



United States Vehicle-to-Infrastructure Communications; Day One Deployment Guide

5GAA Automotive Association
Technical Report



CONTACT INFORMATION:

Lead Coordinator – Thomas Linget
Email: liaison@5gaa.org

MAILING ADDRESS:

5GAA c/o MCI Munich
Neumarkter Str. 21
81673 München, Germany
www.5gaa.org

Copyright © 2023 5GAA. All Rights Reserved.

No part may be reproduced except as authorised by written permission. The copyright and the foregoing restriction extend to reproduction in all media.

VERSION:

DATE OF PUBLICATION:

DOCUMENT TYPE:

Technical Report

EXTERNAL PUBLICATION:

Yes

DATE OF APPROVAL BY 5GAA BOARD:

October 12th 2023

Contents

	Foreword.....	5
1	Introduction and Scope.....	6
2	End-to-End Deployment Process Guidance.....	8
2.1	Deployment Tasks.....	8
2.2	Deployment Task Descriptions.....	11
2.2.1	Application Message Set Identification and Planning.....	11
2.2.2	Procurement, Evaluation, and Agency Testing.....	11
2.2.3	Conformance Testing and Certificate Provisioning.....	12
2.2.4	Deployment.....	12
2.3	Deployment Task Report References.....	13
3	Day One Messages.....	15
3.1	Message Descriptions.....	16
3.2	Message Users.....	19
4	WAVE Protocol Stack.....	20
4.1	SDO Message Report References.....	20
4.2	SAE J3161 SDO Report.....	24
4.3	IEEE 1609 SDO Report References.....	26
4.3.1	IEEE 1609.3 WAVE Service Announcement Profile.....	26
4.4	3GPP Release 14 Report References.....	27
4.5	Supporting Report References.....	27
5	Hardware.....	28
5.1	Report References.....	28
5.2	System Architecture.....	30
5.3	Physical Installation.....	30
5.4	Environmental, Mechanical, and Power Considerations.....	32
5.5	RF Configuration.....	33
5.6	RTCM Corrections Support.....	34
5.7	Local Certificate Download Support.....	34
5.8	Hardware Capabilities for Future Use-Cases.....	34
6	Security.....	35
6.1	Background.....	35
6.2	SCMS Manager.....	36
6.2.1	Trusted (End-Entity) Devices.....	37
6.2.2	Trusted Messages.....	37
6.3	Certification Entity.....	37
6.3.1	OmniAir Conformance Specifications.....	37
6.3.2	Message Conformance Test Procedures.....	38
6.4	Misbehavior Reporting and Revocation.....	40
6.5	SCMS-related Report References.....	41
7	Other Things and What's Next.....	42
7.1	Emerging Guidance from CTI.....	42
7.2	Additional Considerations and Guidance.....	42
8	References.....	44
9	Definitions and Abbreviations.....	45
9.1	Definitions.....	45
9.2	Abbreviations.....	45

Annex A:	Simulation Results	48
Annex B:	Day Two Messages	54
B.1:	Message Descriptions	54
B.2:	Message Users	55
B.3:	SDO Message Reports.....	56
Annex C:	Future Hardware Capabilities	57
Annex D:	FHWA Vehicle Category Classifications	58



Foreword

This Technical Report has been produced by 5GAA.

The contents of the present document are subject to continuing work within the Working Groups (WG) and may change following formal WG approval. Should the WG modify the contents of the present document, it will be re-released by the WG with an identifying change of the consistent numbering that all WG meeting documents and files should follow (according to 5GAA Rules of Procedure):

x-nnzzzz

- (1) This numbering system has six logical elements:
 - (a) x: a single letter corresponding to the working group:
where x =
 - T (Use cases and Technical Requirements)
 - A (System Architecture and Solution Development)
 - P (Evaluation, Testbed and Pilots)
 - S (Standards and Spectrum)
 - B (Business Models and Go-To-Market Strategies)
 - (b) nn: two digits to indicate the year. i.e. ,17,18 19, etc
 - (c) zzzz: unique number of the document
- (2) No provision is made for the use of revision numbers. Documents which are a revision of a previous version should indicate the document number of that previous version
- (3) The file name of documents shall be the document number. For example, document S-160357 will be contained in file S-160357.doc

1 Introduction and Scope

This Technical Report and guide originated from a coalition of Vehicle-to-Everything (V2X) deployment stakeholders, initially drawn from the 5G Automotive Association (5GAA) and Crash Avoidance Metrics Partners (CAMP). It quickly expanded to include valuable perspectives from the Utah Department of Transportation and other Infrastructure Owners and Operators (IOOs); the National Electrical Manufacturers Association (NEMA), OmniAir, ITS America, and University of Michigan researchers.

The goal of this guidance is to serve as a straightforward reference for “Day One” 5.9 GHz Channel 183 Long-Term Evolution (LTE)-V2X deployment considerations and requirements in the United States (US). It is primarily targeted at road IOOs, reflecting a consensus view initially driven by the automotive vehicle Original Equipment Manufacturers (OEMs), IOOs and their suppliers, traffic equipment manufacturers, and others eager to usher in the safety and efficiency benefits expected from Intelligent Transportation Systems (ITS). LTE-V2X is commonly used to describe Cellular V2X (C-V2X). C-V2X is an umbrella term which encapsulates all 3rd Generation Partnership Project (3GPP) V2X technologies, including both direct (PC5) and mobile network communications (Uu) interfaces. This document focuses on V2X solutions using C-V2X direct communications.

This Day One guidance intends to reduce the broad array of variables and potential message sets implicit with V2X into a tightly focused cohort of profiles. These commonly understood profiles will hasten deployment timelines and ensure that vehicles and other road users can effectively communicate in a language that installed infrastructure will understand and properly process. Specifically, this document is a filtered collection of findings from the various guidelines, standards, and heuristics learned in deployment projects. It is a comprehensive, yet simple-to-follow deployment guide indicating the finite set of Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) messages necessary to support the anticipated Day One Connected Vehicle (CV) applications. The applications may be mentioned but will not be covered in detail.

Therefore, to put the US on a V2X ready-to-deploy footing, this document will:

- ▶ Put an emphasis on clarifying expectations that all participants of safe traffic communications need for a swift V2X roadside unit deployment. This guidance includes pointers to existing and anticipated references and standardization efforts. It will present these crucial materials in a concise and accessible format.
- ▶ Identify a set of limited (but important) existing messages, interoperability needs, minimum performance requirements, as well as conformance and certification criteria that must be supported for expedited deployments agreed on by representatives of the diverse deploying stakeholder community on both the vehicle and infrastructure sides. While not a standard, it is a consensus agreement on which messages are included – and by virtue of omission – which are excluded to deliver an orderly and safety-critical set of messages.
- ▶ Provide the SAE J3161 communication profiles and parameters so that

vehicle OEMs and IOOs have a common set of channel access and rules for optimal use of the aforementioned set of messages for 20 MHz LTE-V2X radio defined by Channel 183.

The goal is to ensure V2X communications provide the required interoperability and data integrity to support the requisite performance of the various implementations utilizing the Day One messages. This document will also show what requirements and documents are complete and where work may still be required or gaps exist, such as in standards. Furthermore, this document will identify what may be coming next with a Day Two set of messages. This will convey a preview for the V2X community to prepare for the second stage of deployment.

2 End-to-End Deployment Process Guidance

This section provides guidance on the steps to follow regarding the deployment of one or more of the Day One message sets described in Section 3 and corresponding to the message categories defined in Section 3. The guidance applies to any agency (e.g., IOO) that intends to deploy a system to transmit one or more of the Day One message sets. It is expected that most agencies will support the message sets corresponding to the Mass Use Production Vehicle (MUPV) category in order to support automotive OEM private passenger vehicles, which are expected to make up most of the Day One deployment.

2.1 Deployment Tasks

For the purposes of this Technical Report, or guidebook, a set of ten functional tasks has been identified. Each of the tasks provides guidance on some of the things that may need to be considered or activities that may need to be performed, starting from application message set determination, and going through to the deployment of systems supporting these application message sets. General guidance is provided which could be expected to be mapped to agency specific processes. So, the task names should not matter as much as the items to be considered within each task. Also, for IOOs that may already support LTE-V2X deployments, all the tasks may not be required.

The ten tasks have been grouped into four different process categories. Figure 1 provides an illustration of the process categories and tasks within each. Section 2.2 provides descriptions of each of the tasks, and Section 2.3 provides a mapping for each task to the sections within this guidebook as well as to the steps identified in the Connected Intersection Guidance Document (see Table 6) that have aspects pertaining to the task. The following are the process categories and tasks within each category:

Application Message Set Identification and Planning

- Task 1: Identify Application Message Set(s)
- Task 2: Planning

Procurement, Evaluation, and Agency Testing

- Task 3: Application Development Procurement
- Task 4: Certified Device and Other Procurement
- Task 5: Agency Component Testing
- Task 6: Agency Integrated System Testing

Conformance Testing and Certificate Provisioning

- Task 7: Component Conformance Testing

Task 8: Integrated System Conformance Testing

Task 9: Certificate Provisioning Deployment

Deployment

Task 10:Deployment

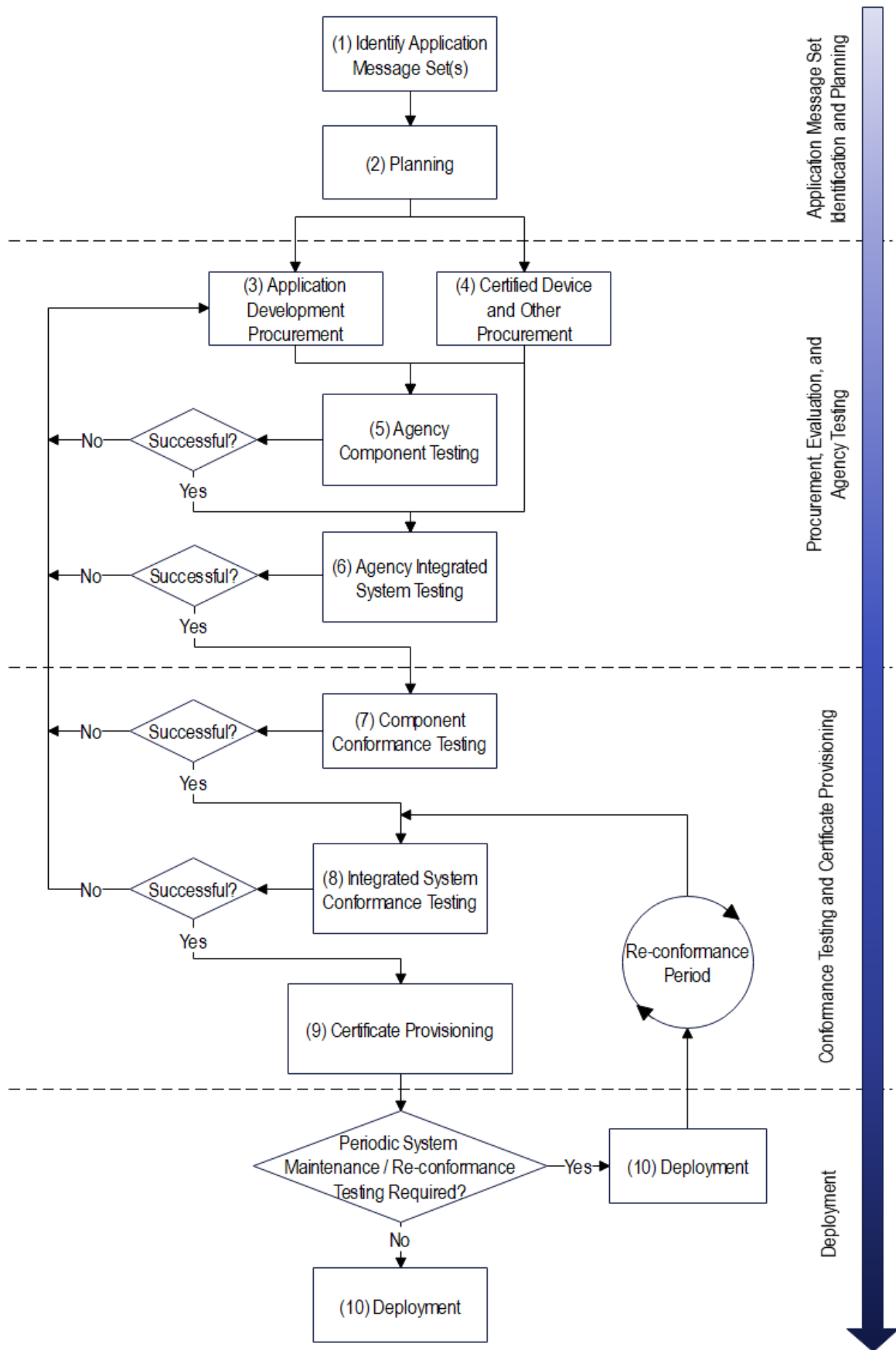


Figure 1: End-to-End Deployment Process Flow Illustration

2.2 Deployment Task Descriptions

The following subsections provide a brief description of what each of the tasks address.

2.2.1 Application Message Set Identification and Planning

Application message set identification and planning include the following two tasks:

Task 1 – Identify Application Message Set(s): As its name suggests, this involves identifying those message sets that are required for the intended set of applications to be supported. Section 3 has categorized the Day One messages into three distinct categories. It is expected that the message sets corresponding to one or more of those categories would be selected as part of this task.

Task 2 – Planning: This involves all the items that may need to be considered regarding support for the identified set of Day One messages. It includes items such as identifying equipment, installation, regulatory, security, etc. needs and requirements; determining what equipment and capabilities are already supported versus those that may need to be acquired; identifying suppliers, contractors, or other staff needed to support message development, acquiring the equipment and/or required capabilities; and assigning roles and responsibilities.

2.2.2 Procurement, Evaluation, and Agency Testing

Procurement, evaluation, and agency testing include the following four tasks:

Task 3 – Application Development Procurement: This involves any software or other application development that is required to support the generation of the Day One messages identified in Task 1. Depending on the message and how aspects of it are to be handled within the Connected Infrastructure (CI)¹, some aspects of the development may be handled internally while others may need to be externally procured. Any externally procured development would have been identified in Task 2. This task may take place in parallel with Task 4 - Certified Device and Other Procurement.

Task 4 – Certified Device and Other Procurement: This involves procuring the certified devices and other equipment, services, authorization, etc. that were identified in Task 2. The application development aspects of procurement are referenced in Task 3 – Application Development Procurement – which may take place in parallel with this task.

NOTE: It is anticipated that the device manufacturer and the agency (i.e., deployer of the device) will work together to get the device enrolled during procurement with a chosen Security Credential Management System (SCMS) provider.

Task 5 – Agency Component Testing: This involves testing the aspects of the Day One message generation and transmission that can be tested at a component level

¹ In other reports “CI” stands for Connected Intersection wherein this guidebook it is used to refer more generally to Connected Infrastructure which may or may not be an intersection.

(which includes the certified device) where the component(s) may not be fully integrated into the system. This will likely take place in a lab or on a bench and may be done by the IOO or the message developer, if one is procured, or potentially both.

Task 6 – Agency Integrated System Testing: This involves testing the aspects of the Day One message generation and transmission that can only be verified on the component(s)-installed integrated system (i.e., includes all the components of the system from start to finish that produce or influence the contents of the message). Ideally, this would take place at the location where the equipment is installed, however, depending on the messages it is possible that the equipment could be staged to support the testing. This testing will be done by the IOO possibly with support from their contractors and, if applicable, the other system component manufacturers (e.g., signal control manufacturer).

2.2.3 Conformance Testing and Certificate Provisioning

Conformance testing and certificate provisioning includes the following three tasks:

Task 7 – Component Conformance Testing: This has the same scope as Task 5 – Agency Component Testing – but will be performed by an organization recognized by the SCMS Manager for performing conformance testing of certified components/devices to validate a message implementation which, depending on the policies of the SCMS Manager for the message, could potentially include self-attestation.

NOTE: If a certified device was procured during Task 4, Component Conformance Testing may have already been performed. If that is the case this task may be bypassed and proceed directly to Task 8.

Task 8 – Integrated System Conformance Testing: This has the same scope as Task 6 – Agency Integrated System Testing – but will be performed by an organization recognized by the SCMS Manager for performing conformance testing for validating a fully configured and deployed system which, depending on the policies of the SCMS Manager for the message, could potentially include self-attestation.

Task 9 – Certificate Provisioning: This involves the system operator demonstrating to the SCMS provider that the steps required by the SCMS Manager for obtaining production message signing certificates, including demonstrated message conformance, have been completed. A transmitting device is then provisioned with production message-specific signing certificates authorizing it to send the message.

NOTE: Some messages will require a device to be re-enrolled with its SCMS provider for it to continue to obtain certificates and remain operational. If that is required, it would take place in this task. See the NOTE attached to Task 4 for the initial device enrollment.

2.2.4 Deployment

Task 10 – Deployment involves the system becoming field operational, transmitting the messages. If the message requires periodic re-conformance testing to ensure

that it is maintaining conformance to the requisite standards, the system owner should plan for this. The results of re-conformance testing will need to be communicated to the SCMS provider so that the device can continue to receive production message signing certificates.

NOTE: Periodic conformance testing may or may not be linked to the need for a device to be re-enrolled with its SCMS provider. See the NOTE attached to Task 9 for device re-enrollment.

2.3 Deployment Task Report References

For each of the deployment tasks, Table 1 provides references to the sections contained in this guidebook as well as the eight steps in the Connected Intersection Guidance Document (see Table 6). Many of the steps have corresponding templates to enhance the guidance and facilitate CI deployment.

NOTE: While the Connected Intersection Guidance Document primarily addresses connected intersections, which support the Signal Phase and Timing (SPaT), Map Data (MAP), and Radio Technical Commission for Maritime Services (RTCM) Corrections, many of the steps are applicable to the other infrastructure-related messages contained in this guidance document.

Table 1: End-to-End Deployment Process Report References

Deployment Tasks		References within this Guidebook		References to the Connected Intersection Guidance Document	
Task	Task Title	Section	Section Title/Table Reference	Step	Step Title
Application Message Set Identification and Planning					
1	Identify Application Message Set(s)	3	Day One Messages		
2	Planning	5.3	Physical Installation	1	Assemble Data and Information
		5.4	Environmental, Mechanical, and Power Considerations	2	Determine Capabilities and Options to Meet CI Requirements ⁽¹⁾
		5.6	RTCM Corrections Support	3	Determine Procurement Specifications
		5.7	Local Certificate Download Support		
Procurement, Evaluation, and Agency Testing					
3	Application Development Procurement	4.1	SDO Message Report References – Table 3: Payload Format Definition/Payload Content and Performance Requirements	4	Procure System Components (as it relates to message development)
		4.2	SAE J3161 SDO Report		
		4.3	IEEE 1609 SDO Report References		
		4.4	3GPP Release 14 Report References		
		4.5	Supporting Reports References (if applicable)		
4	Certified Device and Other Procurement			4	Procure System Components (non-development procurement)
5	Agency Component Testing	4.1	SDO Message Report References – Table 3: Component Test Procedures	5	Assemble and Test System Off-line (Bench Testing)
		6.3.2	Message Conformance Test Procedures – Table 9: Component (if no report is provided in Section 4.1)		
		4.2	SAE J3161 SDO Report (for the message-specific LTE-V2X settings to test)		
6	Agency Integrated System Testing	4.1	Day One SDO Message Reports – Table 3: Integrated System Test Procedures	6	Deployment and Field Validation
		6.3.2	Message Conformance Test Procedures – Table 9: Integrated System (if no report is provided in Section 4.1)		
		4.2	SAE J3161 SDO Report (for the field-deployed LTE-V2X settings, e.g., transmit power)		
		5.5	RF Configuration		
Conformance Testing and Certificate Provisioning					
7	Component Conformance Testing	6.3.2	Message Conformance Test Procedures – Table 9: Component		
8	Integrated System Conformance Testing	6.3.2	Message Conformance Test Procedures – Table 9: Integrated System / Maintenance (if periodic re-conformance required)	7	Vehicle Validation
				8	Operations and Monitoring (if periodic re-conformance required)
9	Certificate Provisioning → Refer to SCMS Manager policies and procedures				
Deployment					
10	Deployment: No report references				

(1) In the Connected Intersection Guidance Document “CI” stands for Connected Intersection wherein this guidebook it is used to refer more generally to Connected Infrastructure which may or may not be an intersection.

3 Day One Messages

This section provides information on the set of Day One messages. While various stakeholders have contributed to the content of this guidebook, there are several factors outside their control which will influence when Day One deployment will come about. In fact, for each of the messages and, depending on the application, there may be varying degrees of message use within the vehicle OEM and IOO communities, potentially leading to multiple Day One deployments. Given this, this guidebook does not indicate a date or time frame for when a Day One deployment will take place. Rather, it lays the groundwork for stakeholders to plan for and understand what can be expected on Day One when it comes to fruition. However, to provide some clarity to those referencing this guidebook, the Day One messages have been grouped by the category of vehicle expected to support the messages and for which there may be a different Day One deployment. It should be noted that the categories also indicate the level of Day One support an IOO can expect for a given message or message set.

The Day One message categories used within this guidebook are the following:

- ▶ Mass Use Production Vehicle (MUPV) – These messages are expected to be supported broadly across automotive OEM private passenger vehicles but may also be supported less broadly by other vehicle types. Given this, it is anticipated that a wide set of IOOs across the US will likewise provide support for these messages.
- ▶ Limited Use Fleet Vehicle (LUFV) – These messages are expected to be supported by vehicles within the purview or authority of individual IOO agencies, as opposed to mass-produced private passenger vehicles. The messages in this category necessarily include many of those involving MUPVs.
- ▶ Limited Use Mixed Vehicle (LUMV) – These messages are likely to happen under bound circumstances and be supported by potentially only a subset of the MUPVs and LUFVs.

NOTE: It is important to note that for a host of deploying agencies, Day One LUFV and LUMV message support might occur before Day One MUPV message support. Should these agencies also support the Day One MUPV messages, it is essential for the corresponding messages to be broadcast in accordance with this guidebook, to establish an interoperable V2I ecosystem warranting automotive OEM and customer investment in LTE-V2X deployments.

The Day One messages need to be developed according to the reports referenced in Sections 4.1, 4.3, and 4.4, and must follow the channel access and other configuration settings provided in Section 4.2. They also need to be tested for conformance according to Section 6.3.2. This is so that the messages, which pertain to different deployments, can support interoperability across stakeholders and coexist in the limited spectrum available for LTE-V2X to deliver the intended application fidelity. These criteria necessarily limit Day One deployment to a practical set of interoperable messages to effect safety and mobility applications that the stakeholder community can confidently deploy.

NOTE: While the main body of this guidebook addresses the Day One messages, Annex B provides a set of Day Two messages. These messages may not meet the criteria laid out above for the Day One messages, and the channel access and other configuration rules are not provided in Section 4.2 for those messages. If those messages and associated applications come to fore, a consensus Day Two guidebook may be developed.

3.1 Message Descriptions

The following provides the anticipated set of Day One messages, grouped by the categories from Section 3, along with a brief description of the message and the primary users involved in the message exchange, i.e., a CV or CI:

Message Category: Mass Use Production Vehicle (MUPV)

- ▶ Basic Safety Message (BSM) – Primarily intended for a CV to provide information about its basic vehicle state. This information can be used by applications within other CVs to assess the potential for crash threats and alert the driver if deemed necessary. It can also be used by CI to assess traffic flow and other information which may be useful for mobility, roadway safety, and other applications.

NOTE: Within the context of this guidebook, only United States Department of Transportation (USDOT) Federal Highway Administration (FHWA) vehicle classes 1 through 7, rigid body vehicles, are considered. See Annex D for a mapping of vehicle types to these classes. Non-rigid body FHWA vehicle classes 8 through 13 are listed in Annex B for Day Two support.

NOTE: These class restrictions apply only to the BSM and not to the other Day One messages in this guidebook.

- ▶ Signal Phase and Timing (SPaT) – Primarily intended for CI to provide information about the current, and potentially future, signal status and timing for each of the lanes approaching a signalized intersection. This can be used by CVs, for example, to alert the driver that they may be about to run a red light if actions are not taken to bring the vehicle to a stop.
- ▶ Map Data (MAP) – Enables CI to provide information about the individual lane geometry (e.g., width, curvature) and attributes that apply to the lane (e.g., speed, allowed maneuvers at lane connections). It is primarily intended to support signalized intersections but can also support non-signalized intersection road segments.
- ▶ Radio Technical Commission for Maritime Services (RTCM) Corrections – Enables CI to provide local Global Navigation Satellite Systems (GNSS) satellite corrections information for the Global Positioning System (GPS), which is operated by the US, and potentially other GNSS such as Galileo, operated by the European Union (EU), BeiDou Navigation Satellite system (BDS), operated by the People's Republic of China, and the *Globalnaya Navigatsionnaya Sputnikovaya Sistema* (Global Navigation Satellite System,

GLONASS) operated by the Russian Federation. A CV applies this information to its local measured GNSS position information to improve the accuracy of the measured position. This is needed for some applications, which require the CV to know the specific road lane where it is located, such as the Red-Light Violation Warning (RLVW) application.

- ▶ Traveler Information Message (TIM) – Enables CI to provide International Traveler Information Systems (ITIS) codes and text to CVs related to advisory, work zone, road sign, speed limit, school zones, midblock crossings, and roadside service information. CVs can use this information to help drivers be more aware of their environment and be more prepared for current and upcoming traffic and roadway situations.
- ▶ Road Safety Message (RSM) – This message is an evolution of the TIM. In addition to dynamic traveler information, it enables CI to provide information to CVs regarding curve- and work-zone speeds, lane closures and various incidents. As with TIM, CVs can use this information to help drivers be more aware of their environment and more prepared for current and upcoming traffic and roadway situations.

Message Category: Limited Use Fleet Vehicle (LUFV)

- ▶ Signal Request Message (SRM) – This enables emergency, transit, road maintenance, and potentially other CV types (depending on which ones local IOOs have decided to support), to request preferential treatment at a signalized intersection. The preferential treatment provided by CI can include priority treatment; where the CI may, for example, extend the time that a signal will remain green to enable the vehicle to traverse the intersection without needing to come to a stop, or preemption service; where the CI may, for example, terminate a green signal in favor of turning the conflicting lane signals green to enable a vehicle in the conflicting lane to traverse the intersection without coming to a stop.
- ▶ Signal Status Message (SSM) – This message is paired with the SRM. It enables CI to provide a CV the status of its request for preferential treatment. Other CVs may also use this information for greater situation awareness, that a priority or preemption is being granted at a particular intersection.

Message Category: Limited Use Mixed Vehicle (LUMV)

- ▶ Toll Advertisement Message (TAM)² – Used to provide the toll point data to the vehicle, including charges/fees. This message is sent from CI to the CV to provide information on the toll-zone geometry and toll charges. The information is referred to as the “toll-charging data”.
- ▶ Toll Usage Message (TUM) – Used to initiate a toll transaction by the vehicle. This message is sent from the CV to CI and contains the information necessary for the toll to be charged to the appropriate user, which enables payment of the fee.
- ▶ Toll Usage Message Acknowledgement (TUMack) – This message is sent from CI to the CV and confirms that the CI at a specific toll point has received and

² The TAM information is provided to the vehicle within the payload of a Wave Service Advertisement (WSA).

verified the signature of the TUM.

- ▶ WAVE Service Advertisement (WSA) – This message enables CI to advertise the services it supports to the CVs. A CV uses parameters contained within the WSA to participate in and/or access the service.

Figure 2 provides an illustration of each of the message categories and the messages or message sets that have been allocated to them per the above. Given the message categorization, green arrows show messages/message sets that are likely to be transmitted or received, blue arrows show those where at least one of the blue arrow messages/message sets are likely to be transmitted or received, yellow arrows show those which may be transmitted or received, and orange arrows show those where reception is conditional upon support for a different message/message set. However, it should be noted that within any category, messages or message sets shown under another category may be supported should the CI or CV choose to do so. This is shown explicitly with the BSM but could also be true for some of the other message types. For example, while WSAs are shown for LUMV, per the categorization above, to support local certificate download, MUPV or LUFV could also support this.

NOTE: Refer to Section 6 for aspects of the illustration related to the SCMS Manager, SCMS providers, and security credentials.

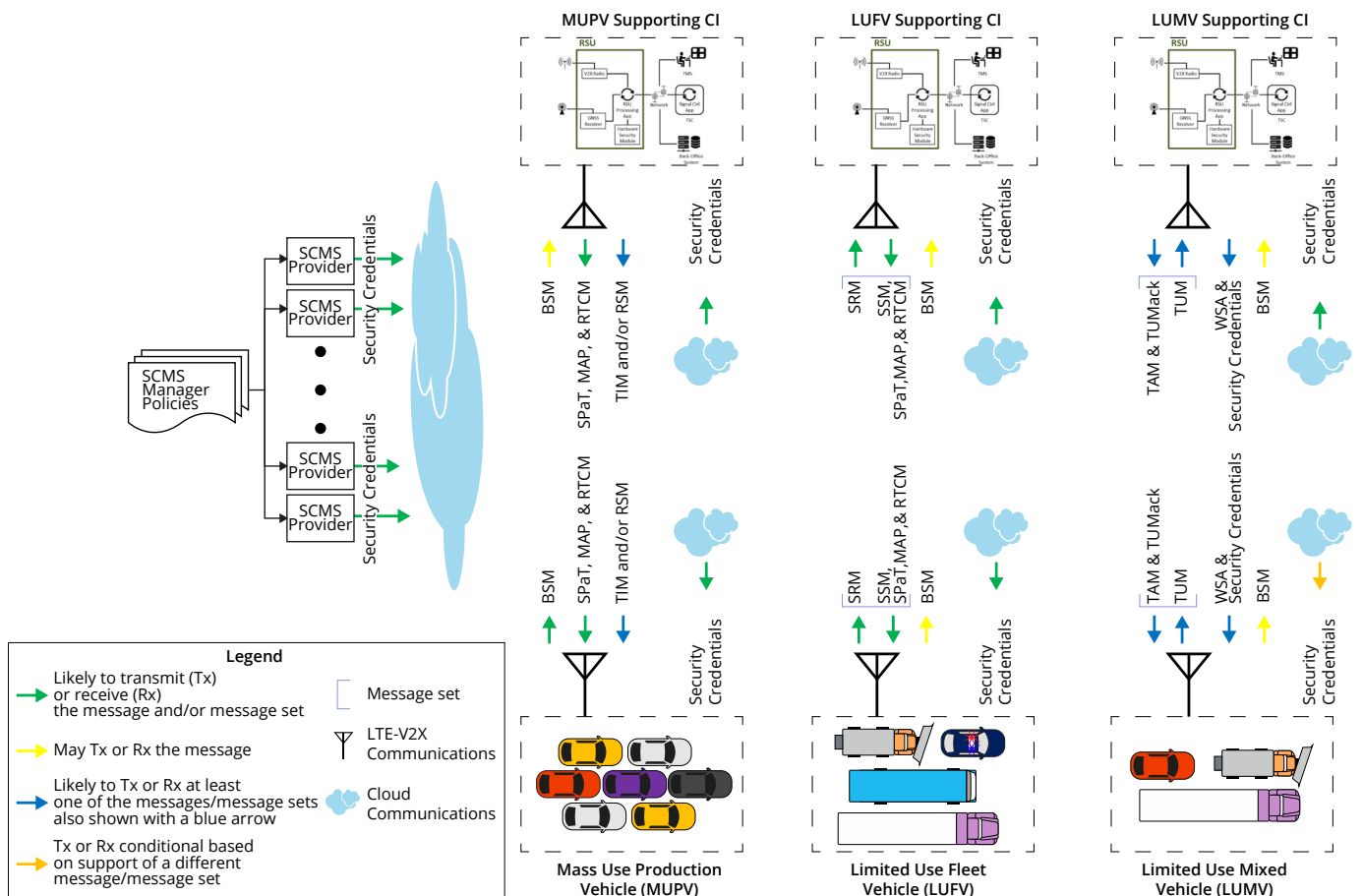


Figure 2: Message Category Illustration

3.2 Message Users

For each of the Day One messages, Table 2 provides information on the primary and potential secondary users of the messages. For sending the message only a primary sender is considered. For receiving the message both primary and secondary recipients are considered. The primary senders and recipients are the main target audience of this guidebook. The secondary recipients are users who may benefit by processing the message contents, beyond that for which the message is intended, and are expected to benefit from this guidebook as well. For example, while the BSM is intended to be exchanged between CVs to support V2V safety applications, CI (as secondary recipients) may benefit from processing the BSM to assess traffic flow and other information – which may be useful for mobility, roadway safety, and other applications.

Table 2: Day One Message Senders and Recipients List

Message	Primary Sender	Primary Recipient	Secondary Recipient
Message Category: Mass Use Production Vehicle (MUPV)			
BSM	CV ⁽¹⁾	CV	CI
SPaT	CI	CV	CI
MAP	CI	CV	
RTCM Corrections	CI	CV	
TIM	CI	CV	
RSM	CI	CV	
Message Category: Limited Use Fleet Vehicle (LUFV)			
SRM	CV: Non-private vehicles	CI	
SSM	CI	CV: Non-private vehicles	CV: Private passenger vehicles
Message Category: Limited Use Mixed Vehicle (LUMV)			
TAM	CI	CV	
TUM	CV	CI	
TUMack	CI	CV	
WSA	CI	CV	

⁽¹⁾ See the note within the message category BSM description in Section 3.1 for the intended Day One FHWA vehicle classes.

4 WAVE Protocol Stack

This section provides implementation guidance on the Wireless Access for Vehicular Environments (WAVE) protocol stack. It addresses the standards and reports that have been developed and which provide the message definitions, requirements, design, and other items necessary to deploy each of the Day One messages.

Figure 3 provides an illustration of the LTE-V2X protocol stack and which standards, or report areas, address the different layers of the protocol stack. The top layer is V2X Applications which is within the Day One message reports scope. The non-application layers are in the scope of either the SAE J3161, IEEE 1609, or 3GPP Release 14 standards.

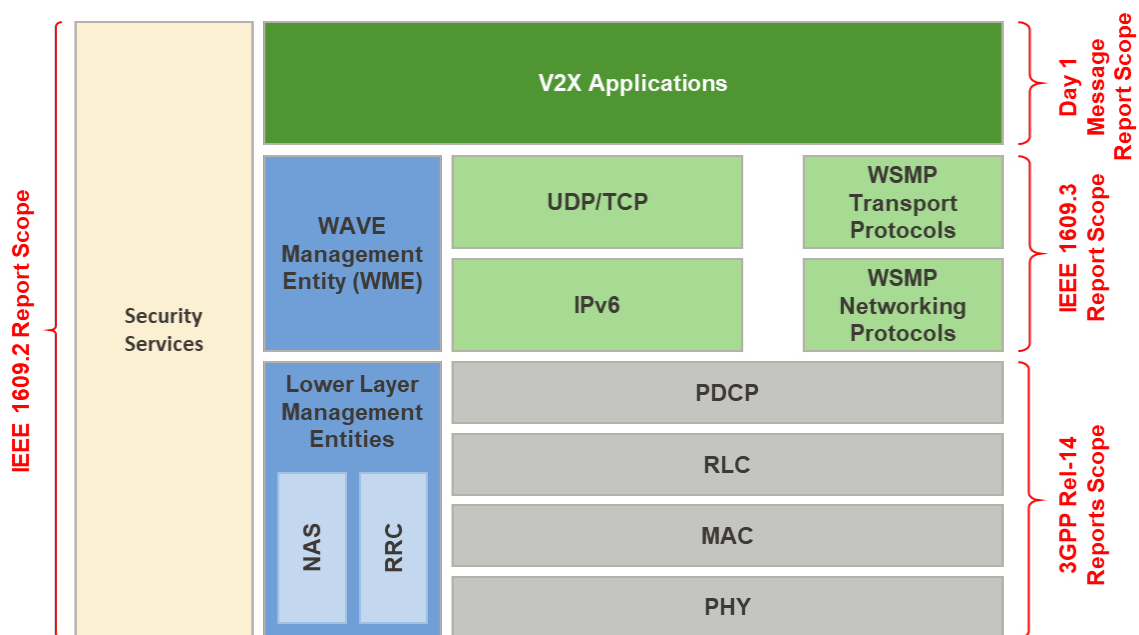


Figure 3: LTE-V2X Protocol Stack

4.1 SDO Message Report References

Deployment of the Day One messages requires that there be interoperability between the senders and receivers of messages. To ensure interoperability, the following is needed:

- 1) Payload Format Definition – The Abstract Syntax Notation One (ASN.1) or other message payload format file has been developed and written according to the appropriate programming language.
- 2) Payload Content and Performance Requirements – Address required/conditional/optional data-element inclusion and, data element accuracy,

transmission behaviors, and other aspects of payload or message performance.

- 3) Component Test Procedures – To be run on the component(s) which include the certified device (or may be just the certified device) and used to test that the message/payload meets the format and content requirements which are unrelated to the accuracy and/or performance requirements.
- 4) Integrated System Test Procedures – To be run on the component(s)-installed integrated system (i.e., includes all the components from start to finish that produce the content of the message including the certified device) to test that payload and message performance requirements (e.g., content correctness/accuracy, transmission intervals/power) are being met.

For each of the messages, Table 3 lists the Standards Development Organization (SDO) reports which provide the information listed above. These are the reports that should be referenced during the internal agency message development and test. If a cell is empty that means that there is no known report at the time of writing. For a message to be considered for Day One deployment, reports for the first two of the above are required. For the test procedures, SDO developed reports may or may not exist. If they do not, it is possible the test procedures may be addressed by component and/or integrated conformance test specifications (see Section 6.3.2). In that case, an implementation may want to reference those reports during the development and testing stages.

Table 3: Day One Message Development and Test SDO Reports List

Message	Message Reports			
	Payload Format Definition	Payload Content and Performance Requirements	Component Test Procedures	Integrated System Test Procedures
Message Category: Mass Use Production Vehicle (MUPV)				
BSM ⁽¹⁾	SAE J2735 & ASN	SAE J2945/1 ⁽²⁾	SAE J3161/1A	SAE J3161/1A
		SAE J3161/1 ⁽³⁾ SAE J2945/1B ⁽⁴⁾		
SPaT	SAE J2735 & ASN	CTI 4501 ⁽⁵⁾	CTI 4502	SAE J3238/1 ⁽⁶⁾
MAP	SAE J2735 & ASN	CTI 4501 ⁽⁵⁾	CTI 4502	SAE J3238/2 ⁽⁶⁾
RTCM Corrections	SAE J2735 & ASN	CTI 4501 ⁽⁵⁾ (Requirements) SAE J3258 ⁽⁶⁾ (Design)	CTI 4502	SAE J3238/2 ⁽⁶⁾
TIM	SAE J2735 & ASN			
RSM	SAE J2945/4 SAE J2735 ASN	SAE J2945/4		
Message Category: Limited Use Fleet Vehicle (LUFV)				
SRM	SAE J2735 & ASN ⁽⁵⁾	SAE J2945/B ⁽⁶⁾		
SSM	SAE J2735 & ASN ⁽⁵⁾	SAE J2945/B ⁽⁶⁾		
Message Category: Limited Use Mixed Vehicle (LUMV)				
TAM	SAE J3217 & ASN	SAE J3217		
TUM	SAE J3217 & ASN	SAE J3217		
TUMack	SAE J3217 & ASN	SAE J3217		
WSA	IEEE 1609.3			

⁽¹⁾ See the note within the message category BSM description in Section 3.1 for the intended FHWA vehicle classes.

⁽²⁾ Report supports FHWA class 2 and 3 light passenger vehicles.

⁽³⁾ In addition to class 2 and 3 light passenger vehicles, report adds support for FHWA class 2, 3, or 5 public safety vehicles.

⁽⁴⁾ Report adds support for FHWA class 1 and 4 through 13 vehicles, but this guidance report only addresses a subset of these vehicles classes, as stated in the note within the message category BSM description Section 3.1.

⁽⁵⁾ The SAE Connected Transportation Interoperability Committee (CTIC) (see Section 7.1) is in the process of defining the updates to this report.

⁽⁶⁾ The SAE Connected Transportation Interoperability Committee (CTIC) (see Section 7.1) is in the process of developing this report.

For each of the reports listed in Table 3, Table 4 provides details of the reports, listed in alphabetical order, including the title, publisher, base revision to reference, type of report (e.g., standard), and the availability status.

NOTE: Table 4 has the base version of the reports that need to be supported. Newer versions of a report may be used if they are backward compatible with the version provided in Table 4.

Table 4: Day One Message SDO Reports Details

Report	Title	Publisher	Current Revision	Type	Availability Status
CTI 4501	Connected Intersections Implementation Guide – Guidance to Setting Up and Operating a Connected Intersection (CI)	AASHTO, ITE, NEMA, SAE International	New Revision Under Development (Previous Revision: CTI 4501 v01.01)	Recommended Practice	New Revision Not Available: Under Development
CTI 4502	Connected Intersections Validation Report - Findings from the Connected Intersections (CI) Project Validation Phase	Connected Intersections (CI) Committee	V01.00	Report	Available: Published
SAE J2735	V2X Communications Message Set Dictionary	SAE International	J2735_202309	Standard	Available: Published
SAE J2735 ASN	V2X Communications Message Set Dictionary™ ASN file	SAE International	J2735ASN_202309	ASN.1 definitions files	Available: Published
SAE J2945/1	On-Board System Requirements for V2V Safety Communications	SAE International	J2945/1_202004	Standard	Available: Published
SAE J3161/1A	Vehicle Level Validation Test Procedures for V2V Safety Communications	SAE International	J3161/1A_202204	Recommended Practice	Available: Published
SAE J2945/1B	On-Board System Requirements for V2V Safety Communications by Non-Light-Duty Vehicles and Motorcycles	SAE International	J2945/1B_202212	Standard	Available: Published
SAE J2945/4	Road Safety Applications	SAE International	J2945/4_202305	Standard	Available: Published
SAE J2945/B	Minimum Requirements to Support Traffic Signal Priority and Preemption	SAE International	Under Development	Recommended Practice	Not Available: Under Development
SAE J3161/1	On-Board System Requirements for LTE-V2X V2V Safety Communications	SAE International	J3161/1_202203	Standard	Available: Published
SAE J3217	V2X-Based Fee Collection	SAE International	J3217_202206	Standard	Available: Published
SAE J3238/1	Testing & Validation of SPaT information broadcast from Connected Intersections to support in-vehicle Red Light Violation Warning	SAE International	Under Development	Recommended Practice	Not Available: Under Development
SAE J3238/2	Testing & Assessment of MAP using RTCM information broadcast from Connected Intersections to support in-vehicle Red Light Violation Warning	SAE International	Under Development	Recommended Practice	Not Available: Under Development
SAE J3252	V2X Infrastructure Support for GNSS Corrections	SAE International	Under Development	Standard	Not Available: Under Development

4.2 SAE J3161 SDO Report

SAE J3161 provides the common design elements, PC5 sidelink profiles, communication parameters and other related items for LTE-V2X communications, as specified in 3GPP Release 14. Table 5 provides some of the message specific LTE-V2X settings. For some settings, the value to be used is provided while for others the report in which the value of these settings can be found is provided. The settings include the following:

- ▶ Provider Service Identifier (PSID): Indicates the application service that is being provided. Both the decimal and p-encoded PSID values are provided along with the report which was referenced for these values.
- ▶ Destination Layer-2 ID: Provides the ability to filter messages of interest which have this ID. The value is provided along with the report, which was referenced for the value, if one exists.
- ▶ Channel Identifier: The LTE-V2X channel the message is transmitted on. While all messages are to be sent on Channel 183, the Channel Identifier is included to reinforce this.
- ▶ Traffic Family: SAE J3161 defines seven traffic families used to textually indicate the message priority settings. The one that applies to each message is provided.

NOTE: Message priority settings are selected considering the overall performance of the system and do not necessarily indicate the priority of the message. For example, in Table 5, the MAP is assigned a higher priority than the SPaT and some BSMs, not because it is more important than those messages, but more so given that it is transmitted less frequently. So, when it is transmitted, the likelihood that it will be successfully received is improved.

- ▶ ProSe Per-Packet Priority (PPPP) Settings: A priority value assigned to a message, where lower values have higher priority. Some of the message reports contain a setting for the PPPP value. In many cases what is provided is a minimum PPPP setting, as indicated in SAE J3161. Rather than using the PPPP settings provided in the message reports or those from J3161, which are minimum values, the ones in Table 5 are to be used. This value is generally selected to be consistent with the Traffic Family priority.
- ▶ Packet Delay Budget (PDB) Settings: The maximum delay that a packet can tolerate before transmission, which is generally associated with the PPPP setting. SAE J3161 provides minimum PDB values, so the ones in Table 5 below are to be used. This value is generally selected to be consistent with the Traffic Family priority.
- ▶ Channel Occupancy Ratio (CR) Limit: Helps to control how much of the channel is being used by a message, primarily during congested channel situations. For this item, a reference to the report which defines the value is provided.
- ▶ Transmit Power Level: The maximum transmit power for the message. For this item, a reference to the report which defines the value is provided.

Annex A provides simulation results that validate the assigned system parameters.

Table 5: LTE-V2X Configuration Parameters for Day One Messages

Message	PSID Value: Decimal / P-encoding & (Reference)	Destination Layer-2 ID & (Reference)	Channel Identifier	Traffic Family	PPPP	PDB (ms)	CR Limit	Transmit Power Level
Message Category: Mass Use Production Vehicle (MUPV)								
BSM	32 / 0p20 (SAE J3161/1)	0xFFFFF (SAE J3161/1)	183	Critical V2V ⁽¹⁾ Essential V2V ⁽²⁾	2 ⁽¹⁾ 5 ⁽²⁾	50 100	SAE J3161/1	SAE J3161/1
SPaT	130 / 0p80-02 (CTI 4501)	0x010013 (SAE J3161) ⁽³⁾	183	Essential I2V	5	100	SAE J3161	SAE J3161
MAP	2113687 / 0pE0-00-17 (CTI 4501)	0x010012 (SAE J3161) ⁽³⁾	183	Critical I2V	3	100	SAE J3161	SAE J3161
RTCM Corrections	129 / 0p80-01 (CTI 4501)	0x01001C (SAE J3161) ⁽³⁾	183	Essential I2V	5	100	SAE J3161	SAE J3161
TIM	131 / 0p80-03 (SAE J3268 – see Traveler information and roadside signage)	0x01001F (SAE J3161) ⁽³⁾	183	Critical I2V	3	100	SAE J3161	SAE J3161
RSM	131 / 0p80-03 (SAE J2945/4)	0x010021 (SAE J3161) ⁽³⁾	183	Critical I2V	3	100	SAE J3161	SAE J3161
Message Category: Limited Use Fleet Vehicle (LUFV)								
SRM	2113686 / 0pE0-00-16 (SAE J3268 – see Traffic signal prioritization request)	0x01001D (SAE J3161) ⁽³⁾	183	Critical V2I ⁽⁵⁾ Transactional V2I ⁽⁶⁾	3 ⁽⁵⁾ 6 ⁽⁶⁾	100 100	SAE J3161	SAE J3161
SSM	2113685 / 0pE0-00-15 (SAE J3268 – see Traffic signal prioritization status)	0x01001E (SAE J3161) ⁽³⁾	183	Critical I2V ⁽⁵⁾ Transactional I2V ⁽⁶⁾	3 ⁽⁵⁾ 6 ⁽⁶⁾	100 100	SAE J3161	SAE J3161
Message Category: Limited Use Mixed Vehicle (LUMV)								
TAM	143 / 0p80-0F (SAE J3217)	0x000087 (SAE J3217) ⁽⁴⁾	183	Transactional I2V	6	100	SAE J3161	SAE J3161
TUM	143 / 0p80-0F (SAE J3217)	0x020087 (SAE J3217)	183	Transactional I2V	6	100	SAE J3161	SAE J3161
TUMack	143 / 0p80-0F (SAE J3217)	0x030087 (SAE J3217)	183	Transactional I2V	6	100	SAE J3161	SAE J3161
WSA	135 / 0p80-07 (IEEE 1609.3)	0x000087 (SAE J3161)	183	⁽⁷⁾	⁽⁷⁾	⁽⁷⁾	SAE J3161	SAE J3161

⁽¹⁾ For event-based BSMs with the critical event flag set or for public safety vehicle BSMs when engaged in an emergency response.

⁽²⁾ All other BSMs.

⁽³⁾ This value is based on the formula provided in SAE J3161 and should be used unless otherwise specified in the application standard.

⁽⁴⁾ The TAM is sent as part of a WSA advertising the tolling service and thus takes on the value of the WSA.

⁽⁵⁾ Preemption request/response.

⁽⁶⁾ Priority request/response.

⁽⁷⁾ This is application specific and should take the value of the highest priority service being advertised.

4.3 IEEE 1609 SDO Report References

Except for the BSM, many of the Day One message standards or reports attempt to be communications protocol neutral and thus only refer to the IEEE 1609 standards. Depending on when the Day One message reports were published, the versions of the IEEE 1609 standards referenced by the message reports may be out of date as newer revisions of the IEEE standards became available. However, given that there is only one protocol stack, all Day One messages will need to utilize the same, base versions of the IEEE standards to support interoperability. Since SAE J3161 establishes the common design elements for the LTE-V2X channel, the base versions of the IEEE standards are often maintained therein. The following are the primary IEEE standards referenced in the message reports that are relevant to Day One deployment. The base version that needs to be supported is indicated in SAE J3161 unless otherwise indicated.

- ▶ IEEE 1609.2 – IEEE Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages
Base Reference Version: IEEE Std 1609.2-2022
- ▶ IEEE 1609.3 – IEEE Standard for Wireless Access in Vehicular Environments (WAVE) – Networking Services
Base Reference Version: Refer to SAE J3161

4.3.1 IEEE 1609.3 WAVE Service Announcement Profile

The IEEE1609.3 WSA shall only be transmitted when there is at least one application service to advertise. Given that there is no report which provides the required WSA settings, those settings are included here. When such a report becomes available this section may be revised.

- ▶ WSAs should always include the following IEEE 1609.3 options:
 - 3D Location, WAVE Element ID #6 populated with the antenna location of the WSA transmitter
 - Compact Time Confidence, WAVE Element ID #25
 - IEEE1609.2 signature
 - WSA Count Threshold and WSA Count Threshold Interval
 - May include the LTEv2xChannelInfo extended channel info element, but only with pMax, minPeriodicity, maxSpeed, MaxRange, maxCbr (no other optional data LTEv2xChannelInfo elements should be included)

NOTE: LTE-V2X WSAs may never include RCPI Threshold which is not included per IEEE1609.3 Table M.3.

- ▶ The WSA security profile will be per an IEEE 1609.3 corrigendum (1609.3-2020_Corr1) to update the security profile in Annex H of IEEE 1609.3 to be consistent with the new format provided in the version of IEEE 1609.2 referenced in Section 4.3.

NOTE: At the time of release of this guidebook, this corrigendum was under development and a public reference was not available.

- ▶ WSAs will be sent no more frequently than 1 Hz.
- ▶ Each WSA will have a full certificate attached (i.e., certificate digests will not be used with WSAs).
- ▶ A Roadside Unit (RSU) transmitting a WSA, which is expecting to support any unicast or Internet Protocol (IP) applications, should disable the T5000 timer (3GPP L2 SRC randomization) or set it to the largest supported value.
- ▶ See Table 5 for the PSID and Destination Layer-2 ID for the WSA. The Service ID “handle” in the 3gPP 24.385 v2x.xml shall be set at the decimal value of 134, linked to the L2 DST specified.

4.4 3GPP Release 14 Report References

All the messages in this guidebook use a PC5-based sidelink low-latency direct communications interface defined by the 3GPP Release 14 specifications, as provided in SAE J3161 and referenced herein.

4.5 Supporting Report References

Table 6 provides reports with additional information on some of the messages and may have been referenced during the development of the message reports provided in Table 3.

Table 6: Day One Message Supporting Reports Details

Message	Report/Title	Publisher	Current Revision	Type	Availability Status
MAP	Guidance Document for MAP Preparation	The Connected Vehicle Pooled Fund Study – University of Virginia Center for Transportation Studies	Revision #2, May 2023	Guidance Document	Available: Public
MAP, SPaT, RTCM Corrections	Connected Intersections Program: Program Management and Technical Support – Connected Intersection Guidance Document	The Connected Vehicle Pooled Fund Study – University of Virginia Center for Transportation Studies	December 2022	Guidance Document	Available: Public
	Connected Intersection Performance Assessment – Supporting Basic Red Light Violation Warning ⁽¹⁾	CAMP LLC, Vehicle-to-Infrastructure (V2I-5) Consortium	December 7, 2022	Report	Available: Public

⁽¹⁾ This report will be superseded by SAE J3238/1 and SAE J3238/2 when they are published.

5 Hardware

This section covers the basic hardware architecture, related requirements, and installation for a CI that supports the Day One message requirements. Although the hardware requirements have been made to be as generic as practical, all communication aspects assume that the installation supports PC5-based LTE-V2X communications, as specified in SAE J3161 (see Section 4.2). The architecture and layout provided here is targeted for installation at a typical signalized intersection. It can also be adapted with minimal changes for a CI installation on the roadside, along highways, and at unsignalized intersections.

5.1 Report References

The hardware requirements, including environmental and mechanical considerations, should conform to relevant Institute of Transportation Engineers (ITE), American Association of State Highway and Transportation Officials (AASHTO), and the National Electrical Manufacturers Association (NEMA) guidelines for Connected Transportation Interoperability (CTI) for RSUs, as specified in Table 7, unless otherwise stated in this guidebook. Table 7 lists various documents which provide requirements and guidelines for CI deployment from the organizations above as well as others.

Table 7: Day One Hardware Supporting Reports Details

Standard Designation and Title	URL	Scope Summary	Status
Connected Intersections Program: Program Management and Technical Support – Connected Intersection Guidance Document	https://engineering.virginia.edu/sites/default/files/common/Centers/CTS/CVPFS/projects/ConnectedIntersections/CI%20Guidance%20Document%20Version%202.0%20Final%20.pdf	Guidance, organized into eight steps, intended to facilitate the connected intersection deployment process by following an approach that should be familiar to practitioners who have experience deploying traditional signalized intersections.	Publicly Available: Guidance Document
CTI 4001 v01.01 – Amendment 1 Roadside Unit (RSU) Standard	https://www.ite.org/ITEORG/assets/File/Standards/CTI%204001v0101-amended.pdf	CTI 4001 establishes a non-proprietary, communications-agnostic, industry consensus RSU standard.	Publicly Available: Standard
CTI 4501	Refer to Section 4.1, Table 4 for report details.		
NEMA TS 2-2021 Traffic Controller Assemblies with NTCIP requirements	https://www.nema.org/standards/view/traffic-controller-assemblies-with-ntcip-requirements-version-03-07	NEMA TS 2 covers traffic signaling equipment used to facilitate and expedite the safe movement of pedestrians and vehicular traffic. This incorporates the “Flashing Yellow” feature as well as associated configuration, pin assignment, and other related information	Revision commencing later this year
NEMA TS 8-2018 Cyber and Physical Security for Intelligent Transportation Systems	https://www.nema.org/standards/view/Cyber-and-Physical-Security-for-Intelligent-Transportation-Systems-ITS	NEMA TS 8 defines functional cybersecurity attributes along with minimum performance baselines that owners and operators of critical infrastructure can use for procurement purposes. It addresses the following areas: physical security, local access security, communications security (between field and central system), and central systems security	Revision underway: Expected completion later in 2023
NEMA TS 10-2020 Connected Vehicle Infrastructure- Roadside Equipment	https://www.nema.org/standards/view/connected-vehicle-infrastructure-roadside-equipment	NEMA TS 10 is a Standard for the equipment deployed at roadside to support standardized over-the-air wireless messages, applications, and cybersecurity measures of communications with Connected Vehicles. This Standard describes physical and performance interfaces as well as functionality requirements.	Revision underway: Expected completion later in 2023
NTCIP 1202 v03B Object Definitions for Actuated Signal Controllers (ASC) Interface	Under Development	NTCIP 1202 identifies and defines how a management station (e.g., traffic management system, local maintenance laptop) interfaces with a field device to control and monitor traffic signal controllers and associated detectors in an NTCIP-conformant fashion.	Not Available: Under Development
NTCIP 1218 v01.38 National Transportation Communications for ITS Protocol – Object Definitions for Roadside Units	https://www.ntcip.org/file/2021/01/NTCIP-1218v0138-RSU-toUSDOT-20200905.pdf	NTCIP 1218 identifies and specifies how a management station (e.g., traffic management system, local maintenance laptop) interfaces with an RSU.	Publicly Available: Standard

NOTE: While this section focuses on the RSU and other CI hardware, the CV On-board Unit (OBU) and other hardware capabilities need to be compatible with that of the CI and as specified in the message reports provided in this guidebook.

5.2 System Architecture

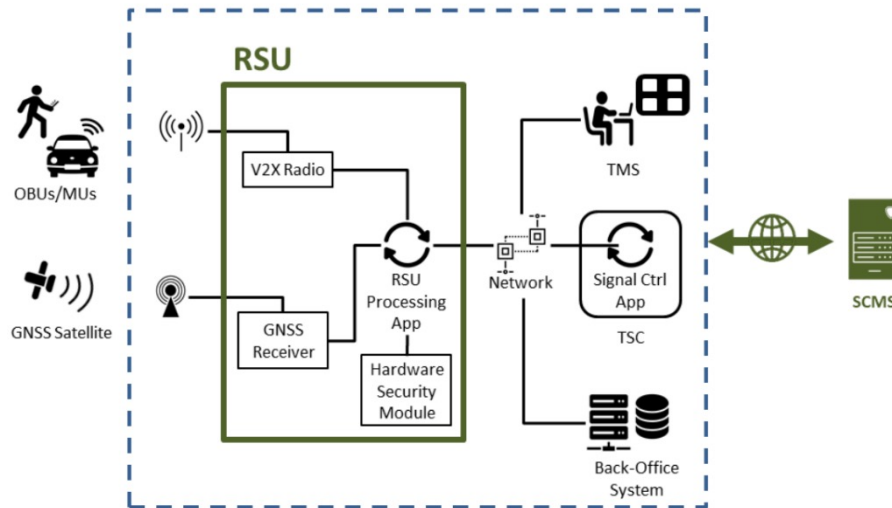


Figure 4: Logical Architecture and the Traffic Management System³

Figure 4 shows where the RSU fits within the overall logical system architecture which was originally outlined in the USDOT RSU Specification Document 4.1. That document was superseded by the CTI 4001 v01.01 – Amendment 1 (see Table 7) guidance document (herein referred to as just CTI 4001) which updated the system architecture and requirements. The RSU is expected to meet the requirements of CTI 4001.

The overall system architecture is designed to facilitate communication between the various traffic management system components, i.e., the Traffic Signal Controller (TSC), Traffic Management System (TMS), and the traffic network (“Backend”) as well as the CV OBU and potentially other mobile units (MUs) within the reception range of the RSU. Details of these components can be found in CTI 4001.

Figure 4 also shows MUs to indicate that there may be additional Day Two RSU and CI hardware support items; however, within the remainder of this section just CVs will be referred to. See Section 5.8 for a discussion on potential Day Two hardware capabilities.

5.3 Physical Installation

There are two basic RSU architectures provided in CTI 4001, referred to in this guidebook as integrated and distributed architectures. The following provides a description and illustration of these architectures.

- ▶ Integrated Architecture: The integrated RSU architecture includes all the

³ This figure is the same as Figure 5 from the CTI CTI4001v01.01 guidance document. Used by permission. Original text © AASHTO / ITE / NEMA / SAE.

functionality in a single enclosure. The antennas are connected to the RSU enclosure, as shown in Figure 5 for a signalized CI. A similar RSU architecture can be deployed for a non-signalized CI.

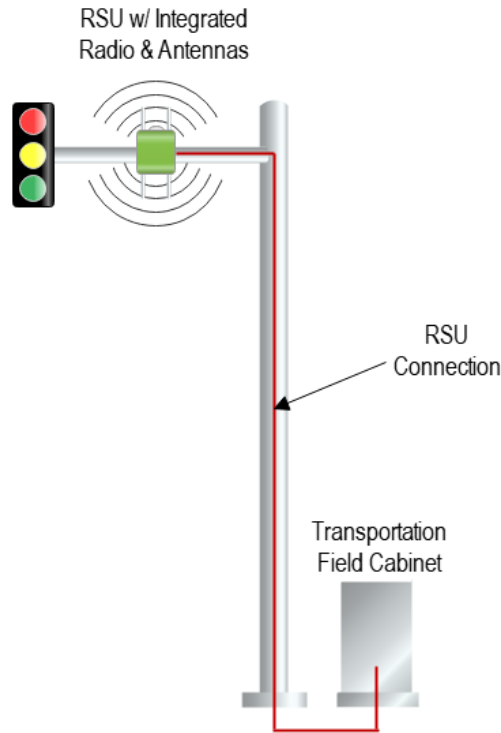


Figure 5: Integrated RSU Architecture

- ▶ Distributed Architecture: For the distributed RSU architecture there are at least two possible sub-architectures, one in which the antennas are mounted remote to the RSU as shown in the left illustration of Figure 6 and the other in which there are two separate units comprising the RSU functionality as shown in the right illustration of Figure 6. Both Figure 6 illustrations show a signalized CI, however, a similar RSU architecture can be deployed for a non-signalized CI.
 - Remote Antennas (left illustration of Figure 6): Remote mounting of the antennas can provide several benefits including increased antenna isolation, improved communication reliability, and a reduction in possible near frequency interference for multi-frequency installations that include multi-channel LTE-V2X and high-band Wi-Fi (e.g., Wi-Fi 6, 5.8 GHz 802.11AC, etc.). When remote mounting the antennas, the cable losses need to be considered to ensure the overall RF performance of the system is maintained.
 - Multiple Units (right illustration of Figure 6): One unit includes the radio with a digital output and antennas installed on the unit. The other unit includes the computing element, radio power supply (usually Power

over Ethernet [PoE]), as well as network interfaces. This second unit resides in the transportation field cabinet where it is co-located with other devices such as a traffic signal control unit, power source, back-haul data connections, etc. This approach can reduce the environmental requirements, make the network interface more flexible, and offer an easier upgrade path for the computing element, which is the most frequently upgraded part of these systems.

In the end there may be a balancing act between how it makes sense or is desirable to deploy the RSU and its components and maintaining the required performance of the system, which affects the selected architecture.

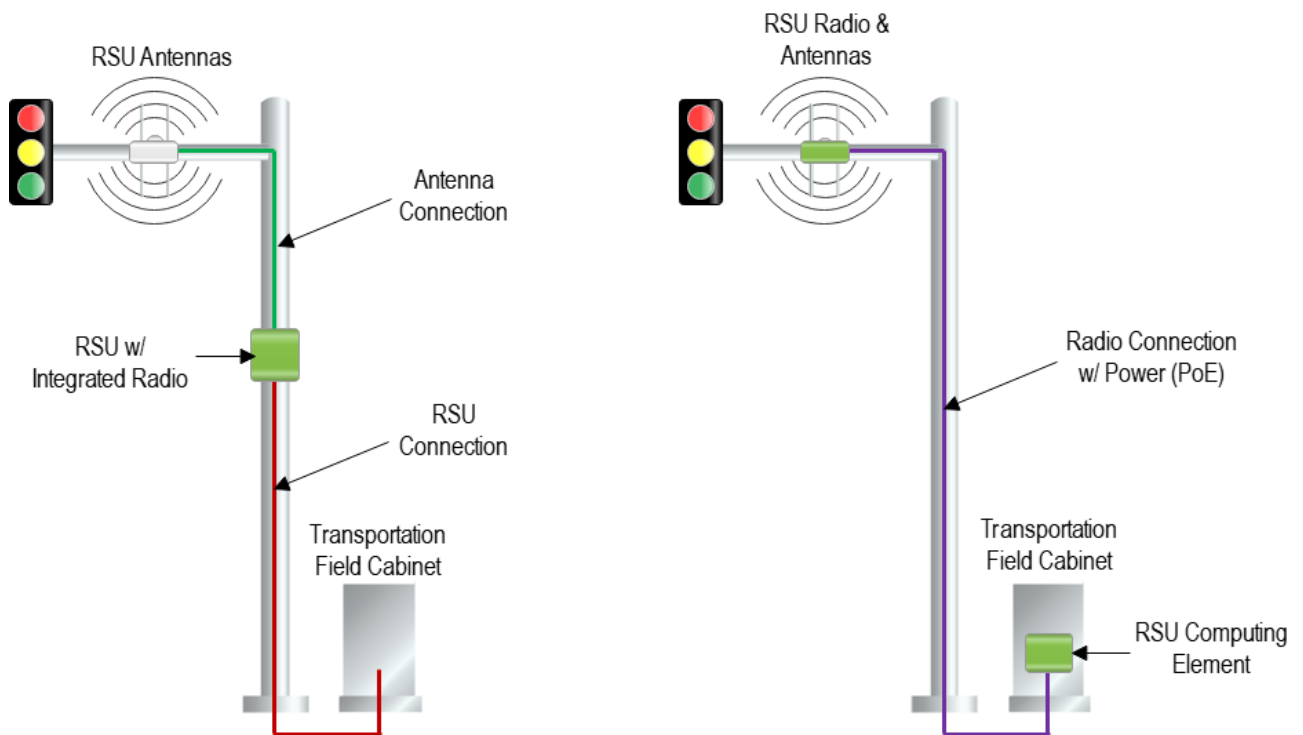


Figure 6: Distributed RSU Architectures

5.4 Environmental, Mechanical, and Power Considerations

Since some aspect of the RSU (either the whole RSU or components of it, depending on the architecture) will be installed on an outdoor pole or signal mast arm, meeting environmental requirements as well as mechanical and power requirements is critical. These requirements for the RSU were originally defined in the USDOT RSU Specification Document 4.1. With the advent of LTE-V2X, the requirements were updated as part of the CTI 4001 specification and thus supersede the specifications in the USDOT RSU Specification Document 4.1. Section 3.3.1 in CTI 4001 contains the requirements and

includes items such as the following:

Environmental requirements:

- ▶ Operational and storage temperature range for the device
- ▶ Vibration and shock for operation and transportation of the system
- ▶ Weather resistance including water (“ingress protection” or IP rating), humidity, salt, fog

Mechanical requirements:

- ▶ Size
- ▶ Weight
- ▶ Installation options

Power requirements:

- ▶ PoE Voltage and power requirements

NOTE: Some of the CTI 4001 requirements reference the NEMA TS2 and TS10 standards. For convenience, the details of those standards have been added to Table 7.

5.5 RF Configuration

It is important to remember that short-range Radio Frequency (RF) communication is at the heart of the system. In the end, all the information is channeled through the RF link to the intended users. Depending on the supported applications the required range or distance of communications may vary and must be considered. This makes it very important to consider the RF setup of the system with respect to the antenna type, its position in the intersection or along the highway, connection to the antenna (especially in the case of remote antennas – see Section 5.3), position of the system within the intersection or along the highway, as well as its proximity to other buildings and structures.

The system operating frequency is in the 5.9 GHz band, which, at this high frequency, has limited performance around corners and through obstructions such as buildings. This essentially limits the transmission path to the Line-of-Site (LoS) which can vary with terrain. Therefore, reliable performance requires that a direct and minimally obstructed path between the transmitter and the receiver is maintained. It is important to carefully review the position of the RSU (especially its antennas) at the intersection or along the highway. This is why at intersections many RSUs (or their antennas if a distributed architecture is employed – see Section 5.3) are installed on the traffic signal mast arm near the middle of the intersection. This kind of placement provides LoS access to CVs coming from any direction in a typical intersection. CVs can communicate with the RSU even without a direct path, but the range may be greatly reduced.

At the time of writing the Federal Communications Commission (FCC) has granted two tranches of waivers to applications conforming to the technical parameters cited in Paragraph 23 of the Waiver to Deploy (See: <https://docs.fcc.gov/public/attachments/DA-23-343A1.pdf>). The precondition of the RF configuration in a deployment is for the

IOO and OEM to apply for and conform to those technical parameters.

The SAE J3161 specification for the RSU calls for a signal strength of 23 dBm on the antenna connector and 33 dBm maximum Effective Radiated Power (ERP) over the air. This gives the operator the flexibility to use a high-gain antenna (typically 9-12 dBi gain) to achieve the requisite communications performance while staying within the technical parameters of the FCC waiver. Another possibility is to use a directional antenna if the expected target for the communication is concentrated in a known direction or area (i.e., along a highway). In the case of a remote antenna, the cable losses must be taken into consideration to calculate the radiated RF power. Output power from the RSU can be adjusted to ensure maximum power is radiated while adhering to the specified connected and radiated power limits mentioned earlier.

5.6 RTCM Corrections Support

The RSU must broadcast RTCM Correction messages as specified in CTI 4501 (see Table 6). To support this, the RSU may choose to obtain the corrections information from a remote reference station, reference information provider, or generate the corrections locally; in which case there may be additional specific hardware considerations.

5.7 Local Certificate Download Support

For IOOs that want to provide a service to support a CV topping off (i.e., requesting and downloading) security certificates from the local infrastructure, support needs to be provided for an Internet Protocol version 6 (IPv6) global addressing connection, either directly or via an IPv4 tunnel and Domain Name System (DNS) access.

NOTE: To facilitate this, the CI needs to support the broadcast of the WSA which in turn provides support for certificate management. See Table 3 for the WSA reports and Section 4.3.1 for the WSA settings to use.

NOTE: Given that it is not a Day One requirement for CI to provide a local certificate download service, CVs may need to consider other non-LTE-V2X mechanisms for topping off their certificates.

5.8 Hardware Capabilities for Future Use-Cases

During the Day One infrastructure setup and build, IOOs may want to consider the future V2X needs of the CI. Doing so could enable the addition of capabilities to the CI to support additional use-cases without significant infrastructure or re-installation costs. Towards this end, based on the current vision of Day Two and beyond use-cases, Annex C provides some of the potential future hardware capabilities that may want to be considered.

6 Security

6.1 Background

A security system is needed to establish a level of trust between senders and receivers, such that messages are authentic and can be trusted. A security system is also needed to provide mechanisms to identify and remove misbehaving devices sending messages with unreliable content despite having valid credentials.

The V2X security system achieves these objectives by using a Public Key Infrastructure (PKI) system. Certified devices are issued certificates that are cryptographically signed by the private key of a Certificate Authority (CA) within the SCMS. There can be multiple CAs within the SCMS. The SCMS consists of all CAs as well as policy and operational functions that ensure consistent and correct operations across all CAs within the SCMS. SCMS service providers adhere to a Certificate Policy (CP) and are audited by third-party entities to verify compliance with specifications, policies, and procedures to ensure interoperability and mutual trust.

The certificates obtained from a CA contain unique public keys corresponding to private keys known only to the device. Private keys are required to be stored by certified devices in a Hardware Security Module (HSM) or virtual HSM (vHSM) to preserve the security of the system. A sender selects a signing certificate containing the public key, cryptographically signs the message with the certificate's private key, and attaches the certificate (or an identifier of the certificate) to the message.

All receiving devices have the public key of the issuing CA (or have a means to obtain and trust that public key). The receiver can authenticate the certificate with the CA's public key and is able to ensure the message has been sent from a certified device and has not been changed from transmission to reception, by checking the message signature with the public key in the certificate.

The certificates contain a Provider Service Identifier (PSID) that states the message types that the sender is allowed to transmit. In addition, the certificate may include additional authorizations in Service Specific Permissions (SSPs). For example, a public safety vehicle may have a certificate with a PSID that authorizes it to send BSMs. The certificate may also include an SSP that authorizes it to state its role (i.e., police, fire, or ambulance) and to include emergency details (e.g., light bar/siren in use) in the BSM.

Senders obtain certificates by requesting them from a CA using an agreed protocol (see below for details). Certificates have an associated lifetime/validity period, i.e., a start validity date and an end validity date. Signed messages should only be considered trustworthy if the signature was generated during the validity period of the certificate. Because certificates expire, all sending devices are expected to be able request and obtain new certificates from their CA before the current certificate(s) expire. IOOs will need to support certificate request and download on an ongoing basis for CI and for fleet vehicles which they may be maintaining. For the latter, as well as for vehicles not under the control of the IOO, IOOs may choose to allow the CI to be used for certificate request and download via LTE-V2X communications (see Section 5.7).

Details of certificate management and use can depend on the application that the certificate authorizes (which is indicated by the PSID). For example, for BSM signing certificates, the convention is that private-use vehicles have multiple concurrently valid certificates (called a “batch”); the BSM signer changes the signing certificate in use from time to time to protect the privacy of the sender. For BSM signing certificates, it is also common practice to download certificate batches some time in advance of when those certificates become valid. For infrastructure-based applications that have no privacy requirements, the convention is that there is one certificate valid at a time and the next certificate is requested and downloaded only slightly before the current certificate expires.

Certificates for private-use vehicles are referred to as “pseudonym” certificates, while those used by agency or fleet vehicles to request privileged services like signal prioritization are referred to as “identification” certificates. Pseudonym certificates make use of privacy-protecting mechanisms such as those discussed for the BSM above, whereas identification certificates do not. Although certificate management approaches are application-specific, in general all certificate type-specific (e.g., pseudonym, identification) management approaches are similar.

A sender’s certificate can be revoked by adding it to a Certificate Revocation List (CRL). This will typically be done if a sender is found to be persistently sending out seriously incorrect data and tells devices that have received the CRL not to trust messages signed with that sending certificate. In the case of pseudonym certificates, where there may be many certificates per period and the sender may have downloaded many time periods worth of certificates, these certificates are cryptographically linked so they can be revoked with a single CRL entry. If a device’s certificates are revoked, it is not issued new certificates until remediation. See Section 6.4 for a discussion on misbehavior reporting and revocation.

6.2 SCMS Manager

The SCMS Manager is a functional component of the SCMS, as defined in IEEE 1609.2.1 (see Table 10). The conceptual SCMS architecture is defined in IEEE 1609.2.1 and is partially based on a previous architecture developed by CAMP specifically for V2X communications. The purpose of the SCMS is to provision End-Entities (EEs) in the system with certificates that accompany messages such that message recipients have assurance of the message authenticity.

In the IEEE 1609.2.1 standard, the SCMS Manager is a component of the SCMS whose role is to govern the entire SCMS, including defining and enforcing the certificate and security policies to be applied to electors and root CAs. According to IEEE1609.2.1, an SCMS Manager is needed to set and update the security policies and procedures for the V2X ecosystem including both the CVs and deployed CI.

The industry is working on the process for a lead SCMS Manager authority to be established to set the security policies and procedures enabling multiple SCMSs to provide V2X PKI security services, following the IEEE 1609.2.1 process.

6.2.1 Trusted (End-Entity) Devices

Trust is established in a device through the device being certified. To enable device certification, the SCMS Manager will need to publish the rules and requirements on the end-to-end process for device certification.

An example of such a report for the US is the one accessible at: <https://www.scmsmanager.org/wp-content/uploads/2022/06/SCMS-Manager-End-Entity-Requirements-Design-Guidance-and-Validation-Approach-v1.00.pdf>

6.2.2 Trusted Messages

Trust is established in the messages sent by a device through the established PKI system and the device being provisioned with certificates from an SCMS Manager authorized/trusted PKI entity. Like device certification, the SCMS Manager will need to publish the rules and requirements on the process for the certified devices to be additionally certified to send specific V2X messages.

It is expected that the rules and requirements will build upon existing certification work, where available, to ensure evidence has been provided and policies followed to enable devices to obtain security certificates. It is also expected that the rules and requirements will allow for separate security certificates at a reduced level of trust (e.g., test certificates), for example, pre-production development, technology readiness events (“plugfests”), and technology evaluation pilots.

6.3 Certification Entity

Deployment of the Day One messages requires a level of trust between the sender and the receiver. To this end, device/component-level and operational certification is required for a device to obtain security certificates to aid in over-the-air conformance and interoperability. Given that the security certificates need to operate properly on fully functional, conformant devices/components, work is under way in the US by multiple organizations (e.g., OmniAir, SCMS Manager organization) on security and V2X device and system test criteria for certification to provide trusted message transmissions.

6.3.1 OmniAir Conformance Specifications

OmniAir Consortium is a leading industry association promoting interoperability and certification for ITS, tolling, and CVs. The certification body has developed a members-driven process and procedures for implementing device-level scope, test cases, test-control interfaces, test-equipment qualification, test-laboratory authorization, field-test site authorization, reference devices, certification awarding/listing, re-certification policy, and surveillance. Bench and field black-box testing covers radio/physical layer, protocol, security, network services, minimum performance, interoperability, and applications elements in modules, for both OBU and RSU device types.

Document 753-OA-CertScope-Matrixes describes the scope, process, components, and test specifications for Connected V2X and RFID Tolling. This document is accessible at: <https://omniair.org/services/connected-vehicle-certification> under the publicly

available documents for reference “753-OA-CERTSCOPE-MATRIXES” link.

Examples of OmniAir test specifications are provided in Table 8. The set of test cases developed to support the test specifications are provided in Document 755a-OA-TCsList-LTEV2X available at: <https://omniair.org/services/connected-vehicle-certification> under the publicly available documents for reference “755A-OA-TCsList-LTEV2X” link.

These tests, or their equivalent, are required for a device to be evaluated for trusted message conformance.

Table 8: Example OmniAir Test Conformance Specifications⁴

3.4. Test Specifications regarding Connected Vehicle

721-OA-V2X is the governing document in defining the Connected Vehicle V2X Test Plan based on device capabilities and uses individual test specifications “700 series” shown below and their recommended parameters guidelines (* - Planned or In-works):

[53]	737-OA-TCI2	Test Control Interface v2
[54]	739-OA-TCI3	Test Control Interface v3
[55]	748-OA-CertGen-Testing	SCMS Certificates Request Instructions
[56]	759-OA-TSS&TP-CV2XModule	LTE-V Module-Global
[57]	760-OA-TSS&TP-80211p	WAVE MAC & Physical Layer (PHY)
[58]	761-OA-TSS&TP-36521	3GPP LTE-V Radio Release 14
[59]	762-OA-TSS&TP-J31611	LTE-V2X V-V Minimum Performance & Message Profiles
[60]	763-OA-TSS&TP-16092	WAVE Security Services
[61]	764a-OA-TSS&TP-CAMP	SCMS Security Certificates & Services (CAMP-based)
[62]	764b-OA-TSS&TP-160921 *	SCMS Security Certificates & Services (IEEE 1609-2-1based)
[63]	765-OA-TSS&TP-16093	WAVE Network Services
[64]	766-OA-TSS&TP-16094	WAVE Multi-Channel & EDCA
[65]	767-OA-TSS&TP-J29451	V-V Minimum Performance (Bench)
[66]	768-OA-TSS&TP-J29451A	V-V Minimum Performance (Device-Level Field)
[67]	769-OA-TSS&TP-J29451A	V-V Minimum Performance / BSM Drive Test Checklist (Device-Level Field)
[68]	770-OA-TSS&TP-RSU41	RSU 4.1 Procedure
[69]	771-OA-TSS&TP-TS10	Dual Operating RSU
[70]	772-OA-TSS&TP-CTI4001 *	CTI 4001 RSU
[71]	773-OA-TSS&TP-CI-TSCRSUIF *	Connected Intersection - TSC RSU Interface
[72]	780a-OA-TSS&TP-V2VApps *	V2V Applications Set
[73]	780b-OA-TSS&TP-V2IApps*	V2I or I2V Applications Set
[74]	781-OA-TSS&TP-V2XHUB *	V2XHUB Usage
[75]	782-OA-TSS&TP-MAP	MAP Message Transmission
[76]	783-OA-TSS&TP-SPAT	SPaT Message Transmission
[77]	784-OA-TSS&TP-SPAT1202	SPAT Message Transmission with NEMA 1202v3 Interface
[78]	785-OA-TSS&TP-1218 *	NTCIP 1218 Interface with V2X Operations
[79]	786-OA-TSS&TP-TIM *	Travelers Information Message Transmission
[80]	787-OA-TSS&TP-PSM *	Personal Safety Message Transmission
[81]	788-OA-TSS&TP-J3217 *	J3217 V2X Tolling

6.3.2 Message Conformance Test Procedures

For certification, trusted message conformance test procedures are needed for each of the messages the device/component transmits. These procedures test for message conformance at multiple levels and include:

⁴ This table material is reused from OmniAir document 753-OA-CertScope-Matrixes, V1.0. Used by permission. Copyright © 2023 OmniAir Consortium, Inc. All rights reserved.

- 1) Component Conformance Test Procedures – These procedures are to be run on the component(s), which includes the certified device or may be just the certified device (but could be run on a component(s)-installed integrated system – see item 2) to validate that the message payload meets the format requirements. These tests just confirm that the proper payload is present but may not be able to confirm if the values are correct. Those tests would be part of the integrated system procedures.
- 2) Integrated System Conformance Test Procedures – These procedures are to be run on the device-installed integrated system (i.e., all the components from start to finish including the certified device that produce the contents of the message), which will be deployed to validate that the payload and message performance requirements (e.g., content correctness, content accuracy, transmission intervals, transmission power) have been met.
- 3) (Message Dependent) Maintenance Conformance Test Procedures – These procedures are to be run periodically to ensure ongoing validation of the deployed integrated system.

For a message to be considered for Day One deployment, the first two of the above are required and, depending on the message, the third of the above may also be required.

Depending on the message there may need to be conformance at a national level, meaning that anywhere in the US a CV can understand and use the information in the message as intended, or possibly just a regional or local level, meaning that only select vehicles in that region are expected to understand and use the information. For each of the messages, Table 9 lists which of the above conformance test procedures are known to be supported for each of the Day One messages at a national level. For messages which may require only regional or local support, Table 9 may not apply, and those message cells are marked with a hyphen.

NOTE: The SCMS Manager will establish the policies regarding conformance certification – e.g., recognized certification organization, third-party certification, need for re-certification – which could potentially include self-attestation. Also, it will be up to the SCMS Manager to determine which conformance reports are approved for demonstrating message conformance. For example, some of the SDO test reports listed in Table 3 may suffice for demonstrating message conformance.

NOTE: Demonstration of message conformance is exhibited by a component being provisioned with production message-specific signing certificates (see Task 9 in Section 2.2.3).

Table 9: Day One Message National Conformance Procedure and Day One Support Status

Message	Conformance Test Procedures		
	Component	Integrated System	Maintenance
Message Category: Mass Use Production Vehicle (MUPV)			
BSM	Yes	Yes	NA
SPaT	Yes	In Progress	In Progress
MAP	Yes	In Progress	In Progress
RTCM Corrections	Yes	In Progress	In Progress
TIM	Yes	No	NA
RSM	Yes	No	NA
Message Category: Limited Use Fleet Vehicle (LUFV)			
SRM ⁽¹⁾	-	-	-
SSM ⁽¹⁾	-	-	-
Message Category: Limited Use Mixed Vehicle (LUMV)			
TAM	No	No	NA
TUM	No	No	NA
TUMack	No	No	NA
WSA	Yes	No	NA

⁽¹⁾ Day One message which may only require regional or local conformance certification.

6.4 Misbehavior Reporting and Revocation

The term Misbehavior Reporting refers to field-deployed devices detecting that received messages are believed to be wrong and reporting these messages to a CA which is part of the SCMS Manager. While devices report misbehavior, the CA makes the final decision regarding misbehavior and, if necessary, the decision to revoke the device's certificates.

Misbehavior Reporting is being standardized in SAE J3287, which is under development. SAE J3287 is expected to evolve through multiple versions that will specify an increasing set of misbehavior report types and contents. While this functionality is not expected to be required by the SCMS Manager as part of a Day One deployment in the US, once J3287 is published, and over time as it evolves, it is expected that the SCMS Manager will create requirements for some or all devices to support misbehavior reporting.

For certificate revocation, in IEEE 1609.2, certificates contain one of the following:

- 1) An indication that they will not be revoked.
- 2) An identifier for the CRL that they will appear on if they are revoked.

For the former, that means that if the EE that holds the certificate is compromised, that entity will be able to continue sending the message until that certificate expires but will not receive any additional authorization certificates. This may make sense for messages which have certificates reissued, for example, daily. In this case, it may make sense to stop reissuing certificates if the device has been determined by the CA to be misbehaving, rather than having to issue a CRL that then must be distributed to all devices that might need it.

For the latter, if a CA issues any certificates that might be revoked, there must be an associated CRL signer to issue the relevant CRL. The CRL is made available via direct download from each device’s Registration Authority (RA), as specified in IEEE 1609.2.1 (and may be made available by other means as well). If a device holds any certificate that might be revoked, then the device must ensure that it can obtain the most recent copy of the CRL that would revoke that certificate (or otherwise obtain revocation information about itself). If a device’s certificates for a particular application are revoked, the device must stop signing and transmitting messages for that application. It is expected that conformance with this behavior will be required by the SCMS Manager for Day One. In fact, some of the Day One message reports already have this as a requirement.

NOTE: Received messages signed by revoked certificates are invalid. It is recommended that all devices that receive messages can receive CRLs and use those CRLs to check the revocation status of any revocable certificate that signed the received message. However, this is not expected to be a Day One SCMS Manager requirement.

NOTE: Certificates may be revoked for any reason considered appropriate by the SCMS Manager and, therefore, there may be reasons other than misbehavior for device certificates to be revoked. Thus, there is a need for revocation support even if misbehavior detection is not required.

6.5 SCMS-related Report References

Table 10 provides details on the security-related reports referenced in the other subsections of Section 6. The reports are listed in alphabetical order and include the title, publisher, current revision at the time of writing, type of report (e.g., standard), and the availability status.

Table 10: SCMS-related SDO Reports Details

Report	Title	Publisher	Current Revision	Type	Availability Status
IEEE 1609.2.1	IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Certificate Management Interfaces for End Entities	IEEE	2022	Standard	Available: Published
SAE J3287	V2X Misbehavior Reporting	SAE International	Under Development	Standard	Not Available: Under Development

7 Other Things and What's Next

7.1 Emerging Guidance from CTI

The USDOT successfully developed a Connected Transportation Interoperability (CTI) Connected Intersections Implementation Guide, CTI 4501 v01.01, under an equal equity voting membership between the automotive stakeholder community led by SAE International and the ITS infrastructure community stakeholders led by ITE, AASHTO, and NEMA. CTI 4501 provides guidance and concepts necessary to help deploy nationally interoperable connected intersection applications based on the use of the SPaT, MAP, and RCTM Corrections messages. During development and validation of CTI 4501, several potential activities were identified to update and enhance the existing guidance moving forward, as part of a phase two effort.

In the fall of 2022, the Connected Transportation Interoperability Committee (CTIC) was formed under SAE International with the same equal voting arrangement that was established with ITE, AASHTO and NEMA during the phase one effort. Under the phase two effort, the CTIC intends to:

- ▶ Support the development of updated and enhanced positioning guidance specifically as it relates to the use of RTCM Corrections, but also potentially other positioning techniques in addition to those which use GNSS.
- ▶ Support the development of enhancements to the SPaT and MAP which were identified in phase one.
- ▶ Support the development of additional verification and validation test procedures for the SPaT, MAP, and RTCM Corrections messages.
- ▶ Support the development of signal priority and preemption guidance, which includes a concept of operations (ConOps), requirements, design, and verification and validation test procedures.
- ▶ Support message and connected intersection deployment evaluation via test tool development and conducting test activities to support verification and validation of not only the messages but also test procedures developed as part of the other technical activities.

Some of the reports under development in the CTIC have been referenced in Table 3 for the Day One message reports. It is expected that the CTIC efforts will be key to developing material required for the messages addressed within this guidebook to be ready for Day One deployment support.

7.2 Additional Considerations and Guidance

Sections 2 through 6 address considerations and requirements to deploy one or more of the Day One message sets along with the report references to support them. This section provides additional considerations and guidance, some of which

may be required for both the initial deployment as well as post development. While there was mention of some of those items in this guidebook, the following is a more comprehensive list of items.

- ▶ Certificate Top off: Production certificates are obtained in batches which are time limited. A mechanism for acquiring additional batches of certificates, referred to as certificate top off or sometimes top up, will be needed.
- ▶ System Availability: While system availability is in the purview of the agency deploying the system, items which affect the availability of the system should be considered to ensure that the benefits of deploying the system are maintained on a continuous basis, not including planned system maintenance, updates, etc.
- ▶ Payload Size: LTE-V2X Channel 183 has a finite capacity for providing information. Some of the message payload format definitions include optional content to provide flexibility in what is included in the payload of the message, for example, to support optional application features. When possible, the size of the payload should be kept to a minimum. So, when adding optional content to the payload of the message, there should be consideration on the benefit of the information versus the impact on the size of the payload.
- ▶ Device Repair/Replacement: Provisions will likely be required to handle a device that is malfunctioning or otherwise becomes suspect in its operation and needs to be taken offline and repaired or replaced.
- ▶ Device Decommissioning: Provisions will likely be required to handle a device that is no longer required and needs to be decommissioned.
- ▶ Device Theft: Provisions will likely be required to handle a device that has been stolen, to limit the impact should there be an attempt to use it as a misbehaving device.

NOTE: For the items that involve a device being removed from the system (e.g., device repair, decommissioning, theft), it is expected that the SCMS Manager will provide policies and procedures relating to correct cybersecurity practice for this event, including withdrawal/revocation and (if appropriate) reinstatement of certificates. Other items such as financial, law enforcement, etc. are necessarily in the purview of the equipment owner.

8 References

Documents references can be found in the following tables:

- ▶ Table 4: Day One Message SDO Reports Details
- ▶ Table 6: Day One Message Supporting Reports Details
- ▶ Table 7: Day One Hardware Supporting Reports Details
- ▶ Table 10: SCMS-related SDO Reports Details

NOTE: These tables include the underlying report references to support the Day One message deployment. In many cases the reports provided in the tables reference other reports which are not included for brevity.

9 Definitions and Abbreviations

9.1 Definitions

For the purposes of the present document, the following definitions apply:

Certified Device: A device which has been certified by a third-party certification body, tested by an independent, accredited test laboratory using qualified test systems and validated test cases/specifications, verifying device-level conformance with the minimum set of applicable industry standards, security, and meeting interoperability requirements. A certified device should bear certification marks and its public listing as evidence of certification.

NOTE: A certified device is necessary and may require system-level conformance/validation and performance testing for obtaining production message signing certificates.

Connected Infrastructure: An infrastructure component that communicates with external entities using a wireless interface. Examples of wireless interfaces include cellular networks, Wi-Fi networks, and V2X.

Connected Vehicle: A vehicle that communicates with external entities using a wireless interface. Examples of wireless interfaces include cellular networks, Wi-Fi networks, and V2X.

Day One: The period when devices that support one or more of the message sets provided in Section 3 are deployed, either nationally or regionally, after being certified per the requisite SCMS Manager policies and procedures for those messages.

Day Two: The period after Day One when devices that support one or more of the messages provided in Annex B, or possibly other messages, are deployed, either nationally or regionally, after being certified per the requisite SCMS Manager policies and procedures for those messages.

9.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

Glossary

3GPP	3 rd Generation Partnership Project
5GAA	5G Automotive Association
AASHTO	American Association of State Highway and Transportation Officials
ASN.1	Abstract Syntax Notation One
BDS	BeiDou Navigation Satellite system
BSM	Basic Safety Message
CA	Certificate Authority
CAMP	Crash Avoidance Metrics Partners
CI	Connected Infrastructure

ConOps	Concept of Operations
CP	Certificate Policy
CR	Channel Occupancy Ratio
CRL	Certificate Revocation List
CTI	Connected Transportation Interoperability
CTIC	Connected Transportation Interoperability Committee
CV	Connected Vehicle
C-V2X	Cellular V2X
DNS	Domain Name System
EE	End-Entity
ERP	Effective Radiated Power
EU	European Union
FCC	Federal Communications Commission
FHWA	Federal Highway Administration
GLONASS	<i>Globalnaya Navigatsionnaya Sputnikovaya Sistema</i> (Global Navigation Satellite System)
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
HARQ	Hybrid Automatic Repeat Request
HSM	Hardware Security Module
IOO	Infrastructure Owner Operator
I2V	Infrastructure-to-Vehicle
IP	Ingress Protection
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ITE	Institute of Transportation Engineers
ITS	Intelligent Transportation Systems
ITIS	International Traveler Information Systems
LoS	Line-of-Sight
LTE	Long-Term Evolution (4G radio)
LUFV	Limited Use Fleet Vehicle
LUMV	Limited Use Mixed Vehicle
MAP	Map Data
MCS	Modulation and Coding Scheme
MUPV	Mass Use Production Vehicle
MU	Mobile Unit
NEMA	National Electrical Manufacturers Association
OBU	On-board Unit
OEM	Original Equipment Manufacturer
PDB	Packet Delay Budget
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PoE	Power over Ethernet
PPPP	ProSe Per-Packet Priority
PRR	Packet Reception Ratio

PSID	Provider Service Identifier
PSM	Personal Safety Message
RA	Registration Authority
RF	Radio Frequency
RGA	Road Geometry and Attributes
RLVW	Red Light Violation Warning
RSM	Road Safety Message
RSU	Roadside Unit
RTCM	Radio Technical Commission for Maritime Services
Rx	Receive
SAE	SAE International (formerly Society of Automotive Engineers, USA)
SDO	Standards Development Organization
SDSM	Sensor Data Sharing Message
SCMS	Security Credential Management System
SPS	Semi-Persistent Scheduling
SPaT	Signal Phase and Timing
SRM	Signal Request Message
SSM	Signal Status Message
SSP	Service Specific Permissions
TAM	Toll Advertisement Message
TIM	Traveler Information Message
TMS	Traffic Management System
TSC	Traffic Signal Controller
TUM	Toll Usage Message
TUMack	Toll Usage Message Acknowledgement
Tx	Transmit
US	United States
USDOT	United States Department of Transportation
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
vHSM	Virtual Hardware Security Module
VRU	Vulnerable Road User
WAVE	Wireless Access for Vehicular Environments
WSA	WAVE Service Advertisement

Annex A: Simulation Results⁵

Given that the primary V2X communications channel is the 20 MHz Channel 183, all Day One messages are slated to be transmitted on that channel (See 'Channel Identifier' in Section 4.2 Table 5). BSM transmissions, which are one of the primary intended uses of the channel, need to be reliable to support the safety-critical V2V crash-imminent scenarios for which they were defined. Therefore, simulations were run to evaluate the effect of the other Day One messages on the BSM reception performance by the CVs. The simulation results were used to either validate or, if necessary, revise the LTE-V2X settings provided in Table 5, such that the BSM reception performance is not adversely affected by the inclusion of the other messages on the channel.

In this section, the performance of the LTE-V2X communication is examined when the Day One Intersection-to-Vehicle (I2V) traffic is added to the V2V safety traffic (i.e., BSM). For this purpose, an urban environment has been selected as most of the I2V-based message generation is going to happen in an urban environment with RSUs located at intersections. Rural areas are expected to have better performance as the number of RSUs is expected to be lower. In the simulation scenario, an urban environment with a set of vertical blocks (one block wide), as shown in Figure A.1, is selected, where there is an RSU in each intersection transmitting the MAP, SPaT, and RTCM Corrections messages and vehicles transmitting the BSMs. The simulation layout is described in Figure A.1 where the number and length of the vertical blocks varies depending on the congestion scenario that is being analyzed while the width of the horizontal block remains fixed. Typical in many simulations, when vehicles depart from one side of the simulated boundary (e.g., the far side of a block) they reappear at the other side in a circular fashion. This is depicted in Figure A.1 by the dotted red lines along with the RSUs only being shown on one side of the block.

⁵ The simulation was done by Qualcomm Technologies, Inc. as a part of parameter specification for the 20 MHz Channel 183 in SAE J3161 in SAE C-V2X Technical Committee

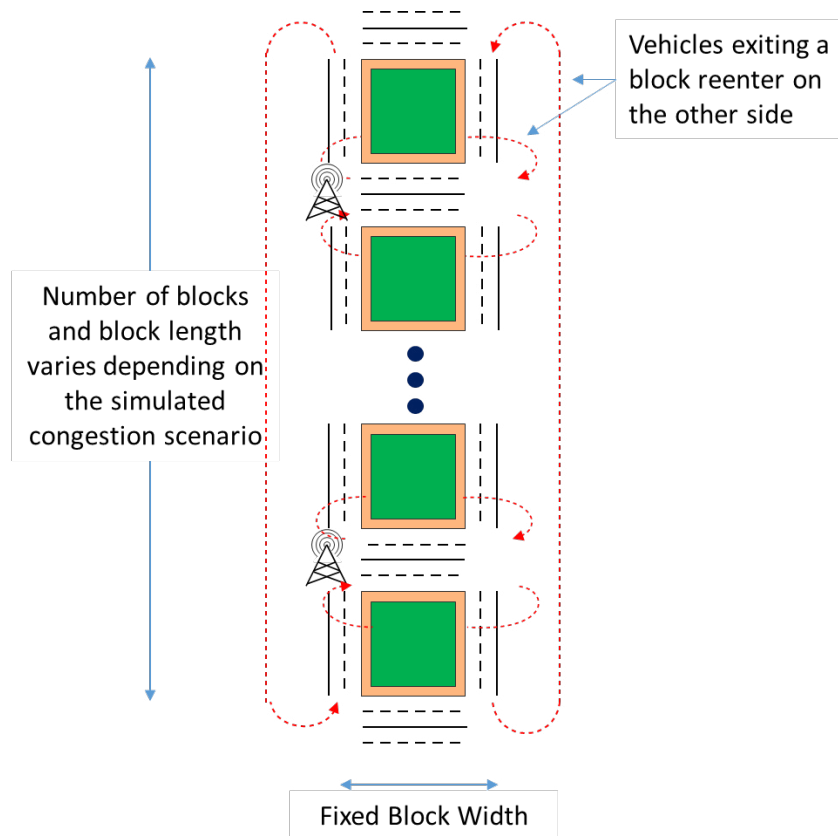


Figure A.1: Urban Environment with an RSU in Each Intersection Transmitting MAP, SPaT, and RTCM Messages

Table A.1 describes the transmit (Tx) parameters for a select set of Day One messages. In the RSUs, MAP and SPaT are transmitted through Semi-Persistent Scheduling (SPS) flows while the RTCM Corrections are transmitted through One-Shot (see SAE J3161/1 – Table 4). In the OBUs, each BSM is transmitted with a signature and either a security certificate containing a public key or a certificate digest (see SAE J3161/1). The BSM is transmitted with a full certificate (total packet size approximately 300 Bytes) approximately every 500 ms with the other BSMs transmitted with a certificate digest (total packet size approximately 190 Bytes) to reduce the overall message length. The PPPP and PDB values (see Section 4.2) are assigned based on the guidance provided in this guidebook and the other radio parameters (i.e., Modulation and Coding Scheme [MCS] and Number of Subchannels) which are affected by the packet size and are chosen based on values assigned in SAE J3161.

Table A.1: Tx Parameters of Select Day One Messages

Message	Message Size	MCS	Transmission Rate	PPPP	PDB	Number of Subchannels
BSM	20% of Tx 300 Bytes	11	10 Hz	5	100 ms	2
	80% of Tx 190 Bytes	5				
MAP	1500 Bytes	11	1 Hz	3	1000 ms	10
SPaT	500 Bytes	11	10 Hz	5	100 ms	3
RTCM Corrections	850 Bytes	11	1 Hz	5	1000 ms	5

Table A.2 describes the high-level simulation assumptions specifying the parameters for the V2V and I2V communication link. The RSU is assumed to have a 6 dBi antenna gain, which is a measure of how much the antenna amplifies the signal, and a 20 dBm conducted power, which is the amount of power the RSU conducts to the antenna. The RSU antenna is assumed to be placed at a height of 5.5 meters above the ground. On the other hand, the OBU is assumed to have a 3 dBi antenna gain and a 20 dBm conducted power. The OBU antenna is placed at a height of 1.5 meters above the ground. The pathloss model used is the Winner B2, which is a standard model for vehicular communication that considers various parameters such as the distance between the transmitter and receiver, the antenna height, and the frequency of operation.

Table A.2: Simulation Assumptions

Parameter	Value/Description
Antenna Gain	RSU: 6 dBi OBU: 3 dBi
Antenna Height	RSU: 5.5 m OBU: 1.5 m
Conducted Power	20 dBm
Pathloss	Winner B2
Channel	Rayleigh
HARQ	Enabled both in RSU and OBU
Noise Figure	9 dB

The channel model assumed is Rayleigh, which is widely used in wireless communication to simulate the effects of multipath fading. Hybrid Automatic Repeat Request (HARQ) is enabled for both the RSU and OBU. The Noise Figure is 9 dB, which is a measure of the amount of noise added to the signal by the communication system.

In the simulation, there are also two congestion scenarios – medium and high – as described by the parameter settings in Table A.3 below:

Table A.3: Congestion Scenarios

Parameter/Description	Medium Congestion Scenario	High Congestion Scenario
Number of Vertical Blocks	20	13
Inter-RSU distance/block length	240 m	60 m
Block width	250 m	250 m
Vehicle Separation	40 m	10 m
Vehicle Speed	60 kmph	15 kmph
Number of RSUs	20	13
Number of Vehicles	1,057	1,810

The purpose of the simulation is to evaluate the performance of the V2V safety communication on Channel 183 when I2V traffic is added to the channel as well. The simulation aims to examine the impact of introducing I2V traffic on the PC5 interface. To accomplish this, the simulation generates MAP, SPaT, and RTCM messages from

the RSU side, which are transmitted along with vehicle BSM V2V messages on the 20 MHz Channel 183. The impact of I2V traffic on the V2V communication link's reliability is assessed through Packet Reception Ratio (PRR) and communication range. PRR is a measure of packets that are received correctly by the receiver compared to the total number of packets transmitted, and communication range is defined as the maximum distance at which PRR remains above 90%.

Figure A.2 illustrates the performance of the V2V communication with and without the I2V traffic between intersecting vehicles (i.e., vehicles with building blockage in between). In the figure, the red plot shows the performance of BSM when there is no I2V traffic and the blue plot is when the I2V traffic is added to the channel. As shown in Figure A.2, the degradation of the BSM performance when I2V traffic is added to the channel is very small between intersecting vehicles both for high congestion and medium congestion scenarios.

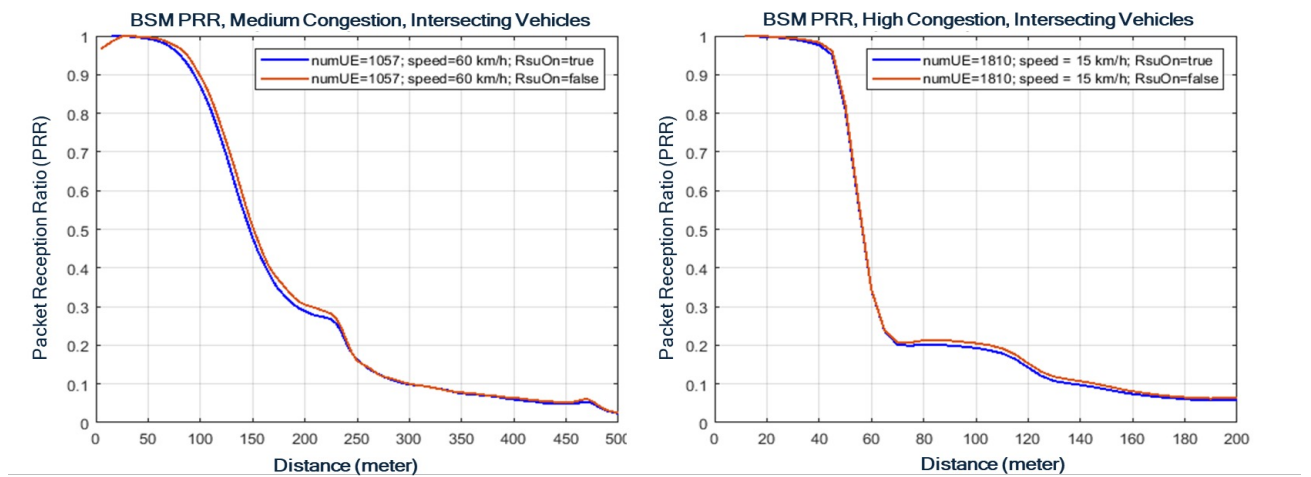


Figure A.2: The Performance of the V2V Communication with and without the I2V Traffic Between Intersecting Vehicles

Figure A.3 also illustrates the performance of the V2V communication, but in this case with and without the I2V traffic between non-intersecting vehicles (i.e., vehicles with no building blockage in between). As shown in Figure A.3, the degradation of the BSM performance when I2V traffic is added to the channel is small between non-intersecting vehicles as well both for high congestion and medium congestion scenarios.

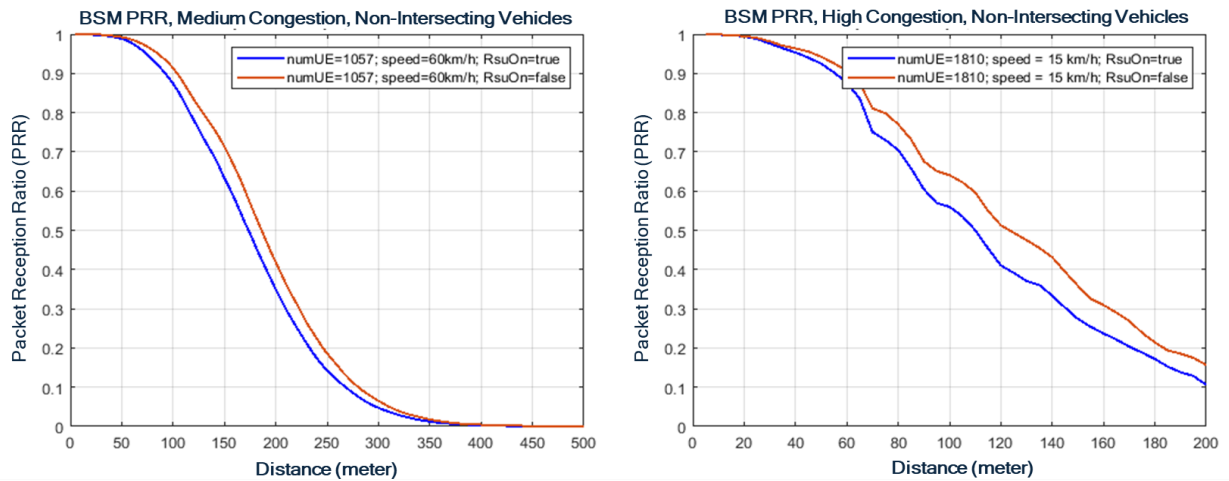


Figure A.3: The Performance of the V2V Communication with and without the I2V Traffic Between Non-intersecting Vehicles.

Figure A.4, A.5, and A.6 also represent the performance of the I2V traffic in presence of the V2V safety messages. As shown in Figure A.4, the communication range for MAP message in high congestion and medium congestion scenarios are almost 120 and 350 meters, respectively.

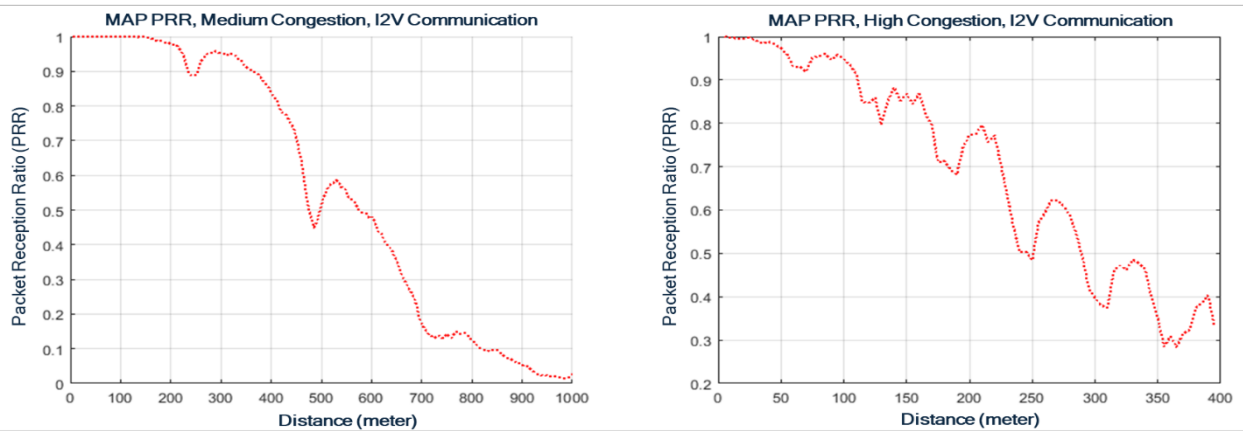


Figure A.4: Performance of MAP Message Both in Medium Congestion and High Congestion Scenarios

The communication range for the SPaT message in high congestion and medium congestion scenarios are almost 170 and 350 meters, respectively (as illustrated in Figure A.5).

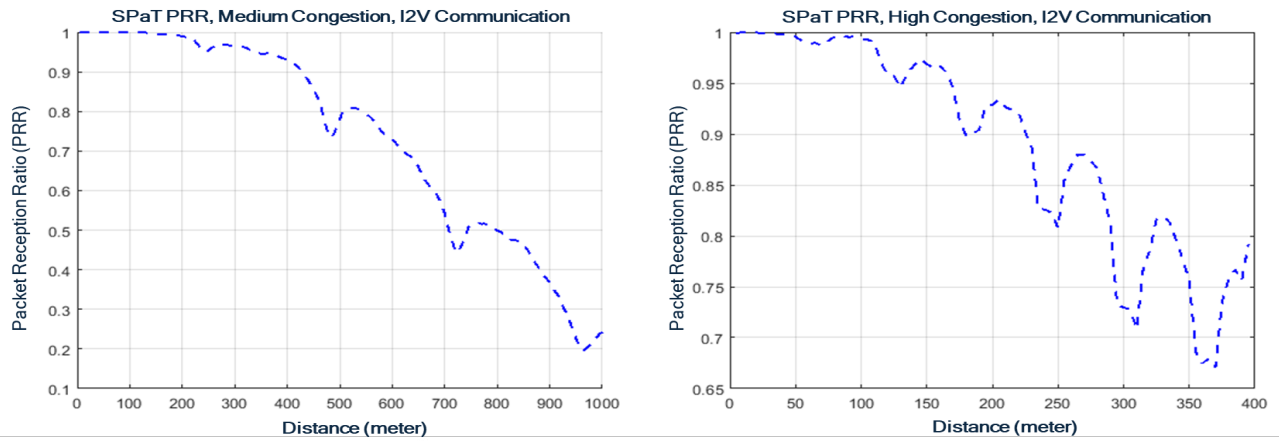


Figure A.5: Performance of SPaT Message Both in Medium Congestion and High Congestion Scenarios

The communication range for the RTCM message is illustrated in Figure A.6. For the RTCM message in high congestion and medium congestion scenarios the range is almost 170 and 370 meters, respectively.

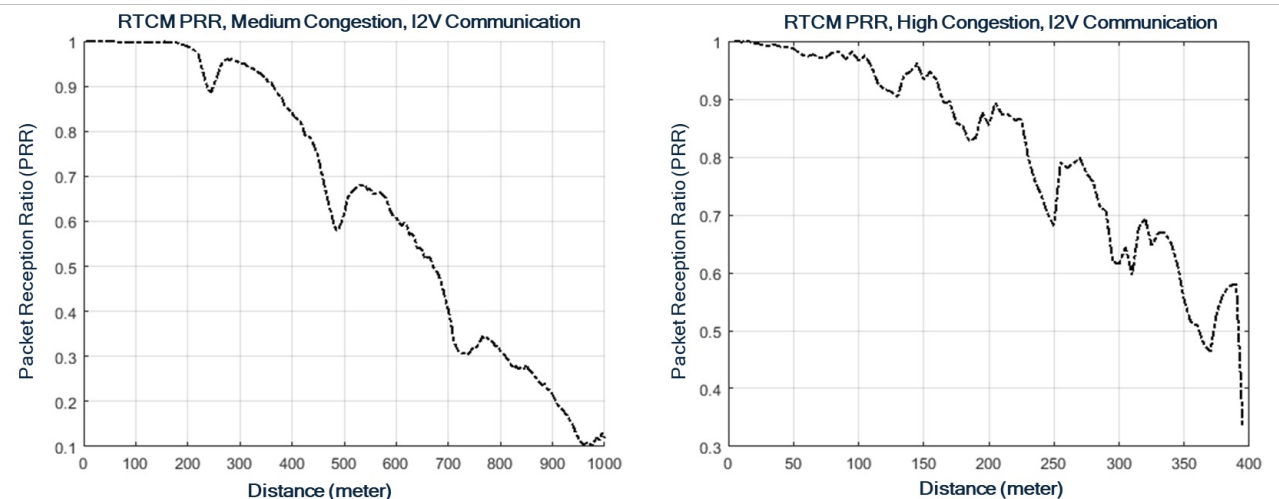


Figure A.6: Performance of RTCM Message Both in Medium Congestion and High Congestion Scenarios

As discussed, and illustrated in this appendix, the 20 MHz channel can accommodate the Day One I2V messages. The performance of the V2V safety traffic was studied in the presence of various types of Day One I2V messages in urban environments and simulation results showed that the degradation in the performance of V2V traffic is acceptable even in high congestion scenarios.

Annex B: Day Two Messages

This section provides information on a potential set of Day Two messages. Like the Day One messages, depending on the application, there may be varying degrees of message use within the vehicle OEM and IOO communities, potentially leading to multiple Day Two deployments. However, unlike the Day One messages, this annex does not attempt to place these messages into different Day Two message categories but does separate them by the following:

- ▶ Expanded Day One Message Support – This is primarily an expansion of the devices that may support the messages for Day Two and potentially, depending on the device, the capabilities of the message.
- ▶ New Messages – These are messages that are not included in the Day One list of messages but, if not already published as a Standard, are anticipated to be.
- ▶ Messages Under Development – These are messages that are not included in the Day One list of messages but are under development and are similar to some of the Day One messages. These are anticipated to be released initially as a Recommended Practice.

B.1: Message Descriptions

The following provides a brief description of the messages and the primary users involved in the message exchange, i.e., a CV or CI.

Expanded Day One Message Support

- ▶ Basic Safety Message (BSM) – Whereas the Day One BSM vehicle classes consider just rigid body vehicles (i.e., FHWA class 1 through 7). Day Two expands the class of vehicles that are anticipated to support transmission of the BSMs to FHWA classes 8 to 13 articulating vehicles.

New Messages

- ▶ Misbehavior Reports – Enables CVs to report on specific “other CV misbehaviors” to the SCMS. The misbehaviors that will be supported are provided in the report.
- ▶ Certificate Revocation List (CRL) – Enables the SCMS to provide message signer revocation information, for multiple message signers, to a CV. This can be used by the CVs and other connected devices, such as CI, to determine whether a message signer has been revoked by the SCMS and so should not be trusted. Key technical features of the CRL include the ability to revoke multiple pseudonym certificates for multiple time periods for a message signer with a single CRL entry.
- ▶ Personal Safety Message (PSM) – Enables a Vulnerable Road User (VRU) device to provide information about select VRU dynamics and non-

Personally Identifiable Information (PII). This can be used by CVs and other connected devices, such as CI, to support VRU detection and, if necessary, alert applications.

- ▶ Sensor Data Sharing Message (SDSM) – Enables CVs and CI to share information of detected road users and/or objects to other V2X entities including information such as the road user or object’s size, location, motion state, etc. This can be used by CVs and CI, for example, to be aware of entities that they may not otherwise be aware of to assist driving-related decision-making (safety, efficiency, etc.).

Messages Under Development

- ▶ Road Geometry and Attributes (RGA) message – Like the MAP, it enables CI to provide information about the road geometry (e.g., lane geometry) and attributes that apply to the road (e.g., speed, allowed maneuvers at lane connections). It is intended to support a broad set of road geometries as well as take a data-layering approach to provide the requisite geometry and attribute information.

B.2 Message Users

For each of the Day Two messages Table B.1 provides information on the primary and potential secondary users of the messages. See Section 3.2 for a description of primary and secondary users.

NOTE: For Day Two messages the primary sender and recipient list expands beyond the CI and the CV to also include VRUs and the SCMS.

Table B.1: Day Two Message Senders and Recipients List

Message	Primary Sender	Primary Recipient	Secondary Recipient
Expanded Day One Message Support			
BSM	CV ⁽¹⁾	CV	CI
New Messages			
Misbehavior Reports	CV	SCMS	
CRL	SCMS	CV	CI
PSM	VRU	CV CI	
SDSM	CI CV	CV CI	
Under Development Messages			
RGA	CI	CV	

⁽¹⁾ See the message category BSM description in Section B.1 for the intended Day Two FHWA vehicle classes.

B.3 SDO Message Reports

Deployment of the Day Two messages requires that there be interoperability between the senders and receivers of messages. To ensure interoperability, the same report types as discussed in Section 4.1 are needed.

For each of the messages, Table B.2 lists the Standards Development Organization (SDO) reports which provide the information discussed in Section 4.1. Refer to that section for a discussion on which reports are required, and which may be addressed via message conformance specifications.

Table B.2: Day Two Message Development and Test SDO Reports List

Message	Message Reports			
	Payload Format Definition	Payload Content and Performance Requirements	Device Test Procedures	Integrated System Test Procedures
Expanded Day One Message Support				
BSM ⁽¹⁾	SAE J2735 & ASN	SAE J2945/1B		
New Messages				
Misbehavior Reports	SAE J3287 & ASN	SAE J3287		
CRL	IEEE 1609.2			
PSM	SAE J2945/9 & ASN	SAE J2945/9		
SDSM	SAE J3224 & ASN	SAE J3224		
Under Development Messages				
RGA	SAE J2945/A & ASN	SAE J2945/A		

⁽¹⁾ See the message category BSM description in Section B.1 for the intended Day Two FHWA vehicle classes.

For the reports listed in Table B.2, Table B.3 provides details on the reports, listed in alphabetical order, including the title, publisher, current revision at the time of this guidance report, type of report (e.g., standard), and the status of its availability.

Table B.3: Day Two Message SDO Reports Details

Report	Title	Publisher	Current Revision	Type	Availability Status
IEEE 1609.2	See Section 4.3 for report details.				
SAE J2735	See Section 4.1 Table 4 for report details.				
SAE J2735 ASN	See Section 4.1 Table 4 for report details.				
SAE J2945/1B	See Section 4.1 Table 4 for report details.				
SAE J2945/9	Vulnerable Road User Safety Message Minimum Performance Requirements	SAE International	New Revision Under Development (Previous Revision: J2945/9_201703)	Standard	New Revision Not Available: Under Development
SAE J2945/A	Minimum Requirements for Road Geometry and Attributes Definition	SAE International	Under Development	Recommended Practice	Not Available: Under Development
SAE J3224	V2X Sensor-Sharing for Cooperative and Automated Driving	SAE International	J3224_202208	Standard	Available: Published
SAE J3287	See Section 6.5, Table 10 for report details.				

Annex C: Future Hardware Capabilities

Included in this annex are some of the future hardware capabilities an RSU may need to support depending on the supported Day Two messages.

- ▶ Misbehavior Reports/CRL Distribution – For IOOs that want to support local CV misbehavior reporting and/or CRL distributions, the same support as is needed for local certificate download is required (see Section 5.7). This will enable a CV to connect to its SCMS provider to report misbehavior and the CI to obtain the CRL from the SCMS for distribution to the CV.
- ▶ Infrastructure-based Sensor Data Sharing – For IOOs planning to support an infrastructure-based SDSM, sensing hardware capable of populating the SDSM may want to be considered. To aid in identifying sensing hardware that can support the requirements, see Table B.2 for the SDSM payload format, content, and performance requirements reports.

NOTE: For VRU Safety, as per Table B.2, SAE J2945/9 provides the payload format, content, and performance requirements; however, like many of the SDO message reports, it is technology agnostic when it comes to transmitting the PSM. Therefore, at this time, no future hardware support guidance can be provided.

Annex D: FHWA Vehicle Category Classifications

Figure D.1, which is reprinted from the USDOT FHWA (highways.dot.gov, search term “vehicle types” or “vehicle classification”), provides a list of the 13 FHWA vehicle category classifications. It can be used as a source for mapping the vehicle classes mentioned in other parts of this document to the types or categories of vehicles to which the classes pertain.


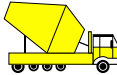

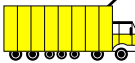

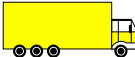










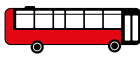






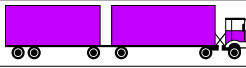

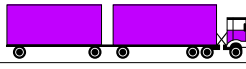


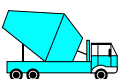
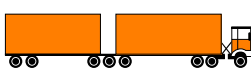
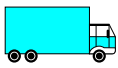



Class 1 Motorcycles		Class 7 Four or more axle, single unit	
Class 2 Passenger cars		Class 8 Four or less axle, single trailer	
			
			
			
Class 3 Four tire, single unit		Class 9 5-Axle tractor semitrailer	
			
			
Class 4 Buses		Class 10 Six or more axle, single trailer	
			
		Class 11 Five or less axle, multi trailer	
Class 5 Two axle, six tire, single unit		Class 12 Six axle, multi-trailer	
			
		Class 13 Seven or more axle, multi-trailer	
Class 6 Three axle, single unit			
			
			

Figure D.1: FHWA 13 Vehicle Category Classification

This Technical Report is a result of the US_DPLOY Work Item project in 5GAA.

By participating in the 5GAA US_DPLOY Work Item meeting each entity, and each of its employees, officers, and representatives that participated in the US_DPLOY WI meetings grants to 5GAA – 5G Automotive Association e.V. and to each of its members a worldwide irrevocable, non-exclusive, non-transferable, sub-licensable (through multiple tiers of sublicensees), royalty-free copyright license to reproduce, adapt create derivative works of, distribute, display, and perform any of the contributions made by the entity or its employees, officers, and representatives, during or in relation to the US_DPLOY WI meeting, be it in writing or orally, solely for the purposes of developing, publishing, and distributing a work product created during, as a consequence of, or as a result of the 5GAA US_DPLOY Work Item.

5GAA is a multi-industry association to develop, test and promote communications solutions, initiate their standardisation and accelerate their commercial availability and global market penetration to address societal need. For more information such as a complete mission statement and a list of members please see <https://5gaa.org>

