CMAP Communications Systems Whitepaper

March 4th, 2020

Authors: Scott Lee, Charlie McCarthy, Yuan Chu, Duana Love, Andy Murray

Revision 1.6

Contents

1. Introduction

Intelligent Transportation Systems (ITS) consist of various systems and devices both in the field and at centers like the Traffic Management Center (TMC). The ITS communication network provides connectivity to these devices and centers, and facilitates successful command and control of transportation systems.

Fiber optic communication remains the state-of-the-art solution for traffic network infrastructure in terms of performance. This technology offers the highest level of speed, capacity and reliability. However, fiber-based communication is expensive and can be logistically challenging to deploy. It requires a continuous physical connection across the full communication distance, making installation and maintenance disruptive to the existing infrastructure. Fiber infrastructure is also prone to damage during adjacent construction activity and traffic incidents. The cables can be buried in a protective raceway to reduce the potential for damage, but this significantly increases the cost. Despite the associated costs, it is still the best solution when possible due to the performance benefits.

In scenarios where fiber is too expensive or impractical to use due to externalities, wireless alternatives exist and have been deployed in the region. Sections 3 and 5 further discuss these alternatives and their role in ITS regionally and nationally.

2. Regional State of the Practice

The Northeastern Illinois region features a wide variety of communication means and infrastructure dedicated to supporting Intelligent Transportation Systems.

The region’ s expressways and limited access toll facilities are largely operated by two entities: The Illinois Department of Transportation (IDOT) and the Illinois State Toll Highway Authority (ISTHA, or Illinois Tollway). Both have deployed substantial fiber optic networks throughout their regional facilities, which provide communications services for systems such as roadway lighting, pump stations, CCTV cameras, Dynamic Message Signs (DMS), Lane Control Signs (LCS), Active Traffic Management (ATM) gantries, and Active Travel Demand Management strategies such as ramp metering.

The fiber optic backbones from these limited access facilities are connected in specific locations to support Center-to-Center communications. There are direct connection points between IDOT and Illinois Tollway to support interagency data and video sharing. This connectivity also extends to regional county operations. Through fiber-sharing agreements Lake County, Illinois Tollway and IDOT are able to share video and other data. Traffic signals managed by IDOT and Lake County are connected to the fiber systems along IDOT expressways and Illinois Tollway facilities. The Lake County Passage Center is connected to IDOT District One’ s ComCenter, the IDOT Traffic Operations groups and the Illinois Tollway’ s TOC.

The fiber backbones provide sufficient communication capacity to support all agency activity. The use of virtual private networks (VPN), switching strategies, and appropriate security measures allow stakeholders within an agency to use dedicated bandwidth. IT management strategies including change control activities and coordinated and cultivated stakeholder relationships support these successes. For example, the Illinois Tollway’ s internal Business Systems and Traffic Operations networks are physically separate and isolated to provide high levels of autonomy and security, but are configured to allow the highly-controlled, real-time sharing of operational incident data and video between ISP and the TOC. In terms of maintenance and operations for the Illinois Tollway, the TOC and ITS systems are maintained through ITS Maintenance contracting.

IDOT, the seven counties, and the regional municipalities routinely work together to advance regional corridor connectivity. Expanding and enhancing local fiber network is a shared goal and pursuit across the regional municipalities. Arterial fiber optic network improvements are most often performed when and where those opportunities can be tied to other roadway or traffic signal capital improvements. As regional fiber coverage continues to increase, the quantity of traditional dial-up systems is decreasing towards zero.

Stakeholders are also exploring and deploying alternatives to fiber from a rapidly evolving marketplace. Like fiber enhancement projects, wireless deployments most often align with roadway and traffic signal construction contracts. Centralized Signal System software deployments are used in the region to operate large-scale signal systems, although the effectiveness depends on the reach and reliability of their network communication with signals - whether fiber or wireless.

The use of NTCIP standards has greatly improved interoperability between signal systems, particularly for larger deployments such as Lake County Passage. While those interoperability requirements remove obstacles and facilitate regional operational strategies for most stakeholders, there is progress to be made in the region. Going forward, interoperability requirements will allow for more dynamic approaches to control and monitoring agreements between agencies. Most signal timing operations remain the responsibility of the owning agency.

Regional transit agencies CTA, Pace Suburban Bus and Metra also make use of fiber optic communication, for use cases such as traffic monitoring and traveler information. Generally, rail transit throughout the region uses fiber communication to transport signal data, videos and Positive Train Control (PTC) to the control centers. These networks are also used to provide station Wi-Fi service to customers. CTA has installed fiber along all rail lines while Metra fiber installations are still underway. The regional bus services operated by CTA and Pace use fiber for transit signal priority (TSP) communication, transferring information between the traffic control center and roadside units. At transit stations, digital screens receive and display real-time traveler information via fiber.

With recent enhancements to the cellular network across much of the US, most municipalities are making use of cellular communications as part of their ITS network. Cellular services are common for temporary deployments and are generally reliable for most purposes. They are widely used in work zones to support portable devices, such as video cameras and electronic message boards. To date, cellular service has not been an effective method for sharing of HD video data. As 5G promises to enhance cellular communication capabilities by one to two orders of magnitude, that is expected to become more feasible.

Use of 5G cellular networks is expected to become widespread during 2020 and 2021. For now, counties and municipalities are diligent in monitoring the status of regional 5G deployments while considering the potential and expected impacts on ITS planning and deployment.

The region is beginning to consider ITS deployments in the environment of connected and autonomous vehicles - a handful of small-scale pilots are underway, but most stakeholders are awaiting industry lessons from the larger national pilot deployments. Note that the availability of 5G will greatly enhance the feasibility of cellular-based connected vehicle technology. In the following sections, we describe these emerging technologies in more detail.

3. National Perspectives of Telecommunications

Below is a brief discussion of three communication topics from the national perspective - fiber optics, cellular networks and communication safety and security issues. The discussion of each includes some background functionality details.

3.1 Fiber-Optic Communication

As stated above, fiber-optic based communication has long been viewed in the industry as the best option for ITS. Fiber-optic communication is a method of transmitting information by sending pulses of light through an optical fiber, in which the light forms a modulated electromagnetic carrier wave to carry information. A fiber-optic cable may consist of one to hundreds of individual fibers to carry light: the optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment.

The light in a fiber-optic cable travels through the core (hallway) by constantly bouncing from the cladding (mirror-lined walls), a principle called total internal reflection. Because the cladding does not absorb any light from the core, the light wave can travel great distances in ideal situation. However, some of the light signal degrades within the fiber, mostly due to impurities in the glass. The extent that the signal degrades depends on the purity of the glass and the wavelength of the transmitted light. Each fiber can carry many independent channels, each using a different wavelength of light.

Fiber is now preferred over electrical cabling when high bandwidth, long distances, or immunity to electromagnetic interference are required. A single fiber can carry much more data than electrical cables, is smaller and lighter, and is immune to electrical interference; there is no crosstalk between signals in different cables, and no pickup of environmental noise. Non-armored fiber cables do not conduct electricity, which makes it a good solution for protecting communications equipment in high voltage environments.

3.1.2 Typical Fiber Deployment Costs

The typical costs of fiber-based communication deployments are difficult to assess in isolation. Generally, communication enhancements are scheduled strategically to fit within other agency projects – for example, when an intersection is resurfaced or when a traffic signal is replaced, the fiber connectivity will also be enhanced as part of that project signal project.

While not applicable to all cases, a generic model was developed to frame the costs associated with fiber deployments. This is illustrated in Image X: Project Cost Model for Fiber Optic Cables.

The graph is a general model applicable to any communications system. Each labeled point on the graph is detailed in the bullets below:

- Offset "A" represents the fixed costs at the operations/data center. It includes the hardware, software, installation, and system testing. While the cost varies by the size and scope of the system, it is independent of the distance or length of the fiber cable run.
- Line-segments "B" represents a linear cost function based on fiber distance. It should include the cost of the cable and its installation, and the cost of the infrastructure. If required, additional splices can be included as an average cost per distance. This would increase the slop of the line segment associated with line-segments "B".
- Offset "C" represents the field equipment. It includes the communications hardware, cabinets, termination panels, network equipment, installation (including splicing), and testing.
- Line-segment "D" can be used as a rough estimate of total project costs. This line tends to underestimate the costs for short distances if it based on actual costs for a longer project. Rather than a line starting at the origin, a linear cost based on the following formula is more accurate:

$$Project\ Cost = A + (B * distance) + (C * number\ of\ cabinets)$$

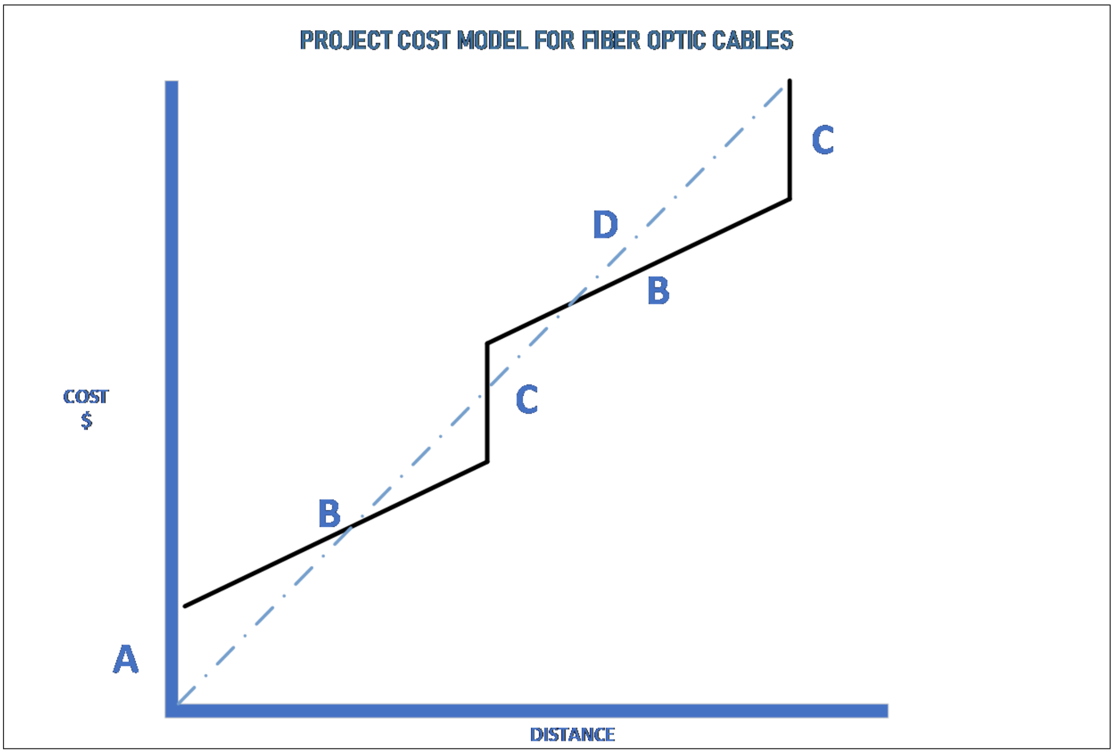

Image X: Project Cost Model for Fiber Optic Cables

3.2 Wireless Communications

Wireless ITS communications may be used when fiber optic cable may not be available or practical. Typical conditions that may prevent fiber use include:

- Lack of Right of Way
- Restricted Right of Way
- Environmentally sensitive areas
- Construction projects affecting existing fiber
- No nearby fiber infrastructure

3.2.1 Private Agency Wireless Network

Private wireless networks are agency owned and not shared by the public. This type of network is more secure and will not have recurring monthly costs like cellular or leased lines. The design of the network needs to take into consideration many factors including interference. The use of FCC Licensed frequencies will minimize interference. However, unlicensed frequency designed properly will work well.

Unlicensed wireless radio systems can transfer data at rates of 10Mbps to 300 Mbps over great distances in point-to-point or mesh configurations. The City of Chicago is a major user of wireless radio systems. A wireless network is typically designed to extend from the edge of the existing fiber network to cover an area that contains one or more devices.

3.2.2 Public Cellular Network

A cellular network, or mobile network, is a communication network where the last link is wireless. The network is distributed over land areas called "cells", each served by at least one fixed-location transceiver, but typically three-cell sites or base transceiver stations.

The original iteration of a national cellular network was known as 1G, while the most recent is referred to as 5G. Below is a summary of both iterations and those in between:

- 1G: The first commercial analog cellular network. Launched in Tokyo, Japan by Nippon Telegraph and Telephone Corporation (NTT) in 1979.
- 2G: The first commercial digital cellular network launched in 1991, introduced data services for mobile phones.
- 3G: High-speed cellular network compared to 2G. Increased information transfer rate to at least 200 Kbit/s.
- 4G: Currently deployed in most US areas, 4G provides a peak speed at 100 Mbit/s for high mobility communication, and 1 Gbit/s for low mobility communication.
- 5G: Current generation being developed and deployed today. It is expected that the speed of a 5G FR1 network will be 2Gbit/s. International Telecommunication Union's IMT-2020 standard required a 5G theoretical peak download speed of 20 Gbit/s and 10 Gbit/s upload speed.

The air interface for 5G is known as New Radio (NR), and the specification is subdivided into two frequency bands, FR1 (below 6 GHz) and FR2 (mmWave, >24 GHz). FR2 mmWave has a lack of signal coverage as it uses a higher frequency to transmit signals and will have less penetration through building walls or underground basements, or attenuation due to rain.

Agency systems using cellular networks are easy to deploy where service is available. The public cellular network should be a second choice when a private agency network is not available. The network availability is not guaranteed on the public network, as all users of cellular communication in the area share the same network. Major events or incidents can cause localized network congestion, and agencies sharing these same resources are subject to that congestion. Agencies may be able to negotiate priority preemption with the carrier to guarantee level of service over the general public for public safety.

3.2.3 Cellular 5G: Trends and Trajectory

As of 2020, cellular providers have moved toward a multi-tier 5G strategy that relies on three types of 5G radios: low-band, mid-band, and high-band (high-band is sometimes referred to as ultra-high-band, small-cell or mmWave). Each type of 5G features its own distinct frequency and transmission range (these two characteristics have an inverse relationship).

For example, the high-band mmWave technology has a very short range and cannot penetrate walls, but provides extremely high speeds. While range is limited to around 0.75 miles in urban settings, demonstrations and deployments to date have yielded speeds of 1-3 Gbps (30-80 times faster than typical 4G speeds). Further, chip manufacturers claim subsequent versions will achieve speeds of up to 7 Gbps using the high-band technology.

Initially, mobile providers and enthusiasts considered the high-band 5G to be the only 'true' opportunity to achieve 5G technology. Verizon, for instance, was of this mindset as recently as 2019. However, the interference limitations of high-band coupled with the feasibility and speed provided by low-and mid-band solutions have recently altered this landscape.

The trajectory toward a multi-tiered 5G was recently clarified and solidified by the wireless provider T-Mobile. Their low-band 5G network is now widely available and can be measured for performance and use cases against 4G and the faster high-band 5G.

Low-band 5G operates in the 600 MHz range, which has been used in the past for legacy technologies such as analog television broadcasts. At this frequency, a single Low-band 5G tower can provide an enormous coverage range - according to T-Mobile, hundreds of square miles. While significantly slower than the mid-and high-band varieties, low-band 5G could provide a worst-case coverage across the entire country for locations unable to receive mid- or high-band coverage. For many use cases, low-band will be sufficiently fast - to date- T-Mobile' s low-band 5G has shown top speeds around 225 Mbps, which is approximately six times faster than typical 4G speeds in the US today.

Mid-band falls in between low-and high-band performance in terms of both speed and coverage. Operating in the 3.5-3.7 GHz range, often referred to as 'sub 6GHz bands,' mid-band radios can provide coverage for users within several miles of the tower. One benefit of this frequency range is that there is more transmitting spectrum available for use.

The mobile provider Sprint has deployed mid-band 5G in the US using 2.5 GHz frequencies. Testing has shown this network to provide speeds of at least 125 Mbps. In some Asian countries, carriers are already promising speeds as high as 2 Gbps using mid-band 5G networks.

Mid-band networks are likely to be deployed widely in US cities and suburban areas, but existing coverage remains very limited to date. It is quite possible that certain mobile providers decide to provide only mid- and high-band networks, skipping the low-band 5G altogether. As users, this will mostly occur in the background – wireless providers will shift individual users from low-, to mid-, to high-band networks seamlessly based on location, use case, and network capacity.

3.2.4 Wireless Providers: Leveraging Expertise and Infrastructure Access

Wireless providers and related industries are actively working to standardize, regulate, deploy, and popularize the use of 5G wireless networks. Simultaneously, transportation agencies in the region are all actively working to expand and enhance their ITS communication systems and network, as outlined in previous sections. These parallel pursuits, in addition to the greatly enhanced capabilities that 5G networks promise in general, provide a unique opportunity to revisit the region' s typical interactions with wireless providers.

Plans must be made to account for immediate and future expansion of communication networks, wireless, fiber based, and others. Wireless carriers in particular are focused on time-to-market, given the race to 5G, and their interest in network expansion, that is both efficient and economical.

Wireless providers have a variety of solutions to choose from when it comes to building their networks: public right-of-way, private property, collocation on existing structures, and acquiring property rights for construction of new structures as part of long-term property leases. Because wireless providers have options, and in order to position itself better for future communications needs, the Region should look to work with wireless providers, provide a transparent process, and work to understand the needs of wireless providers, so that a deployment in the Region meets their time-to-market demands.

Beyond choice, wireless providers seek solutions for equipment installation that have favorable zoning and permitting processes. The Region will put itself in a position for success by having an outlined review and permitting process that is clear, consistent, efficient, and seeks to engage with wireless providers early and regularly. Typically, this can be accomplished with intake meetings, regular status meetings, and field walks as necessary. These meetings facilitate communication, so that the Region may establish guidelines and requirements to the wireless providers, and the wireless provider in turn may express their priorities, plans, and questions. Online review and permitting portals will help facilitate this, allowing the Region to maintain control, and also for access, as appropriate, for applicants (wireless providers, and others).

The need for an organized process is fueled by the exponential expansion of telecommunications, as part of the race to 5G. The increased capacities of these 5G and other networks pave the way for development of the Region' s ITS-supportive communication system.

3.3 Network Security

As public and private demand for connectivity continues to increase, systems inherently become more vulnerable to attack. Indeed, as the nation ushers in Connected and Autonomous Vehicle technologies for ground vehicles, and drones begin to fill the skies, vehicles themselves are increasingly vulnerable. Simultaneously, the use of cyber-based attacks has become prevalent nationally and globally. As malicious techniques continue to mature, this growing threat is unlikely to dissipate in the near future.

Nationally, there have been many examples of ITS devices and systems being hacked in recent years. While examples of successfully hacked electronic message boards can be framed as harmless (e.g., 'Zombie Apocalypse Ahead'), the potential for nefarious interference with system operations is clear and should not be taken lightly.

The recent wave of ransomware attacks on local government agencies have led to major service disruptions and many millions of dollars in data recovery expenses. Well known examples of attacks on transportation agencies include the San Francisco Municipal Transportation Agency (SFMTA) ransomware attack in 2016 and the Colorado DOT ransomware attack in 2018. In each attack, over 2,000 agency computers were infected. At the Colorado DOT, its affected systems were only 80% restored after 30 days and some data was permanently lost.

Effective, modern network security is facilitated by a complete understanding of the included systems, their interdependencies, and their respective importance. Systems that must be well-integrated into these considerations include: the cyber-physical control systems, traffic and information management systems, fare collection systems, safety management systems, and traveler and operator services. In ITS operations, it is imperative to be able to quickly interpret the relevance, accuracy, importance, and the associated dependencies of any information that is received or used.

Fortunately, these security considerations and processes fit well within the greater systems engineering process, which is already being used in regional ITS planning and deployment. Cybersecurity best practices - such as risk assessment, lifecycle consideration, standardization, certification, maintenance and operations – need to be regularly evaluated and further integrated into the regional design and deployment processes to enable a sustainable and resilient ITS cybersecurity ecosystem.

As society's dependence on information systems and networks continues to increase, the associated security risks become more significant. Creating a local and regional culture around the importance of cybersecurity will help to align stakeholders. Widespread collaboration will be critical in achieving and maintaining this evolving environment.

The National Institute of Standards and Technology (NIST) was directed by a 2014 law to develop a cybersecurity risk framework for voluntary use by critical infrastructure owners and operators. It has since evolved into a family of standards, guidelines and practices. However, governmental bodies and industries face different threats, and have different vulnerabilities and risk tolerance. Accordingly, these guidelines are to be tailored as needed.

The US Department of Homeland Security (DHS) published guidelines for applying the NIST framework to transportation systems in 2015. The USDOT published a "Best Practice Guide" in 2019 addressing how to plan and conduct a "Penetration Test" to uncover any exploitable vulnerability in your transportation organization.

With 8.5 million residents, 25% of the nation's freight trains and 50% of the nation's intermodal trains passing through, the Chicago area is one of America's largest transportation hubs. The compromise of cybersecurity at any level in the Chicagoland regional transportation system could result in one or several of the following adverse outcomes:

- The endangerment of public or employee safety
- The loss of private personal data or proprietary business information
- Economic losses
- Impact on National Security

Each transportation organization in the region – one where transportation is the critical infrastructure that keeps its economy functioning – should consider the importance of voluntarily creating themselves a Cybersecurity plan. It is time for agencies to treat cybersecurity attacks as inevitable occurrences and plan accordingly.

3.4 Network Management System

The Network Management System is also critical to operations. The system is a server in a data center or cloud that uses software to interrogate devices on the network. The system can proactively detect problems to alert personnel.

4. ITS Industry Assessment

The industry as a whole has a broad spectrum of ITS network topologies. Layer 2 and 3 networks are prevalent nationally and throughout this region. Many of the networks in the region resemble this type of topology. Implementation of these networks remains routinely tied to other capital improvements such as intersection improvements or reconstruction projects.

ITS Networks currently are designed with the TMC connected via fiber to Node buildings spaced at several miles apart. The Nodes typically have fiber on both sides of the roadway and are connected in a ring fashion to form a protected loop. The network link is typically a dual 10G (Gbps) fiber path between each node on both sides of the roadway to provide redundancy in the event of incidental fiber damage. The ITS field devices are then connected to each Node in a protected ring so that if the connection is lost or damaged the ring can heal to prevent a communication outage. The devices are typically connected with a 1G fiber path to the Node. Virtual LANs are also used to segregate network traffic and optimize performance.

TMC core fiber network and node buildings often inclue stacked layer 3 switches for redundancy with 10G and 1G fiber ports. The switch hardware must be scaled to support the network traffic from the field. Video devices in the field consume the most bandwidth and multicast video design needs to be utilized for network congestion.

Utilizing fiber optic cabling allows for scalability. When 10G needs to be increased (40G, 100G), the fiber itself can accommodate the new network hardware architecture.

At this time CCTV video is the biggest user of bandwidth on these networks. The ability to effectively share and control high resolution video streams is the driver of network configurations and designs. The forecast for connected vehicle data transmission such as Basic Safety Message data is generally straightforward to estimate given existing standards and the ability to project the number of vehicles on the roadway. However, DSRC and/or 5G C-V2X opportunities and prevalence are still very low. Based on pilot tests, a very small percentage of vehicles are broadcasting data directly consumable by stakeholders. Many automobile manufacturers are using private cellular services to collect data per manufacturer versus broadcasting directly into a V2X environment.

Regionally CDOT, IDOT and county level signal improvement projects and reconstruction projects continue to replace copper based comm with fiber optic solutions which better support CCTV video and the potential for more V2I types of connectivity. These connectivity goals extend to regional initiatives and the dedication of several fiber strands to fill agency to agency gaps and to promote regional integration.

5. Connected and Autonomous Vehicles

Connected vehicle technology has the potential to transform the way Americans travel by using modern telecommunication technologies to share safety, mobility, and environmental information. This is achieved by the transmission of high or low-frequency, low-latency messages containing vehicular or infrastructure-based data, sent between vehicles, devices, and networks.

Four common bidirectional transmission paths of message transmissions are included in connected vehicle technologies:

- Vehicle-to-vehicle (V2V)
- Vehicle-to-infrastructure (V2I)
- Vehicle-to-network (V2N)
- Vehicle-to-pedestrian (V2P)

These four message paths are commonly referred to together as Vehicle-to-everything, or V2X communication.

Typical Equipment in a connected vehicle deployment, leveraging DSRC to achieve V2V and/or V2I services, consists of two device types: On-Board Units (OBUs) and Roadside Units (RSUs).

An OBU is a transceiver that is normally mounted in or on a vehicle, or in some instances may be a portable unit. An RSU is a transceiver that is mounted along a road or pedestrian passageway, generally attached to part of the existing infrastructure in the same way other ITS devices would be. RSUs and OBUs can exchange two-way information with each other when within range, and can also exchange information with pedestrians (via smart phones) and the agency's communication network.

From 1999 – when 75 MHz of spectrum were reserved for DSRC-based vehicle safety applications – until very recently, the intention of USDOT and the industry had been to rely on Dedicated Short-Range Communication (DSRC) technology to achieve this connectivity between vehicles and other entities.

However, since the original DSRC plan, an abundance of subsequent occurrences and decisions have contributed to the rise of a suitable alternative. This technology uses cellular-based communication, and is referred to as C-V2X, or 'cellular vehicle to everything.'

As of December 2019, the FCC has proposed and voted to alter the spectrum in the following ways:

- Removal of the lower 45 MHz (5.85 to 5.895 GHz) portion of the reserved spectrum for unlicensed use, and
- Re-allocation of another 20 MHz (5.905 to 5.925 GHz) to vehicle communication applications using C-V2X.
- Maintain 10 MHz for DSRC-based vehicle communication applications.

The recent vote has not been met favorably by some national transportation stakeholders, including USDOT. The FCC is now requesting comments on this preliminary approval from stakeholders before solidifying the spectrum change policy. Relevant stakeholders are encouraged to submit commentary as they see fit.

There is a noteworthy proposal by the IEEE 802.2 LAN/WAN standards committee to harmonize C-V2X and DSRC in their next generation V2X standards (NGV). This would allow C-V2X and DSRC to operate in the same band and be compatible with existing DSRC infrastructure.

The conversation on connected vehicles, DSRC and C-V2X is ongoing, complicated, and has expanded to include many industries. While a single technology could theoretically prevail as the sole CV communication method eventually - for instance, through a federal vehicular mandate - it is best for now that the industry and region approach and understand both technologies as plausible alternatives. Indeed, both technologies are actively being deployed nationally. Accordingly, sections 5.1 and 5.2 provide details on these two technology types.

5.1 Connected Vehicle Communications: DSRC

Dedicated short range communications (DSRC) has been the primary V2X strategy of the U.S. Department of Transportation (USDOT) with extensive research and testing, but is now challenged by Cellular V2X (C-V2X) as 5G technologies emerged.

DSRC is a two-way short-to-medium range wireless communication protocol, as a derivative of Wi-Fi. While Wi-Fi is used mainly for wireless Local Area Networks, DSRC is intended for highly secure, high-speed wireless communication between vehicles and the infrastructure. In October 1999, The Federal Communications Commission (FCC) allocated 75MHz in the 5.9 GHz band for DSRC-based ITS applications and adopted basic technical rules for DSRC operations. Since April 2010, **IEEE 802.11p** amendment has been the basis for DSRC to add wireless access in vehicular environment.

DSRC communications mainly involve V2V and V2I deployment strategies, helping to protect the safety of the traveling public while also providing mobility and environmental benefits. In contrast to V2V and V2I applications, V2P has not received as much attention in the past due to the unavailability of communication mechanisms between pedestrians and vehicles. However, recent advances in enabling DSRC-based communication using smartphones have begun to change this trend.

With DSRC deployments, RSUs operate under 47 C.F.R, Parts 90. DSRC is also based on IEEE 1609.2 Security Services, IEEE 1609.3 Networking Services, and 1609.4 Multi-channel operation standards, and integrates with SAE J2735 message set dictionaries, and SAE J2945 DSRC performance requirements.

5.2 Connected Vehicle Communications: C-V2X

An additional alternative of connected vehicle communication has proceeded, using the 3GPP standard. This is commonly referred to as C-V2X. Even though **3GPP Release 14** C-V2X specifications were based on 4G LTE technologies, they are now expanded in **3GPP Release 15** to support 5G for low latency, high speed of delivery and enhancing system security. Some stakeholders on the national level have advocated for the use of 5G-based C-V2X communication to replace the DSRC-based communication path the USDOT has been pursuing since 1999.

C-V2X defines two transmission modes that enable a broad range of use cases. Direct mode means V2V, V2I and V2P operate in ITS 5.9GHz bands independent of cellular network, covering short range (<1km) and implemented over PC5 Interface. Network (Up/Downlink) V2N operates in the traditional mobile broadband licensed spectrum, which offers long range (>1km) and is implemented over the "Uu interface" (radio interface between the mobile device and the radio access network.)

An important feature of this standard is its PC5 Interface, which uses a side-channel of the DSRC band and standardized cellular connectivity to achieve peer-to-peer transmissions (i.e., V2V) without requiring immediate network connectivity. C-V2X uses a harmonized, dedicated spectrum for vehicles to talk to each other and reuses the DSRC/C-ITS established service and app layers. Note that communication using this portion of the C-V2X 3GPP standard would not include the private cellular networks.

5.3 Security Credential Management System (SCMS)

As connected vehicle applications exchange information between vehicles, roadway infrastructure, traffic management centers, and wireless mobile devices, a security management system is needed to ensure that users can trust the validity of information received from other indistinct users whom they have never met and do not know personally.

The Security Credential Management System (SCMS) is a Proof of Concept (POC) message security solution for V2V and V2I communication. It uses a Public Key

Infrastructure (PKI)-based approach that employs highly innovative methods of encryption and certificate management to facilitate trusted communication. Authorized system participants use digital certificates issued by the SCMS to authenticate and validate the safety and mobility messages that form the foundation for connected vehicle technologies. To protect the privacy of vehicle owners, these certificates contain no personal or equipment-identifying information but serve as system credentials so that other users in the system can trust the source of each message. The SCMS also plays a key function in protecting the content of each message by identifying and removing misbehaving devices, while maintaining privacy.

The SCMS provides several benefits, including:

- Ensures integrity—users can trust that the message was not modified between sender and receiver.
- Ensures authenticity—users can trust that the message originates from a trustworthy and legitimate source.
- Ensures privacy—users can trust that the message appropriately protects their privacy.
- Helps achieve interoperability—vehicles from different manufacturers will be able to interact and exchange trusted data without pre-existing agreements or altering vehicle designs.

Being in a proof-of-concept stage, only projects funded by the USDOT are eligible to request enrollment in the SCMS. While security remains critical for CAV deployments including V2I, substantial work remains to support long term SCMS deployments.

The USDOT has initiated a National SCMS Development project that will work with a diverse population of V2X stakeholders to explore strategies for the establishment and governance of a National SCMS. SCMS is initially designed for IEEE 802.11p DSRC, but existing research suggests that C-V2X will also reuse SCMS in the future. Ultimately, this function is likely to be provided by industry, in a manner similar to the certification testing of V2X equipment.

5.4 Forecasting the Connected Vehicle Marketplace

As the DSRC and C-V2X conversation continues, security methods will continue to be tested and developed as part of USDOT CV pilot deployments and corridors.

The infancy and uncertainty of vehicle communication security means agencies should continue to rely on a Systems Engineering approach by project, with the Concept of Operations and Needs remaining the focus in deployments.

During these rapid changes in technology and policy, some vendors have responded by creating better solutions. For example, several Roadside Unit (RSU) providers are now offering dual-band devices, which support both DSRC and C-V2X without increasing the cost significantly.

6. Core Conclusions

- Fiber Optic Infrastructure will and should remain a foundational investment for our transportation system.
- Program requirements will be driven by the concepts of shared control and integrated operations facilities among multiple stakeholders.
- Examine our procurement models where appropriate and embrace creativity through partnerships.
- Continue to monitor the industry and learn from regional and national best practices.
- Stay open-minded and engaged in the regional and national deployments.

For ITS planning and deployments, stakeholders must meet the core functionality first. It is key for the region to encourage continuous commitment to maintaining high-capacity fiber networks while developing and enhancing the ability to share video and other data securely.

CES 2020 highlighted the need for cities, counties, and states to increasingly invest in IT infrastructure. However, it is not clear if there is an optimal method for deployment.

A commitment to safety and security is critical. It is also critical to maintain willingness to dedicate resources to integration, explore lessons learned, maintain open dialog and treat goals as a collective. To fulfill these commitments, multi-agency engagement is needed in the following focus areas:

- Clear definition of needs
- Communications system inventories and capabilities
- Gap assessment
- Commitment to appropriate requirements
- Commitment to change control procedures that ensure needs are met securely and systems are maintainable.

7. References

[1] USDOT ITS Joint Program Office: Connected Vehicles. https://its.dot.gov/cv_basics/index.htm

[2] Cisco: What Is Network Security? https://www.cisco.com/c/en/us/products/security/what-is-network-security.html

[3] Federal Communications Commission (FCC): Dedicated Short Range Communications (DSRC) Service. https://www.fcc.gov/wireless/bureau-divisions/mobility-division/dedicated-short-range-communications-dsrc-service

[4] IEEE 802.11p-2010 - IEEE Standard for Information Technology-Part 11 Amendment 6: Wireless Access in Vehicular Environments. https://standards.ieee.org/standard/802_11p-2010.html

[5] USDOT ITS Joint Program Office: Vehicle-to-Pedestrian Communications for Safety. https://its.dot.gov/research_archives/safety/v2p_comm_safety.htm

[6] Performance Analysis of DSRC Priority Mechanism for Road Safety Applications in Vehicular Networks. https://onlinelibrary.wiley.com/doi/full/10.1002/wcm.821

[7] “Why DSRC?”—Presentation on 2016 IEEE Vehicular Technology Conference. http://www.ieeevtc.org/conf-admin/vtc2016fall/20.pdf

[8] Qualcomm: Connecting vehicles to everything with C-V2X. https://www.qualcomm.com/invention/5g/cellular-v2x

[9] USDOT ITS Joint Program Office: SCMS. https://its.dot.gov/resources/scms.htm

[10] USDOT Fact Sheets: SCMS Proof of Concept. https://its.dot.gov/factsheets/pdf/CV_SCMS.pdf

[11] USDOT Talking Technology and Transportation (T3) Webinar - Introduction to Cyber Security Issues for Transportation. https://www.ahcusa.org/uploads/2/1/9/8/21985670/s111207_dinning_overviewof_transportation_cyber_issues.pdf