SURFACE VEHICLE STANDARD

J2945/1

PropDft XXX2015

Issued	xxxx-xx
Revised	Draft 3.0
Reaffirmed	xxxx-xx
Stabilized	xxxx-xx
Cancelled	xxxx-xx

Superseding Jxxxxx Date

On-board System Requirements for V2V Safety Communications

RATIONALE

This standard is the first edition of performance requirements for V2V safety communications systems. It provides the information necessary to build interoperable systems that support safety applications, which rely on the exchange of Basic Safety Messages.

TO PLACE A DOCUMENT ORDER: **Tel: 877-606-7323 (inside USA and Canada)**
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE WEB ADDRESS: **http://www.sae.org**

SAE values your input. To provide feedback on this Technical Report, please visit http://www.sae.org/technical/standards/PRODCODE

TABLE OF CONTENTS

1. SCOPE

This standard specifies the system requirements for an on-board vehicle-to-vehicle (V2V) safety communications system for light vehicles[1], including standards profiles, functional requirements, and Minimum Performance Requirements (MPR). The system is capable of transmitting the Society of Automotive Engineers (SAE) J2735-defined Basic Safety Message (BSM) [6] over a Dedicated Short Range Communications (DSRC) wireless communications link as defined in the Institute of Electrical and Electronics Engineers (IEEE) 1609 suite and IEEE 802.11 standards [1] - [5].

1.1 Purpose

This standard addresses the on-board system needs for ensuring the transmission of BSMs in V2V safety communications provides the desired interoperability and data integrity to support the performance of the envisioned safety applications.

2. REFERENCES

2.1 Applicable Documents

The following publications form a part of this specification to the extent specified herein.

2.1.1 IEEE Publications

[1] Available from IEEE Operations Center, 445 Hoes Lane, Piscataway, NJ 08854-4141, Tel: 732-981-0060, www.ieee.org.IEEE Std 802.11™-2012Standard for LAN/MAN - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[2] IEEE Std 1609.2™ Draft IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages. December 9, 2015 *(anticipated publication date)*

[3] IEEE Std 1609.3™ Draft IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services. December 9, 2015 *(anticipated publication date)*

[4] IEEE Std 1609.4™ Draft IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Multi-channel Operation. December 9, 2015 *(anticipated publication date)*

[5] IEEE Std 1609.12™ Draft IEEE Standard for Wireless Access in Vehicular Environments (WAVE) – Identifier Allocations. December 9, 2015 *(anticipated publication date)*

2.1.2 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or 724-776-4970 (outside USA), www.sae.org.

[6] SAE J2735 DECEMBER 2015 Dedicated Short Range Communications (DSRC) Message Set Dictionary *(this 2945/1 version based on the Septermber draft which is undergoing parallel ballot)*

2.2 Related Publications

[1] Refer to section 3.1 for the definition of light vehicle. Other vehicle classes and trailers will be addressed in future revisions of this standard, or in other standards within the SAE J2945 family of standards. These revisions or additional standards are expected to be compatible with the requirements of this standard and may define additional capabilities beyond the requirements for light vehicles.

[7] Federal Communications Commission (FCC) 47 Code of Federal Regulations (CFR) Parts 0, 1, 2, and 95 amendments for Dedicated Short Range Communications Services and Mobile Service for Dedicated Short Range Communications of Intelligent Transportation Service in the 5.850-5.925 GHz Band (5.9 GHz Band), http://www.gpo.gov/fdsys/pkg/FR-2006-09-07/pdf/E6-14795.pdf

[8] Mitigation Strategies for Design Exceptions. Federal Highway Administration, October 15, 2014 http://safety.fhwa.dot.gov/geometric/pubs/mitigationstrategies/chapter3/3_lanewidth.cfm

[9] CAMP Vehicle Safety Communications Security Studies: Study 3 Final Report: Definition of Communication Protocols between SCMS Components and Specification of the Components Psuedonym Certificate Authority, Registration Authority, and Linkage Authority: National Highway Traffic Safety Administration (Cooperative Agreement Number DTFH61-01-X-00014). July 31, 2014.

[10] CAMP Vehicle Safety Communications Security Studies: Study 1: Security Credential Management System (DTFH61-01-X-00014): National Highway Traffic Safety Administration. July 31, 2014.

[11] National Highway Traffic Safety Administration, “Vehicle Safety Communications – Applications (VSC-A) Final Report,” DOT HS 811 492A, September 2011. http://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2011/811492A.pdf

[12] National Highway Traffic Safety Administration: Vehicle-to-Vehicle Safety System and Vehicle Build for Safety Pilot (V2V-SP) Final Report, Volume 1 of 2, Driver Acceptance Clinics: National Highway Traffic Safety Administration (Cooperative Agreement Number DTFH61-01-X-00014). April 10, 2014. http://www.regulations.gov/contentStreamer?documentId=NHTSA-2014-0022-0042&attachmentNumber=1&disposition=attachment&contentType=pdf

[13] Vehicle Safety Communications – Applications Final Report: Appendix Volume 1 System Design and Objective Test,” DOT HS 811 492B, September 2011. http://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2011/811492B.pdf

[14] Vehicle-to-Vehicle Safety System Light Vehicle Builds and Model Deployment Support (V2V-MD): Test Plan and Test Procedures for Vehicle Awareness Devices and Aftermarket Safety Devices: National Highway Traffic Safety Administration (Cooperative Agreement Number DTFH61-01-X-00014). March 4, 2014

[15] ITU-R TF.460-6: Standard-frequency and time-signal emissions

[16] FIPS PUB 140-2: Federal Information Processing Standards Publication: Security Requirements for Cryptographic Modules

3. TERMS AND DEFINITIONS

3.1 Definitions

For the purposes of this standard, the following definitions apply.

Security Credential Management System: The private key infrastructure that issues certificates and other credentials

Crash: A collision between two vehicles

Event Condition: When an event that corresponds to one of the flags in DE_VehicleEventFlags occurs

Latency: The delay from an an event occurance to the desired outcome

Light Vehicle: A class 2 or class 3 vehicle as defined by FHWA (http://onlinemanuals.txdot.gov/txdotmanuals/tri/vehicle_classification_using_fhwa_13category_scheme.htm)

Packet Collision: When two or more transmissions overlap in time at a potential receiver, causing the receiver to fail to interpret the content of any of the transmissions

Within 1-Sigma of the Absolute Error: 68% of data samples in a test deviate less than a defined error threshold from the reference value

Within 3-Sigma of the Absolute Error: 99% of data samples in a test deviate less than a defined error threshold from the reference value

3.2 Abbreviations and Acronyms

The abbreviations and acronyms cited below are terms used in this Standard.

AES	Advanced Encryption Standard
ABS	Antilock Brake System
ASN.1	Abstract Syntax Notation One
BSM	Basic Safety Message
BSS	Basic Service Set
BSW	Blind Spot Warning
CA	Certificate Authority
CAMP	Crash Avoidance Metrics Partnership
CAN	Controller Area Network
CBP	Channel Busy Percentage
CCH	Control Channel
CCM	Counter Mode with Cipher Block Chaining Message Authentication Code
CFR	Code of Federal Regulations
CLW	Control Loss Warning
CME	Certificate Management Entity
CPR	Certificate Provisioning Request
CRL	Certificate Revocation List
CRLG	Certificate Revocation List Generator
CTS	Clear To Send
DCM	Device Configuration Manager
DE	Data Element
DF	Data Frame
DNS	Domain Name Services
DOT	Department of Transportation
DSRC	Dedicated Short Range Communications
DTI	Distance to Intersection
DVI	Driver Vehicle Interface
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
ECU	Electronic Control Unit
EDCA	Enhanced Distributed Channel Access
EEBL	Emergency Electronic Brake Lights

EGNOS	European Geostationary Navigation Overlay Service
FCC	Federal Communications Commission
FCW	Forward Crash Warning
FHWA	Federal Highway Administration
FIPS	Federal Information Processing Standards
GHz	Gigahertz
GNSS	Global Navigation Satellite System
HCF	Hybrid Coordination Function
HSM	Hardware Security Module
HV	Host Vehicle
Hz	Hertz
ICA	Intermediate Certificate Authority
IEEE	Institute of Electrical and Electronics Engineers
IMA	Intersection Movement Assist
IPv6	Internet Protocol Version 6
ITT	Inter-transmit Time
kph	Kilometers per hour
LCW	Lane Change Warning
LOS	Line of Sight
LTA	Left Turn Assist
MA	Misbehavior Authority
MAC	Medium Access Control
MD	Model Deployment
MHz	Megahertz
MIB	Management Information Base
MLME	MAC Sublayer Management Entity
mph	Miles per hour
MPR	Minimum Performance Requirements
NHTSA	National Highway Traffic Safety Administration
NMEA	National Marine Electronics Association
OBE	Onboard Equipment
OCB	Outside the Context of a BSS
OFDM	Orthogonal Frequency Division Multiplexing
OTA	Over The Air
PCA	Pseudonym Certificate Authority
PER	Packet Error Rate
PH	Path History
PHY	Physical Layer
PICS	Protocol Implementation Conformance Statement

PLME	Physical Layer Management Entity
PP	Path Prediction
PPS	Pulse Per Second
PSID	Provider Service ID
RA	Registration Authority
RF	Radio Frequency
RSE	Roadside Equipment
RTP	Radiated Transmit Power
RTS	Request To Send
RV	Remote Vehicle
SAE	Society of Automotive Engineers
SAP	Service Access Point
SBAS	Satellite Based Augmentation System
SCH	Service Channel
SCMS	Security Credential Management System
STA	Station
3D	Three-Dimensional
TSF	Time Synchronization Function
TTC	Time-to-Crash
TTI	Time-to-Intersection
Tx	Transmit
UPER	Unaligned Packet Encoding Rules
URL	Uniform Resource Locator
UTC	Universal Coordinated Time
V2V	Vehicle to Vehicle
V2V-SE	Vehicle-to-Vehicle Systems Engineering and Vehicle Integration Research for Deployment (Project)
V2X	Vehicle to X
VOD	Verify on Demand
VSA	Vendor Specific Action
VSC-A	Vehicle Safety Communication - Applications
VSC4	Vehicle Safety Communications 4 (Consortium)
WAAS	Wide Area Augmentation System
WAVE	Wireless Access in Vehicular Environments
WGS	World Geodetic System
WME	WAVE Management Entity
WSM	WAVE Short Message
WSA	WAVE Service Advertisement
WSMP	WAVE Short Message Protocol

3.3 Requirement Numbering Convention

Each requirement in this standard is tagged with a requirement number of the form:

<Subsection Number>-V2V-< Category Abbreviation>-<Subcategory Abbreviation>-<Number>

For example, if the requirement number is 6.5.2-V2V-SECPRIV-BSMSIGN-005, the subsection is 6.5.2, the category is Security and Privacy Transmit (Tx), the subcategory is BSM signing, and it is requirement number 5 in the subcategory. Table 1 identifies the sections in this standard and the corresponding subsections and abbreviations that are used. The abbreviation is also in parentheses following each section heading in this standard. The requirement numbering convention applies to both mandatory and optional features.

Table 1: Requirement Numbering Abbreviations

Section	Subsection	Category	Category Abbreviation	Subcategory	Subcategory Abbreviation
6.1	6.1.1	Standards Compliance	STD	IEEE 802.11	802.11
	6.1.2			IEEE 1609.2	1609.2
	6.1.3			IEEE 1609.3	1609.3
	6.1.4			IEEE 1609.4	1609.4
	6.1.5			IEEE 1609.12	1609.12
	6.1.6			SAE J2735	J2735
6.2	6.2.1	Positioning and Timing	POSTIM	Position Determination	POSDETER
	6.2.2			Wide Area Augmentation System	WAAS
	6.2.3			Coordinate System and Reference	COORDSYSREF
	6.2.4			System Time Coordination	SYSTIMCOORD
6.3	6.3.1	BSM Transmission	BSMTX	BSM Contents	BSMCONT
	6.3.2			Channel and Data Rate	CHDATARATE
	6.3.3			Transmit Timing	TXTIM
	6.3.4			User Priority and EDCA Settings	UPEDCA
	6.3.5			Minimum Transmission Criteria	MINTX
	6.3.6			Data Element Accuracy	DATAACC
	6.3.7			Data Persistency	DATAPERSIST
	6.3.8			Congestion Control	CONGCTRL
6.4	6.4.1	RF Performance Requirements	RFPERF	DSRC Transmit Power Accuracy and Radiated Transmit Power	DSRCTX
	6.4.2			DSRC Receive Sensitivity	DSRCRXSENS
	6.4.3			DSRC Antenna Polarization	DSRCPOL
6.5	6.5.1	Security and Privacy Tx	SECPRIV	ID Randomization	IDRAND
	6.5.2			BSM Signing	BSMSIGN
	6.5.3			BSM Verification	BSMVERIFY

Section	Subsection	Category	Category Abbreviation	Subcategory	Subcategory Abbreviation
	6.5.4			Certificate Change	CERTCHG
	6.5.5			Certificate Revocation	CERTREV
6.6	6.6.1	Security Management	SECMGMT	Bootstrap: Enrollment and Initialization Processing	ENINIT
	6.6.2			Certificate Loading	CERTLOAD
	6.6.3			Certificate Storage	CERTSTORE
	6.6.4			CRL Loading	CRLLOAD
	6.6.5			Secure Hardware	SECHW

4. V2V SAFETY SYSTEMS CONCEPT OF OPERATIONS AND SYSTEM DESCRIPTION

This section provides a high-level description of the V2V safety systems concept of operations and system description. Section 4.1 provides an overview of the V2V system, Section 4.2 provides the system description for V2V safety features, Section 4.3 provides the over-the-air interface description for V2V safety features, and Section 4.4 provides a reference to the objective test procedures for V2V safety features.

4.1 V2V System Overview

V2V safety communications are designed to exchange basic safety information among vehicles for driver assistance by supporting detection of imminent crash threats and alerting the driver. V2V communications use Dedicated Short Range Communications (DSRC) radios to transmit BSMs, including vehicle position, speed, heading, brake status, and other information, and receive the same information from other vehicles within communication range. Onboard safety applications use the information about the host vehicle (HV) and remote vehicles (RVs) to detect potential crash threats and alert the driver. Messages can be used for additional purposes, but only the scenarios described herein were used to develop this Standard. For the purposes of the crash scenarios described herein, the HV and RV terminology is used to identify which which vehicle is receiving and acting on BSMs (HV), and the set of vehicles from which BSMs are being received (RVs).

V2V communications can enable improved safety system effectiveness by complementing or providing an alternative to self-contained sensors such as radar, lidar, or camera systems. V2V communications provide the vehicle and driver with 360-degree awareness and can detect potential threats at a greater distance than other types of sensors as well detecting potential threats to some degree even under non-line-of-sight or low visibility conditions. This enables the driver to receive alerts earlier and have more time to take action to avoid crashes.

Because vehicles need to trust messages from each other, security is essential to protect messages from attacks such as spoofing, alteration, or replay that could cause false alerts or suppress true alerts. In addition, consumer privacy is protected appropriately, so the system does not disclose identifying information about the driver, or allow for easy tracking. All BSMs are sent with a signature that enables the receiving device to verify the validity of the message. Broadcast information that could potentially be used to identify and track drivers is anonymous and randomized, and other system security measures are also incorporated to protect privacy appropriately.

Figure 1 illustrates the V2V network components. An infrastructure-based Security Credential Management System (SCMS) is responsible for generating and delivering the security certificates that are used in the message verification process. The SCMS can also revoke certificates that cannot be trusted (e.g., the associated device may have been tampered with or is misbehaving) by placing them on a Certificate Revocation List (CRL) that the SCMS distributes to all systems. Section 6.6 in this standard describes the SCMS interface.

The V2V onboard equipment (OBE), which is the on-board vehicle-to-vehicle (V2V) safety communications system defined in this standard, typically consists of multiple subsystem components, which may be discrete or integrated depending on the implementation. Figure 1 illustrates the following subsystems within the system:

- DSRC radio – Supports the transmission and reception of BSMs. In this standard a DSRC radio subsystem is assumed to be a single-channel-at-a-time device. The OBE can include one or more DSRC radio subsystems and still comply with this standard.

- Global Navigation Satellite System (GNSS) receiver – The positioning subsystem that provides vehicle position, heading, speed, and time information. The system may be augmented with additional components, which are not shown in Figure 1. Examples of these are speed data from the CAN bus, dead reckoning and optical/camera based systems.

- OBE Control Processor Electronic Control Unit (ECU) – Executes software to support on-board system requirements including the transmission of BSMs.
- Antennas – Support radio frequency (RF) links for the DSRC radio and GNSS receiver. A second diversity antenna for the DSRC radio subsystem is recommended to improve performance.

Systems communicate amongst themselves using the DSRC radio subsystem as an interface. The OBE can interface to a Safety Application ECU that detects threats and issues alerts through a driver-vehicle interface (DVI). The DVI can provide visual, audio, and/or haptic alerts. The OBE can also interface with the vehicle Controller Area Network (CAN) bus to obtain vehicle dynamic and status information. The safety application ECU, CAN bus and DVI are outside the scope of this standard.

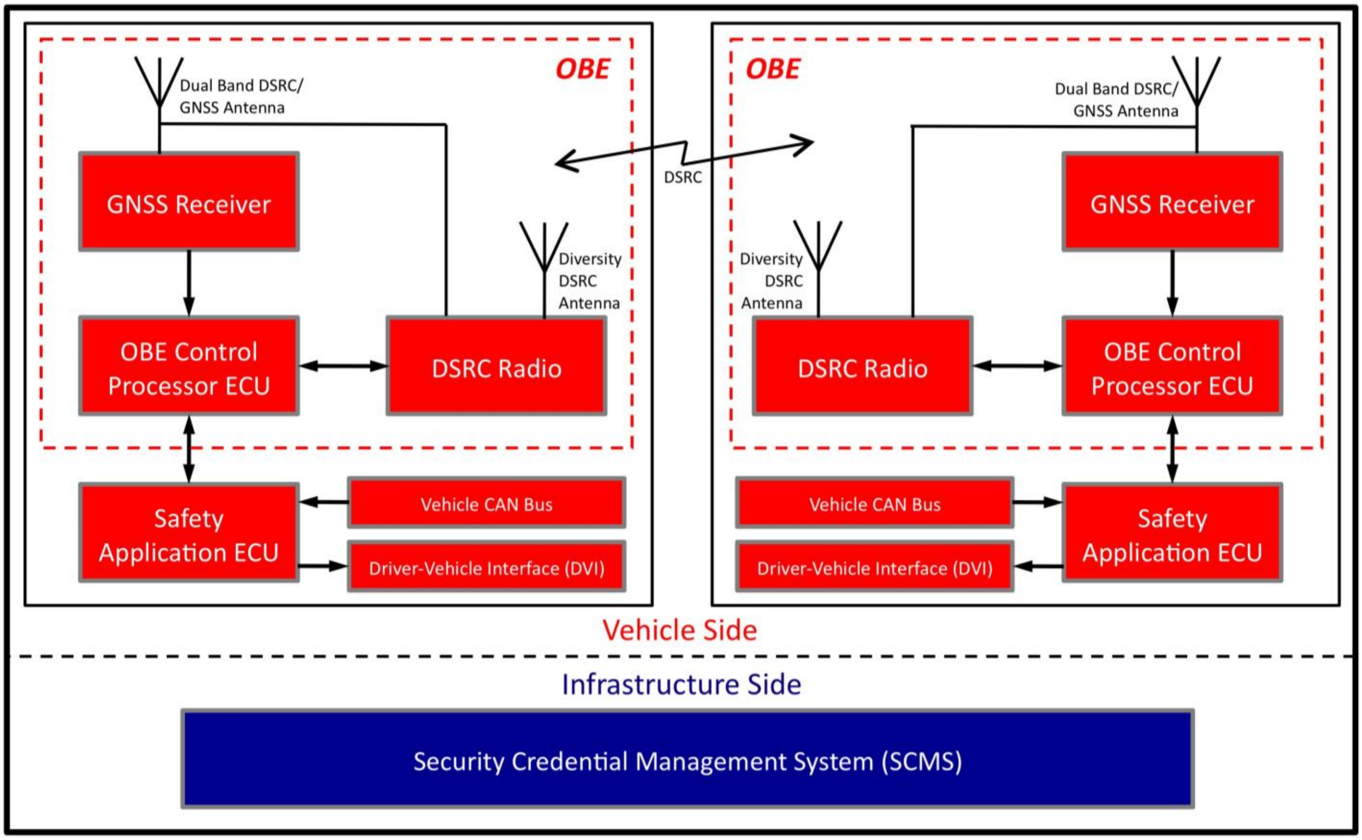

OBE
Dual Band DSRC/ GNSS Antenna
GNSS Receiver
Diversity DSRC Antenna
OBE Control Processor ECU
DSRC Radio
Safety Application ECU
Vehicle CAN Bus
Driver-Vehicle Interface (DVI)
DSRC
OBE
Dual Band DSRC/ GNSS Antenna
GNSS Receiver
Diversity DSRC Antenna
DSRC Radio
OBE Control Processor ECU
Vehicle CAN Bus
Driver-Vehicle Interface (DVI)
Safety Application ECU
Vehicle Side
Infrastructure Side
Security Credential Management System (SCMS)

Figure 1: V2V System

4.2 V2V Safety Features

4.2.1 Critical Crash Scenarios for V2V Safety

The set of crash scenarios that could be addressed by V2V safety communications were initially analyzed and documented in the Crash Avoidance Metrics Partnership (CAMP) Vehicle Safety Communications-Applications (VSC-A) project [11]. Table 2 lists the seven scenarios selected based on a composite ranking of crash frequency, crash cost, and functional years lost[2]. Scenario 7 was subsequently added to address left-turn-across-path intersection crashes during the CAMP VSC 3 driver acceptance clinics project [12].

Table 2: Selected crash-imminent scenarios

Crash Imminent Scenario	Crash Category		
	Frequency	**Cost**	**Functional Years Lost**
Lead Vehicle Stopped	✓	✓	✓
Control Loss without Prior Vehicle Action	✓	✓	✓
Vehicle(s) Turning at Non-Signalized Junctions	✓	✓	
Straight Crossing Paths at Non-Signalized Junctions			✓
Lead Vehicle Decelerating	✓	✓	
Vehicle(s) Changing Lanes – Same Direction	✓		
Left Turn Across Path – Opposite Direction			

✓ Denotes Top Five Ranking for the Crash Category

4.2.2 Mapping Between Critical Crash Scenarios and the Selection of V2V Safety Applications

In [11] and [12], V2V safety applications were developed to address the selected scenarios. Table 3 illustrates the mapping between the crash-imminent scenarios identified in Table 2 and the list of safety applications. These safety applications are defined and discussed in more detail below.

Table 3 Crash-imminent scenario to V2V safety application mapping

Safety Applications **Crash Scenarios**	**EEBL**	**FCW**	**BSW/LCW**	**IMA**	**LTA**	**CLW**
Lead Vehicle Stopped		✓				
Control Loss without Prior Vehicle Action						✓
Vehicle(s) Turning at Non-Signalized Junctions				✓	✓	
Straight Crossing Paths at Non-Signalized Junctions				✓		
Lead Vehicle Decelerating	✓	✓				
Vehicle(s) Changing Lanes – Same Direction			✓			
Left Turn Across Path – Opposite Direction					✓	

4.2.3 Emergency Electronic Brake Lights (EEBL)

4.2.3.1 Definition

The EEBL safety application warns the driver of the HV in the case of a hard-braking event, as defined in J2735 [6], by an RV that is ahead and in the same lane or an adjacent lane. The RV broadcasts a hard-braking event in the BSM upon a hard braking maneuver. Upon receiving such event information, the HV determines the relevance of the event and provides a warning to the driver, if appropriate. Additional information on EEBL may be found in J2735 [6].

4.2.3.2 EEBL Use Case Scenario

a) EEBL: Abruptly Slowing RV (Figure 2)

[2] Functional years lost is a composite measure of crash severity. It measures the loss of an individual's productive time due to injuries sustained in a crash.

- The HV follows a moving RV-2, which in turn follows RV-1 that abruptly brakes hard. RV-2 may or may not be equipped with V2V communications, but RV-1 is equipped with V2V capability
- The HV receives a warning from the EEBL feature when RV-1 applies brakes and decelerates at a high rate.
- The timing of the warning is expected to be set such that the driver of the HV can avoid a rear-end crash with the vehicle (RV-2) in front.

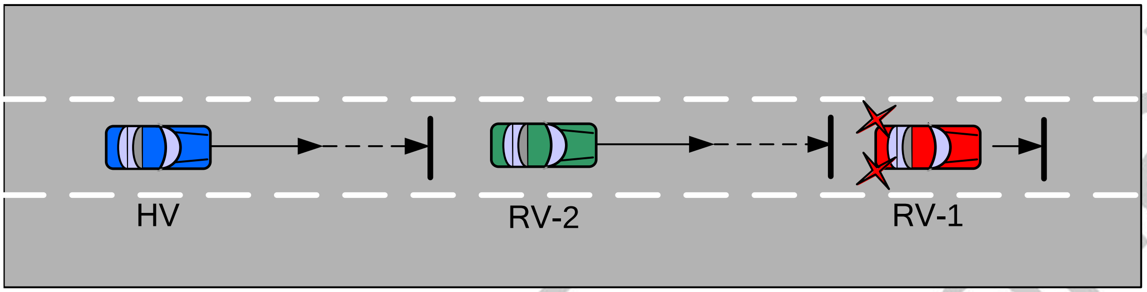


Figure 2: EEBL abruptly slowing RV

4.2.3.3 EEBL Feature Systems Description

The EEBL feature warns the driver of the HV in the case of an hard-braking event by an RV that is ahead and in the same lane or in an adjacent lane. The relevant RV zones for the EEBL feature are illustrated in Figure 3. The EEBL feature is expected to function in both straight and curved roadway geometries.

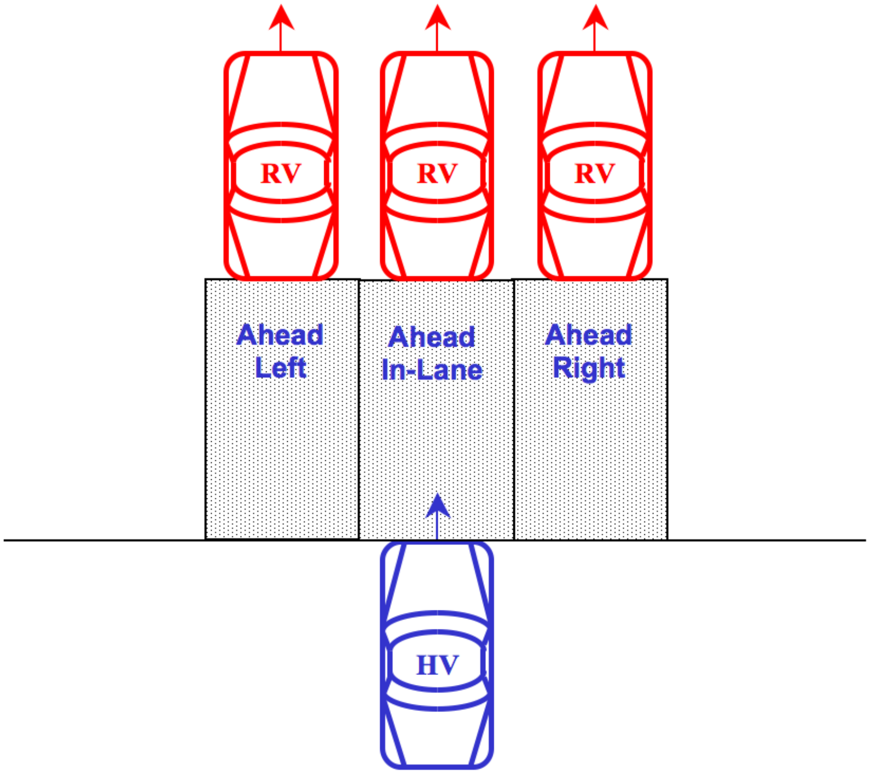


Figure 3: Relevant RV zones for the EEBL feature

EEBL performs the following operations:

- The RV includes an hard-braking event in the broadcasted BSM during a hard-braking maneuver.

Upon receiving such event information, the HV performs the following operations:

- Determines which, if any, RVs have reported a hard-braking event.
- For each RV that has reported a hard-braking event and is classified as “ahead in-lane,” “ahead left,” or “ahead right,” determines if the longitudinal range is less than a threshold value.
- Calculates the EEBL threat levels among all RVs identified above, determines the principal threat, and sets the appropriate threat status.
- Provides a warning to the driver via a DVI.

4.2.4 Forward Crash Warning (FCW)

4.2.4.1 Definition

The FCW safety application warns the driver of the HV in the case of an impending rear-end crash with an RV directly ahead in the same lane and direction of travel. The FCW is intended to help drivers avoid or mitigate rear-end vehicle crashes in the forward path of travel.

4.2.4.2 FCW Use Case Scenarios

a) FCW: Stopped RV in Same Lane (Figure 4)

- The HV approaches RV-1, which is stopped in the same lane as the HV.
- The HV receives a warning from the FCW feature when there is imminent danger of a rear-end crash with the stopped RV-1 in its lane of travel.
- The timing of the warning is expected to be set such that the driver of the HV can avoid a rear-end crash with the stopped RV-1.

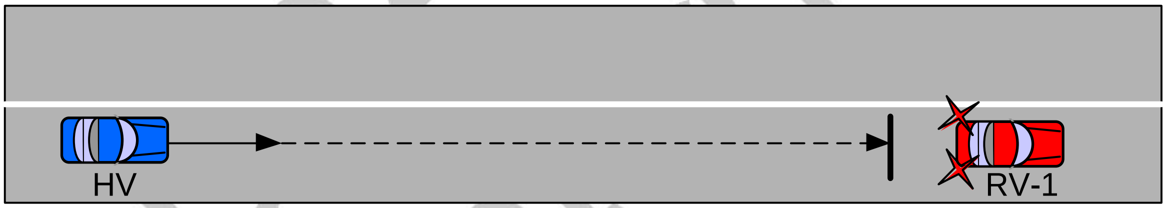


Figure 4: FCW stopped RV in same lane

b) FCW: Stopped RV in Adjacent Lane (Figure 5)

- The HV approaches RV-1, which is stopped in the lane adjacent to the HV.
- The driver of the HV does not receive a warning from the FCW feature since there is no imminent danger of a rear-end crash.

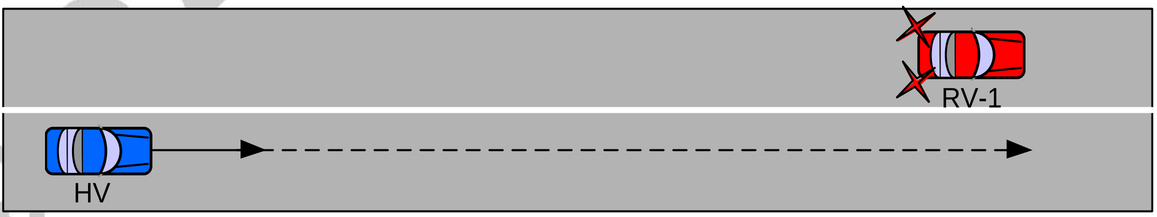


Figure 5: FCW stopped RV in adjacent lane

c) FCW: Slower-Moving or Decelerating RV in Same Lane (Figure 6)

- The HV approaches RV-1, which is moving slower and/or decelerating in the same lane as the HV.

- The HV driver receives a warning from the FCW feature when there is imminent danger of a rear-end crash with the slow-moving RV-1 in its lane of travel.
- The timing of the warning is expected to be set such that the driver can avoid a rear-end crash with the slow-moving RV-1.

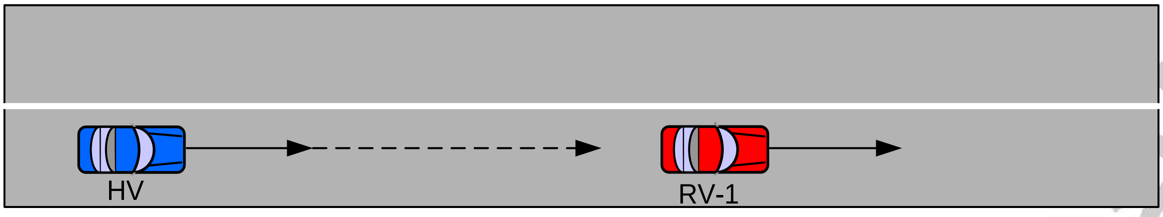


Figure 6: FCW slow-moving RV in same lane

d) FCW: Stopped and Obstructed RV (Figure 7)

- The HV follows a moving RV-2, which in turn approaches RV-1 that is stopped in the same lane. RV-2 may or may not be equipped with V2V communications, but RV-1 is equipped with V2V capability.
- RV-2 makes a lane change to avoid the stopped RV-1.
- The HV driver receives a warning from the FCW feature when there is imminent danger of a rear-end crash with the stopped RV-1 in its lane of travel.
- The timing of the warning is expected to be set such that the driver of the HV can avoid a rear-end crash with the stopped vehicle RV-1.

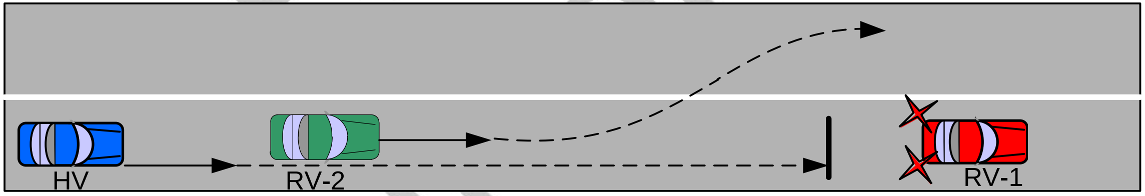


Figure 7: FCW stopped and Obstructed RV

4.2.4.3 FCW Feature Systems Description

The FCW warns the driver of the HV when there is imminent danger of a rear-end crash with a remote lead vehicle in its lane of travel. The FCW does not warn the driver of the HV when a remote lead vehicle is not in its lane of travel. The FCW feature is expected to function in straight and curved roadway geometries. The relevant RV zones for the FCW feature are illustrated in Figure 8.

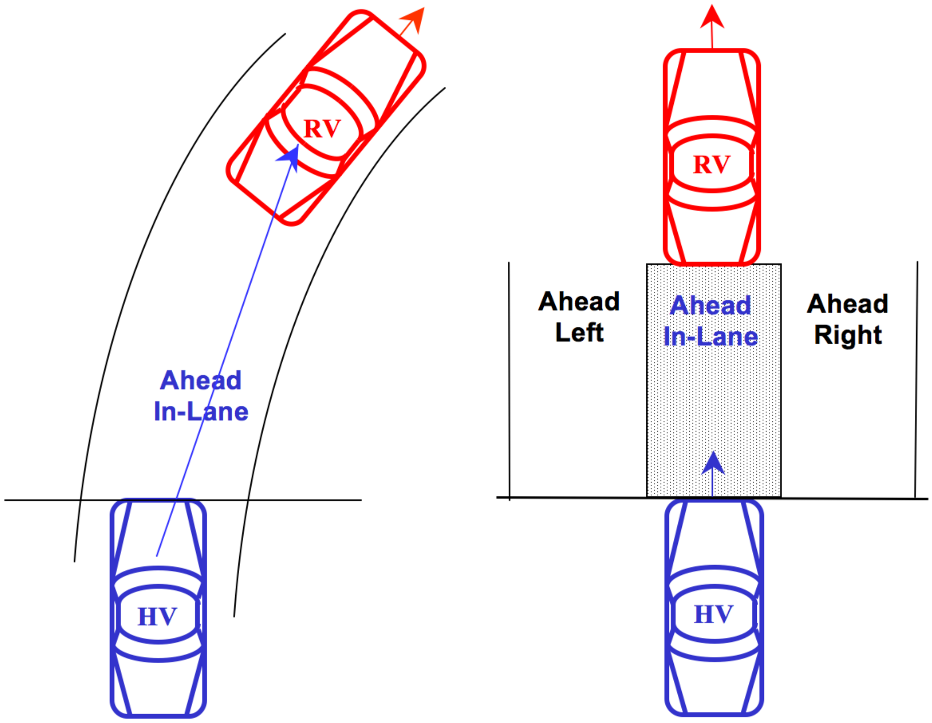


Figure 8: Relevant RV zones for FCW feature

FCW performs the following operations:

- Analyzes received BSMs from each of the RVs and determines which of the RVs are classified as “ahead in-lane” to determine if the HV is at risk of being involved in a rear-end crash with an RV located in the same lane of travel.
- Determines which, if any, RVs classified as “ahead in-lane” are within a longitudinal range threshold.
- Calculates time to crash (TTC) and/or crash avoidance range for each “ahead in-lane” RV to determine potential forward crash threats.
- Identifies the principal threat, if at least one RV is determined to be a threat.
- Provides a warning to the driver via a DVI.

4.2.5 Blind Spot Warning/Lane Change Warning (BSW/LCW)

4.2.5.1 Definition

The BSW/LCW safety application warns the driver of the HV during a lane change attempt if the blind-spot zone into which the HV intends to move into is, or will soon be, occupied by another vehicle traveling in the same direction. Moreover, the application may also provide advisory information that is intended to inform the driver of the HV that a vehicle in an adjacent lane is positioned in a blind-spot zone of the HV when a lane change is not being attempted.

4.2.5.2 BSW/LCW Use Case Scenarios

a) BSW: RV in blind-spot zone (Figure 9)

- The HV drives in its lane while RV-1 is alongside the HV within the blind-spot zone.
- The HV driver may receive an advisory warning from the BSW feature indicating the presence of RV-1 in the blind-spot zone.

- The HV driver receives a warning if the HV detects the driver's intent to change lanes into the lane occupied by RV-1 (for example through the use of the turn signal).
- The timing of the warning is expected to be set such that the driver of the HV can avoid a crash with RV-1 in the adjacent lane.

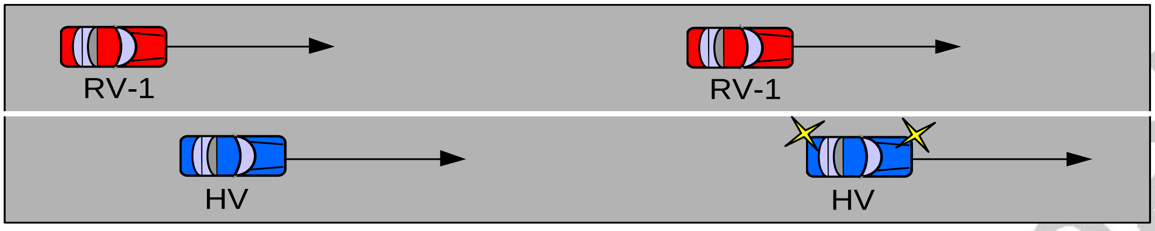


Figure 9: BSW RV in blind-spot zone

b) LCW: Approaching RV in adjacent lane (Figure 10)

- The HV drives in its lane. A faster moving RV-1 traveling in the same direction in an adjacent lane will soon occupy the HV's blind-spot zone.
- The HV driver may receive an advisory warning from the LCW feature anticipating the presence of RV-1 in the blind-spot zone.
- The HV driver receives a warning if the HV detects the driver's intent to change lanes into the lane that will soon be occupied by RV-1.
- The timing of the warning is expected to be set such that the driver of the HV can avoid a crash with a faster-moving RV-1 in the adjacent lane.

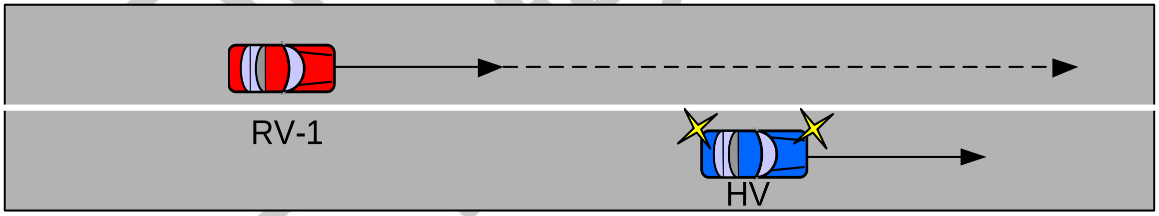


Figure 10: LCW approaching RV in adjacent lane

4.2.5.3 BSW/LCW Feature Systems Description

The BSW/LCW safety application warns the driver of the HV during an attempted lane change if the blind-spot zone into which the HV intends to move into is, or will soon be, occupied by another vehicle traveling in the same direction. The relevant RV zones to the BSW/LCW feature are illustrated in Figure 11. The BSW/LCW feature is expected to function in straight and curved roadway geometries.

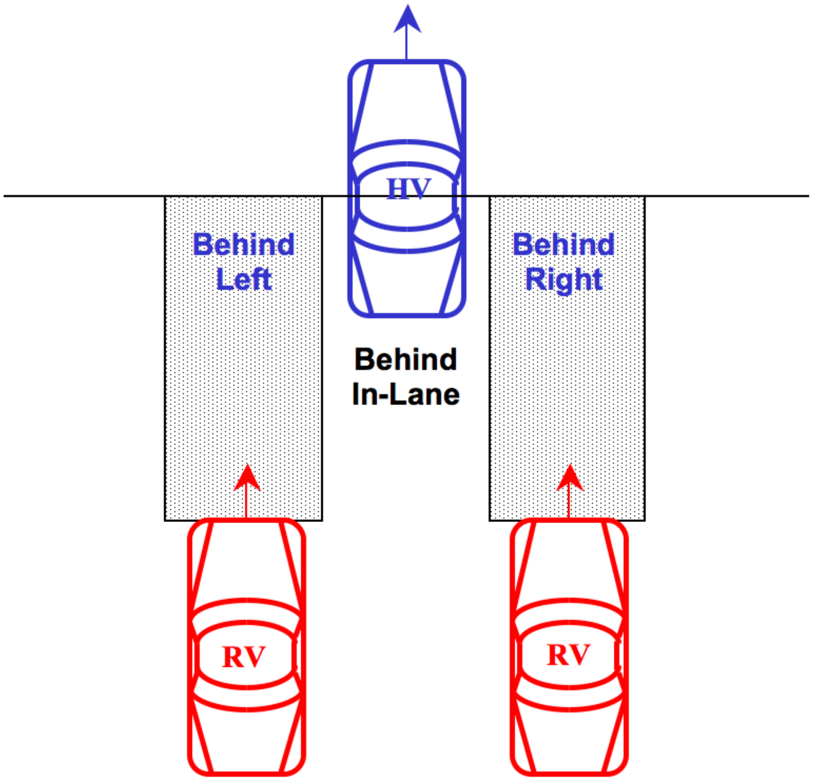


Figure 11: Relevant RV zones for BSW/LCW feature

BSW/LCW performs the following operations:

- Determines which RVs have been classified as behind in the adjacent left lane or behind in the adjacent right lane relative to the HV.
- Evaluates the position of each RV relative to the HV to determine if that RV is currently positioned within the HV’s blind-spot zone or if that RV is predicted to soon be within the HV’s blind-spot zone.
- Sets the threat status corresponding to each side (left and right) to advise the HV driver if an RV is or will be located in the corresponding left or right blind spot.
- Sets the threat status to warn the HV driver of the current or predicted presence of a threat in an adjacent lane during an attempted lane-change maneuver.
- Provides an advisory or warning to the driver via a DVI.

4.2.6 Intersection Movement Assist (IMA)

4.2.6.1 Definition

The IMA safety application warns the driver of an HV when it is not safe to enter an intersection due to a crash possibility with RVs.

4.2.6.2 IMA Use Case Scenarios

a) IMA: Stopped HV at Intersection (Figure 12)

- The HV is stopped at an intersection and visibility may be limited by the presence of RV-2. RV-2 may or may not be equipped with V2V communications, which has no impact on the scenario, but RV-1 is equipped with V2V capability.
- RV-1 approaches the intersection from the left or right of the HV.
- The HV driver receives a warning from the IMA feature indicating that a crash is predicted with RV-1 if the HV begins to enter the intersection.

- The timing of the warning is expected to be set such that the driver of the HV can avoid a crash with the approaching RV-1.

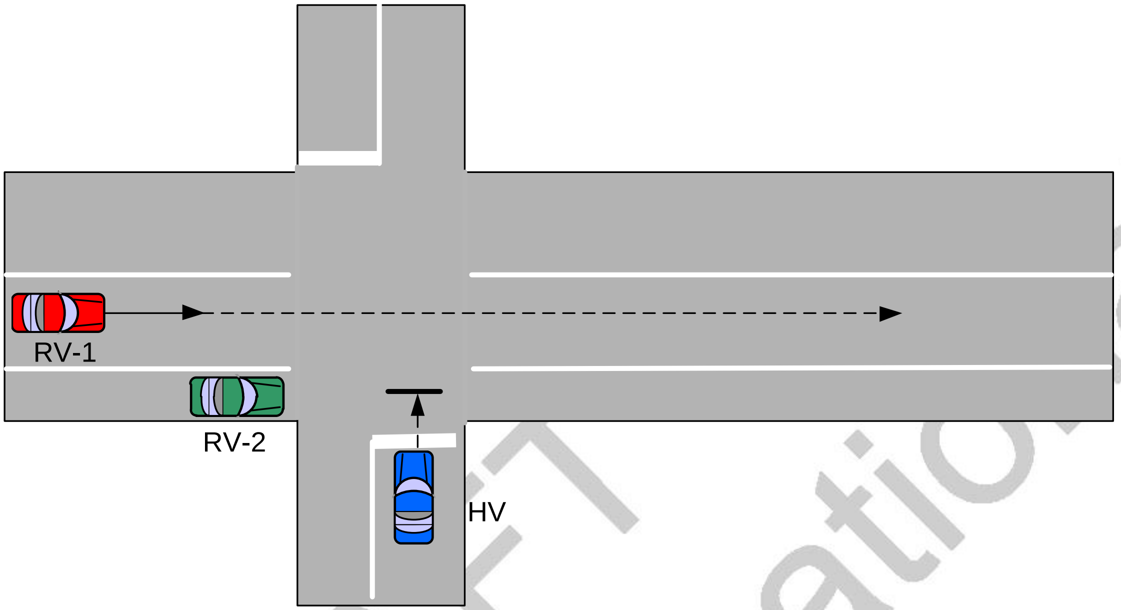


Figure 12: IMA stopped HV at the intersection

b) IMA: Both Vehicles Approaching Intersection (Figure 13)

- The HV approaches the intersection and visibility may be limited by the presence of RV-2. RV-2 may or may not be equipped with V2V communications, but RV-1 is equipped with V2V capability.
- RV-1 approaches the intersection from the left or right of the HV.
- The HV driver receives a warning from the IMA feature indicating that a conflict is predicted with RV-1 if the HV tries to enter the intersection.
- The timing of the warning is expected to be set such that the driver of the HV can avoid a crash with the approaching vehicle, RV-1.

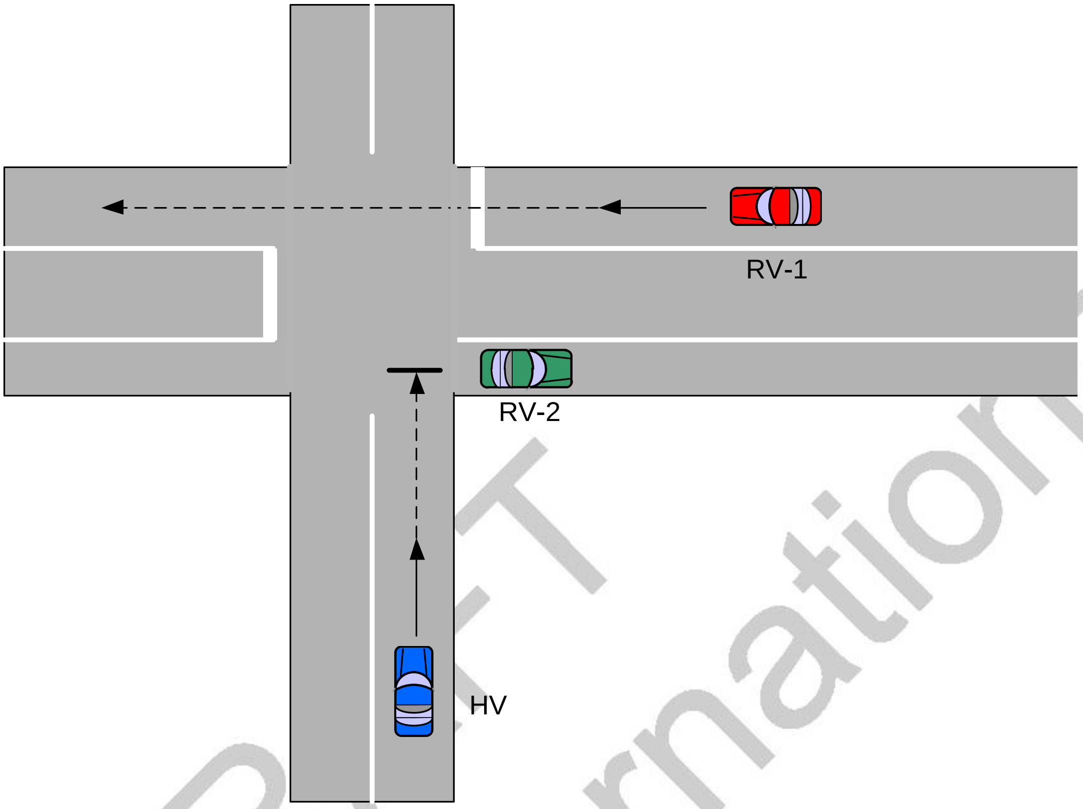


Figure 13: IMA both vehicles approaching intersection

4.2.6.3 IMA Feature Systems Description

IMA warns the driver of the HV when there is imminent danger of a crash with a remote vehicle that is approaching the same intersection. The relevant RV zones for the IMA feature are illustrated in Figure 14.

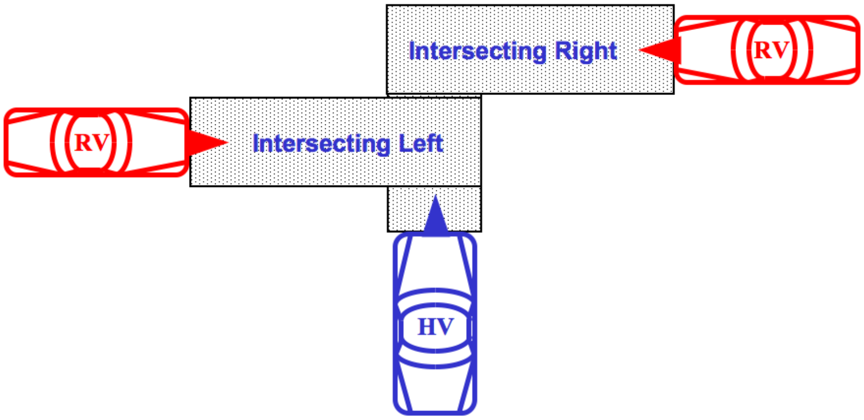


Figure 14: Relevant RV zones for IMA feature

IMA performs the following operations:

- Analyzes received BSMs from RVs approaching the intersection and determines which of the RVs are classified as “intersecting left” or “intersecting right.”

- Determines which, if any, RVs classified as “intersecting left” or “intersecting-right” are within a lateral range threshold.
- Calculates time-to-intersection (TTI) and distance-to-intersection (DTI) for each “intersecting left” or “intersecting right” RV to determine if the HV is at risk of being involved in a crash with an RV traveling toward the same intersection.
- Identifies the principal threat, if at least one RV is determined to be a threat.
- Provides a warning to the driver via a DVI.

4.2.7 Left Turn Assist (LTA)

4.2.7.1 Definition

The LTA safety application warns the driver of an HV that, due to oncoming traffic, it may not be safe to proceed when attempting a left turn.

4.2.7.2 LTA Use Case Scenarios

a) LTA: Left Turn Across Path (Figure 15)

- The HV approaches an intersection to make a left turn and visibility may be limited or obstructed by RV-2. RV-2 may or may not be equipped with V2V communications, but RV-1 is equipped with V2V capability.
- RV-1 approaches the intersection from the opposite direction.
- The HV driver receives a warning from the LTA feature when the HV driver attempts a left turn.
- The timing of the warning is expected to be set such that the driver of the HV can avoid a crash with the approaching vehicle, RV-1.

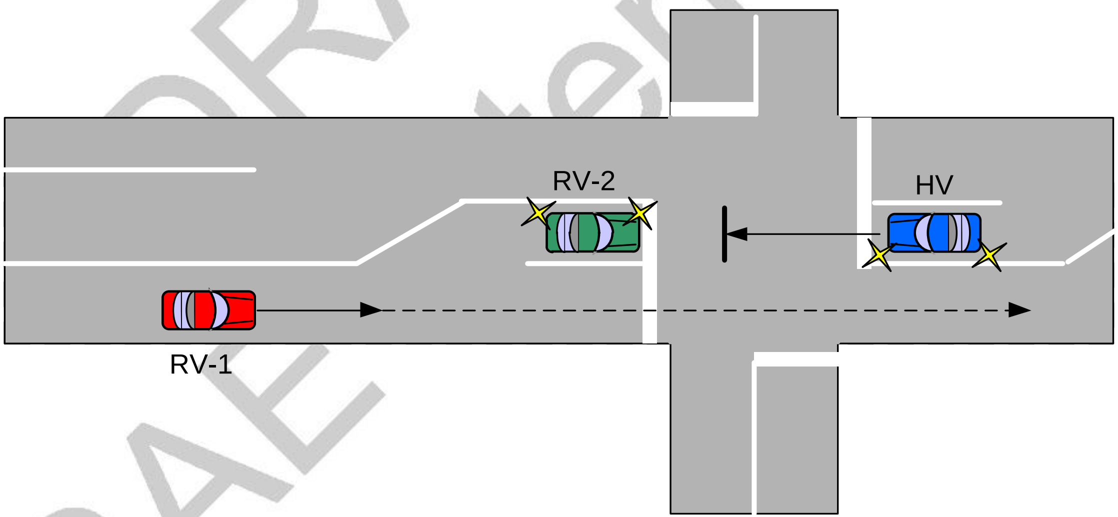


Figure 15: LTA left turn across path

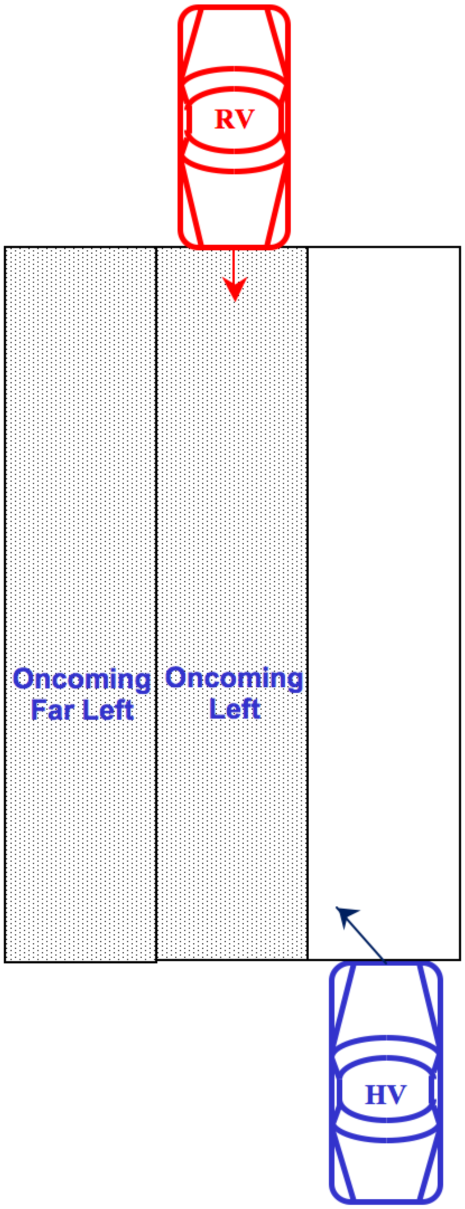


Figure 16: Relevant RV zones for LTA feature

4.2.7.3 LTA Feature Systems Description

LTA should warn a driver intending to make a left turn across an intersection path when there is imminent danger of a crash with an RV in an oncoming opposite lane of travel. The relevant RV zones for the LTA feature are illustrated in Figure 16.

LTA performs the following operations:

- Analyzes received BSMs from the RVs approaching the intersection and determines which of the RVs are classified as “oncoming left” or “oncoming far left” to determine if the HV is at risk of being involved in an intersecting crash with an RV approaching in an oncoming lane of travel.
- Determines which, if any, RVs classified as “oncoming left” or “oncoming far left” are within a longitudinal range threshold.
- Calculates the clearance gap for each “oncoming left” or “oncoming far left” RV to determine potential intersecting crash threats.

- Identifies the principal threat, if at least one RV is determined to be a threat.
- Provides a warning to the driver via a DVI.

4.2.8 Control Loss Warning (CLW)

4.2.8.1 Definition

The CLW safety application warns the driver of the HV in the case of an emergency control loss event (defined as activation of the Antilock Brake System, Traction Control System, or Stability Control System) by an RV traveling in the same or opposite direction. The RV broadcasts control loss event information within the BSM. Upon receiving such event information, the HV determines the relevance of the event and provides a warning to the driver of the HV.

4.2.8.2 CLW Use Case Scenarios

a) CLW: RV Same Direction of Travel (Figure 17)

- The HV follows the RV in the same direction.
- The HV receives BSMs from the RV indicating a control loss event (Antilock Brake System, Traction Control System or Stability Control System active).
- The timing of the corresponding warning to the driver is expected to be such that the driver of the HV can avoid a crash with the RV.

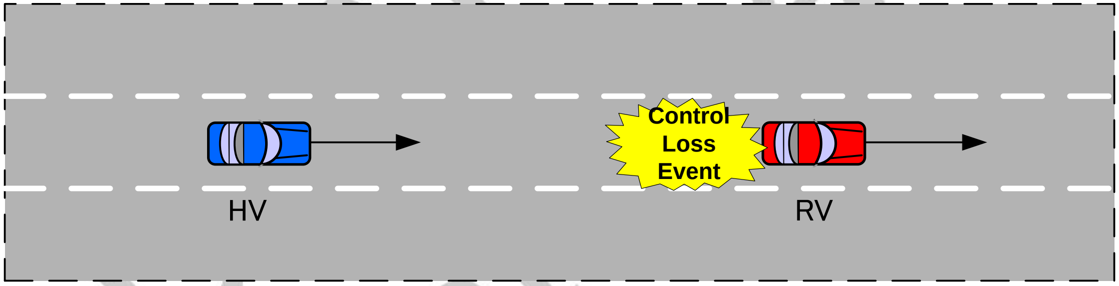


Figure 17: CLW RV same direction of travel

b) CLW: RV Travelling in Opposite Direction (Figure 18)

- The RV approaches the HV from the opposite direction.
- The HV receives BSMs from the oncoming RV indicating a control loss event (Antilock Brake System, Traction Control System or Stability Control System active).
- The timing of the corresponding warning to the driver is expected to be such that the driver of the HV can avoid a crash with the RV.

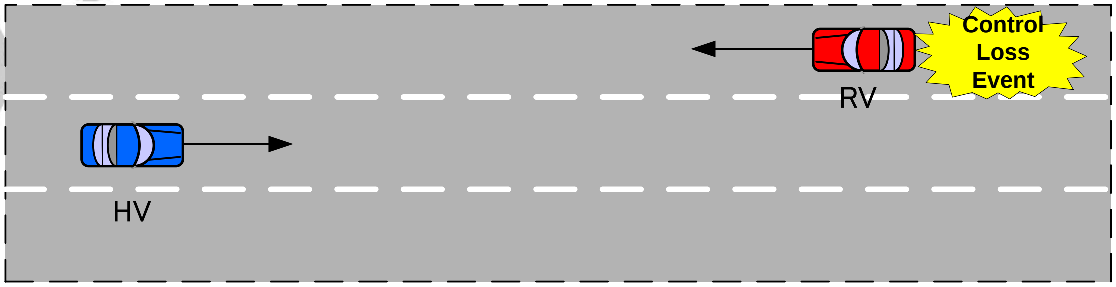


Figure 18: CLW RV traveling in opposite direction

4.2.8.3 CLW Feature Systems Description

The CLW safety application warns the driver of the HV in the case of an emergency control loss event by an RV traveling in the same or opposite direction. The relevant zones for the CLW features are illustrated in Figure 19.

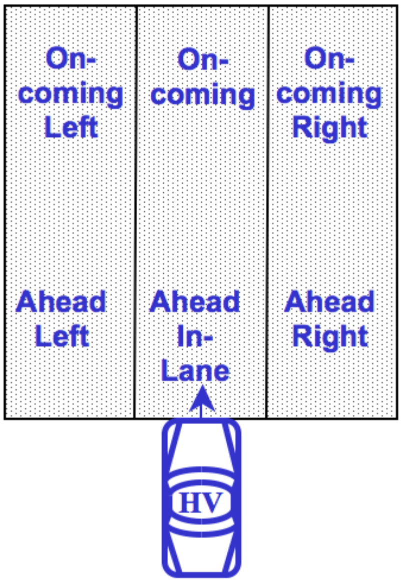


Figure 19: Relevant RV zones for CLW feature

CLW performs the following operations:

- The RV broadcasts a control loss event in the BSM upon activation of the Antilock Brake System, Traction Control System, or Stability Control System.

Upon receiving such event information, the HV performs the following operations:

- Determines which, if any, RVs have reported a control loss event.
- For each RV that has reported an event and is classified as “ahead in-lane,” “ahead left,” “ahead right,” “oncoming,” “oncoming left,” or “oncoming right,” determines if the longitudinal range or TTC is less than a threshold value.
- Calculates the CLW threat levels among all RVs identified above, determines the principal threat, and sets the appropriate threat status.
- Provides a warning to the driver via a DVI.

4.3 V2V Over-the-Air Data Description

4.3.1 Basic Safety Message Exchange

The BSM, which is defined in SAE J2735 **Error! Reference source not found.**, is the message used for V2V safety communications. Each vehicle periodically broadcasts a BSM to provide neighboring vehicles with trajectory and status information. The BSM consists of all data elements listed in Part I and selected data elements and data frames listed in Part II of the SAE J2735 standard. Part I contains the vehicle position, speed, heading, acceleration, transmission, steering-wheel angle, brake, and vehicle-size information.

For V2V safety communications, the following additional information is transmitted as part of the Part II Vehicle Safety Extension:

- Event Flags, which convey the sender's status with respect to safety-related events such as Antilock Brake System activation, Stability Control activation, hard braking, and airbag deployment.
- Path History, which provides a concise representation of the vehicle's recent movement. It consists of a sequence of positions selected to represent the vehicle's path within an allowable error.
- Path Prediction, which provides an estimate of the vehicle's future trajectory. The trajectory is represented as a radius of curvature.
- Exterior Lights, which provides the vehicle light status, including turn signals.

4.3.2 Positioning

Many V2V safety applications need relative lane-level positioning of the HV and RVs. For example, a safety application can determine if the HV and an RV are in the same lane. The V2V OBE includes a GNSS receiver to enable the system to determine its own position and accurate time. The OBE also maintains its own path history and calculates its path prediction. Each vehicle broadcasts its time-tagged position, heading, speed, and acceleration, plus its path history and path prediction in the BSM. Based on the HV and RV information, the V2V system can calculate the range, range-rate, difference in headings, and relative position between vehicles. The path history and path prediction information are used to estimate the relative lane positioning between the HV and RV.

4.3.3 Security and Privacy

To support trust in message exchange between vehicles, BSM signing and verification are performed using a public key digital signature algorithm. The transmitter computes a signature using an Elliptic Curve Digital Signature Algorithm (ECDSA) with a private key, and the receiver verifies the signature using the associated certificate.

Each BSM is transmitted with a signature and either a security certificate containing the public key or a digest (hash of the current security certificate). The certificate is transmitted periodically, and other BSMs are transmitted with a digest to reduce the overall message length. The receiver buffers recently received certificates and is able to identify the certificate corresponding to a received digest.

The receiver can verify every message or use a Verify on Demand (VOD) approach where only a subset of BSMs is verified. For example, the receiver may verify only BSMs containing information that would trigger an alert to the driver. Upon selecting a BSM for verification, if the BSM contains a security certificate, the receiver uses the public key in the certificate to perform the verification. If the BSM contains a digest, the receiver can use the digest to identify the corresponding buffered certificate for use in the verification.

The SCMS is responsible for generating and distributing security certificates. The SCMS is also responsible for generating and distributing a Certificate Revocation List (CRL), which contains a list of linkage information that all receiving devices can use to identify non-trustworthy certificates. Certificates and the CRL are stored within the OBE system, and are periodically updated by the SCMS. A transmitter does not send a BSM if its linkage information is on the CRL. If a receiver receives a BSM with linkage information on the CRL, the BSM is considered invalid. More information about the CRL is available in 1609.2 [2].

To protect privacy, the signing security certificate is changed after a variable length of time (for example every 5 minutes), and fields within the broadcast message that could be used to identify and track a vehicle are randomized whenever the certificate is changed. The SCMS is structured as a set of components, so the component generating the certificates has no knowledge of which certificates are used by a particular device. For a more detailed description of the SCMS and associated security system design and operation see [9] and [10].

4.3.4 Startup and Shutdown

To ensure performance, systems include additional capabilities related to device startup and shutdown. Systems store the last known heading and path history information on shutdown so they can be retrieved for use in BSMs upon the next device startup. Systems also randomize their transmission schedule upon startup to avoid repeated collisions of transmitted BSMs with those transmitted by other systems.

4.3.5 Mapping to the V2V Over-the-Air Data

A generic logic design of the safety features is shown by the flowchart in Figure 20. Table 4 provides a mapping to the V2V over-the-air data.

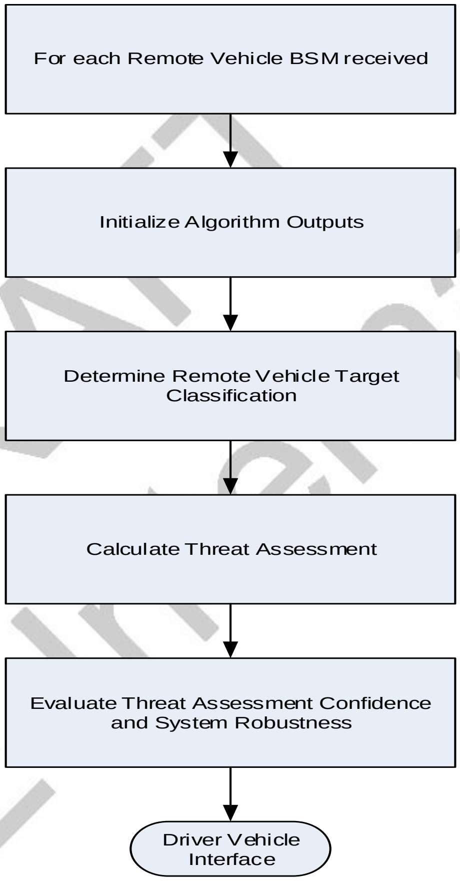

For each Remote Vehicle BSM received
Initialize Algorithm Outputs
Determine Remote Vehicle Target Classification
Calculate Threat Assessment
Evaluate Threat Assessment Confidence and System Robustness
Driver Vehicle Interface

Figure 20: Safety feature logic

Table 4: Mapping Crash Scenarios to the V2V Over-the-Air Data

V2V Safety Message BSM Contents (see J2735 [6])		FCW, BSW/LCW, IMA Stopped, LTA	EEBL, CLW, IMA Moving
DE_Dsecond DE_Latitude DE_Longitude DE_Elevation	Relative Road Level Positioning		Required for: • Relative Road Level Target Classification • Threat Assessment • Threat Assessment

V2V Safety Message BSM Contents (see J2735 [6])		FCW, BSW/LCW, IMA Stopped, LTA	EEBL, CLW, IMA Moving
DF_PositionalAccuracy DE_Heading			Confidence and System Robustness
	Relative Lane Level Positioning	Required for: • Relative Lane Level Target Classification • Threat Assessment • Threat Assessment Confidence and System Robustness	
DE_VehicleWidth DF_PathHistory DF_PathPrediction		Required for: • Relative Lane Level Target Classification	Required for: • Relative Road Level Target Classification
DE_Speed DE_TransmissionState DE_Acceleration (Longitudinal) DF_BrakeSystemStatus DE_ExteriorLights DE_VehicleLength		Required for: • Threat Assessment • Threat Assessment Confidence and System Robustness	Required for: • Threat Assessment • Threat Assessment Confidence and System Robustness
DE_SteeringWheelAngle DE_Acceleration (Lateral) DE_Acceleration (Vertical) DE_YawRate		Required for: • Threat Assessment Confidence and System Robustness	Required for: • Threat Assessment Confidence and System Robustness
DE_VehicleEventFlags			Required for (EEBL and CLW only): • Hard-Braking Event Notification • Control-Loss Event Notification

Note: The positioning and other related data (e.g. speed, heading) accuracy requirements in this standard are designed to meet the relative lane level positioning needs of the crash scenarios described in the preceeding sections. See 6.3.6.5 through 6.3.6.11.

4.4 Objective Tests Conducted for V2V Safety Applications (informative)

Details and results from testing for the crash scenarios described in this Standard can be found in the VSC-A final report, Appendices C-2 and C-3 [14]. Refer to the report for details.

5. INTERFACE DESCRIPTION

This section provides an overview of the vehicle interfaces. Section 6 provides the detailed requirements for these interfaces.

5.1 Vehicle to Vehicle Communications Interface

The system interfaces to other vehicles by transmitting and receiving BSMs.

- The format and contents of the BSM are compliant with SAE J2735 [6]
- The BSM is transmitted as a Wireless Access in Vehicular Environments (WAVE) Short Message (WSM) using the WAVE Short Message Protocol (WSMP) as defined in IEEE 1609.3 [3]
- BSM security is compliant with IEEE 1609.2 [2]
- The over-the-air Medium Access Control (MAC) and Physical Layer (PHY) protocol are compliant with IEEE 1609.4 [4] and IEEE 802.11 [1]
- The WSM Provider Service ID (PSID) is set as specified in IEEE 1609.12 [5]

Section 6.1 of this standard profiles the applicable requirements from each of these standards.

5.2 Vehicle to SCMS Communications Interface

The system interfaces to the SCMS to request security credential generation, download security credentials, and receive CRLs. The requirements listed in this standard are based on the following reports, which include dialogs and other SCMS interface details:

- CAMP Vehicle Safety Communications Security Studies: Study 1 – Security Credential Management System [10].
- CAMP Vehicle Safety Communications Security Studies: Study 3 Final Report: Protocols and Components of the SCMS [9].

Section 6.6 of this standard defines the applicable requirements for interfacing to the SCMS.

5.3 Vehicle to Positioning Subystem Interface

The system has access to positioning system information to meet the positioning and timing requirements of Section 6.2.

6. MINIMUM REQUIREMENTS

6.1 Standards Compliance (STD)

The Standards Compliance subsections below describe the requirements from the corresponding standards specifications necessary to support V2V operation. Additional requirements apply if the system optionally supports the SCMS interface via DSRC-equipped Roadside Equipment (RSE). If a clause from the referenced standard is not explicitly referenced below, then it and its sub-clauses are considered informative or optional and not required for either V2V or SCMS operation, unless they are implicitly referenced from one of the mandatory clauses of that referenced standard.

6.1.1 IEEE 802.11 (802.11)

This section specifies the requirements from IEEE 802.11 [1] to support V2V and SCMS operation, as described in Section 6.1. Items marked V2V are required, and items marked SCMS are additionally required only if interfacing to an SCMS over DSRC is implemented.

Table 5: IEEE 802.11 Requirements

802.11 Clause	Title (802.11 Clause)	Required For	Requirement
4.3.11	STA transmission of data frames outside the context of a BSS	V2V	The system shall operate within the procedures for STA transmission of data frames outside the context of a BSS (dot11OCBActivated=True), as specified. [6.1.1-V2V-STD-802.11-001]
5	MAC Service Definition		
5.1	Overview of MAC services	V2V	The system shall comply with MAC services with dot11OCBActivated equal to true, as specified. [6.1.1-V2V-STD-802.11-002]
5.2	MAC data service specification	V2V	The system shall comply with MAC data service specification features with dot11OCBActivated equal to true, as specified. [6.1.1-V2V-STD-802.11-003]
6	Layer Management		
6.3	MLME-SAP interface		Note: MLME-SAP primitives provide guidance when determining actual requirements. The system needs to include the specified functionality corresponding to each service primitive, but the method in which it is implemented may be implementation specific.
6.3.10, 6.5.2	Reset	V2V	The system shall be capable of changing the radio MAC address during operation [6.1.1-V2V-STD-802.11-004]
6.3.42	Get TSF timer	SCMS	The system should include the Get TSF timer feature to aid in enhanced time synchronization. Other methods may also be utilized for enhanced time synchronization. [6.1.1-V2V-STD-802.11-005]
7	PHY service specification		
7.1	Scope	V2V	The system should include the PHY service specification scope features with dot11OCBActivated equal to true, as specified. [6.1.1-V2V-STD-802.11-006]
7.2	PHY functions	V2V	The system should include the PHY functions with dot11OCBActivated equal to true, as specified. [6.1.1-V2V-STD-802.11-007]
7.3	Detailed PHY service specification	V2V	The system should include the detailed PHY services specifications with dot11OCBActivated equal to true, as specified. [6.1.1-V2V-STD-802.11-008]
8	Frame Formats		
8.1	General requirements	V2V	The system shall comply with the frame format general requirements with dot11OCBActivated equal to true, as specified. [6.1.1-V2V-STD-802.11-009]
8.2	MAC frame formats	V2V	The system shall comply with the MAC frame formats with dot11OCBActivated equal to true, as specified. [6.1.1-V2V-STD-802.11-010]
8.3	Format of individual frame types		
8.3.1	Control Frames		
8.3.1.1	Format of control frames	SCMS	The system shall comply with the control frame format with dot11OCBActivated equal to true, as specified. [6.1.1-V2V-STD-802.11-011]
8.3.1.4	ACK frame format	SCMS	The system shall comply with the ACK frame format with dot11OCBActivated equal to true, as specified. [6.1.1-V2V-STD-802.11-012]
8.3.2	Data Frames	V2V	The system shall comply with the data frame with dot11OCBActivated equal to true, as specified. [6.1.1-V2V-STD-802.11-013]

802.11 Clause	Title (802.11 Clause)	Required For	Requirement
8.3.2.1	Data Frame Format	V2V	The system shall set the data frame fields to the following values for V2V operation: Frame Control (bits) • Protocol version=00 • Type = 10 (Data) • Subtype = 1000 (QoS Data) • ToDS = 0 • FromDS = 0 • More Fragments = 0 • Retry = 0 • Power Mgmt = 0 • More Data = 0 • Protected Frame = 0 • Order = 0 Duration ID = 0 Address 1 (destination) = ff ff ff ff ff ff Address 2 (source) = <random 6 octets, changed per rules defined in Section 6.5.1> Address 3 (BSS ID) = ff ff ff ff ff ff Sequence Control • Fragment Number = 0 • Sequence Number = <incrementing value for each transmitted frame> Address 4 field is omitted QoS Control • TID (bits 0-3) = <User Priority (0-7)> • EOSP (bit 4)= 0 • Ack Policy: bit 5=1, bit 6=0 (No ACK) • A-MSDU Present (bit 7) = 0 • Tx Op Duration Req (bits 8-15) = 0 HT Control field is omitted Frame Body content is defined by the higher layers and shall not exceed 1500 octets FCS contains the 32-bit CRC of the MAC header and frame body field. [6.1.1-V2V-STD-802.11-014]
8.4.2.31	EDCA Parameter Set element	V2V	The system shall comply with the EDCA parameter set element, with the default EDCA values set as specified in Section 6.3.4 of this standard. [6.1.1-V2V-STD-802.11-015]

802.11 Clause	Title (802.11 Clause)	Required For	Requirement
9	MAC sublayer functional description		
9.2	MAC Architecture		
9.2.4	Hybrid Coordination Function	V2V	The system shall comply with the Enhanced Distributed Channel Access (EDCA) mechanism of the Hybrid Coordination Function (HCF) with dot11OCBActivated equal to true, as specified. [6.1.1-V2V-STD-802.11-016]
9.7	Multirate support	V2V	The system shall comply with the multirate support feature with dot11OCBActivated equal to true, as specified. [6.1.1-V2V-STD-802.11-017]
9.19	HCF		
9.19.1	General	V2V	The system shall comply with the HCF general features with dot11OCBActivated equal to true, as specified. [6.1.1-V2V-STD-802.11-018]
9.19.2	HCF contention-based channel access (EDCA)	V2V	The system shall comply with the HCF contention-based channel access (EDCA) features with dot11OCBActivated equal to true, as specified. [6.1.1-V2V-STD-802.11-019]
10	MLME		
10.1	Synchronization	V2V	The system shall comply with the MLME synchronization feature with dot11OCBActivated equal to true, as specified. [6.1.1-V2V-STD-802.11-020]
10.20	STAs communicating data frames outside the context of a BSS	V2V	The system shall comply with the protocol of STAs communicating data frames outside the context of a BSS, with dot11OCBActivated equal to true, as specified. [6.1.1-V2V-STD-802.11-021]
18	Orthogonal frequency division multiplexing (OFDM) PHY specification	V2V	The system shall comply with the orthogonal frequency division multiplexing (OFDM) PHY specification with dot11OCBActivated equal to true, as specified. [6.1.1-V2V-STD-802.11-022]
Annex C	ASN.1 encoding of the MAC and PHY MIB	V2V	The system shall include the MIB items used to support OFDM and the features with dot11OCBActivated equal to true, as specified. [6.1.1-V2V-STD-802.11-024]
Annex D	Regulatory references		
Annex D.1	External regulatory references	V2V	The system shall comply with the United States Federal Communications Commission (FCC) specifications, as specified. [6.1.1-V2V-STD-802.11-025]
Annex D.1	External regulatory references	V2V	The system shall comply with the behavior limits set for ITS_mobile_operations, as specified. [6.1.1-V2V-STD-802.11-026]
Annex D2.1	Transmit and receive in-band and out-of-band spurious emissions	V2V	The system shall comply with transmit and receive in-band and out-of-band spurious emissions, as specified. [6.1.1-V2V-STD-802.11-027]
Annex D2.2	Transmit power levels	V2V	The system shall comply with the transmit power level requirements for STA transmit power classification C, as specified. [6.1.1-V2V-STD-802.11-028]
Annex D2.3	Transmit spectrum mask	V2V	The system shall comply with the transmit spectrum mask requirements for 10 MHz channel spacing for STA transmit power classification C, as specified. [6.1.1-V2V-STD-802.11-029]
Annex E	Country elements and operating classes		
Annex E.1	Country information and operating classes	V2V	The system shall comply with the country element and operating classes, as specified to support operating class 17, channel *vChannelNumber*. [6.1.1-V2V-STD-802.11-030]
Annex E.1	Country information and operating classes	SCMS	The system shall comply with the country element and operating classes, as specified to support operating class 17. [6.1.1-V2V-STD-802.11-031]

802.11 Clause	Title (802.11 Clause)	Required For	Requirement
Annex E.2.3	5.9 GHz band in the United States (5.850-5.925 GHz)	V2V	The system shall comply rules to support the 5.9 GHz band in the United States (5.850-5.925 GHz), as specified. [6.1.1-V2V-STD-802.11-032]

6.1.2 IEEE 1609.2 (1609.2)

This section specifies the requirements from IEEE 1609.2 [2] to support V2V and SCMS operation, as described in Section 6.1.

6.1.2.1 PICS Statement

Using the Protocol Implementation Conformance Statement (PICS) from IEEE 1609.2 [2] the profile for BSM transmissions on channel *vChannelNumber* is provided in this section. Items left blank in the support column are not identified for use by this standard and are left to the implementer. Items marked “Y” are required to be implemented, and items marked “N” shall not be used for BSM transmissions on channel *vChannelNumber.* Items marked “O” are optional. In some cases a value is specified, in which case the requirement is to comply with the noted value in the Support column.

6.1.2.1.1 Security Services

- The system shall comply with the following Security Services Items and all corresponding sub-items as noted in Table 6, with the exception of items marked optional:
  - Support 1609.2
  - SDEE Identification
  - Generate Secure Data

  [6.1.2-V2V-STD-1609.2-001]

Optional items may be implemented but are not required.

- When the system chooses to verify a received BSM, the system shall comply with the following Security Services Item and all corresponding sub-items as noted in Table 6, with the exception of items marked optional:
  - Received SPDU

  [6.1.2-V2V-STD-1609.2-002]

Optional items may be implemented but are not required.

Table 6: IEEE 1609.2 Security Services Profile

Item	Security configuration (top-level)	Reference	Status	Support
S1.	**Support 1609.2**		M	Y
S2.	**SDEE Identification**		S1:M	Y
S2.1.	Support only one SDEE	4.2.2.1	S2:C1	Choose one of these items
S2.2.	Provide unique SDEE Identifiers	4.2.2.1, 9.3.1, 9.3.2	S2:C1	

Item	Security configuration (top-level)	Reference	Status	Support
S2.3.	Distinguish between SDEEs by other means	4.2.2.1, 9.3.1, 9.3.2	S2:C1	
S3.	**Generate Secure Data**		S1:G1	Y
S3.1.	Create Ieee1609Dot2Data containing Unsecured Data	4.2.2.2.2	S3:G2	N
S3.2.	Create Ieee1609Dot2Data containing valid SignedData	4.2.2.2.3, 5.2, 5.4.1, 5.4.3, 5.4.7, 6.3.4, 6.3.9, 9.3.21	S3:G2	Y
S3.2.1.	Using a valid HashAlgorithm	6.3.5	S3.2:M	Y
S3.2.1.1.	Support signing with hash algorithm SHA-256	6.3.5	S3.2:M	Y
S3.2.1.2.	Support signing with hash algorithm other than SHA-256	6.3.5	S3.2:O	N
S3.2.2.	Containing a Signed Data payload	6.3.6	S3.2:M	Y
S3.2.2.1.	… with payload containing data	9.3.21	S3.2.2:G1	Y
S3.2.2.2.	… with payload containing extDataHash	9.3.21	S3.2.2: G1	N
S3.2.2.3.	… with generationTime in the security headers	6.3.9, 6.3.11	S3.2.2: O	Y
S3.2.2.4.	… with expiryTime in the security headers	6.3.9, 6.3.12	S3.2.2: O	N
S3.2.2.5.	… with generationLocation in the security headers	6.3.9, 6.3.13	S3.2.2: O	N
S3.2.2.6.	… with certLearningRequest in the security headers	6.3.9, 6.3.25	S3.2.2: O	O
S3.2.2.7.	… with missingCrlIdentifier in the security headers	6.3.9, 6.3.17	S3.2.2: O	O
S3.2.2.8.	… with encryptionKey in the security headers	6.3.9, 6.3.19	S3.2.2: O	N
S3.2.2.8.1.	… … With a PublicEncryptionKey	6.3.9, 6.3.19, 6.3.20	S3.2.2.8:G1	N
S3.2.2.8.2.	… … With a SymmetricEncryptionKey	6.3.9, 6.3.19, 6.3.21	S3.2.2.8:G1	N
S3.2.3.	Support a SignerIdentifier	6.3.24	S2.2:M	Y
S3.2.3.1.	… of type digest	6.3.26	S2.2.5:G1	Y
S3.2.3.2.	… of type certificate	6.4.2	S2.2.5:G1	Y
S3.2.3.2.1.	… … Maximum number of Certificates in the chain	5.1.2.2	S3.2.3.2 8:M > 8:O	1
S3.2.3.3.	… of type self	6.3.24	S2.2.5:G1	N
S3.2.4.	Support a Signature	6.3.28	S2.2:M	Y

Item	Security configuration (top-level)	Reference	Status	Support
S3.2.4.1.	… a ecdsa256Signature	6.3.29	S3.2.4:M	Y
S3.2.4.1.1.	… … with a x-only r value	6.3.31	S3.2.4.1:G1	Choose one of these Items
S3.2.4.1.2.	… … with a compressed r value	6.3.31	S3.2.4.1:G1	
S3.2.4.1.3.	… … with an uncompressed r value	6.3.31	S3.2.4.1:G1	Y
S3.2.5.	Ensure that certificate used to sign data is valid (part of a consistent chain, valid at the current time and location, hasn't been revoked)	5.2, 6.4.2	S3.2:M	Y
S3.2.5.1.	Ensure that the region is correct	6.4.8, 6.4.17	S3.2.5:O	Y
S3.2.5.1.1.	Support a circularRegion	6.4.17, 6.4.18	S3.2.5.1:G1	N
S3.2.5.1.2.	Support a rectangular region	6.4.17, 6.4.20	S3.2.5.1:G1	N
S3.2.5.1.2.1.	Maximum number of rectangularRegions supported	6.4.17, 6.4.20	S3.2.5.1.2 8:M > 8:O	N/A
S3.2.5.1.3.	Support a polygonalRegion	6.4.17, 6.4.21	S3.2.5.1:G1	N
S3.2.5.1.3.1.	Maximum number of points in a polygonalRegion	6.4.17, 6.4.21	S3.2.5.1.3 8:M > 8:O	N/A
S3.2.5.1.4.	Support identifiedRegion PLUS SUBREGION	6.4.17, 6.4.22	S3.2.5.1:G1	Y
S3.2.5.1.4.1.	Maximum number of identifiedRegions supported	6.4.17, 6.4.22	S3.2.5.1.4: 8:M > 8:O	Minimum of 3 **Note:** US, Canada, Mexico supported per IEEE 1609.2 [2].
S3.2.5.1.4.2.	Support IdentifiedRegion of type CountryOnly	6.4.22, 6.4.23	S3.2.5.1.4: G1	Y
S3.2.5.1.4.3.	Support IdentifiedRegion of type CountryAndRegions	6.4.22, 6.4.24	S3.2.5.1.4: G1	N
S3.2.5.1.4.4.	Support IdentifiedRegion of type CountryAndSubregions	6.4.22, 6.4.25	S3.2.5.1.4: G1	N
S3.2.5.2.	Ensure the certificate has the proper appPermissions	6.4.8, 6.4.28	S3.2.5:O	N
S3.2.5.2.1.	Maximum number of PsidSsp in the appPermissions sequence	6.4.8, 6.4.28	S3.2.5.2 8:M > 8:O	2
S3.2.6.	Ensure that key and certificate used to sign are a valid pair	5.4.7	S3.2:M	Y
S3.2.7.	Support signing with explicit certificates	6.4.6	S3.2.5:G1	N
S3.2.8.	Support signing with implicit certificates	5.4.2, 6.4.5	S3.2.5:G1	Y
S3.2.9.	Generate ECDSA keypairs using a high-quality random number generator	5.4.6	S3.2.4.1: M	Y

Item	Security configuration (top-level)	Reference	Status	Support
S3.3.	Create Ieee1609Dot2Data containing EncryptedData	4.2.2.2.4, 5.4.4, 6.3.32	S3:G2	N
S3.4.	Generate ECIES ephemeral keypairs using a high-quality random number generator	5.4.4, 5.4.5, 5.4.6	S4.3: M	N
S3.4.1.	Maximum number of recipients supported	6.3.32	S3.3 8:M > 8:O	
S3.4.2.	Containing PreSharedKeyRecipientInfo	6.3.33, 6.3.34	S3.4.1:G1	
S3.4.2.1.	Containing symmRecipientInfo	6.3.33, 6.3.35	S3.4.1:G1	
S3.4.2.2.	Containing certRecipientInfo	6.3.33, 6.3.36	S3.4.1:G1	
S3.4.2.3.	Containing signedDataRecipientInfo	6.3.33, 6.3.36	S3.4.1:G1	
S3.4.2.4.	Containing rekRecipientInfo	6.3.33, 6.3.36	S3.4.1:G1	
S3.4.3.	Support public-key encryption	6.3.38	S3.3:G1	
S3.4.3.1.	… using ECIES-256	6.3.38	S3.4.3:M	
S3.4.3.1.1.	Support encrypting to an uncompressed encryption key	9.3.23	S3.4.3.1:G1	
S3.4.3.1.2.	Support encrypting to a compressed encryption key	9.3.23	S3.4.3.1:G1	
S3.4.3.1.3.	Support encrypting to an encryption key included in an explicit cert	9.3.23	S3.4.3.1:G2	
S3.4.3.1.4.	Support encrypting to an encryption key included in an implicit cert	9.3.23	S3.4.3.1:G2	
S3.4.3.2.	… using a different algorithm introduced at a later date	9.3.23	S3.4.3:O	
S3.4.4.	Support symmetric encryption	6.3.40	S3.3:G1	
S3.4.4.1.	… using AES-128	5.4.8, 6.3.40	S3.4.4:M	
S3.4.4.2.	… using a different algorithm introduced at a later date	6.3.40	S3.4.4:O	
S4.	**Receive SPDU**		S1:G1	Y
S4.1.	Support preprocessing SPDUs	4.2.2.3.1	S4:O S4.2.3.1:M S6.1:M	Y
S4.2.	Verify Ieee1609Dot2Data containing SignedData	4.2.2.2.3, 5.2, 5.4.1, 5.4.3, 5.4.7, 6.3.4, 6.3.9, 9.3.21	S4:G1	Y
S4.2.1.	Using a valid HashAlgorithm		S4.2:M	Y
S4.2.1.1.	Verify signed data using HashAlgorithm SHA-256	6.3.5	S4.2.1:M	Y

Item	Security configuration (top-level)	Reference	Status	Support
S4.2.1.2.	Verify signed data using a HashAlgorithm other than SHA-256	6.3.5	S4.2.1:O	N
S4.2.2.	Containing a Signed Data payload	6.3.6	S4.2:M	Y
S4.2.2.1.	… with payload containing data	9.3.21	S4.2.2:G1	Y
S4.2.2.2.	… with payload containing extDataHash	9.3.21	S4.2.2:G1	N
S4.2.2.3.	… with generationTime in the security headers	6.3.9, 6.3.11	S4.2.2:O	Y
S4.2.2.4.	… with expiryTime in the security headers	6.3.9, 6.3.12	S4.2.2:O	N
S4.2.2.5.	… with generationLocation in the security headers	6.3.9, 6.3.13	S4.2.2:O	N
S4.2.2.6.	… with missingCertIdentifier in the security headers	6.3.9, 6.3.25	S4.2.2:O	O
S4.2.2.7.	… with missingCrlIdentifier in the security headers	6.3.9, 6.3.17	S4.2.2:O	O
S4.2.2.8.	… with encryptionKey in the security headers	6.3.9, 6.3.19	S4.2.2:O	N
S4.2.2.8.1.	… … With a PublicEncryptionKey	6.3.9, 6.3.19, 6.3.20	S4.2.2.8:G1	N
S4.2.2.8.2.	… … With a SymmetricEncryptionKey	6.3.9, 6.3.19, 6.3.21	S4.2.2.8:G1	N
S4.2.3.	Support a SignerIdentifier	6.3.24	S4.2:M	Y
S4.2.3.1.	… of type digest	6.3.26	S4.2.3:G1	Y
S4.2.3.2.	… of type certificate	6.4.2	S4.2.3:G1	Y
S4.2.3.2.1.	… … Maximum number of Certificates in the chain	5.1.2.2	S4.2.3.2 1:M > 1:O	1
S4.2.3.3.	… of type self		S4.2.3:G1	N
S4.2.4.	Support a Signature	6.3.28	S4.2:M	Y
S4.2.4.1.	… a ecdsa256Signature	6.3.29	S4.2.4:M	Y
S4.2.4.1.1.	… … with a x-only r value	6.3.31	S4.2.4.1:G1	Y
S4.2.4.1.2.	… … with a compressed r value	6.3.31	S4.2.4.1:G1	Y
S4.2.4.1.3.	… … with a compressed r value and fast verification	6.3.31	S4.2.4.1:G1	O
S4.2.4.1.4.	… … with a uncompressed r value	6.3.31	S4.2.4.1:G1	N
S4.2.4.1.5.	… … with a uncompressed r value and fast verification	6.3.31	S4.2.4.1:G1	N
S4.2.5.	SignedData verification fails if the certificate is not valid (part of a consistent chain, valid at the current time and location, hasn't been revoked)	**5.2, 6.4.2**	S4.2:M	Y

Item	Security configuration (top-level)	Reference	Status	Support
S4.2.5.1.	Reject data based on generation location being inconsistent with certificate	6.4.8, 6.4.17	S4.2.5:O	Y **Note:** the position information comes from the BSM payload.
S4.2.5.1.1.	… using a circularRegion	6.4.17, 6.4.18	S4.2.5.1:G1	N
S4.2.5.1.2.	Support a rectangular region	6.4.17, 6.4.20	S4.2.5.1:G1	N
S4.2.5.1.3.	Maximum number of rectangularRegions supported	6.4.17, 6.4.20	S4.2.5.1.2 8:M > 8:O	N/A
S4.2.5.1.4.	Support a polygonalRegion	6.4.17, 6.4.21	S4.2.5.1:G1	N
S4.2.5.1.5.	Maximum number of points in a polygonalRegion	6.4.17, 6.4.21	S4.2.5.1.4 8:G1 > 8:O	N
S4.2.5.1.6.	Support identifiedRegion	6.4.17, 6.4.22	S4.2.5.1 8:G1 > 8:O	Y
S4.2.5.1.6.1.	Maximum number of identifiedRegions supported	6.4.17, 6.4.22	S4.2.5.1.6: 8:M > 8:O	Minimum of 3
S4.2.5.1.6.2.	Support IdentifiedRegion of type CountryOnly	6.4.22, 6.4.23	S4.2.5.1.6:G1	Y
S4.2.5.1.6.3.	Support IdentifiedRegion of type CountryAndRegions	6.4.22, 6.4.24	S4.2.5.1.6:G1	Y
S4.2.5.1.6.4.	Support IdentifiedRegion of type CountryAndSubregions	6.4.22, 6.4.25	S4.2.5.1.6:G1	N
S4.2.5.1.7.	Maximum number of identifiedRegions supported	6.4.17, 6.4.22	S4.2.5.1.6 8:G1 > 8:O	N
S4.2.5.2.	Reject data if the certificate does not have the proper appPermissions	6.4.8, 6.4.28	S4.2.5:O	Y
S4.2.5.3.	Maximum number of PsidSsp in the appPermissions sequence	6.4.8, 6.4.28	S4.2.5 8:O > 8:O	Minimum of 2
S4.2.5.4.	Ensure that the assuranceLevel is an acceptable level	6.4.8, 6.4.27	S4.2.5:O	N
S4.2.6.	Support verifying SPDUs signed with explicit authorization certificates	6.4.5, 9.3.27	S4.2:G1	N
S4.2.7.	Support verifying SPDUs signed with implicit authorization certificates	5.4.2, 6.4.5, 9.3.27	S4.2:G1	Y
S4.2.8.	Support explicit CA certificates	6.4.2, 6.4.6, 9.3.27	S4.2:M	Y
S4.2.9.	Support receiving implicit CA certificates	6.4.2, 6.4.5, 9.3.27	S4.2:O	N
S4.2.10.	SignedData verification fails in the following circumstances:	9.3.28	S4.2:M	Y
S4.2.10.1.	… SPDU-Parsing: Invalid Input	9.3.28	S4.2.10:M	Y

Item	Security configuration (top-level)	Reference	Status	Support
S4.2.10.2.	… SPDU-Parsing: Unspported critical information field	9.3.28	S4.2.10:M	Y
S4.2.10.3.	… SPDU-Parsing: Certifcate not found	9.3.28	S4.2.10:M	Y
S4.2.10.4.	… SPDU-Parsing:Generation time not available	9.3.28	S4.2.10:M	Y
S4.2.10.5.	… SPDU-Parsing:Generation location not available	9.3.28	S4.2.10:M	Y
S4.2.10.6.	… SPDU-Certificate-Chain: Not enough information to construct chain	9.3.28	S4.2.10:M	Y
S4.2.10.7.	… SPDU-Certificate-Chain: Chain ended at untrusted root	9.3.28	S4.2.10:M	Y
S4.2.10.8.	… SPDU-Certificate-Chain: Chain was too long for implementation	9.3.28	S4.2.10:M	Y
S4.2.10.9.	… SPDU-Certificate-Chain: Certificate revoked	9.3.28	S4.2.10:M	Y
S4.2.10.10.	… SPDU-Certificate-Chain: Overdue CRL	9.3.28	S4.2.10:M	Y
S4.2.10.11.	… SPDU-Certificate-Chain: Inconsistent expiry times	9.3.28	S4.2.10:M	Y
S4.2.10.12.	… SPDU-Certificate-Chain: Inconsistent start times	9.3.28	S4.2.10:M	Y
S4.2.10.13.	… SPDU-Certificate-Chain: Inconsistent chain permissions	9.3.28	S4.2.10:M	Y
S4.2.10.14.	… SPDU-Crypto: Verification failure	9.3.28	S4.2.10:M	Y
S4.2.10.15.	… SPDU-Consistency: Future certificate at generation time	9.3.28	S4.2.10:M	Y
S4.2.10.16.	… SPDU-Consistency: Expired certificate at generation time	9.3.28	S4.2.10:M	Y
S4.2.10.17.	… SPDU-Consistency: Expiry date too early	9.3.28	S4.2.10:M	Y
S4.2.10.18.	… SPDU-Consistency: Expiry date too late	9.3.28	S4.2.10:M	Y
S4.2.10.19.	… SPDU-Consistency: Generation location outside validity region	9.3.28	S4.2.10:M	Y
S4.2.10.20.	… SPDU-Consistency: Unauthorized PSID	9.3.28	S4.2.10:M	Y
S4.2.10.21.	… SPDU-Internal-Consistency: Expiry time before generation time	6.4.8, 6.4.14, 9.3.28	S4.2.10:M	Y
S4.2.10.22.	… SPDU-Internal-Consistency: extDataHash doesn’t match	9.3.28	S4.2.10:M	Y
S4.2.10.23.	… SPDU-Local-Consistency: PSIDs don’t match	9.3.28	S4.2.10:O	Y
S4.2.10.24.	… SPDU-Local-Consistency: Chain was too long for SDEE	9.3.28	S4.2.10:M	Y
S4.2.10.25.	… SPDU-Relevance: SPDU Too Old	9.3.28	S4.2.10:O	Y
S4.2.10.26.	… SPDU-Relevance: Future SPDU	9.3.28	S4.2.10:O	Y
S4.2.10.27.	… SPDU-Relevance: Expired SPDU	9.3.28	S4.2.10:O	N
S4.2.10.28.	… SPDU-Relevance: SPDU Too Distant	9.3.28	S4.2.10:O	N

Item	Security configuration (top-level)	Reference	Status	Support
S4.2.10.29.	… SPDU-Relevance: Replayed SPDU	9.3.28	S4.2.10:O	N
S4.3.	**Decrypt Ieee1609Dot2Data containing EncryptedData**	4.2.2.3.3, 5.4.5, 6.3.32,	S4:O1	N
S4.3.1.	Generate ECIES keypairs using a high-quality random number generator	5.4.4, 5.4.5, 5.4.6	S4.3: M	
S4.3.2.	Maximum number of RecipientInfos supported in an incoming EncryptedData	6.3.32	S4.3: 8:M > 8:O	
S4.3.2.1.	Containing symmRecipientInfo	6.3.33, 6.3.34	S4.3.2:G1	
S4.3.2.2.	Containing certRecipientInfo	6.3.33, 6.3.36	S4.3.2:G1	
S4.3.2.3.	Containing signedDataRecipientInfo	6.3.33, 6.3.36	S4.3.2:G1	
S4.3.2.4.	Containing rekRecipientInfo	6.3.33, 6.3.36	S4.3.2:G1	
S4.3.3.	Support decrypting using a public-key algorithm	6.3.38	S4.3:G1	
S4.3.3.1.	… using ECIES-256	6.3.38	S4.3.3:M	
S4.3.3.2.	… using a different algorithm introduced at a later date	6.3.38	S4.3.3:O	
S4.3.4.	Support decrypting using a symmetric algorithm	6.3.40	S4.3:G!	
S4.3.4.1.	.. using AES-128	6.3.40	S4.3.4:M	
S4.3.4.2.	… using a different algorithm introduced at a later date	6.3.40	S4.3.4:O	

6.1.2.1.2 CRL Exchange

- The system shall comply with CRL Exchange Items in Table 7, with the exception of items marked optional. [6.1.2-V2V-STD-1609.2-003]

Optional items may be implemented but are not required.

Table 7. IEEE 1609.2 CRL Exchange Profile

Item	Security configuration (top-level)	Reference	Status	Suppport
S5.	Support CRL exchange	7	O	Y
S5.1.	Correctly verify received CRL	7.3	O	Y
S5.1.1.	… of type fullHashCrl	**7.2**	S5.1:G1	Y
S5.1.2.	… of type deltaHashCrl	**7.2**	S5.1:O	O
S5.1.3.	… of type fullLinkedCrl	**7.2**	S5.1:G1	Y
S5.1.4.	… of type deltaLinkedCrl	**7.2**	S5.1:O	O
S5.1.5.	… containing individual linkage values	7.2.6	S5.1.2: G1 S5.1.4: G1	Y

S5.1.6.	… containing group linkage values	7.2.6	S5.1.2: G1 S5.1.4: G1	Y

6.1.2.1.3 Certificate Learning

All Certificate Learning items are optional.

- If Certificate Learning is implemented, the system shall comply with the requirements in Table 8. [6.1.2-V2V-STD-1609.2-004]

Table 8. IEEE 1609.2 Certificate Learning Profile

Item	Security configuration (top-level)	Reference	Status	Suppport
S6.	Support Certificate Learning	8	O	O
S6.1.	Support certificate learning in the requester role	8	S6:M	O
S6.2.	Support certificate learning in the responder role	8	S6:M	O
S6.3.	Number of supported SDEEs	8.7	S6: 1:O > 1:O	Minimum of 1
S6.4.	Number of supported instances of state variable *isResponseActive*	8.7	S6: 1:O > 1:O	Minimum of 1
S6.5.	Number of supported instances of state variable *isRequestActive*	8.7	S6: 1:O > 1:O	Minimum of 1
S6.6.	Number of supported instances of state variable *p2pcdResponseCount*	8.7	S6: 1:O > 1:O	Minimum of 1
S6.7.	Number of supported instances of state variable *queuedMissingCertIndicators*	8.7	S6: 1:O > 1:O	Minimum of 1
S6.8.	Number of supported instances of variables *recentlyUsedSigningCertificates*	8.7	S6: 1:O > 1:O	Minimum of 1
S6.9.	Number of supported instances of state variable *isResponseActive* for a single SDEE	8.7	S6: 1:O > 1:O	Minimum of 1
S6.10.	Number of supported instances of state variable *isRequestActive* for a single SDEE	8.7	S6: 1:O > 1:O	Minimum of 1
S6.11.	Number of supported instances of state variable *p2pcdResponseCount* for a single SDEE	8.7	S6: 1:O > 1:O	Minimum of 1
S6.12.	Number of supported instances of state variable *queuedMissingCertIndicators* for a single SDEE	8.7	S6: 1:O > 1:O	Minimum of 1
S6.13.	Number of supported instances of variables *recentlyUsedSigningCertificates* for a single SDEE	8.7	S6: 1:O > 1:O	Minimum of 1
S6.14.	Support certificate learning over WSMP with TPID = 0 or 1	8.6	O	O

6.1.2.2 BSM Security Profile Proforma

A Security Profile Proforma is provided in IEEE 1609.2 [2]. This profile is used to further state requirements for BSM transmissions on channel *vChannelNumber.* An example hexadecimal representation of the BSM based on this security profile and the corresponding ASN.1 is provided in Appendix A.9.

6.1.2.2.1 IEEE 1609.2 Security Profile Identification

- The system shall use the security profile identified in Table 9. [6.1.2-V2V-STD-1609.2-005]

Table 9. Security Profile Identification

Field	Value	Notes
Name	Security Profile for BSMs transmitted on channel *vChannelNumber* for light vehicles	
PSIDs	0x20	
Other considerations	This security profile is to be used for BSMs transmitted on channel *vChannelNumber*	

6.1.2.2.2 Sending

- The system shall use the security profile for sending defined in Table 10 [6.1.2-V2V-STD-1609.2-006]

Table 10. Security Profile for Transmitting BSMs

Field	Value	Notes
Sign Data	True	All BSMs are signed
Signed Data In Payload	True	BSM data is encapsulated in the signed data
External Data	False	No additional data is signed
External Data Source	False	
External Data Hash Algorithm	False	
Set Generation Time In Security Headers	True	Prevents replay attacks
Set Generation Location In Security Headers	False	Not necessary, already included in BSM
Set Expiry Time In Security Headers	False	Not necessary, application discards old messages
Signed SPDU Lifetime	N/A	
Signer Identifier Policy Type	Simple	See IEEE 1609.2 [2]
Simple Signer Identifier Policy: Minimum Inter - Cert Time	vMaxCertDigestInterval	Attach certificates at a rate of 1/vMaxCertDigestInterval
Simple Signer Identifier Policy: Exceptions	True	Use full certificate when an event flag in DE_VehicleEventFlags is set.
Simple Signer Identifier Policy: Signer Identifier Cert Chain Length	1	When sending certificates, send only the BSM signer certificate and not the CA certificates.
Text Signer Identifier Policy	N/A	
Sign With Fast Verification	Optional	Doesn't change signature
EC Point Format	Compressed	Reduces packet size. See IEEE 1609.2 [2]
Use Peer To Peer Cert Distribution	Optional	Items indented in the rows below only apply if this option is implemented.
p2pcd_maxResponseBackoff	*vP2pcd_maxResponseBackoff*	Wait no more than *p2pcd_maxResponseBackoff*seconds before deciding to send a response
p2pcd_responseActiveTimeout	*vP2pcd_responseActiveTimeout*	Send a response no more than 1/*vP2pcd_responseActiveTimeout* per second
p2pcd_requestActiveTimeout	*VP2pcd_requestActiveTimeout*	*VP2pcd_requestActiveTimeout*
p2pcd_currentlyUsedTriggerCertificateTime	*VP2pcd_currentlyUsedTriggerCertificateTime*	Response only to requests for certificates that have been used within the *VP2pcd_currentlyUsedTriggerCertificateTime*
p2pcd_responseCountThreshold	*vP2pcd_responseCountThreshold*	Respond only if fewer than *vP2pcd_responseCountThreshold* responses were seen during the backoff time
Repeat Signed SPDUs	False	Each BSM is uniquely signed before transmission
Time Between Signing	N/A	
Encrypt Data	False	Encryption is not used for BSMs

6.1.2.2.3 Receiving

- When the system chooses to verify a received BSM, it shall use the security profile for receiving defined in Table 11 [6.1.2-V2V-STD-1609.2-007]

Table 11. Security Profile for Receiving BSMs

Field	Value	Notes
Use Preprocessing	True	Store certificates even for messages that aren't being verified. Used to verify a digest.
Verify Data	True	
Maximum Certificate Chain Length	1	
Relevance: Replay	False	Application handles duplication within the Validity Period.
Relevance: Generation Time in Past	True	Guards against replay attacks.
Validity Period	30 seconds	Corresponds to the maximum value of +/-DE_DSecond/2
Rejection Threshold for Generation Time in Past	Default as recommended by 1609.2	See IEEE 1609.2 [ref]. Value assigned by 1609.2 is 0.5.
Relevance: Generation Time in Future	Yes	See IEEE 1609.2. Applies to messages newer than the Validity Period allows. Applications can filter messages inside the Validity Period.
Acceptable Future Data Period	30 seconds	Corresponds to +/- the maximum value of DE_DSecond/2
Rejection Threshold for Generation Time in Future	30 seconds	Corresponds to +/- the maximum value of DE_DSecond/2
Generation Time Source	Security headers	See IEEE 1609.2 [2]
Relevance: Expiry Time	False	
Rejection Threshold For Expiry Time	N/A	
Expiry Time Source	N/A	
RejectionThresholdForExpiredData	N/A	
Maximum Certificate Chain Length	1	
Consistency: Generation Location	True	Use the position data from the BSM to compare to validity region.
Relevance: Generation Location Distance	False	
Validity Distance	N/A	
Generation Location Source	Payload	BSM (see 6.3.1)
Overdue CRL Tolerance	3 years	Setting that corresponds to the number of certificates with which a system is initially equipped.
Encrypted Data	False	Encryption is not used for BSMs

6.1.2.2.4 Security management

The system shall comply with the Security Management profile defined in Table 12. [6.1.2-V2V-STD-1609.2-008]

Table 12. Security Mangement Profile

Field	Value	Notes
Signing Key Algorithm	ECDSA-256	This is the only supported signing algorithm in this standard.
Encryption Algorithm	N/A	Encryption is not used for BSMs
Implicit or Explicit Certificates	Implicit	Reduces packet size. Reduces verification time for verification on demand (see 1609.2 [2]).
EC Point Format	Compressed	Reduces packet size.
Supported Geographic Regions	Identified Country only	U.S., Canada, Mexico
MaximumCertificateChainLength	1	
Use Individual Linkage ID	True	Support privacy preserving revocation
Use Group Linkage ID	True	Support privacy preserving revocation

6.1.2.2.5 Other

Table 13 identifies security fields that may be subject to future policy updates.

Table 13. Fields Subject to Policy Updates

Field	Value	Notes
Fields that may be subject to policy update	Overdue CRL Tolerance, Supported Geographic Regions, Use peer-to-peer certificate distribution.	These fields may be updated by a SCMS in the future.

6.1.3 IEEE 1609.3 (1609.3)

This section specifies the requirements from IEEE 1609.3 [3] to support V2V and SCMS operation, as described in Section 6.1. Using the Protocol Implementation Conformance Statement from IEEE 1609.3 [3] the profile for BSM transmissions on channel *vChannelNumber* is provided in this section. Items left blank in the support column are not identified for use by this standard. Items marked V2V are required for transmitting and receiving BSMs, and items marked SCMS are required only if interfacing to an SCMS over DSRC is supported. None of the PICS items including and after item 2.2, so all subsequent items in the 1609.3 PICS table are ommitted from this section.

- The DSRC Radio subsystem shall comply with the V2V items identified in Table 14. If values are specified in the table, the items are set as stated [6.1.3-V2V-STD-1609.3-001].

- If the system supports interfacing to an SCMS over DSRC, the DSRC Radio subsystem shall comply with the SCMS items identified in Table 14. [6.1.3-V2V-STD-1609.3-002]

Table 14: IEEE 1609.3 Requirements

Item	**Feature**	**Value**	**Reference**	**Status**	**Support**
N1.	**DATA PLANE**		—	—	
N1.1.	**IPv6**		5.2, 6.4	O1	SCMS
N1.1.1.	Service channel usage only		6.4.1	M	SCMS
N1.1.2.	Use stateless configuration		6.4	O	SCMS
N1.1.3.	IP readdressing		6.4.2	M	SCMS
N1.1.4.	Send IP datagrams		5.2	O2	SCMS
N1.1.5.	Receive IP datagrams		5.2	O2	SCMS
N1.1.5.1.	Receive by link-local address		6.4	M	SCMS
N1.1.5.2.	Receive by global address		6.4	M	SCMS
N1.1.5.3.	Receive by host multicast addresses		6.4	O3	
N1.1.5.4.	Receive by router multicast addresses		6.4	O3	

Item	Feature	Value	Reference	Status	Support
N1.1.6.	UDP		5.3	O	
N1.1.7.	TCP		5.3	O	SCMS
N1.1.8.	Other IETF protocols	( )[a]	5.3	O	
N1.2.	**WSMP**		5.4	O1	V2V
N1.2.1.	***WSM reception***		5.4.3	O4	V2V
N1.2.1.1.	Check WsmpVersion number	( )[b]	5.4.3, 8.3.2.1	O	V2V (Version = 3)
N1.2.1.2.	Check Subtype field	( )[r]	5.4.3, 8.3.2.1	M	V2V (Subtype = 0 or 1)
N1.2.1.3.	Check TPID field	( )[s]	5.4.3, 8.3.2.2	M	V2V (TPID = 0)
N1.2.1.4.	WAVE Info Elem Extension field		8.1.1	M	V2V
N1.2.1.5.	Deliver message based on Destination Address (PSID)		5.4.3	M	V2V
N1.2.2.	***WSM transmission***		5.4.2	O4	V2V
N1.2.2.1.	Insert WSMP version number		8.3.2.1	M	V2V (Version = 3)
N1.2.2.2.	Insert Destination Address (PSID)		8.3.3	M	V2V
N1.2.2.3.	Outbound message size	( )[c]	5.4.2	M	V2V
N1.2.2.4.	Transmit channel number		8.3.4.2	O	
N1.2.2.5.	Transmit data rate		8.3.4.3	O	
N1.2.2.6.	Transmit Power Used		8.3.4.4	O	
N1.2.2.7.	Channel Load		8.3.4.5	O	
N1.2.2.8.	Insert Subtype features	( )[r]	8.3.2.1	M	V2V (Subtype = 0 or 1)
N1.2.2.9.	Insert TPID features	( )[s]	8.3.3.1	M	V2V (TPID = 0)
N2.	**MANAGEMENT PLANE**		—	—	
N2.1.	**User role**		6.2.1	O	SCMS
N2.1.1.	Receive WSAs over WSMP		6.3.2	O5	SCMS
N2.1.2.	Verify and accept Secured WSA		6.3.3	O5	SCMS
N2.1.3.	Accept unsecured WSA		6.3.3	O5	
N2.1.4.	WAVE Info Elem Extension fields		8.1.1	M	
N2.1.5.	Calculate avail service link quality		6.3.4	O	
N2.1.6.	***WSA header***		8.2.2	M	
N2.1.6.1.	Check WSA version number	( )[d]	8.2.2.2	M	SCMS
N2.1.6.2.	Check WSA Identifier		8.2.2.4	O	
N2.1.6.3.	Check Content Count		8.2.2.5	O	
N2.1.6.4.	WSA Header Info Element Ext field		8.2.2.6	M	SCMS
N2.1.6.4.1.	Repeat Rate		8.2.2.6.1	O	
N2.1.6.4.2.	2DLocation		8.2.2.6.2	O	
N2.1.6.4.3.	3DLocation		8.2.2.6.3	O	
N2.1.6.4.4.	Advertiser Identifier		8.2.2.6.4	O	
N2.1.6.4.5.	Other info elements	( )[e]	8.2.2.6	O	
N2.1.7.	***Service Info Segment***		8.2.3	M	SCMS
N2.1.7.1.	Number of Service Info	( )[f]	8.2.3	M	SCMS

Item	Feature	Value	Reference	Status	Support
	Instances				
N2.1.7.2.	WAVE Info Element Extension field		8.2.3.5	M	SCMS
N2.1.7.2.1.	PSC		8.2.3.5.1	O	SCMS
N2.1.7.2.2.	IPv6Address		8.2.3.5.2	O	SCMS
N2.1.7.2.3.	Service Port		8.2.3.5.3	O	SCMS
N2.1.7.2.4.	Provider MAC Address		8.2.3.5.4	O	SCMS
N2.1.7.2.5.	RCPI Threshold		8.2.3.5.5	O	SCMS
N2.1.7.2.6.	WSA Count Threshold		8.2.3.5.6	O	SCMS
N2.1.7.2.6.	WSA Count Threshold Interval		8.2.3.5.7	O	SCMS
N2.1.7.2.7.	Other info elements	( )[g]	8.2.3.5	O	
N2.1.8.	***Channel Info Segment***		8.2.4	M	SCMS
N2.1.8.1.	Number of Channel Info Instances	( )[h]	8.2.4	M	SCMS
N2.1.8.2.	WAVE Info Elem Extension field		8.2.4.8	M	SCMS
N2.1.8.2.1.	EDCA Parameter Set		8.2.4.8.1	O	SCMS
N2.1.8.2.2.	Channel Access		8.2.4.8.2	O	SCMS
N2.1.8.2.3.	Other info elements	( )[i]	8.2.4.8	O	
N2.1.9.	***WAVE Router Advertisement***		8.2.5.1	O	SCMS
N2.1.9.1.	WAVE Info Elem Extension field		8.2.5.7	M	SCMS
N2.1.9.1.1.	Secondary DNS		8.2.5.7.1	O	SCMS
N2.1.9.1.2.	Gateway MAC Address		8.2.5.7.2	O	SCMS
N2.1.9.1.3.	Other info elements	( )[j]	8.2.5.7	O	
N2.2.	**Provider role**		6.2.1	O	**Note:** The provider role is not applicable to the OBE system. Thus, the provider section of the PICS is not included.

[a] List protocols supported.
[b] List version numbers supported.
[c] Enter maximum WAVE Short Message length.
[d] List version numbers supported.
[e] List any other WSA header information elements processed on reception.
[f] Enter maximum number of Service Info Iinstances processed on reception.
[g] List any other Service Info Segment information elements processed on reception.
[h] Enter maximum number of Channel Info Iinstances processed on reception.
[i] List any other Channel Info Segment information elements processed on reception.
[j] List any other WAVE routing advertisement information elements processed on reception.
[k] List any other WSA header information elements supported on transmission.
[l] Enter maximum number of Service Info Iinstances supported on transmission.
[m] List any other Service Info Segment Iinformation elements supported on transmission.
[n] Enter maximum number of Channel Info Iinstances supported on transmission.
[o] List any other Channel Info Segment information elements supported on transmission.
[p] List any other WAVE routing advertisement information elements supported on transmission.
[q] List any other MIBs supported.
[r] List Subtype values supported.
[s] List TPID values supported.
[t] Enter encoding method, e.g. UTF-8 or other encoding.

6.1.4 IEEE 1609.4 (1609.4)

This section specifies the requirements from IEEE 1609.4 [4] to support V2V and SCMS operation, as described in Section 6.1. Using the Protocol Implementation Conformance Statement from IEEE 1609.4 [4] the profile for BSM transmissions on channel *vChannelNumber* is provided in this section. Items left blank in the support column are not identified for use by this standard. Items marked V2V are required for transmitting and receiving BSMs, and items marked SCMS are required only if interfacing to an SCMS over DSRC is supported.

- The DSRC Radio subsystem shall comply with the V2V items identified in Table 15. If values are specified in the table, the items are set as stated [6.1.4-V2V-STD-1609.4-001].

- If the system supports interfacing to an SCMS over DSRC, the DSRC Radio subsystem shall comply with the SCMS items identified in Table 15. [6.1.4-V2V-STD-1609.4-002]

Table 15: IEEE 1609.4 Requirements

Item	Feature	Value	Reference	Status	Support
M1.	Single-PHY device		5.1, 6.3.1	C1	V2V: Choose one of these items.
M2.	Multi-PHY device	( )[a]	6.3.1	C1	
M3.	Operation on CCH	( )[b]	5.2	O4	
M3.1.	Continuous CCH access		6.3.3	O	
M4.	Operation on SCH	( )[c]	5.2	O4	V2V (USA, Channel 172, Class C)
M4.1.	Continuous SCH access		6.3.1	O	V2V
M5.	**Mixed operation**		5.2	O4	SCMS
M5.1.	Immediate access		6.3.3	O6	SCMS: optional
M5.2.	Extended access		6.3.4	O6	SCMS: Choose one of these items
M5.3.	Alternating access		6.3.2	O6	
M5.3.1.	Use common time reference		5.2.2, 6.2.1	M	SCMS
M5.3.1.1.	Derive timing from GPS		6.2.3	O5	SCMS
M5.3.1.2.	Derive timing from Timing Advertisement frame		6.2.3	O5	
M5.3.1.3.	Derive timing from other timing source	( )[d]	6.2.3	O5	
M5.3.2.	Guard interval on transmit		6.2.5	M	SCMS
M5.3.3.	Medium busy at end of guard interval		6.2.5	M	SCMS
M6.	**Transmit**		5.3.2	O2	V2V
M6.1.	EDCA and user priority		5.4	M	V2V
M6.2.	Cancel transmissions		7.3.5	O	
M6.3.	Send TA		6.2.6	O	
M6.4.	Send other IEEE 802.11 frames	( )[e]	6.4	O	
M6.5.	Send WSM		5.3.3	O3	V2V
M6.5.1.	Expiry time		5.3.3	O	
M6.6.	Send IPv6		5.3.4	O3	SCMS
M7.	**Receive**		5.3.5	O2	V2V
M7.1.	Receive TA		6.2.7	O	
M7.2.	Receive WSM		5.3.3	O3	V2V

Item	Feature	Value	Reference	Status	Support
M7.3.	Receive IPv6		5.3.4	O3	SCMS
M8.	**Device readdressing**		6.6	O	V2V
M9.	**MIB maintenance**		6.5	—	
M9.1.	Managed WAVE device		3.1, 6.5	O	
M9.2.	Per Annex E		6.5	M17.1: M	
M9.3.	Other MIB	( )[f]	6.5	O	

[a]Enter number of simultaneous channels supported.
[b]List supported control channel(s), including country and operating class.
[c]List supported service channel(s), including country and operating class.
[d]Indicate device's timing source(s).
[e]Enter IEEE 802.11 management frames/service request primitives supported.
[f]Enter references to other management information bases supported.

6.1.5 IEEE 1609.12 (1609.12)

This section specifies the requirements from IEEE 1609.12 [5] to support V2V and SCMS operation, as described in Section 6.1.

Table 16: IEEE 1609.12 Requirements

1609.12 Clause	Title (1609.12 Clause)	Required For	Requirement
4	WAVE Identifiers		
4.1.x	Provider service identifier (PSID)	V2V	The system shall set the PSID value to the value assigned to "vehicle to vehicle safety and awareness" as specified. [6.1.5-V2V-STD-1609.12-001]
4.1.x	Provider service identifier (PSID)	SCMS	The system shall set the PSID value the value assigned to "WAVE security management" as specified. [6.1.5-V2V-STD-1609.12-002]
4.3	Ethertype	V2V	The system shall set the Ethertype value for WSMP as specified. [6.1.5-V2V-STD-1609.12-003]
4.3	Ethertype	SCMS	The system shall set the Ethertype value for IPv6 as specified. [6.1.5-V2V-STD-1609.12-004]

6.1.6 SAE J2735 (J2735)

This section identifies the BSM data frames and data elements from J2735 [6] used to support V2V safety operations. All requirements in Table 17 refer to J2735 unless otherwise noted. The functional and performance requirements corresponding to these data frames and data elements are specified Sections 6.2 through 6.6 of this standard.

Table 17: SAE J2735 Requirements

Title (J2735 Clause)	Requirement
Message Encoding	The system shall conform to ASN encoding of the Basic Safety Message as specified. [6.1.6-V2V-STD-J2735-001]
MSG_MessageFrame	
Data Element: DE_DSRC_MessageID	The system shall comply with the data element DE_DSRC_MessageID, as specified. [6.1.6-V2V-STD-J2735-002]
Message: MSG_BasicSafetyMessage (BSM)	The system shall conform to Part I of the Basic Safety Message, as specified. [6.1.6-V2V-STD-J2735-003]
Message: MSG_BasicSafetyMessage (BSM)	The system shall conform to Part II of the Basic Safety Message to as specified in J2735 [6], this table and Section 6.3 of this standard. [6.1.6-V2V-STD-J2735-004]

Title (J2735 Clause)	Requirement
Data Frames	**Note:** The system includes the Data Frames required for Part I and Part II in the Basic Safety Message as specified in J2735 [6], this table and Section 6.3 of this standard
Data Frame: DF_AccelerationSet4Way	The system shall conform to the data frame DF_AccelerationSet4Way, as specified. [6.1.6-V2V-STD-J2735-005]
Data Frame: DF_BrakeSystemStatus	The system shall conform to the data frame DF_BrakeSystemStatus, as specified. [6.1.6-V2V-STD-J2735-006]
Data Frame: DF_BSMcoreData	The system shall conform to the data frame DF_BSMcoreData, as specified. [6.1.6-V2V-STD-J2735-007]
Data Frame: DF_PathHistory	The system shall conform to the data frame DF_PathHistory, as specified. [6.1.6-V2V-STD-J2735-008]
Data Frame: DF_PathHistoryPointList	The system shall conform to the data frame Data Frame: DF_PathHistoryPointList, as specified. [6.1.6-V2V-STD-J2735-009]
Data Frame: DF_PathHistoryPoint	The system shall conform to the data frame DF_PathHistoryPoint, as specified. [6.1.6-V2V-STD-J2735-010]
Data Frame: DF_PathPrediction	The system shall conform to the data frame DF_PathPrediction, as specified. [6.1.6-V2V-STD-J2735-011]
Data Frame: DF_PositionalAccuracy	The system shall conform to the data frame DF_Positional Accuracy, as specified. [6.1.6-V2V-STD-J2735-012]
Data Frame: DF_VehicleSafetyExtensions	The system shall conform to the data frame DF_VehicleSafetyExtensions, as specified. [6.1.6-V2V-STD-J2735-013]
Data Frame: DF_VehicleSize	The system shall conform to the data frame DF_VehicleSize. [6.1.6-V2V-STD-J2735-014]
Data Elements	**Note:** The system includes the Data Elements required for Part I and Part II in the Basic Safety Message as specified in J2735 [6], this table and Section 6.3 of this standard.
Data Element: DE_Acceleration	The system shall conform to the data element DE_Acceleration, as specified. [6.1.6-V2V-STD-J2735-015]
Data Element: DE_AntiLockBrakeStatus	The system shall conform to the data element DE_AntiLockBrakeStatus, as specified. [6.1.6-V2V-STD-J2735-016]
Data Element: DE_AuxiliaryBrakeStatus	The system shall conform to the data element DE_AuxiliaryBrakeStatus, as specified. [6.1.6-V2V-STD-J2735-017]
Data Element: DE_BrakeAppliedStatus	The system shall conform to the data element DE_BrakeAppliedStatus, as specified. [6.1.6-V2V-STD-J2735-018]
Data Element: DE_BrakeBoostApplied	The system shall conform to the data element DE_BrakeBoostApplied, as specified. [6.1.6-V2V-STD-J2735-019]
Data Element: DE_Confidence	The system shall conform to the data element DE_Confidence, as specified. [6.1.6-V2V-STD-J2735-020]
Data Element: DE_DSecond	The system shall conform to the data element DE_DSecond, as specified. [6.1.6-V2V-STD-J2735-021]
Data Element: DE_Elevation	The system shall conform to the data element DE_Elevation, as specified. [6.1.6-V2V-STD-J2735-022]
Data Element: DE_ExteriorLights	When DE_ExteriorLights is included in the BSM, the system shall conform to the data element DE_ExteriorLights, as specified. [6.1.6-V2V-STD-J2735-023]
Data Element: DE_Heading	The system shall conform to the data element DE_Heading, as specified. [6.1.6-V2V-STD-J2735-024]
Data Element: DE_Latitude	The system shall conform to the data element DE_Latitude, as specified. [6.1.6-V2V-STD-J2735-025]
Data Element: DE_Longitude	The system shall conform to the data element DE_Longitude, as specified. [6.1.6-V2V-STD-J2735-026]
Data Element: DE_MsgCount	The system shall conform to the data element DE_MsgCount, as specified. [6.1.6-V2V-STD-J2735-027]
Data Element: DE_OffsetLL-B18	The system shall conform to the data element DE_OffsetLL-B18, as specified. [6.1.6-V2V-STD-J2735-028]

Title (J2735 Clause)	Requirement
Data Element: DE_RadiusOfCurvature	The system shall conform to the data element DE_RadiusOfCurvature, as specified. [6.1.6-V2V-STD-J2735-029]
Data Element: DE_SemiMajorAxisAccuracy	The system shall conform to the data element DE_SemiMajorAxisAccuracy, as specified. [6.1.6-V2V-STD-J2735-030]
Data Element: DE_SemiMajorAxisOrientation	The system shall conform to the data element DE_SemiMajorAxisOrientation, as specified. [6.1.6-V2V-STD-J2735-031]
Data Element: DE_SemiMinorAxisAccuracy	The system shall conform to the data element DE_SemiMinorAxisAccuracy, as specified. [6.1.6-V2V-STD-J2735-032]
Data Element: DE_Speed	The system shall conform to the data element DE_Speed, as specified. [6.1.6-V2V-STD-J2735-033]
Data Element: DE_StabilityControlStatus	The system shall conform to the data element DE_StabilityControlStatus, as specified. [6.1.6-V2V-STD-J2735-034]
Data Element: DE_SteeringWheelAngle	The system shall conform to the data element DE_SteeringWheelAngle, as specified. [6.1.6-V2V-STD-J2735-035]
Data Element: DE_TemporaryID	The system shall conform to the data element DE_TemporaryID, as specified. [6.1.6-V2V-STD-J2735-036]
DE_TimeOffset	The system shall conform to the data element DE_TimeOffset, as specified. [6.1.6-V2V-STD-J2735-037]
Data Element: DE_TractionControlStatus	The system shall conform to the data element DE_TractionControlStatus, as specified. [6.1.6-V2V-STD-J2735-038]
Data Element: DE_TransmissionState	The system shall conform to the data element DE_TransmissionState, as specified. [6.1.6-V2V-STD-J2735-039]
Data Element: DE_VehicleEventFlags	When DE_VehicleEventFlags is included in the BSM, the system shall conform to the data element DE_VehicleEventFlags as specified in J2735 [6] and this standard. [6.1.6-V2V-STD-J2735-040]
Data Element: DE_VehicleLength	The system shall conform to the data element DE_VehicleLength, as specified. [6.1.6-V2V-STD-J2735-041]
Data Element: DE_VehicleWidth	The system shall conform to the data element DE_VehicleWidth, as specified. [6.1.6-V2V-STD-J2735-042]
Data Element: DE_VerticalAcceleration	The system shall conform to the data element DE_VerticalAcceleration, as specified. [6.1.6-V2V-STD-J2735-043]
DE_VertOffset-B12	The system shall conform to the data element DE_VertOffset-B12, as specified. [6.1.6-V2V-STD-J2735-044]
Data Element: DE_YawRate	The system shall conform to the data element DE_YawRate, as specified. [6.1.6-V2V-STD-J2735-045]

6.1.7 FCC 47 CFR, Parts 0, 1, 2, and 95 (Informative)

Regulatory requirements for the DSRC Radio subsystem within the United States are available from the Federal Communications Commission (FCC), Title 47 of the Code of Federal Regulations (CFR), Parts 0, 1, 2, and 95.

Note: Regulatory domains outside the United States may be subject to different regulatory requirements. FCC type certifications are required in the United States as defined in the CFR.

6.2 Positioning and Timing Requirements (POSTIM)

6.2.1 Position Determination (POSDETER)

- The positioning subsystem shall include a GNSS receiver. In the United States this requires that the GNSS receiver includes GPS. [6.2.1-V2V-POSTIM-POSDETER-001]

  Note: Additional positioning and augmentation capabilities can be used.

- The system shall determine the position of the vehicle as defined in 6.2.3 at a nominal rate of *vPosDetRate* and the Coordinated Universal Time (UTC) time when at that position. [6.2.1-V2V-POSTIM-POSDETER-002]

Note: If the position update rate deviates from the nominal times governed by *vPosDetRate*, the system can compute vehicle position and time using the method described in Appendix A.3. Using this method, time and position can computed as closely as possible to the time when the BSM is generated.

- The position shall be “Unavailable” if the positioning subsystem is unable to provide a 3D position. BSMs are not transmitted if position is Unavailable (see 6.3.5). [6.2.1-V2V-POSTIM-POSDETER-003]

Note: Position and UTC time are based on estimates provided by the positioning system and are subject to the accuracy requirements in **Error! Reference source not found.**, 6.3.6.5 and 6.3.6.6.

6.2.2 Wide Area Augmentation System (WAAS)

- The positioning subsystem shall use WAAS corrections, when the WAAS signal is available, in order to improve the position accuracy. [6.2.2-V2V-POSTIM-WAAS-001]

  Note: This requirement establishes a common source of positional corrections used by the GNSS receivers in V2V systems and provides better accuracy of the resulting relative position between vehicles. Additional augmentation and correction systems may be used in addition to WAAS.

6.2.3 Coordinate System and Reference (COORDSYSREF)

Position Reference: The vehicle position reported in a BSM shall be a point (latitude, longitude and elevation) projected onto the surface of the roadway (road plane) with reference to the WGS-84 coordinate system and its reference ellipsoid. This point is the center of the rectangle on the road plane, oriented about the vehicle that encompasses the farthest forward, rearward, and side-to-side points on the vehicle, including original equipment such as outside side view mirrors (see Figure 21). [6.2.3-V2V-POSTIM-COORDSYSREF-001]

Note: The GNSS (shown as GPS in Figure 21) antenna reference position is not the same as the position reference. See Appendix A.4 for an example of how to translate from the position of the GNSS antenna to the position reference. Incline of the road and yaw result in negligible change in position. Testing can be done using a flat ground plane.

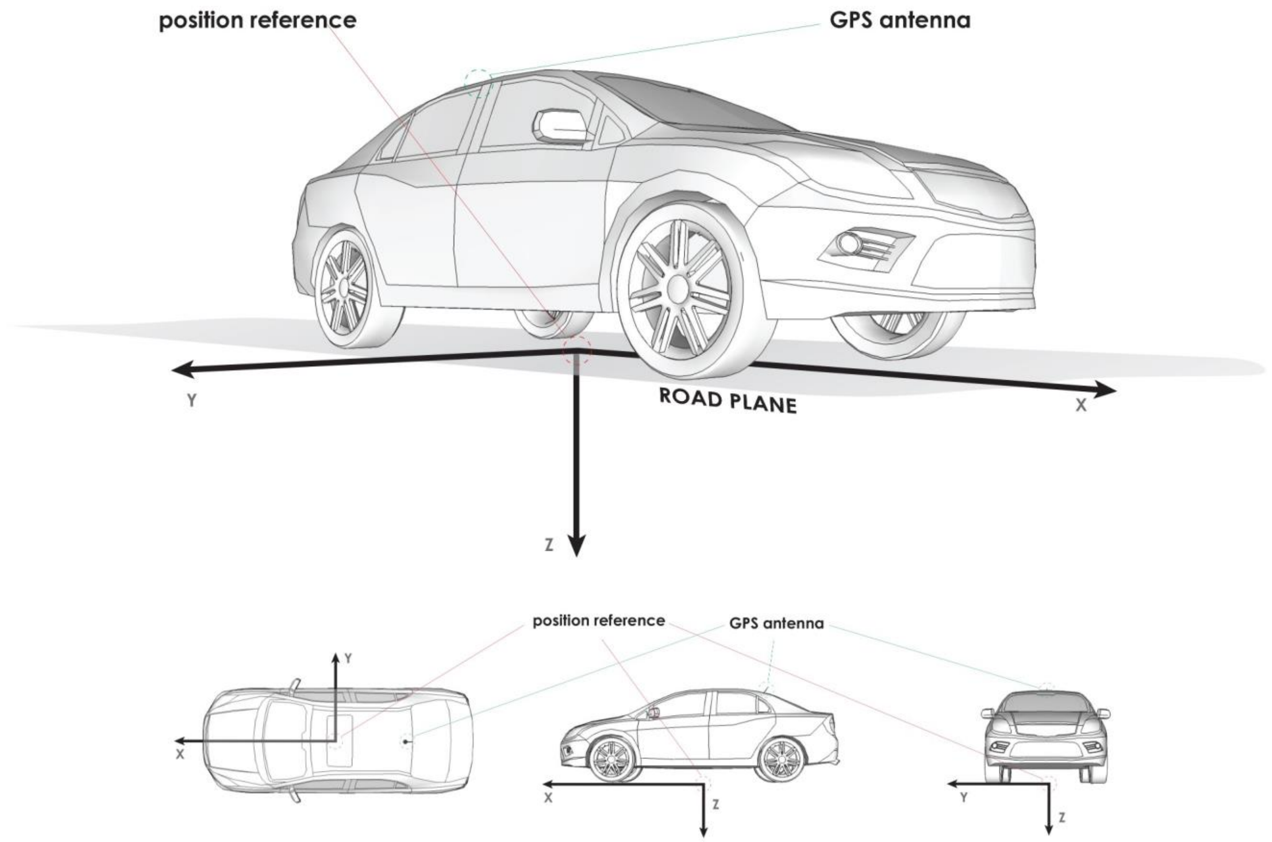


Figure 21: BSM Position Reference

6.2.4 System Time Coordination (SYSTIMCOORD)

- The system shall include a reference clock that conforms to UTC [15]. [6.2.4-V2V-POSTIM-SYSTIMCOORD-001]
- The system clock shall be accurate to within *vTimeAccuracy* of the UTC reference. [6.2.4-V2V-POSTIM-SYSTIMCOORD-002]
- The system shall determine the time at which position is determined, using the UTC reference. [6.2.4-V2V-POSTIM-SYSTIMCOORD-003]

Note: The system has time synchronized to UTC in order to support position and time extrapolation, and security requirements. The system can implement the reference clock using the GNSS receiver and the corresponding one pulse per second (1PPS).

6.3 BSM Transmission Requirements on Channel *vChannel Number* (BSMTX)

6.3.1 BSM Contents (BSMCONT)

- When transmitting a BSM, the system shall generate the BSM data as specified in J2735 [6] and containing the data frames and data elements defined in this standard. All BSMs contain the BSM Part I content as specified in J2735 [6]. [6.3.1-V2V-BSMTX-BSMCONT-001]
- The system shall include additional BSM content as follows:
    - The system transmitting a BSM shall include the DF_VehicleSafetyExtensions data frame in Part II. [6.3.1-V2V-BSMTX-BSMCONT-002]

- The DF_VehicleSafetyExtensions data frame shall include [6.3.1-V2V-BSMTX-BSMCONT-003]:
    - DF_PathHistory
    - DF_PathPrediction
    - DE_ExteriorLights
- If one or more event conditions corresponding to an event flag is met, the BSM Part II shall include the DF_VehicleSafetyExtensions data element, DE_VehicleEventFlags. (DE_VehicleEventFlags is not included if no event condition corresponding to any event flag is met.). [6.3.1-V2V-BSMTX-BSMCONT-004]

  Note: Vehicle type (DE_VehicleType) is intentionally not included in the BSM Part II for light vehicles. However, it can be inferred for light vehicles as long as all other classes of vehicles include the field in their BSMs as defined in future revisions of this standard, or in other standards in the J2945 family of standards.

- Each BSM shall be ASN.1 encoded using Unaligned Packed Encoding Rules (UPER) [6.3.1-V2V-BSMTX-BSMCONT-005]

6.3.2 Channel and Data Rate (CHDATARATE)

- The system shall transmit BSMs on channel *vChannelNumber* with 10 MHz channel spacing (per 802.11 regulatory guidelines [1]). [6.3.2-V2V-BSMTX-CHDATARATE-001]
- The system shall transmit BSMs at a data rate of *vDataRate*. [6.3.2-V2V-BSMTX-CHDATARATE-002]

6.3.3 Transmit Timing (TXTIM)

- The system shall transmit BSMs that do not include DE_VehicleEventFlags at a nominal message rate of *vBSMTxRate* (default) unless the congestion control procedures specified in Section 6.3.8 require a different message transmission rate. [6.3.3-V2V-BSMTX-TXTIM-001]
- Transmission of BSMs shall have a random start time. [6.3.3-V2V-BSMTX-TXTIM-002]

  Note: To meet these requirements, upon system device startup, the first BSM transmitted may choose a random epoch based on *vBSMTxRate*. Each subsequent BSM may be transmitted at nominal rate of *vBSMTxRate* based on that epoch.

- The system shall vary each BSM transmission by adding a uniformly distributed random value between -*vTxRand* and +*vTxRand* to each scheduled transmissison time, uniquely computed before every transmission. [6.3.3-V2V-BSMTX-TXTIM-003]

Note: The randomization minimizes repeated packet collisions of transmitted BSMs from multiple systems.

- The system shall transmit a BSM containing DE_VehicleEventFlags, triggered by one or more event conditions corresponding to event flags defined in J2735 [6], within the time constraints specified in **Error! Reference source not found.**. Subsequent BSMs are transmitted at the nominal message rate of *vBSMTxRate*. After the event condition(s) ends, BSM transmissions return to the appropriate rate based on congestion control. [6.3.3-V2V-BSMTX-TXTIM-004]

  Note: The intent is to transmit the BSM as soon as possible after an event condition is met.

- The system shall be capable of adjusting BSM transmission rates from *vBSMTxRateMin* to *vBSMTxRateMax* when required by the congestion control procedures specified in Section 6.3.8. [6.3.3-V2V-BSMTX-TXTIM-005]

6.3.4 User Priority and EDCA Settings (UPEDCA)

- The system shall set the User Priority field defined in 802.11 [1] to 5 for BSMs with no event flags. [6.3.4-V2V-BSMTX-UPEDCA-001]
- The system shall set the User Priority field defined in 802.11 [1] to 7 for BSMs that include one or more event flags. [6.3.4-V2V-BSMTX-UPEDCA-002]
- The system shall set the EDCA values defined in 802.11 [1] as shown in Table 18 for BSM transmissions on channel *vChannelNumber*. [6.3.4-V2V-BSMTX-UPEDCA- 003]

Table 18: EDCA Parameter Set

User Priority	AC	CWmin	CWmax	AIFSN	TXOP Limit OFDM/CCKOFDM PHY
1, 2	AC_BK	15	1023	9	0
0, 3	AC_BE	15	1023	6	0
4, 5	AC_VI	15	1023	4	0
6, 7	AC_VO	3	7	2	0

Note: The CWmin and AIFSN values for AC_VI are different than the default EDCA parameter set when dot11OCBActivated is equal to true (see 802.11 [1]). AIFSN was changed from a default of 3 to 4, CWmin was changed from a default of 7 to 15, and CWmax was changed from a default of 15 to 1023. These changes improve throughput for BSMs and priortitize BSMs over other potential background and best-effort messages on the same channel.

6.3.5 Minimum Transmission Criteria (MINTX)

The system shall transmit a BSM only if the BSM meets the minimum criteria for BSM transmission specified in Table 19 and Table 20. If at anytime the system cannot formulate a BSM that meets the minimum transmission criteria, the system ceases transmitting BSMs until the criteria are met. [6.3.5-V2V-BSMTX-MINTX-001]

Table 19: BSM Part I: Minimum Criteria for BSM Transmission

Data Element/Field	Can be set to unavailable, or represent an unknown value, as specified in J2735 [6]?	Section Reference (this standard)
DE_DSRC_MessageID	No	6.3.6.1
DE_Dsecond	No	**Error! Reference source not found.**
DE_MsgCount	No	6.3.6.3
DE_TemporaryID	No	6.3.6.4
DE_Latitude	No	6.3.6.5
DE_Longitude	No	6.3.6.5
DE_Elevation	No	6.3.6.6
DF_PositionalAccuracy	No	6.3.6.7
DE_SemiMajorAxisAccuracy	No	6.3.6.7
DE_SemiMinorAxisAccuracy	No	6.3.6.7
DE_SemiMajorAxisOrientation	No	6.3.6.7
DE_TransmissionState	Yes	6.3.6.8
DE_Speed	No	6.3.6.8
DE_Heading	No	6.3.6.10
DE_SteeringWheelAngle	Yes	6.3.6.11
DF_AccelerationSet4Way		
DE_Acceleration (Longitudinal)	No	6.3.6.12

Data Element/Field	Can be set to unavailable, or represent an unknown value, as specified in J2735 [6]?	Section Reference (this standard)
DE_Acceleration (Lateral)	Yes	6.3.6.12
DE_VerticalAcceleration	Yes	6.3.6.12
DE_YawRate	No	6.3.6.12
DF_BrakeSystemStatus	Yes **Note:** All parameters in DF_BrakeSystemStatus may be set to Unavailable.	6.3.6.13
DF_VehicleSize		
DE_VehicleWidth	No	6.3.6.14
DE_VehicleLength	No	6.3.6.14

Table 20: BSM Part II: Minimum Criteria for BSM Transmission

Data Element/Field	Can a BSM be transmitted without the Data Frame/Element?	Notes	Section Reference (this standard)
DE_VehicleEventFlags	Yes	DE_VehicleEventFlags is not included in the BSM if no event conditions are met	**Error! Reference source not found.**
DF_PathHistory	No	A BSM cannot be transmitted without DF_PathHistory	6.3.6.16
DF_PathPrediction	No	A BSM cannot be transmitted without DF_PathPrediction	6.3.6.17
DE_ExteriorLights	Yes	DE_ExteriorLights is not included in the BSM if the corresponding status is unavailable or the exterior lights are turned off	6.3.6.18

6.3.6 Data Element Accuracy (DATAACC)

6.3.6.1 DE_DSRC_MessageID

- The system shall set the DE_DSRC_MessageID to the value assigned to basicSafetyMessage. (see J2735 [6]). [6.3.6-V2V-BSMTX-DATAACC-001]

6.3.6.2 DE_DSecond

- The system shall set the DE_DSecond as specified in J2735 [6], using UTC as the time of reference. [6.3.6-V2V-BSMTX-DATAACC-008]

Note: The time represented by DE_DSecond is the time at which the BSM Part I vehicle location data was determined by the positioning system.

- DE_DSecond shall be accurate to within *vTimeAccuracy* of the UTC at which position was determined. [6.3.6-V2V-BSMTX-DATAACC-009]
- In order to ensure the transmitted information is current, the difference between the UTC time at which the BSM is transmitted and the value of DE_Dsecond shall be less than *vMaxPosAge*. [6.3.6-V2V-BSMTX-DATAACC-010]

Note: The result of this requirement is that BSMs do not contain information that is older than UTC minus *vMaxPosAge*.

6.3.6.3 DE_MsgCount

- The system shall initialize the DE_MsgCount to a random value within the range defined by J2735 [6] when sending the first BSM after system startup. [6.3.6-V2V-BSMTX-DATAACC-002]
- If the certificate used to sign the BSM has changed since transmitting the most recent BSM, the system shall re-initialize the DE_MsgCount field to a new random value within the range defined by J2735 [6] before transmitting the next BSM. [6.3.6-V2V-BSMTX-DATAACC-003]
- The system shall set DE_MsgCount equal to one greater than the value used in the previously transmitted BSM, according to J2735 [6] if the certificate used to sign the BSM has not changed since sending the most recent BSM. For this element the value after 127 is 0 per J2735 [6]. [6.3.6-V2V-BSMTX-DATAACC-004]

Note: DE_MsgCount, DE_TemporaryID and the DSRC radio MAC address are randomly reinitialized after the security certificate changes.

6.3.6.4 DE_TemporaryID

- The system shall initialize the DE_TemporaryID to a random value within the range defined by J2735 [6]. [6.3.6-V2V-BSMTX-DATAACC-005]
- If the certificate used to sign the BSM has changed since transmitting the most recent BSM, the system shall re-initialize the DE_TemporaryID to a new random value within the range defined by J2735[6]. [6.3.6-V2V-BSMTX-DATAACC-006]
- The system shall re-initialize the DE_TemporaryID to a new random value within the range defined by J2735 [6] when it receives a BSM with the same DE_TemporaryID. [6.3.6-V2V-BSMTX-DATAACC-007]

Note: DE_MsgCount, DE_TemporaryID and the DSRC radio MAC address are randomly reinitialized after the security certificate changes.

Note: J2735 [6] states in a remark that other measurements present in the BSM are aligned to DE_DSecond insofar as possible in the implementation. Practical implementations to date have used the most recent measurement updates known to the transmitter at the time when the BSM is composed.

6.3.6.5 DE_Latitude & DE_Longitude

- The system shall set the DE_Latitude and DE_Longitude data elements with values corresponding to its two-dimensional (2-D) horizontal position with reference to the WGS-84 coordinate system. [6.3.6-V2V-BSMTX-DATAACC-011]
- The position of the system transmitting a BSM shall be accurate to within *vPosAccuracy* of the vehicle's actual 2-D horizontal position under open sky conditions within the 1-sigma absolute error. [6.3.6-V2V-BSMTX-DATAACC-012]

Note: The position accuracy requirements apply under test conditions. It is not possible to continually test systems in operation. See Appendix A.7 for the definition of open sky conditions

Note: The 1-sigma accuracy requirement results in 95% confidence with respect to lane-level relative positioning based on testing done to support the use cases described in Section 4.

Note: The intent of these requirements is for the position to be accurate enough to support safety applications requiring lane-level accuracy. The accuracy requirement is based on the 3.0 m minimum Federal Highway Administration (FHWA) recommended width of any roadway equal to or wider than a collector roadway [8]. See Appendix A.7 for the definition of open sky conditions.

6.3.6.6 DE_Elevation

- The system shall set DE_Elevation to the “Height above Reference Ellipsoid”, above or below the WGS-84 reference ellipsoid. [6.3.6-V2V-BSMTX-DATAACC-013]
- The DE_Elevation data element shall be accurate to within *vElevAccuracy* of the actual elevation under open sky conditions within the 1-sigma absolute error. [6.3.6-V2V-BSMTX-DATAACC-014]

  Note: The elevation accuracy requirements apply under test conditions. It is not possible to continually test systems in operation. See Appendix A.7 for the definition of open sky conditions.

  Note: The 1-sigma accuracy requirement results in 95% confidence with respect to lane-level relative positioning based on testing done to support the use cases described in Section 4. See Appendix A.7 for the definition of open sky conditions.

6.3.6.7 DF_PositionalAccuracy

- The system shall set the value of the DF_PositionalAccuracy data frame of the BSM with the corresponding values observed by the positioning system for each determined position. [6.3.6-V2V-BSMTX-DATAACC-015]
- DF_PositionalAccuracy shall provide the errors for DE_SemiMajorAxisAccuracy and DE_SemiMinorAxisAccuracy of the error ellipsoid at one standard deviation, as well as the DE_SemiMajorAxisOrientation for the semi-major axis. [6.3.6-V2V-BSMTX-DATAACC-016]

6.3.6.8 DE_Speed

- The DE_Speed data element in this data frame shall be accurate to within *vSpeedAccuracy* of the actual vehicle speed under open sky conditions within the 1-sigma absolute error. [6.3.6-V2V-BSMTX-DATAACC-017]

  Note: The speed accuracy requirements apply under test conditions. It is not possible to continually test systems in operation. See Appendix A.7 for the definition of open sky conditions.

6.3.6.9 DE_TransmissionState

- The DE_TransmissionState data element in this data frame shall correctly reflect the state of the vehicle’s transmission [6.3.6-V2V-BSMTX-DATAACC-018]

6.3.6.10 DE_Heading

- DE_Heading shall describe the moving direction of the vehicle reference point and its value increases clockwise from north. [6.3.6-V2V-BSMTX-DATAACC-019]
- DE_Heading shall be accurate to within *vHeadAccuracyB* within the 1-sigma absolute error of the actual vehicle heading when the vehicle speed is less than or equal to *vHeadingSpeedThresh* under open sky conditions,. [6.3.6-V2V-BSMTX-DATAACC-020]
- DE_Heading shall be accurate to within *vHeadAccuracyA* within the 1-sigma absolute error of the actual vehicle heading when the vehicle speed is greater than *vHeadingSpeedThresh* under open sky conditions. [6.3.6-V2V-BSMTX-DATAACC-021]
- The system shall latch the value of DE_Heading to the last known heading value when the speed was above *vHeadLatchThresh* when the vehicle speed drops below *vHeadLatchThresh*. [6.3.6-V2V-BSMTX-DATAACC-022]
- The system shall unlatch the value of DE_Heading when the vehicle speed exceeds *vHeadUnlatchThresh*. [6.3.6-V2V-BSMTX-DATAACC-023]

  Note: The heading accuracy requirements apply under test conditions. It is not possible to continually test systems in operation. See Appendix A.7 for the definition of open sky conditions.

6.3.6.11 DE_SteeringWheelAngle

- If the DE_SteeringWheelAngle is available, it shall be accurate to within *vStWhAnAccuracy* of the actual vehicle steering wheel angle within the 3-sigma absolute error. [6.3.6-V2V-BSMTX-DATAACC-024]

  Note: This information is available from the vehicle CAN bus or other vehicle interface, or DE_SteeringWheelAngle is unavailable.

6.3.6.12 DF_AccelerationSet4Way

- DE_Acceleration (Longitudinal) and DE_Acceleration (Lateral) data elements in this data frame shall be accurate to within *vAccelAccuracy* under open sky conditions within the 1-sigma absolute error of the actual vehicle longitudinal and lateral accelerations, respectively. [6.3.6-V2V-BSMTX-DATAACC-025]
- DE_VerticalAcceleration data element in this data frame shall be accurate to within *vVertAccelAccuracy* under open sky conditions within the 1-sigma absolute error of the actual vehicle vertical acceleration. [6.3.6-V2V-BSMTX-DATAACC-026]
- DE_YawRate data element in this data frame shall be accurate to within *vYawRateAccuracy* under open sky conditions within the 1-sigma absolute error of the actual vehicle yaw rate. [6.3.6-V2V-BSMTX-DATAACC-027]

  Note: The acceleration accuracy requirements apply under test conditions. It is not possible to continually test systems in operation. See Appendix A.7 for the definition of open sky conditions.

6.3.6.13 DF_BrakeSystemStatus

- If available, the system shall use the vehicle bus as the data source for DF_BrakeSystemStatus. [6.3.6-V2V-BSMTX-DATAACC-028]
- When braking status for each wheel is available, the system shall set each bit in the wheelBrakes field to 1 (= true) or 0 (= false) based on the brake status for the corresponding wheel, and set the wheelBrakesUnavailable field to 0 (= false). [6.3.6-V2V-BSMTX-DATAACC-029]
- If only one braking status indication is available (individual wheel status not available), the system shall set the bits for all wheels in the wheelBrakes field on or off depending on the braking status and set the wheelBrakesUnavailable field to 0 (= false). [6.3.6-V2V-BSMTX-DATAACC-030]
- When no braking status is available, the system shall set the wheelBrakesUnavailable field to 1 (= true). [6.3.6-V2V-BSMTX-DATAACC-031]
- The system shall set the traction, abs, scs, brakeBoost, and auxBrakes fields in accordance with J2735 [6]. [6.3.6-V2V-BSMTX-DATAACC-032]

6.3.6.14 DF_VehicleSize

- The accuracy of DE_VehicleLength and DE_VehicleWidth data elements in this data frame shall be accurate to within *vSizeAccuracy* of the actual vehicle length and vehicle width, respectively. [6.3.6-V2V-BSMTX-DATAACC-033]

6.3.6.15 DE_VehicleEventFlags

- The latency between the time at which an event condition is met and transmission of the BSM with the corresponding DE_VehicleEventFlags shall be less than *vEventDetectLatency*. [6.3.6-V2V-BSMTX-DATAACC-034]
- The system shall set the Hard Braking event flag when the corresponding event condition is met (see J2735 [6]). If the information is available, the system sets the ABS, Traction Control, and Stability Control event flags when the corresponding event conditions occur, and the system may support additional event flags. [6.3.6-V2V-BSMTX-DATAACC-35]

6.3.6.16 DF_PathHistory

- The system shall populate DF_PathHistory in the BSM Part II DF_VehicleSafetyExtensions data frame as follows:
  - crumbData: DF_PathHistoryPointList [6.3.6-V2V-BSMTX-DATAACC-036]
  - Within the DF_PathHistoryPointList, the system shall populate the DF_PathHistoryPoint data frame with the following data elements [6.3.6-V2V-BSMTX-DATAACC-037]:
    - latOffset: DE_OffsetLL-B18
    - lonOffset: DE_OffsetLL-B18
    - elevationOffset: DE_VertOffset-B12
    - timeOffset: DE_TimeOffset

  - DF_PathHistory and DF_PathHistoryPoint do not include any additional data elements or frames within the BSMs transmitted on channel *vChannelNumber*. [6.3.6-V2V-BSMTX-DATAACC-038]

- The system shall populate DF_PathHistory with the minimum number of Path History (PH) points so that the represented PH distance (i.e., the distance between the first and last PH point) is at least *vMinPHistDistance* and no more than *vMaxPHistDistance* unless initially, or due to the unavailability of position, there is less than *vMinPHistDistance* of PH. [6.3.6-V2V-BSMTX-DATAACC-39]

  Note: 7 points or fewer are used 92.4% of the time based on extensive testing. PathHistoryPoint (see J2735 [6]) requires 8 bytes per point, so the corresponding data will be less than or equal to 56 bytes in over 90% of BSMs.

- The system shall maintain a vehicle path comprised of data elements derived from the positioning system sampled at a periodic time interval (typically the same as the rate of BSM transmissions) representing the vehicle's recent movement over a corresponding distance. [6.3.6-V2V-BSMTX-DATAACC-040]
- The system shall incorporate PH points in DF_PathHistory such that the perpendicular distance between any point on the vehicle path and the straight line connecting two adjacent PH points is less than *vPathPerpendicularDist*. [6.3.6-V2V-BSMTX-DATAACC-041]
- The system shall populate DF_PathHistory with a minimum number of PH points, selected as a subset of the available vehicle path position data, necessary to satisfy the required *vPathPerpendicularDist* between the vehicle path and its PH representation. [6.3.6-V2V-BSMTX-DATAACC-042]
- The system shall populate DF_PathHistory with time-ordered PH points, with the first PH point being the closest in time to the current UTC time. [6.3.6-V2V-BSMTX-DATAACC-043]
- If the number of PH points needed to meet the requirements previously stated in this section exceeds *vMaxPHistPoints*, the system shall populate DF_PathHistory with not more than *vMaxPHistPoints* points from the computed set of points (effectively the distance requirement is relaxed). [6.3.6-V2V-BSMTX-DATAACC-044]

Note: An example PH algorithm is provided in Method One of Appendix A.5.

6.3.6.17 DF_PathPrediction

- The system shall populate the DF_PathPrediction data frame in the BSM Part II DF_VehicleSafetyExtensions data frame as follows [6.3.6-V2V-BSMTX-DATAACC-045]:
  - DE_RadiusOfCurvature
  - DE_Confidence
- The system shall populate DF_PathPrediction with a calculated radius that has less than *vPPredRadiusError* error from the actual radius when the vehicle is in steady state conditions over a range from *vMinCurveRadius* to *vMaxCurveRadius*. [6.3.6-V2V-BSMTX-DATAACC-046]

  Note: For the purposes of the Path Prediction (PP), steady state conditions occur when the vehicle is driving on a curve with a constant radius. In steady state the average of the absolute value of the change of yaw rate over time is smaller than 0.5 deg/s^2.

- The system shall repopulate DF_PathPrediction after a transition from a constant radius of curvature (R1) to a new constant radius of curvature (R2) within *vPPredTransitionTime* under the maximum allowable error bound defined above. [6.3.6-V2V-BSMTX-DATAACC-047]
- The system shall report a "straight path" radius of value 32,767 and confidence of value 100% (corresponds to a value of 200 for the data element) when the transmitting vehicle speed is less than *vStationarySpeedThresh*. [6.3.6-V2V-BSMTX-DATAACC-048]

Note: An example PP algorithm is provided in Appendix A.6. Using constant radii provides sufficiently high confidence to support the target use cases because the PP is updated for every BSM transmission.

6.3.6.18 DE_ExteriorLights

- The system shall set the individual light indications in the DE_ExteriorLights consistent with the available vehicle status data. [6.3.6-V2V-BSMTX-DATAACC-049]

6.3.6.19 Additional Data Elements

- The system shall not include any additional data elements or data frames in transmitted BSMs beyond those required in this standard. [6.3.6-V2V-BSMTX-DATAACC-050]

Note: This requirement is needed to ensure that vehicle safety communications are not subject to undesired channel congestion caused by excessive message size.

6.3.7 Data Persistency (DATAPERSIST)

6.3.7.1 Heading

- The system shall store the last known heading value in persistent memory upon device shutdown. [6.3.7-V2V-BSMTX-DATAPERSIST-001]

  Note: This is to enable the heading to be retrieved upon system device startup.

- The system shall read the heading value from persistent memory upon device startup. [6.3.7-V2V-BSMTX-DATAPERSIST-002]

  Note: This is to enable the use of a last known heading upon system device startup.

Note: These data persistency requirements ensure robustness of the system upon device startup and addresses crash scenarios involving stationary and stopped vehicles.

6.3.7.2 Path History

- The system shall store the last known PH in persistent memory upon device shutdown. [6.3.7-V2V-BSMTX-DATAPERSIST-003]

  Note: This is to enable the PH to be retrieved upon device startup.

- The system shall read the PH from persistent memory upon device startup. [6.3.7-V2V-BSMTX-DATAPERSIST-004]

  Note: This is to enable the use of a last-known PH upon device startup.

6.3.8 Congestion Control (CONGCTRL)

This section specifies the requirements and functional capabilities the system needs to support for congestion control. Refer to Appendix A.8 of this document for additional implementation details for the congestion control algorithm.

- The system shall estimate the *RawCBP* every *vCBPMeasInt,* calculated as the percent of time the channel was busy over the previous *vCBPMeasInt* as follows:

  $$RawCBP = \frac{(100 \times DurationChannelIndicated\,as\,Busy)}{vCBPMeasInt} \quad (1)$$

  Raw channel busy is defined as when the carrier sense mechanism, as defined in [1], indicates the channel is busy. [6.3.8-V2V-BSMTX-CONGCTRL-001]

- When the *RawCBP* is less than *vCBPThreshold*, the system shall transmit using the default transmit timing methodology specified in Section 6.3.3 and a Radiated Transmit Power (RTP) of at least *vRTPmin.* Section 6.4.2 defines the requirements for RTP. [6.3.8-V2V-BSMTX-CONGCTRL-002]

- When the *RawCBP* is greater than or equal to *vCBPThreshold*, the system shall support the congestion control algorithm defined in Sections 6.3.8.1 through 6.3.8.8. [6.3.8-V2V-BSMTX-CONGCTRL-003].

6.3.8.1 Inputs

This section specifies the set of inputs that are used by the congestion control algorithm in the system.

- Smooth Channel Busy Percentage (*CBP*): The system calculates the smooth CBP based on *RawCBP* by filtering out the temporal noise or disturbance in the measurement as follows:

  $$\begin{aligned} CBP(k) = {} & vCBPWeightFactor \times RawCBP(k) + \\ & (1 - vCBPWeightFactor) \times CBP(k-1) \end{aligned} \quad (2)$$

- Packet Error Rate (*PER*): For each RV, the system calculates the sliding window *PER* over an interval of *vPERInterval,* and sub-interval of *vPERSubInterval* as follows:

  Let *δ* be *vPERInterval* and *w* be the *vPERSubInterval*. In Figure 22, *δ* = *n* * *w*, where *n* denotes the *PER* subinterval count. At the end of each sub-interval *w*, the number of missed packets and the number of transmitted packets are calculated for the interval *δ*. The *PER* is calculated at the end of each sub-interval *w* for the last *n* sub-intervals that are part of *δ* as follows:

$$PER_{j-n+1} = \frac{missed\ seq\,\#\ from\, RV_i\ during\,[w_{j-n+1}, w_j]}{total\ extected\, seq\,\#\ from\, RV_i\ during\,[w_{j-n+1}, w_j]} \qquad (3)$$

where $j \geq n$.

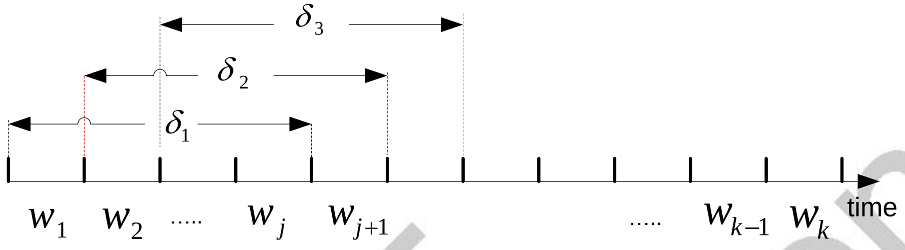


Figure 22: Sliding Window

Note: A sliding window *PER* is used to smooth out the sudden fluctuations in the measurements. The *PER* is calculated using the DE_MsgCount data element contained in each BSM, and is calculated between a receiving HV and a transmitting RV. When calculating the *PER*, consideration must be given to the rollover of DE_MsgCount.

- Vehicle Density in Range (*N*): The system calculates *N* as the number of unique RVs received by the HV over an interval *vPERInterval* that are within *vPERRange* of the HV at the end of each sub-interval *vPERSubInterval*.

  Note: At the end of each sub-interval *vPERSubInterval*, the number of RVs within *vPERRange* of the HV is calculated. Position information received from the RVs, or the coasted RV position, (latest of the two) is used to determine the RVs that are within *vPERRange* from the HV.

- Channel Quality Indicator (Π): The system calculates Π as an average of the *PERs* observed by the HV from all of the RVs within *vPERRange* of the HV over an interval *vPERInterval,* and updated at the end of each sub-interval *vPERSubInterval*.

  Let *AVGPER* be calculated as:

$$AVGPER(k) = \frac{1}{N(k)} \sum_{i=1}^{N(k)} PER_i(k) \qquad (4)$$

  where PER_i is from equation (3) for RV ‘i’ and *N(k)* is the Vehicle Density within *vPERRange*.

  Next, Π is calculated by smoothening *AVGPER* to filter out temporal noise or disturbance in the measurement as follows:

$$\begin{aligned} &\Pi(k) = \lambda_1 \times AVGPER(k) + (1 - \lambda_1) \times \Pi(k-1) \\ &\text{If } \left(\Pi(k) > vPERMax\right) \qquad (5) \\ &\Pi(k) = vPERMax \end{aligned}$$

  where λ_1 is the weight factor *vPERWeightFactor*, $\Pi(k)$ is the channel quality indicator for the current interval window. Note that, if $\Pi(k)$ exceeds *vPERMax*, then it is set to *vPERMax*.

6.3.8.2 Calculate Tracking Error

This section specifies the set of steps that calculate the tracking error in the congestion control algorithm for the system. Note that the tracking error is communications-induced and independent of the positioning system tracking error. The system performs the following operations every *vTxRateCntrlInt.*

- The system estimates the position of the HV at the current time, defined as HV local estimator, per Appendix A.3, using the configuration parameters *vHVLocalPosEstIntMin* and *vHVLocalPosEstIntMax*.
- The system makes an assumption of the latest HV state information received by the RVs based on a Bernoulli trial corresponding to the quality of channel indicator per Appendix A.8.1.
- Using the latest HV state information assumption at RVs, the system estimates the position of the HV at the current time, defined as HV remote estimator, per Appendix A.3, indicating where the HV believes the RVs think the HV is located at the current time. The HV remote estimator uses the configuration parameters *vHVRemotePosEstIntMin* and *vHVRemotePosEstMax*.
- The system calculates the tracking error *e(k)*, between where the HV believes its current position is and where the HV believes RVs think the HV is located at the current time. It is also known as the suspected, expected or estimated tracking error between the HV local estimator and the HV remote estimator.

  Note: Tracking error is the 2-D distance between HV local estimator position and output of the HV remote estimator position. A reference implementation is shown in Appendix A.8.2.

6.3.8.3 Calculate Transmission Probability

- The system performs the following operations every *vTxRateCntrlInt.*
- The system calculates a transmission probability using the tracking error calculation as follows:

$$p(k)=\left\{\begin{array}{ll} 1-\exp(-\alpha\times|e(k)-T|^2) & \text{if } T\le e(k) < S \\ 1 & \text{if } e(k)\ge S \\ 0 & \text{otherwise} \end{array}\right\} \qquad (6)$$

where *T* is the minimum communications-induced tracking error threshold, *vTrackingErrMin*, α is the error sensitivity *vErrSensitivity,* and *S* is the communications-induced tracking error saturation value *vTrackingErrMax*.

Note: The design rationale of equation (6) is that, when the tracking error is below the pre-defined threshold *T*, an HV does not broadcast any state information at all and leaves the channel to be used by other HVs with larger tracking error. When the tracking error exceeds this threshold, the larger magnitude of violation would result in a higher transmission probability. Since not all HVs have the same tracking error, they will use different levels of transmission probabilities to broadcast self-state information.

6.3.8.4 Calculate Maximum Inter-Transmit Time (Max_ITT)

This section specifies the steps involved in calculation of the maximum message transmission interval *Max_ITT*. The system performs the following operations every *vTxRateCntrlInt.*

- The system smoothens the calculated current vehicle density in range, *N(k),* as follows:

$$N_s(k)=\lambda_2\times N(k)+(1-\lambda_2)\times N_s(k-1) \qquad (7)$$

where λ_2 is the weight factor *vDensityWeightFactor*, and $N_s(k)$ is the smoothened current vehicle density in range.

- The system calculates *Max_ITT* as follows:

$$Max\_ITT(k)=\begin{cases} 100 & N_s(k)\le B \\ 100\times\dfrac{N_s(k)}{\mathrm{B}} & B < N_s(k) < \dfrac{vMax\_ITT}{100}\times B \\ vMax\_ITT & \dfrac{vMax\_ITT}{100}\times B\le N_s(k) \end{cases} \qquad (8)$$

where *Max_ITT* is the message transmission interval in milliseconds*, B* is the density co-efficient *vDensityCoefficient*, *vMax_ITT* is the maximum transmission interval*.*

Note: The HV decreases its *Max_ITT* in regions of lower vehicle density and increases its *Max_ITT* in regions of higher vehicle density. By doing so, BSMs generated due to high tracking error have more access to the channel in regions of higher density.

6.3.8.5 Transmission Decision

This section specifies the steps involved in making the transmission decision. The system performs the following operations every *vTxRateCntrlInt.*

- The system makes a transmission decision using the transmission probability calculation, considering status of events if any, and also taking into account the change in computed *Max_ITT*. The following logic is used to make the transmission decision:

  Transmission based on Event: If the message is generated by an event and the conditions of the event are still present, then

  - Set TxDecision_Event = 1

  Transmission based on Vehicle Dynamics: Use a uniform random number generator for a Bernoulli trial, *rand().* If the outcome of the Bernoulli trial is true, and the time for the next scheduled message is greater than or equal to *vRescheduleTh,* i.e.

  If (*rand()<=p(k)* && (*NextScheduledMsgTime – CurrentTime*)*>=vRescheduleTh*),

  then

  - Set TxDecision_Dynamics = 1

  Transmission based on change in *Max_ITT*: Changes in the value of *Max_ITT* affect the transmission decision as follows:

  If (*NextScheduledMsgTime* - (*LastTxTime* + *Max_ITT*) *>= vRescheduleTh*),

  - Set TxDecision_Max_ITT = 1

  where, *NextScheduledMsgTime* is the UTC time in milliseconds at which the next message is scheduled for transmission, *CurrentTime* is the current UTC time in milliseconds, *LastTxTime* is the UTC time in milliseconds when the previous message was transmitted by the system, and *vRescheduleTh* is the threshold in milliseconds used in the transmission decision.

6.3.8.6 Reschedule Transmission

This section specifies the steps involved to reschedule message transmissions. The system performs the following operations every *vTxRateCntrlInt* following the Transmission Decision function.

- The system reschedules message transmissions as and when required using the following logic:

  If the transmission decision is based on an event (as defined in this document) or based on vehicle dynamics, the previously scheduled message is cancelled and a message is rescheduled immediately, i.e.

  If TxDecision_Event == 1 or TxDecision_Dynamics == 1

  - Cancel scheduled transmission
  - Schedule transmission now, i.e. NextScheduledMsgTime = CurrentTime

  If the transmission decision is based on change in Max_ITT, the previously scheduled message is cancelled and a message is rescheduled using the current Max_ITT, i.e.

  If TxDecision_Max_ITT == 1

  - Cancel scheduled transmission
  - Schedule next transmission at NextScheduledMsgTime = LastTxTime + Max_ITT(k)

  Else, message is transmitted as previously scheduled, i.e.

  If TxDecision_Event == 0 and TxDecision_Dynamics == 0 and TxDecision_Max_ITT == 0

  - No change to scheduled message

6.3.8.7 Transmission Power

This section specifies the steps involved to determine the transmission power for the transmitted BSM.

Note: For the congestion control requirements of Section 6.3.8, the term "transmission power" refers to the Radiated Transmit Power (RTP).

The system shall perform the following operations when the transmission timer expires based on NextScheduledMsgTime.

- The system determines the BSM transmission power calculated as follows:

  For transmission of messages based on an event (as defined in this document) or based on vehicle dynamics, transmission power P_{k+1} shall be set to P_{max} i.e.

  If TxDecision_Event == 1 or TxDecision_Dynamics == 1
  $P_{k+1} = P_{max}$

  For transmission of scheduled messages based on Max_ITT, the transmission power P_{k+1} is calculated using the smooth *CBP* as:

$$f(U_k) = \begin{cases} P_{max} & U_k \le U_{min} \\ P_{\max} - (\frac{P_{max} - P_{\min}}{U_{max} - U_{min}}) \times (U_k - U_{min}) & U_{min} < U_k < U_{max} \\ P_{min} & U_{max} \le U_k \end{cases} \quad (9)$$

$$P_{K+1} = P_k + \eta.(f(U_k) - P_k) \quad (10)$$

  where U_k is the smooth *CBP* from equation (2) at the current time, P_{max} is the maximum transmission power, *vPMax* , P_{min} is the minimum transmission power, *vPMin*, U_{min} is the lower threshold considered for channel utilization, *vMinChanUtil*, U_{max} is the higher threshold considered for channel utilization, *vMaxChanUtil*, and η is the Stateful Utilization-based Power Adaptation (SUPRA) gain, *vSUPRAGain.*

- The system transmits the next BSM at the calculated transmit power P_{k+1} .

Note: If P_{k+1} is higher than the system supports, the system transmits at the highest supported transmit power.

6.3.8.8 Transmit BSM

This section specifies the final step to transmit the BSM using the calculated transmission power at the scheduled time, and schedule the next BSM to be transmitted. The system performs the following operations when transmission timer expires based on NextScheduledMsgTime.

- The system transmits the BSM using the calculated Tx power.
- The system assigns *LastTxTime = CurrentTime.*
- The system schedules the next BSM to be transmitted at

NextScheduledMsgTime = LastTxTime + Max_ITT(k)

6.4 RF Performance Requirements (RFPERF)

6.4.1 DSRC Transmit Power Accuracy and Radiated Transmit Power (DSRCTX)

6.4.1.1 Transmit Power Accuracy

- The system shall have the capability to use transmit power settings to control the conducted transmit power of the transmitter over the range of conducted output power that maps to the range of Radiated Transmit Power (RTP) from *vPMin* to *MaxSupportedCongCtrlRTP* as specified in Section 6.4.1.3 in *vRTPCongCtrlStep* steps. [6.4.1-V2V-RFPERF-DSRCTX-001]

Note 1: This requirement is included because 802.11 [1] does not specify transmit power step accuracy below the maximum conducted power value.

Note 2: It is more cost-effective to verify compliance with transmit power step accuracy at the transmitter level instead of the final vehicle implementation stage.

6.4.1.2 Radiated Transmit Power (RTP)

- The system shall be capable of transmitting with a maximum RTP of at least *vRTPmin*. The maximum RTP, measured at the maximum transmit power setting, is calculated by averaging measured RTP at discrete spacings of *vRTPElev* degrees in elevation and *vRTPAzim* degrees in azimuth, in a sector from *vMinEl* to *vMaxEl* degrees of elevation with respect to the horizon, and 0 to 360 degrees of azimuth. [6.4.1-V2V-RFPERF-DSRCTX-002]

  Note 1: The maximum transmitter power setting used to obtain the maximum RTP should be noted as it gives the mapping used by the system supplier to set lower RTP values. The system supplier in self-certification testing will determine the lower transmit power settings needed to obtain low RTP values for congestion control.

  Note 2: The maximum RTP specification presumes closure of a line of sight (LOS) link between two DSRC vehicles separated by 300m; with a nominal receive sensitivity of -92dBm, measured at the radio connector on the system housing.

6.4.1.3 Range of RTP

- The system shall support a range of RTP levels controllable by the transmitter power setting from *vPMin* to *MaxSupportedCongCtrlRTP* in steps of *vRTPCongCtrlStep. MaxSupportedCongCtrlRTP* is defined as the lower of the maximum RTP the system supports (6.4.1.2) and *vPMax.* [6.4.1-V2V-RFPERF-DSRCTX-003]

  Note 1: This requirement supports the congestion control requirements in Section 6.3.8. The mapping to achieve the lower RTP values is system supplier dependent.

  Note 2: It is not a requirement that RTP be measured at all RTP congestion control steps at the final system integration level. This is because full compliance with transmit power accuracy steps has already been established (6.4.1.1) and a full characterization of max RTP at max transmit power setting over azimuth and elevation has been made (6.4.1.2).

6.4.2 DSRC Receive Sensitivity (DSRCRXSENS)

- The system shall have a Receive sensitivity of ≤ *vRxSens* at 10% Packet Error Rate (PER), measured at the radio connector on the system housing. The receive sensitivity assumes the 802.11 [1] burst rate of 6Mbps. [6.4.2-V2V-RFPERF-DSRCRXSENS-001]

6.4.3 DSRC Polarization (DSRCPOL)

The DSRC Radio subsystem shall use antenna(s) with a nominally vertical polarization pattern. [6.4.3-V2V-RFPERF-DSRCPOL-001]

6.5 Security and Privacy Tx Requirements (SECPRIV)

6.5.1 Identification Randomization (IDRAND)

- The system shall randomize its DSRC radio Medium Access Control (MAC) address upon power-up. [6.5.1-V2V-SECPRIV-IDRAND-001]
- If the certificate used to sign the BSM has changed since transmitting the most recent BSM, the system shall re-randomize its DSRC radio MAC. [6.5.1-V2V-SECPRIV-IDRAND-002]

  Note: DE_MsgCount, DE_TemporaryID and the DSRC radio MAC address are randomly reinitialized after the security certificate changes. Refer to Sections 6.3.6.3 and 6.3.6.4 for randomization requirements for the BSM DE_MsgCount and DE_Temporary ID fields.

6.5.2 BSM Signing (BSMSIGN)

- The system shall sign every BSM using the security credentials defined by 1609.2 [2], as profiled in 6.1.2. [6.5.2-V2V-SECPRIV-BSMSIGN-001]

- The system shall attach a certificate or certificate digest to every BSM as defined by 1609.2 [2]. [6.5.2-V2V-SECPRIV-BSMSIGN-002]
- The system shall attach a certificate to a BSM when the time interval between the current BSM and the generation of a previous BSM with an attached certificate (not certificate digest) is greater than or equal to *vMaxCertDigestInterval*. [6.5.2-V2V-SECPRIV-BSMSIGN-003]
- The system shall attach the entire certificate (not a certificate digest) to the BSM when an event flag is set in DE_Event_Flags. [6.5.2-V2V-SECPRIV-BSMSIGN-004]
- The system shall not transmit BSMs when it has no valid certificates. [6.5.2-V2V-SECPRIV-BSMSIGN-005]

6.5.3 BSM Cryptographic Verification (BSMVERIFY)

- If a system chooses to verify a BSM, the system shall verify the BSM using the signature of the BSM and the attached certificate. If a certificate digest instead of a certificate is received with the BSM, the system verifies the BSM using the certificate corresponding to the digest that was received with an earlier BSM. [6.5.3-V2V-SECPRIV-BSMVERIFY-001]

6.5.4 Certificate Change (CERTCHG)

- To preserve privacy, the system shall not use the same certificate for more than 5 consecutive minutes, unless during an event condition. The system waits until the event condition is no longer met to change its certificate. [6.5.4-V2V-SECPRIV-CERTCHG-001]
- The system shall not change its certificate as long as one or more event conditions is met. [6.5.4-V2V-SECPRIV-CERTCHG-002]

Note: Certificates are typically rotated every five minutes, and the rotation order typically changes every 100 minutes. In a light duty passenger vehicle, each system is typically equipped with 20 active certificates per week. DE_MsgCount, DE_Temporary ID and the DSRC radio MAC address are simultaneously randomly reinitialized when the security certificate changes.

6.5.5 Certificate Revocation (CERTREV)

- The system shall not transmit any messages with a certificate that is included in a Certificate Revocation List (CRL) that has been received and verified by the system. [6.5.5-V2V-SECPRIV-CERTREV-001]

6.6 Security Management (SECMGMT)

The system interfaces to a Device Configuration Manager (DCM) function for bootstrap processing and to the SCMS to request and download pseudonym certificates. Refer to [9] and [10] for a description of the DCM and SCMS.

The DCM function is expected to be a proprietary capability developed by device manufacturers to support the functions described in Section 6.6.1. The system to DCM interface is expected to be trusted and proprietary.

The system to SCMS protocol will be described in an interface specification published by the SCMS entity. The system uses the interface specification protocol to communicate with the SCMS, or any other secure protocol supported by the SCMS. This specification describes the system functions based on Bootstrap: Initialization and Enrollment Processing (Informative).

The interface between the system and the Device Configuration Manager (DCM) may be via a direct, wired, or wireless communication. The system can interface with the SCMS via DSRC, Cellular, or other wireless network. The connection types are outside of the scope of this specification.

For the purpose of the security management requirements in this specification, the system is assumed to have access to a DCM connection during the bootstrap process and to an SCMS connection for subsequent security management functions. The SCMS connection is not always available on a continuous basis (e.g., if the system is using DSRC and is outside the range of an RSE with connectivity to the SCMS).

The system needs to be capable of resolving IP addresses using a secure Domain Name System (DNS). The methodology for doing this is outside the scope of this specification.

6.6.1 Bootstrap: Initialization and Enrollment Processing (Informative)

The bootstrap process takes place in a secure environment. The exact implementation of the bootstrap process is proprietary and outside the scope of this standard.

6.6.1.1 Initialization Processing

- The system interfaces to a DCM to acquire the Root Certificate Authority (CA) certificate.
- The system interfaces to a DCM to acquire the Uniform Resource Locator (URL) of the Registration Authority (RA), Pseudonym Certificate Authority (PCA) certificates, Intermediate Certificate Authority (ICA) certificates, Misbehavior Authority (MA) certificate, Certificate Revocation List Generator (CRLG) certificate, security policies, and the current global Certificate Revocation List (CRL).
- The system is expected to obtain the RA certificate from the DCM. If the system does not receive an RA certificate from the DCM, it requests the certificate from the RA.
- The system resolves the IP address of the RA using a secure Domain Name System (DNS).

6.6.1.2 Enrollment Processing

- After a system completes initialization, it interfaces to a DCM to acquire an Enrollment certificate.

  The system generates an enrollment public/private key pair, and provides the public key to the DCM for use in generating the Enrollment certificate. Alternatively, an external-to-the-device and trusted entity may generate a public/private key pair and provide them to the system.

6.6.2 Certificate Loading (CERTLOAD)

- The system securely generates encryption and signing key pairs
- The system obtains pseudonym certificates from the SCMS over a secure interface.
- The system obtains new batches of pseudonym certificates when necessary and connectivity to the SCMS is available.
- The system shall be capable of securely updating root CA certificates. [**Error! Reference source not found.**-V2V-SECMGMT-CERTLOAD-001]

6.6.3 Certificate Storage (CERTSTORE)

- The system shall have at least *vCertNvMemSize* of non-volatile memory for storage of pseudonym certificates. [6.6.3-V2V-SECMGMT-CERTSTORE-001]
- The system shall have at least *vSecMemSize* of secure memory available for data requiring secure storage. [6.6.3-V2V-SECMGMT-CERTSTORE-002]
- The system shall store the individual, pseudonym certificates, the RA address, RA, Intermediate CA, and PCA certificates, system configurations, and security policies in non-volatile memory. [6.6.3-V2V-SECMGMT-CERTSTORE-003]
- The system shall store the Root CA certificate, Enrollment certificate, and system private keys in secure, tamper evident, non-volatile memory. [6.6.3-V2V-SECMGMT-CERTSTORE-004]

  Note: Tamper evidence requirements are defined by FIPS 140-2 [16]

6.6.4 Certificate Revocation List Loading (CRLLOAD)

- The system shall verify all CRL messages on receipt as defined by 1609.2 [2]. [6.6.4-V2V-SECMGMT-CRLLOAD-001]
- The system shall store the most up-to-date CRL information it has received in non-volatile memory, subject to the minimum storage requirements below. [6.6.4-V2V-SECMGMT-CRLLOAD-002]
- The system shall have at least *vCrlStoreSize* of non-volatile memory for storing the CRL. [6.6.4-V2V-SECMGMT-CRLLOAD-003]

  Note: The minimum CRL storage requirement (see Section 7) enables the storage of 10,000 CRL entries of 40 bytes each.

6.6.5 Secure Hardware (SECHW)

- The system shall incorporate secure hardware that complies with FIPS 140-2 [16] requirements as specified for security level 2:

- Operator authentication
- Physical security
- Operating system requirements
- Cryptographic key management
- Design assurance

[6.6.5-V2V-SECMGMT-SECHW-001]

- The system shall perform all private key operations within the secure hardware. [6.6.5-V2V-SECMGMT-SECHW-002].

7. PARAMETER SETTINGS FOR V2V SAFETY

This section contains the values assigned to the parameters identified in Section 6 of this standard (Table 21).

Table 21: Parameter Settings for V2V Safety

Section Reference(s)	Parameter	Value	Rationale(s)
6.1.1, 6.3.2	vChannelNumber	172	1
6.1.2.2.2	vP2pcd_maxResponseBackoff	.25 seconds	7
6.1.2.2.2	vP2pcd_responseActiveTimeout	.25 seconds	7
6.1.2.2.2	VP2pcd_requestActiveTimeout	.25 seconds	7
6.1.2.2.2	VP2pcd_currentlyUsedTriggerCertificateTime	1 minutes	7
6.1.2.2.2	vP2pcd_responseCountThreshold	3	7
6.2.1	vPosDetRate	10 Hertz	2, 3
6.3.2	vDataRate	6 Mbps	3, 4, 5
6.3.3	vBSMTxRate	10 Hertz	2
6.3.3	vTxRand	5 milliseconds	4
6.3.3	vBSMTxRateMin	1 Hertz	4
6.3.3	vBSMTxRateMax	10 Hertz	4
6.2.4, 6.3.6.4	vTimeAccuracy	1 milliseconds	2, 3
6.3.6.4	vMaxPosAge	150 milliseconds	3
6.3.6.5	vPosAccuracy	1.5 meters	2, 3
6.3.6.6	vElevAccuracy	3 meters	2, 3
6.3.6.8	vSpeedAccuracy	1 kph	2, 3
6.3.6.9	vHeadAccuracyA	2 degrees	2, 3
6.3.6.9	vHeadAccuracyB	3 degrees	2, 3
6.3.6.9	vHeadingSpeedThresh	45 kph	2, 3
6.3.6.9	vHeadLatchThresh	4 kph	2, 3
6.3.6.9	vHeadUnlatchThresh	5 kph	2, 3
6.3.6.10	vStWhAnAccuracy	5 degrees	2, 3

Section Reference(s)	Parameter	Value	Rationale(s)
6.3.6.11	vAccelAccuracy	0.3 meters/second^2	2, 3
6.3.6.11	vVertAccelAccuracy	1 meters/second^2	2, 3
6.3.6.11	vYawRateAccuracy	0.5 degrees/second	2, 3
6.3.6.13	vSizeAccuracy	0.2 meters	2, 3
6.3.6.14	vEventDetectLatency	250 milliseconds	2
6.3.6.15	vMinPHistDistance	300 meters	2, 5
6.3.6.15	vMaxPHistDistance	310 meters	2, 5
6.3.6.15	vPathPerpendicularDist	1 meter	2
6.3.6.15	vMaxPHistPoints	23	J2735 [6]
6.3.6.16	vPPredRadiusError	2%	2, 3
6.3.6.16	vMinCurveRadius	100 meters	2, 3
6.3.6.16	vMaxCurveRadius	2,500 meters	2, 3
6.3.6.16	vPPredTransitionTime	4 seconds	2, 3
6.3.6.16	vStationarySpeedThresh	1 meter/second	2, 3
6.3.8	vCBPMeasInt	100 msec	4
6.3.8	vCBPThreshold	20%	4
6.3.8.1	vCBPWeightFactor	0.5	4
6.3.8.1	vPERInterval	5000 msec	4
6.3.8.1	vPERSubInterval	1000 msec	4
6.3.8.1	vPERRange	100 m	4
6.3.8.1	vPERMax	0.3	4
6.3.8.1	vPERWeightFactor	0.9	4
6.3.8.2, 6.3.8.3, 6.3.8.4, 6.3.8.5, 6.3.8.6	vTxRateCntrlInt	100 msec	4
6.3.8.2	vHVLocalPosEstIntMin	50 msec	4
6.3.8.2	vHVLocalPosEstIntMax	150 msec	4
6.3.8.2	vHVRemotePosEstIntMin	50 msec	4
6.3.8.2	vHVRemotePosEstIntMax	3000 msec	4
6.3.8.3	vTrackingErrMin	0.2 m	4
6.3.8.3	vTrackingErrMax	0.5 m	4
	vErrSensitivity	75	4
6.3.8.4	vMax_ITT	600 msec	4
6.3.8.4	vDensityWeightFactor	0.05	4
6.3.8.4	vDensityCoefficient	25	4
6.3.8.5	vRescheduleTh	25 msec	4
6.3.8.7	vMinChanUtil	50%	4

Section Reference(s)	Parameter	Value	Rationale(s)
6.3.8.7	vMaxChanUtil	80%	4
6.3.8.7, 6.4.1.1, 6.4.1.3	vPMin	10 dBm	4
6.3.8.7, 6.4.1.3	vPMax	20 dBm	4
A.6.1	vMaxSuccessiveFail	3	4
6.3.8.7	vSUPRAGain	0.5	4
6.4.1.1, 6.4.1.2	vRTPCongCtrlStep	1 dB	4
6.4.1.1, 6.4.1.2	MaxSupportedCongCtrlRTP	Implementation dependent	4
6.4.1.2	vRTPmin	17 dBm	4
6.4.1.2	vRTPElev	2 degrees	4
6.4.1.2	vRTPAzim	1 degree	4
6.4.1.2	vMinEl	-6 degrees	4
6.4.1.2	vMaxEl	+10 degrees	4
6.4.2	vRxSens	-92 dBm	4
6.6.3	vCertNvMemSize	500 kilobytes	6
6.6.3	vSecMemSize	100 kilobytes	6
6.6.4	vCrlStoreSize	400 kilobytes	6

Rationales:

1) The setting is the RF channel designated for public safety applications involving safety of life and property according to FCC rules [7].
2) The setting is based on the need to provide accurate and timely safety alerts for the use cases described in Section 4 (see [12]).
3) The setting was obtained by extensively testing commercially available equipment and automotive sensors in a wide variety of driving environments, and the numbers were proven to be reasonable based on the equipment and sensor capabilities, while also supporting the use cases described in Section 4. (See references [8], [12] – [14]).
4) The parameter setting improves RF performance (reduces packet collisions) and/or is based on extensive congestion control research (see [12]).
5) The setting is based on the design range of DSRC in the V2V environment, which is 300 meters (see [12]).
6) The settings are derived from calculations based on the size of certificates and/or best engineering judgement (see [9], [10]).
7) The setting is based on recommendations from IEEE 1609.

APPENDIX A

A.1 IMPLEMENTATION CONFORMANCE STATEMENT

A conformance table is provided in Table 22. The “Conformant?” column is intended to be filled out by an implementer or tester to indicate compliance with mandatory and optional features.

Table 22: Implementation Conformance Table

Section (this standard)	**Requirement (Req.) Category**	**Req. Number**	**Mandatory/ Optional/ (M/O)**	**Conform -ant? (Y/N)**	**Requirement or Section Title (this standard)**
6.1	**Standards compliance**				
6.1.1	*IEEE 802.11: General description*				
	V2V-STD-802.11	001	M		STA transmission of data frames outside the context of a BSS
6.1.1	*IEEE 802.11: MAC service definition*				
	V2V-STD-802.11	002	M		Overview of MAC services
		003	M		MAC data service specification
6.1.1	*IEEE 802.11: Layer management*				
	V2V-STD-802.11	004	M		Reset
		005	O		Get TSF timer
6.1.1	*IEEE 802.11: PHY service specification*				
	V2V-STD-802.11	006	O		Scope
		007	O		PHY functions
		008	O		Detailed PHY service specification
6.1.1	*IEEE 802.11: Frame Formats*				
	V2V-STD-802.11	009	M		General requirements
		010	M		MAC frame formats
6.1.1	*IEEE 802.11: Format of individual frame types*				
	V2V-STD-802.11	011	O		Format of control frames
		012	O		ACK frame format
		013	M		Data Frames
		014	M		Data Frame Format
		015	M		EDCA Parameter Set element
6.1.1	*IEEE 802.11: MAC sublayer functional description*				
	V2V-STD-802.11	016	M		Hybrid Coordination Function
		017	M		Multirate support
6.1.1	*IEEE 802.11: HCF*				
	V2V-STD-802.11	018	M		General
		019	M		HCF contention-based channel access (EDCA)
6.1.1	*IEEE 802.11: MLME*				
	V2V-STD-802.11	020	M		Synchronization
		021	M		STAs communicating data frames outside the context of a BSS
		022	M		Orthogonal frequency division multiplexing (OFDM) PHY specification
		023	M		ASN.1 encoding of the MAC and PHY MIB
6.1.1	*IEEE 802.11: Regulatory References*				
	V2V-STD-802.11	024	M		External regulatory references
		025	M		External regulatory references
		026	M		Transmit and receive in-band and out-of-band spurious emissions
		027	M		Transmit power levels
		028	M		Transmit spectrum mask

Section (this standard)	**Requirement (Req.) Category**	**Req. Number**	**Mandatory/ Optional/ (M/O)**	**Conform -ant? (Y/N)**	**Requirement or Section Title (this standard)**
6.1.1	*IEEE 802.11: Country elements and operating classes*				
	V2V-STD-802.11	029	M		Country information and operating classes
		030	O		Country information and operating classes
		031	M		5.9 GHz band in the United States (5.850-5.925 GHz)
6.1.2	*IEEE 1609.2*				
Use the 1609.2 [2] PICS for this section					
6.1.3	*IEEE 1609.3*				
Use the 1609.3 [3] PICS for this section					
6.1.4	*IEEE 1609.4*				
Use the 1609.4 [4] PICS for this section					
6.1.5	*IEEE 1609.12: WAVE identifiers*				
	V2V-STD-1609.12	001	M		Provider service identifier (PSID)
		002	O (SCMS only)		Provider service identifier (PSID)
		003	M		Ethertype
		004	O (SCMS only)		Ethertype
6.1.6	*SAE J2735: Message encoding*				
	V2V-STD-J2735	001	M		Message Encoding
6.1.6	*SAE J2735: Message_MessageFrame*				
	V2V-STD-J2735	002	M		DE_DSRC_MessageID
		003	M		Message: MSG_BasicSafetyMessage (BSM)
		004	M		Message: MSG_BasicSafetyMessage (BSM)
6.1.6	*SAE J2735: Data frames*				
	V2V-STD-J2735	005	M		Data Frame: DF_AccelerationSet4Way
		006	M		Data Frame: DF_BrakeSystemStatus
		007	M		Data Frame: DF_BSMcoreData
		008	M		Data Frame: DF_PathHistory
		009	M		Data Frame: DF_PathHistoryPointList
		010	M		Data Frame: DF_PathHistoryPoint
		011	M		Data Frame: DF_PathPrediction
		012	M		Data Frame: DF_PositionalAccuracy
		013	M		Data Frame: DF_VehicleSafetyExtensions
		014	M		Data Frame: DF_VehicleSize
6.1.6	*SAE J2735: Data elements*				
	V2V-STD-J2735	015	M		Data Element: DE_Acceleration
		016	M		Data Element: DE_AntiLockBrakeStatus
		017	M		Data Element: DE_AuxiliaryBrakeStatus
		018	M		Data Element: DE_BrakeAppliedStatus
		019	M		Data Element: DE_BrakeBoostApplied
		020	M		Data Element: DE_Confidence
		021	M		Data Element: DE_DSecond
		022	M		Data Element: DE_Elevation
		023	O		Data Element: DE_ExteriorLights
		024	M		Data Element: DE_Heading
		025	M		Data Element: DE_Latitude

Section (this standard)	Requirement (Req.) Category	Req. Number	Mandatory/ Optional/ (M/O)	Conform -ant? (Y/N)	Requirement or Section Title (this standard)
		026	M		Data Element: DE_Longitude
		027	M		Data Element: DE_MsgCount
		028	M		Data Element: DE_OffsetLL-B18
		029	M		Data Element: DE_RadiusOfCurvature
		030	M		Data Element: DE_SemiMajorAxisAccuracy
		031	M		Data Element: DE_SemiMajorAxisOrientation
		032	M		Data Element: DE_SemiMinorAxisAccuracy
		033	M		Data Element: DE_Speed
		034	M		Data Element: DE_StabilityControlStatus
		035	M		Data Element: DE_SteeringWheelAngle
		036	M		Data Element: DE_TemporaryID
		037			DE_TimeOffset
		038	M		Data Element: DE_TractionControlStatus
		039	M		Data Element: DE_TransmissionStatus
		040	M		Data Element: DE_VehicleEventFlags
		041	M		Data Element: DE_VehicleLength
		042	M		Data Element: DE_VehicleWidth
		043	M		Data Element: DE_VerticalAcceleration
		044	M		DE_VertOffset-B12
		045	M		Data Element: DE_YawRate
6.2	**Position and timing requirements**				
6.2.1	V2V-POSTIM-POSDETER	001	M		Position determination
		002	M		
		003	M		
6.2.2	V2V-POSTIM-WAAS	001	M		WAAS
6.2.3	V2V-POSTIM-COORDSYSREF	001	M		Coordinate system reference
6.2.4	V2V-POSTIM-SYSTIMCOORD	001	M		System time coordination
		002	M		
		003	M		
6.3	**BSM transmission requirements**				
6.3.1	BSMTX-BSMCONT	001	M		BSM contents
		002	M		
		003	M		
		004	M		
		005	M		
6.3.2	V2V-BSMTX-CHDATARATE	001	M		Channel and data rate
		002	M		
6.3.3	V2V-BSMTX-TXTIM	001	M		Transmit timing
		002	M		
		004	M		
		005	M		

Section (this standard)	Requirement (Req.) Category	Req. Number	Mandatory/ Optional/ (M/O)	Conform -ant? (Y/N)	Requirement or Section Title (this standard)
		003	M		
6.3.4	V2V-BSMTX-UPEDCA	001	M		User Priority and EDCA Settings
		002	M		
		003	M		
6.3.5	V2V-BSMTX-MINTX	001	M		Minimum Transmission Criteria
6.3.6	*Data element accuracy*				
6.3.6.1	V2V-BSMTX-DATAACC	001	M		DE_DSRC_MessageID
6.3.6.2		002	M		DE_DSecond
		003	M		
		004	M		
6.3.6.3		005	M		DE_MsgCount
		006	M		
		007	M		
6.3.6.4		008	M		DE_TemporaryID
		009	M		
		010	M		
6.3.6.5		011	M		DE_Latitude & DE_Longitude
		012	M		
6.3.6.6		013	M		DE_Elevation
		014	M		
6.3.6.7		015	M		DF_PositionalAccuracy
		016	M		
6.3.6.8		017	M		DE_Speed
6.3.6.9		018	M		DE_Transmission
6.3.6.10		019	M		DE_Heading
		020	M		
		021	M		
		022	M		
		023	M		
6.3.6.11		024	M		DE_SteeringWheelAngle
6.3.6.12		025	M		DF_AccelerationSet4Way
		026	M		
		027	M		
6.3.6.13		028	M		DF_BrakeSystemStatus
		029	M		
		030	M		
		031	M		
		032	M		
6.3.6.14		033	M		DF_VehicleSize
6.3.6.15		034	M		DE_VehicleEventFlags
		035	M		
6.3.6.16		036	M		DF_PathHistory
		037	M		
		038	M		
		039	M		
		040	M		
		041	M		
		042	M		
		043	M		
		044	M		
6.3.6.17		045	M		DF_PathPrediction
		046	M		

Section (this standard)	Requirement (Req.) Category	Req. Number	Mandatory/ Optional/ (M/O)	Conform -ant? (Y/N)	Requirement or Section Title (this standard)
		047	M		
		048	M		
6.3.6.18		049	M		DE_ExteriorLights
6.3.6.19		050	M		Additional Data Elements
6.3.7	V2V-BSMTX-DATAPERSIST	001	M		Data Persistency
		002	M		
6.3.8	V2V-BSMTX-CONGCTRL	001	M		Congestion Control
		003	M		
		002	M		
6.4	**RF Performance requirements**				
6.4.1	*Transmit Power*				
6.4.1.1	V2V-RFPERF-DSRCTX	001	M		Transmit Power Accuracy
6.4.1.2		002	M		RTP
6.4.1.3		003	M		Range of RTP
6.4.2	V2V-RFPERF-DSRCRXSENS	001	M		Receive Sensitivity
6.4.3	V2V-RFPERF-DSRCPOL	001	M		DSRC Polarization
6.5	**Security and Privacy Tx Requirements**				
6.5.1	V2V-SECPRIV-IDRAND	001	M		Identification Randomization
		002	M		
6.5.2	V2V-SECPRIV-BSMSIGN	001	M		BSM Signing
		002	M		
		003	M		
		004	M		
		005	M		
6.5.3	V2V-SECPRIV-BSMVERIFY	001	O		BSM Verification
6.5.4	V2V-SECPRIV-CERTCHG	001	M		Certificate Change
		002	M		
6.5.5	V2V-SECPRIV-CERTREV	001	M		Certificate Revocation
6.6	**Security management**				
6.6.2	V2V-SECMGMT-CERTLOAD	001	M		Certificate Loading
6.6.3	V2V-SECMGMT-CERTSTORE	001	M		Certificate Storage
		002	M		
6.6.4	V2V-SECMGMT-CERTLOAD	001	M		CRL Loading
		002	M		
		003	M		
6.6.5	V2V-SECMGMT-SECHW	001	M		Secure Hardware
		002	M		

A.2 COORDINATE TRANSFORMATION

FUNCTION

ConvertXYtoLatLon(…)

INPUT

RefLat	= e.g., REF_LATITUDE (rad)
RefLon	= e.g., REF_LONGITUDE (rad)
RefHeading	= e.g., REF_HEADING (rad)
Y	= ACROSS_DISTANCE (m w.r.t. REF LATLON)
X	= AHEAD_DISTANCE (m w.r.t. REF LATLON)

```
a = 6378137;                                   # semi-major axis of earth
f = 0.003353;                                  # flattening
f1 = (f*(2-f))^0.5;                            # eccentricity
f2 = a*(1-f1^2)/(1-f1^2*(sin(RefLat))^2)^(3/2);   # radius of earth in meridian
f3 = a/(1-f1^2*(sin(RefLat))^2)^(1/2);            # radius of earth in prime vertical

E = (cos(RefHeading)*Y + sin(RefHeading)*X;
N = (cos(RefHeading)*X - sin(RefHeading)*Y;
```

OUTPUT

NEW_LATITUDE (rad)	= (1/f2)*N + RefLat;
NEW_LONGITUDE (rad)	= (1/(f3*cos(RefLat)))*E + RefLon;

Note: The vehicle's local coordinate frame is represented in Figure 23.

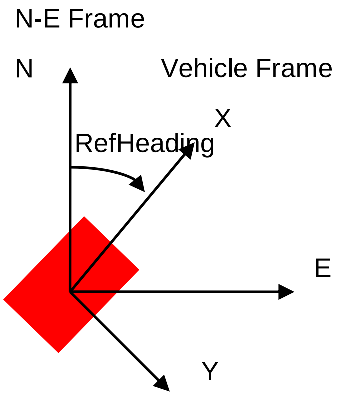


Figure 23: Vehicle Coordinate Frame

A.3 POSITION EXTRAPOLATION

Position extrapolation for the HV local estimator and HV remote estimator are performed up to the current time based on the extrapolation details presented here. Position extrapolation estimates the vehicle's current position at time T' (current time), based on the vehicle's last known position, heading, and speed at time T (older time). The estimation assumes that the vehicle is moving at a constant speed and constant heading.

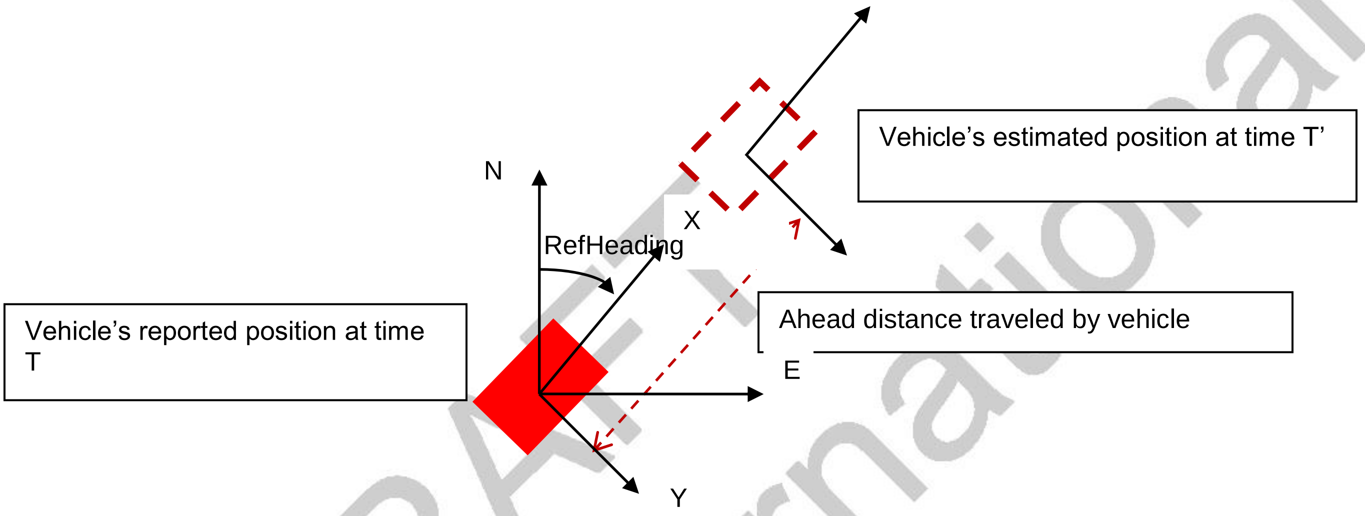

N
X
RefHeading
E
Y
Vehicle's estimated position at time T'
Ahead distance traveled by vehicle
Vehicle's reported position at time T

Figure 24: GNSS Position Extrapolation

1. First find Delta_time, the time since vehicle's last known position.
   - Delta_time_ms = T' – T
2. Do not perform position extrapolation in the following cases:
   - If Delta_time_ms < 0, then there is a time-related error.
   - If Delta_time_ms > *vHVPosEstIntMax*, then the vehicle has not received a position update for a very long time and its position is outdated.
3. If *vHPosEstIntMin* <= Delta_time_ms <= *vHPosEstIntMax*, then perform position extrapolation:
   - Calculate the estimated distance traveled by the vehicle in Delta_time_ms.
   - Ahead_distance_m = Speed_mps * Delta_time_ms / 1000
   - Across_distance_m = 0
4. Use ConvertXYtoLatLon function (provided in Appendix A.2) to find the vehicle's new position at time T'.
5. For all future calculations, use the calculated New_Latitude and New_Longitude as vehicle's position, and current time.

A.4 CALCULATIONS INTO VEHICLE'S POSITION REFERENCE POINT

Consider Figure 21 where the BSM vehicle position reference point with respect to GNSS antenna location on the vehicle is represented as follows:

antOffsetX = Distance in meters to GNSS antenna location from vehicle position reference along the X axis (signed value)

antOffsetY = Distance in meters to GNSS antenna location from vehicle position reference along the Y axis (signed value)

antOffsetZ = Height in meters to the GNSS antenna from vehicle position reference along the Z-axis for an unloaded stationary vehicle on a planar surface. This value will always be negative. For example, for an antenna at the highest point on the roof, this value will be: − height of the antenna above ground (negative value) in meters. If the antenna is 1.05 m above the ground, then antOffsetZ = −1.05

Let

RefLat = e.g., GNSS Measured LATITUDE (rad)

RefLon = e.g., GNSS Measured LONGITUDE (rad)

RefHeading = e.g., GNSS Measured HEADING (rad)

Y = −antOffsetY

X = −antOffsetX

Use ConvertXYtoLatLon function (provided in Appendix A.2) to find the vehicle's 2-D position at position reference point.

For transmitting V2V safety messages, use the calculated New_Latitude and New_Longitude as vehicle's 2-D position at position reference point. These values are calculated for every V2V safety message transmitted.

Finally,

New_Elevation = antOffsetZ + GNSS measured elevation (in meters).

A.5 PATH HISTORY REFERENCE DESIGN

A.5.1 Introduction

The Path History (PH) module for the V2V communications system uses a history of the past Global Navigation Satellite System (GNSS) locations traversed by the Host Vehicle (HV) and computes an adaptable, concise PH representation of recent vehicle movement over a certain distance. The PH communicated by a vehicle provides other vehicles with information needed for predicting the roadway geometry. It plays an important role in target vehicle classification, relative to the HV, with reference to the roadway. There are different methods for design and implementation of the PH module. Three different design methods are described here, each with a slightly different approach.

The PH module in the HV carries out these basic operations:

Maintains a buffer of its recent GNSS positions and sensor data (updated at 100 ms) over a certain travel distance.

Computes concise representation(s) of the actual PH of the vehicle based on allowable position error tolerance between the actual vehicle path and its concise path history representation.

Updates the PH concise representation as an output periodically for use by other V2V systems.

Besides having the capability to represent its PH adequately and use it internally, the HV transmits the concise representation of the path history data wirelessly over-the-air (OTA) to other vehicles in the vicinity. Other vehicles use this information for predicting the roadway geometry and for target vehicle classification.

A.5.2 Path History Requirements

The PH module requirements are as follows:

PH shall represent the HV actual path with a set of concise data elements. The concise data elements shall be a sampled subset of the actual data elements. As shown in Figure 25, the orange circles represent the sampled data concise points, and the chord connecting two consecutive concise data elements represents an approximation of the actual vehicle path segment.

The concise data elements shall be selected such that the perpendicular distance between any point on the actual vehicle path and the chord connecting two concise points (the concise representation of the actual vehicle path) is less than PH_ActualError, as shown in Figure 25.

The size of the buffer containing the concise data elements shall be adaptable so that the represented PH distance computed using the elements of the buffer is at least a certain minimum length defined by the calibration parameter, K_PHDISTANCE_M (in meters). Referring to Figure 25 , the total distance of all the chords connecting the orange concise data elements is a minimum distance of, K_PHDISTANCE_M meters.

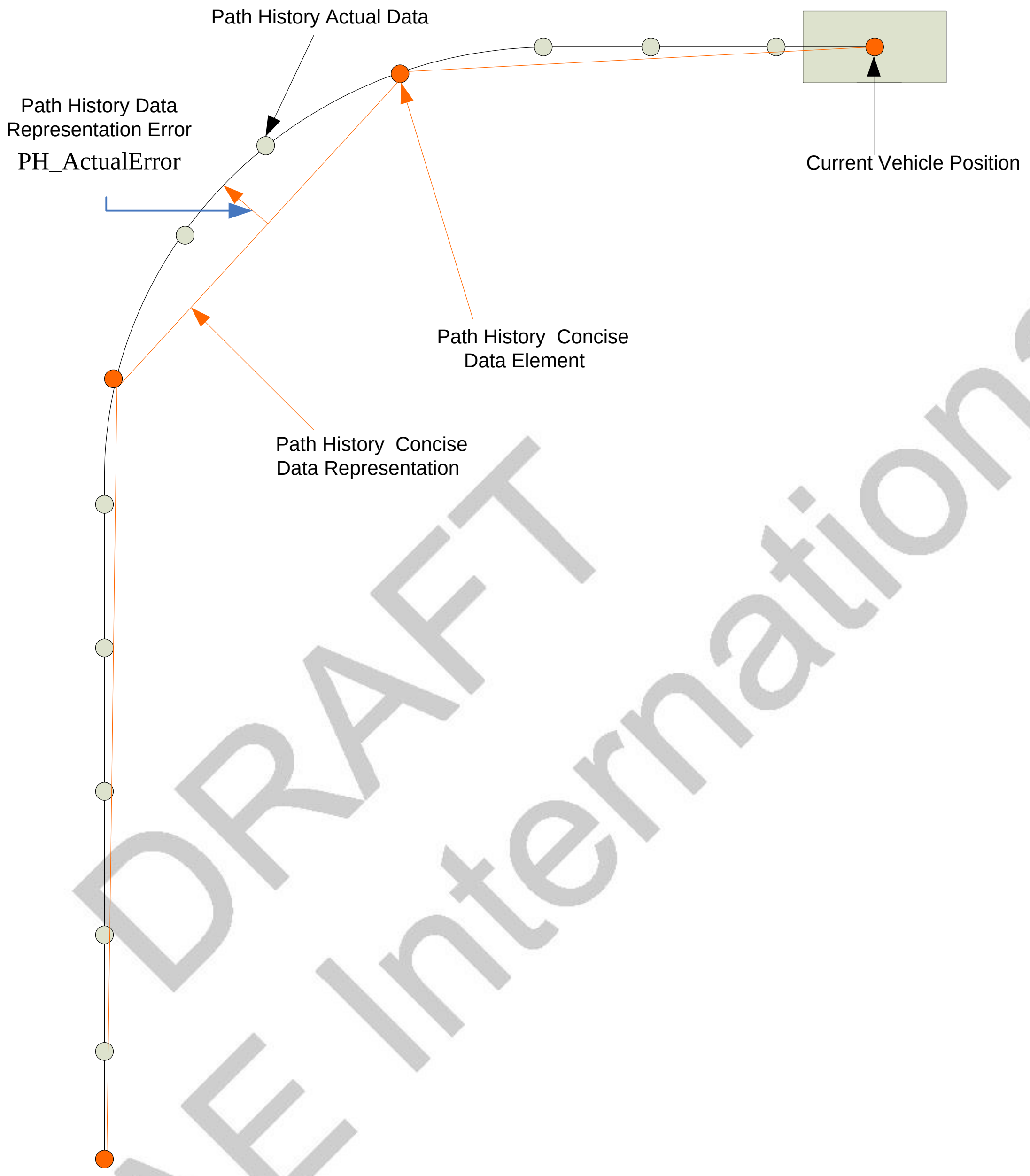


Figure 25: Concise and Actual Path History Representation

A.5.3 Path History Design

Design Preliminaries

Three design methods for PH are presented below. This section defines some basic design preliminaries used by PH design.

a) It is assumed that the vehicle path is composed of straight and circular segments.

b) PH_ActualError is defined as the perpendicular distance between any point on the actual vehicle path and the chord connecting two concise points on the concise representation of the vehicle path. Some of the sampled points on the actual vehicle path may become part of the concise PH representation data elements according to the algorithm used. Please refer to Figure 26 for an illustration of PH_ActualError and actual and concise PH data elements.

c) Figure 26 illustrates points P_1, P_2, P_3, etc. that lie on a circular vehicle path. As illustrated, PH_ActualError varies based on the location of the points selected on the circular path.

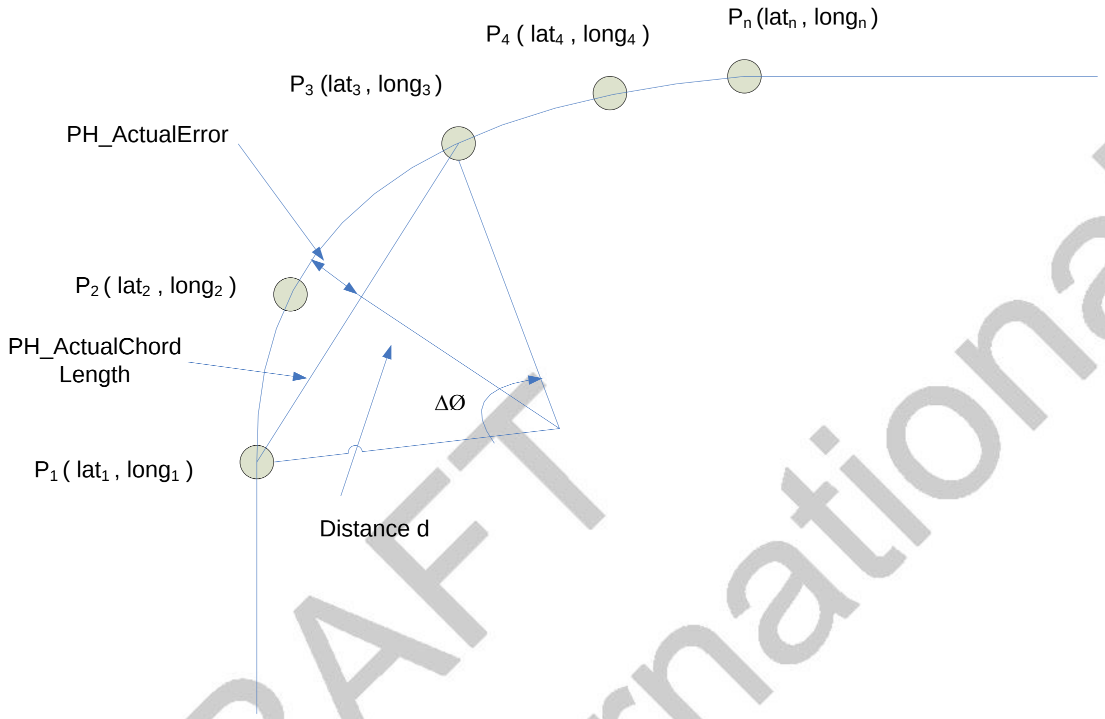


Figure 26: Representation of Error

d) Consider Figure 27. The angle ΔØ subtended by points P_1 and P_2 at the center of the circle can be approximated as ΔØ = $H_2 - H_1$, where H_1 and H_2 represent the GNSS headings of the vehicle at locations P_1 and P_2 respectively on the circular path.

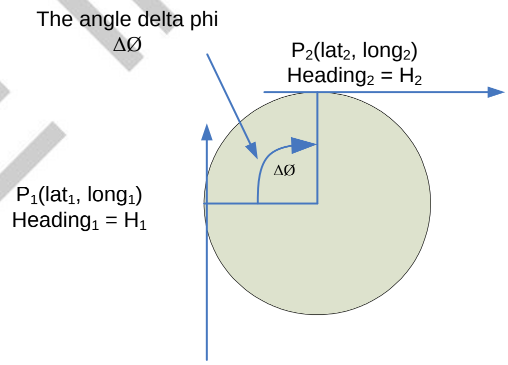


Figure 27: Representation of ΔØ

e) Referring to Figure 26, we define the actual chord length between two PH GNSS points on the circular vehicle path as PH_ActualChordLength. PH_ActualChordLength is the distance between two GNSS data points each defined by its latitude and longitude

f) Let P_1 be defined by latitude, lat_1, and longitude, $long_1$. Similarly, let P_2 be defined by latitude, lat_2, and its longitude, $long_2$. These values are in radians. Define the radius of the earth (in meters) at the meridian as REarthMeridian. Then the actual distance of the chord is given by:

$$PH\_ActualChordLength = REarthMeridian * \cos^{-1}[\cos(lat_1)\cos(lat_2)\cos(long_1 - long_2) + \sin(lat_1)\sin(lat_2)] \qquad (1)$$

g) Another critical parameter that is calculated during the design is PH_EstimatedR, which is the radius of curvature of a circular vehicle path connecting two PH GNSS data points.

A.5.3.1 Design Method One

The steps involved in the design of the concise PH representation of a vehicle path using Method One are described as pseudo code next.

Step One: Assume that a number of actual vehicle path GNSS data points that follow the circular vehicle path are sampled. The minimum number of points required is three. Initial conditions of these points are (see Figure 26):

```
i = 3
Starting Point, $P_{starting}$ = $P_{i-2}$
Previous Point, $P_{previous}$ = $P_{i-1}$
Next Point, $P_{next}$ = $P_i$
elementPos = 0
totalDist = 0
incrementDist = 0
```

Include the GNSS point, $P_{starting,}$ as part of the concise PH representation data buffer and increment the elementPos by one as follows:

```
PH_ConciseDataBuffer[elementPos] = $P_{starting}$
elementPos++
```

Step Two: Calculate PH_ActualChordLength (i.e., chord length in meters) between two points, the starting point, $P_{starting}$, and the next point P_{next}, as shown in Figure 26 and Equation 1. Now check if this value is greater than a certain threshold as follows:

```
If PH_ActualChordLength > K_PH_CHORDLENGTHTHRESHOLD,
    Set PH_ActualError to K_PHALLOWABLEERROR_M + 1,
    Go to Step Seven,
Otherwise Continue.
```

Step Three: Calculate the angle ΔØ (in radians) subtended by points $P_{starting}$ and P_{next} at the center of the circle as ΔØ = $H_2 – H_{1,}$ where H_1 and H_2 represent the GNSS headings (in radians) of the vehicle at locations $P_{starting}$ and P_{next} respectively (see Figure 26).

Step Four: Using PH_ActualChordLength (Step Two) and ΔØ (Step Three), calculate the estimated radius of the curvature, PH_EstimatedR (in meters), between two points $P_{starting}$ and P_{next} as follows:

PH_EstimatedR = PH_ActualChordLength/(2*sin(ΔØ/2)). (2)

This is the estimated radius of curvature for a circular arc joining $P_{starting}$ and P_{next}.

During this step a specific precaution needs to be taken. If ΔØ is very small or equal to zero (i.e., straight road path), then PH_EstimatedR will be a very large number. To detect such a case, ΔØ is compared to a calibration parameter K_PHSMALLDELTAPHI_R. If ΔØ is less than this calibration parameter, then the radius is very large. In this case the radius is to be limited to a value of K_PH_MAXESTIMATEDRADIUS, and

```
If ΔØ < K_PHSMALLDELTAPHI_R,
    Set PH_ActualError to zero,
    Set PH_EstimatedR to K_PH_MAXESTIMATEDRADIUS,
    Go to Step Eight,
Otherwise Continue.
```

Step Five: Calculate the distance d value (Equation 3), which is the perpendicular distance from the center of curvature to the actual chord connecting the sampled GNSS points $P_{starting}$ and P_{next} on the vehicle PH. From Figure 26,

$$d = PH\_EstimatedR*\cos(\Delta\varnothing/2). \qquad (3)$$

Step Six: Calculate the actual maximum error PH_ActualError as

$$PH\_ActualError = PH\_EstimatedR - d. \qquad (4)$$

Step Seven: If PH_ActualError is greater than the allowable PH error, K_PHALLOWABLEERROR_M, then add the previous point $P_{previous}$ to the concise data buffer as follows:

```
If PH_ActualError > K_PHALLOWABLEERROR_M
PH_ConciseDataBuffer[elementPos] = $P_{previous}$
elementPos++
```

Redefine three GNSS data points for further processing. The new points are set to the Starting Point, Previous Point, and Next Point as follows:

```
$P_{starting} = P_{i-1}$
$P_{next} = P_{i+1}$
$P_{previous} = P_i$
i = i + 1
Go to Step Nine.
```

Step Eight: If PH_ActualError ≤ K_PHALLOWABLEERROR_M, redefine the Previous Point and Next Point as:

```
$P_{next} = P_{i+1}$
$P_{previous} = P_i$
i = i + 1
Go to Step Two.
```

The algorithm repeats itself with the assigned values of Starting Point, Previous Point, and Next Point. This procedure repeats until the error violation occurs.

Step Nine: Calculate the sum of the actual distances between the consecutive PH GNSS data points in the concise buffer PH_ConciseDataBuffer as follows:

```
totalDist = totalDist + incrementDist
```

totalDist is the sum of distances between PH GNSS points in the concise data buffer PH_ConciseDataBuffer.

incrementDist is the distance between the last two PH GNSS data points added to the concise data buffer. Hence, if the total distance is greater or equal to K_PHDISTANCE_M, then keep deleting elements from the bottom of the concise buffer (i.e., the oldest points) until the total distance becomes just enough to maintain a minimum value of K_PHDISTANCE_M. Output the radius of curvature between the recent two selected concise data points as PH_EstimatedSumR. If the number of elements remaining in the concise buffer exceeds the maximum allowed (23), then keep deleting the oldest points in the buffer until only 23 points remain.

Go to Step Two.

A.5.3.2 Design Method Two

Method Two follows the same steps as Method One except for the calculation of the radius of curvature (PH_EstimatedR defined in Equation 2 of Method One). For Method Two, the radius of curvature is an average of the calculation of the radius calculated in Method One and the radius calculated using vehicle speed and yaw rate. The steps involved in the design of the concise PH representation of a vehicle path using Method Two are described in pseudo code next:

Step One: Perform Method One, Step One.

Step Two: Perform Method One, Step Two.

Step Three: Perform Method One, Step Three.

Consider Figure 26 such that there exist n GNSS points, $P_1 \ldots P_n$. Consider P_1 as the Starting Point, and P_n as the Next Point. Define P_2, …, P_{n-1} as the Intermediate Points. Method Two calculates a running average (Step Four) of radii calculated by Equation 5 as follows:

$$\text{Radius} = v/w, \qquad (5)$$

where, v is vehicle speed (meter/s) and w is the vehicle yaw rate (radian/s).

Given n points as in Figure 28, define R_{2i} to be the radii calculated by Method Two at points i such that i = 1, ….n-1. Hence, define the following radii as:

$R_{21} = v_1/w_1$

$R_{22} = v_2/w_2$

$R_{23} = v_3/w_3$

$R_{2(n-1)} = v_{n-1}/w_{n-1}$.

If the radius calculation is higher than a threshold value, set it to the maximum value K_PH_MAXESTIMATEDRADIUS and then ignore that radius, remove it from the radii buffer, and do not include it in the running average calculation in Step Four.

Step Four: Perform Method One, Step Four. We define the radius calculation from Equation 2 as $PH\_EstimatedR_1$. The running average of radii, $PH\_EstimatedR_2$, saved in the radii buffer computed in Step Three is given below as:

$$PH\_EstimatedR_2 = \sum_{i=1}^{i=n-1} {R_{2i}}/{n-1} \qquad (6)$$

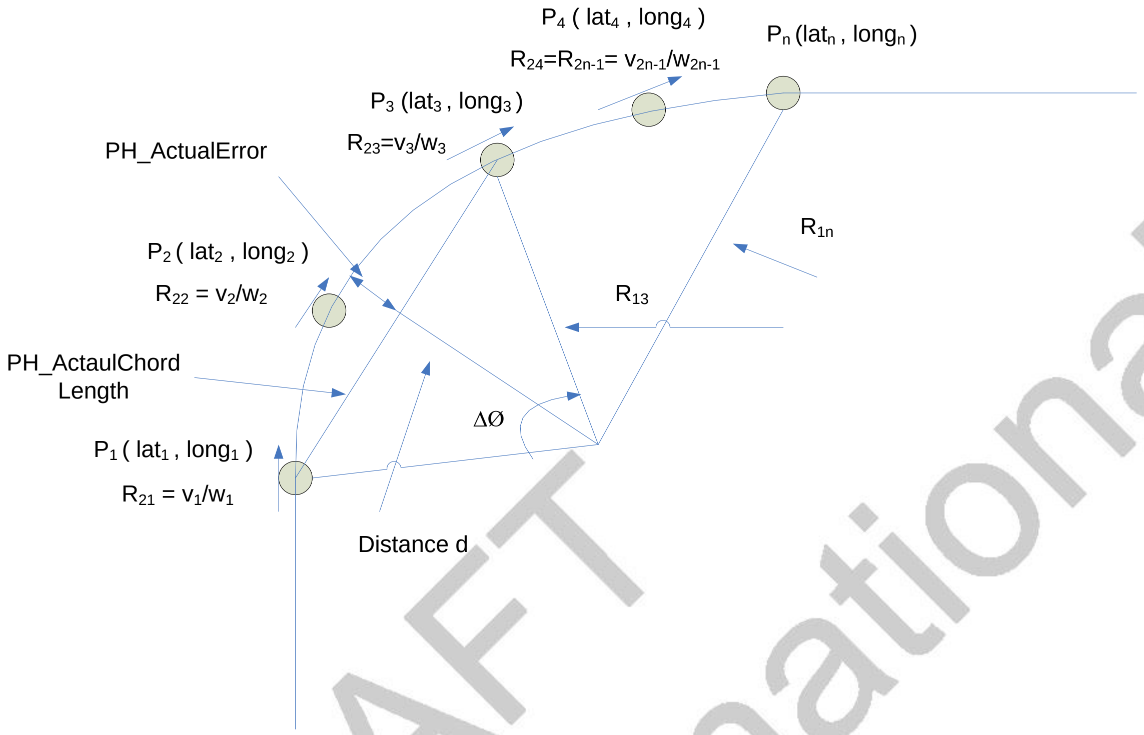

P$_4$ (lat$_4$, long$_4$)
R$_{24}$=R$_{2n-1}$= v$_{2n-1}$/w$_{2n-1}$
P$_n$ (lat$_n$, long$_n$)
P$_3$ (lat$_3$, long$_3$)
R$_{23}$=v$_3$/w$_3$
PH_ActualError
R$_{1n}$
P$_2$ (lat$_2$, long$_2$)
R$_{22}$ = v$_2$/w$_2$
R$_{13}$
PH_ActaulChord Length
ΔØ
P$_1$ (lat$_1$, long$_1$)
R$_{21}$ = v$_1$/w$_1$
Distance d

Figure 28: Representation of Estimated Radius Calculation

The estimated radius of curvature, PH_EstimatedR, is then calculated as a weighted sum between PH_EstimatedR$_1$ and PH_EstimatedR$_2$ as shown below:

$$\begin{aligned}\text{PH\_EstimatedR} &= \text{K\_PH\_RADIUSWEIGHTONE*PH\_EstimatedR}_1 \\ &+ \text{K\_PH\_RADIUSWEIGHTTWO*PH\_EstimatedR}_2\,, \qquad (7)\end{aligned}$$

where, K_PH_RADIUSWEIGHTONE and K_PH_RADIUSWEIGHTTWO are weights that sum up to 1. If the running average radius PH_EstimatedR$_2$ is zero as a result of all the radii in the buffer being set to the maximum value K_PH_MAXESTIMATEDRADIUS, then set K_PH_RADIUSWEIGHTONE = 1, and K_PH_RADIUSWEIGHTTWO = 0.

Step Five: Perform Method One, Step Five.

Step Six: Perform Method One, Step Six.

Step Seven: Perform Method One, Step Seven.

In addition, one has to adjust the running average PH_EstimatedR$_2$ to the following. If radii at the new points, P$_{starting}$ and P$_{next}$, are both equal to K_PH_MAXESTIMATEDRADIUS, then PH_EstimatedR$_2$ would be the resulting running average of these points as calculated using Equation 6. Otherwise, if the radius at the new point, P$_{next,}$ is not equal to K_PH_MAXESTIMATEDRADIUS, then PH_EstimatedR$_2$ would be set to this radius value. Otherwise, if the radius at the new point, P$_{starting}$, is not equal to K_PH_MAXESTIMATEDRADIUS, then PH_EstimatedR$_2$ would be set to this radius value. If none of the above is true, then PH_EstimatedR$_2$ would be set to zero.

Step Eight: Perform Method One, Step Eight.

Step Nine: Perform Method One, Step Nine.

A.5.3.3 Design Method Three

Method Three follows the same steps as Method One except for the calculation of the PH error. In this method, the definition of PH_ActualError and the selection process of the concise PH data element are modified. PH_ActualError is the maximum perpendicular distance between the actual vehicle PH data elements and the chord connecting the concise PH representation data elements.

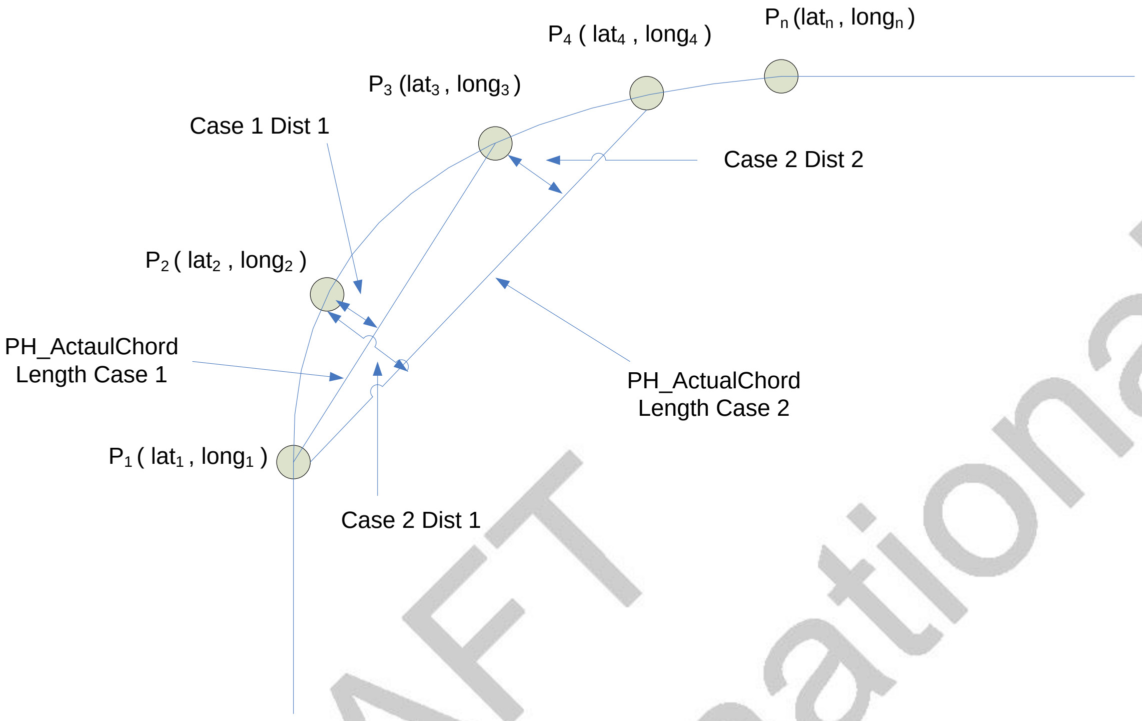

P_n (lat_n , $long_n$)
P_4 (lat_4 , $long_4$)
P_3 (lat_3 , $long_3$)
Case 1 Dist 1
Case 2 Dist 2
P_2 (lat_2 , $long_2$)
PH_ActaulChord Length Case 1
PH_ActualChord Length Case 2
P_1 (lat_1 , $long_1$)
Case 2 Dist 1

Figure 29: Representation of PH Error for Method Three

The steps involved in the design of the concise PH representation of a vehicle path using Method Three are described in pseudo code next.

Step One: Perform Method One, Step One.

Step Two: Calculate PH_ActualChordLength (i.e., chord length in meters) between two points, the Starting Point, $P_{starting}$, and the Next Point P_{next}, as shown in Figure 26 and Equation 1.

```
    If PH_ActualChordLength > K_PH_CHORDLENGTHTHRESHOLD,
    Set PH_ActualError to K_PHALLOWABLEERROR_M + 1
    Go to Step Six.
```

Step Three: Perform Method One, Step Three.

Step Four: Perform Method One, Step Four.

Step Five: Calculate PH_ActualError as follows:

Define PH data elements, such that P_1 is the Starting Point, P_n is the Next Point, and the Intermediate Points are P_2 through P_{n-1} as shown in Figure 29. Define the perpendicular distance between the Intermediate Points and the chord connecting $P_{starting}$ and P_{next} as D_i, where i = 2, …, n-1. Define PH_ActualError as

$$\text{PH\_ActualError} = \text{MAX}(D_i); \quad i = 2, \ldots, n-1. \tag{8}$$

The procedure of calculating the distances D_i is described next. Before performing the following calculations, the GNSS coordinates of the points must be represented into the North-East coordinate frame. The following provides a solution to finding the shortest distance from a point to a line or line segment.

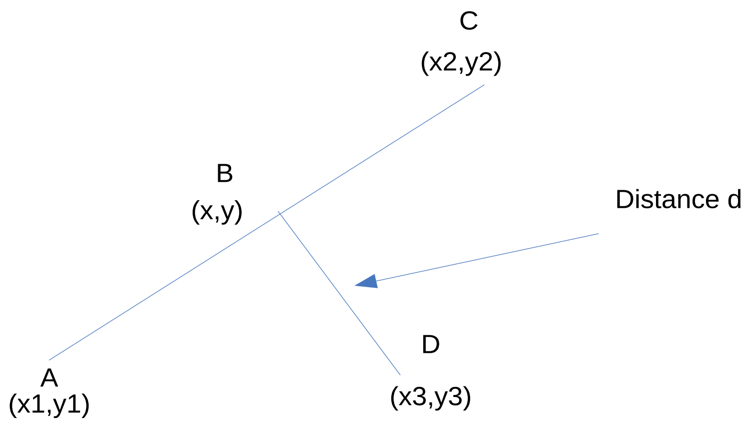


Figure 30: Shortest Distance from a Point to a Line Segment

Consider Figure 30. A solution is provided to the shortest distance from point **D** to the line segment AC. The equation of a line segment defined through two points **A** (x1,y1) and **C** (x2,y2) is given by

B = **A** + u (**C** - **A**),

where u is a value between 0 and 1. The point **B** (x,y) on the line segment AC that is closest to **D**, satisfies

(**D** - **B**) dot (**C** - **A**) = 0,

where “dot” indicates the dot product of the vectors. Substituting for **B** in the above equation gives

[**D** - **A** - u(**C** - **A**)] dot (**C** - **A**) = 0.

Solving this gives the value of u as

$u = ((x3-x1)(x2-x1) + (y3-y1)(y2-y1)) / || C – A||^2$.

Substituting this into the equation of the line gives the point of intersection **B** (x,y) as

x = x1+ u(x2 - x1),

y = y1 + u(y2 - y1).

The distance therefore between the point **D** and the line is the Euclidean distance between (x,y) and **D**:

$d = sqrt((x3-x)^2 + (y3-y)^2)$.

Note: Before computing the distance of the point to a line segment, it is necessary to first test that u lies between 0 and 1.

Step Six: Perform Method One, Step Seven.

Step Seven: Perform Method One, Step Eight.

Step Eight: Perform Method One, Step Nine.

A.5.4 PH Module Signal Interface Description

In this subsection, the inputs, outputs, and calibration parameters used in the PH module are provided.

- Inputs to the PH module are:

  Coordinated Universal Time (UTC) time; latitude; longitude; altitude; speed; heading; yaw rate

- Calibration parameters for the PH Module are:

  K_PHDISTANCE_M300 (meters)

  K_PHDATAPOINTSSAMPLETIME_S100 (ms)

  K_PHALLOWABLEERROR_M1 (meters)

  K_PHSMALLDELTAPHI_R0.02 (radians)

K_PH_RADIUSWEIGHTONE 0.5 (unitless)

K_PH_RADIUSWEIGHTTWO0.5 (unitless)

K_PH_CHORDLENGTHTHRESHOLD310 (meters)

K_PH_MAXESTIMATEDRADIUS7FFFFF (meters)

- The outputs are available in the concise PH data structure buffer and shall be the PH data elements. Outputs of the PH module are:

  N; // number of PH concise representation data elements

  PH_CONCISE_DATA_ELEMENT_1,

  ….

  ….

  PH_CONCISE_DATA_ELEMENT_N,

  where, PH_CONCISE_DATA_ELEMENT consists of,

  PH_UTCTime; PH_Latitude; PH_Longitude; PH_Altitude; PH_Speed; PH_Heading; PH_YawRate; PH_EstimatedSumR.

  Note: If PH_EstimatedSumR is greater than K_PH_MAXESTIMATEDRADIUS, then set PH_EstimatedSumR to K_PH_MAXESTIMATEDRADIUS.

A.5.5 Test Results

A.5.5.1 Concise PH Representation of Vehicle Path

Data were collected over a certain vehicle path as shown in Figure 31 below. GNSS data were collected using a NovAtel® OEMV® receiver with the data sampling interval of the actual vehicle position data being 100 ms. The actual vehicle path is represented by 10,500 GNSS data points.

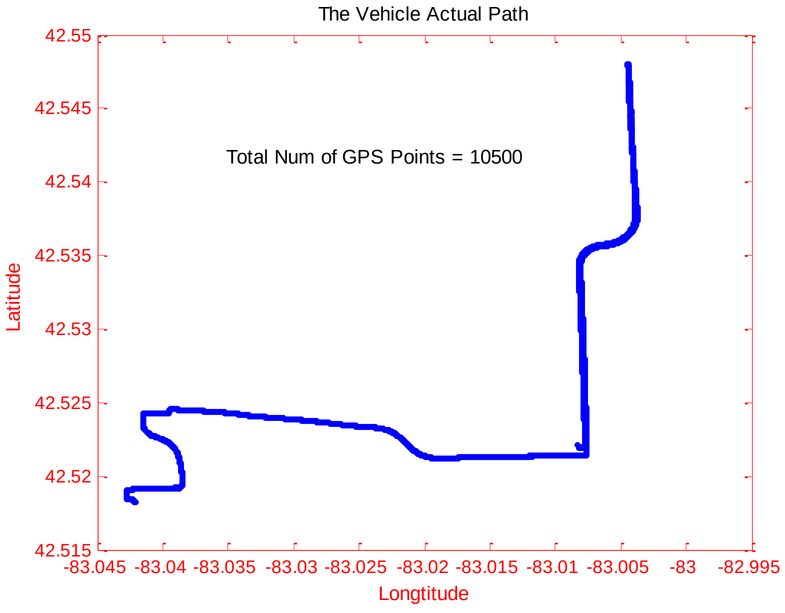


Figure 31: Vehicle Actual Path

The test results evaluated the three PH methods and calculated the concise PH that approximates the actual vehicle path within an error tolerance of 1 m. Figure 32, Figure 33, and Figure 34 show in red circles the concise PH data elements representing the actual vehicle path. The actual vehicle path is shown in blue. Method One shows that the number of concise PH data elements needed to represent the vehicle path is 111. Method Two shows that the number of concise PH data elements needed to represent the vehicle path is 129. Method Three shows that the number of concise PH data elements needed to represent the vehicle path is 124.

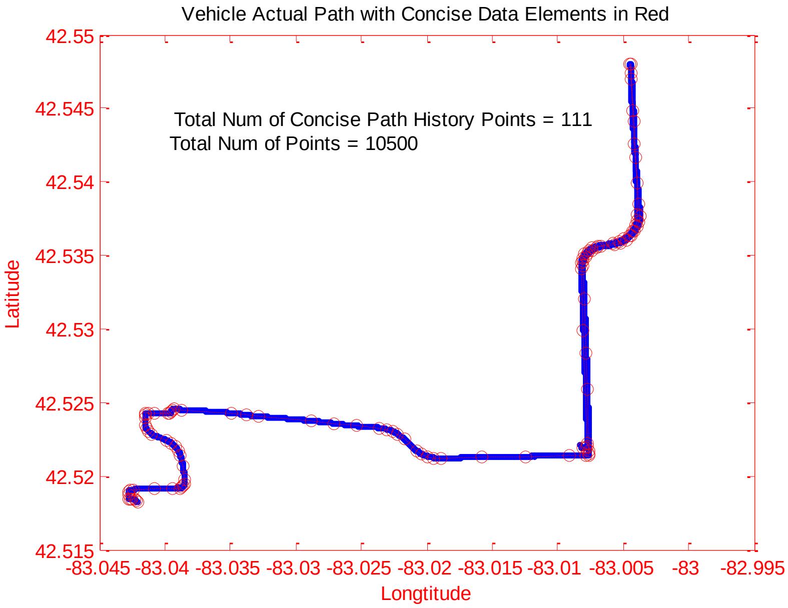


Figure 32: Method One – Representation of Vehicle Path

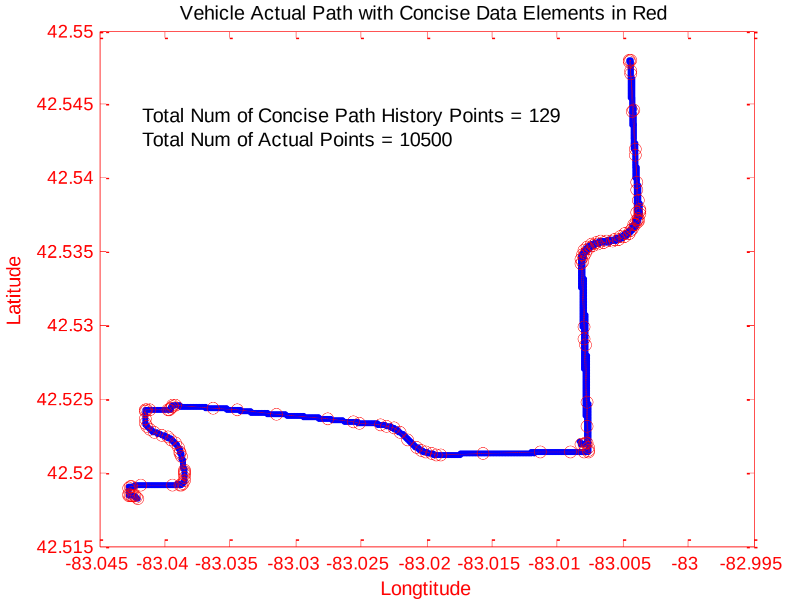


Figure 33: Method Two – Representation of Vehicle Path

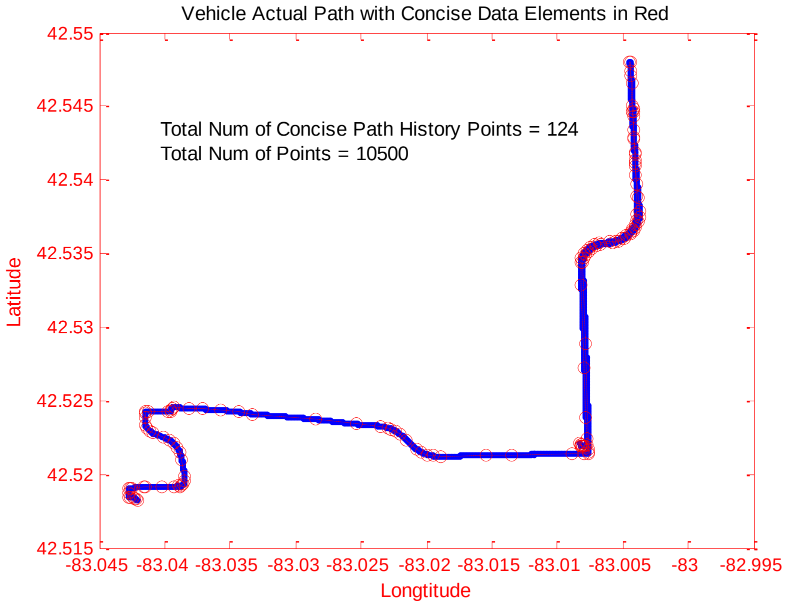


Figure 34: Method Three – Representation of Vehicle Path

A.5.5.2 Radii of Curvature for a Curved Road

Figure 35 (Method One and Method Three) and Figure 36 (Method Two) show the radii of curvature (in meters) between successive, concise PH data points for a sharp, curved road segment of the vehicle path. The radii of curvature clearly indicate the curved nature of the road segment. Notice that the road segment also includes a reasonably straight section represented with a larger radius of curvature. In Figure 35 and Figure 36, the solid line indicates the actual vehicle path and the dotted lines indicate the concise PH representation.

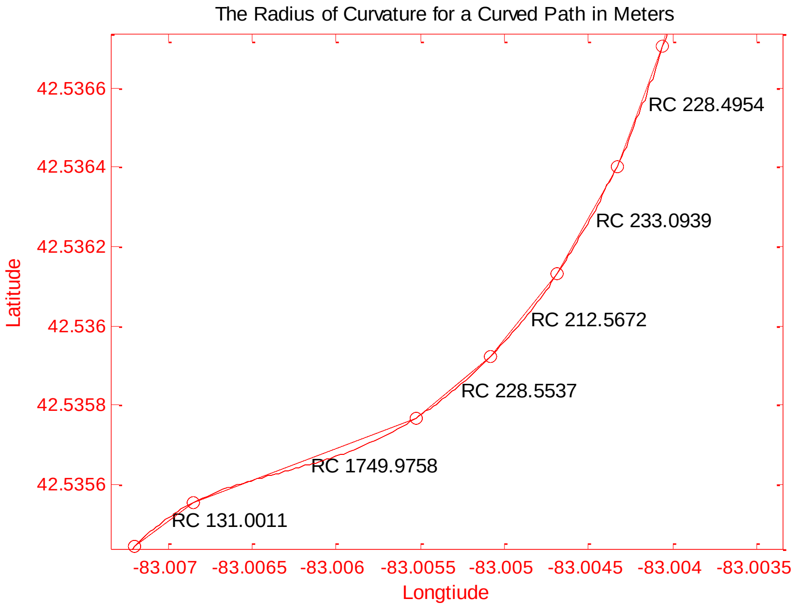


Figure 35: Methods One and Three – Radii of Curvature for Curved Road

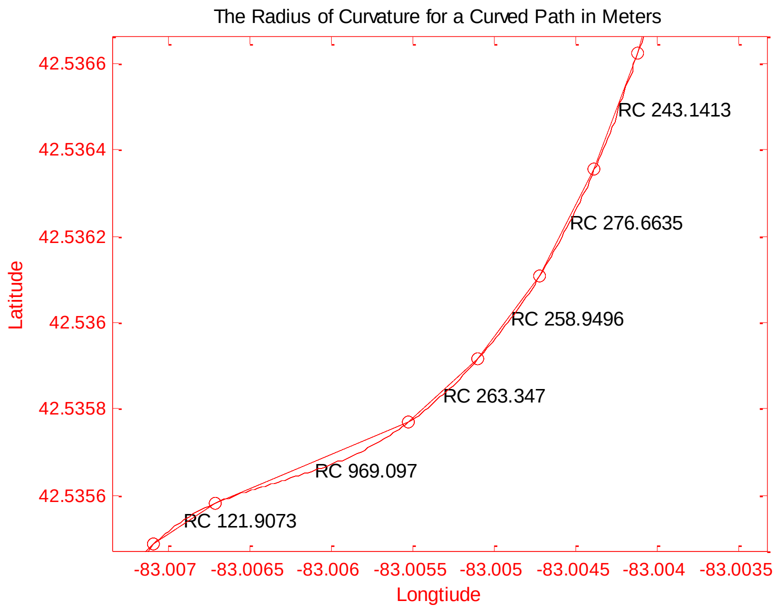


Figure 36: Method Two – Radii of Curvature for Curved Road

A.5.5.3 Radii of Curvature for a Straight Road

Figure 37 (Method One and Method Three) and Figure 38 (Method Two) show the radii of curvature (in meters) between successive concise data points for a straight road segment. The numbers indicate that the radius of curvature for a straight road segment is large. By examining these numbers, it is clear that the straight road segments are easily identified by using a certain threshold for radius of curvature. In Figure 37 and Figure 38, the solid line indicates the actual vehicle path and the dotted lines indicate the concise PH representation.

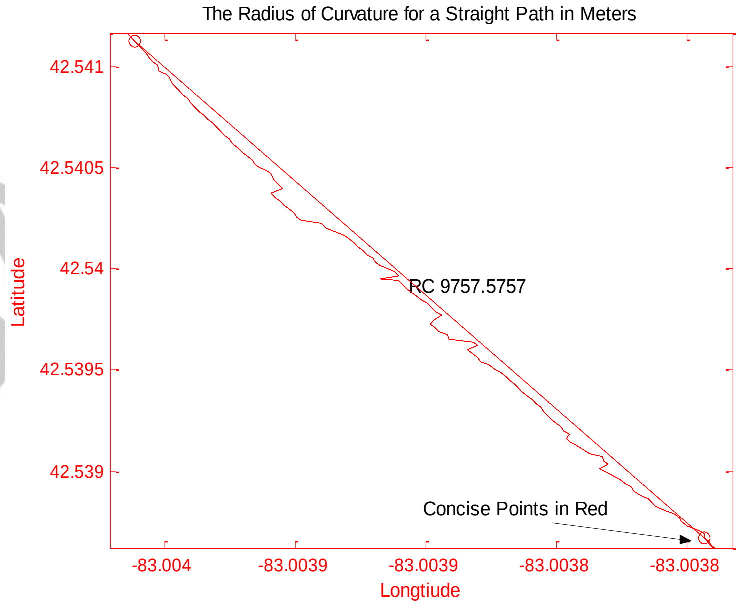


Figure 37: Methods One and Three – Radii of Curvature for Straight Road

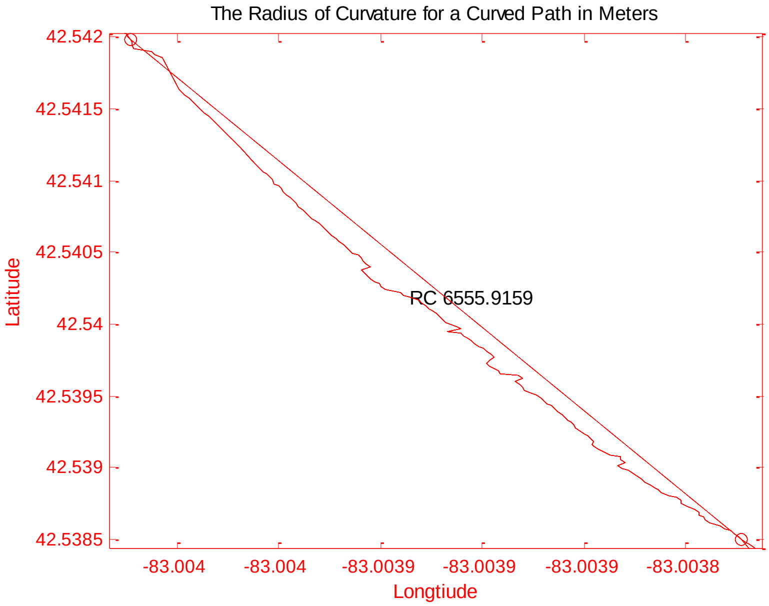


Figure 38: Method Two – Radii of Curvature for Straight Road

A.5.5.4 PH Concise Points and Distances Between Them for a Curved Road

Figure 39 (Method One), Figure 40 (Method Two), and Figure 41 (Method Three) show the result for a curved road segment after concise data points have been computed to maintain the PH distance of at least 300 m from the current vehicle position (shown in green). No additional PH points can be dropped without violating the requirement of a minimum 300-meter PH distance. It is clear all methods require only a few PH points to represent a vehicle PH over a curved roadway segment as shown.

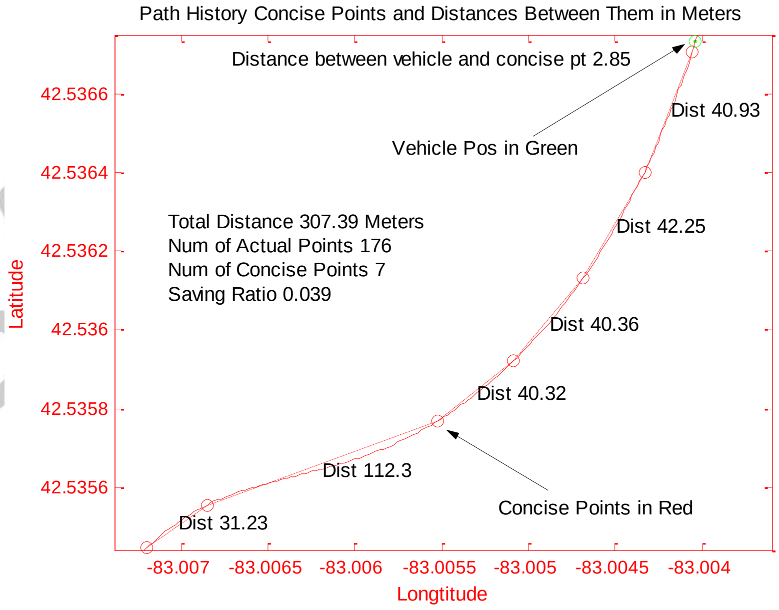


Figure 39: Method One – PH Representation of Curved Road

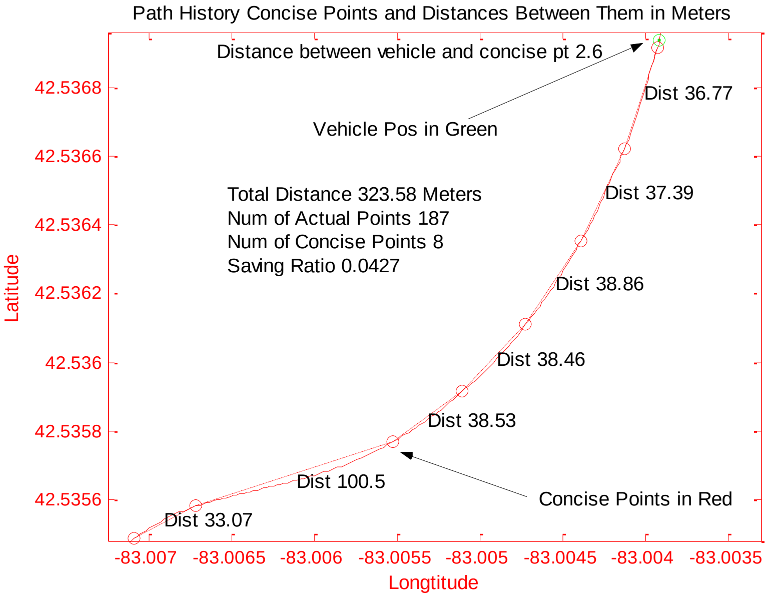


Figure 40: Method Two – PH Representation of Curved Road

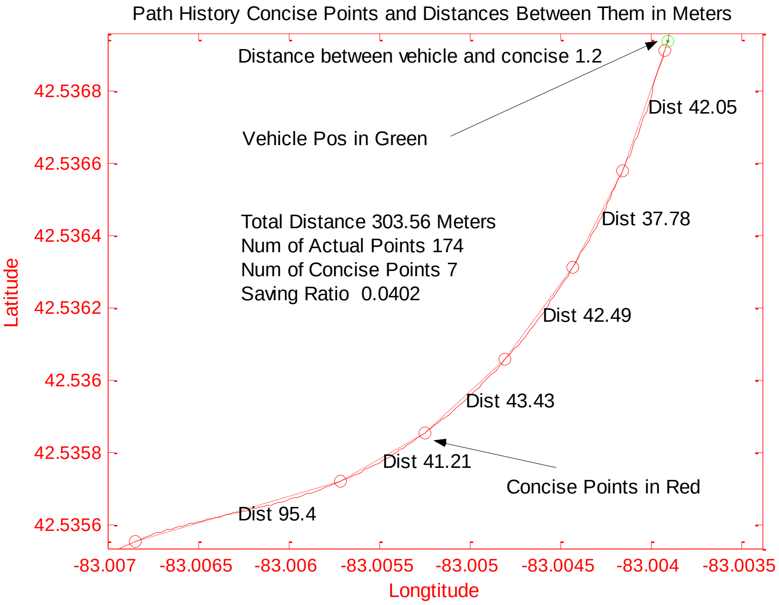


Figure 41: Method Three – PH Representation of Curved Road

The saving ratio shown in Figure 39 through Figure 41 indicates the ratio of concise data elements to the actual data elements. The ratio indicates the saving in the representation of the actual path when using a concise PH representation for each of the proposed methods. In Figure 39 through Figure 41, the solid line indicates the actual vehicle path and the dotted lines indicate the concise PH representation.

A.5.5.5 PH Concise Points and Distances Between Them for a Straight Road

Figure 42 (Method One), Figure 43 (Method Two), and Figure 44 (Method Three) show the result for a straight road segment after concise data points have been computed to maintain the PH distance of at least 300 m from the current vehicle position (shown in green). No additional PH points can be dropped without violating the requirement of a minimum

300-m PH distance. From Figure 42, the algorithm of Method One selects two successive PH concise points for this road segment with a distance between them equal to 375.3 m. Similarly, from Figure 43, the algorithm of Method Two selects two successive PH concise points for this road segment with a distance between them equal to 391.4 m. Subsequent to collection of these test results, Step 2 of all the algorithms was modified so that the maximum distance between two successive PH concise points never exceeds the stated threshold distance of K_PH_CHORDLENGTHTHRESHOLD, the default value of which is 310 m. Also notice from Figure 42 and Figure 43 that the total distance of the path history representation is 381.83 m and 396.4 m, respectively. The increase in path history representation distance is obtained without the need for any additional PH points over the minimum number of PH points needed to represent the path history for a minimum distance defined by the calibration parameter K_PHDISTANCE_M, with a default value of 300 (meters).

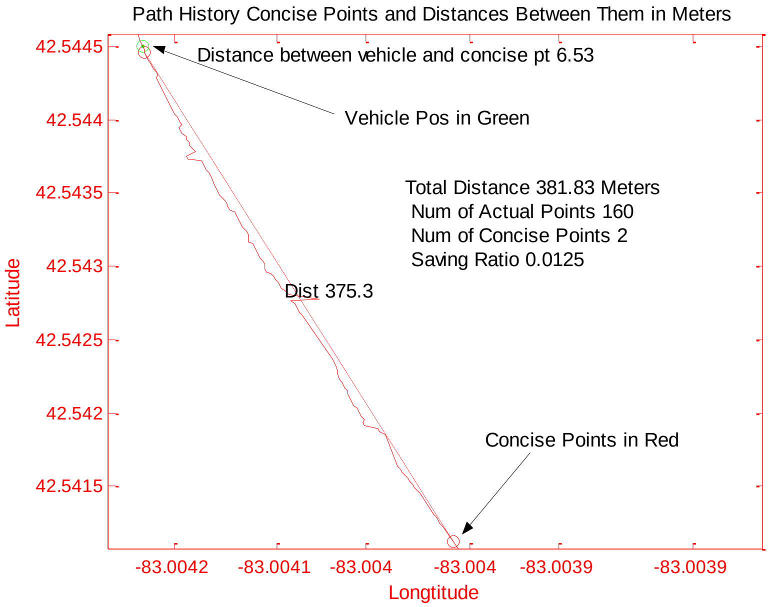


Figure 42: Method One – PH Representation of Straight Road

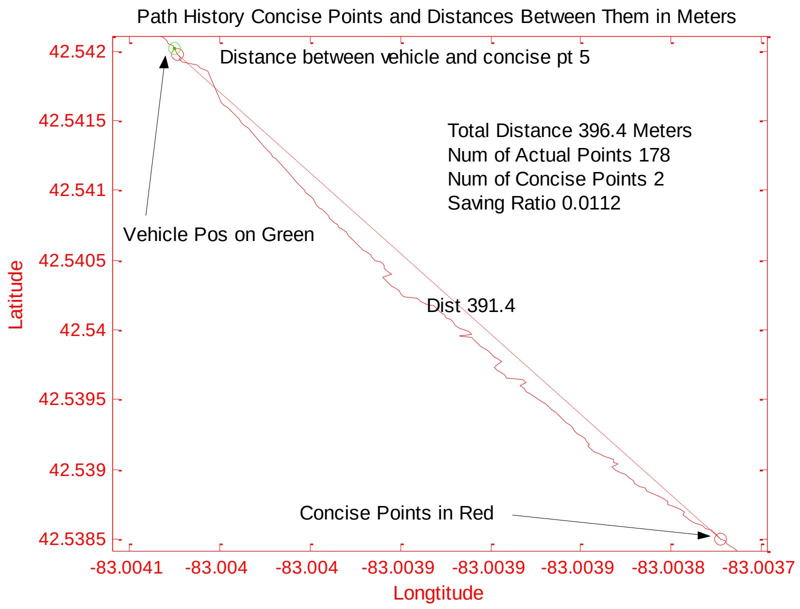


Figure 43: Method Two – PH Representation of Straight Road

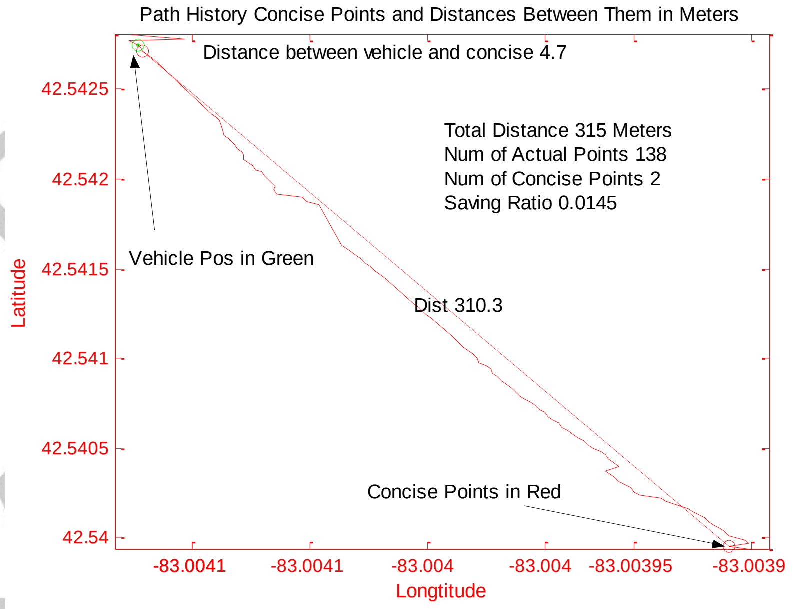


Figure 44: Method Three – PH Representation of Straight Road

The saving ratio shown in Figure 42 through Figure 44 indicates the ratio of concise data elements to the actual data elements. The ratio indicates the saving in the representation of the actual path when using a concise PH representation for each of the proposed methods. In Figure 42 through Figure 44, the solid line indicates the actual vehicle path and the dotted lines indicate the concise PH representation.

A.5.5.6 PH Requirement Analysis

Figure 45 (Method One), Figure 46 (Method Two), and Figure 47 (Method Three) show the actual error between concise PH data elements. Since the concise data points are chosen based on the fact that they do not violate the actual error criterion of 1 m, it is clearly shown and verified in these figures that the actual error is always less than 1 m. Similar results are generated for a straight path. The significance of these results is that the concise PH data points can be used reliably to represent the actual vehicle PH. In Figure 45 through Figure 47, the solid line indicates the actual vehicle path and the dotted lines indicate the concise PH representation.

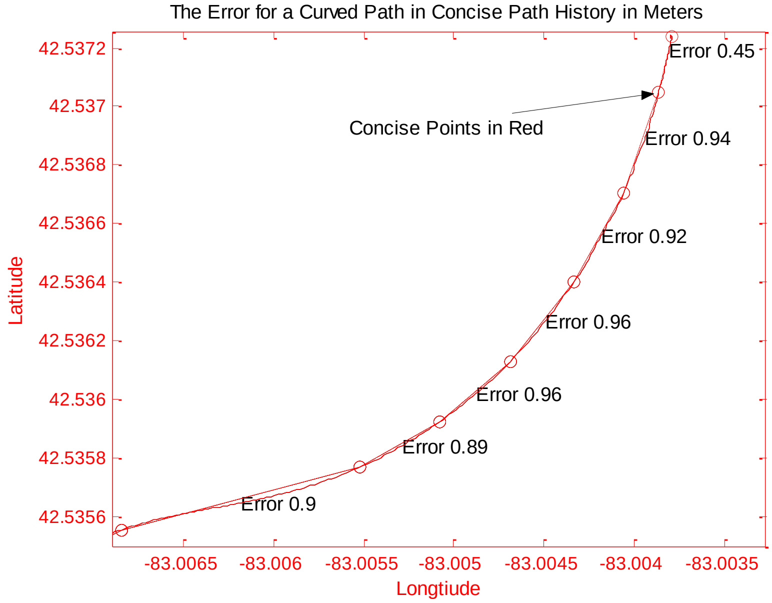


Figure 45: Method One – PH Error Analysis

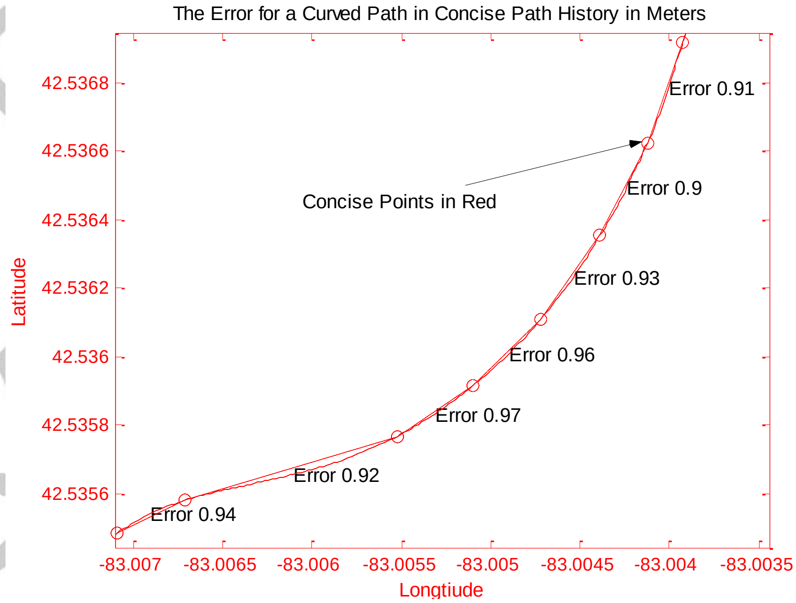


Figure 46: Method Two – PH Error Analysis

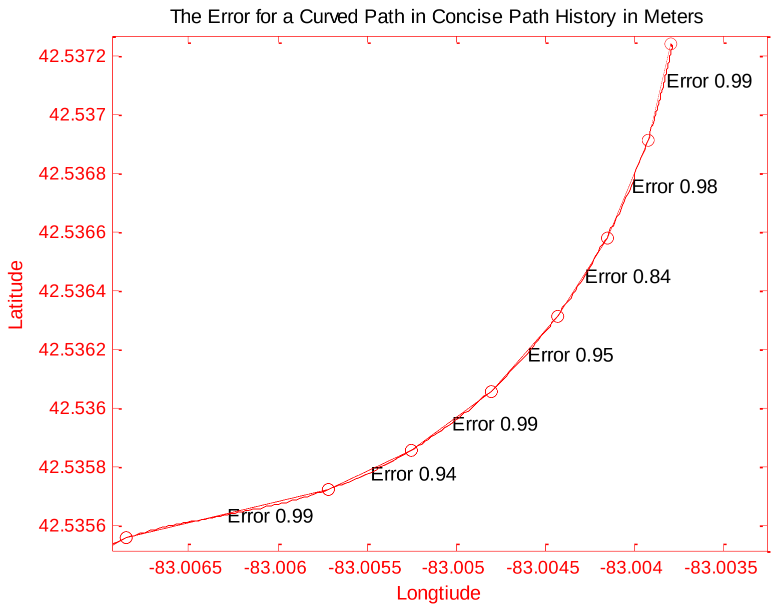


Figure 47: Method Three – PH Error Analysis

A.5.6 Summary

This standard has presented the PH module for a vehicle safety communications system. The module uses a history of the past GNSS locations traversed by the HV and computes an adaptable concise PH representation of recent vehicle movement over a certain distance. The PH communicated by a vehicle provides other vehicles with important information needed for predicting the roadway geometry. It plays an important role in target vehicle classification in vehicle safety communications. Three different methods for design and implementation of the PH module have been presented. These methods have also been implemented and their performance has been evaluated. Extensive testing has shown that the concise representations of the vehicle PH computed by the various methods are very optimal and offer significant savings in OTA wireless bandwidth when transmitting the PH information to other vehicles wirelessly, while guaranteeing that the PH error remains within the allowable tolerance of 1 m. Method One was chosen as the primary method used subsequently for VSC-A objective testing. The objective testing of VSC-A applications have also shown that the PH error tolerance of 1 m that was chosen as default satisfies the needed accuracy and meets the performance requirements of target classification and the safety applications that were developed and demonstrated in the VSC-A Project.

A.6 PATH PREDICTION REFERENCE DESIGN

A.6.1 Introduction

Path Prediction (PP) for the V2V safety communications system utilizes dynamics information provided by the vehicle to estimate the driver's intended future path. The estimate is provided without dependence on future road geometry information obtained from outside sources (e.g., map databases, vehicle probes).

PP carries out the following basic operations:

- Gathers vehicle dynamics information.
- Computes path radius using dynamics information to represent the driver's intended future path:

  Radius = 1/curvature (ρ).

- Computes confidence of the predicted path based upon the rate of change of the vehicle dynamics to infer transient conditions (i.e., non-steady-state conditions).

A.6.2 PP Design Approach

The primary PP design approach for the V2V safety system uses vehicle dynamics information to calculate a (continuous) radius of curvature representing the vehicle's estimated future path. This is accomplished by using simple physics equations to compute curvature based on the vehicle speed and the rate of change of heading (yaw rate). This curvature can be extrapolated forward to provide an estimate of the likely future path of the vehicle (Figure 48).

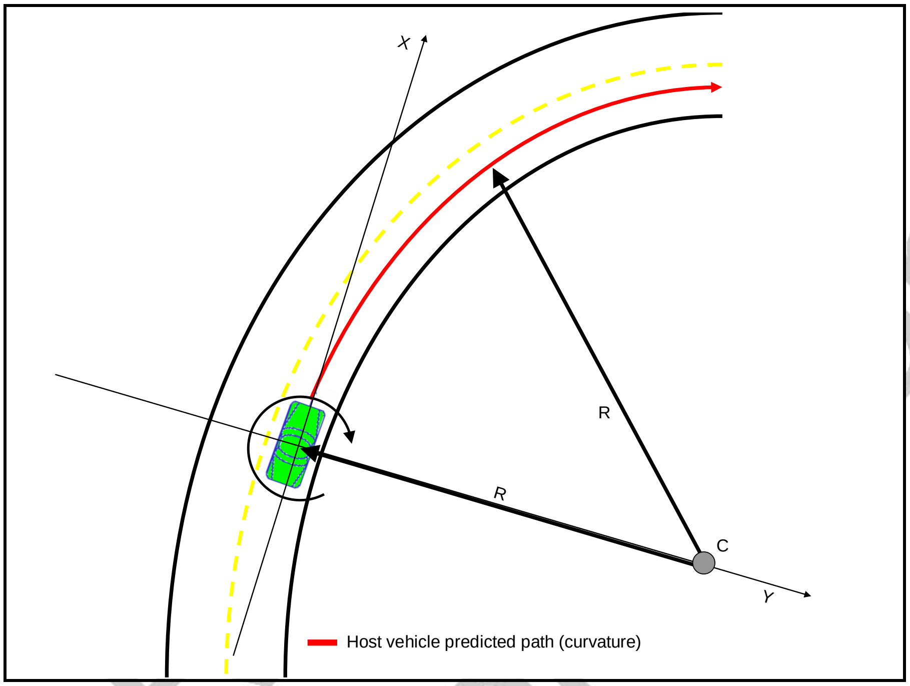


Figure 48: Vehicle Projected Path

The PP module requires the following input signals:

- Vehicle Speed (meters per second [m/s] used in this example)
- Yaw Rate (degrees per second [degrees/s] used in this example)

Developers should pay careful attention to divide-by-zero conditions and appropriately cap intermediate and output calculations to prevent data type overflow. This is particularly important as vehicle speed approaches zero (see Simulink diagrams in subsequent sections).

A.6.3 Radius Calculation

In order to effectively filter a PP radius in meters, a reciprocal is computed in order to perform the filter operations on curvature (1/r). This prevents large discontinuities in the filter input signal when the radius oscillates between positive and negative values approaching infinity. Once the curvature has been computed, the signal is filtered in order to attenuate unwanted high-frequency noise. The filter shall be designed and calibrated to greatly reduce the following effects:

- Road noise
- Sensor noise
- Driver noise (in-lane wandering)

For the PP module, a second order low-pass filter is used to remove these unwanted components from the yaw rate signal. The design is a discretized version of a standard second order unity-gain filter characterized by the following equations.

Discretized (unity-gain) second order low-pass filter:
(Filtered Curvature)

$$\frac{\omega_0^2}{s^2 + 2\omega_0 \zeta s + \omega_0^2} = \frac{\omega_0^2 T_s^2}{z^{-2} - (2+2\omega_0 \zeta T_s)z^{-1} + (\omega_0^2 T_s^2 + 2\omega_0 \zeta T_s + 1)}$$

Continuous (1/s = integrator) Discrete (1/z = unit delay)

$$\underset{(\text{for } n \geq 3)}{y_n} = \frac{-y_{n-2} + (2+2\omega_0 \zeta T_s)y_{n-1} + \omega_0^2 T_s^2 u_n}{(1 + 2\omega_0 \zeta T_s + \omega_0^2 T_s^2)}$$

Initialization: $y_1 = u_1$, $y_2 = u_2$

Figure 49: Discretized Second Order Low-Pass Filter

In Figure 49, $\omega_0 = 2\pi f_0$, f_0 = cutoff frequency, ζ = damping factor, and T_s = sampling time. Note: $\zeta = 1$ (default) for a critically damped system.

The vehicle radius calculation follows the basic formula:

radius (m) = vehicle speed (m/s) / yaw rate (radians/s)

In preparation of the radius calculation, the yaw rate is converted from degrees/s to radians/s. To prevent division by zero when the vehicle is stationary and to eliminate large discontinuities in the filter input signal, the reciprocal of radius is calculated to provide curvature input.

curvature (1/m) = yaw rate (radians/s) / vehicle speed (m/s)

Upon calculation of the curvature, the signal is passed through a discretized second order low-pass filter (Figure 49) that has been calibrated to the appropriate cutoff frequency, damping factor, and sampling rate. Once the curvature calculation has been filtered, it is converted back to a radius in meters using the reciprocal. Special care must be taken to prevent overflow of the radius calculation when curvature is zero (or near zero). Radius calculations follow the SAE sign convention for rotation, where a positive sign represents a clockwise curvature about the vehicle boresight and a negative sign represents counter-clockwise.

A final set of logic checks two conditions to determine if the path should be considered “straight”:

- Vehicle speed is less than a calibrated threshold.
- Radius calculation is greater than a calibrated threshold.

If either of these conditions exists, the filtered radius output is set to a default value identified in J2735 [6] (32,767 m as of revision 35). Figure 50 shows the logic flow for the host vehicle path radius calculation:

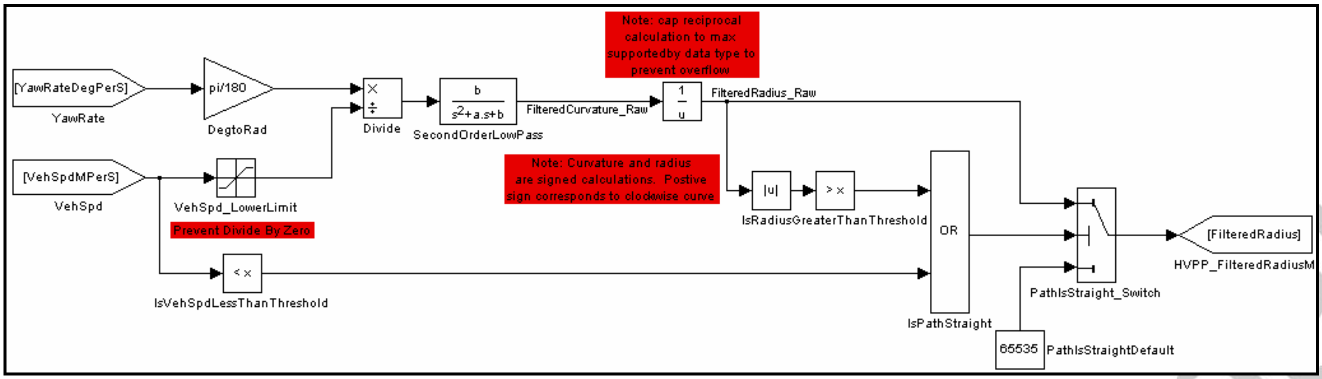


Figure 50: Vehicle Path Radius Calculation

A.6.4 Confidence Calculation

The preceding technique for calculating PP radii is highly effective when applied during “steady state” driving conditions; however, dynamic driving conditions can prove to be a challenge. Therefore a method must exist for identifying and communicating dynamic situations when path estimations may be largely inaccurate. Identifying “steady state” is accomplished by applying a confidence interval to a differentiated and filtered version of the yaw rate signal. The confidence indicator is calibrated to report low confidence when large changes in the vehicle yaw rate are detected over a short period of time. These conditions may include one or more of the following:

- Lane changes
- Curve entry and exit points
- Curve transitions
- Obstacle avoidance…and other highly dynamic driving situations

For the PP module, a second order low-pass filter with differentiator is used to identify that the vehicle is likely in “steady state” based steering input. The design is a discretized version of a standard second order unity-gain filter characterized by the following equations.

Discretized (unity-gain) second order low-pass filter with differentiator:

$$\frac{s\omega_0^2}{s^2 + 2\omega_0 \zeta s + \omega_0^2} = \frac{\omega_0^2 T_s - \omega_0 T_s z^{-1}}{z^{-2} - (2+2\omega_0 \zeta T_s)z^{-1} + (\omega_0^2 T_s^2 + 2\omega_0 \zeta T_s + 1)}$$

Continuous (1/s = integrator) Discrete (1/z = unit delay)

$$y_n = \frac{-y_{n-2} + (2+2\omega_0 \zeta T_s)y_{n-1} + \omega_0^2 T_s u_n - \omega_0^2 T_s u_{n-1}}{(\omega_0^2 T_s^2 + 2\omega_0 \zeta T_s + 1)}$$

(for $n \geq 3$)

Initialization: $y_1 = 0$, $y_2 = 0$

Figure 51: Discretized Second Order Low-Pass Filter with Differentiator

Again, $\omega_0 = 2\pi f_0$, f_0 = cutoff frequency, ζ = damping factor, and T_s = sampling time. Note: $\zeta = 1$ (default) for a critically damped system.

In order for the PP module to provide the highest accuracy future path estimations, the vehicle must be at or near “steady state” conditions. Determining when the host vehicle is in “steady state” is accomplished by a second calculation using the yaw rate sensor input. The PP module monitors the rate of change of the host vehicle yaw rate to determine when “steady state” conditions are most likely to exist. This is accomplished using a discretized second order low-pass filter with differentiator (Figure 51). The confidence filter is tuned with a higher cutoff frequency in order for the indicator to lead the radius calculation during dynamic driving conditions. This ensures that the confidence indicator is capable or reporting changes in confidence prior to the change in radius output.

After filtering and differentiating the yaw rate, the output is applied to a tunable lookup table that provides confidence levels ranging from 0% to 100%.

Figure 52 shows the logic flow for the host vehicle “steady state” confidence calculation:

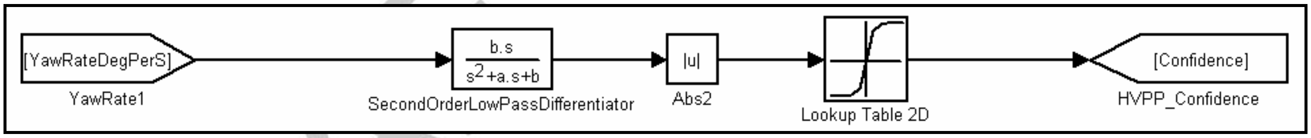


Figure 52: Vehicle Predicted Path Confidence Calculation

A.6.5 Calibration

Table 23 below contains a list of the PP calibration parameters referenced throughout this standard along with their default, minimum, and maximum configurable parameters.

Table 23. PP Calibration Parameters

Calibration Parameter	Description	Default Value	Minimum Value	Maximum Value
Curvature Cutoff Frequency	Low-pass cutoff frequency for curvature filter	0.33 Hz	0.32 Hz	0.34 Hz
Curvature Damping Factor	Curvature filter dampening factor	1	0	2
Curvature Sampling Period	Sample time for discrete curvature filter	100 ms	100 ms	400 ms
Minimum Vehicle Speed	Vehicle speed lower limit for curvature calculation	1 m/s	0 m/s (straight path only)	2 m/s
Maximum Radius	Radius upper limit beyond which the path is considered “straight.”	2,500 m	2,000 m	5,000 m
Straight Path	When radius is greater than the maximum radius, the reported radius is set to this value to indicate a “straight” path. Based on J2735 reserved value for path prediction radius.	32,767	32,767	32,767
Confidence Cutoff Frequency	Low-pass cutoff frequency for confidence filter	1 Hz	0.33 Hz	1 Hz
Confidence Damping Factor	Confidence filter dampening factor	1	0	2
Confidence Sampling Period	Sample time for discrete confidence filter	100 ms	100 ms	400 ms
Confidence Values	Two-dimensional table accepts filtered/differentiated yaw rate and outputs a confidence from 0%–100%	See Table 24 for values		

Table 24. Confidence Lookup Table

Input: Filtered/Differentiated Yaw Rate (degrees/s^2)	25	20	15	10	5	2.5	2	1.5	1	0.5	0
Output: Confidence (%)	0	10	20	30	40	50	60	70	80	90	100

A.7 OPEN SKY TEST CONDITIONS

The designation "Open Sky" environment is intended to describe an environment in which there are minimal obstructions to the device's view of the sky as used for testing in [14]. Open Sky Test Conditions are defined for the purposes of this standard, to be present when the following are all true:

1) No view obstructions external to the vehicle can be seen, from the point of view of the GNSS antennas of reference device and device under test, starting from 5° above the horizontal plane (the elevation mask) containing the antenna phase center, in all directions around the antenna.
2) The number of satellites used, as reported by the reference device for GNSS satellites only, is greater than or equal to 7.
3) The HDOP, as reported by the reference device for GNSS satellites, is less than or equal to 1.5, and VDOP is less than or equal to 3.

A.8 ADDITIONAL CONGESTION CONTROL ALGORITHM DETAILS

A.8.1 Assumption of latest HV State Information at RVs

After each transmission, use a Bernoulli trial with the channel quality indicator $\Pi(k)$ to infer whether this previous transmission is successfully received by RVs.

- If the outcome of this Bernoulli trial is positive, assume that the previous transmission by HV is successfully received by RVs. Update the latest information the RVs have about the HV as the state information contained in previous transmission.
- Else, if the outcome of this Bernoulli trial is negative, treat the previous transmission by HV as a failure and do not update the latest HV state information as that received by RVs.
- Count the number of Bernoulli trials with successive negative outcomes. If this is greater than *vMaxSuccessiveFail*, set the previous transmission as successful and update the latest information the RVs have about the HV as the state information contained in the previous transmission.

Let $\begin{bmatrix} t \\ x \\ y \\ v \\ \theta \end{bmatrix}_{\text{Latest}}$ be the HV's assumed latest state information received by RVs and $\begin{bmatrix} t \\ x \\ y \\ v \\ \theta \end{bmatrix}_{\text{Pre-Tx}}$ be the HV's state information contained in the message of its previous transmission (where t is the time in msec when the longitudinal position x (in degrees), lateral position y (in degrees), speed v (in m/s), and heading $\theta(t)$ (in degrees) are measured. The HV's assumed latest state information received by RVs is updated after each transmission as follows:

```
If $rand() < \Pi(k)$
$TxFailed = TxFailed + 1$
$Else$
$TxFailed = 0$
```

$$\begin{bmatrix} t \\ x \\ y \\ v \\ \theta \end{bmatrix}_{\text{Latest}} = \left\{ \begin{matrix} \begin{bmatrix} t \\ x \\ y \\ v \\ \theta \end{bmatrix}_{\text{Pre-Tx}} & \text{TxFailed} > 0 \text{ and TxFailed} <= \text{vMaxSuccessiveFail} \\ \begin{bmatrix} t \\ x \\ y \\ v \\ \theta \end{bmatrix}_{\text{Latest}} & \text{otherwise set TxFailed} = 0 \end{matrix} \right\}$$

where $rand()$ is a uniform random number generator and $\Pi(k)$ is the estimated channel quality indicator.

Note that this only helps an HV “guess” if the RV received the latest state information or not. The actual latest state information received by RVs might be different for each RV due to different scales of fading in the wireless channel and they might also be different from this HV’s assumed latest state information received by RVs. The derived latest state information only serves as the “expected” state information perceived by an HV and is used to adapt its transmission rate.

A.8.2 Tracking Error

Calculate the tracking error as the distance between HV local estimator position $(\hat{x}(k)$, $(\hat{y}(k)$) and output of the HV remote estimator position, ($\tilde{x}(k)$, $\tilde{y}(k)$) using the great circle formula, i.e.

$$e(k) = R(\hat{x}(k)) \times (\cos^{-1}(\sin(\hat{x}(k)) \times \sin(\tilde{x}(k)) + \cos(\hat{x}(k)) \\ \times \cos(\tilde{x}(k)) \times \cos(\hat{y}(k) - \tilde{y}(k))))$$

where

$$R(\hat{x}(k)) = a \times (1 - f_1^{\,2}) / (1 - f_1^{\,2} \times \sin^2(\hat{x}(k)))^{1.5}$$

is the Meridian Radius of the Earth in meters, at latitude $\hat{x}(k)$, a = 6378137 is the mean radius of earth in meters, $f_1 = (f \times (2 - f))^{0.5}$ is the Eccentricity, and f = 0.003353 is earth’s flattening.

Here $(\hat{x}(k), \hat{y}(k))$ are the latitude and longitude from the HV Local Estimator, converted to radians, and $(\tilde{x}(k), \tilde{y}(k))$ are the latitude and longitude from the HV Remote Estimator, converted to radians.

A.9 EXAMPLE SIGNED MESSAGE WITH CERTIFICATE AND CORRESPONDING ASN.1

Below is an example of the a generic signed message with certificate and the corresponding ASN.1. The 1609.2 [2] profile in 6.1.2 was used to generate this sample. The payload of this security envelope (the message) is the ASCII text string “This is a BSM”.

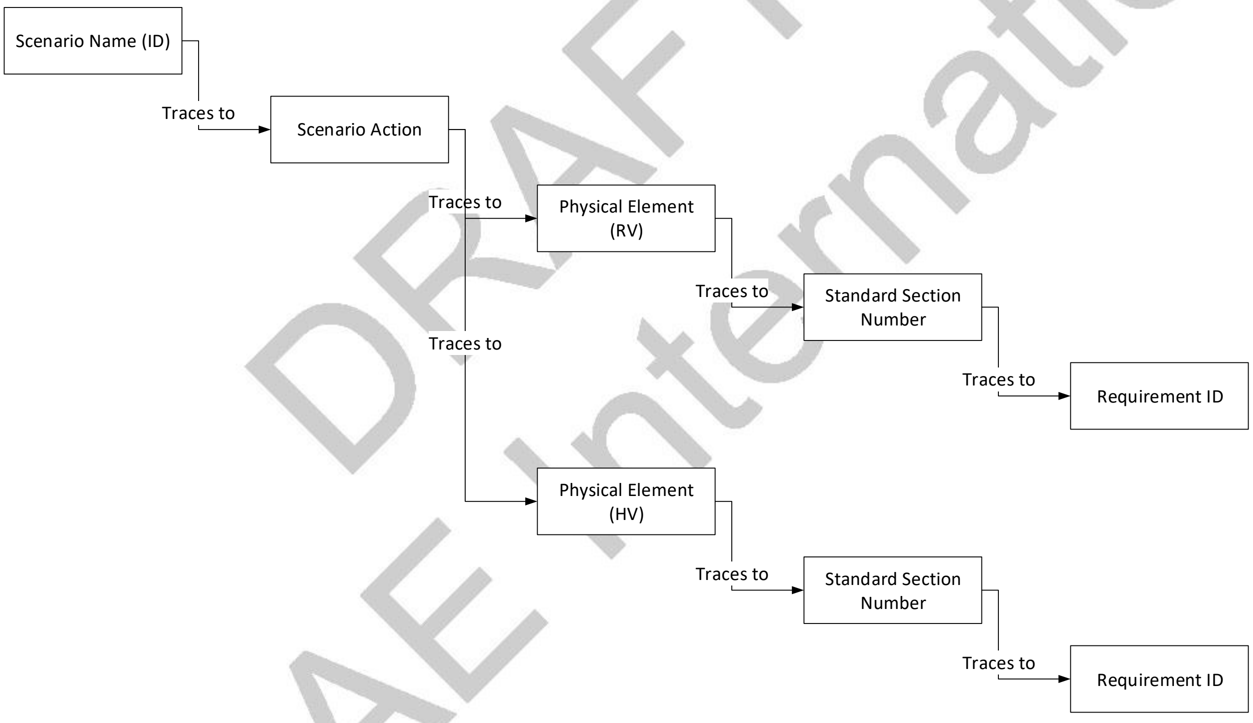
```
03 81 00 40 03 80 0F 54 68 69 73 20 69 73 20 61
20 42 53 4D 0D 0A 40 01 20 00 00 0A 35 23 77 2A
85 00 81 01 01 00 03 01 80 00 11 22 33 44 55 66
77 50 80 80 00 C8 00 11 22 33 44 55 66 77 88 56
70 AB 00 11 22 33 44 55 66 77 88 99 00 11 22 00
01 00 11 22 33 84 00 A9 83 01 03 80 00 7C 80 01
```

```
E4 80 03 48 01 02 00 01 20 00 01 26 81 82 00 11
22 33 44 55 66 77 88 99 AA BB CC DD EE FF 10 11
12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 80 82
00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
FF 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
```

```
value1 TestIeee1609Dot2Data ::= {
  protocolVersion 3,
  content signedData : {
    hashId sha256,
    tbsData {
      payload {
        data {
          protocolVersion 3,
          content unsecuredData : '5468697320697320612042534D0D0A'H
        }
      },
      headerInfo {
        psid 32,
        generationTime {
          time 11223344556677,
          logStdDev 0
        }
      }
    },
    signer certificate : {
      {
        version 3,
        type implicit,
        issuer ecdsaNistP256AndDigest : '0011223344556677'H,
        toBeSigned {
          id linkageData : {
            iCert 200,
            linkage-value '001122334455667788'H,
            group-linkage-value {
              jValue '5670AB'H,
              value '00112233445566778899'H
            }
          },
          cracaId '001122'H,
          crlSeries 1,
          validityPeriod {
            start 1122867,
            duration hours : 169
          },
          region identifiedRegion : {
            countryOnly : 124,
            countryOnly : 484,
            countryOnly : 840
          },
          appPermissions {
            {
              psid 32
            },
            {
              psid 38
            }
          },
          verifyKeyIndicator reconstructionValue : compressed-y-0 :
'00112233445566778899AABBCCDDEEFF101112131415161718191A1B1C1D1E1F'H
        }
      }
    },
    signature ecdsa256Signature : {
      r compressed-y-0 : '00112233445566778899AABBCCDDEEFF101112131415161718191A1B1C1D1E1F'H,
      s 'FF112233445566778899AABBCCDDEEFF101112131415161718191A1B1C1D1E1F'H
    }
  }
}
```

A.10 REQUIREMENTS TRACEABILITY

Figure X describes the traceability of the requirements in this Standard to the Scenarios defined for the Vehicle to Vehicle communications in section 4 or this Standard.



The Scenario Name is the title of a scenario and reference paragraph defined in section 4 of this standard. For example: EEBL – Lead Vehicle Decelerating (4.2.3), etc.

The Scenario Action is the specific action that applies or triggers the scenario(s). For example, RV-1 hard braking triggers the EEBL scenario (4.2.3).

The Physical Element (RV or HV) refers to the subsystem in Figure 1 that is the candidate(s) for implementing the function. When there is a Slash (“/”) mark, e.g. DSRC/ECU, it means the implementation could be in one or the other or both subsystems.

The Standard Section number is the section in this standard that contains the requirements for the scenario.

The Requirement ID is this Standards Requirements ID. When no Requirements ID is given, all requirements in the Standards Section number apply.

Scenario	Scenario Action	Physical Element RV-1 (BSM Transmitter)	Standard Section (for the RV)	Requirement Category (for the RV)	Physical Element HV (BSM receiver)	Standard Section (for the HV)	Requirement Category (for the HV)
Startup (4.3.4)	Power-On						
	Retrieve stored data		6.3.7.1 – Heading 6.3.7.2 - Path History	V2V-BSMTX-DATAPERSIST			V2V-BSMTX-DATAPERSIST
	Randomize ID	OBE Control Processor ECU	6.5.1 - Identification Randomization	V2V-SECPRIV-IDRAND	OBE Control Processor ECU	6.5.1 - Identification Randomization	V2V-SECPRIV-IDRAND
Shutdown (4.3.4)	Power-Off		6.3.7.1 – Heading 6.3.7.2 - Path History	V2V-BSMTX-DATAPERSIST			V2V-BSMTX-DATAPERSIST
Security Management (4.3.3)	Retrieve New Certificates/CRL list	OBE Control Processor ECU	6.6.1 -Bootstrap: Initialization and Enrollment Processing		OBE Control Processor ECU	6.6.1 - Bootstrap: Initialization and Enrollment Processing	
			6.6.1.1 -Initialization Process			6.6.1.1 - Initialization Process	
			6.6.1.2 - Enrollment Process			6.6.1.2 - Enrollment Process	
			6.6.2 - Certificate Loading	V2V-SECMGMT-CERTLOAD		6.6.2 - Certificate Loading	V2V-SECMGMT-CERTLOAD
	Store New Certificates	OBE Control Processor ECU	6.6.3 - Certificate Storage	V2V-SECMGMT-CERTSTORE	OBE Control Processor ECU	6.6.3 - Certificate Storage	V2V-SECMGMT-CERTSTORE
	CRL List	OBE Control Processor ECU	6.6.4 - Certificate Revocation List Loading	V2V-SECMGMT-CERTLOAD	OBE Control Processor ECU	6.6.4 - Certificate Revocation List Loading	V2V-SECMGMT-CERTLOAD
	Securing Certificates/CRL lists	SOBE Control Processor ECU	6.6.5 - Security Hardware	V2V-SECMGMT-SECHW	OBE Control Processor ECU	6.6.6 - Hardware Security Module	V2V-SECMGMT-SECHW

Scenario	**Scenario Action**	**Physical Element RV-1 (BSM Transmitter)**	**Standard Section (for the RV)**	**Requirement Category (for the RV)**	**Physical Element HV (BSM receiver)**	**Standard Section (for the HV)**	**Requirement Category (for the HV)**
Transmit BSM per vBSMTxRate (4.3.1)	Transmit BSM	OBE Control Processor ECU	6.3.3 - Transmit Timing	V2V-BSMTX-TXTIM			
Certificate Change (4.3.3)	5-Minute Rotation	OBE Control Processor ECU	6.5.4 - Certificate Change	V2V-SECPRIV-CERTCHG	GNSS/Safety Application (ECU)		
	Randomize ID		6.5.1 - Identification Randomization	V2V-SECPRIV-IDRAND			
EEBL - Lead Vehicle Decelerating (4.2.3)	RV-1 abruply brakes Hard	GNSS Receiver	6.2.1 - Position Determination	V2V-POSTIM-POSDETER			
			6.2.2 - Wide Area Augmentation*	V2V-POSTIM-WAAS			
		OBE Control Processor ECU	6.2.3 - Coordinate System & Ref	V2V-POSTIM-COORDSYSREF			
		GNSS/OBE Control Processor ECU	6.2.4 - System Time Coordination	V2V-POSTIM-SYSTIMCOORD			
		OBE Control Processor ECU	6.3.1 - BSM Content	BSMTX-BSMCONT			
			6.3.6.1 - DE_DSRC_MessageID	V2V-BSMTX-DATAACC			
			6.3.6.2 - DE_MsgCount				
			6.3.6.3 - DE_TemporaryID				
			6.3.6.4 - DE_Dsecond				
			6.3.6.5 - DE_Latitude & DE_Longitude				
			6.3.6.6 - DE_Elevation				
			6.3.6.7 - DE_Positional Accuracy				
			6.3.6.8 - DF_TransmissionAndSpeed				
			6.3.6.9 - DE_Heading				

Scenario	Scenario Action	Physical Element RV-1 (BSM Transmitter)	Standard Section (for the RV)	Requirement Category (for the RV)	Physical Element HV (BSM receiver)	Standard Section (for the HV)	Requirement Category (for the HV)
			6.3.6.10 - DE_SteeringWheelAngle				
			6.3.6.11 - DF_AccelerationSet4Way				
			6.3.6.12 - DF_BrakeSystemStatus				
			6.3.6.13 - DF_VehicleSize				
			6.3.6.14 - DE_EventFlages (Hard brakeing flag) - not used for all other application use cases				
			6.3.6.15 - DF_PathHistory				
			6.3.6.16 - DF_PathPrediction				
			6.3.6.17 - DE_ExteriorLights				
			6.3.6.18 - Additional Data Elements				
	Signs the Data - using the RV certificate	OBE Control Processor ECU	6.5.2 - BMS Signing	V2V-SECPRIV-BSMSIGN			
		DSRC Radio	6.3.2 - Channel and Data Rate	V2V-BSMTX-CHDATARATE			
		OBE Control Processor ECU	6.3.3 - Transmit Timing	V2V-BSMTX-TXTIM			
		DSRC Radio	6.3.4 - User Priority EDCA settings	V2V-BSMTX-UPEDCA			
		OBE Control Processor ECU	6.3.5 - Minimum Transmission Criteria	V2V-BSMTX-MINTX			
		DSRC Radio	6.4.1 - DSRC Transmit Power Accuracy and Radiated Transmit Power	V2V-RFPERF-DSRCTX			
		Antennas	6.4.3 - DSRC Polarization	V2V-RFPERF-DSRCPOL			
	Verify signature - using Host certificate				OBE Control Processor ECU	6.5.3- BSM Verification	V2V-SECPRIV-BSMVERIFY
	Check Revocation List					6.5.5 - Certification	V2V-SECPRIV-CERTREV

Scenario	**Scenario Action**	**Physical Element RV-1 (BSM Transmitter)**	**Standard Section (for the RV)**	**Requirement Category (for the RV)**	**Physical Element HV (BSM receiver)**	**Standard Section (for the HV)**	**Requirement Category (for the HV)**
						Revocation	
					GNSS Receiver	6.2.1 - Position Determination	V2V-POSTIM-POSDETER
						6.2.2 - Wide Area Augmentation*	V2V-POSTIM-WAAS
					OBE Control Processor ECU	6.2.3 - Coordinate System & Ref	V2V-POSTIM-COORDSYSREF
					GNSS/OBE Control Processor ECU	6.2.4 - System Time Coordination	V2V-POSTIM-SYSTIMCOORD
					DSRC Radio	6.4.2 - DSRC Receive Sensitivity	V2V-RFPERF-DSRCRXSENS
					Antennas	6.4.3 - DSRC Polarization	V2V-RFPERF-DSRCPOL
FCW-Forward Collision Warning (4.2.4)	Vehicle Stopped (Transmit BSM per vBSMTxRate)	OBE Control Processor ECU	6.3.3 - Transmit Timing	V2V-BSMTX-TXTIM			
BSW /LCW-Blind Spot Warning/Lane Change Warning (4.2.5)	Transmit BSM per vBSMTxRate		6.3.3 - Transmit Timing				
IMA-Intersection Movement Assist (4.2.6)	Transmit BSM per vBSMTxRate		6.3.3 - Transmit Timing				
LTA - Left Turn Assist (4.2.7)	Transmit BSM per vBSMTxRate		6.3.3 - Transmit Timing				
CLW - Control Loss Warning	Transmit BSM per vBSMTxRate		6.3.3 - Transmit Timing				

Scenario	Scenario Action	Physical Element RV-1 (BSM Transmitter)	Standard Section (for the RV)	Requirement Category (for the RV)	Physical Element HV (BSM receiver)	Standard Section (for the HV)	Requirement Category (for the HV)
(4.2.8)							
Scenarios 4.2.4 to 4.2.8		GNSS Receiver	6.2.1 - Position Determination	V2V-POSTIM-POSDETER			
			6.2.2 - Wide Area Augmentation*	V2V-POSTIM-WAAS			
		OBE Control Processor ECU	6.2.3 - Coordinate System & Ref	V2V-POSTIM-COORDSYSREF			
			6.2.4 - System Time Coordination	V2V-POSTIM-SYSTIMCOORD			
			6.3.1 - BSM Content	BSMTX-BSMCONT			
			6.3.6.1 - DE_DSRC_MessageID	V2V-BSMTX-DATAACC			
			6.3.6.2 - DE_MsgCount				
			6.3.6.3 - DE_TemporaryID				
			6.3.6.4 - DE_Dsecond				
			6.3.6.5 - DE_Latitude & DE_Longitude				
			6.3.6.6 - DE_Elevation				
			6.3.6.7 - DE_Positional Accuracy				
			6.3.6.8 - DF_TransmissionAndSpeed				
			6.3.6.9 - DE_Heading				
			6.3.6.10 - DE_SteeringWheelAngle				
			6.3.6.11 - DF_AccelerationSet4Way				
			6.3.6.12 - DF_BrakeSystemStatus				
			6.3.6.13 - DF_VehicleSize				
			6.3.6.15 - DF_PathHistory				
			6.3.6.16 - DF_PathPrediction				
			6.3.6.17 -				

Scenario	Scenario Action	Physical Element RV-1 (BSM Transmitter)	Standard Section (for the RV)	Requirement Category (for the RV)	Physical Element HV (BSM receiver)	Standard Section (for the HV)	Requirement Category (for the HV)
			DE_ExteriorLights				
			6.3.6.18 - Additional Data Elements				
	Signs the Data - using the RV certificate	Safety Application (ECU)/DSRC	6.5.2 - BMS Signing	V2V-SECPRIV-BSMSIGN			
		DSRC	6.3.2 - Channel and Data Rate	V2V-BSMTX-CHDATARATE			
			6.3.3 - Transmit Timing	V2V-BSMTX-TXTIM			
			6.3.4 - User Priority EDCA settings	V2V-BSMTX-UPEDCA			
			6.3.5 - Minimum Transmission Criteria	V2V-BSMTX-MINTX			
			6.4.1 - DSRC Transmit EIRP and Conducted Power	V2V-RFPERF-DSRCTX			
			6.4.3 - DSRC Polarization	V2V-RFPERF-DSRCPOL			
	Verify signature - using Host certificate				OBE Control Processor ECU	6.5.3 - BSM Verification	V2V-SECPRIV-BSMVERIFY
	Check Revocation List					6.5.5 - Certification Revcation	V2V-SECPRIV-CERTREV
					GNSS Receiver	6.2.1 - Position Determination	V2V-POSTIM-POSDETER
						6.2.2 - Wide Area Augmentation*	V2V-POSTIM-WAAS
					OBE Control Processor ECU	6.2.3 - Coordinate System & Ref	V2V-POSTIM-COORDSYSREF
						6.2.4 - System Time Coordination	V2V-POSTIM-SYSTIMCOORD
					DSRC Radio	6.4.2 - DSRC Receive Sensitivity	V2V-RFPERF-DSRCRXSENS

Scenario	**Scenario Action**	**Physical Element RV-1 (BSM Transmitter)**	**Standard Section (for the RV)**	**Requirement Category (for the RV)**	**Physical Element HV (BSM receiver)**	**Standard Section (for the HV)**	**Requirement Category (for the HV)**
					Antennas	6.4.3 - DSRC Polarization	V2V-RFPERF-DSRCPOL
All Scenarios	Mac Access Control and Physical Layer	DSRC Radio	6.1.1 - 802.11 Requirements - Table 5	V2V-STD-802.11	DSRC Radio	6.1.1 - 802.11 Requirements - Table 5	V2V-STD-802.11
All Scenarios	Security Services		6.1.2 - IEEE 1609.2 Requirements - Table 6, 10	V2V-STD-1609.2		6.1.2 - IEEE 1609.2 Requirements - Table 7, 11	V2V-STD-1609.2
All Scenarios	Networking Services		6.1.3 - IEEE 1609.3 Requirements - Table 14	V2V-STD-1609.3		6.1.3 - IEEE 1609.3 Requirements - Table 14	V2V-STD-1609.3
All Scenarios	Multi Channel Operations		6.1.4 - IEEE 1609.4 Requirements - Table 15	V2V-STD-1609.4		6.1.4 - IEEE 1609.4 Requirements - Table 15	V2V-STD-1609.4
All Scenarios	Identifier Allocations		6.1.5 - IEEE 1609.12 Requirements - Table 16	V2V-STD-1609.12		6.1.5 - IEEE 1609.12 Requirements - Table 16	V2V-STD-1609.12
All Scenarios	Message Encoding		6.1.6 - SAE J2735 Requirements - Table 17	V2V-STD-J2735		6.1.6 - SAE J2735 Requirements - Table 17	V2V-STD-J2735