TECHNICAL REPORT

ISO/TR 17427-6

First edition
2015-11-01

Intelligent transport systems — Cooperative ITS —

Part 6: 'Core system' risk assessment methodology

Systèmes intelligents de transport — Systèmes intelligents de transport coopératifs —

Partie 6: Méthodologie d'évaluation du risque 'd'un système principal'

Reference number
ISO/TR 17427-6:2015(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

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 ‘C-ITS Core System Risk Assessment Methodology’ for Cooperative Intelligent Transport Systems (C-ITS). It should be studied alongside ISO 17427-1, ISO/TR 17465-1, and other parts of the ISO/TR 17465 series 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* 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.

It is important to understand that *C-ITS* is not an end in itself, but a combination of techniques, protocols, systems and sub-systems to enable 'cooperative'/collaborative service provision.

The purpose of this '*C-ITS* Risk Assessment Methodology' Technical Report is to identify critical technical and cost risks that can impact *C-ITS* vehicle and highway systems service provision deployment, and to provide means to evaluate such risks. Risk varies according to the complexity, size, commercial paradigm, and political paradigm prevalent in each jurisdiction where *C-ITS* are supported.

While the principle causes of risks, both technical and cost risks, will be generally similar in each jurisdiction which encourages and supports *C-ITS* vehicle and highway systems, the quantifiable or assessable risk will vary to some extent in each case, and each jurisdiction, the *core system* operator, and *application service* provider, will need to make their own risk assessment. This Technical Report, therefore, does not provide a calculated 'global' risk assessment for *C-ITS*, but identifies the principal causes of risk, and provides a consistent way for a jurisdiction, *core system* operator, or *application service* provider, to assess the risks that they face.

Some see the evolution of *C-ITS* as possible on a V2V basis, without the need for 'Core Systems' and such casual encounter *C-ITS* is indeed possible and the technology proven. The subject of risks associated with *In-vehicle systems* is outside of the scope of this Technical Report, which is focused on risk assessment for *core system* deployments.

The principle environment that this 'Risk Assessment Technical Report' is designed to embrace are *C-ITS* vehicle and highway systems where there is some institutional involvement and support, by the direct or indirect provision of *core system* support, and it is the risks associated with the deployment of 'Core Systems' that provide the focus of this Technical Report.

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 6: 'Core system' risk assessment methodology

1 Scope

The scope of this Technical Report is to identify critical technical and financial risks that can impact the *core system* deployment supporting *C-ITS* vehicle and highway systems service provision and to provide means to evaluate such risks.

This Technical Report is designed to embrace *C-ITS* vehicle and highway systems where there is some institutional involvement and support, by the direct or indirect provision of *core system* support, and it is the risks associated with the deployment of 'Core Systems' that provide the focus of this Technical Report.

This Technical Report does not provide a calculated 'global' risk assessment for *C-ITS*, but identifies the principal causes of risk, and provides a consistent methodology for a jurisdiction, *core system* operator, or *application service* provider, to assess the risks that they face. The objective of this Technical Report is to raise awareness of and consideration of such issues and to give pointers, where appropriate, to standards deliverables existing 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
application
software application

2.2
application service
service provided by a service provider accessing data from the IVS vehicle in the case of C-ITS, through 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

2.3
cooperative ITS
C-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)]

2.4
'core' system
combination of enabling technologies and services that provides the foundation for the support of a distributed, diverse set of *applications* (2.1)/*application* transactions which works in conjunction with 'external support systems' such as 'Certificate Authorities'

Note 1 to entry: The system boundary for the core system is not defined in terms of devices or agencies or vendors, but by the open, standardized interface specifications that govern the behaviour of all interactions between core system users.

2.5
global navigation satellite system
GNSS
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

2.6
in-vehicle system
hardware, firmware and software on board a vehicle that provides a platform to support *C-ITS* service provision, including that of the ITS-station (ISO 21217), the facilities layer, data pantry and on-board 'apps'

2.7
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

2.8
ITS-station
ITS-S
entity in a communication network [comprised of *application* (2.1), facilities, networking and access layer components] that is capable of executing ITS-S *application* processes, comprised of an ITS-S facilities layer, ITS-S networking & transport layer, ITS-S access layer, ITS-S management entity and ITS-S security entity, which adheres to a minimum set of security principles and procedures so as to establish a level of trust between itself and other similar ITS stations with which it communicates

3 Abbreviated terms

CA	Certificate Authority
CCA	Core Certification Authority
C-ITS	cooperative intelligent transport systems, cooperative ITS
CRL	Certificate Revocation List
ESS	External System Support
ITS	intelligent transport systems (2.7)
IVS	in-vehicle system (2.6)
RA	Registration Authority
V2I	vehicle to/from infrastructure
V2V	vehicle to vehicle

4 How to use this Technical Report

4.1 Acknowledgements

The contribution of the following sources are acknowledged as the prime sources of material for this Technical Report, and thanked for their contribution:

http://www.cvisproject.org/

www.its.dot.gov/research/systems_engineering.htm

Cooperative ITS Regulatory Policy Issues and Cooperative Intelligent Transport Systems Policy Paper, National Transport Commission, Australia.

4.2 C-ITS 'Core System' risks

The purpose of this Technical Report is to identify critical technical and cost risks that can impact a 'Core System' for *C-ITS* vehicle and highway systems service provision deployment, and to provide means to evaluate such risks.

The risks that are faced by any jurisdiction or deployer of a *C-ITS* vehicle and highway system varies according to a number of factors:

- the predominant political paradigm of the jurisdiction in which the deployment is instantiated;
- the predominant commercial paradigm within the jurisdiction in which the deployment is instantiated;
- the size of the transport network covered by the deployment;
- the complexity of the transport network covered by the deployment;
- the extent of service provision covered by the instantiation.

The political paradigm probably has the greatest impact. Some jurisdictions are very centralized, while others are, in some way or the other decentralized and/or federated. Some countries organize as a single monolithic jurisdiction, others are organized as a federation of jurisdictions (states), others somewhere in-between. Some countries are associated into political groups of countries where the member states are the paramount jurisdictions and the central jurisdiction is controlled by the will of unanimity or majority, sometimes both.

The practical effect of this on the management of the transport network is significant. A monolithic jurisdiction (for example, Great Britain, France, China), while they may have regional Departments of Transport (DoT), have a centralized controlling DoT which determines policy and strategy. In some jurisdictions, this may be one of centralized control with management of all core strategic policies, including transport, managed by the central government [for example, China which has one 'super' 'Ministry of Transportation of the People's Republic of China' including the former 'Ministry of Communications', 'Civil Aviation Administration', 'State Post Bureau', 'China Maritime Safety Administration' and (since 2013) the 'Ministry of Railways']. Federated states (for example, USA, Australia) that have their own DoTs and central policy, in some cases, may be determined centrally and imposed locally [by a combination of regulations for consistency across the country, and by control of the allotment of financial resources to implement central policies/strategies (for example, USA)], or may be determined locally and brought to the central DoT for agreement by consensus where achievable (for example, Australia, Switzerland).

In combination with the constraints and opportunities of the political paradigm is the commercial paradigm that it fosters. In nearly all countries, the transport environment, and especially the road network, is 'state' funded and controlled. Highways may be totally state funded from taxation, or outsourced to commercial or pseudo-commercial organizations to fund the development of autoroutes/highways/and infrastructures such as tunnels and bridges, increasingly a combination of both, but the paradigm is almost globally managed by the 'jurisdiction'. However, whether this is the local jurisdictional 'state' or the National DoT varies considerably, and in cases such as Europe, while there may be a European "Directorate General" MOVE (Mobility and Transport), it is the National Member States whose DoTs are paramount, and whose policies vary from one member state to another. Some jurisdictions are sympathetic to the provision of commercial services (including *C-ITS* service provisions), while others are hostile and consider commercialisation to be potentially a safety risk. Most will live with some compromise that suits the local community, but those compromises will vary from jurisdiction to jurisdiction.

The other factors that are most important in shaping the shape of *C-ITS* deployment are the size and complexity of the transport network, and in particular, the road network. In countries such as USA, the network is so complex, with many different layers of governance, and many different local political and commercial environments, and the size, both in terms of road pavement kilometres/miles and in the number of road users, so vast, that would make a monolithic ‘Core System’ impracticable. However, other countries, such as Australia, although the size of the territory is 80 % the size of USA, because the road network is only 12 % of the size of that in USA and serves a population of 7 % of that of USA, a single monolithic ‘National’ *core system* may seem to be the only viable arrangement to support *C-ITS* service provision.

The principle causes of risks, both technical and cost risks, will be generally similar in each jurisdiction which encourages and supports *C-ITS* vehicle and highway systems, but the quantifiable or assessable risk will vary to some extent in each case, and each jurisdiction, *core system* operator, and *application service* (2.2) provider, will need to make their own risk assessment. This Technical Report, therefore, does not provide a calculated ‘global’ risk assessment for *C-ITS*, but identifies the principal causes of risk, and provides a consistent way for a jurisdiction, *core system* operator, or *application service* provider, to assess the risks that they face.

While this Technical Report can provide tools for deployers and enablers of *C-ITS* service provision to assess the general risks that face any implementers of a *core system* to support *C-ITS*, there can also be specific risks specialized to a jurisdiction or implementation that are very location or instantiation specific that are not covered in this Technical Report (for example, the communications and environmental issues in the Australian outback or Siberia), so there is a general section towards the end of this report which reminds the deployer/enabler to consider additional local aspects, (but does not provide specific tools for their assessment). Generally, however, the principal causes of risk inherent in most *C-ITS* instantiations have been included and tools identified to consistently assess them.

Another alternative for consideration is to rely on autonomous safety systems coupled with whatever the commercial sector develops in terms of *C-ITS* vehicle-highway systems (perhaps funded by advertising). In these circumstances, it is the tools available to ‘*application service* providers’ to assess their risk exposure that are relevant, and the principle risk to the jurisdiction/administration in these circumstances are the risks of ‘doing nothing’.

The evolution of *C-ITS* on a V2V basis, without the need for ‘Core Systems’ as casual encounter *C-ITS* presents different issues of risk. While these ‘casual’ or ‘commercial’ *C-ITS* options clearly bring additional benefits over a current, non *C-ITS* service environment, their utility will be limited in scope and the client system will be limited. In any event, the roll out will most probably be significantly slower and many of the life-saving, injury mitigation benefits significantly deferred or even lost altogether. However, in some jurisdictions, such routes, can provide the only feasible, or best, option. In these circumstances, it will be important for the jurisdiction, even if not funding or getting involved in deployment, to at least ensure that such solutions are not proprietarily locked to the extent that safety of life and interoperability and transport system efficiency benefits are impaired, and such jurisdictions would be wise to consider how they will achieve this goal. (Requiring adherence to International Standards is recommended as a first step.)

This Technical Report does not address issues of risk that do not involve ‘Core Systems’.

The principle environment that this ‘Risk Assessment Technical Report’ is designed to embrace are *C-ITS* vehicle and highway systems where there is some institutional involvement and support, probably often by the direct or indirect provision of *core system* support, and it is the risks associated with the deployment of ‘Core Systems’ that provide the focus of this Technical Report.

A common definition of a risk is the probability that a decision or action will result in a negative or unwanted consequence, where the probability of each possible outcome is known or can be estimated. In this Technical Report, risks will be identified along with a discussion of their potential impact on deployment. Each risk will have a qualitative discussion of its impact (e.g. high, medium, or low impact) and its likelihood (e.g. high, medium or low likelihood) that the risk will materialize. For each deployment/proposed deployment, actions or mitigation measures will then need to be listed as a part of the assessment.

Table 1 summarizes the high *core system* risks based on the combination of impact and likelihood. More detail on these and all other identified risks are provided in Clause 6.

Table 1 — High *core system* risks

Subclause	Subject
6.1.1	Timely deployment
6.1.2	Relationships between ‘Core Systems’ and external enterprises
6.2.1	Role and makeup of a ‘Core Certification Authority’
6.2.2	External Support System (ESS) for security
6.2.3	Operations and maintenance (O&M) of External Support System (ESS) for security
6.2.4	Security management

The principle body of this Technical Report consists of the following sections:

— The Introduction provided the context of this Technical Report, and Clause 1 determined its purpose and extent.

— Clause 2 and Clause 3 provide explanation of the terms and abbreviations used.

— Clause 4 provides an overview of how to use this Technical Report and what is meant by the *core system.*

— Clause 5 describes how the risks are organized and explains the ‘scoring’ mechanisms.

— Clause 6 provides the detailed listing of each risk including a ‘Risk statement’, a root cause, the consequence, likelihood it will happen, a graphical summary of the overall risk, and a list of any actions that can be taken to mitigate or reduce the risk.

— A bibliography is provided at the end of the document.

4.3 ‘Core System’ overview

C-ITS vehicle and highway systems service provision envisions the combination of the *applications* (2.1), services and systems necessary to provide the safety, mobility and environmental benefits through the exchange of data between mobile and fixed transportation users. It consists of the following:

— **applications** that provide functionality to realize safety, mobility and environmental benefits;

— **communications** that facilitate data exchange;

— **‘Core Systems’**, which provide the functionality needed to enable data exchange between and among mobile and fixed transportation users;

— **support systems,** including security credentials certificate and registration authorities that allow devices and systems to establish trust relationships.

The ‘Core Systems’ main mission is to enable safety, mobility and environmental communications-based *applications* for both mobile and non-mobile users.

See ISO/TR 17427-2 for a more detailed explanation of the framework and overview of *C-ITS* service provision.

See ISO/TR 17427-3 for a more detailed explanation of the concept of operations for *C-ITS* ‘Core Systems’, and ISO 17427-1 for explanation of the roles and responsibilities involved in *C-ITS* service provision.

Within the *C-ITS vehicle and highway systems* environment, the *core system* concept distinguishes communications mechanisms from data exchange, and from the services needed, to facilitate the data exchange. The *core system* supports the *C-ITS vehicle and highway systems* environment by being responsible for providing the services needed to facilitate the data exchanges. The contents of the data exchange are determined by *applications* unless the data exchange is used as part of the facilitation process between the user and the *core system*.

The *core system* provides the functionality required to support safety, mobility, and environmental *application*s. This same functionality can also enable commercial *application*s but that is not a driving factor for the development of the *core system*. The primary function of the *core system* is the facilitation of communications between system users and many of the communications must also be very secure. The *core system* can also provide data distribution and network support services depending on the needs of the *core system* deployment.

A critical factor driving the conceptual view of the *core system* and the entire *C-ITS* vehicle and highway systems environment is the level of trustworthiness between communicating parties. A complicating factor is the need to maintain the privacy of participants, though not necessarily exclusively through anonymous communication. ISO/TR 14827-7 will address privacy aspects of *C-ITS* service provision in greater detail. ISO/TR 17428-8 will address Liability issues in greater detail.

4.4 Non 'Core System' risks

This Technical Report is focused on risk assessment in respect of 'Core Systems' deployment. The risks associated with *in-vehicle systems* is not assessed, and such systems, may it be OEM or aftermarket, need to face the same risk assessment processes used to assess risk for any vehicle safety equipment.

Some see the evolution of *C-ITS* as possible on a V2V basis, without the need for 'Core Systems' and such casual encounter *C-ITS* is indeed possible and the technology proven. Another alternative for consideration is to rely on autonomous safety systems coupled with whatever the commercial sector develops in terms of *C-ITS* vehicle-highway systems (perhaps funded by advertising). In these circumstances, it is the tools available to '*application service* providers' to assess their risk exposure that are relevant, and the principle risk to the jurisdiction/administration in these circumstances are the risks of 'doing nothing'.

The subject of risks associated with *In-vehicle systems* is outside of the scope of this Technical Report, which is focused on risk assessment for *core system* deployments.

While these 'casual' or 'commercial' *C-ITS* options clearly bring additional benefits over a current, non *C-ITS* service environment, their utility will be limited in scope and the client system will be limited. In any event, the roll out will most probably be significantly slower and many of the life-saving, injury mitigation benefits that are the target of many *C-ITS* services can be significantly deferred or even lost altogether. However, in some jurisdictions, such routes, may provide the only feasible, or best, option. In these circumstances, it will be important for the jurisdiction, even if not funding or getting involved in deployment, to at least ensure that such solutions are not proprietarily locked to the extent that safety of life and interoperability and transport system efficiency benefits are impaired, and such jurisdictions would be wise to consider how they will achieve this goal. (Requiring adherence to International Standards is recommended as a first step.)

However, in the case of 'casual encounter' *C-ITS* systems (V2V without the involvement of a *core system*), there is another layer of risk that needs to be assessed, and this is associated with the risks of

- reliance on receipt of data from other vehicles in order to make system decisions,
- risks associated with processing such data, and
- and risks associated with providing data to other system users.

A Technical Report providing advice and guidance for risk assessment of IVS (in both 'core system' supported and 'casual encounter' *C-ITS* systems) can be produced in this series at a later date to provide guidance for these issues.