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

**Part 18:
ADR (Dangerous Goods)**

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

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



STANDARDSISO.COM : Click to view the full PDF of ISO 15638-18:2017



COPYRIGHT PROTECTED DOCUMENT

© ISO 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

	Page
Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Symbols and abbreviated terms	7
5 Conformance	8
6 General overview and framework requirements	8
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	9
8.4 Marking, labelling and packaging	9
9 Common features of regulated TARV application services	9
9.1 General	9
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	11
9.8 Software engineering quality systems	11
9.9 Quality monitoring station	11
9.10 Audits	11
9.11 Data access control policy	11
9.12 Approval of IVSs and service providers	11
10 TARV ADR consignment monitoring (ADRM)	12
10.1 ADRm service description and scope	12
10.1.1 ADRm use case	12
10.1.2 Description of ADRm regulated application service	12
10.2 Concept of operations for ADRm	13
10.2.1 General	13
10.2.2 Statement of the goals and objectives of ADRm	13
10.2.3 Strategies, tactics, policies and constraints affecting ADRm	13
10.2.4 Organizations, activities, and interactions among participants and stakeholders in ADRm	15
10.2.5 Clear statement of responsibilities and authorities delegated for ADRm	15
10.2.6 Operational processes for the ADRm	16
10.2.7 Role of ADRm service provider	16
10.2.8 Role of ADRm user	16
10.3 Sequence of operations for ADRm	16
10.4 ADRm naming content and quality	17
10.5 Specific ADRm data naming content and quality	17
10.6 ADRm service elements	18
10.6.1 ADRm SE1: Establish jurisdiction regulations or system specification for ADR monitoring	18
10.6.2 ADRm SE2: Request system approval	18
10.6.3 ADRm SE3: User (operator) contracts with prime service provider	18

10.6.4	ADRM SE4: User (operator) equips vehicle with a means to provide consignment data.....	18
10.6.5	ADRM SE5: User contracts with application service provider.....	18
10.6.6	ADRM SE6: Application service provider uploads software into the TARV-equipped vehicles of the operator.....	18
10.6.7	ADRM SE7: Recording of vehicle consignment data.....	18
10.6.8	ADRM SE8: ADRm Trigger.....	19
10.6.9	ADRM SE9: Contact predetermined IPv6 address.....	19
10.6.10	ADRM SE10: Obtain consignment data.....	19
10.6.11	ADRM SE11: “Interrogated” request for ADR data.....	20
10.6.12	ADRM SE12: Notification to operator.....	20
10.7	ADRM access methods to provision and retrieve data.....	20
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 document.....		29
Bibliography		55

Foreword

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

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

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

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

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

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

This first edition of ISO 15638-18 cancels and replaces ISO/TS 15638-18:2013, which has been technically revised to bring the MSD and optional data concept specifications in line with the current revisions to EN 15722 and CEN TS 16405.

A list of all parts in the ISO 15638 series can be found on the ISO website.

Introduction

Many ITS technologies have been embraced by commercial transport operators and freight owners, in the areas of fleet management, safety and security. Telematics applications have also been developed for governmental use. Such regulatory services in use or being considered vary from jurisdiction to jurisdiction but include electronic on-board recorders, digital tachograph, on-board mass monitoring, “mass” data for regulatory control and management, vehicle access methods, hazardous goods tracking and e-call. 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, it is timely to consider an overall architecture (business and functional) that could support these functions from a single platform within a commercial freight vehicle that operate within such regulations. International Standards will allow for a speedy development and specification of new applications that build upon the functionality of a generic specification platform. A series of standards is required to describe and define the framework 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.

This series of standards addresses and defines the framework for a range of cooperative telematics ITS service applications for regulated commercial freight vehicles (such as access, driver fatigue management, speed monitoring, on-board mass monitoring, “mass” data for regulatory control and management). The overall scope includes the concept of operation, legal and regulatory issues and the generic cooperative provision of services to regulated commercial freight vehicles, using an on-board ITS platform. The framework is based on a (multiple) service provider-oriented approach with provisions for the approval and auditing of service providers.

This series of standards will:

- provide the basis for future development of cooperative telematics applications for regulated commercial freight vehicles. Many elements to accomplish this are already available. Existing relevant standards will be referenced and the specifications 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;
- a business architecture based on a (multiple) service provider oriented approach;
- address legal and regulatory aspects for the approval and auditing of service providers.

This series of standards is timely as many governments (Europe, North America, Asia and Australia/New Zealand) are considering the use of telematics 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 document provides specifications for ADR (dangerous goods).

NOTE 1 The definition of what comprises a “regulated” vehicle is regarded as an issue for National decision and can vary from jurisdiction to jurisdiction. This series of standard does not impose any requirements on nations in respect of how they define a regulated vehicle.

NOTE 2 The definition of what comprises a ‘regulated’ service is regarded as an issue for National decision, and can vary from *jurisdiction* to *jurisdiction*. This series of standards documents does not impose any requirements on nations in respect of which services for regulated vehicles *jurisdictions* will require, or support as an option, but will provide standardized sets of requirements descriptions for identified services to enable consistent and cost-efficient implementations where implemented.

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

Part 18: ADR (Dangerous Goods)

1 Scope

This document addresses the provision of “ADR (dangerous goods)” and specifies the form and content of such data required to support such systems and access methods to that data.

The scope of this document is to provide specifications for common communications and data exchange aspects of the application service ADR (dangerous goods) that a regulator may elect to require or support as an option, including

- a) high-level definition of the service that a service provider has to provide (the service definition describes common service elements, but does not define the detail of how such an application service is instantiated, nor the acceptable value ranges of the data concepts defined),
- b) means to realize the service, and
- c) application data, naming content and quality that an IVS has to deliver.

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

ISO 15638 has been developed for use in the context of regulated commercial freight vehicles (hereinafter referred to as “regulated 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.

2 Normative references

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

ISO 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) — Common platform parameters using CALM*

ISO 15638-3, *Intelligent transport systems — Framework for collaborative telematics applications for regulated commercial freight vehicles (TARV) — Operating requirements, ‘approval authority’ procedures, and enforcement provisions for the providers of regulated services*

ISO 15638-4¹⁾, *Intelligent transport systems — Framework for collaborative telematics applications for regulated commercial freight vehicles (TARV) — System security requirements*

ISO 15638-5:2013, *Intelligent transport systems — Framework for collaborative telematics applications for regulated commercial freight vehicles (TARV) — General vehicle information*

ISO 15638-6:2014, *Intelligent transport systems — Framework for collaborative telematics applications for regulated commercial freight vehicles (TARV) — Regulated applications*

ISO 15638-10, *Intelligent transport systems — Framework for cooperative telematics applications for regulated vehicles (TARV) -Emergency messaging system/eCall*

3 Terms and definitions

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

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

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

3.1 access methods

procedures and protocols to provision and retrieve data

3.2 app

small (usually) *Java*[™] (3.28) applets, organized as software bundles, that support *application services* (3.3) by keeping the *data pantry* (3.18) provisioned with up to date data

3.3 application service

service provided by a *service provider* (3.40) enabled by accessing data from the *IVS* (3.25) of a *regulated vehicle* (3.37) via a wireless communications network

3.4 application service provider ASP

party that provides an *application service* (3.3)

3.5 app library

separately secure area of memory in *IVS* (3.25) where apps are stored (with different access controls to *data pantry* (3.18))

3.6 approval

formal affirmation that an applicant has satisfied all the requirements for appointment as an *application service provider* (3.4) or that an application service delivers the required service levels

3.7 approval agreement

written agreement made between an *approval authority (regulatory)* (3.8) and a *service provider* (3.40)

Note 1 to entry: An *approval authority (regulatory)* (3.8) approval agreement recognizes the fact that a *service provider* (3.40), 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.

1) To be published.

3.8**approval authority (regulatory)**

organization (usually independent) which conducts *approval* (3.6) and ongoing *audit* (3.10) for *service providers* (3.40) on behalf of a *jurisdiction* (3.29)

3.9**architecture**

formalized description of the design of the structure of TARV and its *framework* (3.24)

3.10**audit/auditing**

review of a party's capacity to meet, or continue to meet, the initial and ongoing *approval agreements* (3.7) as a *service provider* (3.40)

3.11**basic vehicle data**

data that shall be maintained/provided by all *IVS* (3.25) (regardless of *jurisdiction* (3.29))

3.12**communications access for land mobiles****CALM**

layered solution that enables continuous or quasi continuous communications between vehicles and the infrastructure, or between vehicles, using such (multiple) wireless telecommunications media that are available in any particular location and which have the ability to migrate to a different available media where required and where media selection is at the discretion of *user* (3.45) determined parameters by using a series 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* (3.27) to provide wireless support for applications, such that the application is independent of any particular wireless medium

3.13**commercial application(s)**

ITS applications in *regulated vehicles* (3.37) for commercial (non-regulated) purposes

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

3.14**consignment**

shipment of goods/cargo to a destination

3.15**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* (3.27) 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* (3.26)

3.16**core data**

basic vehicle data (3.11) plus any additional data required to provide an implemented *regulated application service* (3.36)

3.17**dangerous goods****hazardous goods****HAZMAT**

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

3.18

data pantry

secure area of memory in *IVS* (3.25) where data values are stored (with different access controls to *app library* (3.5))

3.19

driver

person driving the *regulated vehicle* (3.37) at any specific point in time

3.20

driver work records

DWR

collection, collation, and transfer of *driver* (3.19) work and rest hours data from an *in-vehicle system* (3.25) to an *application service provider* (3.4)

3.21

eCall

specialized instantiation of an *EMS* (3.22) that provides incident messaging and communication with a public service assistance point via priority wireless telephone communications using its emergency call capabilities

3.22

emergency message system

EMS

collection, collation, and transfer of emergency message data from an *in-vehicle system* (3.25) to an *application service provider* (3.4)

3.23

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

3.24

framework

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

3.25

in-vehicle system

IVS

ITS-station (3.27) and connected equipment on board a vehicle

3.26

ITS service

communication functionality offered by an *ITS-station* (3.27) to an *ITS-station application*

3.27

ITS-station

ITS-s

entity in a communication network, comprised of application, *facilities* (3.23), networking and access layer components specified in ISO 21217 that operate within a bounded secure management domain

3.28

Java™

object-oriented open source operating language developed by SUN systems

3.29

jurisdiction

government, road or traffic authority which owns the *regulatory applications* (3.35)

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

3.30**local data tree****LDT**

frequently updated data concept stored in the on-board *data pantry* (3.18) containing a collection of data values deemed essential for either a) *TARV regulated application service* (3.36) or b) *cooperative intelligent transport systems* (3.15)

3.31**mass**

mass of a given heavy vehicle as measured by equipment affixed to the *regulated vehicle* (3.37)

3.32**“mass” data for regulatory control and management****MRC**

collection, collation, and transfer of vehicle *mass* (3.31) data from an *in-vehicle system* (3.25) to an *application service provider* (3.4) to enable data provision to *jurisdictions* (3.29) for the control and management of equipped vehicles based on the *mass* of the *regulated vehicle* (3.37), or use of such data to enable compliance with the provisions of regulations

3.33**operator**

fleet manager of a *regulated vehicle* (3.37)

3.34**prime service provider**

service provider (3.40) who is the first contractor to provide *regulated application services* (3.36) to the *regulated vehicle* (3.37) or a nominated successor on termination of that initial contract

Note 1 to entry: The *prime service provider* (3.34) is also responsible to maintain the installed *IVS* (3.25).

Note 2 to entry: If the *IVS* was not installed during the manufacture of the vehicle the *prime service provider* (3.34) is also responsible to install and commission the *IVS* (3.25).

3.35**regulated/regulatory application**

application arrangement using TARV utilized by *jurisdictions* (3.29) 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 1 to entry: This may be mandatory or voluntary at the discretion of the jurisdiction.

3.36**regulated application service**

TARV *application service* (3.3) to meet the requirements of a *regulated application* (3.35) that is mandated by a regulation imposed by a *jurisdiction* (3.29) or is an option supported by a jurisdiction

3.37**regulated commercial freight vehicle/regulated vehicle**

vehicle that is subject to regulations determined by the *jurisdiction* (3.29) 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 1 to entry: At the option of jurisdictions, this may require the provision of information via TARV or provide the option to do so.

3.38**regulator**

agent of the *jurisdiction* (3.29) appointed to regulate and manage TARV within the domain of the jurisdiction

Note 1 to entry: This may or may not be the *approval authority (regulatory)* (3.8).

3.39

remote tachograph monitoring

RTM

collection, collation, and transfer of data from an on-board electronic *tachograph* (3.43) system to an *application service provider* (3.4)

3.40

service provider

party which is approved by an approval *authority (regulatory)* (3.8) as suitable to provide regulated or commercial ITS *application services* (3.3)

3.41

session

wireless communication exchange between the *ITS-station* (3.27) of an *IVS* (3.25) and the *ITS-station* of its *application service provider* (3.4) to achieve data update, data provision, upload apps, or otherwise manage the provision of the *application service* (3.3), or a wireless communication provision of data to the *ITS-station* of an *IVS* (3.25) from any other *ITS-station*

3.42

specification

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

3.43

tachograph

sender unit mounted to a vehicle gearbox, a tachograph head and a digital driver card, which records the *regulated vehicle* (3.37) speed and the times at which it was driven and aspects of the *driver's* (3.19) activity selected from a choice of modes

3.44

telematics

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

3.45

user

individual or party that enrolls in and operates within a regulated or *commercial application* (3.13) *service* (3.3)

EXAMPLE *Driver* (3.19), *transport operator* (3.33), freight owner, etc.

3.46

vehicle access control

VAC

control of *regulated vehicles* (3.37) ingress to and egress from controlled areas and associated penalties and levies

3.47

vehicle access management

VAM

monitoring and management of *regulated vehicles* (3.37) approaching or within sensitive and controlled areas

3.48

vehicle location monitoring

VLM

collection, collation, and transfer of vehicle location data from an *in-vehicle system* (3.25) to an *application service provider* (3.4)

3.49**vehicle mass monitoring****VMM**

collection, collation, and transfer of vehicle *mass* (3.31) data from an *in-vehicle system* (3.25) to an *application service provider* (3.4)

3.50**vehicle parking facility****VPF**

system for booking and *access* (3.1) to and egress from a vehicle parking facility (VPF)

3.51**vehicle speed monitoring****VSM**

collection, collation, and transfer of vehicle speed data from an *in-vehicle system* (3.25) to an *application service provider* (3.4)

4 Symbols and abbreviated terms

ADR	<i>Accord européen relatif au transport international des marchandises Dangereuses par Route (dangerous goods)</i>
ADRM	ADR monitoring
app	applet (Java™ application or similar)
ASP	application service provider
CALM	communications access for land mobiles
C-ITS	cooperative intelligent transport systems
DLR	driving licence reader
DRD	driver records device
EMS	emergency message system
ID	identity
IP	Internet protocol
ITS-S	ITS-station
IVS	in-vehicle system
LDT	local data tree
MSD	minimum set of data (<i>eCall</i> , EN 15722)
OID	object identifier
PSAP	public service answering point
SAD	single administrative document (which accompanies ADR consignments in Europe)
SE	service element
s.u.t	system under test

TARV	telematics applications for regulated vehicles
TD	transport document
UML	Unified Modeling Language (see ISO 19501)
UNECE	United Nations Economic Commission for Europe
URL	uniform resource locator
UTC	coordinated universal time

5 Conformance

Requirements to demonstrate conformance to any of the general provisions or specific application services described in this document shall be within the regulations imposed by the jurisdiction where they are instantiated. Conformance requirements to meet the provisions of this document 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 document have been independently tested. [Annex A](#) 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.

6 General overview and framework requirements

ISO 15638-1 provided a framework and architecture 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 and detail and specification of the roles of the actors involved, the reader is referred to ISO 15638-1.

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

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

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

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

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

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

In order to be compliant with this document, 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 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 document contains no general requirements concerning quality of service. Such aspects shall be determined by a jurisdiction as part of its specification for any particular regulated application service. However, where a specified regulated application service has specific Q of S requirements essential to maintain interoperability, these aspects shall be as specified in [Clause 10](#).

8.3 Test requirements

This document contains no general requirements concerning test requirements. Such aspects shall be determined by a jurisdiction as part of its specification for any particular regulated application service, and issued as a formal test requirements specification document. However, where a specified regulated application service 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. Where multiple jurisdictions recognize a benefit to common test procedures for a specific regulated application service, this shall be the subject of a separate standards deliverable.

8.4 Marking, labelling and packaging

This document 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 series, the contracting parties shall make such risk explicitly known to the implementing jurisdiction 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 are as designed by the application service system to meet the requirements of a particular jurisdiction 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 document shall also be compliant with the requirements of ISO 15638-6.

The means by which data is provisioned into the data pantry and the means to obtain the TARV LDT and core data are described in ISO 15638-6:2014, Clause 8.

In order to minimize the demand on the IVS (which it is assumed will be performing multiple application services 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.

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

For further information, see ISO 15638-6:2014, Clause 9.

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

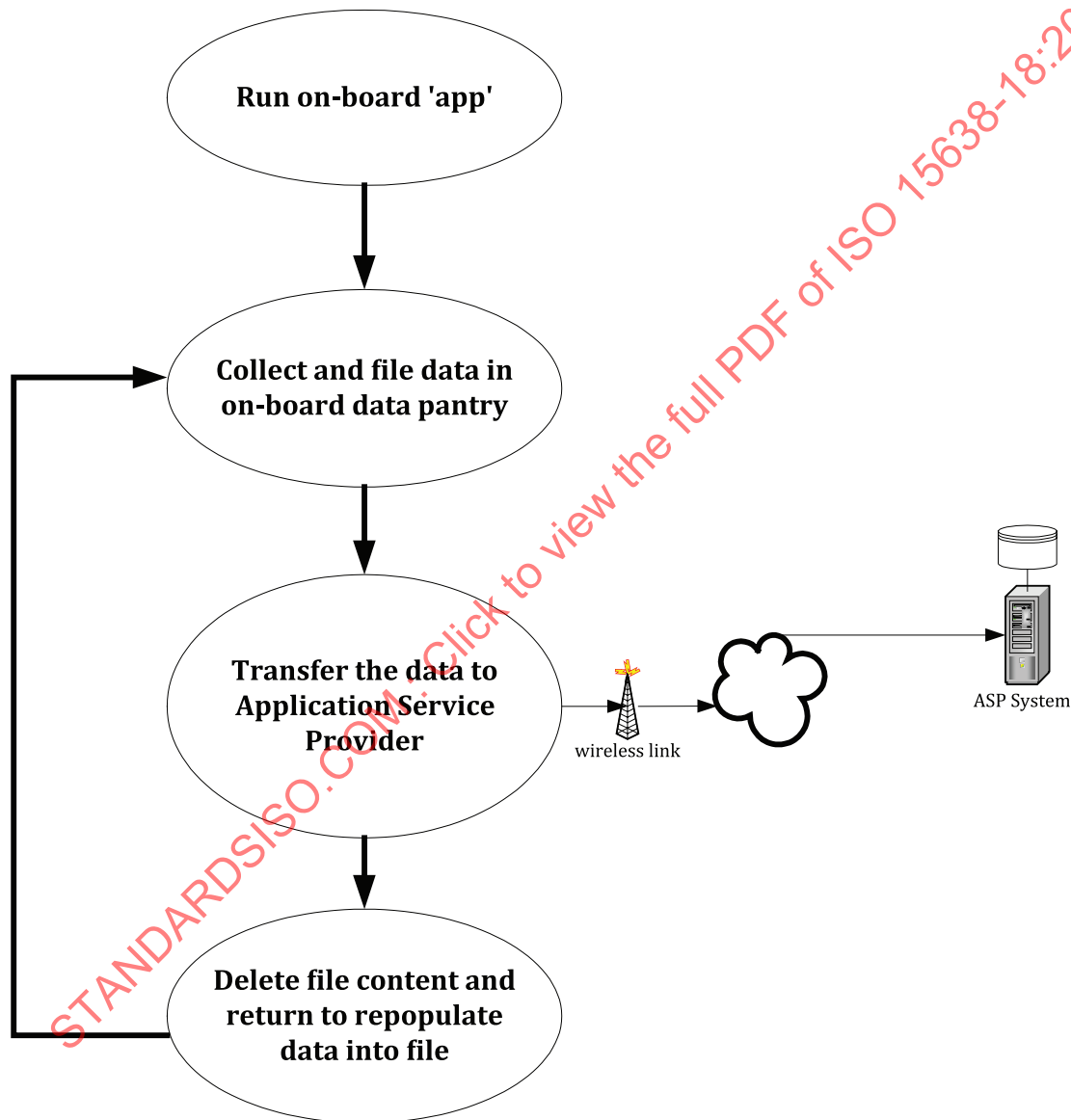


Figure 1 — TARV regulated application service on-board procedure

At a common generic functional level for this application service, the process may be seen as shown in [Figure 2](#). However, the connected equipment may or 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 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 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, 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 of IVSs and service providers shall be as specified in ISO 15638-3. Detailed provisions for specific regulated applications shall be as specified by the regime of the jurisdiction.

10 TARV ADR consignment monitoring (ADRM)

10.1 ADRm service description and scope

NOTE ADR is a requirement in Europe and other countries; it is not a global requirement. Other parts of the ISO 15638 series, particularly ISO 15638-17, provide a means to provide general monitoring of consignments. This document is specified separately because it makes specific reference to very specific provisions for ADR required in nearly 50 countries and UNECE has requested that, in addition to emergency messaging, provision is made for their non-emergency ADR requirements to be accommodated within TARV.

10.1.1 ADRm use case

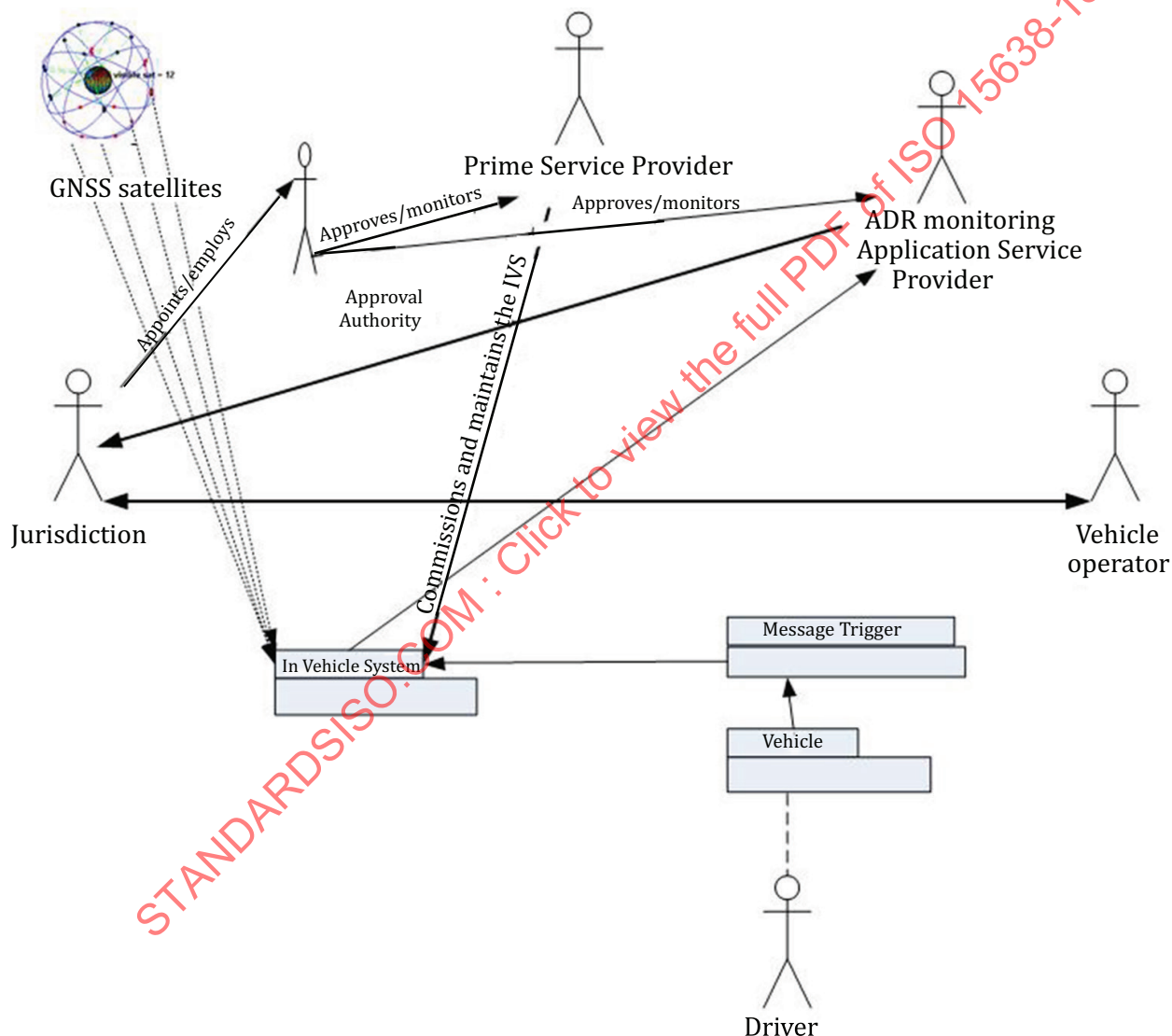


Figure 2 — ADRm use case

10.1.2 Description of ADRm regulated application service

This application service uses the wireless link between the on-board ITS-station (in-vehicle platform) and an application service provider, in order to convey an ADR (Accord européen relatif au transport

international des marchandises Dangereuses par Route), otherwise known as “dangerous goods or HAZMAT”) consignment, data from the regulated vehicle to an ADRm application service provider. See [Figure 2](#).

This use case covers data to be sent in the normal course of business where ADR consignment monitoring is required. In respect of ADR emergency messages, refer to ISO 15638-10.

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

10.2 Concept of operations for ADRm

10.2.1 General

ADR consignments are the subject of special regulations. In most jurisdictions, significant paperwork is processed through the administration system and has to accompany the regulated vehicle 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 PSAPs/emergency responders in response to an incident, see ISO 15638-10.

The majority of access to information is required as part of routine (non-emergency) situations. This document 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 and its consignment, to support ADR regulations together with other key data, as implemented by jurisdictions.

NOTE UNECE JWG RID are currently reviewing their reference pointers to ADR information and this document 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 ADRm data will vary from jurisdiction to jurisdiction, so the nexus of this service is the provision of data from the regulated vehicle to a landside application service provider who will know who provide it to, when and in what format. Those conditions and requirements are not specified in this document, but left to jurisdictions to determine and regulate at their discretion or to UNECE or other regulator to determine and regulate.

The architectural concept is the provision of ADRm data to legitimate enquirers, via an application service provider. The IVS shall provide the data that its on-board ADRm app requires, sending that data to the predetermined IPv6 address of the application service provider, via the ITS-station of the IVS.

The required data may be entirely collated and stored on-board the regulated vehicle 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 (for example, the TARV LDT data from the regulated vehicle and the consignment note/SAD/TD/Customs data from the application service provider database). Apart from the TARV LDT, a service provider may provide all of the current trip consignment data from its own database or a pointer to a database where it may be obtained (for example, one maintained by the operator) or may store some or all of the current consignment data in the IVS of the regulated vehicle 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) obtained from the regulated vehicle 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 closed

and a new communication session opened to a predetermined IPv6 address stored in the data pantry or app library of the IVS and the data sent to that address.

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

- a) direct enquiry to the originator of a consignment note or transport document (TD) [sometimes called the single administrative document (SAD)] for customs control purposes;
- b) broadcast to vehicles entering its territory or a specific location point in that territory;
- c) direct enquiry to a passing vehicle;
- d) a pre-programmed instruction.

In the case of

- a) direct enquiry to the originator of a consignment note or TD/SAD:

The application service provider, on receiving the request, shall, using a communication session between its ITS-station and the ITS-station on-board the regulated vehicle IVS, request an update of any predetermined data held in the data pantry 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 document.

- b) broadcast to vehicles entering its territory or a specific location point in that territory:

The ITS-station on-board the regulated vehicle IVS, on receiving the broadcast request, shall process an update of any predetermined data held in the data pantry 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 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 document.

- c) direct enquiry to a passing vehicle or ITS-station:

The ITS-station on-board the regulated vehicle IVS, 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), shall process an update of any predetermined data held in the data pantry 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 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 document. The form of direct interrogation request for ADR data is defined in ISO 15638-6:2014, Clause 7 as "GETADR". See ISO 15638-6 for details.

- d) pre-programmed instruction:

The ITS-station on-board the regulated vehicle (IVS), as a result of an instruction within the ADRm app 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 of the regulated vehicle. The regulated vehicle shall respond by passing its data to its application service provider. 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 document.

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

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

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

The application service provider is the party who contracts with the user to provide the ADRm service.

The user is the regulated vehicle operator and his/her driver.

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)	Sets requirements for mandatory and supported ADRm	Publishes specifications	ALL
		Obtains regulations	ALL: Establish regime and regulations ASP Register
		Appoints approval authority where appropriate	CA: Contracts, instructs, receive reports
Approval authority (CA)	Implements jurisdiction policy at equipment and service approval level	Approves IVS, application service instantiations	PSP: Approves IVS ASP: Approves application service
		Conducts Q of S maintenance to instruction of jurisdiction	
Prime service provider (PSP)	Responsibility for IVS	Installs and/or commissions IVS	CA: May apply to approve IVS Op: Installation
		Maintains IVS	Op: Maintains IVS
Application service provider (ASP)	Provides ADRm application service	Develops instantiation of ADRm application service	CA: Applies for approval of service
		Contracts with users	Op: Contracts
		Provides ADRm application service to users and jurisdiction	Op: Provides service IVS: Loads data IVS: Receives ADRm messages
Operator (Op)	Provides regulated vehicle	“Employs”/contracts drivers	Dr: Employs/contracts

Table 1 (continued)

Actor	Role	Activities	Interactions
	Uses regulated vehicle for commerce and logistics	Operates regulated vehicle	PSP: Contracts, receives service ASP: Contracts, receives service ASP: Provides consign-ment data
Driver (Dr)	Drives regulated vehicle to instruction of operator	Drives regulated vehicle	Op: to instructions

The prime service provider is responsible to properly install and maintain the equipment which triggers the application service.

The regulated vehicle operator (or owner) commissions the service and contracts with the application service provider, and possibly the prime service provider (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, or one of the legitimate enquirers defined in [10.2.3](#), generates a trigger for the supply of ADRm information via the IVS ITS-station.

The in-vehicle system uses its ITS-station to send the ADRm message and such of its associated data maintained on-board to a predetermined IPv6 address provided by the application service provider, together with the requested final destination address provided by the enquirer.

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

10.2.7 Role of ADRm service provider

The prime service provider installs and maintains the ADRm consignment data system and its triggering mechanism in the regulated vehicle.

The application service provider contracts with the user to provide the ADRm application service.

10.2.8 Role of ADRm user

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

The operator contracts with the application service provider to provide the service and pays any appropriate fees to the application service provider.

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

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

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

10.3 Sequence of operations for ADRm

The sequence of operations in respect of general ADRm shall be as shown in [Figure 3](#).

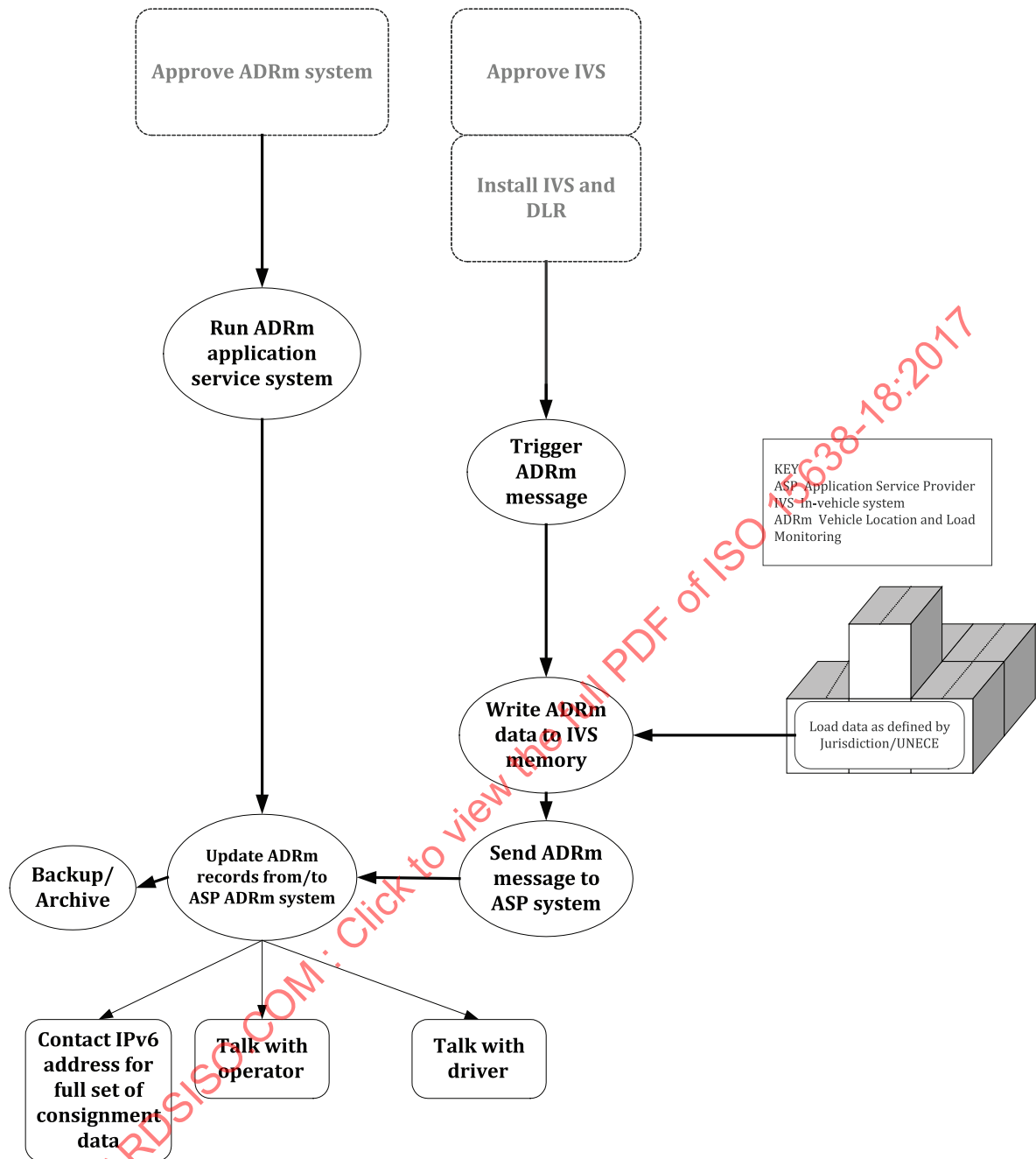


Figure 3 — Sequence of operations for ADRm

10.4 ADRm naming content and quality

The process to obtain basic vehicle data (TARV LDT) data content shall be as defined in ISO 15638-6:2014, 8.3 and ISO 15638-5.

10.5 Specific ADRm data naming content and quality

ADR consignment data shall be determined as required by regulations of the jurisdiction 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 [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 shall be responsible to define its requirements for its variant of the ADRm application service, obtain any legislation and/or regulations and define the procedure for an application service provider to gain approval for its instantiation of the ADRm application service.

10.6.2 ADRm SE2: Request system approval

The application service provider shall seek approval for its instantiation of the ADRm application service from the approval authority (regulatory) in accordance with the regime established by the jurisdiction.

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

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

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

It is a prerequisite for any potential vehicle operator opting or being required to sign up for the ADRm application service that its regulated vehicles are equipped to provide the consignment 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.

If the jurisdiction 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 ADRm application service provider, who may choose to maintain some or all of the information in its application service system (rather than on-board the regulated vehicle).

The ADRm data concept elements agreed with UNECE (in process) are provided in [Table 2](#).

It is further required that there is a maintenance contract with an approved service provider 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 in respect of the provisions of this document.

10.6.5 ADRm SE5: User contracts with application service provider

The user (operator) shall contract with an application service provider who offers an approved ADRm application service to provide the ADRm 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 ADRm app software into the TARV-equipped regulated vehicles of the operator.

10.6.7 ADRm SE7: Recording of vehicle consignment data

The on-board ADRm app shall create a file, type:ADR [ADR file] within this specification named <ADR><YYMMDDhhmm><vehicle registration number>.

Prior to the commencement of each journey, the application service provider shall establish a communications session with the in-vehicle system and update the data content of the ADR file with one of the following options:

- Schema (A): current URL link address to consignment data (Schema A), or
- Schema (B): consignment data (Schema B).

At the start of each journey, the ADRm app held in the library of the IVS shall be initiated.

During the journey, the on-board ADRm app in the IVS shall update the ADRm file with the following data:

```
<IVS ID>,  
<VehicleLocation>,<Schema identifier><ConsignmentData (Schema A or Schema B)>  
<IVS ID>  
<end>
```

NOTE The definition of “location” in ISO 15638-5:—, 9.2.4 includes location, UTC time and direction of travel. Vehicle direction of travel shall be calculated as specified in ISO 15638-5:—, 8.3.12.

10.6.8 ADRm SE8: ADRm Trigger

The points of demand for ADRm data will vary from jurisdiction to jurisdiction, or requirements of UNECE regulation, or requirements of the contract between the operator and the application service provider. Those conditions and requirements are not specified in this document, but are left to jurisdictions to determine and regulate at their discretion, or UNECE or other regulator to determine and regulate. The generation of and submission to the application service provider of ADRm data may be a result of an instruction within the ADRm app 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.

In the event that, from whatever cause, during the journey, an ADRm consignment data request is received, the following SEs shall ensue.

10.6.9 ADRm SE9: Contact predetermined IPv6 address

The IVS shall then use the on-board ITS-station to contact an ITS-station of the application service provider to deliver the ADRm consignment 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, 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, 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 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 shall then contact the predetermined IPv6 address to obtain full detail of the consignment and any associated ADR data where appropriate.

10.6.11 ADRm SE11: “Interrogated” request for ADR data

An interrogating ITS-station shall request ADR-specific data as determined in ISO 15638-6:2014, 7.1 and 8.1.2.

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

On receipt of the request, the IVS shall acknowledge the request with the appropriate acknowledgement defined in ISO 15638-6:2014, 8.3.5, which acknowledges that a request for ADR data has been received.

The IVS shall then close the communication session.

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

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.

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

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

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 document.

The application service provider, having ascertained the validity of the enquirer (this process will usually be automatic/semi-automatic against maintained checklists), shall then contact the enquirer in the agreed format (usually an IPv6 address or email address) as provided by the enquirer, providing the ADRm data to the enquirer. The means by which this is achieved is a matter for agreement between the parties and is outside the scope of this document.

The ADRm system of the application service provider 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 shall then contact the operator to notify them of the enquiry, providing the ADRm 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 (TARV LDT) data content shall be as defined in ISO 15638-6:2014, 8.3 and ISO 15638-5.

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

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

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](#).

Table 2 — ADRA consignment data Schema A — Link to URI

FILE TYPE		Format of file name	Note/Source	
ADRA	Mandatory	<ADRA><YYMMDD><hhmmss><vehicle registration number> Example ADRA 110316 070603 KV76WRR As: ADRA110316 070603KV76WRR	10.8.7 (ADR file)	
ADRA Data Concept element reference	Name	Type	Unit	Description
ADRA-0000	IVS ID	Mandatory	AN (9)	IVS identifier as defined in ISO 15638-5
ADRA-0001 version	ID	Integer	1 byte	ADRA Schema A data concept format version set to 1 to discriminate from later ADRA Schema A data concept formats. Later versions to be backwards compatible with existing versions. Systems receiving an ADRA Schema A data concept to support all standardized ADRA Schema A data concept versions, which are each uniquely identified using an ADRA Schema A data concept format version parameter which will always be contained in the first byte of all (current and future) ADRA Schema A Data concept versions.

Table 2 (continued)

ADRA-0002 numberOfADRtypes	Tanker or other vehicle type plus a 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 1111111 Concatenated as octet within range: 00000000 – 11111111
ADRA-0003 consignmentReference	ADR Consignment reference	Binary 3 Octets	000000000000000000000000 – 111111111111111111111111	Consignors unique reference number expressed as a binary value between 0 – 16,777,215
ADRA-0003 cargoInformationURI	PrintableString		M	Information about the cargo is available through the given URI (max. length: 80 char). The URI should follow the format '<scheme>://<host>[:<port>]/path[?query-string]', for example, see https://cargo.info.com/msdinfo?key=124 The information endpoint should respond in a standardized way, as referenced by cargo-InformationProtocol. That standardization is done to be set elsewhere and is outside the scope of this deliverable.
ADRA-0004 cargoInformation... ...Protocol	RELATIVE-OID		M	Relative object identifier designating the protocol to use to retrieve information through the above named URI.
ADRA-0005	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).

Table 2 (continued)

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-0006	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-0007	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/

Table 3 — ADRB consignment data Scheme B — Consignment Data

FILE TYPE		Format of file name	Notes/Source		
ADRB	Mandatory	<ADRB><YYMMDD><hhmmss><vehicle registration number> Example ADRB 110316 070603 KV76WRR As: ADRB110316 070603KV76WRR	10.8.7 (ADR file)		
ADRBData					
	ADRB-0000	IVS ID	Mandatory	AN (9)	IVS identifier as defined in ISO 15638-5
a The Kemler Code is encoded in a defined type that takes the Kemler Code constraints into account.					

Table 3 (continued)

ADRB-0001	ID		M	ADRB Schema B data concept format version set to 1 to discriminate from later ADRB Schema B data concept formats Later versions to be backwards compatible with existing versions. Systems receiving an ADRB Schema B data concept to support all standardized ADRB Schema B data concept versions, which are each uniquely identified using an ADRB Schema B data concept format version parameter which will always be contained in the first byte of all (current and future) ADRB Schema B Data concept versions.
data				encoded as OCTET STRING
ADRB-0002 commercialVehicleType	ENUM		M	The supported types are: — unknown; — tanker, one compartment; — tanker, more compartments; — truck, (stukvracht).
ADRB-0003 consignorPhone	NumericalString		M	Consignor's contact telephone number or telephone number displayed on goods container as contact number in case of emergency. The number should be specified as international number, thus including the country- and area code (without zero)
ADRB-0004 alarmInfo			0	Information about sensors present is encoded. Each sensor is optional and should be left out if not present. If a sensor is generating an alarm, its value should be set to true. If a sensor is available but not generating an alarm its value is false. 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 MSD 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.
leakageAlarm	BOOLEAN		0	True if leakage has been detected
fireAlarm	BOOLEAN		0	True if fire has been detected
highTempAlarm	BOOLEAN		0	True if high temperature has been detected
lowTempAlarm	BOOLEAN		0	True if low temperature has been detected
shockAlarm	BOOLEAN		0	True if shock has been detected
highPressureAlarm	BOOLEAN		0	True if high pressure has been detected
lowPressureAlarm	BOOLEAN		0	True if low pressure has been detected
orientationAlarm	BOOLEAN		0	True if abnormal orientation has been detected
otherAlarm	BOOLEAN		0	True if any other alarm was raised
ADRB-0005 - ADRB-0011 goodsADR			0	Up to 7 goods can be fully defined.
definedGoodsADR[1]			0	Each defined good has its own container with:
ADRB-000n-01 cargoUNCode	INTEGER		M	UNCode (max. value: 9999)

^a The Kemler Code is encoded in a defined type that takes the Kemler Code constraints into account.

Table 3 (continued)

	ARDB-000n-02	KemlerCode ^a		M	Kemler Code of cargo, up to 4 digits	
	kemlerCode					
	ARDB-000n-03	INTEGER		M	Package group (0, 1, 2 or 3)	
	packageGroup					
	ARDB-000n-04	INTEGER		M	The quantity of the cargo. Possible values are: 0: empty but uncleaned, 1 – 98: the quantity as expressed 99: 99 tonnes / 99 m3 or more	
	quantity					
	ARDB-000n-05	BOOLEAN		M	True: quantity is given in tonnes False: quantity is given in m ³ (rounded up)	
	quantityInTonnes					
	ARDB-000n-06	BOOLEAN		M	True: quantity is gross weight/volume	
	quantityIsGross					
	definedGoodsADRB [2]				O	
	cargoUNCode	See above				
kemlerCode						
packageGroup						
quantity						
quantityInTonnes						
quantityIsGross						
definedGoodsADRB [3]				O		
...						
definedGoodsADRB [7]						
ADRB-00012	INTEGER		M	Number of ADR goods in the vehicle not fully defined in this section. Possible values: 0: no other ADR goods in vehicle, 1-9: specified number of other ADR goods in vehicle 10: 10 or more ADR goods in vehicle 15: unknown number of (other) ADR goods in vehicle		
numberOfUndefined...						
...GoodsADR						
ADRB-00013	Mandatory	<ADRB><YYMMDD><hhmmss><vehicle registration number> Example ADRB 110316 070603 KV76WRR As: ADRB110316 070603KV76WRR			10.8.7 (ADR file)	

^a The Kemler Code is encoded in a defined type that takes the Kemler Code constraints into account.

Table 3 (continued)

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
ADRB 00014	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
ARDB-0015	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/
^a The Kemler Code is encoded in a defined type that takes the Kemler Code constraints into account.				

10.8 ADRm application service-specific provisions for quality of service

Shall be at the determination of UNECE.

The integrity of the data are important and other sensors, as well as parameters, may then be required based on the approaches and techniques used to provide assurance of the quality of the data. The generic quality of service provisions 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. However, in defining such requirements, jurisdictions shall, wherever possible, use performance based or functionally specifications 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](#) 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 the 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 in [9.12](#).

11 Declaration of patents and intellectual property

This document 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 specified within this document 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 of the applications services defined in this document 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 and its regulations for instantiation in this respect.

STANDARDSISO.COM : Click to view the full PDF of ISO 15638-18:2017

Annex A (informative)

Independent testing of the protocols defined in this document

A.1 Objectives

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

Instigation

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

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

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

Recipient address sends acknowledgement.

IVS closes the communication on receipt of acknowledgement.

Interrogation

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

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

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

On receipt, it acknowledges the request (ACK).

It closes the communication.

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

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

Recipient address sends acknowledgement.

IVS closes the communication on receipt of acknowledgement

These scenarios shall be tested using each of 2G, 3G, WiFi, 5,9 GHz (IEEE802.11) using the same data.

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

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

Preconditions, assumptions and simulations

The system under test (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 they 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, Mesh WiFi, 5,9 GHz (IEEE 802.11p).

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

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

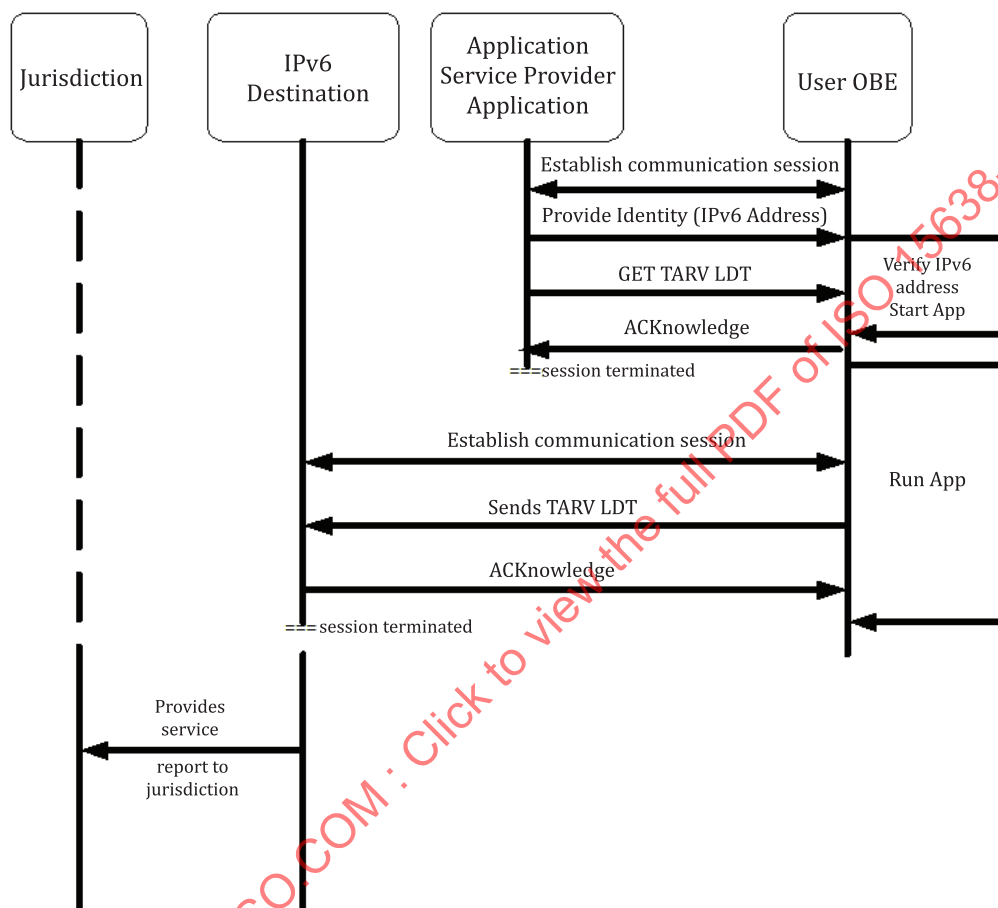


Figure A.1 — Communications sequences to obtain TARV LDT

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 20.2 — 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: ADR110316 070603KV76WRR	19.4.7 [Vehicle/location/consignment monitoring file (ADR file)]	
Number	Data concept name	Use	Format	Notes/Source
ADRm-0000	IVS ID	Mandatory	AN (9)	IVS identifier as defined in ISO 15638-5
ADRm Data Concept element reference	Name	Type	Unit	Description
ADRm-0001	OID	Integer	1 byte	ADRm data concept identifier binary value 1000010 identifying ADRm Schema A (until allocated a revised OID from a central register)

Table 20.2 (continued)

ADRM-0002	ID	Integer	1 byte	ADRM Schema A data concept format version set to 1 to discriminate from later ADRm Schema A data concept formats Later versions to be backwards compatible with existing versions. Systems receiving an ADRm Schema A data concept to support all standardised ADRm Schema A data concept versions, which are each uniquely identified using an ADRm Schema A data concept format version parameter which will always be contained in the first byte of all (current and future) ADRm Schema A Data concept versions.
ADRM-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 1111111 Concatenated as octet within range: 00000000 – 11111111
ADRM-0004	ADR Consignment reference	Binary 3 Octets	000000000000000000000000 - 111111111111111111111111	Consignors unique reference number expressed as a binary value between 0 – 16,777,215

Table 20.2 (continued)

ADRM-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 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 ADRm-0001 – ADRm-0005 data is supplied, no other information is required, but may be provided as backup. If ADRm—0005 data is not supplied the following data concept elements are mandatory.
-----------	--	--------------------------	--------------	---

Table 20.2 (continued)

ADRM-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 prioritized 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 1 000 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 00000x0000000x0000000x0000000x000 0000x0000000x0000000x0000000x0000 000x0000000x0000000x0000000x00000 00x0000000x0000000x00 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
-----------	---	-----------------------	-----------	---

Table 20.2 (continued)

ADRM-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 R1 = reserved for future use Z = Other alarm 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 ADRm 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.
ADRM-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,binary1111111111111111111101, 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,binary1111111111111111111101, 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 shall be tested for each of) several wireless media defined below. The IVS of a vehicle internally triggers a requirement to send a packet of data to a predetermined destination IPv6 (Internet) address. The vehicle sends the data file to the predetermined destination IPv6 (Internet) address. 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 they are copied from the base standards.) CALM and media choice are assumed and not s.u.t. The vehicle is equipped with wireless communications that enable it to make communications using 2G, 3G, WiFi, 5,9 GHz (IEEE 802.11p) The means to trigger the sending of a message from the vehicle is a function of IVS design, not s.u.t., therefore may be simulated The destination address is intended to be an IPv6 address, but may be simulated with an IPv4 address as this is an Internet issue, not s.u.t.		
Stimulus and expected behaviour			
Test point	Tester action	Pass condition	
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,binary11111111111111111111111101, scheme:// domain:port/path?query_string#fragment_id,11234020, 11235005, 11236005, 11237005, 11238005,00000000,binary10111001, D0o3M45S> <END>	File sent and arrives correctly at destination
10.1.1.3	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 T H E N C T P P A S S ELSE CTP FAIL
TEST RESULT: CTP 10.1.1		PASS/FAIL	Date: 29th June 2012
Signature/initials		PASS	 k4, MIRA, Watling St, Nuneaton, Warwickshire, CV10 0TH, UK Tel: +44 (0)7730 922 810 Web: www.innovits.com/advance

STANDARDSISO.COM : Click to view the full PDF of ISO 15638-18:2017

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. It opens a new communication session using one of (and must be tested for each of) several wireless media defined below. It sends the data file 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 they are copied from the base standards.) CALM and media choice are assumed and not s.u.t. The vehicle is equipped with wireless communications that enable it to make communications using 2G, 3G, WiFi, 5,9 GHz (IEEE 802.11p) The means to trigger the sending of a message from the vehicle is a function of IVS design, not s.u.t., therefore may be simulated. The destination address is intended to be an IPv6 address, but may be simulated with an IPv4 address as this is an Internet issue, not s.u.t.		
Stimulus and expected behaviour			
Test point		Tester action	Pass condition
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 AC-Knowledgement <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, 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
10.1.2.6	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 2012
Signature/initials			
		PASS	 k4, MIRA, Watling St, Nuneaton, Warwickshire, CV10 0TU, UK Tel: +44 (0)7730 922 810 Web: www.innovits.com/advance

CTP 10.1.3 Interrogated ADR — Dangerous goods monitoring using 5,9 GHz 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 5,9 GHz (IEEE 802.11p) wireless interrogation requesting a packet of data. On receipt it acknowledges the request (ACK). It closes the communication. It opens a new communication session using 2G or 3G. It sends the data file 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 they are copied from the base standards.) CALM and media choice are assumed and not s.u.t. The vehicle is equipped with wireless communications that enable it to make communications using 2G, 3G, WiFi, 5,9 GHz (IEEE 802.11p). The means to trigger the sending of a message from the vehicle is a function of IVS design, not s.u.t., therefore may be simulated. The destination address is intended to be an IPv6 address, but may be simulated with an IPv4 address as this is an Internet issue, not s.u.t.		
Stimulus and expected behaviour			
Test point		Tester action	Pass condition
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 AC-Knowledgement <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

10.1.3.6	6	IVS sends file named <ADR110316 070603KV76WRR> <START> < D0o3M45S, 1,1,binary00000101,binary1111111111111111111101, scheme://domain:port/path?query_string#fragment_id,11234020, 11235005, 11236005, 11237005, 11238005,00000000,binary10111001,D0o3M45S><END>	File sent and arrives correctly at destination
10.1.3.7	7	Destination address sends ACK <ADX>	
10.1.3.8	8	IVS receives ACK <ADX>	File received and ACK <ADX> sent
10.1.3.9	9	IVS closes communication session	Communication session closed
			If ALL individual pass conditions listed in this column above have been met THEN CTP PASS ELSE CTP FAIL
TEST RESULT: CTP 10.1.3		PASS/FAIL	Date: 29th June 2012
Signature/initials		 PASS	
		 k4, MIRA, Watling St, Nuneaton, Warwickshire, CV10 0TU, UK Tel: +44 (0)7730 922 810 Web: www.innovits.com/advance	

CTP 10.2.1 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 shall be tested for each of) several wireless media defined below. The IVS of a vehicle internally triggers a requirement to send a packet of data to a predetermined destination IPv6 (Internet) address. The vehicle sends the data file to the predetermined destination IPv6 (Internet) address. 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 they are copied from the base standards.) CALM and media choice are assumed and not s.u.t. The vehicle is equipped with wireless communications that enable it to make communications using 2G, 3G, WiFi, 5,9 GHz (IEEE 802.11p). The means to trigger the sending of a message from the vehicle is a function of IVS design, not s.u.t., therefore may be simulated. The destination address is intended to be an IPv6 address, but may be simulated with an IPv4 address as this is an Internet issue, not s.u.t.		
Stimulus and expected behaviour			
Test point		Tester action	Pass condition
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, AaaS,0,0,xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx,128..16511,1G1JF27W8GJ178227,000000 , 1 2 9 7 3 3 9 4 9 9 , 0 x 0 A 5 D 3 7 7 0 , 0 x - 027E2938,0000,8,0,123,1,000,000,010326,UK,- Peter Jones,01,02,03a,h1,120325,010326 124538,Peter Jones 01,02,h1, 120325, ID0o3M45S > <END>	File sent and arrives correctly at destination