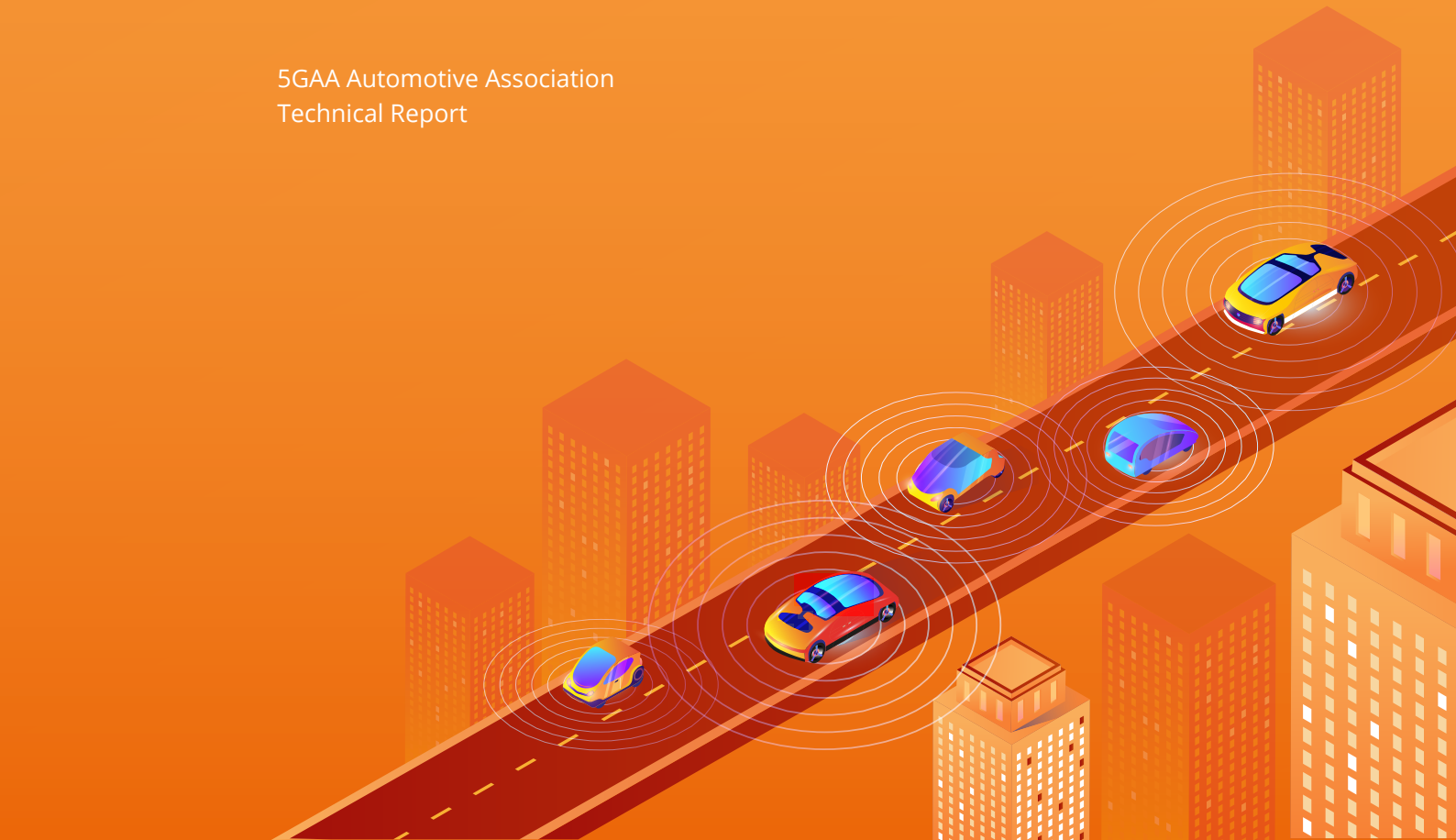
5GAA Automotive Association

Intersection Safety via Infrastructure Sensor-Sharing

5GAA Automotive Association
Technical Report



CONTACT INFORMATION:
Executive Manager – Thomas Linget
Email: liaison@5gaa.org

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

VERSION:	1.0
DATE OF PUBLICATION:	19 December 2024
DOCUMENT TYPE:	Technical Report
EXTERNAL PUBLICATION:	Yes
DATE OF APPROVAL BY 5GAA BOARD:	4 November 2024

Contents

Foreword

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

x-nnzzzz

(1) This numbering system has six logical elements:
- (a) x: a single letter corresponding to the working group:
  where x =
  T (Use cases and Technical Requirements)
  A (System Architecture and Solution Development)
  P (Evaluation, Testbed and Pilots)
  S (Standards and Spectrum)
  B (Business Models and Go-To-Market Strategies)
- (b) nn: two digits to indicate the year. i.e. ,17,18 19, etc
- (c) zzzz: unique number of the document

(2) (2) No provision is made for the use of revision numbers. Documents which are a revision of a previous version should indicate the document number of that previous version

(3) (3) The file name of documents shall be the document number. For example, document S-160357 will be contained in file S-160357.doc

Executive summary

According to various reports and statistics, a major portion of traffic fatalities and injuries occurs at intersections. Intersection safety service via infrastructure sensor-sharing, called the InterSafe Service in this document, is an emerging approach to make intersections safer for road users. There have been various concepts, demos, and product developments related to the sharing of infrastructure sensor data with vehicles at or near intersections, and there are many different Vehicle-to-Everything (V2X) protocol/message standards that could be used for sharing information about infrastructure-sensed objects.

An important step towards mitigating the large percentage of intersection-related fatalities and injuries is to identify the possible implementation options and define respective system-level profile standards to enable development of interoperable implementations for the sharing of infrastructure sensor data with vehicles at or near intersections. Some benefits and the rationale behind this include the need to:

- Increase the safety benefits to road users, especially during early stages of V2X adoption when only a small fraction of road users might be equipped,
- Address a wide range of intersection safety use cases,
- Increase protection for Vulnerable Road Users (VRUs) – such as pedestrians and cyclists – without requiring them to be equipped.

In this document, the applicable use cases, related system requirements, functional flow, reference protocol stack and architecture are first identified. A detailed analysis for several system-level requirements derived from various example use cases is included in an annex. Different deployment options (including the use of direct

communication and/or network-based communication) for infrastructure sensor-sharing are investigated. When using direct communication, simulation test results (included in an annex) show that the InterSafe Service can be neatly operated in the common channel where a plurality of messages for multiple safety services such as BSMs, SPATs, MAPs and RTCMs (see clause 3.2 for explanations of these abbreviations and others introduced in this executive summary) operate without causing a significant impact on them.

There are regionally specific ITS standards on the messages and protocols in organizations such as SAE International, ETSI, and CSAE suitable to the InterSafe Service. This document provides the recommendations that can be used to guide the development of subsequent system-level profiles by standards organizations. Consequently, it will expedite the implementation and deployment of the InterSafe Service which can considerably reduce the traffic fatalities.

Introduction

According to the United States Department of Transportation (USDOT) Federal Highway Administration (FHWA), each year roughly a quarter of traffic fatalities and about half of all traffic injuries in the United States occur at intersections [1]. There have been various concepts, demos, and product developments related to the sharing of infrastructure sensor data with vehicles at or near intersections. There are many different V2X protocol/message standards – including some soon-to-be completed/published standards by Standards Development Organizations (SDOs) including the Society of Automotive Engineers (SAE) International, European Telecommunications Standards Institute (ETSI), and China Society of Automotive Engineers (CSAE) – that could be used for sharing information about infrastructure-sensed objects. Ideally, multiple vendors and stakeholders will develop solutions using common standardized message(s). Different but complementary deployment options of infrastructure sensor data-sharing exist, and they may use different communication technologies, e.g., Cellular-V2X (C-V2X) direct or network-based communications. For C-V2X direct communication, it is also important to understand the data traffic characteristics and delivery requirements of such messages as well as the potential impact of including such messages in the same Intelligent Transportation System (ITS) spectrum in which other safety services are already operating. Thus, successfully reducing the large percentage of intersection-related fatalities and injuries, without negatively impacting other safety services, requires various stakeholders to develop interoperable implementations based on more fully defined system-level infrastructure sensor-sharing profile standards intended to address a specific set of identified key intersection safety use cases.

As outlined above, the main problem to be addressed is the large percentage of intersection-related fatalities and injuries. An important step towards mitigating the problem is to identify the possible implementation options and define respective system-level profile standards enabling the development of interoperable implementations for sharing infrastructure sensor data with vehicles at or near intersections. A key benefit is the potential to increase safety especially during early stages of V2X adoption when only a small fraction of road users might be equipped. The approach also addresses a wide range of intersection safety use cases, and has the ability to increase protection for VRUs, such as pedestrians and cyclists, without them having to be equipped (capable of transmitting or receiving V2X messages).

1. Scope

This document describes the concept of operation, various deployment options, and profile details on the messages and protocols for the infrastructure sensor-sharing for intersection safety. This Technical Report (TR) can be used to guide those involved in the development of corresponding system-level profile standards in organizations such as SAE International, ETSI, and CSAE. Note that there are regionally specific ITS application layer standards that are expected to be used as a basis for such profiles, i.e., SAE J3224 that defines the Sensor Data Sharing Message (SDSM), ETSI TS 103 324 that defines the Collective Perception Message (CPM), and T/CSAE 315.2 that defines the Sensor Sharing Message (SSM).

2. References

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1]	FHWA, "About Intersection Safety", available at: https://highways.dot.gov/safety/intersection-safety/about
[2]	SECUR, "Deliverable 1.1 Accident Data Study – Accident scenarios description", 2022
[3]	SECUR, "Deliverable 1.2 Accident parameters description for the chosen scenarios", 2022
[4]	NHTSA DOT HS 811 366, "Crash Factors in Intersection-Related Crashes: An On-Scene Perspective", 2010
[5]	NHTSA DOT HS 810 767, "Pre-Crash Scenario Typology for Crash Avoidance Research", 2007
[6]	5GAA T-200111, "C-V2X Use Cases and Service Level Requirements Volume I", 2020
[7]	5GAA T-200116, "C-V2X Use Cases and Service Level Requirements Volume II", 2021
[8]	5GAA A-200094, Technical Report, V2X Application Layer Reference Architecture, June 2020
[9]	ETSI EN 302 665 (V1.1.1), "Intelligent Transport Systems (ITS); Communications Architecture", 2010
[10]	SAE J3161, "LTE Vehicle-to-Everything (LTE-V2X) Deployment Profiles and Radio Parameters for Single Radio Channel Multi-Service Coexistence", 2022
[11]	ETSI TS 103 324 (V2.1.1), "Intelligent Transport System (ITS); Vehicular Communications; Basic Set of Applications; Collective Perception Service; Release 2", 2023
[12]	SAE J3224, "V2X Sensor-Sharing for Cooperative and Automated Driving", 2022
[13]	T/CSAE 53-2020, "Cooperative intelligent transportation system – Vehicular communication application layer specification and data exchange standard (Phase I)", 2020
[14]	T/CSAE 157-2020, "Cooperative intelligent transportation system – Vehicular communication application layer specification and data exchange standard (Phase II)", 2020

[15] IEEE Std 1609.2, "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) – Security Services for Applications and Management Messages", 2022

[16] IEEE Std 1609.3, "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) – Networking", 2020

[17] ETSI TS 103 836-4-1 (V2.1.1), "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality; Release 2", 2022

[18] ETSI TS 103 836-4-3 (V2.1.1), 'Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 3: Media-dependent functionalities for NR-V2X PC5 and LTE-V2X PC5; Release 2", 2023

[19] ETSI TS 103 836-5-1 (V2.0.0), "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol; Release 2", 2022

[20] EN 303 798 (V2.1.1), "Intelligent Transport Systems (ITS); LTE-V2X and NR-V2X Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band; Release 2", 2024

[21] ETSI TS 102 965 (V2.1.1), "Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration; Release 2", 2021

[22] SAE J2735, "V2X Communications Message Set Dictionary", 2024

[23] CTI 4501 (V01.01), "Connected Intersections Implementation Guide: Guidance to Setting Up and Operating a Connected Intersection (CI)", June 2022

[24] FHWA, "Mitigation Strategies for Design Exceptions", available at https://safety.fhwa.dot.gov/geometric/pubs/mitigationstrategies/

[25] FHWA, "Walkways, Sidewalks, and Public Spaces", available at: https://safety.fhwa.dot.gov/ped_bike/univcourse/pdf/swless13.pdf

[26] Čulík, Kristián, et al. "Evaluation of Driver's Reaction Time Measured in Driving Simulator", Sensors, vol. 22, no. 9, May 2022, available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9099898/

[27] FHWA, "Signalized Intersections Informational Guide", available at: https://safety.fhwa.dot.gov/intersection/signal/fhwasa13027.pdf

[28] T/CSAE 315.2, "Cooperative intelligent transportation system-Technical requirements for application layer interaction-Part 2: Sensor Data Sharing" (in progress)

[29] YD/T 3707-2020, "Technical requirements of network layer of LTE-based vehicular communication", 2020

[30] YD/T 3957-2021, "LTE-based vehicular communication – Technical requirement of security certificate management system", 2021

[31] YD/T 3340-2018, "Technical requirements of air interface of LTE-based vehicular communication", 2018

[32] 5GAA Technical Report, "Vehicle-to-Network-to-Everything (V2N2X) Communications; Architecture, Solution Blueprint, and Use Case Implementation Examples", April 2024. https://5gaa.org/vehicle-to-networkto-everything-v2n2x-communications-architecture-solution-blueprint-usecases

[33] SAE J2945/9, "Vulnerable Road User Safety Message Minimum Performance Requirements", 2017

3. Definitions and abbreviations

3.1 Definitions

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

5G-V2X: V2X technology of the combination of LTE-V2X and 5G NR-V2X, composed of a network-based (Uu) and direct (PC5) communication mode operated with or without LTE-V2X.

C-V2X (Cellular-V2X): An umbrella term which encapsulates all 3GPP V2X technologies.

Equipped Road User: A road user, i.e., vehicle or VRU, that can transmit or receive any V2X messages relevant to the services described in this TR.

Equipped Vehicle: An Equipped Road User where the road user is a vehicle.

Equipped VRU: An Equipped Road User where the road user is a VRU.

InterSafe Message: A standardized ITS message for InterSafe Service.

InterSafe Receiver System: A functional entity in the InterSafe reference functional architecture that receives the InterSafe Messages from the InterSafe Sender System. The Equipped Road User performs this role.

InterSafe Sender System: A functional entity in the InterSafe reference functional architecture that transmits the InterSafe Messages to the InterSafe Receiver System. The Infrastructure System performs this role.

InterSafe Service: Intersection safety service via infrastructure sensor-sharing.

Infrastructure System: A set of infrastructure components that detects and identifies road users in the environment of the intersection via sensors and associated perception functions, and generates and disseminates sensor-sharing messages conveying the information about the detected road users.

> NOTE1: Infrastructure System may be instantiated by different physical components such as sensor devices, Roadside Units (RSUs), edge computing platforms, network infrastructure components, cloud computing platforms.
>
> NOTE2: This document uses “sensor-sharing message” (lower case) to refer to any of the messages defined by SAE (SDSM), ETSI (CPM) or T/CSAE 315.2 (SSM).

Unequipped Road User: A road user, i.e., vehicle or VRU, that cannot transmit or receive any V2X messages relevant to the services described in this TR.

Unequipped Vehicle: An Unequipped Road User where the road user is a vehicle.

Unequipped VRU: An Unequipped Road User where the road user is a VRU.

Vulnerable Road User: A road user who is not occupying a vehicle such as a passenger car, motorcycle, public transit vehicle, or train. Pedestrians, cyclists, children, elderly, disabled people, and road workers are particularly vulnerable to serious injury or death when involved in a motor vehicle-related collision.

3.2 Abbreviations

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

5G-V2X	5G Vehicle-to-Everything
ACK	Acknowledgement
AID	Application Identifier
AMQP	Advanced Message Queueing Protocol
BSM	Basic Safety Message
CAM	Cooperative Awareness Message
CPM	Collective Perception Message
CSAE	China Society of Automotive Engineers
C-V2X	Cellular Vehicle-to-Everything
DENM	Decentralized Environmental Notification Message
DTLS	Datagram Transmission Control Protocol
E2E	End-to-End
ETSI	European Telecommunications Standards Institute
FHWA	Federal Highway Administration
HARQ	Hybrid Automatic Repeat Request
HV	Host Vehicle
InterSafe	Intersection Safety via Infrastructure Sensor-Sharing
IP	Internet Protocol
IPG	Inter-Packet Gap
IPv6	Internet Protocol version 6
ITS	Intelligent Transportation System
ITS-AID	ITS Application Identifier
LOS	Line of Sight
LTE-V2X	Long Term Evolution-based Vehicle-to-Everything
MAP	Map Data (Message)
MAPEM	MAP (topology) Extended Message
MEC	Mobile Edge Computing (or Multi-access Edge Computing)
MNO	Mobile Network Operator
MQTT	Message Queueing Telemetry Transport
NACK	Negative Acknowledgement
NHTSA	National Highway Traffic Safety Administration
NLOS	Non-Line of Sight
NR-V2X	New Radio (5th generation) Vehicle-to-Everything
OEM	Original Equipment Manufacturer
OTA	Over-the-Air
PC5	Proximity-based Communication (Interface) 5
PPPP	ProSe Per Packet Priority
ProSe	Proximity-based Services
PRR	Packet Reception Ratio
PSID	Provider Service Identifier
PTW	Powered Two-Wheeler
QoS	Quality of Service

RSM	Roadside Safety Message (from T/CSAE 53-2020 [13]) NOTE: This is a distinct message from the Road Safety Message defined in SAE J2735 [22].
RSU	Roadside Unit
RTCM	Radio Technical Commission for Maritime Services
SAE	Society of Automotive Engineers
SAEM	Services Announcement Essential Message
SAM	Service Announcement Message
SECUR	Safety Enhancement through Connected Users on the Road
SDO	Standards Development Organization
SDSM	Sensor Data Sharing Message
SP	Service Provider
SPAT	Signal Phase And Timing Message
SPATEM	Signal Phase And Timing Extended Message
SPDU	Security Services Protocol Data Unit
SSM	Sensor Sharing Message (from T/CSAE 157-2020 [14] and T/CSAE 315.2 [28])
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TR	Technical Report
TTC	Time to Collision
UDP	User Datagram Protocol
UPER	Unaligned Packed Encoding Rules
USDOT	United States Department of Transportation
VRU	Vulnerable Road User
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
WAVE	Wireless Access in Vehicular Environments
WSA	WAVE Service Advertisement
WSMP	WAVE Short Message Protocol

4. Concept of operation and system description

4.1 Use cases and system-level requirements

4.1.1 Overview

As reported by the USDOT FHWA on the "About Intersection Safety" website [1], each year roughly a quarter of traffic fatalities and about half of all traffic injuries in the United States are attributed to intersections. Similar statistics are found in the "Safety Enhancement through Connected Users on the Road" (SECUR) Deliverable 1.1 [2] for Europe. Infrastructure sensor-sharing via V2X technologies illustrated in Figure 1 is an emerging approach to enhance the intersection safety, which is complementary to other approaches such as education, enforcement, intersection geometry design, and post-crash care.

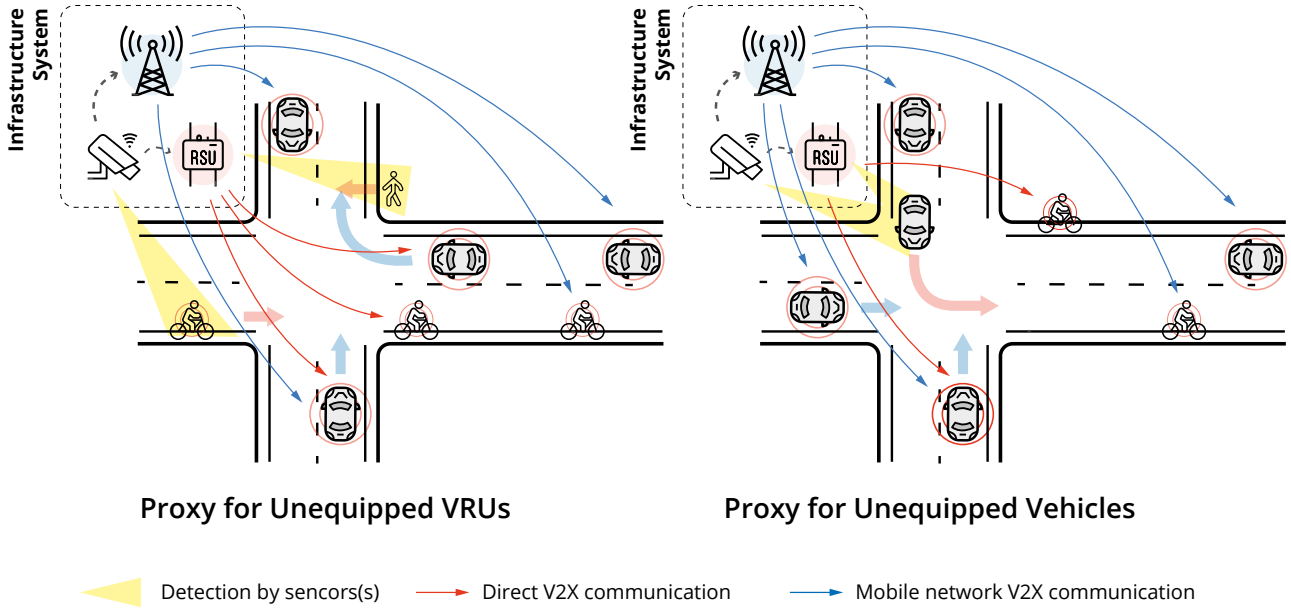


Figure 1: Illustration of sharing infrastructure-sensed objects

Figure 1 thus depicts how Infrastructure Systems work as a proxy for Unequipped VRUs (left in the diagram) and/or Unequipped Vehicles (right) by sharing information about the Unequipped Road Users detected by the Infrastructure System's sensors. The infrastructure sensor-sharing can effectively increase the awareness of road users at intersections given that not all road users are V2X-capable.

4.1.2 Crash scenarios at intersections

Three critical pre-crash events at intersections are shown in the order of frequency in the National Highway Traffic Safety Administration (NHTSA) "Crash Factors in Intersection-Related Crashes" [4] as follows:

- Vehicle turning left at intersection,
- Vehicle crossing in a straight through movement at intersection,
- Vehicle turning right at intersection.

Fifteen accident scenarios are selected and investigated in the SECUR Deliverable 1.2 [3]. The following accident scenarios among them are highly relevant to intersections:

- Vehicle straight crossing path conflicting with bicycles, passenger cars and pedestrians,
- Vehicle left turn across path conflicting with passenger cars and Powered Two-Wheelers (PTWs).

The SECUR Deliverable 1.2 [3] chooses and evaluates the relevant parameters to analyze in depth the causes of the accident in each scenario. The analysis on the parameters for the accident scenarios highly relevant to intersections are summarized as follows:

- Vehicle straight crossing path conflicting with bicycles and passenger cars: A failure to observe the traffic signs regulating the priority is the most frequent main accident causation.
- Vehicle straight crossing path conflicting with pedestrians: Accidents in this scenario happened not so often at intersections. Improper behavior of the pedestrians is the most frequent main accident causation.
- Vehicle left turn across path with opponents of passenger cars and PTWs: A mistake made by the driver when turning to the left and failures to observe the traffic signs regulating the priority are the most frequent main accident causations.

NOTE: This document primarily uses the terms "crash" and "collision" (as opposed to "accident") because they are generally preferred by traffic safety professionals. However, the term "accident" is used here when referencing the SECUR deliverable to be consistent with the terminology used by that program.

The pre-crash scenario typology of 37 scenarios is derived by the NHTSA "Pre-Crash Scenario Typology for Crash Avoidance Research" [5]. They are meaningfully aligned with the accident scenarios and the analyses of SECUR Deliverable 1.2 [3].

4.1.3 Use cases applicable for infrastructure sensor-sharing

A variety of V2X use cases have been found and developed in various organizations. 5GAA developed two volumes of Technical Reports on Cellular Vehicle-to-Everything (C-V2X) Use Cases and Service Level Requirements [6] and [7]. From the TRs, the use cases closely overlapping crash scenarios in clause 4.1.2 and possibly applicable for infrastructure sensor-sharing are listed as follows:

- Cross-Traffic Left-Turn Assist,
- Intersection Movement Assist,
- Vulnerable Road User/Interactive VRU Crossing,
- Automated Intersection Crossing.

CSAE developed standards T/CSAE 53-2020 [13] and T/CSAE 157-2020 [14], in which the relevant use cases to the infrastructure sensor-sharing are:

- Left Turn Assist (LTA),
- Red-Light Violation Warning (RLVW),
- Vulnerable Road User Collision Warning (VRUCW),
- Cooperative Intersection Passing (CIP).

See details on the use cases in [6], [7], [13] and [14].

4.1.4 System-level requirements from the use cases

As shown in Figure 1 in clause 4.1.1, an Infrastructure System can work as proxy for Unequipped Vehicles and Unequipped VRUs by sharing information about the Unequipped Road Users that the Infrastructure System's sensors detect. The related crash scenarios and applicable use cases are described in clauses 4.1.2 and 4.1.3 .

To support the applicable use cases, the Infrastructure System may need to fulfil some system-level requirements such as a minimum sensor range, minimum position accuracy, etc. The system-level requirements for an Infrastructure System can be driven by the targeted use cases, and specific environmental conditions and assumptions including unique geometries, surface conditions (e.g., wet, dry), as well as reaction times.

Annex C provides a detailed analysis for system-level requirements derived from various example use cases involving unequipped vehicles and VRUs. The primary goal is to guarantee an Infrastructure System can function reliably as a proxy for Unequipped Road Users, sharing critical information to prevent potential collisions. These system-level requirements are often beyond the scope of ITS standards but are critical to ensure real-world effectiveness. Examples in Annex C show how these requirements can be calculated in different scenarios.

In particular, the analysis in Annex C.1 examines scenarios such as left-turn assist and intersection movement assist, using a 90-degree intersection as a model. Two approaches for determining minimum sensor range are discussed. The first approach ensures that equipped vehicles have enough time to fully stop before reaching a potential collision point, requiring a sensor range of approximately 216.8 meters

under worst-case conditions. The second approach focuses on initiating a reaction in time, which requires a shorter sensor range of about 96.8 meters. In scenarios such as jaywalking and crossing behind obstructions as shown in Annex C.2, the required sensor range may vary between 40.1 and 51.1 meters.

In the scenarios in Annex C, the required position accuracy of an Infrastructure System for detection remains at lane-level precision (1.8 meters), which is critical for navigating complex intersections.

By summarizing these examples, it becomes clear that the system-level requirements must be adaptable to varying road conditions, vehicle speeds, and user types. Annex C further supports these findings with practical examples and figures, guiding the deployment of infrastructure systems in real-world conditions.

4.2 Functional flow and requirements

A conceptual illustration of the functional entities and flow of information is shown in Figure 2. At the highest level, the illustration depicts an example Infrastructure System in the grey box on the left and an example Equipped Road User in the grey box on the right that are interconnected by Message Delivery Interface(s). The Message Delivery Interface(s) may include direct, mobile network, or both communication options. In some implementation options, the Message Delivery Interface(s) in Figure 2 may consist of multiple concatenated communication links using different communication technologies, as further shown in Figure 6. However, the supported use cases or services may vary depending on the option used.

The Infrastructure System in Figure 2 includes examples of functional blocks, but it should be noted that actual implementations may vary widely, e.g., omitting blocks, combining blocks, including additional blocks, interconnecting blocks differently, etc. The functional blocks in an Infrastructure System may also reside in different physical components such as sensor devices, Roadside Units (RSUs), edge computing platforms, network infrastructure components, cloud computing platforms, etc. The intent of the illustration is to provide a basis for understanding and discussion within this TR, rather than to constrain implementation options. That said, conceptually the Infrastructure System includes sensors and associated perception functions that detect and identify road users, e.g., pedestrians, cyclists, vehicles, in the environment of the intersection. In some implementations, information from multiple sensors may be combined via a fusion function. The Infrastructure System may also make use of information from received messages.

Irrespective of variations in implementation details regarding detection, identification, and analysis of road users, a common aspect of the Infrastructure Systems considered in this TR is that information about some key detected road users will be subsequently included in messages (e.g., CPM, SDSM and SSM) sent by the Infrastructure System via the Message Delivery Interface(s). These common aspects are represented by the output message generation and message dissemination functional blocks, shown via the blue box in the illustration.

NOTE: Depending on the deployment option and region, there can be various additional control signals not shown in the simple data flow depicted in Figure 2. For example, the pull-type interactions are considered for SSM defined in China by CSAE; i.e., service announcements can be initiated by the roadside infrastructure and the Equipped Road User requests the Sensor Data Sharing service to receive SSMs.

Suitably Equipped Road Users near the intersection may receive the messages sent by the Infrastructure System, process those messages, make risk assessments, and determine whether warnings should be generated, as shown by the functional blocks in the example. These receiver-side functions are assumed to be implementation specific.

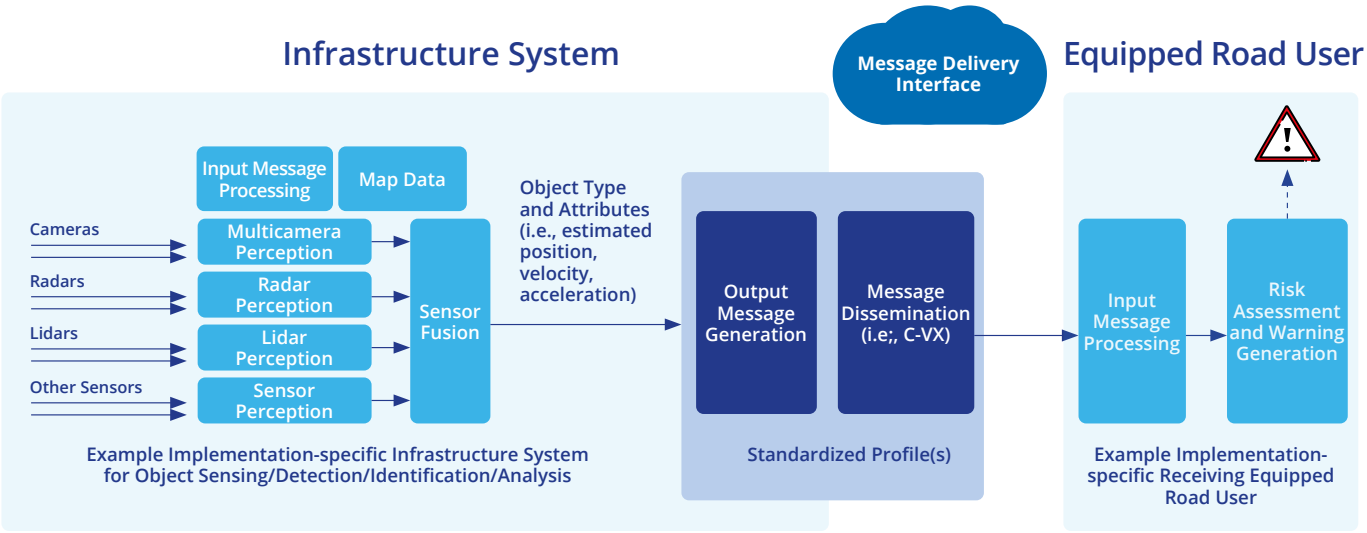


Figure 2: Functional sensor data flow of sharing infrastructure-sensed objects

Figure 2 also serves to highlight where defining a standardized profile is essential for enabling road users receiving information sent by the Infrastructure System to have a clear understanding of the information conveyed in order to make safety critical warning decisions. It should be noted that different regional profiles, e.g., China, Europe, United States, are likely to be needed due to the use of different ITS protocol stacks. The standardization of profiles not only provides clarity about the conveyed information but can also offer a high level of interoperability and performance. Depending on the deployment options, as described in clause 4.4, a profile defines the minimal set of configurations and requirements at one or multiple communication protocol layers to fulfil the End-to-End (E2E) interoperability and performance of InterSafe Service. Further details of the needed profiles are described in clauses 5 and 6.

A conceptual illustration of the detailed timeline according to the functional flow of Figure 2 is shown in Figure 3. It should be noted that actual implementations may vary, e.g., combining steps of Snapshot and Detection.

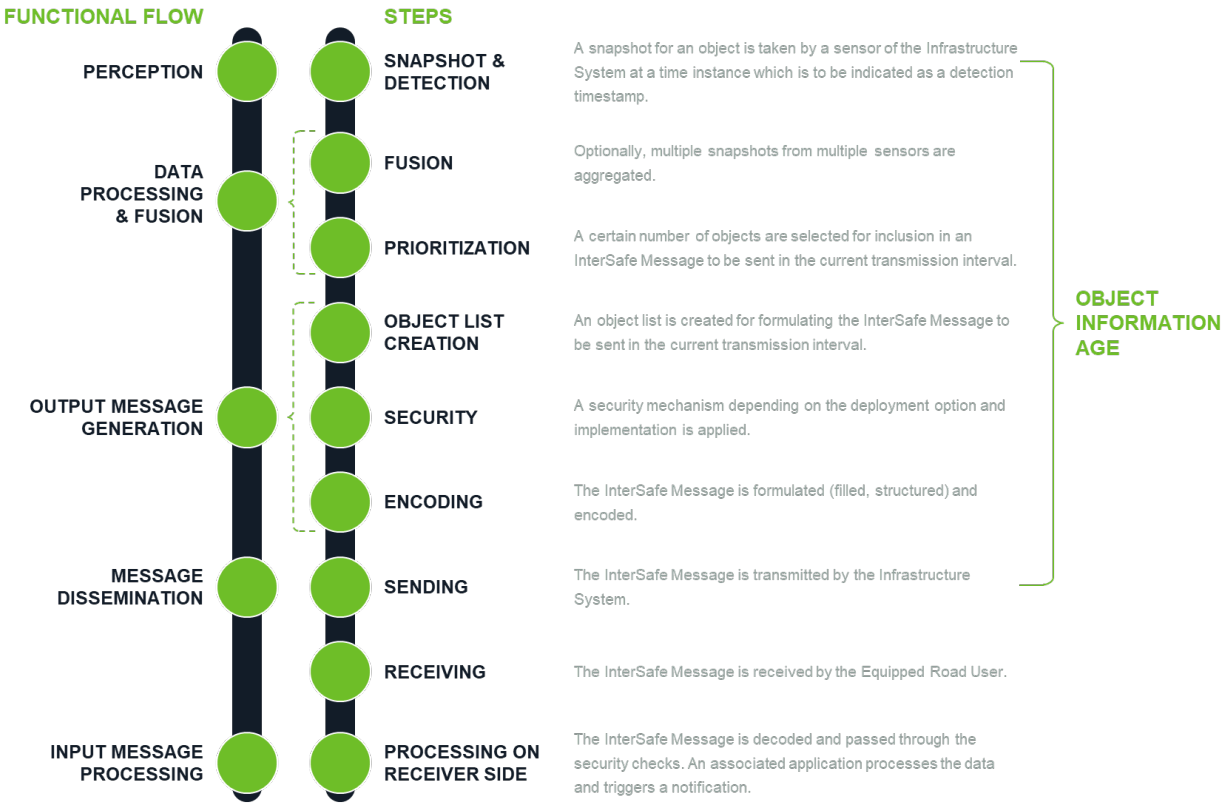


Figure 3: Timeline of the functional flow

4.3 Reference protocol stack and architecture

An illustration of the reference functional architecture and the reference protocol stack for the InterSafe Sender System and InterSafe Receiver System is shown in Figure 4. The reference protocol stack is aligned with ETSI EN 302 665 [9] and SAE J3161 [10].

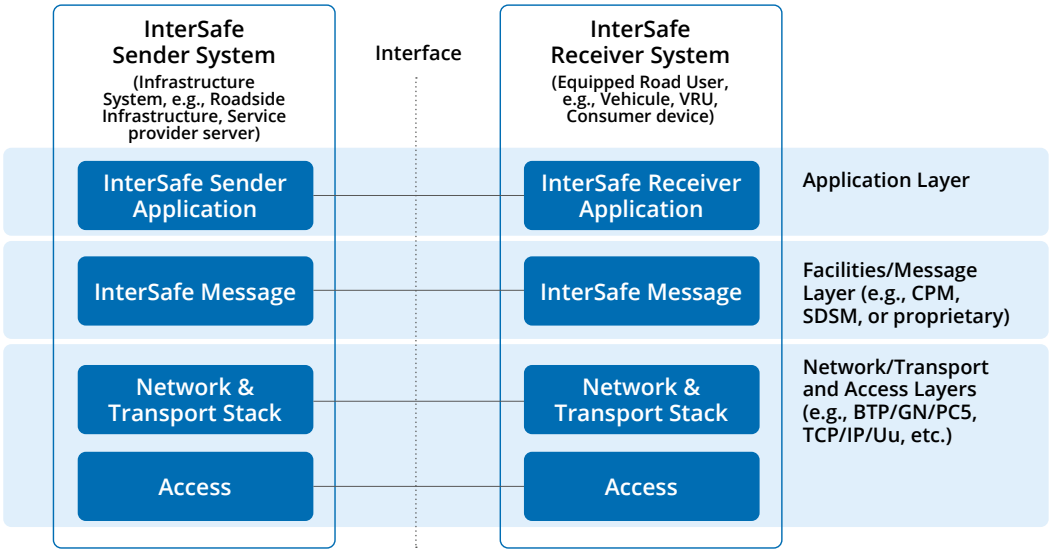


Figure 4: InterSafe Service reference functional architecture and reference protocol stack

The InterSafe Sender and Receiver Applications are the functional entities that exchange the InterSafe Messages with each other while fulfilling InterSafe Service specific requirements. The InterSafe Application may interact with, control, or be controlled by other entities in the systems, and can be implemented in various ways, e.g., an integrated software implementation, separated but interacting software implementation, etc.

Several different messages applicable to infrastructure sensor-sharing are being adopted in different regions according to their different needs. For example, the CPM is defined in ETSI TS 103 324 [11] for Europe, the SDSM is defined in SAE J3224 [12] for US, and the Roadside Safety Message (RSM) and Sensor Sharing Message (SSM) in T/CSAE 53-2020 [13] and T/CSAE 157-2020 [14] respectively for China. Also, there are different ITS protocol stacks for the network, transport and access layers in various regions. The regional differences in the messages and underlying protocol stacks, and the InterSafe Service specific profiles are provided in clauses 5 and 6.

4.4 Deployment options

There are different deployment options for infrastructure sensor-sharing, depending on the employed communication technologies, involved ecosystem stakeholders, and service operation models, etc. In this clause, two deployment options using C-V2X direct communication and network-based communication are described.

The common goal of the use cases is to improve environment perception and traffic safety by sharing trustworthy infrastructure sensor data with road users. Different deployment options can complement each other. To enable the application and message interoperability among different implementation options, implementation requirements for application triggers, message information elements, data quality, etc. need to be specified independent of which communication technology is being considered.

4.4.1 Deployment option using direct communication

In this InterSafe Service deployment option, the Infrastructure System (InterSafe Sender System) disseminates the InterSafe Messages to the Equipped Road Users (InterSafe Receiver Systems) using dedicated ITS network/transport protocols and C-V2X direct communication. In this deployment option, infrastructure components may be primarily instantiated by RSUs (or other components with similar capabilities may be applicable, mentioned in clause 4.2). The reference functional architecture and reference protocol stack are illustrated in Figure 4 (clause 4.3), and the regionally standardized specifics on the protocol stacks, including the access layer and their configuration parameters, are provided in clause 6.1. They are depicted in Figure 5 focused on the direct communication.

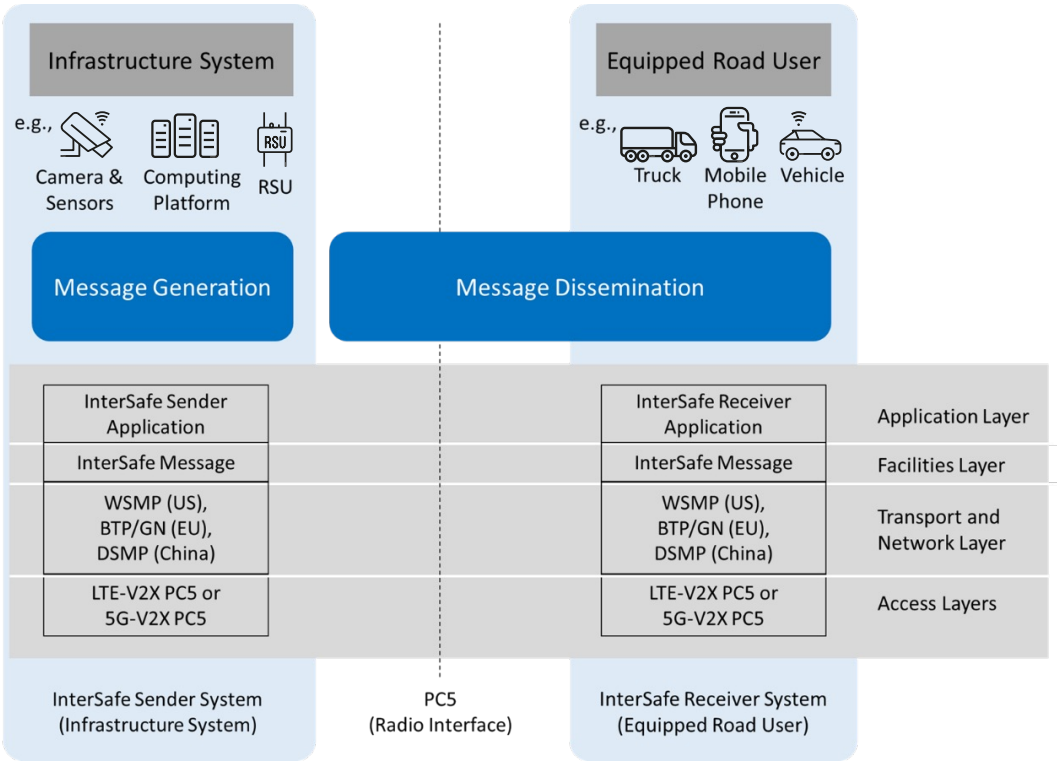


Figure 5: InterSafe Service deployment option using direct communication and E2E protocol stack

Service discovery:

For direct communication, the standardized service identifier (e.g., PSID in US, ITS-AID in Europe and AID in China) is included in the header of V2X messages and used to identify the services being provided. Once messages sent for those services are received, the identifier is used to route messages to the appropriate user applications that wish to receive those messages. The service identifier is also used by the security services as described below. The service identifiers for InterSafe Service are identified in clause 6.1.

Furthermore, the available services can be advertised by the dedicated standardized messages, e.g., WAVE Service Advertisement (WSA) in US, Services Announcement Essential Message (SAEM) in Europe, and Service Announcement Message (SAM) in China. The service advertisement/announcement messages may include a list of identifiers for services that are available via local access points and/or on the network, as well as information needed to receive and process the service advertisement/announcement messages pertaining to each service being advertised.

Security and privacy:

To support trust in V2X message exchange, messages are signed and verified using IEEE 1609.2 digital certificates based on public key cryptography. The transmitter computes a signature using a digital signature algorithm with a private key, and the receiver verifies the signature using the associated certificate. Each V2X message is transmitted as a datagram that includes the digital signature and either a security certificate containing the public key or an identifier for that certificate (obtained from its hash). The certificate includes the sender's application permissions, expressed as one or more PSIDs (indicating which applications the sender is allowed to send for) and, if necessary, Service Specific Permissions for each application PSID indicating specific permissions within the overall set of activities for that application. A signed message is only considered valid if the signature is cryptographically valid, the certificate is current and has not been revoked, and the permissions in the certificate permit the sending of that specific application message.

For users with privacy requirements, the signing security certificate (known as a pseudonym certificate) is changed after a variable length of time (for example, every 5 minutes), and relevant fields within the broadcast message are randomized whenever the certificate is changed.

The security and privacy in the direct communication are managed by the standardized protocols and profiles as described in clause 6.1.

Service interoperability in multi-vendor environments:

The fully standardized set of dedicated ITS protocols and profiles per region, and the simplicity of the communication architecture easily guarantee the interoperability between the Infrastructure System (InterSafe Sender System) and the Equipped Road Users (InterSafe Receiver Systems) regardless of which vendors or ecosystem stakeholders are involved.

4.4.2 Deployment option using network-based communication

In this InterSafe Service deployment option, the Equipped Road User (InterSafe Receiver System) connects to the Infrastructure System (InterSafe Sender System) using IP-based networks to receive sensor data, e.g., the identified objects. More specifically, the Equipped Road User uses a cellular network connection provided by the Mobile Network Operator (MNO) and an E2E IP unicast connection to the server on the Infrastructure System side. Figure 6 shows an example E2E architecture and the protocol stack of this deployment option using cellular network communication. In this scenario, the sensor data is communicated between the Infrastructure System and the Equipped Road User without going through the backend systems of a car Original Equipment Manufacturer (OEM) or a Service Provider (SP). This option is shown in Annex D as the V1/V1' interface option and requires a harmonized implementation profile for the V1 or V1' interface to enable interoperable InterSafe Service among Infrastructure Systems and Equipped Road Users, especially when the Equipped Road Users may need to communicate with different Infrastructure Systems managed by different infrastructure operators and owners. The IP Data Network shown in Figure 6 is the interconnection between the provider of the Infrastructure System and the MNO; this connection may be optimised to ensure performance, e.g. by MEC deployments.

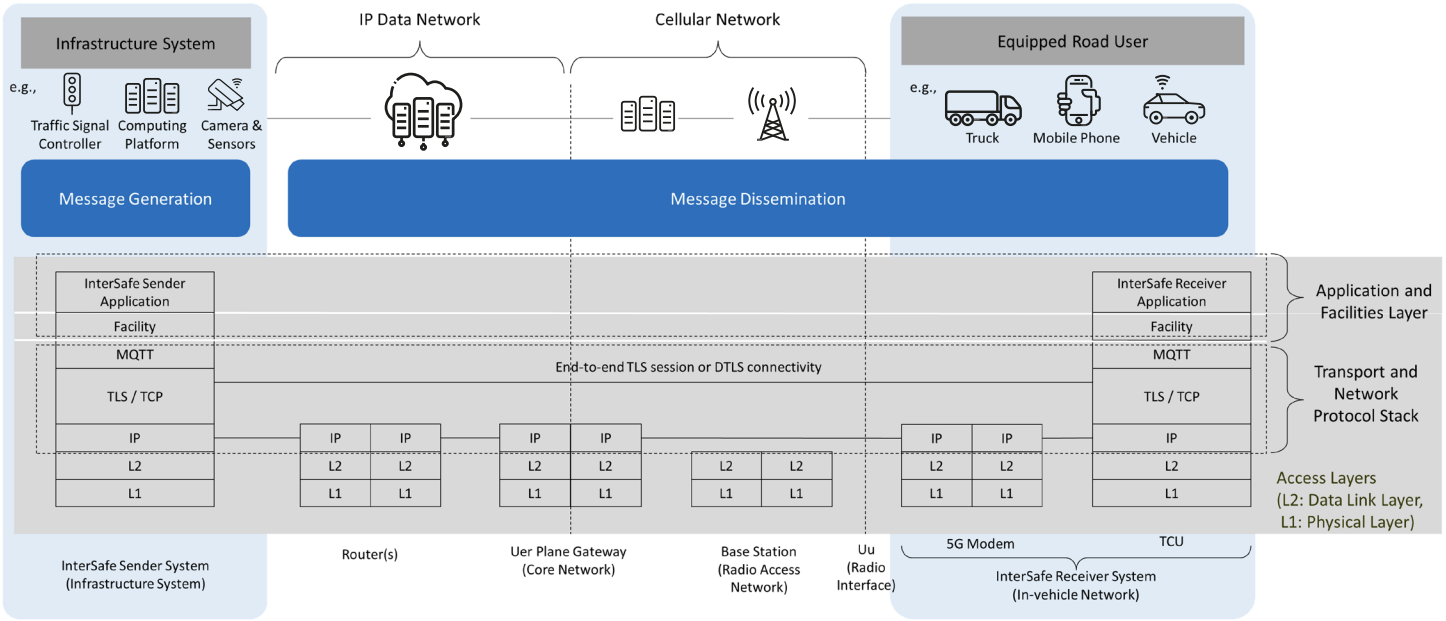


Figure 6: Example InterSafe Service deployment option using network-based communication and the E2E protocol stack

In this deployment option the connection between the Equipped Road User (InterSafe Receiver System) and the Infrastructure System (InterSafe Sender System) is using IP at the network layer and a protocol to secure the communication. This provides a protected, seamless E2E unicast connection through data networks and cellular networks, and hides underlaying access technologies, as shown in Figure 6. The facilities layer message profile ensures the InterSafe Service's interoperability at the

application (service) level, as indicated by the upper dotted boxes and specified in clause 5. The communication protocol stacks on top of the IP need to be agreed between the actors implementing InterSafe Service using the V1/V1' interface option. Message queueing protocols, such as Message Queueing Telemetry Transport (MQTT)[1] in combination with TLS/TCP, are a natural choice for this kind of information transfer and thus proposed in this profile work. The use of standardized and widely applied protocols on the IP layer and the above facilitates layer provides an interoperable E2E solution and easy-to-use interface for the application developers. Clause 6.2 provides examples of the transport protocol stacks for the deployment option using cellular networks with IP as the E2E network layer protocol, as indicated by the lower dotted box in Figure 6.

It is worth noting that the architecture and protocol stacks in Figure 6 focus on the sensor data communication between the InterSafe Sender and Receiver Systems. The full operation of the InterSafe Service using the cellular network-based deployment option involves other preparation steps; the working assumptions in the present document and briefly described below.

NOTE: Detailed description of overall V2X service operation processes and system architecture using cellular network communication are documented in [32]. Section 8.7 of [32] is dedicated to implementation examples of the Object Detection and Sharing use case.)

Service and server discovery:
In order to establish the IP communication with the correct infrastructure server, which provides the sensor data fulfilling the application requirements, the Equipped Road User needs to find the correct server for supported areas (intersections) and receive all information required to set up the secured connection with this server before receiving the sensor data. This information is obtained by the backend system and provided to the Equipped Road User on demand. This step is usually referred to as "service and server discovery" and further described in chapter 5 of [32].

Security:
Only the InterSafe Service from authenticated providers using secured E2E connection can be trusted by the Equipped Road Users. The Equipped Road Users (InterSafe Receiver Systems) need the information and permission from their backend systems to connect to external data sources. The backend system also assists road users/clients with credentials needed to authenticate the InterSafe Infrastructure Systems.

Service operation in multi-ecosystem stakeholder environments:
In public road environments, the Equipped Road Users and Infrastructure Systems may belong to different ecosystem stakeholders, e.g., vehicle fleet owners and road authorities. The actual protocol and security used should be based on a harmonized implementation profile as recommended in clause 6.2. For interoperable InterSafe Service deployment, in addition to the implementation profile the interested ecosystem stakeholders also need to agree on other business and trust conditions. This is further elaborated in section 4.4 and 8.7 of [32].

In addition to the 'V1/V1' Interface' option described above, an alternative deployment option of InterSafe Service using network-based communication is that the Equipped

[1] https://mqtt.org/faq/

Road User receives sensor data from its backend, which can be the car OEM backend or the SP backend. As shown in Annex D, in this 'O1/P1 deployment option' the car OEM backend obtains sensor data from the Infrastructure System using the O5 interface and sends it to the Equipped Road User via the O1 interface. (Similarly, the SP backend obtains the sensor data using the P3 interface and sends it to the Equipped User using the P1 interface.) The O5 and P3 interfaces benefit from a harmonized interface implementation profile based on the IP unicast communication, as recommended in clause 6.2, to enable interoperable InterSafe Service among Infrastructure Systems and backend systems of different stakeholders. The O1 interface between the vehicle and its backend is within the car OEM domain. As the owner of the car OEM domain, the car OEM can decide the implementation solution of the O1 interface. There is no need to agree on a single implementation profile among different car OEMs for the vehicle to OEM backend interface. The same applies for the P1 interface between the SP client and its SP backend, as shown in Annex D. This alternative deployment option is beneficial if a car OEM or SP wish to be in control of data sent to their connected Equipped Road Users, or if the sensor data are processed by the backend systems, e.g., warning messages instead of object data are sent by the backend systems to the receivers. This implementation option may be preferred by car OEMs or SPs due to security reason, as it limits the number of connections a vehicle or SP client need to establish with external entities (i.e., entities out of the car OEM or SP domains).

5. Profile details: ITS messages

5.1 Introduction

Profile details regarding which ITS messages are suited to the InterSafe Service, i.e., InterSafe Messages, and how efficiently and sufficiently the ITS messages can be formulated and implemented, are developed in this clause. Due to the use of different ITS messages in various regions, the regionally different profile details are provided in the following sub-clauses, specifically clause 5.2 for the US, clause 5.3 for Europe, and clause 5.4 for China.

NOTE: No relevant standardization activity is found for other regions.

The profile details on the InterSafe Messages include recommendations on the various aspects such as appropriate interpretation and value setting for some message fields, appropriate inclusion and/or omission of optional message fields with holding the compliance to the current standards defining the InterSafe Messages.

5.2 US

5.2.1 Recommended InterSafe Message

- SDSM defined in SAE J3224 [12]. The simplified SDSM structure is depicted in Figure 7. Further details can be found in SAE J3224 [12].

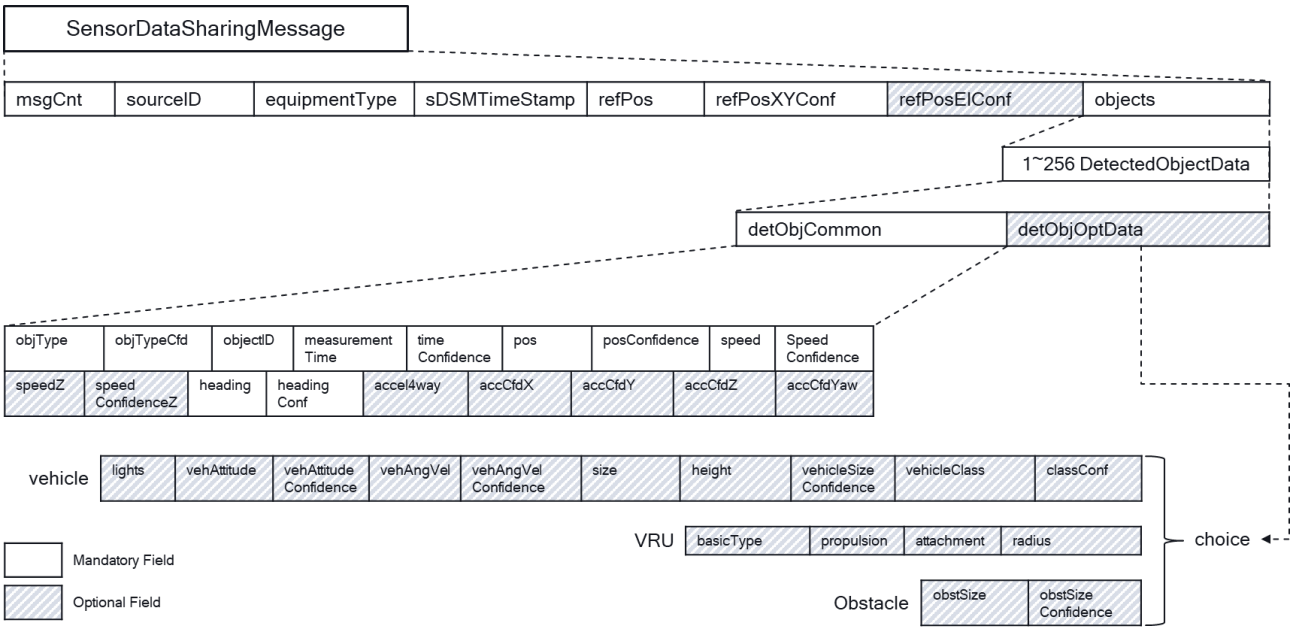


Figure 7: Simplified SDSM structure

5.2.2 Recommended interpretation of message fields for InterSafe Service

- *sDSMTimeStamp (DF_DDateTime)*
  - As described in SAE J3224 [12], the *sDSMTimeStamp* field indicates the generation time of an SDSM. More specifically, SAE J3224 [12] associates the timestamp with the time at which the SDSM originator determines its position.
  - In the case of an Infrastructure System originating SDSMs, positioning in an SDSM could be based on a fixed position (e.g., surveyed and provisioned) that is unchanging with time as opposed to a dynamically estimated position. When the position is fixed and unchanging with time, the *sDSMTimeStamp* should still be interpreted as the generation time of an SDSM, but it can be set to any time which can be reasonably distinguished by those in the sequence of SDSMs without being restricted to be associated with the time at which the SDSM originator determines its position. For example, it can be the time at which the application layer completes (or starts) the formulation of the application layer PDU, or the time at which the application layer passes down the application layer PDU to the lower layer.

5.2.3 Recommended value setting of message fields for InterSafe Service

- *equipmentType (DE_EquipmentType)*
  - As described in SAE J3224 [12], it is defined to indicate the originating device type among unknown (0), rsu (1), obu (2), and vru (3).
  - For InterSafe Service, the *equipmentType* should be set to rsu (1) to indicate that the SDSM originator is an Infrastructure System.

5.2.4 Recommended omission of optional message fields for InterSafe Service

It is generally encouraged that the SDSM includes the most optional message fields for InterSafe Service. Some of the optional message fields, however, are recommended to be omitted under the circumstances in order to reduce the SDSM size.

- Two-dimensional (2D) description
  - Even though SAE J3224 [12] allows three-dimensional (3D) representation for the positions and kinematics of the SDSM originator and its detected objects, most every intersection geometry is flat enough to be described two-dimensionally. In this case and except in some special cases where the 3D representation is meaningful, e.g., collapse or rollover crashes, the following optional message fields are recommended to be omitted from the SDSM formulation for InterSafe Service. However, those optional message fields could be useful in other cases, and thus they are highly recommended to be included especially in some urban scenarios including bridges and overpasses.

<Position of the SDSM originator>

- *refPos (DF_Position3D)* ➔ *elevation (DE_Elevation)*
- *refPosElConf (DE_ElevationConfidence)*

<Position of the detected object in *detObjCommon (DF_DetectedObjectCommonData)*>

- *pos (DF_PositionOffsetXYZ)* ➔ *offsetZ (DE_ObjectDistance)*
- *posConfidence (DF_PositionConfidenceSet)* ➔ *elevation (DE_ElevationConfidence)*

<Kinematics of the detected object in *detObjCommon (DF_DetectedObjectCommonData*)>

- *speedZ (DE_Speed)*
- *speedConfidenceZ (DE_SpeedConfidence)*
- *accCfdZ (DE_AccelerationConfidence)*

NOTE: The vertical acceleration, i.e., acceleration along Z-axis, is indicated by the field *vert* (*DE_VerticalAcceleration*), as defined in SAE J2735 [22]. Its parent field *accel4way* is optional but the vertical acceleration field itself is not optional. This means that the vertical acceleration cannot be omitted without also omitting other acceleration elements of accel4way (longitudinal acceleration, lateral acceleration and yaw rate). Therefore, the vertical acceleration *vert* (*DE_VerticalAcceleration*) should be set to 0 or "unavailable" under this circumstance. It is recommended that the field is revised to an optional field in future revisions of the targeted standard. See the Annex A.1.

▸ Stationary object

- Many fields for the kinematics of a detected object can be omitted in an SDSM when the detected objects are stationary, i.e., the speed of the detected object is zero. In this case, the following optional message fields are recommended to be omitted from the SDSM formulation for InterSafe Service.

<Kinematics of the detected object in *detObjCommon (DF_DetectedObjectCommonData*)>

- *speedZ (DE_Speed)*
- *speedConfidenceZ (DE_SpeedConfidence)*
- *accel4way (DF_AccelerationSet4Way)*
- *accCfdX (DE_AccelerationConfidence)*
- *accCfdY (DE_AccelerationConfidence)*
- *accCfdZ (DE_AccelerationConfidence)*
- *accCfdYaw (DE_YawRateConfidence)*

NOTE1: The speed is not an optional field and therefore cannot be omitted. The field should be set to 0.

NOTE2: The heading is not an optional field and therefore cannot be omitted. The field should be set to 28800 as "unavailable" or the past heading may be used if the trajectory (path) over which the detected object travelled to reach its current location is well detected.

<Kinematics of the detected vehicle in *detVeh (DF_DetectedVehicleData)*>

- *vehAttitude (DF_Attitude)*
- *vehAttitudeConfidence (DF_AttitudeConfidence)*

NOTE: The attitude field *vehAttitude* (*DF_Attitude*) has its offspring fields of the *pitch*, *roll*, and *yaw*. The *pitch* and *roll* are useless with 2D descriptions or for a stationary object, and the *yaw* is useless only for a stationary object. For instance, it would be beneficial if the *pitch* and *roll* could be omitted in 2D descriptions. However, it is not allowed to omit any of the offspring fields when the attitude field is included and only allowed to omit the attitude field as a whole because it is optional, but the offspring fields are not optional. It is recommended that the individual offspring fields of the attitude are revised to optional fields in future revisions of the targeted standard. See the Annex A.1.

<Kinematics of the detected vehicle in *detVeh (DF_DetectedVehicleData)*>

- *vehAngVel (DF_AngularVelocity)*
- *vehAngVelConfidence (DF_AngularVelocityConfidence)*

NOTE: If an optional field is unavailable at the SDSM originator without meeting its corresponding omission condition above, then the field should be set to “unavailable” (or “not equipped”, “unknown”) instead of omitted if the “unavailable” value setting is supported by SAE J3224 [12].

▸ Others

- Even though SAE J3224 [12] allows the inclusion of the following optional fields in an SDSM, they should be omitted from the SDSM formulation for InterSafe Service because their need in the InterSafe Service use cases is not identified.

<Detected vehicle’s height in *detVeh (DF_DetectedVehicleData)*>

- *height (DE_VehicleHeight)*

<Detected VRU’s propulsion in *detVRU (DF_DetectedVRUData)*>

- *propulsion (DF_PropelledInformation)*

5.3 Europe

5.3.1 Recommended InterSafe Message

- CPM defined in ETSI TS 103 324 [11]. The simplified CPM structure is depicted in Figure 8. Further details can be found in ETSI TS 103 324 [11].

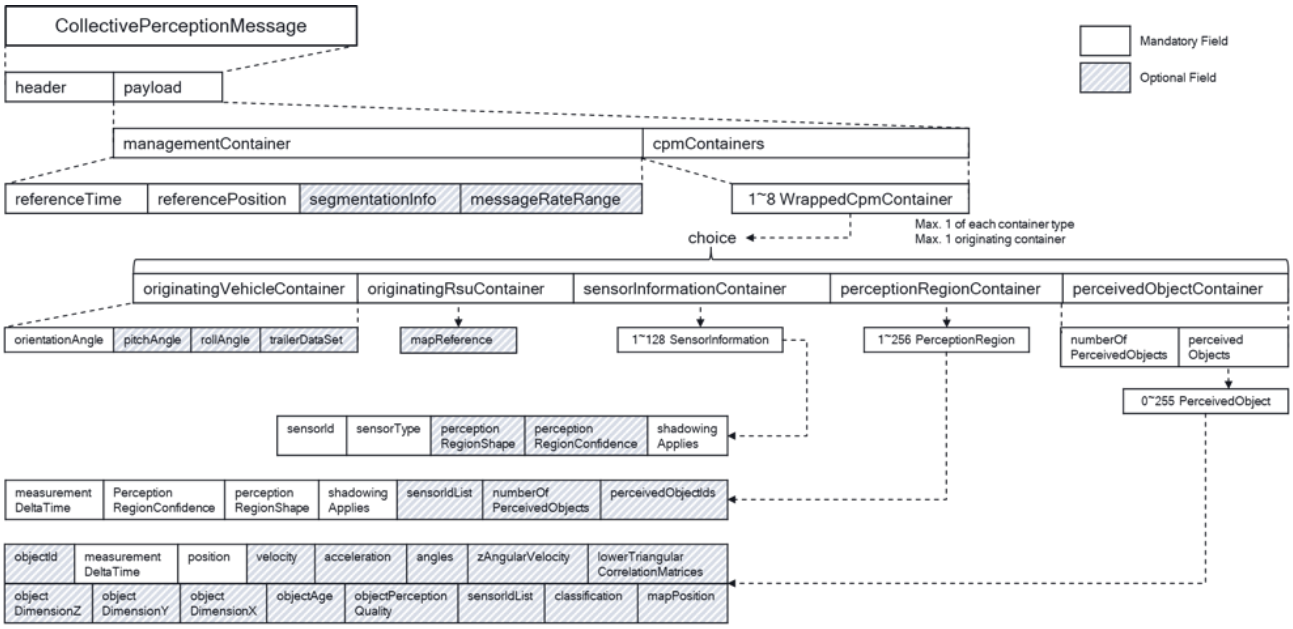


Figure 8: Simplified CPM structure

5.3.2 Recommended interpretation of message fields for InterSafe Service

- *referenceTime (DE_TimestampIts)*
  - The same interpretation as that in clause 5.2.2 is applied for the *referenceTime*.

5.3.3 Recommended container selection for InterSafe Service

For InterSafe Service, one Originating RSU Container of type *OriginatingRsuContainer* should be present to indicate that the CPM originator is an Infrastructure System, and an Originating Vehicle Container of type *OriginatingVehicleContainer* should not be present.

5.3.4 Recommended omission of optional message fields for InterSafe Service

It is generally encouraged that the CPM includes the most optional message fields for InterSafe Service. Some of the optional message fields, however, are recommended to be omitted under the circumstances in order to reduce the CPM size.

▸ Two-dimensional description

- Even though ETSI TS 103 324 [11] allows three-dimensional representation for the positions and kinematics of the CPM originator and its detected objects, most every intersection geometry is flat enough to be described two-dimensionally. In this case and except some special cases where the 3D representation is meaningful, e.g., collapse or rollover crashes, the following optional message fields are recommended to be omitted from the CPM formulation for InterSafe Service. However, those optional message fields could be useful in other cases, and they are highly recommended to be included especially in some urban scenarios including bridges and overpasses.

<Position of the detected object in Perceived Object Container>

- *perceivedObjects (DF_PerceivedObjects) ➔ DF_PerceivedObject ➔ position (DF_CartesianPosition3dWithConfidence) ➔ zCoordinate (DF_CartesianCoordinateWithConfidence)*

<Kinematics of the detected object in Perceived Object Container>

- *perceivedObjects (DF_PerceivedObjects) ➔ DF_PerceivedObject ➔ velocity (DF_Velocity3dWithConfidence) ➔*
  - *polarVelocity (DF_VelocityPolarWithZ) ➔ zVelocity (DF_VelocityComponent)*
  - *cartesianVelocity (DF_VelocityCartesian) ➔ zVelocity (DF_VelocityComponent)*
- *perceivedObjects (DF_PerceivedObjects) ➔ DF_PerceivedObject ➔ acceleration (DF_Acceleration3dWithConfidence) ➔*
  - *polarAcceleration (DF_AccelerationPolarWithZ) ➔ zAcceleration (DF_AccelerationComponent)*
  - *cartesianAcceleration (DF_AccelerationCartesian) ➔ zAcceleration (DF_AccelerationComponent)*

▸ Stationary object

- Many fields for the kinematics of a detected object can be omitted in an CPM when the detected objects are stationary, i.e., the speed of the detected object is zero. In this case, the following optional message fields are recommended to be omitted from the CPM formulation for InterSafe Service.

<Kinematics of the detected object in Perceived Object Container>

- *perceivedObjects (DF_PerceivedObjects) ➔ DF_PerceivedObject ➔ velocity (DF_Velocity3dWithConfidence)*
- *perceivedObjects (DF_PerceivedObjects) ➔ DF_PerceivedObject ➔ acceleration (DF_Acceleration3dWithConfidence)*
- *perceivedObjects (DF_PerceivedObjects) ➔ DF_PerceivedObject ➔ angles (DF_EulerAnglesWithConfidence)*
- *perceivedObjects (DF_PerceivedObjects) ➔ DF_PerceivedObject ➔ zAngularVelocity (DF_CartesianAngularVelocityComponent)*

▸ Others

- Even though ETSI TS 103 324 [11] allows the inclusion of the following optional fields in a CPM, they should be omitted from the CPM formulation for InterSafe Service because their need in the InterSafe Service use cases is not identified.

<Detected object's height in Perceived Object Container>

- *perceivedObjects (DF_PerceivedObjects)* ➔ *DF_PerceivedObject* ➔ *objectDimensionZ (DF_ObjectDimension)*

5.3.5 Recommended feature selections for InterSafe Service

ETSI TS 103 324 [11] leaves the selection of some features/options to the implementation stage. That includes the CPM interval, which has a range (100-1000 ms) but no fixed value, whether the object inclusion rule is applied or not, as well as which CPM assembly mechanism is applied between the object utility function or the perception region. This provides a degree of flexibility in the implementation. At the same time, however, it may complicate implementation having to choose the right features, and it is not investigated how different CPM implementation choices would work together. For the InterSafe Service, it is left for the future study to provide recommendations on the features/options.

5.4 China

5.4.1 Recommended InterSafe Message

▸ SSM defined in CSAE T/CSAE 315.2 [28]. The simplified SSM structure is depicted in Figure 9. Further details can be found in CSAE T/CSAE 315.2 [28].

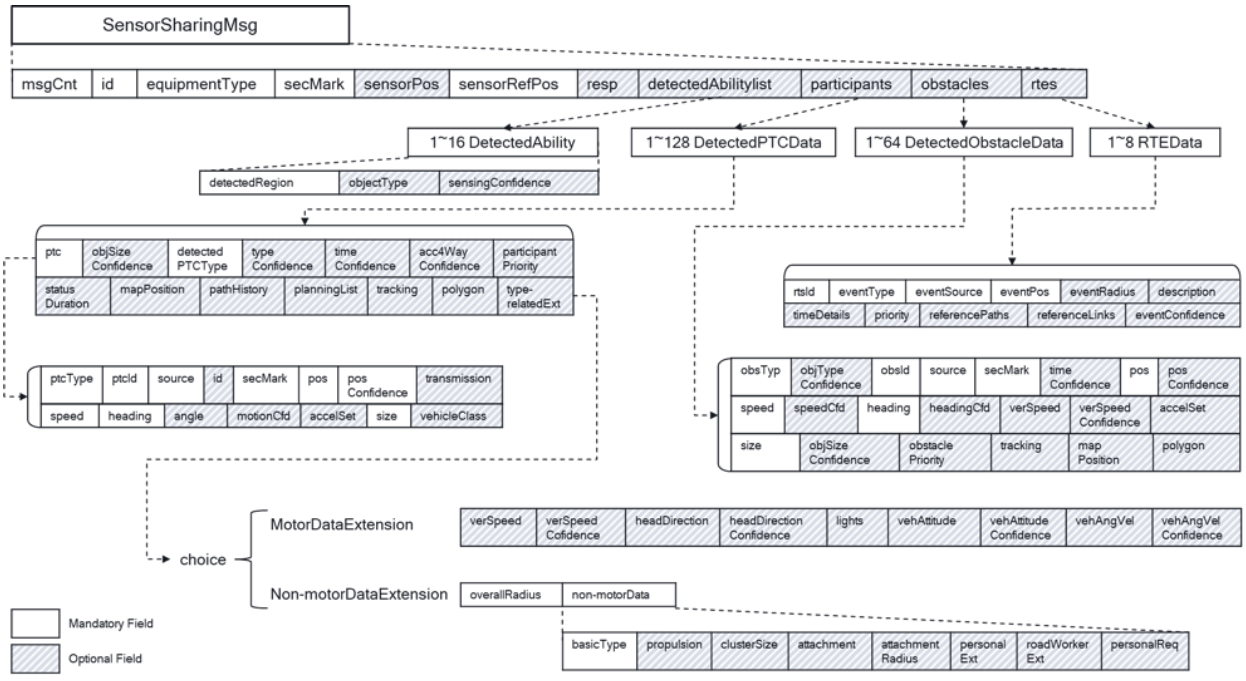


Figure 9: Simplified SSM structure

5.4.2 Recommended interpretation of message fields for InterSafe Service

- *sSMTimeStamp (DE_DSecond)*
  - The same interpretation as that in clause 5.2.2 is applied for the *sSMTimeStamp*.

5.4.3 Recommended value setting of message fields for InterSafe Service

- *Id (OCTET STRING (SIZE(8)))*
  - As described in T/CSAE 315.2 [28], it is defined to indicate the identification of the sender. In the Sensor Data Sharing use case, if the sender is a vehicle, it represents the temporary identification of the Host Vehicle (HV), which is aligned to the BSM temporary ID, or fill in the RSU identifier in a roadside sharing case.
  - For InterSafe Service, because only RSUs can be the SSM originators, it should be filled with the RSU identifier for this *Id*.

- *equipmentType (DE_EquipmentType)*
  - As described in T/CSAE 315.2 [28], it is defined to indicate the originating device type among unknown (0), rsu (1), obu (2), and vru (3).
  - For InterSafe Service, the *equipmentType* should be set to rsu (1) to indicate that the SSM originator is an Infrastructure System.

5.4.4 Recommended omission of optional message fields for InterSafe Service

Although the design of SSM encourages that the SSM includes the most optional message fields for InterSafe Service, some of these fields are recommended to be omitted under the circumstances to reduce the SSM size.

- Stationary object
  - Many fields for the kinematics of a detected object can be omitted in an SSM when the detected objects are stationary, i.e., the speed of the detected object is zero. In this case, the following optional message fields are recommended to be omitted from the SSM formulation for InterSafe Service.

<Kinematics of the detected participant in *DF_DetectedPTCData*>

- *acc4WayConfidence (DF_AccSet4WayConfidence)*

<Kinematics of the detected participant in *pct (DF_ParticipantData)*>

- *transmission (DE_TransmissionState)*
- *angle (DE_SteeringWheelAngl)*
- *motionCfd (DF_MotionConfidenceSet)*
- accelSet (DF_AccelerationSet4Way)

<Kinematics of the detected participant in *motorExt (DF_MotorDataExtension)*>

- *verSpeed (DE_Speed)*
- *verSpeedCofidence (DE_SpeedConfidence)*
- *headDirection (DE_Heading)*
- *headDirectionConfidence (DE_HeadingConfidence)*
- *vehAttitude (DF_Attitude)*
- *vehAttitudeConfidence (DF_AttitudeConfidence)*
- *vehAngVel (DF_AngularVelocity)*
- *vehAngVelConfidence (DF_AngularVelocityConfidence)*

<Kinematics of the detected obstacle in *DF_DetectedObstacleData*>

- *speedCfd (DE_SpeedConfidence)*
- *headingCfd (DE_HeadingConfidence)*
- *verSpeed (DE_Speed)*
- *verSpeedCofidence (DE_SpeedConfidence)*
- *accelSet (DF_AccelerationSet4Way)*

5.5 Object priority and mechanisms for limiting message size

It is anticipated that for some deployment options there could be a limitation on the number of objects which an InterSafe Message can convey even though the message structure is allowed to include a considerable number of objects (e.g., 256 detected objects in an SDSM). While such a limitation seems quite likely to be defined as part of a profile when using direct communication over ITS frequency bands, it might also be applicable in some network-based communication scenarios. Some reasons that could motivate imposing a limitation on the number of objects include:

- A limited channel capacity where there is a need to use a common channel to support various messages for multiple safety services
- A packet size limitation in protocols (usually the PHY/MAC protocols)
- A limitation during implementation (e.g., due to the processing burden in senders)

However, there could be a greater number of detected objects than allowed for after taking into consideration these limitations. This clause of the TR investigates how to address these limitations by selectively including detected objects in an InterSafe Message based on priority settings.

5.5.1 US (Single InterSafe Message in a transmission interval)

SAE J3224 [12] does not allow the SDSM originator to transmit more than one SDSM in a transmission interval. This approach needs a mechanism to prioritize the detected objects. For the InterSafe Service, it is recommended that the InterSafe Sender System assesses the risks associated with detected objects, prioritizes them, and includes the information of the given limited number detected objects orderly according to the prioritization in an InterSafe Message for a transmit interval.

The examples of the risk assessment could be the distance to risky areas, such as intersection/junction or crosswalk areas, the time to the risky area or the Time to Collision (TTC). It is recommended that the risk assessments and associated prioritization mechanisms are standardized in future revisions of the targeted standard.

5.5.2 Europe (Multiple InterSafe Messages in a transmission interval)

ETSI TS 103 324 [11] allows the CPM originator to transmit more than one CPMs in a transmission interval. A CPM originator first selects which detected objects are to be transmitted in the given transmission interval by the mechanism called “perceived object inclusion management”. If the number of selected objects would make the CPM size greater than the given packet size limitation, the CPM originator distributes them to the multiple CPMs according to the mechanism called “CPM assembly” and conveys the CPMs in a transmission interval.

Since this approach would allow an InterSafe Sender System to transmit most detected objects to InterSafe Receiver Systems in return for occupying more channel capacity, an additional mechanism for prioritization is not needed.

5.5.3 China (Multiple InterSafe Messages in a transmission interval)

CSAE T/SAE 315.2 [28] allows the SSM originator to transmit more than one SSM in a transmission interval. An SSM originator first selects which detected objects are to be transmitted in the given transmission interval. If the number of selected objects would make the SSM size greater than the given packet size limitation, as above the SSM originator utilizes multiple SSMs to transmit the related information in a transmission interval.

6. Profile details: Protocol stacks and access layers

6.1 Profile on protocol stacks and access layer for direct communication

6.1.1 Introduction

Profile details regarding which “protocol stacks” and how the “access layer” can best transport the InterSafe Messages described in clause 5 are developed in this clause. Due to the use of different ITS protocol stacks in various regions, the regionally different profile details on the protocol stacks and access layers are provided in the following sub-clauses, specifically clause 6.2 for the US, clause 6.3 for Europe, and clause 6.4 for China.

The profile details on the protocol stacks and access layers include recommendations on the various aspects such as parameters of transport, network and access layers, prioritization relative to other applications/services, congestion control, and any other operational aspects in light of the specific channel usage/configuration for a given region, as well as coexistence with other services already anticipated for deployment based on existing standardized profiles.

6.1.2 US

The ITS protocol stack for the US in SAE J3161 [10] is illustrated in the Figure 10. The automotive industry, through SAE International, ETSI, and IEEE, has done considerable work in defining the applications, the message/facilities layer, security services, and the transport/networking layers. C-V2X leverages all the effort on the 3GPP PHY and MAC layers (commonly called the “access layers”). As illustrated in Figure 10, the ITS protocol stack for the United States adopts the IEEE standards for security services (IEEE Std 1609.2 [15]), and transport/networking protocols (WSMP defined in IEEE Std 1609.3 [16]) as dedicated ITS protocols, while allowing the conventional transport/networking protocols of the TCP, UDP, and IPv6. On top of that, the ITS protocol stack for the US adopts the SAE standards for application/message layers and profiles.

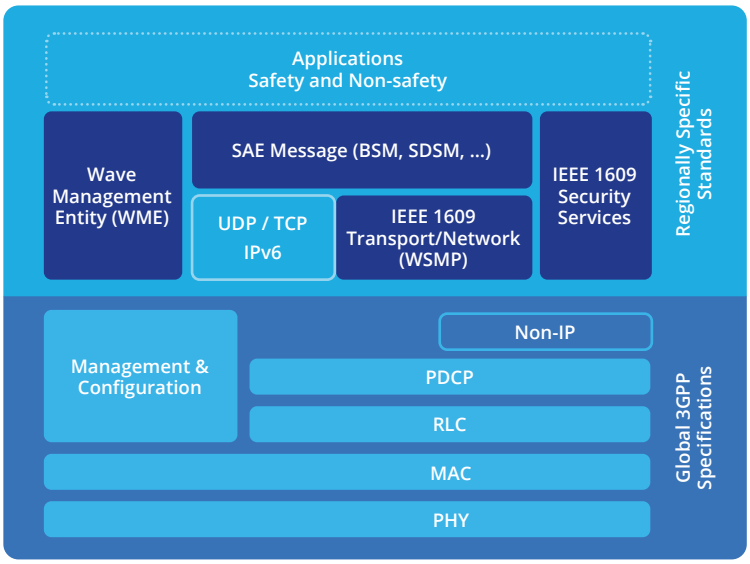


Figure 10: ITS protocol stack for the United States

Based on SAE J3161 [10], which provides the common design elements, PC5 sidelink profiles, communication parameters, and other related items for LTE-V2X communications, the recommended protocol stack and configuration parameters are in Table 1, as follows:

Table 1: Recommended protocol stacks and configuration parameters over direct communication for InterSafe Service in the US

Recommended Protocol Stacks	
Message	SDSM (SAE J3224 [12])
NOTE: Some other messages, e.g., BSM, MAP, SPAT, can be used in conjunction with SDSM for InterSafe Service.	
Network / Transport Protocol	WSMP (IEEE 1609.3 [16])
Security	WAVE Security Services (IEEE 1609.2 [15])
NOTE: The optional field of *generationTime (Time64)* of ***HeaderInfo*** in the Security Services Protocol Data Unit (SPDU) should be omitted since an equivalent timestamp is provided by SDSMs.	
Access Layer	LTE-V2X PC5 (SAE J3161 [10])
Recommended Protocol Stacks	
PSID Value: Decimal / Hex / P-encoding	144 / 0x90 / Op80-10 (SAE J3224 [12])
Destination Layer-2 ID	0x000090 (by the mapping defined in SAE J3161 [10])
Channel	5905 ~ 5925 MHz of LTE band 47, also known as Channel 183 by IEEE
Traffic Family	Essential V2V (tentative)
PPPP	5 (tentative)

NOTE: Other parameters are determined by the channel and PPPP value as defined in SAE J3161 [10].

6.1.3 Europe

The C-V2X ITS protocol stack for Europe, based on ETSI EN 302 665 [9], is illustrated in Figure 11. It adopts the ETSI standards for security services, and transport/networking protocols (BTP/GeoNetworking) as dedicated ITS protocols, while allowing the conventional transport/networking protocols of the TCP, UDP, and IPv6 on the 3GPP PHY and MAC layers. On top of that, the C-V2X ITS protocol stack for Europe also adopts the ETSI standards for applications/facilities layers and profiles.

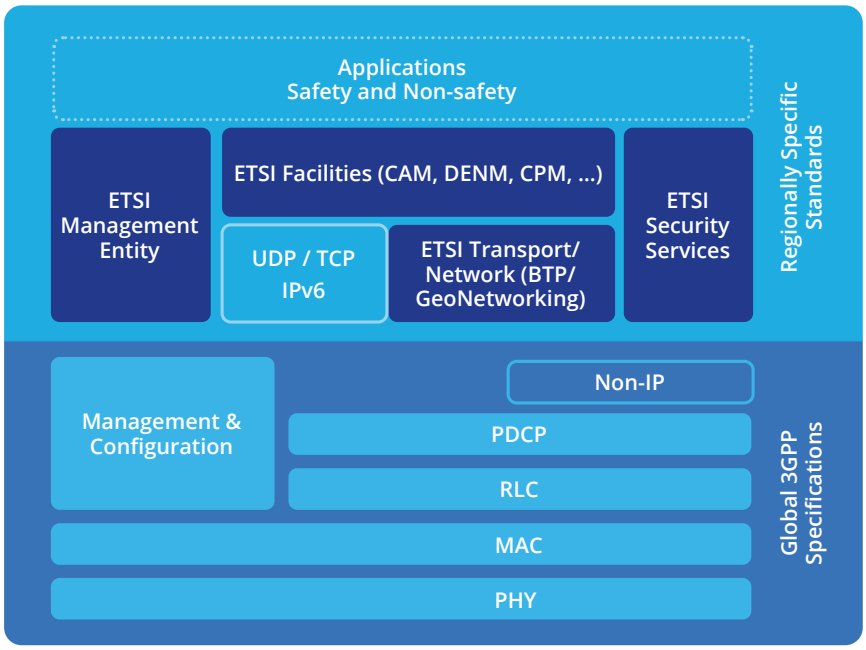


Figure 11: ITS protocol stack for Europe

The recommended protocol stack and configuration parameters for InterSafe Service in Europe are provided in Table 2:

Table 2: Recommended protocol stacks and configuration parameters over direct communication for InterSafe Service in Europe

Recommended Protocol Stacks	
Message	CPM (ETSI TS 103 324 [11])
NOTE: Some other messages, e.g., CAM, DENM, SPATEM, MAPEM, can be used in conjunction with CPM for InterSafe Service.	
Network / Transport Protocol	GeoNetworking (ETSI TS 103 836-4-1 [17], ETSI TS 103 836-4-3 [18]) / BTP (ETSI TS 103 836-5-1 [19])
Access Layer	5G-V2X PC5 (EN 303 798 [20])
Recommended Protocol Stacks	
ITS-AID value	639 (ETSI TS 102 965 [21])
BTP Type	BTP-B
GN Packet Transport Type	For broadcast, Single-hop broadcast (SHB) For groupcast, Single-hop groupcast (SHG) (See ETSI TS 103 836-4-3 [18])
Destination Layer-2 ID	For broadcast, all "1" For groupcast, a service-specific Destination Layer 2 ID (as defined in ETSI) (See ETSI TS 103 836-4-3 [18])
Channel	TBD
Traffic Class (PPPP)	TC ID 4 (PPPP 5) (tentative)

NOTE: Other network/transport protocol parameters are defined in ETSI TS 103 836-4-1 [17], ETSI TS 103 836-4-3 [18], and ETSI TS 103 836-5-1 [19]. Other access layer parameters are determined by the PPPP value as defined in EN 303 798 [20].

The groupcast is a new feature of NR-V2X which is similar to broadcast except that Hybrid Automatic Repeat Request (HARQ) may be exercised to increase reliability. The connection-less groupcast uses NACK-based HARQ for receivers in a specified range parameter. The range, i.e., the Quality of Service (QoS) range, should be set by the application layer and passed to the access layer. The connection-oriented groupcast does ACK/NACK-based HARQ for receivers of a group where the group composition and management are in the application layer scope. When the groupcast is used for InterSafe Service, the connection-less groupcast is recommended.

6.1.4 China

The China Society of Automotive Engineers (CSAE) and China Communications Standards Association (CCSA) have collaborated to formulate service/application-layer standards, as well as security and transport/network-layer standards, tailored for C-V2X. Based on the series of C-V2X standards, the ITS protocol stack for China has been formed and is illustrated in the Figure 12.

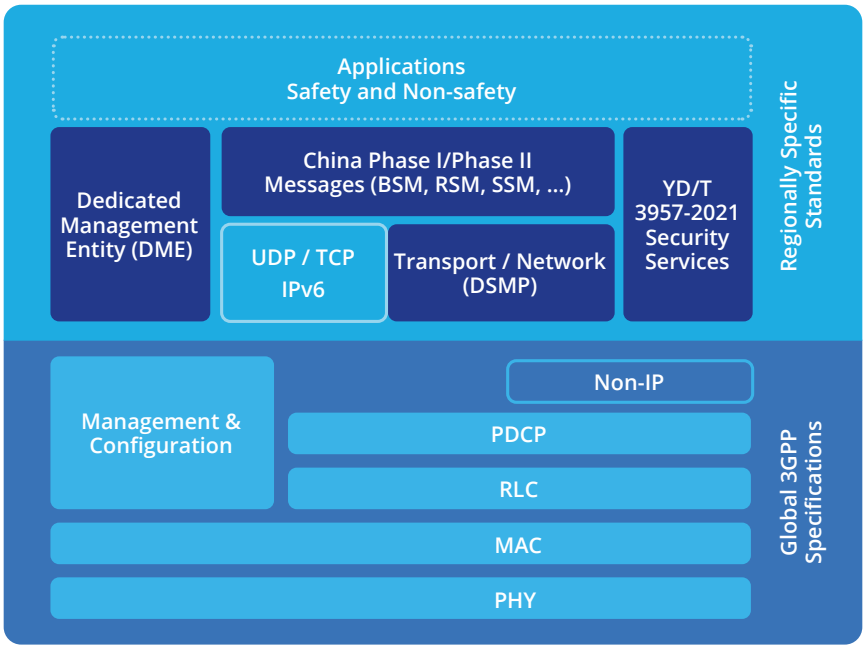


Figure 12: ITS protocol stack for China

The recommended protocol stack and configuration parameters for InterSafe Service in China are in Table 3, as follows:

Table 3: Recommended protocol stacks and configuration parameters over direct communication for InterSafe Service in China

Recommended Protocol Stacks	
Message	SSM (T/CSAE 315.2 [28])
NOTE: Some other messages, e.g., BSM, RSI, MAP, SPAT, SAM, VIR can be used in conjunction with SSM for InterSafe Service	
Network / Transport Protocol	DSMP (YD/T 3707-2020 [29])
Security	Security Services (YD/T 3957-2021 [30])
Access Layer	LTE-V2X PC5 (YD/T 3340-2018 [31])
Recommended Configuration Parameters	
AID Value: Decimal / P-encoding	3625 / 0p8D-A9 (T/CSAE 315.2 [28]) (tentative)
Destination Layer-2 ID	0x00000D (AID that message sent by RSU for test) (tentative)
Channel	5905 ~ 5925 MHz of LTE band 47
PPPP	5

6.1.5 Performance analysis based on simulation

Simulations based on SDSM and US protocols are performed to investigate the impact of the InterSafe Messages on other safety services already operating in the same ITS frequency band. They investigate the performance of the InterSafe Messages, and analyse the data traffic characteristics and delivery requirements of the InterSafe Messages.

It is assumed in a simulation that the RSUs transmit SPATs, MAPs, and RTCMs in addition to SDMSs, and the vehicles transmit BSMs in the same ITS frequency band. Based on that, the impact of SDSMs on BSMs and SPATs as well as the performance of SDSMs are investigated. Moreover, the relations between the performance of SDSMs and C-V2X penetration rate, and the supportable maximum SDSM packet size in various C-V2X penetration situations are analyzed. See the details in Annex B.

The key observations are as follows:

- There is largely no significant impact on the BSM and SPAT due to SDSM traffic for C-V2X penetration rates of 20%, 50%, and 90%.
- SDSM Packet Reception Ratio (PRR) is a function of C-V2X penetration. The higher the C-V2X penetration, the more vehicles transmit BSMs that could interfere with SDSM. However, the packet size of SDSM would be smaller with higher C-V2X penetration and thus improve the PRR.
- The maximum SDSM packet size that can be supported even with 90% C-V2X penetration rate and a requirement of 0.9 PRR at a range of 100 m is approximately 2000 bytes.

6.2 Profile on protocol stacks for network-based communication

6.2.1 Introduction

This clause recommends protocol stacks and configuration parameters for InterSafe Service implementation using network-based communications. The main interest of network-based implementation is to realize InterSafe Service use cases for Equipped Road Users connected using the 3GPP Uu radio interface. As described in clause 4.4.2, and shown in Figure 6, IP is the state-of-the-art technology for E2E interoperability at the network layer, hiding the heterogenous characteristics of access layer technologies in different parts of the transport network. IP is the standard protocol used for application communications globally, and natively supported by mobile networks of different generations. Therefore, InterSafe Service protocol stack profiles for network-based communication provided in this work focus on upper layers sitting on top of IP. Clause 6.2.2 provides the recommended profile for this scenario.

6.2.2 Protocol stacks and configuration parameters

For the deployment option using V1/V1' interface, as described in clause 4.4.2, Table 4 provides recommended protocol stacks and configuration parameters. Additionally, 5GAA V2N2X Technical Report [32] (section 8.7 Object Detection and Sharing Use Case) provides a more comprehensive implementation description for object detection and sharing at intersections supporting the InterSafe Service use case.

Table 4: Protocol stacks and configuration parameters over network-based communication for InterSafe Service

Recommended Protocol Stacks	
Message	SDSM (SAE J3224 [12]), CPM (ETSI TS 103 324 [11]), SSM (T/CSAE 315.2 [28])
NOTE: Some other messages can be used in conjunction with SDSM, CPM and SSM for InterSafe Service. Selection of the messages for InterSafe Service in different regions should follow the specifications referenced in clause 5.	
Message Queuing Protocol	MQTT
Network / Transport Protocol	IPv6 / TCP / TLS (Port: 8883 for MQTT over TLS)
Security	Communication is protected using standard IT technology, e.g., using TLS between the InterSafe Sender System and the InterSafe Receiver System, based on agreement.
Access Layer	Due to the usage of IP at the network layer, E2E data communication is agnostic to the access layer technologies, e.g., C-V2X mobile network-based communication or wired communication among the backends. NOTE: For C-V2X mobile network-based communications, E2E IP communication is natively supported, irrespective of mobile network operators and the generation of mobile network used by the Equipped Road Users.
Example Configuration Parameters	
NOTE: See 5GAA V2N2X Technical Report [32] (section 8.7 Object Detection and Sharing Use Case) for implementation examples.	

Support for multiple users and various services is the normal mode of operation in a multi-service cellular network, where radio base stations schedule users through “fair-share” algorithms on the multitude of frequency bands available to the mobile network operator. If needed, certain users or services (IP flows) such as the InterSafe Service can be prioritized, (e.g. over ordinary mobile broadband services using 3GPP standardized QoS mechanisms). See Annex E of [32] for details about 3GPP QoS assurance and network-slicing mechanisms.

7. Conclusion

According to various reports and statistics, the majority of traffic fatalities occur at intersections. Intersection safety service via infrastructure sensor-sharing – called InterSafe Service in this Technical Report – is an emerging approach to enhance intersection safety.

This document identifies the applicable use cases and related system requirements, functional flow, reference protocol stack and architecture. It then looks at different deployment options (including the use of direct communication and/or network-based communication) for infrastructure sensor-sharing, depending on the employed communication technologies, involved ecosystem stakeholders, service operation models, etc. When using direct communication, the simulation results show how InterSafe Service can operate over a common channel accommodating multiple safety services/messages – i.e., BSMs, SPATs, MAPs and RTCMs.

There are regionally specific ITS standards on the messages and protocols in organizations such as SAE International, ETSI, and CSAE suitable to the InterSafe Service. This document provides the profile details on the standards as well as describing the concept of operation and various deployment options for InterSafe Service.

Findings in this TR serve as a guide to future updates of relevant standards and the development of corresponding system-level profiles. It is suggested that any subsequent standardization work follow the layered structure, as specified in clauses 5 and 6, to enable deployment options using C-V2X direct and/or network communication technologies. Consequently, it will expedite the implementation and deployment of InterSafe Service which can considerably reduce the traffic fatalities.

Annex A: Recommendations for relevant Standards Development Organizations (SDOs)

Recommendations on how to use the existing standards for InterSafe Service are described in clauses 5 and 6. However, in addition to them, several aspects which are potentially beneficial to be developed directly in the SDOs are found, and recommended in the following sub-clauses.

A.1 Recommendations for SAE International

It is recommended for SAE International on SAE J3224 [12] to:

- Develop standardized approaches for error calculation (i.e., accuracy and confidence) for the message fields for object classification, positioning, and kinematics.
- Develop a profile standard for relevant specific applications (e.g., intersection safety, collision warning and control applications).
- Develop test procedures for certification.
- Develop methods on the message structure to decrease radio load, such as for clustered pedestrians as PSM in SAE J2945/9 [33] and J2735 [22].
- Revise some mandatory fields to "optional", as described in clause 5.2.4.
    - acceleration along Z-axis: *detObjCommon (DF_DetectedObjectCommonData)* ➔ *accel4way (DF_AccelerationSet4Way)* ➔ *vert (DE_VerticalAcceleration)*
    - individual offspring fields of the attitude: *detVeh (DF_DetectedVehicleData)* ➔ *vehAttitude (DF_Attitude)* ➔ *pitch (DE_PitchDetected), roll (DE_RollDetected), yaw (DE_YawDetected)*
- Revise the following message fields with new ranges and granularities:
    - The ranges in message fields in *detObjCommon (DF_DetectedObjectCommonData)* are too large for their allowed values in SAE J3224 [12] and SAE J2735 [22].
        - *posConfidence (DF_PositionConfidenceSet)* ➔ *pos (DE_PositionConfidence):* 0.01 to 500 meters, 16 levels with 4 bits
        - *speedConfidence (DE_SpeedConfidence):* 0.01 to 100 meters/second (about 223.7 miles/hour), 8 levels with 3 bits
        - *headingConf (DE_HeadingConfidence):* 0.0125 to 10 degrees, 8 levels with 3 bits
- Develop risk assessments and associated object prioritization mechanisms, as described in clause 5.5.1.

NOTE: The recommendations above are for SAE International, but they may be applicable for other SDOs such as ETSI and CSAE.

Annex B: Simulation results

Simulation results are provided:

- To investigate the impact of the InterSafe Messages on other safety services already operating in the same ITS frequency band
- To investigate the performance of the InterSafe Messages
- To analyze the data traffic characteristics and delivery requirements of the InterSafe Messages

B.1 Simulation results of SDSM

B.1.1 Introduction

The simulation setup on access layer and network traffic, considered intersection layout, and SDSM packet size calculation is provided in B.1.2. It is assumed that RSUs transmit SPATs, MAPs, and RTCMs in addition to SDMSs, and the vehicles transmit BSMs in the same ITS frequency band. Based on that, the impact of SDSMs on BSMs and SPATs are investigated in B.1.3. The performance of SDSMs is investigated in B.1.4 in terms of the Packet Reception Ratio (PRR) and Inter-Packet Gap (IPG). Annex B.1.5 analyzes the supported maximum SDSM packet size in various C-V2X penetration situations, and a summary of the simulation results is provided in B.1.6.

B.1.2 Simulation setup

- Access layer and network traffic
  - HARQ Enabled. BSM Congestion Control Enabled
  - 20 dBm conducted power. 3dBi antenna gain for RSUs,
  - Vehicle traffic
    - BSM traffic: {80% 190 bytes; 20% 300 bytes} with a periodicity of 100 ms
    - 20%, 50%, 90% C-V2X penetration rates (i.e., percent of V2X vehicles that transmit BSMs)
  - RSU traffic

Table 5: RSU traffic in SDSM simulation

Message Type	Packet Size (Bytes)	PPPP	Transmission rate (Hz)	No. of subchannels
MAP	1500	3	1	10
SPAT	500	5	10	3
RTCM	750	5	1	4
SDSM	Variable	5	10	10 (max)

- Intersection layout

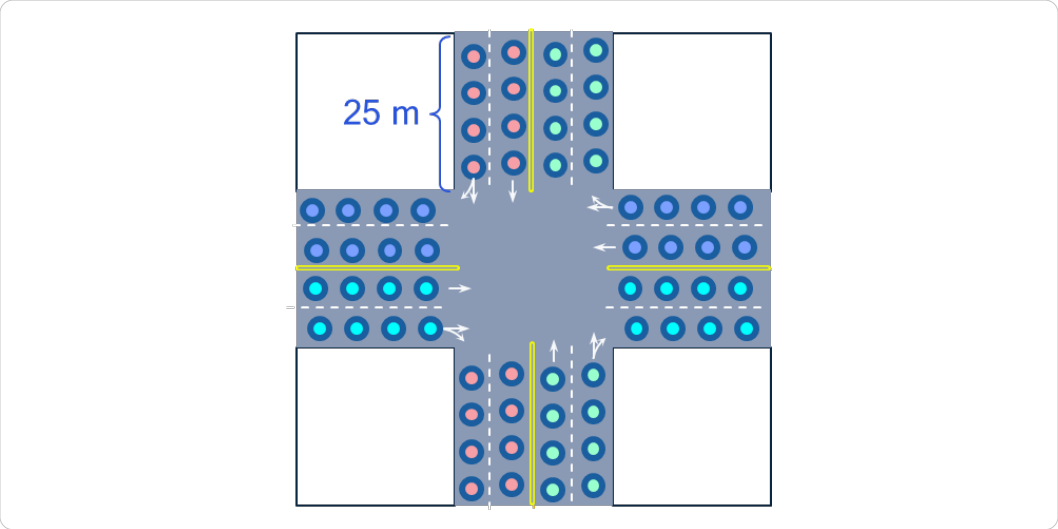


Figure 13: Intersection layout in SDSM simulation

- The perception range of a fish-eye camera has a 25 m radius. Via simulations, this information is used to determine a sample number of objects with SDSM message sizes. Other message sizes have also been simulated and will be discussed.
- Considering the average of length of a car is 5 m, there would be approximately four vehicles in each lane.
- Therefore, approximately 64 vehicles at this intersection within the perception range of the camera sensor.
- Among the 64 vehicles (cars and motorcycles), it is considered that 40 are in motion and 24 are stationary. Additionally, it is considered that there are 10 pedestrians and bicycles (5 moving plus 5 stationary).
- This is represented on a Grid Drop layout of one block with vehicles on the same road having Line of Sight (LOS) links and vehicles on different (perpendicular) roads with Non-Line of Sight (NLOS) links.

- SDSM packet size calculation

- The size of the SDSM mainly depends on the number of vehicles/objects of interest captured by the sensor/camera that has been installed. But it also depends on the following factors:
  - Over-the-Air (OTA) size of the SDSM before adding any objects: 170 bytes (includes RLC/PDCP/WSMP/1609 headers)
  - Full certificate is attached periodically (at least every 450 ms same as BSM): 74 bytes
  - The intersection is assumed to be flat and the related optional message fields are omitted, as suggested in clause 5.2.4. In addition, for the stationary objects, the related optional message fields are omitted, as suggested in clause 5.2.4. Based on these, the Unaligned Packed Encoding Rule (UPER) encoded byte sizes per object are as follows:
    - 2D VRU Stationary: 19 bytes/2D VRU in motion: 27 bytes
    - 2D Bicycle Stationary: 19 bytes/2D Bicycle in motion: 26 bytes
    - 2D Vehicle Stationary: 25 bytes/2D Vehicle in motion: 43 bytes

- The vehicles transmitting BSMs are not included in SDMSs, as defined in SAE J3224 [12]. Therefore, when x% of vehicles at intersection are C-V2X equipped (i.e., x% of C-V2X penetration rate), the SDSM packet size is calculated as
  - SDSM packet Size = 170 + (1 – x/100)*(40*43 + 24*25) + (5*19 + 5*27) + 74 bytes

Table 6: SDSM packet size in SDSM simulation

C-V2X penetration (%)	C-V2X vehicle density (vehs/km)	SDSM packet size with certificate (bytes)
20	128	2120 B (2350 B according to calculation)
50	320	1634 B
90	576	721 B

B.1.3 Impact of SDSM on BSM and SPAT

- Impact on BSM

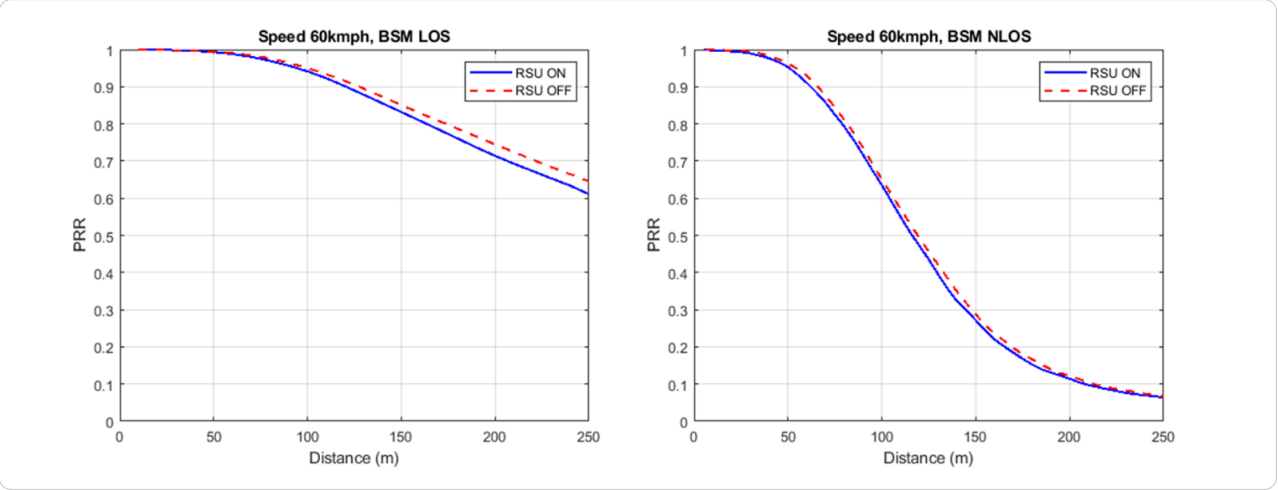


Figure 14: Impact on BSM with 20% C-V2X Penetration (128 vehicles/km)

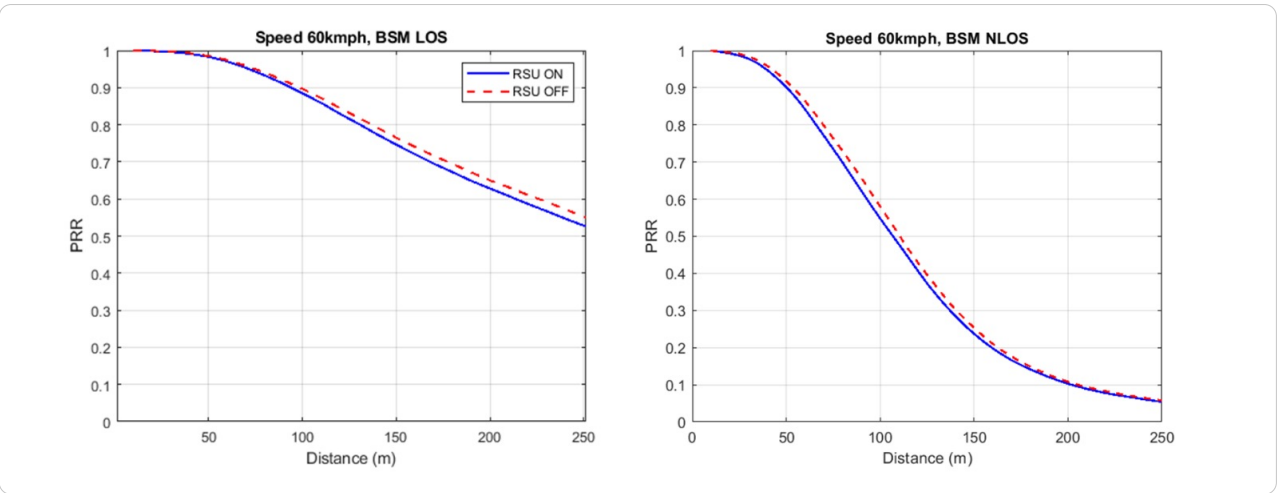


Figure 15: Impact on BSM with 50% C-V2X Penetration (320 vehicles/km)

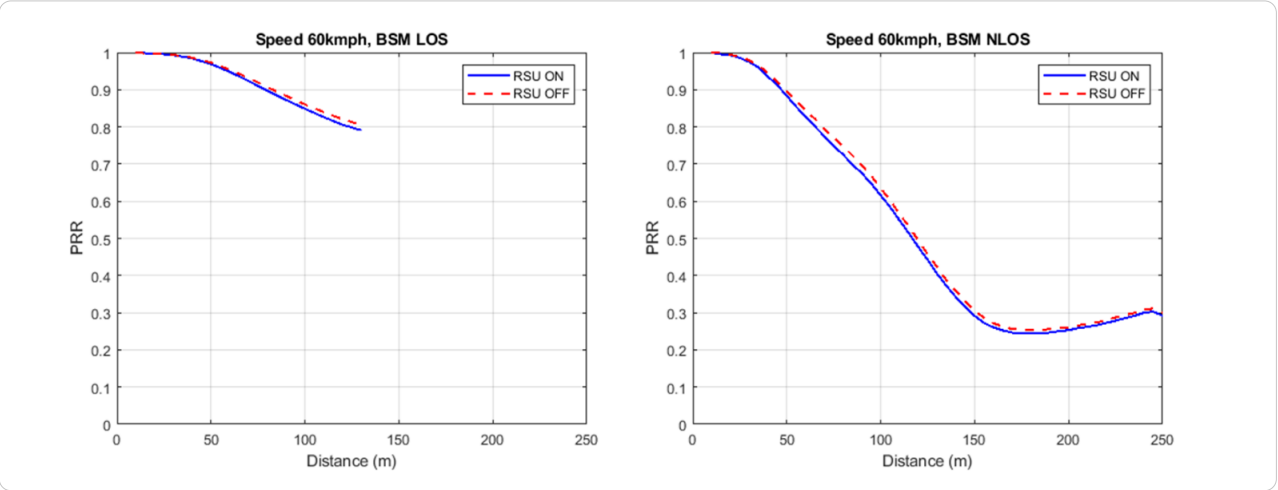


Figure 16: Impact on BSM with 90% C-V2X Penetration (576 vehicles/km)

The results show that there is no significant impact on the PRR of the BSMs due to SDSM traffic for the three different C-V2X penetrations.

- Impact on SPAT

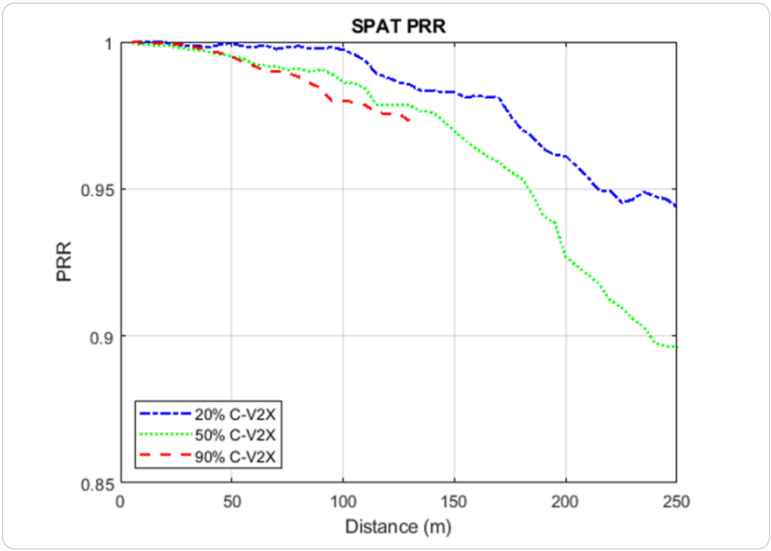


Figure 17: Impact on SPAT

As expected, the SPAT PRR degrades as the C-V2X penetration rate increases (higher interference from BSMs). However, the SPAT PRR remains high (> 0.95 at 100 meters range even with 90% C-V2X penetration rate).

B.1.4 SDSM performance

- In terms of PRR

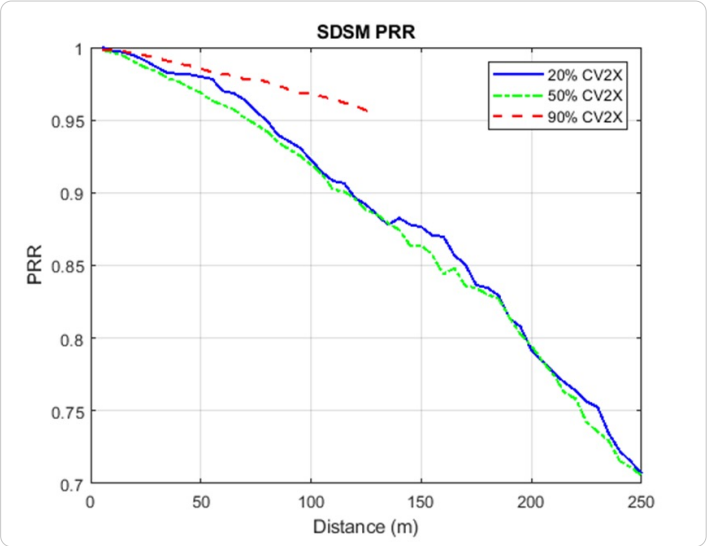


Figure 18: PRR of SDSM

As the C-V2X penetration rate increases, the SDSM packet size decreases but the interference due to BSMs increases. It is shown that the SDSM PRR slightly worsens as C-V2X penetration rate increases from 20% to 50% due to the increased interference from BSMs, and then improves as C-V2X penetration rate increases from 50% to 90% due to the decreased SDSM packet size.

- In terms of IPG

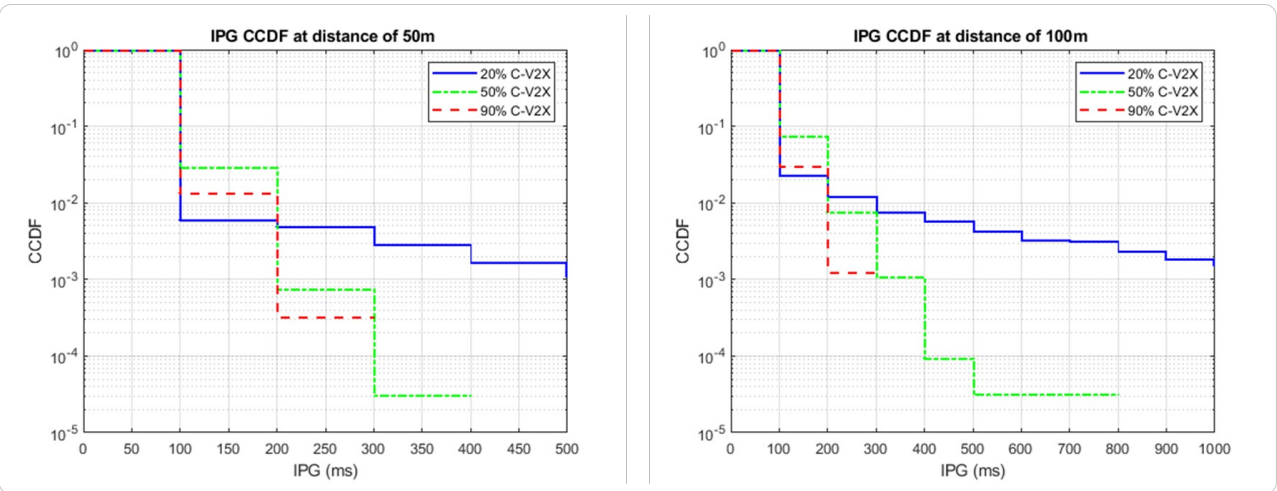


Figure 19: IPG of SDSM

For a 100 ms IPG requirement, 20% C-V2X (lesser interference) is the best. For >300 ms IPG requirement, 90% C-V2X penetration rate (smaller packet size) is the best.

B.1.5 Supportable maximum SDSM packet size

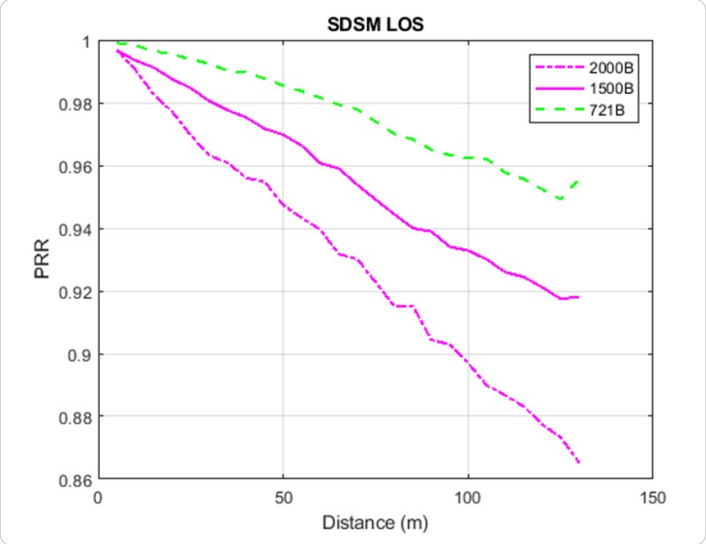


Figure 20: PRR of SDSM for different packet sizes at 90% C-V2X penetration rate

The aim of this simulation is to determine the maximum packet size that can be supported for SDSM at 90% C-V2X penetration rate. Considering a performance requirement of at least 90% PRR at a range of 100 m, the maximum packet size for SDSM that can be supported is approximately 2000 bytes.

B.1.6 Summary

- There is largely no significant impact on the BSM and SPAT due to SDSM traffic for the different C-V2X penetration rates: 20%, 50%, and 90%.
- SDSM PRR is a function of C-V2X penetration. At higher C-V2X penetration, more vehicles transmit BSMs which could interfere more with SDSM. But the packet size of SDSM would be smaller with higher C-V2X penetration and thus improve the PRR.
- The maximum SDSM packet size that can be supported even with 90% C-V2X penetration rate and a requirement of 0.9 PRR at a range of 100 m is approximately 2000 bytes.

Annex C: Examples of system-level requirements from use cases

C.1 System-level requirements for the use cases as a proxy for Unequipped Vehicles

As shown in Figure 1 in clause 4.1.1, an Infrastructure System can work as proxy for Unequipped Vehicles by sharing information about the Unequipped Road Users that the Infrastructure System's sensors detect. The following use case analysis of Left-Turn Assist, Intersection Movement Assist, and Cooperative Intersection Passing is used to develop the system-level requirements. The analysis in this clause is based on a 90-degree intersection as illustrated in Figure 21.

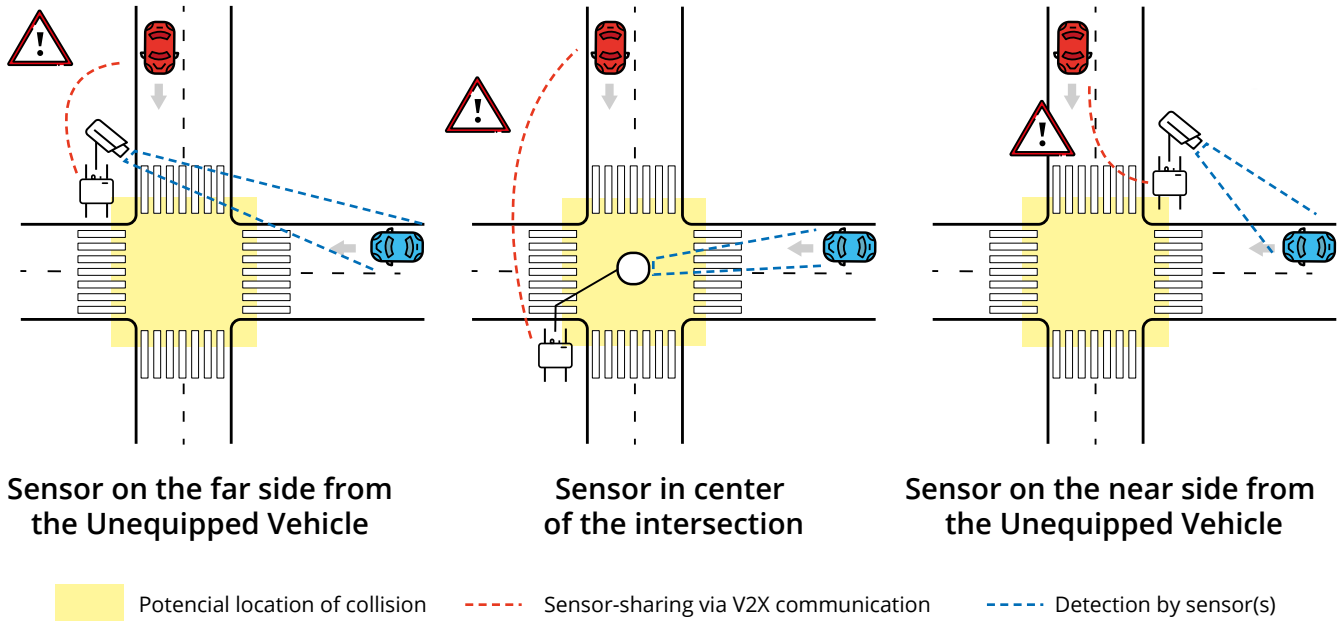


Figure 21: Detecting vehicles in an intersection

C.1.1 Assumptions

Below, the assumptions for calculating the requirements in Annexes C.1.2 and C.1.3, are derived from the specified references and practical considerations.

NOTE: The values are nominal, and infrastructure systems would need to use different values for calculating the requirements based on the different environmental conditions and assumptions, including unique geometries, surface condition (e.g., wet, dry), and reaction times. See Annex C.3 for other example assumptions.

- Traffic lane width [$d_{lanewidth}$] = 3.6 m
  - An example intersection lane width used in CTI 4501 [23]
  - Chapter 3 "Lane Width" in "Mitigation Strategies for Design Exceptions" of FHWA [24]
- Sidewalk width/safety area [$d_{sidewalk}$] = 2 m
  - An example based on the minimum width of sidewalks in "Walkways, Sidewalks, and Public Spaces" of FHWA [25]
- Dividing lane width [$d_{dividinglane}$] = 3.6 m
  - An example intersection dividing lane width used in CTI 4501 [23]
- Number of lanes of each approach leg = 8
  - See Annex C.3 for other examples of lane numbers.
- Human brake reaction time while driving [t_{react}] = 2.4 s
  - The worst-case value from Table 1 in section 2.5 of "Evaluation of Driver's Reaction Time Measured in Driving Simulator" [26]
- Object information age [t_{age}] = 0.2 s
  - It means the difference between an object's detection time and the transmission time of a sensor-sharing message containing the detected object's information (see the Figure 3).
  - The maximum object information age from SAE J3224 [12] is 200 ms.

NOTE: Lower layer delays, e.g., Packet Delay Budget (PDB), are not considered here.

- Minimum deceleration for emergency braking [a_{emerg}] = 4 m/s^2
  - A light vehicle is decelerating at a level greater than 0.4 g, described as "Hard Braking" in clause 7.234 of SAE J2735 [22].
- Maximum speed in the intersection [v_{max}] = 20 m/s (45 mph)
  - All vehicles of interest are assumed to travel at this speed.
  - See Annex C.3 for other examples of maximum speed.
- Buffer factor (mitigating the errors in all measurements) [f_{buffer}] = 1.2 (+20 %)

C.1.2 Minimum sensor range requirement

The describes a sufficient or adequate sensor range making the detection occur early enough to avoid a collision. The minimum sensor range is calculated based on the assumptions shown in Annex C.1.1. Two approaches the infrastructure system may take into account to determine the minimum sensor range are provided below.

Approach #1:

It is assumed safe if the Equipped Vehicles receive a sensor-sharing message early enough to be able to "completely stop" before the Unequipped Vehicle reaches the potential location of collision in/at the intersection.

- Distance between the sensor and the potential location of collision

$((8 * d_{lanewidth}) + d_{sidewalk} + d_{dividinglane})$ [d_{sensor}] = 34.4 m

  - In the worst case, shown in the left illustration of Figure 21, the sensor is on the far side of the intersection.
- Equipped Vehicle's braking time (v_{max} / a_{emerg}) [t_{brake}] = 5 s

- Equipped Vehicle's time to stop after receiving a sensor-sharing message

  $(t_{brake} + tr_{eact})$ $[t_{stop}]$ = 7.4 s

- Unequipped Vehicle's distance to travel after being detected to the Equipped Vehicle stopping

  $(v_{max} * (t_{stop} + t_{age}) * f_{buffer})$ $[d_{detection}]$ = 182.4 m

  - A worst-case situation is assumed where the Unequipped Vehicle does not slow down.
  - This parameter denotes the required minimum detection distance of an Unequipped Vehicle from the potential location of collision.

- Minimum sensor range

  $(d_{detection} + d_{sensor})$ $[d_{minrange}]$ = 216.8 m

If the Unequipped Vehicle is detected by the infrastructure system at the minimum sensor range $d_{minrange}$, the infrastructure system may have enough time to send the sensor-sharing message to the Equipped Vehicle and the Equipped Vehicle may have enough time to be able to process the message, actuate its brakes, and completely stop before the Unequipped Vehicle reaches the potential location of collision.

If the sensor range is greater than $d_{minrange}$, the infrastructure system and the Equipped Vehicle can have more time for message exchange and actuation. On the other hand, if the sensor range is less than $d_{minrange}$, the Equipped Vehicle will have insufficient time to completely stop before the potential location of collision.

However, it does not mean that the Equipped Vehicle will always be able to stop before reaching the potential location of collision. If the Equipped Vehicle is warned sufficiently in advance of physically reaching the intersection, the safe and correct decision might be to stop before reaching the potential location of collision. But if the Equipped Vehicle is not warned sufficiently in advance (i.e., it is too close to the intersection), a judicious decision might be to advance through the intersection before the Unequipped Vehicle reaches it. It is up to the Equipped Vehicle's discretion based on the scenario characteristics.

Approach #2:

It is assumed beneficial to safety if the Equipped Vehicles receive a sensor-sharing message early enough to be able to "react" before the Unequipped Vehicle reaches a potential location of collision in/at an intersection.

- Distance between the sensor and the potential location of collision $[d_{sensor}]$ = 34.4 m

- Unequipped Vehicle's maximum distance to travel after being detected to the human reaction within the Equipped Vehicle

  $(v_{max} * (t_{react} + t_{age}) * f_{buffer})$ $[d_{detection}]$ = 62.4 m

  - A worst-case situation is assumed where the Unequipped Vehicle does not slow down.

- Minimum sensor range

  $(d_{detection} + d_{sensor})$ $[d_{minrange}]$ = 96.8 m

C.1.3 Minimum position accuracy requirement

The position information in the sensor-sharing message should remain below the lane-level accuracy with the 2σ (95%) confidence level for intersections where there is clear sky (satellite) view.

- Maximum length of the accuracy ellipse axis ($d_{lanewidth}$ / 2) [l_{max}] = 1.8 m
- Required lateral accuracy [d_{latacc}] = 1.8 m
- Required longitudinal accuracy [d_{lonacc}] = 1.8 m

C.2 System-level requirements for the use cases as a proxy for Unequipped VRUs

As shown in Figure 1 in clause 4.1.1, an Infrastructure System can also work as a proxy for Unequipped VRUs by sharing information about the Unequipped Road Users that the Infrastructure System's sensors detect. The following use case analysis of Interactive VRU Crossing, and Vulnerable Road User Collision Warning is used to develop the system-level requirements. The analysis in this clause is based on the illustration in Figure 22.

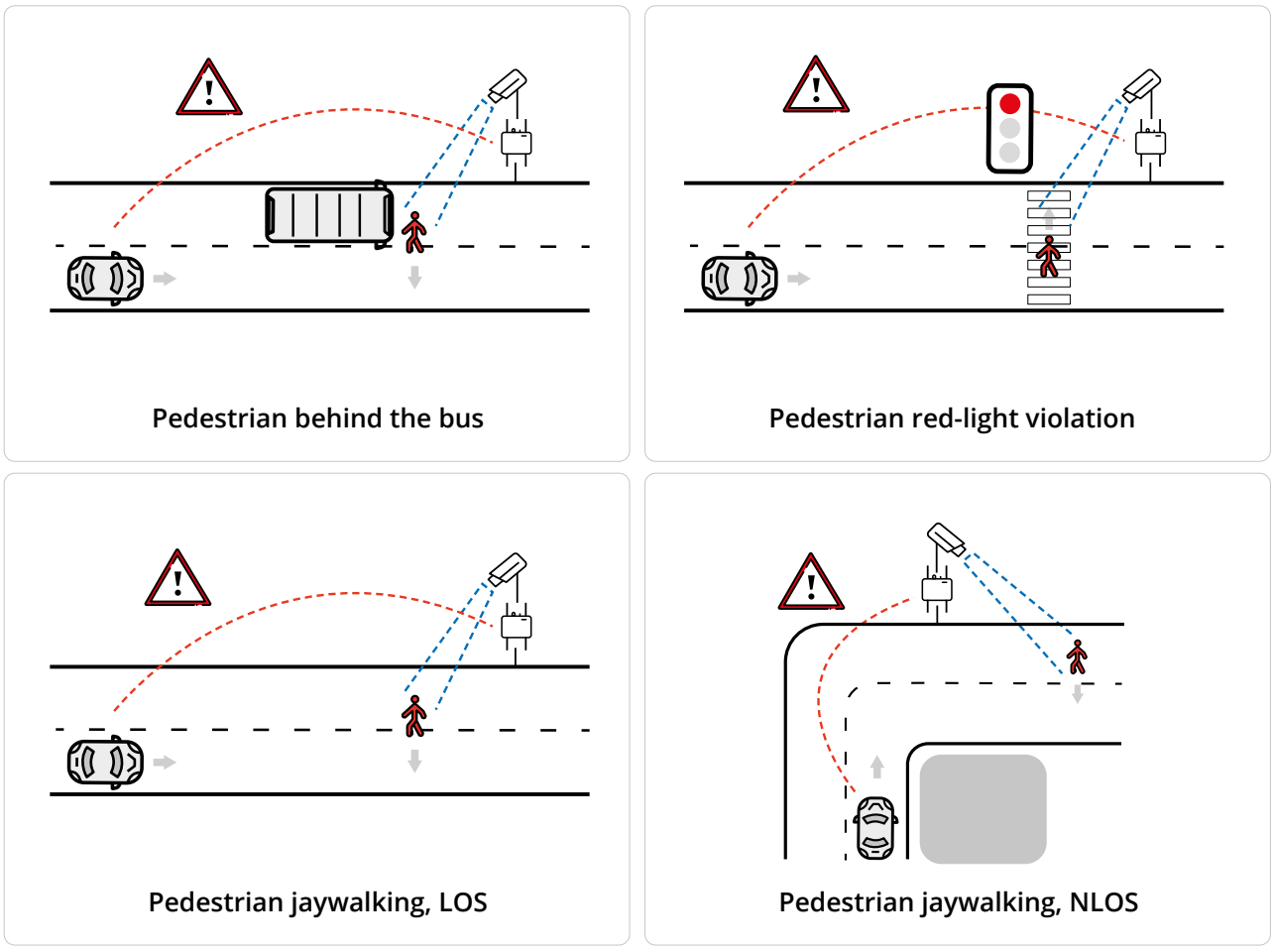


Figure 22: Detecting pedestrians on/near the road

C.2.1 Assumptions

The assumptions (additional to the Annex C.1.1) for calculating the requirements in Annexes C.2.2 and C.2.3 are provided as follows. These assumptions are derived from the specified references and practical considerations.

NOTE: The values are nominal, and Infrastructure Systems may need to use different values for calculating the requirements in light of their own assumptions. See Annex C.3 for other example assumptions.

- Maximum pedestrian walking speeds in the urban environment

  $[v_{ped}]$ = 1.83 m/s (6.0 ft/s)

  - Section 2.2.4 "Pedestrians" in the "Signalized Intersections Informational Guide" [27]

C.2.2 Minimum sensor range requirement

The minimum sensor range is calculated based on the assumptions shown in Annex C.2.1. Two approaches the Infrastructure System may take into account to determine the minimum sensor range are provided below.

Approach #1:

It is assumed safe if the Equipped Vehicles receive a sensor-sharing message early enough to be able to "completely stop" before the Unequipped VRU reaches the potential location of collision in/at the intersection.

- Distance between the sensor and the potential location of collision

  $((8 * d_{lanewidth}) + d_{sidewalk} + d_{dividinglane})$ $[d_{sensor}]$ = 34.4 m

  - Worst case (bottom right illustration in Figure 22), the sensor is on the far side of the intersection.

- Equipped Vehicle's braking time

  (v_{max} / a_{emerg}) $[t_{brake}]$ = 5 s

- Equipped Vehicle's time to stop after receiving a sensor-sharing message

  $(t_{brake} + t_{react})$ $[t_{stop}]$ = 7.4 s

- Unequipped VRU's maximum distance to travel after being detected to the Equipped Vehicle stopping

  $(v_{ped} * (t_{stop} + t_{age}) * f_{buffer})$ $[d_{detection}]$ = 16.7 m

  - A worst-case situation is assumed where the Unequipped VRU does not slow down.

- Minimum sensor range

  $(d_{sensor} + d_{detection})$ $[d_{minrange}]$ = 51.1 m

The detailed explanation on the minimum sensor-range requirements can be found in Annex C.1.2.

Approach #2:
It is assumed beneficial to safety if the Equipped Vehicles receive a sensor-sharing message early enough to be able to "react" before the Unequipped VRU reaches the potential location of collision in/at the intersection.

- Distance between the sensor and the potential location of collision
  $[d_{sensor}]$ = 34.4 m
- Unequipped VRU's maximum distance to travel after being detected to the human reaction within the Equipped Vehicle
  $(v_{ped} * (t_{react} + t_{age}) * f_{buffer})$ $[d_{detection}]$ = 5.7 m
  - A worst-case situation is assumed where the Unequipped VRU does not slow down.
- Minimum sensor range
  $(d_{detection} + d_{sensor})$ $[d_{minrange}]$ = 40.1 m

C.2.3 Minimum position accuracy requirement

The position information in the sensor-sharing message should remain below the lane-level accuracy with the 2σ (95%) confidence level for intersections where there is clear sky (satellite) view.

- Maximum length of the accuracy ellipse axis
  $(d_{lanewidth} / 2)$ $[l_{max}]$ = 1.8 m
- Required lateral accuracy $[d_{latacc}]$ = 1.8 m
- Required longitudinal accuracy $[d_{lonacc}]$ = 1.8 m

C.3 Other example assumptions for system-level requirements

The system-level requirements for the use cases regarding "Proxy for Unequipped Vehicles" and "Proxy for Unequipped VRUs" are developed in Annexes C.1 and C.2. The requirements are calculated from several examples of assumptions provided in Annexes C.1.1 and C.2.1. However, infrastructure systems may need to use different values for calculating the requirements in light of their own assumptions.

Table 7 shows several examples of the sensor distance (i.e., between the location of the sensor and the potential location of collision, and Table 8 shows examples of appropriate detection distances (i.e., required minimum detection distance of an Unequipped Vehicle from the potential location of collision as described in the Approach #1 in Annex C.1.2 and according to various speeds of the Equipped and Unequipped vehicles. These can be used to guide the deployment of the system under different conditions.

Table 7: Distance between the sensor and the potential location of collision

Number of lanes in each direction	2	4	8
Sensor distance	12.8 m	20.0 m	**34.4 m**

Table 8: Detection distance of an Unequipped Vehicle from the potential location of collision

Detection distance		Equipped vehicle speed				
		10 m/s	15 m/s	20 m/s	25 m/s	30 m/s
Unequipped Vehicle speed	10 m/s	61.2 m	91.8 m	122.4 m	153.0 m	183.6 m
	15 m/s	76.2 m	114.3 m	152.4 m	190.5 m	228.6 m
	20 m/s	91.2 m	136.8 m	**182.4 m**	228.0 m	273.6 m
	25 m/s	106.2 m	159.3 m	212.4 m	265.5 m	318.6 m
	30 m/s	121.2 m	181.8 m	242.4 m	303.0 m	363.6 m

Annex D: Deployment options of InterSafe Service using cellular network-based communication

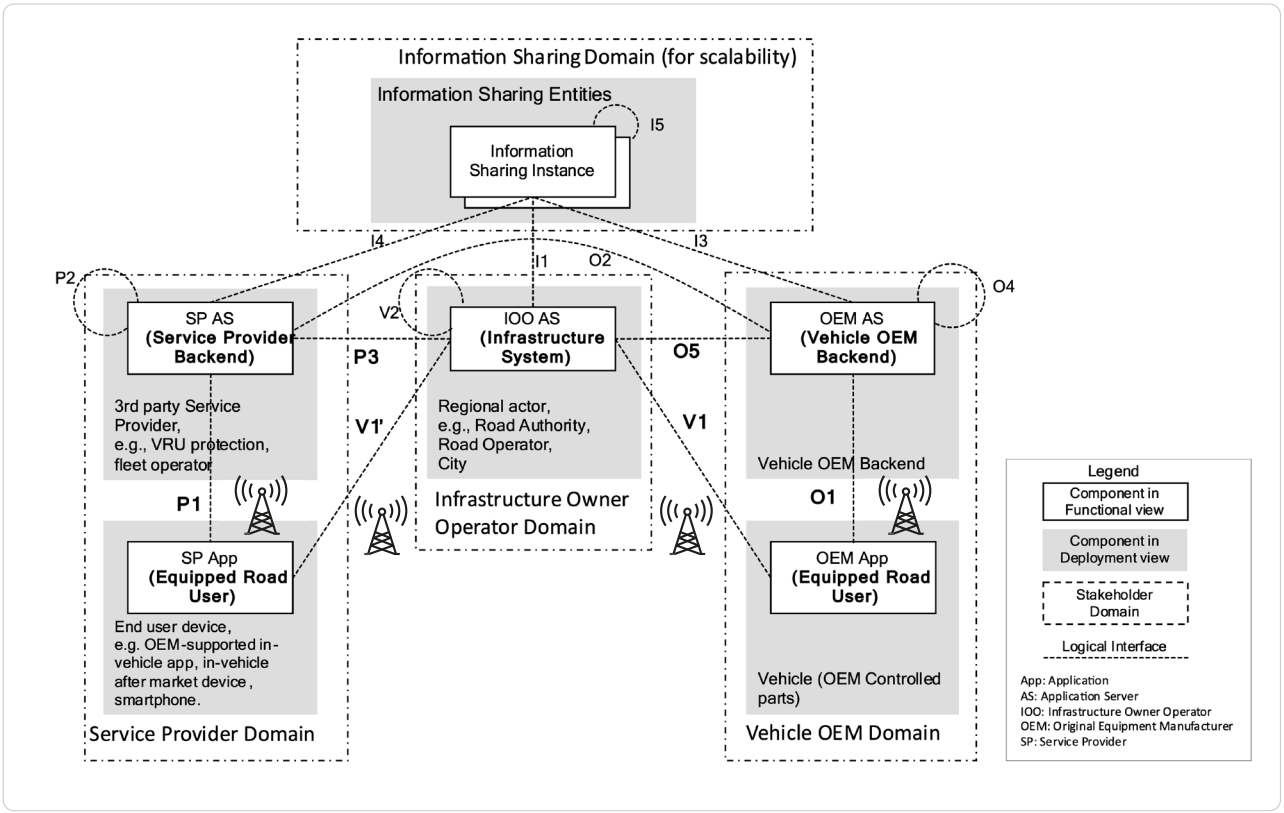


Figure 23: InterSafe Service deployment options using cellular network communications [32]

Multiple InterSafe Service deployment options using the cellular networks and backend communication are illustrated in Figure 23. There are mainly two types of deployment options depending on the interface, from which the Equipped Road User receives the sensor data, as described below.

1) V1/V1' Interface Option

The sensor data is communicated between the Infrastructure System and the Equipped Road User without going through the backend systems of a car OEM or a SP. This option requires a harmonized interface implementation profile to enable interoperable InterSafe Service among Infrastructure Systems and Equipped Road Users, especially when the Equipped Road Users travel may need to communicate with different Infrastructure Systems managed by different infrastructure operators and owners.

2) O1/P1 Interface Option

The Equipped Road User receives sensor data from its backend, which can be the car OEM or SP backend. The car OEM backend obtains sensor data from the Infrastructure System using the O5 interface and sends it to the Equipped Road User via the O1 interface. Similarly, the SP backend obtains the sensor data using the P3 interface and sends it to the Equipped User using the P1 interface. The O5 and P3 interfaces benefit from a harmonized interface implementation profile based on the IP unicast communication. The owner of the car OEM domain can decide the implementation solution of the O1 interface between the vehicle and its backend within its domain. There is no need to agree on a single implementation profile among different car OEMs for the vehicle to OEM backend interface. The same applies for the SP-managed interface between the service client and its own backend, i.e., P1 interface. When this deployment option is chosen, interoperability of InterSafe Service among different Infrastructure Systems, vehicle OEMs, and SPs can be achieved by interconnecting their backend systems and harmonizing the application (facilities) layer messages, service-triggering conditions, data-quality requirements, etc.

The Information Sharing Domain and related interfaces (I1, I3, I4 and I5) in Figure 23 are to enable scalable deployment for information sharing when the number of interconnected ecosystem stakeholders increases. This domain is not directly related to the sensor-data communications in the InterSafe Service. Therefore, the technical details are not described in this document. Interested readers can refer to the 5GAA V2N2X Technical Report [32].

Annex E: Change history

Date	Meeting	TDoc	Subject/Comment
2022-12	Call#1	T-XXX	V0.00 Initial skeleton draft
2024-10	F2F#32	T-XXX	V1.00 Final version

The 5G Automotive Association (5GAA) is a global, cross-industry organization of 120 members, including leading global automakers, Tier-1 suppliers, mobile operators, semiconductor companies, and test equipment vendors. 5GAA members work together to develop end-to-end solutions for future mobility and transport services. 5GAA is committed to helping define and develop the next generation of connected mobility, automated vehicles, and intelligent transport solutions based on C-V2X. For more information, please visit https:/5gaa.org


5GAA
Automotive Association