PD ISO/TR 17427-6:2015

BSI Standards Publication

Intelligent transport systems — Cooperative ITS

Part 6: 'Core system' risk assessment methodology

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of ISO/TR 17427-6:2015.

The UK participation in its preparation was entrusted to Technical Committee EPL/278, Intelligent transport systems.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2015

ISBN 978 0 580 87423 9
ICS 03.220.01; 35.240.60

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 November 2015.

Amendments/corrigenda issued since publication

Date	Text affected

PD ISO/TR 17427-6:2015

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

Page

Foreword ... **iv**
Introduction ... **vi**
1 Scope ... **1**
2 Terms and definitions ... **1**
3 Abbreviated terms ... **2**
4 How to use this Technical Report ... **2**
4.1 Acknowledgements ... 2
4.2 C-ITS 'Core System' risks ... 3
4.3 'Core System' overview ... 5
4.4 Non 'Core System' risks ... 6
5 Tools to assess risk ... **7**
5.1 General ... 7
5.1.1 Technology risk ... 7
5.1.2 Technical risk ... 7
5.1.3 Financial risk ... 7
5.1.4 Liability ... 7
5.2 Operational phases of risk assessment ... 7
5.3 Risk evaluation explanation ... 8
5.4 Categorization of risk ... 10
6 Risks for the core system ... **11**
6.1 Risks associated with an individual 'Core System' ... 11
6.1.1 Timely deployment ... 11
6.1.2 Relationships between 'Core Systems' and external enterprises ... 12
6.1.3 Adequate operations and maintenance personnel ... 13
6.2 Risks associated with multiple 'Core Systems' ... 13
6.2.1 Role and makeup of the 'Core Certification Authority' ... 14
6.2.2 External support system (ESS) for security ... 16
6.2.3 Operations and maintenance (O&M) of the security 'External Support System' (ESS) ... 17
6.2.4 Security management ... 18
6.2.5 System performance management ... 19
6.2.6 Privacy ... 20
6.2.7 Device certification ... 21
6.3 Consideration of other risks ... 21
Bibliography ... **23**

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 system*s (*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 system*s (*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 system*s 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.

TECHNICAL REPORT **ISO/TR 17427-6:2015(E)**

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.