A Primer on the Connected Vehicle Environment

Prepared by the National ITS Architecture Team, supporting the Connected Vehicle Reference Implementation Architecture (CVRIA)

November 2015

The Connected Vehicle program is a large set of research activities centered around a vehicle or a mobile device that is equipped with communications and processing allowing those equipped platforms to be aware of their location and their status and to communicate with each other and with the surrounding infrastructure. This enables Cooperative Intelligent Transportation Systems (C-ITS) or, as commonly known in the US, “connected vehicle”.

This Primer has been developed to provide an overview of the connected vehicle environment and to discuss some of the larger issues that pertain to the overall environment or ecosystem as some have called it– things that make connected vehicle unique from other ITS solutions.

Introduction to the Terminology

First let’s get our terms straight – what do we mean by connected vehicle? Is that the same thing as ITS or is there more to it?

Let’s start with ITS since that term has been around since the 1990s.

What is ITS?

Intelligent Transportation Systems or “ITS” has been defined as the electronics, communications or information processing in transportation infrastructure and in vehicles used singly or integrated to improve transportation safety, improve mobility, and enhance productivity. Intelligent transportation systems (ITS) encompass a broad range of wireless and wired communications-based information and electronics technologies.

OK, so what about Cooperative ITS?

What is Cooperative ITS?

Co-operative ITS is a subset of the overall ITS that Communicates and Shares Information between independently operated and independently authenticated devices to give advice or facilitate actions with the objective of improving safety, sustainability, efficiency, and comfort. This means devices and users in the system have to trust one another. This concept will be explained later.

The term Cooperative ITS is a term used mostly in Europe and other parts of the world.

And Connected Vehicle?

"Connected Vehicle" is currently the term used in the United States to describe the technologies in a vehicle or a mobile device that is equipped with communications and processing allowing those equipped platforms to be aware of their location and their situation (location, time, kinematics) and to communicate with each other and with the surrounding infrastructure. So, connected vehicle implies connections between vehicles and between vehicles and infrastructure devices. The "vehicle" aspect of the US connected vehicle program includes all types of vehicles as well as personal portable devices used in the transportation domain.

You can see from the definitions above that the two programs Cooperative ITS and Connected Vehicle are similar. For purposes of this Primer we'll say that what the US calls "connected vehicle" and what Europe calls "Cooperative ITS" are the same thing and refer to the same basic technologies.

What Is So Unique about Cooperative ITS or Connected Vehicle?

To know what is so unique about a cooperative ITS versus a *regular* ITS we need to go back to the definition and focus on a few key phrases. Knowing what is meant by "*independently operative and independently authenticated devices*" will help us see that there really are some key concepts that make this a truly unique set of technologies.

There are some unique application concepts, new communications media, new use of existing communications media, different institutional relationships, and new concepts when it comes to trust and security that make a connected vehicle environment a truly cooperative intelligent transportation system.

Application Concepts

Independent and yet connected – In the connected vehicle environment cars still move about as they did before; that is they are still independently owned and operated but now they are connected to each other and to the infrastructure. From the infrastructure perspective things are pretty much the same as regular aspects of ITS in that agencies own the rights of way along the road and still deploy their own devices and control them in order to manage the flow of traffic, passengers, and freight through their region. In the connected vehicle environment, however, agencies now have access to data about their network that was generated by in-vehicle devices and sent through communications channels that those agencies don't control. Likewise, to send information to all travelers agencies can take advantage of devices and networks that they don't own or control. This independent yet connected world may be new to some agencies and even some travelers. It may take some getting used to but it should result in better data and lead to better, more timely, decisions.

In some ways these are new concepts but there are some old principles at work. The connected vehicle environment establishes a language and rules for communicating with all parties. Rules for communicating information to drivers go back a long time. For example in the 1930s the transportation domain established that stop signs would be octagonal. Today, that shape immediately communicates critical safety information and drivers around the world know what to do. The connected vehicle environment is establishing some new concepts that will also one day be second nature to agencies and travelers.

Let's look at one simple example of this distributed or independent application concept by looking at Curve Speed Warning. Today, a yellow sign is placed within view of the oncoming driver to warn them in time to slow down in order to safely travel through the curve. In the connected vehicle environment, there is a recognition that not all vehicles are alike and that situations and conditions change. The application concept can be such that the central system can establish locations for all of the dangerous curves in their region. The information could be distributed to vehicles in a number of ways that we'll get into in the communications section. Once that information gets into the mobile devices, the mobile application could determine when the vehicle it is operating in is approaching one of those curves and whether or not a warning is needed. The vehicle may be a large vehicle like a school bus and a definite warning is needed. On the other hand, a small vehicle traveling below the safe speed may not need more than an informational message rather than a warning unless weather conditions have changed to make the pavement more slippery in which case a warning may be needed.

This separation of the underlying data from the presentation of information to the user is a concept that shows up over and over again in the connected vehicle environment.

Communications Concepts

The connected vehicle environment is opening up old assumptions about how projects were deployed and how systems and devices are connected. In the old days an agency like a traffic department would deploy devices in the field and connect them to their central servers using networks that they also built and maintained. In some cities one agency might share networks or even the data on the networks s with another agency in the same city. On the private side, users were accustomed to subscribing to services from one or a few providers. Everything that the traveler had access to came through that single interface to their provider.

The connected vehicle environment has opened up the communications possibilities with new choices for media to carry information in open, secure ways. The connected vehicle environment takes advantage of established network standards such as Internet Protocol version 6 (IPv6) along with transportation specific standards for data and messages between transportation centers and infrastructure.

The newer, mobile portion of the connected vehicle environment makes use of many types of communications media and technologies – basically, whatever works to get the right message to the right place at the right time.

- Short range – so called "Dedicated Short Range Communications" or DSRC have been the "poster child" for the early days of connected vehicle research. Indeed, this unique type of technology enables many safety benefits, including collision avoidance when vehicles can communicate their position and status to each other. This communications path creates a high bandwidth, low latency communications path ideally suited to supporting safety applications. Mobility and environmental benefits can also be gleaned by using this same short range interface for vehicles to communicate with the roadside. For example, roadside devices can provide signal phase and timing data, information about the presence of other vehicles, or speed zone data, or emission zone data to approaching vehicles.

  In the U.S., 75 MHz worth of spectrum have been set aside, or dedicated, around the 5.9 GHz band with an effective range of about 300 meters in most situations. This specific allocation of spectrum has been used to support the DSRC-enabled safety research and remains the fastest way and best way to implement Vehicle-to-Vehicle (V2V) safety. Fortunately, a lot of work has been done to standardize this interface with the Society of Automotive Engineers (SAE) and their J2735 Message Set and the J2945 series of performance standards for the interface. In addition IEEE's 1609 Wireless Access in a Vehicular Environment (WAVE) family of standards for communicating across this interface as well as an extension to their IEEE 802.11 Wi-Fi standard provide the protocol details below the messages. Together, these protocols allow vehicles and other equipped devices to communicate effectively and securely.
- Long range – DSRC may be the way that connected vehicles communicate with each other or with intersection signal-based devices, but there are many other technologies available that are already in use to communicate with the infrastructure. Modern Wide-Area Wireless technologies, chiefly cellular communications such as 4G Long Term Evolution (LTE) allow mobile devices to connect quickly and securely through a reliable network to share information with centers like information service providers or other data distribution systems. Data traditionally held by transportation centers, particularly data of regional interest such as advisories or even traffic signal patterns for an arterial corridor, can be placed in a data warehouse and distributed to mobile devices through mechanisms like publish-and-subscribe when those devices need it.
- Broadcast technologies – The connected vehicle environment can also take advantage of digital broadcast media to send traveler advisories or other connected vehicle data out over potentially very large areas. Satellite communications systems, originally used for entertainment, are also proving to be useful for distributing data to mobile devices over a large geographic area. Terrestrial-based systems that work over FM radio can also be used. These broadcast media may be very economical when everyone needs the same information at roughly the same time. In the connected vehicle environment this might include weather alerts,

bridge/road closings, or lists of 'bad actors' whose messages can no longer be trusted (more on trust and security later).

The point is that as connected vehicle systems are established the deployers and users don't have to feel that they are automatically locked in to one type of communications.

Independence & Trust in a Connected Vehicle Environment

We talked about independence earlier – how in a connected vehicle environment the operators of one type of device, say in a vehicle, will use their device independent of other operators in the overall system, like the traffic control center that is issuing the alerts to drivers in the area. This "duh" concept is actually different than our mindset of command and control where a big control center has access to data sources that it created, including sensors it planted in the roadway, and uses that data to decide what devices to control and how to perform the control, with all this done over networks that it controls. Even on the traveler side – in order to get traveler information about one area a traveler had to get an app for that area/agency, such as a 511 app, and that agency controlled the interface. In the connected vehicle environment, the agency does not know where the data originated – it doesn't need to. Nor does the traveler need to be tied to one agency's app or signage they can use their own device wherever they go and get similar results. Again, they don't need to know who supplied the data.

The connected vehicle environment is built on standardized definitions of the primitive pieces of data that flow from source to destination that can be picked up and used in many different ways. But to do all of this we need to trust that the data we get is what it says it is. Regarding the sender of the data, we don't need to know them or have an established relationship with them so long as we can be sure that they are a trusted member of the environment.

It is this foundation of standardized data and trusted communications that enable and propel the connected vehicle environment with all of its applications, to make a real cooperative ITS.

So how do I trust someone and how far does that go?

We covered independent ownership and operation above but how do I trust the parties on the other side of an interface? We need an independent way to authenticate the other parties.

Trust is established by taking advantage of something the Information Technology industry calls Public Key Infrastructure (PKI). Anyone that has had to electronically 'sign' a form or use a credit card to purchase something online has used PKI in one of its forms.

All users in the connected vehicle environment – all drivers, operators of systems, agencies that deploy field equipment, developers of hardware and software – will apply for credentials called digital certificates. When messages are transmitted over an interface this certificate is used to 'sign' the message. This signature will allow the receiver to know that the message is from a valid/trusted sender. If the signature isn't there or the message is garbled in some way then the receiver can decide not to trust the incoming data. This process will be largely transparent to the end user as it is today when your web browser applies for and receives digital certificates on your behalf to support on-line shopping and other secure applications.

What about privacy? If a driver is driving around and their car is giving out messages to other vehicles or to devices along the roadside won't their privacy be compromised? The answer is no – or at least, No, not if the system can help it. First of all those safety messages don't contain any information that can be tied to an individual. The safety messages just tell a receiver that there is 'something' at this point going in this direction at this speed.

What if I want to conduct a transaction with my connected vehicle or cooperative ITS device like pay for parking? In that case, the same PKI technology is used to encrypt the message. Encryption prevents data that is inside a message from being understood by anyone other than the intended recipient. Even if someone was 'sniffing' for data they would just see a garbled stream of bits and have no idea what was inside it. The sender's device encrypts the data and addresses it to a specific place like a parking service provider. Then only that parking service provider's certificate could be used to decrypt the message.

This concept may actually be commonplace to many users and travelers by now but for agencies that are used to owning their own networks all the way out to their field devices this may require a mindset shift.

To operate successfully and safely in the connected vehicle environment users should think about having secure transmissions between all devices. Get used to setting up secure networks and sending encrypting messages as the default method.

There is a way to think about this as deployers consider how they will build their projects. The US government published Federal Information Processing Standard Publication (FIPS) 199 that established Standards for Security Categorization of Federal Information and Information Systems. FIPS 199 presents a way to assess any information system in the categories of confidentiality, integrity, and availability. With those criteria deployers assign a low, moderate, or high impact rating to a device or an interface. The most severe rating from any category becomes the information system's overall security categorization.

When we conduct this "C. I. A. Analysis" we may find places where data should be kept 'confidential' and to do that in the connected vehicle environment means that we encrypt the data.

How Is Cooperative ITS Deployed?

There are some unique aspects described in the previous section that now must be considered when a set of stakeholders wants to deploy a connected vehicle or cooperative ITS project.

Deployment is the provision of connected vehicle applications in a defined geographic area to a defined group of transportation users.

The Connected Vehicle Reference Implementation Architecture (CVRIA) shows many applications that have been studied and, in some cases, brought to some level of fruition. That reference architecture includes several different types of transportation applications; either safety, mobility, or environmental applications. It also includes support services that make the other applications work in a real world. It's hard to use the word mandatory but some of the support services are close to being required in order for any connected vehicle deployment to work.

The two highest priority support services for any connected vehicle project are:

1. Security Credential Management
2. System Monitoring

If a project is going to involve more than Vehicle to Vehicle (V2V) applications then these other support services will be required:

1. Data Distribution
2. Object Registration and Discovery
3. Infrastructure Management (if the project is deploying roadside equipment)

A deployer is responsible for providing these services, either directly or through a third party, in order to deploy a connected vehicle application.

Does that mean I have to build my own cyber-security credential management system? No, in fact for the CCMS the idea is that there will be one overall architecture for security but everyone will have to show that they are interfacing and using that approach. The details of this scheme are still under development and the USDOT will provide more guidance on this in the future.

How Can I Find Out More?

The purpose of this brief document was to point out some unique aspects of the overall connected vehicle environment.

Here are some pointers to resources online that explain other parts of the connected vehicle technology, architecture resources, and other training sites.

- CV101 is an introduction into the background and motivation behind connected vehicle technology and descriptions of some of the basic applications (https://www.pcb.its.dot.gov/documents/ConnectedVehicle_Program101.PDF)

- US DOT piloted a "CV102" course that goes further into details about deploying connected vehicle applications, see www.its.dot.gov.
- The CVRIA website provides the overall reference architecture for the connected vehicle environment and from that same website there is a free software tool, SET-IT that works with Microsoft Visio to build project architectures based on the CVRIA reference. Use the Sample Project included as part of the SET-IT software tool to see how to include the mandatory support services described in the previous section.

In general, most of these resources can be found on the US DOT's ITS Joint Program Office website (www.its.dot.gov) and training resources are found on the DOT's Professional Capacity Building (PCB) site at www.pcb.dot.gov.