INTERNATIONAL STANDARD

ISO 15638-8

First edition
2014-07-15

Intelligent transport systems — Framework for cooperative telematics applications for regulated vehicles (TARV) —

Part 8: Vehicle access management

Systèmes intelligents de transport — Cadre pour applications télématiques coopératives pour véhicules réglementés (TARV) —

Partie 8: Monitorage de l'accès des véhicules

Reference number
ISO 15638-8:2014(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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 documents 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 204, *Intelligent transport systems*.

This first edition cancels and replaces ISO/TS 15638-8:2013.

ISO 15638 consists of the following parts, under the general title, *Intelligent transport systems — Framework for cooperative telematics applications for regulated vehicles (TARV)*:

- *Part 1: Framework and architecture*
- *Part 2: Common platform parameters using CALM*
- *Part 3: Operating requirements, 'Approval Authority' approval procedures, and enforcement provisions for the providers of regulated services*
- *Part 5: Generic vehicle information*
- *Part 6: Regulated applications*
- *Part 7: Other applications*
- *Part 8: Vehicle access management*
- *Part 9: Remote electronic tachograph monitoring (RTM)*
- *Part 10: Emergency messaging system/eCall (EMS)*
- *Part 11: Driver work records*
- *Part 12: Vehicle mass monitoring*
- *Part 14: Vehicle access control*
- *Part 15: Vehicle location monitoring*
- *Part 16: Vehicle speed monitoring*

- *Part 17: Consignment and location monitoring*
- *Part 18: ADR (Dangerous Goods) transport monitoring (ADR)*
- *Part 19: Vehicle parking facilities (VPF)*

The following parts are under preparation

- *Part 4: System security requirements*
- *Part 13: 'Mass' information for jurisdictional control and enforcement*

Introduction

Many ITS technologies have been embraced by commercial transport *operators* (4.38) and freight owners, in the areas of fleet management, safety and security. *Telematics* (4.52) applications have also been developed for governmental use. Such regulatory services in use or being considered vary from *jurisdiction* (4.33) to *jurisdiction*, but include electronic on-board recorders, vehicle charging, digital *tachograph* (4.51), on-board *mass* (4.36) monitoring, vehicle *access* (4.1) *methods*, *hazardous goods (4.44x)* tracking and e-call (4.26). Additional applications with a regulatory impact being developed include, fatigue management, speed monitoring and heavy vehicle charging based on *mass (57)*, location, distance and time.

In such an emerging environment of regulatory and *commercial applications* (4.17), it is timely to consider an overall *architecture* (4.12) (business and functional) that could support these functions from a single platform within a commercial freight vehicle that operate within such regulations. International Standards will allow for a speedy development and *specification* (4.50) of new applications that build upon the functionality of a generic specification platform. A suite of standards deliverables is required to describe and define the *framework* (4.28) and requirements so that the on board equipment and back office systems can be commercially designed in an open market to meet common requirements of *jurisdictions* (4.33).

This suite of standards addresses and defines the *framework* (4.28) for a range of cooperative *telematics* (4.52) applications for *regulated vehicles* (4.42) (such as *access methods* (4.3), driver *fatigue management*, speed monitoring, on-board *mass* (4.36) monitoring and charging). The overall scope includes the concept of operation, legal and regulatory issues, and the generic cooperative provision of services to *regulated vehicles* (4.42), using an on-board ITS platform. The *framework* is based on a (multiple) *service provider* (4.48) oriented approach with provisions for the *approval* (4.9) and *auditing* (4.13) of *service providers*.

This suite of standards deliverables will

- provide the basis for future development of cooperative *telematics* (4.52) applications for *regulated vehicles* (4.42). Many elements to accomplish this are already available. Existing relevant standards will be referenced, and the *specifications* (4.50) will use existing standards (such as *CALM*) wherever practicable,
- allow for a powerful platform for highly cost-effective delivery of a range of *telematics* applications for *regulated vehicles* (4.42),
- a business *architecture* (4.12) based on a (multiple) *service provider* (4.48) oriented approach, and
- address legal and regulatory aspects for the *approval* (4.9) and *auditing* (4.13) of *service providers.*

This suite of standards deliverables is timely as many governments (Europe, North America, Asia, and Australia/New Zealand) are considering the use of *telematics* (4.52) for a range of regulatory purposes. Ensuring that a single in-vehicle platform can deliver a range of services to both government and industry through open standards and competitive markets is a strategic objective.

This part of the ISO 15638 family of standards deliverables provides *specifications* (4.50) for vehicle access management and monitoring.

NOTE 1 The definition of what comprises a “regulated” vehicle is regarded as an issue for National decision, and may vary from *jurisdiction* (4.33) to *jurisdiction*. This suite of standards deliverables does not impose any requirements on nations in respect of how they define a *regulated vehicle* (4.42).

NOTE 2 The definition of what comprises a “regulated” service is regarded as an issue for National decision, and may vary from *jurisdiction* (4.33) to *jurisdiction*. This suite of standards deliverables does not impose any requirements on nations in respect of which services for *regulated vehicles* (4.42) *jurisdictions* will require, or support as an option, but will provide standardized sets of requirements descriptions for identified services to enable consistent and cost efficient implementations where implemented.

Intelligent transport systems — Framework for cooperative telematics applications for regulated vehicles (TARV) —

Part 8: Vehicle access management

1 Scope

This part of ISO 15638 addresses the provision of "*vehicle access management*" (4.45) (and monitoring) and specifies the form and content of such data required to support such systems, and *access methods* (4.3) to that data.

The scope of this part of ISO 15638 is to provide *specifications* (4.50) for common communications and data exchange aspects of the *application service* (4.6) vehicle access monitoring that a *regulator* (4.43) may elect to require or support as an option, including

a) high level definition of the service that a *service provider* (4.48) has to provide, (The service definition describes common service elements; but does not define the detail of how such an *application service* (4.6) is instantiated, not the acceptable value ranges of the data concepts defined),

b) means to realize the service, and

c) application data, naming content, and quality that an *IVS* (4.29) has to deliver.

The definition of what comprises a "regulated" service is regarded as an issue for National decision, and may vary from *jurisdiction* (4.33) to *jurisdiction*. This International Standard does not impose any requirements on nations in respect of which services for *regulated vehicles jurisdictions* will require, or support as an option, but provides standardized sets of requirements descriptions for identified services to enable consistent and cost efficient implementations where instantiated.

This International Standard has been developed for use in the context of regulated commercial freight vehicles [hereinafter referred to as "*regulated vehicles*" (4.42)]. There is nothing, however, to prevent a jurisdiction extending or adapting the scope to include other types of regulated vehicles, as it deems appropriate.

2 Conformance

Requirements to demonstrate conformance to any of the general provisions or specific *application services* (4.6) described in this part of ISO 15638 shall be within the regulations imposed by the *jurisdiction* (4.33) where they are instantiated. Conformance requirements to meet the provisions of this International Standard are therefore deemed to be under the control of, and to the specification of, the *jurisdiction* where the *application service*(s) is/are instantiated.

The protocols defined in this part of ISO 15638 have been independently tested. Annex B provides results of these tests. In any conformance assurance process undertaken by candidate systems, where appropriate the results may be used as part of its process of conformance compliance.

3 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 15638-1, *Intelligent transport systems — Framework for collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV) — Part 1: Framework and architecture*

ISO 15638-2, *Intelligent transport systems — Framework for collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV) — Part 2: Common platform parameters using CALM*

ISO 15638-3, *Intelligent transport systems — Framework for collaborative telematics applications for regulated commercial freight vehicles (TARV) — Part 3: Operating requirements, 'Approval Authority' procedures, and enforcement provisions for the providers of regulated services*

ISO 15638-4, *Intelligent transport systems — Framework for cooperative telematics applications for regulated vehicles (TARV) — System security requirements (in development)*

ISO 15638-5, *Intelligent transport systems — Framework for collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV) — Part 5: Generic vehicle information*

ISO 15638-6, *Intelligent transport systems — Framework for collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV) — Part 6: Regulated applications*

4 Terms and definitions

For the purposes of this document, the following terms and definitions given in ISO 15638-1 and the following apply.

4.1
access
admittance, entry, permit to use the road network and/or associated infrastructure (bridges, tunnels etc.)

4.2
access control
procedures and measures to control admittance, entry, permit to use the road network, and/or associated infrastructure (bridges, tunnels, etc.)

4.3
access methods
procedures and protocols to provision and retrieve data

4.4
access monitoring
observation and recording of vehicle related data when using the road network and/or associated infrastructure (bridges, tunnels, etc.)

4.5
app
small (usually) *Java™* (4.32) applets, organized as software bundles, that support *application services* (4.6) by keeping the *data pantry* (4.23) provisioned with up to date data

4.6
application service
service provided by a *service provider* (4.48) enabled by accessing data from the *IVS* (4.29) of a *regulated vehicle* (4.42) via a wireless communications network

4.7
application service provider
ASP
party that provides an *application service* (4.6)

4.8
app library
separately secure area of memory in *IVS* (4.29) where apps are stored

[SOURCE: with different access controls to *data pantry* (4.23)]

4.9
approval
formal affirmation that an applicant has satisfied all the requirements for appointment as an *application service provider* (4.7) or that an application service delivers the required service levels

4.10
approval agreement
written agreement made between an *approval authority (regulatory)* (4.11) and a *service provider* (4.48)

Note 1 to entry: An app*roval authority (regulatory)* approval agreement recognizes the fact that a *service provider,* having satisfied the *approval authority's* requirements for appointment as a *service provider,* is appointed in that capacity, and sets out the legal obligations of the parties with respect to the on-going role of the *service provider*

4.11
approval authority (regulatory)
organization (usually independent) which conducts *approval* (4.9) and ongoing *audit* (4.13) for *service provider* (4.48) on behalf of a *jurisdiction* (4.33)

4.12
architecture
formalized description of the design of the structure of *TARV* and its *framework* (4.28)

4.13
audit/auditing
review of a party's capacity to meet, or continue to meet, the initial and ongoing *approval agreements* (4.10) as a *service provider* (4.48)

4.14
basic vehicle data
data that shall be maintained/provided by all *IVS* (4.29)

[SOURCE: regardless of *jurisdiction* (4.33)]

4.15
BigBubble
zones, such as metropolitan area, which include within them several *sensitive/restricted zones* (4.46)

4.16
communications access for land mobiles
CALM
layered solution that enables continuous or quasi continuous communications between vehicles and the infrastructure, or between vehicles, using such (multiple) wireless telecommunications media that are available in any particular location, and which have the ability to migrate to a different available media where required and where media selection is at the discretion of *user* (4.53) determined parameters by using a suite of standards based on ISO 21217 (*CALM* architecture) and ISO 21210 (*CALM* networking) that provide a common platform for a number of standardised media using *ITS-stations* (4.31) to provide wireless support for applications, such that the application is independent of any particular wireless medium

4.17
commercial application(s)
ITS applications in *regulated vehicles* (4.42) for commercial (non-regulated) purposes

EXAMPLE Asset tracking, vehicle and engine monitoring, cargo security, driver management, etc.

4.18
consignment
shipment of goods/cargo to a destination

4.19
controlled zone/controlled access zone
defined physical area which the *jurisdiction* (4.33) or *controlled zone* (4.19) manager determines require *access control* (4.2) for regulated vehicles

4.20
cooperative ITS
C-ITS
ITS applications for both regulatory and commercial purposes that require the exchange of data between uncontracted parties using multiple *ITS-stations* (4.31) communicating with each other and sharing data with other parties with whom they have no direct contractual relationship to provide one or more *ITS services* (4.30)

4.21
'CoreData'
basic vehicle data (4.14) plus any additional data required to provide an implemented *regulated application service* (4.41)

4.22
dangerous goods
substances or articles which are potentially hazardous (for example, poisonous to humans, harmful to the environment, explosive, flammable, or radioactive) that require regulatory control when transported

4.23
data pantry
secure area of memory in *IVS* (4.29) where data values are stored

[SOURCE: with different access controls to *app library* (4.8)]

4.24
driver
person driving the *regulated vehicle* (4.42) at any specific point in time

4.25
driver work records
DWR
collection, collation, and transfer of *driver* (4.24) work and rest hours data from an *in-vehicle system* (4.29) to an *application service provider* (4.7)

4.26
eCall
specialized instantiation of an *EMS* (4.27) that provides incident messaging and communication with a public service assistance point via priority wireless telephone communications using its emergency call capabilities

4.27
emergency message system
EMS
collection, collation, and transfer of emergency message data from an *in-vehicle system* (4.29) to an *application service provider* (4.7)

4.28
framework
particular set of beliefs, ideas referred to in order to describe a scenario or solve a problem

4.29
in-vehicle system
IVS
ITS-station (4.31) and connected equipment on board a vehicle

4.30
ITS service
communication functionality offered by an *ITS-station* (4.31) to an *ITS-station* application

4.31
ITS-station
ITS-s
entity in a communication network, comprised of application, *facilities (4.40x)*, networking and access layer components specified in ISO 21217 that operate within a bounded secure management domain

4.32
Java™
object oriented open source operating language developed by SUN systems

4.33
jurisdiction
government, road or traffic authority which owns the *regulatory applications* (4.40)

EXAMPLE Country, state, city council, road authority, government department (customs, treasury, transport), etc.

4.34
jurisdiction regulator
agent of the *jurisdiction* (4.33) appointed to regulate and manage *TARV* within the domain of the *jurisdiction*; may or may not be the *approval authority (regulatory)* (4.11)

4.35
local data tree
LDT
frequently updated data concept stored in the on on-board *data pantry* (4.23) containing a collection of data values deemed essential for either a) *TARV regulated application service* (4.41), or b) *cooperative intelligent transport systems* (4.20)

4.36
mass
mass of a given heavy vehicle as measured by equipment affixed to the *regulated vehicle* (4.42)

4.37
"Mass" information for jurisdictional control and enforcement
MICE/MRC
collection, collation, and transfer of *vehicle mass* (4.36) data from an *in-vehicle system* (4.29) to an application *service provider* (4.7) to enable data provision to *jurisdictions* (4.33) for the control and management of equipped vehicles based on the mass of the *regulated vehicle* (4.42), or use of such data to enable compliance with the provisions of regulations

4.38
operator
fleet manager of a *regulated vehicle* (4.42)

4.39
prime service provider
service provider (4.48) who is the first contractor to provide *regulated application services* (4.41) to the *regulated vehicle* (4.42), or a nominated successor on termination of that initial contract; the *prime service provider* is also responsible to maintain the installed *IVS* (4.29); if the *IVS* was not installed during the manufacture of the vehicle the *prime service provide*r is also responsible to install and commission the *IVS*

4.40
regulated/regulatory application
application arrangement using TARV utilised by *jurisdictions* (4.33) for granting certain categories of commercial vehicles rights to operate in regulated circumstances subject to certain conditions, or indeed to permit a vehicle to operate within the *jurisdiction*; may be mandatory or voluntary at the discretion of the *jurisdiction*

4.41
regulated application service
TARV application service to meet the requirements of a regulated application that is mandated by a regulation imposed by a *jurisdiction* (4.33), or is an option supported by a *jurisdiction*

4.42
regulated vehicle/regulated commercial freight vehicle
vehicle that is subject to regulations determined by the *jurisdiction* (4.33) as to its use on the road system of the *jurisdiction* in regulated circumstances, subject to certain conditions, and in compliance with specific regulations for that class of regulated vehicle; at the option of *jurisdictions*; this may require the provision of information via *TARV* or provide the option to do so

4.43
regulator
see *jurisdiction regulator* (4.34)

4.44
remote tachograph monitoring
RTM
collection, collation, and transfer of data from an on-board electronic *tachograph* (4.51) system to an *application service provider* (4.7)

4.45
secure parking facility
SPF
parking facility for regulated and other commercial vehicles that meets the requirements of the local *jurisdiction* (4.33) in its ability and associated administration and management to provide safe and secure parking for regulated and other commercial vehicles

4.46
sensitive/restricted zone (*SZM*)
defined physical area which the *jurisdiction* (4.33) or sensitive/restricted zone manager determines require special monitoring (e.g. urban pedestrian areas, school, and hospital surroundings, …), freight villages, ports, road sensitivity infrastructure (bridges, tunnels, …), weight restricted areas, width restricted areas, areas where there has been an accident or incident, etc.

4.47
sensitive/restricted zone management
monitoring and management of *regulated commercial freight vehicles* (4.42) in additional to normal traffic management, as specified by the *jurisdiction* (4.33) or its agents to apply to *regulated commercial freight vehicles*

4.48
service provider
party which is approved by an *approvalauthority (regulatory)* (4.11) as suitable to provide regulated or commercial ITS *application services* (4.6)

4.49
session
wireless communication exchange between the *ITS-station* (4.31) of an *IVS* (4.29) and the *ITS-station* of its *application service provider* (4.7) to achieve data update, data provision, upload apps, or otherwise manage the provision of the *application service* (4.6), or a wireless communication provision of data to the *ITS-station* of an *IVS* (4.29) from any other *ITS-station*

4.50
specification
explicit and detailed description of the nature and functional requirements and minimum performance of equipment, service or a combination of both

4.51
tachograph
sender unit mounted to a vehicle gearbox, a tachograph head and a digital driver card, which records the *regulated commercial freight vehicle* (4.42) speed and the times at which it was driven and aspects of the *driver's* (4.24) activity selected from a choice of modes

4.52
telematics
use of wireless media to obtain and transmit (data) from a distant source

4.53
user
individual or party that enrols in and operates within a regulated or *commercial application* (4.17) *service* (4.6)

EXAMPLE *Driver (4.24)*, transport *operator (4.38)*, freight owner, etc.

4.54
vehicle access control
VAC
control of *regulatedcommercial freight vehicles* (4.42) ingress to and egress from controlled areas, and related charging systems

4.55
vehicle access management
VAM
monitoring and management of *regulated commercial freight vehicles* (4.42) approaching or within sensitive and controlled areas

4.56
vehicle location monitoring
VLM
collection, collation, and transfer of vehicle location data from an *in-vehicle system* (4.29) to an *application service provider* (4.7)

4.57
vehicle mass monitoring
VMM
collection, collation, and transfer of vehicle *mass* (4.36) data from an *in-vehicle system* (4.29) to an *application service provider* (4.7)

4.58
vehicle parking facilities
VPF
system for booking and *access* (4.1) to and egress from a vehicle parking facility (VPF)

4.59
vehicle speed monitoring
VSM
collection, collation, and transfer of vehicle speed data from an *in-vehicle system* (4.29) to an *application service provider* (4.7)

5 Symbols (and abbreviated terms)

AA	*approval authority (regulatory)* (4.11)
ADR	*Accord Européen relatif au transport international des marchandises Dangereuses par Route (4.6x)* [*dangerous goods* (4.22)]
app	*applet* (JAVA$^{\text{TM}}$ application or similar) (4.5)
AS	*application service* (4.6)
ASP	*application service provider* (4.7)
CALM	*communications access for land mobiles* (4.16)
C-ITS	*cooperative intelligent transport systems* (4.20)
Dr	*driver* (4.24)
DWR	*driver work records* (4.25)
EDGE	enhanced data rate GSM evolution
EMS	*emergency message system* (4.27)
GPRS	global packet radio system
GSM	global system mobiles
GHz	gigahertz
Hz	hertz
ID	identity
IP	internet protocol
ITS-S	*ITS station* (4.31)
IVS	*In-vehicle system* (4.29)
J	*jurisdiction* (4.33)
LDT	*local data tree* (4.35)
LTE	long term evolution (mobile phone generation after 3G)
MICE	*“Mass” information for jurisdictional control and enforcement* (4.37)
Op	*operator* (4.38)

PSP	*prime service provider* (4.39)
RTM	*remote tachograph monitoring* (4.44)
SZM	sensitive zone manager/management (4.47)
SE	service element
SZM	*sensitive/restricted zone management* (4.47)/manager
TARV	*telematics* (4.52) applications for *regulated commercial freight vehicles* (4.42)
VAC	*vehicle access control* (4.54)
VAM	*vehicle access management* (4.55)
VLM	*vehicle location monitoring* (4.56)
VMM	*vehicle mass monitoring* (4.57)
VPF	*vehicle parking facility* (4.45)
VSM	*vehicle speed monitoring* (4.59)

6 General overview and framework requirements

ISO 15638-1 provides a *framework* (4.28) and *architecture* (4.12) for *TARV*. It provides a general description of the roles of the actors in *TARV* and their relationships.

To understand clearly the *TARV* framework, *architecture* (4.12) and detail and *specification* (4.50) of the roles of the actors involved, the reader is referred to ISO 15638-1.

ISO 15638-6 provides the core requirements for all regulated applications. To understand clearly the general context in to which the provision of this application service, the reader is referred to ISO 15638-6.

In order to be compliant with this part of ISO 15638, the overall architecture employed shall comply with ISO 15638-1.

In order to be compliant with this part of ISO 15638, the communications employed shall comply with ISO 15638-2.

In order to be compliant with this part of ISO 15638, the operating requirements employed shall comply with ISO 15638-3.

In order to be compliant with this part of ISO 15638, the security employed shall comply with ISO 15638-4.

In order to be compliant with this part of ISO 15638, the basic vehicle data shall comply with ISO 15638-5.

In order to be compliant with this part of ISO 15638, the generic conditions for this application service shall comply with ISO 15638-6.

This International Standard has been developed for use in the context of regulated commercial freight vehicles. There is nothing, however, to prevent a jurisdiction extending or adapting the scope to include other types of regulated vehicles, as it deems appropriate.

7 Requirements for services using generic vehicle data

The means by which the access commands for generic vehicle information specified in ISO 15638-5 can be used to provide all or part of the data required in order to support a *regulated application service* (4.41) shall be as defined in ISO 15638-6.

8 Application services that require data in addition to basic vehicle data

8.1 General

Shall be conducted as defined in ISO 15638-6.

8.2 Quality of service requirements

This part of ISO 15638 contains no general requirements concerning quality of service. Such aspects shall be determined by a *jurisdiction* (4.33) as part of its *specification* (4.50) for any particular *regulated application service* (4.41). However, where a specified *regulated application service* (4.41) has specific Q of S requirements essential to maintain interoperability, these aspects shall be as specified in Clause 10.

8.3 Test requirements

This part of ISO 15638 contains no general requirements concerning test requirements. Such aspects shall be determined by a *jurisdiction* (4.33) as part of its *specification* (4.50) for any particular *regulated application service* (4.41), and issued as a formal test requirements *specification* (4.50) document. However, where a specified *regulated application service* (4.41) has specific test requirements essential to maintain interoperability, these aspects shall be as specified in Clause 10 relating to this *regulated application service,* or in a separate standards deliverable referenced within that clause. And where multiple *jurisdictions* recognize a benefit to common test procedures for a specific *regulated application service,* this shall be the subject of a separate standards deliverable.

8.4 Marking, labelling, and packaging

This part of ISO 15638 has no specific requirements for marking labelling or packaging.

However, where the privacy of an individual may be potentially or actually compromised by any instantiation based on this International Standard, the contracting parties shall make such risk explicitly known to the implementing *jurisdiction* (4.33) and shall abide by the privacy laws and regulations of the implementing *jurisdiction* and shall mark up or label any contracts specifically and explicitly drawing attention to any loss of privacy and precautions taken to protect privacy. Attention is drawn to ISO/TR 12859 in this respect.

9 Common features of regulated TARV application services

9.1 General

The details of the instantiation of *regulated application service* (4.41) are as designed by the application service system to meet the requirements of a particular *jurisdiction* (4.33) and are not defined herein. ISO 15638-6 specifies the generic roles and responsibilities of actors in the systems, and instantiations that claim compliance with this part of ISO 15638 shall also be compliant with the requirements of ISO 15638-6.

The means by which data are provisioned into the *data pantry* (4.23), and the means to obtain the *TARV LDT* (4.35) and *"CoreData"* (4.21) are described in of ISO 15638-6, Clause 8.

In order to minimize demand on the *IVS* (4.29) [which it is assumed will be performing multiple *application services* (4.6) simultaneously, as well as supporting general safety related cooperative vehicle systems, see ISO 15638-1 for further details], and because national requirements and system offerings will differ, a "cloud" approach has been taken in defining *TARV regulated application services* (4.41).

The *TARV* approach is for the on-board *app* (4.5) supporting the application service to collect and collate the relevant data, and at intervals determined by the *app,* or on demand from the *application service provider* (*ASP*) (4.7), pass that data to the *ASP.* All of the actual application service processing shall occur in the mainframe system of the *ASP* (in the "cloud").

For further information, see ISO 15638-6, Clause 9.

At a conceptual level, the *TARV* system is therefore essentially simple, as shown in Figure 1. The process is similar to that for “*CoreData*” (4.21), but data are supplied to a different on-board file in the *data pantry* (4.23).

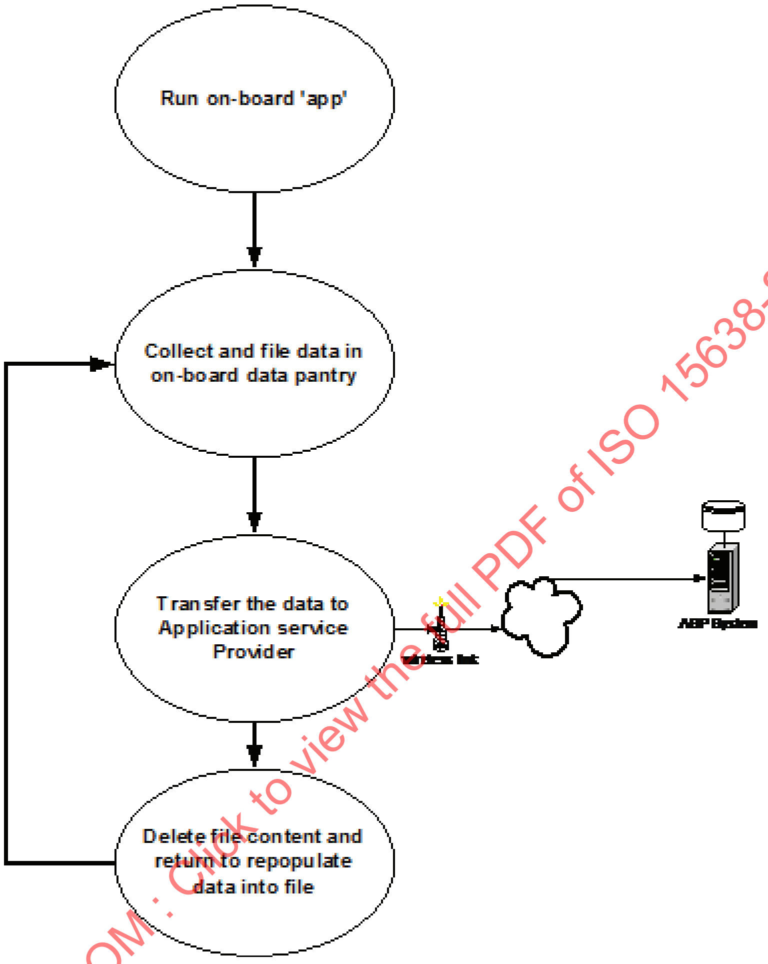
Run on-board 'app'
Collect and file data in on-board data pantry
Transfer the data to Application service Provider
Wireless link
ASP System
Delete file content and return to repopulate data into file

Figure 1 — TARV-regulated application service on-board procedure

At a common generic functional level for this application service, the process may be seen as shown in Figure 2 below, however, the connected equipment may/may not be required in all cases.

9.2 Common role of the jurisdiction, approval authority, service provider, and user

The common role of the jurisdiction, approval authority, application service provider, and user shall be as defined in ISO 15638-6.

9.3 Common characteristics for instantiations of regulated application services

The common characteristics for instantiations of regulated application services shall be as defined in ISO 15638-6.

9.4 Common sequence of operations for regulated application services

The common sequence of operations for regulated application services shall be as defined in ISO 15638-6.

9.5 Quality of service

Generic quality of service provisions for *application services* (4.6) shall be as defined in ISO 15638-6.

9.5 Information security

Information security shall be as defined in ISO 15638-6.

9.6 Data naming content and quality

Data naming and quality shall be as defined in ISO 15638-5, 8.2, 8.3, and 8.4 and ISO 15638-6

Variations specific to the vehicle access monitoring *application service* (4.6) shall be as defined below.

9.7 Software engineering quality systems

Software engineering quality systems shall be as defined in ISO 15638-6.

9.8 Quality monitoring station

The availability of quality monitoring stations shall be as defined in ISO 15638-6.

9.9 Audits

Audits shall be as defined in ISO 15638-6.

9.10 Data access control policy

To protect the data and information held by the *application service provider* (4.7), each provider shall adopt a risk based data access control policy for employees of the provider.

9.11 Approval of IVSs and service providers

Generic provisions for the *approval* (4.9) of *IVSs* and *service providers* (4.48) shall be as specified in ISO 15638-3. Detailed provisions for specific *regulated applications* (4.40) shall be as specified by the regime of the *jurisdiction* (4.33).

10 Vehicle access management (VAM)

10.1 TARV VAM service description and scope - use cases

10.1.1 Jurisdiction — Safety enhancement

Jurisdictions (4.33) need to define *sensitive/restricted zones* (4.46) by issuing specific *access* (4.1) policies in order to enhance the level of road safety in special situations by preserving the traffic efficiency and respecting the environment. *Sensitive/restricted zones* might be special inner city areas (e.g. urban pedestrian areas, school and hospital surroundings, …), freight villages, ports, road sensitivity infrastructure (bridges, tunnels, …)., weight restricted areas, width restricted areas, areas where there has been an accident or incident, etc. Public authorities are normally required to publish the *access* (4.1) rules and the restriction policy.

10.1.2 Sensitive/restricted zone managers — Access monitoring and management

Sensitive/restricted zone managers(*SZM*) (4.47) [who may be an organ of a *jurisdiction* (4.33), local authority or licensed/contracted *operator* (4.38) etc.] may require or be obliged by the *jurisdiction* to monitor vehicles and collect information on vehicles such as type, size, weight, status, condition, and/or driving style etc., in order to properly manage sensitive or otherwise controlled areas. They may also solicit and obtain data from the *regulated vehicle* (4.42) when approaching, when within, or when leaving the *sensitive/restricted zone* (4.46).

Suitable tools for enforcement need to be made available.

10.1.3 Vehicle operators — Access control monitoring and management

Vehicle *operators* (4.38) need to monitor and control the actions of their *drivers* (4.24) in order to best manage their fleets of *regulated vehicles* (4.42), and in many cases, to retain records and process self-regulated reporting and, in some cases, levies related to *access (*4.1).

10.1.4 Jurisdiction — Assessment of levies

In case there are levies associated with entering the critical area, *jurisdictions* (4.33) may need to have access to suitable tools to differentiate levies among fleet *operators* (4.38) depending on their performance over time.

10.1.5 Sensitive/restricted zone managers — Assessment of levies

In case there are levies associated with entering the critical area, the *SZM* (4.47) may need to have access to suitable tools to differentiate levies among fleet *operators* (4.38) depending on their performance over time.

10.2 Concept of operations for vehicle access management

10.2.1 General

The general goal of an *access methods* (4.3) or access management system is to increase the safety and the management efficiency of *sensitive/restricted zone* (4.46) *access* (4.1) management. However, there are different perspectives in use of this term concerning the nature of what comprises *access methods* (4.3) or what comprises an *access* management system.

Taken at its most restrictive interpretation, "access management" is simply the monitoring and control of "*access* (4.1)" to *sensitive/restricted zones* (4.46) of the road network, though even with this interpretation what constitutes a *sensitive/restricted zone*, and what constitutes a "regulated" vehicle, are liable to many interpretations and will, quite rightly, vary in different situations around the globe.

While in some parts of the world, "vehicle access monitoring" is very specific to the control of *access* (4.1) to and monitoring of "*sensitive/restricted zones* (4.46)" or "restricted access" for classes of vehicle or cargo (and related charging and fee payment issues), other *jurisdictions* (4.33) use the term in a much more general manner in respect of *regulated vehicles*. For example in Switzerland, the concept of *access* (4.1) for heavy goods vehicles is extended to charge for vehicular distance travelled in the country, regardless of type of road. The use cases extend beyond monitoring in order to impose penalties and levies and assessment, to generic areas such as asset protection/asset management, traffic management, safety, security, etc., even, in some *jurisdictions*, under the guise of "supervisory intervention orders", to vehicle regulation provisions such as alcohol interlocks, and more detail and *specification* (4.50) is provided for these aspects in Clause 16, *VAC*.

Taken to the extreme, "access management" can be considered as a sub set of control of the total network of public and private roads plus any travel by a motor vehicle anywhere in the country, in this case in the context of "*regulated commercial freight vehicles*" (4.42), however, they may be defined within a particular *jurisdiction* (4.33). While for organizational reasons, International Standards Organizations may organize their working arrangements to functional scopes such as "Freight and Fleet", *jurisdictions* may argue that this support cannot be limited only to "commercial" or "freight" vehicles, and that from their perspective there is little architectural difference between the *access methods* (4.3) and management of a heavy goods vehicle and the *access control* (4.2) of a light vehicle with an alcohol interlock as a supervisory provision for a *driver* (4.24) with a record of driving under the influence, for whom an alcohol interlock is a condition of permission of "*access* (4.1)" to drive.

The concept of "*BigBubble* (4.15)" areas, such as metropolitan area, which include within them several *sensitive/restricted zones* (4.46), can be embraced within the *VAM* (4.55) concept of operations, and may require some specialized techniques and adaptations of the general provisions for *VAM*.

Within the "*BigBubble* (4.15)", the *sensitive/restricted zones* (4.46) require to be defined, i.e. tunnels, bridges, urban areas near a schools or hospitals. Approaching (monitoring) areas to *sensitive/restricted zones* within the "*BigBubble*" need to be specified and provided, with adequate range, where the *regulated vehicle* (4.42) approaching the *sensitive/restricted zone* shall be tracked and monitored. The general *framework* (4.28) for "*BigBubble*" operation is accommodated within the provisions of this Clause.

Many *VAM* application service use cases, although functionally with very different objectives, can operate with only *basic vehicle data* (4.14) as defined in ISO 15638-5, and require no specialized standardization other than the provisions generically specified within ISO 15638-3, ISO 15638-5 and Clauses 8 and 9 of this part of ISO 15638-6 (related to the generic requirements of ISO 15638-6).

But there are many use cases where the objectives and the nature of the system are very specific, such that the means of collecting the required data and processing/sending the required data, while still using the architectural model of the triumvirate *jurisdiction* (4.33)/*application service provider* (4.7)/ *user* (4.53), are very different [vehicle *mass* (4.36) monitoring being a good example because it involves specialized equipment integrally installed in the *regulated vehicle* (4.42), but not normally fitted to all vehicles].

In these specialized *application services* (4.6), data collection, collation, and transfer, specific to that instantiation of *access methods* (4.3) and management shall be required. In general, the more specific the *application service*, the more specific the data required to support that service. So, for example, while remote *tachograph* (4.51) monitoring may be considered an "*access control* (4.2)" condition to enable a *driver* (4.24) to drive a vehicle, the data required, i.e. data from a tacograph, is very specific only to that *application service.* Within this part of ISO 15638, these specialized *application services* are defined in different parts of ISO 15638, which are referenced below.

This part of ISO 15638 focuses on generic *access methods* (4.3) or management systems whose objective is generically increase the safety and the management efficiency of *sensitive/restricted zone* (4.46) access management.

For specialized instantiation of "*access control* (4.2) and management", see the following.

a) VMM	vehicle mass monitoring	ISO 15638-12
b) MRC	"Mass" information for jurisdictional control and enforcement	ISO 15638-13
c) VAC	vehicle access control	ISO 15638-14
d) VLM	vehicle location monitoring	ISO 15638-15
e) VSM	vehicle speed monitoring	ISO 15638-16
f) CLM	consignment and location monitoring	ISO 15638-17
g) ADR	Accord Dangereuses par Route (Dangerous Goods) monitoring	ISO 15638-18
h) VPF	vehicle parking facilities	ISO 15638-19

These *application services* (4.6) are complementary, and the *architecture* (4.12) of *TARV* (ISO 15638-1) and its "operating requirements" (ISO 15638-3) are capable to support operation of any combination of these *application services*, or indeed all of them simultaneously, using one or multiple wireless communication media (as determined in ISO 15638-2). Support for other specialized applications may be included in later versions/issues of this part of ISO 15638.

10.2.2 Statement of the goals and objectives of the TARV VAM system

This Clause focuses on providing standardised support for generic *access methods* (4.3) or management systems to increase the safety and the management efficiency of *sensitive/restricted zone* (4.46) *access* (4.1) management.

The basic concept for "access management" is to monitor vehicles approaching *sensitive/restricted zones* (4.46) in order to monitor entry to/movement within/egress from the *sensitive/restricted zones* [measures to allow/deny the *access* (4.1) are provided in ISO 15638-14 (*VAC*)], as a preventive safety measure for reasons at the discretion of the *jurisdiction* (4.33), such as to avoid accidents, and/or as a tool to control dynamically traffic conditions in restricted areas, by using wireless communication between incoming vehicles and the infrastructure. See Figure 2.

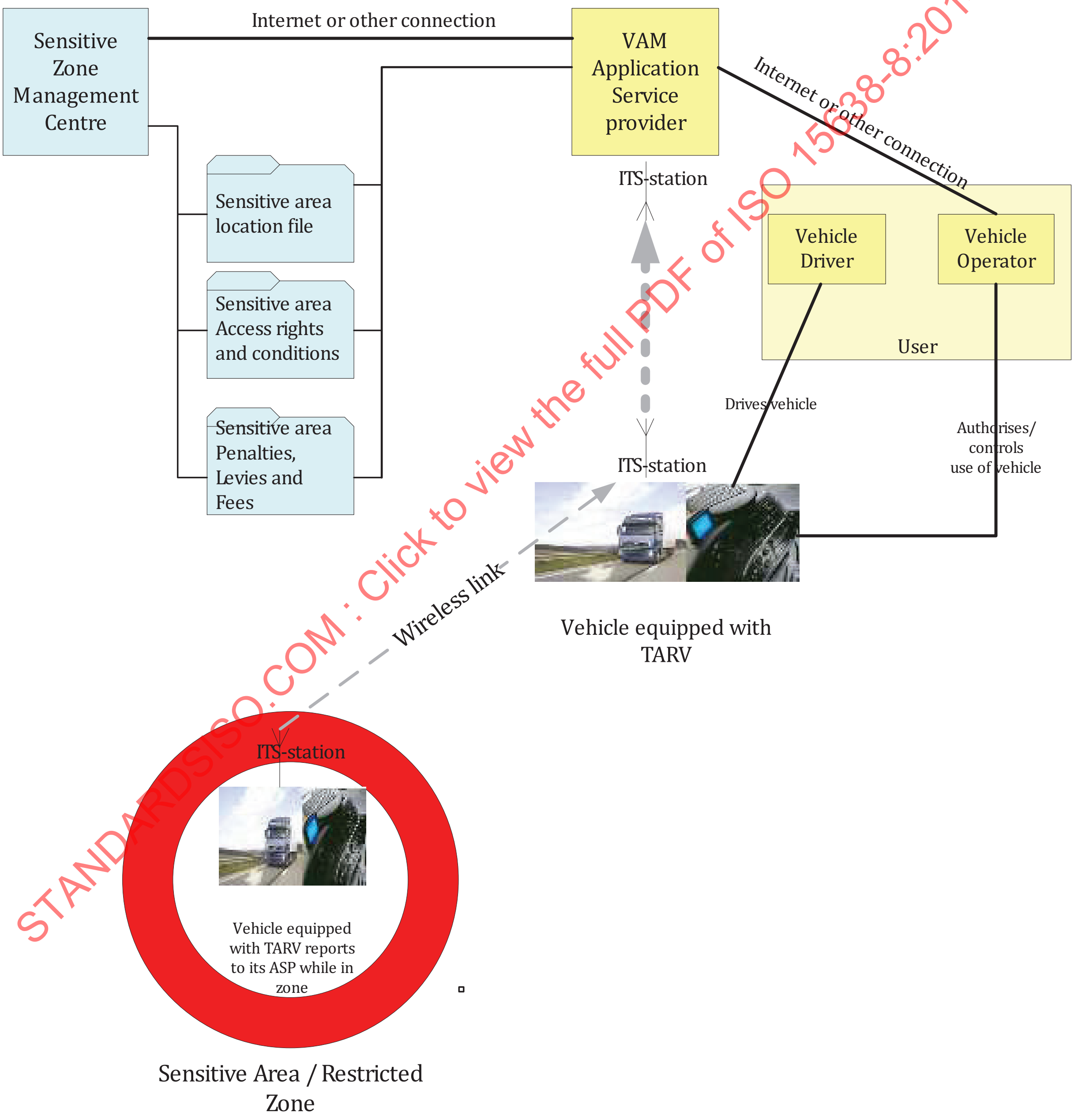
Sensitive Zone Management Centre
Internet or other connection
VAM Application Service provider
Internet or other connection
Sensitive area location file
Sensitive area Access rights and conditions
Sensitive area Penalties, Levies and Fees
ITS-station
Vehicle Driver
Vehicle Operator
User
Drives vehicle
Authorises/ controls use of vehicle
ITS-station
Wireless link
Vehicle equipped with TARV
ITS-station
Vehicle equipped with TARV reports to its ASP while in zone
Sensitive Area / Restricted Zone

Figure 2 — Vehicle access monitoring overview

VAM is normally a zone focused application, in that the greater objective is to know which vehicles, and potentially which loads, *drivers* (4.24) etc. are inside a *sensitive/restricted zone* (4.46) at any point in time, and potentially also where they are within the zone. The core activity elements that are essential to *VAM* may be considered as

a) determine and update *sensitive/restricted zone* (4.46) definition, *access* (4.1) rights and any related charging structures. Define and update *sensitive/restricted zone* definition, *access* rights and any related charging structures,

b) "approaching *access* zone" monitoring,

c) information feedback,

d) *BigBubble (4.15)* approaching and leaving,

e) monitoring while within the sensitive/restricted zone, and

f) egress from sensitive/restricted zone.

After detecting the entrance inside a predefined monitoring area, a monitoring *session* (4.49) is activated and the *regulated vehicle* (4.42) is "tracked" while approaching the *sensitive/restricted zone* (4.46). The approaching vehicle automatically sends relevant data to its *application service provider* (4.7), who obtains relevant information from the "*sensitive/restricted zone management* (4.47) centre". This enables the provision of required information, and to ascertain if the approaching vehicle shall be prevented from *access* (4.1) within the *sensitive/restricted zone,* whether formal *access control* (4.2) is in place and any data relevant to this that is required, and information concerning any charge of fees due and how they are collected. As with all *TARV* applications, the management of the application service is undertaken by the *application service provider* (4.7). This part of ISO 15638 attempts to specify neither how such management or control services are specified nor how their application service provision is designed and installed. It specifies only the communications required between the *regulated vehicle* (4.42) and the application service provider. Most communications are between the *ASP* and the *sensitive/restricted zone management* centre, or between the *vehicle operator* (4.38)/*application service provider/sensitive/restricted zone management* centre, and all of these communications and exchanges are outside of the scope of this part of ISO 15638.

Once within the *sensitive/restricted zone,* if the zone is equipped with *ITS-station* (4.31) interrogation points, if the *SZM* requests data from the *regulated vehicle* (4.42) it is provided indirectly as determined in ISO 15638-6, 8.3, with data from the *regulated vehicle* always provided to a predetermined IPv6 address in a separate communication from that of the interrogation. The *ASP* shall then provide the data to the *sensitive/restricted zone manager* by the means determined by the *sensitive/restricted zone manager* (and outside of the scope of this part of ISO 15638). The *ASP* is responsible to provide the *sensitive/restricted zone manager* with the data required by the regulations controlling *access* conditions for the *sensitive/restricted zone.*

Where appropriate and based on predefined policies and real time potential risk assessment, the *sensitive/restricted zone manager* (4.47) may provide the approaching vehicle with preventive grant or denial of *access* (4.1) to the *sensitive/restricted zone* (4.46). This may be effected via the *ASP*, or directly in communication to the *ITS-station* (4.31) of the vehicle *IVS* (4.29), but may affect the information that is required to be provided by the *regulated vehicle* (4.42). In a situation where *access* to the *sensitive/restricted zone* is controlled, the *driver* (4.24) of the *regulated vehicle* (4.42) needs to know if *access* to the *sensitive/restricted zone* has been granted, and the *IVS* needs to know of any additional data requirements.

The use cases for *access control* (4.2) and associated regulatory control are covered in ISO 15638-13.

Without specifying the specific details of any particular application, the generic *VAM* use case is shown in Figure 3.

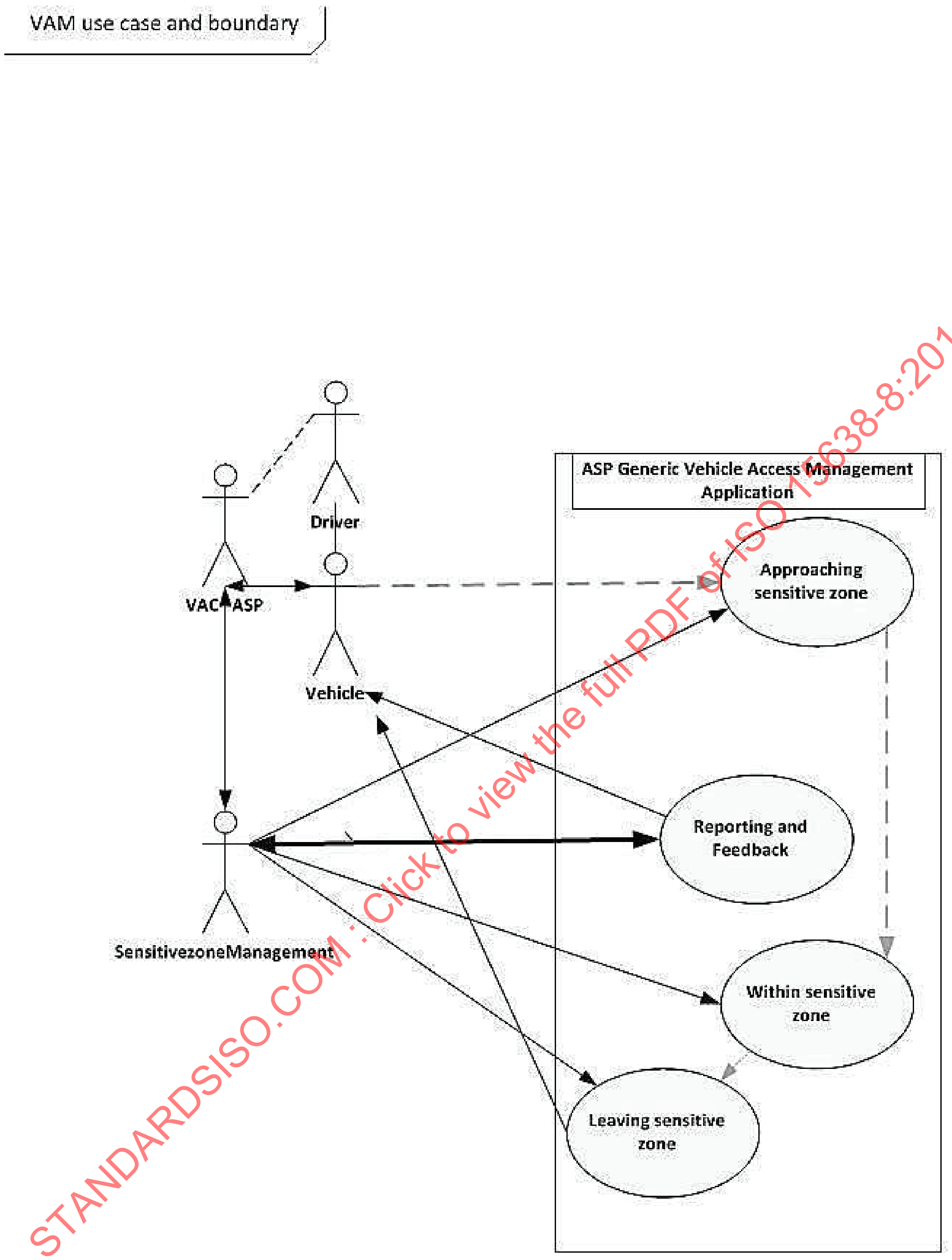

Figure 3 — VAM Use case and boundary

10.2.3 Strategies, tactics, policies, and constraints affecting the system

This application service support is designed for monitoring of vehicles in *sensitive/restricted zones* (4.46). For general monitoring of the location of *regulated vehicles* the *vehicle location monitoring* (4.56) provisions specified in Clause 17, or consignment and load monitoring provisions of ISO 15638-17, or, in the case of monitoring *dangerous goods* (4.22) to meet regulatory requirements, the provisions of ISO 15638-18 will be more appropriate.

However, given a suitable wireless communication the *sensitive/restricted zone manager* (4.47) may have the ability to ascertain where a particular truck is in the *sensitive/restricted zone* (4.46*)* at any time. This is dependent on there being a suitable wireless medium available to make an interrogation and for the vehicle to provide the data to its *ASP*. There is no limit on the size of a *sensitive/restricted zone,* and in some circumstances where the zone is small, one or a limited number of mobile or fixed *ITS-stations* (4.31) supporting full *C-ITS* (4.20) (for example at 5,9 GHz) could be used. However, if the *sensitive/restricted zone* (4.46) were a large area (for example, parts of Siberia or the Australian outback), satellite communications would have to be used to achieve this application service. In other locations, wireless media such as *GSM*/*GPRS*/*EDGE*/3G/*LTE*/4G or wireless mobile broadband may be more appropriate.

In respect of monitoring *drivers* (4.24), the provisions of ISO 15638-9 (*RTM*) and ISO 15638-11 (*DWR*) will be more appropriate than the provisions of this part of ISO 15638 (*VAM*).

Individual *jurisdictions* (4.33) may have specific requirements in respect of issues such as CO^2 emissions, carbon footprint, complex vehicle configurations, noise level, worn suspension air-bags, etc. that are not the subject of the specific application service provisions of ISO 15638 parts 8 et sequitur, and may find that the ability to develop specific requirements for additional data, provided in ISO 15638, 8.3 above, may be, in many cases, more appropriate than the provisions for *VAM* (this Clause) (and where there is common interest of several *jurisdictions* such provisions could be added to subsequent versions/releases of this part of ISO 15638).

10.2.4 Organizations, activities, and interactions among participants and stakeholders

The principle actors that comprise the system are

- *driver* (4.24),
- *regulated commercial freight vehicle* (4.42),
- *application service provider* (4.7), and
- *sensitive/restricted zone management* (4.47).

Three use cases have been identified, namely

a) approaching *sensitive/restricted zone* (4.46*)* — Planned,

b) approaching *sensitive/restricted zone* — Unplanned,

c) reporting and feedback,

d) within sensitive zone, and

e) exiting sensitive zone.

A sixth use case, “decision-making”, is dealt with in ISO 15638-14.

Table 1 provides a list of the actors involved, their activities, and interactions. It should be noted that an entity may perform multiple roles and in doing so takes on the responsibility to perform the functions described under those roles.

Table 1 — TARV VAM actors involved, their activities and interactions

Actor	Role	Activities	Interactions
Jurisdiction (J) (4.33)	Sets requirements for mandatory and supported *TARV VAM* (4.55)	Publishes *specifications* (4.50)	ALL

Table 1 *(continued)*

Actor	Role	Activities	Interactions
		Obtains regulations	ALL: Establish regime and regulations PSP: Register TARV equipment ASP Register Application, receive reports Op: Vehicle Registration Dr: Licence
		Appoints Approval Authority (if required)	AA: Contract. Instruct. Receive reports
		Monitors reports	
		Instigates any enforcement	
Approval authority (AA) (4.11)	Implements jurisdiction policy at equipment and service approval level	Certifies *IVS* (4.29), and vehicle equipment, *application service* (4.6) instantiations	PSP: Approve *IVS* ASP: Approve Application Service
		Conducts Q of S maintenance to instruction of jurisdiction	
Prime service provider (PSP) (4.39)	Responsibility for IVS	Installs and/or commissions *IVS*	AA: May apply to approve IVS Op: Installation
		Maintains *IVS*, related equipment	Op: Maintain IVS and related equipment
Application service provider (ASP) (4.7)	Provides *TARV VAM* application support services	Develops instantiation of *TARV VAM* application service	AA: Applies for approval of Service
		Contracts with *users* (*4.53*)	Op: Contracts
Sensitive/restricted area manager (4.47)	Manages *sensitive/ restricted area* (*4.46*)	Interfaces with *users* (Dr/ Op) and *jurisdiction*, collecting the parameters from the monitored *regulated vehicles*, process them according to the applicable policy and manage the access to the area, provides reports, exception reports, violations	ASP: collects data, passes information and instructions J: Provides reports
		Provides *TARV VAM* application service to users and jurisdiction	Op: Provides service Dr: May provide service J: Provides service/reports
Operator (Op) (4.38)	*Provides regulated vehicle* (4.42)	"Employs"/contracts *drivers* (4.24)	Dr: Employs/Contracts

Table 1 *(continued)*

Actor	Role	Activities	Interactions
	Uses *regulated vehicle* for commerce and logistics	Operates *regulated vehicle*	J: Registers regulated vehicle PSP: Contracts, receives service (install/maintain) ASP: Contracts, receives service
		Receives reports from ASP	
Driver (Dr)(4.24)	Drives *regulated vehicle* to instruction of *operator* (4.38)		Op: to instructions
		Signs into *TARV VAM* system	IVS: signs *driver* into system
		Drives vehicle	

The use case is depicted in Figure 3 above, and in the collaboration diagram shown in Figure 4.

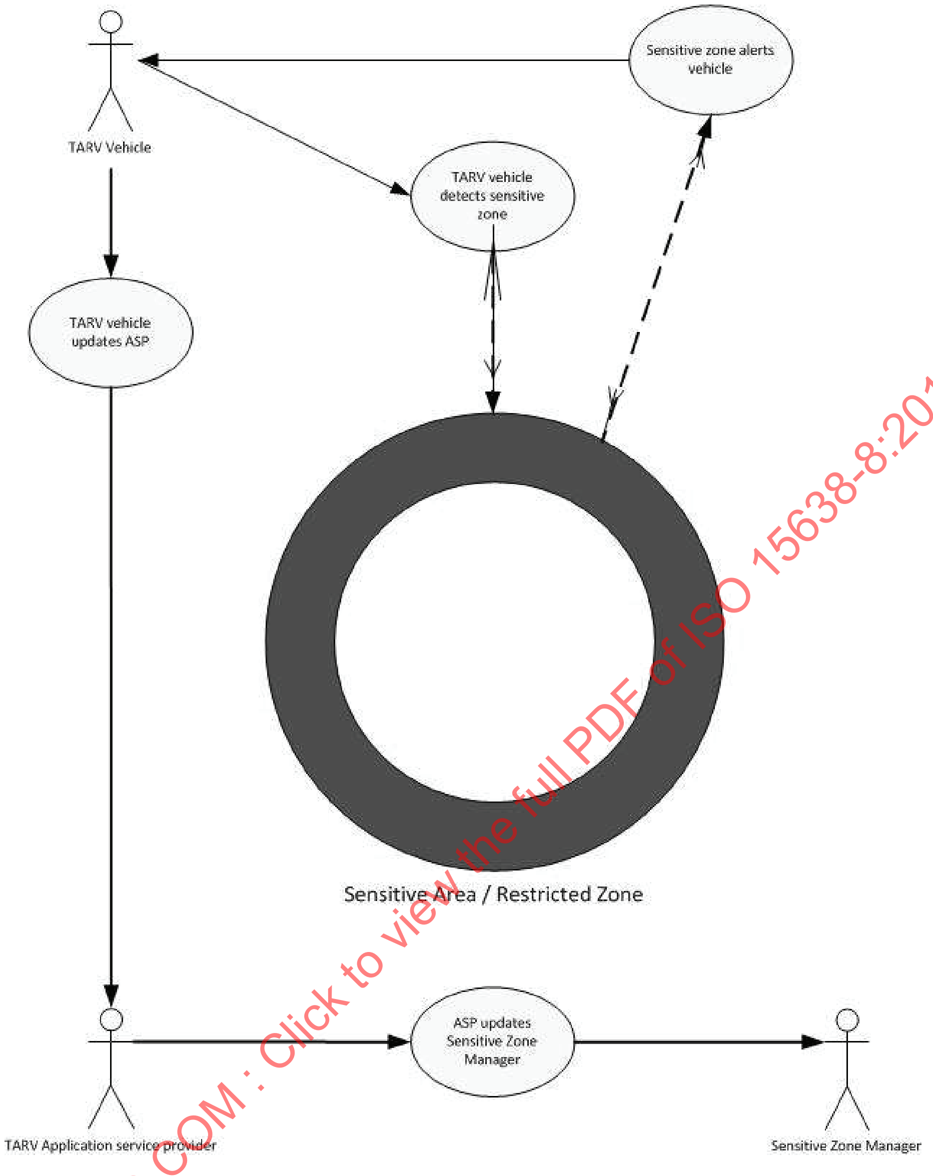
TARV Vehicle
Sensitive zone alerts vehicle
TARV vehicle detects sensitive zone
TARV vehicle updates ASP
Sensitive Area / Restricted Zone
ASP updates Sensitive Zone Manager
TARV Application service provider
Sensitive Zone Manager

Figure 4 — VAM Access collaboration diagram

10.2.4.1 Approaching sensitive/restricted zone — Planned

In this use case, the *ASP* (4.7) of the *regulated commercial freight vehicle* (4.42) shall make contact with the *regulated vehicle* to obtain its current *basic vehicle data* (4.14) as defined in ISO 15638-5. If the *regulated vehicle* is so equipped, the *ASP* may also obtain the *driver* (4.24) identification, and possibly load and its status, if this information is required by the *sensitive/restricted zone* (4.46) manager. If the *regulated vehicle* is not equipped to provide *driver* data or load data and if this is required information then, the *ASP* has the responsibility to obtain and provide that data by other means.

If the *jurisdiction* (4.33) controlling the *sensitive/restricted zone* (4.46) requires additional data supplied from the *regulated vehicle* (4.42), then either it shall provide an *app* (4.5) to the *ASP* who shall be responsible to preload the *app* into the memory of the vehicle *IVS* (4.29), or the *ASP* shall devise and install such an *app*. The communication between the *ASP* and the vehicle *IVS* shall be as determined in ISO 15638-6, 8.3, with data from the *regulated vehicle* (4.42) always provided to a predetermined IPv6 address in a separate communication from that of the interrogation. The *ASP* shall then provide the data to the *sensitive/restricted zone manager* (4.47) by the means determined by the *sensitive/restricted zone manager* (and outside of the scope of this part of ISO 15638). The *ASP* is responsible to provide the *sensitive/restricted zone manager* with the data required by the regulations controlling access conditions for the *sensitive/restricted zone.*

10.2.4.2 Approaching sensitive/restricted zone — Unplanned

In this use case, there has been no pre-planning regarding the *sensitive/restricted zone* (4.46). It may be for example, that a temporary *sensitive/restricted zone* has been created for security reasons or because of an incident or accident. The reasons for and conditions of *access* (4.1) to and reporting from a sensitive/restricted zone are entirely within the discretion of the *jurisdiction* (4.33) and outside of the *specifications* (4.50) of this International Standard.

In this circumstance, the *sensitive/restricted zone manager* (4.47) has the responsibility to alert the driver/vehicle that it is approaching a *sensitive/restricted zone* (4.46).

The *sensitive/restricted zone manager* (4.47) may provide this warning by providing a broadcast signal to a communications medium supported by the *TARV* equipped vehicle. In this case, this message shall stimulate an *app* (4.5) provided by the *ASP* to collect and transmit the *basic vehicle data* (4.14) as determined in ISO 15638-5, plus any additional information received from the broadcast, to the predetermined IPv6 address provided by the *ASP* as determined in ISO 15638-6, 8.3.4.1 to 8.3.4.2 and the *session* (4.49) shall then proceed as a planned approach to the *sensitive/restricted zone* (4.46), as determined in ISO 15638-6, 10.2.4.2.

In the case that the *sensitive/restricted zone manager* (4.47) does not have the means to automatically notify the vehicle *IVS* (4.29), it shall post a visible or audible notification to the *driver* (4.24) of the *regulated vehicle* (4.42), and the *driver* of the *regulated vehicle* shall trigger the *IVS* of the *regulated vehicle* (4.42) to send its *basic vehicle data* (4.14) to the predetermined IPv6 address provided by the *ASP*. The means of this triggering are a matter for system design and not standardization. These means may or may not permit the *driver* to provide further information to the *ASP*.

On receipt of an unplanned, unexpected set of *basic vehicle data* (4.14) the *ASP* (4.7) shall contact an address provided by the *jurisdiction* (4.33) to see if a (probably temporary) *sensitive/restricted zone* (4.46) has been created and obtain its *access* (4.1) conditions. Armed with the updated *basic vehicle data*, the *ASP* shall then meet the information provision requirements of the *sensitive/restricted zone manager* (4.47) by means outside of the scope of this International Standard. If the *access* conditions require an, or regular, updates of the *basic vehicle data* the *ASP* shall obtain these by the normal means of interrogation of the *IVS* (4.29) as determined in ISO 15638-6, Clause 8.

10.2.4.3 Reporting and feedback

The *access* (4.1) conditions provided by the *sensitive/restricted zone management* (4.47) shall determine the data and frequency of its provision that it requires from the *regulated vehicle*. In a planned situation, the *ASP* may have loaded an *app* (4.5) into the memory of the *IVS* (4.29) to provide this information at the intervals required. In an unplanned situation, If the *ASP* otherwise requires an, or regular, updates of the *basic vehicle data* (4.14) it shall obtain these by the normal means of interrogation of the *IVS* as determined in ISO 15638-6, Clause 8.

Access control (4.2) issues are specified in ISO 15638-14.

10.2.4.4 Within sensitive zone

Shall use the reporting and feedback provisions as described in 10.2.4.3

10.2.4.5 Exiting sensitive zone

It may be that the *sensitive/restricted zone manager* (4.47) also requires data when the *regulated vehicle* (4.42) is about to egress from the *sensitive/restricted zone* (4.46). As with the situation approaching the *sensitive/restricted zone,* it may provide that notification via an *ITS-station* (4.31) – *ITS-station* communication with the vehicle *IVS* (4.29), or by a visible or audio notification to the *driver* (4.24), or in this case it could have provided that data to the *ASP* in its exchange of information with them. As the *ASP* has the updated location of the *regulated vehicle* (4.42) every time it is provided with the *basic vehicle data* (4.14), it has the means to provide egress relative data to the *sensitive/restricted zone manager*, or to stimulate a new update of *basic vehicle data* from the *regulated vehicle* (4.42) to enable it to do so. Any associated *access control* (4.2) issues are specified in ISO 15638-14.

10.2.5 Clear statement of responsibilities and authorities delegated

10.2.5.1 The *jurisdiction* (4.33) shall be responsible for the regime and regulations.

10.2.5.2 The *jurisdiction* (4.33) shall employ an approv*al authority (regulatory)* (4.11) or otherwise, provide its function.

10.2.5.3 The *jurisdiction* (4.33) shall provide means for enforcement (where required) to meet the requirements of the regime of the *jurisdiction.*

10.2.5.4 The *prime service provider* (4.39) shall install/commission *IVS* (4.29) and maintain the *IVS*.

10.2.5.5 The *prime service provider* (4.39) shall install/commission, or supervise the installation/commissioning of any on-board equipment connected to the *IVS* (4.29).

10.2.5.6 The *application service provider* (4.7) *(ASP)* shall develop the *TARV VAM* application service or use a *TARV VAM application service* (4.6) provided by the *SZM* (4.47).

10.2.5.7 The *application service provider* (4.7) shall obtain any required *approval* (4.9) of its *TARV VAM* service from the *approval authority (regulatory)* (4.11).

10.2.5.8 The *application service provider* (4.7) shall contract with the *operator* (4.38) of the *regulated vehicle* (4.42).

10.2.5.9 The *application service provider* (4.7) shall be responsible to provide the application service to *jurisdiction* (4.33), *operator* (4.38), and *driver* (4.24) as specified in its service offering. The *ASP* shall be responsible to inform the *driver* (by whatever means the *ASP* deems appropriate and the *jurisdiction* considers adequate), of regulations in respect of the *sensitive/restricted zone* (4.46) and the rules and procedures for entering the *sensitive/restricted zone* in as much as this information is required for the *driver* to perform his tasks and remain within the regulations pertaining.

10.2.5.10 The *operator* (4.38) shall be responsible to provide the *regulated vehicle* (4.42).

10.2.5.11 The *operator* (4.38) shall be responsible to abide by requirements of the regime re *TARV VAM* and to be able to demonstrate compliance.

10.2.5.12 The *operator* (4.38) shall be responsible to pay penalties and levies required by *jurisdiction* (4.33), *SZM* (4.47), *prime service provider* (4.39) and *application service provider* (4.7). Where appropriate, the *operator* (4.38) shall pay any penalties and/or levies due to the *SZM*, or *jurisdiction,* via its *ASP*, but it shall always be the *regulated vehicle* (4.42) *operator* who is responsible for the payment of such penalties and levies.

10.2.5.13 The d*river* (4.24) shall be responsible to follow instructions, including use of the *IVS* (4.29) and associated equipment.

10.2.5.14 The *sensitive/restricted zone manager* (4.47) (*SZM*) shall, within a regime determined by the *jurisdiction* (4.33), be responsible for determining the regulation of the *sensitive/restricted zone* (4.46) and making such regulations as required for its management, and shall be responsible for making such regulations readily, freely, and fairly accessible to *ASPs* (4.7), and vehicle *operators* (4.38).

10.2.5.15 The *sensitive/restricted zone manager* (4.47) shall be responsible for developing and operating any systems required for the management of the *sensitive/restricted zone* (4.46) and for all and any interfaces associated with the zone required by the regime of the *jurisdiction* (4.33), and for providing access to *ASPs* (4.7) to enable them to provide required data to/from the system and for making any broadcasts or other communications requesting data, to the *regulated vehicle* (4.42).

10.2.5.16 In the event that penalties and/or levies imposed to enter, or for movement within or egress from the *controlled access zone* (4.19), the *controlled zone* manager shall provide the *ASP* (4.7) and/or the *regulated vehicle* (4.42) *operator* (4.38) with receipt for the applied penalties and/or levies including detail of the basis of the penalties or levies imposed.

10.2.6 Equipment required for TARV VAM

10.2.6.1 TARV IVS

10.2.6.1.1 The system shall be designed to work using *TARV IVS* (4.29) as defined in the ISO 15638 suite of standards deliverables

10.2.6.1.2 The *prime service provider* (4.39)/*application service provider* (4.7) shall provide to the *approval authority (regulatory)* (4.11) evidence of compliance from an appropriate body to demonstrate the suitability for use in vehicles for the *IVS* (4.29) and all associated components.

10.2.6.1.3 It shall not be possible for collected or stored vehicle data or data values in any software or non-volatile memory within the *IVS* (4.29) to be accessible or capable of being manipulated by any person, device, or system, other than that authorized by the *application service provider* (4.7).

10.2.6.2 Equipment periphery/connected to IVS

10.2.6.2.1 The requirements of this part of ISO 15638 can be met without the requirement for the use of additional equipment, however, for convenience, or to meet the requirements of other parts of ISO 15638, a vehicle may have equipment that is periphery/connected to, the *IVS* (4.29) (for example, driver input device, driver identification device, etc.).

Where such equipment is used it shall have been properly installed by the *prime service provider* (4.39) as approved by the *approval authority (regulatory)* (4.11) of the *jurisdiction* (4.33).

10.2.6.2.2 This part of ISO 15638 specifies the *framework* (4.28) for the communications requirements with vehicles for the monitoring of *regulated vehicle*s within *sensitive/restricted zones* (4.46). It does not specify any additional specific data collection requirements that such a system may require in addition to *basic vehicle data* (4.14). That is a matter for local regulation/system design. If these local system *specifications* (4.50) require data to be collected from additional equipment connected to the *IVS* (4.29), that shall be a local decision which requires clear *specification* (4.50) and control by the *jurisdiction* (4.33)/*SZM* (4.47) and is outside the scope of this part of ISO 15638. The provisions of ISO 15638-6, Clause 8 may however be used to transmit such data

10.2.6.3 TARV VAM “app”

The *ASP* (4.7) shall design and upload an *app* (4.5) designed to provide data to support the *TARV VAM* application or shall install an *app* designed by the *jurisdiction* (4.33) or *SZM* (4.47), to provide any data in addition to the *basic vehicle data* (4.14) required by the *jurisdiction/SZM*. The *specification* (4.50) of that *app* is a matter for the *ASP* and/or *jurisdiction/SZM* and is outside the scope of this part of ISO 15638.

10.2.7 Operational processes for the system — Define and update sensitive/restricted zone

A *sensitive/restricted zone* (4.46) shall be defined by the *SZM* (4.47) [e.g. urban pedestrian areas, school and hospital surroundings, freight villages, ports, road sensitivity infrastructure (bridges, tunnels, ...), weight restricted areas, width restricted areas, areas where there has been an accident or incident, etc.] and an approaching (monitoring) area identified with adequate range, where the *regulated vehicle (*4.42) approaching the *sensitive/restricted zone* shall be tracked and monitored in order to notify its entry to the *sensitive/restricted zone* shall be defined and declared.

In respect of the rules/regulations, these are at the determination of the *jurisdiction* (4.33) or *SZM* (4.47), but may be for example a requirement to receive vehicle information periodically for monitoring specific goods.

Information requirements may relate to/be dependent on issues such as weight restrictions, number of axles, height restrictions, speed limitation, safety distance between vehicles, etc.

Public authorities and/or "road operators" shall publish/define in advance the critical area definition, the policies/rules and recommendations.

The *SZM* (4.47) shall make generally available to *ASP*s (4.7), and shall notify *ASP*s each and every time in immediate response to receiving notification that a vehicle is approaching the *sensitive/restricted zone* (4.46), advising the policies/rules/regulations, requirements, and recommendations associated to the *sensitive/restricted zone.*

10.2.8 Operational processes for the system — Approaching sensitive/restricted zone (planned and unplanned)

The reference points for the "approaching *sensitive/restricted zone* (4.46)" (planned and unplanned) use case are the following.

10.2.8.1 *ASP* (4.7) determines that vehicle is approaching a *sensitive/restricted zone* (4.46) and warns the *driver* (4.24).

10.2.8.2 Equipment of the *SZM* (4.47) shall detect that a vehicle is approaching the *sensitive/restricted zone* (4.46) and its *ITS-station* (4.31) requests vehicle data.

10.2.8.3 Equipment of the *SZM* (4.47) broadcasts an approach warning and request for vehicle data to all approaching vehicles.

10.2.8.4 Vehicle shall detect that it is approaching a *sensitive/restricted zone* (4.46) and warns the *driver* (4.24).

10.2.8.5 Vehicle shall update and send *basic vehicle data* (4.14) to its *ASP* (4.7)

10.2.8.6 *ASP* (4.7) determines that vehicle routing is correct and sends vehicle identification parameters and relevant data to *SZM* (4.47).

10.2.8.7 *ASP* (4.7) instructs *driver* (4.24) not to enter *sensitive/restricted zone* (4.46) and provides re-routing information to *driver.*

10.2.9 Operational processes for the system — Reporting and feedback

The reference points for the reporting and feedback use case are the following.

10.2.9.1 *SZM* (4.47) advises *ASP* (4.7) of its information requirements for the *regulated vehicle* (4.42) while within the *sensitive/restricted zone* (4.46) in advance of journey.

10.2.9.2 *SZM (4.47)* advises *ASP (4.7)* of its information requirements for the *regulated vehicle (4.42)* in response to receipt of notification of vehicle approaching the *sensitive/restricted zone* (4.46).

10.2.9.3 *ASP* (4.7) downloads *app* (4.5) into library of *IVS* (4.29) to program the *regulated vehicle* (4.42) to provide data at requested intervals or triggers.

10.2.9.4 *ITS-station* (4.31) of *SZM* (4.47) interrogates vehicle at points where it requires vehicle data with a request for data and possibly provides some additional reference data to the *regulated vehicle* (4.42).

10.2.9.5 In response to the installed *app* (4.5) or a prompt from an *ITS-station* (4.31) of the *SZM* (4.47), the vehicle *IVS* (4.29) shall update and send *basic vehicle data* (4.14) plus any additional data previously instructed by the *SZM*, together with any reference data provided by the interrogator, to the IPv6 address previously determined by the *ASP* (4.7), who verifies and forwards the data to the system of the *SZM*.

10.2.10 'BigBubble' approaching and leaving

This configuration adopts a big area, for example a metropolitan area, which includes several *sensitive/restricted zones* (4.46) within its monitoring area [referred to in some projects as a *BigBubble* (4.15)]. The design, nature, and complexity will vary from instantiation to instantiation, and will have significant impact on the design and management of the *SZM* (4.47) system. In some *C-ITS* (4.20) implementations, this can have significant impact on the data exchange transactions between the *regulated vehicle* (4.42) and the *SZM* system. With the *architecture* (4.12) of *TARV*, however, all such complications reside in the *SZM* system, or the *ASP* system, and do not impact the *regulated vehicle*, which simply responds to the instructions of the relevant *app* (4.5) or to interrogation requests from an *ITS-station* (4.31) of the *SZM*.

10.3 Sequence of operations for TARV VAM

The sequence of operations for *TARV VAM* are therefore, very simple.

10.3.1 VAM service element (VAM SE1): Define sensitive/restricted zone

The jurisdiction shall define the *sensitive/restricted zone* (4.46) and its *access* (4.1) conditions.

10.3.2 VAM service element (VAM SE2): Publish regulation

The jurisdictions shall post/make *sensitive/restricted zone* (4.46) and its *access* (4.1) conditions regulation information available to *ASPs* (4.7) and *users* (4.53).

10.3.3 VAM service element (VAM SE3): Detect approaching regulated vehicle

By one of several means, the approaching point of entry by a *regulated vehicle* into a *sensitive/restricted zone* (4.46) shall be detected and the *ASP* (4.7) shall be advised.

10.3.4 VAM service element (VAM SE4): ASP notifies SZM of approaching vehicle

The *ASP* (4.7) shall notify the *SZM* (4.47) with relevant vehicle details.

10.3.5 VAM service element (VAM SE5): Periodic or requested updates

When within the *sensitive/restricted zone* (4.46), the *IVS* (4.29) of the *regulated vehicle* (4.42) shall update and send its *basic vehicle data* (4.14) together with other predetermined required data to its *ASP* (4.7) according to its *app* (4.5) or an external trigger, such as requests from an *ITS-station* (4.31) of the *SZM* (4.47).

10.3.6 VAM service element (VAM SE6): "Interrogated" request for vehicle data

10.3.6.1 An interrogating ITS-station shall request specific data as determined in ISO 15638-6, 7.1 and 8.1.2.

10.3.6.2 In the event that the IVS of a vehicle receives a wireless interrogation requesting the LDT or "*CoreData*" (4.21), the interrogator shall also provide at the time of the request, a unique 8 byte reference number (URef), and a destination IPv6 address (ReqDest) where it requests the data to be sent.

10.3.6.3 On receipt of the request, the IVS shall acknowledge the request with the appropriate ACKnowledgement defined in ISO 15638-6, 8.3.5 < L > or < D > , which acknowledges that a request for LDT or "*CoreData*" (4.21) has been received.

10.3.6.4 The IVS shall then close the communication session.

10.3.6.5 The IVS shall then open a new communication session using an available and appropriate CALM wireless medium.

10.3.6.6 The IVS shall then send the LDT or "*CoreData*" (4.21) file to a predetermined destination IPv6 (internet) address that has previously been stored in the memory of the data pantry by its ASP, together with the URef and ReqDest provided by the interrogator.

10.3.6.7 On successful receipt of the data, the recipient at the predetermined destination IPv6 address shall send an acknowledgement < LDX > or < CDX > to the IVS.

10.3.6.8 On receipt of the acknowledgement < LDX > or < CDX >, the IVS shall close its communication session.

10.3.6.9 The ASP shall be responsible to verify that the interrogation is legitimate, appropriate, and from an accepted source, and having verified this, shall be responsible to send the data to the interrogator requested IPv6 address. The means and detail of how this is achieved is outside the scope of this part of ISO 15638.

10.3.7 VAM service element (VAM SE7): ASP updates SZM

The *ASP* (4.7) shall update the *SZM* (4.47) with periodic or requested data.

10.3.8 VAM service element (VAM SE8): Vehicle egress

The *regulated vehicle* (4.42) leaves the *sensitive/restricted zone* (4.46).

10.4 Generic TARV VAM data naming content and quality

The process to obtain *basic vehicle data* (4.14) [*TARV LDT* (4.35)] data content shall be as defined in ISO 15638-5, 8.2, 8.3, and 8.4.

In respect of the URef and Datreq, it shall be defined as in Table 2.

Table 2 — Data definitions

Number	Data concept name	Use	Format	Notes/Source
VAM001	LDT			As defined in ISO 15638-5, 8.2, 8.3, and 8.4.
VAM002	'CoreData'			As defined in ISO 15638-5, 8.2, 8.3, and 8.4.
*VAM*003	Uref	Mandatory	AN (8)	An 8 byte reference provided by the interrogator requesting the data. The alphanumeric or binary content of which is unspecified by this International Standard, but is intended to be used by the interrogator to provide a unique reference to its request for data.
*VAM*004	ReqDes	Mandatory	35 Bytes	Requested destination IPv6 address for the data to be sent as: scheme://domain:port/path?query_string#fragment_id i.e. The scheme name (commonly called protocol), followed by:// then, depending on scheme, a domain name (alternatively, IP address): a port number, and/the path of the resource to be fetched or the program to be run. If the scheme name is http, the "http://" is assumed e.g.: www.example.com/path/to/name https://example.com/47.35868 telnet://192.0.2.16:80/

10.5 Specific TARV VAM data naming content and quality

Sensitive/restricted zone (4.46) specific additional data shall be as specified by the *jurisdiction* (4.33)/ *SZM* (4.47).

10.6 TARV VAM application service specific provisions for quality of service

The integrity of the data are important, and other sensors as well as parameters may then be required based on the approaches and techniques used to provide assurance of the quality of the data. The generic quality of service provisions for the service elements specified in 10.4 are defined in ISO 15638-6 and ISO 15638-5.

Instantiation specific requirements shall be part of the regulation of the *jurisdiction* (4.33). However, in defining such requirements *jurisdictions* shall wherever possible, use performance based or functional *specifications* (4.50) in order to avoid locking requirements into technologies that will become obsolete.

See also Clause 9 above for general quality of service requirements.

10.7 TARV VAM application service specific provisions for test requirements

There are no specific provisions for test requirements specified in this first version of this International Standard.

10.8 TARV VAM application specific rules for the approval of IVSs and "service providers"

Shall be as specified in ISO 15638-6, 9.16.

11 Declaration of patents and intellectual property

This part of ISO 15638 contains no known patents or intellectual property other than that which is implicit in the media standards referenced herein and in ISO 15638-2. While the *CALM* standards themselves are free of patents and intellectual property, *CALM* in many cases relies on the use of public networks and IPR exists in many of the public network media standards. The reader is referred to those standards for the implication of any patents and intellectual property.

Application services (4.6) specified within this part of ISO 15638, ISO 15638-6, and ISO 15638-7 contain no direct patents nor intellectual property other than the copyright of ISO. However, national, regional, or local instantiations of any the applications services defined in this part of ISO 15638, ISO 15638-6 and ISO 15638-7, or of the generic vehicle information defined in ISO 15638-5, the security requirements contained in ISO 15638-4, or the requirements of ISO 15638-3, may have additional requirements which may have patent or intellectual property implications. The reader is referred to the regulation regime of the *jurisdiction* (4.33) and its regulations for instantiation in this respect.

Annex A
(informative)

ASN.1 Modules for ISO 15638-8 data concepts

A.1 Use of ASN.1

ISO TC 204 requires that data concepts defined in ISO TC 204 ITS standards deliverables are elaborated in ASN.1 (ISO 14813-6).

ISO 21217(ITS- CALM -ITS-station communications architecture) and its associated standards require the exchange of data using ASN.1 PER or UPER.

The following example provides a definition for the data concepts used in this Standard.

A.2 ASN.1 modules for ISO 15638-8 (vehicle access monitoring)

A.2.1 Data concepts defined in ISO 15638-5 and used in ISO 15638-8 (VAM)

```
TARVLocalDataTree DEFINITIONS AUTOMATIC TAGS::=
   BEGIN
        LDTData::= SEQUENCE
        {dataFormatVersion      DataFormatVersion,
         messageID              MessageIdentifier,
         primeSPID              PrimeServiceProviderIdentifier,
         applicationSPAddress   ApplicationServiceProviderAddress,
         sessionControlData     SessionControlData OPTIONAL,
         vehicleUniqueID        VehicleUniqueIdentifier OPTIONAL,
         vehicleClassID         VehicleClassIdentification OPTIONAL,
         vin                    VIN,
         propulsionStorageType  PropulsionStorageType,
         time                   TimeAndTimestamp DEFAULT 0,
         location               Location,
         direction              DirectionOfTravel,
         ignition               Ignition,
         movementSensors        OtherMovementSensors,
         driverID               DriverIdentification,
         trailerID              TrailerIdentification OPTIONAL,
         loadData               LoadData
         }

        DataFormatVersion::= VisibleString (SIZE (6))

        MessageIdentifier::= INTEGER

        PrimeServiceProviderIdentifier::= VisibleString (PATTERN “\w#4:\w#4:\w#4:\w#4:\
w#4:\w#4:\w#4:\w#4”) -IPv6 address in the format xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx

        ApplicationServiceProviderAddress::= CHOICE {
        content   [0] INTEGER (128..16511), -contained in two octets
        extension [1] OCTET STRING(SIZE (2))
        }

        SessionControlData::= VisibleString

        VehicleUniqueIdentifier::= SEQUENCE {
        countryCode        VisibleString,
        alphabetIndicator VisibleString,
        licPlateNumber     NumericString
        }
        VehicleClassIdentification::= NumericString (SIZE (2))

        VIN::= VisibleString (SIZE (17))

        PropulsionStorageType::= BIT STRING {
        gasoline (0),
        diesel   (1),
        cng      (2),
        lpg      (3),
        electric (4),
        hydrogen (5)
        } –Enter type value with curly bracket at beginning and end, assignment type will
accept word and binary forms of storage type

        TimeAndTimestamp::= INTEGER

        Location::= SEQUENCE {
                              latitude  VisibleString (SIZE (10)),
                              longitude VisibleString (SIZE (10)),
                              altitude  VisibleString (SIZE (4..5)) DEFAULT “0000”,
                              noOfSats  VisibleString (PATTERN “Sat\d+”), –Type value
must be in the format “SatN”, where N = the number of satellites present
                              trust     INTEGER {
                                                   false (0),
                                                   true  (1)
                                                   } (0 | 1) –accepts true, false, 0 or 1
                              }

        DirectionOfTravel::= INTEGER (0..358) –degrees clockwise

        Ignition::= VisibleString (“Ign 1” | “Ign 0” | “Ign d”) –where 1=on, 0=off,
d=disconnected

        OtherMovementSensors::= SEQUENCE
        {sensorOne VisibleString (PATTERN “\d+\s\Mvt\s[m,n,d]”|”000”) DEFAULT “000”, –Type
value must be in the format “[SensorNumber] Mvt [m/n/d]”, where m=movement, n=no movement,
d=disconnected
        sensorTwo  VisibleString (PATTERN “\d+\s\Mvt\s[m,n,d]”|”000”) DEFAULT “000”
        }

        DriverIdentification::= SEQUENCE
        {jurisdictionID    VisibleString (PATTERN “\d#6\s\w+\s\w+\s(\w+,)*\s\d#6”), –
Must be in the format “[IssueDate(yymmdd)] [IssuingJurisdiction] [Driver’sName]
[VehicleClasses(comma separated)] [ExpiryDate(yymmdd)]”
        userAuthorisation VisibleString (PATTERN “\d#6\s\w+\s\w+\s(\w+,)*\s\d#6”|”000000”)
DEFAULT “000000” –Same format as jurisdictionID
        }

        TrailerIdentification::= VisibleString

        LoadData::= VisibleString
   END
```

A.2.2 Data concepts defined in ISO 15638-8 (VAM)

```
VehicleAccessManagement DEFINITIONS AUTOMATIC TAGS::=
   BEGIN
      IMPORTS LDTData FROM TARVLocalDataTree;

      VAMData::= SEQUENCE
      {vAM001 LDTData,
       vAM002 CoreData,
       vAM003 Uref,
       vAM004 ReqDes
      }

      CoreData::= SEQUENCE
      {ipv6DestinationAddress VisibleString (PATTERN “\w#4:\w#4:\w#4:\w#4:\w#4:\w#4:\
w#4:\w#4”),
      essentialVehicleData     LDTData,
      appData                  AdditionalDataOptions
      }

      AdditionalDataOptions::= SEQUENCE
      {accelerometer    AccelerometerData OPTIONAL,
       gyroscope        GyroscopeData OPTIONAL,
       stillCamData     BIT STRING OPTIONAL,
       videoData        BIT STRING OPTIONAL,
       speed            VehicleSpeedData OPTIONAL,
       alarm            AlarmStatusData OPTIONAL
       }

      AccelerometerData::= SEQUENCE
      {x-axis VisibleString (PATTERN “\w#4\s\w#4\s\w#4\s\d#4\s\d#4\s\d#4\s\d#4”),
       y-axis VisibleString (PATTERN “\w#4\s\w#4\s\w#4\s\d#4\s\d#4\s\d#4\s\d#4”),
       z-axis VisibleString (PATTERN “\w#4\s\w#4\s\w#4\s\d#4\s\d#4\s\d#4\s\d#4”),
       sync   VisibleString (PATTERN “\w#4\s\w#4\s\w#4\s0000\s0000\s0000\s0000”)
      }

      GyroscopeData::= SEQUENCE
      {angularRateX  BIT STRING (SIZE (10)),
       angularRateY  BIT STRING (SIZE (10)),
       angularRateZ  BIT STRING (SIZE (10)),
       accelerationX BIT STRING (SIZE (10)),
       accelerationY BIT STRING (SIZE (10)),
       accelerationZ BIT STRING (SIZE (10))
      }

      VehicleSpeedData::= SEQUENCE
      {serialNumber VisibleString (PATTERN “s0\d#3”), -e.g. s0123
       timeStamp    NumericString (SIZE (6)), -e.g. 110316
       unit         VisibleString (“k”|”m”), -e.g. k
       speed        INTEGER (0..400), -e.g. 53
       latitude     VisibleString (SIZE (10)), -e.g. 0x0A5D3770
       longitude    VisibleString (SIZE (10)), -e.g. 0x027E2938
       direction    INTEGER (0..358) -e.g. 123
      }

      AlarmStatusData::= SEQUENCE
      {recordNumber VisibleString (PATTERN “A0\d#4”),
       dateTime     INTEGER,
       alarmCode    VisibleString (PATTERN “A\d#(1,2)”)
      }

Uref::= VisibleString (SIZE (8))

ReqDes::= VisibleString (SIZE (35))

END
```

Annex B
(informative)

Independent testing of the protocols defined in this part of ISO 15638

B.1 Objectives

To test the validity of TARV standards, it is necessary to simulate the TARV transactions. These are of two types.

I. Instigation

a) The IVS of a vehicle establishes a new communication using one of (and must be tested for each of) several wireless media defined below.

b) The IVS of a vehicle internally triggers a requirement to send a packet of data to a predetermined destination IPv6 (internet) address.

c) The vehicle sends the data file to the predetermined destination IPv6 (internet) address.

d) The recipient address sends acknowledgement.

e) The IVS closes the communication on receipt of acknowledgement.

II. Interrogation

a) The IVS of a vehicle receives a wireless interrogation requesting a packet of data.

b) The IVS of a vehicle is switched on but is not connected.

c) The IVS of a vehicle receives a wireless interrogation requesting a packet of data.

d) On receipt it acknowledges the request (ACK).

e) It closes the communication.

f) It opens a new communication session using one of (and must be tested for each of) several wireless media defined below.

g) It sends the data file to a predetermined destination IPv6 (internet) address.

h) The recipient address sends acknowledgement.

i) The IVS closes the communication on receipt of acknowledgement.

These scenarios need to be tested using each of 2G, 3G, WiFi, 5,9 GHz (IEEE 802.11) using the same data.

A number of different data files (of different length) and acknowledgements need to be sent, which differ according to the application service. Each of the sequences defined below need to be tested.

In respect of “interrogation” scenarios, the ability to receive the interrogation on one medium (esp. 5,9 GHz) and to instigate the subsequent message using a different medium needs to be tested.

Preconditions, assumptions, and simulations

a) The s.u.t. concerns only the communication between the IVS and the application service provider address. No other part of the system specifications are to be tested (they appear in the figures below for context, and because there are copied from the base standards.)

b) CALM and media choice are assumed, and not s.u.t.

c) The vehicle is equipped with wireless communications that enable it to make communications using 2G, 3G, Mesh WiFi, 5,9 GHz (IEEE 802.11p).

d) The means to trigger the sending of a message from the vehicle is a function of IVS design, not s.u.t., therefore, may be simulated.

e) The destination address is intended to be an IPv6 address, but may be simulated with an IPv4 address as this is an internet issue, not s.u.t.

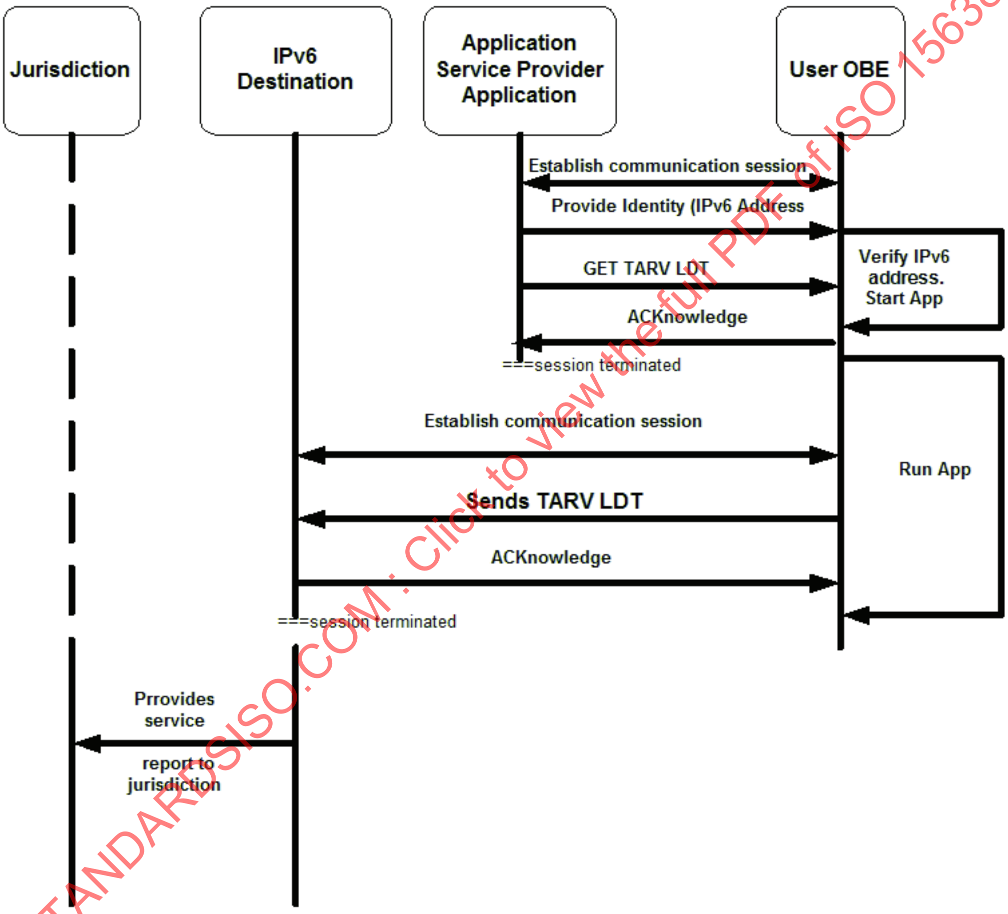

Figure B.1 — Communications sequences to obtain TARV LDT

Application Services where the verity of the communication needs to be physically tested

a) *VAM* *vehicle access monitoring*

b) *RTM* *remote electronic tachograph monitoring*

c) EMS *emergency messaging system*

d) *DWR* *driver work records* (work and rest hours compliance)

e) *VMM* *vehicle mass monitoring*

f) *MRC* *'Mass' data for regulatory control and management (no test - data as VMM)*

g) *VAC* *vehicle access control (no test - data as VAM)*

h) *VLM* *vehicle location monitoring*

i) *VSM* *vehicle speed monitoring*

j) *CLM* *consignment and location monitoring*

k) *ADR* *Accord Dangereuses par Route (Dangerous Goods) monitoring*

l) *VPF* *vehicle parking facilities*

Test Sequences

Each of the following application service data provision sequences needs to be successfully sent.

B.2 Test script 1 LDT Service: VAM vehicle access monitoring (LDT)

CTP 1.1.1 Instigated LDT using 2G

SUT Reference	**Instigated send of LDT data using 2G**
CTP/1.1.1	
SUT Test Objective	The IVS of a vehicle establishes a new communication using one of (and must be tested for each of) several wireless media defined below. The IVS of a vehicle internally triggers a requirement to send a packet of data to a predetermined destination IPv6 (internet) address. The vehicle sends the data file to the predetermined destination IPv6 (internet) address. The recipient address sends acknowledgement. The IVS closes the communication on receipt of acknowledgement.
CTP Origin	CSI
Reference requirement	ISO 15638-8 and ISO 15638-6, 8.3.4.2
Initial Conditions	The s.u.t. concerns only the communication between the IVS and the application service provider address. No other part of the system specifications are to be tested (they appear in the figures below for context, and because there are copied from the base standards). CALM and media choice are assumed and not s.u.t. The vehicle is equipped with wireless communications that enable it to make communications using 2G, 3G, WiFi, 5,9 GHz (IEEE 802.11p). The means to trigger the sending of a message from the vehicle is a function of IVS design, not s.u.t., therefore may be simulated. The destination address is intended to be an IPv6 address, but may be simulated with an IPv4 address as this is an internet issue, not s.u.t.
Stimulus and expected behaviour	

Test point		**Tester action**	**Pass condition**

1.1.1.1	1	IVS instigates a communication session using selected media (2G) to predetermined destination IP address	Session established
1.1.1.2	2	IVS sends file named < 44EMV03WRRLDT > < START > < AaaSs0,,0,xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx,128..16511,1G1JF27W8GJ178227,000000,1297339499,0x0A5D3770,0x027E2938,0000,Sat8,0,123,Ign 1,000,000,010326 UKPeter Jones,01,02,03a,h1,120325,010326 124538, Peter Jones 01,02,h1120325 > < END >	File sent and arrives correctly at destination
1.1.1.3	3	Destination address sends ACK < LDX >	
1.1.1.4	4	IVS receives ACK < LDX >	File received and ACK < LDX > sent
1.1.1.5	5	IVS closes communication session	Communication session closed

			If ALL individual pass conditions listed in this column above have been met
			THEN CTP PASS
			ELSE CTP FAIL

TEST RESULT: CTP 1.1.1	PASS/FAIL	Date: 28th June 2012
Signature/initials	PASS	innovITS ADVANCE k4, MIRA, Watling St, Nuneaton, Warwickshire, CV10 0TU, UK Tel: +44 (0)7730 922 810 Web: www.innovits.com/advance

CTP 1.1.2 Interrogated LDT using 2G

SUT Reference	Interrogated send of LDT data using 2G
CTP/1.1.2	
.	

SUT Test bbjective	The IVS of a vehicle receives a wireless interrogation requesting a packet of data. The IVS of a vehicle is switched on but is not connected. The IVS of a vehicle receives a 2G wireless interrogation requesting a packet of data. On receipt it acknowledges the request (ACK). It closes the communication. Opens a new communication session using one of (and must be tested for each of) several wireless media defined below. Sends the datafile to a predetermined destination IPv6 (internet) address. Recipient address sends acknowledgement. IVS Closes the communication on receipt of acknowledgement.
CTP brigin	CEN
Reference requirement	ISO 15638-8 and ISO 15638-6, 8.3.4.2
Initial conditions	The s.u.t. concerns only the communication between the IVS and the application service provider address. No other part of the system specifications are to be tested (they appear in the figures below for context, and because there are copied from the base standards). CALM and media choice are assumed and not s.u.t. The vehicle is equipped with wireless communications that enable it to make communications using 2G, 3G, WiFi, 5,9 GHz (IEEE 802.11p). The means to trigger the sending of a message from the vehicle is a function of IVS design, not s.u.t., therefore may be simulated. The destination address is intended to be an IPv6 address, but may be simulated with an IPv4 address as this is an internet issue, not s.u.t.

Stimulus and expected behaviour

Test point		**Tester action**	**Pass condition**
1.1.2.1	1	Session connected (incoming call)	Call in progress
1.1.2.2	2	Caller sends data request command (GPRS, EDGE, etc.) GET VAM	Data request sent
1.1.2.3	3	IVS acknowledges request by returning ACKnowledgement < A >	ACK < A > received
1.1.2.4	4	IVS closes communication session	Communication session closed
1.1.2.5	5	IVS instigates a communication session using selected media to predetermined destination IP address	Communication session successfully opened
1.1.2.6	6	IVS sends file named < 44EMV0 < START > < AaaSs0,,0,xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx,128..16511,1G1JF27W8GJ178227,000000,1297339499,0x0A5D3770,0x027E2938,0000,Sat8,0,123,Ign 1,000,000,010326 UKPeter Jones,01,02,03a,h1,120325,010326 124538, Peter Jones 01,02,h1120325 >< END >	File sent and arrives correctly at destination
1.1.2.7	7	Destination address sends ACK < LDX >	
1.1.2.8	8	IVS receives ACK < LDX >	File received and ACK < LDX > sent

1.1.2.9	9	IVS closes communication session	Communication session closed

			If ALL individual pass conditions listed in this column above have been met
			THEN CTP PASS
			ELSE CTP FAIL

TEST RESULT: CTP 1.1.2	PASS/FAIL	Date: 28th June 2012
Signature/initials	PASS	innovITS ADVANCE k4, MIRA, Watling St, Nuneaton, Warwickshire, CV10 0TU, UK Tel: +44 (0)7730 922 810 Web: www.innovits.com/advance

CTP 1.1.3 Interrogated LDT using 5,9 GHz and responding using 2G or 3G

S.U.T. Reference	Interrogated LDT using 5,9 GHz and send of LDT data using 2G or 3G
CTP/1.1.3	
.	
S.U.T. Test objective	The IVS of a vehicle receives a wireless interrogation requesting a packet of data. The IVS of a vehicle is switched on but is not connected. The IVS of a vehicle receives a 5,9 GHz (IEEE 802.11p) wireless interrogation requesting a packet of data. On receipt it acknowledges the request (ACK). It closes the communication. Opens a new communication session using 2G or 3G. Sends the datafile to a predetermined destination IPv6 (internet) address. Recipient address sends acknowledgement. IVS Closes the communication on receipt of acknowledgement.
CTP origin	CEN
Reference requirement	ISO 15638-8 and ISO 15638-6, 8.3.4.2