TECHNICAL SPECIFICATION

ISO/TS 15638-4

First edition
2020-02

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

Part 4: System security requirements

Systèmes intelligents de transport — Cadre pour applications télématiques collaboratives pour véhicules de fret commercial réglementé (TARV) —
Partie 4: Exigences des systèmes de sécurité

Reference number
ISO/TS 15638-4:2020(E)

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

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

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

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

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. While the regulatory services in use or being considered varies from country to country, these include services such as charging, digital tachograph, hazardous goods tracking and e-call. Additional applications with a regulatory impact being developed include access monitoring, on-board mass monitoring, fatigue management, speed monitoring.

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 vehicle that operate within such regulations. Such International Standards will allow for a speedy development and specification of new applications that build upon the functionality of a generic specification platform. The ISO 15638-4 series of standards describes and defines the framework and requirements so that the on-board equipment can be commercially designed in an open market to meet common requirements.

The ISO 15638 series of standards:

— provides the basis for future development of cooperative telematics applications for regulated commercial freight vehicles. Many elements to accomplish this are already available. Existing relevant standards will be referenced, and the specifications will use existing standards (such as published CALM documents) wherever practicable.

— allows for a powerful platform for highly cost-effective delivery of a range of telematics applications for regulated commercial freight vehicles.

— is a business architecture based on a (multiple) service provider oriented approach.

— addresses legal and regulatory aspects for the approval and auditing of service providers.

The ISO 15638 series of standards is timely as many governments (Europe, North America, Asia and Australia/New Zealand) are considering the use of telematics for a range of regulatory purposes. Ensuring that a single in-vehicle platform can deliver a range of services to both government and industry through open standards and competitive markets is a strategic objective.

This document provides general specifications for security for communications and data exchange aspects of candidate regulated applications which are specified in ISO 15638-8 (and Parts 8 to 21 at the time of developing this document, but further parts may be added later if a requirement for additional regulated applications to be standardised are identified), the selection and implementation for all or any of which remain a decision for the implementing jurisdiction.

NOTE 1 The definition of what comprises a 'regulated' vehicle is regarded as an issue for National decision, and can vary from jurisdiction to jurisdiction. The ISO 15638 series of standards 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 jurisdiction to jurisdiction. The ISO 15638 series of standards does not impose any requirements on nations in respect of which services for regulated vehicles jurisdictions will require, or support as an option, but will provide standardised sets of requirements descriptions for identified services to enable consistent and cost-efficient implementations where implemented.

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

Part 4: System security requirements

1 Scope

Security requirements address both hardware and software aspects.

This document addresses the security requirements for:

— the transfer of TARV data from an IVS to an application service provider across a wireless communications interface;

— the receipt of instructions from an application service provider to a TARV IVS;

— the communications aspects of handling of software updates for the IVS over wireless communications.

This document defines the requirements for telematics applications for regulated commercial vehicles for:

a) threat, vulnerability and risk analysis;

b) security services and architecture;

c) identity management;

d) security architecture and management;

e) identity-trust and privacy management;

f) security-access control;

g) security-confidentiality services.

This document provides:

— general specifications for the security of TARV;

— specifications for the security of TARV transactions and data within an ITS-station "bounded secure managed domain" (BSMD);

— specifications for the security of TARV transactions and data transacted with a predetermined address outside of a BSMD.

IVS security requirements are dealt with by the prime service provider and application service provider (See ISO 15638-1).

Application service provision security is dealt with by the application service provider (and could be the subject of a separate TARV standards deliverable).

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

ISO/IEC 15408-1, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

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

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

ISO 17423, *Intelligent transport systems — Cooperative systems — Application requirements and objectives*

ISO 21210, *Intelligent transport systems — Communications access for land mobiles (CALM) — IPv6 Networking*

ISO 21217, *Intelligent transport systems — Communications access for land mobiles (CALM) — Architecture*

ISO 24102-3, *Intelligent transport systems — ITS station management — Part 3: Service access points*

ETSI TS 102 940, *Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management*

3 Terms and definitions

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

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

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
access
admittance, entry, permit to use the road network and/or associated infrastructure, e.g. bridges, tunnels

3.2
access monitoring
observation and recording of vehicle related data when using the road network and/or associated infrastructure, e.g. bridges, tunnels

3.3
application service
service provided by a *service provider* (3.24) enabled by accessing data from the *in-vehicle system* (*IVS*) (3.14) of a regulated vehicle via a wireless communications network

3.4
application service provider
ASP
party that provides an *application service* (3.3)

3.5
architecture
formalised description of the design of the structure of TARV and its *framework* (3.13)

3.6
authentication
function intended to establish and verify a claimed identity

3.7
bounded secure managed domain
BSMD
secure peer-to-peer communications between entities (*ITS-stations* (3.16)) that are themselves capable of being secured and remotely managed;

Note 1 to entry: The bounded nature is derived from the requirement for ITS-stations to be able to communicate amongst themselves, i.e. peer-to-peer, as well as with devices that are not secured (referred to as 'other ITS-stations'), and realizing that to achieve this in a secure manner often requires distribution and storage of security-related material that must be protected within the boundaries of the *ITS-stations,* leads to the secured nature of the entity, as there is great flexibility to achieve desired communication goals, there is a requirement that this flexibility be managed; within C-ITS and ISO 21217 such *ITS-stations* are defined as operating within BSMD, or outside of the BSMD.

3.8
communications access for land mobiles
CALM
layered solution that enables continuous or quasi continuous communications between vehicles and the infrastructure, or between vehicles, using such (multiple) wireless telecommunications media that are available in any particular location, and which have the ability to migrate to a different available media where required and where media selection is at the discretion of *user* (3.27) determined parameters by using a suite of standards based on ISO 21217 (*CALM* architecture) and ISO 21210 (*CALM* networking) that provide a common platform for a number of standardised media using *ITS-stations* (3.16) to provide wireless support for applications, such that the application is independent of any particular wireless medium

3.9
commercial application(s)
ITS applications in regulated vehicles for commercial (non-regulated) purposes

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

3.10
cooperative ITS
C-ITS
ITS applications for both regulatory and commercial purposes that require the exchange of data between uncontracted parties using multiple *ITS-stations* (3.16) communicating with each other and sharing data with other parties with whom they have no direct contractual relationship to provide one or more *ITS services* (3.15)

3.11
data pantry
secure area of memory in *IVS* (3.14) where data values are stored

Note 1 to entry: See ISO 15638-1.

3.12
facilities
layer that sits on top of the communication stack and helps to provide data interoperability and reuse, and to manage applications and enable dynamic real time loading of new applications

3.13
framework
particular set of beliefs and ideas referred to in order to describe a scenario or solve a problem

3.14
in-vehicle system
IVS
ITS-station (3.16) and connected equipment on board a vehicle

3.15
ITS service
communication functionality offered by an *ITS-station* (3.16) to an *ITS-station* application

3.16
ITS-station
ITS-s
entity in a communication network, comprised of application, *facilities* (3.12), networking and access layer components specified in ISO 21217 that operate within a bounded secure management domain

3.17
jurisdiction
government, road or traffic authority which owns the r*egulatory applications* (3.21)

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

3.18
jurisdiction regulator
agent of the *jurisdiction* (3.17) appointed to regulate and manage TARV within the domain of the *jurisdiction*, which may or may not be the *approval authority (regulatory)*

3.19
operator
fleet manager of a regulated vehicle

3.20
prime service provider
service provider (3.24) who is the first contractor to provide *regulated application services* (3.22) to the regulated vehicle, or a nominated successor on termination of that initial contract, and who is responsible to maintain the installed *IVS* (3.14) and if the *IVS* was not installed during the manufacture of the vehicle, the *prime service provider* (3.20) is also responsible to install and commission the *IVS*

3.21
regulated application
regulatory application
application arrangement using TARV utilised by *jurisdictions* (3.17) for granting certain categories of commercial vehicles rights to operate in regulated circumstances subject to certain conditions, or indeed to permit a vehicle to operate within the *jurisdiction* and which may be mandatory or voluntary at the discretion of the *jurisdiction*

3.22
regulated application service
TARV application service (3.3) to meet the requirements of a *regulated application* (3.21) that is mandated by a regulation imposed by a *jurisdiction* (3.17), or is an option supported by a *jurisdiction*

3.23
regulated commercial freight vehicle
regulated commercial regulated vehicle
vehicle that is subject to regulations determined by the *jurisdiction* (3.17) as to its use on the road system of the *jurisdiction* in regulated circumstances, subject to certain conditions, and in compliance with specific regulations for that class of regulated vehicle and which at the option of *jurisdictions* may require the provision of information via TARV or provide the option to do so

3.24
service provider
party which is approved by an approval authority (regulatory) as suitable to provide regulated or commercial ITS *application services* (3.3)

3.25
specification
explicit and detailed description of the nature and functional requirements and minimum performance of equipment, service or a combination of both

3.26
telematics
use of wireless media to obtain and transmit (data) from a distant source

3.27
user
individual or party that enrols in and operates within a regulated or *commercial application* (3.9) service

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

4 Abbreviated terms

ADR	European Agreement concerning the international carriage of Dangerous goods by Road/Accord européen relatif au transport international des marchandises Dangereuses par Route
ASP	application service provider (3.4)
BSMD	bounded secure managed domain
CALM	communications access for land mobiles (3.8)
C-ITS	cooperative intelligent transport systems (3.10)
ID	identity
IP	internet protocol
ITS-s	ITS-station (3.16)
IVS	In-vehicle system (3.14)
TARV	telematics (3.26) applications for regulated vehicles
UNECE	United Nations Economic Commission for Europe

5 General overview and framework

ISO 15638-1 provided a framework and architecture for TARV. It provided a general description of the roles of the actors in TARV and their relationships.

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