TECHNICAL REPORT

ISO/TR 17427-8

First edition
2015-11-01

Intelligent transport systems — Cooperative ITS —

Part 8: Liability aspects

Systèmes intelligents de transport — Systèmes intelligents de transport coopératifs —

Partie 8: Aspects relatifs à la responsabilité

Reference number
ISO/TR 17427-8:2015(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]

Further technical reports in this series are expected to follow. Please also note that these TRs are expected to be updated from time to time as the C-ITS evolves.

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*' are 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, but as these aspects of transport technology advance, the issue of who is liable in the event of a crash will likely become more complex.

The question of how liability will be resolved in the event of *C-ITS* system failure will be important in providing certainty to drivers, manufacturers, insurers and road managers. It may be that, rather than technical difficulties, uncertainty regarding liability issues could prove the largest deterrent to investment in *C-ITS* service provision.

C-ITS applications will need adequate 'audit trails' in order to trace causation. The so called "human factors" will need to be carefully considered and taken into consideration.

This means that manufacturers and services providers of *C-ITS* technology need to carefully consider the safety risks of their systems and qualify their risk carefully, and road network managers will need to assess the risk implications of providing infrastructure-based *C-ITS* solutions.

We are also in a situation where expectations of system performance and liability implications are likely to change as *C-ITS applications* move from being advisory systems to overriding driver actions, and the liability issues are different between these types of system.

The purpose of this Technical Report is to identify potential critical liability issues that *C-ITS* service provision may introduce; to consider how to control, limit or mitigate such liability issues, and to limit the risk of exposure to the financial consequences of liability issues.

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 8:
Liability aspects

1 Scope

The scope of this Technical Report is an informative document to identify potential critical liability issues that *C-ITS* service provision may introduce; to consider strategies for how to control, limit or mitigate such liability issues; and to give pointers, where appropriate, to standards deliverables existing that provide specifications for all or some of these aspects, and to limit the risk of exposure to the financial consequences of liability issues.

The objective of this Technical Report is to raise awareness of and consideration of such issues. This Technical Report does not provide specifications for solutions of these issues.

2 Terms and definitions

2.1
application
app
software application

2.2
application service
service provided by a service provider accessing data from the *IVS*, in the case of *C-ITS* (2.3), 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 providers 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 will provide the foundation for the support of a distributed, diverse set of applications (2.1), and *application* transactions which work 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
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

2.6
in-vehicle system
IVS
hardware, firmware and software on board a vehicle that provides a platform to support *C-ITS* (2.3) service provision, including that of the *ITS-station* (2.8) (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
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 Abbreviations and acronyms

ABS	anti-lock braking system
ACC	adaptive cruise control
ADAS	advanced driver assistance systems
C-ITS	cooperative intelligent transport systems, cooperative ITS
CA	certificate authority
CVIS	cooperative vehicle-infrastructure systems (EC Project)
EC	European Commission
ESC	electronic stability control
EU	European Union
GTR	global technical requirement (UNECE)
ITS	intelligent transport systems (2.7)
IVS	in-vehicle system (2.6)
UNECE	United Nations Economic Commission for Europe
V2V	vehicle to vehicle
V2I	vehicle to/from infrastructure

4 How to use this Technical Report

4.1 Acknowledgement

Much of the inspiration for this document and its considerations and content originate from the reports "*Cooperative ITS Regulatory Policy Issues*" and "*Cooperative Intelligent Transport Systems Policy Paper*" National Transport Commission, Australia.[1][17] And this source is acknowledged and thanked.

Contribution from various TCA (Transport Certification Australia) documents is acknowledged.

4.2 Guidance

This Technical Report is designed to provide guidance and a direction for considering the issues concerning liability associated with the deployment of *C-ITS* (2.3) service provision. It does not purport to be a list of all potential liability factors — which will vary according to the regime of the jurisdiction and to the form of the instantiation. Rather, it discusses the major issues, and provides guidance and direction for considering and managing the future and instantiation specific deployment of *C-ITS*.

4.3 C-ITS 'Liability' aspects

This part if ISO/TR 17427 explores potential business, organisational and regulatory approaches to address liability concerns, and particularly the combination of such aspects in order to manage liability issues related to *C-ITS* service provision.

As transport technology advances, the issue of who is liable in the event of a crash will potentially become more complex. The question of how liability would be resolved in the event of *C-ITS* system failure will be important in providing certainty to drivers, manufacturers, insurers and road managers. It is expected that the number of crashes would be reduced significantly in a fully *C-ITS* equipped environment, however crashes would still occur, with some specific *C-ITS* related reasons such as the following:

— data communication failure or interference;

— conflicting or erroneous warnings being provided to drivers;

— driver failing to respond to a warning received;

— driver over-reliance on the technology;

— driver switching off the *C-ITS* and being involved in injury to a third party that may have been avoided had he been receiving the benefits of the service.

A number of other scenarios could also be imagined, involving either the failure of the technology, limitations of the technology in different conditions or problems in the interaction between the driver and the technology. *C-ITS applications* (2.1) draw together the whole range of parties typically involved in the transport network, including road agencies, drivers, operators and manufacturers.

While *C-ITS applications* have significant potential to increase road safety, crashes will continue to occur and liability issues will arise. *ITS applications* in general raise some broad liability risks.

Within any jurisdiction, any guidance or legislation that seeks to deal with the issues raised by *ITS* based solutions will have to interact with the current regulatory framework in a sufficiently clear and delineated manner and will have to deal with a wide range of causes of liability including the following:

— device or system failure;

— conflict between multiple *ITS* products;

— operator information overload;

— loss of operator attention;

— risk compensation;

— incorrect interpretation of information;

— liability arising as a result of the interaction of both enabled and conventional vehicles.

Although most *C-ITS* service provision is designed to, and overall may be proven to, improve safety and reduce or mitigate death and injury, it must be recognized that *C-ITS application*s could potentially cause a collision, for example, when such an *application*

— fails to provide an appropriate warning in the lead-up to a collision,

— provides incorrect information (for example, in regard to the local speed zone),

— provides a misleading warning (for example, the direction of a potential collision is unclear),

— provides a warning which distracts the driver, leading to a crash, and

— overrides the driver's action in a way that causes a collision (for example, a brake assist *application* that causes a vehicle to brake suddenly in the middle of fast moving traffic).

Failure to provide appropriate warnings could result from a range of sources, including software problems (including those introduced as part of upgrades), limitations on sensors, signal interference, lack of accuracy in mapping or positioning information or other sources. The exact list will depend on the specific *application*s and whether they are merely advisory systems or more interventionist systems.

It is important to understand that liability concerns have been raised as a potential disincentive for manufacturers to develop *C-ITS application*s and other safety systems: *'these technologies pose challenges for manufacturers and may increase their liability risk in ways that discourage the efficient introduction of these technologies'*.[5][6]

The introduction of airbags by the US National Highway Traffic Safety Administration (NHTSA) is a cautionary example, where even safety technology with significant benefits can have unintended consequences.

In 1977, in the USA, NHTSA estimated that air bags would save on the order of 9,000 lives per year and based its regulations on these expectations. Today, by contrast, NHTSA calculates that air bags saved 8,369 lives in the 14 years between 1987 and 2001. Simultaneously, however, it has become evident that air bags pose a risk to some passengers, particularly smaller passengers, such as women of small stature, the elderly, and children. NHTSA determined that 291 deaths were caused by air bags between 1990 and July 2008, primarily due to the extreme force that is necessary to meet the performance standard of protecting the unbelted adult male passenger. Houston and Richardson describe the strong reaction to these losses and a backlash against air bags, despite their benefits.[6]

In another scenario, the European Commission has supported and encouraged the use/implementation of 'Electronic Stability Control' through the development of a UNECE regulation Global technical regulation No. 8 'Electronic Stability Control Systems'. The EU has adopted UNECE GTR's as a requirement for vehicles sold in the EU. "*Crash data studies conducted in the United States of America (U.S.), Europe, and Japan indicate that ESC is very effective in reducing single-vehicle crashes. Studies of the behaviour of ordinary drivers in critical driving situations (using a driving simulator) show a very large reduction in instances of loss of control when the vehicle is equipped with ESC, with estimates that ESC reduces single-vehicle crashes of passenger cars by 34 per cent and single-vehicle crashes of sport utility vehicles (SUVs) by 59 per cent. The same recent U.S. study showed that ESC prevents an estimated 71 per cent of passenger car rollovers and 84 per cent of SUV rollovers in single-vehicle crashes. ESC is also estimated to reduce some multi-vehicle crashes, but at a much lower rate than its effect on single-vehicle crashes. It is evident that the most effective way to reduce deaths and injuries in rollover crashes is to prevent the rollover crash from occurring, something which ESC can help accomplish by increasing the chances for the driver to maintain control and to keep the vehicle on the roadway. It is expected that potential benefits would be maximized by fleet-wide installation of ESC systems meeting the requirements of this gtr.*"

While the evidence is clear that ESC provides a dramatic improvement to road safety, it cannot be ruled out that on some rare occasion, the behaviour of an ESC system, even when functioning normally within and to the requirements of the UNECE 'Global Technical Regulation', may in some odd combination of road camber/surface and weather condition operate in such a way that the consequence resulted in the death or injury of the occupant of a vehicle or of a pedestrian. In the litigious environment of the modern world, how is the 'liability' managed? Could an aggressive lawyer, acting on behalf of the deceased or injured relatives sue the automobile manufacturer by claiming that its equipment was responsible for the death or injury?

The adoption of GTR 8 as a condition of vehicle manufacture/sale in EU means that automotive manufacturers are required by law to equip certain classes of vehicle with ESC. Therefore the automotive manufacturer is protected from, or has a perfect defence against, being sued for liability for any such consequence. This regulatory route is a methodology that should be considered by jurisdictions willing to support the implementation of *C-ITS* service provision.

(However, GTR 8 enables the driver to disable the ESC system, and it has yet to be tested in court as to a driver's liability where he has manually disabled the ESC system and there is an accident that involves death or injury).

Similarly, *C-ITS applications* could potentially save many lives, but cause the loss of a small number of others; a net gain for society but an extremely difficult problem from a liability (and ethical) perspective.

But liability risks could prevent the roll-out of *C-ITS applications* or severely reduce their scope of operations, even where there is a clear overall societal benefit, because manufacturers could become excessively cautious in order to protect themselves against claims. At the same time the threat of future litigation also acts as a safeguard, ensuring rigorous testing and research before any public release.

Jurisdictions need to assess the overall benefits of the provision of specified *C-ITS* assisted service provision and ensure that there is a supportive legislative environment to provide reasonable protection from liability.

For *C-ITS* assisted services with a demonstrable societal benefit, the jurisdiction should seek to provide protection (probably by a legislative requirement) in the case where the system/equipment is operating properly, but retain responsibility to ensure that the equipment/system is operating properly.

Liability may also depend on any schemes for approving or accrediting systems. If systems are accredited, rather than left to manufacturers to develop, this may subtly shift the liability. Separation of the responsibility for the operation of a 'system' and the functional operation of its component equipment, may therefore be very important, and requires an adequate 'audit trail' to identify responsibility.

Finally, there may be circumstances where collisions are caused as a result of deliberate abuse, including sending a false signal (through sensor or software manipulation) or a 'denial of service' attack which interferes with the system by sending a more powerful signal or flooding users with messages.

The risk of such attacks is considered to be low by jurisdictions currently assessing these possibilities, but, deployers need to be protected against being held liable for the consequential losses involved with such malicious attacks. Once again, an adequate 'audit trail' appears to be a strong source of protection, although the audit trail itself must be protected against abuse of privacy (see ISO 17427-7).

5 What are the key liability issues

5.1 Effects of different types of C-ITS applications technology risk

There are a variety of ways to classify *C-ITS applications*, for example those that:

— provide for interventions (braking and/or steering) or for information/warning only

— provide for overridable interventions or for non-overridable interventions

— provide for interventions in time-critical situations or for a kind of continuous support

— provide for interventions in time-critical situations for interventions at an earlier stage when a collision is unavoidable

Each of these will have a separate set of risks:

Functions providing for mere information warnings can easily be overridden and hence be controlled by the driver. Functions providing for automated braking and/or steering interventions bring an increased product liability risk since the driver has to do more than simply ignore a false-positive warning: he/she will have to counteract actively on a false positive intervention. Non-overrideability of automated braking and/or steering interventions increases the product liability risk since, in this case, the driver cannot counteract a false-positive intervention.

In most current generation *application*s (currently being trialled), the *C-ITS application* effectively acts as a secondary safety system, providing an additional set of warnings to the existing safety systems and processes. However, *application*s that actively intervene in the driving task have a different risk profile with regards to liability.

EXAMPLE In a number of cases, overseas courts have found *GNSS* (2.5) navigation systems not to be liable for directions followed, even where they have been incorrect, because these are primarily advisory systems.[8]

A US report concluded that '*autonomous vehicle technologies are likely to reduce liability for drivers but increase liability for manufacturers as perceived responsibility for crashes shifts from drivers to the vehicle itself. This may impede development and use of these technologies.*'[5][6]

While automated 'interventionist' systems may become increasingly common in the longer term, vehicle technology such as *C-ITS* is not likely to become mandatory until

1) the technology is mature enough that manufacturers are completely confident in their operation and reliability, unless incentives are provided to cover liability, and

2) safety effects are well understood, including understanding the performance of the technology in different conditions and with different users.

Most advanced safety systems can also be understood as a series of typical functions: sensing, planning and acting. Each again comes with its own risks.

Sensing involves taking in data from various sensors (which may have limitations) and aggregating that data.

Planning involves predicting movements of other vehicles and formulating appropriate responses.

Acting involves carrying out the appropriate response, which may be to provide a warning or to intervene in the driving task.

5.2 Crash causation

In a cooperative environment, the threads of causation will potentially be much more complex and difficult to trace than in solely *in-vehicle system* (2.6). Potential points of failure could include

— messages not being correctly sent or received,

— signal interference,

— failure to translate a signal into a warning for the driver, and

— failure by a driver to understand or react to a warning.

Understanding the warnings and signals that may or may not have been sent or received in the lead up to a collision will create challenges to crash investigators and may result in greater use of in-vehicle data

logging, such as 'Electronic Data Recorders', by manufacturers. Reducing the number of components in a safety system is another common means in the industry of avoiding single points of failure.

Even more complex scenarios can easily be imagined, such as those involving larger numbers of vehicles, different types or classes of vehicles (such as trucks or public transport), V2V and V2I *applications* (which, if not managed in advance of deployment, could potentially increase the risk of liability for road authorities).

In addition to failures to prevent a collision, other failures could include generation of false positives or unwanted activations possibly causing a crash. Causation may be difficult to determine in these scenarios.

5.3 Types of parties in C-ITS

C-ITS applications draw together a range of parties typically involved in vehicle crashes today. For a more full understanding of the 'roles and responsibilities' involved in *C-ITS* service provision, see ISO 17427-1. In summary, these are likely to include

— vehicle manufacturers,

— technology providers of *in-vehicle systems*, network technologies and roadside devices,

— after-market device manufacturers,

— road managers, both public and private,

— *C-ITS application* system managers,

— information service providers,

— drivers with *C-ITS* enabled systems, and

— drivers without *C-ITS* enabled systems.

There will be different liability concerns for different parties, in particular manufacturers, technology providers, *C-ITS* system managers and road managers.

Manufacturers and technology providers will be exposed to liability – the issue for both will be determining the limits of liability and the standards expected. In the absence of regulatory requirement, guidance or industry standards, this will be a matter for the courts to determine on a case by case basis. As discussed above, reasonable measures of protection for manufacturers can be provided by the timely (pre-deployment) provision of regulatory requirements.

C-ITS core system (2.4) system managers and regulators will manage the communications access rules, architecture and other key elements. These parities will need to consider and contain liability in advance of deployment or they could by default become the point for claims where responsibility is difficult to establish:

Establishing liability against a public body for a failure of infrastructure is a comparatively hit and miss area and is comparatively rarely achieved.

EXAMPLE Authorities are not normally liable for damage caused by poor road surfacing even though this can result in serious accidents.

However, methods of transport that rely more on complex systems maintained by public bodies generally tend to see a higher rate of successful litigation in the event of a failure (e.g. failure of rail or air-travel related infrastructure). It is arguable that complex ITS based solutions are closer to the latter approach and this could lead to a higher likelihood of public bodies being found liable where a system has failed.[9]

Core systems managers could be exposed to liability if certificate issuing systems fail, resulting in the inability of a user to gain access to the benefits of a *C-ITS* assisted system. Road managers will potentially be exposed to liability as the provider of road-based V2I signals as crashes could be caused if incorrect information is sent out, such as incorrect speed limits. Such concerns may slow the roll-out

of V2I systems. However, the experience in similar areas of road management suggests that the liability risk can result in an improved system.

EXAMPLE Dynamic speed signs that are subject to power or communication failures, for example, have resulted in improved back-up systems, redundancy of connections and power supplies and other controls that significantly reduced the liability exposure of road managers.

These liabilities all need to be managed in advance of deployment, and in most cases, can be managed by the pro-active and response driven agreement to considerations of service provision.

5.4 Human factors

As discussed above, human factor considerations for *C-ITS application*s may suggest a greater duty on manufacturers to explain the use and limitations of such systems, including foreseeable misuse and for greater demonstration of how such *application*s would handle system failures:

In this case, the policy issues are closely aligned with issues regarding liability and the responsibility of the driver to be aware of whether the system is operating correctly, and to know how to react if it is not. This has implications for the ability of the system to report faults, or drops in performance that might lead to failure, and how the current system status is reported to the driver. Therefore, there will have to be a policy on system safety to complement policies on highway and vehicle engineering safety.[10]

*C-ITS application*s may need to take into account different types of users in their design:

Recall that standards for air bags were set for only a limited section of the driver and passenger population – namely, average male adults. It became apparent only after widespread implementation that they put smaller passengers at risk of injury or death. Autonomous vehicle technologies, too, will affect different people differently. In the case of driver-warning systems, for example, users' expectations of how and when the technology will work and their ability to understand the system's directions and warnings will affect the effectiveness of the technology. Therefore, standards must be developed that take into account diverse populations.[11]

5.5 What is the standard of safety expected?

Some commentators have suggested that there is a split in approaches between those 'based on consumer expectations' and those which focus on a risk-benefit analysis.

There may in some circumstances be fundamental limitations on the success rate for some *application service* (2.2) provision *application*s in some scenarios.

EXAMPLE 1 Urban canyons can interfere with signals.

EXAMPLE 2 Incidents can cause network overload.

EXAMPLE 3 The wireless communications opportunities are limited in much of the Australian outback, Russia, the Amazon, Northern Canada, etc.

6 Legal Status

6.1 Regional and National variations

6.1.1 General

Liability is an area where there are very well-established principles in most countries. These have been derived from centuries of common law but also incorporating a series of more recent legislative amendments and extensions. Liability varies in extent in different countries, but the accepted principles are remarkably consistent around the world.

In transport crashes, liability encompasses three broad areas of law: tort, contract and product liability. Each of these will be discussed in turn; however, an important initial concept is the driver control of the vehicle. See 6.2.

6.1.2 Europe

In Europe, liability issues have been identified as a key question to be addressed for *ITS* generally:

Liability issues have notably hampered the market introduction of intelligent integrated safety systems, with legal questions regarding product/manufacturer liability and driver responsibility. For advanced driver assistance systems, for instance, the liability risks may be highly complex — the term 'defective product' is used in the EU product liability directive not only in a technical sense but is also linked to human factors including system requirements such as dependability, controllability, comprehensibility, predictability and misuse resistance, which in turn brings in human–machine–interaction safety issues.

However, analysing liability in Europe in relation to driver assistance systems, Van Wees[34] concluded that:

"Product liability stresses the responsibility of the industry and is far more flexible than vehicle safety regulation. This being said, however, we could still agree that it would be undesirable if system developers and car manufacturers are discouraged to develop and market ADAS only because the (perceived) liability risks are too high. Product liability is often labelled as an important 'show stopper' for the market introduction. Certainly, more advanced ADAS such as anti-collision systems that intervene in critical situations, will because of the consequences potentially raise serious and difficult product liability questions which may need some legal intervention.

However, one should not put all the blame on liability. First of all, the threat of product liability will have a preventive effect, helping to keep immature or poorly designed technology off the market. Secondly, an important observation in this respect is that, although product liability is getting a lot of attention in the legal literature, case law on the subject, especially in relation to the automotive sector, is rather rare. Of course, this may certainly not be considered the only indication whether or not product liability must be regarded as a threat for the deployment of ADAS. For instance, most claims will probably not reach court, because manufacturers prefer settlement outside court. Collecting evidence about such settlements is almost an impossible task. It appears, however that in Europe (automotive) producers are, in contrast to the United States, until now not burdened with a great number of claims. Recent evaluations of the Product Liability Directive did not reveal any serious problems of the automotive industry with this Directive either. Furthermore, the introduction of other innovative automotive technologies, such as navigation systems, ABS, ESP or ACC, does not seem to be seriously limited by the impact of the product liability law."

This last point is particularly worth noting in the context of considering whether legislative changes are required.

Europe has also developed a code of practice for the design and evaluation of driver assistance systems, which *'summarizes best practices and proposes methods for risk assessment and controllability evaluation'*.

Recognizing that 'existing technical limits, as well as liability issues, are currently delaying the market introduction of Advanced Driver Assistance Systems', the code of practice is intended to allow manufacturers 'to demonstrate that state-of-the-art procedures in ADAS development have been applied, including risk identification, risk assessment and evaluation methodology.'[16]

6.1.3 USA

As part of its 'Connected Vehicle Program', US DoT RITA has an ongoing policy and Institutional Issues project, one of whose tasks is to look at liability issues, including

— developing a risk inventory,

— developing a framework for addressing potential risks, including risk mitigation strategies, and

— conducting an industry impact analysis.[3]

The US has a thorough website analysis of its strategy towards *C-ITS*, and particularly aspects involving *core systems*. See the links in Reference [3].

Electronic data recorders may play an important role in *C-ITS* systems in order to log events, providing the 'audit trail' mentioned throughout this report. In the US, such data has previously been used in order to prove criminal liability. As far back as 2002, a driver was convicted of manslaughter, in part based on evidence from an electronic data recorder. These issues also arise in regard to compliance and enforcement, considered later in this paper. 'Electronic Data Recorders' also play an important role in monitoring for defects, which can lead to recalls when required.

6.1.4 Australia

Australia has made comprehensive study of *C-ITS* liability issues that have formed the backbone start point and much of the content of this Technical Report. See Reference [1] for further detail.

6.1.5 China

To be discussed in the next edition of this Technical Report.

6.1.6 Japan

To be discussed in the next edition of this Technical Report.

6.1.7 Other Countries

To be discussed in the next edition of this Technical Report.

6.2 Driver remains in charge

To be discussed in the next edition of this Technical Report.

If the liability of the actors required to make *C-ITS* service provision happen is to be reasonably controlled and limited, it is imperative that in most circumstances, the jurisdiction determines and enforces a regulative environment where, in most circumstances, the driver is considered to be in control of the vehicle and must drive safely for the conditions. The liability regime needs to remain premised on 'driver responsibility for the control of the vehicle'. This is derived from the Vienna Convention on Road Traffic.[12] This is an important assumption from a liability perspective but one that may be challenged with increasingly automated systems entering public roads.

This obligation has been found by the courts (in many countries) to operate in a variety of driving scenarios, for example when a driver approaches an intersection:

The common-law duty to act reasonably in all the circumstances is paramount. The failure to take reasonable care in given circumstances is not necessarily answered by reliance upon the expected performance by the driver of the give way vehicle of his obligations under the regulations; for there is no general rule that in all circumstances a driver can rely upon the performance by others of their duties, whether derived from statutory sources or from the common law. Whether or not in particular circumstances it is reasonable to act upon the assumption that another will act in some particular way, as for example by performing his duty under a regulation, must remain a question of fact to be judged in all the particular circumstances of the case.[13]

The obligation of each driver of two vehicles approaching an intersection is to take reasonable care. What amounts to 'reasonable care' is, of course, a question of fact but to our mind, generally speaking, reasonable care requires each driver as he approaches the intersection to have his vehicle so far in hand that he can bring his vehicle to a halt or otherwise avoid an impact, should he find another vehicle approaching from his right or from his left in such a fashion that, if both vehicles continue, a collision may reasonably be expected.[14]

These examples happen to be taken from Australian road use regulations, but similar can be found in most driving/Highway codes. The UK Highway code states very simply for example: "*You MUST exercise proper control of your vehicle at all times*".[14][15]

6.3 Tort

6.3.1 General issues regarding 'tort'

In most countries, a wronged party (for example, one having been in a collision) can take action against another party or parties under the common law action of tort (a wrongful act or an infringement of a right (other than under contract) leading to legal liability). Such cases require the key elements of

— duty of care,

— breach of duty (that is, standard of care),

— causation, and

— damage.

In English Law, and one of the bases of the law regarding tort in many countries, Lord Atkin set the precedent "*You must take reasonable care to avoid acts or omissions which you can reasonably foresee would be likely to injure your neighbour... persons who are so closely and directly affected by my act that I ought reasonably to have them in contemplation as being so affected when I am directing my mind to the acts or omissions which are called in question*." This has been generally broadened to include three basic elements of tort:

— reasonable foresight of harm;

— sufficient proximity of relationship;

— Is it is fair, just and reasonable to impose duty of care.

If all three parts are satisfied, a duty of care may be imposed.

Whilst the duty of care for service providers to their clients is clearly easily established, and also on a public road establishing any breach by the road manager will likely be straightforward. But with *C-ITS* service provision, where decisions are made as a result of information received from parties where there is no direct contractual or clear civil relationship, is there "sufficient proximity of relationship" for tort to be applicable?

C-ITS data provision may raise particular issues in relation to causation and the remoteness of the damage caused, and judges are likely to be minded to turn to the original stipulation of Atkin "*You must take reasonable care to avoid acts or omissions which you can reasonably foresee would be likely to injure your neighbour*". Current legal opinion is likely to interpret this that accidental misinformation, or accidental error in transmission, either causal to the transmission or in the content of the transmitted information, would not be a breach of duty of care, however deliberate misinformation or information transmitted from equipment that was not properly maintained could well be interpreted as a breach of duty of care, even if there be no contractual relationship between the parties. The common law is supplemented and amended by state legislation in most jurisdictions, and often in a particular a series of civil liability acts. There is likely to be different interpretation in different jurisdictions.

Also with *C-ITS* equipped vehicles, the Atkins precedent "*omissions which you can reasonably foresee would be likely to injure your neighbour*" could be taken as a duty of care that *C-ITS* equipped vehicles have a duty to share relevant *C-ITS* information with their neighbour. It is likely that these issues will have to be tested in court, and may provide different results in different jurisdictions, but their potential interpretation can provide guidance to limit liability.

Terms and conditions of use will need to be clearly defined with clear caveats on the limits of liability of the data provider, and the duty of care moved as far as possible to the user of the data having a requirement to use reasonable care in the use and interpretation of received data. Otherwise no-one

will be prepared to share data/information for fear of incurring liability. It has been suggested that 'Terms and Conditions of Use' will need to explicitly define the user of information as the party in charge to treat the received information as being sent 'in good faith' but 'caveat emptor'. This needs to be examined within the paradigm of each jurisdiction.

Under the principle of caveat emptor, the 'buyer' cannot not recover damages from the 'seller' for defects on the property that rendered the property unfit for ordinary purposes. The only exception is if the seller actively concealed latent defects or otherwise made material misrepresentations amounting to fraud. Hence, buyers are advised to be cautious. In respect of caveat emptor, a 'buyer' is a party who contracts to acquire an asset in return for some form of consideration. While the information exchanged in *C-ITS* may have no monetary consideration, 'Estoppel' is an equitable doctrine that provides for the creation of legal obligations if a party has given another an assurance and the other has relied on the assurance to his detriment. That assurance may be considered a 'consideration' in many legal jurisdictions. Indeed in Roman law, and jurisdictions whose legal framework is based on the principles of Roman law, consideration is not an absolute requirement of a contract. That there is no formal contract between the parties in much *C-ITS* service provision, is covered in the circumstances of caveat emptor, as a quasi-contract. Quasi-contracts are defined to be "the lawful and purely voluntary acts of a man, from which there results any obligation whatever to a third person, and sometime a reciprocal obligation between the parties".

This interpretation of an implied contract, rather than 'tort' may be interpreted in some jurisdictions as being more relevant to *C-ITS* systems which are dependent on the mutual exchange of information.

To manage liability, therefore, the terms of participation by all parties in the provision of information need to be agreed in advance in terms and conditions of use. The exact situation and conditions may vary according to the legal paradigm of the jurisdiction, but in general terms should seek to be a relationship of reciprocal obligation between the party receiving and any *C-ITS* equipped party providing the information (data) conducted caveat emptor between both parties. This could minimize the risk of being pursued through 'tort' (which only applies to uncontracted parties).

6.3.2 Consequences of 'breach of duty'

The consequences of 'breach of duty' will vary from jurisdiction to jurisdiction, but generally will encompass such issues as the following.

— For the purpose of deciding the scope of liability, the court will have to consider (among other relevant things) whether or not and why responsibility for the harm should be imposed on the party who was in breach of the duty.

— The court must consider why responsibility should be imposed on the party in breach and these provisions appear designed to bring out any policy issues and judgements in assessing liability.

'Scope of liability' is likely to cover issues, other than factual causation, referred to in terms such as 'legal cause', 'real and effective cause', 'common sense causation', 'foreseeability' and 'remoteness of damage".

Causation is also usually not an 'all-or-nothing' scenario. Multiple factors may contribute to a crash in a cooperative environment and most jurisdictions embrace concepts of joint, several and contributory liability where a manufacturer or service provider could contribute in part to a collision (and be held liable for this contribution) even if they are not wholly responsible.

On the questions of burden of proof, jurisdictions typically hold that *'in deciding liability for breach of a duty, the plaintiff always bears the onus of proving, on the balance of probabilities, any fact relevant to the issue of causation.*' Whilst this remains an important legal principle, due to the potential difficulties in demonstrating factual causation mentioned above, this may be a high barrier for many claimants to overcome.

It is also worth noting from a transport perspective that many jurisdictions provide certain exemptions for road authorities, in particular in relation to the repair of roads and in assessing whether a road authority, infrastructure manager or works manager has a duty of care or has breached a duty of care. These may need to be updated to adequately cover *C-ITS* and *core systems*.

6.3.3 Contract law

Parties in a cooperative system may be linked through a network of contracts (for example, a road operator who contracts for the provision of a V2I system with an equipment provider and an information provider). Questions about the allocation of risks and liabilities under a contract are largely left to the parties to the contract themselves to determine under the principle of freedom of contract, provided that the contract is not illegal. Contracts in this area will need to ensure that they cover details over uses and ownership of data, allocation of risks and costs and any caps on liability.

Two areas of contract law may be of particular relevance to *C-ITS*:

— disclaimers under consumer contracts;

— insurance contracts will be relevant for the allocation of risks and are governed by local Insurance Contracts legislation.

See 6.3.1 for potential aspects regarding informal contracts.

6.4 Product liability

Product liability is a common aspect throughout the world, but legislation and the scope of consumer protection varies from jurisdiction to jurisdiction. Most jurisdictions have regulations that provide general obligations that goods are of merchantable quality and that services supplied are fit for purpose. The regulations also usually set out obligations to comply with prescribed safety standards.

Suppliers can generally reduce exposure to product liability action by using responsible and sensible business practices, including

— conducting regular reviews of product designs and production,

— ensuring that use limitations and liability limitations are clearly displayed on packaging, in instruction manuals and in marketing material,

— where possible, using proactive 'opt-in' procedures and acceptance of liability limitations,

— implementing and reviewing quality assurance procedures,

— testing products regularly to relevant standards, including batch testing,

— conducting appropriate marketing,

— providing clear and thorough user instructions, and

— where necessary, conducting a quick voluntary recall of any products that are defective or unsafe.

6.5 Compulsory third party systems

Many jurisdictions have compulsory third party personal injury schemes, funded through registration payments. Such schemes provide compensation for personal injuries sustained in crashes on public roads, although terms and benefits vary widely between jurisdictions. Some of these schemes are run on a no-fault basis, others are fault-based. There is a direct economic benefit to these schemes if the road toll is reduced and they are typically very involved in improving road safety.

Although no-fault schemes manage liability for most personal injury cases, liability may still be an issue in some cases, including those involving challenges to commission determinations and those involving exceptions within respective Acts (such as contributory negligence).

Incidents involving a person in the course of their employment may also fall under the relevant workplace health and safety legislation, although most state and territory legislation sets out that employees involved in traffic incidents are captured by the motor vehicle legislation.

7 Policy questions and options

7.1 General

As with privacy, the liability issues rest on the question of how well the present laws apply to the new technology; is *C-ITS* so different from what has gone before that a change in approach is required? A series of broad options are set out below.

7.2 Option 1: Continue current approach

Given the established principles in this area and the lack of strong evidence that liability concerns are holding back the development of the technology, there is a legitimate argument that *C-ITS applications* can fit within the existing liability regimes. Liability issues could be dealt with by the courts under existing laws, and parties in *C-ITS* could establish their own approaches to dealing with liability issues and mitigating their liability risks.

This approach will likely, however, impact on the roll-out of *C-ITS*, as there may be a lack of clarity of the risks, and would not encourage automotive manufacturers to roll out the technology for fear of liability risks.

7.3 Option 2: Enact specific C-ITS liability laws to clarify issues

In order to clarify rights and responsibilities within a cooperative system, specific legislation could be developed by jurisdictions to clarify the position and the extent of liabilities, or amendments could be carved out from existing legislation. This might include certain exemptions for particular parties or providing guidance on where liability should fall in order to ensure a just outcome. The question is whether an approach of 'Regulatory pre-emption' should be taken or whether jurisdictions should seek to track progress in technology and update legislation at a later stage. There is a risk with pre-emption, given the evolving nature of the technology, that such legislation could be redundant before it is enacted.

One approach might involve mandating relevant ISO standards, incorporating performance requirements and test procedures. This would provide greater certainty to providers and to consumers. However, ISO standards should not be implemented in such a way as to inhibit innovation in the industry. Regular reviews would also need to be conducted in order to ensure that rules keep up-to-date with technology.

The ISO 'Release' Procedures, and the associated released standards deliverables, may provide a cohesive way to progress this strategy if it were to be adopted by a jurisdiction.

Jurisdictions need to assess the overall benefits of the provision of specified *C-ITS* assisted service provision and ensure that there is a supportive legislative environment to provide reasonable protection from liability.

For *C-ITS* assisted services with a demonstrable societal benefit, the jurisdiction should seek to provide protection (probably by a legislative requirement) in the case where the system/equipment is operating properly, but retain responsibility to ensure that the equipment/system is operating properly.

Liability may also depend on any schemes for approving or accrediting systems. If systems are accredited, rather than left to manufacturers to develop, this may subtly shift the liability. Separation of the responsibility for the operation of a 'system' and the functional operation of its component equipment may therefore be very important, and requires an adequate 'audit trail' to identify responsibility.

7.4 Option 3: Non-legislative approaches

A variety of non-legislative approaches could be considered in order to provide guidance to operators or performance-based standards, whilst allowing the market to develop solutions. An example might be the European code of practice for the design and evaluation of ADAS. Such a document could set out for a jurisdiction the general principles to be followed in the design and development of systems, but also include issues such as communicating system limitations to drivers and appropriate driver training.

Jurisdictions could develop a code of practice for *C-ITS* (or more broadly for ADAS) similar to the European code of practice in order to guide developers of *C-ITS applications*.

A 'connected' approach could also require that systems meet accepted International Standards linked to accreditation schemes in order to ensure consistency of approach. This could lead to design on a modular basis and pre-defined quality and safety standards and certification procedures [which] may help overcome liability concerns in this context.

The US seems to be following a 'carrot and stick' approach, with central government funding for *ITS* support being linked to adoption of central policies, but without the mandated legislative requirement for its States to comply.

7.5 Option 4: Information and education campaigns

Information and education campaigns could assist in raising the profile of these systems in order to better generate benefits, along with encouraging best practice and ensuring the public is informed of capabilities and limitations. This approach may assist in addressing some of the human factor issues, however would not guarantee consistency in the development of systems.

8 C-ITS Actors and Liability

8.1 C-ITS and jurisdictions

Road operators/managers will need to create the regulatory framework to enable *C-ITS*, and that, especially if the jurisdiction is operating or supporting a *core system*(s); see the other parts of ISO 17427 in respect of '*core system*', and, especially, ISO/TR 17427-6 in respect of risks associated with the deployment of *core systems.*

Jurisdictions need also to be aware of their general *C-ITS* risks and how these change over time. These risks will of course be dependent on the policy and strategy of the Jurisdiction and its involvement in the deployment and support of *C-ITS*.

Jurisdictions will need to carefully track technological progress to ensure that policy keeps pace.

8.2 C-ITS and road operators/managers

Road operators/managers will also need to be aware of their risks and how these change over time. Governments and road agencies will need to carefully track technological progress to ensure that policy keeps pace. Allocation of risks will need to be clear between different service providers and scenario analysis will need to be undertaken to search for potentially unforeseen consequences.

If a road operator/manager is providing a *C-ITS core system* is operating or supporting a *core system*, see the other parts of ISO 17427 in respect of *core system*, and, especially, ISO/TR 17427-6 in respect of risks associated with the deployment of *core systems*.

Many of the controls mentioned below for manufacturers will also be relevant for road operators, including ensuring backup systems are in place and that appropriate information on any limitations is provided to consumers.

In particular, operators/managers will likely need to carefully examine

— the operation and reliability of any roadside units deployed,

— the accuracy of information being relied upon (such as mapping and speed zone data) and any limitation on information that is being provided,

— how drivers are made aware of any system faults or limitations and limitations of liability by the operator/manager, and

— potential conflicts between different systems, such as visible traffic signals conflicting with the *C-ITS* signal sent out at an intersection.

8.3 C-ITS and manufacturers

Potential liability will put pressure on manufacturers and service providers to make clear any limitations of the system, for example, signal disruption due to adverse weather conditions. It will be imperative that drivers are aware of limitations and take them into consideration in their driving, much as this information can be difficult to convey. A study on the legal impacts of the *C-ITS* 'Interactive' project in Europe found that *'a comprehensive and comprehensible instruction may well contribute to a reduction of the manufacturer's product liability risk.'*

Mitigating measures for manufacturers and others may include (but not be limited to)

— additional driver training,

— information provision, both in-vehicle and in the owner's handbook, communicating to the driver their responsibilities, any system limitations and a warning that *C-ITS applications* should not be relied on in isolation,

— redundancy of sensors and communication systems to improve reliability,

— additional logging of data for resolution of disputes and system diagnostics (for example, through Electronic Data Recorders, with appropriate safeguard for data),

— fall back measures and warnings to the driver when systems are not functioning correctly (fail-safe provisions),

— prudent advertising and marketing of systems to avoid over-reliance or false expectations,

— appropriate insurance.

The onus will be on manufacturers to produce systems which can stand up to legal scrutiny. But many, if not all, of these measures are already standard practice for major manufacturers as part of their development process and therefore may not require further regulation or other government action.

Manufacturers also need to follow IEC 61508 1-10 when designing E/E/PE safety related systems.

Manufacturers are also advised to take heed of ISO 26262-1-10 in order to minimize their liabilities.

8.4 C-ITS information/application service providers

C-ITS application service providers and information service providers will need to make clear any limitation on information being provided and may need to ensure that commercial features do not conflict with safety features.

8.5 C-ITS and drivers

C-ITS applications could in fact put more onus on the liability of the driver, by providing them with additional warnings that if ignored, put more responsibility on the driver for their actions. It may prove difficult to show definitively that a driver ignored a warning. A report into the potential liability issues of the CVIS project concluded that:

The system should be deployed in a way where the CVIS safety messages are considered as a bonus to something else. The driver remains responsible. All information provided is only additional assistance to the driver. One example for this principle is traffic management systems. If the system fails the traffic lights still work. Thus, safety is never compromised, only additional benefits such as green waves are lost.[2]

The first generation of *C-ITS applications* can be viewed similarly — these will provide additional warnings to drivers that they do not have today, whilst retaining all of the existing signals, signs and information that they have traditionally relied upon. However, as vehicles evolve to have more active

