



SURFACE VEHICLE STANDARD	J3161™/1	SEP2025
	Issued	2022-03
	Revised	2025-09
Superseding J3161/1 SEP2024		
Onboard System Requirements for LTE-V2X V2V Safety Communications		

RATIONALE

This limited scope revision corrects editorial errors in Table A1 of Appendix A and clarifies the SSP requirements in Appendix B.

TABLE OF CONTENTS

1.	SCOPE.....	4
1.1	Purpose.....	4
2.	REFERENCES.....	4
2.1	Applicable Documents	4
2.1.1	SAE Publications.....	4
2.1.2	ETSI/3GPP Publications	5
2.1.3	IEEE Publications.....	5
2.1.4	Code of Federal Regulations (CFR) Publications.....	5
2.2	Related Publications	6
3.	DEFINITIONS AND ABBREVIATIONS.....	6
3.1	Definitions	6
3.2	Abbreviations and Acronyms	7
3.3	Requirement Numbering Convention.....	9
4.	V2V SAFETY SYSTEMS CONCEPT OF OPERATIONS AND SYSTEM DESCRIPTION	11
4.1	V2V System Overview	11
4.2	V2V Safety Features	13
5.	INTERFACE DESCRIPTION	13
5.1	V2V Over-the-Air Data Description	13
5.1.1	Basic Safety Message Exchange	13
5.1.2	Positioning.....	13
5.1.3	Security and Privacy	13
5.1.4	Start-Up and Shutdown.....	14
5.1.5	Mapping to the V2V Over-the-Air Data	14
5.1.6	PC5 Radio Preconfiguration	14

SAE Executive Standards Committee Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2025 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, or used for text and data mining, AI training, or similar technologies, without the prior written permission of SAE.

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
http://www.sae.org

SAE WEB ADDRESS:

Full document details: SAE J3161_1_202509

For more information on this standard, visit
https://www.sae.org/standards/content/J3161/1_202509/

Documents

Standard, visit Sharing Hub

5.2	System Interfaces	15
5.2.1	Vehicle-to-Vehicle Communications Interface	15
5.2.2	System to SCMS Communications Interface.....	15
5.2.3	System to Positioning Subsystem Interface.....	15
6.	MINIMUM REQUIREMENTS	16
6.1	Standards Profiles (STD)	16
6.1.1	ETSI	16
6.1.2	IEEE 1609.2 (1609.2).....	30
6.1.3	IEEE 1609.3 (1609.3).....	33
6.1.4	IEEE 1609.4	33
6.1.5	IEEE 1609.12 (1609.12).....	33
6.1.6	SAE J2735 (J2735).....	34
6.1.7	Regulatory (Informative).....	35
6.2	Positioning and Timing Requirements (POSTIM).....	35
6.3	BSM Transmission Requirements (BSMTX).....	35
6.3.1	BSM Contents (BSMCONT).....	35
6.3.2	Channel and Data Rate.....	35
6.3.3	Generation of the First BSM after System Device Start-Up and Generation Timing (GENTIM)	36
6.3.4	ProSe per Packet Priority (PPPP) Settings.....	37
6.3.5	Minimum Transmission Criteria (MINTX).....	37
6.3.6	Data Element Accuracy (DATAACC).....	37
6.3.7	Data Persistency (DATAPERSIST)	40
6.3.8	BSM Scheduling and Congestion Control (BSMCONGCTRL).....	40
6.4	RF Performance Requirements (RFPERF)	44
6.4.1	Minimum TX RF Performance and Signal Strength (TXSS).....	44
6.4.2	Receiver Sensitivity (RXSENS)	47
6.5	Security and Privacy Requirements (SECPRIV)	47
6.5.1	Identification Randomization (IDRAND).....	47
6.5.2	BSM Signing (BSMSIGN)	48
6.5.3	Identifier Change (IDCHG).....	48
6.5.4	BSM Cryptographic Verification (BSMVERIFY).....	48
6.5.5	Certificate Revocation (CERTREV) (Deprecated)	48
6.6	Security Management (SECMGMT)	49
6.6.1	Certificate Loading (CERTLOAD).....	49
6.6.2	Certificate Storage (CERTSTORE).....	49
6.6.3	Certificate Revocation List Loading (CRLLOAD).....	49
6.6.4	Secure Hardware (SECHW)	49
7.	PARAMETER SETTINGS.....	50
8.	NOTES	50
8.1	Revision Indicator.....	50
APPENDIX A		51
APPENDIX B	SSP DESIGN	62
Figure 1	Onboard V2V system	12
Figure 2	Relationship between computational intervals: vPERSubInterval, vPERInterval, and vTxRateCntrlInt.....	40
Figure 3	Sliding window	41
Figure 4	Definition of TX signal strength zones	45
Table 1	Requirement numbering abbreviations	10
Table 2	Mapping data elements and frames for emergency vehicle notification	14
Table 3	LTE-V2X PC5 preconfiguration requirements	21
Table 4	PSSCH transmission parameter	27
Table 5	PSSCH transmission parameter for speed <120 km/h	28
Table 6	PSSCH transmission parameter for speed ≥120 km/h	29
Table 7	RSRP exclusion threshold (dBm per RE) for different transmitting packet priority versus receiving packet priority	30

Table 8	Security profile identification	30
Table 9	Security profile for transmitting BSMs.....	31
Table 10	Security profile for receiving BSMs	32
Table 11	Security management profile	33
Table 12	IEEE 1609.12 requirements	34
Table 13	SAE J2735 supplemental requirements.....	34
Table 14	20 MHz low speed (<120 km/h)	36
Table 15	20 MHz high speed (≥120 km/h).....	36
Table 16	20 MHz low speed exceptions for event-based transmissions (<120 km/h)	36
Table 17	Minimum linear average TX signal strength around vehicle (70% coverage)	45
Table 18	Parameter exceptions to SAE J2945/1	50

1. SCOPE

This SAE Standard specifies system requirements for an onboard vehicle-to-vehicle (V2V) safety communications system for vehicle classes of 2, 3, 4, and 5,¹ including standards profiles, functional requirements, and performance requirements. The system is capable of transmitting and receiving the SAE J2735-defined basic safety message (BSM) over a PC5 Sidelink V2X (mode 4) communications link as defined in ETSI Release 14.^{2,3} The system uses Institute of Electrical and Electronics Engineers (IEEE) 1609 standards for network and transport layer communications, as well as security.

NOTE 1: For extra data elements related to class 4 school bus, refer to SAE J2945/1C.

NOTE 2: For the functional and performance requirements for V2V safety communications for FHWA classes 1 and 6 to 13, which are not covered in this document, refer to SAE J2945/1B.

NOTE 3: The 2024 version of the document requires the configuration of Sidelink Synchronization Signal (SLSS), and this breaks the backward compatibility with the previous version of this document (SAE J3161/1_202203). Onboard Units (OBUs) that are not configured with SLSS configuration will not be interoperable with OBUs that are configured with SLSS configuration. They will not be able to exchange messages (e.g., BSMs), and transmissions from OBUs with SLSS configuration may interfere with transmissions from OBUs without SLSS configuration.

1.1 Purpose

This standard addresses the onboard system needs for ensuring that the exchange of BSMs in V2V safety communications using LTE-V2X Sidelink 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. Unless otherwise indicated, the latest issue of SAE publications shall apply.

2.1.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (U.S. and Canada only) or +1 724-776-4970 (Outside U.S. and Canada), www.sae.org.

SAE J2735	V2X Communications Message Set Dictionary
SAE J2945/1	On-Board System Requirements for V2V Safety Communications
SAE J2945/1B	On-Board System Requirements for V2V Safety Communications by Non-Light-Duty Vehicles and Motorcycles
SAE J2945/1C	On-Board System Requirements for V2V Safety Communications by School Buses
SAE J2945/5	Service Specific Permissions and Security Guidelines for Connected Vehicle Applications
SAE J3161	LTE Vehicle-to-Everything (LTE-V2X) Deployment Profiles and Radio Parameters for Single Radio Channel Multi-Service Coexistence

¹ Other vehicle classes and trailers are addressed in SAE J2945/1B. These revisions or additional standards are expected to be compatible with the requirements of this standard and may define additional capabilities beyond the requirements defined in this document.

² Hereafter in this document, whenever the terms "LTE-V2X," "Sidelink," or "PC5" are used separately or in any combination, they refer to ETSI Release 14 PC5 Sidelink (mode 4) communication. External documents may also refer to this technology as cellular-V2X or C-V2X.

³ This document recommends the use of transmit diversity. Examples of transmit diversity include switch diversity or Tx diversity with two Tx ports.

2.1.2 ETSI/3GPP Publications

The references to ETSI documents in this section refer to ETSI transposition of specific 3GPP technical specifications available from 3GPP Mobile Competence Centre, c/o ETSI, 650, route des Lucioles, 06921, Sophia Antipolis Cedex, France, www.etsi.org. The equivalent 3GPP documents are listed in brackets below.

Please note that this report incorporates certain ETSI/3GPP specifications by reference. ESSENTIAL IPRs (Intellectual Property Rights) have been declared to ETSI. All information statements and licensing declarations of ESSENTIAL IPRs received by ETSI are publicly available via the ETSI IPR Online Database found at <https://ipr.etsi.org/DynamicReporting.aspx>.

The following list of documents are from the ETSI Release 14 set of standards and are referred to in the body of this document by their document number (e.g., ETSI TS 136 321, which is equivalent to 3GPP TS 36.321):

ETSI TS 123 285	Architecture enhancements for V2X services, V14.9.0 (Release 14) [3GPP TS 23.285]
ETSI TS 123 303	Proximity-based services (ProSe); Stage 2, V14.1.0 (Release 14) [3GPP TS 23.303]
ETSI TS 136 201	Evolved Universal Terrestrial Radio Access (E-UTRA); LTE physical layer; General description v14.1.0 (Release 14) [3GPP TS 36.201]
ETSI TS 136 213	Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures, V14.2.0 (Release 14) [3GPP TS 36.213]
ETSI TS 136 321	Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification, V14.2.1 (Release 14) [3GPP TS 36.321]
ETSI TS 136 322	Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Link Control (RLC) protocol specification, V14.1.0 (Release 14) [3GPP TS 36.322]
ETSI TS 136 331	Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification, V14.14.0 (Release 14) [3GPP TS 36.331]

These documents may reference other related ETSI documents.

2.1.3 IEEE Publications

Available from IEEE Operations Center, 445 and 501 Hoes Lane, Piscataway, NJ 08854-4141, Tel: 732-981-0060, www.ieee.org.

IEEE 1609.2-2022	IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages (as amended by IEEE 1609.2a-2017 and IEEE 1609.2b-2019)
IEEE 1609.2.1	IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Certificate Management Interfaces for End Entities
IEEE 1609.3-2020	IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services
IEEE 1609.12-2019	IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Identifier Allocations

2.1.4 Code of Federal Regulations (CFR) Publications

Copies of these documents are available online at www.ecfr.gov.

47 CFR Part 90	Private Land Mobile Radio Services
47 CFR Part 95	Personal Radio Services

2.2 Related Publications

Refer to 2.2 of SAE J2945/1.

3. DEFINITIONS AND ABBREVIATIONS

3.1 Definitions

Definitions unique to this document are included here. Refer to 3.1 of SAE J2945/1.

3.1.1 ACTIVE EMERGENCY RESPONSE VEHICLE

A public safety vehicle that is in an emergency response.

3.1.2 CRITICAL EVENT CONDITION

When an event that corresponds to a critical event flag occurs or when a public safety vehicle (police, fire, or ambulance) is engaged in an emergency response.

NOTE: The inclusion of emergency response as a critical event condition is supplemental to the SAE J2945/1 definition of a critical event condition. Requirements in SAE J2945/1 that apply when a critical event flag is set also apply to a public safety vehicle engaged in an emergency response.

3.1.3 CRITICAL EVENT FLAG

The hard braking, ABS, traction control, and stability control event flags within DE_VehicleEventFlags.

3.1.4 EMERGENCY RESPONSE

When a public safety vehicle includes DF_EmergencyDetails in its BSM, it will typically indicate the activation of light bar or siren. However, it is crucial to note that a vehicle can be in emergency response mode without the activation of the light bar or sirens. For example, this might occur when the vehicle is near an active incident.

3.1.5 PUBLIC SAFETY VEHICLE

An equipped vehicle that can be engaged in public safety operation or emergency response (i.e., police, fire, or ambulance vehicle). This type of vehicle is presumed to be equipped with an onboard unit specialized for public safety (PSOBV).

NOTE: When a public safety vehicle is not engaged in emergency response, the vehicle operates as a regular vehicle and its corresponding class and type (e.g., lower transmission power not including DF_EmergencyDetails).

3.1.6 USER EQUIPMENT

Any device used to communicate with other devices. In this document, UE is capable of LTE-V2X communication and refers to the LTE-V2X radio that is included both in OBU and RSU.

3.1.7 V2X VEHICLE

A vehicle equipped with devices enabling interoperable direct short-range broadcast communication using 3GPP-defined LTE-V2X Rel-14 PC5 mode to convey safety- and mobility-enhancing messages. The V2X vehicle defined and used in this standard does not include networked communications or commercial connected vehicle applications.

3.2 Abbreviations and Acronyms

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

3D	Three-Dimensional
3GPP	Third Generation Partnership Project
ASN.1	Abstract Syntax Notation One
BSM	Basic Safety Message
CBR	Channel Busy Ratio
CFR	Code of Federal Regulations
CR	Channel Occupancy Ratio
C-V2X	Cellular Vehicle-to-Everything
D2D	Device-to-Device
DE	Data Element
DF	Data Frame
DVI	Driver Vehicle Interface
EARFCN	Evolved-UTRA Absolute Radio Frequency Number
ECU	Electronic Control Unit
EIRP	Effective Isotropic Radiated Power
ETSI	European Telecommunications Standards Institute
E-UTRA	Evolved Universal Mobile Telecommunications System (UMTS) Terrestrial Radio Access
FCC	Federal Communications Commission
GHz	Gigahertz
GNSS	Global Navigation Satellite System
HARQ	Hybrid Automatic Repeat Request
HV	Host Vehicle
Hz	Hertz
IEEE	Institute of Electrical and Electronics Engineers
IPv6	Internet Protocol Version 6
ITT	Inter-Transmit Time
km/h	Kilometers per Hour

LTE	Long-Term Evolution
LTE-V2X	Long-Term Evolution - Vehicle-to-Everything
MAC	Medium Access Control
MCS	Modulation and Coding Scheme
MHz	Megahertz
OBE	Onboard Equipment
OFDM	Orthogonal Frequency Division Multiplexing
PC5	ProSe Communications 5
PDB	Packet Delay Budget
PDCP	Packet Data Convergence Protocol
PDCP SN	Packet Data Convergence Protocol Sequence Number
PER	Packet Error Ratio
PGK	ProSe Group Key
PICS	Protocol Implementation Conformance Statement
PPPP	ProSe Per Packet Priority
PRB	Physical Resource Block
PSCCH	Physical Sidelink Control Channel
PSID	Provider Service ID
PSSCH	Physical Sidelink Shared Channel
PTK	ProSe Traffic Key
QPSK	Quadrature Phase Shift Keying
RAN	Radio Access Network
RF	Radio Frequency
RLC	Radio Link Control
RLC UM	Radio Link Control Unacknowledged Mode
RP	Radiated Power
RSE	Roadside Equipment
RSRP	Reference Signal Received Power
RSSI	Received Signal Strength Indicator

RV	Remote Vehicle
SCI	Sidelink Control Information
SCMS	Security Credential Management System
SFN	System Frame Number
SLSS	Sidelink Synchronization Signal
S-RSRP	Sidelink Reference Signal Received Power
SPS	Semi-Persistent Scheduling
STCH	Sidelink Traffic Channel
TX	Transmit
UE	User Equipment ⁴
USIM	Universal Subscriber Identity Module
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
WAAS	Wide Area Augmentation System
WAVE	Wireless Access in Vehicular Environment
WSA	WAVE Service Advertisement
WSM	WAVE Short Message
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, 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.

⁴ In this document, the terms UE and OBE are used interchangeably. User equipment could also be a transmitting device or receiving device depending on the context.

Table 1 - Requirement numbering abbreviations

Section	Subsection	Category	Category Abbreviation	Subcategory	Subcategory Abbreviation
6.1	6.1.1	Standards Profiles	STD	ETSI PC5 V2X	ETSI
	6.1.2			IEEE 1609.2	1609.2
	6.1.3			IEEE 1609.3	1609.3
	6.1.5			IEEE 1609.12	1609.12
	6.1.6			SAE J2735	SAE 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			First BSM after Start-up and Generation Timing	GENTIM
	6.3.4			Priority Settings	PPPP
	6.3.5			Minimum Transmission Criteria	MINTX
	6.3.6			Data Element Accuracy	DATAACC
	6.3.7			Data Persistency	DATAPERSIST
	6.3.8			BSM Scheduling and Congestion Control	CONGCTRL
6.4	6.4.1	RF Performance	RFPERF	Minimum TX RF Performance and Signal Strength	TXSS
	6.4.2			Receive Sensitivity	RXSENS
6.5	6.5.1	Security and Privacy	SECPRIV	ID Randomization	IDRAND
	6.5.2			BSM Signing	BSMSIGN
	6.5.3			Certificate Change	CERTCHG
	6.5.4			BSM Verification	BSMVERIFY
	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
	Appendix B	Service Specific Permissions	SSP	Emergency Vehicles	EV

* These subsections refer to SAE J2945/1.

4. V2V SAFETY SYSTEMS CONCEPT OF OPERATIONS AND SYSTEM DESCRIPTION

This section provides a high-level description of the V2V safety concept of operations and system description. An overview of the system is provided in 4.1, and 4.2 provides the system description 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 PC5 V2X radios to transmit BSMs that include a subset of the available data frames and elements in SAE J2735. 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 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 as 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, communications security is essential to protect messages from attacks such as spoofing, alteration, or replay, which could cause false alerts or suppress true alerts. All BSMs are sent with a signature and digital certificate information that enables the receiving vehicle to verify that the message has come from an authorized BSM sender and has not been modified since the authorized sender created it.

Additionally, some BSM senders have an expectation of privacy in the sense that sending BSMs should not make it easy for a sender's movements to be tracked across a long stretch of time. This document recognizes two different types of BSM senders: private senders, who use privacy enhancing mechanisms specified later in this document that make it harder for those senders to be identified or tracked; and identified senders, who do not use those privacy enhancing mechanisms and who may include information in their transmissions that allows that sender to be linked with a real-world identity. A private sender does not disclose information about the sender that can be linked to a real-world identity like the license plate. Broadcast information that could potentially be used to identify and track drivers is anonymous and randomized. Fields in the message that are (locally) unique to the sender are changed from time to time, and the signing certificate is also changed when all other identifying fields are changed. If the sender is an identified sender, the certificate may (but is not required to) contain real-world identity information, and broadcast information and certificates are not randomized or changed. For a private sender, the certificate is referred to as a pseudonym certificate; for an identified sender, the certificate is referred to as an identification certificate.

Because privacy enhancing mechanisms introduce implementation complexity (as devices need to manage switching between multiple identities and associated certificates), this document does not require that all BSM senders be private senders. It is anticipated that vehicles operated for personal use will always act as private senders. Other vehicles may choose to (or be required to) act as identified senders to reduce complexity or to satisfy public policy requirements for auditability and accountability or for other reasons. For example, vehicles operating in a public service capacity (such as "on-duty" road maintenance vehicles, buses, or emergency vehicles) are natural candidates to operate in identified mode.

Figure 1 illustrates the components of the V2V system and its interfaces. 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 supporting or participating systems. The services provided by the SCMS are described in 6.6.

The V2V onboard equipment (OBE), which is the onboard vehicle-to-vehicle (V2V) safety communications system defined in this standard (hereafter referred to as the system), 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:

- PC5 radio subsystem: Transmits and receives BSMS. The OBE can include one or more LTE-V2X radio subsystems and still comply with this standard, as long as it meets the performance requirements herein.
- Positioning subsystem: The subsystem that includes a global navigation satellite system (GNSS) receiver and provides vehicle position, heading, speed, and time information. The system may augment and enhance positioning using additional information and components that are not shown in Figure 1. Examples of these are speed data from the controller area network (CAN) bus, dead reckoning sensors, and optical/camera based systems.
- OBE control processor electronic control unit (ECU): Executes software that generates BSMS for transmission according to the requirements in this standard.
- Antennas: Support radio frequency (RF) links for the PC5 radio and GNSS receiver.

Systems (OBE) communicate amongst themselves using the PC5 radio subsystem as an interface. The system 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 CAN bus to obtain vehicle status information. The safety application ECU, CAN bus, and DVI are outside the scope of this standard.

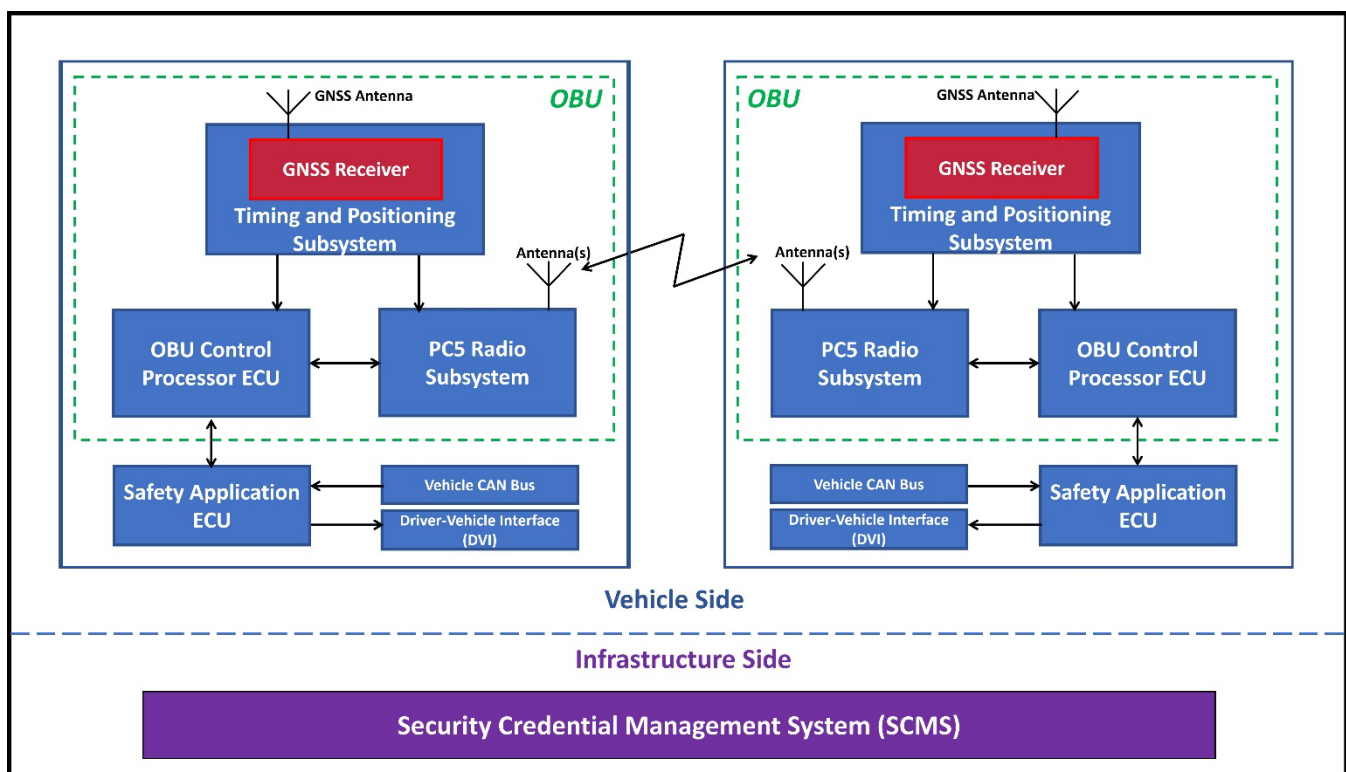


Figure 1 - Onboard V2V system

4.2 V2V Safety Features

The V2V safety features used as the conceptual basis for development of V2V safety communications standards were originally developed for a DSRC-based interface, as defined in SAE J2945/1. Therefore, the entirety of 4.2 of SAE J2945/1 is hereby incorporated by reference.

This document additionally includes support for information transmitted by public safety vehicles engaged in an emergency response (police and fire vehicles and ambulances). This feature allows additional information to be included in the BSM (e.g., light bar and siren information), which enables other vehicles and local infrastructure to be informed of the presence of public safety vehicles engaged in an emergency response.

5. INTERFACE DESCRIPTION

5.1 V2V Over-the-Air Data Description

5.1.1 Basic Safety Message Exchange

Refer to 5.1.1 of SAE J2945/1. This document also includes support for public safety vehicles to include details related to emergencies in their BSM (i.e., use of DF_EmergencyDetails in the BSM).

5.1.2 Positioning

Refer to 5.1.2 of SAE J2945/1.

5.1.3 Security and Privacy

5.1.3.1 Signing and Verification Algorithm

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.

5.1.3.2 BSM Signature and Certificate Transmission

Each BSM is encapsulated in a signed SPDU per IEEE 1609.2 for transmission, i.e., it is transmitted as a datagram that includes a digital signature and either a security certificate containing the public key or a certificate digest (hash of the current security certificate). The BSM is sent with a certificate approximately every 500 ms (see 6.5.2), and other BSMs are sent with a certificate 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.

NOTE: If a receiver does not have the signing certificate associated with a received digest, it cannot verify the message. This is a known feature and considered an acceptable risk.

The certificate indicates that the signer is entitled to sign BSMs. This is indicated using the PSID field in the certificate. A field associated with the PSID, known as the service specific permissions (SSP), can be used to indicate authorization to carry out specific actions or assume specific roles in the context of BSM signing. This document specifies SSPs to be used in the certificates of public safety vehicles.

5.1.3.3 BSM Verification

The receiver can verify every message or use a verify on demand (VOD) approach, whereby 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, or the receiver may verify a subset of messages received to support other functional requirements. 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. In certain cases, a system may obtain (learn) certificate information from peer systems over the same interface.

5.1.3.4 SCMS

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. There may be multiple CRLs, each of which revokes a specific subset of BSM senders. Each certificate identifies which CRL it could potentially be revoked by.

Certificates and the CRL are stored within the OBU system and are updated by the SCMS. A well-behaved system 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 IEEE 1609.2. For the initial equipping of a system, it interfaces to a device configuration manager (DCM) to acquire the root certificate authority (CA) certificate (see 6.6).

5.1.3.5 Privacy

For users with a requirement for privacy, as defined in 4.1, the following mechanisms are put in place to protect privacy: the signing security certificate (known as a pseudonym certificate as noted in 4.1) is changed after a variable length of time (for example, every 5 minutes), and fields within the broadcast message (DE_MsgCount, DE_TemporaryID and the source layer-2 ID) are randomized whenever the certificate is changed. The SCMS is structured as a set of components, and for systems that are requesting pseudonym certificates, the component generating the certificates has no knowledge of which certificates are used by a particular device.

For systems acting as identified senders, a single signing certificate may be used (known as an identification certificate as noted in 4.1). In this case, the certificate has a validity period that ends slightly after the validity period for the next certificate begins. This period when both certificates are valid is referred to as the “overlap period.” The system may stop using the current certificate and start using the next certificate at any point during the overlap period. Once the system has started using the next certificate, it shall continue to use that certificate and shall not reuse the “current” certificate even if the “current” certificate is still valid. When an identification certificate changes, the system is not required to change the fields DE_MsgCount, DE_TemporaryID and the source layer-2 ID.

5.1.4 Start-Up and Shutdown

Refer to 5.1.4 of SAE J2945/1.

5.1.5 Mapping to the V2V Over-the-Air Data

Refer to 5.1.5 of SAE J2945/1. This document also includes data frames and elements that provide information to nearby vehicles about the presence of public safety vehicles. These extra data frames and elements are shown in Table 2.

Table 2 - Mapping data elements and frames for emergency vehicle notification

V2V Safety Message BSM Contents	Emergency Vehicle Notification
DF_SpecialVehicleExtensions DF_EmergencyDetails DE_SirenInUse DE_LightbarInUse DE_MultiVehicleResponse DF_SupplementalVehicleExtensions DF_VehicleClassification DE_BasicVehicleRole	Required for: Target Classification Threat Assessment

5.1.6 PC5 Radio Preconfiguration

The PC5 radio preconfiguration parameters are defined in Table 3.

5.2 System Interfaces

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

5.2.1 Vehicle-to-Vehicle Communications Interface

The system interfaces to other vehicles (systems) by transmitting and receiving BSMs in addition to other supporting V2X messages and their applications.

- The format and contents of the BSM are compliant with SAE J2735.
- The BSM is transmitted over the LTE-V2X interface as a wireless access in vehicular environments (WAVE) short message (WSM) using the WAVE short message protocol (WSMP) specified in IEEE 1609.3 without IEEE 802.3 ethertype. Note that several optional fields available in the WSMP header are not applicable to this document (see 6.1.3 for details).
- BSMs are transmitted in LTE band 47 using EARFCN 55140 with a 20-MHz channel width. This corresponds to 5905 to 5925 MHz.

NOTE: The 20-MHz bandwidth is divided into ten subchannels. Depending on the size of the BSM and the speed of the vehicle, the LTE-V2X radio uses different numbers of subchannels and different MCS values for different BSM transmissions, as described in Tables 14, 15, and 16.

- BSM security is compliant with IEEE 1609.2 as profiled by the security profile in this document.
- The over-the-air interface is compliant with ETSI Release 14 and optionally some features of Release 15.⁵
- The WSM provider service ID (PSID) is set to 0x20.

The applicable requirements from each of these standards are profiled in 6.1.

5.2.2 System to SCMS Communications Interface

The system interfaces to the SCMS to request security credential generation, download security credentials, and receive CRLs. It is recommended that systems use a standard interface such as IEEE 1609.2.

5.2.3 System to Positioning Subsystem Interface

Refer to 5.2.3 of SAE J2945/1.

⁵ Cyclic delay diversity as defined in Release 15 is optional in this specification.

6. MINIMUM REQUIREMENTS

6.1 Standards Profiles (STD)

6.1.1 ETSI

This section specifies the requirements from ETSI Release 14 to support V2V operation as specified in this document. In general, the scope of communications capabilities used by this document is limited to “non-operator managed” [ETSI TS 123 285] V2X Sidelink communications. A universal subscriber identity module (USIM) and radio access network (RAN) infrastructure are not required to implement the functionality specified in this document.

- The PC5 radio subsystem shall implement the user equipment (UE) as specified in the ETSI Release 14 set of technical specifications to the extent necessary to support V2X Sidelink communications (Mode 4) [ETSI TS 136 321, ETSI TS 136 201]. [6.1.1-V2V-STD-ETSI-001]
- For V2V safety communications, the PC5 radio subsystem shall use V2X Sidelink communications as specified in ETSI Release 14 [ETSI TS 136 321]. There is no infrastructure or serving cell. The radio subsystem is assumed to be pre-authorized for the region in which it operates, which in the case of SAE J3161/1 is the United States. [6.1.1-V2V-STD-ETSI-002]

NOTE: “There is no infrastructure or serving cell” means the system (Mode 4) does not require a cellular communications infrastructure. Autonomous resource selection using Mode 4 is implemented by selecting resource blocks for transmission based on energy sensing of resource blocks (RBs) already in use and priority associated with the information in those RBs [ETSI TS 136 213].

- For V2V safety communications, the PC5 radio subsystem shall use the UE procedure for determining subframes and resource blocks for transmitting PSSCH and reserving resources for Sidelink transmission Mode 4 [ETSI TS 136 213, ETSI TS 136 321]. [6.1.1-V2V-STD-ETSI-003]
- The 3-bit SDU-type field in the ETSI PDCP header shall be set to 011, indicating non-IP. The 16-bit PDCP-SN-size shall be used. PGK identity, PTK identity, and PDCP SN shall be set to 0. [6.1.1-V2V-STD-ETSI-004]
- The V2X message family encoding shall be set to the value of 00000001, indicating IEEE 1609. [6.1.1-V2V-STD-ETSI-005]
- The PC5 radio subsystem shall use RLC UM (unacknowledged mode) and the 5-bit RLC SN size. UM window size shall be set to 16. HARQ reordering is possible for STCH reception. [6.1.1-V2V-STD-ETSI-006]
- The 4-bit V field in the ETSI MAC header shall be set to 0011, indicating a 24-bit DST field [ETSI TS 136 321]. [6.1.1-V2V-STD-ETSI-007]
- The 24-bit destination layer-2 ID in the ETSI MAC header shall be set to 0xFFFFFFFF for BSMs [ETSI TS 136 321]. [6.1.1-V2V-STD-ETSI-008]
- The 24-bit source layer-2 ID in the 3GPP MAC header shall be set to a random value at start-up and periodically reset as described in 6.5.1. [6.1.1-V2V-STD-ETSI-009]
- The PC5 radio subsystem shall use the preconfiguration parameters as specified in Table 3. Parameters not included in Table 3 are not used on a PC5 interface that transmits BSMs according to this document [ETSI TS 136 213, 136 321]. [6.1.1-V2V-STD-ETSI-010]
- The maximum EIRP shall be +33 dBm, subject to regulatory constraints. [6.1.1-V2V-STD-ETSI-011]⁶

⁶ See 6.4.1 for additional information on power levels.

- Packets shall be transmitted using one of two methods: [6.1.1-V2V-STD-ETSI-012]
 - Semi-persistent scheduling (SPS) plus One-Shot method (as specified in SAE J3161).
 - Event-based transmission (commonly known as one-shot transmissions):
 - Event-based BSM transmissions are sent either with ProSe packet priority (PPPP) = 2 or 5. Event-based BSMs with the critical event flag set and BSMs generated by a public safety vehicle engaged in an emergency response are sent using PPPP = 2. SPS-based flows for other BSM transmissions are always sent with PPPP = 5.
 - Both types of flows shall adhere to PDB values as defined.
- Packet delay budget (PDB) is defined as the maximum delay that a packet can tolerate once it is received by the modem from an application stack and is generally based on the priority of the packet generated. PDB shall be set according to the following rules: [6.1.1-V2V-STD-ETSI-013]
 - For priority 5, PDB shall be set to 100 ms irrespective of SPS or event-based flows.
 - For priority 2, PDB shall be set to 50 ms irrespective of SPS or event-based flows.
- The configuration specified below details limits on the relevant parameters for transmission of a payload. If a packet is large and does not fit using the maximum allowable MCS and subchannel limits, then UE can choose an option between segmentation, event-based transmission, or dropping the packet as per rules described in ETSI TS 136 321, section 5.14. Additionally, if the choice is to segment the packet, then the segmentation procedure (as defined in ETSI TS 136 322) needs to be followed.

Preconfiguration parameters provide a wide variety of parameters that configure the behavior of the LTE-V2X radio. These parameters are split into multiple areas, and each set of parameters configure a specific area including, but not limited to, channel bandwidth, maximum transmit power, limits on modulation and coding schemes, priority handling, limits on subchannel sizes and number of subchannels, and channel busy ratio and channel access limits (CR-limit).

Table 3 can be effectively broken down into six sets of parameters:

- a. General parameter set
- b. Common RX and TX pool configuration set
- c. Channel busy ratio (CBR) configuration set
- d. Priority-based configuration set
- e. Speed-based configuration set
- f. RSRP-based exclusion parameter set

6.1.1.1 General Parameter Set

This set of parameters configures high level parameters.

- Maximum number of supported carrier frequencies for this particular configuration
- Frequency of operation
- Maximum transmit power
- Configured channel bandwidth

6.1.1.2 Common RX and TX Pool Configuration Set

This set of parameters configures general transmission and reception pool configurations.

- Maximum number of RX and TX pool configurations
- Subframe bitmap for configuration of subframes enabled for LTE-V2X communication
- Subchannel configuration: Size of each subchannel, number of subchannels, and start resource block of the subchannel
- Maximum transmit power for the configured transmit pool; this cannot exceed the maximum configured power in general parameter set 1
- Type of synchronization source

6.1.1.3 Channel Busy Ratio (CBR) Configuration Set

This set of parameters configures CBR levels and transmission parameters based on CBR levels.

- RSSI⁷ threshold above which a subchannel will be considered occupied for channel busy ratio calculation
- Maximum number of CBR configurations based on CBR levels
- For each CBR configuration, these parameters apply:
 - CR-limit: Maximum number of subchannels that can be used in 1 second for a given CBR
 - Minimum and maximum MCS that can be used
 - Minimum and maximum number of subchannels that can be used
 - Retransmission setting

6.1.1.4 Priority-Based Configuration Set

This set of parameters configures various priority configurations.

- Maximum number of priority configurations
- For each priority configuration, it further allows configuration of the below elements:
 - Default CBR configuration to be used when there is no CBR measurement available
 - A mapping from measured CBR range to a CBR configuration to be used when CBR measurement is available

⁷ If measured in a single subchannel, RSSI is the power in that subchannel; if measured across multiple subchannels, RSSI is the linear average of the power in those subchannels.

6.1.1.5 Speed-Based Configuration Set

This set of parameters configures transmission parameters based on speed threshold.

The final transmission parameters are chosen based on a combination of speed-based and congestion-based parameter sets.

- Configuration of a speed threshold
- Parameters within each set of speed configurations include:
 - Minimum and maximum MCS
 - Minimum and maximum number of subchannels
 - Retransmission configuration
- There are two sets of transmission parameters:
 - The first set of parameters needs to be used when speed is above the configured threshold
 - The second set of parameters needs to be used when speed is below the configured threshold
- Speed threshold of 120 km/h is used to select between the parameter sets

6.1.1.6 Resource Selection Procedure

There are two methods of channel access in LTE-V2X: (1) semi-persistent scheduling (SPS) and (2) event-based (one-shot) transmission.

- a. A transceiver can use a sensing-based SPS algorithm to reserve the channel and transmit periodic data. In this scheme, the transmitter senses the channel for 1 second (referred to as the “sensing window”) and selects a set of SPS subchannels for the first transmission after the resource reselection. In subsequent 100-ms intervals, it might transmit a BSM using the same selected subchannels (an “SPS transmission”), it might transmit a BSM using a different set of subchannels selected using the one-shot scheduler, or it might not transmit at all. When it performs resource reselection, it initiates a resource reselection counter (ResourceReselectionCtr) to a random number selected uniformly over the range SPSCtrMin to SPSCtrMax. When it makes an SPS transmission, it decrements ResourceReselectionCtr. When a BSM is ready to be transmitted with SPS, if ResourceReselectionCtr is 0, the transmitter either selects new SPS subchannels (with probability $1 - \text{probResourceKeep-r14}$) or reuses the existing set of SPS subchannels (with probability $\text{probResourceKeep-r14}$). A new ResourceReselectionCtr value is randomly chosen in both cases.
- b. Half-duplex and reselection of reserved resources in SPS flow may cause repetitive packet collision when the transmitter uses SPS flow for periodic packet transmission. To protect against these collisions, LTE-V2X uses one-shot transmissions along with SPS flows to avoid the repetitive packet collision.
- c. For this purpose, the transmitter uses another counter for one-shot transmission (OneShotCtr) along with ResourceReselectionCtr. OneShotCtr is chosen uniformly between OneShotCtrMin and OneShotCtrMax. After each packet transmission using SPS flow (or retransmission if HARQ is enabled), both ResourceReselectionCtr and OneShotCtr are decremented by 1.

When the OneShotCtr becomes 0 and ResourceReselectionCtr is not equal to 0, the transmitter skips the SPS flow and the transmission is made using the one-shot transmission. For this transmission, the PPPP of the one-shot resource grant transmission shall be the same as the PPPP of the SPS resource grant based transmission defined in 6.3.4. [6.1.1-V2V-STD-ETSI-014]

After the one-shot transmission, OneShotCtr will be set to a new random number. The ResourceReselectionCtr is not decremented if a one-shot transmission is made.