TECHNICAL SPECIFICATION

ISO/TS 23374-2

First edition
2023-08

Intelligent transport systems — Automated valet parking systems (AVPS) —

Part 2: Security integration for type 3 AVP

Systèmes de transport intelligents — Systèmes de parking avec voiturier automatisé (AVPS) —

Partie 2: Intégration de la sécurité pour les AVP de type 3

Reference number
ISO/TS 23374-2:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO *[had/had not]* received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*.

A list of all parts in the ISO 23374 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

An automated valet parking system (AVPS) automatically operates unoccupied vehicles from the drop off area where the driver and passengers leave the vehicle, and returns the vehicle to a pickup area upon the user's request to retrieve the vehicle.

AVPS is expected to contribute to:

— enhanced user experience,

— a reduction in accidents,

— the lowering of energy consumption and CO_2 emissions whilst vehicles search for available parking spaces, and

— the effective use of land through parking of vehicles in dense spaces.

As for any kind of automated traffic, AVPS is susceptible to attacks and malfunctioning, which can affect the safety of human life and other properties. Thus, security is an essential prerequisite for deployment of AVPS. Furthermore, it is essential to avoid the proliferation of security means in order to ensure that the overall C-ITS/CCAM (cooperative, connected and automated mobility) security systems remain manageable, and to ensure interoperability.

The aim of this document is to contribute to the realization of secure level 4 driverless operation of vehicles within parking facilities, and to support a fast and smooth market introduction by achieving interoperability among vehicles provided by different manufactures and within different parking facilities.

Clause 6 of this document addresses specifications of basic security requirements for AVPS related to identified operation interfaces and management interfaces. This is complemented by the information in Clause 5 and three informative annexes.

Intelligent transport systems — Automated valet parking systems (AVPS) —

Part 2:
Security integration for type 3 AVP

1 Scope

This document specifies security means and procedures for AVPS Type 3 as specified in ISO 23374-1. It focuses on operation interfaces and management interfaces as defined in ISO 23374-1.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 23374-1:2023, *Intelligent transport systems — Automated valet parking systems (AVPS) — Part 1: System framework, requirements for automated driving and for communications interface*

ISO/SAE 21434, *Road vehicles — Cybersecurity engineering*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 23374-1 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
subject vehicle
SV
light vehicle which is equipped with the vehicle operation sub-system of an automated valet parking system (AVPS)

[SOURCE: ISO 23374-1:2023, 3.4]

3.2
parking facility
public or private car park in which an automated valet parking system (AVPS) is available

Note 1 to entry: An AVPS does not necessarily have to be available in the entire favility in order to achieve conformance to this document. For example, it is possible for only a certain floor within a multi-story parking facility to be dedicated to an AVPS.

[SOURCE: ISO 23374-1:2023, 3.5, modified — Note 2 to entry removed.]

3.3
operation zone
single or multiple geographical area(s) within a parking facility where automated driving can be performed by an automated valet parking system (AVPS)

[SOURCE: ISO 23374-1:2023, 3.6, modified — Notes 1 and 2 to entry removed.]

3.4
drop-off area
location within the operation zone where the user leaves the subject vehicle (SV) and hands over authority to the service provider

[SOURCE: ISO 23374-1:2023, 3.7, modified — Notes 1 and 2 to entry removed.]

3.5
pick-up area
location within the operation zone where the service provider sends the subject vehicle (SV) to the user for boarding and hands over authority

[SOURCE: ISO 23374-1:2023, 3.8, modified — Notes 1 and 2 to entry removed.]

3.6
destination
location within the operation zone to which the subject vehicle (SV) is transferred

Note 1 to entry: For example, parking slots delineated by line markers, service bays (e.g. location beside an electric vehicle charging stations), or a pick-up area can be a destination.

[SOURCE: ISO 23374-1:2023, 3.11, modified — Original Note 1 to entry removed. New Note 1 to entry added.]

3.7
parking area
area within the operation zone consisting of multiple parking spots

[SOURCE: ISO 23374-1:2023, 3.10, modified — Note 1 to entry removed.]

3.8
parking facility equipment
PFE
physical equipment installed in the parking facility for supporting an automated valet parking system (AVPS)

EXAMPLE Communication devices and detection sensors.

[SOURCE: ISO 23374-1:2023, 3.15, modified — Preferred term changed from "automated valet parking facility equipment" to "parking facility equipment".]

3.9
designed speed
physical speed of a subject vehicle (SV) which changes dynamically under the given circumstances under which an automated valet parking system (AVPS) intends to operate while performing automated driving

Note 1 to entry: For example, the AVPS will adjust the SV's operating speed when travelling towards a corner with limited visibility due to occlusion by a wall. This speed depends on the system design. For this reason, most of the test procedures in this document do not specify a specific value and only refer to the "designed speed".

3.10
designed distance
physical distance from the subject vehicle (SV) to an object that an automated valet parking system (AVPS) intends to maintain under the given circumstances while performing automated driving

[SOURCE: ISO 23374-1:2023, 3.19, modified — "Situation-specific" removed from the beginning of the definition; "other facility users, objects or structures" replaced by "an object"; Note 1 to entry removed.]

3.11
sub-system
component of an automated valet parking system (AVPS) at a logical level which includes one or more functions

[SOURCE: ISO 23374-1:2023, 3.21, modified — Note 1 to entry removed.]

3.12
function
smallest composition of an automated valet parking system (AVPS) described in this document which contributes to the system outputs

3.13
state
<system> mutually exclusive condition that each vehicle managed by an automated valet parking system (AVPS) is in

3.14
reservation ID
unique identifier for an established agreement between a user and a service provider to hand over the subject vehicle (SV)'s authority to an automated valet parking system (AVPS) within a specific parking facility

Note 1 to entry: A single reservation ID could be used over a period of time, or could be destroyed each time it is used.

3.15
session ID
unique identifier given each time an authority handover occurs, and destroyed when authority handback occurs

3.16
mission ID
unique identifier given each time a subject vehicle (SV) is given a new destination

4 Abbreviated terms

For the purposes of this document, the abbreviated terms given in ISO 23374-1 and the following apply.

AVP	automated valet parking
AVPS	automated valet parking system
CCAM	cooperative, connected and automated mobility
CRC	cyclic redundancy check
DoS	denial of service
DTLS	datagram transport layer security
ESP	encapsulating security payload

HoL	head-of-line
IKE	internet key exchange
OB	operator backend
OEDR	object and event detection and response
OEM	original equipment manufacturer
PFE	parking facility equipment
PKI	public key infrastructure
RSU	roadside unit
SA	security association
SV	subject vehicle
TCP	Transport Control Protocol
TLS	transport layer security
UB	user backend
UDP	User Datagram Protocol
VB	vehicle backend
VIN	vehicle identification number
VMC	vehicle motion control
WAVE	wireless access in vehicular environments
WMI	world manufacturer identifier

5 General

5.1 Basic operation model of AVPS

5.1.1 Basic functionalities

The basic functionalities of AVPS can be described as the operation functions of an automated vehicle and the management functions of system participants. Table 1 describes these basic functionalities of AVPS.

— Performance requirements associated with the operation functions are specified in ISO 23374-1:2023, Clause 6.

— General requirements associated with the management functions are specified in ISO 23374-1:2023, Clause 7.

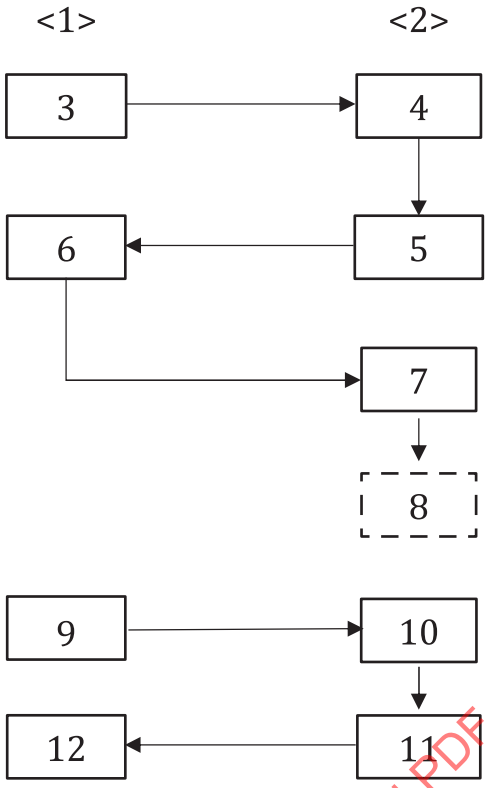
Table 1 — Basic functionalities of AVPS and their description

Basic functionalities	Description
Operation functions of an automated vehicle	— Determine a destination and route — Perform level 4 automated driving — Respond to commands of the system management functionalities
Management functions of system participants	— Manage environmental conditions — Check the compatibility between vehicles and facilities — Identify the correct SV as the communication participant — Remotely engage and disengage an SV — Perform remote assistance when necessary — Issue command to stop the operation when necessary — React upon incapacitation of the automated vehicle operation — Processes user requests

5.1.2 Basic operation flow

Figure 1 describes the basic flow of AVPS based on the user action and the system reaction.

Figure 1 describes the flow in which the user initially hands over authority to the service provider as a representative use case. AVPS can also be utilized for services in which the service provider initially hands over authority to the user (e.g. rental car services). Re-parking is an optional process and not always required to complete the flow.



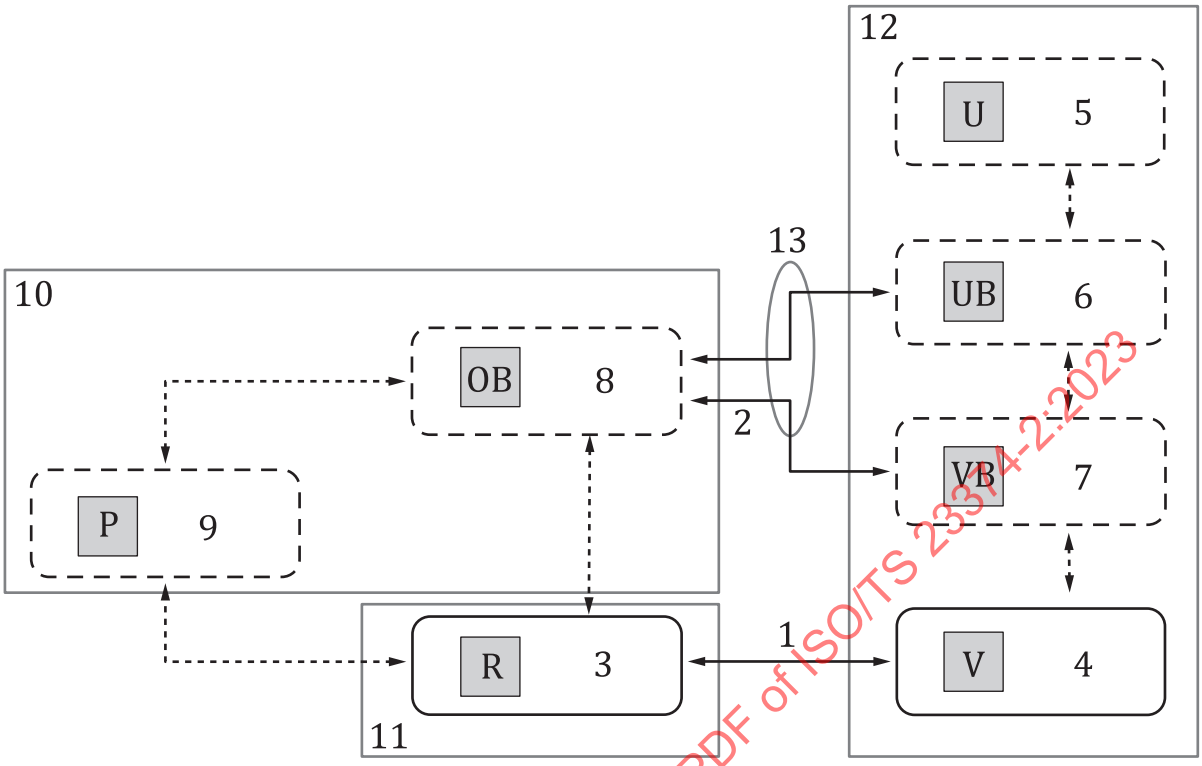
Key

1	user action	2	system reaction
3	requests availability	4	checks vacancy and compatibility
5	identifies SV and initiates check-in procedure	6	hands over authority
7	automated vehicle operation (entering)	8	automated vehicle operation (re-parking)
9	requests retrieval	10	automated vehicle operation (exiting)
11	initiates check-out procedure	12	receives authority

Figure 1 — Basic flow of AVPS

5.1.3 Example functional allocation of logical architecture in AVPS

Figure 2 shows an example image of functional allocation of logical architecture in AVPS.



Key

1	operation interface	2	management interfaces
3	remote vehicle operation	4	on-board vehicle operation
5	user frontend	6	user backend
7	vehicle backend	8	operator backend
9	automated valet parking facility management	10	service server
11	RSU	12	in vehicle
13	internet		

NOTE See Table 2 for definitions of abbreviated terms used in this figure.

Figure 2 — Example functional allocation of logical architecture in AVPS

Table 2 shows the functional allocations described in ISO 23374-1:2023, 5.3.

Table 2 — Functional allocation

ID [a]	Sub-system	Role	Main functions	Remarks
R	Remote vehicle operation	Performs automated vehicle operation	— SV identification. — Destination assignment. — Route planning. — OEDR. — Localization of SV. — Path determination. — Trajectory calculation. — Vehicle motion control. — Emergency stopping.	The functional allocation between the two vehicle operation sub-systems differs depending on the vehicle operation type.
V	On-board vehicle operation			
U	User frontend	Interface to the user	— Sends user requests. — Receives and updates vehicle status to user.	
UB	User backend	Manages the system participants	— User request processing.	The three backend sub-systems cooperate to respond to user requests (e.g. retrieval of vehicles).
VB	Vehicle backend		— Remote engagement/disengagement.	
OB	Operator backend		— Manages parking facility availability. — Checks compatibility between SV and parking facility. — Dispatches SVs into driverless operation. — Performs remote assistance.	
P	Automated valet parking facility management		— Manages environmental conditions. — Responds to incapacitation of the operation functions.	

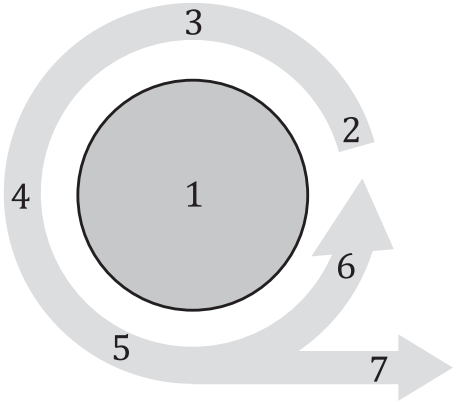
[a] See Figure 2.

5.2 Security lifecycle

ISO/SAE 21434 describes the lifecycle phases of the overall cybersecurity risk management (see Figure 3).

This document refers to the overall cybersecurity risk management described in ISO/SAE 21434.

The AVP functionality within the vehicle preferably is engineered with a security engineering process conforming to ISO/SAE 21434.



Key

1	cybersecurity risk management	2	concept
3	product development	4	production
5	operation	6	maintenance
7	decommissioning/end of cybersecurity support		

Figure 3 — Overall cybersecurity risk management (described in ISO/SAE 21434)

6 Security requirements

6.1 Security requirements for AVPS

Threats and risks concerning AVPS are evaluated in Annex C.

Like any kind of level 4 automated driving service, AVPS is susceptible to attacks and malfunctioning, which can affect the safety of human life and property. Thus, security is an essential prerequisite for the deployment of AVPS.

Within this context, security management for in-vehicle systems shall conform to ISO/SAE 21434.

Furthermore, security for roadside and service servers shall be strong against attacks, especially for type 2 operation.

Specific security methods for in-vehicle and in-roadside and server systems are out of scope of this document. Existing applicable security methods are presented in Annex B.

6.2 Security requirements on AVPS communication

6.2.1 General

The result of the risk analysis shows that the risk values related to AVPS communication between [R] and [V] or [OB] and [VB/UB] are critical and major.

This means that the communication paths in AVPS need to be carefully secured.

AVPS shall perform end-to-end protection of all information assets from threats in the whole system.

Communication paths with direct communications between vehicles or user terminals such as smart phones, i.e. between the [OB] sub-system and [VB]/[UB] sub-system (see Figure 2 and Table 2), are designed by service providers. Specific protocols are chosen by service providers and shall be secured by applying methods as used for general internet applications.

Communication paths between sub-systems are implemented in service servers and shall be secured applying methods as used for general purpose applications.

Annex B shows a list of secured communication protocols which are candidates for use.

If implemented as localized communications, secure communications for AVP, i.e. the communication paths between [R] and [V], and between [OB] and [VB/UB], shall use a public key infrastructure (PKI).

Subclauses 6.2.2 to 6.2.4 specify general security requirements for AVPS communications.

To meet the following requirements, AVPSs communication shall at least apply a signature verification function.

Both infrastructures and vehicles need to verify the validity in every access. The methodology of AVPS communication, at least for localized communications, shall be based on a PKI.

6.2.2 Confidentiality

Every message exchanged over a management interface shall be encrypted and protected to prevent information disclosure. It shall not be possible for an unauthorized entity to reveal the messages within AVPS communication paths.

Every message exchanged over an operation interface should be encrypted and protected to prevent information disclosure. It should not be possible for an unauthorized entity to reveal the messages within AVPS communication paths.

6.2.3 Integrity

All parts of messages shall be secured to ensure completeness, accuracy and absence of unauthorized modifications. It shall be possible to verify and validate the integrity of all parts of messages, and messages shall be protected against unauthorized modification and deletion.

6.2.4 Availability

All entities in the messages shall be readily accessible as the authorized information at all accesses.

6.2.5 Authentication

Authentication is required before establishing a session.

Annex A
(informative)

Communication sequences

A.1 General

The communication sequences presented in Figures A.2 to A.14 define the sequential flow of messages composed of the minimum set of data elements defined in Tables A.1 to A.13 and Tables A.23 to A.26. Different sequences for one transition can be communicated in arbitrary order.

The messages and data elements are defined on a logical level with their respective units. This way, interoperability of the solutions in the field can be achieved without specifying a byte-level message format and protocol, enabling different carrier technologies in different markets, while minimizing the functional impact of low-level technology choices on the overall system.

Figure A.1 shows the legend to be used for understanding the communication sequence charts shown in Figures A.2 through A.14.

Arrows connecting the sub-systems represent a message. The minimum set of data elements to be communicated within each message with solid lines are provided in the "Relevant message" column of corresponding tables. Messages represented by broken lines describe the flow of data. Numbers within brackets of the "Relevant message" column of each table indicate that the respective data element is expected to be communicated between the sub-systems. These solid and broken line representations are identical to those shown in Figure 2.

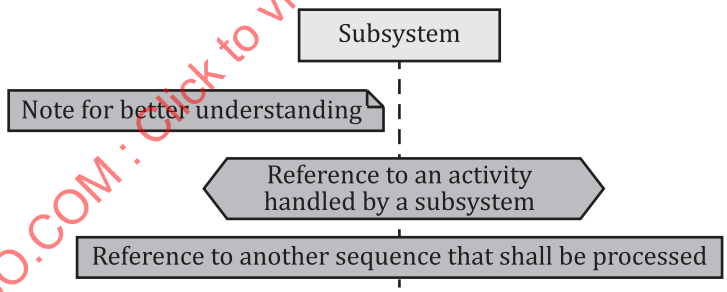
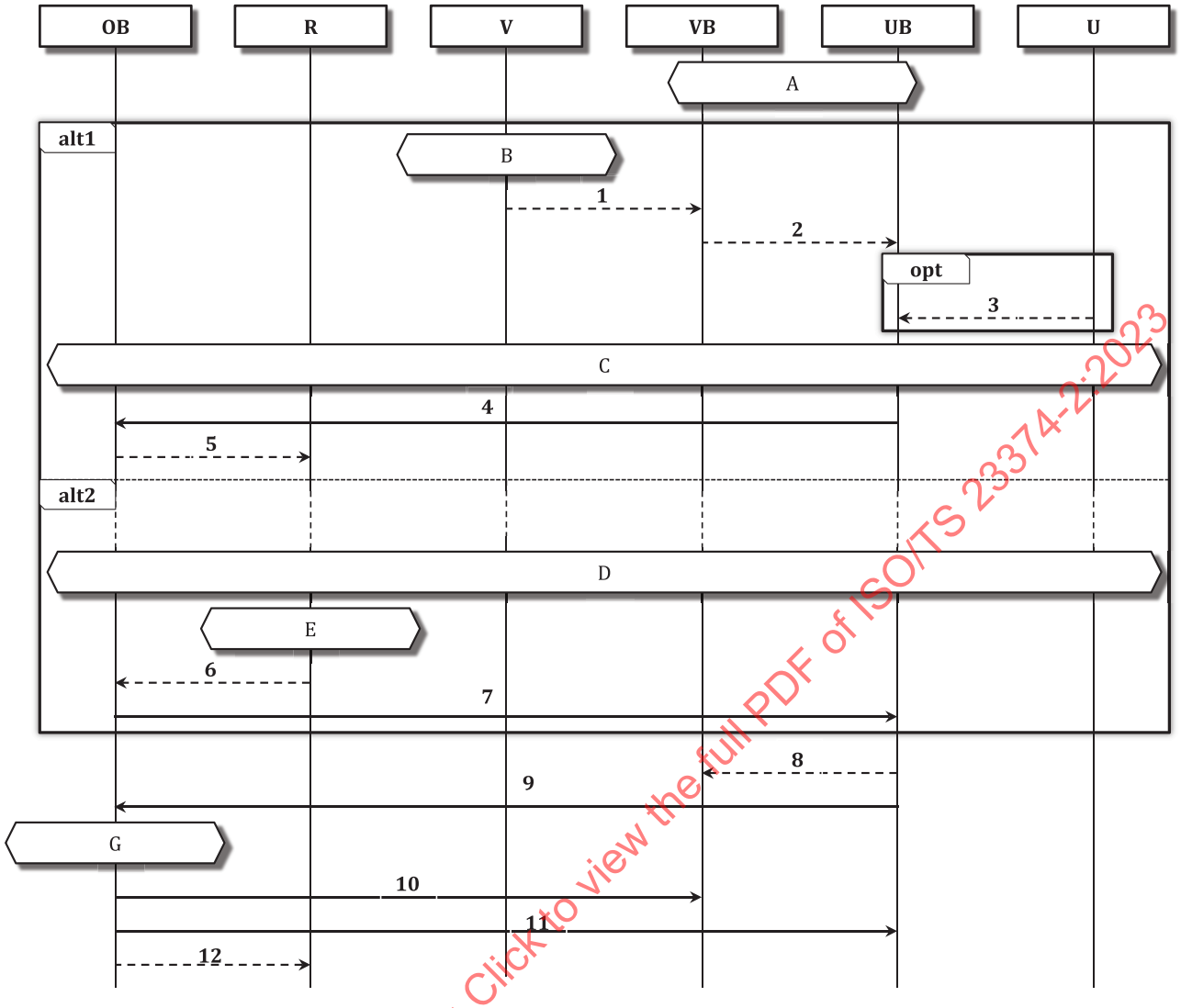


Figure A.1 — Legend

A.2 Communication sequences which trigger a state transition

A.2.1 Check-in sequence



Key

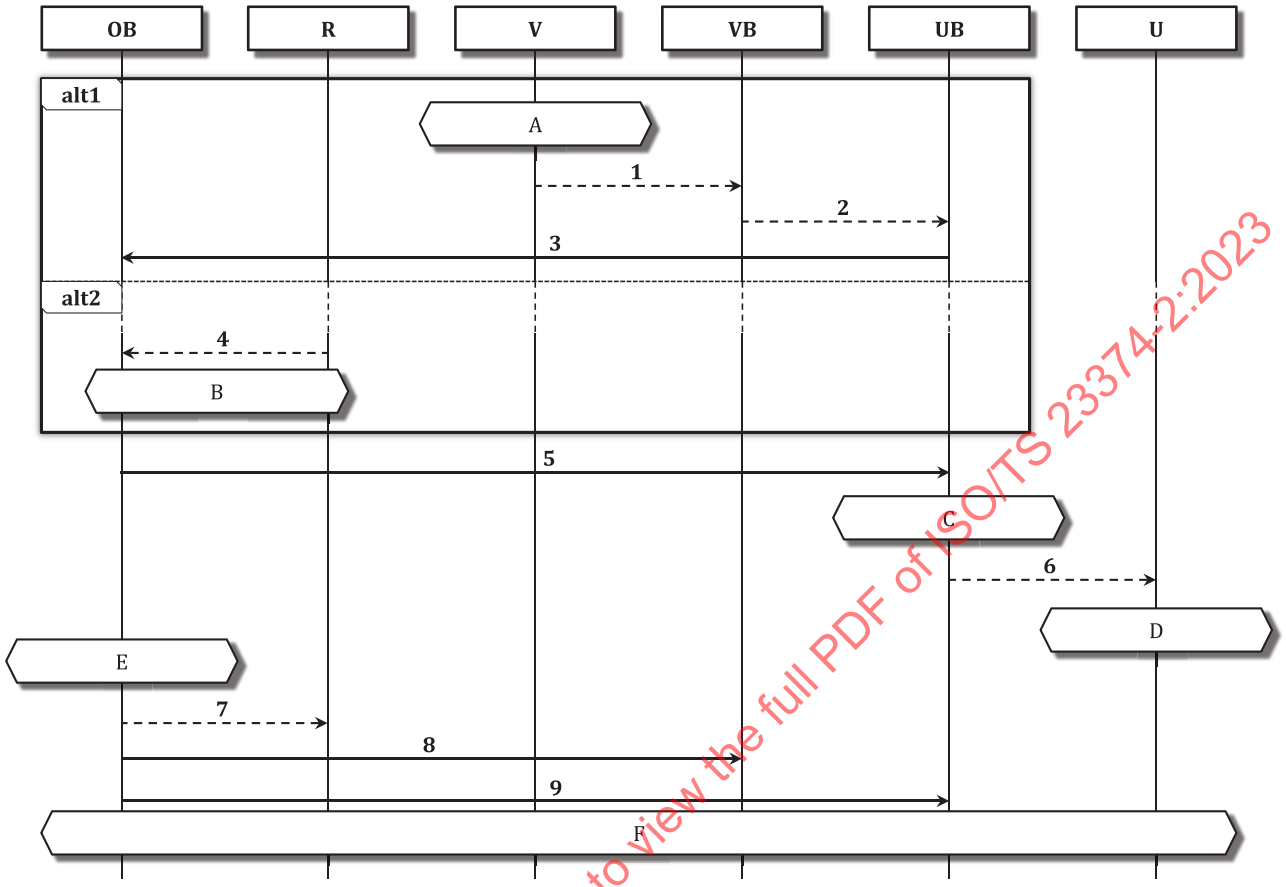
OB	Operator_Backend	R	Remote_Vehicle_Operation
V	Onboard_Vehicle_Operation	VB	Vehicle_Backend
UB	User_Backend	U	User_Frontend
A	User is known and associated with SV	B	Recognizes SV arrival at reserved parking facility
C	AVPS confirms reservation	D	AVPS confirms reservation
E	Recognizes SV arrival at reserved parking facility	G	Create Session_ID
1	SV reached parking facility (FACILITY_ID)	2	SV reached parking facility (SV_ID, FACILITY_ID, OEM_ID)
3	User confirms arrival	4	SV reached parking facility (SV_ID)
5	SV reached parking facility (SV_ID)	6	SV reached parking facility (SV_ID)
7	SV reached parking facility (SV_ID)	8	Reservation Data (Reservation_ID, OEM_ID, SV_ID…)
9	Reservation Data (Reservation_ID, OEM_ID, SV_ID…)	10	Communicate Session_ID (Session_ID)
11	Communicate Session_ID (Session_ID)	12	Communicate Session_ID (Session_ID) (Used AVP protocol version, [Type1 Used vehicle map version])

Figure A.2 — Check-in sequence

Table A.1 — Description of data elements of Figure A.2

Data element	Unit	Value range	Description	Relevant message
Reservation_ID	UID	large enough to identify single session for the legally required storage time in a market	Unique reservation identifier created by AVP_Backend after successful reservation of one SV	9 (8)
OEM_ID	UID	3 Bytes alphanumerical – I, O and Q excluded	Unique manufacturer identifier based on WMI (ISO 3780)	9 (2, 8)
SV_ID	fixed length hash	≥128 bits	Salted hash based on unique vehicle identifier (VIN)	4, 6, 7, 9 (2, 5, 6, 8)
Facility_ID	UID	unique to a market	Unique facility identifier created by OB sub-system	9 (1, 2, 8)
AVP_Session_ID	UID	large enough to identify single session for the legally required storage time in a market	Unique identifier for management of one SV from the time of check-in until the time of check-out	10, 11 (12)
AVP_Timestamp	Unix Time	64 bits	Synchronized point in time	all

A.2.2 Check-out sequence



Key

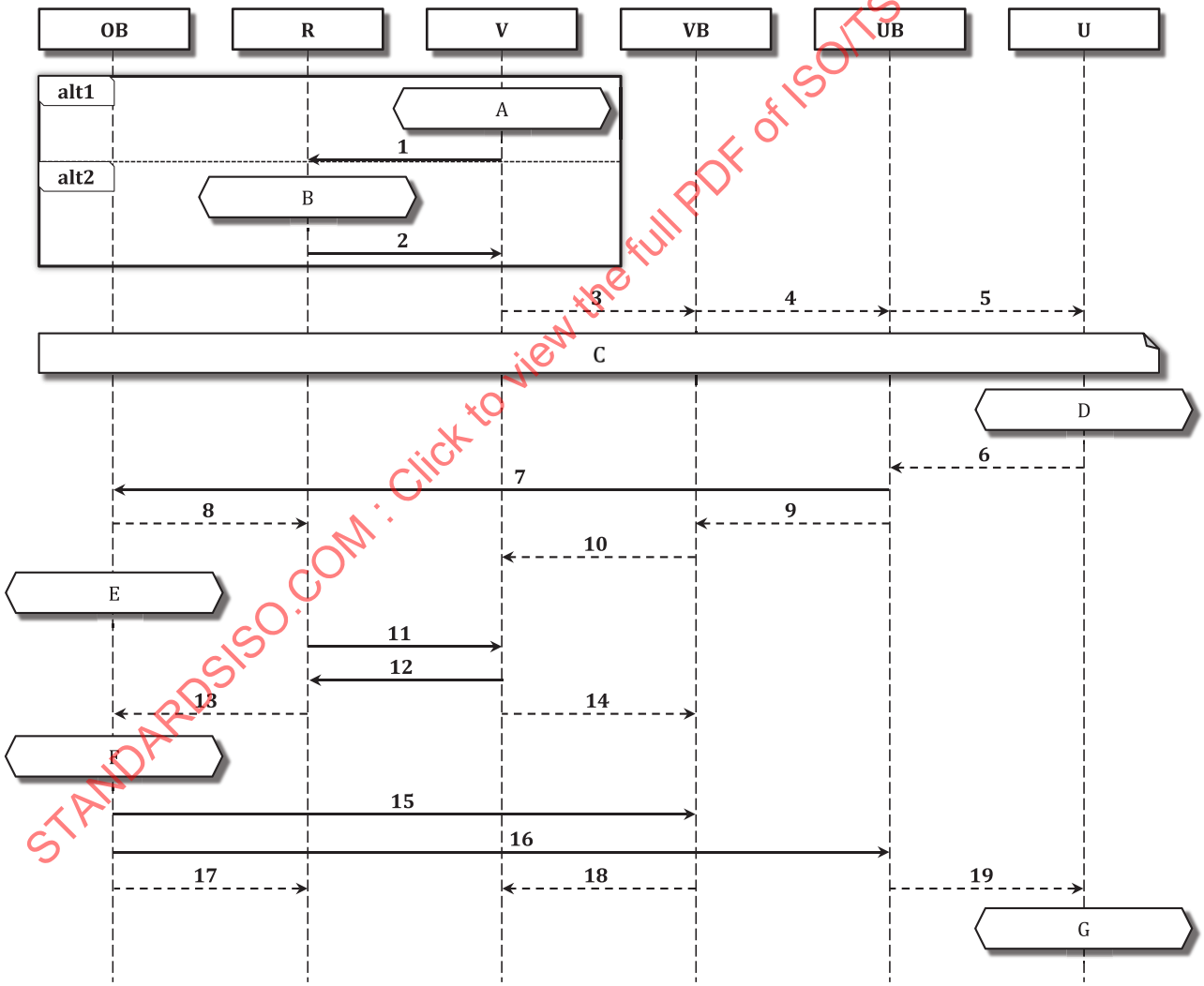
OB	Operator_Backend	R	Remote_Vehicle_Operation
V	Onboard_Vehicle_Operation	VB	Vehicle_Backend
UB	User_Backend	U	User_Frontend
A	Recognizes SV has left parking facility	B	Recognizes SV has left parking facility or is deactivated (failed recovery)
C	Process checkout	D	Display check-out result
E	Revoke Session_ID	F	Update reservation
1	SV left parking facility	2	SV left parking facility
3	SV left parking facility	4	SV left parking facility
5	Check-out report (Session_ID, Provided_Services)	6	Check-out result (e.g. duration, Provided_Services)
7	Close session (Session_ID)	8	Close session (Session_ID)
9	Close Session (Session_ID)		

Figure A.3 — Check-out sequence

Table A.2 — Data elements of Figure A.3

Data element	Unit	Value range	Description	Relevant message
AVP_Session_ID	UID	large enough to identify single session for the legally required storage time in a market	Unique identifier for management of one SV from the time of check-in until the time of check-out	5, 8, 9 (7)
Services_Provided	List of Service Objects	no recommendation	List of information objects containing name, duration and price of services provided during session	5 (6)
AVP_Timestamp	Unix Time	64 bits	Synchronized point in time	all

A.2.3 Handover sequence



Key

OB Operator_Backend
R Remote_Vehicle_Operation
V Onboard_Vehicle_Operation
VB Vehicle_Backend
UB User_Backend
U User_Frontend
A Recognizes SV arrival at drop-off area
B Local sub-system recognizes SV arrival at drop-off area
C User leaves SV
D Receives user command to hand over authority

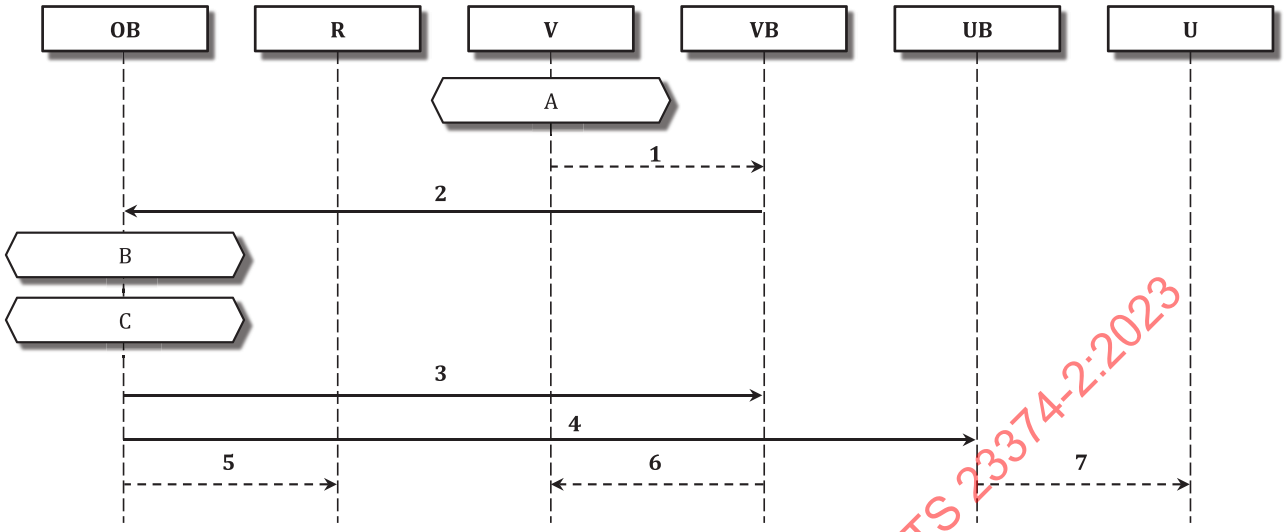
E	Record handover by user	F	Determine system authority
G	Inform handover result (successful or error)		
1	SV in drop-off area	2	SV in drop-off area
3	Notify readiness	4	Notify readiness
5	Notify readiness	6	Handover request
7	Handover request	8	Handover request
9	Handover request	10	Handover request
11	R-System L4Check results	12	V-System L4Check results
13	R-System L4Check results	14	R-System L4Check results
15	System authority (result)	16	System authority (result)
17	System authority (result)	18	System authority (result)
19	System authority (result)		

Figure A.4 — Handover sequence

Table A.3 — Data elements of Figure A.3

Data element	Unit	Value range	Description	Relevant message
Dropoff_ID	UID	No recommendation	Identifier for drop-off zone, unique for one facility	1, 2
Infrastructure_L4_Status	Enum	1) OK 2) NOK 3) Unknown	Result from AVP Operator specific L4 test	11 (13, 14)
SV_L4_status	Enum	1) OK 2) NOK 3) Unknown	Result from OEM specific L4 test	12 (13, 14)
AVP_System_Authority	Enum	1) Established 2) Revoked 3) Unknown	Result of system authority transition to infrastructure as determined by AVP_Backend	7 (6, 8, 9, 10)
AVP_Timestamp	Unix Time	64 bits	Synchronized point in time	all

A.2.4 Handback sequence



Key

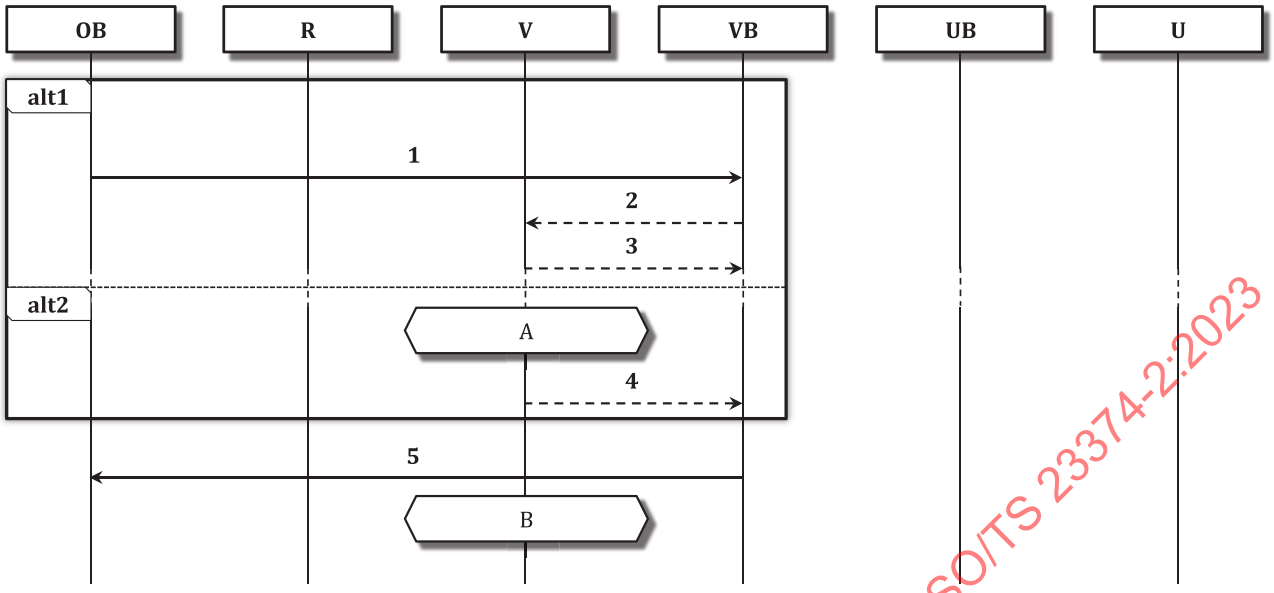
OB Operator_Backend
R Remote_Vehicle_Operation
V Onboard_Vehicle_Operation
VB Vehicle_Backend
UB User_Backend
U User_Frontend
A Recognizes user intent to regain authority
B Record user in vehicle
C Revoke system authority
1 User intent
2 User intent
3 System authority (revoked)
4 System authority (revoked)
5 System authority (revoked)
6 System authority (revoked)
7 System authority (revoked)

Figure A.5 — Handback sequence

Table A.4 — Data elements of Figure A.5

Data element	Unit	Value range	Description	Relevant message
User_Presence_Status	Enum	1) Present 2) Not present	Result of vehicle user presence test	2 (1)
AVP_System_Authority	Enum	1) Established 2) Revoked 3) Unknown	Result of system authority transition to infrastructure as determined by AVP_Backend	3, 4 (5, 6, 7)
AVP_Timestamp	Unix Time	64 bits	Synchronized point in time	All

A.2.5 Sleep sequence



Key

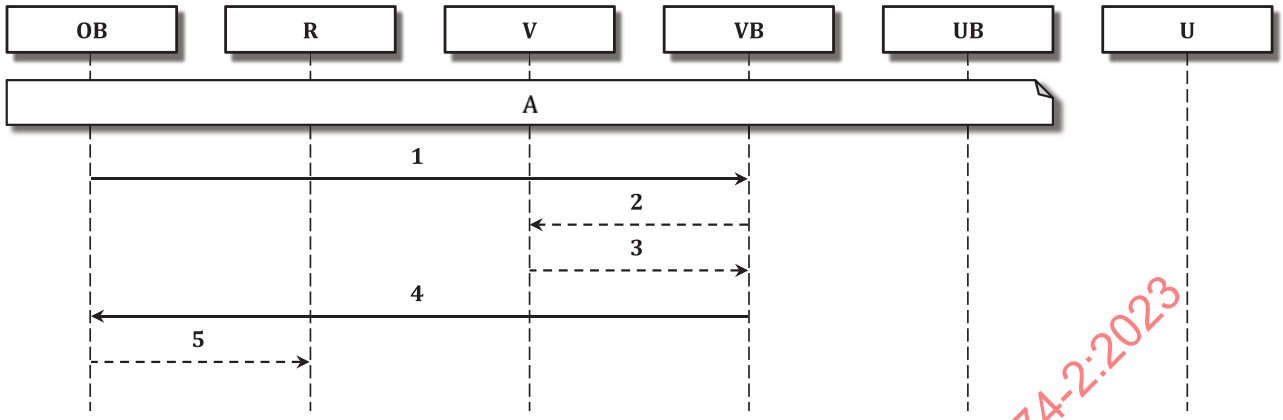
OB	Operator_Backend	R	Remote_Vehicle_Operation
V	Onboard_Vehicle_Operation	VB	Vehicle_Backend
UB	User_Backend	U	User_Frontend
A	Wait duration exceeded	B	Transition to sleep sub-state
1	Request sleep	2	Negotiate minimal power consumption
3	Engaging sleep	4	Engaging sleep
5	Sleep engaged (SV_Latest_Wake-up)		

Figure A.6 — Sleep sequence

Table A.5 — Data elements of Figure A.6

Data element	Unit	Value range	Description	Relevant message
Mission_ID	UID	no recommendation	Unique mission identifier created by AVP_Backend for a disengagement request	1, 5
SV_Latest_Wake-Up	Unix Time	64 bits	Time of latest possible successful wake-up for SV as determined by Vehicle_backend ("maximum sleep time")	5
AVP_Timestamp	Unix Time	64 bits	Synchronized point in time	all

A.2.6 Wake-up sequence



Key

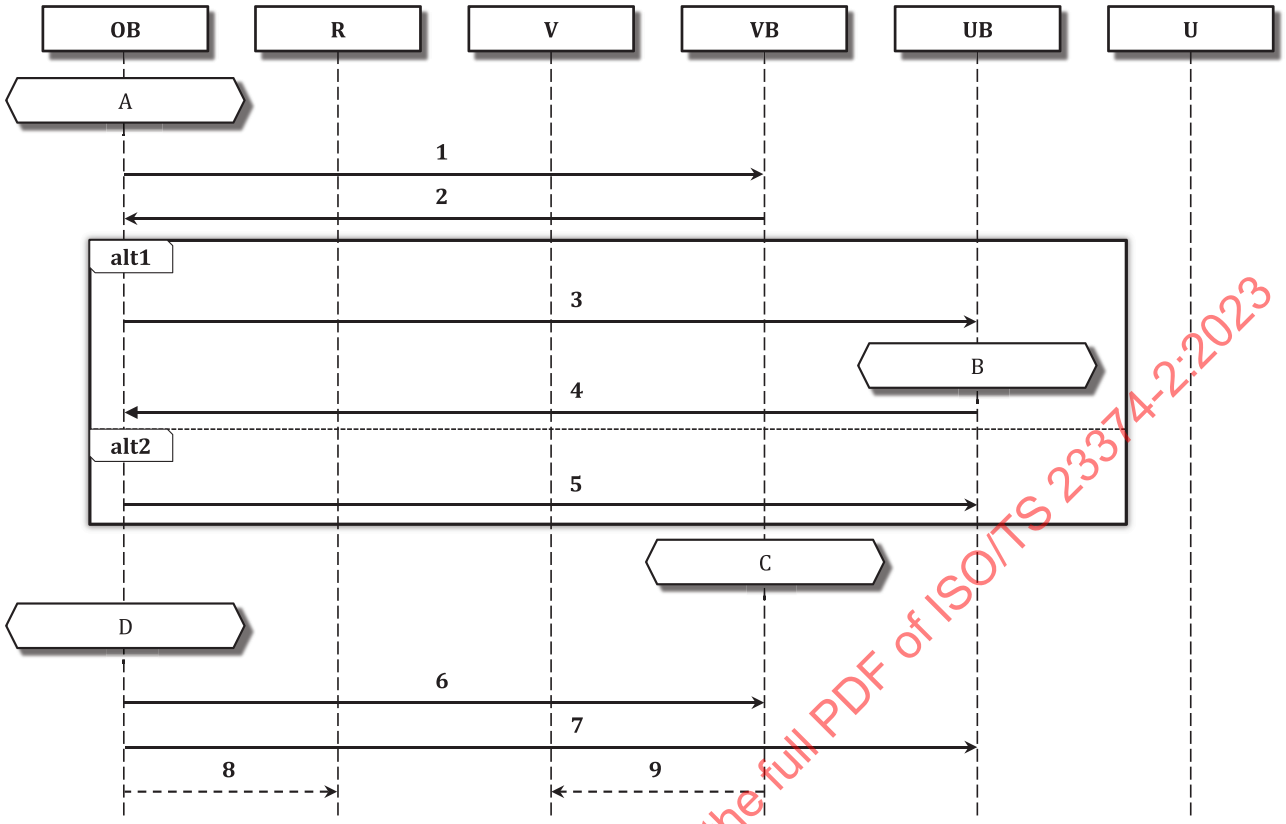
OB Operator_Backend
R Remote_Vehicle_Operation
V Onboard_Vehicle_Operation
VB Vehicle_Backend
UB User_Backend
U User_Frontend
A Mission confirmed by system
1 Request wake up (Mission_ID)
2 Wake up command (Mission_ID)
3 Result wake up (Mission_ID, Wake_Up_Result)
4 Result wake up (Mission_ID, Wake_Up_Result)
5 SV in standby state (SV_ID)

Figure A.7 — Wake-up sequence

Table A.6 — Data elements of Figure A.7

Data element	Unit	Value range	Description	Relevant message
Mission_ID	UID	no recommendation	Unique mission identifier within a session created by OB sub-system for an engagement request	1, 4 (2, 3)
SV_ID	Hashed UID	≥128 bit	Salted hash based on unique vehicle identifier (VIN)	(5)
Wake-Up_Result	Enum	1) Successful 2) Denied	Response to requested wake-up as determined by VB sub-system; in case of Denied, additional error code and reason has to be provided	4 (3)
AVP_Timestamp	Unix Time	64 bits	Synchronized point in time	all

A.2.7 Mission assignment sequence



Key

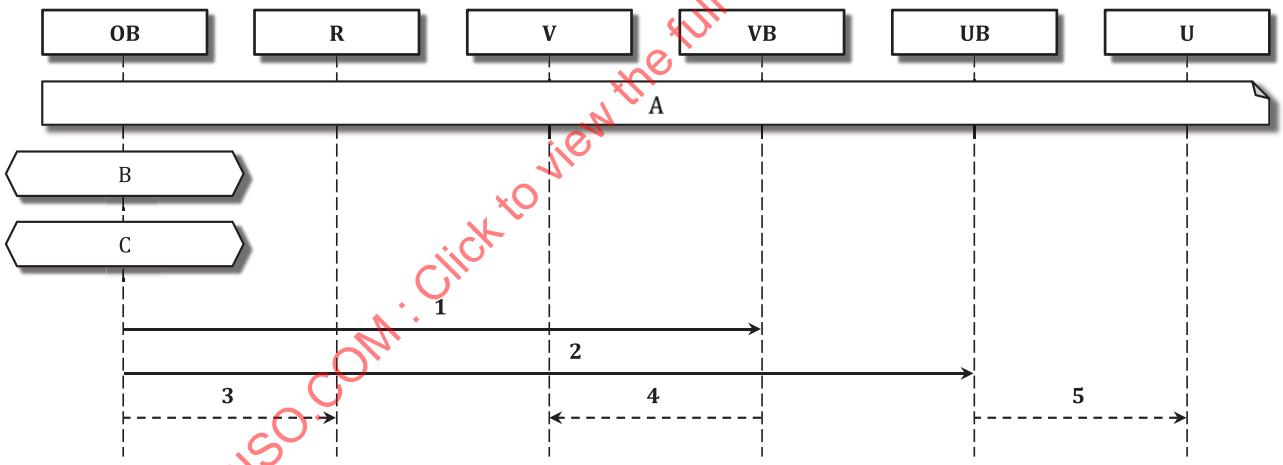
OB	Operator_Backend	R	Remote_Vehicle_Operation
V	Onboard_Vehicle_Operation	VB	Vehicle_Backend
UB	User_Backend	U	User_Frontend
A	Create Mission_ID	B	Determination if purpose suits interests of user
C	Determination if purpose is acceptable for SV and OEM	D	Record or revoke Mission_ID depending on determination of UB and VB
1	Mission request (Mission_ID, Purpose, Session_ID)	2	Mission OEM determination (Mission_ID, Session_ID)
3	Mission request (Mission_ID, Purpose, Session_ID)	4	Mission UB determination (Mission_ID, Session_ID)
5	Mission information (Mission_ID, Purpose, Session_ID)	6	Mission determination (Mission_ID, Purpose, Session_ID)
7	Mission determination (Mission_ID, Purpose, Session_ID)	8	Mission determination (Mission_ID)
9	Mission determination (Mission_ID)		

Figure A.8 — Mission assignment

Table A.7 — Data elements of Figure A.8

Data element	Unit	Value range	Description	Relevant message
AVP_Session_ID	UID	large enough to identify single session for the legally required storage time in a market	Unique identifier for management of one SV from the time of check-in until check-out	1, 2, 3, 4, 5, 6, 7
Mission_ID	UID	no recommendation	Unique mission identifier created by OB sub-system for an engagement request	1, 2, 3, 4, 5, 6, 7 (8, 9)
Mission_Purpose	Enum	0) Initial Parking 1) Retrieval 2) Repark 3) Charging 4) Car wash 5) Trunk delivery 6) xxy	Type identifier for mission purpose created by OB sub-system, only relevant for engagement request	1, 3, 5, 6, 7

A.2.8 Mission accomplished sequence



Key

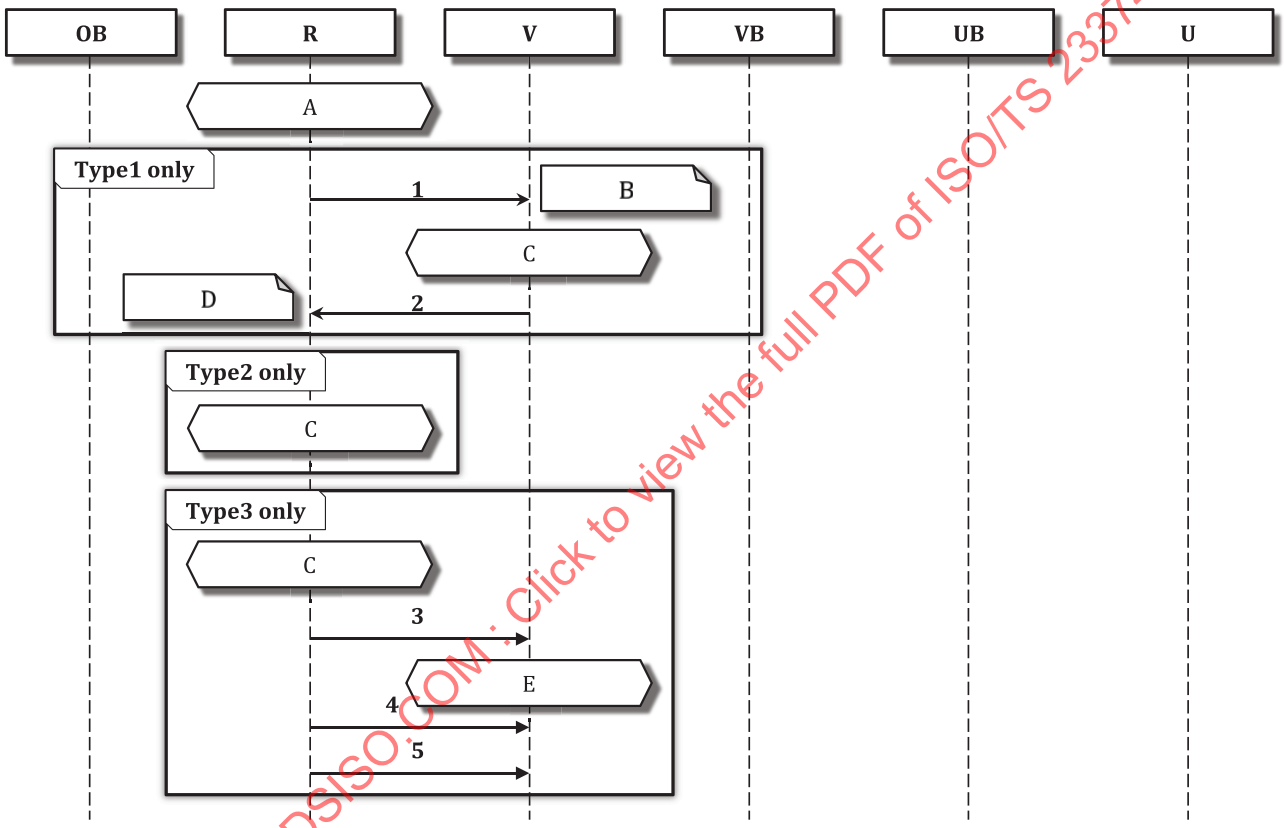
OB Operator_Backend
R Remote_Vehicle_Operation
V Onboard_Vehicle_Operation
VB Vehicle_Backend
UB User_Backend
U User_Frontend
A SV arrived at destination
B Determine and record
C Revoke Mission_ID
1 Mission finished (Mission_ID, Mission_Result)
2 Mission finished (Mission_ID, Mission_Result)
3 Mission finished (Mission_ID, Mission_Result)
4 Mission finished (Mission_ID, Mission_Result)
5 Mission finished (Mission_ID, Mission_Result)

Figure A.9 — Mission accomplished sequence

Table A.8 — Data elements of Figure A.9

Data element	Unit	Value range	Description	Relevant message
Mission_ID	UID	no recommendation	Unique mission identifier created by OB sub-system at the start of engagement request	1, 2 (3, 4, 5)
Mission_Result	Enum	1) Successful 2) Failed	Result of the accomplished mission created by OB sub-system; in case of Failed, additional error code and reason has to be provided	1, 2 (3, 4, 5)
AVP_Timestamp	Unix Time	64 bits	Synchronized point in time	all

A.2.9 Destination and route



Key

OB Operator_Backend
R Remote_Vehicle_Operation
V Onboard_Vehicle_Operation
VB Vehicle_Backend
UB User_Backend
U User_Frontend
A Target position determination
B Prohibited_Route_IDs include road conditions
C Route planning
D Sequence may be restarted if result is not valid
E Localization (initial)
1 Assign target (Target_ID, Service_POI_ID, Vis_Route_IDs, Prohibited_Route_IDs)
2 Send route result (SV_Route_IDs)
3 Landmark information delivery
4 Driving boundaries delivery
5 Route delivery

Figure A.10 — Destination and route sequence

Table A.9 — Data elements of Figure A.10

Data element	Unit	Value range	Description	Relevant message
Mission_ID	UID	no recommendation	Unique mission identifier created by AVP_Backend for an engagement request	1, 2
Target_ID	UID	no recommendation	Identifier of target semantic unique for target type within facility, Type 1 only	1
Target_Type	List of Enum	1) Parking spot 2) Drop-off/Pick-up 3) Parking section 4) Parking area 5) Segment for wait 6) Point of interest	Type identifier for specified target, Type 1 only	1
Behaviour_Constraints	List of Enum	1) Park forward 2) Park backward 3) Leave room to wall 4) Block parking 5) Precise positioning	Instruct SV to obey behaviour at target (e.g. to enable successful service), Type 1 only; "precise positioning" value means SV positioning priority is given to absolute map position (e.g. no influence of neighbouring vehicles)	1
Via_Route_Ids	List of UID	>16 elements	List of edge identifiers to be used in SV routing, only Type 1	1
Prohibited_Route_Ids	List of UID	>16 elements	List of edge identifiers prohibited for use in SV routing, only Type 1	1
SV_Route_Ids	List of UID	>64 elements to enable long transfers in complicated environments	SV route planning result considering possible via or prohibited edges, only Type 1	2
Landmark_ChangeFlag	Enum	1) New 2) Add	Set new landmarks for SV or add to existing, only Type 3	3
Landmarks_Count	Int	≥0	Number of Landmarks identified, only Type 3	3
Landmark Info	List of Landmarks	—	List of landmark items, only Type 3 See Table A.10	3
Landmark_Confirmation	Enum	1) OK 2) NG	Confirmation of landmark delivery, only Type 3	3

Table A.9 *(continued)*

Data element	Unit	Value range	Description	Relevant message
Bounds_ChangeFlag	Enum	1) New 2) Add	Set new boundaries for SV or add to existing, only Type 3	4
Bounds_Count	Int	≥0	Number of boundaries identified, only Type 3	4
Bounds_Info	List of Bounds	—	See Table A.11, only Type 3	4
Bounds_Confirmation	Enum	1) OK 2) NG	Confirmation of landmark delivery, only Type 3	4
Route_ResetFlag	Enum	1) Unreset (Add the route data) 2) Reset and newly add route data	only Type 3	5
Number of nodes	Int	≥0	only Type 3	5
Route_Nodes	List of Route Nodes		See Table A.12, only Type 3	5
AVP_Timestamp	UTC	64 bites	Synchronized point in time	all

Table A.10 — Type 3 landmark elements

Data element	Unit	Value range	Description
Landmark_ID	Int	—	Unique identifier to identify landmark, only Type 3
Landmark_Type	Enum	0: Type A 1: Type B 2: Type C 3-255: reserved	Specify landmark type, only Type 3
Landmark_Location	x,y,z (mm)	—	Show landmark location, only Type 3
Landmark_Orientation	Degrees (3 axis)	0,00 to 359,99	Orientation of Landmark, only Type 3

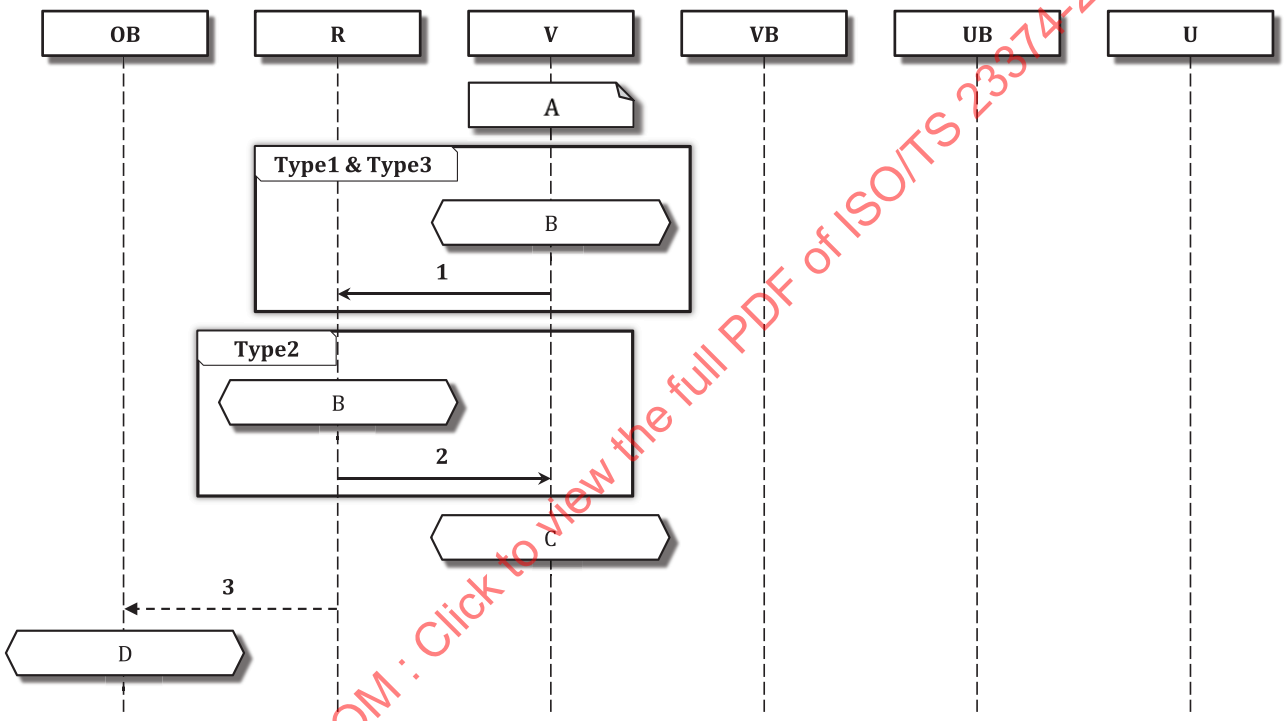
Table A.11 — Type 3 bounds elements

Data element	Unit	Value range	Description
Bounds_Location	x,y,z(mm)	—	Location of all boundaries, only Type 3
Bounds_Orientation	Degrees	0,00 to 359,99	Orientation of boundaries, only Type 3

Table A.12 — Type 3 Route Node Elements

Data element	Unit	Value range	Description
XYZ coordinate	x,y,z(mm)	—	x, y, z in map coordinates
Type	enum	0: Waypoint 1: Target position	
Max velocity	m/s	0,00 to 8,33	Maximum allowed velocity for this part of the route
Direction	degrees	0,00 to 359,99deg	Maximum allowed velocity for this part of the route, only Type 3

A.2.10 Destination reached



Key

OB Operator_Backend
R Remote_Vehicle_Operation
V Onboard_Vehicle_Operation
VB Vehicle_Backend
UB User_Backend
U User_Frontend
A SV arrived at destination (e.g. parking spot)
B Determine SV reached target destination
C Establish stationary conditions
D Determine mission processing
1 Target destination reached (Target_ID, Mission_ID)
2 Target destination reached (Mission_ID)
3 Target destination reached (Target_ID, Mission_ID)

Figure A.11 — Destination reached sequence

Table A.13 — Data elements of Figure A.11

Data element	Unit	Value range	Description	Relevant message
Mission_ID	UID	no recommendation	Unique mission identifier created by OB sub-system for an engagement request	1, 2 (3)

Table A.13 *(continued)*

Data element	Unit	Value range	Description	Relevant message
Confirmed_Target_ID	UID	no recommendation	Identifier of target semantic unique for target type within facility, Type 1 only. Can be different to assigned target, if a search was conducted by SV.	1
SV_Target_Type	List of Enum	1) Parking spot 2) Drop-off/Pick-up 3) Parking Section 4) Parking area 5) Segment for Wait 6) Point of interest	Type identifier for specified target, Type 1 only	1, 2 (3)
AVP_Timestamp	Unix Time	64 bits	Synchronized point in time	all

A.3 Data elements related to automated vehicle operation

A.3.1 R sub-system cyclic message

A.3.1.1 Type 1

Table A.14 — Data elements of Type 1 R sub-system cyclic message

Data element	Unit	Value range	Description
AVP_MovementPermission	Bool	—	Vehicle-specific driving permission by AVP provider; failure to receive permission within a given frequency leads to suspended state
SV_OccupiedMovementAreas	List of UID	>32	List of unique identifiers of map areas in which the specific SV is not allowed to manoeuvre
SV_MaxAllowedVelocity	m/s	0,00 to 8,33	maximum allowed velocity imposed on SV by provider

A.3.1.2 Type 2

There are two interface types for Type 2 R sub-system cyclic message (driving command): the “Path Interface” and the “Acceleration-Curvature (Acc-Curv) Interface”.

With the Path Interface, a path with limitations (or a “snippet”) is sent from the R sub-system and stored within the V sub-system. The V sub-system receives its current position estimated by the R sub-system and determines and performs VMC to keep the SV’s position on the stored path.

With the Acc-Curv Interface, VMC is determined in the R sub-system, and this VMC-relevant information is transmitted to be performed by the V sub-system.

Table A.15 — Data elements of Type 2 R sub-system cyclic message (driving command)

Data element	Unit	Value range	Description
SV_InterfaceType	Enum	1) Path 2) Acc-Curv	Drive control mode, initialized before the vehicle moves, but not during the drive
SV_PathSnippet	UID, list of path poses		Path Interface: This message contains the path the vehicle is supposed to follow; depending on the vehicle's capability this can be either the complete path or just a snippet Path poses contain x,y, ps), parking deck, speed, curvature, driving direction indicator
SV_Position	m, rad, s		Path Interface: 3D vehicle pose (centre of rear axle) as determined by infrastructure in x,y, ψ in garage coordinate system with time of measurement
SV_TargetVelocity	m/s	0,00 to 8,33	Path Interface: Target velocity imposed on SV by provider (can be undercut by MaxDistanceToDrive control)
SV_MaxDistanceToDrive	m	>0	Path Interface: Maximum remaining distance the vehicle is currently allowed to drive
SV_DirectionIndicator	Enum	1) none 2) left 3) right	ACC-Curv Interface: Command for driving direction indicator
SV_DrivingDirection	Enum	1) standstill 2) forwards 3) backwards	ACC-Curv Interface: Command for driving direction
SV_TrajectorySnippet	list of tuples with acceleration and curvature values	ax: -12 m/s2 … + 12 m/s2	ACC-Curv Interface: Target acceleration/deceleration and target curvature

Table A.16 — Data elements of Type 2 R sub-system cyclic message (driving permission)

Data element	Unit	Value range	Description
expirationTime	s	32 bits	unix timestamp, i.e. milliseconds since 1970-01-01, 00:00
velocityMax	m/s	≥0	maximum allowed vehicle velocity when driving a) forwards, and b) when driving backwards.
curvatureMin	1/m		right curvature bounds when driving a) forwards, and b) backwards.
curvatureMax	1/m		left curvature bounds when driving a) forwards, and b) backwards

Table A.17 — Data elements of Type 2 R sub-system cyclic message (safety time sync response)

Data element	Unit	Value range	Description
UID	UID	no recommendation	UID received in the Safety Clock Sync Request.
serverTime	s	> 0	Server time when Safety Time Sync Request was received. Unix timestamp, i.e. milliseconds since 1970-01-01, 00:00
NOTE Safety signals are secured by additional cyclic redundancy check (CRC) in the application layer etc.			

A.3.1.3 Type 3

Table A.18 — Data elements of Type 3 R sub-system cyclic message

Data element	Unit	Value range	Description
Message Counter	int	—	Incremental counter value

A.3.2 V sub-system cyclic message

A.3.2.1 Type 1 and 3

Table A.19 — Data elements of Types 1 and 3 V sub-system cyclic message

Data element	Unit	Value range	Description
Mission_ID	UID	no ISO 23374 recommendation	Unique mission identifier created by AVP_Backend for an engagement request
SV_Position	m, degrees	—	6D Vehicle pose in x,y,z in map coordinate system with respect to center of its rear axle and angles Φ,θ,Ψ
SV_Target_ETA	Seconds	≥0	Estimated time of arrival at current target for current move based on no traffic
System_State	None	0) Inactive 1) Ready 2) Standby 3) Preparation 4) Normal 5) Temp. Error 6) Suspend 7) Recovery	State of vehicle
SV_DrivingState	Enum	1) Cruise 2) Close Quarter Manoeuvering 3) Pausing 4) Stopped	Status of automated driving within state "normal"

Table A.19 *(continued)*

Data element	Unit	Value range	Description
Shift Position	None	0) Neutral 1) Parking 2) Drive 3) Reverse 4-6) Reserve 7) Not defined	Shift position of vehicle
Vehicle Longitudinal Acceleration	m/s^2 (g)		Longitudinal acceleration of vehicle
Vehicle Steering Angle	degrees	-3 070,5 to +3 070,5	Angle of steering
SV_Velocity	m/s	0,00 to 8,33	Subject vehicle speed
AVP_Timestamp	Unix Time	32 bits	Synchronized point in time

A.3.2.2 Type 2

Table A.20 — Data elements of Types 2 V sub-system cyclic message (vehicle state)

Data element	Unit	Value range	Description
pathSnippet_ID	UID		The identifier of the path snippet which the vehicle currently follows; 0 if not applicable
SV_currentCurvature	1/m	>0	The current vehicle curvature as determined by vehicle
SV_Velocity	m/s	0,00 to 8,33	Subject vehicle speed as determined by vehicle
SV_YawRate	rad/s		Current yaw rate
SV_Driving_Direction	Enum	1) Standstill 2) Forward 3) Backward	Subject vehicle driving direction with standstill below 0,01 m/s
SV_Shift_Position	Enum	0) Neutral 1) Parking 2) Drive 3) Reverse 4-6) Reserve 7) Not defined	Shift position of vehicle

Table A.21 — Data elements of Types 2 V sub-system cyclic message (Functional clock sync request)

Data element	Unit	Value range	Description
localVehicleTime	s	>0	Local vehicle time; will be returned in the Functional Time Sync Response together with a server time

Table A.22 — Data elements of Types 2 V sub-system cyclic message (Safety clock sync request)

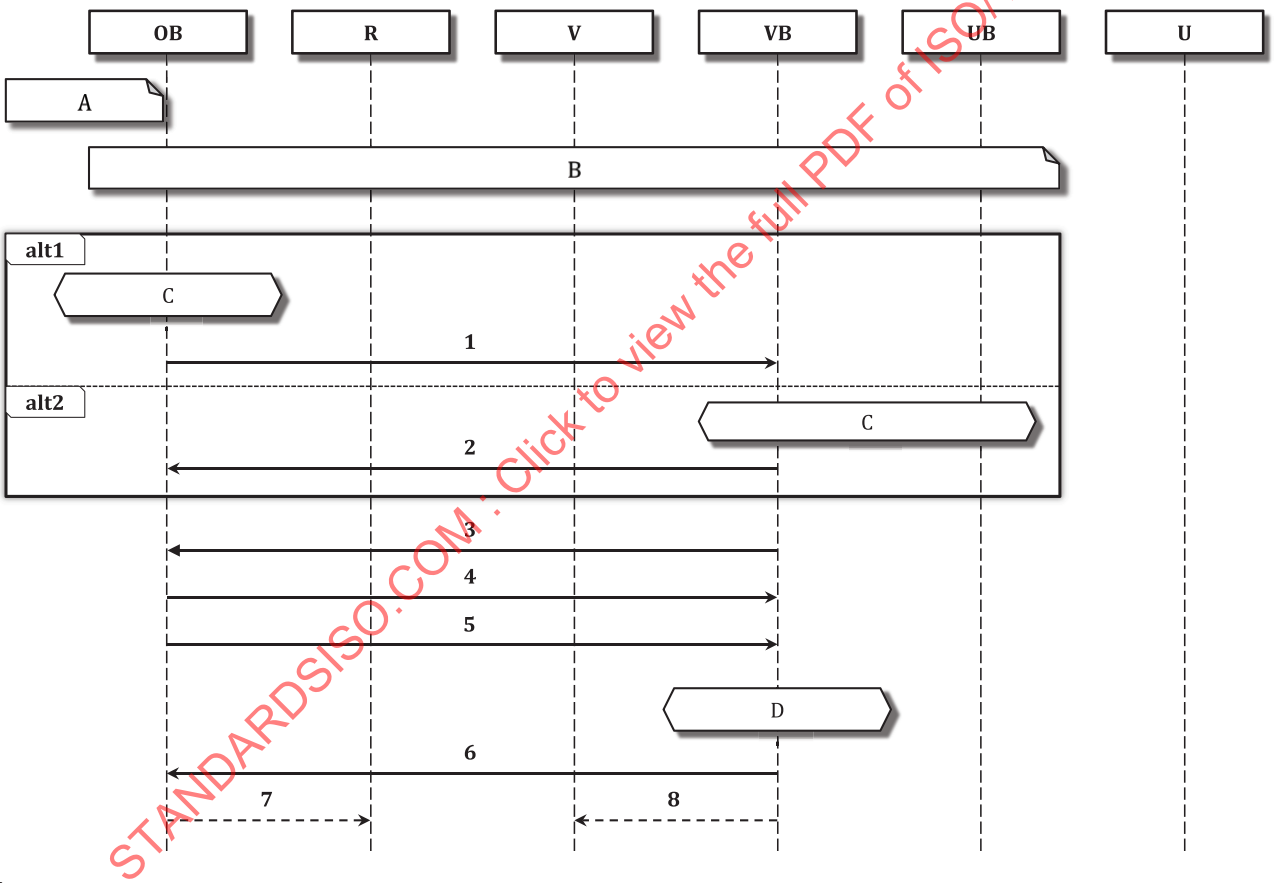
Data element	Unit	Value range	Description
SafetyClockSyncRequest	UID	no recommendation	Safety clock sync request from the vehicle The vehicle shall use this identifier to relate the Safety Time Sync Response to this request
NOTE Safety signals are secured by additional cyclic redundancy check (CRC) in the application layer, etc.			

A.3.3 Suspend condition codes

Refer to ISO 23374-1:2023, 9.4.

A.4 Communication sequences related to system participant management

A.4.1 Communication interface compliance check sequence



Key

OB	Operator_Backend	R	Remote_Vehicle_Operation
V	Onboard_Vehicle_Operation	VB	Vehicle_Backend
UB	User_Backend	U	User_Frontend
A	Event based during session	B	Session confirmed by backend sub-systems
C	AVP protocol version revoked [Type 1: and/or Vehicle map version revoked]	D	Match protocol and map version, update if necessary
1	New protocol request (Session_ID)	2	New protocol request (Session_ID)
3	Supported types offer (Session_ID, SV_Supported_AVP_Types)	4	Type confirmation (Session_ID, Confirmed_AVP_Type)

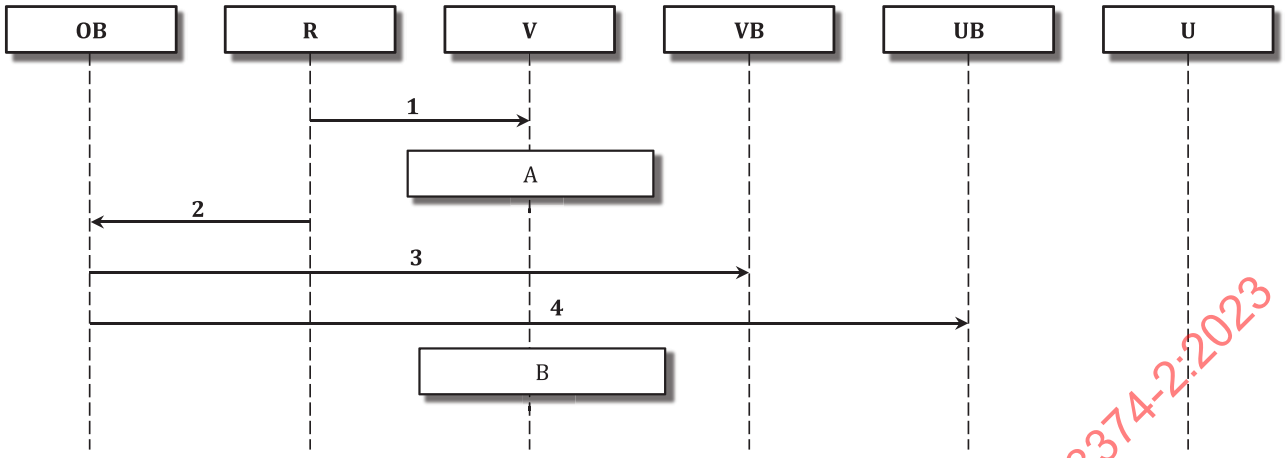
5	Protocol offer (Session_ID, Valid AVP_Protocol_6 Ver, [Type 1: Valid AVP_Map_Ver])	Protocol confirmation (Session_ID, Confirmed AVP protocol version, [Type 1: Confirmed vehicle map version])
7	Protocol confirmation (Confirmed AVP protocol8 version, [Type 1: Confirmed vehicle map version])	Protocol confirmation (Confirmed AVP protocol version, [Type 1: Confirmed vehicle map version])

Figure A.12 — Communication interface compliance check sequence

Table A.23 — Data elements of Figure A.12

Data element	Unit	Value range	Description	Relevant message
AVP_Session_ID	UID	large enough to identify single session for the legally required storage time in a market	Unique identifier for management of one SV from the time of check-in until check-out	1, 2, 3, 4, 5, 6
AVP_Protocol_Ver	List of UIDs	future-proof	Unique identifier for AVP communication protocol used for specified type within this session confirmed by AVP_Backend	5, 6 (7, 8)
AVP_Map_Ver	List of UIDs	no recommendation	Unique identifier for AVP map version used for session confirmed by AVP_Backend; suitable data types from map standards can be applied	5, 6 (7, 8)
SV_Supported_AVP_Types	List of Enum	1) Type 1 exclusive 2) Type 1 mixed 3) Type 2 exclusive 4) Type 2 mixed 5) Type 3 exclusive 6) Type 3 mixed	Type identifier for supported AVP ISO Type offered by SV; contains information about supported scenario (mixed/exclusive) SV may offer multiple values, but only one mode is selected for a session	3, 4
AVP_Timestamp	Unix Time	64 bits	Synchronized point in time	all

A.4.2 Operation stop command



Key

OB	Operator_Backend	R	Remote_Vehicle_Operation
V	Onboard_Vehicle_Operation	VB	Vehicle_Backend
UB	User_Backend	U	User_Frontend
A	Emergency stop (see 6.3.3)	B	Transition to suspend state
1	Operation stop command (Mission_ID, SV_ID)	2	Info stop command (Remote_Stop_Reason)
3	Info stop command (Remote_Stop_Reason)	4	Info stop command (Remote_Stop_Reason)

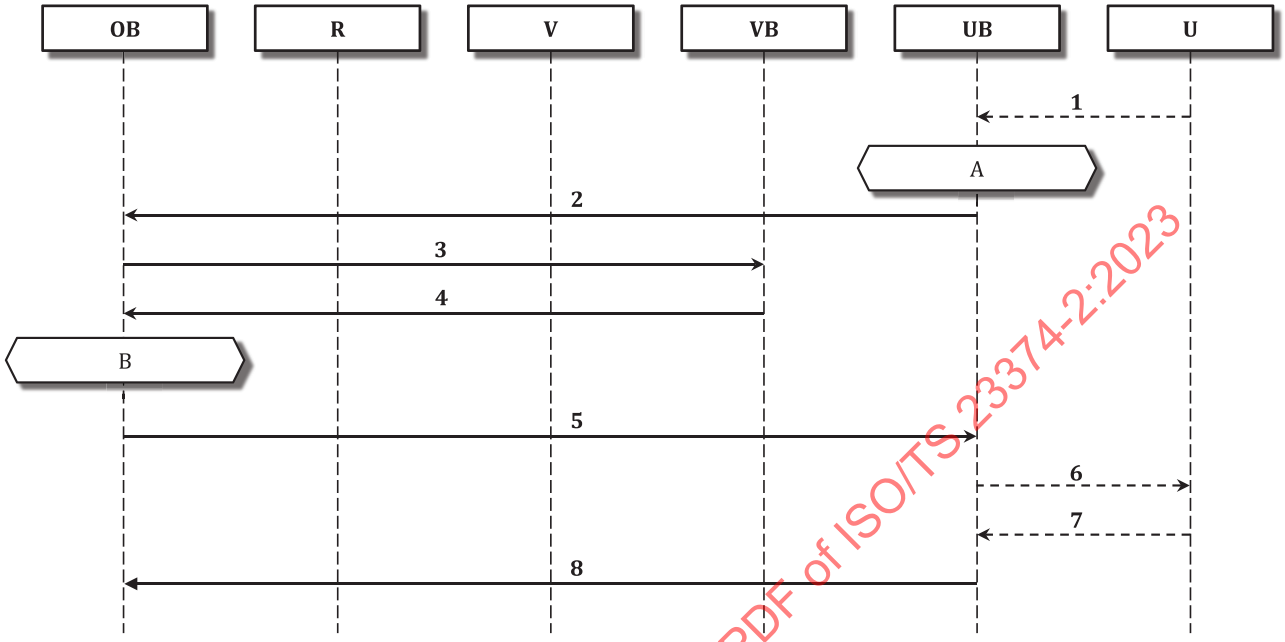
Figure A.13 — Operation stop request sequence

Table A.24 — Data elements of Figure A.13

Data element	Unit	Value range	Description	Relevant message
SV_ID	Hashed UID	≥128 bits	Salted hash based on unique vehicle identifier (VIN)	1
Remote_Stop_Reason	Enum	1) Facility hazard 2) Accident 3) Manual 4) Service failure 5) Invalid SV Behaviour	Reason for AVPS to suspend operation for vehicle (e.g. earthquake = 1)	1, 2, 3, 4
Mission_ID	UID	no recommendation	Unique mission identifier created by AVP_Backend	1
AVP_Timestamp	Unix Time	64 bits	Synchronized point in time	all

A.5 Communication sequences linked to on-demand user requests

A.5.1 Availability request



Key

OB	Operator_Backend	R	Remote_Vehicle_Operation
V	Onboard_Vehicle_Operation	VB	Vehicle_Backend
UB	User_Backend	U	User_Frontend
A	Check user policies	B	Confirm compatibility and vacancy
1	Request reservation	2	Request availability (Duration, Terms, Services)
3	Request compatibility data (facility parameters)	4	Compatibility data
5	Offer reservation (Reservation_ID)	6	Offer reservation
7	Confirm reservation	8	Confirm reservation

Figure A.14 — Availability request sequence

Table A.25 — Data elements of Figure A.14

Data element	Unit	Value range	Description	Relevant message
User_ParkingPreference	List of Enum	1) Forward 2) Backwards 3) Extra door space 4) Indoor only 5) Near exit	User preference identified by UB sub-system to be considered by OB sub-system if offered	(1)
SV_ID	Hashed UID	≥128 bits	Salted hash based on unique vehicle identifier (VIN)	4
SV_Width	m	>0	Vehicle width (Resolution 1 cm)	4

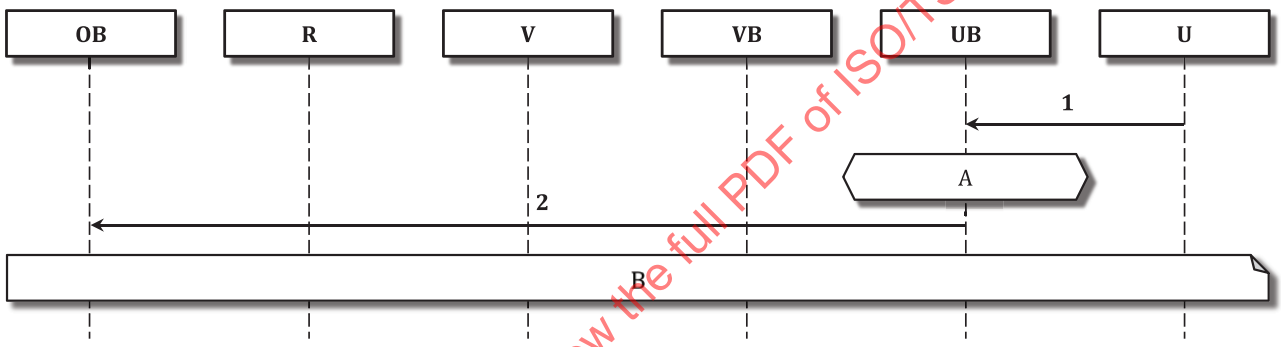
Table A.25 *(continued)*

Data element	Unit	Value range	Description	Relevant message
SV_Length	m	>0	Vehicle length (Resolution 1 cm)	4
SV_Height	m	>0	Vehicle height (Resolution 1 cm)	4
SV_FrontOverhang	m	>0	Vehicle front overhang (Resolution 1 cm)	4
SV_RearOverhang	m	>0	Vehicle rear overhang (Resolution 1 cm)	4
SV_GroundClearance	m	>0	Vehicle ground clearance (Resolution 1 cm)	4
SV_InnerCurveRadius	m	>0	Minimum vehicle inner curve radius (Resolution 1 cm)	4
SV_OuterCurveRadius	m	>0	Minimum vehicle outer curve radius (Resolution 1 cm)	4
SV_Gradient	degree	>0	Maximum vehicle supported gradient (Resolution 0,1°)	4
SV_SupportedForwardVelocity	m/s	0,00 to 8,33	Maximum vehicle supported forward speed	4
SV_SupportedReverseVelocity	m/s	0,00 to 8,33	Maximum vehicle supported reverse speed	4
SV_FuelType	List of Enum	0) invalid 1) petrol 2) diesel 3) LPG 4) CNG 5) Electrical 6) Hydrogen	Vehicle fuel type	4
SV_ElectricAdapterType	Enum	1) AC side 2) DC side 3) Wireless front 4) Wireless rear 5) AC underbody 6) DC underbody	EV connector type	4

Table A.25 *(continued)*

Data element	Unit	Value range	Description	Relevant message
SV_RefuelingAdapterPosition	enum	1) Front left 2) Front middle 3) Front right 4) Rear right 5) Rear middle 6) Rear left	Position of SV fuel or electric inlet in x, y, z with respect to its centre rear axle and angles Φ,θ,Ψ	4
SV_ExpectedMaxSleepTime	hours	>0	Maximum vehicle sleep time	4

A.5.2 Retrieval request



Key

OB	Operator_Backend	R	Remote_Vehicle_Operation
V	Onboard_Vehicle_Operation	VB	Vehicle_Backend
UB	User_Backend	U	User_Frontend
A	Check user policies	B	Mission request
1	Request retrieval	2	Request retrieval

Figure A.15 — Retrieval request sequence