



SURFACE VEHICLE STANDARD

J3292™

APR2026

Issued

2026-04

Automated Vehicle Marshalling System

RATIONALE

This standard is essential for establishing a common framework to support data interoperability for Infrastructure Assisted Automated Vehicle Marshalling. The Automated Vehicle Marshaling (AVM) System will enable SAE Level 4 driving capabilities in controlled geofenced private environments and at controlled speeds utilizing infrastructure-assisted sensing.

TABLE OF CONTENTS

1.	SCOPE.....	7
2.	REFERENCES.....	8
2.1	Applicable Documents	8
2.1.1	SAE Publications.....	8
2.1.2	IEEE Publications.....	9
2.1.3	ISO Publications.....	9
2.1.4	ETSI Publications.....	9
2.1.5	5GAA Publications	10
2.1.6	VDA Publications	10
2.1.7	AUTOSAR Publications	10
3.	DEFINITIONS	10
4.	ABBREVIATIONS	13
5.	CONCEPT OF OPERATIONS.....	16
5.1	AVM Controlled Geofenced Environment ODD	16
5.2	AVM Use Cases	17
5.2.1	Plant Marshalling.....	17
5.2.2	Depot Marshalling	17
5.2.3	Valet Parking.....	17
5.2.4	Electric Vehicle Charging.....	17
5.3	AVM System Reference Architecture	18
5.4	AVM System Wireless Logical Architecture.....	22
5.5	AVM System Wireless Protocol Stack	22
5.5.1	Direct LTE-V2X Protocol Stack.....	22
5.5.2	Network-Based Protocol Stack	23
5.6	AVM Feature Flow	24
5.7	AVM State Flow	26
5.8	AVM Reference Point, Coordinate System, and Curvature.....	28
5.9	AVM Scenario	30

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

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

Copyright © 2026 SAE International

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

TO PLACE A DOCUMENT ORDER: Tel: 1-877-606-7323 (U.S. and Canada only)
Tel: 1-724-776-4970 (outside U.S. and Canada)
Fax: 724-776-0790
Email: CustomerService@sae.org
http://www.sae.org

SAE WEB ADDRESS:

Full document details: SAE J3292™ APR2026 Automated Vehicle Marshalling System

For more information on this standard, visit https://www.sae.org/standards/content/J3292_202604/

Documents

Standard, visit Sharing Hub

5.10	Security Needs	30
5.10.1	Direct (LTE-V2X) Wireless Communications	31
5.10.2	Network-Based Wireless Communications	32
6.	REQUIREMENTS	33
6.1	Requirements Documentation Overview	33
6.1.1	Requirements Details and Notation	33
6.1.2	Requirements Tables	34
6.1.3	Minimum Content Requirements	34
6.2	Data Exchange Requirements	36
6.2.1	Infrastructure Marshalling Message (IMM)	36
6.2.2	Vehicle Marshalling Message (VMM)	91
6.2.3	Common Shared Data for IMM and VMM	143
6.3	Operational Requirements	164
6.3.1	Infrastructure Marshalling Message (IMM)	164
6.3.2	Vehicle Marshalling Message (VMM)	181
6.3.3	Common Shared Data for IMM and VMM	203
6.4	Timestamp	207
6.4.1	Timestamp Reference	207
6.4.2	Timestamp Confidence Reference	208
6.5	Rolling Counter	208
6.6	Functional Safety End-to-End Protection	209
6.6.1	Computation	211
6.6.2	Verification	215
6.7	Vehicle Identification	219
6.7.1	Blinking	220
6.8	Driving Permission Requirements	225
6.8.1	Accuracy Requirements	230
6.9	Pose	233
6.9.1	Pose Requirements	233
6.9.2	Detected Vehicle Pose Requirements	236
6.10	Vehicle Motion Control Interface	238
6.10.1	Path Control (Type 2.1) Requirements	238
6.10.2	Trajectory Control	246
6.11	Wireless Message Communication Interface	262
6.11.1	Wireless Communications Handshaking Common Configurations	263
6.11.2	Network-Based Wireless Communications	265
6.11.3	Direct LTE-V2X Wireless Communications	274
6.12	AVM Feature Flow and State Flow Transitions	283
6.12.1	Un-initiated	283
6.12.2	Activation	284
6.12.3	Identification	287
6.12.4	Automated-Control	290
6.12.5	Unavailable	294
6.12.6	Deactivation	297
6.13	Parameter Settings	299
7.	SYSTEM DESIGN	303
7.1	Sequence Flow Diagrams	303
7.1.1	Activation Feature Flow	303
7.1.2	Identification Feature Flow	304
7.1.3	Automated-Control Feature Flow	306
7.1.4	Unavailable Feature Flow	307
7.1.5	Deactivation Feature Flow	308
7.2	Security Certificates	308
7.2.1	Network-Based	308
7.2.2	Direct (LTE-V2X)	313

8.	ASN.1 ENTITIES	317
8.1	IMM ASN.1	317
8.1.1	Message Frame Structure	317
8.1.2	Message Version: DE_IMMMessageVersion	328
8.1.3	Object Definitions	328
8.2	VMM ASN.1	370
8.2.1	Message Frame Structure	370
8.2.2	Message Version: DE_VMMMessageVersion	381
8.2.3	Object Definitions	381
8.3	AVM Common Shared Data for IMM ASN.1 and VMM ASN.1	432
8.3.1	Imports from SAE J2735	432
8.3.2	Object Definitions	435
9.	NOTES	451
9.1	Revision Indicator	451
APPENDIX A	SAE J2735 EDITING INSTRUCTIONS [NORMATIVE]	452
APPENDIX B	CONFIGURATIONS [NORMATIVE]	453
APPENDIX C	END-TO-END (E2E) LATENCY [NORMATIVE]	458
APPENDIX D	TIMESTAMP IMPLEMENTATION [NORMATIVE]	460
APPENDIX E	VEHICLE IDENTIFICATION [NORMATIVE]	466
APPENDIX F	FUNCTIONAL SAFETY END-TO-END PROTECTION IMPLEMENTATION EXAMPLE [NORMATIVE]	469
APPENDIX G	SAMPLE MESSAGES PAYLOAD [NORMATIVE]	476
APPENDIX H	LTE-V2X PROFILES OPTIMAL CONFIGURATION [INFORMATIVE]	503
Figure 1	Illustration for any general AVM controlled geofenced environment ODD	16
Figure 2	AVM system reference architecture	21
Figure 3	AVM system wireless logical architecture (network-based and direct wireless technologies)	22
Figure 4	Direct LTE-V2X protocol stack	23
Figure 5	Network-based protocol stack	23
Figure 6	AVM feature flow diagram	24
Figure 7	AVM feature flow and state flow diagram	27
Figure 8	AVM coordinate system, reference point diagram, and curvature	29
Figure 9	AVM system scenario logical overview	30
Figure 10	IMM and VMMs rolling counter handshake flow diagram	209
Figure 11	Functional safety end-to-end protection - Computation algorithm flow steps	215
Figure 12	Functional safety end-to-end protection - Verification algorithm flow steps	219
Figure 13	Blinking code computation and verification algorithm flow steps at AVM CS	222
Figure 14	Blinking code verification and algorithm flow steps at AV	225
Figure 15	Driving permission scenarios	229
Figure 16	Driving permission data field ASN structure overview	230
Figure 17	Pose ASN structure overview	234
Figure 18	Detected Vehicle Pose ASN structure overview	237
Figure 19	AVM path control diagram	241
Figure 20	controlInterface->pathControl ASN structure overview	242
Figure 21	AVM trajectory control-acceleration diagram	249
Figure 22	controlInterface->trajectoryControl with trajectoryControlAcceleration ASN structure overview	250
Figure 23	AVM trajectory control-acceleration-state diagram	254
Figure 24	controlInterface->trajectoryControl (controlTrajectory and stateTrajectory) ASN structure overview	255
Figure 25	AVM trajectory control-velocity diagram	259
Figure 26	controlInterface->trajectoryControl with controlVelocity ASN structure overview	260
Figure 27	AV and AVM CS communicating over network-based wireless communications system diagram	265
Figure 28	Messages (IMM and VMM) exchange overview of network-based wireless communications	274
Figure 29	RSE (interfaced with AVM CS) and AV communicating over direct (LTE-V2X) wireless communications system diagram	274

Figure 30	un-initiated.unknown transition diagram	284
Figure 31	activation.inactive transition diagram	285
Figure 32	activation.processing transition diagram	285
Figure 33	activation.active transition diagram	286
Figure 34	identification.initialize/initializing transition diagram	287
Figure 35	identification.identify/identifying transition diagram	288
Figure 36	identification.ready transition diagram	289
Figure 37	automated-control.standby transition diagram	290
Figure 38	automated-control.drive transition diagram	291
Figure 39	automated-control.pause transition diagram	292
Figure 40	automated-control.temp-error transition diagram	293
Figure 41	unavailable.sleep transition diagram	294
Figure 42	unavailable.suspend transition diagram	295
Figure 43	unavailable.recovery transition diagram	296
Figure 44	deactivation.active transition diagram	297
Figure 45	deactivation.processing transition diagram	298
Figure 46	deactivation.inactive transition diagram	299
Figure 47	Activation feature flow handshake sequence diagram for single AV using IMM and VMM	303
Figure 48	Identification feature flow handshake sequence diagram for single AV using IMM and VMM	304
Figure 49	Automated-control feature flow handshake sequence diagram for single AV using IMM and VMM	306
Figure 50	Unavailable feature flow handshake sequence diagram for single AV using IMM and VMM	307
Figure 51	Deactivation feature flow handshake sequence diagram for single AV using IMM and VMM	308
Figure 52	Security scope system diagram for network-based wireless communications	309
Figure 53	Security certificate chain system diagram for network-based wireless communications	310
Figure 54	Infrastructure Marshalling Message ASN.1 structure overview	318
Figure 55	Vehicle Marshalling Message ASN.1 structure overview	371
Table 1	Individual requirements table template	34
Table 2	Minimum content table template	35
Table 3	Minimum infrastructure marshalling message frame content	36
Table 4	Minimum infrastructure marshalling message content	37
Table 5	Minimum vehicle container blob content	38
Table 6	Minimum vehicle container data content	40
Table 7	Minimum IMM data management data E2EProtection data content	42
Table 8	Minimum IMM data management content	43
Table 9	Minimum AVM CS identity management E2EProtection content	45
Table 10	Minimum AVM CS IMM identity management data content	46
Table 11	Minimum feature flow command E2EProtection content	47
Table 12	Minimum feature flow command data content	48
Table 13	Minimum vehicle identification command data E2EProtection content	49
Table 14	Minimum vehicle identification content	49
Table 15	Minimum blinking data content	50
Table 16	Minimum driving permission E2EProtection content	52
Table 17	Minimum driving permission content	53
Table 18	Minimum TimeSync IMM AV MCS request E2EProtection data content	55
Table 19	Minimum safety TimeSync IMM AV MCS request content	56
Table 20	Minimum TimeSync VMM AV response E2EProtection data content	57
Table 21	Minimum safety time sync VMM AV response content	58
Table 22	Minimum safety profile request E2EProtection content	61
Table 23	Minimum safety profile content	62
Table 24	Minimum AVM CS control command E2EProtection content	64
Table 25	Minimum AVM CS control command content	65
Table 26	Minimum infrastructure error E2EProtection data content	70
Table 27	Minimum infrastructure error content	71
Table 28	Minimum detected vehicle pose E2EProtection data content	73
Table 29	Minimum detected vehicle pose content	74

Table 30	Minimum control interface E2EProtection data content.....	76
Table 31	Minimum control interface content	77
Table 32	Minimum path control content	78
Table 33	Minimum path snippet content	79
Table 34	Minimum way point content	80
Table 35	Minimum trajectory control content	82
Table 36	Minimum control trajectory content	84
Table 37	Minimum control point content	85
Table 38	Minimum control parameter content	86
Table 39	Minimum control acceleration content	87
Table 40	Minimum control velocity content.....	88
Table 41	Minimum state trajectory content	89
Table 42	Minimum state point content	90
Table 43	Minimum vehicle marshalling message frame content	91
Table 44	Minimum vehicle marshalling message content	92
Table 45	Minimum VMM data content	93
Table 46	Minimum VMM data management data E2EProtection data content.....	95
Table 47	Minimum VMM data management content	96
Table 48	Minimum feature flow command response E2EProtection data content	99
Table 49	Minimum feature flow command response data content	100
Table 50	Minimum AV identity management E2EProtection data content	101
Table 51	Minimum AV identity management data content	102
Table 52	Minimum vehicle control interface preference E2EProtection data content	103
Table 53	Minimum vehicle control interface preference data content	104
Table 54	Minimum vehicle state E2EProtection data content	105
Table 55	Minimum vehicle state content.....	106
Table 56	Minimum vehicle identification command response data E2EProtection data content	112
Table 57	Minimum vehicle identification command response content.....	113
Table 58	Minimum AV blinking content.....	114
Table 59	Minimum TimeSync VMM AV request E2EProtection data content	116
Table 60	Minimum safety TimeSync VMM AV request content.....	116
Table 61	Minimum TimeSync IMM AVMCS response E2EProtection content.....	117
Table 62	Minimum safety TimeSync IMM AVMCS response content	118
Table 63	Minimum safety profile response E2EProtection data content	121
Table 64	Minimum safety profile response data content	122
Table 65	Minimum vehicle error E2EProtection data content.....	123
Table 66	Minimum vehicle error content.....	124
Table 67	Minimum vehicle safety feedback E2EProtection data content.....	126
Table 68	Minimum vehicle safety feedback content	127
Table 69	Minimum vehicle properties E2EProtection data content	130
Table 70	Minimum vehicle properties content	131
Table 71	Minimum AVM end-to-end protection content	144
Table 72	Minimum feature flow data content	145
Table 73	Minimum lights pattern data content	146
Table 74	Minimum AVM DateTime data content	147
Table 75	Minimum time confidence data content	149
Table 76	Minimum identity management data content	150
Table 77	Minimum direction indicator data	151
Table 78	Minimum motor system data content	152
Table 79	Minimum pose content	153
Table 80	Minimum centimeter data content	154
Table 81	Minimum high resolution curvature data content	155
Table 82	Minimum radians per second data content	155
Table 83	Minimum velocity component value data content	156
Table 84	Minimum vehicle odometer current value data content	157
Table 85	Minimum interval data content	157
Table 86	Minimum message interval data content	158
Table 87	Minimum rolling counter data content.....	159
Table 88	Minimum proprietary extension field data content	159
Table 89	Minimum way point index data content.....	160

Table 90	Minimum AVM error description data content.....	161
Table 91	Minimum challenge data content	161
Table 92	Minimum expected clock drift data content.....	162
Table 93	Minimum custom code data content	163
Table 94	Minimum cartesian angle value data content.....	163
Table 95	10 MHz low speed (<120 km/h)	278
Table 96	LTE-V2X SSP overview for IMM and VMMs.....	281
Table 97	Parameters settings for AVM system.....	299
Table 98	Blinking command - Command response	305
Table 99	Certificate profile for network-based wireless communication.....	311
Table 100	Security profile for direct (LTE-V2X) wireless communication: IMM sending	313
Table 101	Security profile for direct (LTE-V2X) wireless communication: IMM receiving	314
Table 102	Security profile for direct (LTE-V2X) wireless communication: IMM security management	315
Table 103	Security profile for direct (LTE-V2X) wireless communication: VMM sending.....	315
Table 104	Security profile for direct (LTE-V2X) wireless communication: VMM receiving.....	316
Table 105	Security profile for direct (LTE-V2X) wireless communication: VMM security management.....	317

1. SCOPE

The scope of this standard is Automated Vehicle Marshalling (AVM) of vehicles to enable remote control functionality for achieving SAE Level 4 (High Driving Automation according to the Surface Vehicle Recommended Practice SAE J3016) driving capabilities at controlled speeds within geofenced private controlled environments utilizing infrastructure-assisted sensing. It specifies a concept of operations which includes a reference-system architecture and use cases, system functional and performance requirements, multiple wireless communications protocols, and associated wireless messages to support AVM. AVM use cases such as plant marshalling, depot marshalling, valet parking, electric vehicle charging, etc.

The Automated Vehicle Marshalling Central Server (AVM CS) infrastructure does detect objects, vehicles, vulnerable road users, and any obstructions that help guide the Automated Vehicle (AV) starting from uninitiated, activation, identification, automated control, unavailable and deactivation states of the respective feature lifecycle of AVM use cases by using only two wireless messages named Infrastructure Marshalling Message (IMM) and Vehicle Marshalling Message (VMM).

This standard specifies the minimum requirements for the Vehicle-to-Everything (V2X) messages, such as IMM and VMM, and the corresponding data frames and elements which are defined to support Infrastructure guided AVM use cases over Direct (LTE-V2X) and Network-based wireless communications technologies. These messages are utilized to achieve desired interoperability, safety, and data integrity.

This standard focuses on an infrastructure-led implementation of an AVM system analogue to a Type 2 Automated Vehicle Parking (AVP) system implementation as described in International Organization for Standardization (ISO) 23374-1; the functional allocations listed below are part of the Type 2 AVP System where AVM CS of infrastructure carries out most of the operation functions including AV Identification and Emergency Stopping:

- Destination Assignment
- Route Planning
- Object and Event Detection and Response (OEDR)
- AV Localization
- Path Determination
- Trajectory Calculation
- Vehicle Motion Control (VMC)

NOTE 1: Functional Safety rating Automotive Safety Integrity Level (ASIL) related requirements are outside the scope of this standard.

NOTE 2: This standard could be utilized as a base for human operator assisted AVM. The implementation details from human operator assistance without Infrastructure assistance is outside the scope of this standard.

NOTE 3: Unless otherwise marked as Informative, all material in this standard is to be considered normative.

2. REFERENCES

2.1 Applicable Documents

The following publications form a part of this specification to the extent specified herein. Unless otherwise indicated, the applicable issue of SAE, IEEE, ISO, ETSI, 5GAA, VDA, and AUTOSAR publications shall apply.

2.1.1 SAE Publications

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

SAE J2735	V2X Communications Message Set Dictionary
SAE J2945	Dedicated Short Range Communication (DSRC) Systems Engineering Process Guidance for SAE J2945/X Documents and Common Design Concepts™
SAE J2945/A	Minimum Requirements for Road Geometry and Attributes Definition
SAE J2945/1	On-Board System Requirements for V2V Safety Communications
SAE J2945/5	Service Specific Permissions and Security Guidelines for Connected Vehicle Applications
SAE J3016	Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles
SAE J3161	LTE Vehicle-to-Everything (LTE-V2X) Deployment Profiles and Radio Parameters for Single Radio Channel Multi-Service Coexistence
SAE J3161/1	Onboard System Requirements for LTE-V2X V2V Safety Communications
SAE J3161/2	LTE Vehicle-to-Everything (LTE-V2X) Deployment Profiles and Radio Parameters for PC5 Interface in 10 MHz Channel 180
SAE J3268	Listing of Provider Service Identifiers and Associated Application Technical Reports
SAE J3289	SAE V2X ASN.1 Modules - Organization and Management Rules

2.1.2 IEEE Publications

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

Please note that this report incorporates certain IEEE specifications by reference. ESSENTIAL IPRs (Intellectual Property Rights) have been declared to IEEE. All information statements and licensing declarations of ESSENTIAL IPRs received by IEEE are publicly available via the IEEE IPR Online Database found at <https://standards.ieee.org/about/sasb/patcom/patents/>.

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

2.1.3 ISO Publications

Copies of these documents are available online at www.iso.org/store.

ISO 23374-1	Intelligent transport systems — Automated valet parking systems (AVPS) — Part 1: System framework, requirements for automated driving and for communications interface
ISO 23374-2	Intelligent transport systems — Automated valet parking systems (AVPS) — Part 2: Security integration for type 3 AVP
ISO 21448	Road vehicles — Safety of the intended functionality
ISO 21177	Intelligent transport systems — ITS station security services for secure session establishment and authentication between trusted devices
ISO 9594-8	Information technology — Open systems interconnection — Part 8: The Directory: Public-key and attribute certificate frameworks

2.1.4 ETSI Publications

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

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

ETSI TS 103 882 V2.1.1	Intelligent Transport Systems (ITS); Automated Vehicle Marshalling (AVM); (Release 2)
------------------------	---

2.1.5 5GAA Publications

Available from 5GAA, Head Office Neumarkter, Str. 21 81673, Munich, Germany, Tel: +49 89 54909680, www.5gaa.org.

5GAA T-20002 Automated Valet Parking Technology Assessment and Use Case Implementation Description; System Architecture, Cellular Network and PC5 Direct Communication Solutions

2.1.6 VDA Publications

Available from VDA, Behrenstrasse 35, 10117 Berlin, Germany, Tel: +49 30 897842-0, www.vda.de.

avp-operation-interface-3.0.1 Automated Valet Parking Operation Interface Implementation Profile and Requirements

2.1.7 AUTOSAR Publications

Available from AUTOSAR, Niederfeldstrasse 18, 85413 Hörgertshausen, Germany, Tel: +49 87 64 78 93 99 40, www.autosar.org.

Autosar ID 849, R22-11 Autosar Standard: Foundation - E2E Protocol Specification

Autosar ID 016, R21-11 Autosar Standard: Classic Platform - Specification of CRC Routines

3. DEFINITIONS

Cited in this section are the definitions that apply to this standard.

3.1 AUTOMATED VEHICLE MARSHALLING (AVM)

Represents a system and its components that enable vehicles to be maneuvered and marshalled in a controlled environment at an AVM facility.

3.2 AVM FACILITY

Facility which is capable of conducting and supporting the Automated Vehicle operations.

3.3 AUTOMATED VEHICLE (AV)

Automated Vehicle equipped with Automated Vehicle Marshalling (AVM) capability and guided by AVM CS infrastructure system within a controlled environment (AVM facility). The AV executes software that generates wireless messages for transmission according to the requirements in this standard and controls the vehicle maneuvers in response to AVM CS infrastructure commands.

3.4 AUTOMATED VEHICLE MARSHALLING CENTRAL SERVER (AVM CS)

Provides the core logical interface information received from the Automated Vehicle Marshalling Sensors Infrastructure (AVM SI) to the Automated Vehicle (AV) and is responsible for calculating vehicle maneuvers, vehicle identification, automated vehicle operation of the AV within a controlled environment at an AVM facility over the respective wireless communication interfaces being communicated by AV with AVM CS.

3.5 AUTOMATED VEHICLE MARSHALLING SENSORS INFRASTRUCTURE (AVM SI)

AVM SI which provides sensors information to AVM CS to perform the localization functions such as perception, path-planning, detection, controls, and response of the AV synchronized within the AVM coordinate system.

3.6 AUTOMATED VEHICLE MARSHALLING SYSTEM OPERATOR (AVM SO)

Manages/supervises the automated vehicle marshalling during the safe vehicle identification process, at the individual locations/stations, and with overall supervision via in-facility interfaces.

3.7 AUTOMATED VEHICLE CLOUD BACKEND (AV CB)

AV's cloud responsible for remote engagement/disengagement, configurations that are used for Identification, Functional Safety, Safety Profile, Network-based wireless communications, Direct LTE-V2X wireless communications, Network-based security, Direct LTE-V2X security certificates management/dissemination of the respective AV during feature Activation, feature Operational, and feature Deactivation within the AVM system.

3.8 DIRECT WIRELESS COMMUNICATION

Direct Wireless Communication utilizes LTE-V2X PC5, a cellular technology enabling direct communication between vehicles and other entities (Infrastructure, Pedestrian) without relying on cellular network infrastructure.

3.9 INFRASTRUCTURE MARSHALLING MESSAGE (IMM)

An AVM message transmitted by the AVM CS to the AV that contains the information of automated vehicle operation and acknowledgement information to the respective AV.

3.10 INFRASTRUCTURE-TO-VEHICLE (I2V) COMMUNICATION

Direct or Network-based wireless communication of messages originating from AVM CS to one or more AVs.

3.11 INTER-PACKET GAP (IPG)

The time between two successive packets received.

3.12 LATENCY

Calculation of the time taken from the time of message transmission (Tx) to message reception (Rx).

3.13 MARSHALLING

It refers to the goal-oriented vehicle movement that is specifically defined and directed by the AVM CS for the purpose of achieving vehicle displacement. Essentially, it's about the planned and controlled movement of an AV to reach a specific location or complete a specific task, as orchestrated by the AVM CS.

3.14 ON-BOARD EQUIPMENT (OBE)

All required V2X equipment installed in an AV for performing required AVM and V2X communication services.

3.15 PACKET ERROR RATIO (PER)

Calculation of the number of messages lost for a given time interval when considering the total number of messages that were attempted to be exchanged between the transmitter and receiver.

3.16 REFERENCE POINT (RP)

It is a fixed origin within a Cartesian coordinate system for the controlled environment. The vehicle's position is then determined by the coordinates of the center of its rear axle relative to this fixed RP, allowing for both positive and negative values.

3.17 ROAD-SIDE EQUIPMENT (RSE)

All required V2X equipment installed at the roadside/with-in-facility for performing required AVM operations using Direct LTE-V2X wireless communications with AVs and responsible for interfacing with the AVM CS infrastructure.

3.18 TRANSMIT TIME INTERVAL (TTI)

The time interval between successive packets sent.

3.19 NETWORK-BASED WIRELESS COMMUNICATION

Network-based wireless communication refers to technologies, such as Cellular-Uu and Wi-Fi, that rely on an established and controlled infrastructure (e.g., cellular networks or access points) to facilitate communication between AVs and AVM CS.

3.20 VEHICLE-TO-INFRASTRUCTURE (V2I) COMMUNICATIONS

Direct or Network-based wireless communication of messages originating from AV to AVM CS.

3.21 VEHICLE-TO-NETWORK (V2N) COMMUNICATIONS

Network-based wireless communication between AV and AVM CS.

3.22 VEHICLE-TO-NETWORK-TO-EVERYTHING (V2N2X) COMMUNICATIONS

Indirect communication between road users and infrastructure using a host beyond the local infrastructure. V2N2X usually involves preprocessing of data by the host.

3.23 VEHICLE-TO-EVERYTHING (V2X) COMMUNICATIONS

Any LTE-V2X device which supports V2V/V2I/V2X communications flows (message exchanges).

3.24 VEHICLE MARSHALLING MESSAGE (VMM)

An AVM message transmitted by the AV to the AVM CS to update the infrastructure about its current state and acknowledged receipt of IMM messages from the AVM CS.

4. ABBREVIATIONS

Cited in this section are the abbreviations that are used in this report.

1PPS	One Pulse per Second
5GAA	5G Automotive Association
3GPP	Third Generation Partnership Project
ASN.1	Abstract Syntax Notation One
ASIL	Automotive Safety Integrity Level
AV	Automated Vehicle
AVM	Automated Vehicle Marshalling
AVP	Automated Valet Parking
CB	Cloud Backend
CS	Central Server
CA	Certificate Authority
CAN	Controller Area Network
CV	Connected Vehicle
CRC	Cyclic Redundant Check
CAMP	Crash Avoidance Metrics Partners LLC
CBR	Channel Busy Ratio
CR	Channel Occupancy Ratio
DE	Data Element
DF	Data Frame
DOT	Department of Transportation
ECU	Electronic Control Unit
E2E	End-to-End
EV	Electric Vehicle
ETSI	European Telecommunication Standard Institute
E-UTRA	Evolved Universal Mobile Telecommunications System (UMTS) Terrestrial Radio Access
FCC	Federal Communications Commission
FHWA	Federal Highway Administration
FR	Functional Requirement

GNSS	Global Navigation Satellite System
HARQ	Hybrid Automatic Repeat Request
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol Secure (HTTP + TLS)
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPv6	Internet Protocol Version 6
ITT	Inter-Transmit Time
IPG	Inter-Packet Gap
I2V	Infrastructure-to-Vehicle
IMM	Infrastructure Marshalling Message
IPR	Intellectual Property Rights
ISO	International Organization for Standardization
ITS	Intelligent Transportation Systems
MHz	Megahertz
MSG	Message
MTU	Maximum Transmission Unit
OBE	Onboard Equipment
ODD	Operational Design Domain
OEM	Original Equipment Manufacturer
OID	Object Identifier
OEDR	Object and Event Detection and Response
PC5	ProSe Communications 5
PER	Packet Error Ratio or Packet Error Rate
PSID	Provider Service Identifier
PDU	Protocol Data Unit
PDB	Packet Delay Budget
PHY	Physical Layer
PPPP	ProSe per Packet Priority

PPS	Pulse per Second
ProSe	Proximity Services
RP	Radiated Power
Rx	Receive
RF	Radio Frequency
RSE	Roadside Equipment
RSRP	Reference Signal Receive Power
RP	Reference Point
RTT	Round Trip Time
SE	Secure Element
SCMS	Security Credential Management System
SDO	Standards Developing Organizations or Standards Development Organization
SI	Sensors Infrastructure
SLSS	Sidelink Synchronization Signal
SSP	Service Specific Permissions
SPS	Semi-Persistent Scheduling
SO	System Operator
Tx	Transmit
TTI	Transmit Time Interval
TLS	Transport Layer Security
TPM	Trusted Platform Module
UE	User Equipment
UPER	Unaligned Packed Encoding Rules
U.S.	United States
UTC	Coordinated Universal Time
URL	Uniform Resource Locator
VDA	Verband der Automobilindustrie
V2X	Vehicle-to-Everything
V2N	Vehicle-to-Network
V2N2X	Vehicle-to-Network-to-Everything Communications

V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
VIN	Vehicle Identification Number
VMM	Vehicle Marshalling Message
VMC	Vehicle Motion Control
VRU	Vulnerable Road User
V&V	Verification and Validation
WAVE	Wireless Access in Vehicular Environment
WSM	WAVE Short Message
WSMP	WAVE Short Message Protocol
XOR	eXclusive OR

5. CONCEPT OF OPERATIONS

5.1 AVM Controlled Geofenced Environment ODD

The AVM controlled geofenced environment system is an SAE Level-4 (High Driving Automation according to the Surface Vehicle Recommended Practice SAE J3016) automated vehicle operation which is carried out in a controlled geofenced environment Operational Design Domain (ODD).

[Figure 1](#) provides an illustration of an AVM controlled geofenced private environment system consisting of multiple AVs that are part of a marshalling session that are being guided to maneuver from station to station and eventually to parking spots using AVM feature flows (as defined in [5.6](#)). AVs may take different pathways and rendezvous at different stations along the way.

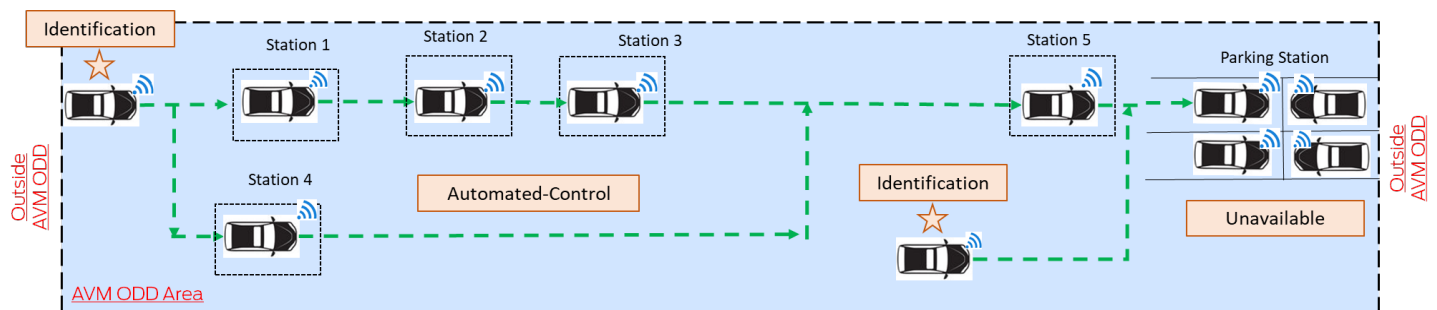


Figure 1 - Illustration for any general AVM controlled geofenced environment ODD

NOTE 1: The AVM geo-fencing Operational Design Domain (ODD) area's size is determined by AVM system implementers and is outside the scope of this standard document.

NOTE 2: The AVM CS is responsible for enforcing and restricting AVM operations to the AVM ODD area.

5.2 AVM Use Cases

The following are application use cases which are defined as part of the AVM system that fall within the realm of ISO 23374 type 2 automated vehicle operation, where vehicles are being controlled by external mounted infrastructure sensors in direct vicinity of the driving path of the AV.

All these use cases are supported within the AVM controlled geofenced environment ODD that adheres to the following requirements:

1. AVM infrastructure (i.e., the combination of AVM SI, AVM SO, and AVM CS) is responsible to detect and identify correct AVs at the right spot, assign a destination for AVs, assign route planning, perform object and event detection, determine the response of AVs, perform AV localization and path determination, perform trajectory calculation and vehicle motion control (including emergency stopping) of AVs.
2. Marshalling maneuvers occur within a geofenced area (i.e., AVM facility) and not on public roads or in areas of unbounded or undefined size.
3. AVs execute SAE Level 4 maneuvers, guided exclusively by the AVM CS using information from AVM SI and AVM SO, without any local or remote human driver input.
4. AVs and AVM CS communicate wirelessly utilizing direct (LTE-V2X) and/or network-based wireless communications between the vehicles and infrastructure in the geofenced AVM facility.
5. AV maneuvers occur at controlled speeds within the safety threshold required in the geofenced AVM facility.
6. The AVM facility can be indoors, outdoors, or a combination of both.
7. The AVM CS and AVs will perform an identification process prior to entering into the automated control marshalling session as guided by the externally mounted sensor infrastructure.

NOTE 1: This section defines selected AVM operational use cases.

NOTE 2: The AVM operational use cases are extendable to geofenced private controlled areas such as those found in Mining, Construction, and Military, etc., applications.

5.2.1 Plant Marshalling

A logistic feature to improve the efficiency of production and vehicle transport within vehicle manufacturing factories/facilities.

5.2.2 Depot Marshalling

A logistic feature for transporting goods inside a depot, improving traffic and safety, and providing additional logistic efficiencies. This will enable a fleet manager to instruct and maneuver AVs between different depot spots (loading, unloading, maneuvering, etc.) by using the external infrastructure sensors.

5.2.3 Valet Parking

A customer feature to provide automated parking services. Valet parking will enable the AV to be parked and summoned autonomously utilizing the support from external infrastructure sensors.

5.2.4 Electric Vehicle Charging

A customer feature to provide electric charging services. An AV will be guided by infrastructure within a facility to an Electric Vehicle (EV) charging spot/s utilizing the support from external infrastructure sensors.

5.3 AVM System Reference Architecture

[Figure 2](#) illustrates the AVM system reference architecture. This standard focuses on the wireless connectivity requirements including messages that are communicated securely for AVM operations over Network-based and/or Direct wireless communications between the AV and AVM CS.

NOTE 1: The definition for the AVM system reference architecture is defined in [Section 3](#).

NOTE 2: Below information provides overview implementation/process details of AVM operations from AV:

- AV using AV CB should communicate with AVM CS and/or AVM SO for enrolling or un-enrolling of AVM use cases (as defined in [5.2](#)) for AVM operations.
 - The configurations that are required for AVM operations between the AV and AVM CS are defined in [Appendix B](#) of this document.
- AV should exchange the VMM upon successful enrolling of respective AVM use case with respective AVM CS by following the feature flow and state flow operations as defined in [5.6](#) and [5.7](#) of this document.
 - Depending on the AV's wireless communication implementation, AV shall request for IMM and receive IMM payload or receive IMM payload for supporting of further AVM operations at respective feature flow and state flows.
 - AV shall communicate VMM upon ignition-ON and respective modules are completely operable to support VMM exchange with AVM CS over respective wireless communications.
 - [5.5](#) provides overview of the AVM system wireless protocol stack for Direct LTE-V2X and Network-based wireless communications.
 - [5.10](#), [6.11](#), and [7.2](#) define the implementation requirements from wireless and security exchange of the VMM and IMM.

NOTE 3: Below information provides overview implementation/process details of AVM operations from AVM CS:

- AVM CS should be capable of enrolling or un-enrolling in multiple AV types/vendors/manufacturers by communicating with AV CB and AVM SO for supporting the AVM operations for respective AVM use cases (as defined in [5.2](#)).
 - AVM CS should be capable of supporting all (as defined in [6.10](#)) vehicle motion control interface types with respective AV for AVM operations.
 - AVM CS should conduct the AVM operations within the AVM controlled geofenced environment ODD.
- AVM CS upon successful reception of VMM from respective AV shall be able to transition the respective feature and state flows (as defined in [5.6](#) and [5.7](#) of this document).
 - AVM CS should be capable of receiving VMM and communicate IMM payload securely over wireless communications using the implementation requirements as defined in [5.10](#), [6.11](#), and [7.2](#).

NOTE 4: AV and AVM CS should follow the concept of operations and implementation requirements for the AVM operations as defined in:

- [5.1](#) contains the AVM operations between the AV and AVM CS in the Controlled Geofenced Environment ODD.
- [5.2](#) contains the AVM use-cases information.
- [5.4](#) contains the information over the AVM system wireless logical architecture.
- [5.5](#) provides overview of the AVM system wireless protocol stacks for Direct LTE-V2X and Network-based wireless communications.
- [5.6](#) provides information on AVM feature flows.
- [5.7](#) provides information on AVM state flows for respective feature flows.
- [5.8](#) provides information about AVM coordinate system including reference point and curvature.
- [5.9](#) provides illustration of AVM logical scenario between the different AVM systems including the human operators.
- [5.10](#) provides requirements information on the security needs for Direct LTE-V2X and Network-based wireless communications.
- [6.1](#) for requirements documentation overview of IMM and VMM.
- [6.2](#) for IMM and VMM data exchange requirements.
- [6.3](#) for IMM and VMM operational requirements.
- [6.4](#) for Timestamp and Timestamp confidence requirements that are used for exchange of IMM and VMM.
- [6.5](#) for Rolling Counter requirements that are used to detect packet loss and latency of the IMM and VMM.
- [6.6](#) for Functional Safety using end-to-end protection computation and verification requirements (including implementation examples as defined in [Appendix F](#)) in the IMM and VMM.
- [6.7](#) for Vehicle Identification process requirements (including implementation examples as defined in [Appendix E](#)) using Blinking method for safe and secure localization/recognition/identification over IMM and VMM.
- [6.8](#) for Driving Permission requirements that are exchanged when respective AV feature flow is in Automated-Control state using IMM and VMM.
- [6.9](#) for Pose requirements including Detected Vehicle Pose when respective AV feature flow is in Automated-Control state using IMM and VMM.
- [6.10](#) for Vehicle Motion Control requirements over Path and Trajectory controls for AVM operations using IMM and VMM.
- [6.11](#) for multiple wireless communications requirements to exchange IMM and VMM securely.
- [6.12](#) with requirements for all feature flows and state flows transitions using IMM and VMM.
- [6.13](#) for parameters settings that are used to/inside the IMM and VMM.

- [7.1](#) with sequence flow diagrams for all feature flows and state flows using IMM and VMM.
- [7.2](#) with security certificate requirements for to exchange IMM and VMM securely.
- [8.1](#) contains the ASN.1 object definitions for IMM.
- [8.2](#) contains the ASN.1 object definitions for VMM.
- [8.3](#) contains the ASN.1 object definitions that are commonly used between the IMM and VMM.
- [Appendix A](#) contains information for editing the SAE J2735 to support IMM and VMM.
- [Appendix B](#) contains information for configurations that are used for automated vehicle operations during computation and verification over IMM and VMM that are agreed privately between the AV using the AV CB and AVM CS for both Direct LTE-V2X wireless communications and Network-based wireless communications.
- [Appendix C](#) contains an overview of the End-to-End latency calculations between the AVM application layers on the AV and AVM CS for both Direct LTE-V2X wireless communications and Network-based wireless communications as reference.
- [Appendix D](#) contains the timestamp implementation methods and algorithms.
- [Appendix E](#) contains the vehicle identification blinking code pattern computation and verification example using IMM and VMM.
- [Appendix F](#) contains the functional safety checksum implementation example for mandatory, mandatory + optional data elements/frames in IMM and VMM.
- [Appendix G](#) contains the sample payloads for the IMM and VMM with mandatory (including payload sizes), mandatory + optional data elements.
- [Appendix H](#) provides an overview of the LTE-V2X optimal configurations recommendation for the AVM transmission and reception pool configurations for the IMM and VMMs.

NOTE 5: BasicVehicleClass (as defined in the SAE J2735 standard) is being used for exchanging as Automated Vehicle type in the VMM.

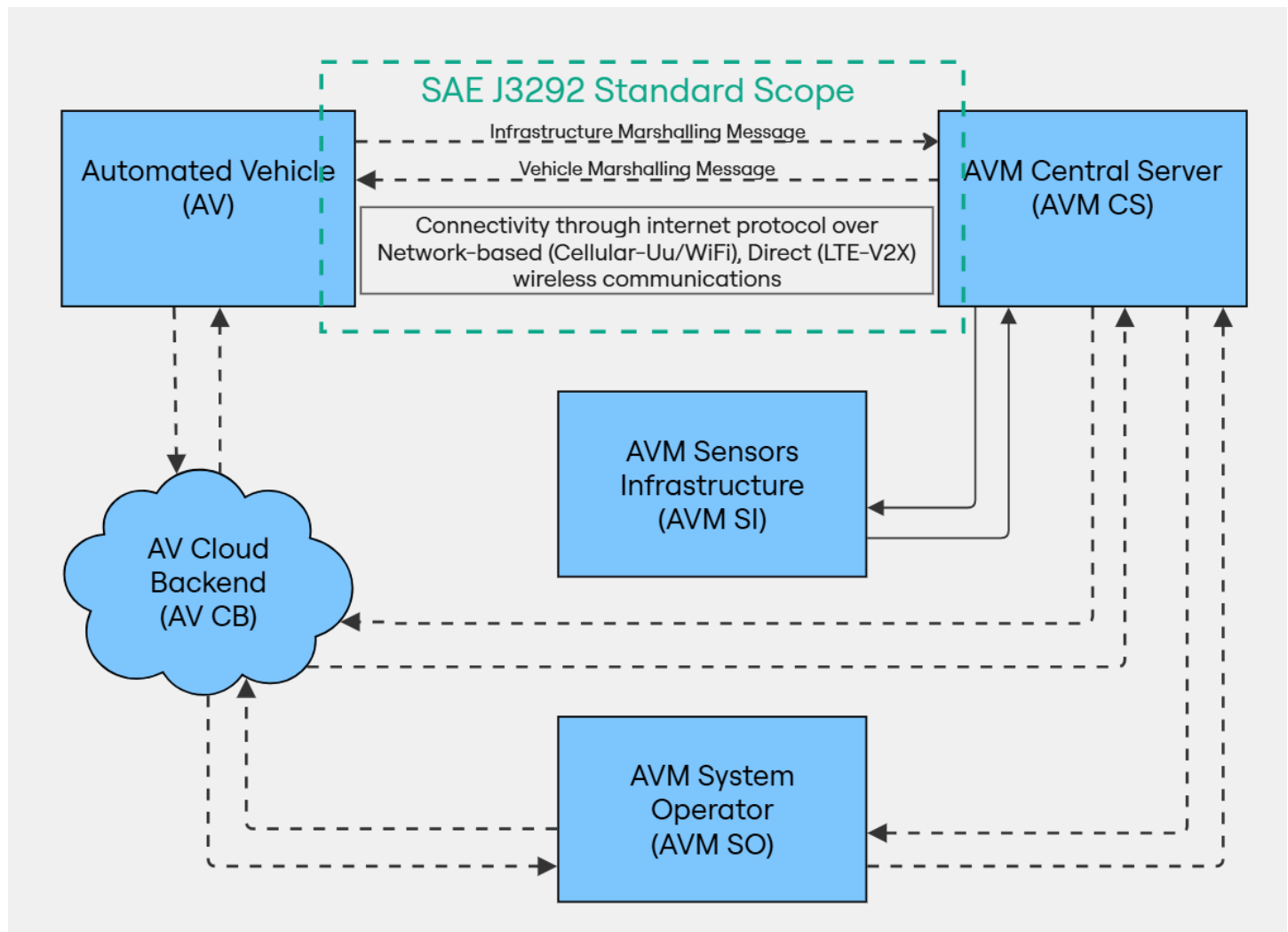


Figure 2 - AVM system reference architecture

5.4 AVM System Wireless Logical Architecture

[Figure 3](#) illustrates the AVM system wireless logical architecture for both Network-based and Direct wireless communication technologies from wireless operational interfaces between AV and AVM CS.

- AV: The AV needs to support a minimum of one Network-based or Direct wireless communications-based technology for IMM and VMM exchange with the AVM CS.
- AVM CS: The AVM CS needs to support the AV the whole time when the AV interfaces with AVM CS via IMM and VMM exchange using one or both wireless communication technologies.

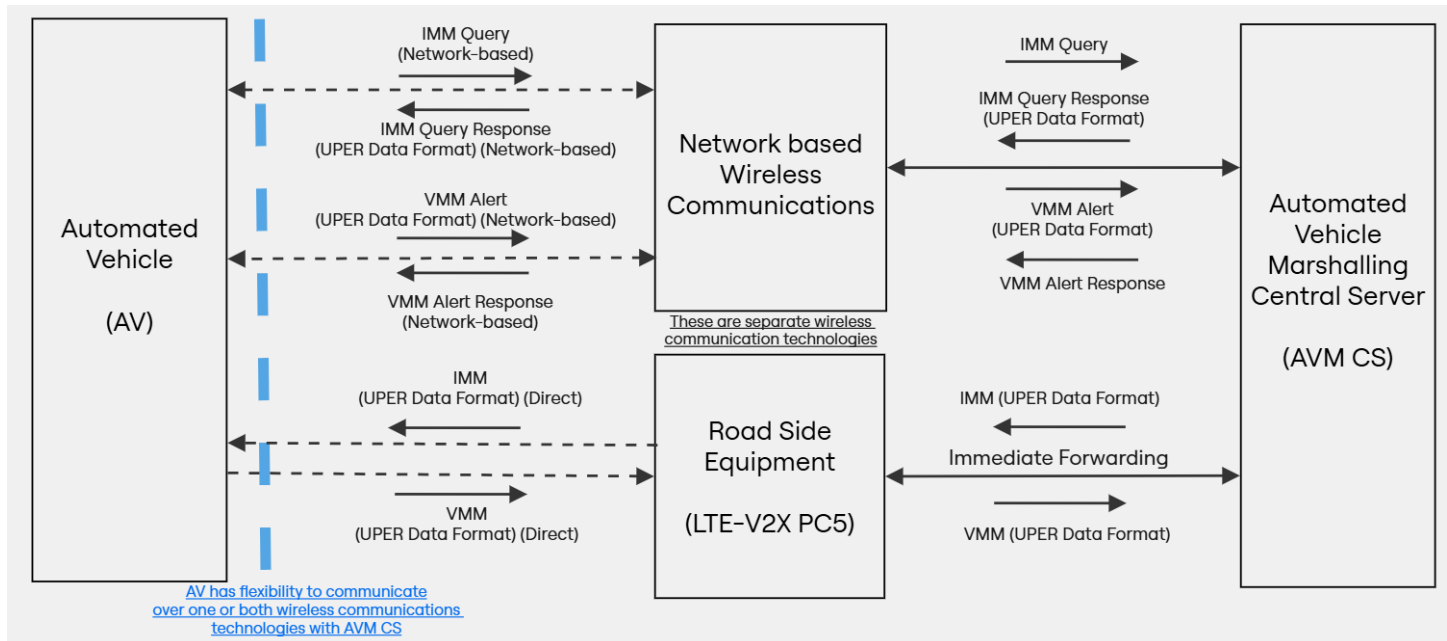


Figure 3 - AVM system wireless logical architecture (network-based and direct wireless technologies)

5.5 AVM System Wireless Protocol Stack

This section provides overview of the AVM system wireless protocol stack for Direct LTE-V2X wireless communications and Network-based wireless communications.

5.5.1 Direct LTE-V2X Protocol Stack

[Figure 4](#) illustrates the exchange of IMMs and VMMS between the AV and AVM CS using RSE. Where:

- AV and RSE exchanges the messages over the Direct LTE-V2X wireless communications using LTE-V2X protocol stack.
- RSE does exchange of the messages with AVM CS using immediate forwarding concept over wired network interface.

NOTE 1: The system of [Figure 4](#) aligns with the SAE J3161 standard from the LTE-V2X protocol stack.

NOTE 2: [Appendix C.1](#) provides overview of End-to-End Latency of IMM and VMM exchange using Direct LTE-V2X wireless communications between AV and AVM CS using RSE.

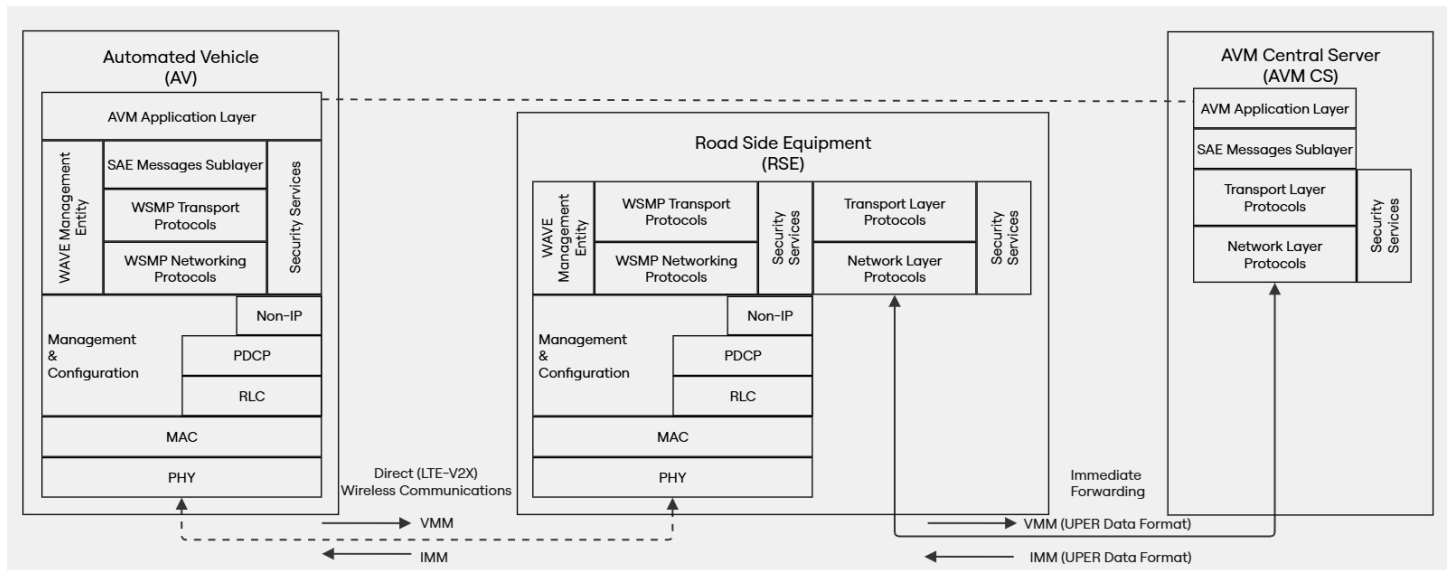


Figure 4 - Direct LTE-V2X protocol stack

5.5.2 Network-Based Protocol Stack

Figure 5 illustrates the exchange of IMM and VMM between the AV and AVM CS. Where:

- AV and AVM CS exchanges the messages over the Network-based wireless communication medium using the Network-based protocol stack.
- Network-based wireless communications medium does exchange of the messages with AVM CS using immediate forwarding concept over wired network interface.

NOTE: [Appendix C.2](#) provides overview of End-to-End Latency of IMM and VMM exchange using Network-based wireless communications between AV and AVM CS using Network-based wireless communication medium.

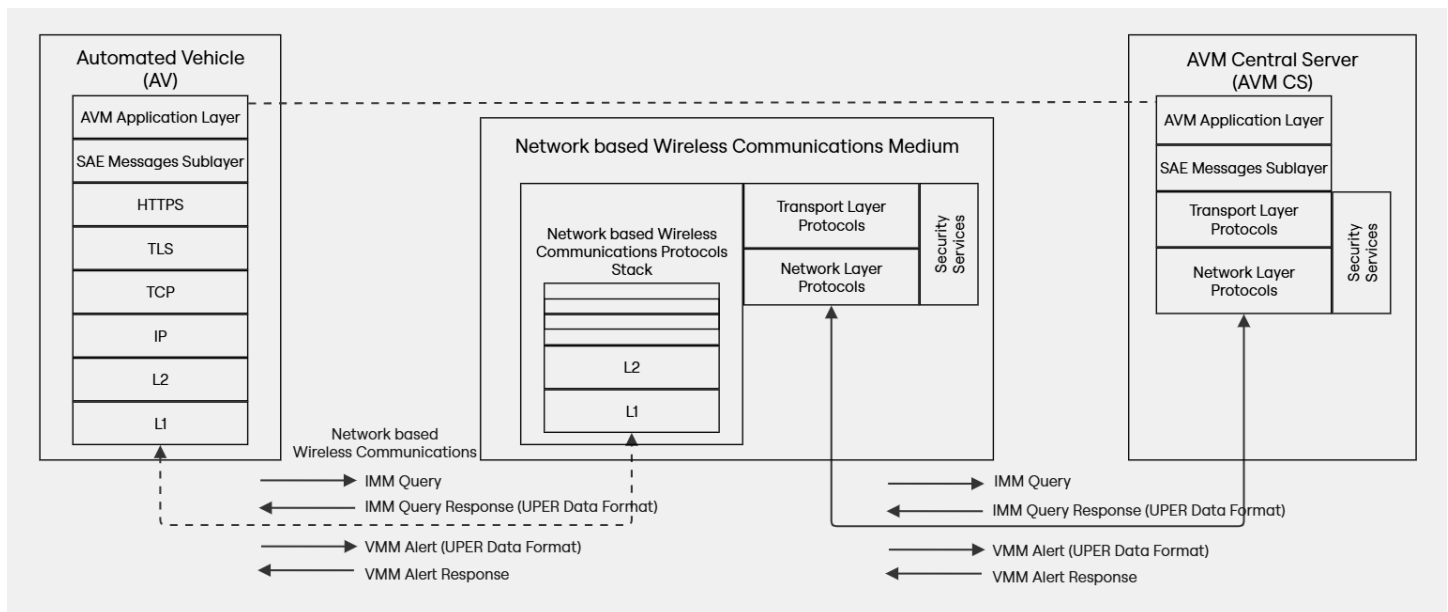


Figure 5 - Network-based protocol stack

5.6 AVM Feature Flow

Figure 6 illustrates the AVM Feature Flow Diagram and transitions between the feature states of a single AV with the AVM CS. When AVM CS manages multiple AVs simultaneously, it requires multiple feature flow operations; with one operation for each AV.

The AVM Feature Flow describes the respective AVM CS and AV's feature lifecycle flow of states within the AVM automated vehicle operation system. The Feature Flow includes all the way from when the AV is not part of the AVM system to feature activation, feature operational and feature deactivation of the AV and AVM CS within the AVM system. For the AVM feature flows, the following conditions apply:

- AVM CS and AVs exchange information about current feature flow wirelessly using the IMM and VMMS.
- AVM CS uses the featureFlowCommand data element from IMM's request for automated vehicle operations with respective AVs.
- AVs respond or acknowledge to AVM CS with the current featureFlowCommandResponse data element using VMMS.

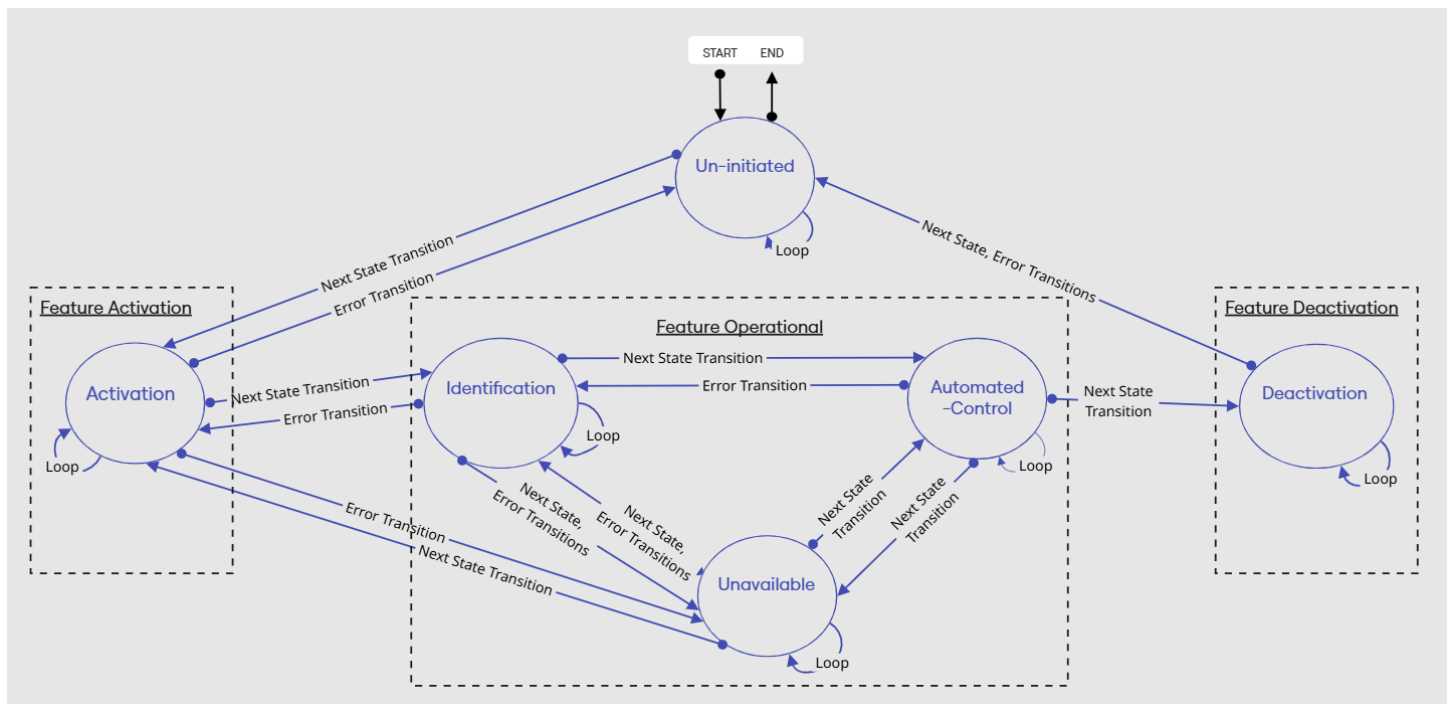


Figure 6 - AVM feature flow diagram

The AVM Feature Flow Diagram consists of the following states:

- Un-initiated
 - Un-initiated is a default state in which the AVM CS and AV system are in an unknown state for the respective AV. Both the AVM CS and AV when subscribed to AVM operation will be in this feature flow state.
- Activation
 - Activation is a state in which the AVM CS and AV are performing the activation process for the respective AVM feature.
- Identification
 - Identification is a state in which the AVM CS and AV completes the necessary authorization process for safe vehicle identification using blinking-light activities. This takes place prior to the AVM CS taking control of the respective AV prior and to the start of the automated vehicle marshalling.
- Automated-Control
 - Automated-Control is a state where the AVM CS controls the AV to marshal autonomously to perform certain actions, and the AV acknowledges back to the AVM CS about automated response via both high-message intervals and low-message intervals using wireless communications.
- Unavailable
 - Unavailable is a state in which the AV is temporarily suspending/sleeping/recovering from the current active automated vehicle operation based on instructions from the AVM CS, due to human intervention, AV leaving the ODD area for certain activities, or the AV is asked to power-cycle, etc., activities. After switching into this state, the wireless communications between the AVM CS and AV may be interrupted and stopped.
- Deactivation
 - Deactivation is a state in which the AVM CS and AV are performing the deactivation process for the respective AVM feature when the AV reaches the end destination and the AVM CS is no longer controlling the AV from the respective ODD area.

5.7 AVM State Flow

[Figure 7](#) illustrates the AVM State Flow Diagram and transitions between the AVM feature states of a single AV with the AVM CS. When the AVM CS manages multiple AVs simultaneously, it requires multiple state flows operations, one operation for each AV. The AVM feature flows contain groupings of one or more states/state flows for Automated Vehicle Operation.

- AVM CS and AVs exchange information about the current Feature Flow and State Flow wirelessly using the IMM and VMMS.
- AVM CS uses the driveCommandAction data element from IMMS to request State Flow operations with the respective AVs.
- AVs respond or acknowledge to the AVM CS with the current operationMode data element using VMMS for the respective automated vehicle State Flow operations.

NOTE 1: The [Figure 7](#) state flow diagram aligns with the states of ISO 23374-1 State Transition Diagram. It contains additional states to complete the AVM system design implementation.

NOTE 2: The examples of state name usage, such as driving, driven, drivable, etc., for the drive state operation, are not part of the scope of this standard and are subject to the implementation of the system operators usage; i.e., the system operator displays.

NOTE 3: [Figure 7](#) contains the brief state flow operations. See [7.1](#) for detailed exchange of handshake sequence flow diagrams between the AVM CS and a single AV for the AVM Feature Flow.

NOTE 4: Not shown in [Figure 7](#) is that for each feature transition there is a featureFlowCommand/featureFlowCommandResponse equal to the name of the feature.

- For example, when transitioning from the Activation Feature Flow to the Identification Feature Flow, there would be a featureFlowCommand = Identification and featureFlowCommandResponse = Identification.

NOTE 5: Not shown in [Figure 7](#) is that for each state transition there is a driveCommandAction/operationMode equal to the name of the state flow.

- For example, when transitioning from the Standby State Flow to the Drive State Flow, there would be driveCommandAction = Drive and operationMode = Drive.
- Exceptions to this are the operationMode for the:
 - Initialize state can be Initialize or Initializing.
 - Identify state can be Identify or Identifying.
 - Suspend state can be Suspend or Human in Control.
 - Pause state can be Pause or Station-Hold.

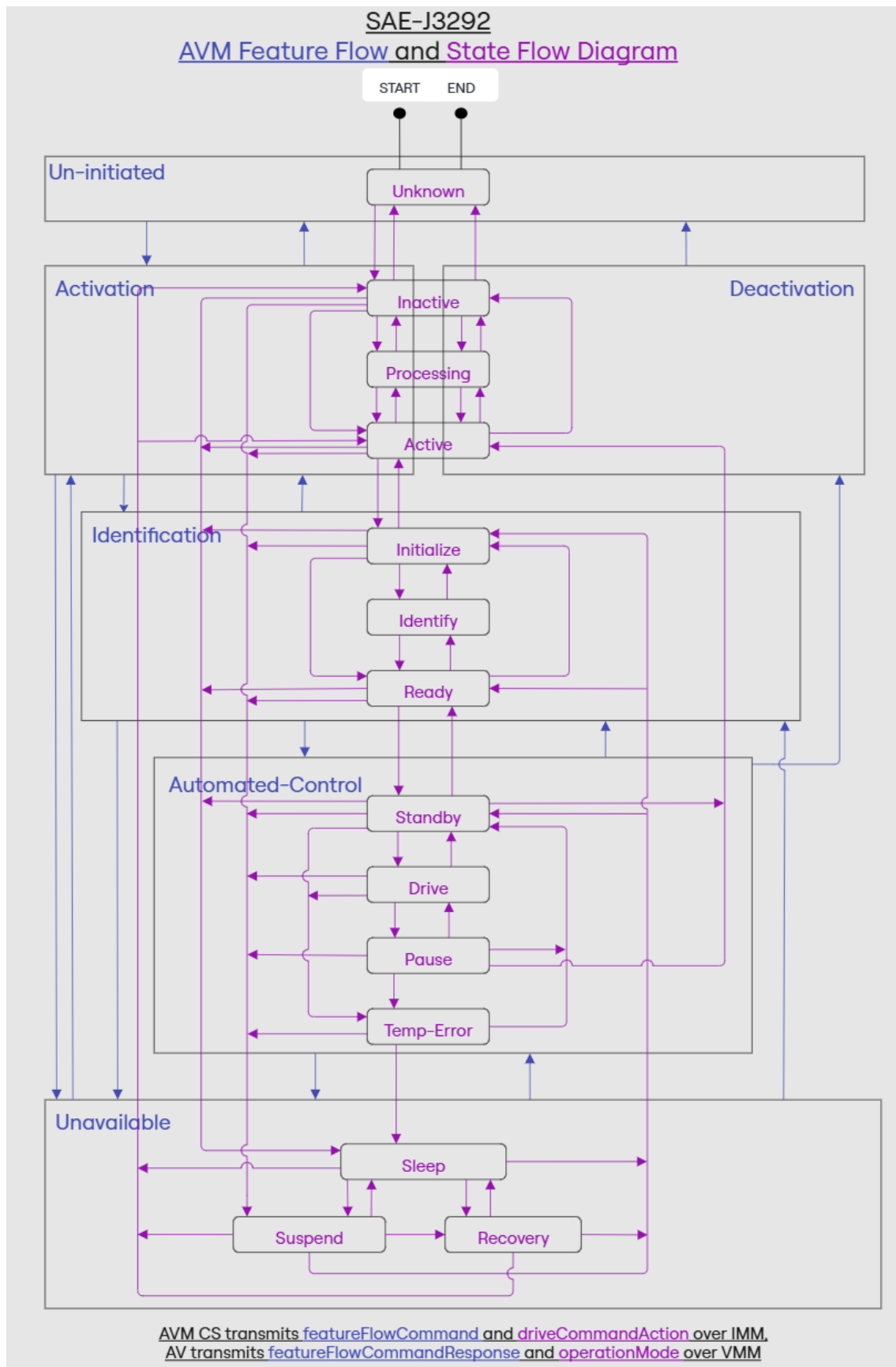


Figure 7 - AVM feature flow and state flow diagram



5.8 AVM Reference Point, Coordinate System, and Curvature

An AVM system uses the Reference Point, Coordinate System, and Curvature as shown in [Figure 8](#).

1. Reference Point:

- a. The reference point of the AV is in the center of the rear axle. The reference point is projected onto the surface of the ground plane with reference to the AVM coordinate system.

NOTE 1: When multiple rear axles are present for the vehicle types; the AVM system should consider the center of the last rear axle from rear side of the vehicle.

NOTE 2: When trailer is attached to the AV, the system shall consider the center of the rear axle of the AV.

NOTE 3: The method for determining an Automated Vehicle's location for AVM operations within an AVM facility, relative to a defined reference point, is at the discretion of AVM system implementers.

2. Coordinate System:

- a. The AVM coordinate system is a cartesian coordinate system with fixed origin. Coordinates can have both positive and negative values.

- i. Where:

- 1) x and y are in centimeters.

- 2) psi (ψ) ranges (0,2 π). psi refers to the orientation of the AV in radians, i.e., relative to the x-axis.

- a) Positive values define a rotation counter clockwise.

3. Curvature:

- a. The curvature κ [$\frac{1}{m}$] describes driving on a circle with radius $r = \frac{1}{\kappa}$

- i. $\kappa = 0$ corresponds to driving straight

- ii. $\kappa > 0$ corresponds to driving left

- iii. $\kappa < 0$ corresponds to driving right

NOTE: For slow speeds as used by AVM, the curvature κ is related to the steering angle δ using wheelbase l as defined by the Acker-mann steering formula: $\delta = \kappa \cdot l$

The steering angle δ equals the front axis steering angle δ_F . The rear axis steering angle is fixed ($\delta_R = 0$).

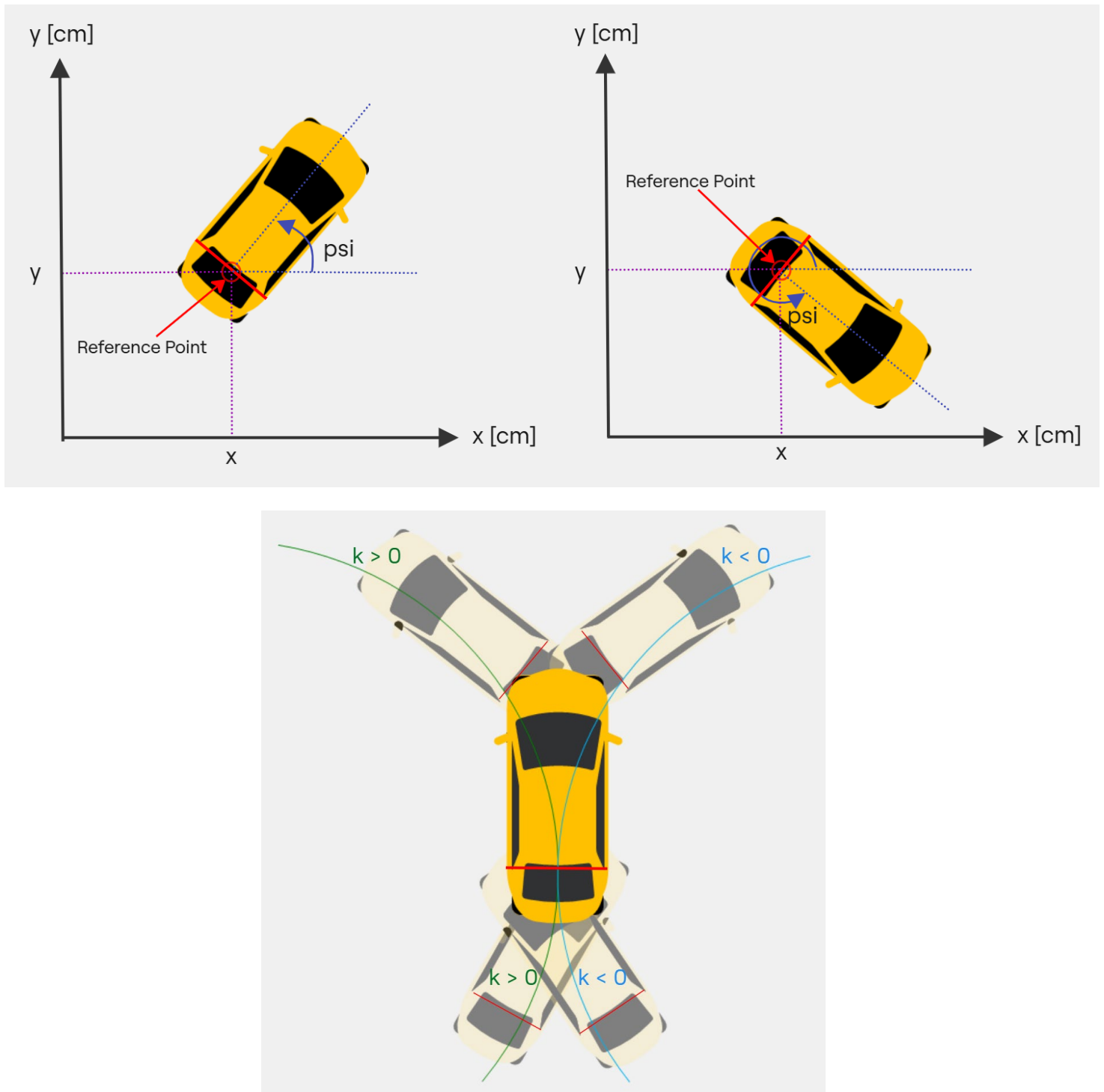


Figure 8 - AVM coordinate system, reference point diagram, and curvature

5.9 AVM Scenario

[Figure 9](#) illustrates the AVM logical scenario with exchange of information between the different AVM systems including the human operators.

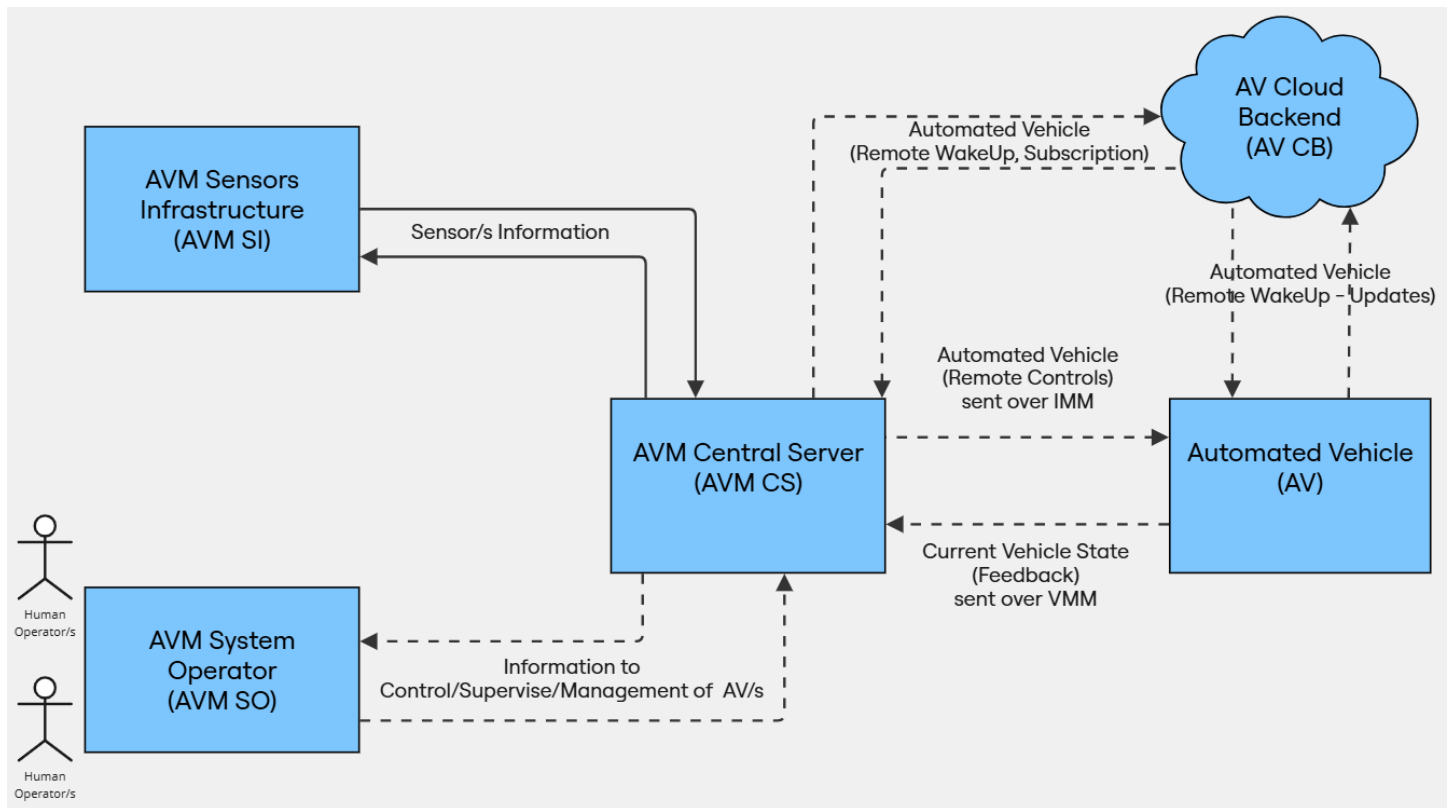


Figure 9 - AVM system scenario logical overview

5.10 Security Needs

This section contains the security needs from both Direct (LTE-V2X) and Network-based wireless communication technologies.

NOTE: It is up to AVM system implementers on the AV and AVM CS for usage of Hardware Security Module (HSM) or Secure Element (SE) or Trusted Platform Module (TPM) or Software-based as sources for the signing and/or encryption. But this standard recommends to use one or more options from the HSM/SE/TPM as sources for the signing and/or encryption that provide greater security when compared to the Software-based.

5.10.1 Direct (LTE-V2X) Wireless Communications

5.10.1.1 Security Credential Management System (SCMS)

- The wireless interface between the AVM CS and AV is secured using techniques defined in IEEE 1609.2. This includes message signing/verification and certificates.
- In order to receive certificates, OBE (AV) and RSE need to have access to a SCMS.
- The SCMS provides certificates for signing the IMM and VMMs.
- The SCMS is outside the scope of this standard, However, the security profiles and aspects regarding the use of the certificates are within scope.

5.10.1.2 Data Source Authenticity and Authorization

- The system needs to provide a mechanism to authenticate sources of data and verify that they are authorized to send such data.
- The system needs to verify that messages transmitted by the OBE are sent by a valid AV sender and messages transmitted from the RSE are sent by a valid AVM CS sender.
- The term Authenticate(d) Sources encompasses not only the authorization of the transmitting device itself to participate in the vehicle-to-everything (V2X) ecosystem, but also its authority to transmit messages on behalf of its associated AVM CS from RSE-Infrastructure.

5.10.1.3 Data Integrity and Availability

- The system needs to ensure messages transmitted by the OBE and RSE were not modified in transit over the V2X interface.
- The system needs to provide a mechanism to verify that data has not been changed or significantly delayed between the entity that produced the data and the entity that consumes the data.
- A critical security assumption is that data inputs to or within the AVM Infrastructure (AVM CS, AVM SI, AVM SO) from external elements are authentic and accurate.

5.10.1.4 Data Non-Repudiation and Confidentiality

- The system needs to ensure that the sender/OBE cannot deny that it sent the information.
- The system needs to ensure protection of personally identifiable information exchanged by the OBE and RSE.

5.10.1.5 Physical Security

- The OBE and RSE need to provide tamper proof or tamper evident levels of physical protection.

5.10.1.6 Misbehavior Detection [Informative]

- The application should enable the detection of misbehaving transmissions and, if any are identified, report them to a Misbehavior Authority (MA) for investigation and possible revocation so that misbehaving entities can be removed from the V2X ecosystem.

5.10.2 Network-Based Wireless Communications

5.10.2.1 Data Source Authenticity and Authorization

- The system needs to ensure that data is from a trusted source and that the source is authorized to send the data, the system will use Mutual Transport Layer Security (mTLS).
- In the one way TLS connection, only the server is authenticated to the client. However, mTLS adds a layer of security by requiring both the client and the server to authenticate each other using digital certificates.
- With mTLS, both the client and the server must have the correct private key to establish a connection.
- This provides an extra layer of security, verifying that both parties are who they claim to be.
- The certificates used by both parties in the TLS handshake chain back to a known Root CA dedicated to the AVM application, providing assurance that those certificates are for use in AVM operations.
- The serial number field in the certificate of the AVM CS certificate shall be globally unique, allowing AVM CS servers to be uniquely identified.
- The AV shall validate that the serial number field in the AVM CS certificate matches a value that has been pre-configured onto the AV.

5.10.2.2 Data Integrity and Availability

- The system needs to provide a mechanism to allow a relying party to determine whether or not the data has been changed since it was generated, and to determine whether or not it is timely.
- The system will ensure that messages are not altered in transit and that the data is consistently available.
- The TLS protocol, ensures data integrity through the use of Message Authentication Codes (MACs).
 - A MAC is a cryptographic checksum that is attached to each message.
 - The receiving party can verify the MAC to ensure that the message has not been tampered with.
- To ensure data availability, the system will implement redundancy and failover mechanisms.
 - This means having backup network-based wireless communication systems and network connections to prevent a single point of failure.
 - Additionally, the system will be monitored in real-time to detect and address any potential issues before they can cause an outage.

5.10.2.3 Data Confidentiality

- The system will ensure that the data is protected.
- TLS encrypts all data transmitted between the AV and the AVM CS.
 - This encryption ensures that sensitive information, such as personally identifiable information, is protected from eavesdropping and unauthorized access.

5.10.2.4 Physical Security

- The AV and AVM CS need to provide tamper proof or tamper evident levels of physical protection.

5.10.2.5 Misbehavior Detection [Informative]

- The application should enable the detection of misbehaving transmissions and, if any are identified, report them to a Misbehavior Authority (MA) of AV CB for investigation and possible revocation so that misbehaving entities can be removed from the AVM ecosystem.
 - If the MA confirms the misbehavior, it can add the device's certificate to a Certificate Revocation List (CRL) or use other mechanisms to block it from the network.

6. REQUIREMENTS

6.1 Requirements Documentation Overview

6.1.1 Requirements Details and Notation

For each requirement in this report the following information is provided:

- Requirement - The individual requirement text.

Each requirement consists of a single action indicated by a shall statement.

- System (SYS) - The system that identifies the requirement.

This standard focuses on data exchange between the two systems: AVM CS and AV as specified in [5.3](#) of AVM System Reference Architecture.

NOTE: Requirements can apply to one or both systems.

- Parameters - Parameters identified within the requirement text which provide the details for the accuracy, timing, resolution, etc., required to support the requirements.

6.1.2 Requirements Tables

6.1.2.1 Individual Requirements

[Table 1](#) provides a template for the tabular format of documenting the requirements as described in [Section 6](#) and contains columns for each main items mentioned in that section.

Table 1 - Individual requirements table template

Requirement	SYS	Parameters

6.1.3 Minimum Content Requirements

For requirements that state the minimum message contents that are to be included, [Table 2](#) provides the format for documenting the minimum content. It consists of the following information:

- Data Exchange Item - An item within the Message that may be exchanged over the interface. This is provided as the field name used in the ASN.1.
- Type - This provides information regarding the data type.

It includes the following types:

- Sequence (SEQ) - Contains an ordered set of data elements and/or data frames.

NOTE: In the table the items contained within the sequence should be indented underneath the sequence data item to make it clear what all is included within the sequence.

- Sequence of Sequences (SEQ of SEQ) - Contains an ordered set of sequences.
- Data Element (DE) - The lowest level data types and forms the building blocks of sequences (e.g., integer, enumeration).
- Choice (CHC) - Provides for a selection of an item where the items can be of the same data type or different data types.

NOTE 1: In the table, the items that can be selected should be indented underneath the CHC data item to make it clear what all can be selected.

NOTE 2: At a minimum, the standard needs to include requirements text for each DE type that are either required or conditionally required for Tx (see 'Required for Tx' bullets), even if that text indicates that the requirements for that item are out of scope of the standard.

- Required for Tx - Indicates whether the Data Exchange Item needs to be included in the assembled message or not to transmit the message.

Options include:

- Yes - The Data Exchange Item must be included in the Message.

NOTE: Items marked as Yes which are contained within another item marked as Conditional (see below), must only be included in the Message if the conditional item they are contained within is included in the Message.

- No - The Data Exchange Item is optional to be included in the Message.
- Conditional - The Data Exchange Item may only be included in the Message if the identified conditions for it or any of its sub-items are met with per the requirements.
- Not Allowed - The Data Exchange Item is not allowed to be included in the Message.

- Can be Set to Unknown or Unavailable - The Data Exchange Item can be set to Unknown or Unavailable if included in the provided Message.

Options include:

- - The Data Exchange Item is not a DE type.
- Yes - The Data Exchange Item can be set to Unknown or Unavailable.
- No - The Data Exchange Item cannot be set to Unknown or Unavailable.
- NA - Unknown or Unavailable are not an option for the Data Exchange Item or the item was marked as 'Not Allowed' in the Required for Tx column and, therefore, should not be included in the Message.

NOTE: This only pertains to DE data types and not all DE data types support an Unknown or Unavailable setting.

Table 2 - Minimum content table template

Data Exchange Item	Type	Required for Tx	Can be Set to Unknown or Unavailable

6.2 Data Exchange Requirements

This section contains the data exchange requirements for the IMM, VMM, and data exchange requirements that are common for both IMM and VMM.

6.2.1 Infrastructure Marshalling Message (IMM)

The Infrastructure Marshalling Message (IMM) is an AVM message transmitted by the AVM CS to the AV to follow the automated vehicle marshalling commands and to also acknowledge messages it has received from the AV.

- This section contains the minimum data content required for the IMM transmission and also includes conditional data content that shall need to be transmitted when certain conditions are identified.

NOTE 1: This standard defines the conditions that are common for all the AVM use cases. It's up to AVM system implementers for defining of their own AVM operations conditions which are beyond the scope of this standard.

NOTE 2: The operational requirements for the IMM data exchange requirements are defined in [6.3.1](#), [6.3.3](#), and also throughout this standard document wherever its applicable.

6.2.1.1 General

Requirement	SYS	Parameters
The system shall use Unaligned Packed Encoding Rules (UPER) to encode the IMM. NOTE: This is to be consistent with the guidance provided in SAE J2735 and the encoding method used by other V2X application specifications.	AVM CS	

6.2.1.2 Message Frame

6.2.1.2.1 Minimum Content

Requirement	SYS	Parameters
The message frame provided by the system shall meet the minimum content specified in Table 3 .	AVM CS	

Table 3 - Minimum infrastructure marshalling message frame content

Data Exchange Item	Type	Required for Tx	Can be Set to Unknown or Unavailable
InfrastructureMarshallingMessage	DE	Yes	NA
Message Type	SEQ	Yes	-

6.2.1.2.2 Message ID

Requirement	SYS	Parameters
The system shall set the Message ID to the value assigned to infrastructureMarshallingMessage within the SAE J2735 'DSRCmsgID' ASN.1 data element. Section 8.1.1.1 contains the IMM ID Use and ASN.1 representation.	AVM CS	

6.2.1.2.3 Message Type

Requirement	SYS	Parameters
When indicating a Message ID of infrastructureMarshallingMessage, the system shall include a Message Type of InfrastructureMarshallingMessage within the SAE J2735 'MessageType' frame.	AVM CS	

6.2.1.3 Message

6.2.1.3.1 Minimum Content

Requirement	SYS	Parameters
The message provided by the system shall meet the minimum content specified in Table 4 .	AVM CS	

Table 4 - Minimum infrastructure marshalling message content

Data Exchange Item	Type	Required for Tx	Can be Set to Unknown or Unavailable
InfrastructureMarshallingMessage	SEQ OF SEQ	Tx	NA
IMME2EProtection	SEQ	No	-
E2ELength	DE	Yes	No
E2EChecksum	DE	Yes	No
E2EPublicKey	DE	Yes	No
E2ERandomIncrementer	DE	Yes	No
E2EDataID	DE	No	No
VehicleContainerBlob	SEQ OF SEQ	Yes	NA



6.2.1.3.2 IMME2EProtection

Requirement	SYS	Parameters
The system shall be capable of supporting End-to-End Protection for Infrastructure Marshalling Message from Functional Safety aspects. Section 8.1.3.3.1.1 contains the DF_IMME2EProtection Use and ASN.1 representation.	AVM CS	

6.2.1.4 Vehicle Container Blob

6.2.1.4.1 Minimum Content

Requirement	SYS	Parameters
The IMM Vehicle Container Blob data provided by the system shall meet the minimum content specified in Table 5 .	AVM CS	

Table 5 - Minimum vehicle container blob content

Data Exchange Item	Type	Required for Tx	Can be Set to Unknown or Unavailable
VehicleContainerBlob	SEQ OF SEQ	Yes	NA
VehicleContainerE2EProtection	SEQ	No	-
E2ELength	DE	Yes	No
E2EChecksum	DE	Yes	No
E2EPublicKey	DE	Yes	No
E2ERandomIncrementer	DE	Yes	No
E2EDataID	DE	No	No
VehicleContainerData	SEQ	Yes	NA

6.2.1.4.2 VehicleContainerBlob

Requirement	SYS	Parameters
<p>The system shall be capable of supporting multiple Vehicle Container Blob within the Infrastructure Marshalling Message. Section 8.1.3.3.2 contains the DF_VehicleContainerBlob Use and ASN.1 representation.</p> <p>NOTE 1: The AVM CS system is not required to include multiple Vehicle Container Blob in an IMM if its handling single AV, but should the need arise for handling multiple AV's, it needs to be capable of supporting the ability to do so.</p> <p>NOTE 2: Inclusion of the multiple Vehicle Container Blob is also dependent on the type of wireless communication the AV is communicating with the AVM CS.</p>	AVM CS	
The system shall be capable of supporting minimum of <avmMinVehiclesDirectLTEV2X> AVs as part of the Vehicle Container Blob of imm within an Infrastructure Marshalling Message during Broadcast Wireless Communication Technologies.	AVM CS AV	avmMinVehicles DirectLTEV2X
The system shall be capable of supporting maximum of <avmMaxVehiclesDirectLTEV2X> AVs as part of the Vehicle Container Blob of imm within an Infrastructure Marshalling Message during Broadcast Wireless Communication Technologies.	AVM CS AV	avmMaxVehicles DirectLTEV2X
The system shall be capable of supporting minimum of <avmMinVehiclesNetworkBased> AVs as part of the Vehicle Container Blob of imm within an Infrastructure Marshalling Message during Unicast Wireless Communication Technologies.	AVM CS AV	avmMinVehicles NetworkBased
The system shall be capable of supporting maximum of <avmMaxVehiclesNetworkBased> AVs as part of the Vehicle Container Blob of imm within an Infrastructure Marshalling Message during Unicast Wireless Communication Technologies.	AVM CS AV	avmMaxVehicles NetworkBased

6.2.1.4.3 VehicleContainerE2EProtection

Requirement	SYS	Parameters
The system shall be capable of supporting End-to-End Protection for Vehicle Container Data of an Infrastructure Marshalling Message from Functional Safety aspects. Section 8.1.3.3.2.1 contains the DF_VehicleContainerE2EProtection Use and ASN.1 representation.	AVM CS	

6.2.1.5 Vehicle Container Data

6.2.1.5.1 Minimum Content

Requirement	SYS	Parameters
The IMM's Vehicle Container Data from Vehicle Container Blob provided by the system shall meet the minimum content specified in Table 6 .	AVM CS	

Table 6 - Minimum vehicle container data content

Data Exchange Item	Type	Required for Tx	Can be Set to Unknown or Unavailable
VehicleContainerData	SEQ	Yes	-
IMMMessageVersion	DE	Yes	No
IMMDataManagementDataE2EProtection	SEQ	Conditional	-
IMMDataManagementData	SEQ	Yes	-
AVMCSIdentityManagementE2EProtection	SEQ	Conditional	-
AVMCSIdentityManagementData	SEQ	Yes	-
FeatureFlowCommandE2EProtection	SEQ	Conditional	-
FeatureFlowCommand	DE	Yes	No
VehicleIdentificationCommandDataE2EProtection	SEQ	Conditional	-
VehicleIdentificationCommandData	CHC	Conditional	-
DrivingPermissionE2EProtection	SEQ	Conditional	-
DrivingPermission	SEQ	Conditional	-
TimeSyncIMMAVMCSRequestE2EProtection	SEQ	Conditional	-
SafetyTimeSyncIMMAVMCSRequestData	SEQ	Conditional	-

Data Exchange Item	Type	Required for Tx	Can be Set to Unknown or Unavailable
TimeSyncVMMAVResponseE2EProtection	SEQ	Conditional	-
SafetyTimeSyncVMMAVResponseData	SEQ	Conditional	-
SafetyProfileRequestE2EProtection	SEQ	Conditional	-
SafetyProfileRequest	SEQ	Conditional	-
AVMCSCControlCommandE2EProtection	SEQ	Conditional	-
AVMCSCControlCommand	SEQ	Yes	-
InfrastructureErrorE2EProtection	SEQ	Conditional	-
InfrastructureError	SEQ	Conditional	-
DetectedVehiclePoseE2EProtection	SEQ	Conditional	-
DetectedVehiclePose	SEQ	Conditional	-
ControlInterfaceE2EProtection	SEQ	Conditional	-
ControlInterface	CHC	Conditional	-

6.2.1.5.2 VehicleContainerData

Requirement	SYS	Parameters
The system shall include the Vehicle Container Data to support for automated vehicle operation for the respective AV over Infrastructure Marshalling Message. Section 8.1.3.3.3 contains the DF_VehicleContainerData Use and ASN.1 representation.	AVM CS	

6.2.1.5.2.1 IMMMessageVersion

Requirement	SYS	Parameters
The system shall set the Infrastructure Marshalling Message version number <immMsgVersion> which is used for verification of the SAE J3292 standard message version number from compatibility and interoperability for Infrastructure Marshalling Message. Section 8.1.2 contains the DE_IMMMessageVersion Use and ASN.1 representation.	AVM CS	immMsgVersion

6.2.1.6 IMM Data Management Data E2EProtection

6.2.1.6.1 Minimum Content

Requirement	SYS	Parameters
The IMM Data Management Data E2EProtection data provided by the system shall meet the minimum content specified in Table 7 .	AVM CS	

Table 7 - Minimum IMM data management data E2EProtection data content

Data Exchange Item	Type	Required for Tx	Can be Set to Unknown or Unavailable
IMMDataManagementDataE2EProtection	SEQ	No	-
E2ELength	DE	Yes	No
E2EChecksum	DE	Yes	No
E2EPublicKey	DE	Yes	No
E2ERandomIncrementer	DE	Yes	No
E2EDataID	DE	No	No

6.2.1.6.2 IMMDataManagementDataE2EProtection

Requirement	SYS	Parameters
The system shall be capable of supporting End-to-End Protection for IMM Data Management Data to check if all data bits are received or if any of data bits are lost or if any data bits are flipped or if errors occur during transmission within IMM from Functional Safety aspects. Section 8.1.3.3.4 contains the DF_IMMDataManagementDataE2EProtection Use and ASN.1 representation.	AVM CS	

6.2.1.7 IMM Data Management

6.2.1.7.1 Minimum Content

Requirement	SYS	Parameters
The IMM Data Management data of Vehicle Container Data provided by the system shall meet the minimum content specified in Table 8 .	AVM CS	

Table 8 - Minimum IMM data management content

Data Exchange Item	Type	Required for Tx	Can be Set to Unknown or Unavailable
IMMDataManagementData	SEQ	Yes	-
IMMMsgIntvl	DE	Yes	No
RollingCounterFromIMMTransmitted	DE	Yes	No
RollingCounterOfVMMReceived	DE	Yes	No
VehicleContainerGenerationTime	SEQ	Yes	-
DYear	DE	Yes	No
DMonth	DE	Yes	No
DDay	DE	Yes	No
DHour	DE	Yes	No
DMinute	DE	Yes	No
DSecond	DE	Yes	No
DOffset	DE	Conditional	No
VehicleContainerGenerationTimeConfidence	DE	Yes	Yes
IMMProprietaryExtensionField	DE	No	No

6.2.1.7.2 IMMDataManagementData

Requirement	SYS	Parameters
The system shall include the IMM Data Management which contains the data information controlling towards the bidirectional wireless communication between the AVM CS and AV over Infrastructure Marshalling Message. Section 8.1.3.3.5 contains the DF_IMMDataManagementData Use and ASN.1 representation.	AVM CS	

6.2.1.7.2.1 IMMMsgIntvl

Requirement	SYS	Parameters
The system shall include the IMM Message Interval to indicate the wireless communication interval of the IMM for the respective AV. Section 8.1.3.3.5.1 contains the DE_IMMMsgIntvl Use and ASN.1 representation.	AVM CS	

6.2.1.7.2.2 RollingCounterFromIMMTransmitted

Requirement	SYS	Parameters
The system shall increment the value of RollingCounterFromIMMTransmitted by one for each IMM being transmitted. Section 8.1.3.3.5.2 contains the DE_RollingCounterFromIMMTransmitted Use and ASN.1 representation.	AVM CS	

6.2.1.7.2.3 RollingCounterOfVMMReceived

Requirement	SYS	Parameters
The system shall set the RollingCounterOfVMMReceived to the value of the last VMM message received from the AV. Section 8.1.3.3.5.3 contains the DE_RollingCounterOfVMMReceived Use and ASN.1 representation.	AVM CS	

6.2.1.7.2.4 VehicleContainerGenerationTime

Requirement	SYS	Parameters
The system shall include the vehicle container generation time to indicate the time at which the system has generated the container generation time for respective AV to be transmitted as part of the IMM. Section 8.1.3.3.5.4 contains the DF_VehicleContainerGenerationTime Use and ASN.1 representation.	AVM CS	

6.2.1.7.2.5 VehicleContainerGenerationTimeConfidence

Requirement	SYS	Parameters
The system shall include the time confidence at which vehicle container generation time is generated for respective AV to be transmitted as part of the IMM. Section 8.1.3.3.5.5 contains the DE_VehicleContainerGenerationTimeConfidence Use and ASN.1 representation.	AVM CS	

6.2.1.7.2.6 IMMProprietaryExtensionField

Requirement	SYS	Parameters
The system shall include the proprietary extension field for respective AV to be transmitted as part of the IMM to indicate any specific proprietary AVM operation between the system and the respective AV. Section 8.1.3.3.5.6 contains the DE_IMMProprietaryExtensionField Use and ASN.1 representation.	AVM CS	

6.2.1.8 AVM CS Identity Management E2EProtection

6.2.1.8.1 Minimum Content

Requirement	SYS	Parameters
The AVM CS Identity Management E2EProtection data of Vehicle Container Data provided by the system shall meet the minimum content specified in Table 9 .	AVM CS	

Table 9 - Minimum AVM CS identity management E2EProtection content

Data Exchange Item	Type	Required for Tx	Can be Set to Unknown or Unavailable
AVMCSIdentityManagementE2EProtection	SEQ	No	-
E2ELength	DE	Yes	No
E2EChecksum	DE	Yes	No
E2EPublicKey	DE	Yes	No
E2ERandomIncrementer	DE	Yes	No
E2EDataID	DE	No	No

6.2.1.8.2 AVMCSIdentityManagementE2EProtection

Requirement	SYS	Parameters
The system shall be capable of supporting End-to-End Protection for AVM CS Identity Management Data to check if all data bits are received or if any of data bits are lost or if any data bits are flipped or if errors occur during transmission within IMM from Functional Safety aspects. Section 8.1.3.3.6 contains the DF_AVMCSIdentityManagementE2EProtection Use and ASN.1 representation.	AVM CS	

6.2.1.9 AVM CS IMM Identity Management

6.2.1.9.1 Minimum Content

Requirement	SYS	Parameters
The AVM CS IMM Identity Management data of Vehicle Container Data provided by the system shall meet the minimum content specified in Table 10 .	AVM CS	

Table 10 - Minimum AVM CS IMM identity management data content

Data Exchange Item	Type	Required for Tx	Can be Set to Unknown or Unavailable
AVMCSIdentityManagementData	SEQ	Yes	-
AVMVehicleID	DE	Yes	No
AVMSessionID	DE	No	No
AVMMissionID	DE	No	No
AVMFacilityID	DE	No	No

6.2.1.9.2 AVMCSIdentityManagementData

Requirement	SYS	Parameters
The system shall set the identifiers of the Identity Management to support for automated vehicle operation with respective AV over Infrastructure Marshalling Message. Section 8.1.3.3.7 contains the DF_AVMCSIdentityManagementData Use and ASN.1 representation.	AVM CS	

6.2.1.10 Feature Flow Command E2EProtection

6.2.1.10.1 Minimum Content

Requirement	SYS	Parameters
The Feature Flow Command E2EProtection data of Vehicle Container Data provided by the system shall meet the minimum content specified in Table 11 .	AVM CS	

Table 11 - Minimum feature flow command E2EProtection content

Data Exchange Item	Type	Required for Tx	Can be Set to Unknown or Unavailable
FeatureFlowCommandE2EProtection	SEQ	No	-
E2ELength	DE	Yes	No
E2EChecksum	DE	Yes	No
E2EPublicKey	DE	Yes	No
E2ERandomIncrementer	DE	Yes	No
E2EDataID	DE	No	No

6.2.1.10.2 FeatureFlowCommandE2EProtection

Requirement	SYS	Parameters
The system shall be capable of supporting End-to-End Protection for Feature Flow Command to check if all data bits are received or if any of data bits are lost or if any data bits are flipped or if errors occur during transmission within IMM from Functional Safety aspects. Section 8.1.3.3.8 contains the DF_FeatureFlowCommandE2EProtection Use and ASN.1 representation.	AVM CS	

6.2.1.11 Feature Flow Command

6.2.1.11.1 Minimum Content

Requirement	SYS	Parameters
The Feature Flow Command data of Vehicle Container Data provided by the system shall meet the minimum content specified in Table 12 .	AVM CS	

Table 12 - Minimum feature flow command data content

Data Exchange Item	Type	Required for Tx	Can be Set to Unknown or Unavailable
FeatureFlowCommand	DE	Yes	No

6.2.1.11.2 FeatureFlowCommand

Requirement	SYS	Parameters
The system shall set the Feature Flow Command which describes the AVM CS and respective AV feature lifecycle it is performing for the automated vehicle operations over Infrastructure Marshalling Message. Section 8.1.3.3.9 contains the DE_FeatureFlowCommand Use and ASN.1 representation.	AVM CS	

6.2.1.12 Vehicle Identification Command Data E2EProtection

6.2.1.12.1 Minimum Content

Requirement	SYS	Parameters
The Vehicle Identification Command Data E2EProtection data of Vehicle Container Data provided by the system shall meet the minimum content specified in Table 13 .	AVM CS	

Table 13 - Minimum vehicle identification command data E2EProtection content

Data Exchange Item	Type	Required for Tx	Can be Set to Unknown or Unavailable
VehicleIdentificationCommandDataE2EProtection	SEQ	No	-
E2ELength	DE	Yes	No
E2EChecksum	DE	Yes	No
E2EPublicKey	DE	Yes	No
E2ERandomIncrementer	DE	Yes	No
E2EDataID	DE	No	No

6.2.1.12.2 VehicleIdentificationCommandDataE2EProtection

Requirement	SYS	Parameters
The system shall be capable of supporting End-to-End Protection for Vehicle Identification Command Data to check if all data bits are received or if any of data bits are lost or if any data bits are flipped or if errors occur during transmission within IMM from Functional Safety aspects. Section 8.1.3.3.10 contains the DF_VehicleIdentificationCommandDataE2EProtection Use and ASN.1 representation.	AVM CS	

6.2.1.13 Vehicle Identification Command

6.2.1.13.1 Minimum Content

Requirement	SYS	Parameters
The Vehicle Identification Command data of Vehicle Container Data provided by the system shall meet the minimum content specified in Table 14 .	AVM CS	

Table 14 - Minimum vehicle identification content

Data Exchange Item	Type	Required for Tx	Can be Set to Unknown or Unavailable
VehicleIdentificationCommandData	CHC	Conditional	-
AVMCSBlinking	SEQ	Yes	-

6.2.1.13.2 VehicleIdentificationCommandData

Requirement	SYS	Parameters
The system shall include the Vehicle Identification Command to support AV identification process of automated vehicle operation for the respective AV from AVM CS over Infrastructure Marshalling Message. Section 8.1.3.3.11 contains the DF_VehicleIdentificationCommandData Use and ASN.1 representation.	AVM CS	

6.2.1.14 Blinking

6.2.1.14.1 Minimum Content

Requirement	SYS	Parameters
The Blinking of Vehicle Identification Command Data provided by the system shall meet the minimum content specified in Table 15 .	AVM CS	

Table 15 - Minimum blinking data content

Data Exchange Item	Type	Required for Tx	Can be Set to Unknown or Unavailable
AVMCSBlinking	SEQ	Yes	-
CSPublicKeyBlinking	DE	Conditional	No
CodeLength	DE	Conditional	No
BlinkingCommandRequest	DE	Yes	Yes
CodeBitIntervalRequest	DE	Conditional	No
SyncBitIntervalRequest	DE	Conditional	No