TECHNICAL REPORT

ISO/TR 17427-4

First edition
2015-11-01

Intelligent transport systems — Cooperative ITS —

Part 4: Minimum system requirements and behaviour for core systems

Systèmes intelligents de transport — Systèmes intelligents de transport coopératifs —
Partie 4: Exigences minimales du système et comportement des systèmes principaux

Reference number
ISO/TR 17427-4:2015(E)

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

Contents

Page

Foreword

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

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

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

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

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

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

ISO 17427 consists of the following parts, under the general title *Intelligent transport systems — Cooperative ITS*:

— *Part 2: Framework Overview [Technical Report]*

— *Part 3: Concept of operations (ConOps) for 'core' systems [Technical Report]*

— *Part 4: Minimum system requirements and behaviour for core systems [Technical Report]*

— *Part 6: 'Core system' risk assessment methodology [Technical Report]*

— *Part 7: Privacy aspects [Technical Report]*

— *Part 8: Liability aspects [Technical Report]*

— *Part 9: Compliance and enforcement aspects [Technical Report]*

— *Part 10: Driver distraction and information display [Technical Report]*

The following parts are under preparation:

— *Part 1: Roles and responsibilities in the context of co-operative ITS architecture(s)*

— *Part 5: Common approaches to security [Technical Report]*

— *Part 11: Compliance and enforcement aspects [Technical Report]*

— *Part 12: Release processes [Technical Report]*

— *Part 13: Use case test cases [Technical Report]*

— *Part 14: Maintenance requirements and processes [Technical Report]*

This Technical Report provides an informative 'minimum system requirements and behaviour for core systems' for Cooperative Intelligent Transport Systems (*C-ITS*). It is intended to be used alongside ISO 17427-1, ISO/TR 17465-1 and other parts of ISO 17465, and ISO 21217. Detailed specifications for the application context will be provided by other ISO, CEN and SAE deliverables, and communications specifications will be provided by ISO, IEEE and ETSI.

Introduction

Intelligent transport systems (*ITS*) are transport systems in which advanced information, communication, sensor and control technologies, including the Internet, are applied to increase safety, sustainability, efficiency, and comfort.

A distinguishing feature of '*ITS*' is its communication with outside entities.

Some *ITS* systems operate autonomously, for example, 'adaptive cruise control' uses radar/lidar and/or video to characterize the behaviour of the vehicle in front and adjust its vehicle speed accordingly. Some *ITS* systems are informative, for example, 'variable message signs' at the roadside or transmitted into the vehicle, provide information and advice to the driver. Some *ITS* systems are semi-autonomous in that they are largely autonomous but rely on 'static' or 'broadcast' data, for example, *GNSS* (2.22) based 'SatNav' systems operate autonomously within a vehicle but are dependent on receiving data broadcast from satellites in order to calculate the location of the vehicle.

Cooperative Intelligent transport systems (*C-ITS*) are a group of *ITS* technologies where service provision is enabled by, or enhanced by, the use of 'live', present situation related, dynamic data/information from other entities of similar *functionality* [for example, from one vehicle to other vehicle(s)], and/or between different elements of the transport network, including vehicles and infrastructure [for example, from the vehicle to an infrastructure managed system or from an infrastructure managed system to vehicle(s)]. Effectively, these systems allow vehicles to 'talk' to each other and to the infrastructure. These systems have significant potential to improve the transport network.

A distinguishing feature of '*C-ITS*' is that data is used across *application*/service boundaries.

This Technical Report is a 'living document' and as our experience with *C-ITS* develops, it is intended that it will be updated from time to time, as and when we see opportunities to improve this Technical Report.

Intelligent transport systems — Cooperative ITS —

Part 4: Minimum system requirements and behaviour for core systems

1 Scope

The scope of this Technical Report is, as an informative document, to identify potential critical minimum system requirements and behaviour for core systems issues that *C-ITS* service provision may face or introduce, to consider strategies for how to identify, control, limit or mitigate such issues. The objective of this Technical Report is to raise awareness of and consideration of such issues and to give pointers, where appropriate, to subject areas and, where available, to existing standards deliverables that provide specifications for all or some of these aspects. This Technical Report does not provide specifications for solutions of these issues.

2 Terms and definitions

2.1
anonymity
lacking individuality, distinction, and recognizability within message exchanges

2.2
anonymous certificate
certificate which contains a pseudonym of the system user instead of their real identity in the subject of the certificate and thus preventing other system service recipients from identifying the certificate owner when the certificate is used to sign or encrypt a message in the connected vehicle/highway system (C-ITS, connected vehicle)

Note 1 to entry: The real identity of the anonymous certificates can be traced by authorized system operators by using the services of a registration authority and/or certification authority.

2.3
application
'app'
software application

2.4
application service
service provided, for example, by a service provider accessing data from the IVS within the vehicle in the case of C-ITS, via a wireless communications network, or provided on-board the vehicle as the result of software (and potentially also hardware and firmware) installed by a service provider or to a service provider's instruction

2.5
authenticity
property of being of undisputed origin and not a copy, authenticated, and having the origin supported by unquestionable evidence

Note 1 to entry: Something that has had its authenticity confirmed could be described as "authenticated" or "verified".

2.6
authorization
process of determining what types of activities or access are permitted on a network

Note 1 to entry: This is usually used in the context of authentication: once you have authenticated a user, they may be authorized to have access to a specific service.

2.7
bad actor
role played by a user or another system that provides false or misleading data, operates in such a fashion as to impede other service recipients, and/or operates outside of its authorized scope

2.8
C-ITS
Cooperative ITS
group of *ITS* technologies where service provision is enabled, or enhanced by, the use of 'live', present situation related, data/information from other entities of similar functionality [(for example, from one vehicle to other vehicle(s)], and/or between different elements of the transport network, including vehicles and infrastructure (for example from the vehicle to an infrastructure managed system or from an infrastructure managed system to vehicle(s)

2.9
catalogue
repository used by the 'Data Distribution subsystem' for maintaining data publishers information including the type of data they are transmitting, frequency of that data, address, data source, etc.

2.10
centre
entity that provides application, management, administrative, and support functions from a fixed location (the terms "back office" and "centre" are used interchangeably)

Note 1 to entry: Centre is, traditionally, a transportation-focused term, evoking management centres to support transportation needs, while back office generally refers to commercial applications; from the perspective of this Technical Report, these are considered the same.

2.11
core services
set of functions within the 'Core System' subsystems that interact with system service recipients

2.12
core system personnel
staff that operate and maintain the 'Core System'

Note 1 to entry: In addition to network managers and operations personnel, 'Core System' personnel includes the administrators, operators, maintainers, developers, deployers and testers.

2.13
coverage area
geographic jurisdiction within which a 'Core System' provides *core services* (2.11)

2.14
data provision
act of providing data to a core system

2.15
delta
updates
records
data that is new since the last block of data that was downloaded

2.16
digital certificate
electronic "identification card" that establishes user credentials when doing business or other transactions

Note 1 to entry: This is issued by a certification authority: contains name, a serial number, expiration dates, a copy of the certificate holder's *public key* (2.40) (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

Note 2 to entry: From the SysAdmin, Audit, Network, Security Institute - www.sans.org

2.17
environment
circumstances, objects, and conditions that surround a system to be built

Note 1 to entry: It includes technical, political, commercial, cultural, organizational, and physical influences, as well as standards and policies that govern what a system shall do or how it will do it.

2.18
error message
message that indicates issues with cross-jurisdictional compatibility, scope coverage service or service availability

2.19
facility
building or group of buildings with access restrictions housing a 'Core System'

2.20
functionality
capabilities of the various computational, user interfaces, input, output, data management, and other features provided by a product

2.21
geo-cast
delivery of a message to a group of network destinations identified by their geographic locations

2.22
global navigation satellite system
GNSS
comprises several networks of satellites that transmit radio signals containing time and distance data that can be picked up by a receiver, allowing the user to identify the location of its receiver anywhere around the globe

EXAMPLE GPS, GLONASS, Galileo.

2.23
integrity
internal consistency or lack of corruption in electronic data

EXAMPLE A system that is secure, complete and conforming to an acceptable conduct without being vulnerable and corruptible.

2.24
intelligent transport systems
ITS
transport systems in which advanced information, communication, sensor and control technologies, including the Internet, are applied to increase safety, sustainability, efficiency, and comfort

2.25
link
locus of relations among nodes

Note 1 to entry: It provides interconnections between nodes for communication and coordination; may be implemented by a wired connection or with some radio frequency (RF) or optical communications media; links implement the primary function of transporting data; links connect to nodes at a *port* (2.38).

2.26
maintainability
keep in an existing operational state preserved from failure or decline of services (with minimum repair, efficiency, or validity)

2.27
misbehaviour
act of providing false or misleading data, operating in such a fashion as to impede other service recipients, or to operate outside of their authorized scope

Note 1 to entry: This includes suspicious behaviour as in wrong message types or frequencies, invalid logins and unauthorized access, or incorrect signed or encrypted messages, etc., either purposeful or unintended.

2.28
misbehaviour information
misbehaviour (2.27) reports from system service recipients, as well as other improper system user acts, such as sending wrong message types, invalid logins, unauthorized access, incorrectly signed messages and other inappropriate system user behaviour

2.29
misbehaviour report
information from a system user identifying suspicious behaviour from another system user that can be characterized as *misbehaviour* (2.27)

2.30
mobile
vehicle types (private/personal, trucks, transit, emergency, commercial, maintenance, and construction vehicles) as well as non-vehicle-based platforms including portable personal devices (smartphones, PDAs, tablets, etc.) used by travellers (vehicle operators, passengers, cyclists, pedestrians, etc.) to provide and receive transportation information

2.31
mode
phase within a state (degraded mode occurs automatically due to certain conditions), such as, when in *operational state* (2.33), there is an automatic transition to degraded mode because of a detected hardware failure

Note 1 to entry: Modes are normal, degraded, restricted and degraded/restricted.

2.32
node
physical hardware engineering object that is a run-time computational resource and generally has at least memory and processing capability

Note 1 to entry: Run-time software engineering objects reside on nodes; node has some well-understood, possibly rapidly moving, location [a node may be composed of two or more (sub) nodes].

2.33
operational state
all activities during the normal conduct of operations and also needs to be able to handle support for services from other 'Cores Systems' including fail-over and/or degraded services

2.34
operator
day-to-day providers of the 'Core System' that monitor the health of the system components, adjust parameters to improve performance, and collect and report statistics of the overall system

2.35
parsing
analysing (a string, text or data) into logical syntactic components

2.36
permission
authorization (2.6) granted to do something (to the 'Core System'), permissions are granted to system service recipients and *operators* (2.34) determining what actions they are allowed to take when interacting with the 'Core System'

2.37
physical security
safeguards to deny access to unauthorized personnel (including attackers or even accidental intruders) from physically accessing a building, *facility* (2.19), resource, or stored information (this can include simply a locked door, badge access controls, or armed security guards)

2.38
port
physical element of a *node* (2.32) where a *link* (2.25) is connected; nodes may have one or more ports;each port may connect to one or more physical ports on (sub) nodes that are contained within the node

2.39
private network
network belonging to a person, company or organization that uses a public network (usually the Internet) to connect its remote sites or service recipients together

2.40
public key
cryptographic key that can be obtained and used by anyone to encrypt messages intended for a particular recipient, such that the encrypted messages can be deciphered only by using a second key that is known only to the recipient (the private key)

2.41
registry
repository for maintaining data requester's information including the type of data they are subscribing to, their address, etc.

2.42
states
distinct system setting in which the same user input will produce different results than it would in other settings

Note 1 to entry: The 'Core System' as a whole is always in one state [a state is typically commanded or placed in that state by an *operator* (2.34); states are installation, operational, maintenance, training, and standby].

3 Abbreviated terms

C-ITS cooperative intelligent transport systems, cooperative ITS

ITS intelligent transport systems (2.24)

IVS in-vehicle system (2.6)

TR technical report

ANSI	American National Standards Institute
CA	certification authority
CALM	Communications Access for Land Mobile Standards
CAMP	Crash Avoidance Metrics Partnership
ConOps	concept of operations
CRL	certification revocation lists
CVIS	Cooperative Vehicle Infrastructure System (Project)
DNS	domain name system
EC	European Commission
ESS	external support system
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
GHz	gigahertz
IEEE	Institute for Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet protocol
LTE	long term evolution
NIST	National Institute of Standards and Technology
PKI	public key infrastructure
PKIX	public key infrastructure based on X.509 certificates
RA	registration authority
RFC	request for comments
RITA	Research and Innovative Technology Administration
RSE	roadside equipment
SAP	service access point
SyRS	system requirements specification
USDOT	US Department of Transportation
UTC	coordinated universal time
VII	vehicle infrastructure integration

4 How to use this Technical Report

4.1 Acknowledgements

Inspiration for the technical content identification and consideration of this Technical Report has been largely obtained from various documents generated and publicized by US DoT RITA, especially "'Core System' Requirements Specification (SyRS)".

Conceptual input from the EC project CVIS is also acknowledged.

Contribution from the Australian National Transport Commission, Cooperative Intelligent Transport Systems Policy Paper (A Report prepared by: National Transport Commission) ISBN: 978-1-921604-47-8) is also acknowledged.

See Bibliography for further details of contributions.

4.2 Guidance

This Technical Report is designed to provide guidance and a direction for considering the issues concerning minimum system requirements and behaviour for core systems associated with the deployment of *C-ITS* service provision. It does not purport to be a list of all potential minimum system requirements and behaviour for core systems factors, which will vary according to the scope of the core system being provided, the regime of the jurisdiction, the location of the instantiation and to the form of the instantiation, nor does it provide definitive specification. Rather, this Technical Report discusses and raises awareness of the major minimum system requirements and behaviour for core systems issues to be considered and provides guidance in the context of future and instantiation specific deployments of *C-ITS* core systems.

This document should be read in conjunction with, and in most cases, following consideration of the following:

— ISO 17427-1, *Intelligent transport systems — Cooperative ITS — Part 1: Roles and responsibilities in the context of co-operative ITS architecture(s);*

— ISO/TR 17427-2, *Intelligent transport systems — Cooperative ITS — Part 2: Framework Overview;*

— ISO/TR 17427-3, *Intelligent transport systems — Cooperative ITS — Part 3: Concept of operations (ConOps) for 'core' systems.*

These documents, as their titles imply, identify the principal actor groups and their roles and responsibilities in *C-ITS* service provision, overview for such systems, and describe the concept of operations for core systems supporting *C-ITS* service provision. Frequent reference to these documents and their provisions will be made, but largely not re-described, so familiarity with those documents is a precursor to comprehension and understanding of this Technical Report. The objective of this Technical Report is, within the context of ISO 17427-1, ISO/TR 17427-2, and ISO/TR 17427-3, to identify the minimum system capabilities and behaviour implicitly required to provide 'Core System' service provision and support to participating actors.

4.3 Stakeholders

The term "stakeholder" may be somewhat overused but generally refers to any individual or organization that is affected by the activities of a business process or, in this case, a system being developed. They may have a direct or indirect interest in the activity and their level of participation may vary. The term here includes public agencies, private organizations or the travelling public (end service recipients) with a vested interest, or a "stake" in one or more aspect of the connected vehicle/highway system *environment* (2.17) and the 'Core System'. 'Core System' stakeholders span the breadth of the transportation *environment* including the following:

— transportation service recipients, e.g. private vehicle drivers, public safety vehicle *operators* (2.24), commercial vehicle *operators*, passengers, cyclists and pedestrians;