FINAL
DRAFT

TECHNICAL SPECIFICATION

ISO/DTS 23374-2

ISO/TC **204**

Secretariat: **ANSI**

Voting begins on:
2023-05-25

Voting terminates on:
2023-07-20

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/DTS 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:—[1], *Intelligent transport systems — Automated valet parking systems (AVPS) — Part 1: System framework, requirements for automated driving, and communication 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:—[2], 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:—, 3.5, modified — Note 2 to entry removed.]

1) Under preparation. Stage at the time of publication: ISO/FDIS 23374-1:2023.

2) Under preparation. Stage at the time of publication: ISO/FDIS 23374-1:2023.

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:—, 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:—, 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:—, 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:—, 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:—, 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:—, 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:—, 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:—, 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
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:—, Clause 6.

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

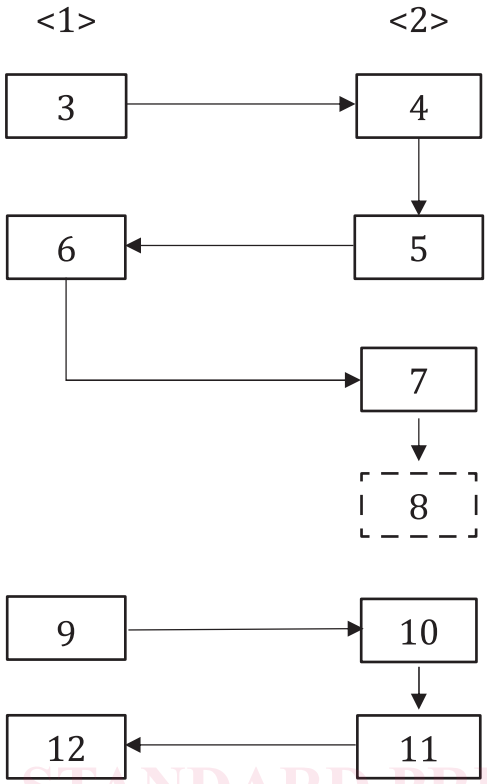
Table 1 — Basic functionalities of AVPS and their description

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.



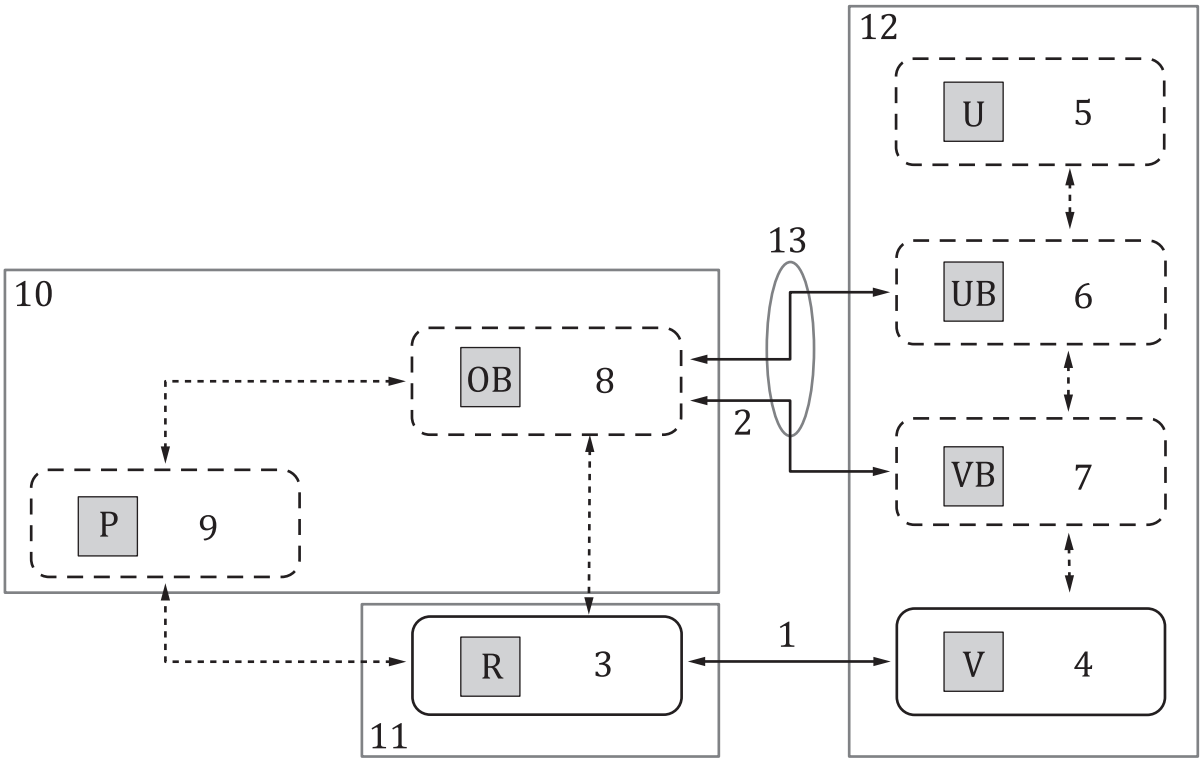
Key

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:—, 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.	

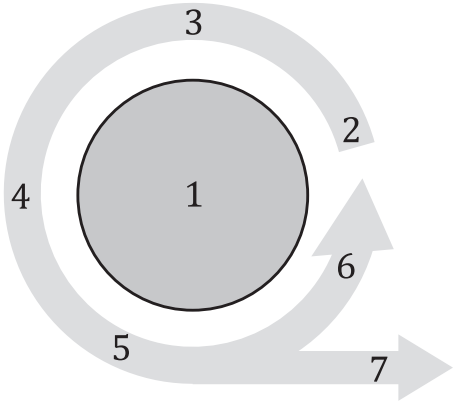
[a] See Figure 2.

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.