Module 63
CV265: Introduction to IEEE 1609 Family of Standards for Wireless Access in a Vehicular Environments (WAVE)

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.

Raman Patel: Okay. This module, CV265, is about Introduction to IEEE 1609 Family of Standards for Wireless Access in Vehicular Environment (WAVE). WAVE is the terminology that we use collectively for the 1609 family of standards. I'm Raman Patel, your instructor for this module.

There are four learning objectives. The first learning objective is to describe IEEE 1609 Family of standards, what they are. We list them, components, standards as well. Learning objective two is to discuss IEEE 1609.3 Networking Services in a little more detail and the mechanics of it. Learning objective three deals with the role of 1609.4, Multi-channel Operations, how we conduct them. And the last learning objective, we're going to review 1609.2 security services provided by the standards, and we'll identify certain WAVE implementation issues and challenges.

Learning objective one is about what the CV environment is and how this standards, 1609 family standards play a role in that. So what is CV environment, Connected Vehicle environment? Actually, it's composed of three different parts. And the first part is consisting of the Vehicle to Everything: devices, users, V2V, V2I, and V2—P for pedestrians or users or road users—so that's the users. The second component to this environment is the CV communications, this mixture of two types of wireless communication for short range, and we are also using remote communication that we have been using for NTCIP, for example, from traffic management standard with the field devices. So it's going to be a mixture of two types of communication processes.

The third component, which is the main one also in this environment, is the safety and mobility applications. This application process is messages between different devices and they exchange information with each other and then if necessary, they issue warnings for driver, so the drivers can take certain actions. So there are three components, users, participants, devices, communication mediums and applications.

So what is CV environment? What is so unique about CV environment? Well, dynamic operational characteristics. Everything is changing. The participants are constantly changing. The devices' needs under this changing condition is also changing. For example, as shown here in the diagram, if you look at these two vehicles moving in opposition direction, there's a Doppler shift in the speed, for example. Both vehicles' total speed will be 120 or so, as an example. So that's the changing condition among the vehicles, the way they move on the roadway.

The third thing is the safety applications require frequent communications. For example, the safety applications require ten times per second kind of communication. So all these things are changing, that's what makes the CV environment dynamic. It's constantly changing. What is the WAVE communication system? WAVE communication system is a communication system, as the title suggests. But more precisely, it is a radio communications system. Everything is being broadcasted in the sense that it is an RF energy. And it provides ad hoc wireless connectivity for V2X. V2X means V to everything, to enable safety and mobility applications at the higher level entities.

All applications are considered higher level entities. So you will hear this word or terminology, applications at higher layer, very often in this discussion. And they provide privacy. It's like pseudonymity, where the data is coming from, who owns the data, and how the data is to be used. So those issues are privacy-related issues. And then security, of course, is authentication, where the message came from, who sent the message, and how it's supposed to be used. So the integrity of data that is being produced by the message is also an issue.

If you look at this diagram on the right side, which shows the general environment of connected vehicle operations in the field, and it gives us situational awareness. It provides more information in a dynamic way. Users and participants, everybody's together in this diagram shown are connected wirelessly. So that's what wireless system is. It's a communication system. Precisely, it's a radio communication system. So what is the mission of the WAVE—WAVE standard is?

Well, as this title suggests, the mission drives three key important ingredients. First, the development of interoperable and low-latency and low overhead. All these three key ingredients are embedded in the mission of WAVE standards. So devices need to work with each other. Also, they need to work faster in terms of delivery of message, and also low overheads. The messages cannot be lengthy. It has to be short and delivered very quickly. So what is the latency supposed to mean? Latency is a measure of time delay experienced in a system. It's end-to-end delay, how long it will take.

For example, in this diagram we are showing, Connected Vehicle Environment, all these different devices connect to each other, and the information or the messages, the exchange needs to be delivered very quickly. So the latency, for example, for the collision warning application is set at around 0.1 seconds. So all of the expectations that the message will be delivered within that latency limit is now fulfilled by the WAVE mission, WAVE standards.

Okay. So there are two types of communication technologies under consideration and we are using both of them, and we will discuss. The first one being the Dedicated Short Range Communication, or DSRC, which we have been using in the United States for many number of years now for different purposes. But here, we are using it for wireless connectivity on the roadside. So that is SAE standard J2945/1 for V2V safety application, and IEEE 160 family, particularly 1609.3 here shown, networking. We are using that as part of the Dedicated Short-Range Communication, DSRC.

The second alternative available is under preparation right now, and that is called LTE, Long-Term Evolution, V2X. It works on the Sidelink Mode 4 using PC5 interface. This is a 3GPP, third generation partnership project, release 14, 15, and now WAVE standards are being adjusted or under revision to make these WAVE standards available or suitable for this approach of LTE-V2X. So this is the second option available for us to use in Connected Vehicle deployments.

So uses of WAVE, J2735: V2X Data Dictionary messages, includes basic safety messages and the mobility-related messages. J3061 system engineering enhancement to the dictionary, 2735, is an information report. So these are published reports. So to also look at this list here, we also have additional published reports available, which are related to the standards, J2945, 45/1, 45/2, 45/3, 45/5, and 45/9. All of these standards collectively, and they are all published, and they are using WAVE standards, related to WAVE standards.

Also documents that are being developed now—or standards and documents both being developed right now—that will use or uses WAVE includes 2945/1, which is a vehicle-to-vehicle safety communications. This is a comparative to 2945, and this will be used for LTE purpose, LTE-V2X purpose. There is also 45/4, here is used for road safety applications for curve speed warning, work zone safety, and reduced speed zones. So there are certain application base standards profiles which will be available for us to be using it in CV deployments. This list is pretty much under preparation right now, in the development process, and it will be available once this process is completed.

There are standards—SAE standards—also in development, which uses WAVE standards. It includes particularly the important one here—right now shown at the top—is J3161/1, which is an on-board system for LTE-V2X.T hat was the second communication options that was mentioned earlier, and we will be using WAVE, using this particular J3161 standard one profile and discussion that will be available. That will make it suitable for PC5 Mode 4, physical interface, and that's something we will be using down the road.

The J3161 C-V2X profile shown here in the second bullet is giving us the 5G type of approach for using Connected Vehicle applications. And the other one is J3180, 86, J3216 and J3217 and J3224, all of them are related user with standards—that they use with standards—and they are all related to SAEs. So what is the relationship of WAVE protocols, the architecture to the OSI? There are two other models that we have been showing literally in the standard documentation as well as here in this slide.

In the middle, you are looking at the OSI reference model, which is a seven-layer reference model beginning with physical one, layer one at the bottom, data link two, network layer three, transport layer four and all the way up to the application layer. On the right, we are looking at the protocol approach applied to WAVE architecture. Layer five to seven are not used by WAVE. We are dealing only below that, meaning that network layer and transport layer, LLC, and physical layers.

So layer one, two, three, four are now addressed by the WAVE architecture. If you look at on the left side of the middle OSI reference model, we'll be looking at the idea station reference architecture, which also uses the OSI reference models for general connectivity requirements. And it begins with the access layer at the bottom, which is layer one and two, and network and transportation layer, three and four, is also combined. And then, of course, they also have the terminology used as facilities layers, which includes layer five, six, and seven.

As I said earlier, WAVE does not use level five to seven, and we generally refer to the higher-level entities or applications, which is being handled under the other standards, such as SAE J-Series standards. So this is the relationship of WAVE to architecture referenced to the other two models that are shown here. So what are the standards used by WAVE protocol architecture or stack as we might say? We might say that 1609.0, which is the architecture general guidance provided under this standard, is pretty good, and it covers all aspects of the WAVE standards.

1609.2 deals with the security services. 1609.3 deals with networking services, and 1609.4 deals with multi-channel operations, which are important contributions of the standards in the sense that we are able to now move from one channel to another channel to receive messages. 1609.12 is the general identifier. It's an organization that provides for the family of standards. IEEE 802.11 plays an important role here. MAC layer, the media access control layer, the sublayer and physical layer. This is where the activities for data actually—or message actually—gets transferred to the physical medium.

This is a very simplified architecture diagram, which is very helpful to us to understand how the standards are now coming together in each different layers. So, let me explain with saying that higher layer entities is not shown here. The message part of the discussion is not appearing here, but the rest of the other standards are here. So, let's start with WSMP. Wave short message protocol, it is a customized protocol for low latency in general. Also, the IPv6 features are also optimized for low latency.

So, both protocol stacks are existing in this architecture side-by-side. WSMP, which is a new one, and the traditional IPv6 are shown together. At the physical layer, at the lower two layers, layer one and two, we have applied 1609.4, which is now multi-channel operation, and at the lower two layers, we have a MAC and physical layers (PHY) are now governed by 802.11 standard. On the other side, on the left side, we are showing 1609.2, security services, provided by the WAVE standards architecture. This is shown outside of the management plane. It's an independent standard, and it's now being amended in many ways to take care of other aspects of the security. 1609.3 is currently under revision, as I said earlier.

Also, this new version will accommodate LTE-V2X. It's not able to do that. We are okay with 802.11 DSRC, but we are not okay with PC5 3GPP at LTE-V2X. That adjustment in 1609.3 is a necessity, and now the working group is working. So that aspect should be done sometime in calendar 2020. So, when that's available, this WAVE standards can also be used for LTE-V2X. So WSMP protocol, what is the purpose? What is the value?

However you say it, it is well suited to messages based on applications. So, it provides us with the low latency needs of CV applications, and it only supports broadcast, like one-hop messages. Once you put the message in broadcasting, it goes out to the receiving device. So, it's a one-hop direct communication. And the other part is it deals both at the network and transport layer. It's a common protocol that we use for both networking and for transporting messages. The IPv6 is also adjusted for low latency needs. There was some adjustment necessary so that it can be used in the environment that we are discussing today, which is the Connected Vehicle applications.

It has a little higher overhead and it also supports Unicast at the end-to-end kind of communication, and also handles larger messages, such as the information transfer, private conversations, and also dealing with the network communication. And it can be used with the traditional combination of UDP/IP or TCP/IP. So, both these protocols are deployable in CV architecture, WAVE architecture that we've been discussing here. So now let's look at the 5.9 GHz spectrum assigned by Federal Communication Commission (FCC). This is actually the current design that we are discussing.

So, the current design includes the concept of service channel, SCH. For example, SCH 172, shown here, is actually generally known as safety channels. Only safety related applications, life and property applications that are dealing with such a high level of safety issues are now covered by SCH 172. There's no other traffic on that except for the basic safety messages and safety related applications. Channel 178 currently is assigned—most typically, it deals with the broadcasting of advertising services. So, what are the other types of services available on other channels? This current spectrum design has seven channels. There are six SCH or service channels and one control channel, 178. So, 178 tells us where the information is available on the other channels and what that information is. 184, SCH 184 is used for emergency vehicles, and has a little higher power definition in terms of broadcasting power and that kind of requirements. Channel 174 and 176 are used for downloading application software parameters. For example, over there, you want to provide the updates. Without touching the devices, you want to conduct upgrading the devices, then you can use channel 174 and 176.

Similarly, channel 180 and 182 are also reserved for uploading mobility type of operations and performance logs. So, this kind of combination in this current design is allowing us to use seven channels, and this is current design. The reason why we use the word "current design" is that at the moment, this is the current design. It could in the future change, and it's governed by the FCC.

So how do devices work? This is another terminology we use very often in this discussion is the WAVE devices. So, WAVE devices actually transmit and receive messages or data from other devices in the vicinity. They're only interested in the messages of transmission and receiving messages in the vicinity. So, for example, a roadside unit, (RSU), is mounted on the pole or the mast arm as shown here in the left diagram that we're looking at, right?

On the right side, we are showing onboard, OBU, which is a roaming device, which is actually inside the vehicle. And between these two, RSU, which is a fixed device, and OBU, which is the roaming device, the information transfer or the message transfer is occurring over the air in a broadcasting manner. So that's what the devices do. They transmit and they receive message from each other in the vicinity. There are two terminology that are attached to the WAVE devices.

The provider. The provider is the device that uses or sends the messages. So provider uses WSA, WAVE Service Advertisement, which is normally conducted on channel 178 to indicate whether there is some other information available or opportunities are there for you to tune to other channels so you can get additional information. All right? So that's the job 178 performs. And this device is also called provider or sender, because it sends the message to others. The user functional—the activity is conducted by the device. So, channel 178 is being monitored by the user device.

Those devices who wants to receive or desires to get the information will tune to 178 and see what's available. So, devices play two roles, provider or sender, or user or receiver. So, let's have one activity now in our learning objective one.

So, the question is: which of the following is an incorrect statement related to WAVE system? A) WAVE devices deploy IEEE 1609.3 standard; B) WSMP/IPv6, both protocols, can be used at the network layer; C) WAVE Service Advertising, WSA, indicates BSMs, basic safety messages, on SCH 172; and D) V2X includes all forms of CV communication services. So, let's review the answers now.

The correct answer is C because WAVE Services or WSA indicates BSM on channel 172. That's actually not correct. So WSA is not used for safety 172 messages, because safety messages are always present on 172 channels only, so you don't need WSA. And A statement is incorrect, because 1609.3 standard is actually providing networking capability. It's actually a workhorse of the WAVE standards. Answer B is also similar, the statement is correct, because both protocols, as we discussed, are provided or supported by the WAVE standards. And the last answer D, the statement is correct, because V2X includes everything, V2V, vehicle-to-vehicle, vehicle-to-infrastructure, vehicle-to-positions, so everything is included in V2X.

Now, let's look at learning objective two, 1609.3, networking services. In the standards, networking services is a collection of management and data services. There are two planes. The data plane deals strictly about the messages and the management plane deals strictly about how to support whatever activities is going on in the data plane. So, there are two separate roles assigned in these two different planes. Let's look at the management plane here.

The management plane actually contains the function, full function in directly supporting what is happening in the data plane, WSA monitoring services, MIB. MIB stands for Management Information Base. It's a collection of data elements for device to manage itself, and IPv6 configuration. These three key functions are performed by the management plane. On the right side, we are showing data plane. So, let's look at what the data plane provides. So, data plane services includes WSMP, the protocol that we discussed earlier, this protocol at the network layer, and at the transport layer. So that is a key part of one-hop broadcasting messages.

For example, basic safety messages are transferred in one just single hop, and it goes on the device. So that's the job performed by WSMP. The LLC layer also is supported, and we also want to include that in this standard, we are discussing protocols supported by the transport and network layer and at other system layers. The IPv6 is also used for larger data transfer. For example, probe uploads, unicast messages between private conversations, and also the networking services, and we'll use one example for RSU to see how RSU can be used for routing services.

So, these activities are taking place in the data side or data plane services. And at the lower layer, we will have other types of services performed by the other standards. So, both standards, both protocols here mentioned, WSMP and IPv6, are distinct. They're both separate and distinct networking protocols. I put this note here just in case you are dealing with both of them together, and I want to make sure that we understand that both are independent, and they are distinct. They are not contained in each other's data frames. In other words, for example, IPv6 frames are not transported over WSMP or vice versa.

So, both of them have been assigned a particular task throughout this architecture process. The data services use this WSM, very short message, WSM, and has an N-Header and it has a T-Header, N-Header for networking, and T-Header for transport layer. So, in the front, you have an address information to recognize what the message is about, and that job is assigned to PSID. PSID stands for Provider Service Identifier. We will talk about it in a second, but this is a unique identifier, which will actually tell us the content identification. So PSID is—there are nearly a hundred applications are registered with this unique integer called PSID. PSID is registered by IEEE, and this link (https://standards.ieee.org/products-services/regauth/psid/public.html) provided here will tell you a little more about it if you'd like to get more details. Just go ahead and visit the site. And also, in our supplement, we are providing additional information for you.

So, every device has to deal with this issue of PSID. Let's look at this example here. OBU, onboard unit, has WAVE protocols inside and the other unit on the other side is also OBU. So, both of them are talking to each other using this air interface. And the WAVE devices create a list of PSID that are actively registered in that application process. For example, here, BSM, basic safety message, 020 will mean that it's a safety message, all right, and that's how this device is recognized, what's coming their way, or what the message is about.

Let's look at scenario one here. Scenario one, for example, is about 172 communication. Channel 172, as we discussed earlier, is reserved for safety messages. So WSA, Wave Service Advertisement, is not necessary for 172, because everyone or every device is configured only for 172. So here we're showing that—on the left side WAVE device, we are showing 172. And on the right-side device, we are showing also 172. Both these devices are configured at 172. So, they will continuously exchange information on 172 about messages. For example, WAVE safety message is transported or broadcasted, actually, at ten times per second.

The example could be V2I or SPaT messages. SPaT stands for signal phase and timing information. And SPaT/MAP data can also be transmitted on 172. So those two types of messages will appear on channel 172, and one being the safety message on V2V and the other is also V2I. So, this arrangement or this communication on 172 supports both kinds of applications. In scenario two, switches now gears to 178, CCH, control channel 178 communication. This is strictly reserved or most typically reserved for WSA. WSA are the additional services provided.

Here the device, that is provider device, will send a WSA indicating where the opportunities are available, which channel has what information, and how to receive it, you know. So that's a pretty good service that is provided by 178. And the user device listens to these things and says, "Oh, okay. I'm interested in it," and then they will switch to that other channel, whatever channel is provided in the message, and then they will participate. And they may not participate. It's up to the device configuration.

Let's look at the illustration of how V2X broadcast message will take place. On the left, we are showing RSU or OBU. On the right, we are showing OBU, one OBU. So, between these two types of devices or two devices actually communicates with WSM. Wave Safety Message is going to the other end, and it is going, you know, channel two support and says, "There is information available on some of the other channels." So, this communication is pretty secure in the sense that the WSM transmission takes place continuously between the different devices.

Let's look at the clear example of V2V safety. What is that vehicle-to-vehicle safety will look like? Here, in step one, is sending a provider device. This is the terminology we are very keen about using it in this discussion in the CV module or this particular Connected Vehicle modules, because each device has been given a role, either to send or provide the information using WSA. It's not required, for example, for safety messages, right, so this why I have the note here. So, 172 is assigned to do only—or conduct messages only related to safety. And these messages are appearing ten times. So, these devices are sending—or provider device—will send messages ten times a second and other devices in the vicinity will receive that.

How do we know that? Well, because the PSID, hex 20 here (0x20hex), is strictly assigned to those devices. So that's how the receiving device on the other end or the user device—this is the terminology we use. Any device that receives is considered as user device, right? And this device will recognize that PSID hex 20 is actually meant to say V2V safety. So, they will be most definitely, most likely be interested in this, and they will use that and process it, and then benefit from this communication. And that's how V2V safety applications are deploying this communication process.

Let's look at how V2I will work in a localized manner. RSU is a local fixed device. It's in one place. OBU is a roaming device, right? So, between these two, WSA plays an important role. RSU will send information about location, and the OBU will benefit from that. And whatever the information that OBU is interested, it will change those channels, switch the channel, and then it could do it with WSMP and get that information, or it can also use IP. Both protocols are now deployable here. And, for example, IP could be used in multiple ways. And one example here that comes to mind is the electronic fee collection or toll collection, right? So, you can use it.

There are other additional protocols that may be also deployed in this fashion. So, standard does not exclude the use of other standards. If you are dealing with the RSU and it has a connectivity with the host or cloud, and such applications are many these days, so OBU can also benefit from making connection in that sense to the RSU. So, after receiving the WSA, there is information in WSA, which is called WRA. RA stands for routing information, advertising, right?

For example, IP address could show up in our WRA, and that's how OBU can switch the channel and go to whichever channel suggested by WSA and make a contact with the host and the cloud, and then get the transfer or exchange the information. Example for this kind of application could be data collection. You can collect probe data from multiple sources and contact in the cloud. You can collect those data and bring it to your home-base device, and then benefit from that. So, such things are now being considered for V2I localized or cloud-based applications.

Let's look at the example or the illustration here about how do we make RSU a gateway? For example, you are in an OBU and a vehicle wants to make a connection to Internet or Traffic Management Center (TMC). How do we do that? Well, RSU, shown in the middle, will send WSA on channel 178 and that 178 message will appear using WAVE lower layer, and that's how the OBU will know that there is some additional information available. And then they will go through the IP process or TCP/IP process and switch to the channel, whatever channel it is, and that channel, using RSU/IP process, they will connect to TMC or wherever that information is available.

So that's how IP process will be conducted. So WRA is a routing information advertising, and that has the addresses of where to get this information, so generally its IP address is considered. Okay? So, this example for that matter could be used in any moving environment in OBU. It could be a snowplow, or it could be any other emergency vehicle trying to find out more information, and they have a need to connect to TMC, then they can do this. So, as I showed here, the TMC is connecting now to the OBU, which is a snowplow machine, and this is one of the examples that can be used in a generalized way.

We come to now our second activity. Let's ask this question here. Which of the following is not included in the IEEE 1609.3 standard? A) WSA; B) PSID; C WSMP; or D) BSM. Let's review the answers. The correct answer is: D) BSM. Correct, BSM is not included in 1609.3 standard. So where is it included? It's part of J2735, J2945.1 standards. Those are the standards that we deal with at the higher layer entities, which we call applications, right? Answer A is incorrect, because WSA is included in 1609.3. Actually, it is a workhorse. And PSID is also included in 1609.3, is another workhorse. And both protocols are supported in the standards.

So, we come to now our learning objective three. What is the role of IEEE 1609.4, multi-channel operations? So, let's review that. What is multi-channel operation supposed to mean? Well, we have generally said earlier as well, this current design is seven channels, right, available, and a device can only send one broadcast message over the air. So now what do we do? We end up switching channels between one to seven—one of those other channels—so it's communication between channels. So that's why multi-channel, the word "multi-channel" appears.

So, 1609.4 plays a very important role in providing us four different types of services in the management plane. Multi-channel synchronization. Channel synchronization is an important aspect. Channel access, which channel to access and how to access. Maintenance, as I said, is management information base constantly requires some updating here and there. Readdressing MAC address. MAC address, as we will discuss shortly, is a physical address, and this address gets changed during the process.

So, these are four functions provided by the management plane. The data services provided by 1609.4 includes the upper layers and also, we look at the connectivity. The MLME stands for MAC layer management entity, which is an extension provided to conduct the productivities that we will be discussing in details and channel coordination, channel synchronization, and all those things are supported through 1609.4. So, 1609.4, multi-channel operation, it does provide the extension to 802.11 MAC sublayer. It adds one sublayer above to utilize more than one channel and coordination. And it supports multi-channel operations. There are seven channels, as we discussed earlier, and this is supported by this extension.

So, 1609.4 multi-channel operation also supports dual radio operations. So dual radio operations can operate on multiple channels to ensure benefits of safety and other information of interest. So, what are we talking about here actually is bringing us back to the original concept that channel 172 is reserved for safety messages, as we said, right, by current design. So, if you don't want to miss, and you want to always receive safety messages on 172 channel, then radio one will be tuned to that 172. So now if you need to switch to other channels to see what's going on, what information is available, what opportunities are there, to be able to do that, you need another radio, two, which can be configured to switch channels. And that functionality of switching capability is provided by 1609.4.

So, radio two can switch from one channel to another to get additional information. So if you are from public sector and if you are wondering whether do I need one radio or two radio operations, this may be an important point you have to understand, that if you don't want to miss the 172 message, safety messages, which is your primary purpose in many applications, then you will probably have to consider using two radio operations. So, the role of 802.11 is to move data between MAC and physical layer, right, since layer gets transferred.

So after the message is constructed and brought down by transport layer, it has to cross to the physical layer so it can be put on the air and then broadcasting bits and bytes in RF energy, right? That job is performed by 802.11. So, it does provide the DSRC connectivity, and generally we refer to this as a radio operation. If you'd like more information on this particular standard, please visit this link that we have provided underneath (https://ieeexplore.ieee.org/document/6361248).

There are two types of addresses will show up in the MAC and physical layers, and both of them are important in our discussions, because IEEE assigns this 48-bits MAC address, which is the physical—which is at the network card, which is at the manufacturing layer, right? So, once it's assigned, that address cannot be changed. It remains permanent. And then IP address is also 128-bit in IPv6. It's currently in use heavily, IPv6. We also have 32-bits IPv4 also used in other applications, but not in Connected Vehicle.

So, we have these two addresses, and both are subject to change to preserve the anonymity or to provide pseudo anonymity to the devices. Okay. So now, what is channel coordination? Well, channel coordination supports data exchanges involving one or more switching devices with concurrent alternating operations on multiple channels. There are seven channels shown here, 172 on the left, 174 followed, 176 next, 178 in the blue, that is the control channel, SCH 180, SCH 192, and the last one is SCH 184. So, these are multi-channels, seven of them, right? And they are allocated two time slots, either time slot zero to begin with and time slot one.

So, zero and one time slots are alternated, right? So, safety channel, 172 to 184, all of the seven channels will be accessing the information, and multi-channel operation will be conducted between these two time slots, zero and one. Channel 178, CCH 178 is always tuned to slot zero, the first slot, which is the zero, okay? So, the next one is slot one, which is a 50-millisecond interval. Both of them are 50-millisecond intervals. And they are alternatively taking place as shown here in this diagram.

So, control operation will take place on slot zero, and SCH operation will take place in slot one. And that's how this time management is configured so that we can access multiple channels. So, they are at the lower layer. This is taking place at the lower layer, and it includes when and how these different devices will be accessed at the physical layer, right, and specific radio channels. So, this work is done at the lower layers. So, what are the options we have?

We have three options to access different channels, continuous channel, one channel continuously accessed as shown in the upper portion of the diagram here, right? CCH or 178, or SCH 172, those channels can be continuously taking part as shown here in a continuous manner. The second option we have is the alternating access. First is shown here in time slot zero, as it should be is the control channel, CCH, right? So, CCH could take place, or SCH can also take place. And in that way, we are now alternating. Next time slot one will be used for another channel.

The last option we have here is the immediate access. You are in the middle of a control operation, and you don't want to wait, and you've found something important or necessary or critical, whatever it is, and you want to continue immediate access. You want to gain access right away. Then the third option will allow you to jump in other time slots and continue until you finish your operation and come back to the original channel, time slot zero, right? That is the possibility [that] has been created by this standard.

So, there are three options: continuous access, alternative access, and immediate access. So how do we now make sure that this channel synchronization between slot zero and one takes place? So, there is a coordinated universal time, UTC. It is derived from a GPS, global positioning system, or GNSS. Generally, both of them amount to the same thing, GPS or GNSS, and they both can help us to get this UTC so that all different devices—RSU shown, for example, in the left diagram, right, and OBU shown on the right diagram, on the right side. So, you can communicate between the V2I, V2X, whichever part of the communication process you are under. You can use this synchronization using UTC. And this time it's available. If you would like to see while you are taking this—if you would like to see what the current time is, please click on this link: ***https://time.is/UTC***.

That's provided on the slide and you'll be able to know what the UTC currently is showing, and then you can actually synchronize your own watch and see what the value of UTC brings to this.

Now, the one point I want to make before we leave this slide is that if RSU and OBU are not on the same wavelength, in other words, if the timing is different between the two different devices and they're not synchronized properly in the time slots, the messages arriving in time slot one will not be synchronized. And that means that both devices will be disconnected in sort of communication-wise, right? So, the value of message will disappear if time synchronization does not take place properly, and that's the important part of this message.

We have now come to our activity for learning objective three. Which of the following is an incorrect statement? A) 1609.4 supports channel-switching capability; B) BSM messages are typically received on channel 172; C) channel switching operating occurs at network layer; and D) dual radio ensures continuous listening of safety messages.

Okay. Let's review now the answers. The correct answer is C, because the statement is incorrect. Channel switching occurs at physical layer, not network layer, right? Network layer creates the messages and brings it down, but the physical layer is where actual channel switching is occurring. Answer A is a correct statement. 1609 does provide us channel-switching capability. Answer B is also a correct statement. 172 is actually reserved for BSM. And answer D is a correct statement, because various operation—radio one operation is tuned to 172 for safety messages, and radio two can be switched to other channels. So, we have a win-win situation if we do both radio operations.

This brings us to now our last learning objective four. Let's discuss the role of 1609.2 security services and also some of the implementation issues and challenges presented by this deployment using WAVE standards. So, in this diagram, we are showing a number of vehicle are moving in both directions. Let's consider two vehicles and they're part of the dynamic ad-hoc network as shown here. So, the important issues here are these vehicles, they never encounter each other. They just showed up, right?

Second, they must establish trust between each other so they can comfortably send information to each other, and there's only a fraction of seconds left before an impending collision can occur, and also we have a need to maintain anonymity, you know, who these vehicles are, who these devices are, right? And system needs the capability to revoke credential. If something is not working out right and is misbehaving behavior from any of these devices or messaging structures, then we need to do some action. We need to revoke the credential of these vehicles so they cannot transfer data in a bad manner, right?

So, some of these issues are challenges that we have to look at it. So, let's start with the role of 1609.2, security services provided by this WAVE standard. So, WAVE standard features includes signing and verification of services, that is V2V broadcast messages are correctly taking place. WSMP protocol payloads, the data in the protocol, both broadcast and unicast, can be signed or unsigned, right, and encrypted. There are certain options currently available, is also including ISO 21177, which is a transport layer option there with the TLS, TLS stands for transport layer security, using 1609.2 certificates. So, this option is also available. And then security is not a layer. That's something that we want to mention here, because it is a plane. It's outside of the management plane shown here on the left side of the diagram, and it is a standard which is provided by IEEE 1609.2.

So, this standard applies to all layers of the protocol architecture in the WAVE. And it is the function of this service layer, 1609.2 services, to make sure that data transfers are occurring within the parameters specified by 1609.2 requirements. Okay. So, what are the additional features this standard, 1609.2, is going to be providing us? There are ongoing amendments and revisions being made to 1609.2.1, which will be the amendment, will support the SCMS, the security condition/credential management system, which is a separate development that is now going to be brought back to—brought into actually the WAVE standards through this process of amendment 1609.2.1. It is under preparation, and it should be available sometime in 2020, and it will support the certificate authorities as well.

So, WAVE security services deals with the certificate distributed using WSMP. So, this is the protocol that is brought by the WAVE standards, right? CRL stands for certificate revocation list, is distributed by the SCMS over the IP interface. That's a good use of IP interface so that the WSMP is now not doing that function, but it's done by the IP. The other point we want to make is that the certificates issues are constantly limited in lifespan. They're not constant. In other words, they're regularly renewed through automated processes. This allows the size of the CRL to be managed. CRL is the outcome of the misbehavior, it's called MBD in short, and it is related to revoking the certificate.

If something is not working out and there's a misbehavior of many different types, for example, duplication of messages, you know, the messages are changing after they are issued, many of these things could occur in this process, and this takes care of that. So digital certificate defines credential granted for what is the certificate is about. That's done through the certificate process, and it transmits the authorization. It transmits the authorization that this message being produced by a certain device or a provider or a sender is actually authorized. It's actually authentic, right? And the receiver device or user devices always constantly checks if the standard has the permission to carry out these actions, whatever the information they are sending.

So, if it is WSA, for example, is the information sent by WSA right? Is the device authorized to do that, and is something not make believe, it's correct, it's right, whatever you want to say, but the user device wants to know that. That is being clear by this certificate, digital certificate. And it has two parts. PSID is the first part where the application for which this standard is authorized is showing up. So every application has a PSID assigned, which cannot be changed, and if the sender's PSID is correctly displaying that message, then that is an authentic message that the certificate will be saying, who shoot is and what purpose, that means what application.

The other part—the second part to this process is SSP, service specific permissions. So this certificate will also indicate as additional detail what authorization is supposed to be meant for. It indicates what the details are about, what application it is about. So between PSID and SSP, enough information is given to the receiving device or the user device to be trustworthy and recognize that this is authentic process. This example of a TSP, transit signal priority, for V2I reminds us how SSP is going to be used.

So if you look at the TSP and understand that who is authorized to request the priority service, well, the bus, the bus device, onboard device is a priority requester, and this device will be honored by the traffic signal controller. And this environment is multiple. There are pedestrians walking. There is all kinds of users on the roadways, and signal controller is only one authorized to grant this request, right? So SSP process will ensure through the details provided and said, "What kind of information is provided, and who can actually utilize, and who can actually request that kind of messaging service?"

The role of application at the higher-level entity is signing the message, and applications that are higher-level entities, because that's where the process begins. That's where the application process—the messages—and actually develop the messages. So that's where the credentials are signed. So security service is now requested at that layer. And cryptographically, it binds a certificate to each message. It demonstrates that original message is authentic and has not been altered after it was issued. It's also binding by signing, and credential is issued by certificate authority. The authorities are known. This is like in between authorities who are now specifically asked to provide the service.

Some messages are signed and encrypted for authentication purposes. Others are only signed and encrypted only through the data protection purposes. So we have to ensure that how this process begins at the higher layer entity, and then when devices receive this information, signing process will ensure that these messages are authentic, and this is how confidentiality within the city is preserved.

The security consideration for WSA. WSA arrives on 178 channel, and it has a mark PSID 87. That's how it's signed. And any misbehavior can be reported using this service. So if a device finds something and notices and it says it's worthy of letting other people know about it, other devices know about it, that could actually generate a message on 178 and transmit using with PSID. So WSA security header is also signed with something called SPDU, the secure protocol data unit. And when it's signed and S is placed in front, the protocol data unit is actually encrypted that way.

What are the implementation challenges? We heard some of them. Let's look at the key areas where there are additional challenges, or what are the key areas we have to start with? Number one begins with evolving WAVE standards. We know that standards now are now in 2016. We are in version three of the WAVE standards. They are not experimental. They are not trial use standards. We have now established them, and they are published. So they are also constantly changing. Amendments are prepared, as you heard several times, and then SAE standards are also being revised and some of them are being published and amendments are under preparation. So all of the standards working together, you can say that they are evolving, and we should be aware of what is what. That is one of the reasons why we provided this listing of these current standards early on in learning objective one, okay? So you should be aware of that.

The second is the communication medium, what communication technology we are using so WAVE can take place and support CV environment, right? DSRC. It is something that we've been using for many years, and it's available, and we have experience with it. And that other option is now emerging, which is not quite yet available like now, but it will be available sometime in 2020, and that will be LTE-V2X, which will use WAVE standards as well, right? So this is something we have to know.

Dual radio operations, particularly if you are from public sector, are preparing specifications, it's an immediate issue. Do you ask for two radios or one radio? So that's an important area to pay attention to because you don't want to miss safety messages. Then you bring up the integration issues, and there are many of them, one being the interoperability, key issue, right? So that's a key area to pay attention to. Procurement issues. Multiple vendor relationships. There are more than one vendor involved in this process, so we have to be aware of that. We know that through this process over decades, dealing with ITS deployments. And a number of us have dealt with this, so we know what the real issues in dealing with multiple vendor is.

Then you have SCMS, the security implementation, and we have to be aware of that. It's an important issue. Intersection management for V2I traffic controllers' synchronization. These are different types of devices working in different environments. They need to work together, and that also means time synchronization with each other. And there are maybe project specific issues or Metropolitan Planning Organization (MPO), regional type of planning issues. So these are the key areas where our challenges will emerge from.

We look at this general list of stakeholders presented here: public agencies; vehicle designers; Original Equipment Manufacturing (OEM) manufacturers; after safety device vendors; after market safety ASD devices, which is retrofitting vendors; developers of application software standards; testing engineers. We also have certification groups, academic researchers both at the university layers, research layers, also at the U.S. DOT research programs and vehicle and fleet owners. That makes up a good list of stakeholders, which are affected by a number of issues either individually or collectively.

All of the stakeholders have to deal with some of these issues in that manner. Data exchange issues, support that we need for ITS information, WSA broadcasts, SPaT-MAP-BSM messages. In terms of standards, interoperability support, 802.11. We have 2016 now standards available. Earlier we mentioned in deployments we use 802.11p, which is now being replaced with these standards in 2016. IEEE 1609 family, version three standards published in 2016. Also the amendments are coming. SAE J2735 standards. USDOT also has issues version 4.1 of RSU specifications, which are practices that we need to look at it. And NTCIP 1202 version 3 traffic controller standard is also new, version three, and also V2IHUB controller interfaces. These are some of the good technical interface standards that we need to make sure that we have support for during the deployment and after that. And also WSMP version three, as I mentioned, and IPv6, and both of them are optimized. So we need to make sure that both of them support, if needed, is available in a proper way.

Security version two SCMS is a connected issue. So we brought these stakeholders and the issues together, because this is a general list of where a few issues and implementation challenges will come from. PICS sample portion. Here, PICS stands for protocol implementation conformance statement, which is provided each one of the standards. And this is a tool that allows us to ensure that everything that we are supposed to deploy together to make Connected Vehicle environment properly deployed so that we end up with the interoperability and all the features that we are looking for.

How do you know that? Well, this is one of the tools that will make sure that we include everything. So on this list, for example, M stands for mandatory and O stands for operational. So all of the mandatory features required by the standards, we have to find the support, yes. We have to make sure that we are allowing the community or suppliers to know that we need support for this functionality, okay? So, for example, IPv6, the standard does not tell you that you should have it, right, but if you do use it, and if you are going to have large data transfers, you need IPv6 data support, or the protocol support. And in that way, you are now utilizing this PICS to make sure that everything that you need is now listed here.

So what are the benefits of using PICS in particular and in general? Let's start with the in general. In general, the entire project will benefit. All stakeholders, all those issues that we mentioned earlier, all types of stakeholders will benefit. Specifically, an implementer, for example, will know what functions the implementer wants from the deployment, and it could indicate features and ensures that the support provided at the implementation level is required. If you're a vendor, you unambiguously know upfront, right? You know what the client wants, and you give the client what they client wants, then you don't have issue to deal with later on. There's no finger pointing.

So what project needs are, and we are avoid finger pointing or disputes later on. “You said this, I said that,” that kind of thing, right? The confrontation is now almost eliminated if you use certain tools like this. If you are a tester, this is a delightful way to begin your testing process, very methodically. Organization is provided, and the checklist could be used against each one of these conformance requirements. Hence, the deployment deliver what the PICS' suggesting, right? So the tool can be used in that manner as well. If you are a system integrator, whose role is to bring everything together, it's peace of mind, right?

Interoperability, functionality, different devices, durability, dependency, security, privacy, all of these things are now piling up on you as a system integrator, and at different stages they may show up. But at the end of the project, you have to ensure that all of these things are taken care of peacefully, and that is the job PICS can help you perform better and gain some peace of mind. So multi-vendor relationship, it comes in a big way in Connected Vehicle. We know dealing with ITS issues over the decades that this is a different issue. Sometimes it becomes more than difficult, and then it becomes complex actually. But here in this environment of Connected Vehicles, we are now dealing with vendor A, which is the supplier of RSU, and it has all kinds of different RSU used in the projects, different locations, and you have vendor B, which is another vendor supplying also RSU.

So you have multiple vendors now providing the same device in a different timeframe or different applications, then this issue between A and B you will have to deal with. Vendor C, retrofitting, and most of the retrofitting on a V2X side, vehicle-to-vehicle, examples are here, taxi, trucks, buses. All of these vehicles are retrofitted with OBUs, and sometimes it's called after market safety devices, ASD. And there are so many of them, and this way, you have in a vendor A, B, C kind of relationship all over, and now you have to deal and answer this question, “What are we procuring, and how we are dealing with that procurement?”

So this coordination between different vendors is necessary. And I might also want to add that sometimes you might find resistance between different vendors in providing you necessary information. Then you should be prepared to deal with these issues. So this is a huge challenge out there, and you should be prepared to deal with it. In terms of U.S. deployments, Connected Vehicle deployments, this is a very good chart provided by Volpe and prepared in February of 2020, pretty up to date. It has a large number of operational devices and their combination out there.

You have roughly over 19,000 different devices in play, and all kinds of applications, including the one you see here very prominently is SPaT. So these are small cities, big cities, regions, different parts of the country. Any way you look at it, deployments are out there, and they are still underway, and so this chart gives us an opportunity to look at it, how the deployments at different scale are occurring within the country. Specifically, the three pilots that we heard about—Wyoming, for example. If you look at the RSU, roadside unit, 75 of them, and you also look at Tampa. You have 742 different devices coming into play and the roadside units also, the RSUs are also listed here, 47.

So this discussion we have been following for a while in terms of multiple devices in multiple environments, multiple application, multiple vendors also present in the pilots. Look at the New York pilot, which is the largest of the three, and it has a large number of vehicles involved, 400 RSUs out 450 already installed out there in different terrains and in different mounting details. They are showing here on the right side RSUs are mounted on the pole. Sometimes they are mounted on the mast arm, but created with visibility, and also there is no obstruction, right, in the canyons.

In a city environment, urban environment, buildings may block the line of sight. So such things are very important to make sure. And we have to verify that over the air, firmware updates can be made. For example, this is one issue that has shown up in deployment, which needs to be highlighted is that we are not going to every RSU or every device out there in the field, right, and make the software changes. We want to be able to do that using over-the-air facility, broadcast facilities, and that's something we tested, and it's working pretty good.

So we want to make sure the installation process and dealing with the devices also gives us some comfort level, and that's what the New York City pilot has done for us. U.S. DOT has also provided us a great deal of information, lessons learned through this multiple vendor ASD interoperability testing process that they have conducted. I urge you all to visit this site listed at the bottom and understand what this interoperability testing process is. These are different devices used in different pilots, so that means different region of the country, right? And they test them together and to see if this device is nationally also interoperable in terms of the utility, and the answer is pretty good, so that's a good part.

So what have we tested? Well, in this report issued by DOT, we learned that the reception of the V2V and V2I communication interoperability process is pretty complete. Test messages do arrive as expected, and they are constructed as they should be, right? So anything about the message and interoperability has been tested, and that is—well, this report tells us that. What it does not tell us is that performance testing, how well we have performed the Connected Vehicle operation. That job is left to each individual deployment project, and the project will have to deal with that performance issue themselves.

So this case study that we are presenting here is from Florida's Regional Advanced Mobility Elements called FRAME and it deals with device testing for interoperability. It has a definite structure, what this testing process looks like, what are the devices being tested, and in which environment the testing is taking place. So the lab set up included 21 manufacturers and three different types of devices, five controller manufacturers supplying different controllers, nine RSU manufacturers supplying different RSUs, seven OBUs.

So you have 21 manufacturers all together for all these three types of different devices, right? And they have been tested in the laboratory environment, as well as in the field testing to validate whether these messages shown here in this diagram are arriving as they should be on the receiving side and they are formed properly at the transmit side. So the relationship between sender device and a user device for this SPaT, MAP, and TIM messages is being tested by this project very nicely.

So when we look at the details, it tells us a very complex level saying that, “Yes, all the deployment expectations around these different devices from different manufacturers actually has occurred and verified.” So to make sure that all our devices are conforming to standard so we get all the benefits that we just mentioned and talked about, conformance to the standards is necessary as the implementation progresses and the requirements are met. So standards specifications must conform to—the WAVE devices must conform to the standards, and conformance is to 1609.3, 1609.4, and all of the standards listed here. The WAVE device must be compliant to that.

1609.3, particularly, implements the LLC layer, both protocols. So we’ve got to make sure that we’ve got the support for both protocols, not just one, you know, WSMP, and transmit/receive functionality also has to be verified. So 1609.4, we are discussing here about the receive process, and all of the other transmission process is taking place in a proper way. Details are actually in the standards. I have not discussed this in detail, because the standard is actually very detailed about this particular process. So I suggest you make sure that all of the requirements are included in the specification.

Here’s an example of compliance language for dual radios because dual radio is supposed to be a very critical part of your specification writing process. And this example tells us—this is a publication available at the lower link: https://www.cvp.nyc/project-status. I have shown below, and each RSU shall include two radios. You need to be aware early on and make sure that these two dual radio operations is asked for if you are making sure that you will get there. And nominally, all the process is connected to that. For example here, the standard specification means that channel 172 will do this, this and that, right? So that’s just an illustration of how DSRC specification can be returned.

Our last activity, which of the following is an incorrect statement? Answer A) WAVE supports both WSMP and IP protocols; B) IPv6 protocols, compliant devices are typically interoperable; C) PICS should be included in a CV project specification; and D) WSA broadcasts opportunity on any channel. Okay. Let’s review the answers.

The correct answer is: D) WSA broadcasts opportunity on any channel. It’s correct because WSA is typically issued on channel 178. It is reserved for transmission of WSA on 178, right? A is incorrect, because WAVE does support both protocols. B is also incorrect, because they are tested and messages are exchanged for interoperability, and C is also incorrect, because PICS can be used as a checklist. We discussed that, and everybody benefits from using the checklist. There are additional technical resources available, and we have provided this information as well in the supplement, so please look at that.

The supplement provides a lot of details. I would also suggest you look at the standards development effort going on at ITE link: (https://www.ite.org/technical-resources/standards/rsu-standardization/). You will gain more information about what the RSU standard development process looks like. And the last, the RSU specification 4.1, is also available, which you can download and consult with your specification if you need to work on that.

So these efforts are to us—are improving the—not only are they improving, but also providing additional information in terms of how to make CV deployment a successful venture. In terms of training modules, [they] are available related to CV listed here. How to test Connected Vehicles certification process is in T160 module. CV-261 and CV-262 together provides V2V and V2I standards that are used for managers. CV-271 deals with the original intersection related applications. CV-273 SPaT and MAP related implementation. Transit 11 is specifically about standards necessary and required and how to put them together for transit CV applications. Transit 24 actually deals with TSP and is pretty up to date. And two modules on cybersecurity, CSE-201 and CSE-202, are also providing us more information related to how to deal with cybersecurity issues. So there's a pretty good resource arsenal at our disposal at this Professional Capacity Building (PCB) ITS site.

So let's review what we have discussed in this module. We discussed the different type of standards used in the CV environment to support CV environment and we particularly discussed the WAVE standards. We also mentioned SAE J standards and how they work together. These standards work collectively together to deliver the WAVE environment. In learning objective two, we discussed specifically the services, networking levels services provided by the 1609.3.

In learning objective three, we discussed in details about channel synchronization, multi-channel operations, multi-channel accessing taking place, and we also brought out a couple of times how various devices will need to work with each other in time slots so the messages are now delivered and received on time in [the] proper way. And we just finished reviewing the last learning objective is the challenges presented by services, security services, and also in the deployment level, what important key areas that we need to pay attention and what are those issues affecting different types of stakeholders.