PD ISO/TS 15638-18:2013

BSI Standards Publication

Intelligent transport systems — Framework for collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV)

Part 18: ADR (Dangerous Goods) transport monitoring (ADR)

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of ISO/TS 15638-18:2013.

The UK participation in its preparation was entrusted to Technical Committee EPL/278, Intelligent transport systems.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 80632 2

ICS 03.220.20; 35.240.60

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 July 2013.

Amendments issued since publication

Date	Text affected

PD ISO/TS 15638-18:2013

TECHNICAL SPECIFICATION

ISO/TS 15638-18

First edition
2013-07-01

Intelligent transport systems — Framework for collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV) —

Part 18: ADR (Dangerous Goods) transport monitoring (ADR)

Systèmes intelligents de transport — Cadre pour applications télématiques collaboratives pour véhicules de fret commercial réglementé (TARV) —

Partie 18: Monitorage du transport (de biens dangereux) d'ADR

Reference number
ISO/TS 15638-18:2013(E)

COPYRIGHT PROTECTED DOCUMENT

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 v
Introduction vii
1 Scope 1
2 Conformance 1
3 Normative references 2
4 Terms and definitions 2
5 Symbols and abbreviated terms 7
6 General overview and framework requirements 9
7 Requirements for services using generic vehicle data 9
8 Application services that require data in addition to basic vehicle data 9
8.1 General 9
8.2 Quality of service requirements 9
8.3 Test requirements 10
8.4 Marking, labelling and packaging 10
9 Common features of regulated TARV application services 10
9.1 General 10
9.2 Common role of the jurisdiction, approval authority, service provider and user. 11
9.3 Common characteristics for instantiations of regulated application services 11
9.4 Common sequence of operations for regulated application services 11
9.5 Quality of service 11
9.6 Information security 11
9.7 Data naming content and quality 12
9.8 Software engineering quality systems 12
9.9 Quality monitoring station 12
9.10 Audits 12
9.11 Data access control policy 12
9.12 Approval of IVSs and service providers 12
10 TARV ADR consignment monitoring (*ADR*m) 12
10.1 ADRm service description and scope 12
10.1.1 ADRm use case 13
10.1.2 Description of ADRm regulated application service 13
10.2 Concept of operations for ADRm 14
10.2.1 General 14
10.2.2 Statement of the goals and objectives of ADRm 14
10.2.3 Strategies, tactics, policies, and constraints affecting ADRm 14
10.2.4 Organisations, activities, and interactions among participants and stakeholders in ADRm 15
10.2.5 Clear statement of responsibilities and authorities delegated for ADRm 16
10.2.6 Operational processes for the ADRm 16
10.2.7 Role of ADRm service provider 17
10.2.8 Role of ADRm user 17
10.3 Sequence of operations for ADRm 17
10.4 ADRm naming content and quality 18
10.5 Specific ADRm data naming content and quality 18
10.6 ADRm service elements 19
10.6.1 ADRm SE1: Establish jurisdiction regulations or system specification for ADR monitoring 19
10.6.2 ADRm SE2: Request system approval 19
10.6.3 ADRm SE3: User (operator) contracts with prime service provider 19

10.6.4 ADRm SE4: User (operator) equips vehicle with a means to provide consignment data.....19
10.6.5 ADRm SE5: User contracts with application service provider 19
10.6.6 ADRm SE6: application service provider uploads software into the TARV equipped vehicles of the operator 19
10.6.7 ADRm SE7: Recording of vehicle consignment data 20
10.6.8 ADRm SE8: ADRm Trigger 20
10.6.9 ADRm SE9: Contact predetermined IPv6 address 20
10.6.10 ADRm SE10: Obtain consignment data 21
10.6.11 ADRm SE11: 'Interrogated' request for ADR data.....21
10.6.12 ADRm SE12: Notification to *operator*.....21
10.7 ADRm access methods to provision and retrieve data 22
10.8 ADRm application service specific provisions for quality of service 27
10.9 ADRm application service specific provisions for test requirements 27
10.10 ADRm application specific rules for the approval of IVSs and 'Service Providers' 27

11 Declaration of patents and intellectual property 28

Annex A (informative) **Independent testing of the protocols defined in this part of ISO 15638 .....29**
A.1 Objectives.....29
A.2 TEST SCRIPT SERVICE: ADR Dangerous Goods 31
CTP 10.1.1 Instigated ADR - Dangerous Goods Monitoring using 2G.....36
CTP 10.1.2 Interrogated ADR - Dangerous goods monitoring using 2G 38
CTP 10.1.3 Interrogated ADR - Dangerous goods monitoring using 5.9GHz and responding using 2G or 3G 40
CTP 10.2.1 Instigated ADR - Dangerous goods monitoring using 3G 42
CTP 10.2.2 Interrogated at 5.9 GHz and send of ADR - Dangerous goods monitoring using 3G.....44
CTP 10.3.1 Instigated ADR - Dangerous goods monitoring using 802.11p (WAVE) 5.9 GHz 46
CTP 10.3.2 Interrogated ADR - Dangerous goods monitoring using 802.11p (WAVE) 5.9 GHz.....48
CTP 10.4.1 Instigated ADR - Dangerous goods monitoring using Mesh WiFi 50
CTP 10.4.2 Interrogated ADR - Dangerous goods monitoring using Mesh WiFi 52

Bibliography.....54

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. 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. 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.

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

ISO 15638 consists of the following parts, under the general title *Intelligent transport systems — Framework for collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV)*:

— *Part 1 Framework and architecture*

— *Part 2: Common platform parameters using CALM*

— *Part 3: Operating requirements, 'Approval Authority' procedures, and enforcement provisions for the providers of regulated services*

— *Part 5: Generic vehicle information*

— *Part 6: Regulated applications* [Technical Specification]

— *Part 7: Other applications*

— *Part 8: Vehicle access monitoring (VAM)* [Technical Specification]

— *Part 9: Remote electronic tachograph monitoring (RTM)* [Technical Specification]

— *Part 10: Emergency messaging system/eCall (EMS)* [Technical Specification]

— *Part 11: Driver work records (work and rest hours compliance) (DWR)* [Technical Specification]

— *Part 12: Vehicle mass monitoring (VMM)* [Technical Specification]

— *Part 14: Vehicle access control (VAC)* [Technical Specification]

— *Part 15: Vehicle location monitoring (VLM)* [Technical Specification]

— *Part 16: Vehicle speed monitoring (VSM)* [Technical Specification]

— *Part 17: Consignment and location monitoring (CLM)* [Technical Specification]

— *Part 18: ADR (Dangerous Goods) transport monitoring (ADR)* [Technical Specification]

— *Part 19: Vehicle parking facilities (VPF)* [Technical Specification]

— The following parts are under preparation:

— *Part 4: System security requirements* [Technical Specification]

— *Part 13: 'Mass' information for jurisdictional control and enforcement*

Introduction

Many ITS technologies have been embraced by commercial transport *operators (4.34)* and freight owners, in the areas of fleet management, safety and security. *Telematics (4.45)* applications have also been developed for governmental use. Such regulatory services in use or being considered vary from *jurisdiction (4.30)* to *jurisdiction*, but include electronic on-board recorders, digital *tachograph (4.44)*, on-board *mass (4.32)* monitoring, 'mass' data for regulatory control and management *(4.33), vehicle access (4.1) methods*, *hazardous goods (4.25)* tracking and e-call *(4.21)*. Additional applications with a regulatory impact being developed include fatigue management, speed monitoring and heavy vehicle penalties imposed based on location, distance and time.

In such an emerging environment of regulatory and *commercial applications (4.13)*, it is timely to consider an overall *architecture (4.9)* (business and functional) that could support these functions from a single platform within a commercial freight vehicle that operates within such regulations. International Standards will allow for a speedy development and *specification (4.43)* of new applications that build upon the functionality of a generic specification platform. A suite of standards is required to describe and define the *framework (4.24)* 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 (4.30)*.

This suite of standards addresses and defines the *framework (4.24)* for a range of cooperative *telematics (4.45)* ITS service *(4.27)* applications for *regulated commercial freight vehicles (4.38)* [such as access, driver fatigue management, speed monitoring, on-board *mass (4.32)* monitoring, *'mass' data for regulatory control and management (4.33)*]. The overall scope includes the concept of operation, legal and regulatory issues, and the generic cooperative provision of services to *regulated commercial freight vehicles (4.38)*, using an on-board ITS platform. The *framework* is based on a (multiple) *service provider (4.41)* oriented approach with provisions for the *approval (4.6)* and *auditing (4.10)* of *service providers*.

This suite of standards will:

- provide the basis for future development of cooperative *telematics (4.45)* applications for *regulated commercial freight vehicles (4.38)*. Many elements to accomplish this are already available. Existing relevant standards will be referenced, and the *specifications (4.43)* 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 (4.38);*
- a business *architecture (4.9)* based on a (multiple) *service provider (4.41)* oriented approach;
- address legal and regulatory aspects for the *approval (4.6)* and *auditing (4.10)* 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 (4.45)* 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 ISO 15638 provides *specifications (4.43)* for ADR (Dangerous goods).

NOTE 1 The definition of what comprises a 'regulated' vehicle is regarded as an issue for national decision, and may vary from *jurisdiction (4.30)* to *jurisdiction*. This suite of standards does not impose any requirements on nations in respect of how they define a *regulated vehicle (4.38)*.

NOTE 2 The definition of what comprises a 'regulated' service is regarded as an issue for national decision, and may vary from *jurisdiction (4.30)* to *jurisdiction*. This suite of standards does not impose any requirements on nations in respect of which services for *regulated vehicle*s *(4.38) 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 collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV) —

Part 18:
ADR (Dangerous Goods) transport monitoring (ADR)

1 Scope

This part of ISO 15638 addresses the provision of *'ADR (Dangerous goods)'* and specifies the form and content of such data required to support such systems, and *access methods (4.1)* to that data.

This part of ISO 15638 provides *specifications (4.43)* for common communications and data exchange aspects of the *application service (4.3) ADR* [dangerous goods *(4.17)*] that a *regulator (4.39)* may elect to require or support as an option, including:

a) high level definition of the service that a s*ervice provider (4.41)* has to provide (the service definition describes common service elements, but does not define the detail of how such an *application service (4.3)* is instantiated, nor the acceptable value ranges of the data concepts defined);

b) means to realise the service;

c) application data, naming content and quality that an *IVS (4.26)* has to deliver.

The definition of what comprises a 'regulated' service is regarded as an issue for national decision, and may vary from *jurisdiction (4.30)* to *jurisdiction*. This part of ISO 15638 does not impose any requirements on nations in respect of which services for *regulated vehicle*s *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.

ISO 15638 has been developed for use in the context of regulated commercial freight vehicles [hereinafter referred to as 'regulated vehicles' *(4.38)*]. 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 (4.3)* described in this part of ISO 15638 shall be within the regulations imposed by the *jurisdiction (4.30)* where they are instantiated. Conformance requirements to meet the provisions of this part of ISO 15638 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 A (Informative) 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 referenced 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 collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV) — Part 4: System security requirements*[1]

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

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

ISO/TS 15638-10 *Intelligent transport systems — Framework for collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV) — Part 10: Emergency messaging system/eCall (EMS)*

ISO/TS 15638-17 *Intelligent transport systems — Framework for collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV) — Part 17: Consignment and location monitoring (CLM)*

4 Terms and definitions

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

4.1
access methods
procedures and protocols for the provision and retrieval of data

4.2
app
small (usually) *Java™ (4.29)* applets, organized as software bundles, that support *application services (4.3)* by keeping the *data pantry (4.18)* provisioned with up-to-date data

4.3
application service
service provided by a *service provider (4.41)* enabled by accessing data from the *IVS (4.26)* of a *regulated vehicle (4.38)* via a wireless communications network

1 Under preparation.

4.4
application service provider
ASP
party that provides an *application service (4.3)*

4.5
app library
separately secure area of memory in *IVS (4.26)* where apps are stored [with different access controls to *data pantry (4.18)*]

4.6
approval
formal affirmation that an applicant has satisfied all the requirements for appointment as an *application service provider (4.4)* or that an application service delivers the required service levels

4.7
approval agreement
written agreement made between an *approval authority (regulatory) (4.8)* and a *service provider (4.41)*

NOTE An *approval authority (regulatory) (4.8)* approval agreement recognizes the fact that a *service provider (4.41),* 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 ongoing role of the *service provider.*

4.8
approval authority (regulatory)
organization (usually independent) which conducts *approval (4.6)* and ongoing *audit (4.10)* for *service providers (4.41)* on behalf of a *jurisdiction (4.30)*

4.9
architecture
formalized description of the design of the structure of *TARV* and its *framework (4.24)*

4.10
audit/auditing
review of a party's capacity to meet, or continue to meet, the initial and ongoing *approval agreements (4.7)* as a *service provider (4.41)*

4.11
basic vehicle data
data that shall be maintained/provided by all *IVS (4.26)* [regardless of *jurisdiction (4.30)*]

4.12
CALM communications access for land mobiles
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 (4.46)* 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 standardized media using *ITS-stations (4.28)* to provide wireless support for applications, such that the application is independent of any particular wireless medium

4.13
commercial application(s)
ITS applications in *regulated vehicles (4.38)* for commercial (non-regulated) purposes

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

4.14
consignment
shipment of goods/cargo to a destination

4.15
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 (4.28)* 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 (4.27)*

4.16
core data
basic vehicle data (4.11) plus any additional data required to provide an implemented *regulated application service (4.37)*

4.17
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

4.18
data pantry
secure area of memory in *IVS (4.26)* where data values are stored [with different access controls to *app library (4.5)*]

4.19
driver
person driving the *regulated vehicle* at any specific point in time

4.20
driver work records
DWR
collection, collation, and transfer of *driver (4.19)* work and rest hours data from an *in-vehicle system (4.26)* to an *application service provider (4.4)*

4.21
eCall
specialized instantiation of an *EMS (4.22)* that provides incident messaging and communication with a public service assistance point via priority wireless telephone communications using its emergency call capabilities

4.22
emergency message system
EMS
collection, collation, and transfer of emergency message data from an *in-vehicle system (4.26)* to an *application service provider (4.4)*

4.23
facilities
layer that sits on top of the communication stack and helps to provide data interoperability and reuse, and to manage applications and enable dynamic real time loading of new applications

4.24
framework
particular set of beliefs, ideas referred to in order to describe a scenario or solve a problem

4.25
hazardous goods
HAZMAT
see *dangerous goods (4.32)*/ *Accord européen relatif au transport international des marchandises Dangereuses par Route (ADR) (4.6)*

4.26
in-vehicle system
IVS
ITS-station (4.28) and connected equipment on board a vehicle

4.27
ITS service
communication functionality offered by an *ITS-station (4.28)* to an *ITS-station* application

4.28
ITS-station
ITS-s
entity in a communication network, comprised of application, *facilities (4.23)*, networking and access layer components specified in ISO 21217 that operate within a bounded secure management domain

4.29
Java™
object oriented open source operating language developed by SUN systems

4.30
jurisdiction
government, road or traffic authority which owns the r*egulatory applications (4.36)*

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

4.31
local data tree
LDT
frequently updated data concept stored in the on on-board *data pantry (4.18)* containing a collection of data values deemed essential for either a) *TARV regulated application service (4.37)*, or b) *cooperative intelligent transport systems (4.15)*

4.32
mass
mass of a given heavy vehicle as measured by equipment affixed to the *regulated vehicle (4.38)*

4.33
'mass' data for regulatory control and management
MRC
collection, collation, and transfer of vehicle *mass (4.32)* data from an *in-vehicle system (4.26)* to an *application service provider (4.4)* to enable data provision to *jurisdictions (4.30)* for the control and management of equipped vehicles based on the *mass* of the *regulated vehicle (4.38),* or use of such data to enable compliance with the provisions of regulations

4.34
operator
fleet manager of a *regulated vehicle*

4.35
prime service provider
service provider (4.41) who is the first contractor to provide *regulated application services (4.37)* to the *regulated vehicle (4.38),* or a nominated successor on termination of that initial contract

NOTE The *prime service provider (4.35)* is also responsible to maintain the installed *IVS (4.26)*; if the *IVS* was not installed during the manufacture of the vehicle, the *prime service provider (4.35)* is also responsible for installing and commissioning the *IVS (4.26).*

4.36
regulated/regulatory application
application arrangement using TARV utilized by *jurisdictions (4.30)* 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*

NOTE This may be mandatory or voluntary at the discretion of the *jurisdiction.*

4.37
regulated application service
TARV application service to meet the requirements of a regulated application that is mandated by a regulation imposed by a *jurisdiction (4.30),* or is an option supported by a *jurisdiction*

4.38
regulated commercial freight vehicle/regulated vehicle
vehicle that is subject to regulations determined by the *jurisdiction (4.30)* 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

NOTE At the option of *jurisdictions*; this may require the provision of information via *TARV* or provide the option to do so.

4.39
regulator
agent of the *jurisdiction (4.30)* appointed to regulate and manage *TARV* within the domain of the *jurisdiction*

NOTE This may or may not be the approval authority (regulatory) (4.8).

4.40
remote tachograph monitoring
RTM
collection, collation, and transfer of data from an on-board electronic *tachograph (4.44)* system to an *application service provider (4.4)*

4.41
service provider
party which is approved by a approval *authority (regulatory) (4.8)* as suitable to provide regulated or commercial ITS *application services (4.3)*

4.42
session
wireless communication exchange between the *ITS-station (4.28)* of an *IVS (4.26)* and the *ITS-station* of its *application service provider (4.4)* to achieve data update, data provision, upload apps, or otherwise manage the provision of the *application service (4.3),* or a wireless communication provision of data to the *ITS-station* of an *IVS (4.26)* from any other *ITS-station*

4.43
specification
explicit and detailed description of the nature and functional requirements and minimum performance of equipment, service or a combination of both

4.44
tachograph
sender unit mounted to a vehicle gearbox, a tachograph head and a digital driver card, which records the *regulated vehicle (4.38)* speed and the times at which it was driven and aspects of the *driver's (4.19)* activity selected from a choice of modes

4.45
telematics
use of wireless media to obtain and transmit (data) from a distant source

4.46
user
individual or party that enrols in and operates within a regulated or *commercial application (4.13) service (4.3)*

EXAMPLE *Driver (4.19),* transport *operator (4.34),* freight owner, etc.

4.47
vehicle access control
VAC
control of *regulated vehicle*s ingress to and egress from controlled areas and associated penalties and levies

4.48
vehicle access management
VAM
monitoring and management of *regulated vehicle*s approaching or within sensitive and controlled areas

4.49
vehicle location monitoring
VLM
collection, collation, and transfer of vehicle location data from an *in-vehicle system (4.26)* to an *application service provider (4.4)*

4.50
vehicle mass monitoring
VMM
collection, collation, and transfer of vehicle *mass (4.32)* data from an *in-vehicle system (4.26)* to an *application service provider (4.4)*

4.51
vehicle parking facility
VPF
system for booking and *access (4.1)* to and egress from a *vehicle parking facility (VPF) (4.51)*

4.52
vehicle speed monitoring
VSM
collection, collation, and transfer of vehicle speed data from an *in-vehicle system (4.26)* to an *application service provider (4.4)*

5 Symbols and abbreviated terms

ADR
Accord européen relatif au transport international des marchandises Dangereuses par Route (4.6) (*dangerous goods (4.17)*)

ADRm
ADR monitoring

app
applet (JAVA™ application or similar) *(4.2)*

ASP
application service provider (4.4)

CALM
communications access for land mobiles (4.12)

C-ITS
cooperative intelligent transport systems *(4.15)*

DLR
driving licence reader

DRD
driver records device

EMS
emergency message system *(4.22)*

ID
identity

IP
internet protocol

ITS-S
ITS station *(4.28)*

IVS
In-vehicle system *(4.26)*

LDT
local data tree *(4.31)*

MSD
minimum set of data
[*eCall* *(4.21)* . EN 15722]

OID
object identifier

PSAP
public service answering point

SAD
single administrative document (which accompanies ADR consignments in Europe)

SE
service element

TARV
telematics *(4.45)* applications for *regulated vehicles* *(4.38)*

UML
Unified Modeling Language *(4.77)* (ISO 19501)

UNECE
United Nations Economic Commission for Europe

URL
uniform resource locator

UTC
coordinated universal time

6 General overview and framework requirements

ISO TS 15638-1 provided a *framework (4.24)* and *architecture (4.9)* for *TARV*. It provided a general description of the roles of the actors in *TARV* and their relationships.

To understand clearly the *TARV* framework, *architecture (4.9)* and detail and *specification (4.43)* of the roles of the actors involved, the reader is referred to ISO TS 15638-1.

ISO TS 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 TS 15638-6.

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

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

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

In order to be compliant with this part of ISO 15638, the security employed shall comply to ISO 15638-4[2].

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

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

ISO 15638 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 (4.37)* 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 (4.30)* as part of its *specification (4.43)* for any particular *regulated application service (4.37).* However, where a specified *regulated application service (4.37)* has specific Q of S requirements essential to maintain interoperability, these aspects shall be as specified in Clause 10.

2 Under preparation.

8.3 Test requirements

This part of ISO 15638 contains no general requirements concerning test requirements. Such aspects shall be determined by a *jurisdiction (4.30)* as part of its *specification (4.43)* for any particular *regulated application service (4.37),* and issued as a formal test requirements *specification* document. However, where a specified *regulated application service (4.37)* 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 document referenced within that Clause. And where multiple *jurisdictions* recognise a benefit to common test procedures for a specific *regulated application service,* this shall be the subject of a separate standards document.

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 the ISO 15638 family of Standards, the contracting parties shall make such risk explicitly known to the implementing *jurisdiction (4.30)* 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 (4.37)* are as designed by the application service system to meet the requirements of a particular *jurisdiction (4.30)* 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 is provisioned into the *data pantry (4.18)*, and the means to obtain the *TARV LDT (4.31)* and *core data (4.16)* are described in Clause 8 of ISO 15638-6.

In order to minimise demand on the *IVS (4.26)* (which it is assumed will be performing multiple *application services (4.3)* simultaneously, as well as supporting general safety related cooperative ITS systems), and because national requirements and system offerings will differ, a ‘cloud’ approach has been taken in defining *TARV regulated application services (4.37)*.

The *TARV* approach is for the on-board *app (4.2)* 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 (4.4) (ASP),* 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 Clause 9 of ISO 15638-6.

At a conceptual level, The *TARV* system is therefore essentially simple, as shown in Figure 1. The process is similar to that for CoreData, but data is supplied to a different on-board file in the *data pantry (4.18)*.

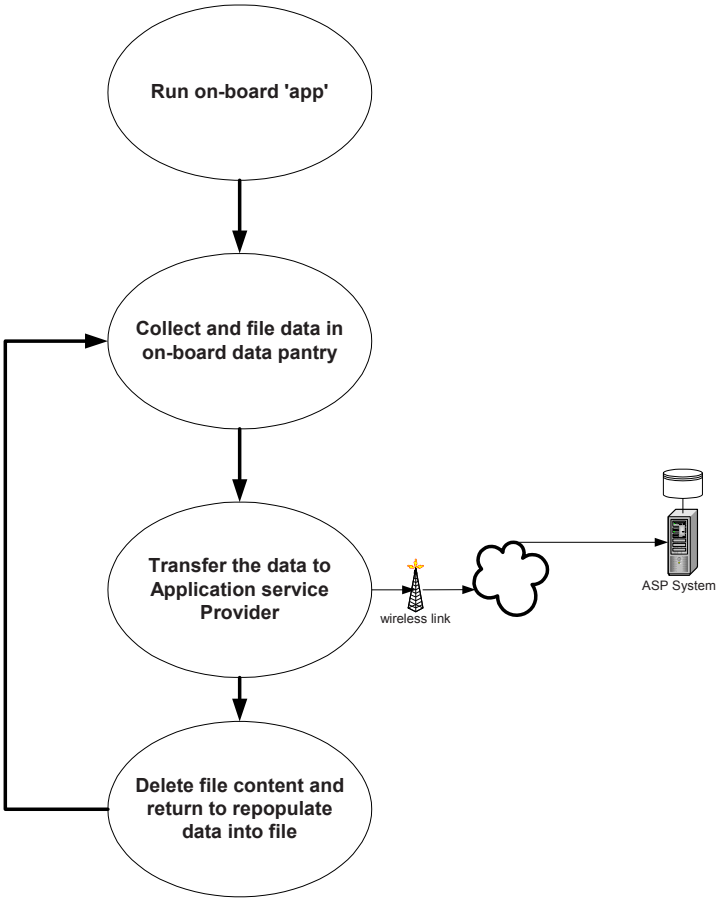

Figure 1 — TARV Regulated application service on-board procedure

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 (4.3)* shall be as defined in ISO 15638-6.

9.6 Information security

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

9.7 Data naming content and quality

Data naming and quality shall be as defined in ISO 15638-6

Variations specific to the ADR (Dangerous goods) *application service (4.3)* shall be as defined below.

9.8 Software engineering quality systems

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

9.9 Quality monitoring station

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

9.10 Audits

Audits shall be as defined in ISO 15638-6.

9.11 Data access control policy

To protect the data and information held by the *application service provider (4.4),* each provider shall adopt a risk based data access control policy for employees of the provider.

9.12 Approval of IVSs and service providers

Generic provisions for the *approval (4.6)* of *IVSs* and *service providers (4.41)* shall be as specified in ISO 15638-3 (*TARV* –Operating requirements, approval procedures, and enforcement provisions for the providers of regulated services). Detailed provisions for specific *regulated applications (4.36)* shall be as specified by the regime of the *jurisdiction (4.30).*

10 TARV ADR consignment monitoring (*ADR*m)

10.1 ADRm service description and scope

NOTE 1 The content of this section, while remaining under ISO TC204 control, is being shared with *UNECE* JWG RID for improvement and harmonisation. We are scheduled to meet with *UNECE* JWG RID regularly, hopefully to develop a full IS Standard. Either the data concepts defined in such a future International Standard, or a revision to this TS will align itself to planned changes to the MSD and HGV eCall optional additional data planned for the near future.

NOTE 2 *ADR* is a requirement in Europe and other countries, it is not a global requirement, other clauses, or Parts of ISO 15638 for similar measures will be constructed, if ISO 15638-10 (TARV Emergency message service/eCall) or ISO 15638-17 (TARV Consignment location monitoring) are unable to accommodate them within the existing *specifications (4.43)*. This part of ISO 15638 (Part 18) is specified separately because it makes specific reference to very specific provisions for *ADR* required in nearly 50 countries and UN ECE has requested that, in addition to emergency messaging, we make, if possible, provision for their non-emergency requirements to be accommodated within *TARV*.

10.1.1 ADRm use case

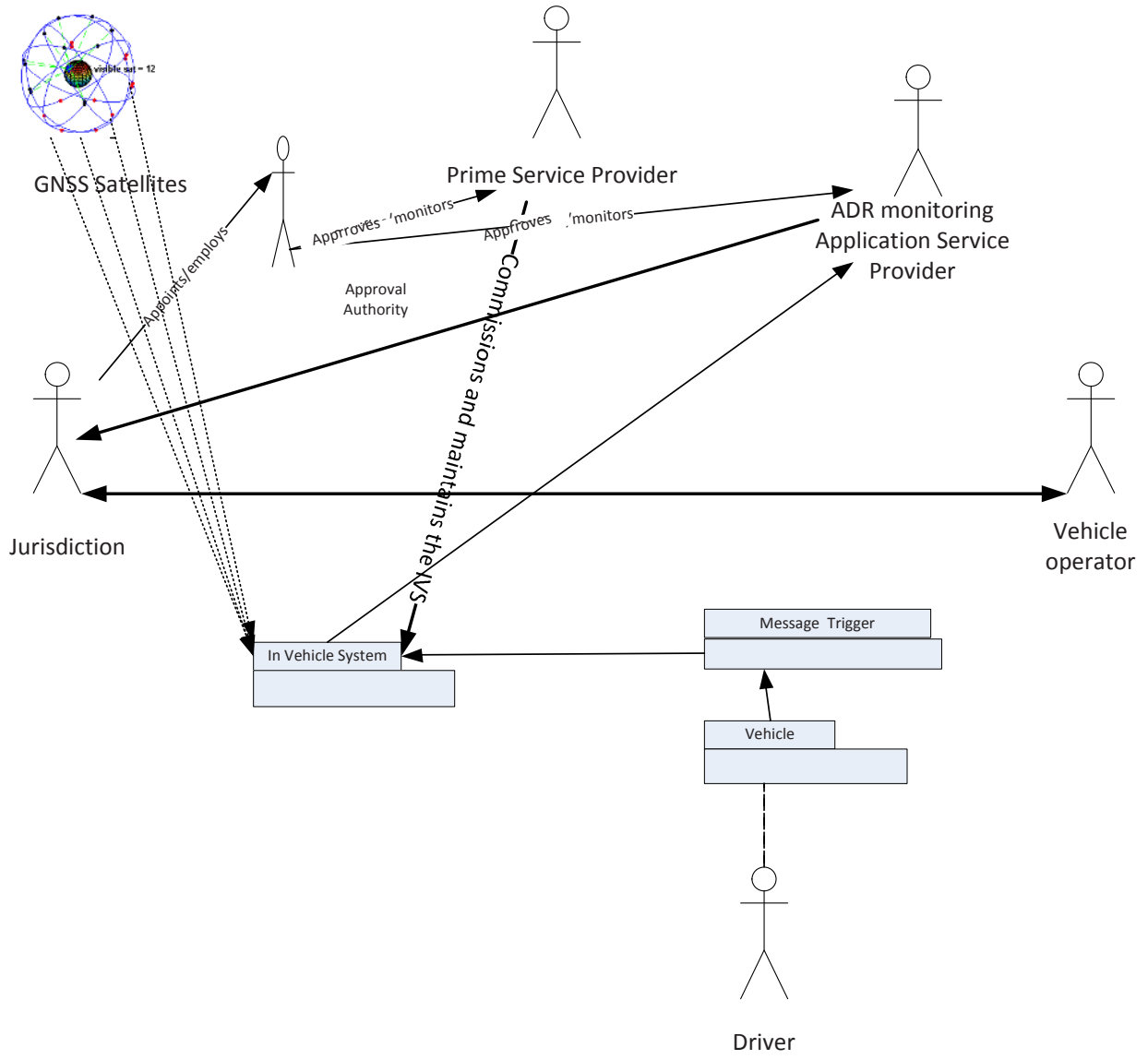

Figure 2 — ADRm use case

10.1.2 Description of ADRm regulated application service

This application service uses the wireless link between the on-board *ITS-station (4.28)* (in-vehicle platform) and an *application service provider (4.4),* in order to convey an *ADR* (*Accord européen relatif au transport international des marchandises Dangereuses par Route*) *(4.6)*, otherwise known as '*dangerous goods (4.17)* or '*HAZMAT (4.25)*') *consignment (4.14),* data from the *regulated vehicle (4.38)* to an *ADR*m *application service provider.* See Figure 2.

This use case covers data to be sent in the normal course of business where *ADR (4.6)* consignment monitoring is required. In respect of *ADR* emergency messages, refer to ISO 15638-10 (TARV Emergency message system/eCall).

The content of any message shall adhere to the requirements of the regulations in force in that *jurisdiction (4.30),* or shall follow the data content defined herein.

10.2 Concept of operations for ADRm

10.2.1 General

ADR consignments (4.14) are the subject of special regulation. In most *jurisdictions (4.30)*, significant paperwork is processed through the administration system, and has to accompany the *regulated vehicle (4.38)* throughout its journey.

As a step towards paperless management it is the goal of *UNECE* JWG RID to encourage and define means of paperless access to data required in the management of ADR cargos. For information required to be supplied to *PSAP*s/emergency responders in response to an incident, see ISO 15638-10 (TARV Emergency message system/eCall).

The majority of access to information is required as part of routine (non-emergency) situations. This Part of ISO 15638 specifies how this information can be provided using *TARV*.

10.2.2 Statement of the goals and objectives of ADRm

The objective of the system is to provide legitimate interested parties with key information concerning the *regulated vehicle (4.38)* and its *consignment (4.14)*, to support *ADR* regulations together with other key data, as implemented by *jurisdictions (4.30)*.

NOTE *UNECE* JWG RID are currently reviewing their reference pointers to *ADR* information, and this Part of ISO 15638 and its table(s) will be revised if material change is made.

10.2.3 Strategies, tactics, policies, and constraints affecting ADRm

The points of demand for *ADR*m data will vary from *jurisdiction (4.30)* to *jurisdiction,* so the nexus of this service is the provision of data from the *regulated vehicle (4.38)* to a landside *application service provider (4.4)* who will know who provide it to, when, and in what format. Those conditions and requirements are not specified in this part of ISO 15638, but left to *jurisdictions* to determine and regulate at their discretion, or *UNECE* or other *regulator (4.39)* to determine and regulate.

The architectural concept is the provision of *ADR*m data to legitimate enquirers, via an *application service provider (4.4).* The *IVS (4.26)* shall provide the data that its on-board *ADR*m *app (4.2)* requires, sending that data to the predetermined IPv6 address of the *application service provider,* via the *ITS-station (4.28)* of the *IVS*.

The required data may be entirely collated and stored on-board the *regulated vehicle (4.38)*, or may be a combination of information provisioned on-board the *regulated vehicle* together with information held in the database of the *application service provider (4.4)* (for example the *TARV LDT (4.31)* data from the *regulated vehicle* and the consignment Note/SAD/Customs data from the *application service provider* database). Apart from the *TARV LDT*, a service provider may provide all of the current trip *consignment (4.14)* data from its own database, or a pointer to a database where it may be obtained (for example one maintained by the *operator (4.34)*), or may store some or all of the current *consignment (4.14)* data in the *IVS (4.26)* of the *regulated vehicle (4.38)* and contribute the shortfall from its central database or provide a pointer to a database where it may be obtained (for example one maintained by the *operator (4.34)*) obtained from the *regulated vehicle (4.38) IVS*.

Architecturally, consistent with other *TARV* applications, for reasons of security, a direct and targeted enquiry for data from a particular vehicle shall be acknowledged, the communication *session (4.42)* closed, and a new communication *session (4.42)* opened to a predetermined IPv6 address stored in the *data pantry (4.18)* or *app library (4.5)* of the *IVS (4.26)*, and the data sent to that address.

A legitimate enquirer (for example the enforcement office of a *jurisdiction (4.30),* insurer, police department, customs etc.), may request *ADR* data by one or more of several options

a) By direct enquiry to the originator of a consignment note or SAD
b) By broadcast to vehicles entering its territory or a specific location point in that territory
c) By direct enquiry to a passing vehicle
d) By a pre-programmed instruction

In the case of

(a) By direct enquiry to the originator of a consignment note or SAD

The *application service provider (4.4),* on receiving the request, shall, using a communication *session (4.42)* between its *ITS-station (4.28)* and the *ITS-station* on-board the *regulated vehicle (4.38)* *IVS (4.26)*, request an update of any predetermined data held in the *data pantry (4.18)* of the *regulated vehicle*, and current vehicle status as determined by the enquiry to the *regulated vehicle*. The *regulated vehicle* shall respond by passing its data to the *application service provider* together with a requested final destination address(es) for the data. It is the responsibility of the *application service provider* to ascertain that the final destination address is genuine, and the means by which they do this are not specified in this part of ISO 15638.

(b) By broadcast to vehicles entering its territory or a specific location point in that territory

The *ITS-station (4.28)* on board the *regulated vehicle (4.38)* *IVS (4.26)*, on receiving the broadcast request, shall process an update of any predetermined data held in the *data pantry (4.18)* of the *regulated vehicle*, and current vehicle status as determined by the enquiry to the *regulated vehicle*. The *regulated vehicle (4.38)* *IVS* shall respond by passing its data to its *application service provider (4.4)* together with the requested final destination address(es) for the data. It is the responsibility of the *application service provider* to ascertain that the final destination address is genuine, and the means by which they do this are not specified in this part of ISO 15638.

(c) By direct enquiry to a passing vehicle or *ITS-station (4.28)*

The *ITS-station (4.28)* on board the *regulated vehicle (4.38)* *IVS (4.26)*, on receiving the direct request from an apparently genuine *ITS-station* (usually infrastructure based *ITS-station*, or a portable *ITS-station* in the hands of an authorised officer of the *jurisdiction (4.30)*), shall process an update of any predetermined data held in the *data pantry (4.18)* of the *regulated vehicle*, and current vehicle status as determined by the enquiry to the *regulated vehicle*. The *regulated vehicle IVS* shall respond by passing its data to its *application service provider (4.4)* together with the requested final destination address(es) for the data. It is the responsibility of the *application service provider* to ascertain that the final destination address is genuine, and the means by which they do this are not specified in this part of ISO 15638. The form of direct interrogation request for ADR data is defined in ISO 15638-6 Clause 7 as ‘GETADR’. See ISO 15638-6 for detail.

(d) By pre-programmed instruction

The *ITS-station (4.28)* on board the *regulated vehicle (4.38)* (*IVS (4.26)*), as a result of an instruction within the *ADR*m *app (4.2)* in the on-board applications library, or triggered by some event such as timing, or an alarm, shall process an update of any predetermined data held in the *data pantry (4.18)* of the *regulated vehicle (4.38x.*The *regulated vehicle (4.38)* shall respond by passing its data to its *application service provider (4.4)*. It is the responsibility of the *application service provider* to ascertain the appropriate final destination address, and the means by which they do this are not specified in this part of ISO 15638.

10.2.4 Organisations, activities, and interactions among participants and stakeholders in ADRm

The interrogator shall be an *app (4.2)* in the library of the *IVS (4.26)*, or the receipt of a message from an *ITS-station (4.28)* within communications range (for example a roadside *ITS-station*) or any interrogator deemed appropriate by the contract between the *user (4.46)* and the *application service provider (4.4).*

The *prime service provider (4.35)* is the actor who is responsible to install and maintain the *ADR consignment (4.14)* data monitoring equipment and its triggering mechanism in the *regulated vehicle (4.38)*.

The *application service provider (4.4)* is the party who contracts with the *user (4.46)* to provide the *ADR*m service.

The *user (4.46)* is the *regulated vehicle (4.38)* *operator (4.34)* and his *driver (4.19).*

10.2.5 Clear statement of responsibilities and authorities delegated for ADRm

Table 1 — TARV: ADRm actors involved, their activities and interactions

ACTOR	ROLE	ACTIVITIES	INTERACTIONS
***UNECE* JWG RID**	*ADR* Regulator	Provides international regulations and *ADR* Tables	(J) Provides international requirements (Op) Provides international requirements
***Jurisdiction* (J)** *(4.30)*	Sets requirements for mandatory and supported *ADR*m	Publishes *specifications (4.43)*	ALL
		Obtains regulations	ALL: Establish regime and regulations *ASP* Register
		Appoints *Approval Authority* where appropriate	CA: Contract. Instruct . Receive reports
***Approval authority* (CA)** (4.8)	Implements *jurisdiction* policy at equipment and service approval level	Approves *IVS (4.26)*, *Application Service* (4.3) instantiations	PSP: Approve *IVS* *ASP* : Approve *Application Service*
		Conducts Q of S maintenance to instruction of *jurisdiction*	
***Prime service provider* (PSP)** *(4.35)*	Responsibility for *IVS*	Installs and/or commissions *IVS*	CA: May Apply to approve *IVS* Op; Installation
		Maintains *IVS*	Op: Maintain *IVS*
***Application service provider* (*ASP*)** *(4.4)*	Provides *ADR*m *application service*	Develops instantiation of *ADR*m *application service*	CA : Applies for approval of Service
		Contracts with *users (4.46)*	Op: Contracts
		Provides *ADR*m *application service* to *users (4.46)* and *jurisdiction*	Op: Provides service IVS: Loads data IVS: Receives *ADR*m Messages
***operator* (Op)** *(4.34)*	Provides *regulated vehicle (4.38)*	'Employs'/contracts *drivers*	Dr: Employs/Contracts
	Uses *regulated vehicle* for commerce and logistics	Operates *regulated vehicle*	PSP: Contracts,receives service *ASP* :Contracts, receives service *ASP* : Provides consignment data
***Driver* (Dr)** *(4.19)*	Drives *regulated vehicle* to instruction of *operator (4.34)*	Drives *regulated vehicle*	Op: to instructions

The *prime service provider (4.35)* is responsible to properly install and maintain the equipment which triggers the *application service (4.3)*.

The *regulated vehicle (4.38)* *operator (4.34)* (or owner) commissions the service and contracts with the *application service provider (4.4),* and possibly the *prime service provider (4.35)* (although that may be a subcontract of the application service contract with the *application service provider)*.

10.2.6 Operational processes for the ADRm

An 'App' on-board the *regulated vehicle (4.38)*, or one of the legitimate enquirers defined in 10.2.3, generates a trigger for the supply of *ADR*m information via the *IVS (4.26)* *ITS-station (4.28)*.

The *in-vehicle system (4.26)* uses its *ITS-station (4.28)* to send the *ADR*m message and such of its associated data maintained on-board to a predetermined IPv6 address provided by the *application service provider (4.4),* together with the requested final destination address proved by the enquirer.

The *application service provider (4.4)* validates the requested final destination address, and if valid, completes the instantiation of the data concept from its own database and then provides the *ADR*m data to the legitimate enquirer.

10.2.7 Role of ADRm service provider

The *prime service provider (4.35)* installs and maintains the *ADR*m *consignment (4.14)* data system and its triggering mechanism in the *regulated vehicle (4.38)*.

The *application service provider (4.4)* contracts with the *user (4.46)* to provide the *ADR*m *application service (4.3)*.

10.2.8 Role of ADRm user

The *user (4.46)* (*operator (4.34)* + *driver (4.19)*) are contracting parties to the service, either by choice or regulation.

The *operator (4.34)* contracts with the *application service provider (4.4)* to provide the service and pays any appropriate fees to the *application service provider.*

The *application service provider (4.4)* may maintain a website (IPv6 address) where data relating to the *consignment (4.14)* is made available.

The *user (4.46)* (*operator (4.34)*) may maintain a website (IPv6 address) where data relating to the *consignment (4.14)* is made available.

The *user (4.46)* (*operator (4.34)*) may maintain a telephone hotline where data relating to the *consignment (4.14)* is made available.

10.3 Sequence of operations for ADRm

The sequence of operations in respect of general *ADR*m shall be as shown in Figure 3.

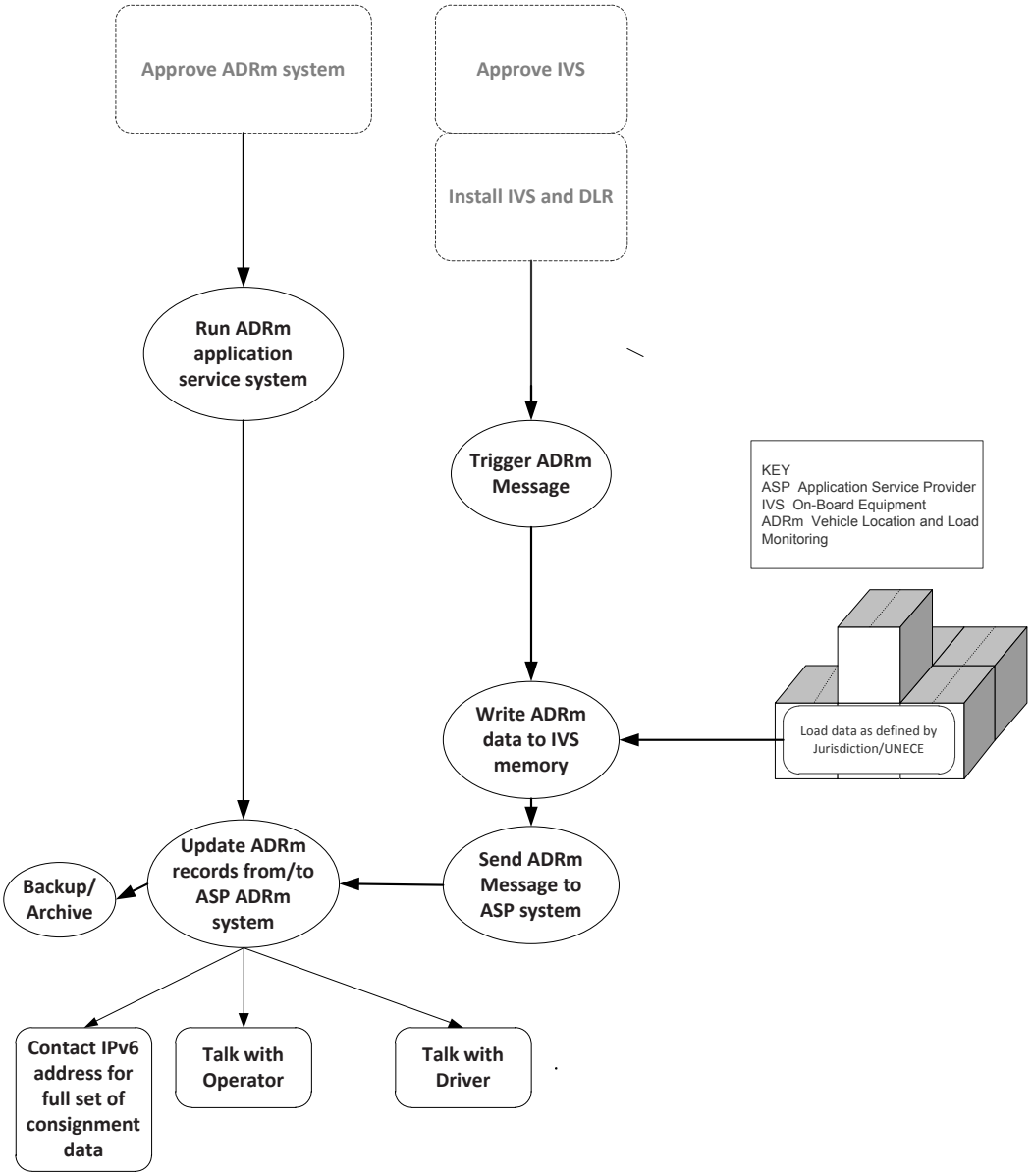

Figure 3 — Sequence of operations for ADRm

10.4 ADRm naming content and quality

The process to obtain *basic vehicle data (4.11)* (*TARV LDT (4.31)*) data content shall be as defined in 8.3 of ISO 15638-6 and ISO 15638-5.

10.5 Specific ADRm data naming content and quality

ADR consignment (4.14) data shall be determined as required by regulations of the *jurisdiction (4.30)* or *UNECE* JWG RID. The format and content shall be as defined in the regulations pertaining, or the subject of a written agreement between the parties. However, for consistency, interpretation and data reuse, wherever the following data concept elements are used they shall be represented as defined in Clause 10.9, Table 2.

10.6 ADRm service elements

The service elements for *ADR* monitoring shall be as defined in the following subClauses:

10.6.1 ADRm SE1: Establish jurisdiction regulations or system specification for ADR monitoring

The *jurisdiction (4.30)* shall be responsible to define its requirements for its variant of the *ADR*m *application service (4.3),* obtain any legislation and/or regulations, and define the procedure for an *application service provider (4.4)* to gain approval for its instantiation of the *ADR*m *application service.*

10.6.2 ADRm SE2: Request system approval

The *application service provider (4.4)* shall seek approval for its instantiation of the *ADR*m application service *(4.3)* from the *approval authority (regulatory) (4.8)* in accordance with the regime established by the *jurisdiction (4.30)*.

10.6.3 ADRm SE3: User (operator) contracts with prime service provider

It is a prerequisite for any potential vehicle *operator (4.34)* opting or being required to sign up for the *ADR*m application service that its *regulated vehicles (4.38)* are *TARV* equipped with a *TARV* compliant *IVS (4.26)* at point of manufacture or installed by a *prime service provider (4.35)*, and that there is a maintenance contract with a *prime service provider* for that equipment. (See ISO 15638-1 *TARV* framework and architecture).

10.6.4 ADRm SE4: User (operator) equips vehicle with a means to provide consignment data

10.6.4.1 It is a prerequisite for any potential vehicle *operator (4.34)* opting or being required to sign up for the *ADR*m application service that its *regulated vehicles (4.38)* are equipped to provide the *consignment (4.14)* data required. If the data is provided via an IPv6 link to a website, no further data is required, but may optionally be provided as backup.

10.6.4.2 If the *jurisdiction (4.30)* or *UNECE* has specified the required data it shall be provided to the requirement of the *jurisdiction* or *UNECE* as appropriate, or otherwise as agreed between the *operator* and the *ADR*m *application service provider (4.4),* who may choose to maintain some or all of the information in its application service *(4.3)* system (rather than on-board the *regulated vehicle*).

10.6.4.3 The *ADR*m data concept elements agreed with *UNECE* ***(*in process***) are provided in Table 2 below.

10.6.4.4 It is further required that there is a maintenance contract with an approved *service provider (4.41)* for any equipment required to be installed in the *regulated vehicle*. That *service provider* shall be, or shall be considered as an agent of, the *prime service provider (4.35)* in respect of the provisions of this part of ISO 15638.

10.6.5 ADRm SE5: User contracts with application service provider

The *user (4.46)* (*operator (4.34)*) shall contract with an *application service provider (4.4)* who offers an approved *ADR*m application service to provide the *ADR*m application service to nominated vehicles.

10.6.6 ADRm SE6: application service provider uploads software into the TARV equipped vehicles of the operator

The service provider shall upload and commission the on-board *ADR*m *app (4.2)* software into the *TARV* equipped *regulated vehicles* (4.38) of the *operator (4.34)*.

10.6.7 ADRm SE7: Recording of vehicle consignment data

The on-board *ADR*m *app (4.2)* shall create a file, type :*ADR* [*ADR* file] within this *specification (4.43)*), named

<*ADR*><YYMMDDhhmm><vehicle registration number>

Prior to the commencement of each journey, the *application service provider (4.4)* shall establish a communications *session (4.42)* with the *in-vehicle system (4.26)* and update the data content of the *ADR* file with one of the following options (in order of precedence):

a) current consignment data (or url link address to that data*)* as required by the *jurisdiction (4.30),*
b) current consignment (or url link address to that data*)* as required by *UNECE*,
c) current consignment data (or url link address to that data) as required by the contract between the *application service provider (4.4)* and the *user (4.46)*
d) a combination of the *TARV LDT (4.31)* data and the consignment data determined in Table 2 below (as far as it is available, with padded null fields where a data concept element data is not available or not required)

At the start of each journey the *ADR*m *app (4.2)* held in the library of the *IVS (4.26)* shall be initiated.

During the journey the on-board *ADR*m *app (4.2)* in the in the *IVS (4.26)* shall update the *ADR*m file with the following data

<IVS ID>,
<VehicleLocation>,<ConsignmentData>
<IVS ID>
<end>

NOTE ISO 15638-5 Clause 9.2.4 definition of location includes location, *UTC* time and direction of travel

Vehicle direction of travel shall be calculated as specified in ISO 15638-5 Clause 8.3.12

10.6.8 ADRm SE8: ADRm Trigger

The points of demand for *ADR*m data will vary from *jurisdiction (4.30)* to *jurisdiction,* or requirements of *UNECE* regulation, or requirements of the contract between the *operator (4.34)* and the *application service provider (4.4).* Those conditions and requirements are not specified in this part of ISO 15638.,but left to *jurisdictions* to determine and regulate at their discretion, or *UNECE* or other *regulator (4.39)* to determine and regulate. The generation of and submission to the *application service provider* of *ADR*m data may be as a result of an instruction within the *ADR*m *app (4.2)* in the on-board applications library, or may be triggered by some event such as timing, an alarm, or by interrogation (e.g. spot check) from another *ITS-station (4.28)*.

In the event that, from whatever cause, during the journey, an *ADR*m *consignment (4.14)* data request is received, the following SEs shall ensue.

10.6.9 ADRm SE9: Contact predetermined IPv6 address

The *IVS (4.26)* shall then use the on-board *ITS-station (4.28)* to contact an *ITS-station* of the *application service provider (4.4)* to deliver the *ADR*m *consignment (4.14)* data, together with the enquirer's identification and requested destination, to the predetermined IPv6 address.

NOTE In the *TARV* system, for security reasons, to prevent spoofing, phishing and other illegitimate demands for data, data is never provided directly to an enquirer/interrogator, but is always sent to a predetermined IPv6 address of the *application service provider (4.4),* who is then responsible to ascertain that it is a legitimate enquirer, and then takes responsibility to get the data promptly to the legitimate enquirer. As the identification of legitimate enquirers and their destination IPv6 address is normally known in advance (in this use case it is likely to be police, customs, agent of *jurisdiction (4.30),* haulier, depot, consignment agent, emergency service responder, etc.), this process will usually be automatic/semi-automatic against maintained check lists, and will normally add only a few seconds to the time when the legitimate enquirer receives the requested data

The *IVS (4.26)* shall also write a log of the event and associated data into the memory of the *IVS* as a record of the request.

10.6.10 ADRm SE10: Obtain consignment data

The *application service provider (4.4)* shall then contact the predetermined IPv6 address to obtain full detail of the *consignment (4.14)* and any associated *ADR* data where appropriate.

10.6.11 ADRm SE11: 'Interrogated' request for ADR data

10.6.11.1 An interrogating ITS-station shall request ADR specific data as determined in ISO15638-6 clauses 7.1 and 8.1.2.

10.6.11.2 In the event that the IVS of a vehicle receives a wireless interrogation requesting the ADR data, 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.

10.6.11.3 On receipt of the request the IVS shall acknowledge the request with the appropriate ACKnowledgement defined in 8.3.5 of ISO15638-6, <Y>, which acknowledges that a request for ADR data has been received.

10.6.11.4 The IVS shall then close the communication session.

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

10.6.11.6 The IVS shall then send the ADR datafile (as defined in 10.9) 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.

10.6.11.7 On successful receipt of the data, the recipient at the predetermined destination IPv6 address shall send an acknowledgement <ADX> to the IVS.

10.6.11.8 On receipt of the acknowledgement <ADX> the IVS shall close its communication session.

10.6.11.9 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.

The *application service provider (4.4),* having ascertained the validity of the enquirer (this process will usually be automatic/semi-automatic against maintained check lists), shall then contact the enquirer in the agreed format (usually an IPv6 address or email address) as provided by the enquirer, providing the *ADR*m data to the enquirer. The means by which this is achieved is a matter for agreement between the parties and is outwith the scope of this part of ISO 15638.

The *ADR*m system of the *application service provider (4.4)* shall also write a log of the event and associated data into the memory of the backup/archive of the *application service provider* as a record of the incident for audit trail purposes.

10.6.12 ADRm SE12: Notification to *operator*

The *application service provider (4.4)* shall then contact the *operator (4.34)* to notify them of the enquiry, providing the *ADR*m data supplied, and enquirers address details to the *operator*.

10.7 ADRm access methods to provision and retrieve data

The process to obtain *basic vehicle data (4.11)* (*TARV LDT (4.31)*) data content shall be as defined in 8.3 of ISO 15638-6 and ISO 15638-5.

The electronic records declared and stored by the *IVS (4.26)* shall be authenticated, have integrity and be secure from interception or corruption, in accordance with ISO 15638-4.

Consignment (4.14) data shall be provided before the journey commences to the *application service provider (4.4),* normally by electronic means, and the *application service provider* shall be responsible to provision any data required into the *data pantry (4.18)* of the *in-vehicle system (4.26)* via the *ITS-station (4.28)* of the *IVS (4.26)*.

The format and content shall be the subject of a written agreement between the parties. However, for consistency, interpretation and data reuse, wherever the following data concept elements are used they shall be represented as defined in Table 2.

NOTE: *UNECE* JWG RID are currently reviewing their reference pointers to *ADR* information, and this table will be revised if material change is made.

Table 2 — ADRm consignment data

FILE TYPE		**Format of file name**	**Notes/Source**
CLM	**Mandatory**	<*CLM*><YYMMDD><hhmmss><vehicle registration number> Example *CLM* 110316 070603 KV76WRR As: *CLM*110316 070603KV76WRR	Clause 19.4.7 (Vehicle/Location/Consignment monitoring file [*CLM* file])

Number	**Data concept name**	**Use**	**Format**	**Notes/Source**
*ADR*m-0000	IVS ID	Mandatory	AN (9)	IVS identifier as defined in ISO 15638-5
***ADR*m Data Concept element reference**	**Name**	**Type**	**Unit**	**Description**
*ADR*m-0001	*OID*	Integer	1 byte	*ADR*m data concept identifier binary value 1000010 identifying *ADR*m Schema A (until allocated a revised *OID* from a central register)
*ADR*m-0002	ID	Integer	1 byte	*ADR*m Schema A data concept format version set to 1 to discriminate from later *ADR*m Schema A data concept formats Later versions to be backwards compatible with existing versions. Systems receiving an *ADR*m Schema A data concept to support all standardised *ADR*m Schema A data concept versions, which are each uniquely identified using an *ADR*m

				Schema A data concept format version parameter which will always be contained in the first byte of all [current and future] *ADR*m Schema A Data concept versions.
*ADR*m-0003	Tanker or other vehicle type plus number of dangerous goods on-board	Octet string (1 Byte) Binary	00000000-11111111	The first binary position of the octet to indicate whether the affected vehicle is a tanker or other type of vehicle where 1nnnnnnn = Tanker 0nnnnnnn = Other type of vehicle The remaining 7 binary positions of the octet to identify the number of types of dangerous goods being carried Seven binary bits. x0000000 = no *ADR* goods on board x1111111= mixed load (unspecified number of types of dangerous goods present on-board, but number unknown) x1111110= more than 120 types of *ADR* goods on-board x0000001 – x1111100 = 1 – 124 decimal expressed as binary range: 0 0000000- 1 111111 Concatenated as octet within range : 00000000 – 11111111
*ADR*m-0004	*ADR* Consignment reference	Binary 3 Octets	000000000000000000000000 - 111111111111111111111111	Consignors unique reference number expressed as a binary value between 0 – 16,777,215
*ADR*m-0005	*ADR* data address *URL* (information endpoint)	Octet string 35 bytes	As specified	An IPv6 *URL* to a website containing the full *UNECE* Consignment note details. 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/ The information endpoint to be contacted and respond in a standardized* way using an access to a standardized method to retrieve data, *the standardized way this is done to be set elsewhere and is outside of the scope of this document. Data at that website to provide at a minimum: As specified in Chapter 5.4 of *ADR* . The key requirements are that the documentation contains the following information (5.4.1.1): – The UN Number – Proper shipping name – Class (with subsidiary hazard, if any, in brackets) – Packing group (where assigned) – Number and description of packages – Total quantity of each item of different UN Number – name/address of consignor – name /address of consignee(s). Where there are multiple consignees not known at the start of the journey, the words "Delivery Sale" may be used. – Declaration relating to any special agreement, where applicable (uncommon) – Where assigned, the tunnel code, except where it is known that the journey will not involve passing through a relevant tunnel.
				If *ADR*m-0001 - *ADR*m-0005 data is supplied, no other information is required, but may be provided as backup. **If *ADR*m—0005 data is not supplied the following data concept elements are**

				mandatory
*ADR*m-0005	UN unambiguous identifier of hazardous goods	Integer (8 octets)	00000 000	Up to 10 *ADR* materials (most dangerous (based on response code), within same response code prioritised to most impact in fire or largest volume) semantically identified as: *1 UN ECE unique unambiguous identifier to a specific line of the *UNECE* Economic Commission for Europe, Committee on Inland Transport, European Agreement Concerning the International Carriage of Dangerous Goods by Road: *ADR* (Accord européen relatif au transport international des marchandises dangereuses par Route: *Annex A: General provisions and provisions concerning dangerous articles and substances: Part 3* *Dangerous goods list, special provisions and exemptions related to limited and excepted quantities* **This unambiguous one time identifier is currently under development by** *UNECE*, **and is more specific than just the** *ADR* **number currently in use** *2 quantity in tonnes or 1000 cubic metres ;grossmass/net mass; Signed magnitude is used in the first of these binary places, to indicate 1=gross mass, 0=net mass Each integer therefore comprises 00000 x00; (where x= signed magnitude of 0 or1) Concatenated as as 00000x00, 00000x00, 00000x00, 00000x00, 00000x00, 00000x00, 00000x00, 00000x00, 00000x00, 00000x00, 00000x00, 00000x00, 00000x00, 00000x00, 00000x00, Or 00000x0000000x0000000x000 0000x0000000x0000000x0000

				000x0000000x0000000x00000 00x0000000x0000000x000000 0x0000000x0000000x00 No/no more Hazardous goods identified by '00000000' *1 Issued by UN. May be obtained from http://live.unece.org/trans/danger/publi/adr/adr2011/11contentse.html or http://the-ncec.com/assets/Resources/EAClist2011.pdf
*ADR*m-0006	Alarm information	Octet string (1 Byte)		Any alarm information from on-board sensors (pressure, leakage, shock, temperature etc) Binary Flag 0 = no alarm 1 = alarm 00000000 Binary position L F T S P O R[1] Z L = Leakage alarm F = Fire alarm T = Temperature alarm S = Shock alarm P = Pressure alarm O = Orientation alarm R[1] = reserved for future use Z = Other alarm IMPORTANT NOTE: Emergency services need to be aware that the absence of an alarm indicates only that there was no alarm showing as activated at the time of compiling the data. Alarms raised post the population of/sending of the *ADR*m data will not be transmitted. These codes therefore only indicate status before or at the point of the incident, and cannot be taken as the current status post incident.
*ADR*m-0007	IVS ID	Mandatory	AN (9)	IVS identifier as defined in ISO 15638-5 (to indicate end of consignment data, as this data will vary from journey to journey)

In the event that data is sent in response to an interrogation requesting data, the following data shall be appended:				
Number	**Data concept name**	**Use**	**Format**	**Notes/Source**
ADRm-0008	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 ISO 15638, but is intended to be used by the interrogator to provide a unique reference to its request for data
ARDm-0009	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/

10.8 ADRm application service specific provisions for quality of service

Shall be at the determination of *UNECE*.

The integrity of the data is 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 that are 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 (4.30)*. However, in defining such requirements *jurisdictions* shall wherever possible, use performance based or functionally *specifications (4.43)* in order to avoid locking requirements into technologies that will become obsolete.

NOTE Having prescribed integrity and its parameters into an operational system, it is harder to move to other integrity indicators when new technologies come along.

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

10.9 ADRm application service specific provisions for test requirements

There are no specific provisions for test requirements specified in this Technical Specification version of this document. (May be added by UNECE in a later version).

10.10 ADRm application specific rules for the approval of IVSs and 'Service Providers'

As 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 (4.3) specified within this part of ISO 15638 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 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 (4.30)* and its regulations for instantiation in this respect.

Annex A
(informative)

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

A.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 datafile to the predetermined destination IPv6 (internet) address.

d) Recipient address sends acknowledgement.

e) IVS closes the communication on receipt of acknowledgement.

II. Interrogation

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

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

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

c) On receipt it acknowledges the request (ACK)

d) It closes the communication

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

f) Sends the datafile to a predetermined destination IPv6 (internet) address

g) Recipient address sends acknowledgement

h) IVS Closes the communication on receipt of acknowledgement

These scenarios need to be tested using each of 2G, 3G, WiFi, 5.9GHz (IEEE802.11) using the same data

A number of different datafiles (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

1. 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.)

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

3. The vehicle is equipped with wireless communications that enable it to make communications using 2G, 3G, Mesh WiFi, 5.9GHz (IEEE 802.11p)

4. 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

5. 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.

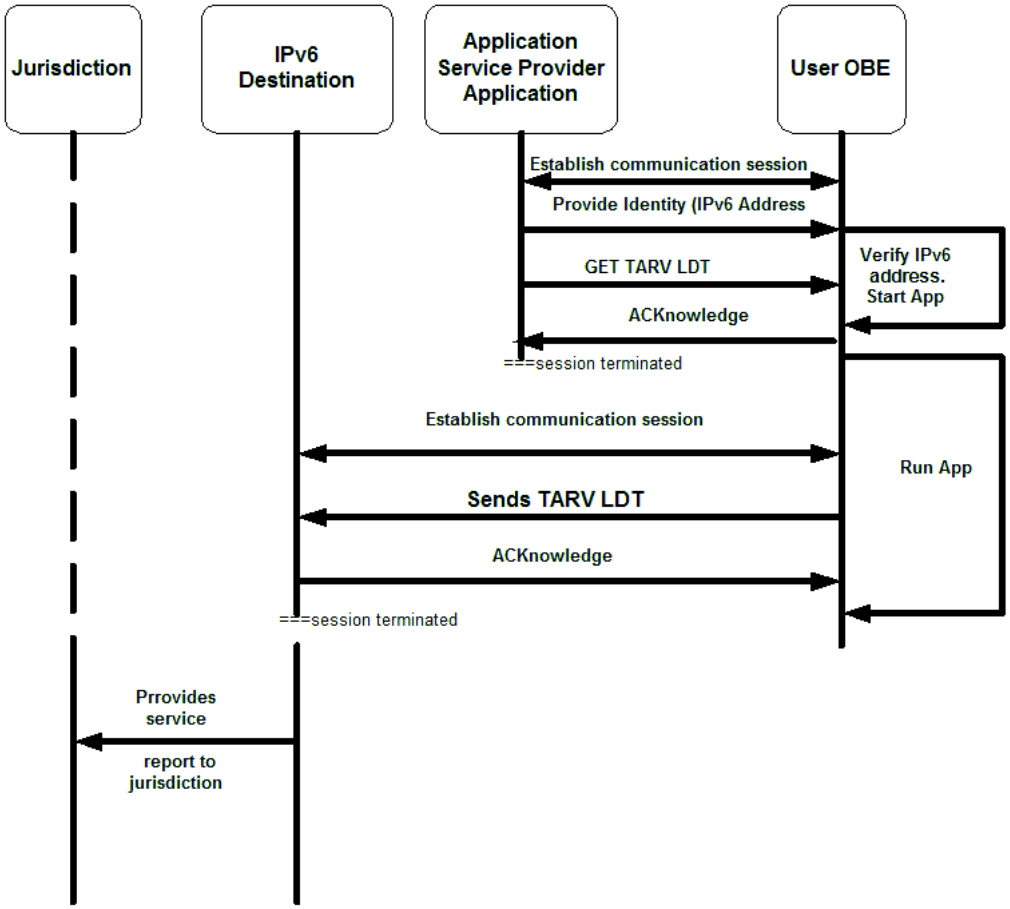

Figure A.1 — Communications sequences to obtain TARV LDT

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

VAM	*vehicle access monitoring*
RTM	*remote electronic tachograph monitoring*
EMS	*emergency messaging system*

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

VMM *vehicle mass monitoring*

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

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

VLM *vehicle location monitoring*

VSM *vehicle speed monitoring*

CLM *consignment and location monitoring*

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

VPF *vehicle parking facilities*

A.2 TEST SCRIPT SERVICE: ADR Dangerous Goods

TEST 10.1 .1: ADR– via 2G. Instigated

STEP 10.1.1.1 IVS instigates a communication session using 2G media to predetermined destination IP address
AS API IPv6 address
As AS 00000000 00000000 xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
Example: PSP 128..16511 1050:0000:0000:0000:0005:0600:300c:326b

Using ',' as a datafield separator

<IVS ID>,
<VehicleLocation>,<ADRConsignmentData>
<IVS ID>
<end>

Table A.1 — ADRm consignment data

FILE TYPE		Format of file name	Notes/Source
ADR	Mandatory	<*ADR*><YYMMDD><hhmmss><vehicle registration number> Example *ADR* 110316 070603 KV76WRR As: *ADR*110316 070603KV76WRR	Clause 19.4.7 (Vehicle/Location/Consignment monitoring file [*ADR* file])

Number	Data concept name	Use	Format	Notes/Source
*ADR*m-0000	IVS ID	Mandatory	AN (9)	IVS identifier as defined in ISO 15638-5

*ADR*m Data Concept element reference	Name	Type	Unit	Description
*ADR*m-0001	*OID*	Integer	1 byte	*ADR*m data concept identifier binary value 1000010 identifying *ADR*m Schema A (until allocated a revised *OID* from a central register)
*ADR*m-0002	ID	Integer	1 byte	*ADR*m Schema A data concept format version set to 1 to discriminate from later *ADR*m Schema A data concept formats Later versions to be backwards compatible with existing versions. Systems receiving an *ADR*m Schema A data concept to support all standardised *ADR*m Schema A data concept versions, which are each uniquely identified using an *ADR*m Schema A data concept format version parameter which will always be contained in the first byte of all [current and future] *ADR*m Schema A Data concept versions.
*ADR*m-0003	Tanker or other vehicle type plus number of dangerous goods on-board	Octet string (1 Byte) Binary	00000000-11111111	The first binary position of the octet to indicate whether the affected vehicle is a tanker or other type of vehicle where 1nnnnnnn = Tanker 0nnnnnnn = Other type of vehicle The remaining 7 binary positions of the octet to identify the number of types of dangerous goods being carried Seven binary bits. x0000000 = no *ADR* goods on board x1111111= mixed load (unspecified number of types of dangerous goods present on-board, but number unknown) x1111110= more than 120 types of *ADR* goods on-board x0000001 – x1111100 = 1 – 124 decimal expressed as binary range: 0 0000000- 1 111111 Concatenated as octet within range : 00000000 – 11111111

*ADR*m-0004	*ADR* Consignment reference	Binary 3 Octets	000000000000000000000000 - 111111111111111111111111	Consignors unique reference number expressed as a binary value between 0 – 16,777,215
*ADR*m-0005	*ADR* data address *URL* (information endpoint)	Octet string 35 bytes	As specified	An IPv6 *URL* to a website containing the full *UNECE* Consignment note details. 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/ The information endpoint to be contacted and respond in a standardized* way using an access to a standardized method to retrieve data, *the standardized way this is done to be set elsewhere and is outside of the scope of this document. Data at that website to provide at a minimum: As specified in Chapter 5.4 of *ADR* . The key requirements are that the documentation contains the following information (5.4.1.1): The UN Number Proper shipping name Class (with subsidiary hazard, if any, in brackets) Packing group (where assigned) Number and description of packages Total quantity of each item of different UN Number name/address of consignor name /address of consignee(s). Where there are multiple consignees not known at the start of the journey, the words "Delivery Sale" may be used. Declaration relating to any special agreement, where applicable (uncommon) Where assigned, the tunnel code, except where it is known that the journey will not involve passing through a relevant tunnel.
				If *ADR*m-0001 - *ADR*m-0005 data is supplied, no other information is required, but may be provided as backup.

				If *ADR*m—0005 data is not supplied the following data concept elements are mandatory
*ADR*m-0005	UN unambiguous identifier of hazardous goods	Integer (8 octets)	00000 000	Up to 10 *ADR* materials (most dangerous (based on response code), within same response code prioritised to most impact in fire or largest volume) semantically identified as: *1 UN ECE unique unambiguous identifier to a specific line of the *UNECE* Economic Commission for Europe, Committee on Inland Transport, European Agreement Concerning the International Carriage of Dangerous Goods by Road: *ADR* (Accord européen relatif au transport international des marchandises dangereuses par Route: *Annex A: General provisions and provisions concerning dangerous articles and substances: Part 3 Dangerous goods list, special provisions and exemptions related to limited and excepted quantities* **This unambiguous one time identifier is currently under development by *UNECE*, and is more specific than just the *ADR* number currently in use** *2 quantity in tonnes or 1000 cubic metres ;grossmass/net mass; Signed magnitude is used in the first of these binary places, to indicate 1=gross mass, 0=net mass Each integer therefore comprises 00000 x00; (where x= signed magnitude of 0 or1) Concatenated as as 00000x00, 00000x00, 00000x00, 00000x00, 00000x00, 00000x00, 00000x00, 00000x00, 00000x00, 00000x00, 00000x00, 00000x00, 00000x00, 00000x00, 00000x00, Or 00000x0000000x0000000x0000000x0000000x0000000x0000000x0000000x0000000x0000000x0000000x0000000x0000000x0000000x0000000x00 No/no more Hazardous goods identified by ‘00000000’

				*1 Issued by UN. May be obtained from http://live.unece.org/trans/danger/publi/adr/adr2011/11contentse.html or http://the-ncec.com/assets/Resources/EAClist2011.pdf
*ADR*m-0006	Alarm information	Octet string (1 Byte)		Any alarm information from on-board sensors (pressure, leakage, shock, temperature etc) Binary Flag 0 = no alarm 1 = alarm 00000000 Binary position L F T S P O R[1] Z L = Leakage alarm F = Fire alarm T = Temperature alarm S = Shock alarm P = Pressure alarm O = Orientation alarm R[1] = reserved for future use Z = Other alarm IMPORTANT NOTE: Emergency services need to be aware that the absence of an alarm indicates only that there was no alarm showing as activated at the time of compiling the data. Alarms raised post the population of/sending of the *ADR*m data will not be transmitted. These codes therefore only indicate status before or at the point of the incident, and cannot be taken as the current status post incident.
*ADR*m-0007	IVS ID	Mandatory	AN (9)	IVS identifier as defined in ISO 15638-5 (to indicate end of consignment data, as this data will vary from journey to journey)

FILENAME: <ADR110316 070603KV76WRR>

FILE CONTENT:< D0o3M45S ,1,1,binary00000101,binary111111111111111111111101, scheme://domain:port/path?query_string#fragment_id,11234020, 11235005, 11236005, 11237005, 11238005,00000000,binary10111001, D0o3M45S>

STEP 10.1.1.2 IVS sends file named <ADR110316 070603KV76WRR>
< D0o3M45S ,1,1,binary00000101,binary111111111111111111111101, scheme://domain:port/path?query_string#fragment_id,11234020, 11235005, 11236005, 11237005, 11238005,00000000,binary10111001, D0o3M45S>

STEP 10.1.1.3 Destination address sends ACK <ADR>

STEP 10.1.1.4 IVS receives ACK <ADR>

STEP 10.1.1.5 IVS closes communication session

CTP 10.1.1 Instigated ADR - Dangerous Goods Monitoring using 2G

SUT Reference	Instigated send of ADR - Dangerous goods monitoring using 2G
CTP/10.1.1	
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 datafile to the predetermined destination IPv6 (internet) address Recipient address sends acknowledgement IVS closes the communication on receipt of acknowledgement
CTP Origin	CSI
Reference requirement	ISO 15638-18
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, 5.9GHz (IEEE802.11p) 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
10.1.1.1	1	IVS instigates a communication session using selected media (2G) to predetermined destination IP address	Session established
10.1.1.2	2	IVS sends file named <ADR110316 070603KV76WRR> <START> < D0o3M45S ,1,1,binary00000101,binary111111111111111111111101, scheme://domain:port/path?query_string#fragment_id,112 34020, 11235005, 11236005, 11237005, 11238005,00000000,binary10111001, D0o3M45S> <END>	File sent and arrives correctly at destination

10.1.1.3	3	Destination address sends ACK <ADX>	
10.1.1.4	4	IVS receives ACK <ADX>	File received and ACK <ADX> sent
10.1.1.5	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 10.1.1	PASS / FAIL	Date: 29th June 2102
Signature/initials 	PASS	 k4, MIRA, Watling St, Nuneaton, Warwickshire, CV10 0TU, UK Tel: +44 (0)7730 922 810 Web: www.innovits.com/advance

CTP 10.1.2 Interrogated ADR - Dangerous goods monitoring using 2G

SUT Reference	Interrogated send of ADR - Dangerous goods monitoring using 2G
CTP/10.1.2	
SUT 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 to an active wireless communication session 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 Origin	CEN
Reference requirement	ISO 15638-18
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, 5.9GHz (IEEE802.11p) 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
10.1.2.1	1	session connected (incoming call)	Call in progress
10.1.2.2	2	Caller sends data request command (GPRS, EDGE etc) GET ADR	Data request sent
10.1.2.3	3	IVS acknowledges request by returning ACKnowledgement <Y>	ACK<Y> received
10.1.2.4	4	IVS closes communication session	Communication session closed
10.1.2.5	5	IVS instigates a communication session using selected media to predetermined destination IP address	Communication session successfully opened
10.1.2.5	6	IVS sends file named <ADR110316 070603KV76WRR> <START> < D0o3M45S	File sent and arrives correctly at destination

		,1,1,binary00000101,binary11111111111111111111111, scheme://domain:port/path?query_string#fragment_id,11234020, 11235005, 11236005, 11237005, 11238005,00000000,binary10111001, D0o3M45S> <END>	
10.1.2.6	7	Destination address sends ACK <ADX>	
10.1.2.7	8	IVS receives ACK <ADX>	File received and ACK <ADX> sent
10.1.2.8	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 10.1.2	PASS / FAIL	Date: 29th June 2102
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 10.1.3 Interrogated ADR - Dangerous goods monitoring using 5.9GHz and responding using 2G or 3G

SUT Reference	Interrogated ADR - Dangerous goods monitoring using 5.9 GHz and send of ADR - Dangerous goods monitoring using 2G or 3G
CTP/10.1.3	
SUT 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 to an active wireless communication session The IVS of a vehicle receives a 5.9GHz (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 15638-18
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, 5.9GHz (IEEE802.11p) 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
10.1.3.1	1	session connected (incoming call) using 5.9 Ghz (IEEE 802.11p)	Call in progress
10.1.3.2	2	Caller sends data request command GET ADR	Data request sent
10.1.3.3	3	IVS acknowledges request by returning ACKnowledgement <y>	ACK<Y> received
10.1.3.4	4	IVS closes communication session	Communication session closed
10.1.3.5	5	IVS instigates a communication session using 2G or 3G	Communication session successfully opened
10.1.3.5	6	IVS sends file named <ADR110316 070603KV76WRR> <START> < D0o3M45S ,1,1,binary00000101,binary111111111111111111111101, scheme://domain:port/path?query_string#fragment_id,11234	File sent and arrives correctly at destination

		020, 11235005, 11236005, 11237005, 11238005,00000000,binary10111001, D0o3M45S><END>	
10.1.3.6	7	Destination address sends ACK <ADX>	
10.1.3.7	8	IVS receives ACK <ADX>	File received and ACK <ADX> sent
10.1.3.8	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 10.1.3	PASS / FAIL	Date: 29th June 2102
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 10.2.1 Instigated ADR - Dangerous goods monitoring using 3G

SUT Reference	Instigated send of ADR - Dangerous goods monitoring using 3G
CTP/10.2.1	
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 datafile to the predetermined destination IPv6 (internet) address Recipient address sends acknowledgement IVS closes the communication on receipt of acknowledgement
CTP Origin	CSI
Reference requirement	ISO 15638-18
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, 5.9GHz (IEEE802.11p) 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
10.2.1.1	1	IVS instigates a communication session using selected media (3G) to predetermined destination IP address	Session established
10.2.1.2	2	IVS sends file named <ADR110316 070603KV76WRR> <START> <ID0o3M45S, s0123^110316 x0A5D3770 0x027E2938 >0123, 123456,T43,03,12345,12355, AaaSs,0,0,xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx,128..16 511,1G1JF27W8GJ178227,000000 ,1297339499,0x0A5D3770,0x027E2938,0000,8,0,123,1,00 0,000,010326,UK,Peter Jones,01,02,03a,h1,120325,010326 124538,Peter Jones 01,02,h1 ,120325, ID0o3M45S >	File sent and arrives correctly at destination

		<END>	
10.2.1.3	3	Destination address sends ACK <ADX>	
10.2.1.4	4	IVS receives ACK <ADX>	File received and ACK <ADX> sent
10.2.1.5	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 10.2.1	PASS / FAIL	Date: 29th June 2102
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 10.2.2 Interrogated at 5.9 GHz and send of ADR - Dangerous goods monitoring using 3G

SUT Reference	5.9 GHz Interrogated and send of ADR - Dangerous goods monitoring using 3G
CTP/10.2.2	
SUT 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 to an active wireless communication session The IVS of a vehicle receives a 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 Origin	CEN
Reference requirement	ISO 15638-18
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, 5.9GHz (IEEE802.11p) 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
10.2.2.1	1	session connected (incoming call) using 5.9 Ghz (IEEE 802.11p)	Call in progress
10.2.2.2	2	Caller sends data request command GET ADR	Data request sent
10.2.2.3	3	IVS acknowledges request by returning ACKnowledgement <Y>	ACK<Y> received
10.2.2.4	4	IVS closes communication session	Communication session closed
10.2.2.5	5	IVS instigates a communication session using selected media (2G or 3G) to predetermined destination IP address	Communication session successfully opened
10.2.2.5	6	IVS sends file named <ADR110316 070603KV76WRR> <START> < D0o3M45S	File sent and arrives correctly at destination

		,1,1,binary00000101,binary11111111111111111111111, scheme://domain:port/path?query_string#fragment_id,11234020, 11235005, 11236005, 11237005, 11238005,00000000,binary10111001, D0o3M45S> <END>	
10.2.2.6	7	Destination address sends ACK <ADX>	
10.2.2.7	8	IVS receives ACK <ADX>	File received and ACK <ADX> sent
10.2.2.8	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 10.2.2	PASS / FAIL	Date: 29th June 2102
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 10.3.1 Instigated ADR - Dangerous goods monitoring using 802.11p (WAVE) 5.9 GHz

SUT Reference	Instigated ADR - Dangerous goods monitoring using 802.11p (WAVE) 5.9 GHz
CTP/10.3.1	
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 datafile to the predetermined destination IPv6 (internet) address Recipient address sends acknowledgement IVS closes the communication on receipt of acknowledgement
CTP Origin	CSI
Reference requirement	ISO 15638-18
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, 5.9GHz (IEEE802.11p) 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
10.3.1.1	1	IVS instigates a communication session using selected media (5.9G) to predetermined destination IP address	Session established
10.3.1.2	2	IVS sends file named <ADR110316 070603KV76WRR> <START> < D0o3M45S ,1,1,binary00000101,binary111111111111111111111101, scheme://domain:port/path?query_string#fragment_id,11234020, 11235005, 11236005, 11237005, 11238005,00000000,binary10111001, D0o3M45S> <END>	File sent and arrives correctly at destination

10.3.1.3	3	Destination address sends ACK <ADX>	
10.3.1.4	4	IVS receives ACK <ADX>	File received and ACK <ADX> sent
10.3.1.5	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 10.3.1	PASS / FAIL	Date: 29th June 2102
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 10.3.2 Interrogated ADR - Dangerous goods monitoring using 802.11p (WAVE) 5.9 GHz

SUT Reference	Interrogated send of ADR - Dangerous goods monitoring using 802.11p (WAVE) 5.9 GHz
CTP/10.3.2	
SUT 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 to an active wireless communication session The IVS of a vehicle receives a 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 Origin	CEN
Reference requirement	ISO 15638-18
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, 5.9GHz (IEEE802.11p) 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
10.3.2.1	1	session connected (incoming call) using 5.9 Ghz (IEEE 802.11p)	Call in progress
10.3.2.2	2	Caller sends data request command GET ADR	Data request sent
10.3.2.3	3	IVS acknowledges request by returning ACKnowledgement <Y>	ACK<Y> received
10.3.2.4	4	IVS closes communication session	Communication session closed
10.3.2.5	5	IVS instigates a communication session using 5.9GHz selected media to predetermined destination IP address	Communication session successfully opened
10.3.2.5	6	IVS sends file named <ADR110316 070603KV76WRR> <START> < D0o3M45S	File sent and arrives correctly at destination

		,1,1,binary00000101,binary11111111111111111111111, scheme://domain:port/path?query_string#fragment_id,11234020 , 11235005, 11236005, 11237005, 11238005,00000000,binary10111001, D0o3M45S> <END>	
10.3.2.6	7	Destination address sends ACK <ADX>	
10.3.2.7	8	IVS receives ACK <ADX>	File received and ACK <ADX> sent
10.3.2.8	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 10.3.2	PASS / FAIL	Date: 29th June 2102
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 10.4.1 Instigated ADR - Dangerous goods monitoring using Mesh WiFi

SUT Reference	Instigated send of ADR - Dangerous goods monitoring using Mesh WiFi
CTP/10.4.1	
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 datafile to the predetermined destination IPv6 (internet) address Recipient address sends acknowledgement IVS closes the communication on receipt of acknowledgement
CTP Origin	CSI
Reference requirement	ISO 15638-18
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, 5.9GHz (IEEE802.11p) 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
10.4.1.1	1	IVS instigates a communication session using selected media (Mesh WiFi) to predetermined destination IP address	Session established
10.4.1.2	2	IVS sends file named <ADR110316 070603KV76WRR> <START> < D0o3M45S ,1,1,binary00000101,binary111111111111111111111101, scheme://domain:port/path?query_string#fragment_id,112 34020, 11235005, 11236005, 11237005, 11238005,00000000,binary10111001, D0o3M45S> <END>	File sent and arrives correctly at destination

10.4.1.3	3	Destination address sends ACK <ADX>	
10.4.1.4	4	IVS receives ACK <ADX>	File received and ACK <ADX> sent
10.4.1.5	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 10.4.1	PASS / FAIL	Date: 29th June 2102
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 10.4.2 Interrogated ADR - Dangerous goods monitoring using Mesh WiFi

SUT Reference	5.9 GHz Interrogated and send of ADR - Dangerous goods monitoring using Mesh WiFi
CTP/10.4.2	
SUT 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 to an active wireless communication session The IVS of a vehicle receives a 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 Origin	CEN
Reference requirement	ISO 15638-18
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, 5.9GHz (IEEE802.11p) 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
10.4.2.1	1	session connected (incoming call) using 5.9 Ghz (IEEE 802.11p)	Call in progress
10.4.2.2	2	Caller sends data request command (GPRS, EDGE etc) GET ADR	Data request sent

10.4.2.3	3	IVS acknowledges request by returning ACKnowledgement <Y>	ACK<Y> received
10.4.2.4	4	IVS closes communication session	Communication session closed
10.4.2.5	5	IVS instigates a communication session using mesh WiFi selected media to predetermined destination IP address	Communication session successfully opened
10.4.2.5	6	IVS sends file named <ADR110316 070603KV76WRR> <START> < D0o3M45S ,1,1,binary00000101,binary111111111111111111111101, scheme://domain:port/path?query_string#fragment_id,1123 4020, 11235005, 11236005, 11237005, 11238005,00000000,binary10111001, D0o3M45S> <END>	File sent and arrives correctly at destination
10.4.2.6	7	Destination address sends ACK <ADX>	
10.4.2.7	8	IVS receives ACK <ADX>	File received and ACK <ADX> sent
10.4.2.8	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 10.4.2	PASS / FAIL	Date: 29th June 2102
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

Bibliography

[1] ISO/IEC Directives, Part 2, *Rules for the structure and drafting of International Standards*

[2] ISO/IEC TR 10000-1, *Information technology — Framework and taxonomy of International Standardized Profiles — Part 1: General principles and documentation framework*

[3] ISO 10241, *Terminological entries in standards*

[4] ISO 128-30, *Technical drawings — General principles of presentation — Part 30: Basic conventions for views*

[5] ISO 128-34, *Technical drawings — General principles of presentation — Part 34: Views on mechanical engineering drawings*

[6] ISO 128-40, *Technical drawings — General principles of presentation — Part 40: Basic conventions for cuts and sections*

[7] ISO 128-44, *Technical drawings — General principles of presentation — Part 44: Sections on mechanical engineering drawings*

[8] ISO 80000 (all parts), *Quantities and units*

[9] IEC 80000 (all parts), *Quantities and units*

[10] IEC 60027 (all parts), *Letter symbols to be used in electrical technology*

[11] ISO 1000, *SI units and recommendations for the use* of thei*r multiples and of certain other units*

[12] ISO 690, *Information and documentation — Guidelines for bibliographic references and citations to information resources*

[13] ISO 690-2, *Information and documentation — Guidelines for bibliographic references and citations to information resources — Part 2: Electronic documents or parts thereof*

[14] UNECE: *Accord européen relatif au transport international des marchandises Dangereuses par Route*

ICS 03.220.20; 35.240.60

Price based on 54 pages

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™