TECHNICAL REPORT

ISO/TR 17427-3

First edition
2015-11-01

Intelligent transport systems — Cooperative ITS —

Part 3: Concept of operations (ConOps) for 'core' systems

Systèmes intelligents de transport — Systèmes intelligents de transport coopératifs —

Partie 3: Concept des opérations (ConOps) pour les systèmes 'principaux'

Reference number
ISO/TR 17427-3:2015(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 systems 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 architectures(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 'Concept of operations for ore systems' supporting *Cooperative intelligent transport systems* (*C-ITS*). It is intended to be used alongside ISO 17427-1, ISO/TR 17465-1 and other parts of ISO 17465, and ISO 21217. Detailed specifications for the application context will be provided by other ISO, CEN and SAE deliverables, and communications specifications will be provided by ISO, IEEE and ETSI.

Introduction

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

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

Some *ITS*s 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*s are informative, for example, 'Variable Message Signs' at the roadside, or transmitted into the vehicle, provide information and advice to the driver. Some *ITS*s 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 technologies enable vehicles to 'talk' to each other and to the infrastructure, and in so doing will have significant potential to improve the safe, sustainable and efficient operation of the transport network.

A distinguishing feature of '*C-ITS*' is that data is used across application/service boundaries. This means that data collected at one point and/or processed by one application becomes available to be re-used by other applications, which may be operating in the same, or different physical entities.

The difference between any '*ITS* implementation' and a '*C-ITS* implementation' is that *C-ITS*s are dependent on the interaction with other vehicles and/or the infrastructure, and the exchange of dynamic data, to receive data to enable their function, or conversely to provide data to other vehicles/infrastructure to enable their *C-ITS*s to function.

C-ITS as an entity, is therefore the *functionality that enables* such 'cooperative' and collaborative exchange of data, and in some cases, collaborative control, or even decision making, that will enable applications to provide their services to one or more *actors* (3.1).

ISO/TR 17465-1 provides a summary definition of *C-ITS* as a "subset paradigm of overall *ITS* that communicates and shares information between *ITS-station*s to give advice or facilitate actions with the objective of improving safety, sustainability, efficiency and comfort beyond the scope of stand-alone systems".

ISO 17427-1 will provide descriptions of the roles and responsibilities of *actors* involved in the provision and use of *C-ITS*.

ISO/TR 17427-2 provides a framework overview which characterize the components of a *Cooperative-ITS* (*C-ITS*), its context and relevance for *ITS service* provision, and provides references to Standards deliverables where specific aspects of *C-ITS* are defined.

This Technical Report concerns the high-level generic requirements for the "Concept of operations" for a 'Core System' (*CorSys)* (3.10) to support *C-ITS* in a connected vehicle-highway system paradigm. It is agnostic in respect of technology and operates with whatever (and probably multiple) *communications* technologies and hardware technologies that can support its functionalities.

The benefits of *Intelligent Co-operative Systems* (*C-ITS*) stem from the increased information that is available from the vehicle and its environment and from other vehicles. The same set of information can be used to extend the functionality of the in-vehicle safety systems and through vehicle-to-

infrastructure *communications* for more efficient traffic control and management. The benefits include the following:

— improved safety;

— increased road network capacity;

— reduced congestion and pollution;

— shorter and more predictable journey times;

— improved traffic safety for all road users;

— lower vehicle operating costs;

— more efficient logistics;

— improved management and control of the road network (both urban and inter-urban);

— increased efficiency of the public transport systems;

— better and more efficient response to hazards, incidents and accidents.

(source: EC project CVIS)

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 in a connected vehicle-highway system paradigm.

Other parts in this family of *C-ITS* standards will define specific aspects of technology and behaviour, and the roles and responsibilities within the context of *C-ITS*.

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 3:
Concept of operations (ConOps) for 'core' systems

1 Scope

This Technical Report provides the high-level generic requirements for the "Concept of operations" for a 'Core System' (*CorSys)* (3.10) to support *C-ITS service* delivery. It is intended as an input to the planning and development elaboration of core functions that will support the deployment of *cooperative intelligent transport systems* (*C-ITS*) in a connected vehicle-highway paradigm.

The objective of this Technical Report is to raise awareness of and consideration of such issues and to give pointers, where appropriate, to standards existing that provide specifications for all or some of these aspects. This Technical Report does not provide specifications for solutions of these issues.

This Technical Report is agnostic in respect of technology and operates with whatever (and probably multiple) *communications* technologies and hardware technologies that can support its functionalities.

2 Normative references

There are no normative references.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
actor
party participating in a system, within this Technical Report participating in *C-ITS* (3.6) service provision/receipt

3.2
application
'app'
software application to provide functionality to realize *C-ITS* (3.6)

3.3
application service
service provided by a service provider accessing data from the *IVS* vehicle in the case of *C-ITS* (3.6), via a wireless *communications* network, or provided on-board the vehicle as the result of software (and potentially also hardware and firmware) installed by a service provider or to a service provider's instruction

3.4
back office
central system ('*centre*'/*CorSys*) for commercial *applications* (3.2)

Note 1 to entry: The terms '*back office*' and '*Centre*' are used interchangeably throughout this Technical Report. '*Centre*' is a traditionally transport-focused term, evoking management *centres* to support transport needs, while *back office* generally refers to commercial *applications* (3.2). From the perspective of this *ConOps,* their functions are considered to be similar.

3.5
bounded secure managed domain
BSMD
secure *ITS-station* entity capable to conduct secure peer-to-peer *communications* (3.8) between entities (*ITS-stations*) that are themselves capable of being secured and remotely managed

Note 1 to entry: The bounded nature is derived from the requirement for *ITS-stations* to be able to communicate amongst themselves, i.e. peer-to-peer, as well as with devices that are not secured (referred to as 'other *ITS-stations*'),and realizing that to achieve this in a secure manner often requires distribution and storage of security-related material that needs to be protected within the boundaries of the *ITS-stations*, leads to the secured nature of the entity - as there is great flexibility to achieve desired *communication* goals, there is a requirement that this flexibility be managed; within *C-ITS* (3.6) and ISO 21217 such *ITS-stations* are defined as operating within *bounded secured managed domains* (*BSMD*), or outside of the *BSMD*.

3.6
cooperative ITS
C-ITS
group of *ITS* technologies where service provision is enabled, or enhanced by, cooperating to provide 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)

3.7
centre
central system
traditionally transport-focused term, evoking management *centres* (3.7) to support transport needs and/or providing/supporting *application service(s)* (3.3) managed through a central facility; from the perspective of the *CorSys* similar to '*back office*'

3.8
communication
communications
wireless (and in some cases, *wireline*) networks that facilitate data exchange, including roadside *ITS-stations* where appropriate

3.9
Concept of operations
ConOps
document describing the characteristics of a proposed system from the viewpoint of an individual who will use that system

Note 1 to entry: It is used to communicate the quantitative and qualitative system characteristics to all stakeholders.

3.10
core system
CorSys
combination of enabling technologies and services that will provide the foundation for the support of a distributed, diverse set of *applications* (3.2)/*application* transactions which work in conjunction with external *support systems* (3.24) such as certificate authorities

Note 1 to entry: The system boundary for the *CorSys* 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 *CorSys* users.

3.11
data store
permanent storehouse of data (files, databases, text documents, etc.)

3.12
end user
citizen or legal entity who exercises or benefits from the services of the transport system

3.13
equipped person(s)
persons with mobile phones, tablets or similar *communications* (3.8) devices that provide data collection and processing capacity to perform in the *C-ITS* (3.6) context

3.14
equipped vehicle(s)
vehicles equipped with the device(s) that provide the role of an *ITS-station* in the *C-ITS* (3.6) context

3.15
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

3.16
home agent
'IPv6 router' with which mobiles register their current Care-of Address (RFC 3753)

3.17
in-vehicle system
IVS
hardware, firmware and software on board a vehicle that provides a platform to support *C-ITS* (3.6) service provision, including that of the *ITS-station* (ISO 21217), its facilities layer, data pantry and on-board 'apps'

3.18
intelligent transport system
ITS
transport systems in which advanced information, *communication* (3.8), sensor and control technologies, including the Internet, are applied to increase safety, sustainability, efficiency, and comfort

3.19
ITS application
functionality that either completely provides what is required by an *ITS service* (3.21) or works in conjunction with other *ITS applications* (3.2) to provide one or more *ITS services*

3.20
ITS-s border router
ITS-S router with additional functionality that provides connectivity to other ITS *communication* (3.8) nodes over external networks

3.21
ITS service
functionality provided to surface transport system users

3.22
ITS-station
ITS-s
entity in a *communication* (3.8) network [comprised of *application* (3.2), facilities, networking and access layer components] that is capable of executing *ITS-S* application processes (sometimes within a bounded, secured, managed domain), comprised of an *ITS-S* facilities layer, *ITS-S* networking and 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

3.23
jurisdiction
government, road or traffic authority which owns the *regulatory applications* (3.2)

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

3.24
support system(s)
facilities that assist in *C-ITS* (3.6) service provision, including security credentials certificate and registration authorities, that allow devices and systems to establish trust relationships

3.25
wireline
traditional permanent 'wired' connection (although may in reality include microwave and other wireless connections)

4 Abbreviated terms

2G	second-generation cellular phone technology, e.g. GSM
3G	third-generation mobile phone technology, e.g. UMTS
4G	fourth-generation mobile phone technology, e.g. E-UTRAN (sometimes known as LTE)
BSMD	bounded secure managed domain
C-ITS	cooperative intelligent transport systems, cooperative ITS
CALM	Communications Access for Land Mobiles
ConOps	concept of operations
CorSys	core system
CVIS	Cooperative Vehicle Infrastructure Systems
DoT	Department of Transport
ESS	External System Support
E-UTRAN	Evolved UMTS Terrestrial Radio Access Network
GNSS	global navigation satellite systems
GSM	Global System for Mobile Communication (2G mobile communications)
IPv6	Internet Protocol version 6
ITS	intelligent transport systems
ITS-s	ITS-station
IVS	in-vehicle system
PII	personal identification information
RSE	roadside equipment
SatNav	Satellite Navigation (see 3.15)

TMC	transport management centres
V2I	vehicle to/from infrastructure
V2V	vehicle to vehicle
VANET	vehicular ad hoc network
VMS	variable message sign
UML	Unified Modelling Language (ISO/IEC 19501)

5 Using this Technical Report

This Technical Report is intended to assist parties instantiating a *CorSys*, becoming involved as an *actor* in a *C-ITS* (3.6) that involves the use of a *CorSys*, or becoming involved with the development or use of such a *CorSys*.

This Technical Report provides guidance on the aspects to be considered in developing a 'Concept of operations' (*ConOps*) for a *CorSys* for *C-ITS* support. As such, the advice in this Technical Report is generic and not instantiation specific to any one *jurisdiction* (3.23) or implementation.

This Technical Report is intended to provide a framework and guidance to enable the development of an instantiation specific *Conops* specification after taking into account the aspects specified herein together with the location specific situation (technical and political) and conditions.

6 Overview of the role of a 'Core System' in C-ITS

6.1 What is a Concept of operations?

A 'Concept of operations' is a user-oriented document that describes system characteristics for a proposed system from the users' viewpoint. This 'Concept of operations' describes *C-ITS* stakeholders, their roles and responsibilities in a connected vehicle-highway system paradigm, an overview of the emerging system design, and provides a high-level description of how such systems may operate.

A concept of operations document describes the systems' objectives, user needs, the functions, the *actors* (3.1) and stakeholders involved, and the enactment of roles and responsibilities. (ISO 17427-1 contains an explanation of roles and responsibilities.) A concept of operations is one of the early phases of the Systems Engineering approach. Systems Engineering is an interdisciplinary approach used to enable the realization of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, and then proceeding with design synthesis and system validation.

In respect of *C-ITS*, additional information can be obtained from one of the "standard" architectures such as the US 'Connected Vehicle Reference Implementation Architecture',[3] or the 'European ITS Framework (FRAME) Architecture',[12] or in the architecture document supporting a specific implementation.

It is important to understand that this 'Concept of operations' is focused on, and relates to the provision of, *CorSys* requirements that are necessary in order to facilitate and enable *C-ITS* assisted service provision. This deliverable does not consider in any depth the whole *C-ITS* perspective in a connected vehicle-highway systems paradigm (ISO/TR 17427-2 and ISO 17427-1 contains more detailed consideration of such aspects). This Technical Report is focused on the 'core' system aspects required to support *C-ITS* in a connected vehicle-highway system paradigm. This '*Core system* Concept of operations' does not provide a concept of operations for any particular *application service(s)* (3.3), but for the background facilitation and infrastructure support required for such service provision.

Much of the source material for this deliverable has been obtained from the US DoT RITA "connected Vehicle" initiative [Connected Vehicle Technology. US DoT; Connected Vehicle Reference Implementation

Architecture. (CVRIA); Core System- System Architecture Document (service architecture document), US DoT; Core System- System Requirements Specification (SyRS)]; from relevant Australian publications (*Cooperative ITS* (3.6): Concept of operations for *C-ITS* core functions – Draft Report. ARRB; Cooperative ITS Regulatory Policy Issues. National Transport Commission, Australia) and from the European Project CVIS. See Bibliography for further detail. The permission of these bodies to freely use their material is gratefully appreciated and their source acknowledged.

6.2 What are the core functions?

The 'core' functions are functions that enable the trusted and secure data exchange necessary to enable a platform for *C-ITS applications* (3.2) in a connected vehicle-highway system paradigm. These 'core' functions can be seen as a collection of operational and institutional functions, such as the exchange of security certificates, storage and redistribution of *application* data, and exchange of system management information like subscriptions to *C-ITS applications*. These core functions require policies and management structures to be in place as a basis from which to operate. An example of a policy requirement is a policy on whether core functions are required for *all C-ITS applications*, or only for *some*. Also, ensuring correct implementation of system components and correct functioning of the system requires some form of compliance insurance, such as accreditation, certification, type approval or auditing, to be in place.

This Concept of operations aims to identify those core functions that are required to enable connected vehicle highway systems (*cooperative ITS*) to evolve, as well as the institutional changes required, to enable *C-ITS applications* to be deployed and positive transport and societal outcomes to be realized. Based on an assessment of international *C-ITS* developments, and an assessment of the current local situation, it is proposed that the core functions required to support *C-ITS* are the following:

— Secure exchange of data between users and *applications*;

— Facilitate trust between users;

— Maintain integrity of data;

— Assure privacy between users and from third parties;

— Facilitate a platform for sharing of data and efficient use of resources;

— Assure national/regional interoperability and nationally/regionally consistent service access.

In the predicted paradigm, connected vehicle-highway systems (*C-ITS*) will use several wireless media, as available, in order to provide *C-ITS* based *application services* (3.3), and in all probability, in many circumstances, will use multi-media simultaneously. Service provision will, in all probability, in many cases, not depend on a single wireless medium and will also use on-board sensors and other available data in order to effect robust service provision. Media selection will depend on media availability at the location of the vehicle at the time of service provision and suitability of the characteristics of the media for the particular *application service* provision. Vehicular ad hoc networks (VANETS) are likely to use the allocated 5,9 GHz spectrum for vehicle-vehicle *communications* (3.8), particularly for time-critical safety *applications*, and the infrastructure will use 5,9 GHz spectrum for infrastructure-vehicle *communications* at safety-critical locations. Although this Technical Report uses this working hypothesis, it does not require the use of any particular wireless medium for any particular purpose, rather it considers the consequences of such selection and the *CorSys* support requirements that will need to be in place to enable such service provision.

6.3 Functional subsystems

Within this Concept of operations, the *C-ITS* core functions are clustered in seven functional subsystems, performing

— data distribution,

— misbehaviour management,

— network services,

— service monitoring,

— time synchronisation,

— user permissions management, and

— user trust management.

These core subsystems interact with other *C-ITS* components, such as the *applications*, the networking and transport algorithms and the *communication* infrastructures.

6.4 Institutional context

The *C-ITS* core functions will need an institutional context to operate. This is essential because the functions are executed on different physical *C-ITS* components, being

— vehicles,

— *ITS* roadside equipment,

— mobile devices and

— back office (3.4)/control centres (3.7).

These components are management managed by different stakeholders.

Roles that need to be performed are

— governance roles,

— management roles,

— installation roles,

— certification roles,

— operational roles and

— user roles.

Examples of activities that may require new institutional entities or structures to enable *C-ITS* in a connected vehicle-highway paradigm, include a device certification and possibly registration, security credential distribution, application certification, and compliance insurance. These roles could be assigned to existing organizations or new organizations can be created.

ISO 17427-1 contains further detail regarding the roles and responsibilities of *actors* involved in *C-ITS service* provision and ISO/TR 17427-2 for a framework overview.

Additionally, a policy framework, including the following policies, needs to be put in place:

— a policy setting National, regional or international compliance requirements;

— a policy authorising the issuing of security certificates;

— a policy authorising road users to use certain *C-ITS applications* and send certain *C-ITS* messages;

— a policy defining interpretation of the privacy rules and regulations and 'privacy by design' aspects.

6.5 Specific service features characterizing C-ITS service provision

A nation's road transport system is critical not only to its economy, but also to its social and environmental well-being. It includes numerous different modes of transport, including passenger vehicles (cars and vans), buses, trucks and motorcycles, and needs to be considerate and inclusive of vulnerable road users such as pedestrians and bicycle riders. It also is increasingly integrated and interfacing with other non-road transport modes, such as trains.

ISO 14813-1 describes the ITS service groups and services that are generally considered to comprise the realm of ITS. From ISO 14813-1, we can establish that ITS services can operate in different paradigms, and some application services (3.3) operate autonomously (see examples given in the introduction).

Some *ITS*s are semi-autonomous, in that they are largely autonomous, but rely on 'static' or 'broadcast' data (see examples given in the introduction).

Cooperative ITS (*C-ITS*) is a subset of the broader suite of *ITS*, within a paradigm of connected vehicle-highway systems. *C-ITS* refers to the use of wireless *communication*s to share information from vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) and infrastructure-to-vehicle (I2V). This will enable a paradigm that allows vehicle and transport *applications* to cooperatively work together to deliver outcomes that are beyond what is achievable with standalone *ITS* and vehicle *applications*.

The *cooperative intelligent transport system*s that are evolving will involve wireless connections between the *actors* involved in road transport, and its deployment will be multimodal, as shown in Figure 1.

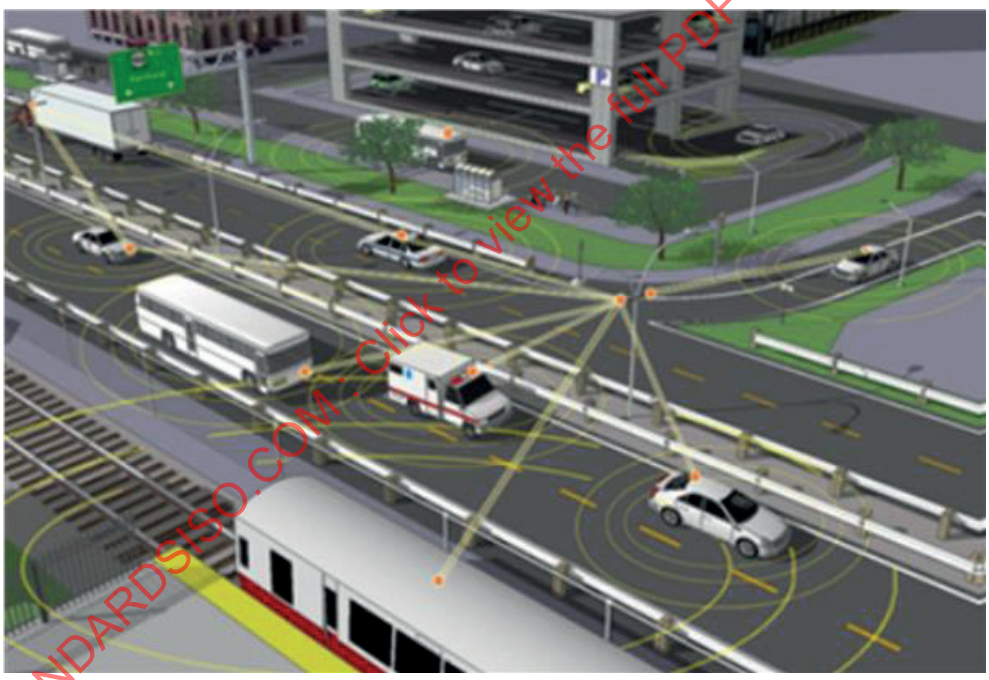

Figure 1 — Multimodal cooperative intelligent transport domain [Source: ARRB/Andersen and McKeever (2011)]

The emerging cooperative intelligent transport domain will involve connections between the following:

— Vehicles – equipped with built-in, aftermarket, or nomadic, *C-ITS* devices

— Infrastructure – *ITS* roadside infrastructure connected through *C-ITS*

— Centres – traffic management centres and service providers' *back office/ centre*s.

The cooperative intelligent transport domain will also include mobile devices (e.g. cellular smart-phones), and also other nomadic devices, focused on assisting vulnerable road users (e.g. bicycle riders, pedestrians, physically and mentally challenged).

In addition, many *C-ITS applications* and services will also require a connection with 'Global Navigation Satellite Systems' (*GNSS*) for positioning, navigation and timing data. The connections between the various *actors* in the cooperative intelligent transport domain are illustrated in Figure 2.

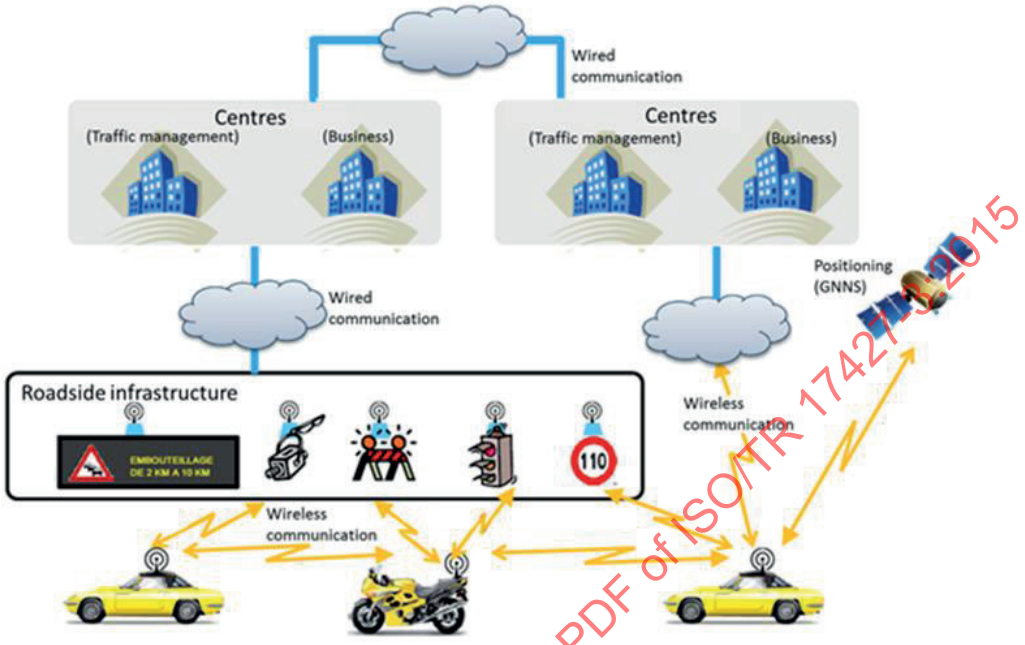

Figure 2 — Cooperative intelligent transport domain
[Source: ARRB/Modified from Lan (2013)]

Cooperative intelligent transport systems (*C-ITS*) are a group of *ITS* technologies where service provision is enabled, or enhanced by, the use of 'live', dynamic, present situation related, data/information from other entities.

Example: from one vehicle to other vehicle(s) and/or between different elements of the transport network, including vehicles and infrastructure.

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 thus have significant potential to improve the transport network. See also ISO/TR 17465-1, ISO 17427-1 and ISO/TR 17427-2.

For specifications regarding *C-ITS* terms, definitions and guidance for standards documents, see ISO 17465-1.

For specifications regarding the structure of specific *C-ITS* Standards deliverables and general *C-ITS* definitions, see ISO/TR 17465-2.

For specifications regarding 'Release' procedures for consistent groups of *C-ITS* Standards, see ISO 17465-3.

It is important to understand that *C-ITS* is not an end in itself, but a combination of techniques, protocols, systems and functions to enable 'cooperative'/collaborative service provision. What separates *C-ITS* from any other *ITS communication* is the sharing and exchange of data to provide information, and in some cases control, cooperatively between *actors* in the road network.

6.6 C-ITS and communication technologies

6.6.1 General

The functionality of *C-ITS* is based on wireless *communications* (vehicle-infrastructure, inter-vehicle), between *communications* facilities called *"ITS-stations"* (3.22), potentially over several different wireless media, and in some cases supported by wired infrastructure-infrastructure *communications*, and also by intra-vehicle exchange of data and, in some cases, control. The *C-ITS* 'Internal Enterprise Objects', are therefore closely aligned with ISO 21217 (*ITS-station* architecture) and its associated family of Standards (See ISO 21217).

Within Figure 5 (6.7), the 'Internal' enterprise objects are surrounded by the wireless and wired media used to communicate between *actors* in most *C-ITS* situations.

While Figure 5 highlights *ITS-station* wireless *communications* as a boundary *actor* (3.1) between the internal and external objects, it should be noted that, in the infrastructure-infrastructure *C-ITS* context, *communications* may be wired, and that so called 'wired' *communications* now commonly also use microwave and other wireless techniques.

In *communications* terms, "*ITS-station communications*" are peer-to-peer *communications*. But in *application service* (3.3) terms, they are *communications* between *actors* involved in *C-ITS service* provision, in which one *actor* will be the service requestor, and the other party will be the service provider. There may of course also be intermediaries in the provision of service chain, and some transactions will require the service of intermediaries for certification, data collation, anonymisation etc., who are not directly involved in a role either as the service requestor or the service provider.

NOTE The party requesting the service is usually the party receiving the service, but this is not always the case. In some circumstances, there are more than two parties to the transaction.

While *C-ITS* involves both infrastructure and vehicles/travellers, and while the infrastructure may (but not always) be in a fixed location, the nature of the *communications* are most frequently 'ad hoc' networks, formed for the duration that *ITS-stations* are communicating with each other, whether they be other vehicles or are in *communication* with the infrastructure that they are currently driving past, or are in their vicinity.

The range of the *communication* zone where such *communication* can take place will depend on the *communication* technology used and the local topography. Typically, a 5 MHz 802.11p *communication* will have a range of 0,25 km to 0,5 km, while a WiFi connection will have a range of 100 m or less and a GSM/UMTS cell range is measured in kilometres. 4G/LTE *communication* will have a shorter range than GSM/3G, but the cellular networked paradigm of GSM/UMTS means that there can be effectively seamless network access over great distances. However, the latency involved in these systems has significantly poorer performance than that of 802.11p 5,9 GHz.

The advent of E-UTRAN (4G/LTE) cellular networks will provide far more capable *communications*, capable of carrying significantly greater amounts of data, and enabling much more rapid transactions, and provide a generally more suitable commercial operating environment for non-time-critical *C-ITS service* provision. It has the strength of the cellular network architecture, meaning that there is continuous session maintenance over the whole covered network, but with a higher latency than 5,9GHz *communications*.

6.6.2 VANETs, MANETs and 'latency'

Vehicle ad hoc networks, so called 'VANETs' or mobile ad hoc networks (MANETs) form the basis of most *C-ITS communications*; and though transient, indeed often because they are transient, and are frequently time critical/safety critical, they frequently need a high level of user trust and low latency.

Data 'latency' can be taken to mean the time duration between issuing a message from its sender until it is received by receiver vehicles. An important parameter to be considered in sending and receiving a data packet is transmission time delay. Examples where latency is of great significance are collision

avoidance and dynamic ramp access control systems. Examples where latency requirements are comparatively low significance would involve ice alerts, and even post incident systems such as eCall.

However, the current *ITS* environment does not adequately support time-critical safety *C-ITS applications*. These will require VANETs with a secure and trusted low-latency data exchange that current cellular (GSM/UMTS) and broadcast technologies cannot provide, although the packet switched E-UTRAN (4G/LTE) has faster data rate and lower latency than GSM/UMTS. For the I2V applications, this function is already provided by commercial *C-ITS service* providers and tele*communications* carriers in the case of the existing cellular-based *applications*.

C-ITS fits into the broader view of what an *ITS* architecture may look like, as shown in Figure 3. With the emergence of *C-ITS* and the subsequent wider use of wireless *communications*, there is the potential to broaden the interaction between vehicles and the field through the use of V2V and V2I/I2V *communications*.

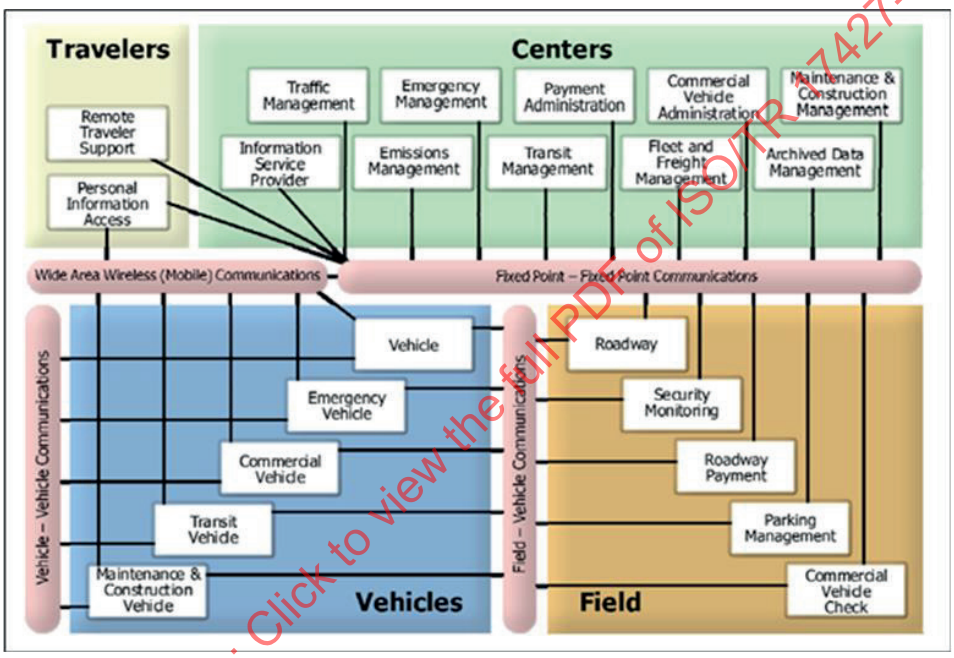

Figure 3 — ITS physical architecture
[Source: Research and Innovative Technology Administration (2012)]

The sharing of data within these situations enables more efficient, safer and efficient service performance and delivery.

There are four important aspects that are significant to understanding the roles of, and therefore the concept of operations for, a *core system*.

a) Some processes relate to the provision of a specific *application service* (external processes, objects and data).

b) Some processes are required to enable a) but are not specifically part of that service provision (internal processes, objects and data).

c) Different transactions require different levels of security.

d) Different transactions require or can tolerate different levels of latency.

Some transactions may be required to operate within what ISO 21217 describes as a 'bounded, secured, managed domain', comprised of an *ITS-s* facilities layer, *ITS-s* networking and 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-station*s with which it communicates (see ISO 21217, ISO 21210, ISO 29281 (all parts), ETSI EN 302 636, and associated standards). Other *C-ITS communication*s, and especially broadcast *communication*s, may not have need of such high levels of security.

Some transactions require very low latency, while others are relatively insensitive to latency.

Systems that require a high level of trust, and in many cases, systems that require low latency, have to be managed during, or preferably before, the event. This can only be achieved by measures such as certification verification, and prioritization, and this requires support from 'central' 'core' services, such as user permissions management, user trust management, data distribution, misbehaviour management, network services, service monitoring, time synchronisation.

For a high level overview of how *ITS-station*s communicate within the context of *C-ITS service* provision, see ISO/TR 17465-1, and for a more detailed specification, see ISO 21217.

Ideally, an *ITS application service*, particularly in the *C-ITS* context, needs a *communication* sub system that

— is available wherever and whenever a vehicle is present in a traffic situation,

— can communicate vehicle-vehicle and vehicle-roadside in a transparent way (see ISO 21217:2014, 8.3.3),

— relieves the applications from the need to know about *communication*s setup and management,

— uses modern Internet techniques and standards for global usability (e.g. IPv6), and

— provides a range of different possibilities related to data speeds, *communication* distance, cost, and many other parameters.

However, in terms of security, all systems are not equal. Some *ITS*s can utilize security from the *communication*s network over which their wireless *communication* is made, which provides adequate security for the provision of their service, and others can control their data so it is only provided to a legitimate destination, indeed some data may not be sensitive to misuse. But most data in the *C-ITS* context has some sensitivity, and therefore will have to be effected within layers of security, and some *C-ITS communication*s will have to be effected within the high levels of security that ISO 21217 calls a 'Bounded Secure Management Domain'. (See ISO 21217 and 6.7.)

For detail of aspects of *communication*s aspects of *C-ITS service* provision, see the following:

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

ISO 21210 Intelligent transport systems — Communications access for land mobiles — IPv6 Networking

ISO 21212 Intelligent transport systems — Communications, air-interface, long and medium range (CALM) — 2G Cellular systems

ISO 21213 Intelligent transport systems — Communications access for land mobiles (CALM) — 3G Cellular systems

ISO 21214 Intelligent transport systems — Communications access for land mobiles (CALM) — Infra-red systems

ISO 21215 Intelligent Transport Systems — Communications access for land mobiles (CALM) — M5

ISO 21216 Intelligent Transport Systems — Communications access for land mobiles (CALM) — Millimetre communications

ISO 21218	Intelligent Transport Systems — Continuous Air Interface, Long and Medium Range — Medium Service Access Points
ISO 24102	Intelligent transport systems — Communications access for land mobiles (CALM) — Management
ISO 24103	Intelligent Transport Systems — Communication access for land mobiles (CALM) — Media adapted interface layer (MAIL)
ISO 25111	Intelligent transport systems — Continuous air-interface, long and medium range (CALM) — ITS using mobile wireless broadband- General requirements
ISO 25112	Intelligent transport systems — Communications access for land mobiles (CALM) — Mobile wireless broadband using IEEE 802.16e/IEEE 802.16g
ISO 25113	Intelligent transport systems — Communications access for land mobiles (CALM) — Mobile wireless broadband using HC-SDMA
ISO 29281 (all parts)	Intelligent transport systems — Communications access for land mobiles (CALM) — Non-IP networking
ISO 29282	Intelligent transport systems — Communications access for land mobiles (CALM) — Using satellite communications
ISO 29283	Intelligent Transport Systems — Communications access for land mobiles (CALM) — Mobile wireless broadband using IEEE 802.20
ISO 17515-1	Intelligent Transport Systems — Communications access for land mobiles (CALM) — E-UTRAN (LTE)

Other *ITS*/*C-ITS communication*s standards will be developed according to need.

The standard networking protocol for most *C-ITS*s will be IPv6 (Internet protocol version 6), although provision for rapid safety critical *communication*s are provided in ISO 29281 (all parts).

6.6.3 Hybrid communications

As described above, *C-ITS* uses wireless *communication*s to share information between V2V and V2I/I2V. *C-ITS* will involve a range of *communication*s technologies, and many *C-ITS* applications will likely use a hybrid *communication*s approach. That is, an application may use several *communication* mediums, and not necessarily rely on just one type.

For reasons of both effectiveness and control and mitigation of liability issues (see ISO/TR 17427-8), applications are also likely to use a combination of *communication*s and on-board sensors, equipment and available on-board data, in order to provide robust *application service* provision (and are unlikely to rely on one *communication* media based solution for provision of any safety-critical *application service*).

Many emerging *C-ITS* applications will likely use a hybrid *communication*s approach, dynamically selecting different *communication* technologies for different types of content, or in different locations. Different *communication* technologies have different characteristics and attributes and are suited to different *communication* requirements. This section explains the hybrid *communication* approach and then explains the categories of *communication* technologies and some of their attributes, and how this affects the nature and type of 'core' systems support required to enable *C-ITS application service* provision in a connected vehicle-highway paradigm.

None of the available *communication* technologies can facilitate the full range of *communication* requirements. For example, time-critical safety warnings would usually require low-latency *communication*. Currently, the only *communication* technology that meets this latency requirement is 5,9 GHz [in some countries called 'Dedicated Short Range *Communication*' (DSRC)]. But it has very limited bandwidth. As E-UTRAN (4G/LTE) rolls out, where supported, it will provide an alternative for

all but very low-latency service requirements (such as collision avoidance and ramp access control). Many traveller information services require a long range *communication* connection and more bandwidth, and are better offered by cellular *communication* technologies, or broadcast. DSRC is less suitable for this type of application. Some messages, for example, a road works warning message, could be better sent via different *communication* technologies, where available. This also spreads the loading on any one wireless medium, which is particularly important in respect of the limited bandwidth at 5,9 GHz most suited for time-critical safety applications.

Another aspect of the need for hybrid *communication*s and the availability of bandwidth is the desirability for the *ITS-station* to be able to retain data it has downloaded. This reduces the frequency that downloads need to be repeated, and enables some data to be downloaded in less busy periods.

Even a single application, for example, an intersection collision avoidance application, is likely to have different *communication* flows with different *communication* requirements. Warning messages that involve vehicular control (collision avoidance, ramp access control, etc.) will need very low latency. The *communication* of detailed mapping data on the layout of the intersection may have less demanding latency requirements. The same application might also have other requirements for the download of new security certificates for the following week. This type of *communication* flow does not have any low-latency requirement, but it does require bandwidth. These *communication* flows, and probably others, might all be needed for this application to function optimally. A hybrid *communication* approach allows for a more efficient and more robust *C-ITS* because vehicles can choose the best available *communication* channel dynamically.

Which *communication* technology is selected by an application is obviously also subject to the local availability of the *communication* technologies and the minimal *communication* requirements. The ISO standard for *communication*s access for land mobiles (ISO 21217), provides the mechanism for this hybrid *communication* approach. The future availability and coverage of *communication* technologies throughout the network is currently hard to predict and will depend on the local conditions, the demand for *communication*, and allocation of frequencies.

The hybrid approach is also of significant importance because the optimum medium available may vary from one location to another.

VANETs, ad hoc networks (between vehicles), are most likely to use 5,9 GHz for the foreseeable future as a prime source of V2V *communication*. The role of E-UTRAN for V2V *communication*s is as yet unknown and unproven, but will in all probability also have an important role in the future for non-time-critical networking.

Table 1 shows the categories of *communication* technologies and their attributes.

Table 1 — Wireless communication technologies and attributes

Category	Communication technologies	Attributes
Short range *communications*	Examples include: — 5,9 GHz DSRC — Wireless LAN (e.g. WiFi) — Bluetooth — Infra-Red	— Short range — Low to very low latency — Two-way *communications* — Small data packets
Long range *communications*	Examples include: — Cellular networks, including — UMTS (3G) — LTE (4G) — Satellite	— Long range — Medium to low latency — Two-way *communications* — larger data packets
Wide area broadcast	Examples include: — Digital radio (e.g. DAB+) — Analogue radio	— Long range — Medium to high latency — One-way — Medium-size data packets

6.6.4 Short and medium range communication

Examples of short range *communication* technologies include 5,9 GHz (so called DSRC), Bluetooth and wireless LAN. 5,9 GHz *communication* technologies will generally communicate over distances of 250 m to less than 1 000 m, dependant on topology and atmospheric conditions. Bluetooth offers a range of up to 30 m to 100 m depending on the variant [40 m for Bluetooth 4 (Bluetooth LE)].

So called (and misnamed) Dedicated Short Range *Communications* (DSRC) is short-to-medium range wireless *communication* technology specifically designed for automotive use. It can be used for one-way and two-way *communication*. Currently, a version of DSRC is used for electronic toll collection in the 5,8 GHz band. Globally DSRC based *C-ITS* have been developed and tested extensively in pilots and early deployments, mainly in the 5,9 GHz band. It is technically quite different and more capable than the 5,8 GHz version of DSRC. It has the benefits of having low latency, high mobility and, currently, no *communication* connection charges. Limitations are the narrow bandwidth and limited coverage. Because DSRC is the only technology that can provide ad hoc short or mid-range low latency *communication*, it is required for service announcements and time-critical safety services in ad hoc networks, especially VANETs. However, 5,9 GHz DSRC *communication* is less suitable for *C-ITS services* needing wide area coverage and/or high bandwidth because the 5,9 GHz band is limited in capacity, easily saturated and expensive to deploy. Though it should be noted that, at the time of writing, there is international lobbying in the USA and Europe to open up the whole 5,9 GHz band, including those frequencies currently reserved for automotive safety applications, for general wireless broadband use. At the same time, US DoT NHTSA has announced a decision in principle to take next steps to require light vehicles to be equipped to be able to communicate using 5,9 GHz technology.

Bluetooth technology is a global wireless standard for the exchange of data over short distances using radio transmissions in the unlicensed 2,4 GHz to 2,485 GHz band. Bluetooth is available in many of the current mobile devices such as smartphones or car-kits. The *communication* range varies by Bluetooth specification, but typically effective ranges varies from a few metres to about 30 m (Bluetooth marketing 2011). Bluetooth is sometimes used for traffic monitoring.

A wireless local area network (LAN) links two or more devices using some wireless distribution method, and generally provides a connection to the Internet. This allows users to move around within a local coverage area and still be connected to the network and Internet. Many modern WLANs are based on IEEE 802.11a) to n) standards, marketed under the Wi-Fi brand name. (The basis of 5,9 GHz DSRC is actually another variant, 801.11p).

The range of a WLAN [802.11 a) to n)] network depends on the number of routers but is generally linked to a building and its direct surroundings. Wireless (802.11 a)-n) LANs are not suitable for 'fast' moving *C-ITS* devices, but it could be used for exchange of data in stationary situations; for example, the download of security certificates or for application data services at service stations.

6.6.5 Long range communication

For the purpose of this Technical Report, long range *communication*s are considered to include those media that enable 2-way, unique *communication* connections over many kilometres. Current long range *communication* technologies include cellular network and satellite *communication*. Cellular *communication*s networks offer apparent 'seamless' *communication* sessions across the cells of the network.

Cellular *communication* technologies such as UMTS/3G, LTE/4G and WiMAX/4G have the advantage of providing high bandwidth, wide coverage and high mobility. Disadvantages of UMTS/3G are the relatively high latency, and the required *communication* costs. LTE/4G has a much lower latency, and is comparable to that of DSRC.[13] It is as yet unclear to what extent time critical safety applications can use LTE. From a deployment point of view, it is an advantage that cellular *communication* infrastructure already has significant coverage, and offers cell-cell transfer of ongoing *communication* sessions.

Satellite *communication*s provide *communication* via an orbiting tele*communication*s satellite. Satellite *communication*s could be used in remote areas, for example, using digital radio technology. Satellite *communication*s can be used to broadcast data to *equipped vehicles* (3.14), and some systems can be used for bidirectional *communication*s, although the data latency is comparatively high. As with cellular *communication*, using satellite *communication* requires a subscription with a provider. An example of the current use of satellite *communication*s is an Australian implementation of its 'Intelligent Access Programme' application using satellite *communication* to cover areas where no cellular coverage is available.

NOTE Not all satellite *communication*s telephony options offer 24/7 coverage, and depend on the number and orbit of available satellites. Geostationary orbit based systems offer 24/7 coverage.

6.6.6 Wide area broadcast

For the purpose of this Technical Report, wide-area broadcast is considered to include one-way *communication* that involves messages to be broadcast over areas of many kilometres.

RDS-TMC is widely used to broadcast traffic information messages on conventional FM radio broadcasts. Traffic Message Channel (TMC) is a technology for delivering traffic and travel information to motor vehicle drivers. It is digitally coded, using the Radio Data System (RDS).

6.6.7 Positioning services

Global Navigation Satellite Systems (*GNSS*) refers to constellations of satellites that broadcast positioning, navigation and timing data that receivers on earth can receive and use for various applications. *GNSS* is offered by satellite navigation systems of USA (GPS), Russia (GLONASS), China (COMPASS), and Europe is in the process of rolling out its high precision GALILEO system (expected fully operational circa 2020).

A standalone *GNSS* receiver typically achieves a spatial accuracy of 10 m to 20 m. Increasingly, there is a trend towards using a multi-*GNSS* approach where other *GNSS* constellations (e.g. the Russian GLONASS) are used to supplement GPS. This approach can improve spatial accuracy and integrity, and has been demonstrated to achieve a spatial accuracy in the range 5 m to 10 m.

However, many safety-critical *C-ITS* applications emerging internationally require a spatial accuracy of less than 1 m, and also require high integrity, availability and timeliness. Standalone *GNSS* and multi-*GNSS* receivers cannot repeatedly achieve this, although multi-*GNSS* including GALILEO will come close to these accuracies.

International *C-ITS* developments are now often using wide-area augmented *GNSS*, where the positioning signals from a satellite constellation are augmented with correction signals, which are transmitted from satellites and/or ground stations. This is further supplemented by relative positioning

measurements from on-board vehicle sensors to achieve the stringent positioning requirements. As stated above, safety-critical systems are most likely to use multiple technologies in order to improve system robustness and reliability.

6.6.8 Digital road map data

There are a number of emerging *C-ITS applications* that will require highly accurate digital road map data, which will work together with *GNSS* positioning services and a vehicle's on board sensors to determine the position of a vehicle's position relative to attributes in the road environment. Examples of such emerging applications include intersection assistance, and some collision avoidance applications. (However, as such systems largely require a high percentage of *equipped vehicle*s, there is time-in-hand to address these issues)

The accuracy requirement for *C-ITS* safety applications can be classified into three levels:

— road: on which road the vehicle is placed (metre level)

— lane: which lane of a road the vehicle is in (sub-metre level)

— where-in-lane: where within the lane is the vehicle positioned. (decimetre level)

Emerging safety critical *C-ITS application*s will require high-accuracy digital map data down to lane level (sub-metre) or where-in-lane level (decimetre). The enhanced maps required to achieve this level of accuracy are often referred to as the fourth generation of digital mapping, or eMaps. These eMaps are still emerging internationally, and much development is still required both in terms of standards and with the data supply chain to support them.

Commercial map data companies currently capture and supply digital road map data for use in automotive applications, primarily for navigation and other location services. These companies are progressively improving their coverage, spatial accuracy and timeliness of the road data they supply.

Further to this, government land and transport agencies are the authoritative source for a number of road safety attributes (e.g. speed zone data). This data are not always made accessible to the commercial map data companies that provide data to the end-user applications, and does not always meet the requirements for *C-ITS*. Thus, there are a number of changes that will need to be made locally if the map data requirements of emerging *C-ITS* are to be met.

It is always essential to remember that *C-ITS* is not an end objective in itself, but is a means of achieving *application service* delivery.

In order to understand the role, and therefore the concept of operations of a *C-ITS core system*, it is also necessary to consider the architecture of its *actors* and its *communication*s.

6.7 Actors involved in C-ITS service provision

ISO 17427-1 contains a more detailed characterization of the 'roles and responsibilities' of the *'actors'* engaged in *C-ITS service* provision and receipt/use.

We can visualize the *C-ITS* paradigm as it is shown in Figure 4, which is an update and enhancement of a figure used in the CVIS project, and the authors acknowledge that work in the development of this Technical Report, and advise that the same figure is now also used in ISO 21217, (2013).

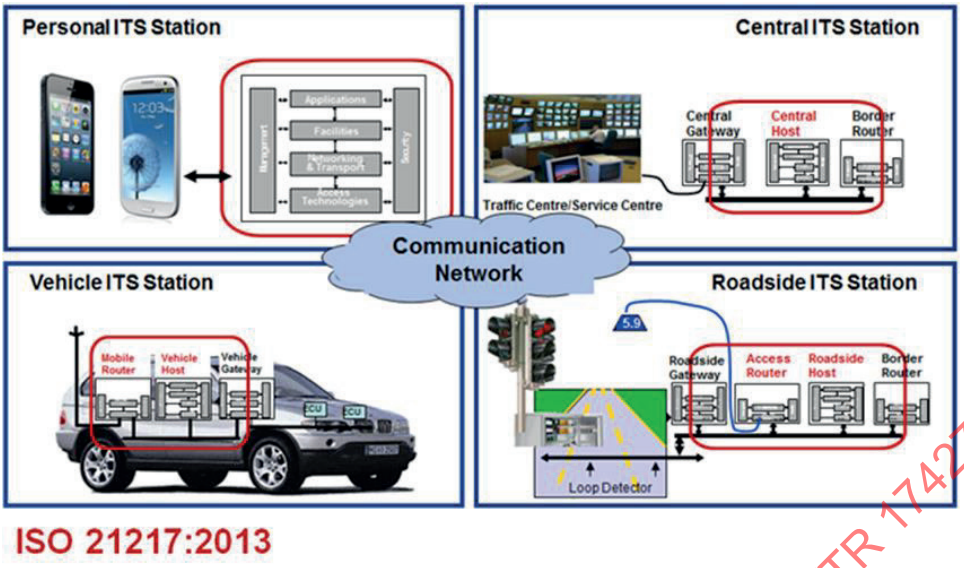

Figure 4 — High level C-ITS connectivity paradigm

In order to achieve *C-ITS service* provision, a combination of applications and systems are necessary to deliver the services that will realize safety, mobility and/or environmental benefits through the exchange of data between mobile and fixed transport system users. The principal system components are therefore:

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

— **Equipped vehicles**– (mobile *ITS-stations*) vehicles equipped with the *communications* and data collection and processing capacity to perform in the *C-ITS* context;

— **Equipped persons** – (personal *ITS-stations*, personal mobile *ITS-stations*) persons with mobile phones, tablets or similar devices having *communications* and data collection and processing capacity to perform in the *C-ITS* context;

— **Mobility assistance** – (mobility assistance *ITS-stations*) equipment/systems to assist vulnerable road users (for example, sight impairment, hearing impairment, physical mobility impairment) who may be assisted by specially designed 'apps' that enable the user to better cope with their disability, and/or provide a safer travelling environment for the user especially by raising awareness of other road users. More advanced 'apps' may provide prioritization at road crossings and other assistances, or provide collision avoidance capabilities, etc. either as devices tailored to meet the special requirement, such as glasses, wheelchairs, etc., which may be equipped with *ITS-station* capabilities, or as specialized 'apps' on a smartphone;

— **Intermodal connection/display** – likely to largely be Internet based or *wireline* connections to an *application service* provider, then *ITS-station* or wireless Internet provision between the *application service* provider and personal *end user* of the *application service*. In other circumstances, they may simply be broadcast data interpreted by an 'app' on-board the device containing an *ITS-station*, usually, but not necessarily, a personal *communication* device such as a smartphone, or mobility assistance device;

— **Communications**– that facilitate data exchange between *ITS-stations*, including roadside *ITS-stations* where appropriate;

— **Core systems**– which provide the functionality needed to enable data exchange between and among mobile and fixed transport system users;

— **Static roadside equipment** – to provide *ITS-station communications* between mobile/personal/mobility users and/or the infrastructure/*CorSys* and connect with other 'Field' equipment;

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

See ISO 17427-1 contains an in depth analysis of the roles and responsibilities in *C-ITS*. Figure 5, from ISO 17427-1, provides an overview, in which it can be seen that *communications* take place in different security environments. ISO 17427-1 contains further details.

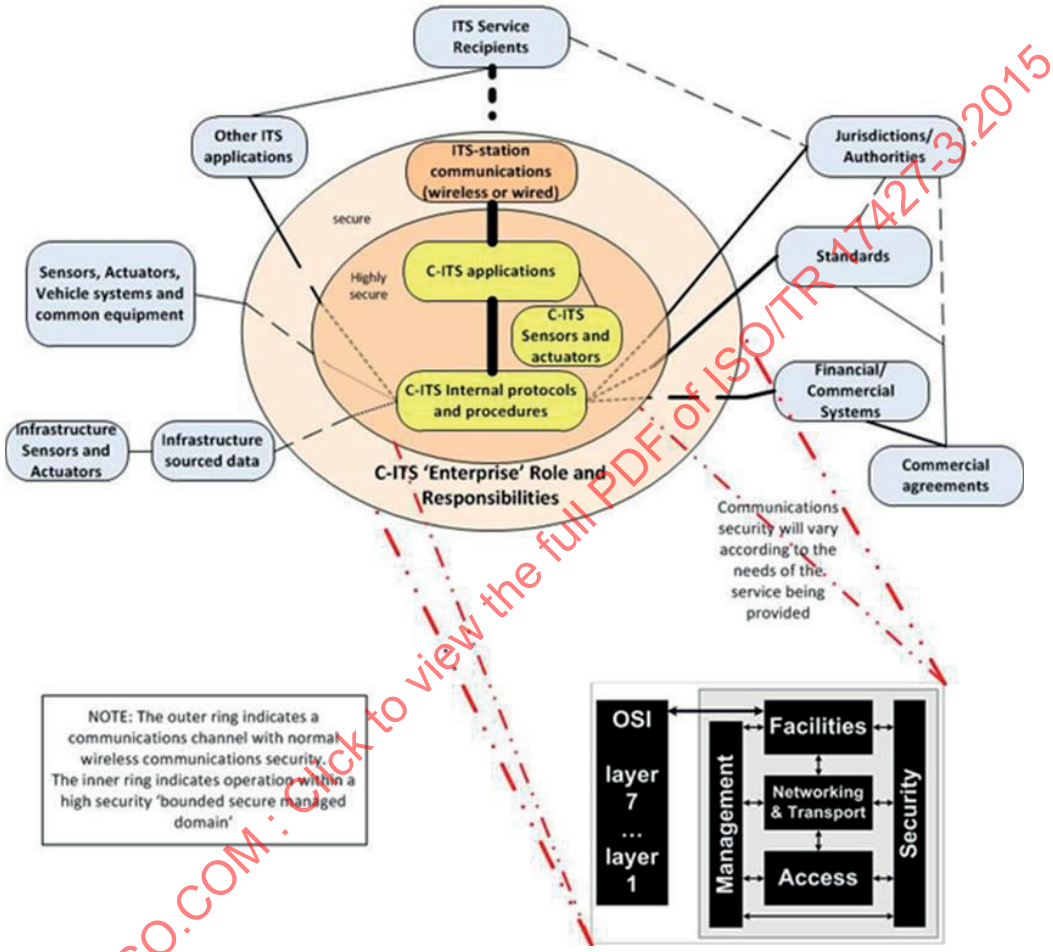

Figure 5 — 'External' and 'Internal' enterprise objects in a C-ITS Community

NOTE Standards are included in Figure 5 because they enable meaningful *communications* and comprehension of messages and data.

The provision of the essential 'enabling' services are known as *CorSys*, and are the subject of this Concept of operations.

CorSys are an essential component in the case of the provision of some *C-ITS services* (for example, intelligent ramp access to highways, level (grade) crossing management, etc.), where it is essential that data can be provided securely and speedily. *CorSys* can provide also more capable and comprehensive provision of some other *C-ITS* assisted services (for example 'ice', 'obstacle' and other road condition alerts).

Figure 5 therefore shows the context for which a "Concept of operations" for such *CorSys* is required.

In terms of *communications* sessions across wireless *communications*, it is important to understand that most *actors* in *C-ITS* implementation communicate wirelessly (over whatever wireless medium is available) in the same way, in a peer-to-peer *communication* dialogue (see ISO 21217).

NOTE In some instances, existing *wireline* links are used, e.g. roadside to *centre*/*centre* to *centre,* etc.

6.8 C-ITS enabling data

In respect of enabling *C-ITS*, vehicle ad hoc networks (VANETs) require the support of a *core system* to provide the aspects that are not directly related to the application data but are essential to enable the service provision to take place safely, reliably and successfully. These services may generally be categorised as: user permissions management, user trust management, data distribution, misbehaviour management, network services, service monitoring, time synchronisation.

These may be described as '*core system* support services and are based on the exchange of relevant data.

These data messages that will be transmitted and received by *C-ITS* devices are planned to be aligned with international *C-ITS* message set standards. However, at the time of writing this 'Concept of operations', there is still debate regarding the exact content and frequency of such messages. To consider the basic requirements for the provision of 'core' services, it is not necessary to wait until the exact content and frequency of such data are finally agreed internationally. At this level of abstraction, it is adequate to understand that provision has to be made to handle data of these types. But in order to comprehend the general required tasks, it is perhaps useful to summarize the main contenders at the time of developing this deliverable. The following primary message types are examples of likely 'core' messages, and are likely to include all or some of the following, or some internationally agreed variant thereof:

— BSM: basic safety message

One of three messages outlined in SAE J2735, the others being the roadside alert (RSA) message (BSM) and probe vehicle message (PVM). The BSM message is used to communicate safety messages from vehicles to vehicles and infrastructure (e.g. V2V and V2I), and from infrastructure to vehicles (I2V). BSM is the US equivalent of the CAM and DENM message. The EU-US harmonization task force currently works on harmonizing the BSM with the CAM and DENM message sets.

— CAM: cooperative awareness message

The CAM message is a periodically transmitted message containing transient data on the vehicle status. The CAM message is designed primarily for *communication* from vehicles to vehicles and infrastructure (e.g. V2V and V2I), but may also be sent from infrastructure to vehicles (I2V). The CAM message is defined by the ETSI/TS 102 637-2.

— DENM: decentralised environmental notification message

A DENM messages is an event triggered message which is generated upon detecting an event and containing information about the event. DENM messages are typically relevant for a defined geographic area. The DENM is sent from vehicles to vehicles (V2V), vehicles to infrastructure (V2I), and from infrastructure to vehicles (I2V). DENM is defined by the ETSI/TS 102 637-3.

— RSA: roadside alert message

One of three messages outlined in SAE J2735, the others being a basic safety message (BSM) and a probe vehicle message (PVM). The RSA message is used to communicate traveller information applications from roadside infrastructure.

— PVM: probe vehicle message

One of three messages outlined in SAE J2735. The PVM message is used to communicate probe information obtained from the vehicle to roadside infrastructure.

— PVD: probe vehicle data

PVD is used to communicate the status of a vehicle to the roadside *ITS-station* to allow the collection of information about vehicle movements along a segment of road. The PVD message will be defined by CEN and ISO standards.

— PDM: probe data management

PDM is used to control the type of data collected and sent by the vehicle to the roadside *ITS-station*. PDM is sent from the roadside *ITS-station* to the vehicle. PDM message will be defined by CEN and ISO standards.

— Map: geometric intersection description

A message containing geometric details of the road such that the vehicle can cross-reference information contained in other messages sent from the roadside *ITS-station* against the map message to determine how to apply the message (e.g. determine if the message applies to the lane the vehicle is currently in).

— SPaT: signal phasing and timing

A SPaT message contains information about the signal phasing and timing including current phase and time remaining so that it can be used by a vehicle to provide warnings about potential red light violations or advice on optimal speed. The SPaT message is sent from a roadside *ITS-station* integrated with a traffic signal.

— SRM: signal request message

SRM is sent by a vehicle to a roadside *ITS-station* at a signalised intersection [or *central system* (3.7)]. It is used for either a priority signal request or a pre-emption signal request depending on the way the message flag is set. In either case, the vehicle identifies itself, its current speed, heading and location, and makes a specific request for service, as well as an anticipated time of service.

— SSM: signal status message

SSM is sent by a roadside *ITS-station* at a signalised intersection (or *central system*). It is used to relate the current signal status of the signal and any collection of pending or active pre-emption or priority events acknowledged by the controller. The data contained in this message allows other users to determine their 'ranking' for any request they have made.

— IVI: in-vehicle information

The in-vehicle information (IVI) data structures specifies the data required to be transmitted between *ITS-station*s (I2V) in order to deliver in-vehicle signage associated with various *ITS service*s (e.g. contextual speed, roadwork warning, vehicle restrictions, lane restrictions, road hazard warning and re-routing). The information will be specified in terms such as content/data elements and data structures. A technical standard is being developed that will specify a general data structure that is future proof, extensible and *communication*s agnostic.

— TPEG: Transport Protocol Expert Group

TPEG produced a set of specifications addressing the transmission of language independent multi-modal traffic and travel information. They are standardised through CEN and ISO and consisting of the following applications:

— RTM - Road Traffic Message

— PTI - Public Transport Information

— Loc - Location referencing, used in conjunction with applications

Other applications are under development including parking information, congestion and travel time and weather information for travellers.

6.9 Cooperative ITS applications and services

The emerging cooperative intelligent transport paradigm will provide a platform on which service providers can use their initiative to develop and deploy a wide range of applications services. While it may be difficult to predict the full range of applications that we may see in future, it is possible to categorize the types of applications that are currently under development.

A typical categorization is by policy impact area, distinguishing safety, traffic efficiency and environmental impacts. However, there are several ways to categorise *C-ITS applications* and services, for example, by the following:

— policy impact area : traffic safety, traffic efficiency or environmental impacts

— *communication* latency requirements : time critically or non-time critical, or the possible value range in ISO/TS 17423 on *ITS application* requirement for selection of *communication* profiles (smaller than 1 ms, 10 ms, 1 s, 10 s, 1 min, 10 min or 1 h)

— positioning : accuracy requirements

— safety-of-life and property risk : safety critical and non-safety critical

— level of guidance : informing, warning or automated

— driving task : strategic driving tasks (navigation, trip planning), tactical driving tasks (lane choice, speed choice) or operational driving tasks (steering, braking).

— type of user : fleet management, traffic management or consumer market applications

A common categorization used by ERTICO and other stakeholders is based on the applications' influence on the driving task. These categories include the following:

— Information – e.g. travel time services

— Awareness – e.g. road works warning

— Assistance – e.g. intelligent speed adaptation

— Warning – e.g. collision warning

— Avoidance – e.g. electronic break assist

— Automated – e.g. cooperative adaptive cruise control

Figure 6 shows a modified version of a diagram from ERTICO, which plots these application categories on a graph based on their latency and spatial accuracy requirements. While this is a useful representation, it is noted that there may be some types of application that do not fit neatly in this categorization.

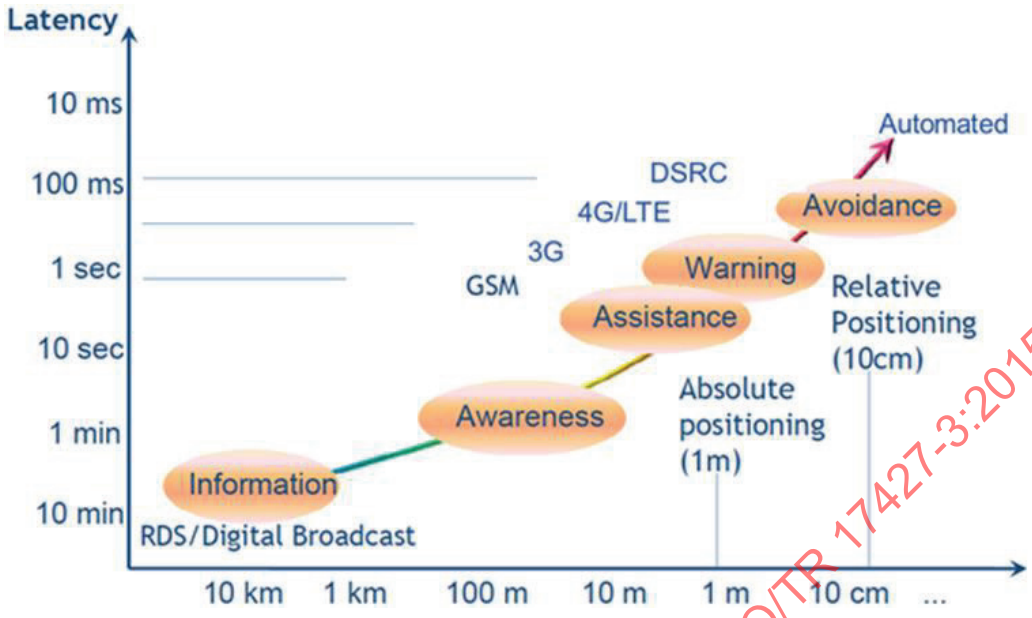

Figure 6 — Types of C-ITS by latency and spatial accuracy
[Source: Modified from ERTICO 2011]

6.9.1 System of systems

The *C-ITS* paradigm comprises a dynamic, distributed computing environment with computing units in vehicles, roadside infrastructure, mobile devices and *central systems*. *C-ITS* can be described as a 'system of interoperable systems'.

6.10 C-ITS Privacy and anonymity

6.10.1 Privacy overview

The core functionality described in this subsection is specifically to enable an appropriate level of privacy assurance.

Due to much of the data within the emerging *C-ITS* domain having the potential to be linked to an individual, the issue of privacy is a real concern that will need to be appropriately addressed. Where required, elements of the *C-ITS* will need to demonstrate compliance with the relevant Privacy Acts, Surveillance Acts and privacy principles, at international, regional, national and state level.

Privacy is a sensitive issue for *C-ITS* implementation because *C-ITS* stations and applications have the capability to collate data in a way that can compromise the privacy of *end user*s. Significant privacy regulations are now in place around the world. See ISO 12859. ISO/TR 17427-7 has been developed to examine these issues in greater detail in specific respect of *C-ITS* aspects.

*End user*s are rightly concerned to protect their privacy and there will be user resistance to *C-ITS* unless *C-ITS*s adequately protect *end user* privacy. On the other hand, experience with the use of mobile phones has shown that *end user*s are often prepared to trade off their privacy for service benefits.

C-ITS service provision needs to being planned to provide privacy, and where practicable, anonymity, and this applies particularly to the *CorSys* where the collation and storage of data could be a significant threat to privacy if not properly implemented. However, where an *end user* knowingly trades off privacy for service provision that would not otherwise be possible, the *C-ITS service*, and the *CorSys*, should not prevent this. These possibilities are already available on the market today and the levels of anonymity and privacy inherent to these systems are typically governed by agreements between *communication*/service providers and consumers. So while privacy is not compromised for an individual, what happens between that individual and their *communication*/service provider (e.g. 3G

service provider, Sat/Nav route guidance provider) may well consensually compromise privacy. Some application providers may require personal information in order to function. In these circumstances, this needs to require the user of the application to opt-in to use that application in advance of provision of the service.

Nevertheless, *C-ITS service* provision should make every reasonable effort to preserve privacy, and where practicable, anonymity, and the data protection regulations and recommendations of the *jurisdiction* need to be respected and applied. Every measure should be taken to prevent the careless or accidental compromise of privacy, and current EU regulation describes this as 'privacy by design'.

Privacy-by-design is an approach to systems engineering which takes privacy into account throughout the whole engineering process. This includes building privacy protection into the information and *communication*s technologies, the business processes, and the physical systems, this includes anonymisation of data at the earliest practicable stage.

*C-ITS*s need to normally plan anonymity into the trusted exchange of data wherever possible, using the *jurisdiction*s existing privacy principles as guidelines, and then balancing privacy against security and safety. Privacy of participants is paramount, except where safety of life is at risk. Anonymity is a preferred route, but privacy is not necessarily exclusively obtained through anonymous *communication*, and other data protection methods need to be employed if the provision of anonymity is impracticable or not commercially viable.

The general aspects to be covered in greater detail in ISO 17427-7 include the following:

— personal data should not be retained longer than is necessary to accomplish the data transport or transmission;

— maintaining the security of personal information;

— protecting confidentiality of personal information against improper access;

— assuring the quality and integrity of personal information collected or maintained;

— personal information subjects should be kept aware and informed about:

  — the nature and extent of personal information collected from them,

  — the purposes for which such personal information is collected,

  — the uses of personal information made by personal information users, and

  — the opportunity not to provide personal information;

— the protections for confidentiality, integrity, and quality of personal information;

— the consequences of providing or withholding personal information;

— opportunities to remain anonymous;

— rights of recourse and redress for misuse of personal information.

6.10.2 Data messages and privacy

As summarized in 6.8, there will be a wide range of standardised data messages that will be transmitted and received within the *C-ITS* domain. Many of these standardised messages will contain data attributes that could potentially be used to identify an individual. For example, the standard basic safety message that is proposed to be transmitted by *C-ITS equipped vehicle*s up to 10 times per second will likely contain a unique ID number, a unique MAC number, a unique security certificate code, and potentially a subscription code depending on the services to which the vehicle owner has subscribed. Further to this, the messages will include location and time data that could be used to identify where an individual has been.

Personally identifiable information includes not just data that contains data that could reasonably identify an individual, but also data that could reasonably be joined with other readily accessible data to then identify an individual.

While the final design of how data messages will be handled and the security processes around them have not yet been finalised internationally, there are a number of concepts that have been developed and trialled that are intended to address privacy concerns with the data messages. These include the following:

— the PKI approach using short-term pseudonym certificates;

— the unique ID being a rolling ID that changes over time;

— data messages captured by another *ITS-station* only being maintained for as long as it is still serving its intended purpose;

— consent or opt-in being required from vehicle owners for those authorities and service providers that wish to capture historic data from vehicles to use for various purposes.

The main enabler of privacy is the PKI approach using short-term pseudonymity certificates. Similar to a rolling ID, frequently changing pseudonym certificates ensure that outsiders cannot monitor a device for a period longer than the period that the short-term pseudonym certificate is used. This period has not been determined but initial plans suggest between 5 min and a week (Schulman 2012). The other reason why a PKI ensures privacy is that the PKI separates registration and certificate issuing in different authorities and different systems. This means that no single authority will be able to link personal data with the constantly changing ID and certificates.

Clearly, such privacy provision requires the provision of central 'core' services.

6.10.3 Security

Any implementation that uses *C-ITS* needs to be designed with security in mind. It is important to understand that security issues are not the same as privacy issues. In designing a system, thought needs to be given as to how the system can be protected against compromise by criminals and what mechanisms need to be integrated into the system to protect it from such vulnerabilities. A *C-ITS application* faces many of the same risks as any other online wireless Internet-based application, but with additional risk to life and limb.

6.10.4 Data management (including capture, storage and access)

A significant amount of data will be created by *C-ITS*. With data being created and potentially accessible from a large range of road users, much of which previously did not exist or was not accessible, the resultant scenario could be described as *big data*. The term 'big data' refers to a collection of data that is so large and complex that it becomes very difficult for traditional relational database tools to be of much use.

While the creation of more data may appear to provide significant opportunities for service providers and authorities to create value-added services and improved outcomes, there are potential privacy concerns that will need to be considered with the management of this data.

Depending on the *jurisdiction*, there will be a relevant 'surveillance' regulation or 'data privacy' regulation which will restrict what data can be collected, particularly if it has the potential to identify and track an individual's location. Further to this, relevant privacy legislation and privacy principles may then restrict what any captured data can be used for.

See ISO/TR 17427-7 for further discussion of privacy issues.

7 'Core' systems

7.1 Core system overview

7.1.1 General

NOTE 1 Much of the *CorSys* conceptual context description has been obtained from various documents generated and publicised by US DoT RITA, especially 'CoreSystem*ConOps*RevE2', and the ARRB draft document "Austroads Report: *Cooperative ITS* (Stage 2b): Concept of operations for *C-ITS* core functions – Draft Report", also 'Cooperative ITS Regulatory Policy Issues', National Transport Commission, Australia, and these sources are acknowledged and thanks expressed for the contribution.

NOTE 2 Accommodation of International Architectures: The US "Connected Vehicle Reference Implementation Architecture" (CVRIA) and "The Framework Architecture Made for Europe" (FRAME) (recently updated to include *Cooperative ITS*s) are accommodated in the user needs discussed in this *ConOps*. The '*Communication*s, Air-interface, Long and Medium range' (CALM) set of standards referred to in 6 above, which define a set of system interactions for the wireless vehicular environment, are also covered by the user needs captured in this *ConOps*.

CorSys for *C-ITS* envision the combination of the applications, services and systems necessary to provide the safety, mobility and environmental benefits through the exchange of data between mobile and fixed transport system users. A subset of the components listed in 6.2, they consist 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 transport system users, and

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

6.1 describes the different modes of *C-ITS*. While some of those modes are autonomous, many require, or will be improved by, the presence of a central *CorSys*.

The main mission of the *CorSys* system is to enable safety, mobility and environmental *communications*-based applications for both mobile and non-mobile users. The scope of the *CorSys* includes those enabling technologies and services that will provide the foundation for application transactions but not the provision of the *application services* themselves.

Jurisdictions/*centres* may of course provide *application services* to users, but these application services should not be considered part of the *CorSys* and should be specified and managed separately from the *CorSys* (even where the same operator provides both).

The system boundary for the *CorSys* 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 *CorSys* users.

It is important to understand that a *CorSys* is not a fixed entity, neither in the way it is instantiated, nor in the number and scope of the *C-ITS service*s that it supports. It will be instantiated in different ways by different *jurisdictions*/operators, and, most importantly, it will evolve over time. Cooperation and coordination between *jurisdictions*, and between *jurisdictions* and operators will avoid wasting time and money in duplicated services implemented in slightly different ways

One does not define a television service by the title or content of particular programmes. To use a closer analogy; in system architecture we often use the term *'actor'* (3.1) to describe the participants in the system. If we borrow the analogy from our thespian friends, a good film or television series is characterized not by the plot of any one episode, but by the relationships and behaviour of and between the principal *actors* within the framework that the series is set. We do not define our 'smartphone' by

the particular 'apps' that it supports on the day we purchased it, but by its ability to load and support 'apps'. So it is with *C-ITS*, and, particularly, the capability and behaviour of its *CorSys*.

In Clause 8, a number of application 'use cases' are described and within this high-level *ConOps*, the use cases are described texturally with the support of high-level figures. A deployment version of a *C-ITS ConOps* will need to define them further with an architecture and context diagrams that itemise and characterize the outputs that are produced. Activity diagrams and recognized and standardised elaboration are recommended to support and characterize the use cases and describe the interactions between system users, *CorSys* personnel and *CorSys* subsystems.

But the list of use cases described in Clause 8 are examples, albeit of key elements of a *C-ITS CorSys*. They do not comprise the total extent of the system, and more will be added (and need to be characterized) over time. The extent of any instantiation of a *ConOps* for a '*C-ITS CorSys* will therefore vary between *jurisdiction*s according to the scope and content of the services being provided, and, importantly, will be a 'living' document, that will need to be revised as the system evolves, and new use cases will need to be characterized and their behaviour and management by the *CorSys* characterized and codified as they evolve.

Additionally, the *CorSys* works in conjunction with external *support systems* (3.24) such as the 'Certificate Authorities' security of wireless *communication*s (e.g. as defined in IEEE Standard 1609.2 with respect to 5,9 GHz systems). A critical factor driving the conceptual view of the entire cooperative vehicle and highway systems environment is the level of trustworthiness between communicating parties. While the *CorSys* is being planned for privacy and, where practicable, anonymity, it is also providing a foundation from which to leverage alternative *communication*s methods for non-safety applications.

The primary function of the *CorSys* is the facilitation of *communication*s, and exchange and processing of information between system users, and some of the *communication*s may also be secure (*bounded secure managed domain* (3.5)). The *CorSys* may also provide data distribution and network support services depending on the needs of the *CorSys* deployment. The *CorSys* provides the functionality required to support safety, mobility, and environmental applications. This same functionality may also enable commercial applications but that is not a driving factor for the development of the *CorSys*.

7.1.2 Single core systems

Within some *jurisdiction*s, it is envisaged that a single administration operated *CorSys* can cover the whole area of its domain in respect of *C-ITS service* provision, and there may be significant simplification and efficiency benefits in this route where it is practicable.

7.1.3 Multiple core systems

It is possible that within some geographical areas, several *CorSys* may operate. For example, there may be a regional implementation covering the whole *jurisdiction*, and metropolitan districts within the *jurisdiction* may also operate a *core system*. In some *jurisdiction*s, it is expected that State administrations, rather than a single National administration, will separately operate *CorSys* (or in the case of the EU, Member states within the Union). In some cases, commercial competition between *CorSys* providers may also be allowed. In all of these cases, there is an added layer of complexity because it is essential that *CorSys* interact and interoperate, and that there is consistency in the operation of different *CorSys*. See 7.5.9.

7.1.4 Other 'Central' systems

The *CorSys* works in conjunction with field equipment for certification across wireless media, (such as the 'Certificate Authority' for 5,9 GHz security, as defined in IEEE Standard 1609.2 and ETSI 102 94x series of standards deliverables).

The *CorSys* works in conjunction with field equipment systems. These may often be operated by the same '*centre*' near or along the transport network which perform surveillance (e.g. traffic detectors, cameras), traffic control (e.g. signal controllers), information provision (e.g. VMS) and local transaction (e.g. tolling, parking) functions and also include RSE supporting wireless *communication*s infrastructure

(probably including 5,9 GHz at 'hot-spots), that provide *communication*s between mobile entities and fixed infrastructure. Typically, their operation is governed by transport management functions running in *back office*s/management *centre*s. But they work with and are not part of the *CorSys*.

7.1.5 Facilitate a platform for sharing of information and efficient use of resources

An essential attribute of *Cooperative-ITS* is that information is shared between both applications in a single *C-ITS* equipped device (*C-ITS* station) and applications running in different *C-ITS* devices.

Cooperative-ITS have, amongst others, the following features:

— the sharing of information between any *C-ITS* device (vehicle, roadside, central and mobile);

— the sharing of information between applications in a single *C-ITS* device;

— the sharing of resources (*communication*, positioning, security,...) by applications in a *C-ITS* device.

The objectives of this function are to better realize the *C-ITS service* in a more efficient way. The sharing of information requires several functions including *communication*, prioritization, and authorization. Not all of these functions are core functions. The core functions are the functions that require coordination between different system components, using a central resource. The main function is a publish-subscribe function with a central registration of which devices subscribe to which enables more efficient targeted *communication*.

7.2 Justification for 'Core Systems'

This subclause provides a rationale for the need to provide *core system* support that will enable the emerging cooperative intelligent transport paradigm to be progressively deployed. It details the vision and objectives, the nature of these changes, and considers constraints and assumptions.

7.2.1 Vision, drivers and objectives

The following two approaches can be taken to *C-ITS*.

— an ad hoc, vehicle led approach;

— a *core system* supported approach.

In the ad hoc approach, the implementation of *Co-operative ITS* is left to the market place, and initial systems are a mixture of vehicle-to-vehicle VANET-based systems and cellular network vehicle-to-vehicle *communication*s often via a commercial service provider or commercial service provider based (e.g. SatNavsystems providing traffic and congestion information).

For the *jurisdiction*(s) in which *C-ITS* is being implemented, the short-term advantage of this approach is that it requires no investment by the *jurisdiction*. However, if take-up of commercially based emergency call systems provides a yardstick, take-up will be slow and centred around upper market 'elite' vehicles. Mass exploitation of the benefits, particularly safety-of-life benefits, of *C-ITS* will probably never be achieved. The significant benefits of widespread implementation are unlikely to happen in the foreseeable future and many benefits of the sharing and reuse of data will not occur. Many of the key safety services will be difficult to operate, and the safety of life benefits will simply not accrue in the same scale. Issues about certification will be approached by commercial 'silo' solutions and so interoperability will be a significant problem.

The second approach is for the *jurisdiction* to provide some limited and controlled support for central 'core' services to enable *C-ITS* to achieve its core objectives. *Jurisdiction*s may well consider also providing some of the important *application services*, but these are not considered here.

Using this strategy, investment in providing the essential *core system* services to support a transport system that utilizes *C-ITS* through a nationally harmonized platform, will enable and provide a safer, more productive, efficient, cost effective, and environmentally friendly road-based transport system,

and will enable enhanced road user and road operator services and information. Particularly, it will enable the faster roll-out of safety of life and safety critical services and provide a more stable basis for interoperability and reuse of data.

7.2.2 Key strategic objectives for the deployment of core system support

The key objectives for the deployment of *Core system* support are the following:

— Improved road safety – Road crashes cause many thousand road deaths and millions of injuries every year. Most countries are committed to halving road deaths each decade. The easy savings have already been made. This scale of saving can only be achieved if the benefits of *C-ITS* are enabled. Accidents, their direct costs and indirect costs of congestion and associated costs represent a significant burden, so apart from the humane reasons for improving safety of life and injury mitigation, there is a strong financial case to reduce this burden. The single most effective means to achieve these savings are by the provision of 'core' service support.

— Increased transport efficiency and productivity – The avoidable cost of traffic congestion is many billions of whatever currency unit you choose to count in, in every country, in every year. Congestion also has a social cost, as it impacts on people and their social activities. *C-ITS* will enable in-vehicle applications and adaptive traffic management systems that could deliver improved efficiency and productivity to the road transport system.

— Reduced environmental impacts – Transport is a significant contributor to greenhouse gas emissions, accounting for approximately 16 % of total emissions, of which road transport makes up over 85 %. *C-ITS* technologies have been shown to improve traffic and vehicle efficiency, thus reducing fuel use and emissions.

7.2.3 Key technical objectives for the deployment of core system support

— Agreed governance or management arrangements to ensure integrity/trust of message and for issuing security certificates;

— Secure exchange of data between users and applications;

— Consistent mechanisms to authorize sending/receiving messages;

— Assurance of privacy between users and from third parties;

— Agreed approaches for *C-ITS* privacy and agreed 'privacy-by-design' approaches;

— Workable arrangements for probe data;

— Provide initial (certification) or ongoing (audit) compliance with standards for both devices and services;

— Enabling critical safety applications such as intersection safety applications that would not be possible without core functions in the foreseeable future.

Table 2 — C-ITS capabilities with and without the identified core functions

Capabilities of fully market driven C-ITS deployment (no core)	C-ITS capabilities with core functions
— Separate agreements to access data from organizations — Applications navigate to organizations individually to find accessible data—slow — Island solutions – no easy data exchange — Gains still possible but some capabilities and functionalities will remain out of reach	— Can request any data without having a relationship to the data provider – no need for existing contracts or agreements — Data are readily accessible and trusted from multiple sources; rapid access in real-time; and of consistent format/quality
Source: Federal Highway Administration (2012).	

7.2.4 Principal elements of a core system

To summarize, this *ConOps* description is intended as a user-oriented document describing characteristics of a to-be-delivered system from viewpoint of the user. The roles and responsibilities of the *actors* in the system are defined in ISO 17427-1, and the overall summary of the framework and overview for *C-ITS* are described in ISO 17427-2.

The main mission of the *CorSys* is to enable safety, mobility and environmental *communications*-based applications for both mobile and non-mobile users. The scope of the *CorSys* includes those enabling technologies and services that will in turn provide the foundation for applications.

The function of the *CorSys* is to support the operational functionality of *C-ITS service* provision within a given geographical, *jurisdictional* or service area. It is therefore supporting all of the *actors* described in 6.2. It does this via one or more control/service *centres*.

The system boundary for the *CorSys* 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 users of the *CorSys*.

The *CorSys* supports a distributed, diverse set of applications. These applications use both wireless and *wireline communications* to provide the following:

— wireless *communications* with and between mobile elements including vehicles (of all types), pedestrians, cyclists, and other transport system users;

— wireless *communications* between mobile elements and field infrastructure;

— wireless and *wireline communications* between mobile elements, field infrastructure, and *back office/centres*.

The Control/Service *centre*(s) of a *CorSys* will support the following:

— central host management;

— *core system* gateway(s);

— *ITS-s border router(s)* (3.20);

— *home agent* (3.16).

See ISO 17427-2 for description of these features, and ISO 17427-1 will provide descriptions of their roles and responsibilities.

7.2.5 Proposed features of C-ITS core systems

7.2.5.1 Increased communications options

Support for a variety of *communication*s options for mobile users, including 5,9 GHz, cellular, wireless mobile broadband/Wi-Fi, etc. provides flexibility and increased performance over the entire *communication*s layer. Allowing cellular/broadband access to core services frees up dedicated 5,9 GHz bandwidth to focus more on time-critical safety applications. By providing multiple *communication*s options, as well as improving the success for time-critical safety applications, there is also greater probability that non time-critical applications will also have better access to the *communication*s resources they require in order to provide benefits. This strategy also enables *C-ITS* functionality without the specific requirement for the presence of, and investment in, a dedicated wireless *communication* installation and its infrastructure.

7.2.5.2 Light infrastructure deployments

Older conceptions for *CorSys* started with the offering, management, and control of a specific *communication* medium, and defining and managing the services that could be offered across that medium. In those conceptions, the key aspects of a *CorSys*, in respect of roles, responsibilities, operational concepts and client system support, were therefore driven, and largely a by-product of, the limitations of the selected *communication*s medium. This thinking was understandable as it was the possibility of a new low latency wireless *communications* channel that opened up the possibilities for the concept of *C-ITS service* provision. However, with hindsight, it was operational concepts, roles and responsibilities being driven by, and limited by, a single technology solution, rather than by the objective needs of the client system.

To use an analogy, it was rather like designing the highway system around the design and limitations of the Model 'T' Ford. Although the Model 'T' was the most significant automotive invention, the highway system was not built around its limitations. But the full success of the Model 'T' was made possible by the development of the highway system. The analogy of the chicken and the egg comes to mind.

In both system architecture and engineering, good design should always start with the client system need, not with the technology solution.

By focusing the *CorSys* as an enabler of service provision (and removing its responsibility for operating and maintaining a *communication*s network), it is possible to deploy Core services without an extensive network of RSEs. This enables deployments of *CorSys* independent of the time or other resources required to establish significant field infrastructure, allowing some operational benefits in a shorter time. For example, a *CorSys* could be deployed to distribute certificates, thereby facilitating trust and enabling V2V safety applications between *equipped vehicle*s. Meanwhile, deployment of RSEs with V2I safety applications at key intersections can proceed at its own pace, without being constrained by the need to provide *all* services in the *C-ITS* vehicle-highway environment. There is still the question on how to effectively distribute large numbers of certificates. The certificate management scheme has not yet been architected, and the suitability of cellular and Wi-Fi *communication*s for the distribution of large numbers of certificates is a topic for further study.

7.2.5.3 Publish-subscribe data distribution

Publish-subscribe offers those deploying an efficient way to distribute data that could not be easily achieved otherwise. Including this functionality in the *CorSys* ensures that it is constrained by the relevant privacy policies and may provide users more faith that their data are being handled in a way they are comfortable with. Further, broadening publish-subscribe beyond probe data offers application developers more options with regard to reaching their *end user*s.

7.2.5.4 Open standards

Open standards offer the promise of high reliability with a technology refresh advantage. This also provides an open market place for application development and integration, which should yield a rich, broad suite of applications from a variety of providers.

Scalable, Deployable Certificate Management: Certificate management is the basis for establishing and maintaining trust and enabling encrypted data exchange. Viewing the *CorSys* as a set of services that can be implemented independent of a specific box of hardware provides the foundation for a scalable system design. Architectural design will have to pass the scalability test, particularly in regard to the structure of the ESS that supports IEEE 1609.2 certificate management, but by considering scalability and certificate distribution issues now, the foundation has been laid for a deployable, scalable certificate management system.

7.2.5.5 Physical environment mitigation

The ability to maintain systems, delivering high-availability services, is crucial to the user's perception of system utility. If a system is not available when a user needs it, from his perspective it does not work. The *CorSys* includes availability monitoring, interface status and performance monitoring and mechanisms for users to determine which services are available and where.

7.2.5.6 System deployment options

The *CorSys* is conceived such that it can be deployed independently within a single *jurisdiction*, or widely on a large scale, depending on the requirements and desires of the entity deploying the system. This allows each entity and *jurisdiction* to make their own decisions about when, where and how extensively to offer Core services. It keeps the *CorSys* small enough that it could be implemented by a wide variety of capable enterprises, not dependent on large-scale organizations. This concept is also consistent with traditional transport funding and operations policies. While the *CorSys* may not be deployed by a transport entity, they are one likely candidate for doing so and by allowing the scope and services of the *CorSys* to vary, that option is preserved.

7.2.5.7 Use of core functions

Not all *C-ITS applications* and services will necessarily need the core functions as proposed in this *ConOps* to operate. Trust and security are more crucial for time-critical safety-critical applications than for travel information applications.

For some *communications* technologies, some of the core functions might already be provided by the *communications* network provider. For example, cellular networks might already provide sufficient security and privacy functions for some *C-ITS applications*, such as road condition alerts.

The decision on what core functions are needed will very likely be determined for each application on a case-by-case basis. It should be remembered that, in the case of safety message and actions, in order to limit liability, multiple sources and types of data will likely be used wherever possible. So for example, a collision avoidance system will likely use a combination of vehicle sensors, cameras, and DSRC *communications* from and to other vehicles, in order to perform the collision avoidance service.

Where an application is deemed to be safety-critical, such as collision avoidance applications, there may potentially be a regulated requirement for the relevant core functions to be used. There may also be a need for assurance of compliance with agreed standards for such applications.

To facilitate the decision making on which applications should use the core functions, applications may need to be classified. For example, classification could be by the following:

— the time criticality of information exchanges and management functions

  (For example, collision avoidance has a high time criticality, whereas traveller information may have a low time criticality, and road condition alerts (ice, obstacles, pot-hole, etc.) have some time sensitivity, but not time criticality in the same way as, say, collision avoidance or ramp access control)

— the safety risk of an application being provided with incorrect or delayed information

(For example, if an intersection assistance application receives incorrect signal phasing data, the safety implications could be significant)

— the security risk in relation to either safety or privacy

(For example, *communication*s that could be maliciously hacked and used to cause a safety incident, or could be used to compromise an individual's privacy)

These classifications are preferably developed based on International Standards and implemented based on a national strategy.

7.2.5.8 Secure exchange of data between users and applications

The core functionality described herein is with the objective to enable a secure connection between *ITS-station*s. It is therefore important to define the meaning of security in the context of *C-ITS communication*s.

Security relates to the information being exchanged and the system used to interact. Information is secure if it cannot be intercepted, understood if intercepted, altered or faked. System resources are considered secure if they are free from unauthorised access change and destruction. Both trust and security also extends beyond an interaction. Information is only secure if it is not released after the interaction. See ISO/TR 17427-5.

People are an integral part of any secure system. Therefore, technological solutions on their own are not sufficient in guaranteeing security. A complete solution should also include legal and social regulations, called the institutional context. This institutional context is proposed in this *ConOps* based on the concept of public key encryption and a 'Security Credential Management system' as part of that.

7.2.5.9 Public key infrastructure

A public key infrastructure (PKI) enables users of a public network to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The PKI's security credential management system provides for a digital certificate that can identify a *C-ITS* device and provides directory services that can store and, when necessary, revoke the certificates.

7.2.5.10 Security credential management system

To achieve security and trust, a 'Security Credential Management system '(SCMS) with three separate certification management entities (Certificate Authority, Registration Authority and Linking Authority) has been proposed by the 'Crash Avoidance Metrics Partnership' (CAMP) 'Vehicle Safety *Communication*s 3 Consortium' as part of cooperative projects with the USDOT (Shulman 2012).

Figure 7 shows the SCMS, which includes the in-vehicle *C-ITS* implementation (which it calls 'OBE') and the roadside infrastructure, as well as the 'Certificate Authority', 'Registration Authority' and 'Linking Authority'. The physical systems of these certification management entities are called external *support system*s. The infrastructure for issuing security certificates is called a public key infrastructure (PKI). It can provide an initial deployment model for secure V2V *communication* with sufficient certificates for a period of three years without *communication*. This is as stated by the 'V2V *Communication*s Security Project' performed by leading car manufacturers in the USA (Shulman 2012). This means that the vehicle systems and roadside infrastructure systems interact with these external *support system*s.

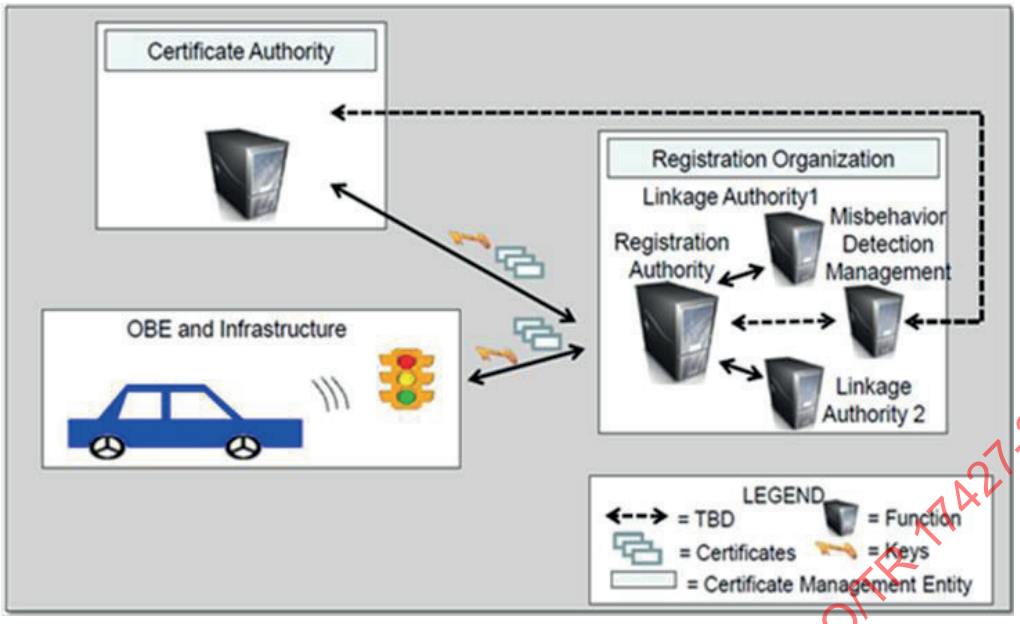

Figure 7 — Security credential management system (Source: Briggs 2012)

The European project PRESERVE intends to design, implement, and test a secure and scalable V2X Security Subsystem for realistic deployment scenarios (PRESERVE 2013). Figure 7 reflects the CAMP architecture rather than the PRESERVE architecture, but the two are very similar (EU-US harmonization task force 2012b).

7.2.5.11 Provide trust in and integrity of data

The core functionality described herein is specifically to assure that the messages communicated can be trusted.

"Trust relates to participants in an interaction (they are who they say they are), the information that is exchanged and the system used to interact. Something can be trusted when it can be unambiguously identified, operates exactly as designed and expected, does not do anything it was not designed to do (fit-for-purpose) and operates without interruption. Naturally, the longer the system works as we expect it to, the more we are likely to trust it." (CSIRO 2011).

CEN TC 278 (2013) states that trust in *C-ITS* requires the following:

— globally unique identifiers;

— related registries;

— certification laboratories;

— trust authorities;

— public key infrastructure.

In *C-ITS*, trust is ensured with the Bounded Secured Managed Domain (ISO 21217).

People are an integral part of any secure system. Therefore, technological solutions on their own are not sufficient in guaranteeing security. A complete solution should also include legal and social regulations (CSIRO 2011), called the institutional context. The proposed compliance authority is part of that.

7.2.6 Main mission of the 'Core System'

Within the context described above, the main mission of the *CorSys* is, as stated above, to enable safety, mobility and environmental *communications*-based applications for both mobile and non-mobile users. The scope of the *CorSys* includes those enabling technologies and services that will provide the foundation to enable application transactions (but the *CorSys* does not itself provide those *application services*).

The *CorSys* also needs to work in conjunction with external *support systems*. 7.1.1 to 7.1.3 describe different organizational paradigms in which *C-ITS* will have to function and will include locally and regionally oriented deployments and therefore needs to be able to grow organically to support the changing needs of its user base. Deployments will most often probably be managed regionally but follow International Standards and national standards to ensure that the essential capabilities are compatible no matter where the deployments are established.

Within *C-ITS* assisted service provision, the *CorSys* concept distinguishes *communications* mechanisms from data exchange and from the services needed to facilitate the data exchange. The *CorSys* supports the cooperative 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'.

While the *CorSys* provides a 'central' functionality required to support safety, mobility and environmental applications, this same functionality may also enable commercial applications but that is not a driving factor. The primary function of the *CorSys* is the facilitation of *communications* between system users, and some of the *communications* needs to also be secure. The *CorSys* may also provide data distribution and network support services depending on the needs of the *CorSys* deployment. 7.2, et seq. describe the *CorSys* in greater detail.

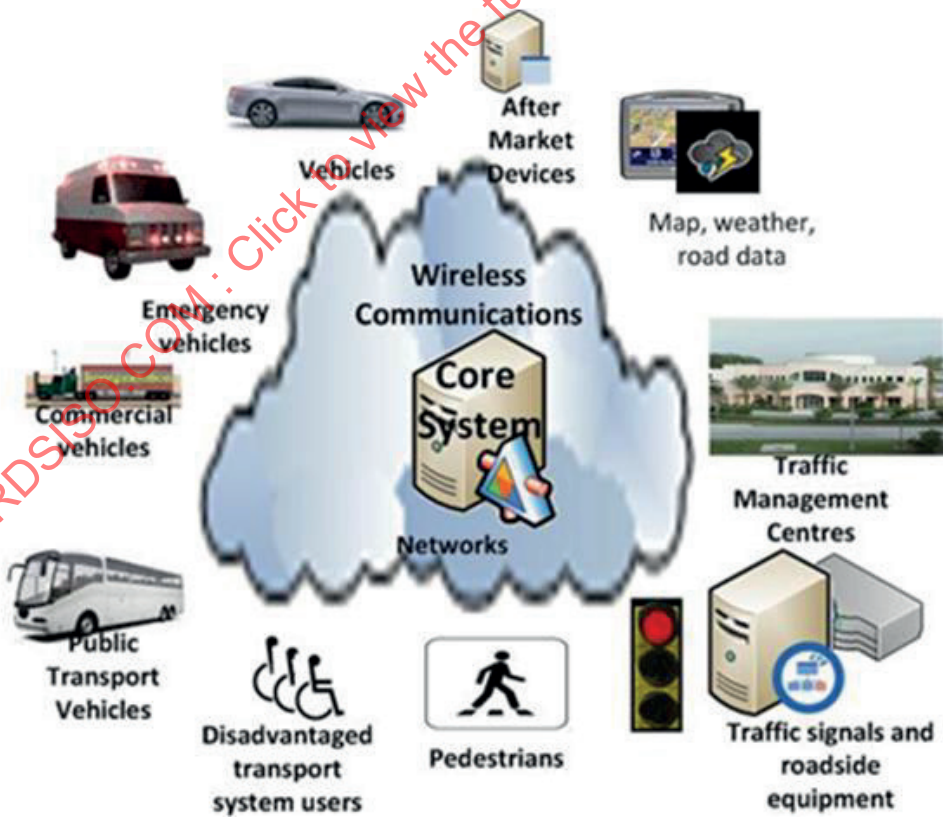

Figure 8 — *CorSys* boundary diagram

In Figure 8, the users, their devices, and software *application services* they use are outside of the *CorSys*; but the *CorSys* is still responsible for facilitating their security. Where security requirements are relatively low, this may be provided by the general security provisions of the wireless network, but

where high levels of trust are required (for example, involving moving and manoeuvring vehicles in close proximity), a higher level of security is required, and this is chiefly achieved by providing digital certificate-based mechanisms to ensure trust between users.

The *CorSys* also provides networking services to facilitate *communications* which enable or enhance the provision of *application services*, though it does not comprise the *communications* network.

7.2.7 Scope of 'Core System' services

The set of functionalities included in the *CorSys* has been limited to just those that are necessary to enable the *C-ITS* vehicle-highway environment:

— ensuring the integrity of the system;

— establishing and maintain trust between system users;

— distributing data;

— monitoring *CorSys* performance.

Applications such as collection of data or support for regional standardized clearing houses for data may be useful considerations for certain types of data or for certain regions.

It is also important to note that the *CorSys* is not meant to mandate or change existing transportation equipment, technology or transport *centres*. The *CorSys* provides mechanisms for efficiently collecting and distributing *ITS* data, but does not necessarily replace existing systems, though it is likely that many existing data collection mechanisms may be made obsolete by its data collection and distribution function.

7.2.8 Exclusions from *CorSys*

From Figure 8, the reader should note that the following are not part of the *CorSys*.

— Mobile users (e.g. vehicle devices, pedestrian smartphones) – any user device

— Roadside equipment (RSE) – both public and commercial fixed devices

— Transport management *centres* (TMC) and other public or private back-office or *centres*

Throughout the development of this *CorSys ConOps*, a number of alternatives and trade-offs have been considered that will affect the definition of the *CorSys*. Those excluded include the following:

— Storage of collected transport related (probe) data within the *CorSys;*

— Placement of RSEs with respect to the *CorSys* boundary;

— No external *support systems* (ESS);

— *Communications* options for deployment;

— *Jurisdiction*/administration databases.

7.2.9 Probe data storage

Alternatives for data storage within the *CorSys* were considered. It is considered that the *CorSys* itself does not require probe data storage in order for the system to function. Probe data are not needed within the system. That data are collected for, and passed to, other applications and the *CorSys* will provide the services to ensure that the data can be made available to requesting systems, but the *CorSys* should not archive or store such data beyond the near term requirement to service applications. The duration of 'near term' requirement may vary if a specific case is made and justified, but should not normally exceed 24 h.

7.2.10 Roadside equipment (RSE)

Although RSEs are the point of wireless contact between mobile devices and the transport infrastructure, and indeed provide the point of contact between the mobile user and the *CorSys*, the RSE (which includes the radio *communication*s to mobile devices) is considered outside the *CorSys* boundary and is included as part of the 'Field' element. The *CorSys* will normally define the RSE as a 'Field User' that has an *ITS-station* interface. It is outside the *CorSys*, and thus not responsible for implementing core services. Some core services may be accessed through proxies provided by the RSE, but RSE is not required to provide these proxies.

In the now discarded concept of a monolithic single means of wireless *communication*s, these *communication*s aspects of the RSE could be included as part of the *core system* (in reality they were simply coincident to it). But with the modern concept of multiple means of wireless *communication* fundamentally expanding the capability of the *C-ITS* implementation, should come the realization that many of those means of *communication* (e.g. 2G, 3G, 4G telephony, mobile wireless broadband, and many sources of WiFi connectivity), will not be under the full control of the *CorSys* (as for example, 5,9 GHz was to the US VII project). They are therefore by definition outside of the '*core system*. The case of *ITS* dedicated 5,9 GHz, infrared and millimetre *communication* systems should be that they are, where present, complementary *ITS*s with their own interface management, but outside of the functions of the *CorSys*. This allows the *CorSys* to maintain the interface at the application boundary, allowing the applications maximum flexibility in their user interface design. This also allows for more flexibility in the definition of the field equipment. Field equipment can be developed to include the 5,9 GHz, infrared and/or millimetre, along with sensors or controllers or storage as locally appropriate. Drawing the RSEs outside the *CorSys* boundary also eases the transition to allowing for third party or private ownership of RSEs.

7.2.11 External support systems (ESS)

The *CorSys* could be conceived to be complete and not require any ESS. This would force all capabilities to be included in the *CorSys*, but the consequence would be to reduce the flexibility of implementation. This is especially apparent with regard to the distribution of digital certificates.

The architecture for certificate distribution infrastructure is still not clear, but will likely vary around the world. Allowing ESS to provide particular niche roles in the *C-ITS* vehicle-highway environment does not eliminate the organizational problem entirely (someone still has to manage the ESS), but does provide flexibility and distinguish it from the management of the *CorSys*.

Other ESS could also be considered to provide or support *CorSys* functionalities (for example, data aggregation and analysis, situation analysis, etc). As with digital certificates, such 'outsourcing' would take the function outside of the *CorSys*, but providing services to it and its client system.

However, in a different instantiation, all *support system*s could be included within the *CorSys*, without the requirement for ESS.

7.2.12 Communications options

The current concept is to enable the use of any available wireless network. This brings the benefits of being able to utilize existing infrastructures, without the need for specific wireless infrastructures for *C-ITS*. It is expected that 5,9 GHz will be used for direct *C-ITS communication*s between vehicles (V2V) and infrastructure provided at 'hotspots' [such as high risk and complex intersections, highway access ramps, accident black spots, and railway level (grade) crossings, etc.].

The *CorSys* is not in control of what *communication*s capabilities are installed in the *ITS-station*s it is in dialogue with (vehicles/pedestrians/field equipment). In the case of vehicles, that may be a combination of multiple wireless *communication*s (such as 3G/4G, 5,9 GHz and wireless mobile broadband); in the case of pedestrian and static users, it is more likely to be limited to one form of *communication* [though in the case of cellular *communication*s that may have automatic degrade default capabilities (e.g 4G E-UTRAN to GSM/UMTS; 3G UMTS to GSM, etc.)].

To enable the overall system and its *CorSys* to function, the operators of the *CorSys* will have to determine which of these wireless interfaces the *CorSys* will support. It is expected that most *CorSys* will have the

ability to support most of the key locally available wireless media, but that is an operational decision. (For example: in areas where a combination of 3G/3G/4G is ubiquitous, this is unlikely to include satellite *communication*s. In sparsely populated 'outback' type locations, satellite *communication*s may be the only *communication* available to the *CorSys*; some areas have wireless mobile broadband coverage, some do not, and even where provided there are different variants and support of all the variants is unlikely).

The *CorSys* has to connect to whatever wireless media carriers its operator determines to support, and then the function of the *CorSys* is to operate within these *communication* channels, once established. (Mobile and field equipment will therefore have to support at least one, or more, of the wireless *communication* means that the *CorSys* supports in order to enable service provision). The actual interface equipment required for the *CorSys* to support these *communication*s is therefore considered to be 'Field Equipment', and outside of the *CorSys*.

Once the data providers are registered with a *CorSys* and the data consumers set up a subscription for the data, the data can pass between directly between *application service* providers and consumers without involving the *CorSys*.

7.2.13 Authority/jurisdiction databases

*Jurisdiction*s and their authorities (in-house or appointed) may maintain databases for a number of reasons. These may be associated with registration and regulation of vehicles, local regulations and controls policing, fee and payment collection systems, etc. Such facilities are external to the *CorSys*.

Authorities/*jurisdiction*s will also operate or approve the operation of certificate and registration authorities, manage security credentials that allow devices and systems to establish trust relationships. The *CorSys* works in conjunction with external *support system*s (ESS) for certification across wireless media, but those ESS operate outside of the *CorSys*.

All databases have, of course, to respect the local regulations in respect of privacy.

Other typical exclusions will be:

— **User/Field user** : Field devices such as signal controllers and toll systems are outside *C-ITS CorSys* even though the *IVS*)/*ITS-station* will be used to access them.

— **Public service mobile user/mobile user** : The *CorSys* considers all mobile users the same, potentially with different roles and responsibilities, but still using the same *core system* interfaces, but users of, and not part of, the *CorSys*.

— **Infrastructure service provider management systems** : The *CorSys* is strictly a provider of services, so the requirement for interfaces to separate *communication*s management is unnecessary.

— **Application service providers** : Third party *application service* providers (commercial or regulatory) and their applications may use common wireless networks/core interfaces, but are users of, and not part of, the *CorSys*.

— **Prime service providers (*IVS* equipment providers/ installers)** : may use common wireless networks/*core system* interfaces, but are users of, and not part of, the *CorSys*

7.2.14 Core system stakeholders

Core system stakeholders span the breadth of the transport environment, including users, operators, deployers and maintainers of roads, devices and vehicles. *CorSys* stakeholders include the following:

— Transport system users, e.g. private vehicle drivers, public safety vehicle operators, transit vehicle operators, commercial vehicle operators, passengers, cyclists and pedestrians;

— Transport operators, e.g. traffic managers, transit managers, fleet managers, toll operators, road maintenance and construction;

— Public safety, e.g. incident and emergency management, including fire, police and medical support;

— Information service providers, e.g. data and information providers for transport-related data, including traffic, weather and convenience applications;

— Environmental managers, including emissions and air quality monitors;

— Original Equipment vehicle Manufacturers (OEMs);

— In-vehicle device manufacturers;

— In-vehicle, personal hand-held, roadside and back-office application developers;

— *Communication*s providers, including cellular network operators;

— *Jurisdiction* regulatory and research agencies;

— Policy setting entities may include *Jurisdiction*, State, and local level transport agencies, as well as standards development organizations and perhaps a consortium of public and private sector entities overseeing the development, deployment, and operation of a *core system*.

7.2.15 Core system communications

Early conceptions for *C-ITS* envisioned that all of the *communication* would take place using a single, dedicated (5,9 GHz) *communication* technology within a single bandwidth. This potentially caused problems of overload within a restricted bandwidth, and its evolution and development has consequentially been slow.

One of the significant changes since these early instantiations is the way in which mobile users access services. In the intervening period of research, development and harmonization, wireless access has become widely available from multiple sources at speeds sufficient to enable many applications envisioned for *C-ITS*, without the need for a dedicated transport-focused *communication*s network. The 5,9 GHz technology developed specifically for *ITS*, leveraged the low latency of the medium to enable time sensitive (chiefly safety) applications, while the additional available bandwidth would be used to deliver non time-critical (largely mobility and commercial) services. Today however, cellular data services provide similar or greater bandwidth to the designated 5,9 GHz technology, making it a practical alternative for non-time critical applications.

NOTE Time-critical in this context meaning bidirectional *communication*s within milliseconds.

Also, the architecture and capability of the Internet, and evolution of so called 'smart-phones', have eased the ability to support an 'apps' based environment for the provision of many ITS and *C-ITS service*s over general purpose (and already widely deployed) wireless *communication*s. This leads to the need to support multiple, disparate wireless interfaces between *ITS-station*s, depending on the media through which a user accesses the *CorSys*. Fortunately, this was already foreseen in the CALM architecture and standards are already in place to support this diverse *communication*s environment (see 6.1).

However, some applications, and especially some applications that need to operate within a *bounded secure managed domain* (e.g. collision avoidance, highway ramp access control, etc.) will still require a dedicated, time-critical, and secure channel, and the 5,9 GHz technology, developed over the past decade, at this point of time, remains the probable best option for such service provision. Dedicated

ITS 5,9 GHz infrastructure is therefore likely to be supported only at key infrastructure points, and between (more capable) vehicles.

It should be noted that in the early conceptions of *C-ITS*, it was envisaged that a single wireless technology would be the only technology used for safety-critical service provision. However, it is now envisioned that safety-critical equipment will be able to harness multiple technologies to effect *ITS service* provision (e.g. collision avoidance systems are likely to use a combination of wireless *communication*s, radar/lidar, video, infrared, gyroscope, accelerometers, etc., and not just have to rely on an exchange of data between vehicles using a secure wireless network).

*Communication*s technologies evolve on a much more rapid time cycle than automotive technologies, so it is most probable that future, as yet unforeseen *communication* technology developments may again change the paradigm within the life of any vehicle or *ITS*/*C-ITS* implementation, and it is important that the specification of any *CorSys* has to take the enablement of such migrations to future *communication*s technologies into account.

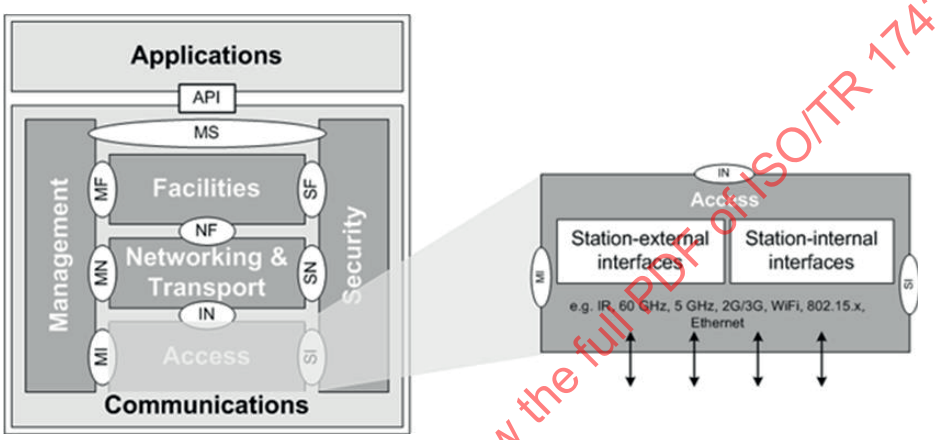

Figure 9 — *ITS-S* reference architecture — *ITS-S* access layer (Source: ISO 21217)

As a result, lower layer connectivity is distinguished as being outside the *CorSys*. The *CorSys* provides a group of functions meeting needs aside from lower layer connectivity. The *CorSys* needs to accommodate users of various access media, but is not managing those media or networks as part of its functionality. Figure 9, from ISO 21217 shows the media connections as below the *CorSys* which are accessed using 'Service Access Protocols' defined in the CALM standards (see 6.3), that effect the session initiation and validation in accordance with the standardised protocols for the chosen medium. It is expected that in many cases, the *ITS-station* will be simultaneously connected to multiple wireless media and will select the most appropriate medium for each instance of service provision. The *CorSys* will also therefore have to support interface via multiple wireless networks, and the "*Core system*" will, in all probability, also interface using *wireline communication*s for *communication*s with TMC's, service providers and other *CorSys*.

The '*communication*s layer' provides wireless *communication*s between *CorSys* services and safety, mobility, and environmental applications. Which *communication*s mechanisms are implemented at each deployment will vary. It could include cellular (e.g. 3G, 4G), WiMAX or other wide-area- wireless, or a network of short-range *communication*s hot-spots based on 5,9 GHz. It could be privately operated, such as a typical cellular network is today, or publicly, such as a municipal WiMAX solution. There is, however, one primary function that any such *communication*s layer needs to include: access. The *communication*s layer needs to provide logically addressable access to the *CorSys*. How it does this, by short range or wide area, through public or private channels, is a question of implementation. Desirable *communication*s performance characteristics will vary depending on the wireless *communication*s systems available to the *ITS-station*s.

The *CorSys* provides functionality enabling the trusted and secure exchange of data between users. *CorSys* personnel operate, maintain, update and expand the *CorSys* as necessary to provide services.

They also implement local policies using *CorSys* services where appropriate. The *CorSys* provides interfaces to the services it provides.

This leads to a matrix environment as shown in Figure 10.

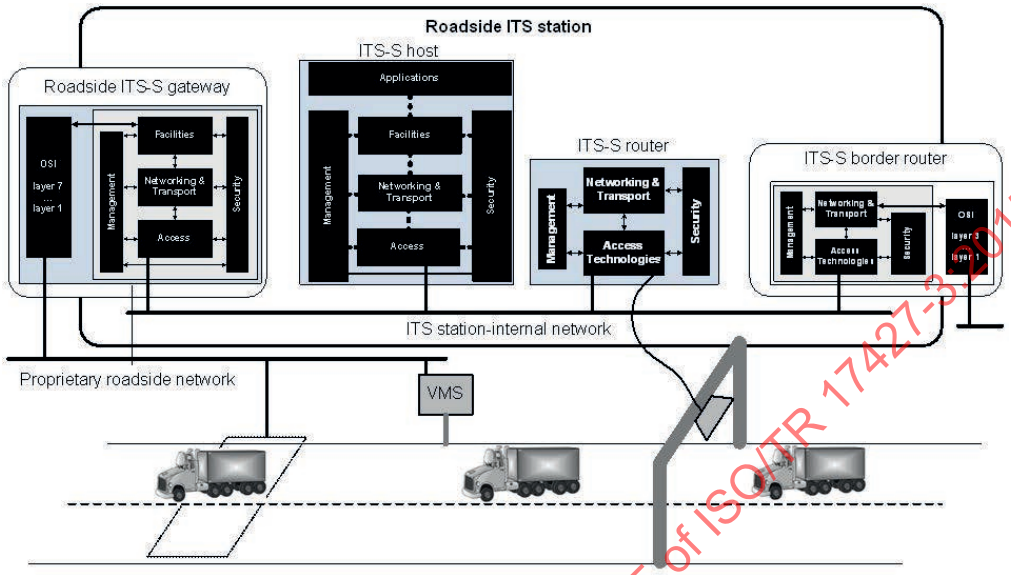

Figure 10 — Roadside ITS subsystem (Source: ISO 21217)

The more detailed *ITS-station* architecture is shown in summary in Figure 11.

See ISO 21217 for more detail and explanation.

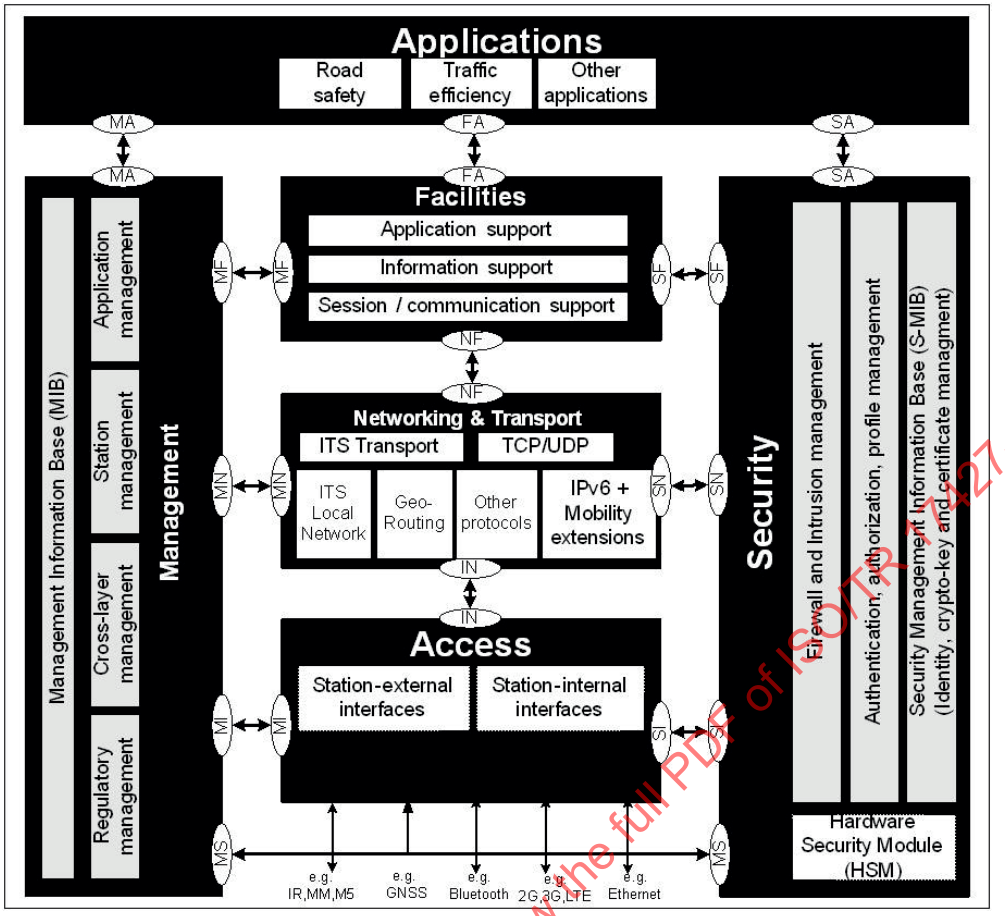

Figure 11 — ITS-Station reference architecture (Source: ISO 21217)

7.2.16 Applications

Applications provide benefits, primarily in the area of safety, mobility, or the environment, to users. Applications may include components in vehicles, hand-held mobile devices, in *back office* environments and/or field infrastructure. Applications use the *CorSys* services to facilitate their interactions with other applications or users. Applications are produced and maintained by *application service* providers and developers.

The interfaces between layers include physical specifications, *communications* protocols and message set definitions, and vary depending on originator, destination and *communications* media chosen.

While an administration/*centre* may provide some *application services* from the same physical facilities, those 'applications services' are outside of the *CorSys*.

7.2.17 Core system interactions

The *CorSys* interacts with four types of entities.

— **Mobile** which includes all vehicle types (private/personal, trucks, transit, emergency, commercial, maintenance, and construction vehicles), as well as non-vehicle-based platforms including portable personal devices (smart phones, tablets, etc.) used by travellers (vehicle operators, passengers, cyclists, pedestrians, etc.) usually via an '*ITS-station*' (ISO 21217) to provide and receive transport information. Mobile entities interact with other mobile and field entities [e.g. Variable Message Signs (VMS), Roadside Equipment (RSE)] in the mobile entity's vicinity, and *centre* entities from any location.

— **Field** represents the deployed intelligent infrastructure distributed near or along the transport network which perform surveillance (e.g. traffic detectors, cameras), traffic control (e.g. signal controllers), information provision (e.g. VMS) and local transaction (e.g. tolling, parking) functions. Typically, their operation is governed by transport management functions running in *back office*s. Field entities also include RSE supporting wireless *communication*s infrastructure (probably including 5,9 GHz at 'hot-spots), that provide *communication*s between mobile entities and fixed infrastructure.

— ***Centre*** represents *back office* systems including public and commercial transport and non-transport systems that provide management, administrative, information dissemination, and support functions. These systems may exchange information relevant to the *C-ITS* vehicle-highway environment with other '*Centre*' systems. All of these systems take advantage of the *CorSys* to provide or also make use of application data.

— ***CorSys* personnel** are the people that operate and maintain the *CorSys*. In addition to network managers and operations personnel, *CorSys* personnel also include those that are deploying and provisioning core elements. Other personnel interacting with the *CorSys* include developers of software services that maintain, fix and expand core services or extend the system as required.

— **Other *CorSys*.** The *CorSys* may also interact with other instantiations of *Core system*s. More than one *CorSys* may exist, each providing services over given geographic or topical areas. Some may provide backup or standby services for others; some may provide more or less services than others.

— **Radio/satellite sources** refers to terrestrial radio and satellite broadcast, including *Global Navigation Satellite System* (*GNSS*) (3.15) broadcasts, and position correction broadcasts.

— **External Support Systems** (ESS) provide services on behalf of and/or in support of the *CorSys*. These services are provided by the ESS because it makes more sense to manage, maintain and share the service between multiple *CorSys* due to overriding institutional, performance or functional constraints.

It should be noted that in addition to OEM *equipped vehicle*s, aftermarket, retrofit and carry-in devices are all potential means for implementing mobile solutions.

7.2.18 Core system operational goals

The overarching goals begin to define the performance characteristics that the *CorSys* needs to demonstrate the following:

— **Flexibility:** The *CorSys* design needs to be able to adapt to external change without requiring redesign.

— **Extensibility:** The *CorSys* implementation needs to take future growth into consideration. Extensions may be achieved by adding new functionality or by modifying functionality that exists at the time extension is required.

— **Scalability:** The *CorSys* needs to be able to handle growing amounts of work in a graceful manner or to be enlarged to handle growing amounts of work, without requiring redesign.

— **Maintainability:** The *CorSys* needs to be maintainable in such a way so as to minimize maintenance time, with the least cost and application of supporting resources. More specifically, the figures of merit that needs to be defined are the following:

  — The probability that a given item within the *CorSys* will be restored to operating condition within a given period of time when maintenance is performed as designed.

  — The probability that maintenance will not be required more than a given number of times in a given period, when the system is operated as designed.

— The probability that the maintenance cost for the system will not exceed a designated value when the system is operated and maintained as designed.

— **Deployability:** The *CorSys* needs to be able to be deployed in existing transport environments, without requiring replacement of existing systems, in order to provide measurable improvements.

— **Reliability:** The *CorSys* needs to perform in a satisfactory manner when operated and maintained as designed.

7.3 'Core system' overview of requirements

7.3.1 Definition of a requirement

A requirement is a capability that is identified to accomplish a specific goal or solve a problem, specifically, in this case, to be supported by the *CorSys*. It describes what is required -while avoiding the implementation specifics, or the how.

Each requirement needs to be identified uniquely, contain a description and a rationale. Rationale may include examples of how the system capability may be exercised.

The two types of requirements that are identified for the *CorSys* are the following:

— user requirements that describe a capability required by a user in order for that user to accomplish a goal;

— system requirements that describe a capability required by the *CorSys* in order to meet operational goals.

All of the typical requirements in 7.3.2 are framed from the perspective of the *CorSys*.

7.3.2 'Core System' requirements identification process

Every implementation process will need to liaise and discuss the particular requirements for the *CorSys* that is to be implemented or revised. The requirements and conceptual goals of the *jurisdiction* or body instantiating the *CorSys* will be of priority consideration, but all involved *actors* need to be consulted and need to 'buy in' to the solution eventually proposed. A formal process with formal feedback and reviews is recommended.

This section lists typical requirements that drive the definition of a *CorSys*, including the name, description, and rationale of each requirement. In many cases, the rationale terminates with a statement referencing applications, often calling out specific examples of applications that drive the requirement. The reason for this is simple: without applications, the *CorSys* accomplishes nothing. All *CorSys* requirements are focused on delivering services that will at some point be used to support applications.

The following requirements are typical and needs to be taken into consideration in developing the *ConOps* for all *CorSys* instantiations (though individual cases may implement the satisfaction of the 'need' embodied in the requirement in different ways). For each of these requirements, the *ConOps* will have to specify the following:

— objective;

— criteria;

— specification of means of requirement satisfaction;

— means to measure success/failure;

— procedures in the event of failure.

The sequence of the list that follows does not imply prioritization, which may differ from case-to-case:

7.3.2.1 Requirement: Core trust

The *CorSys* needs a process to establish trust with its system users. Such trust relationships are necessary so that the *CorSys* can be assured that system users are who they say they are, and therefore trust the source and data it receives. Specify the 'Core Trust' objectives, criteria, means to achieve satisfaction, means to measure success/failure and procedures in the event of failure.

7.3.2.2 Requirement: Core trust revocation

The *CorSys* needs to be able to revoke the trust relationship it has with its system users when necessary. A trusted system user may operate in a fashion that indicates it should no longer be trusted, in which case the *CorSys* needs to have a way of revoking that trust. Specify the 'Core Trust Revocation' objectives, criteria, means to achieve satisfaction, means to measure success/failure and procedures in the event of failure.

7.3.2.3 Requirement: System user trust

The *CorSys* also needs a process to facilitate trust between system users. Such trust relationships are necessary so that system users can be ensured that other system users are who they say they are, and therefore, the user can trust the source and data received. Specify the 'System User Trust' objectives, criteria, means to achieve satisfaction, means to measure success/failure and procedures in the event of failure.

The user trust management subsystem manages trust between and among system users and the core by providing digital certificates that system users can use to demonstrate that they are legitimate system users. It provides digital certificates to qualified users and it accepts notification of misbehaving users from the misbehaviour management and revokes the certificates of misbehaving users. It also maintains the certificate revocation list (CRL).

7.3.2.4 Requirement: System user trust revocation

The *CorSys* needs to facilitate the revocation of the trust relationships between system users when necessary. A trusted system user may operate in a fashion that indicates it should no longer be trusted, in which case the *CorSys* needs to have a way of facilitating revocation of trust between system users. Specify the 'System User Trust Revocation' objectives, criteria, means to achieve satisfaction, means to measure success/failure and procedures in the event of failure.

7.3.2.5 Requirement: Time base and synchronisation

The *CorSys* and system users need to operate on a common time base. Coordination of time between the internal systems that operate the *CorSys* prevents internal synchronization errors and enables time-sensitive interactions with system users. Specify the 'Time Base' objectives, criteria, means to achieve satisfaction, means to measure success/failure and procedures in the event of failure.

This subsystem makes a time base available to services on each *C-ITS* device. This function will be provided by the *GNSS*. No additional subsystem needs to be developed.

7.3.2.6 Requirement: Data request

The *CorSys* needs to provide a mechanism for data consumers to request data that is produced by data providers. This is a single request for a subscription to a certain type of data, and subsequent modification of the request to change data types or subscription parameters. Parameters include data frequency, type and location of where the data was generated. This enables the distribution of anonymously provided data to interested data consumers, without requiring them to enter into a relationship with data providers. Request formats need to provide data consumers with the ability to differentiate and receive only the types of data they requested. For example, this includes data type, geographic range, frequency and sampling rate. This request method supports a wide variety of user requirements, for example, from planners requesting all traffic data all the time, to traveller

information services requesting a subset of traffic data, to weather information services only interested in windshield wiper status for vehicles in a specific area. Specify the 'Data Request' objectives, criteria, means to achieve satisfaction, means to measure success/failure and procedures in the event of failure.

7.3.2.7 Requirement: Data provision/distribution

The *CorSys* needs to supply information to data providers enabling them to transmit data to interested data consumers. At a minimum, data characteristics will need to include type, frequency and location where data was generated, so that users who have requested data (see 7.3.2.6) can differentiate between available data. This requirement enables data providers to direct the data they create to data consumers, and serves as the provider-side corollary to the data request requirement. This may support a variety of applications, including those focused on the provision of data to users. Specify the 'Data Provision' objectives, criteria, means to achieve satisfaction, means to measure success/failure and procedures in the event of failure.

The data distribution subsystem has centralised and decentralised components. It maintains a central registry recording which service each device has subscribed to. Each device, e.g. a roadside *C-ITS* unit, can then send data to vehicles in their *communication* range who subscribed to it. It thus supports multiple distribution mechanisms, including source-to-points and publish-subscribe. This means it has to manage anonymisation and be able to repackage the data it receives from data providers, stripping away the source header information while maintaining the message payload. It then sends the repackaged payload data to subscribers of that data.

7.3.2.8 Requirement: Data forward

The *CorSys* needs to provide a mechanism to distribute data that is produced by a system user acting as a data provider and requested by another system user. The *CorSys* needs to provide this distribution mechanism, rather than relying on individual provider- consumer relationships, because multiple consumers may want access to the same data. For example, by having the *CorSys* distribute the data, system users are relieved of the requirement to transmit the data multiple times. Also, some data that may be critical to the proper functioning of mandatory applications, such as data supporting geo-location of users (position corrections), time base data and roadway geometry data, all of which will probably in most cases originate from a single source and will need to be distributed to large numbers of system users. Additionally, system users may interact over resource-constrained *communication* links, so *CorSys* provided data redistribution reduces the potential load on those links. Specify the 'Data Forward' objectives, criteria, means to achieve satisfaction, means to measure success/failure and procedures in the event of failure.

7.3.2.9 Requirement: Network connectivity

The *CorSys* needs to connect to the Internet. This allows the *CorSys* to provide services to any system user capable of connecting to the Internet. Specify the 'Network Connectivity' objectives, criteria, means to achieve satisfaction, means to measure success/failure and procedures in the event of failure.

7.3.2.10 Requirement: Core system data protection

The *CorSys* needs to protect data it maintains from unauthorized access. This ensures that information held by the *CorSys*, which may include sensitive information about system users, is accessed only by authorized users. Specify the '*Core system* Data Protection' objectives, criteria, means to achieve satisfaction, means to measure success/failure and procedures in the event of failure.

7.3.2.11 Requirement: Data protection

The *CorSys* needs to be able to protect data it handles from unauthorized access. This is required to support applications that exchange sensitive information, such as personally identifying or financial information, which, if intercepted, could compromise the privacy or financial records of the user. See 6.4. Specify the 'Data Protection' objectives, criteria, means to achieve satisfaction, means to measure success/failure and procedures in the event of failure.

7.3.2.12 Requirement: Anonymity preservation

The *CorSys* needs to be designed to aim preserve the anonymity of system users that use *ITS service*s as its normative operating modus-operandi, and deviate from that only with the consent of the user (usually in exchange for the user being able to receive additional benefits as a result of the loss of anonymity, and receiving strong privacy protection in these circumstances). This ensures that system users communicating with the *CorSys* who wish to remain anonymous will not have their anonymity breached as a result of communicating with the *CorSys*. Specify the 'Anonymity Preservation' objectives, criteria, means to achieve satisfaction, means to measure success/failure and procedures in the event of failure.

7.3.2.13 Requirement: Network services

The network services subsystem provides management for *communication*s layer resources. Each *C-ITS* device makes decisions about which *communication*s medium to use when more than one is available. A hybrid *communication* concept is proposed, which means that service provision on the roads and in the vehicles will rely on different *communication* technologies (ISO/CEN CALM concepts 2000-2009; ISO 21217; Amsterdam Group 2013). The network services subsystem is also responsible for protecting the system from cyber threats.

7.3.2.14 Requirement: Private network connectivity

The *CorSys* may need to be able to connect to appropriate private networks. This allows the *CorSys* to provide services to any legitimate system user that provides a private network connection to the *CorSys*. Determining what networks are 'appropriate' will be an important task in the development of any *CorSys* specification and *ConOps*. Specify the 'Private Network Connectivity' objectives, criteria, means to achieve satisfaction, means to measure success/failure and procedures in the event of failure.

7.3.2.15 Requirement: Private network routing

The *CorSys* may need to route *communication*s between other *CorSys* and system users, when one or both of the parties involved in the *communication* is connected to the *CorSys* by a private network. This enables system users connected by private network to interact with *centre*-based applications, and also facilitates backup operations between *CorSys*. Specify the 'Network Routing' objectives, criteria, means to achieve satisfaction, means to measure success/failure and procedures in the event of failure.

7.3.2.16 Requirement: Authorization management and user permissions

The *CorSys* needs to manage authorization mechanisms to define roles, responsibilities and permissions for system users. This enables the *CorSys* to establish operational environments where different system users may have different capabilities in terms of accessing *core system* services and interacting with one another. For instance, some mobile elements may be authorized to request signal priority, or some *centre*s may be permitted to use a geographic broadcast service, while those without those permissions would not. Specify the 'Authorization Management' objectives, criteria, means to achieve satisfaction, means to measure success/failure and procedures in the event of failure.

This subsystem verifies whether a system user is authorized to perform the action requested in the message payload. It therefore maintains the status of system users and operators, maintains their allowed behaviours (publish, subscribe, actions allowed to request, administrate, etc.). A *central system* also accepts and acts upon user permission change requests provided by misbehaviour management.

7.3.2.17 Requirement: Authorization verification

Where required, the *CorSys* needs to be able to verify that system users (and *CorSys* operations personnel) are authorized to perform an attempted operation. This enables the *CorSys* to restrict operations to those users that are permitted to use those operations. (For example, geo-broadcast may be restricted to transport or public safety agencies, so other users may be prohibited from performing geo-broadcast). Specify the 'Authorization Verification' objectives, criteria, means to achieve satisfaction, means to measure success/failure and procedures in the event of failure.

7.3.2.18 Requirement: Misbehaviour management

The *CorSys* needs to be able to identify system users acting as bad *actors*. Bad *actors* are not necessarily malicious; they could be malfunctioning devices that may interfere with other system users. Identifying bad *actors* enables subsequent action to protect the integrity of all users sharing the transport domain. Specify the 'Misbehaviour Management' objectives, criteria, means to achieve satisfaction, means to measure success/failure and procedures in the event of failure.

The misbehaviour management subsystem analyses messages in each *ITS* device and sends suspicious messages to a central *back office* which can then identify if users operate outside of their assigned permissions. It identifies suspicious requests and maintains a record of users that provide false or misleading data, impede other users, or operate outside of their authorized scope. It will determine when to revoke credentials from such reported misbehaving users.

7.3.2.19 Requirement: Geographic broadcast

The *CorSys* needs to provide the information necessary for system users who wish to communicate with groups of system users in a specific location. This capability enables system users to target those in a specific area for information they wish to distribute without having to send individual messages to each recipient. Examples of applications that might use this include location-specific amber alerts, traffic information, road condition alerts. and air quality alerts. Specify the 'Geographic Broadcast' objectives, criteria, means to achieve satisfaction, means to measure success/failure and procedures in the event of failure.

7.3.2.20 Requirement: Core system service status monitor

The *CorSys* needs to be able to monitor the status of *CorSys* services and provide accurate status information to system users. The *CorSys* can then inform *CorSys* operations personnel when a service operates in abnormal or degraded fashion. Additionally, system users may not be able to access a *CorSys* service (because of their location for example) and may want to know where and when they could expect access to the service. Specify the '*Core system* Service Status' objectives, criteria, means to achieve satisfaction, means to measure success/failure and procedures in the event of failure.

The service monitor subsystem monitors the status of core functions, interfaces, and *communication*s networks. Monitoring is likely to have both decentralised and centralised components. Status information provided by service monitoring functions can inform travellers of the availability and reliability of the *C-ITS service*s and application it uses.

7.3.2.21 Requirement: System integrity protection

The *CorSys* needs to be able to protect its integrity. This includes defence against the loss of integrity from a deliberate attack, software bug, environmental or hardware failure. Protection of the *CorSys* will ensure that system users can have a high confidence in the security of the information they entrust to the *CorSys*. Specify the 'System Integrity Protection' objectives, criteria, means to achieve satisfaction, means to measure success/failure and procedures in the event of failure.

7.3.2.22 Requirement: System availability

The *CorSys* needs to be available in order for system users to access *CorSys* services. This includes both operational availability and the predictable return to normal operations after service degradation. Availability and a predictable return to normal operations will ensure that system users have a high confidence in the ability of the *CorSys* to provide the services they require. Specify the 'System Availability' objectives, criteria, means to achieve satisfaction, means to measure success/failure and procedures in the event of failure.

7.3.2.23 Requirement: System operational performance monitoring

The *CorSys* will need to have an organized and measurable system to monitor its performance. This will probably include the status of interfaces, services, and metrics for the demand for services and the resolution of those demands. Monitoring the performance of *CorSys* services and interfaces will be necessary to understand when the system is operating properly, and to gauge when the system may be nearing capacity so that action may be taken to prevent the system from failing to provide services, e.g. maximum number of transactions/second, or internal *communication* bandwidth, and to give users confidence in the system. Specify the 'System Operational Performance Monitoring' objectives, criteria, means to achieve satisfaction, means to measure success/failure and procedures in the event of failure.

7.3.2.24 Requirement: Core system independence

The *CorSys* needs to be structured, deployed, managed, and operated in a manner providing *CorSys* services to all system users within its operational scope, in a manner that is seen to be fair. This will most often be achieved if the *CorSys* is run independently. However, in some circumstances, the *jurisdiction* may need or want to control and possibly operate the *CorSys*. In this event, it needs to have clearly defined and publicly known goals and an open system of 'audit' with regular auditing and reporting both to its sponsor and system users. Specify the '*core system* Independence' objectives, criteria, means to achieve satisfaction, means to measure success/failure and procedures in the event of failure.

7.3.2.25 Requirement: Core system interoperability

Ideally, the *CorSys* needs to provide services in such a way that if a mobile user moves into the area of another *CorSys*, their interface to the *CorSys* still operates. This is essential in the situation of multiple *CorSys* within one *jurisdiction* or group of *jurisdictions* within a Nation, for example, or within a group of nations (such as within the European Union); it is desirable with other adjacent *jurisdiction*s, especially within a land mass where vehicles frequently and easily move from one *jurisdiction* to another. This helps manage user expectations and helps ensure that when a mobile user subscribes to a service or installs an application, the user experience is consistent across multiple *CorSys*. Specify the '*Core system* Interoperability' objectives, criteria, means to achieve satisfaction, means to measure success/failure and procedures in the event of failure.

7.3.2.26 Requirement: Core system interdependence

The *CorSys* needs to be able to operate in coordination with other *CorSys*. This ensures that *core system* services deliver information that is consistent with information delivered by other *CorSys*, which will help avoid inconsistencies and incompatibilities between *Core system*s and between system users interacting with multiple *CorSys*. This will largely be achieved by development of, and adherence to, International Standards. Specify the '*Core system* Interdependence' objectives, criteria, means to achieve satisfaction, means to measure success/failure and procedures in the event of failure.

7.3.3 Functional components

A breakdown of the functional components into more specific functions of the detailed *ITS-station* reference architecture is shown in Figure 12. This shows a mapping of the functional subsystems to the functions of the detailed *ITS-station* reference architecture as follows:

— The *Data distribution* functions are equivalent to the *Management Information Base (MIB)* functions and the *Application support* functions in the *ITS-station* reference architecture.

— The Misbehaviour management functions are part of the Authentication, authorization and profile management functions.

— The Network services include Firewall and Intrusion management and the selection of the communication medium. The Selection of the communication medium functions are part of the cross layer management in the ITS-station reference architecture. Communication profiles for applications are defined as part of the Session/Communication support in the facilities layer.

— The Service *monitor* functions are part of the *Application management* functions.

— The *Time synchronisation* functions are part of the *Application support* functions.

— The User permissions functions are part of the Authentication, authorization and profile management functions.

— The User trust management functions are part of the Security Management Information Base (SMIB) functions.

This provides an indication of the interfacing between the core and the other parts of the *C-ITS* implementation. The detailed implementation will be further specified in the detailed design phase.

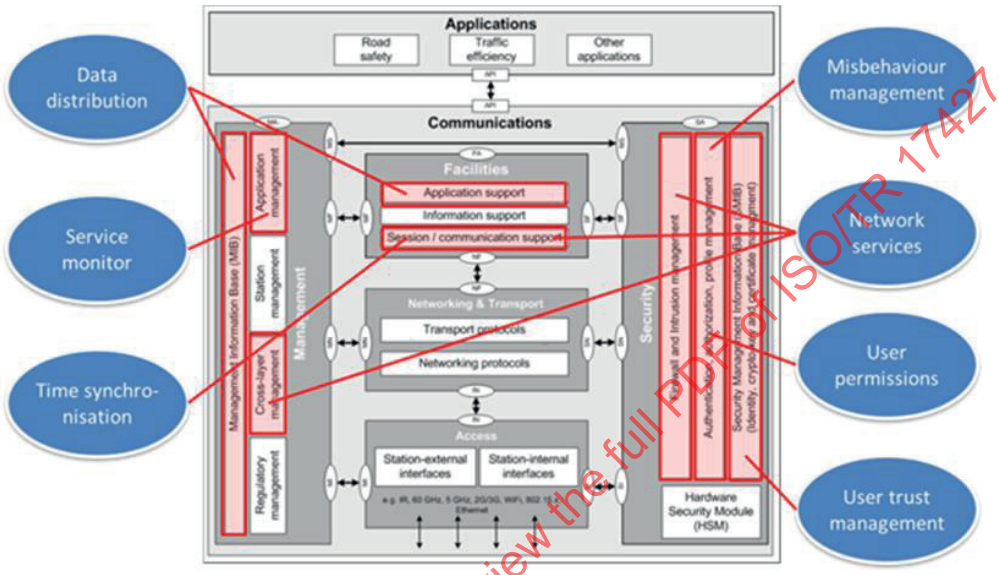

Figure 12 — Core subsystems maps to detailed ITS-station reference architecture [From ISO 21217 (modified)]

7.4 Background, objectives and scope of a 'Core System'

Throughout this *ConOps* specification of requirements, a distinction is made between the applications that are visible to users (travellers, operators, planners, advertisers, etc.) and the services of the *CorSys* that support those applications.

The technologies and applications that will be deployed as part of a *CorSys* implementation can transform travel as we know it. Combining leading edge technologies such as advanced wireless *communications*, on-board computer processing, advanced vehicle-sensors, navigation, and smart infrastructure can provide the capability for travellers to identify threats, hazards, and delays on the roadway and to communicate this information over wireless networks to provide alerts, warnings, and real-time road network information. This program makes use of wireless *communications* networks that use both V2V and V2I *communications* to support the cooperative system capabilities necessary to support the applications. Within vehicles, the following four types of devices are supported:

— **embedded devices** (devices that are installed as part of the vehicle's systems by the vehicle manufacturer);

— **retro-fit devices** (devices installed after the vehicle leaves the vehicle manufacturer, but which connect to in-vehicle information systems);

— **aftermarket devices** (devices that are installed either at the time of vehicle purchase or later, that are not necessarily connected to in-vehicle information systems but in some circumstances can be, at the vehicle owner's option);

— **carry-in devices** (devices that can be temporarily installed in vehicles and are not necessarily connected to in-vehicle information systems). Carry-in devices include the category of hand-held devices (e.g. smart phones) that could also be carried by pedestrians or other users of the roadways (e.g. cyclists or wheelchair-bound travellers). *Communication*s to and from each of these types of devices will be supported whether the *communication*s is one-way or two-way and whether the *communication* is between any combination of vehicles, infrastructure and mobile devices.

The ability to collect, process and exchange real-time data provides travellers with an opportunity for greater situational awareness of the events, potential threats, and imminent hazards within their environment. When combined with technologies that intuitively and clearly present alerts, advice, and warnings, travellers can make better and safer decisions. Additionally, the connected environment of cooperative vehicle and highway systems will provide the opportunity to enhance the efficacy of automated vehicle-safety applications.

The USDOT's VII project, the European Communications for eSafety (COMeSafety), Co-operative Systems for Intelligent Road Safety (COOPERS), the Cooperative Vehicle-Infrastructure Systems (CVIS) program, the Car 2 Car consortium, Japanese projects such as Smartway, as well as the Communications Access for Land Mobiles (CALM) standards' effort in International Organization for Standardization (ISO) Technical Committee (TC) 204, all have slightly different perspectives of the same general objective.

The lessons learned from these various parts of the world provide input to the definition of the requirements for a ConOps in this deliverable.

7.5 Operational policies and constraints

7.5.1 Certification

It is assumed that system user devices will have to be certified that they meet the specifications defined for interaction within the system. An entity or entities, granted authority by the *jurisdiction*, probably involving local DoTs and vehicle manufacturers, will have to oversee this certification process.

Similarly for software, there needs to be a means by which an authority can certify that the applications that are part of the *C-ITS* vehicle-highway environment meet standards for application behaviour wherever they are deployed.

Exactly which devices and software requirement to be certified is uncertain and may indeed vary from *jurisdiction* to *jurisdiction* according to the local paradigm for state and/or commercial management. Safety of life devices and software will almost certainly need to be certified within most *jurisdiction*s.

Mechanisms need to be established to facilitate certification so that the actual practice of certification does not constrain the policy decision of what needs to be certified.

It is expected that within most *jurisdiction*s, *CorSys* themselves will also have to be certified or at least publicly audited for verity, fitness for purpose and operational performance. This control requirement will have to be determined by the local *jurisdiction*, National Regulation or International Agreement, as appropriate. An entity or entities granted authority by the *jurisdiction* and acknowledged by the state and probably involving local DoTs and vehicle manufacturers will have to oversee this certification process.

CorSys certification should include some notion of monitoring and periodic recertification to help ensure that *CorSys* maintain operational compatibility with one another. This will be especially relevant to managing software maintenance of *CorSys*.

7.5.2 Operations and maintenance

Adequate provision needs to be made, and specified, in order to operate and maintain the system. Audit and recertification processes probably therefore have also to be specified in any *Core system ConOps* specification.

NOTE A constraint that will be particularly felt by public sector agencies that will be hosting and operating *CorSys* elements is that they are constantly under pressure to cut costs, and they can often have limited ability to hire and train qualified staff. It will be a challenge to ensure the system is functional without compromising system security and integrity. How this is to be achieved, and seen to be achieved, needs to be specified in each instantiation of the *ConOps*.

7.5.3 Security management

This subject is dealt with in greater depth in ISO 17427-5.

The management of digital certificates required for wireless *communication*s will need to ensure *jurisdiction*al, national, or in some cases, international interoperability. Some entity or entities, granted authority by the *jurisdiction* and recognized by the owners and operators of system user devices, will have to manage these digital certificates. A specific instantiation of a *ConOps* for a *CorSys* will have to define and specify these aspects.

Identification of misbehaving users will require *communication* between every *CorSys*, or at least a proxy *communication* with each *CorSys* communicating to the same certificate management entity. This will also require some coordination, as the treatment of misbehaviour in one *jurisdiction* may not be the same as the treatment in another. For example, one locality may wish to revoke permissions for misbehaving users, while another would not. This leads to a situation where a misbehaving user may still participate in the *C-ITS* vehicle-highway environment, might lose his permissions in one or more localities but maintain them in others.

Clear specification of these aspects is required to enable adjacent/interoperating *CorSys* to compare and harmonize their regimes and conditions or establish rules for treatment where the operating conditions differ.

7.5.4 Data provision/ownership

Determination of who owns data produced by mobile devices, including probe data, will affect deployments and secondary markets. This policy area needs to be addressed and determined by the *jurisdiction*, who may have also to take national and international requirements into account. Most issues may probably be best addressed in ways that are consistent with current practices for data sharing agreements of *ITS* deployments in metropolitan areas today, or consistent with the regulations and practices in place concerning the wireless media over which such data are being carried.

Issues of ownership may also need to be settled via policy of the *jurisdiction* to ensure that public agencies seeking to manage their transport operations have access to data while at the same time preserving the investment that other agencies or private entities may have put into the collection of that data.

Incentives may be needed from the data collectors in order to persuade entities to 'opt-in' to providing data.

7.5.5 System performance management

Policies and procedures for revocation of certificates for devices that fall outside the standards of operation will have to be developed as part of the specific *ConOps*, and where necessary backed by the regulation of the *jurisdiction*. This includes devices that are malfunctioning in some way but are still transmitting (potentially erroneous) messages to other system users (e.g. field users transmitting incorrect weather data due to a faulty sensor, or mobile users transmitting incorrect safety messages due to a positioning error) or devices that have been deliberately tampered with that could cause confusion or threaten the safety and security of other users. The *CorSys* will need to include functions

to monitor the behaviour of devices and applications interacting with and through the *CorSys* to identify activity that might indicate a risk to the C-ITS vehicle-highway environment.

The development of these policies and procedures needs to be consistent and these policies and procedures need to be accepted and implemented everywhere the system is deployed.

7.5.6 Flexibility

The *ConOps* and implemented *CorSys* need to recognize that *C-ITS* and its *CorSys* deployment will evolve and develop over time. Technology will advance. System requirements, architecture, operational policies all need to consider multiple deployment options, and migrateability to new generations of equipment and systems, and in particular the evolution of *communication*s systems and capabilities.

7.5.7 Core system characteristics and environment

Each *CorSys* (and its *ConOps*) requires its own determined and specified scope, defining the following:

— the geographic area over which it provides services;

— the performance of the services the *CorSys* provides;

— the data types it supports;

— the optional data distribution functionality (data sampling, aggregation, parsing) it supports;

— the system user types it supports.

In addition, the operators and managers of *CorSys* may need to negotiate the terms of the relationships between itself and adjacent and/or other connected/cooperating *CorSys*. The number and types of relationships between *CorSys* will vary; relationships will depend on the *CorSys* scope and the availability of any other *CorSys* that share scope boundaries with it.

An individual *CorSys* is currently expected to be composed of eight subsystems that provide all Core services and interfaces to system users, *CorSys* Personnel and other *CorSys*:

— User Permissions

— Network Services

— Misbehaviour Management

— Core2Core

— User Trust Management

— Time Synchronization

— Data Distribution

— Service Monitoring

The operational environment in which the *CorSys* exists may vary from a single *jurisdiction*-wide monolithic system to a heterogeneous community of systems run by multiple agencies at different levels of complexity and various locations. The potential number of scenarios involving transport-related system users is unlimited but all will involve some sort of wireless *communication*. Applications may be deployed in complex configurations supporting a major metropolitan area or a minimal configuration to support a set of isolated rural road warning systems.

As *CorSys* are deployed, some may include just the essential functions to support a particular local area and rely on an interface to another *CorSys* to provide additional services. For instance, one *CorSys* could include the necessary hardware and software to manage a subset of the subsystems for their local area and rely on a connection to another *CorSys* subsystems for additional services.

The *CorSys* will not necessarily require a control *centre* with large video screens or employ a large number of operators. A *CorSys* can function in an office or data *centre* environment as long as there is access to a network that enables *communication*s between system users and the *CorSys*.

7.5.8 Deployment configurations

The *CorSys* may have different deployment configurations.

— Standalone system – where the deploying agency (public or private) includes all hardware, software and *communication*s necessary to support their services in an office or *Centre* environment that is dedicated to support safety, mobility, and environmental applications.

— Co-located with other transport services – where the deploying agency (public or private) installs the hardware, software, *communication*s in an office or *centre* environment that is also used to house the operations for another transport service such as a traffic management *centre* or a traveller information service provider.

— Distributed across geographic locations, including remote hosting – where one deploying agency has the hardware and software for part of the services but uses Internet *communication*s to run some *CorSys* services remotely, either at another facility owned by the same agency, another similar agency, or a software as a service provider for some utilities.

7.5.9 Deployment footprint

The footprint of a *CorSys* deployment includes the following:

— The geographic area over which it provides services: This area may coincide with political boundaries, geographic features, *communication*s deployments, or may be defined independent of any external factors by the entity deploying the *CorSys*.

— The performance of the services the *CorSys* provides: This includes identification of the services the *CorSys* provides, as well as the performance of those services. Service performance will be a factor of several items: performance of the hardware and software on which the service operates, but most significantly the *communication* path over which the service is accessed by the system user. Hardware can usually be quickly scaled to improve performance, but deployment of higher speed or lower latency wireless *communication*s is a more lengthy process. Consequently, the performance aspect of service delivery will be primarily constrained by the performance of wireless *communication*s available in the deployment area. This mostly affects mobile users, since field and *centre* users usually have access to *wireline communication*s offering performance sufficient to their requirements.

— The data types it supports: This defines the data types and associated message formats for all data accepted by the *CorSys's* Data Distribution subsystem. Since all *CorSys* interfaces will need to be defined by standards, this should be expressed as a reference to applicable standards (e.g. SAE J2735, UMTS Release 13, ISO 21215, etc.).

— The optional data distribution functionality (data sampling, aggregation, parsing) it supports: These facilities needs to be characterized in terms of what data types are supported for each capability, ranges (e.g. sampling limited to between 1 in 10 and 1 in 50 and only over a specific geographic area) and any restrictions on the use of this functionality (e.g. aggregation limited to a particular group of system users).

— The system user types it support: This explains if the *CorSys* has any group concepts for particular system user types (e.g. public transport vehicle mobile users). This could include a description of any particular functionality that is applicable to this group in the *CorSys's* geographic area (e.g. public transport signal priority).

The deployer of the *CorSys* needs to be able to describe the deployment footprint in a format that other parties understand so that this information can be communicated and understood by other *CorSys* deployers and interested system users. This is an important task for the *ConOps* not only in

heterogeneous communities of systems run by multiple agencies but also for single *jurisdiction*-wide monolithic systems.

Further complicating the operational environment is the relationship between *CorSys*. *CorSys* may provide service backup for one another; i.e. one *CorSys* providing services in lieu of another, to support maintenance or emergency operations. Service backup requires institutional relationships between the *CorSys* operators, as well as sufficient *CorSys* and *communication*s capacities to fulfil such requirements.

Institutional relationships need to also address boundary conditions (i.e. what occurs when a mobile user transitions between the deployment footprints of two *CorSys*?). The following examples of *CorSys* operational environments focus on the *communication*s available between *CorSys* and system users and the geographic boundaries between *CorSys* deployments.

7.5.9.1 Example 1: Single or monolithic *CorSys* deployment

Monolithic or isolated *CorSys* provide the baseline for illustrating *CorSys* operational environments. In this example, a single *CorSys* provides services for a given geographic area. This area has 3G UMTS cellular services available throughout, as well as two areas where 5,9 GHz *ITS communication* based roadside equipment (IEEE 802.11p WAVE) is deployed. Core services are available through 3G everywhere, and through 5,9 GHz (to backhaul of some type, could be wired or wireless) in two smaller 'hot-spots'. There are no conflicts or boundary conditions with other *CorSys*. All Mobile User data distribution functions are provided by the single *CorSys*.

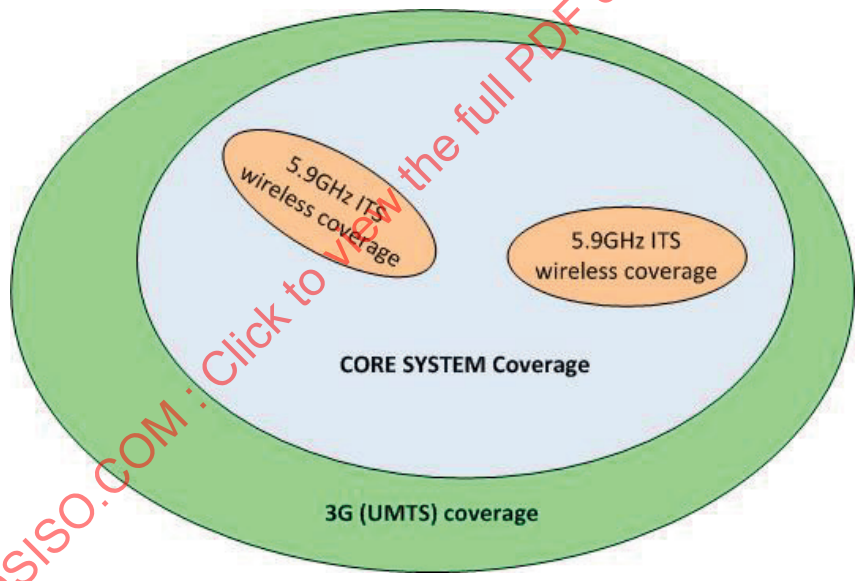

Figure 13 — Single *CorSys* deployment

7.5.9.2 Example 2: Two adjacent *CorSys*

Adjacent *CorSys* require interaction between both *CorSys* and the entities that operate those *CorSys*. In the example below, one *CorSys* overlaps coverage with another *CorSys*; for example, a metropolitan system abutting a state-wide system. In this example, *CorSys* 2 provides all of its services in the yellow area, and all by 3G links. 'Core System 1' provides its services in the blue area, some by 3G and some by 5,9 GHz. The adjacent area between the *CorSys* requires agreement between the *CorSys* operators as to which *CorSys* provides services. Mobile users that move between the areas serviced by the *CorSys* would transition between *CorSys* after they had left the boundary area between the two *CorSys* coverage areas. The size of the boundary area may be expressed in distance or time, and is a topic for further technical study and agreement between the deployers of the two *CorSys*.

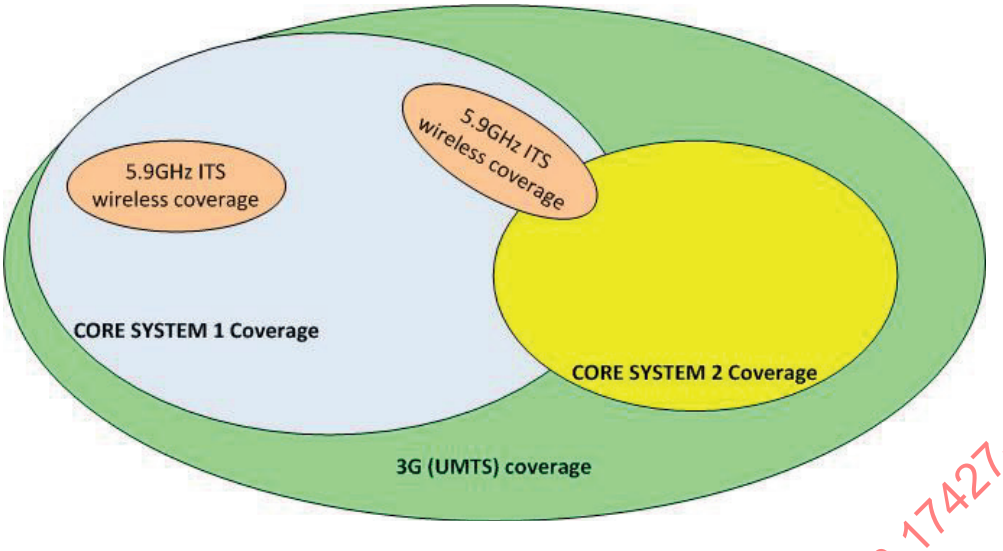

Figure 14 — Adjacent *CorSys* deployment

7.5.9.3 Example 3: Two Overlapping *CorSys* with shared service

In Figure 15, the *CorSys* share responsibility over an overlap area. They would have to negotiate agreements over data ownership and distribution; relationships could be as peers or one *CorSys* could be dominant for certain services while the other could be dominant for other services. Core 1 would provide some services in the area by 5,9 GHz, while both provide services in the shared area by 3G cellular. 5,9 GHz users would interact only with Core 1, while 3G users could interact with either Core depending on the nature of the data distribution agreement.

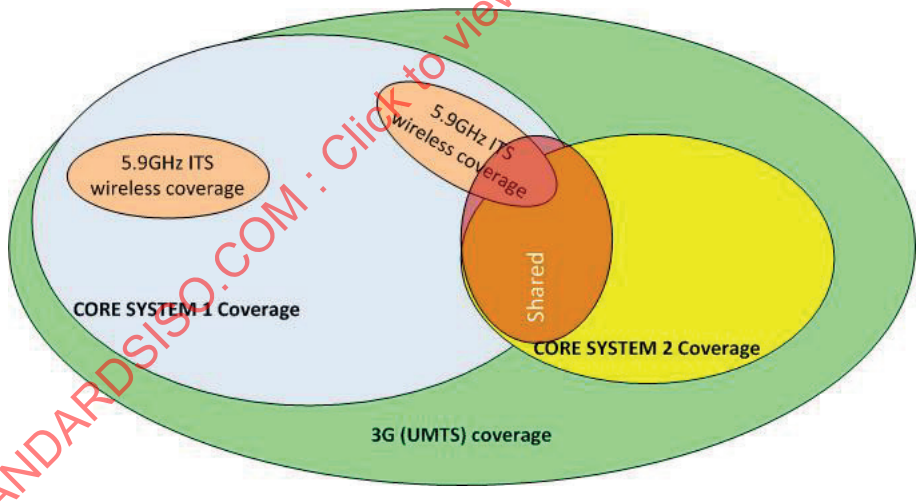

Figure 15 — Overlapping core deployments with shared service

These examples illustrate some of the potential for overlap and shared service between *CorSys* in a mixed *communications* environment. Other situations may, for example, include one *CorSys* supporting public wireless networks (GSM/UMTS/E-UTRAN) while another *CorSys* supports 5,9 GHz networks. Another possibility is a *jurisdiction* allowing competing core networks (such as mobile phone network competition). Situations will vary according to both the geography and political and economic paradigm within the *jurisdiction*. Interaction between *CorSys* is necessary when mobile users request services offered by one and not another in a shared space, and also when mobile users move between coverage areas, at least to coordinate operational boundaries.

One consequence of this analysis illustrates a significant difference from the architecture conceived in the earlier designs for *C-ITS*: A *CorSys* can be deployed without any 5,9 GHz field equipment. 5,9 GHz

field equipment will enable many applications particularly including safety applications with the involvement of/management by the *CorSys*, via V2I *communication*s. V2V interactions rely only on the *CorSys's* facilitation of trust relationships which can be managed by several means. In its current conception, 5,9 GHz will only be for V2V *communication*s and to cover so called hot-spots, where an economic or political argument can be made for the infrastructure investment.

7.5.10 Subsystems

This subclause describes the subsystems of the *CorSys*, how they relate to the requirements that were defined in 7.2.2, and how they relate to each other to support the overall operation of the *CorSys*.

While at this level in the system engineering process, it is premature to fully develop the major system components some high-level concepts can be related. The *CorSys* is all about standardized *communication*s that satisfy system user application requirements. The *CorSys* and the overall framework of applications need to be flexible to allow for staged deployments both large and small. The *CorSys* is really just enabling *communication*s between system users (and service providers) and as such is only comprised of standardized interfaces and the services required to make the interfaces work. The interfaces need to be standardized in order to permit interoperability among the external systems.

It is probably useful to note that with respect to the *CorSys*, the 'system users' involved are the applications or external systems (i.e. Mobile, *Centre*, and Field) that are interacting with the *CorSys*. The only human users of the *CorSys* are the administrative personnel that operate and maintain *CorSys* services. The human '*End user*s' of the *C-ITS service*s rarely, if ever, have direct contact with the *CorSys*.

7.5.11 Subsystem descriptions

This section provides a description of each of the subsystems of the *CorSys*, arranged alphabetically.

A subsystem can be defined as "an integrated set of components that accomplish a clearly distinguishable set of functions with similar or related uses".

7.5.11.1 'Core2Core' subsystem

The 'Core2Core' subsystem interfaces with other *CorSys*, advertising its *jurisdiction*al scope, and offers services, and services it wishes to obtain from other *CorSys*.

The *CorSys* 2Core subsystem will maintain knowledge base and services available from other *CorSys*. In this way, the *CorSys* can act as a user to another *CorSys*, providing proxy services that it does not offer but another does.

Additionally, Core2Core is responsible for compatibility between *CorSys*, ensuring that one *CorSys* does not encroach on the scope of another *CorSys*, and similarly accepting error messages from mobile users that might indicate a cross-*jurisdiction*al compatibility or scope coverage issue.

Core2Core also manages backup of configuration data between *CorSys*, restoration of backup data between *CorSys*, and takeover of services between *CorSys* (where one *CorSys* asks another *CorSys* in order to provide a service so that it may perform a maintenance action or other activity that renders it unable to deliver all services).

Interfaces between *CorSys* need to be formalized in interface specifications. Conflicts and discrepancies between *CorSys* will have to be resolved by agreements between the agencies responsible for the respective *CorSys*.

7.5.11.2 'Data Distribution' subsystem

The 'Data Distribution Subsystem' interacts with system users taking one of two roles:

— System user as a 'Data Provider', where the system user provides data to the *CorSys* for the *CorSys* to distribute to other system users;

— System user as a 'Data Subscriber', where the system user receives data that was provided by other system users but distributed by the *CorSys.*

'Data Distribution' needs to maintain a directory of system users that want data ('Data Subscribers') and facilitates the delivery of data received from data providers to those data subscribers. It supports multiple distribution mechanisms, including the following:

— **Source-to-Points:** The data provider communicates data directly to data consumers. In this case, no data are sent to the *CorSys*, however, the *CorSys* is involved to check user permissions and provide addressing services through those subsystems.

— **Publish-Subscribe:** The data provider communicates data to the data distribution subsystem, which forwards it to all users that are subscribed to receive the data.

'Data Distribution' allows data consumers to specify (and change the specification of) data they wish to receive using criteria including the following:

— Data type;

— Data quality characteristics;

— Data format requirements;

— Geographic area;

— Sampling rate;

— Minimum and maximum frequency of data forwarding.

'Data Distribution' maintains a registry of which data consumers receive what data. Data distribution does not store or buffer data beyond that which is necessary to complete publish-subscribe actions. If a given data consumer is unable to receive data that it has subscribed to (because of a *communication*s or other system failure), the data in question may be lost. The degree to which data distribution buffering accommodates connectivity failures will be up to the *CorSys* deployment. Some *CorSys* may offer temporary storage - in this fashion, data distribution repackages data it receives from data providers, stripping away the source header information while maintaining the message payload. It then sends the repackaged payload data to subscribers of that data. It may aggregate, sample or break data into individual elements, depending on the deployment.

Data distribution does not share or exchange data with other *CorSys*. System users that want data from multiple *CorSys* need to subscribe to each *CorSys* who they want to receive data from.

7.5.11.3 'Misbehaviour Management' subsystem

The 'Misbehaviour Management' subsystem analyses messages sent to the *CorSys* to identify users operating outside of their assigned permissions. It works with the 'User Permissions' subsystem to identify suspicious requests and to maintain a record of specifically identifiable users that

— provide false or misleading data,

— operate in such a fashion as to impede other users, and

— operate outside of their authorized scope.

Because most *end user*s will rarely interface with the *CorSys*, 'Misbehaviour Management' will also accept reports of misbehaving users from other users. *Centre*, mobile and field users can send misbehaviour reports that reference credentials attached to messages and note the type of misbehaviour in question. 'Misbehaviour Management' will record such reports, and according to a set of controlled rules, and determine when to revoke credentials from such reported misbehaving users. For anonymous users, revocation is more complex and may result instead in a lack of credential renewal. Regardless of the result, 'Misbehaviour Management' provides such revocation/renewal notifications to 'User Trust

Management' (which is responsible for managing certificates) and 'User Permissions' (which is responsible for managing access to the *CorSys*).

Large numbers of failed renewals could have a significant effect on operations; system requirements and design activities will need to ensure that renewal failures do not adversely affect system performance or user experience.

Also, since some field users could provide services that enable geo-casting to mobile users, 'Misbehaviour Management' needs to notify 'Data Distribution' of misbehaving field users, so that they can be removed from any geo-casting distributions.

7.5.11.4 'Network Services' subsystem

The 'Network Services' subsystem provides connectivity between the *CorSys* and system users. This includes both an Internet connection and any private network connections that the *CorSys* supports to other *CorSys* or system users.

The 'Network Services' subsystem also provides management for *communication*s layer resources. It will enable decisions about which *communication*s medium to use when more than one is available and take into account message priority when passing messages and choosing media. This requires identifying available *communication*s methods' current performance characteristics and applicable user permission levels. Permission requirements need to be coordinated with the 'User Permissions' subsystem.

The 'Network Services' subsystem is responsible for protecting the *CorSys* from cyber threats. It needs to examine all *CorSys* network traffic in order to identify malicious activity, to log information about such activity, and should attempt to stop the activity and notify *CorSys* personnel of the malicious action or attempt and its resolution.

7.5.11.5 'Service Monitor' subsystem

The 'Service Monitor' subsystem monitors the status of *CorSys* services, interfaces, and *communication*s networks connected to the *CorSys*. It informs system users of the availability and status of its services.

The 'Service Monitor' subsystem also monitors the integrity of internal *CorSys* components and supporting software and mitigates against vulnerabilities. This includes periodic verification of the authenticity of *CorSys* service software and supporting software. This also includes monitoring for patches to third-party components. Should a vulnerability be detected, or a component of the *CorSys* found to have lost integrity, the 'Service Monitor' subsystem takes steps to mitigate against damage and performance degradation.

The 'Service Monitor' subsystem needs to ensure the physical security of *CorSys* services by monitoring the environmental conditions that *CorSys* components operate in (temperature, humidity), as well as the condition of its power system. It needs to take steps to mitigate against system failures in the event that environmental conditions exceeding operating thresholds. Actions could include the activation of environmental or backup power systems and/or the modification of Core service operations, as well as notification of *CorSys* personnel.

The 'Service Monitor' also needs to monitor the performance of all services and interfaces and provide performance metrics.

7.5.11.6 'Time Synchronization' subsystem

The 'Time Synchronization' subsystem makes a consistent 'time base' available to all system users and makes this time available to all *CorSys* services which use this 'time base' whenever a time reference is required.

7.5.11.7 'User Permissions' subsystem

The 'User Permissions' subsystem provides tools allowing operators and other *CorSys* subsystems to verify whether a given system user is authorized to request or perform the action requested in the message payload. It also needs to maintain the status of system users and operators, whether they have a specific account, their allowed behaviours (publish, subscribe, actions allowed to request, administrate, etc.) with defined permissions or belong to an anonymous group. The 'User Permissions' subsystem provides tools for *CorSys* personnel to create new users and groups, modify existing users and groups, and modify permissions associated with users and groups. The 'User Permissions' subsystem needs to accept and act upon user permissions change requests provided by 'Misbehaviour Management'.

7.5.11.8 'User Trust Management' subsystem

The 'User Trust Management' subsystem manages trust between and among system users and the *CorSys*. It does this by providing digital certificates that system users can use to demonstrate to other system users and *CorSys* that they are legitimate system users. The *CorSys* provides digital certificates to qualifying 'Field' and '*Centre*' users. For example, the 'User Trust Management' subsystem will work with an ESS to distribute IEEE 1609.2 certificates to 5,9 GHz enabled mobile and field users, and ensure that those certificates include the proper permissions for using applications whose use is governed by certificate permissions. The 'User Trust Management' subsystem accepts notification of misbehaving users from 'Misbehaviour Management'.

7.5.11.9 Subsystem to requirements

Table 3 shows the relationship between the *CorSys* Subsystems and the requirements defined in 7.2.2. In most cases, a subsystem will satisfy multiple requirements and in some cases, requirements may be satisfied in multiple subsystems.

User Trust Management maintains the Certificate Revocation List. For example, it obtains a copy of the IEEE 1609.2 Certificate Revocation List from the ESS. It distributes both X.509 and IEEE 1609.2 Certificate Revocation Lists.

Table 3 — Subsystem to requirements

Core subsystem	Requirements
Core2Core	*CorSys* Independence, *CorSys* Interoperability, *CorSys* Interdependence, *CorSys* Data Protection
Data Distribution	Data Request, Data Provision, Data Forward, Geographic Broadcast, *CorSys* Interoperability, *CorSys* Interdependence, Anonymity Preservation
Misbehaviour Management	Misbehaviour Management, Core Trust Revocation, system user Trust Revocation, *CorSys* Interoperability, *CorSys* Interdependence
Network Services	Network Connectivity, *CorSys* Interoperability, *CorSys* Interdependence, *CorSys* Data Protection, Private Network Connectivity, Private Network Routing
Service Monitor	Core System Service Status, System Integrity Protection, System Availability, System Operational Performance Monitoring, *CorSys* Independence, *CorSys* Interoperability, *CorSys* Data Protection
Time Synchronization	Time Base, *CorSys* Interoperability, Core System Interdependence
User Permissions	Authorization Verification, Authorization Management, Core System Independence, *CorSys* Data Protection, Anonymity Preservation
User Trust Management	Data Protection, Core Trust, system user Trust, Core Trust Revocation, system user Trust Revocation, *CorSys* Independence, *CorSys* Interoperability, *CorSys* Interdependence, *CorSys* Data Protection

7.5.11.10 System user — Subsystem interfaces

Figure 5 can now be redrawn from a systematic viewpoint, as is shown in Figure 16.

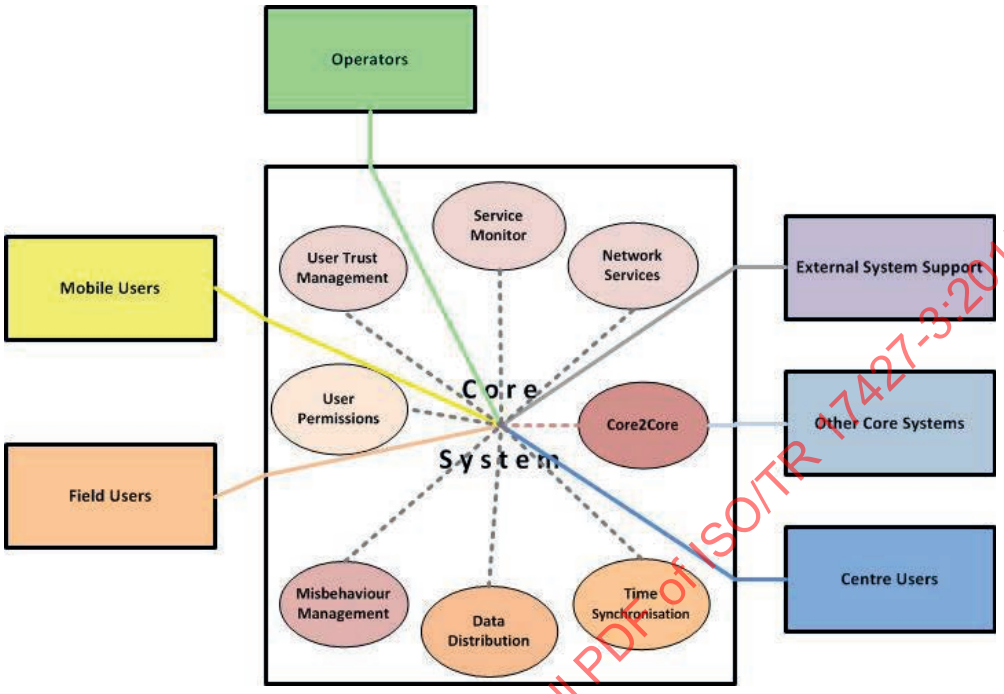

Figure 16 — Subsystem interfaces

The user-oriented Figure 16 should be compared with the *communications*-oriented Figure 5.

Figure 16 shows the actors accessing the subsystems via the core system. To provide different services, the *actors* will access a combination of the subsystems. The only exception is the Core2Core subsystem where all interactions with other *CorSys* are managed by the *CorSys* on a Core2Core basis. This subsystem manages interactions between Core subsystems and other *CorSys*, serving as proxy for interactions with the other subsystems.

All subsystems have interactions with other *CorSys*. Data distribution coordinates subscriptions and registrations for boundary conditions, so *CorSys* are consistent in who collects and distributes data over what area (not propagating subscriptions). Misbehaviour management provides misbehaviour reports and analysis results. Network services shares cyber-security threat information. Service monitor provides service status and performance information (see the discussion on states and modes later in this section). User trust management coordinates the revocation of certificates and ensures consistency among certificates that are distributed so that no duplications occur. All subsystems may provide configuration and backup information.

7.5.11.11 Subsystem — Subsystem interfaces

Core subsystems interact extensively. Interfaces between the *CorSys* subsystems include the following examples:

a) All subsystems provide configuration (including Data Distribution data acceptance and provision information) and backup data to Core2Core.

b) Core2Core provides restore data to all subsystems.

c) Core2Core exchanges Certificate Revocation Lists with user trust management.

d) Data distribution provides suspicious data (including geo-cast data) to misbehaviour management for analysis.

e) Misbehaviour management provides system user misbehaviour reports and its own misbehaviour analysis results to Core2Core.

f) Misbehaviour management provides changes to geo-cast configurations to data distribution.

g) Network services provides notifications of possible network intrusions to misbehaviour management.

h) Network services provide measures of *CorSys* component (i.e. hardware) performance to service monitor.

i) Service monitor provides Core System performance information to Core2Core.

j) Time synchronization provides time sync information to all subsystems.

k) User permissions provide system user and operator permission check results to all subsystems.

l) User trust management provides certificate distribution configuration information to Core2Core.

7.5.11.12 Data stores in the core system

While long term storage of data are not a service of the *CorSys*, there needs to be the facility for *data stores* (3.11) within the system to support and manage the system services. This will include the information necessary to communicate with other *CorSys*, with external system support, *communications* layer systems, and will include *data stores* to organize misbehaviour, states and modes, subsystem configurations, credential management, subscriptions, data acceptance criteria and system user information. For mobile users, this information will only be collected and stored for as long as necessary in accordance with the predetermined 'Privacy Policies' (see 6.4). Specific details with regard to the exact types, locations and contents of the various *data stores* need to be specified in a service architecture document.

7.6 Modes of operation

The states and modes of operation of the *CorSys* are described in this section. Subsystems may be in one of four states, as illustrated in Figure 17.

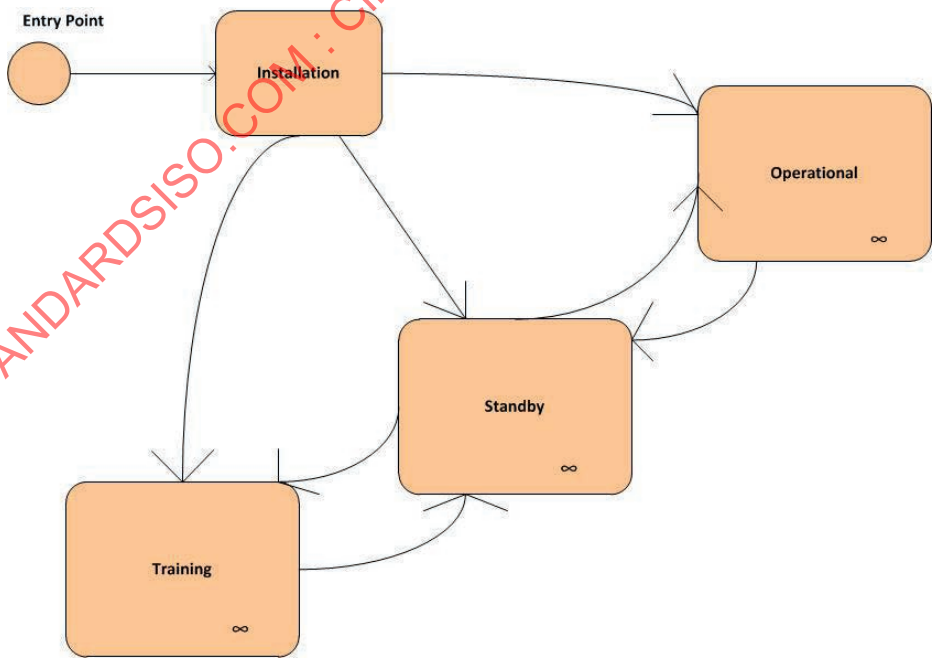

Figure 17 — Subsystem states

Standby: The *CorSys* or subsystem operating in a standby state provides backup to one or more other *CorSys* or other *CorSys* subsystems. From the standby state, the *CorSys* or subsystem may take over the functions of another *CorSys* or subsystem if required.

Training: The *CorSys* is placed in a training state when it is used for imparting training on the *CorSys* features. Certain features such as real-time display of log messages and debug messages may be enabled in the training state which may not otherwise be accessible under normal conditions.

While within the 'Standby' and 'Operational' states, each subsystem may be in one of five modes, as illustrated in Figure 18.

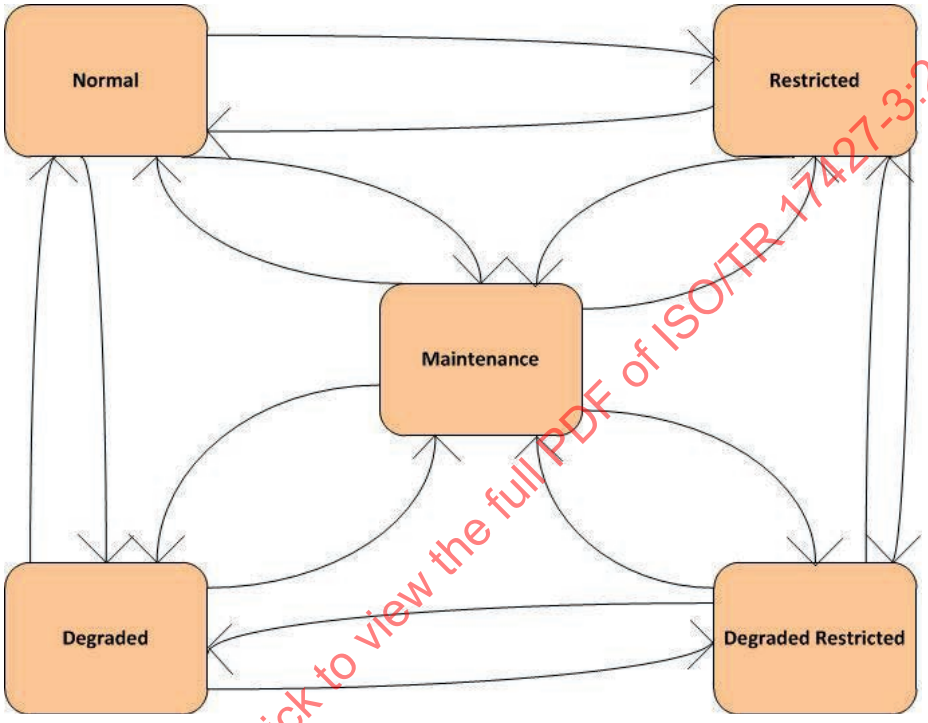

Figure 18 — Standby and operational modes

Normal mode: In the normal mode, there is little or no functional or performance impacts on the ability of the subsystem to provide its services.

Degraded mode: In the degraded mode, the subsystem is impaired to a significant extent: its ability to provide services is greatly reduced or eliminated completely. Degraded mode is a reflection of conditions; it is not a mode that is voluntarily entered.

Restricted mode: In the restricted mode, the subsystem is capable of performing as expected; however, certain services or features are disabled to support a specific event such as an evacuation. The restriction is commanded by core system personnel. It may also be implemented via a policy-based management system whereby pre-specified policies are automatically implemented by the *CorSys* in response to detection of events, behaviours or performance thresholds. In a restricted mode, the *CorSys* could curtail the use of particular subsystems to privileged users, such as first responders and other emergency personnel.

Degraded/Restricted mode: If during the course of operating in a restricted mode there is a loss of functionality, or if while in degraded mode there is a requirement to enter restricted mode, the subsystem may enter the degraded/restricted mode. This mode is a combination of the restricted and degraded modes, where subsystem services are offered only to particular users, but performance is degraded.

Maintenance mode: Core system personnel may place a subsystem in maintenance mode to replace an impaired component or upgrade a component. Depending on the nature of maintenance planned, the

impact on the subsystem's ability to provide services may be impacted. Also, its ability to manage itself and provide visibility into how it is performing may be impacted.

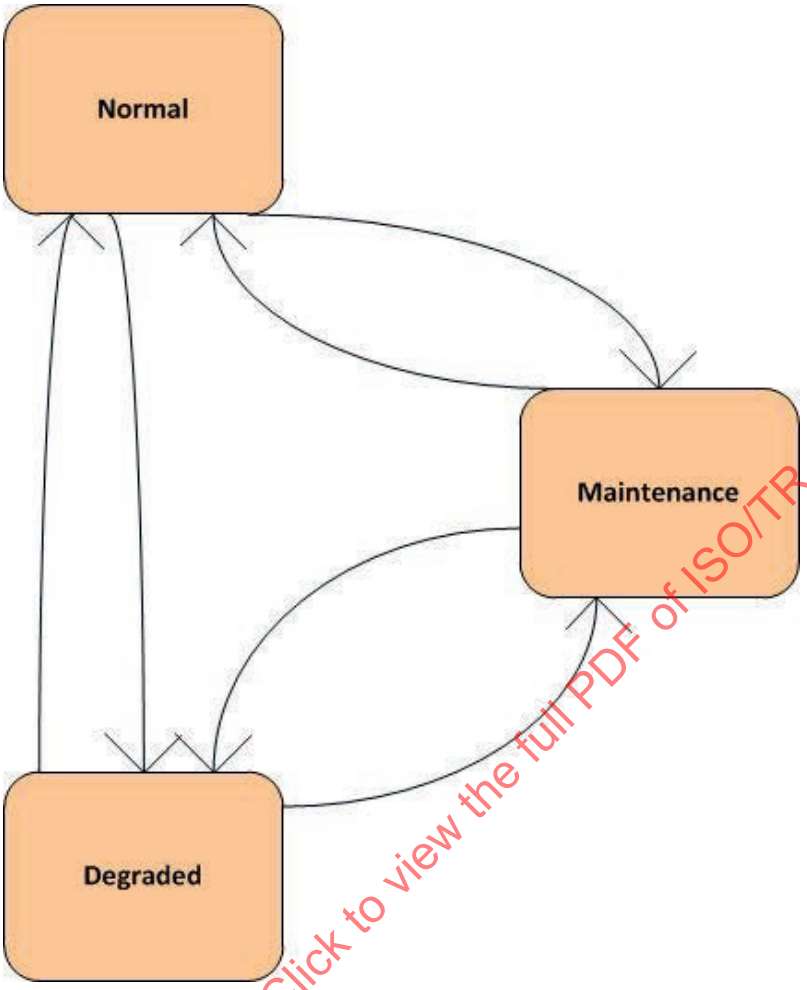

Figure 19 — Training and Installation modes

While in the 'Training' and 'Installation' states, each subsystem may be in one of three modes, as illustrated in Figure 19. Definitions of these modes are the same as those defined above under 'Standby' and 'Operational'.

7.7 User types and other involved personnel

This section discusses the users in terms of the types of *actors* and their interactions with the *CorSys*, including support or operations personnel. These user types are used as part of the example use case scenarios in Clause 8.

System users (systems and applications that use/interact with the *CorSys*), include the following:

Mobile applications – These include applications running on vehicles of all types (private cars, trucks, buses, commercial vehicles, motorcycles). This also includes applications running on personal devices such as smartphones that allow pedestrians, bicyclists, or disabled road users to provide and receive data.

Field applications – These include applications running on roadside devices collecting data about their surroundings, communicating with mobile devices, controlling and managing transport systems such as signs or traffic signals. Accessing the services of the *CorSys* allows these applications to participate in secure, authenticated data exchanges with mobile applications or other field applications. These could also include applications supporting transactions such as payment of tolls, parking, or reservation systems, again, using the services of the *CorSys* to support the secure, authenticated exchange of data.

***Centre* applications** – These include many types of central data systems or information services that support travellers, manage transportation resources, or provide more general applications that use or provide data to Mobile, Field, or other *Centre* applications. Examples include traffic management *centres*, transit operations *centres*, archived data management systems, information service providers, emissions management systems, public safety or emergency management systems, and weather service applications.

CorSys personnel, the human users that interact with the *CorSys*, include the following:

Deployers – These users represent the initial installers for a Core System. Their interaction with the *CorSys* itself will be similar to an administrator or maintainer in that they will be accessing system configuration files, setting parameters and policies as part of the initial installation and check out of the system before turning it over to the other *CorSys* personnel for regular operations.

Developers – These users are the code writers that build software enhancements for the system. They will be accessing the published interface definitions and configuration data about the *CorSys* in order to develop additional features or expanded capabilities.

Testers – These users verify the *CorSys* operation when any changes are made to its operating hardware or software.

Administrators – These are the operators that set control parameters, implement system policies, monitor system configuration, and make changes to the system as needed.

Operators – These are the day-to-day users of the *CorSys* that monitor the health of the system components, adjust parameters to improve performance, and collect and report statistics of the overall system.

Maintainers – These users interact with the system to install updated software or to repair or upgrade hardware components to keep the system up to date and running efficiently.

The operational context of where the application is located may affect the operations of that application. For instance, if a mobile application or its host device detects that it has boarded a bus, it may stop transmission of its location messages over 5,9 GHz until the device/application detects that it has left the bus and should start transmitting again. In other situations, the same application may be both a provider of data, as well as a consumer of data from other sources of data.

7.8 Operational scenarios

The EU-US harmonisation task force (2012) identified five 5,9 GHz *communication* scenarios for *C-ITS*, being

— vehicle-originated broadcast,

— infrastructure-originated broadcast,

— infrastructure-vehicle-unicast,

— local time-critical sessions,

— local non-time-critical sessions, and

— multi-road side unit sessions.

This section describes the first and third of the operational scenarios that show how the core functions are applied as part of *C-ITS communication*.

The vehicle-originated broadcast and the infrastructure-vehicle-unicast are addressed as examples of how the core functions work in different *communication* scenarios.

The vehicle-originated broadcast *communication* scenario is used for the most time-critical and safety-critical applications such as forward collision warning, blind spot warning, emergency vehicle approach warning and overtaking (do not pass) warning.

The infrastructure-vehicle-unicast *communication* scenario is used when the infrastructure needs to respond to a specific vehicle about whether it can provide a service, for example, traffic signal priority or pre-emption, or access to a location such as a private parking facility.

These scenarios intend to give an idea of how a *C-ITS* device might go through the different algorithms for different functions. They are described at a conceptual level. The order of the steps at this level may depend on design choices at a more detailed level. This means that the order of some of the steps may change.

7.9 Vehicle-originated broadcast

Vehicles broadcast information about their movements and safety-related attributes frequently to make sure that this information is available to other vehicles so that they can identify potentially hazardous situations or in support of other applications. Typical examples are the broadcast of

— Basic Safety Messages (BSM), or

— Cooperative Awareness Messages (CAM)

which are individual single-hop broadcast V2V or V2I messages, with highest time criticality and small but frequent transactions (EU-US harmonization task force 2012a).

The scenario shows the steps for a *C-ITS* device in a vehicle to generate a message and broadcast it, and then for another *C-ITS* device in another vehicle to receive and use it. The scenario focuses on those steps performed by the core functions.

Figure 20 shows the path that the message takes from being created (step1) in the application layer to being physically sent through the (typically 5,9 GHz DSRC) antenna.

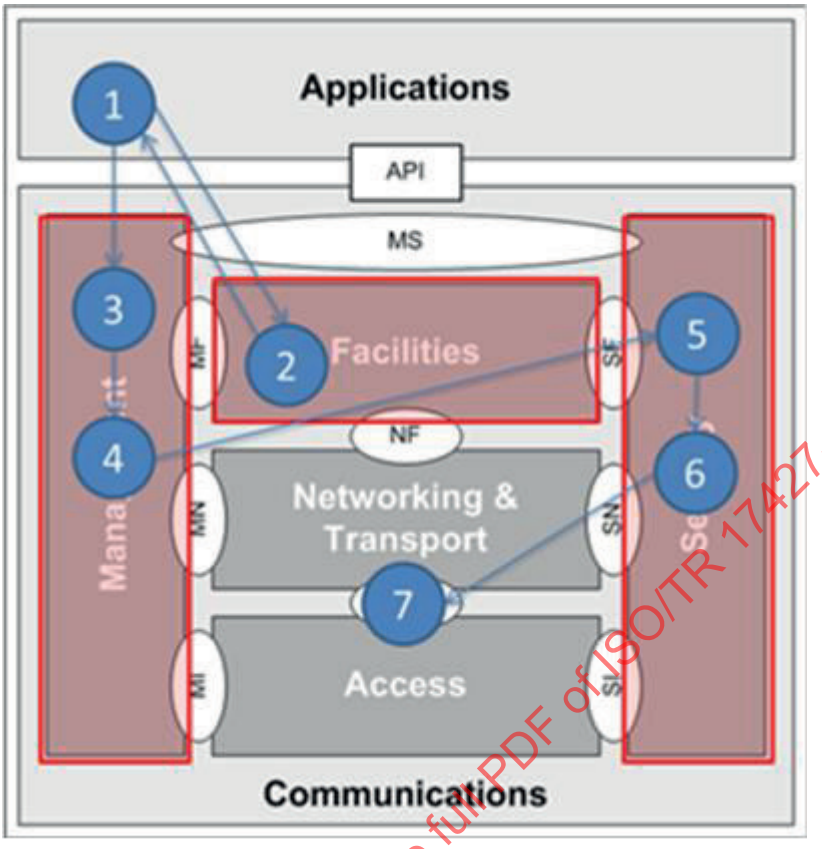

Figure 20 — Vehicle-originated broadcast scenario (sending)
[From ISO 21217 (modified)]

The steps can be describes as follows. The functional subsystem that performs this function is added in brackets.

a) Create a message, e.g. a Basic Safety Message

b) Include time stamp (Time synchronisation)

c) Monitor the status of *communication* technologies (Service monitor)

d) Select *communication* technology (Network services)

e) Confirm if allowed to broadcast BSM (User permissions)

f) Add security certificate (User trust management)

g) Send message

NOTE Not all sub systems are used in this scenario. E.g. the data distribution subsystem is not used because this is a broadcast scenario so there is no need to check if the any of possible receivers have subscribed to this type of message. The misbehaviour management subsystem is not used either. This is only used for received messages.

After the message has been broadcast, it might be received by other *C-ITS* devices from other vehicles. Figure 21 shows the path that the message takes from being received through the (typically 5,9 GHz DSRC) antenna (step1) to the usage of the message content in an application.

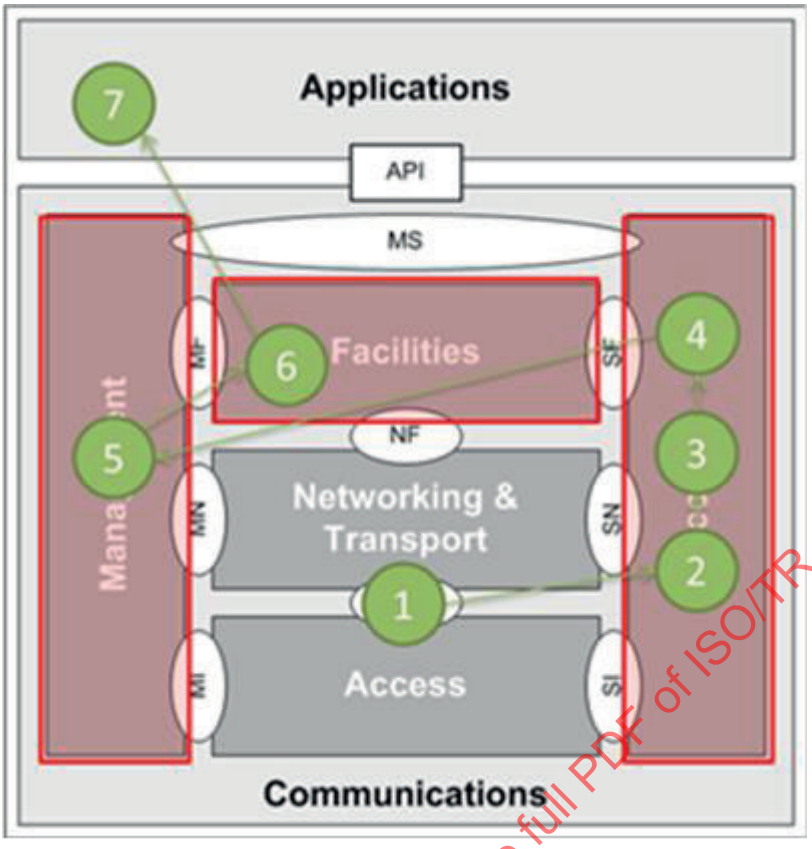

Figure 21 — Vehicle-originated broadcast scenario (receiving)
[From ISO 21217 (modified)]

The steps can be described as follows. The functional subsystem that performs this function is added in brackets.

a) Receive message

b) Check security certificate (User trust management)

c) Confirm if allowed to use BSM (User permissions)

d) Check for consistency, possibly forward to central management system (Misbehaviour man.)

e) Check if subscribed to this message type (Data distribution)

f) Check timeliness (Time synchronisation)

g) Use Basic Safety Message

NOTE The network services subsystem is not used. The network services subsystem selects the *communication* technology, which is not part of the scenario of receiving a message. Also the service monitor subsystem was not used as no service availability needs to be checked to receive and use messages.

7.10 Infrastructure-vehicle-unicast

Infrastructure-vehicle-unicast messages are individual transactions between a vehicle requesting service from the infrastructure and the infrastructure responding to that vehicle about whether it can provide that service. Typical examples of these services are

— traffic signal priority or pre-emption or

— access to a location such as a private parking facility.

These messages are generally unicast local sessions with low time criticality, low transaction frequency and small transactions (EU-US harmonisation task force 2012a).

From a security point of view, there are three ways to implement this type of *communication* scenario, being the following (EU-US harmonisation task force 2012b):

— Messages from both sender and receiver are protected using security mechanisms for broadcast.

— The first message from the *C-ITS* device in the vehicle is protected using security mechanisms for broadcast, subsequent messages are protected using security mechanisms for a session.

— All messages are protected using security mechanisms for sessions with pre-arranged keys.

This scenario described the exchange of messages which are protected using security mechanisms for a session. This means that messages are encrypted.

The scenario shows the steps for a *C-ITS* device in roadside *ITS* infrastructure to generate a message and send it to a specific vehicle, and then for the *C-ITS* device in this vehicle to receive and use it. The scenario assumes that the *communication* session has already been set up. The scenario focuses on those steps performed by the core functions.

Figure 22 shows the path that the message takes from being created (step1) in the application layer to its being physically sent through the (typically 5,9 GHz DSRC) antenna.

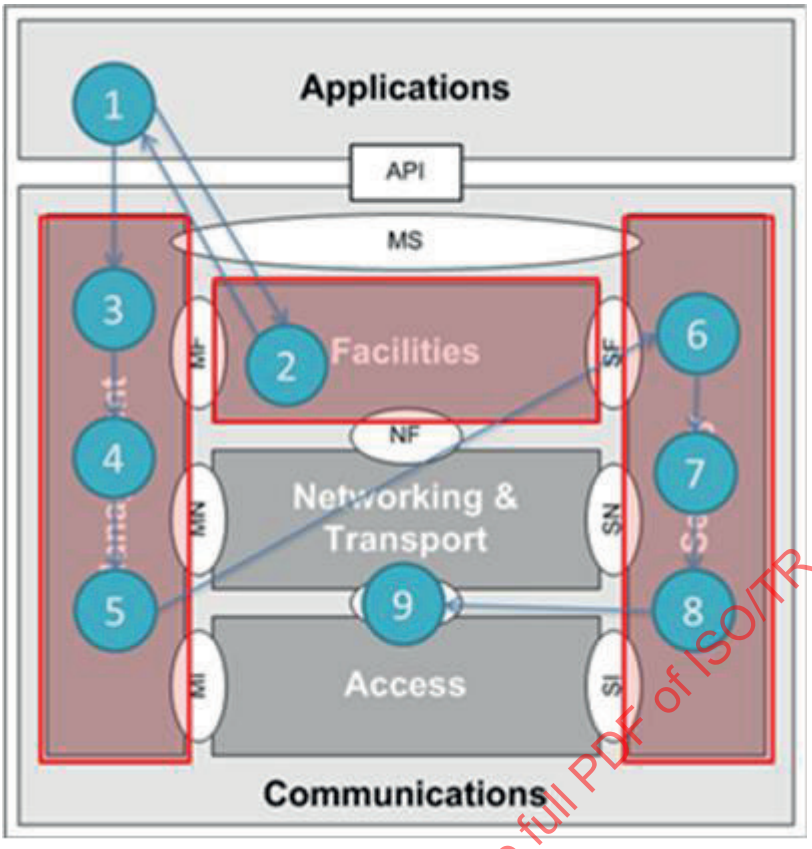

Figure 22 — Infrastructure-vehicle-unicast scenario (sending)
[From ISO 21217 (modified)]

The steps can be described as follows. The functional subsystem that performs this function is added in brackets.

a) Create message, e.g. a traffic signal priority message to confirm pre-emption for an approaching vehicle

b) Include time stamp (Time synchronisation)

c) Check if receiving vehicle subscribed to this message/application type (Data distribution)

d) Monitor the status of *communication* technologies (Service monitor)

e) Select *communication* technology (Network services)

f) Confirm if allowed to broadcast BSM (User permissions)

g) Encrypt message (User trust management)

h) Add security certificate (User trust management)

i) Send message

NOTE Similar to the vehicle-originated broadcast scenario, the misbehaviour management subsystem is not used when sending messages. This is only used for received messages.

After the message has been sent, it might be received by the *C-ITS* devices from addressed vehicles. Figure 23 shows the path that the message takes from being received through the (typically 5,9 GHz DSRC) antenna (step1) to the usage of the message content in an application.

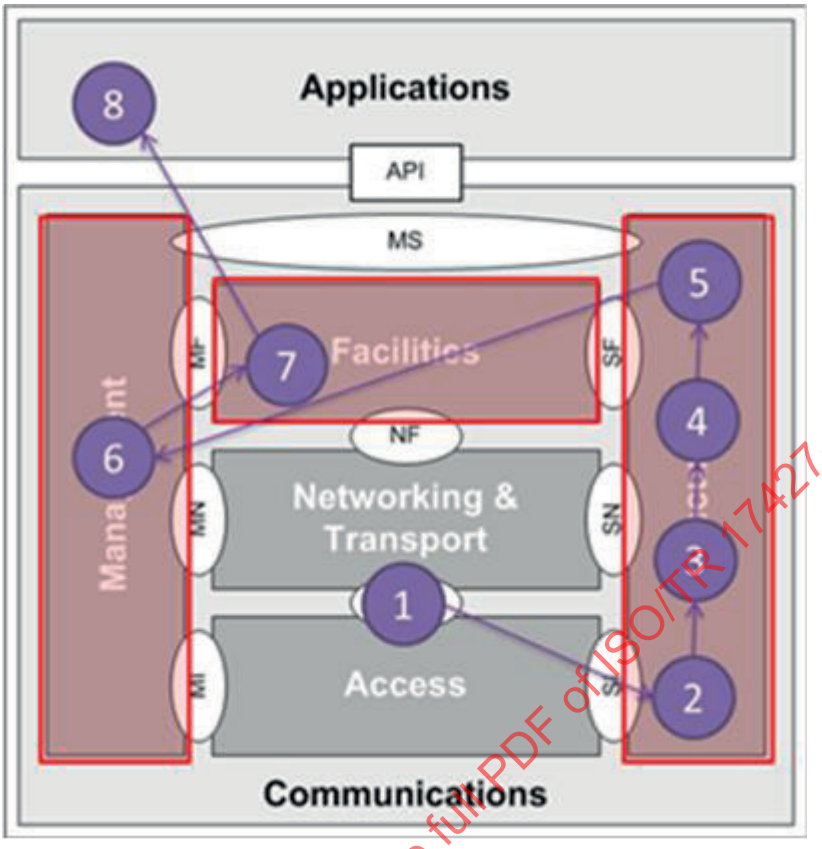

Figure 23 — Infrastructure-vehicle-unicast scenario (receiving)
[From ISO 21217 (modified)]

The steps can be described as follows. The functional subsystem that performs this function is added in brackets.

a) Receive message

b) Decrypt message (User trust management)

c) Check security certificate (User trust management)

d) Confirm if allowed to use message (User permissions)

e) Check for consistency, possibly forward to central management system (Misbehaviour man.)

f) Check if subscribed to this message type (Data distribution)

g) Check timeliness (Time synchronisation)

h) Use message

NOTE Similar to the vehicle-originated broadcast scenario, the network services subsystem is not used. The network services subsystem selects the *communication* technology, which is not part of the scenario of receiving a message. Also, the service monitor subsystem was not used as no service availability needs to be checked to receive and use messages.

7.11 Support environment

This section discusses the systems, personnel, and processes that make up the support environment for the *CorSys*. This system is different than other systems in that the support for the system is, to a large degree, part of the system.

7.11.1 Subsystems

The features in the subsystems were summarized in 7.5.10 and 7.5.11.

The service monitor subsystem provides support for the *CorSys* by maintaining efficient operations of the system, alerting operators of issues, and providing mechanisms to isolate problems, fix them, and bring the system back online.

To some degree, other subsystems such as time, user permissions or Core2Core also provide necessary functionality to complete the support environment. Beyond these subsystems that are part of the *CorSys*, there will be additional hardware and software to complete the support environment. In order to isolate, debug, fix, and test repairs to the system, a *CorSys* maintainer will need access to a hardware and software configuration representative of the configuration of the live system where the problem occurred.

The overall concept is that the *CorSys* will be based on commercially available hardware and either commercially available software or software based on open source specifications. This will minimize the impact on the maintainers of the system to have to keep unique hardware/software sets just for the new framework of safety, mobility, or environmental applications. Specifics of the actual hardware and software will be defined as the *CorSys* components are implemented.

7.11.2 Personnel

In terms of the *CorSys* support environment, the personnel supporting the system will be the maintainers, administrators, and developers identified in 7.6. In deployments where a *CorSys* is implemented by a public sector agency, some of the same system administration or maintenance personnel may be called upon to support the *CorSys*. Other configurations may involve private sector entities. A hybrid environment may exist where some devices and software are maintained by private or external agencies while others are under the control of existing organizations. In this case, agreements will need to be recorded that delineate the areas of responsibility for the maintenance of the system, including the coordination of resources to ensure that overall system availability is maintained.

7.11.3 Processes

The third component to a support environment is the establishment of processes to ensure that the systems are kept up to date and that adequate numbers of staff with appropriate skill sets are available to support the system. This includes the establishment of checklists for operators to be able to quickly isolate issues, development of repair or replacement criteria, establishment of maintenance levels and update cycles, as well as agreement on the storage, distribution, administration and supply of replacement parts or software updates.

As the *CorSys* is deployed in different locations/*jurisdictions* and probably also at different times and with different configurations of hardware and software, there will be local differences in the policies that govern the support environment. This is inevitable. The important consideration is that the *support systems* are in place, that personnel are trained and ready, and that processes are agreed upon by all of the stakeholders to maintain a functioning *CorSys*.

7.12 Disadvantages and limitations

Deploying *CorSys* is by no means a turnkey operation. This is because the *CorSys* is not a one-size fits all localities kind of system. The *CorSys* will have to be refined for each locality to meet the specific requirements of that locality. Also, it will be necessary to address what to do with existing legacy systems. It will take a long time for Core deployments to integrate with or even supplant traditional *ITS*. The challenge will be to integrate these different *CorSys* to work together within the context of standards, policy, budget, and institutional constraints.

The *CorSys* will need to monitor the performance of the *communications* networks. For example, if 5,9 GHz channels become congested during a disaster or other emergency situation, system users using 5,9 GHz need to be informed and *communications* suggestions to reroute made. Alternatively, the *CorSys* could switch to a restricted mode in an emergency condition. This would reduce its *communications*

requirements without breaking system services. Without direct access to the 5,9 GHz medium however, it is difficult for the *CorSys* to monitor that part of the *C-ITS* vehicle-highway environment. The *CorSys* needs to rely on information provided by system users that use 5,9 GHz.

System users that connect to the *CorSys* through cellular technologies will pay for that access in the form of a regular/contract fees. If the system user sees a benefit to paying for a particular type of media access, they will use that service.

8 Example use cases

8.1 General

The following scenario examples use cases describe how the system may operate, with an emphasis on *CorSys* interaction. These scenarios are illustrative, showing how the system functions, not how the given scenarios should be implemented. They do not describe the whole system, but each use case needs to be defined in the solution to be implemented.

They are broken down into four types of interactions, based on the entities involved:

— Exchange of data between system users;

— Interactions between system users and the *CorSys;*

— *CorSys* to Core interactions;

— Core System facilities operations and maintenance, including *CorSys* personnel interaction with the *CorSys*.

The example use cases below model 12 different use cases, and sometimes multiple models are included for the same scenario depending on the operational state of the *CorSys* or the system user. The multiple models may be in single or multiple diagrams but are always discussed in the accompanying text. It is important to understand that a *CorSys* is not a fixed entity, neither in the way it is instantiated, nor in the number and scope of the *C-ITS services* that it supports. It will be instantiated in different ways by different *jurisdictions*/operators, and, most importantly, it will evolve over time.

This list of use cases described below are examples, albeit of key elements of a *C-ITS CorSys*. They do not comprise the total extent of the system, and more will be added (and need to be characterized) over time. The extent of any instantiation of a *ConOps* for a '*C-ITS CorSys* will therefore be a 'living' document, that will need to be revised as the system evolves, and new use cases will need to be characterized and their behaviour and management by the *CorSys* characterized and codified as they evolve.

Within this high level *ConOps*, the use cases are described texturally with the support of high level figures. In a deployment, the principal anticipated use cases should be supported by context diagrams describing the inputs (data, existing relationships, user input), enablers (involved Core subsystems, *Communications* Layer, relationships between *CorSys* and other entities) and controls (policies, constraints) that feed into the *CorSys*, and itemise and characterize the outputs that are produced. Activity diagrams, drawn using Systems Modelling Language (SysML, an extension of Unified Modelling Language (UML)), UML (ISO/IEC 19501), 'Open Distributed Processing' (ISO 10746), or similar are recommended to support and characterize the use cases and describe the interactions between system users, *CorSys* personnel and core subsystems.

The 'Core2Core' subsystem is involved in many of these scenarios, but it is only shown when it provides functionality beyond simple connectivity with other *CorSys*.

Similarly, the 'Network Services' subsystem is technically used in every scenario where a system user or other *CorSys* interacts with the *CorSys*, but is implicit rather than described.

Core trust relationships are listed as enablers for many of these scenarios. These refer to the relationships established between managers and operators of *CorSys* which enable interactions between the respective Core2Core subsystems.

8.2 Example Use Case (1): User data exchange

There are three basic types of data exchange.

— One system user uni-casting or geo-casting data that it wants other users to access;

— One system user providing data directly to another user that it can specifically address;

— One system user providing data to the *CorSys* for retransmission to a group of users.

In this example use case, system user data broadcasts are made via *ITS-station*s. This form of data exchange does not directly involve the *CorSys*. However, messages that are signed or encrypted rely on credentials issued by the *CorSys* or an ESS. So while the messages do not pass through the *CorSys*, senders and receivers rely on Core services in order to encrypt, decrypt and/or trust the messages.

Data Providers providing data to more than one Data Consumer may rely on the *CorSys* 'Data Distribution' service to facilitate the distribution of data to multiple recipients. The *CorSys* does this through two distinct activities:

a) Provide a subscription service for a data subscriber, telling it what data are available, and if the data subscriber is qualified (again, according to *CorSys* local policies) to register the subscriber to receive data. Data exchange could be through the *CorSys* or it could be direct from provider to subscriber, again depending on local policies, capacities and whether anyone besides this particular data subscriber wants the data. Example use case 5 describes a subscription scenario.

b) Provide a distribution service, where registered data providers send data to the *CorSys*, which publishes that data to one or more subscribed data subscribers. The context diagram describing this data distribution is shown in Figure 24.

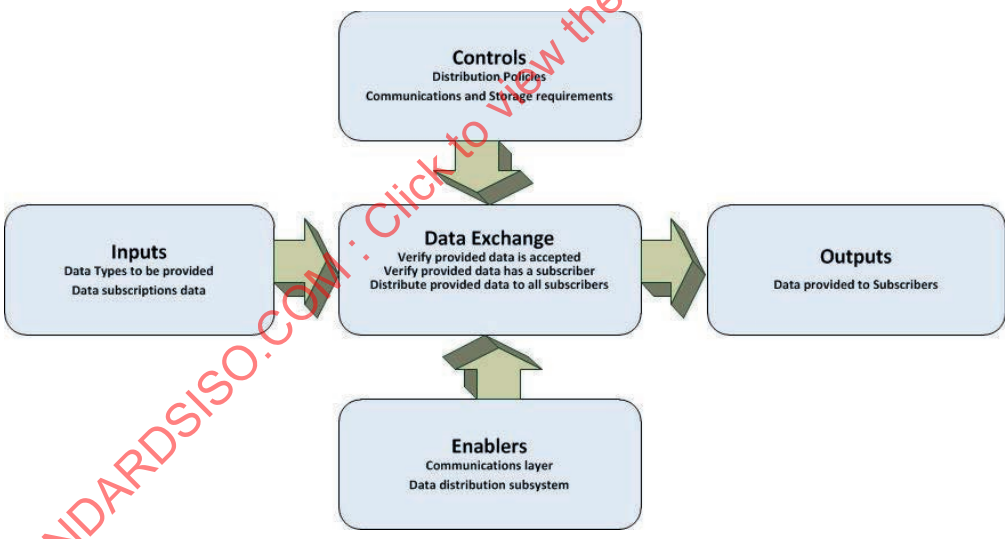

Figure 24 — User data exchange context diagram

Data are provided to the *CorSys* by a system user. If the data are not of a type that the *CorSys* accepts, it provides a message to the system user indicating it does not accept this data. If the data is accepted by the *CorSys*, and if the *CorSys* has subscribers to this type of data, then it publishes the data to the subscribers. Data can be anything, but primarily the following:

— Data provided by mobile users will typically include probe data describing the operating conditions sensed by the vehicle carrying the mobile user device or by the device itself. (See SAE J2735.)

— Data provided by *centre* users will include advisory or alert information.

— Data provided by field users will be traffic or environmental data.

The publication step may include parsing, sampling, and aggregation functions. Parsing is where the *CorSys* examines each packet of data, extracts the elements that subscribers are interested in, and provides only those elements to the subscribers. Sampling is where the *CorSys* provides a percentage of the data that subscribers are interested in; for example, a 1:10 sample would see the *CorSys* providing one data packet to a subscriber for every 10 received from providers. Aggregation is where the *CorSys* combines multiple like data packets, summarizes the data within, and retains all information but reduces the amount of data sent to each subscriber. For instance, if the *CorSys* received 5 speed measurements of 30 mph in a given area, it would provide a data packet stating that there are 5 instances of 30 mph in that area.

In the special case where a registered data provider is sending data directly to a third-party because the Core does not support distribution of the data that the system user provides, and the *CorSys* is upgraded to provide such distribution, there needs to be a mechanism for notifying data providers of this change. See use case 11 for an example of this case.

8.3 Example Use Case (2): Certificate distribution

Certificates can be viewed as the 'entry ticket' in order to use the system services. This scenario describes how system users interact with a *CorSys* to get a new certificate. This scenario addresses certificates distributed by the *CorSys* and also certificates distributed by an ESS.

As shown in the context diagram (Figure 25), the primary activities are verifying previous behaviour, verifying permissions, and issuing new certificates. If the certificates are managed by an ESS, then the *CorSys* involvement is limited to providing the system user with the contact information of the ESS.

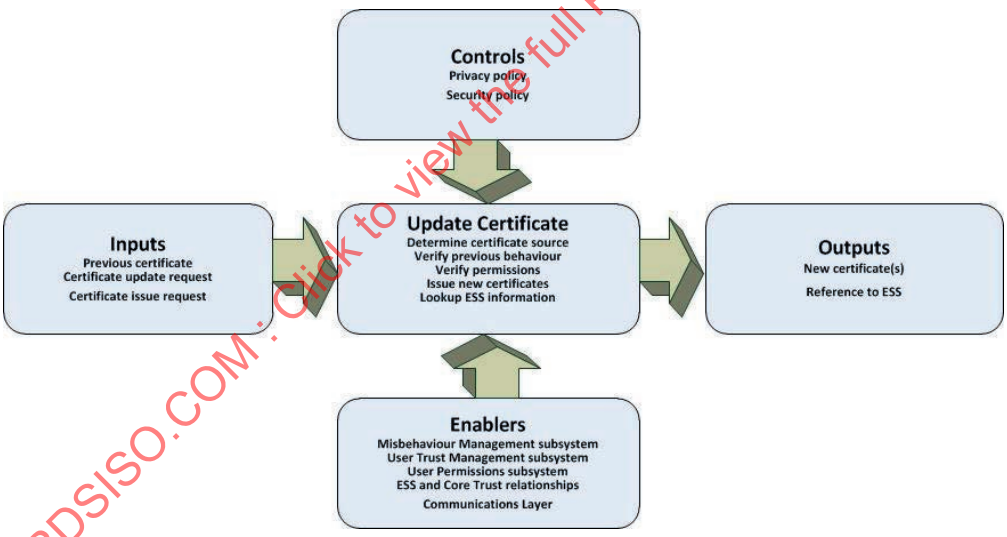

Figure 25 — Certificate distribution context diagram

A system user typically provides a request for a certificate to the *CorSys*, including any desired special permission information, its current certificate and a unique identifier associated with the request. All of this information may already be included in the certificate used by the system user, but if it is not, it needs to be included as part of the message.

If the *CorSys* provides the type of certificate that the system user is requesting, it will service the request. An improperly formatted request will result in a misbehaviour report and response to the originator but no certificate. A request sent using a certificate on the 'Certificate Revocation List' will generate a misbehaviour report and termination of the activity flow.

8.4 Example Use Case (3): Certificate revocation list distribution

This scenario addresses the distribution of 'Certificate Revocation Lists' to system users, including those maintained by the *CorSys*, those maintained by other *CorSys*, and those maintained by ESS.

The context diagram for 'Certificate Revocation List' distribution is shown in Figure 26.

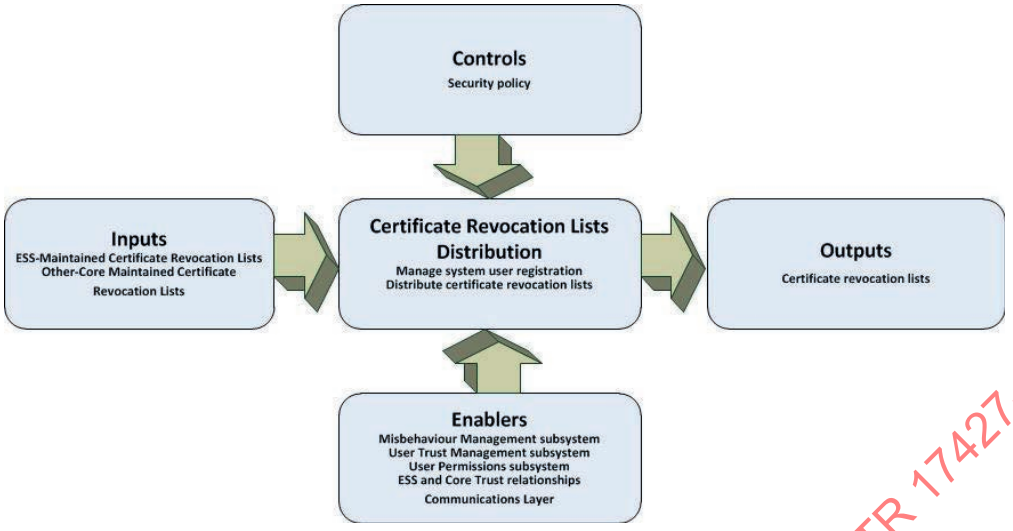

Figure 26 — Certificate revocation list distribution context diagram

The *CorSys* stores and distributes 'Certificate Revocation Lists' that it maintains, as well as those it acquires from other *CorSys* and ESS. System users receive 'Certificate Revocation Lists' by registering with the *CorSys* to receive a regular distribution of 'Certificate Revocation Lists'. This means that anonymous users and mobile users that do not have persistent *communications* to the *CorSys* will not receive 'Certificate Revocation Lists'. Other mechanisms outside of the *CorSys* are planned to provide this information however. Mobile users can receive 'Certificate Revocation Lists' from nearby field users (for example, as documented in IEEE 1609.2).

There are three distinct processes involved.

a) The *CorSys* acquires 'Certificate Revocation Lists' from external sources. This acquisition may be a query-response or a periodic distribution, depending on the other *CorSys* or ESS implementation.

b) The *CorSys* provides a registration interface to system users and other *CorSys*, enabling the system user or *CorSys* to register for 'Certificate Revocation List' distribution.

c) The *CorSys* distributes 'Certificate Revocation Lists' to all *CorSys* and system users that are registered to receive them.

NOTE The Core2Core subsystem is involved in establishing and maintaining the relationships the *CorSys* has with other *CorSys*.

8.5 Example Use Case (4): Misbehaviour action: Certificate revocation list addition

Certificates can be revoked if the *CorSys* determines they are being used in a fashion incompatible with approved uses. There are two ways to have certificates revoked:

— *CorSys* personnel can manually revoke a certificate by placing it in the certificate revocation list;

— the 'Misbehaviour Management' subsystem can automatically revoke certificates based on a policy.

If the certificate in question is managed by an ESS, then the *CorSys* notifies the ESS to place the certificate in the 'Certificate Revocation List'.

The context diagram for Certificate Revocation List Addition is shown in Figure 27.

