INTERNATIONAL STANDARD

ISO 15638-3

First edition
2013-06-15

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

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

Partie 3: Exigences de fonctionnement, modes opératoires de l'Autorité d'approbation et dispositions d'exécution pour les fournisseurs de services réglementés

Reference number
ISO 15638-3:2013(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

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 Penalties and Levies (VMC)*

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 varies from country to country, but include vehicle charging, digital tachograph, electronic on-board recorders, on-board mass monitoring, vehicle access monitoring, hazardous goods tracking and e-call. Additional applications with a regulatory impact being developed include, fatigue management, speed monitoring and heavy vehicle charging based on mass, 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 suite of standards deliverables is required to describe and define the framework and requirements so that the in-vehicle system and *back office* [4.7] systems can be commercially designed in an open market to meet common requirements of jurisdictions.

This suite of standards addresses and defines the framework for a range of cooperative telematics applications for *regulated commercial freight vehicles* [4.25] (such as access monitoring, driver fatigue management, speed monitoring, on-board mass monitoring and charging). The overall scope includes the concept of operation, legal and regulatory issues, and the generic cooperative provision of services to *regulated commercial freight vehicles* [4.25] using an on-board ITS platform. The framework is based on a (multiple) service provider oriented approach provisions for the *approval authority* [4.4] approval and auditing of *service providers* [4.27].

This suite of standards deliverables will:

- provide the basis for future development of cooperative telematics applications for *regulated commercial freight vehicles* [4.25]. 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 commercial freight vehicles* [4.25].
- a business architecture based on a (multiple) service provider oriented approach
- address legal and regulatory aspects for the *approval authority* [4.4] approval and auditing of *service providers* [4.27].

This suite of standards deliverables 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.

NOTE 1: The definition of what comprises a ‘regulated’ vehicle is regarded as an issue for national decision, and may vary from country to country. This suite of standards deliverables 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 may vary from country to country. This suite of standards deliverables does not impose any requirements on nations in respect of which services for regulated vehicles countries will require, or support as an option, but will provide standardised sets of requirements descriptions for identified services to enable consistent and cost efficient implementations where implemented.

NOTE 3: Cooperative ITS applications, in this context, are defined as the use of an in-vehicle ITS platform to meet both commercial and regulatory needs from a (functionally) single on-board platform.

This part of the ISO 15638 family of standards deliverables provides specifications for operating requirements, *approval authority* [4.4] approval procedures and enforcement provisions for the providers of regulated services.

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

1 Scope

This part of ISO 15638 defines provisions to enable monitoring and enforcement of regulated vehicles and *approval authority* [4.4] approval procedures, specifically:

a) Definition of the roles and responsibilities of key entities: user, service provider, jurisdictions, and 'Approval Authorities'
b) Operating requirements ensuring that a cooperative in-vehicle platform can deliver a range of services to both government and industry through open standards and competitive markets
c) Basic service requirements for *service providers* [4.27] that are generic and independent of a specific application
d) Requirements for the *approval authority* [4.4] approval of *IVS*s and *service providers* [4.27]
e) Legal, regulatory, and enforcement aspects.

The scope includes the requirements for the *IVS* capability in the vehicle, and the definition of the roles of the *service provider* [4.27], 'Communications Service Provider', *IVS installer* [4.16], '*IVS maintainer* [4.17] ', *approval authority* [4.4], and the *user* [4.31], for cooperative telematics applications for *regulated commercial freight vehicles* [4.25].

NOTE The specific 'certification' or 'approval' procedures for specific application services are a matter for the jurisdiction and are outside the scope of this (or any) part of ISO 15638. However, approval authorities and jurisdictions are recommended to use the guidance of ISO 17000 and ISO guide 65 when developing and implementing such procedures.

2 Conformance

This part of ISO 15638 defines requirements for provisions to enable monitoring and enforcement of regulated vehicles and *approval authority* [4.4] approval procedures within the *TARV* context, and has no specific conformance tests defined herein. Principal requirements for conformance tests are specified in 14, but the tests themselves are not elaborated. Some aspects defined within may have conformance tests defined in other parts of ISO 15638.

Conformance declarations for the various parts of a CALM-compliant system shall be based on the relevant CALM-related International Standards that are normatively referenced in ISO 15638-2.

Conformance to any other International Standard or specification referenced in this part of ISO 15638 shall be ascertained according to the requirements of the referenced deliverable.

Conformance to this part of ISO 15638 is therefore a matter of self-declaration of compliance, or by submission to a test house to ascertain that the provisions of the clauses of this part of ISO 15638 have been adhered to.

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 11519-1 *Road vehicles — Low-speed serial data communication — Part 1: General and definitions*

ISO 11519-2 *Road vehicles — Low-speed serial data communication — Part 2: Low-speed controller area network (CAN)*

ISO 11519-3 *Road vehicles — Low-speed serial data communication — Part 3: Vehicle area network (VAN)*

ISO 11898-1 *Road vehicles — Controller area network (CAN) — Part 1: Data link layer and physical signalling*

ISO 11898-2 *Road vehicles — Controller area network (CAN) — Part 2: High-speed medium access unit*

ISO 11898-3 *Road vehicles — Controller area network (CAN) — Part 3: Low-speed, fault-tolerant, medium-dependent interface*

ISO 11898-4 *Road vehicles — Controller area network (CAN) — Part 4: Time-triggered communication*

ISO 11898-5 *Road vehicles — Controller area network (CAN) — Part 5: High-speed medium access unit with low-power mode*

ISO/TR 12859 *Intelligent transport systems — System architecture — Privacy aspects in ITS standards and systems*

ISO 14816 *Road transport and traffic telemantics — Automatic vehicle and equipment identification — Numbering and data structures*

ISO 17262 *Intelligent transport systems — Automatic vehicle and equipment identification — Numbering and data structures*

ISO 26683-2 *Intelligent transport systems — Freight land conveyance content identification and communication — Part 2: Application interface profiles*

SAE J1939 *Recommended Practice for a Serial Control and Communications Vehicle Network*

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
actor
coherent set of roles that users of an entity can play when interacting with the entity

NOTE An actor may be considered to play a separate role with regard to each use case with which it communicates. In the metamodel, Actor is a subclass of Classifier. An Actor has a Name and may communicate with a set of UseCases, and, at realization level, with Classifiers taking part in the realization of these UseCases. An Actor may also have a set of Interfaces, each describing how other elements may communicate with the Actor.

4.2
applicant
party which has applied for approval authority [4.4] approval as a service provider [4.27]

4.3
application service
service provided by a service provider accessing data from the *IVS* of a regulated commercial freight vehicle via a wireless communications network

4.4
approval authority
organization (usually independent) which conducts approval and ongoing *audit* [4.5] for *service providers* [4.27]

4.5
audit
review of a party's capacity to meet, or continue to meet, the initial and ongoing *certificate of approvals* [4.11] as a *service provider* [4.27]

4.6
auditor
person or organization approved as an auditor by an *approval authority* [4.4]

4.7
back office
generic term for the computing and communication facilities of a *service provider* [4.27] or an *approval authority* [4.4] or *jurisdiction regulator* [4.16]

4.8
basic vehicle data
data that shall be maintained/provided by all *IVS* (regardless of *jurisdiction* [4.18])

4.9
CAN bus
network designed for use in automotives

NOTE 1 It uses a single terminated twisted pair cable; is multi master; maximum signal frequency used is 1 Mbit/sec; length is typically 40M at 1Mbit/sec up to 10KM at 5Kbits/sec; it has high reliability with extensive error checking; typical maximum data rate achievable is 40KBytes/sec; maximum latency of high priority message <120 µsec at 1Mbit/sec.

NOTE 2 CAN is unusual in that the entities on the network, called nodes, are not given specific addresses. Instead, it is the messages themselves that have an identifier which also determines the messages' priority. For this reason there is no theoretical limit to the number of nodes although in practice it is ~64.

4.10
certification
formal affirmation that an *applicant* [4.2] has satisfied all the requirements for appointment as a *service provider* [4.27]

4.11
certificate of approval
written agreement made between an *approval authority* [4.4] and a *service provider* [4.27]

NOTE An *approval authority* [4.4] approval agreement recognizes the fact that a *service provider* [4.27], having satisfied the '*approval authority's'* requirements for appointment as a *service provider,* is appointed in that capacity, and sets out the legal obligations of the parties with respect to the on-going role of the *service provider*.

4.12
clear-down
call clear-down
termination of call and freeing up of communication channel

4.13
core application data
basic vehicle data [4.8] plus any additional data required to provide an implemented regulated application service

4.14
entity
something that exists independently

4.15
in-vehicle system
IVS
equipment on-board a vehicle that can provide the specified telematics functionality of the in-vehicle system

NOTE This equipment may comprise a single physical *on-board unit* [4.20], or a telematics functionality within one or multiple equipments on-board a vehicle

4.16
IVS installer
actor (4.1) who installs *IVS* on behalf of the vehicle manufacturer or the initial *prime service provider* [4.21]

4.17
IVS maintainer
actor [4.1] who installs *IVS* on behalf of the *prime service provider* [4.21]

4.18
jurisdiction
government, road or traffic authority which owns the *regulatory applications* [4.23]

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

4.19
jurisdiction regulator
regulator
agent of the jurisdiction appointed to regulate and manage *TARV* within the domain of the jurisdiction

NOTE This may or may not be the *approval authority* [4.4].

4.20
on-board unit
OBU
integrated telematics unit installed on-board which provides specified in-vehicle system functionality

4.21
prime service provider
service provider who is the first contractor to provide *regulated application services* [4.24] to the regulated commercial freight vehicle, or a nominated (by the user) successor on termination of that initial contract

NOTE The prime service provider is also responsible to maintain the installed *IVS*; if the *IVS* was not installed during the manufacture of the vehicle the prime service provider is also responsible to install and commission the *IVS*s.

4.22
prime user
principal *user* [4.31] of the *TARV* services

4.23
regulated/regulatory application
approval arrangement utilised by *jurisdictions* [4.18] for granting certain categories of commercial vehicles rights to operate in regulated circumstances subject to certain conditions

NOTE Each *jurisdiction* may use their own terminology including, but not limited to, permit, application, scheme, concession, exemption, gazettal and notice.

4.24
regulated application service
TARV application service that is mandated by a regulation imposed by a *jurisdiction* [4.18], or is an option supported by a *jurisdiction*

4.25
regulated commercial freight vehicle
vehicle designed to haul commercial freight that is subject to regulations determined by the *jurisdiction* [4.18] as to the use of the road system of the *jurisdiction* and the compliance with specific regulations for that class of commercial freight vehicle, often through the provision of information via *TARV*

4.26
secondary user
other user(s) of the *TARV* services who are not the *prime user* [4.22]

4.27
service provider
party which is certified by an *approval authority* [4.4] as suitable to provide regulated or commercial ITS services

4.28
tamper/tampering
conduct towards *IVS* or a *service provider's* [4.27] system which is intended to prevent the *IVS* or the *service provider's* system from functioning correctly including, but not limited to, preventing accurate recording of data or allowing unauthorized modifications to data

4.29
type approved
equipment or system approved by a process determined by the *jurisdiction regulator* [4.19]

4.30
unique vehicle identification
unambiguous identification of the vehicle

4.31
user
individual or party that enrols in and operates within a regulated or commercial *application service* [4.3]

EXAMPLE Driver, transport operator, freight owner, etc.

5 Symbols (and abbreviated terms)

CISPR
Comité International Spécial des Perturbations Radioélectriques

CAD
core application data

GNSS
global navigation satellite system

HMI
human/machine interface

IVS

In-vehicle system [4.15]

LDT
local data tree

MEMS
micro electro mechanical system

OBU
on-board unit [4.20]

OEM
original equipment manufacturer

RAM
random access memory

ROM
read only memory

TARV
telematics applications for *regulated commercial freight vehicles* [4.25]

TID
trailer identification device

6 General overview and framework

ISO/TS 15638-1 provided a framework and architecture for *TARV*. It provided a general description of the roles of the actors [4.1] in *TARV* and their relationships.

To understand clearly the *TARV* framework the reader is referred to ISO/TS 15638-1.

Figure 1 shows the role model conceptual architecture of ISO/TS 156638-1 showing the key actors [4.1] and their relationships.

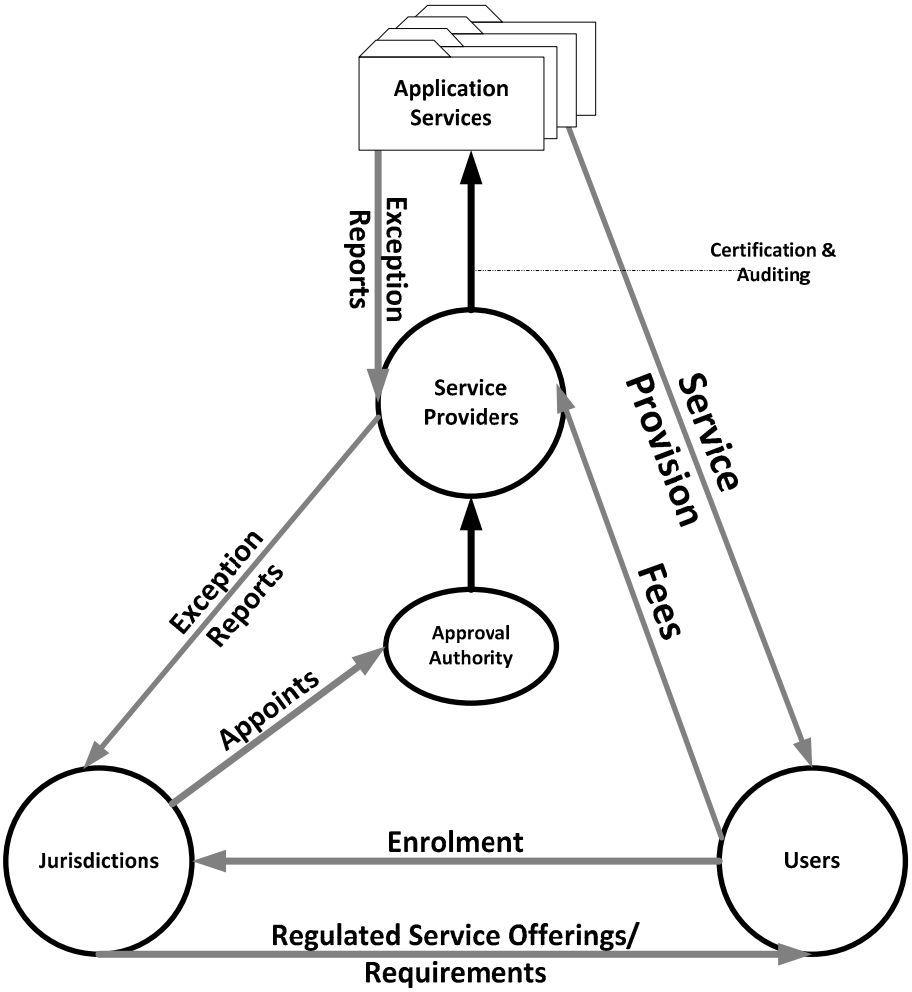

Figure 1 — Role model conceptual architecture
(Source: ISO 15638-1)

ISO 15638 provides a suite of standards deliverables addresses and defines the framework for a range of cooperative telematics applications for *regulated commercial freight vehicles* [4.25] (such as access monitoring, driver fatigue management, speed monitoring, on-board mass monitoring and charging). The overall scope includes the concept of operation, legal and regulatory issues, and the generic cooperative ITS service platform. The framework is based on a (multiple) service provider oriented approach provisions for the *approval authority* [4.4] approval and auditing of *service providers* [4.27].

ISO 15638 is comprised of seven framework parts, and twelve application specific parts. The framework parts are:

- 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 4: System security requirements
- Part 5:Generic vehicle information
- Part 6: Regulated applications [Technical Specification]

- Part 7: Other applications

This part of ISO 15638-3 (Operating requirements, *approval authority* [4.4] procedures, and enforcement provisions for the providers of regulated services) provides both generic *approval authority* approval procedures and basic service requirements for *service providers* [4.27] that are generic and independent of a specific application.

(for example, shall have secure processing, shall have map-matching capability, shall keep records in a transparent and auditable way, shall read *IVS* data at defined intervals etc.). ISO 15638-3 (this part of ISO 15638) provides specifications for these issues.

ISO 15638-2 has provided specifications for communications aspects. ISO 15638-4 provides specifications for security issues.

Application service provision is in part provided by 'core *IVS* capabilities*'* and in part by requirements specific only to a regulated service application.

Examples of 'core *IVS* capabilities' includes aspects such as: shall have unique identifier, shall collect time and location data, shall have secure data processing and storage, shall be physically and environmentally robust, shall be able to communicate with the service provider etc.

ISO 15638-5 has defined the common data concepts for vehicle information.

Jurisdictions [4.18] may develop and make available schemes, permits, applications, notices, concessions, exemptions or gazettals (variously named in accordance with individual jurisdictional practice) which provide improved access to the road network and utilise *TARV* application services as a compliance solution. Other *jurisdictions* [4.18] will support some *TARV* application services as voluntary services, but not support others; some a combination of required and 'supported but not required' application services. The specifications in this part of ISO 15638 are designed to enable this flexibility, but provide specifications that enable *IVS* designers and manufacturers to design common equipment.

7 Requirements

The requirements of this part of ISO 15638 are determined in Clauses 8 to 14.

8 DEFINITION OF THE ROLES AND RESPONSIBILITIES OF KEY ACTORS

8.1 Generic service requirements

ISO/TS 15638-1 provided a framework and architecture for *TARV.* It provided a general description of the roles of the actors [4.1] in *TARV* and their relationships. To understand clearly the *TARV* framework the reader is referred to ISO/TS 15638-1. This Clause provides definition of the responsibilities of each of the actors described in ISO/TS 15638-1 in respect of the fitting, maintenance and provision use of *IVS, TID,* and the provision and availability of generic data and the provision of application services.

Security aspects are dealt with in ISO 15638-4 *TARV* System security requirements.

Generic vehicle information and data aspects are specified in ISO 15638-5.

Specific application service provision aspects are defined in ISO 15638-6 '*TARV* Regulated applications', and ISO 15638-7 '*TARV* Other applications'.

The framework and architecture for the roles of the actors [4.1] in *TARV* are described in ISO 15638-1. The Clauses and subClauses of this part of ISO 15638 specify the responsibilities of these actors.

8.2 User

Firstly, it is important to be clear that, as the objective of *TARV* is application service provision, the *user* [4.31] is the *user* of the application service(s).

ISO 15638-1 identifies that are a number of possibilities for the role of the *user* [4.31] of the application service

- Owner of the vehicle
- Operator of the vehicle
- Driver
- Owner of the load
- Other support functions.

ISO TS 15638-1 concludes that:

'The user may therefore in some circumstances be the operator of the vehicle, and in other circumstances, be the driver of the vehicle. Regulated application system specifications must therefore specify and define who the user of the regulated application system is deemed to be.

It is true to say that the user is most commonly the operator of the regulated vehicle.

In cases where the user is defined as the driver, the operator of the regulated vehicle should determine in the contract employing the driver that the driver will use the in-vehicle platform to undertake all regulated application services including driver specific services, and that the driver will provide all information in his possession that are required by the regulated application services.

As the driver is driving because he or she has been instructed to do so by the operator, any requirements that relate specifically to the driver being provided with an application service (such as reporting tachograph data or other driver related data required by the regulator) he or she is performing this duty as part of the fulfilment of his contract with the vehicle operator to drive the vehicle on any specific journey. The 'prime' user of the application service is therefore always the vehicle operator, and the driver is a secondary user, even if any regulatory action, if taken, may be taken directly against the driver (much as he or she is also required to obey speed limits, drive in a safe manner, and could be prosecuted directly if he or she is in violation).'

8.2.1 User specification US1: 'Prime User'

The *prime user* [4.22] of the application service shall be the operator of the regulated commercial freight vehicle.

8.2.2 User specification US2: 'Secondary User'

The driver shall be considered a *secondary user* [4.26] when fulfilling regulatory requirements for the provision of driver information and data to the regulator or his agent.

8.2.3 User specification US3: Mandatory application service enrolment

Users shall be required to enrol in mandatory applications for *regulated commercial freight vehicles* [4.25], as determined by regulations of the jurisdiction, and offered by a *service provider* [4.27], and this may vary from *jurisdiction* [4.18] to *jurisdiction.*

8.2.4 User specification US4: Voluntary application service enrolment

8.2.4.1 Voluntary commercial application service enrolment

Users may, at the discretion of the user, choose to enrol into a voluntary commercial application service for *regulated commercial freight vehicles* [4.25] using the *IVS,* offered by an application *service provider* [4.27], and this may vary from *jurisdiction* [4.18] to *jurisdiction*.

8.2.4.2 Voluntary regulated application service enrolment

Users may, at the discretion of the user, choose to enrol into a voluntary *regulated application service* [4.24] for *regulated commercial freight vehicles* [4.25] using the *IVS*, offered by the *jurisdiction* [4.18], and this may vary from *jurisdiction* to *jurisdiction*.

8.2.5 User specification US5: Service provider engagement

Upon the enrolment of an application, the *user* [4.31] shall engage a *service provider* [4.27] to start operations under the enrolled application and shall pay any required fees to/through the *service provider* in accordance with the terms of the contract between the *service provider* and the *user.*

8.3 Service provider

8.3.1 Service provider specification SP1 : Service provider definition

A *regulated application* [4.23] *service provider* [4.27] shall be an *actor* [4.1] that provides a *regulated application service* [4.24] for *regulated commercial freight vehicles* [4.25].

8.3.2 Service provider specification SP2: Service provider 'Approval Authority' requirement

A *service provider* [4.27] that provides a *regulated application service* [4.24] for *regulated commercial freight vehicles* [4.25] shall be certified as 'approved' by the *approval authority* [4.4] (of the *jurisdiction regulator* [4.19]), in a manner determined by the jurisdiction, as suitable to provide regulated or commercial ITS services to *regulated commercial freight vehicles* [4.25].

8.3.3 Regimes for regulated application service provision

The application *service providers* [4.27] may be provided or subcontracted by the jurisdiction, but are more likely to be by the use of third party commercial enterprises which provide ITS services.

NOTE It is expected that in many cases, and particularly in the early years, the *service providers* [4.27] will also install the *IVS* into the users' vehicles, although in the future the *IVS* platforms may be an option for installed equipment at manufacture, or may be mandated equipment at manufacture, according to the jurisdiction, and separation of the provision and maintenance of equipment and service provision may also be possible if allowed by the *jurisdiction* [4.18].

In the open market context, application *service providers* [4.27] are third party commercial enterprises which provide ITS services based on the applications using a wireless communications link between the application *service provider* [4.27] and the vehicle. Where a *user* [4.31] employs a single *service provider* to provide all of the regulated services (and possibly some additional commercial services) it may be expected that the *service providers* may also install and maintain *IVSs* in the users' vehicles. See *IVS installer* [4.16] and the *IVS maintainer* [4.17], as essential sub-*actor* [4.1] roles in the architecture.

NOTE The choices may not necessarily be only those of the *user* [4.31]. In some jurisdictions, in order to maintain control and assure quality of service to its *regulated application services* [4.24], and because of issues of liability, a *jurisdiction* [4.18] may limit the option of the *user t*o that of a single or limited number of *service providers* [4.27].

See ISO 15638-1 for further description of the regimes for application *service providers* [4.27].

8.3.4 Service provider specification SP3: Application service definition

Application services for *regulated commercial freight vehicles* [4.25], whether regulated or commercial, shall be clearly defined in terms of the requirements on the service provider, and the provision of information and data to the *jurisdiction* [4.18] and its agents and to the *user* [4.31].

NOTE Some guidelines and specification or application services are provided in 15638-6 and 15638-7.

8.3.5 Service provider specification SP4: Service provision

The *service provider* [4.27] shall provide the application service, interacting wirelessly with the vehicle to collect relevant data from the *IVS*, process the data and provide the *jurisdiction* [4.18] reports according to the requirements of the application service provided (as specified by the *jurisdiction* in respect of *regulated application services* [4.24]), and provide relevant data to the *user* [4.31] in accordance with its contract with the *user*.

NOTE In most cases, although collecting data from the vehicle constitutes a crucial part of the service provision, the end results are sorted and evaluated by and at the *service provider* [4.27] and communicated to the *jurisdiction* [4.18] (as demanded by the regulation) and to the *user* [4.31] (as agreed in the contract between the *service provider* and the user).

8.3.6 Service provider specification SP5: Service provider charging

The *service providers* [4.27] shall charge the users any fees for the service provided as agreed in the contract between the *user* [4.31] and the service provider, within the context of the agreement and contracts between the *jurisdiction regulator* [4.19] and the *service provider* for the provision of the regulated application service.

8.3.7 Service provider specification SP6: Service provider charging fees on behalf of jurisdiction regulator

The *service provider* [4.27] shall also collect fees from the *user* [4.31] as required by the regulation on behalf of the *jurisdiction regulator* [4.19] (for example fees for permits, road use payment, possibly even fees for violations) collecting these fees from the *user* [4.31] and forwarding these payments to the *jurisdiction* [4.18].

The responsibility for determination of such fees (or the scope within which the *service provider* [4.27] can set its fees) has to rest with the *jurisdiction* [4.18] and will depend on the legislation and regulation imposed by the *jurisdiction*.

8.3.8 Service provider specification SP7: Service provider transmission of data to the jurisdiction and/or its agents

Service providers [4.27] shall also transmit raw road usage data to the jurisdiction, as required by the regulation of the *jurisdiction* [4.18] but shall not provide any information relating to a specific vehicle, fleet of vehicles or driver other than that required by the regulations of the *jurisdiction*.

NOTE There are situations where government authorities and researchers require vehicle-specific data to fulfil specific purposes (research studies, special safety oversight programs, voluntary programs). This provision shall not prevent vehicle-specific data collection, so long as there is an agreement in place between the vehicle operators and the *entity* [4.14] collecting the data.

Service providers [4.27] shall not be required to provide any information that breaches the privacy laws of the *jurisdiction* [4.18]. See also 16.

Service providers [4.27] may, on request, provide anonymous aggregated data to the jurisdiction, the transport departments of the jurisdiction, for which they may expect to receive fees, or it may be a condition of their licence. In these cases privacy aspects need to be carefully considered by both the *jurisdiction* [4.18] and *service provider***.** The *jurisdiction* shall not send to any third party whatsoever nor use any information that conflicts with or compromises the privacy regulations of the *jurisdiction*.

8.3.9 Service provider specification SP8: Provision of non-regulated commercial services

Where permitted by the jurisdiction, *service providers* [4.27] may also provide additional commercial services to users using the same *IVS*, However, in this event the *service provider* shall:

a) obtain the approval of the *jurisdiction regulator* [4.19] or its *approval authority* [4.4] to permit such service provision (which shall not be unreasonably withheld)
b) ensure and assure that the provision of a non-regulated service does not affect the quality of the service provision of any regulated services in any significant way.

8.4 Wireless communications service provider

8.4.1 Service provider specification SP9: Wireless communications service provision

Service provision may take place using different wireless media, which shall conform to ISO 15638-2.

8.4.2 Service provider specification SP10: Responsibility for wireless communications service provision

The *service provider* [4.27] shall accept prime responsibility for any contract with any third party *service provider* [4.27] used to provide any regulated or commercial application services and shall be responsible to ensure that the communication *service provider* [4.27] meets the requirements of the regulation in respect of the wireless provision of the application service.

In the event that a general communications medium is used (for example GSM/UMTS) to provide a regulated application service, the *service provider* [4.27] shall ensure and assure that it has adequate access to that medium to enable the regulated service provision in accordance with the requirements of the *jurisdiction* [4.18].

8.5 IVS installer

The *IVS* equipment installer shall install the *IVS* communications equipment and shall be responsible to connect it to other equipment required in order to deliver the application service(s).

EXAMPLE In the case of remotely monitoring an electronic tachograph, to connect the tachograph into the *IVS*; in the case of on-board weigh in motion monitoring, connecting that equipment to the *IVS*; etc.

The *IVS* equipment installer shall be responsible to test the functionality of the installed equipment, and that where multiple equipment is connected, that all regulated services can be provided without detriment of one because of another.

The *IVS* equipment installer shall, in installing *IVSs* and *TIDs*, use only suitably qualified and trained personnel and shall maintain a register of those personnel.

The *IVS* equipment installer shall have in place documented and appropriate procedures for the installation of its *type approved* [4.29] *IVS*(s) and *TID*(s) and shall supply the same to its installation personnel.

The *IVS* equipment installer shall have in place, document and implement, appropriate procedures for the training of its installation personnel.

The *IVS* equipment installer shall install the *IVS* and *TID*(s) such that they do not interfere with the normal, safe operation of the vehicle. To that end, the *IVS* equipment installer shall consult with the manufacturer of the vehicle, and with other parties as necessary (such as the engine manufacturer) before an installation seeking their advice on issues such as equipment placement, sensor wiring and power take-off points. The training of all application *service provider* [4.27] installation personnel shall include manufacturer specific training on particular equipment.

8.5.1 Original equipment manufacturer specification OEM1: Responsibility where IVS is installed at time of vehicle manufacture

If the *IVS* is installed at the time of vehicle manufacture as part of the *OEM* vehicle equipment specification the *IVS* equipment installer shall be the vehicle manufacturer or his agent and the vehicle manufacturer shall accept responsibility to ensure that the equipment is *type approved* [4.29], or meets or exceeds regulatory performance requirements (as applicable) and is installed correctly and functioning at the time of sale.

8.5.2 Service provider specification SP11: Responsibility where IVS is installed post manufacture of the vehicle

Where the market model is that a *user* [4.31] selects a single *service provider* [4.27] (or is required to do so) the *service provider* shall accept responsibility to ensure that the equipment is *type approved* [4.29], or meets or exceeds regulatory performance requirements (as applicable) and is installed correctly.

NOTE In this environment each *service provider* [4.27] offers and installs their own type of *IVS* and have the freedom to offer different market models to recoup the cost of the equipment and its installation (much as those conditions which operate in the mobile telecommunications and satellite television markets).

In a situation where the *user* [4.31] is able to, and elects to, use multiple *service providers* [4.27], the *IVS* equipment installer is likely to be a third party commercial enterprise. In these circumstances, it will be up to the *jurisdiction* [4.18] to establish a regime that ensures effective quality control, and multi-equipment and system functionality, as such a regime will depend on the nature of the particular regulations for that *jurisdiction* [4.18]. The regime shall ensure that a single party is allocated responsibility for proper installation and the functionality of the equipment.

In all circumstances where the *IVS* is not part of the original equipment it is expected (but not required by this Standard) that these equipment installers will in many *jurisdictions* [4.18] have to be registered with, and approved by, the *approval authority* [4.4].

NOTE While the requirements of the application service are determined by the jurisdiction, it also certifies, approves and appoints service provider(s) and holds them accountable for the provision of the application service. The *jurisdiction* [4.18] may decide that it also has to approve *IVS* equipment providers, or it may leave this function to the *service provider* [4.27] which it will hold to account, and give the *service provider* freedom (possibly within some limits) as to how he or she controls his subcontractors.

8.6 IVS maintainer

Once installed, the *IVS* equipment has to be maintained. Functionality and capabilities have to be checked from time to time, and the equipment may have to be recalibrated and recertified from time to time in accordance with the regime imposed by the jurisdictions.

A number of business models for this can be envisaged. Maintenance may be a service provided by the service provider; it may be provided by the equipment installer; it may be provided by the vehicle maintainer; it may be provided by the vehicle inspector used for vehicle safety test certification; etc.

The regime allowed will depend on how the *jurisdiction* [4.18] best believes that its regime can be implemented and maintained, and will vary from *jurisdiction* to *jurisdiction*.

8.6.1 User responsibility US6: Responsibility to maintain the IVS

The *user* [4.31] shall nominate and contract with one service provider, to maintain the *IVS*, and this *service provider* [4.27] shall become the '*prime service provider* [4.21] ' and undertake all of the responsibilities of the '*prime service provider'* defined in this specification as part of its contract with the *user* for the duration of the contract.

8.6.2 Service provider specification SP12: Responsibility of the service provider contracted to maintain an IVS

8.6.2.1 Responsibility

An application *service provider* [4.27] who contracts to maintain an *IVS* shall report the contract and accept responsibility for maintenance to the *jurisdiction regulator* [4.19] in a manner defined and prescribed by the *jurisdiction* [4.18].

8.6.2.2 In the event of malfunction

In the event that an *IVS* or *TID* does not function in accordance with this specification, as soon as the application service provider/maintainer is made aware of the situation, it shall:

a) immediately liaise with the *user* [4.31] to commence to resolve the malfunction
b) report the malfunction (including an estimated resolution period) to the *jurisdiction regulator* [4.19] within a timeframe determined by the *jurisdiction* [4.18] in its regulations
c) The application service provider/maintainer shall within a timeframe determined by the *jurisdiction* [4.18] in its regulations, report to the *jurisdiction regulator* [4.19] ; and
d) make immediate and best efforts to ensure that *IVS* data records held within the *IVS* memory are transferred to the *prime service provider* [4.21] system, or have already been transferred.

8.6.2.3 Tampering

The application service provider/maintainer shall within a timeframe determined by the *jurisdiction* [4.18] in its regulations, report to the *jurisdiction regulator* [4.19]:

a) evidence of any *tampering* [4.28] or attempt at *tampering* [4.28] with the *IVS* security seal(s), the *TID*(s) or any connection(s); and
b) any *IVS* or *TID* malfunction which appears to be the result of *tampering* [4.28] or an attempt at *tampering*.

The application service provider/maintainer shall NOT advise a *user* [4.31] of any detection of *tampering* [4.28], or suspected *tampering*, with their *IVS* and/or *TID*(s).

In the event that any *type approved* [4.29] *IVS* or *TID* is subject to more than one instance of malfunction of a particular type (not being of a programmed maintenance type) the application service provider/maintainer shall notify *jurisdiction regulator* [4.19] of each malfunction, the apparent cause and the remedy.

NOTE Any remedy involving any change to the *type approved* [4.29] *IVS* or *TID* hardware or software shall require re-certification.

8.6.2.4 Documentation

For each *IVS* and *TID*, the *prime service provider* [4.21] or its installation and maintenance agents shall document all installation, operation, programmed maintenance and remediation-of-malfunction activity.

The documentation shall contain:

1) *IVS* ID and, if applicable, *TID* ID
2) version numbers of the hardware and software
3) date and time of activity
4) identification of personnel responsible
5) details of the activity including cause of malfunction and the remediation
6) personnel signatures.

The documentation shall be available for auditing by *jurisdiction regulator* [4.19].

The *prime service provider* [4.21] or its installation and maintenance agents shall maintain archives of the documentation described in this subClause for a period of years determined by the *jurisdiction* [4.18] (it is recommended that this period should be not less than four years).

8.7 Jurisdiction

The *jurisdiction* [4.18] is the body that has official power to make legal decisions and impose regulations. How this operates will vary from country to country according to their constitution or legal structure. Countries may have a single jurisdiction, or may delegate such authorities to their constituent states, or, as in the case of Europe, independent states may concede part of their independent National *jurisdiction* [4.18] to a common *jurisdiction* union to achieve common goals and interoperability within common conditions, while retaining independent *jurisdiction* in other matters.

The *jurisdictions* [4.18] are the owners of the *regulated applications* [4.23]. These may be required by regulation, or may be offered by a *jurisdiction* as an option to demonstrate compliance to a regulation, according to the choice of the *jurisdiction* and the regulations that it enforces.

8.7.1 Jurisdiction specification JS1: Definition of regulated application services for TARV

The *jurisdiction* [4.18] shall define and specify *regulated application services* [4.24] that are mandatory or voluntary for *regulated commercial freight vehicles* [4.25].

8.7.2 Jurisdiction specification JS2: Definition of status of regulated application services for TARV

The *jurisdiction* [4.18] shall determine whether the provision of a defined *regulated application service* [4.24] for *TARV* shall be mandatory or voluntary.

8.7.3 Jurisdiction specification JS3: Obtain supporting legislation/regulation for a regulated application service for TARV

The *jurisdiction* [4.18] shall be responsible to obtain all legislation and regulations that are required to implement a regulated application service.

8.7.4 Jurisdiction specification JS4: Manage and regulate the provision of the regulated application services

Without this part of ISO 15638 prescribing the domestic arrangements within any jurisdiction, the *jurisdiction* [4.18] shall be responsible to manage and regulate the provision of the *regulated application services* [4.24] that it elects to implement, including selecting standards to be adopted; adjudication and mediation; and determining and managing certification and auditing arrangements and procedures.

NOTE This may be achieved directly through the function of the jurisdiction, or by the appointment of a *regulator* [4.26] who may or may not be the *approval authority* [4.4], at the election of the jurisdiction.

8.8 ‘Approval Authority’

ISO 15638-1 expounds that if third party *service providers* [4.27] are to provide a service determined by the *jurisdiction* [4.18] to users, the jurisdiction, and for that matter the users, need to be assured that this service is being properly provided according to the requirements of the jurisdiction and its regulation. The *service provider* will therefore need to be approved by the regulator, and so some form of *approval authority* [4.4] forms an essential component of the architecture (even where this function is in practice carried out by the staff of the *jurisdiction* [4.18] or the *jurisdiction regulator* [4.19]), and the approval authority may, at its discretion, appoint *auditors* [4.6] to *audit* [4.5] the services provided to ensure their compliance.

NOTE An ‘Approval Authority’ describes an entity that certifies the ‘Service Providers’ and ensures that the level of service provided by the service providers is maintained. The Approval Authority functions might be provided by a single independent organisation selected by the responsible jurisdiction, they might be provided by the jurisdiction itself, or they might be provided via other arrangements as specified by the jurisdiction.

Specific *certification* [4.10] procedures providing formal affirmation that an applicant [4.2] has satisfied all the requirements for appointment as a *service provider* [4.27], are not defined in this (or any) part of ISO 15638, but are the responsibility of the *approval authority* [4.4] and its *jurisdiction* [4.18].

While the specific 'certification' procedures for specific application services are a matter for the jurisdiction and are outside the scope of this (or any) part of ISO 15638, approval authorities are recommended to use the guidance of ISO 17000 and ISO guide 65 when developing and implementing such procedures.

8.8.1 Jurisdiction specification JS5: create or appoint a 'Approval Authority'

Without this part of ISO 15638 prescribing the domestic arrangements within any jurisdiction, the *jurisdiction* [4.18] shall be responsible for determining the role and responsibilities of any *approval authority* [4.4] it creates or appoints to approve *service providers* [4.27] and *IVS*.

NOTE An *approval authority* [4.4] is an *actor* [4.1] that certifies the '*Service providers* [4.27] ', and ensures that the level of service provided by the *service providers* [4.27] is maintained. The *approval authority* [4.4] functions may be provided by a single independent organisation selected by the *jurisdiction* [4.18] responsible, they may be provided by the *jurisdiction* itself, or they may be provided by other arrangements as specified by the *jurisdiction*.

Approval authority [4.4] approval refers to the confirmation of certain characteristics of an object, person or organisation. In this context, *approval authority* approval applies to both the *service providers* [4.27] and the *IVS* and any *TIDs* for which requirements need to be formulated. These requirements need be described as tests to be passed. Each requirement leads to a verdict (passed or failed) on which the *approval authority* approval is based.

8.8.2 'Approval Authority' specification AA1: Consider and appoint candidates to be service providers

On behalf of the jurisdiction, and to its regime, the 'Approval Authority' shall consider candidates to be *service providers* [4.27] and shall appoint candidates to be *service providers*.

8.8.3 'Approval Authority' specification AA2: Test and approve service providers

On behalf of the jurisdiction, and to its regime, the *approval authority* [4.4] shall test and approve that appointed *service providers* [4.27] can meet the requirements necessary to provide the application service, and shall examine and approve their business model in relation to charging users and shall have the responsibility to determine the duration of the *approval authority* approval and renewal options and requirements.

8.8.4 'Approval Authority' specification AA3: Audit service providers

While *approval authority* [4.4] approval provides assurance that a *service provider* [4.27] meets certification requirements at a point in time, a process of on-going *audits* [4.5] is also required to ensure that the *service provider* continues to maintain the minimum level of service in accordance with the *certificate of approval* [4.11].

On behalf of the jurisdiction, and to its regime, the *approval authority* [4.4] shall *audit* [4.5] the performance of *service providers* [4.27] from time to a regime determined by the *jurisdiction* [4.18].

The *audit* [4.5] requirements comprise a variety of aspects which include operational, technical and financial capabilities. The process of *audit* is specific to the *regulated application* [4.23]. But the generic common objectives of the *audit* function form a second set of requirements for the *approval authority* [4.4], which are to:

a) support the policy objectives to the various legislation and requirements
b) monitor compliance by *service providers* [4.27] with the standard and the *approval authority* [4.4] approval agreement
c) ensure that information provided by the *service provider* [4.27] is reliable, compete and accurate
d) assist in determining the integrity of information provided by the service provider
e) enhance transparency, integrity and public credibility of the *regulated applications* [4.23].

8.8.5 'Approval Authority' specification AA4: Type approve IVS

On behalf of the jurisdiction, and to its regime, the *approval authority* [4.4] shall 'type approve' the *IVS* offered for installation post the manufacture of the vehicle. (*OEM* equipment installed during the vehicle manufacturing process shall be certified as part of the vehicle type approval certification).

8.8.6 'Approval Authority' specification AA5: Test IVS functionality

On behalf of the jurisdiction, and to its regime, the *approval authority* [4.4] shall provide a regime to test and provide assurance that *IVS* equipment is capable and properly installed in order to provide the application services.

NOTE It is expected that most jurisdictions/certification authorities will elect to meet this requirement using an independent test house. But the elected method is at the choice of the *jurisdiction* [4.18].

8.9 Contract options

8.9.1 User requirement US6 : 'Service Provider - User Contract''

Once installed, whether as *OEM* equipment or aftermarket equipment, and whether voluntary use or mandated use, the operator of the regulated commercial vehicle shall be required to sign a contract with one (or according to the regime of the jurisdiction) possibly more than one service provider, to obtain access to the elected application service(s).

The contract shall be between a *user* [4.31] and a *service provider* [4.27] and shall be specific to a regulated commercial vehicle or group of identified and nominated vehicles. The nature of the contract(s) established and the terms and services provided by the contract are outside the scope of this part of ISO 15638, save that any such contract shall be conformant to the regime established by the *jurisdiction* [4.18].

The duration of the contract is outside the scope of this contract, as are the cancellation terms, but users are advised that a *regulated application service* [4.24] if made mandatory by the *jurisdiction* [4.18] is not an option but a requirement and therefore at the termination of a contract for a mandated *regulated application service* the *user* [4.31] shall be under obligation to effect a replacement contract. *Jurisdictions* [4.18] are advised (but not required by this part of ISO 15638) to implement a regime of significant penalties for any *user* [4.31] who operates a registered commercial freight vehicle without a contract for its mandated application services (if any).

Except in a situation where the *service provider* [4.27] is mandated by the jurisdiction, in an environment where there may be multiple *service providers*, users should have the normal contract freedoms (within reasonable contract conditions) to elect to change *service provider*.

As specified in this part of ISO 15638, the installing/first contracting *service provider* [4.27] shall assume the role as '*prime service provider* [4.21] ' and shall be responsible for the maintenance of the *IVS* as part of its contract with the *user* [4.31]. In the event that the contract between the *prime service provider* and the *user* is terminated for any reason whatsoever, the *user* shall elect another *service provider* and contract with them to be the *prime service provider*.

On becoming the *prime service provider* [4.21], whether at point of installation and commissioning or subsequently, the *service provider* [4.27] shall advise the *jurisdiction* [4.18] of its appointment in a manner prescribed by the jurisdiction, that it has become the *prime service provider* to the nominated *IVS*/regulated commercial freight vehicle combination.

In the event of a *user* [4.31] selling or passing on usage of a regulated commercial freight vehicle to another user, the *IVS* and vehicle identity shall remain unchanged and the *jurisdiction* [4.18] shall have the task to accommodate such transfer (probably but not necessarily through the vehicle registration process). Any (new) *service provider* [4.27] now contracted to provide application service(s) to the vehicle shall have the responsibility to advise the *jurisdiction* or its *approval authority* [4.4] or *regulator* [4.19] the change of *user* [4.31]. The service provider, or one of the *service providers* in a multiple environment, shall contract with the *user* to become the '*prime service provider'* [4.21] with the responsibilities described above.

9 IVS REQUIREMENTS

9.1 Physical

9.1.1 IVS functional description

The *IVS* is the equipment on-board a vehicle that can provide the specified telematics functionality. This equipment may comprise a single physical *on-board unit* [4.20], or a telematics functionality within one or multiple equipments on-board a vehicle.

IVS can be installed by an *OEM*, usually the vehicle manufacturer, in which case it is likely to comprise multiple functions, some of which are performed within the *IVS* and others of which are performed elsewhere and the data fed, probably by the vehicle *CAN bus* [4.9] or J1939 bus network, to the *IVS*.

IVS can also be installed by the *prime service provider* [4.21] or his agent, in which case it is much less likely to obtain its information from elsewhere in the vehicle and far more likely to instantiate as an *OBU* with all or most of the functionality that it requires developed within the *IVS*/*OBU*.

9.1.2 HMI aspects

The *IVS* shall provide clear visual and/or audible information regarding the status of the system and its wireless connection and shall provide indication as to when a transaction is in progress. The nature of such notification is not specified but is left to the marketplace to design or the *jurisdiction* [4.18] to specify.

9.2 Data

9.2.1 IVS essential data collection

The *IVS* shall collect and store at least the following data:

a) *IVS* identification
b) vehicle identification
c) vehicle class identification
d) propulsion storage type
e) *GNSS* data
f) date and time data
g) vehicle position data
h) vehicle direction of travel data
i) vehicle speed data
j) trailer identification data (if applicable)
k) alarm status data
l) movement sensor status
m) ignition status
n) driver identification (if applicable)
o) load data (if applicable
p) self declaration data (if applicable).

The means by which this is achieved is defined in ISO 15638-5 (*TARV* generic vehicle information).

9.2.2 IVS essential data processing

The *IVS* shall be capable to calculate and store:

a) position records
b) speed records
c) alarm records
d) driver records

For the eventuality that these are required in performance of an application service, but shall not actually make these calculations unless required to do so by an application service.

The means by which this is achieved shall be as defined in ISO 15638-1, Clause 12 (Interoperability and the *TARV*-ROAM 'facilities' layer, and the data detail shall be as defined in ISO 15638-5 (*TARV* generic vehicle information).

9.2.3 IVS identification

Each *IVS*, or each *OBU* that comprises part of an *IVS*, shall have a unique unambiguous identifier (*IVS* ID), as specified in ISO 15638-5 (*TARV* – Generic vehicle information) that will be used to unambiguously identify the particular *IVS*:

- The *IVS* ID shall be visibly etched or marked on the outside casing of the unit in a manner such that it cannot be modified or removed.
- The *IVS* ID shall be stored in the non-volatile programmable read-only memory of the *IVS* (See 9.6 below).
- The *IVS* ID shall not be able to be set or altered by any person other than the *prime service provider* [4.21], or otherwise tampered with.

9.3 IVS specification IVS1: Robustness and suitability

9.3.1 Robustness

The *IVS*, in whatever form, units and connections, that it is instantiated, shall ensure that its mechanical, electrical and electronic strength matches the actual stresses of the operating environment.

IVS design shall take account of:

a) Communication capability
b) Electronic capability
c) Mechanical capability, durability and response
d) Vibration, bump, fall, shock
e) Eigenfrequencies, eigenvalue, eigenvector, and eigenspace concepts (innate, distinct, self) in the field of linear algebra. which are represented by matrices acting on vectors
f) Material data
g) Design methods
h) etc.

In achieving these requirements, designers of systems shall need to consider the evolving threats associated with the electronic environment and the necessary technical competency required to rectify faults; and ensure that consideration of the combination of all of these factors ensures that its mechanical, electrical and electronic strength matches the actual stresses of the operating environment and any likely situation that the equipment is likely to encounter. ISO 15638-4 provides specification for security in *TARV* application services.

The *OBU*(s) of an *IVS* shall be robustly connected to the prime mover/rigid truck.

In respect of robustness aspects of software see 9.27.1,11.7, 12.10.5, 14.4.4, 14.4.19, and 14.6.2.

9.3.2 Suitability for use

9.3.2.1 The *IVS* manufacturer or installer shall provide to the *jurisdiction regulator* [4.19], evidence of compliance from an appropriate body, with the following, or equivalent(s) as approved by *jurisdiction regulator*:

a) *IVS* complies with all of the performance requirements in this specification when subjected to the vibration to a reference specified by the *jurisdiction* [4.18].

b) *IVS* complies with all of the performance requirements in this specification when subjected to the impact to a reference specified by the *jurisdiction* [4.18].

c) *IVS* complies with all of the performance requirements in this specification when subjected to the temperature and humidity specified to a reference specified by the *jurisdiction* [4.18].

d) *IVS* complies with the electromagnetic compatibility conditions specified in a reference specified by the *jurisdiction* [4.18].

e) *IVS* components exposed to the elements comply with the dust and water ingress protection requirements of IEC 60529 Ed 2.1:2001; Table 7, Item 6 and Clause 13.4 and Table 8, Item 6 and Clause 14.2.6.

f) *IVS* components mounted in the cabin shall comply with the dust and water ingress protection requirements of IEC 60529 Ed 2.1:2001; Table 7 Item 5 Clause 13.4 and Table 8, Item 4 and Clause 14.2.4.

g) *IVS* and *TID* shall be tolerant to radio frequency and electrical interference as defined in 2004/104/EC, sections 6.7 and 6.8 with functional status 'A', Table 1.

h) electromagnetic emissions from the *IVS* and *TID* shall not exceed the limits in 2004/104/EC, sections 6.9 using the pulse amplitude levels for either 12 or 24 volt systems as appropriate, Table 2.

i) electromagnetic emissions from the *IVS* and *TID* shall not exceed the limits in *CISPR* 22:2004 (CIS participants report 22:2003), Class B, Table 6.

j) Security seals of the *IVS* shall remain intact when exposed to the vibration and impact as specified above.

9.4 IVS specification IVS2: Availability

The *IVS* shall always be available if the ignition of the vehicle is switched on.

If the *IVS* is for any reason not available, the driver shall receive a warning. The nature of such warning is not specified but is left to the marketplace to design or the *jurisdiction* [4.18] to specify in what form this is achieved.

9.5 IVS specification IVS3: Environmental

The **IVS** shall meet the legislation and regulations of the *jurisdiction* [4.18] in respect of environmental aspects of electronic equipment.

9.6 IVS specification IVS4: Secure data storage

The *IVS* manufacturer and the *IVS installer* [4.16] shall ensure that the non-volatile data storage equipment can survive a crash of Delta-V (as calculated according to SAE J1455, with a duration of 50 ms) equating to 130 kph.

The *IVS* manufacturer and installer shall ensure that the non-volatile data storage is *tamper* [4.28] resistant.

The *IVS* manufacturer and installer shall ensure that the data in the non-volatile data storage and in the *RAM* is accessible only to the application *service provider* [4.27] and cannot be accessed from within the vehicle other than by the *IVS installer* [4.16] and *IVS maintainer* [4.17].

Data storage security shall meet the requirements of ISO 15638-4 (*TARV* – System security requirements). It shall not be possible for collected or stored data or software memory within the *IVS* to be accessible or

capable of being manipulated by any person, device or system, other than that authorised by the *prime service provider* [4.21]. Security and confidentiality of data stored in the *IVS* shall be maintained at all times.

The means by which these measures are achieved are not defined within this part of ISO 15638 but are left to the marketplace or regulation of the *jurisdiction* [4.18].

NOTE Where police or other regulatory authorities require this information, they will be able to obtain it from the application *service provider* [4.27] in accordance with the local regulations, but not directly from the vehicle. This enables good security to be maintained regarding data held on-board the vehicle.

9.7 IVS specification IVS5: Data storage means

The *IVS* shall have a means of non-volatile data storage that can retain the stored information even when not powered (such as hard disc, flash memory etc.) with a minimum memory capacity of 100 Gigabytes.

In the unlikely event that the volume of data collected and generated prior to transfer to the application *service provider* [4.27] exceeds the data storage capacity of the IVU, new data shall not overwrite stored data.

NOTE This is for evidentiary reasons. It prohibits the overwriting of data already collected, albeit at the expense of collecting new data.

9.8 IVS specification IVS6: Data input means

There shall be a means for the driver to input his driving licence number each time he/she takes control of the vehicle. The form of that interface shall be a matter for the regulation of the *jurisdiction* [4.18] (such as an IC card reader, RFID reader, USB2, barcode reader, fingerprint reader, etc) according to the physical form of the drivers licence.

The non-volatile data storage and *RAM* shall not be available from within the vehicle except to the *IVS installer* [4.16] and the *IVS maintainer* [4.17].

9.9 IVS specification IVS7: Central processing unit

The *IVS* shall be able to prove that it is able to perform the program of operations required in order to fulfil regulated service provision. The central processor unit shall comprise at least:

- a processor with a minimum processing capability of 1 GigaHertz or higher
- volatile memory (*RAM*/*DRAM*/*SRAM* etc.) of at least 100 Gigabytes
- recognised operating system (e.g. Linux)
- means to interact with process ISO 11519* and ISO 11898** CAN bus data

Reference Standards:

ISO 11519-1 *Road vehicles -- Low-speed serial data communication-- Part 1: General and definitions*

ISO 11519-2 *Road vehicles -- Low-speed serial data communication -- Part 2: Low-speed controller area network (CAN)*

ISO 11519-3 *Road vehicles -- Low-speed serial data communication -- Part 3: Vehicle area network (VAN)*

ISO 11898-1 *Road vehicles -- Controller area network (CAN) -- Part 1: Data link layer and physical signalling*

ISO 11898-2 *Road vehicles -- Controller area network (CAN) -- Part 2: High-speed medium access unit*

ISO 11898-3 *Road vehicles -- Controller area network (CAN) -- Part 3: Low-speed, fault-tolerant, medium-dependent interface*

ISO 11898-4 *Road vehicles -- Controller area network (CAN) -- Part 4: Time-triggered communication*

ISO 11898-5 *Road vehicles -- Controller area network (CAN) -- Part 5: High-speed medium access unit with low-power mode*

NOTE providers of in-vehicle platforms that may perform multiple functions in the vehicle in addition to regulated services may be advised to use high performance processors, but this should not be a requirement for the provision of currently envisaged regulated services.

The testing of the central processing unit performance shall be completely independent of any envisaged application service.

9.10 IVS specification IVS8: Secure data processing

Secure data processing shall be achieved by compliance to ISO 15638-4.

9.11 IVS specification IVS9: Connectivity means to/from auxiliary equipment

The *IVS* shall have a means to receive inputs from and communicate with auxiliary equipment.

The *IVS* shall have multiple means to connect with auxiliary equipment using standard physical interfaces (USB2, USB3,USB Micro A and B, USB mini A and B, RS232, RS422 etc.) and the *CAN bus* [4.9] (PCAN TJA1054 or PCAN-BD10011S).

The *IVS* shall have an internal clock that operates independently of the supporting external power supply.

In the event the external power supply fails or shuts down, the *IVS* internal clock shall operate for a period of at least 28 days.

The accuracy of the *IVS* internal clock shall be such that it does not deviate by more than 1 second from the UTC date and time over any 28 day period when using *GNSS* signals.

The accuracy of the *IVS* internal clock shall be such that it does not deviate by more than 20 seconds per day from the UTC date and time over any 28 day period when not using *GNSS* signals.

9.12 IVS specification IVS11: Communications means

The *IVS* shall have a means to receive inputs from and communicate with its communications capability (in order to receive and process instructions from the service provider).

The nature of that communication shall comply to one of the options defined in ISO 15638-2, which shall determine the nature and specification of the equipment required.

9.13 IVS Classification

There shall be two classes of *IVS* (Class A and Class B) according to their ability to communicate with trailers attached to them.

NOTE Some types of prime mover do not have trailers attached to them (e.g. permanent rigid body trucks) so do not need the ability to obtain data from trailers. In other situations the application services specified by the *jurisdiction certification agreement* may have no requirement for trailer information. In cases such as these the *IVS* need not have this functionality.

9.13.1 IVS specification IVS12: *CLASS A* - able to communicate with its attached trailers

An *IVS* shall be defined as a *CLASS A IVS* if it is able to identify trailers that are attached to it (in order of connection where there are multiple trailers and the connection is hard wired) and meet all of the trailer identification requirements defined later in 9.

CLASS A IVSs shall, in addition to monitoring a prime mover/rigid truck, have the ability to communicate with trailer identification devices on attached* trailers in order to identify and record trailer identification (and possibly content) information:

a) from each trailer identification device fitted to an attached trailer
b) up to a maximum of 10 attached trailers

NOTE * 'Attached' means that the trailer(s) are connected to the prime mover/rigid truck such that the trailer(s) move automatically in unison with the prime mover/rigid truck in a manner complying with all applicable laws, regulations and standards.

9.13.2 IVS specification IVS13: *CLASS B* – not able to communicate with its attached trailers

An *IVS* shall be defined as a *CLASS B IVS if* it is unable to identify trailers that are attached to it or not meet the all of trailer identification requirements defined below in 9.

9.14 IVS specification IVS14: IVS identification of attached trailers

A *CLASS A IVS* shall identify and record the trailer identification of all attached trailers in the overall vehicle combination for a maximum of up to ten trailers. The means by which this is achieved is not standardised, but may be a wired connection, or a wireless connection. (see also 9.18)

The instigation of such identification may, at the election of the jurisdiction, be:

a) automatically performed by an application service,
b) automatic when the vehicle ignition is turned on,
c) manually instigated by the driver

or to some other regime defined by the **jurisdiction** [4.18].

9.15 IVS specification IVS15: Physical trailer marking

The trailer ID shall be visibly etched or marked on the outside casing of the trailer in a manner prescribed by the *jurisdiction* [4.18].

9.16 IVS specification IVS16: Equipped trailer identification (trailer ID)

Whether or not a trailer is equipped with a trailer identification device shall be at either the election of the *jurisdiction* [4.18]., or to meet the requirements of an application service (regulated or commercial).

9.17 IVS specification IVS17: Freight land conveyance content identification and communication

The equipped trailer ID shall use a unique identification scheme in accordance with ISO 26683-2 (Freight land conveyance content identification and communication – Application profiles) or ISO 17262 (Intelligent transport systems — Automatic vehicle and equipment identification — Numbering and data structures) or an unambiguous identification scheme specified by the *jurisdiction* [4.18] (in which case the *jurisdiction* shall accept the responsibility to ensure that the identification scheme is unique and unambiguous).

9.18 Equipped trailer identification devices

9.18.1 IVS specification IVS18: Equipped trailer identification devices

Equipped trailers shall each be equipped with a 'trailer identification device' (*TID*) in order to enable automatic identification and recording of fitted trailers by the *IVS*.

The *TID* shall be used to uniquely identify:

a) the trailer
b) the trailer configuration (i.e. number of axles etc.)
c) data pertaining to the connection of the trailer to the prime mover/rigid truck, as part of the performance of an application service
d) may provide identification and status information about the cargo on-board the trailer.

The form of the trailer identification device is not standardised but it shall be robustly connected to each trailer to be monitored by the application *service provider* [4.27] and shall be inclusive of the hardware, software and communications (wired cabling or wireless) and connections leading up to, but not including the *IVS*.

The trailer identification device shall only communicate with the prime mover *IVS* when the trailer is physically connected to the prime mover or another connected trailer. The means by which this is achieved is not standardised, but that it is achieved is a requirement.

9.18.2 IVS specification IVS19: Trailer identification device requirements

The trailer identification device shall comprise:

a) Central processor
b) *RAM*
c) include non-volatile programmable read-only memory

The trailer identification device (*TID*) include shall include non-volatile programmable read-only memory of a minimum of 1 gigabyte.

The trailer ID shall be recorded permanently into the non-volatile programmable read-only memory of the *TID*.

It shall not be possible to alter the Trailer ID in the non-volatile programmable memory without making the **TID** permanently inoperable.

9.18.3 IVS specification IVS20: Integrity of trailer identification

The transmission of trailer identification data from the *TID* to the *IVS* shall support a form of Trailer ID data authentication (i.e. some form of message authentication code only known and accessible to the application service provider), subject to the approval of the jurisdiction, that can prove the origin and integrity of the trailer ID (*TID*) data.

The application *service provider* [4.27] shall document, to the satisfaction of the *jurisdiction regulator* [4.19], the trailer ID data authentication mechanism.

See also ISO 15638-4 (*TARV* - System security requirements)

9.19 IVS specification IVS21: Power supply

An *IVS* fitted to a prime mover shall normally obtain its power supply from the main power supply of the vehicle, although other arrangements may be made so long as they assure an adequate and reliable power supply to the *IVS*. Uninterruptible back-up power supply is also required in the event of disconnection (for example in the event of an accident), or where the vehicle power supply has been intentionally removed (such as during service or vehicle lay-up).

The *IVS* shall be supplied with a reliable power supply that shall function whenever the vehicle ignition is switched on.

The *IVS* shall have access to a separate protected independent power supply(ies) in the event of the disconnection of the vehicle power supply that shall enable the *IVS* to remain on standby for 7 days.

The *IVS* shall have access to a separate protected independent power supply(ies) in the event of the disconnection of the vehicle power supply that shall enable the *IVS* to remain fully operational for 1 hour.

The requirements in this Clause relate to the power supply available to enable the IVS to function, but do not apply to the powering of any other equipment connected to the *IVS*, and the back-up power supply to the *IVS* shall be arranged such that it cannot be drained by any other connected equipment such that it fails to meet the requirements of this Clause.

In the event of their being separate/additional *IVS* installed on trailers, the installer shall make provision for an adequate power supply to the *IVS* and its recharging. The means by which he achieves this is not specified. It is preferable that the features defined above also apply to an *IVS* installed on a trailer, but where this is not practicable the device shall at the least have a low power warning that can be automatically sent to the service provider, and there shall be a means of warning the driver (the means by which this is achieved is not specified).

9.20 IVS specification IVS 22: external power supply failure/shut down

In the event that the external power supply supporting the *IVS* fails or shuts down, the *IVS* shall be capable of:

a) retaining stored data for at least 28 days; and

b) monitoring the status of the ignition and other independent movement sensors for at least 7 days

c) remaining fully operational for at least 1 hour

NOTE The primary purpose of continuing to monitor after the external power supply fails or shuts down is to facilitate the detection of any disconnection of the *IVS* and/or movement of the prime mover/rigid truck independently of the *GNSS* signal.

9.21 IVS specification IVS23: Security seals

Any *OBU* of an *IVS* or *TID* shall be protected by security seal(s) to ensure detection of any unauthorised removal or opening of the *OBU* in accordance with the regulations determined by the *jurisdiction* [4.18].

Removal or opening of an *OBU* shall be possible only by breaking the security seal(s) and the security seal(s) shall be such that if broken they cannot be reinstated.

The *OBU* shall be placed in a position that facilitates inspection of the integrity of the security seal(s).

The security seal(s) shall clearly display signs of any unauthorised access, either visually and/or physically.

9.22 IVS specification IVS24: GNSS capability

The *IVS* shall have or shall have access to global navigation satellite positioning system (*GNSS*) receiver capability which shall consist of a *GNSS* receiver connected to a *GNSS* antenna.

The *IVS GNSS* receiver and *GNSS* antenna shall comply with the radio communications regulations of the *jurisdiction* [4.18] and shall meet performance specifications defined by the *jurisdiction***.**

The *IVS GNSS* antenna shall be mounted in a position that meets the manufacturer's specification for the vehicle combination and such that it optimises signal strength from the *GNSS* satellites.

The quality of *GNSS* data shall be measured by the number of satellites used and the horizontal dilution of precision. For the purposes of quality measurement, the horizontal dilution of precision from the *IVS GNSS* receiver shall be measured and stored to a resolution of one degree or better.

NOTE 'used' means the number of satellites whose signal is received and taken into account by the *IVS* in the determination of data.

9.23 IVS specification IVS25: Accelerometer capability

9.27.2 below determines the requirement for multiple independent features to facilitate the indication of vehicle movement. One common way to achieve this is to use an accelerometer. Various equipment in the regulated commercial freight vehicle may already include accelerometers, or one may be incorporated into an *IVS*. An accelerometer measures acceleration. A 3-axis accelerometer provides the orientation of a stationary platform relative to earth's surface.

Accelerometers have become low cost and common in a wide range of applications and equipment. Most new vehicles use accelerometers in multiple systems. One of the most common uses for *MEMS* accelerometers is in airbag deployment systems. In this case the accelerometers are used to detect the rapid negative acceleration of the vehicle to determine when a collision has occurred and the severity of the collision. Another common automotive use is in electronic stability control systems, which use a lateral accelerometer to measure cornering forces.

NOTE A 3-axis accelerometer provides the orientation of a stationary platform relative to earth's surface. However, once that platform starts moving, it may provide apparently questionable results. For example, if the platform is in free-fall, it will show zero acceleration. If it is accelerating in a particular direction, that acceleration will simply be added to whatever acceleration is being provided by gravity, and it will not be possible to distinguish. A 3-axis accelerometer in an aircraft in a properly coordinated turn with a 60 degree angle of bank, for instance, will show 2 G "vertical" acceleration in the aircraft, despite the fact that the aircraft is tilted 60 degrees relative to the horizon.

This part of ISO 15638 does not determine any application or interpretation of accelerometer data, solely the architecture of the data and message.

An accelerometer is not mandatory, but where accelerometer data is provided the data shall be stored in accordance with ISO 15638-5 (9.2.1).

9.24 IVS specification IVS26: Gyroscope capability

A gyroscope measures rate of rotation around a particular axis, they are frequently used to determine the attitude of a vehicle, for example in a stability control system, but used alone can provide misleading information

EXAMPLE a roll gyro in an aircraft in a coordinated turn with a 60 degree bank will be measure a rate of zero, the same as an aircraft flying straight and level.

Gyroscope data also drifts with time, so additional error will accumulate over a period of minutes or even seconds.

Therefore a combination of accelerometer and gyroscope are often used for applications.

This part of ISO 15638 does not determine any application or interpretation of a combination of gyroscope and accelerometer data, solely the architecture of the data and messages.

A gyroscope is not mandatory but where gyroscope data is provided the data shall be stored in accordance with ISO 15638-5 (9.2.2).

9.25 IVS specification IVS27: Still camera data

Where still images are recorded they shall be recorded as determined in ISO 15638-5 (9.2.3.1, JPEG/.jpg).

9.26 IVS specification IVS28: Video data

Where video images are recorded they shall be recorded as determined in ISO 15638-5 (9.2.3.2, MPEG/.mpg).

9.27 Alarm status data and records

9.27.1 IVS specification IVS29: Alarm types and data

The *IVS* shall generate and store alarm records in its non-volatile data storage for each of the following events:

a) the external power supply is disconnected from the *IVS*;

b) the external power supply is reconnected to the *IVS*;
c) movement is indicated by the ignition while the external power supply is disconnected from the *IVS*, using two different features independent from the *GNSS* signal. (see 9.27.2)
d) movement is detected by the other independent movement sensor while the external power supply is disconnected from the *IVS*, using two different features independent from the *GNSS* signal.(see 9.27.2)
e) the ignition is disconnected from the *IVS* (with and without external power being connected);
f) the ignition is reconnected to the *IVS* (with and without external power being connected);
g) the other independent movement sensor is disconnected from the *IVS* (with and without external power being connected);
h) the other independent movement sensor is reconnected to the *IVS* (with and without external power being connected);
i) unauthorised access to data in the *IVS* is detected;
j) unauthorised access to *IVS* software is detected;
k) the *GNSS* antenna is disconnected from the *IVS*;
l) the *GNSS* antenna is reconnected to the *IVS*.

The data shall be stored in the format defined in ISO 15638-5.

9.27.2 IVS specification IVS30: Independent movement sensing

The connection of the independent movement features to the *IVS* is monitored so as to detect any attempts to *tamper* [4.28] which may include any attempts to disconnect and/or remove the *IVS*. The purpose of the independent movement features are to be able to facilitate the detection of movement of the vehicle independently of the *GNSS* satellite signal.

a) One independent feature to facilitate the indication of vehicle movement shall be the ignition status.

b) The other independent movement feature to facilitate the detection of vehicle movement shall, subject to the approval of *jurisdiction regulator* [4.19], be sensors such as:

1) the engine control module;
2) an odometer;
3) a tachograph; or
4) some other such independent movement sensor such as an accelerometer or gyroscope or combination of the two.

The *IVS* manufacturer shall document its chosen method of independent movement detection and connection.

The connection of the independent movement features to the *IVS* shall be monitored and reported upon in accordance with 9.27.1 e through 9.27.1 h.

9.28 IVS specification IVS31: Vehicle location

The *IVS* shall be capable of calculation, storing and presenting the vehicle location with data defined in accordance with ISO 15638-5 (Claus 8.10 Location)

When providing or recording location data the *IVS* shall also record and present the number of satellites present during the calculation as specified in ISO 15638-5.

When providing or recording location data the *IVS* shall also record and present the status of the vehicle ignition (on / off / disconnected) as specified in ISO 15638-5.

When providing or recording location data the *IVS* shall also record and present the status of any other independent movement sensors present (movement/no movement/disconnected) as specified in ISO 15638-5.

10 PROCEDURES FOLLOWING POWER-UP OF THE VEHICLE

10.1 IVS specification IVS32: When vehicle is powered up (ignition status ON)

10.1.1 The *IVS* shall immediately power-up and on power-up the *IVS* shall normally perform a self-test without attempting to connect to the network. In the event of a critical system failure which would result in an inability to execute an application service detected during or following the self-test, a warning shall be given to the driver of the vehicle. The nature of such warning is a feature of product design and is not standardised in this part of ISO 15638. It is then the responsibility of the driver of the vehicle to consider his next actions. Correct *IVS* functionality cannot be ensured as long such a critical system failure is present. *Jurisdictions* [4.18] are advised to implement regulations to instruct the driver what to do in these circumstances.

10.1.2 All enrolled application services shall commence.

10.1.3 The system shall activate the update sequences for dynamic information.

10.1.4 The system shall note the engine start event.

10.1.5 The communication channels shall be checked and then moved to standby until required. Some applications systems will be designed to cope with intermittent communication opportunity in which event data will be collected by the service application in the vehicle and transmitted when a communications link is available according to the design of the application service. For other application services such failure may be critical. In the event of that the absence of the possibility of an adequate communication link which would result in an inability to execute an application service as it has been designed, is detected during or following the test of the communications link, a warning shall be given to the driver of the vehicle. The nature of such warning is a feature of product design and is not standardised in this part of ISO 15638, but may be standardised in the specification of the particular application service.

It is then the responsibility of the driver of the vehicle to consider his next actions. Application service provision cannot be ensured if a critical communication system failure is present. *Jurisdictions* [4.18] are advised to implement regulations to instruct the driver what to do in these circumstances.

NOTE Some application services will require immediate and constant activation of the communication link.

10.2 IVS specification IVS33: Communication set-up

A communication for an application may be instigated either by the vehicle *IVS* or by the application *service provider* [4.27]. In the latter case the *IVS* shall have to first contact the application service provider, using the IPv6 address of the application *service provider* [4.27] (which is stored in the *IVS*), to advise that it is operating. The details of such communication shall be specified in the application service specification.

On activation of an application service, the *core application data* [4.13] fields are populated and updated in accordance with the requirements of this part of ISO 15638 or the requirements of the application service as appropriate.

The means by which the in-vehicle equipment provider populates and updates the *basic vehicle data* [4.8] and the *core application data* [4.13] is defined in ISO 15638-1, Clause 12 (Interoperability and the *TARV*-ROAM facilities layer) and ISO 15638-5 (*TARV* Generic vehicle information).

The means by which data is obtained from the vehicle shall be strictly controlled as defined in ISO 15638-1, Clause 12 (Interoperability and the *TARV*-ROAM facilities layer) using commands and defined destination addresses as defined in ISO 15638-5 (*TARV* Generic vehicle information).

There shall be 5 generic commands for use by any application:

1) GET *TARV LDT* data

2) GET CVS *LDT* data

3) CREATE core data

4) GET core data

5) GET Archive.

The specification and enactment of these commands are defined in ISO 15638-5 (*TARV* Generic vehicle information), 8.2 'Commands for vehicle data'.

10.2.1 Application service provider generates request for 'Core Application Data'

10.2.1.1 ISO 15638-1 provides specification of *basic vehicle data* [4.8] and *core application data* [4.13]. The *basic vehicle data* [4.8] concept is created and maintained in all circumstances regardless of *jurisdiction* [4.18]. The *core application data* [4.13] concept is *basic vehicle data* [4.8] plus additional data elements required by the *jurisdiction* [4.18]. (see also 12)

10.2.1.2 An application *service provider* [4.27] with whom the *user* [4.31] has enrolled may trigger a request to the *IVS* to send the *core application data* [4.13] at any time as defined in ISO 15638-5 (*TARV* Generic vehicle information)

In the CALM environment such requests may be targeted to a specific vehicle, or may be broadcast to all vehicles within the range of the communication network station.

10.2.2 IVS generates send of 'Core Application Data' (CAD)

The *IVS* may send the *core application data* [4.13] to the application *service provider* [4.27] at any time in accordance with the instructions of the on-board application service programme, as determined in ISO 15638-5.

10.2.3 Data compression

The data shall be sent using ASN.1 packed encoding rules (ISO 8824/ISO 8825).

10.2.4 Data acknowledgement

On successful receipt of the data requested by a command application *service provider* [4.27] shall send an acknowledgement **'***DATA-ACK'* which shall take the form of one byte of ones (12012011).

10.2.5 *In* the event of failure to receive the 'DATA-ACK'

If the **IVS** does not receive the '*DATA-ACK'* within 30 seconds it shall update the *basic vehicle data* [4.8] field as determined in ISO 15638-5 and resend the data requested by the command, preceded by one byte of zeros (0000000). It shall continue to do this until it receives the '*DATA-ACK'*.

10.3 IVS specification IVS34: Communication session clear-down

The application *service provider* [4.27] may clear-down an in-progress communication session at any time.

The *IVS* shall not clear down any in-progress communication session that was instigated by the application *service provider* [4.27].

So long as the requirements provisions of the application service permit, the *IVS* may clear-down an in-progress communication session that it instigated at any time.

The session clear-down procedures shall be as determined in ISO 15638-2 and the relevant CALM Media standard(s).

10.4 CAD not received correctly

In the event that the *CAD* data is not received correctly, the application *service provider* [4.27] shall not send the '*DATA-ACK'* (the absence of which will stimulate the *IVS* to resend the *core application data* [4.13]).

11 RECORDS TRANSFER AND BACKUP PROCEDURES

11.1 Periodicity determined by the jurisdiction

The frequency at which *IVS* records are transferred to the system of the *prime service provider* [4.21] ('Interval I') shall be determined by the *jurisdiction* [4.18].

11.2 Frequency of records transfer

11.2.1 The transfer of stored data from the *IVS* to the application *service provider* [4.27] shall be performed at 'interval I' provided that the *IVS* is in the communication coverage area offered by the application *service provider* [4.27] and the vehicle is in operation.

11.2.2 If the vehicle is out of communication coverage or not in operation at the time of the scheduled data transfer, then data transfer shall commence within 5 minutes of when the communication network becomes available and the vehicle is in operation.

11.3 Records to be transferred

The *IVS* shall send ALL records created since the last transfer of stored data. Within this part of ISO 15638 the data concept containing records created since the last transfer of stored data is known as '*stored data*'. The data in the *stored data* field shall commence with the *IVS* identification as specified in ISO 15638-5, followed by a timestamp as specified in ISO 15638-5, and shall be terminated by the *IVS* identification as specified in ISO 15638-5, as:

IVS unambiguous identity
timestamp
data
.....data
IVS unambiguous identity

11.4 Procedures for transfer of 'stored data'

11.4.1 IVS specification IVS35: 'stored data' Communication set-up

On reaching 'interval I' the data concept 'stored data' shall be populated with all records created since the last transfer of 'stored data' to the *prime service provider* [4.21] (or shall have been accumulated in a file since that last data transfer and shall be updated) and the identity and timestamp specified in 11.3 above.

The means by which the in-vehicle equipment provider populates and updates the 'stored data' concept is a matter for product design and outside the scope of this Standard.

11.4.2 IVS generates send of 'stored data'

If the communication channel with the application *service provider* [4.27] is already open the *IVS* simply sends the 'stored data' field; or the *IVS* shall first have to establish the communication link by 'calling' the IPv6 address of the application *service provider* (which is stored in the *IVS*) in accordance with the appropriate CALM media standard and the protocols for that communication medium - see ISO 15638-2, and then once the communication channel is open, send the 'stored data' field, preceded by one byte of alternate zeros and ones starting with zero (01010101).

NOTE The stored data field contains all of the information for the application *service provider* [4.27] to be able to interpret it uniquely.

11.4.3 Data compression

The data shall be sent using ASN.1 packed encoding rules (ISO 8824/ISO 8825).

11.4.4 Stored data acknowledgement

On successful receipt of the '*stored data*' the application *service provider* [4.27] shall send an acknowledgement **'***SD-ACK'* which shall take the form of one byte of alternate zeros and ones starting with '1' (10101010).

11.4.5 In the event of failure to receive the 'SD-ACK'

If the *IVS* does not receive the '*SD-ACK'* within 30 seconds of completing the send of data it shall update the *stored data* field and resend the *stored data* field, preceded by one byte of alternate zeros and ones starting with zero (01010101). It shall continue to do this until it receives the '*SD-ACK'*.

11.5 Deletion of data stored in the non-volatile memory of the IVS

11.5.1 IVS data records deleted only after fulfilment of conditions

IVS data records stored in the *IVS* shall only be deleted after fulfilment of the following conditions:

The data has been successfully transferred and acknowledged as received by the application service provider

and either

The data is more than one year old

or

The memory allocated in the data specifications in this part of ISO 15638 or ISO 15638-5 has been filled and the data field is overwritten as specified elsewhere in this part of ISO 15638 or in ISO 15638-5

or

To meet the requirements of ISO 15638-4.

11.6 Data testing

The application *service provider* [4.27] shall monitor that each '*stored data*' transfer occurs within the interval I determined by the *jurisdiction* [4.18].

The application *service provider* [4.27] shall test:

a) The application *service provider* shall test all incoming *IVS* data records for completeness, consistency and freedom from error.

b) Records received, (for consecutive record numbering)

Note An alarm is to be generated in the event that either of the numbering sequences legitimately resets to a lower value (e.g. because all numbers within the sequence have been used).

c) The application *service provider* shall test that within *IVS* data records, record numbers increase chronologically.

d) The application *service provider* shall test 'stored data' for integrity and authenticity.

e) The application *service provider* shall test records for plausibility.

f) The application *service provider* shall test whether the determined distance between the last position record prior to a period of non-operation, and the first position record after that period of non-operation that has a non-blank/void position, exceeds 500 metres. In the case that there is more than one period of non-operation between these two position records, only one alarm shall be raised.

g) The application *service provider* shall test whether for more than seven consecutive days, an *IVS* was malfunctioning.

The means by which such tests are effected are at the discretion of the application service provider, who shall satisfy the *jurisdiction regulator* as to the adequacy of their test regime.

11.7 Data backup and archiving

The application *service provider* [4.27] shall document and have in place, appropriate procedures for daily backup of data and applications.

The application *service provider* [4.27] shall test its procedures for data retrieval from backup storage no less frequently than once every three months.

Full system backups of data, applications and operating system shall be performed before and after any hardware or software changes.

The application *service provider* [4.27] shall document and have in place, appropriate procedures for the archiving and retrieval of data.

The application *service provider* [4.27] shall maintain weekly archives, for a period of four years from the date received.

The application *service provider* [4.27] shall maintain, for a period of twenty years all versions of the *IVS* software and system application software.

The application *service provider* [4.27] shall, at the expiration of the respective periods referred to in this clause, destroy the archived data.

All archived data shall be stored at two separate places:

a) one copy shall be kept at the application service provider's premises; and
b) one copy shall be kept at a secure off-site facility (within five working days of archiving the data).

The application *service provider* [4.27] shall perform a data retrieval of the archived data within five working days of being requested to do so by either the *jurisdiction* [4.18] or *jurisdiction regulator* [4.19].

The application *service provider* [4.27] shall test its procedures for archive retrieval no less frequently than once every three months.

See also 12.10.3.

12 IVS - VEHICLE

12.1 'Core Application Data'

The data required to provide a *regulated application service* [4.24] shall comprise the *basic vehicle data* [4.8] that is required for all *regulated application services*, and is defined in ISO 15638-5 as the *TARV* 'local data tree' (*LDT*).

Additional application specific data required for the *regulated application services* [4.24] that the *jurisdiction* [4.18] has determined are required or are supported as optional, or required for a specific class of vehicle

operating within its *jurisdiction* are provided via an 'app' held in the on board apps library defined in ISO 15638-5 (*TARV* generic vehicle information), which will populate and provision data values in the on-board data pantry as defined in ISO 15638-1 (*TARV* framework and architecture) and ISO 15638-5 (*TARV* generic vehicle information). The *basic vehicle data* [4.8] together with information that is required by the *jurisdiction* shall form a data concept known as the *core application data* [4.13].

It is therefore at the election of the *jurisdiction* [4.18] to determine the *core application data* [4.13] concept for their regime, and shall provide the legislation/regulation to require this.

ISO 15638-5 *TARV* – 'Generic vehicle information and application service contract requirements' provides definition of the date elements in the data concept *basic vehicle data* [4.8] and the form and content of the *TARV LDT*'.

ISO 15638-6 *TARV* – 'Regulated applications' provides candidate *core application data* [4.13] concepts for *regulated commercial freight vehicles* [4.25]. The *jurisdiction* [4.18] shall determine which if any of these data concepts are required in addition to the *basic vehicle data* [4.8].

The *core application data* [4.13] shall always include the *basic vehicle data* [4.8] defined in ISO 15638-5.

Some *core application data* [4.13] will be permanent (e.g. vehicle identification) while some data will be variable and trip dependent (e.g. driver and load data) and committed to the memory of the *IVS* en-route a journey.

The *core application data* [4.13] shall be transmitted using one or more wireless communications media as defined in ISO 15638-2 (Common platform parameters using CALM), and shall be presented in Abstract Syntax Notation, ASN.1 Packed encoding rules (PER unaligned) as defined in ISO 8825-2 using ASN1 definitions defined by the *jurisdiction* [4.18] in their determination of what comprises *core application data* [4.13] within their regime.

12.1.1 Jurisdiction specification JS6: 'Core Application Data'

The *jurisdiction* [4.18] shall determine which data concept(s) in addition to the *basic vehicle data* [4.8] concept (12.2) shall comprise their requirement to determine the *core application data* [4.13] concept for their regime, and shall provide the legislation/regulation to require this. However *core application data* shall always include the *basic vehicle data* defined in ISO 15638-5. The *jurisdiction* [shall make an 'app' available either dynamically via wireless communications as defined in ISO 15638-1 and ISO 15638-5, at the point of entry to the *jurisdiction* or online in advance of journeys (or both) that will enable the on board data *pantry* to be provisioned with the data that it requires (See ISO 15638-1, Clause 12, 'Interoperability and the **TARV**-ROAM facilities layer').

12.2 'Basic Vehicle Data'

Some essential information is needed to support all, or most *regulated application services* [4.24]. This information is therefore required in all circumstances and shall always form part of the *core application data* [4.13] This data concept shall be known as the *basic vehicle data* [4.8] and is defined in ISO 15638-5 as the *TARV* local data tree (*LDT*).

ISO 15638-5 provides specification of the content of the *basic vehicle data* [4.8] concept and the form and content of the *LDT*.

12.2.1 Jurisdiction specification JS7: 'Basic Vehicle Data'

The *jurisdiction* [4.18] shall determine the elected options within the *basic vehicle data* [4.8] concept that shall apply as part of the *core application data* [4.13] concept within their regime and which shall be available in the on board data pantry of the *IVS*, and shall provide the legislation/regulation to require this.

12.3 OEM installed IVS

12.3.1 Regulation regime

The equipment shall be part of the vehicle original equipment and *type approved* [4.29] as part of the vehicle type approval.

12.3.2 Physical installation aspects

12.3.2.1 Physical form

The physical form of the *IVS* is not specified and shall be a market place decision. The *IVS* may be a single *on-board unit* [4.20], but is more likely to be a software function linked to the supply of data through the vehicle databus (e.g. CAN or J1939 databus) and possibly part of an in-vehicle communications platform.

12.3.2.2 Physical installation

In this instantiation, the installation of the *IVS* is undertaken as part of the manufacturing process of the vehicle. The *IVS* may be provided as a standard component of the vehicle specification, or may be an option selected by the customer at the time of ordering the vehicle.

Installation of the *IVS* includes the installation of the physical components that comprise the *IVS* into the vehicle; the installation of any software and permanent data into the *IVS* operating system and storage media; the connection to the power supply of the vehicle; the connection and commissioning of all equipment external to the *IVS* and connection to common vehicle equipment (such as *GNSS*, GSM/UMTS SIM card and communication media etc.), possibly via the vehicle databus; the installation and commissioning of the human machine interface (*HMI*) and the fitting of connection to antennas for the wireless communication between the infrastructure. In the *OEM* fitted scenario it is envisaged that some components of the *IVS* are shared with other applications, (for example the wireless communication devices, *GNSS*, road map data and the *HMI*).

12.3.3 Vehicle data bus

The physical form of the *IVS* is not specified and shall be a market place decision, however, in the case of an *OEM* factory installed *IVS* during the manufacture of the vehicle, it is expected that the *IVS* will have (albeit limited) access to the vehicle CAN or J1939 databus.

12.3.4 Initial set-up

12.3.4.1 Service provider specification SP13: Prime service provider

The first *service provider* [4.27] to contract with the *user* [4.31] with respect to any specific *IVS*/regulated commercial freight vehicle shall assume the role of '*prime service provider* [4.21]'. The *prime service provider* shall be responsible for the initial commissioning of the *IVS* and its subsequent maintenance. In the event that the contract between the *prime service provider* and the *user* [4.31] is terminated for any reason whatsoever, the *user* shall elect another *service provider* [4.27] and contract with them to be the *prime service provider*.

On becoming the *prime service provider* [4.21], the *service provider* [4.27] shall advise the *jurisdiction* [4.18] in a manner prescribed by the jurisdiction, that it has become the *prime service provider* to the nominated *IVS*/regulated commercial freight vehicle combination.

The *prime service provider* [4.21] shall be responsible for the maintenance of the *IVS* and any related *TIDs*, and for the transmission and back-up of 'stored data'.

The *prime service provider* [4.21] shall program the *IVS* memory with the IPv6 address of the *prime service provider*, in the form prescribed in ISO 15638-5.

12.3.4.2 Service provider specification SP14: Set access conditions

The first contracted *service provider* [4.27] and subsequently the *prime service provider* [4.21] shall set the access conditions and shall decide who shall have the possibility to read or write to the *IVS* memory.

12.3.4.3 'Approval Authority' specification AA6: vehicle unique identification

The *approval authority* [4.4] shall assign each regulated commercial freight vehicle a unique identification number or code. According to the regime of the *jurisdiction* [4.18] that identification may be made available to the vehicle operator or to approved *service providers* [4.27]. Guidance as to appropriate coding systems can be found in Annex B of this part of ISO 15638.

12.3.4.4 Service provider specification SP15: IVS unique identification

At the time of handing over the vehicle to the user, it is probable that the *approval authority* [4.4] will not yet have provided a unique identification number/code to the vehicle *user* [4.31]. The first contracted *service provider* [4.27] shall assign the *IVS*, or it shall be assigned at the point of its manufacture, a unique and unambiguous identification in a form designated by the *jurisdiction* [4.18]. The first contracted *service provider* shall commit both the identification code of the registered commercial freight vehicle, and the unique *IVS* identity to the memory of the *IVS*.

12.3.4.5 Service provider specification SP16: 'Basic Vehicle Data'

The first contracted *service provider* [4.27] shall commit the permanent elements of the *basic vehicle data* [4.8] (as defined in ISO 15638-5) of the registered commercial freight vehicle to the memory of the *IVS*.

12.4 Aftermarket installed IVS

12.4.1 Regulation regime

The *IVS* shall be *type approved* [4.29] by the *approval authority* [4.4] or shall be self-certified according to the regime of the *jurisdiction* [4.18].

12.4.2 Physical installation aspects

12.4.2.1 Physical form

The physical form of the *IVS* is not specified and shall be a market place decision. However, the *IVS* will in all probability, at least initially, be a discrete stand-alone unit (*OBU*) with internal functions (such as *GNSS* etc.) and connections to external functions (such as tachograph etc.).

12.4.2.2 Physical installation

In this scenario, the installation of the *IVS* is undertaken as part of the first contracted *service provider* [4.27] contract.

The unit that houses the *IVS* functionality will have already been *type approved* [4.29] or self-certified See 14, and 8.8.5). The installing *service provider* [4.27] takes the responsibility to ensure that the equipment is correctly installed and functioning properly.

Installation of the *IVS* includes the installation of the physical components that comprise the *IVS* into the vehicle; the installation of any software and permanent data into the *IVS* operating system and storage media; the connection to the power supply of the vehicle; the connection and commissioning of all equipment external to the *IVS* and commissioning of *IVS* features (such as *GNSS*, GSM/UMTS SIM card and communication media etc.). It is assumed that the *IVS* may not have access to the vehicle databus, so equipment to provide the *basic vehicle data* [4.8] /'Core Application Data' is likely to form part of the *IVS* or be

separate equipment connected to the *IVS*. However the possibility of using data from the vehicle databus may be effected where such access and data is provided by the vehicle manufacturer.

NOTE Some *jurisdictions* [4.18] may legislate/regulate that it is a condition of vehicle type approval or registration for regulated vehicles that certain data is made available or that certain specified manufacturer fitted equipment is able to be connected to the *IVS*.

In this instantiation the *service provider* [4.27] shall be responsible for the installation and commissioning of the human machine interface (*HMI*) and the fitting of connection to antennas for the wireless communication between the infrastructure.

12.4.3 Vehicle data bus

The physical form of the *IVS* is not specified and shall be a market place decision, however this part of ISO 15638 assumes that the *IVS* may not have access to the vehicle databus.

12.4.4 Initial set-up

12.4.4.1 Service provider specification SP18: Prime service provider

The *service provider* [4.27] who installs the *IVS* into a regulated commercial freight vehicle shall do so under contract with the *user* [4.31] and shall assume the role of '*prime service provider* [4.21]'. The *prime service provider* shall be responsible for the initial commissioning of the *IVS* and its subsequent maintenance. In the event that the contract between the *prime service provider* and the *user* is terminated for any reason whatsoever, the *user* shall elect another *service provider* and contract with them to be the *prime service provider*.

On becoming the *prime service provider* [4.21], whether at point of installation and commissioning or subsequently, the *service provider* [4.27] shall advise the *jurisdiction* [4.18] in a manner prescribed by the jurisdiction, that it has become the *prime service provider* to the nominated *IVS*/regulated commercial freight vehicle combination.

The *prime service provider* [4.21] shall be responsible for the maintenance of the *IVS* and any related *TIDs*, and for the transmission and back-up of 'stored data'.

The *prime service provider* [4.21] shall program the *IVS* memory with the IPv6 address of the *prime service provider*, in the form prescribed in ISO 15638-5.

12.4.4.2 Service Provider specification SP19: Set access conditions

The first contracted service provider, and subsequently the *prime service provider* [4.21], shall set the access conditions and shall decide who shall have the possibility to read or write to the *IVS* memory.

12.4.4.3 'Approval Authority' specification AA7: regulated commercial vehicle unique identification

The *approval authority* [4.4] shall assign each regulated commercial freight vehicle a unique identification number or code. According to the regime of the *jurisdiction* [4.18] that identification may be made available to the vehicle operator or to approved *service providers* [4.27]. Guidance as to appropriate coding systems can be found in Annex B of this part of ISO 15638.

12.4.4.4 Service provider specification SP20: IVS unique identification

The *service provider* [4.27] installing the *IVS* shall assign the *IVS* a permanent unique identification or it shall be assigned at the point of its manufacture. The *service provider* installing the *IVS* shall commit both the identification code of the registered commercial freight vehicle, and the unique *IVS* identity to the memory of the *IVS*.

12.4.4.5 Service provider specification SP21: 'Basic Vehicle Data'

The *service provider* [4.27] installing the *IVS* shall commit the permanent elements of the *basic vehicle data* [4.8] (as determined in ISO 15638-5) of the registered commercial freight vehicle to the memory of the *IVS*.

12.4.4.6 Service provider specification SP22: 'Core Application Data'

The *service provider* [4.27] installing the *IVS* shall commit the permanent elements of the *core application data* [4.13] (as determined by the jurisdiction) of the registered commercial freight vehicle to the memory of the *IVS*.

12.5 Interoperability certificate

Manufacturers of sensors and equipment to be connected to the *IVS* for *regulated commercial freight vehicles* [4.25] shall have to prove the interoperability of their products with those already *type approved* [4.29] (for example a card manufacturer will have to prove that its tachograph card is readable by any other *type approved* digital tachograph and vice versa) or against a set of criteria determined by the 'Approval Authority'. These tests shall be performed by a test house approved by the *jurisdiction* [4.18].

12.6 Non-TARV functionality in IVS

12.6.1 Complementary access and use

It shall be permissible, subject to the approval of *jurisdiction regulator* [4.19] from the perspective of preservation of the integrity of the *TARV*, for non-*TARV* functionality to be accommodated within the *IVS*.

12.6.2 Reporting to jurisdiction regulator

The *prime service provider* [4.21] shall document, to the satisfaction of *jurisdiction regulator* [4.19], any non-*TARV* functionality to be provided by the *IVS*.

12.6.3 IVS specification IVS36: Shall not interfere with TARV application service provision

Any non-*TARV* functionality shall be isolated from any *TARV* functionality by and within the *IVS* such that the performance of the *IVS* for *TARV* purposes is not hindered or degraded below the requirements of this part of ISO 15638, and such that the *TARV* is not compromised.

12.6.4 IVS specification IVS37: Shall demonstrate complementariness

The *IVS* manufacturer or the *prime service provider* [4.21] shall document, to the satisfaction of *jurisdiction regulator* [4.19], the design features of the *IVS* which isolate and protect *TARV* functionality from any non-*TARV* functionality.

12.7 Post installation events

12.7.1 Service provider requirement SP23: Replacement of IVS

In the event of the replacement of *IVS* in the regulated vehicle, the *service provider* [4.27] replacing the *IVS* shall have the responsibility to ensure and assure that the new *IVS* is correctly programmed with its new permanent identification and that the data associated with the specific regulated commercial freight vehicle is programmed as if it were a new *IVS*, as defined above, and the replacing *service provider* shall advise the *jurisdiction regulator* [4.19] or his agent of the change of the *IVS* unique and unambiguous identification. The old *IVS* unique identification shall never be transferred to the new *IVS*.

12.7.2 Service provider requirement SP24: Upgrade of the IVS

All *IVS* upgrade work shall be undertaken by or under the supervision of the *prime service provider* [4.21]. After completing any upgrade of the *IVS* the *prime service provider* shall be responsible to ensure that the *IVS* is functioning properly.

12.7.3 Service provider requirement SP25: Repair of the IVS

All *IVS* repair work shall be undertaken by or under the supervision of the *prime service provider* [4.21]. After completing any repair of the *IVS* the *prime service provider* [4.21] shall be responsible to ensure that the *IVS* is functioning properly.

12.7.4 Service provider requirement SP26: Service of the IVS

All servicing of the *IVS*, whether to meet the requirements of the regime of the jurisdiction, or an internal maintenance regime, shall be undertaken by or under the supervision of the *prime service provider* [4.21]. After completing any repair of the *IVS* the *prime service provider* [4.21] shall be responsible to ensure that the *IVS* is functioning properly. The *prime service provider* shall have the freedom to subcontract aspects of maintenance (for example to a garage or test station), but shall retain responsibility to ensure that the *IVS* is functioning properly.

12.8 Change of regulated commercial freight vehicle properties

If any of the properties of the regulated commercial freight vehicle are changed such that the *basic vehicle data* [4.8] needs to be changed the *user* [4.31] shall have the responsibility to advise the *prime service provider* [4.21] and the *prime service provider* shall have the responsibility to update the *IVS* and advise the *jurisdiction* [4.18] in a form prescribed by the *jurisdiction* [4.18].

NOTE The *jurisdiction* [4.18] determines the data that comprises the data concept *core application data* [4.13] (which includes the *basic vehicle data* [4.8]). See 12 above.

Examples of why the *IVS* may need to be reprogrammed with a change of vehicle properties will vary from *jurisdiction* [4.18] to *jurisdiction* according to what the *jurisdiction* determines to be the *core application data* [4.13], but may be reasons such as:

- an error is detected in the *basic vehicle data* [4.8]
- change in the *jurisdiction's* [4.18] regulations for *core application data* [4.13] (for example an additional requirement or change in vehicle classification regulations)
- permanent changes to the vehicle have been made, such as a change of the engine power or emissions, number of axles, vehicle colour.

12.8.1 User responsibility US7: Change of regulated commercial freight vehicle properties

The *user* [4.31] shall be responsible to advise the *prime service provider* [4.21] of any change of vehicle properties whatsoever.

NOTE The *user* [4.31] may reasonably be requested to notify any changes of the vehicle properties, but could argue that he or she does not know what constitutes the 'essential' vehicle properties. Hence he or she should be required to notify all changes to the *prime service provider* [4.21].

12.8.2 Service provider responsibility SP27: Change of regulated commercial freight vehicle properties

When advised by the *user* [4.31] of any changes to the properties of a regulated commercial freight vehicle the *prime service provider* [4.21] shall be responsible to determine if the notified changes affect the *basic vehicle data* [4.8] or *core application data* [4.13] and shall be responsible to update the data in the *IVS* memory accordingly. The means by which that update is made are not specified in this part of ISO 15638, but shall be

in accordance with ISO 15638-1 Clause 12 (Interoperability and the *TARV*-ROAM 'facilities' layer, and ISO 15638-5 (*TARV* Generic vehicle information).

12.9 Activation

12.9.1 Service provider responsibility SP28: IVS activation

The *prime service provider* [4.21] shall be responsible for the activation of the *IVS*, and making any submissions and declarations in respect of the activation that are required by the regime of the *jurisdiction* [4.18] and committing the IPv6 address of the *prime service provider* to the permanent non volatile memory of the *IVS* in the form prescribed in ISO 15638-5.

12.10 Maintenance and continuity of application service provider systems

12.10.1 Update and installation of applications

Although a multi service provider environment has significant benefits, it is also important to consider the complexity that this introduces. A multi service provider environment means that updates to the applications, need to be installed with multiple *service providers* [4.27], each of whom may support a different range of regulated and non-*regulated application services* [4.24]. With software, particularly software operating on different hardware platforms, any change or upgrades incur the risk of introducing errors or faults to other applications. These effects may be different for different *service providers*.

12.10.2 Introduction of new applications

The introduction of new applications has also to be carefully managed. Each new application will require resources of the *IVS*: will make demands on its CPU, its *RAM* and its *ROM*. It is important validate that the existing applications are not compromised to the detriment of their service provision, and that the *IVS* has adequate *RAM* and *ROM*.

12.10.3 Service provider responsibility SP29: System modifications, upgrades and changes

All modifications upgrades and changes to systems shall require full recertification of the system and its affected components.

As an *IVS* may exist in the vehicle without material upgrade for the life of the regulated commercial freight vehicle, which may be in excess of 20 years, new applications should be sparing on their additional processing and memory demands within the *IVS*. The *regulator* [4.19] shall take care that the provision of additional regulated services does not cause a requirement to replace all *IVSs* in the entire regulated commercial freight vehicle fleet in the *jurisdiction* [4.18]. The jurisdiction, its *regulator* [4.19] and *approval authority* [4.4] shall also ensure that additional non-regulated service provision, and particularly a combination of additional application services, does not overload the already installed population of *IVS's*.

When introducing new applications, and at all stages of development and testing, appropriate care should be taken at all stages of the process to prevent uploading viruses or other malicious programs to the *IVS* and its *OBU*(s).

12.10.4 Service provider responsibility SP30: Minimisation of on board processing and memory demands

As a general practice, and in line with current cloud computing concepts, as a general principle for all application services, the *IVS* should be required to process and store only very limited volumes of data, and all significant processing should be effected within the *service provider* [4.27] main system, if necessary downloading the result to the *IVS* (but only when necessary), rather than processing within the *IVS*.

12.10.5 Service provider responsibility SP31: Responsibility for design, development, testing

Except for *jurisdiction* [4.18] provided application service software, the *service provider* [4.27] shall be responsible for the design, development and testing of the application service software and onboard *IVS* implementation and the *prime service provider* [4.21] shall be responsible for continued monitoring of the *IVS* performance.

12.10.6 'Approval Authority' specification AA8: Approve new applications

The *approval authority* [4.4] shall be responsible for approving the introduction of new applications to the *IVS* based on information provided by the application *service provider* [4.27] and independent verification testing.

12.11 Deactivation

In circumstances where the *IVS* is the property of the *user* [4.31] or owner of the regulated commercial freight vehicle, it shall remain with the vehicle for all of the life of the vehicle, so long as the vehicle is used in a jurisdiction requiring use of the IVS. Provisions for change of *prime service provider* [4.21] are given in 8.9. (Contract options).

In circumstances where the *IVS* remains the property of the service provider, on ending a contract to be the *prime service provider* [4.21], the *prime service provider* shall offer the *IVS* to the vehicle owner on reasonable terms, taking into account the length of time that the equipment has been rented. If these terms are not acceptable to the vehicle owner, the *service provider* [4.27] shall be given reasonable access to remove the equipment from the vehicle.

The owner of the vehicle shall then be responsible to ensure that the *user* [4.31] takes steps to ensure that the vehicle is re-equipped to meet the regulations of the *jurisdiction* [4.18].

This part of ISO 15638 makes no specifications regarding the terms of such sale or access conditions for removal, but *jurisdictions* [4.18] are recommended to take such issues into account when determining their regime.

12.12 End of life provisions.

At the end of the life of the regulated commercial freight vehicle, the owner has the responsibility to advise the *prime service provider* [4.21] that the vehicle has been terminated.

12.12.1 User responsibility US8: End of life notification

The *user* [4.31] shall notify the *prime service provider* [4.21] when a regulated commercial freight vehicle has reached the end of its service life and has been terminated.

12.12.2 Service provider responsibility SP32: End of life notification

On receipt of notification from a *user* [4.31] that a regulated commercial freight vehicle has reached the end of its service life and has been terminated, the *prime service provider* [4.21] shall inform the *jurisdiction* [4.18] or its agent of the termination of this *IVS*/regulated commercial freight vehicle combination in a form specified by the *jurisdiction* or its agent.

If the *prime service provider* [4.21] recovers the *IVS* from the vehicle it shall not reissue that *IVS* to any other vehicle with the same *IVS* unique reference number/code. However, if the *IVS* is assigned a new unique reference number/code the equipment may be reused on the same conditions as a new *IVS*, defined above.

13 PROVISIONS TO ENABLE MONITORING AND ENFORCEMENT OF REGULATED COMMERCIAL FREIGHT VEHICLES

13.1 Jurisdiction specification JS8: Definition of regulated commercial freight vehicle

The *jurisdiction* [4.18] shall be responsible to provide and make freely and publicly available a clear and unambiguous definition of the characteristics that determine whether or not a vehicle is classified as a *regulated commercial freight vehicle* [4.25] within its domain.

13.2 Jurisdiction specification JS9: Provision of regulations to monitor and enforce

The *jurisdiction* [4.18] shall be responsible that it has obtained regulations to enable it to monitor and enforce *regulated commercial freight vehicles* [4.25] in order to support its mandated and voluntary *regulated application services* [4.24] for *regulated commercial freight vehicles*.

Enforcement and the means of enforcement shall be determined by the *jurisdiction* [4.18].

14 'Approval Authority' PROCEDURES

14.1 General 'Approval Authority' process

Clause 8.8 specifies the responsibilities in respect of *approval authority* [4.4] approval and the (high level) requirements for *approval authority* approval. This Clause provides further detail of *approval authority* approval procedures. However it is recognised that different *jurisdictions* [4.18] will adopt different regulations and procedures in accordance with their particular requirements, practices and culture. Section 8.8 and this section therefore provide general specification of aspects that need to be provided for, but do not attempt a final specification of requirements, which is left to the *jurisdiction* to provide.

While the specific 'approval' or 'certification' procedures for specific application services are a matter for the jurisdiction and are outside the scope of this (or any) part of 15638, approval authorities are recommended to use the guidance of ISO 17000 and ISO guide 65 when developing and implementing such procedures.

Generally, *approval authority* [4.4] approval refers to the confirmation of certain characteristics of an object, person or organisation. In the ISO 15638 suite of standards deliverables, *approval authority* approval applies to:

- *IVS*
- application *service providers* [4.27]
- *regulated application service* [4.24] systems

and may, at the discretion of the jurisdiction, also apply to

- commercial application service systems.

Requirements for *approval authority* [4.4] approval are specified as tests to be passed. Each requirement leads to a verdict (passed or failed) on which the *approval authority* approval is based.

For example, consider IEC 60529, IP code, which classifies the degrees of protection provided against – among others – water in electrical enclosures, which provides more detailed information than vague marketing terms such as "waterproof". The requirements can be directly defined as test cases.

It is, however, preferable to first define the requirements on a functional level and then define them, wherever possible, as PASS/FAIL test cases. The advantage of this approach is that agreement on the functional requirements can be reached, before reformulating these requirements as tests to be passed. See Figure 2.

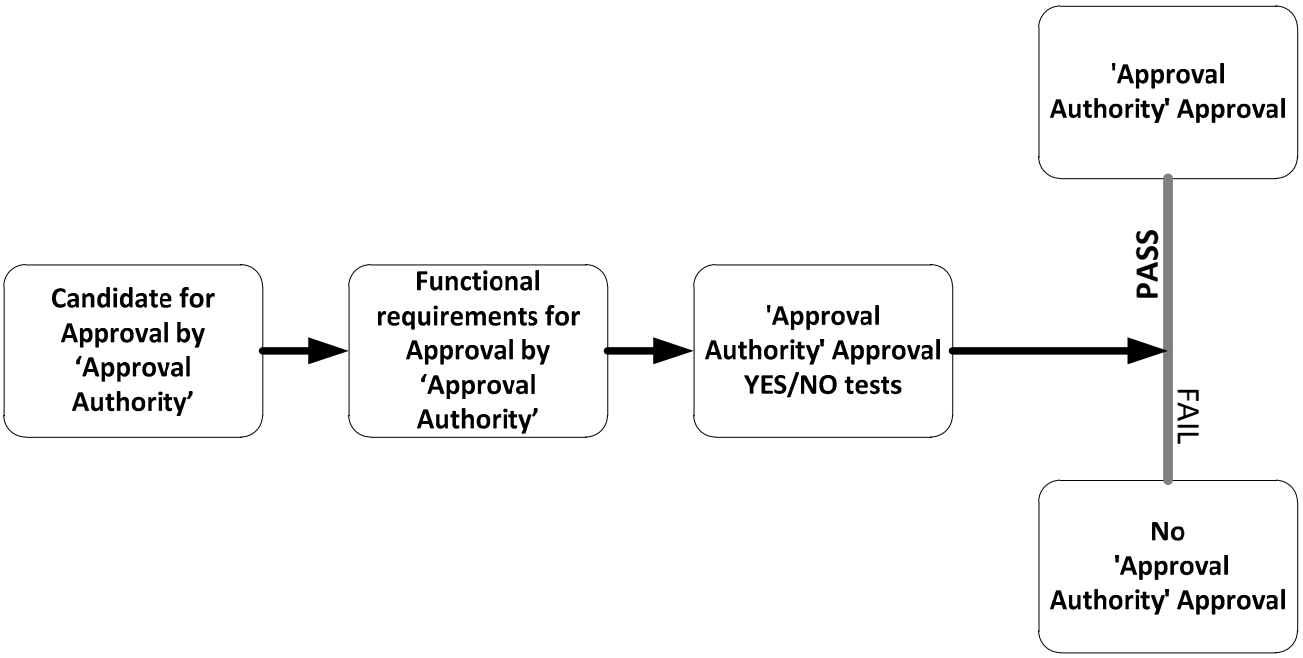

Figure 2 — 'Approval Authority' process for IVS, and service provider and application service systems

However, some test aspects are difficult to reduce to simple PASS/FAIL tests (for example 14.7.4 *service provider* [4.27] charging regime) and rely on the judgement of the inspector. Where this occurs it is recommended to provide the inspector with check lists to get as close as possible to YES/NO, PASS/FAIL checks.

In designing *approval authority* [4.4] approval procedures, it should be borne in mind that companies that fail *approval authority* approval (of themselves or their products during the *approval authority* approval process) might seek recourse to the law, so the *approval authority* approval process must be accurate, sound and court-proof.

14.2 Jurisdiction specification JS10: Provision of 'Approval Authority' test regime

The *jurisdiction* [4.18] shall design and impose the regime for *approval authority* approval testing by the introduction of specific clear and unambiguous regulation in accordance with the customs of the regime. The regulations shall cover at least the definition of what/who is required to be tested and the aspects to be tested and what in principle constitutes a pass or fail of the *approval authority* approval tests the duration of the *approval authority* approval, what happens at the end of the certified period, and the provisions and direct consequences in the event of failure to pass *approval authority* approval tests.

The *jurisdiction* [4.18] shall use its own resources or appoint an agent to manage the *approval authority* [4.4] approval process. This may be the *jurisdiction regulator* [4.19], or it may be another agent which is given the responsibility for the assessment of candidates or candidate products seeking *approval authority* approval and for granting *approval authority* approval where appropriate. That discretion lies entirely with the *jurisdiction*. Throughout the ISO 15638 family of standards deliverables this body is known as the '*approval authority*', although *jurisdictions* are free to use other descriptors for this function.

14.3 Jurisdiction specification JS11: Provision of 'Approval Authority' test suites

The *jurisdiction* [4.18] shall be responsible to design internally, or appoint an *approval authority* [4.4] to design, specific tests to acquire *approval authority* approval. Such tests shall, wherever possible, each have a clear PASS/FAIL criteria and the *jurisdiction* shall determine which tests are 'critical' i.e. the failure of any one of these tests automatically means failure to be certified, and which tests may be retested in the event of failure within a certain range determined in the test procedures, without having to retest all aspects again.

14.4 IVS 'Approval Authority'

The objective of the *IVS approval authority* [4.4] approval process is to determine if an *IVS* and its corresponding equipment (e.g. software) meets minimum standards to assure the required quality, and can operate in an environment where multiple *IVSs* are in the presence of one ITS communication station.

This part of ISO 15638 does not set out formal detailed requirements as to how *IVSs* are *type approved* [4.29], but it shall be a requirement that *IVSs* are manufactured to a standard that enables them to reliably provide the application services determined in the ISO 15638 family of standards deliverables.

Different *jurisdictions* [4.18] may adopt different regimes to ensure this. Some may opt for type approval by an independent test house, others for type approval by a *jurisdiction* managed or appointed test house, others by self-certification etc.

When designing tests for *IVS approval authority* [4.4] approval, it must be remembered that *IVS* will come in different forms, for example those designed into a vehicle at the vehicle build stage, and those installed after the vehicle is manufactured and on the road. *IVS approval authority* approval shall therefore have two distinct aspects.

a) The functioning of the *IVS* in a typical situation

b) The *OBU*(s) that comprise the *IVS*

(b) is satisfied simply by requiring that the provisions of 14.5 are conformed to, and the *IVS* tests therefore focuses on the functioning of the system, while the *IVS* tests described in 14.5 concentrate on the electromechanical aspects of a 'unit' and its connections and fixings.

In respect of *TIDs*, these can be regarded as *OBUs* that may be part of an *IVS*, and are therefore to be covered within the *IVS* tests described in 14.5.

In designing tests for *IVSs*, it has to be remembered that the *IVS* under test may comprise multiple *OBUs* working in concert, and connected to other external sources of data, to provide the *IVS* functionality.

EXAMPLE A prime mover where the *IVS* comprises one unit that houses the communications unit and CPU, a separate unit that comprises the *GNSS*/accelerometer and gyroscope and a link to the vehicle databus, and has two trailers each with its *TID* unit.

IVS may be certified individually on installation to a regulated commercial freight vehicle, with all tests made on installation, or the generic properties of an *IVS* or *OBU* may be *type approved* [4.29] by a process determined by the jurisdiction.

To facilitate type-approval testing, a number of *IVSs*/*OBUs* specified by the *jurisdiction* [4.18], but in any event a minimum of two, shall be provided to a body authorised by the *jurisdiction* to undertake type approval testing. The applicant shall detail the supply of these *IVSs* in a manner prescribed by the *jurisdiction* or its appointed agent.

The *IVS approval authority* [4.4] approval tests will be designed by the *approval authority*,, but in order to comply with this part of ISO 15638 should include testing the following aspects.

14.4.1 IVS specification IVS1: Robustness and suitability

14.4.1.1 Test communication capability

Test that the *IVS* meets the requirements of ISO 16538-2 (*TARV* – Common platform parameters using CALM.)

14.4.1.2 Test electronic capability

Test that the declared electronic capabilities can be achieved by the equipment.

14.4.1.3 Test security

Test that the *IVS* meets the requirements of ISO 16538-4 (*TARV* –System security requirements.)

14.4.2 IVS specification IVS2: Availability

Test that the *IVS* shall always be available (99.99% or better) if the ignition of the vehicle is switched on.

Test that if the *IVS* is for any reason not available, the driver receives a warning which operates reliably in accordance with the specification of the manufacturer.

14.4.3 IVS specification IVS3: Environmental

Test that the *IVS* meets the legislation and regulations of the *jurisdiction* [4.18] in respect of environmental aspects of electronic equipment.

14.4.4 IVS specification IVS4: Secure data storage

Test that the *IVS* the non-volatile data storage equipment is can survive a crash of up to 130 kph.

Test that the non-volatile data storage is *tamper* [4.28] resistant.

Test that there are adequate measures to ensure that the data in the non-volatile data storage and in the *RAM* is accessible only to the application *service provider* [4.27] and cannot be accessed from within the vehicle other than by the *IVS installer* [4.16] and *IVS maintainer* [4.17].

Test that data storage security meets the requirements of ISO 15638-4 (*TARV* – System security requirements).

Test that it is not reasonably possible for collected or stored data or software memory within the *IVS* to be accessible or capable of being manipulated by any person, device or system, other than one authorised by the *prime service provider* [4.21].

14.4.5 IVS specification IVS6: Data input means

Test that there is a means, approved by the jurisdiction, for the driver to input his driving licence number each time he/she takes control of the vehicle.

Test that the non-volatile data storage and *RAM* shall not be available from within the vehicle except to the *IVS installer* [4.16] and the *IVS maintainer* [4.17].

14.4.6 IVS specification IVS7: Central processing unit

Test that the central processor unit comprises at least:

- a processor with a minimum processing capability of 1 GigaHertz or higher
- volatile memory (*RAM*/*DRAM/SRAM* etc.) of at least 100 Gigabytes
- recognised operating system (e.g. Linux)
- means to interact with and process ISO 11519* and ISO 11898** CAN bus data or its SAE J1939 equivalent

Test that the *IVS* is able to perform the program of operations required in order to fulfil regulated service provision.

Test that the *IVS* is capable and programmed to collect and store at least the following data:

a) *IVS* identification
b) *Prime service provider* [4.21] IPv6 address
c) vehicle identification
d) vehicle class identification
e) propulsion storage type
f) *GNSS* data
g) date and time data
h) vehicle position data
i) vehicle
j) vehicle direction of travel data
k) vehicle speed data
l) trailer identification data (if applicable)
m) IPv6address for each subscribed application service
n) alarm status data
o) driver identification (if applicable)
p) load data (if applicable
q) self declaration data (if applicable).

as defined in ISO 15638-5 (*TARV* Generic vehicle information).

14.4.7 IVS specification IVS8: Secure data processing

Test that the device is compliant to all relevant Clauses of ISO 15638-4.

14.4.8 IVS specification IVS9: Connectivity means to/from auxiliary equipment

Test that the *IVS* shall has a means to receive inputs from and communicate with auxiliary equipment using standard physical interfaces (USB2, B3,USB Micro A and B, USB mini A and B, RS232, RS422 etc) and the *CAN bus* [4.9] (PCAN TJA1054 or PCAN-BD10011S) or J1939 bus.

14.4.9 IVS specification 10: IVS clock

Test that the *IVS* shall has an internal clock that operates independently of the supporting external power supply.

Test that in the event the external power supply fails or shuts down, the *IVS* internal clock shall operate for a period of at least 28 days.

Test that the *IVS* internal clock does not deviate by more than 1 second from the UTC date and time over any 28 day period when using *GNSS* signals.

Test that the *IVS* internal clock does not deviate by more than 10 seconds per day from the UTC date and time over any 28 day period when not using *GNSS* signals.

14.4.10 IVS specification IVS11: Communications means

Test that the *IVS* has a means to receive inputs from and communicate with its communications capability and that the nature of that communication complies to one of the options defined in ISO 15638-2.

14.4.11 IVS Classification (IVS12, IVS13, IVS 14)

Check that the *IVS* is classified correctly (Class A and Class B) and if Class A can communicate with the *TID* devices of up to 10 trailers attached to it.

14.4.12 IVS specification IVS21: Power supply

Test that the *IVS* is supplied with a reliable power supply that functions reliably whenever the vehicle ignition is switched on.

Test that the *IVS* has access to a separate protected independent power supply(ies) that in the event of the disconnection of the vehicle power supply enables the *IVS* to remain on standby for a minimum of 7 days.

Test that the *IVS* has access to a separate protected independent power supply(ies) that in the event of the disconnection of the vehicle power supply enables the *IVS* to remain operational for a minimum of 1 hour.

14.4.13 IVS specification IVS 22: external power supply failure/shut down

Test that in the event that the external power supply supporting the *IVS* fails or shuts down, the *IVS*:

a) retains stored data for at least 28 days; and
b) monitors the status of the ignition and other independent movement sensors for at least 7 days.

14.4.14 IVS specification IVS24: GNSS capability

Test that the *IVS* has or has access to global navigation satellite positioning system (*GNSS*) receiver capability consisting of a *GNSS* receiver connected to a *GNSS* antenna.

Test that the *IVS GNSS* receiver and *GNSS* antenna complies with the radio communications regulations of the *jurisdiction* [4.18] (this may be accepted as sight of a conformance certificate) and meets the performance specifications defined by the *jurisdiction***.**

Check that the *IVS GNSS* antenna is mounted in a position that meets the manufacturer's specification or is in a good position to optimise signal strength from the *GNSS* satellites.

14.4.15 IVS specification IVS25: Accelerometer capability

If an accelerometer is fitted test that it operates to the manufacturers specification.

14.4.16 IVS specification IVS26: Gyroscope capability

If a gyroscope is fitted test that it operates to the manufacturers specification.

14.4.17 IVS specification IVS27: Still camera data

Where still images are recorded test that they are recorded as determined in ISO 15638-5 (Clause 9.2.3.1, JPEG/.jpg).

14.4.18 IVS specification IVS28: Video data

Where video images are recorded test that they are recorded as determined in ISO 15638-5 (9.2.3.2, MPEG/.mpg)

14.4.19 IVS specification IVS29: Alarm types and data

Test that the *IVS* generates and stores alarm records in its non-volatile data storage for each of the following events:

a) the external power supply is disconnected from the *IVS*;

b) the external power supply is reconnected to the *IVS*;

c) movement is indicated by the ignition while the external power supply is disconnected from the *IVS*, using two different features independent from the *GNSS* signal. (see 9.27.2)

d) movement is detected by the other independent movement sensor while the external power supply is disconnected from the *IVS*, using two different features independent from the *GNSS* signal.(see 9.27.2)

e) the ignition is disconnected from the *IVS* (with and without external power being connected);

f) the ignition is reconnected to the *IVS* (with and without external power being connected);

g) the other independent movement sensor is disconnected from the *IVS* (with and without external power being connected);

h) the other independent movement sensor is reconnected to the *IVS* (with and without external power being connected);

i) unauthorised access to data in the *IVS* is detected;

j) unauthorised access to *IVS* software is detected;

k) the *GNSS* antenna is disconnected from the *IVS*;

l) the *GNSS* antenna is reconnected to the *IVS*.

Test that the data is stored in the format defined in ISO 15638-5.

14.4.20 IVS specification IVS30: Independent movement sensing

Test that the ignition status is used to provide a record of movement sensing

Test that a second sensor, which shall be one or more of the engine control module, odometer, tachograph, or some other such independent movement sensor such as an accelerometer or gyroscope or combination of the two is used to provide a record of movement sensing.

Test that the connection of the independent movement features to the *IVS* is monitored and reported upon in accordance with 9.27.1 e through 9.27.1 l.

14.4.21 IVS specification IVS31: Vehicle location

Test that the *IVS* is capable of calculating, storing and presenting the vehicle location with data defined in accordance with ISO 15638-5 (8.10 Location)

Test that when providing or recording location data the *IVS* also records and presents the number of satellites present during the calculation as specified in ISO 15638-5.

Test that when providing or recording location data the *IVS* also records and presents the status of the vehicle ignition (on / off / disconnected) as specified in ISO 15638-5.

Test that when providing or recording location data the *IVS* shall also record and present the status of any other independent movement sensors present (movement/no movement/disconnected) as specified in ISO 15638-5.

14.4.22 IVS specification IVS32: When vehicle is powered up (ignition status ON)

Test that the *IVS* immediately the vehicle is powered up performs a self-test without attempting to connect to the network. In the event of a critical system failure which would result in an inability to execute an application service is detected during or following the self-test, test that a warning is given to the driver of the vehicle.

Test that all enrolled application services can commence.

Test that the *core application data* [4.13] and *basic vehicle data* [4.8] fields are updated.

Test that the system can activate any installed update sequences for dynamic information.

Test that the system records the engine start event.

Test that the communication channels are checked and then moved to standby until required.

Test that in the event of that the absence of the possibility of an adequate communication link which would result in an inability to execute an application service as it has been designed, is detected during or following the test of the communications link, a warning is to the driver of the vehicle.

14.4.23 IVS specification IVS33: Communication set-up (1)

Test that when an application *service provider* [4.27] generates request for *core application data* [4.13] or by the application *service provider* that the *IVS* responds in an appropriate manner.

In this use case test that the *IVS* first contacts the application *service provider* [4.27] to advise that it is operating. The details of such communication shall be specified in the application service specification.

Test that on activation of an application service, the *core application data* [4.13] fields are populated and updated in accordance with the requirements of this part of ISO 15638 or the requirements of the application service as appropriate.

Test that where communication for an application is instigated by the vehicle *IVS*, that the *IVS* can successfully instigate the wireless communication with an application *service provider* [4.27] and instigate an example service.

Test that whether the communication set-up is instigated by the *IVS* or an application *service provider* [4.27] that that the *core application data* [4.13] and *basic vehicle data* [4.8] fields are updated.

14.4.24 IVS specification IVS33: Communication set-up (2) SEND 'Core Application Data'

Test that on receipt of an instruction from an application *service provider* [4.27] to '*SEND CAD*' that the *IVS* responds in a proper manner and sends the *CAD* data field to the IPv6 address of the application *service provider*.

Test that the *IVS* is capable to send the *core application data* [4.13] to the application *service provider* [4.27] at any time in accordance with the instructions of the on-board application service programme and 10.2.2 and 10.2.3 - 10.2.5.

14.4.25 IVS specification IVS34: Communication session clear-down

Test that the application *service provider* [4.27] can clear-down an in-progress communication session at any time.

Test that there are measures to ensure that the *IVS* does not clear down any in-progress communication session that was instigated by the application *service provider* [4.27].

Test that, so long as the requirements provisions of the application service permit, the *IVS* is capable to clear-down an in-progress communication session that it instigated at any time.

Test that the session clear-down procedures are as determined in 10.3, 10.4, ISO 15638-2 and the relevant CALM Media standard(s).

14.4.26 IVS specification IVS35: Communication set-up : transfer of 'stored data'

Test that on reaching 'interval I' as determined in 11.4, the data concept *'stored data*' shall be populated with all records created since the last transfer of '*stored data*' to the *prime service provider* [4.21] (or shall have been accumulated in a file since that last data transfer and shall be updated) and the identity and timestamp specified in 11.3 above.

Test that in the event that the communication channel with the application *service provider* [4.27] is already open the *IVS* sends the '*stored data*' field; or the *IVS* first establishes the communication link by 'calling' the IPv6 address of the application *service provider* [4.27] (in accordance with the appropriate CALM media standard and the protocols for that communication medium see ISO 15638-2) and then once the communication channel is open, sends the '*stored data*' field, preceded by one byte of alternate zeros and ones starting with zero (01010101), and 11.4.3 – 11.4.5.

14.4.27 IVS data records deleted only after fulfilment of conditions

Test that *IVS* data records stored in the *IVS* are only be deleted AFTER fulfilment of the following conditions:

The data has been successfully transferred and acknowledged as received by the application service provider

and either

The data is more than one year old

or

The memory allocated in the data specifications in this part of ISO 15638 or ISO 15638-5 has been filled and the data field is overwritten as specified elsewhere in this part of ISO 15638 or in ISO 15638-5.

or

To meet the requirements of ISO 15638-4.

14.4.28 IVS unique identification

Test that the *IVS* can be programmed with the *IVS* permanent unique identification or has so been programmed at the point of its manufacture. The *service provider* [4.27] installing the *IVS* shall commit the identification code of the registered commercial freight vehicle, and the unique *IVS* identity and the IPv6 address of the *prime service provider* [4.21], to the memory of the *IVS*.

14.4.29 Identification code of the registered commercial freight vehicle

Test that the *IVS* can be programmed with the identification code of the registered commercial freight vehicle *IVS* permanent unique identification in accordance with ISO 14816 CS4 Vehicle licence number coding (4.10)

```
CS4 ::= SEQUENCE {
        countryCode   CountryCode,   alphabetIndicator   AlphabetIndicator,
        licPlateNumber LicPlateNumber
}
```

14.4.30 Non-TARV functionality in IVS: Complementary access and use

Test that the *IVS* is capable to support non *TARV* functionality, and that any non-*TARV* functionality is isolated from any *TARV* functionality by and within the *IVS* such that the performance of the *IVS* for *TARV* purposes is not hindered or degraded below the requirements of this specification, and such that the *TARV* is not compromised.

14.4.31 Change of regulated commercial freight vehicle properties

Test that any of the properties of the regulated commercial freight vehicle may be changed by the *prime service provider* [4.21] and that there are measures to prevent alteration of this data by any other party.

14.5 IVS 'Approval Authority'

This part of ISO 15638 does not set out formal detailed requirements as to how *IVSs* and *TIDs* are *type approved* [4.29], but it is a requirement that *IVSs* and *TIDs* are manufactured to a standard that enables them to reliably provide the application services determined in the ISO 15638 family of standards deliverables.

Different *jurisdictions* [4.18] may adopt different regimes to ensure this. Some may opt for type approval by an independent test house, others for type approval by a *jurisdiction* managed or appointed test house, others by self-certification etc.

When designing tests for *IVS approval authority* [4.4] approval, it must be remembered that *IVS* will come in different forms, however, by definition, an *OBU*, unlike many *IVSs*, will comprise a single self-contained unit which can be certified independent of the vehicle in which it is to operate.

The *IVS* tests described in this Clause concentrate on the electromechanical aspects of a 'unit' and its connections and fixings.

In respect of *TIDs*, these can be regarded as *OBUs* that may be part of an *IVS*, and are therefore to be covered within the *IVS* tests described in this clause.

The *IVS approval authority* [4.4] approval tests will be designed by the *approval authority*, but in order to comply with this part of ISO 15638 should include testing the following aspects.

14.5.1 Unique unambiguous identifier (IVS ID)

Test that the *OBU* (that comprises part of an *IVS*), has a unique unambiguous identifier (*OBU* ID), as specified in ISO 15638-5 (*TARV* - Generic vehicle information) that will be used to unambiguously identify the particular *OBU*.

14.5.2 Affixation

Where already installed on a prime mover/rigid truck/trailer, test that the *IVS* is robustly connected to the prime mover/rigid truck, or in the case of a *TID*, a trailer.

14.5.3 Test mechanical capability

Test that *IVS* survives and remains functioning when the vehicle is subjected to a crash into a barrier as described in E/ECE/TRANS/505} Rev.1/Add.93/Rev.1 Regulation No. 94 at a speed of 130 kph.

14.5.4 Test connection to prime mover/rigid truck

Test that *IVS* survives and remains functioning when the vehicle is subjected to a crash into a barrier as described in E/ECE/TRANS/505} Rev.1/Add.93/Rev.1 Regulation No. 94 at a speed of 130 kph.

14.5.5 Test durability

Test that *IVS* survives and remains functioning when the vehicle is subjected to a crash into a barrier as described in E/ECE/TRANS/505} Rev.1/Add.93/Rev.1 Regulation No. 94 at a speed of 130 kph.

14.5.6 Test vibration

Test that *IVS* and its security seals survive and remain functioning/intact when subjected to vibration to a reference specified by the *jurisdiction* [4.18].

14.5.7 Test bump/impact/shock

Test that *IVS* and its security seals survive and remain functioning/intact when subjected to an impact to a reference specified by the *jurisdiction* [4.18].

14.5.8 Test fall

Test that *IVS* and its security seals survive and remains functioning/intact when subjected to a fall impact to a reference specified by the *jurisdiction* [4.18].

14.5.9 Test humidity

Test that *IVS* survives and remains functioning when subjected to the temperature ranges specified in a reference specified by the *jurisdiction* [4.18].

14.5.10 Test temperature

Test that *IVS* survives and remains functioning when subjected to the humidity specified in a reference specified by the *jurisdiction* [4.18].

14.5.11 Test dust and water ingress protection (1)

Test that *IVS* components exposed to the elements survive and remains protected and functioning when subjected to dust and water ingress protection requirements according to IEC 60529 Ed 2.1:2001; Table 7, Item 6 and 13.4 and Table 8, Item 6 and 14.2.6.

14.5.12 Test dust and water ingress protection (2)

Test that *IVS* components mounted in the cabin survive and remains protected and functioning when subjected to dust and water ingress protection requirements of IEC 60529 Ed 2.1:2001; Table 7 Item 4 13.4 and Table 8, Item 4 and 14.2.4.

14.5.13 Test radio frequency and electrical interference

Test that *IVS* survives and remains functioning when subjected to radio frequency and electrical interference as defined in 2004/104/EC, sections 6.7 and 6.8 with functional status ‘A’, Table 1.

14.5.14 Electromagnetic emissions

Test that electromagnetic emissions from the *IVS* and *TID* shall not exceed the limits in 2004/104/EC, sections 6.9 using the pulse amplitude levels for either 12 or 24 volt systems as appropriate, Table 2.

Test that electromagnetic emissions from the *IVS* and *TID* shall not exceed the limits in *CISPR22*:2006 (CIS participants report 22:2003), Class B, Table 6.

14.5.15 IVS specification IVS9: Connectivity means to/from auxiliary equipment

Test that the *IVS* has a means to receive inputs from and communicate with auxiliary equipment using standard physical interfaces (USB2, B3,USB Micro A and B, USB mini A and B, RS232, RS422 etc) and the CAN Bus (PCAN TJA1054 or PCAN-BD10011S or J1939 bus).

14.5.16 Equipped trailer identification devices

The form and capability of trailer identification devices and their connection to the *IVS* is not standardised in this part of ISO 15638, though it is clearly preferable that a *user* [4.31] uses common systems throughout its fleet to enable changes to prime mover/trailer combinations. However, that is a commercial issue and not a standardisation issue at the point of time that this part of ISO 15638 has been developed.

The *user* [4.31] may also elect to connect a *TID* physically via a wired connection, or use one of a number of wireless communications connections. These aspects are not standardised, only that there is a communications connection between the *TID* and the *IVS* that achieves certain characteristics and performance, and acts as any other *OBU* that forms part of the *IVS*.

In the event that the *IVS* is a trailer identification device (*TID*):

14.5.16.1 IVS specification IVS19: Trailer identification device requirements

Test that the trailer identification device comprises:

- Central processor
- *RAM*
- include non-volatile programmable read-only memory.

Test that the trailer identification device (*TID*) has non-volatile programmable read-only memory of a minimum of 1 gigabyte.

When the *TID* is installed on to the trailer, test that the trailer ID has been recorded permanently into the non-volatile programmable read-only memory of the *TID*.

Test that there are measures to ensure that it shall not be possible to alter the Trailer ID in the non-volatile programmable memory without making the *TID* permanently inoperable.

14.5.16.2 IVS specification IVS18: Equipped trailer identification devices

Test that the equipped trailer is equipped with a 'trailer identification device' (*TID*) in order to enable automatic identification and recording of fitted trailers by the *IVS*.

Test that the *TID* is capable to uniquely identify:

a) the trailer

b) data pertaining to the connection of the trailer to the prime mover/rigid truck, as part of the performance of an application service

c) may provide identification and status information about the cargo on-board the trailer

in conformance with ISO 15638.

While the form of the trailer identification device is not standardised test that it is robustly connected to its trailer and is inclusive of the hardware, software and communications (wired cabling or wireless) and connections leading up to, but not including the *IVS*.

Test that the trailer identification device shall only communicate with the prime mover *IVS* when the trailer is physically connected to the prime mover or another connected trailer.

The means by which this is achieved is not standardised, but that it is achieved is a requirement.

NOTE This provision does not prohibit the use of untethered trailer tracking systems installed and operated independently of any mandated system, and applies only to *TIDs* that communicate with the *IVS*.

14.5.16.3 IVS specification IVS20: Integrity of trailer identification

Test that the transmission of trailer identification data from the *TID* to the *IVS* supports a form of Trailer ID data authentication (i.e. some form of message authentication code only known and accessible to the application service provider), subject to the approval of the jurisdiction, that can prove the origin and integrity of the trailer ID (*TID*) data.

Test that such authentication complies to ISO 15638-4 (*TARV* - System security requirements)

14.5.16.4 IVS specification IVS15: Physical trailer marking

Where the *IVS* is a *TID*, check that the trailer ID has been visibly etched or marked on the outside casing of the trailer in a manner prescribed by the *jurisdiction* [4.18].

14.5.16.5 IVS specification IVS17: Freight land conveyance content identification and communication

Where the *IVS* is a *TID* test that the equipped trailer ID uses a unique identification scheme in accordance with ISO 26683-2 (Freight land conveyance content identification and communication – Application profiles) or ISO 17262 (Intelligent transport systems — Automatic vehicle and equipment identification — Numbering and data structures) or an unambiguous identification scheme specified by the *jurisdiction* [4.18] (in which case the *jurisdiction* [4.18] shall accept the responsibility to ensure that the identification scheme is unique and unambiguous).

14.5.17 IVS specification IVS23: Security seals

Test that the *OBU* is protected by security seal(s) to ensure detection of any unauthorised removal or opening of the *OBU* in accordance with the regulations determined by the *jurisdiction* [4.18].

Test that removal or opening of an *OBU* is only possible by breaking the security seal(s) and the security seal(s) is such that if broken they cannot be reinstated.

Inspect that *OBU* shall be placed in a position that facilitates inspection of the integrity of the security seal(s).

Test that security seal(s) include measures that will clearly display signs of any unauthorised access, either visually and/or physically.

14.6 Application service provider ‘Approval Authority’

14.6.1 General requirements

TARV application services will only be provided by entities certified by the *approval authority* [4.4] as an approved or ‘certified’ application *service provider* [4.27].

The objective of the application *service provider* [4.27] *approval authority* [4.4] approval process is to determine if an applicant application *service provider* and its corresponding systems meet minimum standards to assure the required quality.

This part of ISO 15638 does not set out formal detailed requirements as to how application *service providers* [4.27] are certified, but it is a requirement that application *service providers* operate to a standard that enables them to reliably provide the application services determined in the ISO 15638 family of standards deliverables.

The requirements for an application *service provider* [4.27] to be certified shall be determined by the jurisdiction, or the *jurisdiction regulator* [4.19] acting as the agent of the jurisdiction, and implemented via the function of the approval authority [4.4] (however that function is organised by the jurisdiction).

An organisation is certified as being able to competently complete the tasks to be fulfilled as a provider of application services for *regulated commercial freight vehicles* [4.25]. *Approval authority* [4.4] approval of *service providers* [4.27] will include requirements for both the organisation and the processes.

It is recommended that in approving an application *service provider* [4.27] for *regulated commercial freight vehicles* [4.25], the maximum number of vehicles that a *service provider* is certified to support forms part of the *approval authority* [4.4] approval.

While not attempting to determine the regulatory regime of the jurisdiction, in order to minimise the day to day workload on the system, it is strongly recommended that as part of the application *service provider* [4.27] *approval authority* [4.4] approval, the applicant should be required to commit that it shall only install *IVSs* and *TIDs* which have been type-approved by the *approval authority*.

Different *jurisdictions* [4.18] may adopt different regimes to ensure this, but there are some common features which include that *approval authority* [4.4] approval as an application *service provider* [4.27] is granted on the basis of the *approval authority* being satisfied as to the conformance with this specification of the application service providers:

a) application *service provider* [4.27] system, being the application service provider's hardware and software (excluding *IVSs*, *OBUs*, *TIDs*) used in the collection, processing, testing, storage and reporting of *TARV* data;

b) Quality monitoring

14.6.2 In the event of malfunction

Test that there are systems in place that in the event that the application *service provider* [4.27] system does not function in accordance with its specification, the application *service provider* [4.27] system:

a) immediately commences to resolve the malfunction

b) immediately reports the malfunction (including an estimated resolution period) to *jurisdiction regulator* [4.19]

c) reports the malfunction to its client within a timeframe agreed in the service contract between the application *service provider* [4.27] and the application service provider

d) has measures in place to complete the resolution process to the reasonable satisfaction of *jurisdiction regulator* [4.19]

e) has procedures, equipment and resources available such that, in the event of a component part of the system becoming inoperable, the application *service provider* [4.27] system can be returned to an operational state within a defined number of working days

f) has documented their plan for duplicating *TARV*- application service system operations in the event of a catastrophic event, including procedures for activating critical information systems in a new location and recovering critical information systems within a defined number of working days

g) has documented all installation, system, software, programmed maintenance and remediation-of-malfunction activity for the application *service provider* [4.27] system

h) has in place systems and equipment to maintain archives of the documentation for a period of not less than a number of years defined by the *jurisdiction* [4.18] (a minimum of four years is recommended).

14.6.3 Service provider specification SP4: Service provision

Test that the *service provider* [4.27] is capable to provide nominated *regulated application services* [4.24] to *regulated commercial freight vehicles* [4.25], interacting wirelessly with the vehicle to collect relevant data from the *IVS*, process the data and provide the *jurisdictions* [4.18] reports according to the requirements of the application service provided (as specified by the *jurisdiction* [4.18] in respect of *regulated application services* [4.24]), and provide relevant data to the *user* [4.31] in accordance with its contract with the *user*.

Regulated application service [4.24] provision includes collecting data from the vehicle which constitutes a crucial part of the service provision, but is only a part of the service provision. Other components to be tested are the sorting and evaluation by and at the *service provider* [4.27] and communicated to the *jurisdiction* [4.18] (as demanded by the regulation) and to the *user* [4.31] (as agreed in the contract between the *service* **provider** [4.27] and the user).

14.6.4 Service provider specification SP5: Service provider charging regime

Examine the *service providers* [4.27] specimen contracts for users to ensure that terms, conditions and charges to users are fair and reasonable, within the context of the agreement and contracts between the *jurisdiction regulator* [4.19] and the *service provider* [4.27] for the provision of the regulated application service.

14.6.5 Service provider specification SP6: Service provider charging fees on behalf of jurisdiction regulator

Where appropriate, to examine the *service providers* [4.27] arrangements and test its systems to collect fees from the *user* [4.31] as required by the regulation on behalf of the *jurisdiction regulator* [4.19] (for example fees for permits, road use payment, additional policing, possibly even fees for violations) collecting these fees from the *user* and forwarding these payments to the *jurisdiction* [4.18].

14.6.6 Service provider specification SP7: Service provider transmission of data to the jurisdiction and/or its agents

Where appropriate, to examine the *service providers* [4.27] arrangements and test its systems to transmit raw road usage data to the jurisdiction, as required by the regulation of the *jurisdiction* [4.18].

14.6.7 Service provider specification SP8: Provision of non-regulated commercial services

Where permitted by the *jurisdiction* [4.18] that *service providers* [4.27] may also provide additional commercial services to users using the same *IVS*, to test that the systems of the *service provider* [4.27] ensure and assure that the provision of a non-regulated service does not affect the quality of the service provision of any regulated services in any significant way.

14.6.8 Service provider specification SP9: Wireless communications service provision

Test that wireless media used conforms to ISO 15638-2 and meets the requirements of the regulation in respect of the wireless provision of the application services, and when appropriate that the application *service provider* [4.27] has valid and viable contracts that are fit for purpose with any required wireless communications *service providers*.

14.6.9 Service provider specification SP12/SP18/SP19/SP20/SP23/SP24/SP25/SP26/SP28: Responsibility of the service provider contracted to maintain an IVS

Examine the support arrangements proposed by the candidate application *service provider* [4.27] to ensure that they are designed to provide an adequate level of installing programming and commissioning, maintenance servicing, repair, support, upgrading and replacement of *IVSs* in conformance with the provisions of the ISO 15638 suite of standards, with special attention to ISO 15638-3 (this part) and ISO 15638-5.

14.6.10 Service provider specification SP16/SP21: 'Basic Vehicle Data'

Test that the candidate application *service provider* [4.27] is capable to commit the permanent *basic vehicle data* [4.8] of the registered commercial freight vehicle to the memory of the *IVS*.

14.6.11 Service provider specification SP17/SP22: 'Core Application Data'

Test that the candidate application *service provider* [4.27] is capable to commit any additional permanent *core application data* [4.13] (as determined by the jurisdiction) of the registered commercial freight vehicle to the memory of the *IVS*.

14.6.12 Service provider specification SP19: Set access conditions

Test that the candidate application *service provider* [4.27] is capable to set the access conditions and shall decide who shall have the possibility to read or write to the *IVS* memory.

14.6.13 Service provider responsibility SP27: Change of regulated commercial freight vehicle properties

Test that the candidate application *service provider* [4.27] is capable to update the data in the *IVS* memory accordingly. The means by which that update is made are not specified in this part of ISO 15638.

14.7 Application service 'Approval Authority'

14.7.1 General requirements

It is important to understand the difference between *approval authority* [4.4] approval of the application *service provider* [4.27] and *approval authority* approval of the application service. Where there is only one *service provider* providing the service across the jurisdiction, or where a *user* [4.31] is tied to a single *service provider* for the provision of all of its services, the difference may at times seem somewhat academic, however there is a functional difference of significance, which is described in greater detail in ISO 15638-1.

ISO 15638-3, this part of ISO 15638, provides specification for two simple generic application services:

- *core application data* [4.13]
- Stored data

ISO 15638-5 will provide some core common requirements definitions for application services which it is expected will be implemented in some jurisdictions. Again, the election of which application services are implemented, and the election of whether they are supported or mandated, is the choice of the *jurisdiction* [4.18].

ISO 15638-5 provides common core specification for *regulated application services* [4.24] that *jurisdictions* [4.18] may elect to implement. The specifications in ISO 15638-5 therefore provide *jurisdictions* with a way to ensure that the service provided and received for these application services is homogenous across its regime. However, *jurisdictions* or their appointed *regulator* [4.19] or *approval authority* [4.4] retain responsibility to ensure that the quality of service provision meets their requirements and is consistent from *service provider* [4.27] to *service provider*.

For regulated services, both the inputs and outputs, together with the process requirements to provide the service, need to be specified in a way that is independent of any *service provider* [4.27] or *IVS* technology. Process requirements refer to the IT system used in, for example, the collection, processing, data storage, data reporting, security and quality management procedures. The application *service provider* system shall provide sufficient transfer capability in its specified communication coverage area, and sufficient storage and processing capacity to support the number of *IVSs* for which it has been certified, so the minimum specifications for these requirements shall also be defined for each application service.

This part of ISO 15638 does not set out formal detailed requirements of how application services are defined, certified or *type approved* [4.29], but in all cases it is a requirement that:

- application services are specified to a standard that enables them to reliably provide the application services determined in the ISO 15638 family of standards deliverables
- the IPv6address of each application service for which the *user* [4.31] has enrolled is committed to the permanent non-volatile memory of the *IVS*.

Different *jurisdictions* [4.18] may adopt different regimes to ensure this. Some may opt for type approval by an independent test house, others for type approval by a *jurisdiction* managed or appointed test house, others by self-certification etc.

14.7.2 Application service 'Approval Authority' tests

Each application service, shall be tested to assure that:

a) The system provides the application service and its data consistent with its specification and documentation

b) The documentation is adequate

c) The provision of the application service does not adversely impact the provision other *regulated application services* [4.24].

Where *service providers* [4.27] are also permitted to provide commercial services to users using the same **IVS** the commercial service systems shall be tested to assure that the provision of a non-regulated service does not affect the quality of the service provision of any regulated services.

The technical requirements for a service provision should be performance based. That is, the *jurisdiction regulator* [4.19] defines required outputs and it is up to each potential *service provider* [4.27] to establish, to the satisfaction of the *jurisdiction regulator*, or its *approval authority* [4.4], that its equipment and related back-office systems deliver the required outputs. The *jurisdiction regulator*, and its *approval authority*, should not normally specify the particular equipment and systems required. Thus, competing companies whose equipment and systems differ significantly may be certified, as long as they deliver the required outputs.

This enables *service providers* [4.27] to have the flexibility to take full advantage of innovative, cutting edge ITS technologies when designing and developing their equipment and systems, and to evolve those systems over time as technology advances. Coupled with market competition between *service providers* (where permitted by the jurisdiction), this flexibility will ensure that the technology keeps pace with world-wide advances in broader ITS technologies.

The format of *approval authority* [4.4] approval tests for application services will depend both on the nature of the service provided and the regime of the *jurisdiction* [4.18]. The *approval authority* shall therefore have the responsibility to develop appropriate tests to meet the criteria in this, together with any additional requirements of the *jurisdiction***.**

14.7.2 Service provider specification SP3: Application service definition

Review the application service specification to identify any obvious inconsistencies.

Test that, to a test suite of input data, the system under test for the provision of the application service for *regulated commercial freight vehicles* [4.25], produces identical outputs to the test suite reference output data.

14.7.3 HMI aspects

Test the system both at the *service provider* [4.27] and in the vehicle to assure that human machine interface aspects are to an acceptable standard (as determined by the jurisdiction), and that any instructions to the vehicle *user* [4.31] or driver are clear and unambiguous and do not pose any road safety dangers.

14.7.4 Documentation

Check that the application service is adequately and properly documented.

14.7.4 Service provider specification SP5: Service provider charging regime

Examine the *service providers* [4.27] specimen contracts for users for the provision of the application service sdiction under test to ensure that terms, conditions and charges to users are fair and reasonable, within the context of the agreement and contracts between the *jurisdiction regulator* [4.19] and the *service provider* for the provision of the regulated application service.

14.8 Maintenance and continuity of application service provider systems

NOTE For context sees 12.10.4 – 12.10.6.

14.8.1 Service provider responsibility SP30: Minimisation of on-board processing and memory demands

Examine applicant application service provision systems to ensure that on-board processing and memory demands are reasonably minimised.

14.8.2 Service provider responsibility SP31: Responsibility for design, development, testing (continued monitoring of the IVS performance)

Test that the *prime service provider* [4.21] has systems for continued monitoring of *IVS* performance.

15 Auditing

The application *service provider* [4.27] shall carry out both internal *audits* [4.5] and formal external *audits* by a qualified independent party. The form and frequency of such *audits* shall be determined by the *jurisdiction* [4.18]/*jurisdiction regulator* [4.19], however should ascertain whether the *approval authority* [4.4] approval is still valid, and if not provide opportunity to identify and remedy the problem, and if necessary recommend to the *jurisdiction regulator* that the contract of the application *service provider* [4.27] is terminated.

Audits [4.5] may be used to reapprove application *service providers* [4.27] after a certain period of time, or that function may remain a determined process at the end of the *approval authority* [4.4] approval period, at the discretion of the *jurisdiction* [4.18].

The application *service provider* [4.27] shall document all internal *audits* [4.5], including feedback received and corrective actions taken, and shall provide reports to the *jurisdiction regulator* [4.19] as specified by the *jurisdiction* [4.18].

IVSs shall also be audited from time to time to assure that they remain compliant. The frequency of such *audit* [4.5], its scope or sampling, and other related issues shall be determined by the *jurisdiction* [4.18] and implemented by the *jurisdiction regulator* [4.19] or *approval authority* [4.4] according to the regime of the *jurisdiction***.** Where the *IVS* forms part of a general on-board platform, such *audit* shall ensure that adequate resource of the general on-board platform is reserved for the function of the *IVS* for the regulated commercial freight vehicle.

16 Privacy

16.1 Business privacy

16.1.1 General

In case of the provision of *regulated application services* [4.24] for *regulated commercial freight vehicles* [4.25], compliance with the regulations is a condition of use and license, so business privacy is not an issue of choice for the *user* [4.31].

However, in order to comply, as appropriate, with European data privacy directives, the APEC privacy framework, OECD's 1980 guidelines on the protection and privacy and trans-border flows of personal data (OECD Guidelines), and national implementation of these and local privacy requirements, some essential rules need to be followed. Refer to ISO TR 12859 for detail of these international regulations.

16.1.2 Explicit and legitimate and must be determined at the time of collection of the data

Specifically, the purposes for which data is collected and/or stored must be

'Explicit and legitimate and must be determined at the time of collection of the data'

and use of the data limited to the fulfilment of those purposes (or such others as are not incompatible with those purposes specified); and '*the subsequent use shall be limited to the fulfilment of those purposes (or such others as are not incompatible with those purposes) All personal data collected shall be adequate, relevant and not excessive in relation to the purposes for which they are processed';*

(EU Privacy Framework. 7.14.11 Cl 28, 56,57; 7.19.5 (c) ; OECD Part 2. Cl.9).

16.1.3 Not further processed in a way incompatible with the purposes for which it was originally collected

Data, and especially personal data, shall not be further processed or used in a way incompatible with the purposes for which it was originally collected.

(EU Privacy Directive 7.14.1.1 Cl. 28,29; 7.19.5 (b); 7.40.1 (2); OECD Part 1 Cl 9, 24).

16.1.4 Not be disclosed without the consent of the data subject

Data shall not be disclosed, made available or otherwise used for purposes other than those specified.

(EU Privacy Directive 7.4)

To secure such information is a challenge for the organisational structure and internal processes. The data collection process must be organised in such a way that the staff does not have full access to all collected data. It is very common to separate several data streams. For example, staff concerned with movement data should not have access to financial data and vice versa.

Application service systems shall take all reasonable precautions against hacking or other access to their data either by employees or third parties.

The application *service provider* [4.27] has access to detailed, sensitive movement data of companies. Such data may also have value to competitors or the providers of other goods and services.

Jurisdictions [4.18] may be tempted to use these data for other purposes, but would find themselves in violation of EC or APEC regulations if they do.

16.2 Driver privacy

Although driver privacy is not a main issue for *regulated application services* [4.24] for *regulated commercial freight vehicles* [4.25], the element of privacy between driver, user, and *jurisdiction* [4.18] is paramount. The aspects in 16.1 above are all very relevant to driver privacy as well, whether the data is directly personal (such as driver ID) or whether data is subsequently aggregated and regardless of whom the data is aggregated by (for example aggregating the driver identity and the location identity of the truck, and time, provides the drivers location at a particular point in time.) In EU and many *jurisdictions* of members of APEC, the application *service provider* [4.27] will be expected to take positive measures to reasonably prevent the misuse of data. (for example, in the European eCall service provision, where multiple locations are provided to enable the direction of travel to be identified, it is forbidden to transmit the timing of the multiple location events to prevent the data to be used for the calculation of vehicle speed). All aspects of ISO TR 12859 shall be taken into consideration, and although that deliverable is only a technical report, it summarises legal requirements in most countries in the world which need to be complied with.

17 Interoperability

ISO 15638-1 (*TARV* Framework and architecture) provides description of the interoperability approaches of the ISO 15638 suite of standards deliverables, and 12 of that standards deliverable specifically defines provisions for Interoperability and the *TARV-ROAM* 'facilities' layer.

Commands to access *IVS* data are specified in ISO 15638-5 (Generic vehicle information).

The third step to achieve interoperability is accomplished by the provision for a common specification for *basic vehicle data* [4.8], and common options for *core application data* [4.13] specified in ISO 15638-5.

The core common specifications to provide a number of *regulated application services* [4.24] are defined in ISO 15638-6.

The framework to provide non-regulated application services are defined in ISO 15638-7.

A further key approach to achieve interoperability is to rely wherever possible to specification by reference to other standards for identification and for commercial vehicle applications.

18 Legal, regulatory and enforcement aspects

Legal and regulatory aspects are the responsibility of each jurisdiction, who have freedom to determine them as they see fit within the framework of international law and their domestic environment. See also 13.

19 Quality of service requirements

19.1 General

This part of ISO 15638 contains no specific detailed requirements concerning quality of service. Such aspects will be determined by a *jurisdiction* [4.18] as part of its specification for any particular regulated application service.

Although not specified as a requirement in this standard, the quality of service aspects monitored and measured, through test procedures, test results and operational results, and the quality of the performance of the algorithms that measure them, should include aspects such as:

- compare position records against the spatial conditions
- speed records and events
- alarms
- continuity of records collected
- number of system inconsistencies and errors
- *Tampering* [4.28] reporting and frequency of *tampering* [4.28] alarms and consequent malfunctions
- etc.

19.2 IVS and TID type approvals and monitoring

The *jurisdiction* [4.18] shall establish a regime to type approve *IVS* and *TID* products for use in *regulated commercial freight vehicles* [4.25]. See 8.8 and 14 for specification of these aspects.

The *jurisdiction regulators* [4.19] are recommended to maintain ongoing quality monitoring of all approved *IVSs* and *TIDs*.

NOTE This could for example be achieved through a quality monitoring station operated on behalf of the *jurisdiction* [4.18] to facilitate the monitoring of the performance of Type-approved *IVS* and Type-approved *TIDs*, if applicable, to ensure their continued compliance with this specification and the requirements of the jurisdiction, maintaining a log of performance for subsequent analysis. Setup should be as representative of a normal installation as is possible.

All quality monitoring documentation should be retained for a period of not less than four years or as directed by the jurisdiction [4.18], whichever is greater.

19.3 Application service provider system specifications

The *jurisdiction* [4.18] shall establish a regime to type approve application service systems for *regulated commercial freight vehicles* [4.25], offered by application *service providers* [4.27] to users. It is a requirement that application service systems are developed to a standard that enables them to reliably provide the application services determined in the ISO 15638 family of standards deliverables. See 8.8 and 14.

Subsequent to approval of an application service system for *regulated commercial freight vehicles* [4.25], certified application *service providers* [4.27] shall not, without prior written approval of *jurisdiction regulator* [4.19] by way of re-approval:

a) make any change to its application *service provider* [4.27] system or quality monitoring arrangements; and

b) make any material change to its quality control and measurement systems.

20 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 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* [4.18] and shall abide by the privacy laws and regulations of the implementing *jurisdiction* [4.18] 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 and 16 of this part of ISO 15638 in this respect.

21 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 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 wireless 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 ISO 15638-6 and ISO 15638-7 contain no direct patents nor intellectual property other than the copyright of ISO. However, national, regional or local instantiations of any the applications services defined in ISO 15638-6 and ISO 15638-7, or of the generic vehicle information defined in ISO 15638-5, the security requirements contained in ISO 15638-4, or the requirements of this part of ISO 15638, may have additional requirements which may have patent or intellectual property implications. The reader is referred to the regulation regime of the *jurisdiction* [4.18] and its regulations for instantiation in this respect.

Annex A
(informative)

Summary of Requirements and specification categories by actor

A.1 General

This Annex summarises the requirements of this part of ISO 15638 by actor [4.1] class for quick reference.

The reader is advised that each requirement may take multiple actions to satisfy, and the referenced clauses of the main document should always be consulted for the detail of what is required.

A.2 Jurisdiction

JS1	*Jurisdiction* [4.18] specification: Definition of *regulated application services* [4.24] for *TARV*	s.8.7.1
JS2	*Jurisdiction* [4.18] specification: Definition of status of *regulated application services* [4.24] for *TARV*	s.8.7.2
JS3	*Jurisdiction* [4.18] specification: Obtain supporting legislation/regulation for a *regulated application service* [4.24] for *TARV*	s.8.7.3
JS4	*Jurisdiction* [4.18] specification: Manage and regulate the provision of the *regulated application services* [4.24]	s.8.7.4
JS5	*Jurisdiction* [4.18] specification: create or appoint an *approval authority* [4.4]	s.8.8.1
JS6	*Jurisdiction* [4.18] specification: *core application data* [4.13]	s.12.1.1
JS7	*Jurisdiction* [4.18] specification : *basic vehicle data* [4.8]	s.12.2.1
JS8	*Jurisdiction* [4.18] specification: Definition of regulated commercial freight vehicle	s.13.1
JS9	*Jurisdiction* [4.18] specification: Provision of regulations to monitor and enforce	s.13.2

A.3 'Approval Authority'

AA1	*approval authority* [4.4] specification: Consider and appoint candidates to be *service providers* [4.27]	s.8.8.2
AA2	*approval authority* [4.4] specification: Test and approve *service providers* [4.27]	s.8.8.3
AA3	*approval authority* [4.4] specification: Audit *service providers* [4.27]	s.8.8.4
AA4	*approval authority* [4.4] specification: Type approve *IVS*	s.8.8.5
AA5	*approval authority* [4.4] specification: Test *IVS* functionality	s.8.8.6
AA6	*approval authority* [4.4] specification: *OEM* vehicle unique identification	s.12.3.4.3
AA7	*approval authority* [4.4] specification :Aftermarket regulated commercial vehicle unique identification	s.12.4.4.3
AA8	*approval authority* [4.4] specification: Approve new applications	s.12.10.6

A.4 Service provider

SP1	Service provider specification: *Service provider* [4.27] definition	s.8.3.1
SP2	Service provider specification: *Service provider* [4.27] *approval authority* [4.4] approval requirement	s.8.3.2
SP3	Service provider specification: Application service definition	s.8.3.4
SP4	Service provider specification: Service provision	s.8.3.5
SP5	Service provider specification: *Service provider* [4.27] charging	s.8.3.6
SP6	Service provider specification: *Service provider* [4.27] charging fees on behalf of *jurisdiction regulator* [4.19]	s.8.3.7
SP7	Service provider specification: *Service provider* [4.27] transmission of data to the jurisdiction and/or its agents	s.8.3.8
SP8	Service provider specification: Provision of non-regulated commercial services	s.8.3.9
SP8.a)	obtain approval	
SP8.b)	ensure does not affect the quality of the service provision of any regulated services	
SP9	Service provider specification: Wireless communications service provision	s.8.4.1
SP10	Service provider specification: Responsibility for wireless communications service provision	s.8.4.2
SP11	Service provider specification: Responsibility where *IVS* is installed post manufacture of the vehicle	s.8.5.2

SP12	Service provider specification: Responsibility of the *service provider* [4.27] contracted to maintain an *IVS*	s.8.6.2
SP12.a)	Responsibility	s.8.6.2.1
SP12.1)	In the event of malfunction	s.8.6.2.2
SP12.1 a)	immediately liaise with the *user* [4.31]	
SP12.1 b)	report the malfunction to the *jurisdiction regulator* [4.19]	
SP12.1 c)	complete the resolution process	
SP12.1 d)	*IVS* memory are transferred to the *prime service provider* [4.21] system	
SP12.2	*Tampering* [4.28]	s.8.6.2.3
	report to the *jurisdiction regulator* [4.19] :	
SP12.2 a)	evidence of any *tampering* [4.28] or attempt at *tampering* [4.28]	
SP12.2 b)	any *IVS* or *TID* malfunction	
SP12,2 c)	shall NOT advise a *user* [4.31]	
SP12.3	Documentation	s.8.6.2.4
SP12.3 a)	Document contents	
SP12.3 b)	The documentation shall be available for auditing by *jurisdiction regulator* [4.19].	
SP12.3 c)	Maintain archives of the documentation	
SP13	Service provider specification :*OEM Prime service provider* [4.21]	s.12.3.4.1
SP14	Service provider specification : *OEM* Set access conditions	s.12.3.4.2
SP15	Service provider specification: *OEM IVS* unique identification	s.12.3.4.4
SP16	Service provider specification: *OEM basic vehicle data* [4.8]	s.12.3.4.5
SP17	Service provider specification: *core application data* [4.13]	s.12.3.4.6
SP18	Service provider specification : Aftermarket *Prime service provider* [4.21]	s.12.4.4.1
SP19	Service provider specification: Aftermarket Set access conditions	s.12.4.4.2
SP20	Service provider specification: Aftermarket *IVS* unique identification	s.12.4.4.4
SP21	Service provider specification: Aftermarket *basic vehicle data* [4.8]	s.12.4.4.5
SP22	Service provider specification: Aftermarket *core application data* [4.13]	s.12.4.4.6
SP23	Service provider requirement: Replacement of *IVS*	s.12.7.1
SP24	Service provider requirement: Upgrade of the *IVS*	s.12.7.2
SP25	Service provider requirement: Repair of the *IVS*	s.12.7.3
SP26	Service provider requirement: Service of the *IVS*	s.12.7.4
SP27	Service provider responsibility: Change of regulated commercial freight vehicle properties	s.12.8.2
SP28	Service provider responsibility: *IVS* activation	s.12.9.1
SP29	Service provider responsibility: System modifications, upgrades and changes	s.12.10.3
SP30	Service provider responsibility: Minimisation of on board processing and memory demands	s.12.10.4
SP31	Service provider responsibility: Responsibility for design, development, testing	s.12.10.5
SP32	Service provider responsibility: End of life notification	s.12.12.2

A.5 IVS

IVS1	*IVS* specification: Robustness and suitability	s.9.3
IVS2	*IVS* specification: Availability	s.9.4
IVS3	*IVS* specification: Environmental	s.9.5
IVS4	*IVS* specification: Secure data storage	s.9.6
IVS4 a)	The *IVS* can survive a crash of up to 130 kph.	
IVS4 b)	*Tamper* [4.28] resistant.	
IVS4 c)	non-volatile data storage and in the *RAM* is accessible only to the application service	
IVS4 d)	Data storage security meets requirements of ISO 15638-4	
IVS4 e)	Not possible to manipulate data	
IVS4 f)	Security and confidentiality of data maintained at all times.	
IVS5	*IVS* specification: Data storage means	s.9.7
IVS6	*IVS* specification *IVS6*: Data input means	s.9.8
IVS7	*IVS* specification: Central processing unit	s.9.9
IVS7 a)	1 GigaHertz or higher processor	
IVS7 b)	volatile memory (*RAM*/*DRAM*/*SRAM* etc.) of at least 100 Gigabytes	
IVS7 c)	recognised operating system (e.g. Linux)	
IVS7 d)	means to interact with process ISO 11519* and ISO 11898** CAN bus data	
IVS8	*IVS* specification: Secure data processing	s.9.10
IVS9	*IVS specification: Connectivity means to/from auxiliary equipment*	*s.9.11*
*IVS*10	*IVS* specification: *IVS* clock	s.9.12
IVS11	*IVS* specification: Communications means	s.9.12
IVS12	*IVS* specification: CLASS A - able to communicate with its attached trailers	s.9.13.1
IVS13	*IVS* specification: Class B – not able to communicate with its attached trailers	s.9.13.2
IVS14	*IVS* specification: *IVS* identification of attached trailers	s.9.14
IVS15	*IVS* specification: Physical trailer marking	s.9.15
IVS16	*IVS* specification: Equipped trailer identification (trailer ID)	s.9.16

IVS17	*IVS* specification: Freight land conveyance content identification and communication	s.9.17
IVS18	*IVS* specification: Equipped trailer identification devices	s.9.18.1
IVS19	*IVS* specification: Trailer identification device requirements	s.9.18.2
IVS20	*IVS* specification: Integrity of trailer identification	s.9.18.3
IVS21	*IVS* specification: Power supply	s.9.19
IVS 22	*IVS* specification: external power supply failure/shut down	s.9.20
IVS23	*IVS* specification: Security seals	s.9.21
IVS24	*IVS* specification: GNSS capability	s.9.22
IVS25	*IVS* specification: Accelerometer capability	s.9.23
IVS26	*IVS* specification: Gyroscope capability	s.9.24
IVS27	*IVS* specification: Still camera data	s.9.25
IVS28	*IVS* specification: Video data	s.9.26
IVS29	*IVS* specification: Alarm types and data	s.9.27.1
IVS30	*IVS* specification: Independent movement sensing	s.9.27.2
IVS31	*IVS* specification: Vehicle location	s.9.28
IVS32	*IVS* specification: When vehicle is powered up (ignition status ON)	s.10.1
IVS33	*IVS* specification: Communication set-up	s.10.2
IVS34	*IVS* specification: Communication session clear-down	s.10.3
IVS35	*IVS* specification: 'stored data' Communication set-up	s.11.4.1
IVS36	*IVS* specification: Shall not interfere with *TARV* application service provision	s.12.6.3
IVS37	*IVS* specification: Shall demonstrate complementariness	s.12.6.4

A.6 User

US1	User specification: '*Prime user* [4.22] '	s.8.2.1
US2	User specification: *secondary user* [4.26]	s.8.2.2
US3	User specification: Mandatory application service enrolment	s.8.2.3
US4	User specification: Voluntary application service enrolment	s.8.2.4
US4.1	Voluntary *regulated application service* [4.24] enrolment	s.8.2.4.1
US4.2	Voluntary commercial application service enrolment	s.8.2.4.2
US5	User specification US5: *Service provider* [4.27] engagement	s 8.2.5
US6	User responsibility: Responsibility to maintain the *IVS*	s.8.6.1
US6	User requirement : '*Service provider* [4.27] - *User* [4.31] Contract'	s.8.9.1
US7	User responsibility: Change of regulated commercial freight vehicle properties	s.12.8.1
US8	User responsibility: End of life notification	s.12.12.1

A.7 OEM

OEM1	Original equipment manufacturer specification: Responsibility where *IVS* is installed at time of vehicle manufacture	s.8.5.1

Annex B
(informative)

Appropriate coding systems for unambiguous vehicle identification

B.1 General

It is not for this part of ISO 15638 to require any *jurisdiction* [4.18] to use any particular method to unambiguously identify a vehicle. This part of ISO 15638 only has the requirement that the vehicle has an unambiguous identification. The objective of this informative Annex is to suggest some efficient methods to do this in a globally unambiguous way.

B.2 Countries with existing unambiguous vehicle identification schema

Jurisdictions [4.18] are likely to have established practices in respect of unambiguous vehicle identification. However, in some cases these have been developed from a National perspective only, so it is possible that a vehicle from a different country could carry the same identification.

The easiest way to adapt such systems for international use is to precede the existing code with either the ISO standard country code (ISO 3166-1 Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes)

and possibly, in the case of federal countries, also the subdivision code (ISO 3166-2, Codes for the representation of names of countries and their subdivisions — Part 2: Country subdivision codes).

An alternate method could be to use the ITU-T E..164, Numbering plan of the international telephone service, as a prefix to the existing coding scheme.

The format would therefore be

Jurisdiction (Country or country/subdivision) identifier/ existing unambiguous vehicle identification.

B.3 Countries without an existing unambiguous vehicle identification schema

Jurisdictions [4.18] that do not currently have an existing unambiguous vehicle identification schema for commercial vehicles are of course free to invent their own. However a number of existing options already exist and should be considered.

a) The VIN number of the vehicle is almost unambiguous in its 17 digit format, and can be interpreted via websites such as www.nisrinc.com/cmv_id/cmv_id.asp.

b) The National registration plate number of the vehicle, preceded by ISO standard country code (ISO 3166-1 Codes for the representation of names of countries and their subdivisions — Part 1: Country codes).

and possibly, in the case of federal countries, also the subdivision code (ISO 3166-2, Codes for the representation of names of countries and their subdivisions — Part 2: Country subdivision codes).

An alternate method could be to use the ITU-T E..164, Numbering plan of the international telephone service, as a prefix to the existing coding scheme.

The format would therefore be

Jurisdiction (Country or country/subdivision) identifier/ National registration plate number

c) ISO 14816 (Road Traffic and Transport Telematics — Automatic Vehicle and Equipment Identification — Numbering and Data Structures) and ISO 17262 (ISO 17262, Intelligent transport systems — Automatic vehicle and equipment identification — Numbering and data structures) also offer several schema for *unique vehicle identification* [4.30] EN/ ISO 14816.

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 — Preparation and layout*

[4] ISO 3166-1, *Codes for the representation of names of countries and their subdivisions — Part 1: Country codes*

[5] ISO 3166-2, *Codes for the representation of names of countries and their subdivisions — Part 2: Country subdivision codes*

[6] ISO 3779, Road vehicles — Vehicle identification number (VIN) — Content and structure

[7] ISO 6709, *Standard representation of geographic point location by coordinates*

ICS 03.220.20; 35.240.60

Price based on 67 pages