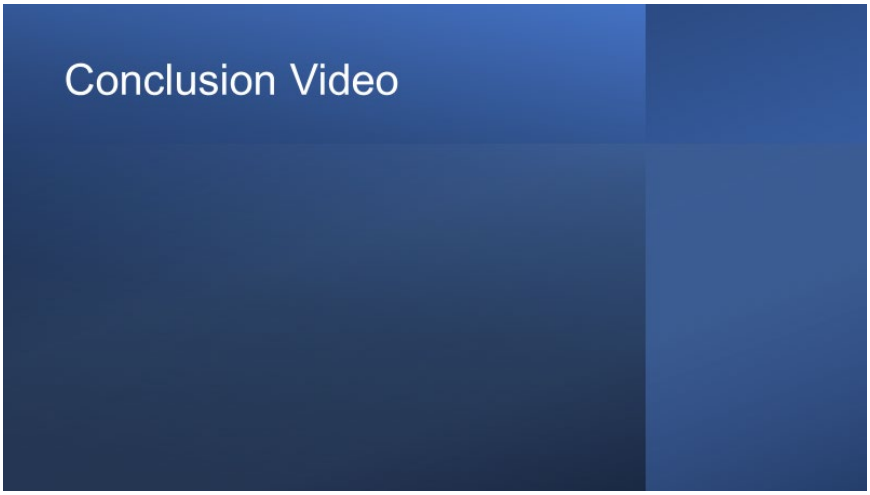
In Module 10 - ITS Use Cases, we will discuss use cases to provide an overview of cooperatively operating wired and wireless communications technologies.

Remember the Quiz



Remember, there is a quiz at the end of each module with five questions for you to answer. At the end of the training, there will be an overall test with 20 questions.

Conclusion Video



Wired and wireless technologies are critical to modern Intelligent Transportation Systems (ITS). Intersections are a common area for technology implementation to connect traffic control cabinets to other intersections as well as the Traffic Operations Centers (TOC). At its most basic, this connectivity allows Departments of Transportation (DOTs) to monitor and maintain traffic signal controller firmware and timing plans.

The connection can be through a combination of technologies. Fiber installations run under or above ground from TOCs and can be converted to ethernet via a network switch or to a mesh network via a gateway. Once converted additional connections can be made, for example from ethernet a Wi-Fi connection can be made through an access point or a 5G connection via a small cell. Once connected additional technologies can be added such a CCTV camera via ethernet to fiber or Road-Side Units (or RSUs) via ethernet to Cellular Vehicle to Everything (C-V2X).

Additionally, cameras and lidars can be connected to send data via ethernet to a processing system in the intersection cabinet. Those devices can be used to determine the presence of vehicles and pedestrians which

can then be transmitted from the RSU via a connection such as cellular. Traffic signal phase and timing data can also be transmitted for applications such as Red-Light Violation Warning and Optimize Speed Approach.

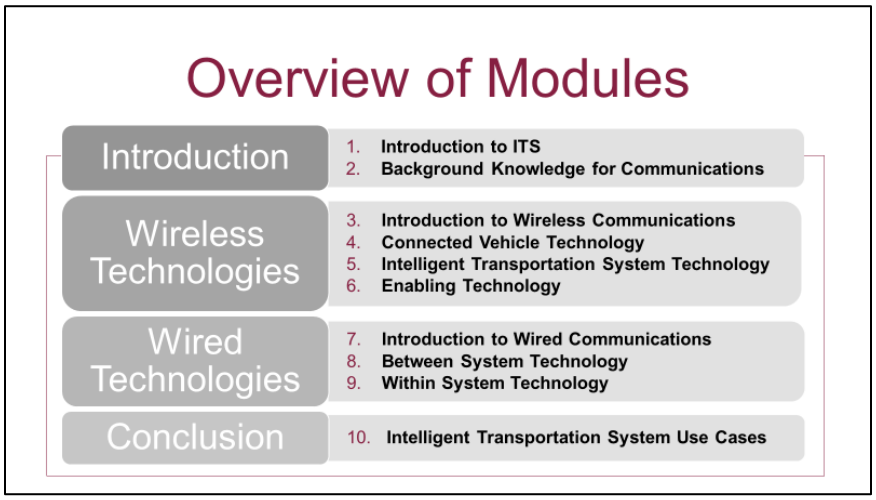
Vehicles are another key point of connectivity in ITS. Within vehicles a CAN bus to USB adapter can be used to connect radars to the onboard unit for detecting surrounding pedestrians and vehicles. As vehicles approach connected infrastructure such as RSUs the On-Board Unit transmits Basic Safety Messages (BSMs) including vehicle location, vehicle lane position, and speed via technology such as C-V2X.

Pedestrians themselves may have a phone or handset in communication with a server broadcasting their location out through the RSU as well as providing information regarding approaching vehicle trajectory and location.

In a mobile setting such as a work zone, an RSU can be mounted to a Truck Mounted Attenuator (or TMA) or Automated Truck Mounted Attenuator (known as an ATMA) allowing for workers to receive alerts when a connected vehicle approaches the activity area. This is made possible through BSMs and Personal Safety Messages (PSMs) containing similar information about location and movement.

Conclusion

Overview of Modules



This concludes Module 10 – ITS Use Cases.