Module 38
CV262: Vehicle-to-Vehicle (V2V) ITS Standards for Project Managers

Ken Leonard: ITS Standards can make your life easier. Your procurements will go more smoothly and you'll encourage competition, but only if you know how to write them into your specifications and test them. This module is one in a series that covers practical applications for acquiring and testing standards-based ITS systems.

I am Ken Leonard, director of the ITS Joint Program Office for USDOT, and I want to welcome you to our newly-redesigned ITS standards training program of which this module is a part. We are pleased to be working with our partner, the Institute of Transportation Engineers, to deliver this new approach to training that combines web-based modules with instructor interaction to bring the latest in ITS learning to busy professionals like yourself.

This combined approach allows interested professionals to schedule training at your convenience, without the need to travel. After you complete this training, we hope that you will tell colleagues and customers about the latest ITS standards and encourage them to take advantage of the archived version of the webinars.

ITS Standards training is one of the first offerings of our updated Professional Capacity Training Program. Through the PCB program we prepare professionals to adopt proven and emerging ITS technologies that will make surface transportation safer, smarter, and greener, which improves livability for us all. You can find information on additional modules and training programs on our website, www.pcb.its.dot.gov.

Please help us make even more improvements to our training modules through the evaluation process. We look forward to hearing your comments. Thank you again for participating and we hope you find this module helpful.

Ken Vaughn: Hi. This is the introduction to vehicle-to-vehicle communications for ITS Standards for project managers. It was recently updated in November 2019. I'm your instructor today, Kenneth Vaughn. I'm the president of Trevilon LLC and I am the convener of ISO/TC 204 Working Group 1 which is on architecture for intelligent transport systems. I've been dealing with connected vehicles in that role for quite some time now.

But we will talk about various learning objectives today, the first of which will be describing the connected vehicle environment. Then we'll move onto discuss V2V communications and then we'll talk about the roles of standards for these communications. Then we'll finally look into addressing the challenges in realizing this type of environment and describing the current status of the standards with connected vehicles.

Let's talk about learning objective one, which is describing the connected vehicle environment. This diagram shows the overall view from the U.S. national architecture known as ARC-IT, Architecture Reference for Cooperative and Intelligence Transport Systems. You see here the five major components that are used to describe the environment. You have a vehicle, traveler, field devices, support equipment and then centers as well.

This course will focus on what's known as the vehicle-to-vehicle communications which is vehicles communicating to other vehicles as you would expect. We also include within it the vehicle-to-pedestrian and actually pedestrians and other travelers that might be vulnerable road

users. That's the focus of this course is a V2V and the V2P area on the right-hand side of the diagram.

Another corresponding course, the V2I course, deals with kind of that middle section of connections between either the traveler and the vehicle back over to both the field support and the center systems. Those are known as vehicle-to-infrastructure connections, or the V2I course. In particular, though, we do want to focus that we are dealing directly with traveler and we will touch on those topics during this course.
What is this connected vehicle environment? Well, it consists of connected vehicles that are able to communicate to one another as well as connected vulnerable road users. And then, finally, the connected infrastructure that enables all of this to happen. Within the communications environment we're looking at, obviously, a wireless network. Vehicles talking to other vehicles you can't have wired lines. They're by necessity wireless, but there's a mixture of short-range communications and remote communications. Within the V2V course, this course will focus primarily on short range but when you get into vehicle-to-infrastructure there is also a wide variety of remote communications. What's the goals of all this? Is this just technology facing a problem? No, this is very real results we're expecting.

We believe that we can reduce accidents by a significant number. That number range is rather large between 20 and 80 percent. But when you're looking at 40,000 fatalities a year on our roadways in the U.S., that's quite a bit of reduction that can be achieved. That's not even to mention the six million plus crashes every year, as well, in the U.S. We can also look at reducing congestion by 15 to 42 percent from various studies. And, once again, we're talking about six billion wasted hours a year on our roadways, so a 15 to 42 percent reduction can be quite significant. Also automated or connected vehicle technologies will support automated driving which can even further reduce congestion.

Finally, we're also looking at improving mobility of those with disabilities and reducing pollution by roughly 10 percent. Right now we're producing eight million tons of CO2 from the transportation sector, so a 10 percent reduction is significant. We are looking at some real benefits to safety, mobility, and the environment. One other aspect of the connected vehicle environment which is worth noting is we're moving from a traditional ITS into what's known as cooperative ITS. There's a big distinction here.

Traditional ITS systems are systems. They are managed, controlled by one entity. And even if you wanted, in the case of traffic management centers communicating with other traffic management centers owned and operated by different agency, there are agreements in place to enable those connections to occur between those two agencies. A cooperative ITS system is a complex system of systems. In other words, the different systems that are components of the system of systems are owned and operated and maintained by different entities which means they might update their software at different cycles and there may not be any formal contract between the two entities.

So if you think about driving down the road in your vehicle, your vehicle has to communicate with the vehicle next to it even though it's never seen that vehicle before. It doesn't know who the owner is. And it has to have confidence that the information it's receiving from that other vehicle is accurate, is authenticated, and is properly authorized to provide the services it's providing. That results in a much more complex environment, especially for security. And the

reality is most connected vehicle applications are, in fact, cooperative ITS. That's a major topic that we'll discuss within this module.

Now, a little bit about the difference between the V2V in this course, and the V2I course which is the parallel course. This course will talk about vehicle-to-vehicle, vehicle/pedestrian or road users, vulnerable road users. And, as such, virtually everything we're talking about we're really concerned about roughly a 300-meter range of communications. And we will touch a little bit on the support infrastructure required to make sure that you have proper authentication and security of each communication.

The V2I course, on the other hand, will focus on vehicle and pedestrians or vulnerable road users, so the roadside and to center. There they'll talk about short range communications as well as wide area communications and they'll go a little bit deeper with the infrastructure information. These two areas grouped together are known as a vehicle-to-anything, or V2X, and that term will come up periodically during this presentation.

Vulnerable road users include a variety of people that you might see on the road, basically anyone not in a four-wheeled vehicle. This includes pedestrians, those with disabilities, any sort of alternative mode. It might be a bicycle. It might be an e-scooter. It might be a skateboard or anything. Maintenance construction workers and emergency personnel, the last two, are very important because that's really kind of a focus of this course a little bit in that we're primarily presenting to agencies what they need to be concerned about. And this is the area of vehicle-to-vehicle communications that most directly impacts agencies because it's their workers on the road that might be impacted by this technology.

Let's look at some of the basic safety services that are driving vehicle-to-vehicle deployments. One of them is a simple "do not pass" warning. If you're trailing behind a vehicle, you're looking to pass, there might be another car coming the other way, this sort of V2V communications will allow you to see around the vehicle and for your car to warn you about any oncoming traffic without you having to peek out.

Another condition is the blind spot warning, or lane change warning, so that if a vehicle is in your blind spot and you start to change lanes, it will provide a warning there as well. There's also a forward collision warning so if the vehicle in front of you is stopping and your car notices you're not slowing down then you'll get a warning. And likewise, emergency electronic brake light, this is when a vehicle, perhaps several, in front of you slams on their brakes—hard brake—that will be notified to everyone around it so that even if you cannot see that vehicle directly in front of you, you still get the warning. This will help prevent the crashes that recently occurred in Virginia during the fog where you had, I think, it was 69 vehicles all collide together.

This is a key technology to provide to mitigate that sort of collision. We also have intersections so basic intersection movement assist will alert users that someone is about to run their signal as well as a left turn assist will provide assurance that you can safely make your left turn. There are other safety services. All of those were the basic safety but there's also conditions where that vehicle-to-vehicle communications will provide vehicle control events such as a tire blowout or something like this. It will alert users to wrong way vehicles and provide hazard notifications, particularly with more automated vehicles if they're equipped with sensors like you see on that top figure there. It might see a tree or a branch down in the roadway. It will notify vehicles behind it that there's that hazard in the roadway.

There's also agency relevant vehicle-to-vehicle safety services. These are things like slow stationary vehicles that might be your post office delivery vehicle. It might be your construction vehicle on the highway, work zone warnings, emergency vehicle warnings, vehicle emergency response. So as your vehicle is approaching a vehicle that's been in a collision, it can get all sorts of detailed information about that vehicle and how severe the impact was. And then, also, vehicles turning in front of a transit vehicle, so those collisions are avoided as well.

Now, those were all safety scenarios. We also have mobility services. These are things like Queue warning cooperative, adaptive, cruise control and platooning services. And then there's environmental services that are defined, which relate to connected eco-driving so that you match the vehicle speed in front of you and cooperative adaptive cruise control as well. Now, we also have services that are really focused on the pedestrians. Why are the pedestrians so important? Well, in 2017, a third of all fatalities on the roadway were vulnerable road users. About half of these were motorcyclists. About the other half—or actually even more than that—were pedestrians and pedal cyclists and other non-occupants.

What's particularly concerning about this is if you look at the actual statistics over time, we start seeing that in 2009, those numbers had dropped quite a bit. But since 2009, they've increased by almost 50 percent. That has particularly impacted those that are aged between 20 and 69. So what do you think has changed since 2009 to create this condition? In many cases, it is the smart phones that are creating distracted pedestrians and then they get into accidents. And what better way to warn them about emerging dangerous situations when they're looking at their cell phone to have that cell phone warn them that they're walking into the middle of the street? They're looking directly at the technology that can provide that warning. All we need to do is create that application.

The good news is the technological solutions are pretty much available. We need to deploy that technology, though. We're also looking at use cases for the accessibility challenged. There's Accessible Transportation Technologies Research Initiative (ATTRI) that is looking into the complete trip that allows someone to plan and book a trip, travel to a public transport station, ride that facility—the bus or subway—and then get to their destination safely across the street and arrive at their destination all as a single unit to make sure that these vulnerable within us are able to travel safely across the network as well.

In summary, there's a whole set of societal benefits for connected vehicles. There are safety benefits that include a 360-degree visibility around your vehicle, so you know the risks involved. You can identify the hazards and thereby reduce crashes. Those reduced crashes result in mobility benefits that provide reduced congestion and, as well, will provide an increased mobility with those with disabilities and providing smoother traffic flow. Your reduced congestion results in reduced emissions. Smoother traffic flow also results in reduced emissions. And there's also improved efficiency that enables automated driving systems. So very significant benefits from this technology.

With that, we come to our first activity. The question is: which of the following does USDOT not include in its list of benefits of connected vehicles? The answer choices are: improved safety; improved environment; enhanced entertainment; or improved mobility. Go ahead and make your selection now and we'll review the answers here in a second. We'll look at the answers.

The correct answer is: enhanced entertainment. And while connected vehicles may be able to deliver entertainment, this is not included in the USDOT list of benefits since it's not really a matter of major public interest. The ones that are of public interests are improved safety—they have identified that as a primary benefit provided by connected vehicles. It's also improved environment. USDOT has identified various environmental benefits of connected vehicle services. And, finally, improved mobility is also on the USDOT list because it provides benefits for connected vehicles as well.

With that, we've come to learning objective number two: discuss V2V communications. This figure shows you the overview of what is inside of your vehicle or of your pedestrian smart device. Basically, either one of these devices will have antennae that will connect to your V2X radios or if you're pedestrian, it would be a P2X radio and a GPS receiver. Those units—those radios will then communicate to your on-board equipment, your on-board applications that actually provide the logic and services of what we've talked about as connected vehicle services. Those applications interact with your platform of the device that provides memory and processing power and everything. And that, all together, in a secure environment is what's known as the on-board equipment. And those are one or more integrated units. Each individual unit would be the on-board unit. This is also sometimes called an ITS station.

Now, that secure environment also needs to interact with the remainder portion of the device, your internal device communications (comms). For example, in your car that might be your CAN bus that connects all of your steering wheel and your accelerator and your engine controls, as well as your infotainment system and everything. And then, also a human interface so you can interact with that application. So all of that is the connected—are the components of that V2X network. Within that network we have various data requirements, communication requirements, and security requirements to make these technologies work.

Now, clearly, the details of each of these are going to vary a little bit service-to-service but a lot of these details can be summarized up into a high level using one as an example. The example we'll use will talk about your basic safety capabilities which includes forward collision warning, intersection movement assist, electronic brake light and other applications that we've talked about. And CAMP, the Crash Avoidance Metrics Partners, have spent a lot of times researching this condition and they've developed a lot of detailed requirements for how this will work. And the information requirements for these define the data that's needed, when that data is needed, from whom the data are needed, what conditions the data are needed, and then how the data are exchanged is the final item. That final item we'll talk about as a standard. That's the next learning objective.

This learning objective will talk about those other four bullet points. When we talk about the "what" requirements for data exchange, we look at what do you need to understand for the safety of your vehicle? My vehicle to your vehicle, what information do we need to exchange? Well, we need to understand the location of your vehicle, at least in respect to mine and how fast we might be approaching each other. Any changes of that speed and acceleration, the direction of travel, the acceleration rate. Brake status, are we braking? And are we perhaps sliding on the roadway? Lengthen and width of the vehicle. I don't need to know just a point location but how big of a vehicle are you? Steering wheel angle.

Once again, this relates to whether your angle and your acceleration rates correspond to your braking and other conditions is determined if you're sliding on the roadway. And then, other

variables as needed, special conditions, if you've had a tire blowout, if there's special conditions in your vehicle that are going on I might need to know those as well. That's the "what" of the information that we need to exchange on a very frequent basis to avoid collisions.

But then when do we need to know this? Well, what do we need to know? It has to be very accurate information so we have to find very precise accuracy requirements for every piece of information that we define. Then we also need to make sure that it's provided often enough and that it's current enough. The latency has to be less than about 10 milliseconds. And I need updates roughly every 100 milliseconds. This starts becoming a very intense level of communications. As you can imagine, lots of different vehicles on the roadway, each one of them sending out their information 10 times a second and that gets to be very, very intensive communications environment.

The next question, though, is who and where do I need this data from? Well, the short answer is I need the information from anyone who's within a distance where I might need to react to. If we look at two cars approaching each other at speed 70 miles an hour each, well, that's combined approach speed of 140 miles an hour. So if I have a communication range of 300 meters, that gets me roughly a 4.8 second horizon, which should be enough time to react to anything even if some of those communications get lost if the packets are corrupted or anything. 4.8 seconds should give me time to be able to accurately detect that there's a vehicle approaching and to respond to that vehicle. There are factors, though, in minimizing this distance. Longer is not always better. The larger we make that perimeter—that 300 meters into something larger—the more vehicles occur within that scope.

So larger transmission distance may end up resulting in your communications at work being overloaded because there's too many people trying to speak all at once. The other issue is I don't necessarily want people to know outside of that 300-meter range that I am there. I don't want someone a kilometer away from me to be able to track me without me knowing about it. A 300 meters distance is something that you can typically see and is comfortable within people knowing that we are there. 300 meters tends to align with customs. It tends to align with what's needed in the field and that's how that figure was developed. With that said, it should be noted that radio transmissions can vary based on the environment. They can vary based on fog conditions, humidity conditions, tree cover, and other things. So that 300 meters is a guideline. It's not a precise value because it's radio communications.

The other thing we have to deal with is the latency requirements. We mentioned need to be roughly in the range of 10 milliseconds. That's very fast compared to most communications environments, particularly wireless communication environments. And we're talking about very frequent communications, separate packets, every one to two milliseconds with potentially hundreds or even thousands of vehicles all doing that at the same time. It's a very large number of devices and it's dynamic; it's constantly changing. In fact, it's a continuum of devices. What we mean by that is as I drive down the road and there's vehicles passing me in the other direction, there's no point do I have a stable network. My network of vehicles within that 300-meter range is potentially constantly changing. It's just a continuum of devices entering and leaving my communications network. And this sort of conditioning can exist in rural environments without any roadside infrastructure. I need to be able to make sure that I can communicate with them without roadside infrastructure. And I need to be able to authenticate and know who they are to make sure they're authorized for that communication when I can't talk to any central security agency.

We have to have a design for that as well. Target transmission range as we've mentioned is 300 meters. Also very important is no subscription is necessary. The idea here is we're promoting public safety as a whole, not as an individual user. Therefore, we want to make sure everyone has this technology available to them for free. Now, it's fair enough to say not all applications have such strict requirements but there are some applications that have even more strict requirements. For example, platooning has even higher data exchange requirements at more frequent rates, but the vehicle-to-vehicle safety application is a typical baseline use case that everyone has to support. That's why it's a good example for designing the system.

We also have security requirements we have to deal with. We have to be able to protect our confidential information. This includes our personally identifiable information. We don't want to know, necessarily, who's in the vehicle. Likewise we want to protect management information. We want to make sure that someone can't get in and reconfigure my system or to make assumptions about my system based on how I have things configured. Likewise, we want to prevent information leakage through data fusion. So we really don't want vehicles or people to be able to identify the fact that I park my vehicle at a particular address every night and then follow me throughout the network and identifying my origin destination. And, therefore, provide all sorts of details about who I am and where I go and everything else. Those things need to be protected.

We also want to make sure that we authenticate communications. This means that we need to make sure that communications that are received we know are from an authenticated source. As well as, we need to authorize any communications, so that when information is received not only do we know who it's received from, but that we can make sure that that person making a particular request is authorized for that request.

So if they are making any specific requests we can authenticate that and authorize it. Finally, we have to provide the security within that connected vehicle environment we talked about, which means two vehicles that have potentially never seen each other have 4.8 seconds, potentially in a rural environment, without communications with anyone else to be able to authenticate and authorize each other to do what they need to do. It's a very time-critical nature of security approvals without any tracking of the certificates; a very detailed environment. We'll talk a little bit about that in the standard section of the next learning objective.

But, first, let's take another look at our second activity. What data is not included as a basic safety requirement? The location of a vehicle; the weight of a vehicle; the length of vehicle; or the steering wheel angle. You can go ahead and make your selection now.

Well, the correct answer is: the weight of the vehicle. The basic safety application is intended to avoid collisions and the weight of the other vehicle has not been deemed to be a significant factor in these calculations. That may have implications as far as impact conditions, but our goal is to avoid the impact altogether. The location vehicle is used to determine how close the vehicle is. The length of the vehicle is to determine the limits of the vehicle. And then finally, the steering wheel angle, it can be used to identify when a vehicle is sliding on the pavement.

That brings us to learning objective number three: describing the roles of standards for V2V communications. Well, first off, it's very important to recognize that standards are absolutely essential for this type of environment. Standards generally enhance interoperability in a multi-

vendor environment. Interoperability is the degree to which two or more systems, products, or components can exchange information and use the information that has been exchanged. And when you think about the vehicle-to-vehicle communications, you think about all the different manufacturers of vehicles in the roadway today.

No more than any one vendor or manufacturer vehicle doesn't have more than—I think it's a 17 percent market share. So it's very important that we make sure that all of the different vendors of equipment out there agree to the same standards so that communications for manufacturer A can be understood by manufacture B as well. It also, though, makes testing integration and management much easier, making sure that everyone supports one solution rather than having multiple solutions out there drastically simplifies all of this. And then finally, it helps with the design and procurement of a system so that when I go out and buy a car for my agency-owned vehicle fleet, I know that they're going to conform to the standard because there's only one for the entire country.

The benefits of standardization, it provides a common baseline. It defines your terminology. It defines levels of quality. It defines the testing environment. All of this is fine, so you know what you're getting. It reduces risks by clearly identifying and defining functionality. It improves interoperability and interchangeability. And by making sure that we all agree on the definition when problems are found, we can revise that standard once and implement it for everyone as opposed to having multiple solutions, always having to integrate, always finding new bugs in the integration. Having that single solution really helps out. It reduces costly and risky customized integration efforts and creates more competitive marketplace so that when I go out, I don't have to worry about, well, which technology is being used. They all use the same technology. I can now focus on other aspects that I really need out of my vehicles. But it also encourages deployment of new and emerging technologies because they have that base technology all agreed upon so it accelerates adoption of new technologies.

When we talk about communications in the environment, we have to recognize that there are many different components of how vehicles communicate. They communicate over a particular communications media, they exchange information in certain ways, they authenticate information in certain ways, they try to perform different activities. All of these different components fit into a basic model.

The model that's used within our environment is primarily the ITS station architecture that's shown here. We have the access layer at the bottom, in the middle that shows—it's also called the SubNet layer. The access layer provides access to a communications media. It defines the rules for how I exchange information over the airwaves since we're talking about wireless communications. The network and transport layer, what we also call the TransNet layer, provides communications—it defines how I connect my data from one device at point A to a remote device at point X. And I might have to go through multiple connections to get there. And my information that I want to exchange might be more than one data packet.

So I might have to send multiple data packets over this network all arriving at the end destination. They all have to be reassembled at the destination to form the entire message I'm dealing with. That's what the networking transport layer deals with. The facilities layer defines how I structure my messages and the actual content of those messages.

Finally, the application entity at the very top defines what that data is and how often a need to exchange it, the rules for exchanging it, the functionality, performance requirements, all those details. Over on the right-hand side, we have a security entity that deals with all of the services needed in order to authenticate and authorize communications in that secure environment. All of the different layers, access layers, network layer, transport layer, facilities layer, application entity all have access to that security entity to provide services there. Likewise, the management entity over on the other side—on the left-hand side—provides management conditions.

Now, as I enter into a new region, I can be told there are new traffic regulations within this region. I can be configured for those traffic regulations. I could be told that there's new regulations on how I transmit data. That can all be stored in that management entity for my configuration. So that's how all of that works. As we go through the different standards, we'll be mapping those standards to what aspects they cover within this region. That's why this figure is important because it's going to structure the next slides.

If we look at that application entity, we look at standards that define how my applications work. It defines how do you use management facilities and security to implement a specific application as defined by specific use cases. It includes performance requirements and it follows a format generally for vehicle-to-vehicle communications that define the format defined in SAE J2945, which is also known as /0 which is the one document that doesn't have a number after it.

This document defines the format for all of the other J2945 standards. It includes the concept of operations, the functional requirements, dialogs and data, the requirements for a traceability matrix. It doesn't define a content. It defines a structure that is used to define the content and all of the other standards we're about to talk about. With that, we have the suite of standards within the J2945 family that define vehicle-to-vehicle communications. Slash-1 "/1" defines vehicle safety application, vehicle-to-vehicle safety application. Those are the basic safety services we talked about earlier in the presentation, collision avoidance, things like this. That is a full standard that was last updated in 2016.

Slash-2 "/2" deals with vehicle-to-vehicle awareness applications. This includes things like emergency vehicle alert, roadside alert, about stopped/slowed vehicles and safety awareness talking about objects and other things in the roadway. That is a recommended practice last published in 2018 and will probably be updated to a full standard at some point in the future. Slash-6 "/6" is cooperative adaptive cruise control and platooning. That is currently in progress being developed as well as Slash-8 "/8" cooperative perception symptoms, also under development.

And then the final one here is Slash-9 "/9", is a current recommended practice related to vulnerable road users last published in 2017. All of these standards use the same base data definitions. Those are defined in SAE J2735, which was last published in 2016. So this is at the facilities layer and it defines the message of how I put these things together and the actual individual data elements. So the data elements and how those data elements are put together into a message.

When the messages are sent, are defined by the standards we discussed other previous slide, J2945, this only defines the actual data itself. A prime example of this data is contained in the basic safety message and that basic safety message contains two parts. Part one defines all of

the data elements that are necessary for safety applications that are expected to be broadcast frequently. That's the list of data that we talked about earlier on the presentation: location, speed, headings, steering wheel angle, et cetera.

And then the part two elements was that last bullet on the previous page of—there's additional things you may need to know under certain conditions such as your emergency braking, your antilock brake activation, you have a tire blowout, whatever. It's kind of exceptional cases that are used less frequently.

Once again, J2735 only defines what that message is. When I transmit each piece of information, that's part of your application definition, that's a J2945. Moving off to the side now, our management standards those are included, generally speaking, in other standards and proprietary definitions. For example, the application might require the use of a specific radio. So J2945/1 for the basic safety message says you shall use DSRC as your communications and it defines priorities for the different messages.

Another example is jurisdiction might transmit configuration or operational parameters that affect device operation. For example, as you're traveling into a new area, you might have a roadside device tell you if you want to access this service you need to tune to channel X. It will tell you which channel to tune to. Now, I know how to configure and communicate for that service.

If we move over now to the right side of the diagram security entity, we look at the security services for applications and management messages. This is IEEE 1609.2 noting that there are a couple of amendments since this was last published in 2016. This is the standard that defines your base security processing requirements. It defines communication security for what's known as the WAVE environment, the Wireless Access and Vehicular Environments, service advertisements and WAVE short messages. Basically any messages used over DSRC would use this security mechanism. It also defines additional security services that may be provided. And these are services that can be used for higher levels.

So your application itself may be secured as well as your communications at the lower layers. The key portions of this have been adopted in other environments as well. It was originally developed for this WAVE environment, the IEEE 1609 series documents, which included DSRC but is also being adopted internationally with the European solutions, which is also another DSRC based solution, as well as C-V2X. They all agree this is the way to do security regardless of what lower layer technologies you are using.

There might be applications even beyond ITS for this. We are talking about smart cities, near net of things and then they may have some similar use cases where this technology, for security, may come in handy for them as well. There is a separate module, CV265, that talks about the security documents in much more detail. In addition to 1609.2, there's an additional specification known as 1609.2.1 which is a current work in progress. It defines how digital certificates are provided into and managed within end entities. An example end entity might be your vehicle or it might be your smartphone or any other device communicating within this environment. The certificates are provided by the security credential management system known as the SCMS. And it creates an ITS trust domain among entities that have no direct relationship.

An example of how this works is in the diagram you see vehicle A and vehicle B. They're approaching each other at a high rate of speed. They have perhaps 4.8 seconds to be able to identify and recognize each other. How does this work if they've never encountered each other before? There's no contractual relationship directly between these two. While the SCMS is a central agency that before these vehicles even come near each other that SCMS is granted certificates to each one of those. There's a prolonged process by which those certificates are granted to make sure they're authenticated users. And how that gets distributed is defined in 1609.2.1 and the management of those certificates and how all of that works is within that standard.

Once those vehicles have those certificates, they can now exchange each other when they encounter each other by simply sharing those certificates. And they demonstrate to each other that they're part of the same trust domain because ultimately, they can somehow recognize each other's SCMS service, they knew that the root is the same, therefore they can trust each other. Now, I will say this is drastically simplified from the way it really works. There's a lot more to it to make sure everyone maintains their privacy and everything else. But conceptually that's a very high-level view of how the two vehicles are able to recognize each other even though they've never even encountered each other before.

Very quickly they can exchange certificates. They can recognize those certificates are being authenticated. And then they can consider the data valid. If we move down the spec now, we've talked about with the upper layer and the site entities. We're now the TransNet layer. This layer talks about how we exchange data from point A to point X on a network. It's defined in IEEE 1609.3, which was last published in 2016. It specifies use of how I can use the standard IPv6 protocol.

In theory, that initial communications can then be sent anywhere in the world to any device. And then, also, how it works with the WAVE short message protocol, known as WSMP, as well as associated management functions for how all of that is managed. Now, we get into the interesting bit. At the SubNet layer, or the access layer, we have—the FCC has allocated a 5.9 gigahertz (5.9 GHz) spectrum for intelligent transport systems. In particular, this was done in 1999.

They dedicated non-voice radio techniques to transfer data over short distances between the roadside and mobile radio units, between mobile units, and between portable and mobile units to perform operations related to the improvement of traffic flow, traffic safety, and to other intelligent transportation service applications in a variety of public and commercial environments. DSRC systems may also transmit status and structural messages related to the units involved. That was done in 1999.

Shortly after that in 2003, the IEEE 1609.4 standard, which was last published in 2016, was designated as the protocol to be used within this 5.9 gigahertz (5.9 GHz) spectrum. This is a specialized type of Wi-Fi technology. The same exact Wi-Fi technology that's in your house, that's specified in IEEE 802.11, this same technology has been customized a little bit for the vehicle environment. And it uses that same base technology, though, of multiple access collision avoidance that's been proven for decades of how multiple entities that want to talk simultaneously, there's a way for them to see if anyone else is talking. If there is, they step back for a random interval. Then they'll transmit what they need to.

This is a specialized version that's been extensively tested since the 2000s. It's been specialized to make sure that it supports the very low latency environment, the fact that you don't have to register on the network before you communicate on the network. All of these little details are very different than your house, but all of the core technologies are the same. It's part of that same standard series. It is, in fact, the basis for all existing U.S. deployments to date. When I say deployments, I mean permanent conditions.

The reason for this is because this is the designated technology for this frequency at present. We'll talk about some exceptions coming up. Efforts are underway to update the standards and support new features. And the slow deployment to date, though, has resulted in the FCC reviewing this technology and that may result in the assignment of spectrum to an alternative technology, such as the C-V2X. It may result in spectrum sharing; that's been discussed. That's looking like it may not go that way.

The other possibility is a loss of spectrum and some of that may go to the Wi-Fi community or someone else. The FCC is currently reviewing these. This is an active discussion. We're not going to know perhaps for another year what their final decision is but that's something for you to look into and follow as time progresses.

But a little bit about the technology that may supplant this that's being discussed about, this is C-V2X. And this starts becoming a very confusing discussion because one, there's a lot of misinformation out there. And two, it's just a complex issue to begin with. Let's look at what this is. Cellular data, this is one type of cellular data. It's all based on cellular technologies as opposed to Wi-Fi technologies. We're looking at the 3GPP standards as opposed to the IEEE 802.11 standards.

Cellular data has always been viewed to be a part of the connected vehicle environment. But initially, it was focused primarily as a mechanism for infotainment, large file transfers, and vehicle-to-center communications. These were all conditions where traditional 3G technologies and LTE, as well, C-V2X, cellular-vehicle-to-anything, alluded to on the previous slide, there are other proposals out there that we're also following.

The Wi-Fi community has separately proposed to share or take over part of the 5.9 GHz spectrum. This would intermix ITS with non-ITS uses; that's the sharing proposal. Dividing up the spectrum would not intermix those, but it would decrease the bandwidth that would be made available. All of these conditions are possible. As I say, this is an active discussion within the FCC. And that's something that we need to follow as an industry.

It's also worth noting that C-V2X has been chosen as the DSRC deployment technology in China. So that technology will continue to be developed even if it's not selected here in the U.S. But a little bit more. When we talk about C-V2X, we are talking about something that's very specific. And it gets very confusing because the way that the 3GPP community uses terms to mean different things. Strictly speaking, the LTE technology that most people are familiar with that's been in their phones since 2010 or so—virtually in every smartphone today—is LTE. It is the major deployed technology right now. That was first standardized in 2008, in Release 8 of the 3GPP standards.

But LTE—all of the 3GPP standards go through these generation settings. But within those generation settings, they have more specific releases. The first version of LTE was Release 8.

And the final version of LTE was Release 14. The first version came along in 2008 and was standardized. The final version was standardized in 2017. A lot of development occurred between there. And, in particular, Release 14 had some major improvements related to V2X. It added, for the first time, a standalone capability of communications.

Now, in theory, a Release 14 phone can talk to another Release 14 phone outside of any infrastructure. You don't need that cell tower anymore, in theory. You can talk device-to-device without that infrastructure of a cell tower. That allows that rural communications to occur that we need so desperately for C-V2X to work. It also provides, or it claims to provide, sufficiently low latency, roughly that 10 millisecond latency for communications to occur. Now, all of a sudden, the base core technology is there. In order to meet all of our needs, though, there are some other proprietary logic required in order to enable the basic of details of when devices know that they can speak, that's handled within a Wi-Fi community.

There are some additional details related to that that have to be addressed still. There is a claimed solution for this. Our understanding is that's proprietary right now but is being submitted as a part of the SAE J3161 standard that will define how this works in an open environment. USDOT is currently testing all of this to see if those claims are accurate, to make sure that this will provide adequate safety and everything else for this environment. That's under active testing. That is the current C-V2X technology solution. It is based on the final version of LTE. It is not, in theory, very technically—it is not a 5G technology. Even though many magazine articles are out there saying that this is 5G, technically it's actually the last version of LTE.

There are some significant differences there. That uses a different radio and a particular band and everything else because 5G is not backwards compatible with LTE within the same band. You can use— as your phones today, you have a phone that speaks LTE, but it can fall back for 3G. The way it does that is the LTE bandwidth, is a different set of bandwidth than the 3G bandwidth. So you're changing where you're communicating in the radio spectrum when you switch those technologies. The same is true here. I can't talk LTE and 5G in the same band, but the same device can support two in two different bands. 5G will eventually, hopefully, in Release 16—to be released in 2020—will provide ultra-low latency, which is needed for platooning.

That will be in a different band than the current bandwidth being reserved for C-V2X. This platooning technology is true 5G technology. It is also sometimes referred to as C-V2X, although really it's completely different technology and that term really should not be used for both bands together because that just really confuses things. The timing of decisions and deployments might affect whether C-V2X, i.e. that 5.9 solution, is based on LTE or 5G technology. My guess, and everyone's assumptions at this point, is that if it is successful, it will be based on the LTE technology because that's what's needed today.

It's worth noting that the dates here are when the specifications are finalized. They are not when products are available. It typically takes one to two years for products to become available after the final spec is provided, especially on the first version of a major technology. For example, the Release 14 specifications with C-V2X technology, it is still rather difficult to find those chips available for commercial purchase immediately right now. You have to get on a waiting list, and it takes times to get those chips. But they are now being manufactured. They are being produced. It's just taken two-plus years in order to get that into the marketplace.

Whereas the 5G technology will be standardized in 2020, you probably won't see those chips available until at least 2022. And then who knows what other additional developments may occur after that. Where are we in the current situation with all of this? Infrastructure deployments are underway using DSRC WAVE technology. Those are the deployments that are underway. All the Florida, New York, and Wyoming deployments were all based on that technology. Virtually all of these at challenge implementations have also all been based on this technology.

Deployments provide agencies that experience and begin to deploy core technologies. So even if the technology changes, deploying at least one signal or something with this technology gives that agency all sorts of experience with what issues come up, what things they have to deal with and consider for these deployments. And there's a lot to learn. Getting involved in this is a very useful exercise for your agency because when this technology starts rolling out, it is going to start rolling out very, very quickly.

Deployments of infrastructure encourage automobile manufacturers to use the technology. One of the issues that this is even a debate right now is because industry has been so slow to actually start deploying it. No one wants to go first because then they're the ones being cut out the middle. The longer we delay, the more of a chance we risk in losing all of our bandwidth all together. We really need to start deploying our technology to make sure the FCC gives us this technology so that we can actually save lives that we've talked about.

The modular equipment exists that can support both technologies so it's not like we're asking you to deploy something that you then have to totally throw away. Because we're dealing with modular technologies, because we've developed all of our standards to be modular in their design then you can simply switch out the radio if there is a need to switch out that radio. That's very important even if we don't switch over to C-V2X because sooner or later, there will be a time that we need to change our lower layer technologies. And we've designed our standards for that evolution to take place. And products are available in the marketplace that allow that evolution to take place.

The recommendation from USDOT is that infrastructure deployments should go ahead and proceed. Let's get that experience in the field so that we know how to start rolling this out when we need to go full speed ahead. And deployments, very importantly, should use modular equipment that allows upgrades to radios, hardware, and software when needed because none of this technology is stagnant. It will evolve overtime. We have to plan for the evolution.

The final topic here is the performance and testing program certification. USDOT did work with industry to develop a conformance test specification and for specifically the SAE J2945/1; that's the vehicle basic safety conditions. Hopefully, when you go out and buy a vehicle and you expect it to have this technology because they advertise it, they've all been tested to the same specification and you know it's all going to work the same way. The intent, though, is that along with virtually all of our other safety testing, there will be a private testing market with multiple vendors that enable this sort of test. And that those ratings and everything will come from that private marketplace that's self-sustaining rather than being paid through via tax dollars.

Well, that brings us to our third activity. Which of the following is not part of the ITS station architecture?: A) application entity; B) facilities layer; C) security entity; or D) presentation layer. Which one of those is not part of the ITS station architecture? Go ahead and answer now.

Well, if you look at our little icon in the upper right, you'll notice that the presentation layer is not a part of our ITS station architecture. It is a part of the open systems interconnect reference model. It is fully contained within the facilities layer of the ITS station architecture. But it's not identified as its own layer within the ITS station architecture. The other items that we listed; the application entity sits on top of the stack. The facilities layer is immediately below the application layer. And finally, the security entity is on the right side of the stack.

That brings us to learning objective number four: address any challenges and realizing of V2V environments. The first thing we needed to do, or what's been the key since our last presentation that this is an update of, is that we have completed—we fully standardized now—SAE J2945/1. We've completed /2 and /9 of that series. Those are still recommended practices as opposed to full standards, but they are complete now. And then we've also completed the conformance test specifications for SAE J2945/1.

We have made significant progress here. We have basically the complete set of standards that are needed. In fact, we even revised based on lessons learned SAE J2735, which is the DSRC message set dictionary that defines your BSM and other messages and data elements. And we've revised all of your lower layers, the Comm stack, which is your IEEE 1609 series, parts two, three, and four. So all of that has been updated. We now have essentially a complete solution.

As we've alluded to, these are now being deployed wide scale, that they are being deployed in the pilot deployments in Florida and New York and Wyoming. And there are many other deployments of that challenge across the U.S. Nonetheless, there are technical and institutional challenges that we need to address. We have access layer challenges that we've alluded to, implementation issues, new applications and software updates and how they're handled. We have the continuing evolution of standards and then data ownership privacy issues on the institutional side, as well as testing and certification and long-term support for the security environment.

What are the access layer challenges? Clearly, we have a challenge here. There are some challenges— some technical challenges—that apply to both C-V2X and the WAVE environment. In particular, we have a consistency of deployed technology making sure that what's been deployed is going to be the same technology throughout the country. The two technologies simply are not compatible with each other. They are competing to use that same spectrum within the 5.9 GHz bandwidth; that issue needs to be resolved. And the coexistence of the technologies in that band need to be resolved.

So one of the proposals right now is essentially that we would divide part of that band up; part of it using the C-V2X, part of it using WAVE. Is that even technically possible? And if so, how does it all get achieved? There's also the question of coexistence within non-ITS Wi-Fi, such as spectrum sharing. If there is spectrum sharing how do non-safety uses know to back off of the network when there are safety uses occurring? If they're being divided by different spectrum and subdividing the spectrum, what are those rules?

All of that is up in the air at the moment. Evolution of selected technology, even if we define which technology we're going to use, we know to date none of this technology stays static. Somehow, we have to define over time how do we migrate from today's technology to a future technology? And that has to be addressed as well. There are also additional challenges that

apply to C-V2X that WAVE has already solved because it's been under testing for 20 years. C-V2X, once again, is a fairly new technology. It's been fairly recently that we've actually been able to get a hold of chips to test.

Now, we have to start testing to make sure that they actually work. And there are some real technical challenges here that the testing with WAVE does not address, for example, communications scheduling in the dynamic environment. We mentioned before the WAVE technology is based on Wi-Fi. It's based on Ethernet type technologies. Let's say if I have two people who want to speak at the same time, they first listen. If someone else is speaking, they back off at a random interval and then speak. This technology is well proven, within the cellular environment it came from a different baseline. Right? The baseline was people reserve spots for timeslots, so that the concept of how it works is my device—it says I'm going to reserve this slot in time in advance of that time so that I'm going to be speaking at that point.

Well, if my network is constantly changing, how do I know if I can reserve a time slot in advance without some other vehicle entering into my network that has already reserved that same time slow? Now, we both try to speak at the same time. Is that an issue? How big of an issue is it? And how do we mitigate that issue? That all has to be tested out and figured out. The second issue is within the Ethernet environment, all of your communications are, in theory, constantly broadcasted on your local channel. When I speak everyone hears it. And if it's not addressed to them, they ignore it. That's the way that first link works.

Within C-V2X, that's not true. C-V2X traditionally has spoken to your cell tower which then communicates and creates a link to the other device. People can't hear you. So this changes the environment completely because so many of our core technologies are expected to be broadcast. Our whole design has been centered around that everyone could share these communications. If my device has to now communicate separate messages with every other vehicle in my communication range, that drastically increases the number of messages I'm sending.

So we have to figure out how does that true broadcast technology work? And is this really working the way we intend it to? There's also, as we mentioned or alluded to before, the potential possibility of stalking. Hopefully, this is something that's easy to resolve. We just power down the radio a little bit more. That by default that device-to-device communications transmits up to a kilometer rather than 300 meters. There are many reasons why we want to limit that communication distance. That should be fairly easy to resolve but there are specifications that have to be written to deal with that. They don't exist today. That has to be addressed.

There's also the anonymity capability. I don't want people tracking me through the network. There is a lot of work to make sure that even my physical address on my WAVE device would change every once in a while. My Mac address every few minutes would change so that someone who saw my communications at one point couldn't track me across town by recognizing my address at that point. And that's the anonymity that we want to achieve within this connected vehicle environment. Is C-V2X able to provide that same level of anonymity? That's one of the things that we have to figure out.

Overall performance of the C-V2X in all environments. So they've added device-to-device communications that allows that rural environment to work but will it also work within the congested parking lot of a stadium. As everyone's getting in their car after a game, they're all

turning into their cars, all communicating at once in a very, very dense environment. That has to be tested out as well. What other impacts to existing investments have been made? We have deployments all over the country. We have standards written all based on this other technology. What are the challenges there and upgrading those to meet this technology? And then finally, there's still some questions revolving around the royalty and service fee policies regarding this technology.

Cellular communications traditionally has been a fee-for-service environment. This would radically change that. Is everyone on board with that change? Because it's really critical that we don't charge fees for maintaining people's safety. Other implementation issues—the C-V2X environment has a lot of challenges in front of it. Once again, that's not to say that the technology is not going to be selected but those challenges need to be resolved before we make that final decision. That's one of the reasons why it'll likely be a year, perhaps, before we actually get to that final decision. Other implementation issues V2V, in order for vehicle-to-vehicle communications to work they both need to rely on the same technology.

This has actually been one of the reasons, more recently, why you've seen delay in having this technology deployed in vehicles because car manufacturers have been reluctant to deploy the technology unless they see all the other car manufacturers jump in first. So it's kind of a chicken and egg why am I spending money making my car more expensive when none of my competitors are providing this technology? Really, two vehicles have to be equipped and interoperable for the benefits to be able to be achieved. Here's this statistic that no manufacturer has more than 17 percent of market share. The average car is more than 11 years old and that number is actually increasing.

So as you see on the right, there in that graph, that number of how old the cars are is increasing which means if I deploy a car today in one of my products, in the first year I only have—even if I'm the major product—I only have maybe a one percent market share in that first year of what's actually out on the roads. The benefit that my customers received is pretty minimal. All of car manufacturers need to sign up to this. The good news is we are starting to see that occur. There are some car companies that are moving ahead with these deployments, but this is also pushing a lot of pressure on the FCC to finalize the decisions as soon as possible.

We also have to recognize that the level of technology will vary across the cars. So many vehicles will predate technology as the graph shows. For the first few years, the majority of the vehicles out on the roadways will predate the implementation of this technology. Further, even if the car I'm approaching does have this technology they may only have an aftermarket listen-only type device. So just because they have some sort of technology doesn't mean the technology actually support transmitting. And really, the transmission is where you're doing something, but the benefit primarily occurs to the person who's receiving your message because then they get to process it and make sure that you avoid a collision.

The other issue is that even if you equip vehicles, you might have the various levels of support. Basic safety will probably be supported by any device that has this technology. But reporting remote objects is going to be based on whether or not I have the sensors on my vehicle, so maybe only automated vehicles will report remote objects or heavily sensored vehicles will. Some vehicles might be equipped with automated driving systems, others won't. So how they use that data once that data is received will vary as well. Do they immediately apply automated braking? Or do they just warn the driver that there's a condition that he may want to brake, too.

Also the interaction with the driver might vary. There's no standards right now for how you alert a driver to someone in their blind spot or a car braking in front of them. One car might shake the steering wheel a little bit. Another car might rumble the seat. Another car might show an audible warning. And if I'm getting in a rental car what happens the first time that that happens to me? Do I even know what's going on? Or am I just distracted by this warning? So all of these things have to be sorted out within the marketplace.

There's other implementation issues. Agencies have little experience in deploying V2V technologies. Once again, we're talking about V2V technologies, agencies deploying—people tend to focus on collision avoidance. We're really looking at—right now—slow stationary vehicles, work zone warnings, emergency vehicle warnings, vehicle emergency response, vehicle turning in front of a transit vehicle; these things that have direct agency impact that are still vehicle-to-vehicle within this course. What we recommend is that agencies start looking at developing a deployment strategy for connecting vehicle technologies. One of the things they need to do is develop a deployment timeline to meet likely constituent demands. As your constituents start going out and buying automated vehicles and start buying connected vehicles, they're going to expect that the agencies have also made similar investments. If they're buying equipment and cars then they approach a work zone and they don't get a warning they're going to be upset, right? They spent a lot of money buying this product. And they feel like they should be warned when they approach a work zone, especially when the jurisdiction next to you has that technology and you don't.

So you need to start looking at how I start scheduling these things I have to implement in the future to meet my public demand now, so that the budget is there in place when you need to start investing it. We also need to consider the institutional issues, such as the need to develop an update agency policies and practices to meet these V2V needs. In other words, when should I use this sort of connected vehicle technology with my work zones? When will I use this for emergency vehicles? So combining with my timeline, what are my policies of when I deploy this? Which work zones get this technology first? How do I phase it into everything? All of those details. That will all help you to establish the budget for deployment and maintenance.

As we mentioned, all this technology is going to evolve. We have to plan for that, as well. And then finally, access necessary expertise for its successful projects. These are well outside traditional transportation applications. We need to make sure that you have the expertise needed and, hopefully as much as possible, be able to build the expertise within house to enable these projects to go forward smoothly. All of that suggests that your agencies should start looking at "how do we do this today?" because once technology starts getting deployed in new vehicles, that demand is going to happen very quickly for your public agency.

Now, we also talked about—there's a challenge of new applications and software updates. New applications will emerge and update continually. We need a way to install new and update applications within vehicles conceptually. They could be installed with a smartphone, the same basic way where you go to the app store and you download the application you want. The challenge here, though, is that if my smartphone crashes on me, that's no big deal. If the operating system within my vehicle crashes on me—and that's controlling my automated vehicle—now I have a real problem.

So the safety critical nature of a vehicle really complicates the installation. We don't want applications running within this environment that can cause any real problems with your safety critical functions of the vehicle. And recognizing that the applications, many of them will have need to access safety critical features of the vehicle. There is a need for collision avoidance applications to apply the brakes. If you're creating that link between that application, you really want to be able to constrain what sort of applications I can just randomly install on my equipment now. The applications—the interactions between applications—are likely to require extensive testing, which means you're probably not just going to a very open app store. You're probably going to a very dedicated app store where these things have not only been tested at a level of what the current smartphone manufacturers do, they've been tested on that particular make and model of vehicle, perhaps even your vehicle, to make sure that no adverse conditions occur.

This means that that first testing becomes very expensive. It will be a very dedicated type of application that you get for this type of installation. But we also have to deal with standards evolution. Those updates will have to be made. Any application on your vehicle today already goes through extensive testing. These applications and these updates will need to exist. You will need to install them. But that addresses how do we deal with standards evolution? So as the standards themselves evolve, you then have to implement them in the actual applications. And then you have the issue how does a Version 1 car deal with a Version 2 car? And how do they interoperate together? So that when we update the standards, we have to be very careful and there has to be backwards compatibility built in from day one. And that issue has to be addressed for each area of the communication stack.

So as we change from our access layers, whether it's a WAVE to C-V2X or whether it's WAVE Version 1, WAVE Version 2 or C-V2X Version 1 or C-V2X version 2, whatever the distinguishing characteristics are there we have to allow for the evolution to occur. That evolution might occur on a completely different timeframe than my facilities layer changing or my applications entity changing. In each one of these areas, we have to deal with evolution. We also have to deal with data ownership and privacy. There's a need to make sure that we limit the distribution of sensitive data. That sensitive data can reveal personally identifiable information that's very sensitive. And even if you're not directly revealing that information, it can be inferred many times.

So we mentioned before about if I know where the vehicle is parked every night then I can start inferring whose vehicle it is. Establishing rules on what information can be shared and used for what purposes. Right now within the U.S., there are very few regulations on this. But it is an area that we really, as we get in connected vehicles, really start and need to look into because right now that basic vehicle information that's being transmitted 300 meters—what happens if someone is sharing all of the data with another device and another device and they're collecting information across the city? Can I now consolidate that all into one massive data lake? There needs to be rules there on what data can be shared and used for specific purposes.

There's also a need for anonymity of vehicles and vulnerable road users. We talked about a little bit; the capability of tracking a vehicle. But even more so, if you're just a pedestrian on the sidewalk, I really don't want my smartphone to be able to transmit my location a kilometer away so that people can track me from that far away when I'm just walking down the street. There needs to be very clear rules on what data is actually transmitted that even could be used to what distance and making sure that that information is only available upon needs.

With that said, there is a need to reveal very personal information. For example, when I'm going through a toll booth, I need to link to my personal account which deals with my personal wallet and everything else. All of that needs to be dealt with in a secure manner. And then finally, there's still an open issue for C-V2X of how that data privacy might work within there as far as the lower layer identifiers that are connected to your phone, making sure that they're sufficiently unique and changing and anonymous.

There's also institutional challenges we mentioned; testing and certification within the V2V aspects of this. This is largely left to the private sector, or at least to a national testing facility that local agencies won't really need to worry about too much. They will be supported probably by USDOT projects, as appropriate, and development of common test pressure procedures, as appropriate.

Another institutional challenge is the SCMS. We mentioned a little bit that this has been sponsored. The current system is being sponsored by USDOT in order to get the pilot deployments up and running. That was done 2017. That was known as the proof of concept. And that was initiated intended to operate through 2020. So they have about another year to go on that. But there's a separate SCMS development project that is working closely with stakeholders to try to develop a viable ecosystem to determine how this goes forward and is then self-sustaining, so it's not constantly subsidized by the USDOT. They will develop a deployment strategy and define long-term governance of this national SCMS. That is still to come and that's actually being worked on.

In the meantime, USDOT is funding this and they are funding improvements to it to make sure that it incorporates all the latest standards. And we've alluded to this aspect little bit, as well. Deployment of the technology is another institutional issue. We've mentioned the importance of planning ahead and budgetary aspects. If we look at the way technology is adapted by the community, we start seeing we have innovators, early adopters, early majority, late majority, et cetera. And we look at the general innovation adoption lifecycle and then we start looking at where we are within connected vehicle applications.

We see that we are starting to get into—we're currently innovators moving into early adopters. If you look at the chart on the left, there you see in 2020, we're looking at an expectation of roughly one-and-a-half percent of new products made will be with connected vehicles. That's well into the innovator range. And then by 2022, we'll be into early adopters. And that's when you start getting pressure to have support services enabled, which isn't that far away, which means we need to start planning for the stuff now.

In fact, by 2024, we expect to be in pretty much full mode and to getting to the majority of systems, the early majority adopting this technology. We need to start developing plans to begin phasing in these applications. Once again, within the vehicle-to-vehicle context of this module, we're mainly talking about slow stationary vehicles, work zone worker safety, and emergency vehicle warnings. We need to ensure deployments, rely on modular designs to allow upgrading to new technologies. Because even this chart we see, the concept of multiple years to roll this technology out. Within those multiple years, we're almost certainly going to see updates to a lot of these different standards. We need to allow capabilities to upgrade our equipment as we're moving forward.

Well, that brings us to our fourth learning activity. Which of the following has not been identified in this presentation as a V2V service that agencies might need to consider for implementing?: A) work zone warnings; B) fleet management; C) emergency vehicle warnings; or D) slow vehicle warnings. Go ahead and make your selection and we'll review the answers here in a second.

Well, the correct answer is: B) fleet management. And while agencies may need to manage a fleet of vehicles, the V2V component of this was not identified in this presentation. Work zone warnings are included. That is certainly a topic that agencies consider equipping their work zone vehicles with technologies as well as any pylons or anything else with those technologies. Emergency vehicle warnings also should equip their emergency vehicles with technologies to recognize their presence, not only that there is emergency vehicle responding but where that emergency vehicle is. And then finally, slow vehicle warnings could also be deployed as well.

Well, that brings us to our last learning objective: describing the current status of connected vehicles. National SCMS development project, this ends in 2020 in December. USDOT is testing the V2X SubNet layer. So they're looking at how the Wi-Fi spectrum might be charged DSRC. They're looking into C-V2X. And another topic that we didn't mention much about is that same 5.9 GHz band is also used for some military radar issues. And there has been testing in that in the past with WAVE but there has not been with C-V2X, so the Department of Transportation (DOT) is also testing that out with C-V2X. Hopefully, those issues—both the SCMS development project and the V2X SubNet layer testing—will be addressed by the end of 2020.

There's also the C-V2X specification. Right now that is still under development. Hopefully, they can finish that up so we know how that works, if that's chosen as the technology. There's also active work going on, as we mentioned, for platooning and cooperative adaptive cruise control as well as cooperative perception. And then finally, all of the standards are being maintained constantly with lessons learned rolled back into them. And as a case study of that, we have the connected vehicle pilot deployments. There's more information about this in the supplements, including links to their websites.

But the pilot deployments identified several major issues that helped to address V2V challenges and kick start the connected vehicle ecosystem. They identified issues with privacy and they promoted additional privacy by refining the security certificate policies about how things change over time, particularly in taxis working in a very concise environment. They also helped refine a definition of crosswalks within MAP messages, so some of the more detailed items of—it's great to look on paper of how these things will—but when we actually get into real intersections with real crosswalks and other things, it really helps having a wide variety of intersections to look out to make sure that we all understand how to deploy this technology in the same way.

We also demonstrated over the air interoperability, demonstrating that these different products from different manufacturers who are all able to interoperate together. And they highlighted the need for vehicle support dual 1609.4 radios. There was a discussion early on that maybe a vehicle would only have a single radio and would switch channels back and forth. It was determined that really all implementations need to support dual radios, be able to listen to the main channel always and then switch channels on the other secondary radio. Adjusting each of these issues will facilitate all future deployments. That's the importance of having these pilot deployments go first, that identify some issues in different environments—very urban in the case

of New York City, very rural in Wyoming, and a third product in-between in Tampa. Other sources of information are available as well.

The primary resource for how these systems go together, the functions they provide is provided within the ARC-IT, which is the architecture reference for intelligent operative transportation. That is the major reference architecture for the ITS industry. The website there is shown, it's arc-it.org. It spans all of ITS so that includes connected vehicles. It also provides detailed references and standards with explanations of gaps, overlaps, and inconsistencies between the standards. So it's a very valuable resource with ARC-IT 9.0, will be available starting in April or so of 2020. It can be used as a resource for planning or deployment. There's toolsets there on the website as well to help you build your specific architectures.

That brings us to our final activity. Which of the following is USDOT currently testing in relation to communications technology alternatives offered by C-V2X and DSRC?: Are they testing the access layer; the transmit layer; the facilities layer; or the management entity? Go ahead and make your selection and we'll review those here in a second.

The correct answer is: access layer. DSRC and C-V2X are competing access layer communication technologies. The expectation, at this point, is all of the other layers would largely stay the same. It's just the access layer that is being debated at this point. The TransNet layer is defined by IEEE 1609.3. The facilities layer is defined by SAE J2735. And the security entities is defined by IEEE 1609.2.

So in summary, we've talked about the connected vehicle environment, we've then discussed the V2V communications and how that works, and then we described the rules of standards for V2V communications. We identified challenges realizing a V2V environment and then finally, we described the current status of connected vehicles. With that, that completes the V2V portion of the discussion. We mentioned before, there is CV261, which talks about vehicle-to-infrastructure for project managers. And you should have already taken the ITS Standards overview, and that completes that main course for project managers.

There are some more detailed connected vehicle modules. There's CV263, dealing with roadside equipment requirements. CV265 is an introduction to the IEEE 1609 family of standards. We had a few slides on 1609 during this presentation but that course will be devoted to that one topic. And then CV-273 deals with the SPaT and MAP messages. And then finally, CSE 201 is an introduction to the SCMS and goes a lot more into detail about the SCMS and how that works.

Well, thank you for your time. I encourage you to go online and take the survey for this course, giving information about how useful this course was. And I thank you for your time and look forward to seeing you back on other webinars offered by the ITS Standards program. Thank you.