ETSI TR 103 903 V2.1.1 (2026-03)

TECHNICAL REPORT

Intelligent Transport Systems (ITS);
Framework;
Basic principles;
Release 2

Reference
DTR/ITS-232

Keywords
ecosystem, ITS, system

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the
ETSI Search & Browse Standards application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on ETSI deliver repository.

Users should be aware that the present document may be revised or have its status changed, this information is available in the Milestones listing.

If you find errors in the present document, please send your comments to the relevant service listed under Committee Support Staff.

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure (CVD) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2026.
All rights reserved.

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Intelligent Transport Systems (ITS).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The present document is intended for users and writers of the ETSI ITS deliverables e.g. technical specifications and reports. It provides instructions and guides users how to relate ETSI ITS deliverables. For writers it provides structure and guides in how to realize consistent ETSI ITS deliverables.

The ITS Framework identifies what is part of the ITS domain. It provides guidance in the ETSI ITS standardization process for the purpose of realizing consistency among the ETSI ITS standards and hence improve conformity and interoperability. Where applicable it also identifies backward compatibility.

The present document addresses the following aspects:

- It provides context to the set of ETSI ITS deliverables and their possible use;
- It provides guidelines and best practices extending the ETSI Drafting Rules [i.3] to achieve a high level of consistency among the documents within ETSI ITS;
- It provides an ETSI ITS documents relation structure including the relations among documents inside of an ETSI ITS Release, but also the relation between different releases;
- It provides guidance on how ETSI ITS deliverables can be used, and on their lifecycle.

The present document is one of the three framing documents of an ETSI ITS release. The other two framing documents are:

- ETSI TR 101 607 [i.1], which lists all ETSI ITS deliverables part of a specific Release. This report can be seen as the starting point for readers to find all relevant documents for a specific release, including the other framing documents.
- ETSI TR 103 902 [i.2], which includes all common terms, symbols and abbreviates relevant for a specific release.

1 Scope

The present document identifies the ITS domain and its elements. It provides the ITS architectural and ecosystem context. The present document complements and extends the ETSI drafting rules [i.3] and identifies consistency aspects related to the protocol stack layering and referencing between the ITS specifications and other documents. Further, it provides the ETSI ITS deliverable structure.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI TR 101 607: "Intelligent Transport Systems (ITS); Cooperative ITS (C-ITS); Release 1".

[i.2] ETSI TR 103 902: "Intelligent Transport Systems (ITS); ITS Framework; Terms, Symbols and Abbreviations; Release 2".

[i.3] ETSI Drafting Rules.

[i.4] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[i.5] Car Connectivity Consortium's MirrorLink.

[i.6] Fransman, M. (2010): "The new ICT Ecosystem: Implications for policy and regulation". Cambridge, UK: Cambridge University Press. Gillwald, A. (2012). Review of department of communications' colloquium on an integrated national ICT policy. Research ICT Africa.

[i.7] "The Roadmap for Open ICT Ecosystems", citation 2005.

[i.8] ISO/IEC 27001:2013: "Information technology — Security techniques — Information security management systems — Requirements".

[i.9] Directive (EU) 2023/2661 of the European Parliament and of the Council of 22 November 2023 amending Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport.

[i.10] ETSI EN 302 665 (V1.1.1): "Intelligent Transport Systems (ITS); Communications Architecture".

[i.11] ISO 26262-9:2018: "Road vehicles — Functional safety, "Part 9: Automotive safety integrity level (ASIL)-oriented and safety-oriented analyses".

[i.12] ISO/IEC 7498-1: "Information technology - Open Systems Interconnection - Basic Reference, Model: The Basic Model".

[i.13] ETSI TS 103 723: "Intelligent Transport Systems (ITS); Profile for LTE-V2X Direct Communication".

[i.14] Data For Road Safety (DFRS).

[i.15] National Access Point Coordination Organisation for Europe (NAPCORE).

[i.16] C-Roads Profile 1: "Release 2.0 of C-ROADs harmonised C-ITS specifications".

[i.17] C2C-CC_RS_2037: "Basic System Profile (BSP)".

[i.18] DATEX II: "DATEX II is the reference data standard in Europe for road traffic and travel information".

[i.19] ETSI standard skeletons.

[i.20] ISO/IEC 10746: "Information Technology - Open Distributed Processing - Reference Model: The Open Group Architecture Framework" (TOGAF)".

[i.21] ETSI TS 103 544 (all parts): "Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); MirrorLink®; parts 1-24".

[i.22] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)".

[i.23] EU CCMS: "European Commission to support the deployment of C-ITS services within the European Union C-ITS Security Credential Management System (EU CCMS)".

[i.24] Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport".

[i.25] Commission Delegated Regulation (EU) No 886/2013 of 15 May 2013 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to data and procedures for the provision, where possible, of traffic safety-related minimum universal traffic information free of charge to users (SRTI).

[i.26] Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services (RTTI).

[i.27] Commission Delegated Regulation (EU) 2022/670 of 2 February 2022 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services (NAPS Regulation).

[i.28] CEN/TS 17268:2018: "Intelligent transport systems - ITS spatial data - Data exchange on changes in road attributes".

[i.29] DFRS technical document: "Increasing road safety by sharing road safety related data in public and private cooperation".

3 Definition of terms, symbols, and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

backward compatibility: ability of a newer system to interoperate with an older system

NOTE: An ITS-S based on Release x+1 (Rx+1) is backward compatible with Release x when, Rx+1 is able to obtain the same level of services of a Rx station in an environment based on Rx, and Rx+1 is specified in a such a way, that C-ITS stations implemented based on Rx is able to maintain its full functionality in an environment based on Rx+1.

component: concrete part or element that contributes to the function of a larger system, including hardware (like CPUs and hard drives), software (such as operating systems and applications), and other elements like data, procedures

data: raw facts, figures, statistics or bytes

domain: area or interest

NOTE: If used in the context of communications, refers to any group of users, workstations, devices, printers, computers and database servers that share different types of data via network resources.

ecosystem: concept in which technical systems e.g. information, technologies, applications, are considered in their user and environmental context e.g. policies, strategies, and organizational processes

enterprise architecture: architecture of a complete organization, the top-level architecture

NOTE: It recognizes general aspects, mission, objectives, organization considering common aspects often identified as part of the ecosystem requirements.

entity: abstract thing that exists, did exist, or can possibly exist, including associations among these things

ERRATA document: document listing of errors discovered in a published work, along with their corrections

equipment: set-up of hardware, software, data and the actor(s) who use them

functionality: generalized function which can consist of many components, processes and can have many interfaces

NOTE: It can be also composed of many more specific functionalities. The term is functional and not technically used.

information: data with specific meaning

ITS-S application: fragment of an ITS application available at an ITS station that uses ITS-S services to connect to one or more other fragments of the same ITS application

ITS-S service: functionality or a group of functionalities offered by an ITS-S to other ITS-S services or to an ITS application

ITS service: service provided by an ITS application to the user of ITS

ITS station: functional entity specified by the ITS station (ITS-S) reference architecture

ITS sub-system: sub-system of ITS with ITS components for a specific context

metadata: data about data, that provides context and makes it easier to find, use, and manage information

misbehaviour: act by which a C-ITS station transmits false or misleading information, or information that was not authorized by a commonly agreed policy, either purposefully or unintendedly

Multi-Model: multimodal transport (also known as combined transport) is the transportation of goods or people realized by least two different modes of transport

networking configuration: method in which there is a physical or virtual process of assigning network settings, polities, flows and controls such as an IP networks

networking constellation: method in which there is no configuration process but where the network settings, policies, flows and controls are commonly at system level agreed

party: singular individual, stakeholder, organization, governmental institution or business entity

prescriptive document: document that specifying specific requirements to which other documents within a certain context need to comply to

private: organizations which are owned, controlled and managed by individuals, groups or business entities

protobuf: protocol buffer, a free and open-source cross-platform data format used to serialize structured data

public: organizations which are owned, controlled and managed by governmental or other state or locally managed bodies

repository: central location where things are stored, which can be a physical place like a storage facility or a digital space like a computer server

representational state transfer: HTTP request to a server, and the server processes it and sends back a corresponding HTTP response according to the request/reply client-server communication model

safety related: everything which can have a direct or indirect positive impact on the safety situation

scheduling: process in which decisions are made about through what specific technology, timing, delay or prioritization and by which parameters the dissemination should happen

NOTE: This definition needs to be reviewed when implemented in the related document.

sink: type of computer program or device that collects, stores and possibly processes data from other devices, programs or sources

solution architecture: architecture practice designing functionalities or specific system addressing specific ecosystem requirements, integrating various components/logic that governs them, and the information associated with them

source: location where data originates from

strategical: information which brings awareness about possible upcoming safety situation to be managed. (there is no direct impact)

tactical: information or processes which have direct impact on the cause of action as a response to immediate situation

technical architecture: architecture providing the description of technical components; their relations and the data associated with them

NOTE: At the higher level, the technical architecture shows the relations of software and hardware architectures and can have a direct relation with solution architectures when considering systems.

V-model: graphical representation of a systems development lifecycle

NOTE: See Wikipedia®: https://en.wikipedia.org/wiki/V-model.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

5G-NR	5th Generation New Radio
AD	Automated Driving
ADAS	Advanced Driver Assistance Systems
AID	Application Identifier
AL	Access Layer
ALI	Access Layer Instance
ASIL	Automative Safety Integrity Level
ASN	Abstract Syntax Notation
B2B	Business to Business
BSP	Basic System Profile
BTP	Basic Transport Protocol
CAM	Cooperative Awareness Message
CAS	Cooperative Awareness Service
CC	Congestion Control
CCC	CarConnectivity Consortium
CCMS	C-ITS Security Credential Management System

CDD	Common Data Dictionary
CIA	Confidentiality, Integrity and Availability
C-ITS	Cooperative Intelligent Transport Systems
CPU	Central Processor Unit
DATEX	Data Exchange
DFRS	Data For Traffic Safety
DLL	Data Link Layer
DPIA	Data Protection Impact Assessment
DSRC	Dedicated Short-Range Communication
EA	Enterprise Architecture
EN	European Norm
EU	Europe
FL	Facilities Layer
GDPR	General Data Protection Regulation
HMI	Human Machine Interface
HSM	Hardware Security Modules
HTTPS	Hypertext Transfer Protocol Secure and is the encrypted version of HTTP
I2X	Infrastructure to Everything
IBM	Information Basic Model
ICT	Information and Communications Technology
ID	Identifier
IP	Internet Protocol
IT	Information Technology
ITS	Intelligent Transport Systems
ITS-S	Intelligent Transport Systems Station
JSON	JavaScript Object Notation
LDM	Local Dynamic Map
LLC	Logical Link Control layer
LTE	Long-Term Evolution
MAC	Media Access Control
MDM	Mobility Data Marketplace
MIB	Management Information Base
NAP	National Access Point
NAPCORE	National Access Point Coordination Organization For Europe
NL	Netherlands
NTL	Networking & Transport Layer
OBU	On Board Unit
OS	Operating System
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
PHY	Physical Layer
PoTi	Position and Time
PTW	Power Two-Wheeler
PVD	Probe Vehicle Data
REST	Representational State Transfer
R-ITS	Road-ITS
RM	Resource Management
SA	Service Announcement
SAM	Service Announcement Message
SAP	Service Access Point
SAS	Service Announcement Service
SCMS	Security Credential Management System
SDO	Standardization Development Organization
SDU	Service Data Unit
SIB	Security Information Base
SNMP	Simple Network Management Protocol
SOA	Service-Oriented Architecture
SP	Service Provider
SPS-NL	Safety Priority Service Netherlands
SRTI	Safety Related Traffic Information
SSL	Secure Sockets Layer
SSP	Service Specific Permissions

TA	Technical Architecture
TC	Technical Committee
TISA	Traveller Information Service Association
TLS	Transport Layer security
TOGAF	The Open Group Architecture Framework
TPEG	Transport Protocol Experts Group
TR	Technical Report
TS	Technical Specification
TVRA	Threat and Vulnerability Risk Assessment
U-ITS	Urban rail-ITS
UML	Unified Modelling Language
V2X	Vehicle to Everything

4 The ITS Context

4.1 In general

The purpose of communication standardization is to enable participants in the communication, to exchange data in a conform and interoperable way. Such standardization encourages competition in an open market, as referred to in European single market Regulation (EU) 2022/2065 [i.4]. The development of standards requires the understanding not only of functional and technical requirements but also understanding about the context such as business context, realization context, trust and regulations in which these are used. Ecosystem requirements lead to additional requirements and to additional standards (see ecosystems, clause 4.4).

4.2 The ITS Communications Domain

Intelligent Transport Systems (ITS) are systems that combine and apply ICT and electromechanical technologies with the intend to improve traffic flow, traffic safety and transport efficiency. In principle, it covers transport systems for road, water and rail covering e.g. logistics, fleet resource management, traffic information, emergency/police, public transport, road user services, navigation user services and safety user services.

The ITS Communications Domain is depicted in Figure 1 and related ITS standardization evaluates and specifies ITS communication aspects including functional and technical requirements for the purpose of realizing interoperable information exchange between different ITS equipment. At present, other functional and technical aspects such as ITS related equipment internal sensor interfacing, and functionalities are out-of-scope of ITS Communications Domain.

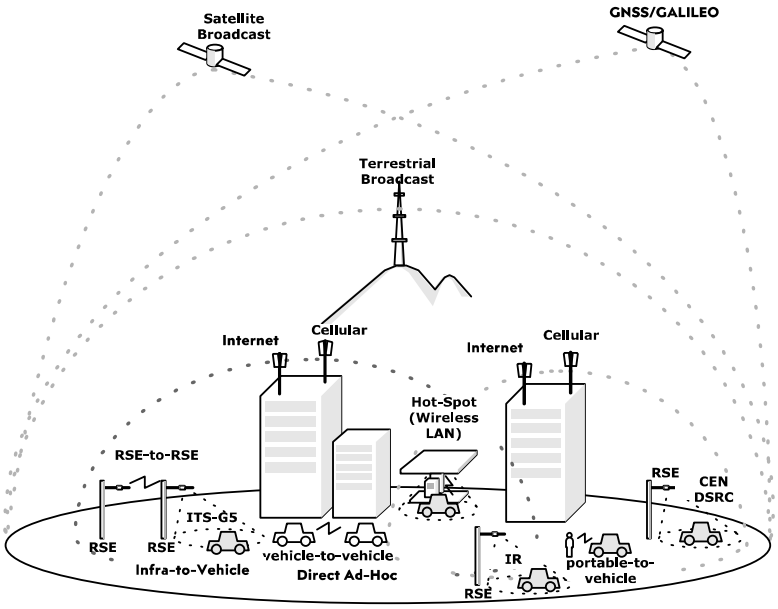

Figure 1: ITS Communications Domain

Although not all types of road users are identified in Figure 1, ITS communications also apply to all road users e.g. Vehicles, Power Two Wheelers (PTW), Bicyclists, Pedestrians, Trams, Trains and Special Users such as people with disabilities and emergency services. Besides the road users, ITS information is usually also exchanged with authorities, infrastructure providers and businesses. An ITS service (see clause 4.5) is able to realize a single or multiple use cases simultaneously. The equipment supplier as well as the operator are free to choose how to configure their ITS equipment and how user services should look like. At present, the look and feel of equipment and services are out of scope.

4.3 ICT architectures

In Information and Communication Technologies (ICT) the following architectural levels are defined, allowing users to identify related communication requirements.

The Open Group Architecture Framework (TOGAF) ISO/IEC 10746 [i.20]) defined three main architecture types.

- Enterprise Architecture (EA) level. This is the high-level view that defines how the ICT strategy aligns with business goals, encompassing all aspects of the organization's ICT systems and their business objectives. This is often used to describe the overall ICT ecosystem within a specific context, such as a smart city or a large corporation.
- Technical Architecture (TA) level. This is a more detailed view that specifies the technology standards, protocols, and products used to implement the functions and layers of the ecosystem.
- Solution Architecture (SA) level. This level focuses on the architecture of a specific solution or project within the broader enterprise architecture, an architecture specific for a specific business case for example.

The EA recognizes general aspects, mission, objectives, organization considering common aspects often identified as part of Ecosystem requirements. It has a role within organizations and therefore could be of relevance to profiles but is not of relevance to standardization except for those functional and technical aspects impacting interoperability and conformity as recognized part of any ITS Ecosystem (see clause 4.4).

4.4 Ecosystems

4.4.1 Introduction

ITS ecosystems encompass all ITS related policies, strategies, processes, information, technologies, applications, and stakeholders that together make up the requirements, and it is realized in a specific trusted technical environment for a country, region, government, or enterprise.

Most importantly, an ICT ecosystem includes people - diverse individuals who create, buy, sell, regulate, manage and use technology (The Roadmap for Open ICT Ecosystems, Citation 2005, [i.7], but also Fransman [i.6]).

ITS ecosystems are closed systems in which information is exchanged based on predefined social, business and legal requirements, including trust, security and governance models. An ecosystem is always limited as it cannot encompass every possibility and cannot satisfy all stakeholders, social, business and legal requirements at the same time, therefore, it is specific for a certain objective or use.

To enable enterprise possibilities on the internet, the Internet Protocols are in continues development, enabling more and more advanced business process possibilities extending Internet services. The internet has become an open environment in which new services and new business can be developed based on existing ICT building blocks, processes, methods, principles, protocols and tools.

Fransman (2010) and Gillwald (2012) [i.6] described it conceptually as the "Open ICT ecosystem framework" (Figure 2). As stated, it is a framework enabling any stakeholder group interested in the same or similar functional area, trust, social, legal and or business areas can realize their ecosystem based on available ICT building blocks and where needed extend it with new building blocks and processes. The fundaments for this framework can use various ICT communication architectures.

ITS ecosystems comply to this ICT ecosystem Framework. Some make use of many, or all identified "Open ICT ecosystem framework" building blocks and others could be based on only a subset of these building blocks.

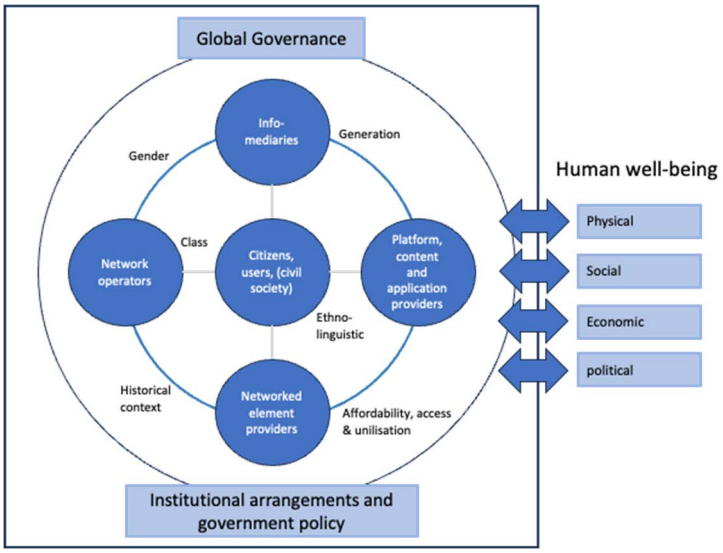

Figure 2: The "Open ICT ecosystems Framework"

4.4.2 ITS ecosystems

4.4.2.1 Introduction

Within ITS there are various ITS ecosystems in operation e.g. Traffic light infrastructure systems, Tolling systems, Logistics systems and safety related ITS.

The present ETSI ITS releases (Release 1 and 2) do not cover the above mentioned ITS ecosystems but focus on safety related ITS ecosystems e.g. road traffic safety and road traffic efficiency ITS ecosystems.

Compared to the other ITS ecosystems, safety related ITS ecosystems put more functional and technical critical requirements on to the ITS system, in particular on security and communication system requirements. Often these requirements are assessed through standard assessment methods such as Threat and Vulnerability Risk Assessments (TVRAs) and Data Protection Impact Assessments (DPIAs). For example, for DPIA the ISO 27001 [i.8] could be used.

At present for Europe, three safety related ITS ecosystems can be identified:

1) the C-ITS ecosystem for which the basic aspects are laydown by the European Union (EU) regulation framework formed by the Directive 2010/40/EU [i.24] and its amendment (EU) 2023/2661 [i.9];

2) the Data for Traffic Safety (DFRS) ecosystem [i.14]; and

3) the European National Access Point Coordination Organisation for Europe (NAPCORE) [i.15] ecosystem.

The minimum requirement for these three ecosystems is that they support the Commission Delegated Regulation (EU) No 886/2013 (SRTI) [i.25].

In the following clauses these differentiating ITS ecosystems are highlighted. Starting with the C-ITS ecosystem as this is the one which was the first to be supported by ETSI ITS Release 1 standardization.

4.4.2.2 The Cooperative-ITS (C-ITS) ecosystem

As referenced, the C-ITS ecosystem is defined by Directive (EU) 2023/2661 [i.9] and its amendment (EU) 2023/2661 [i.9]. As such the term C-ITS when used in the domain of ITS in Europe, is legally limited to what is defined by this EU regulation. The C-ITS ecosystem is intended to increase traffic safety and traffic efficiency. With regards to Traffic Safety, it supports the Commission Delegated Regulation (EU) No 886/2013 (SRTI) [i.25] extended with safety related ADAS and AD use cases.

The C-ITS ecosystem uses a reduced ICT ecosystem framework and uses non-IP based information exchange protocols with specific functional requirements, common criteria and security criteria. Non-IP C-ITS packages (including security) can be exchanged via open IP based network as long as the C-ITS packet is not unpacked.

The Directive 2010/40/EU [i.24] and its amendment (EU) 2023/2661 [i.9] form the fundament for the C-ITS services. In this regulation framework C-ITS is defined as "intelligent transport systems that enable ITS users to interact and cooperate by exchanging secured and trusted messages, without any prior knowledge of each other and in a non-discriminatory manner".

C-ITS information sharing is characterized as tactical information sharing, as the related information sharing is direct impact oriented, requiring direct course of action as a response to immediate situation, which is the case for timely critical (around 1 second) safety-relevant or safety-critical use cases, such as for ADAS and Automated Driving (AD). Besides tactical also strategical information sharing can be recognized. Strategically shared information is primarily intended to be used for warning use cases and generally is shared at least several seconds before impact.

Tactical information sharing comes with more stringent functional and technical requirements, for instance more stringent data quality then the requirements coming with strategic information sharing. Tactical information sharing could be of benefit for strategic use cases, while strategic information sharing mostly cannot be used for ADAS and AD functions.

NOTE: The information shared for a use case such as "Queue ahead" when having sufficient data quality to serve tactical actions, also has value for further away traffic as they could change their route to their final destination.

The present European regulatory framework is supported by ETSI ITS Release 1 standards and following ETSI releases.

As Tactical intended information is openly shared it should be ensured that the data shared does not reveals any information about the source which could compromise its role, state or legal position as identified by the European General Data Protection Regulation (GDPR) Regulation (EU) 2016/679 [i.22]. For this reason, the C-ITS Ecosystem includes specific functional and security measures to ensure required trust and privacy levels. For Europe, the EU Directive (EU) 2023/2661 [i.9] related certification and security policies are referenced and elsewhere under EU regulation specified.

C-ITS message specifications comply to the C-ITS Ecosystem trust, liability and safety integrity, functional safety and legal requirements e.g. Functional Safety Integrity Level (ASIL) levels laid down in the ISO 26262-9:2018 [i.11].

For Strategical intended information other communications then direct V2X communications can be used as long as the use is compliant with existing legal frameworks and installed certification and security policies.

Most of the C-ITS specifications refer to ETSI ITS standards but also to CEN/ISO standards there were applicably. ETSI ITS Releases support the realization of C-ITS equipment.

When projecting C-ITS Ecosystem on the Fransman (2010) and Gillwald (2012) [i.6] Ecosystem model (Figure 3), it can be recognized that the number of active actors is very limited compared to other ITS Ecosystems.

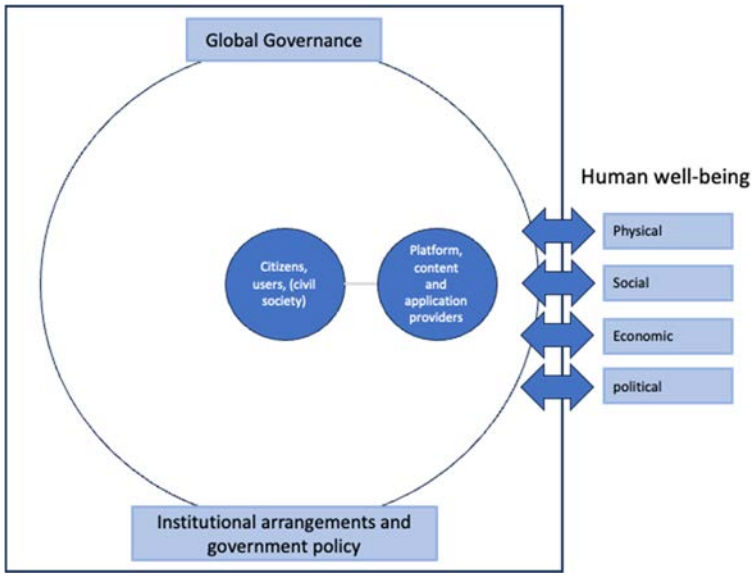

Figure 3: C-ITS ecosystems Framework

4.4.2.3 The DFRS ecosystem

At present Data for Traffic Safety (DFRS) [i.14], facilitated by ERTICO, has defined their DFRS ecosystem in their technical specification [i.29]. The Commission Delegated Regulation (EU) No 886/2013 (SRTI) [i.25] is realized not only by DFRS [i.14] but also by NAPCORE [i.15], C-ROADS [i.16] and C2C-CC [i.17].

The DFRS ecosystem as defined in [i.29] (see also Figure 4) is an answer to the SRTI regulation by the industry, facilitating SRTI strategic information exchange. It is a typical IP protocol based "Open ICT ecosystems Framework" Enterprise Architecture (EA).

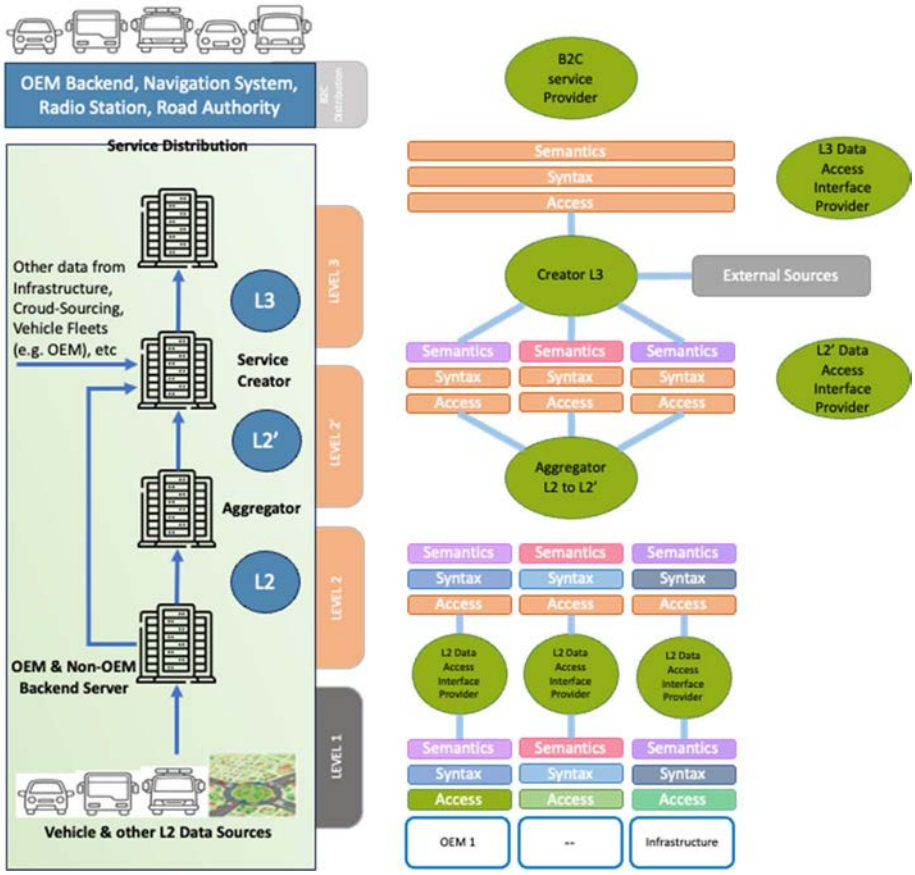

Figure 4: The DFRS ecosystem

The DFRS typical EA architecture is characterized by the following aspects:

- It is a Service providers architecture with information providers, information aggregators, service providers, service distributors and service users.
- Data sets are classified in the L2 Data; L2' Data and L3 Data categories. At all categories various data standards are used. At the L2 lever the number of used data standards is higher than on the L3 level. At present DATEX II is specified for L3 but it is not normatively specified. As DATEX II is not interoperable at present coding schemes are investigated. For category L2, SENSORIS is reference but also here there is no interoperable encoding defined, and it is open to use others.
- There is also no single access technology and message encoding selected, it depends on the interface used between each of the partners in the B2B interfaces selected. At present the DFRS technical specification [i.29] states the following about this: "It needs to be distinguished between the data format of the actual content (i.e. how are the messages encoded) and the access technology. Throughout the DFRS ecosystem, there are various access paradigms usable, ranging from request/ reply REST like access schemes towards streaming like access schemes like HERE's Open Location Platform. REST interfaces typically offer ASCII-JSON and binary protobuf as message encoding, whereas streaming like access schemes often provide binary protobuf only."

- DFRS has defined a metadata repository - Mobility Data Marketplace (MDM) where partners (B2B) can find which information is available where and in what format, metadata for the data access interfaces needs to be made available to all partners. Since not all data access interfaces are public, a protected, DFRS Ecosystem partner internal metadata repository is required. For now, all metadata is to be made available at the MDM (Mobility Data Marketplace) repository. This is the German NAP and currently acts as an intermediate solution. The following is the step-by-step instruction for creating so-called "data publications" (metadata for one data access interface) within the MDM.

- In order to be able to enter and edit metadata in the MDM, certification is required. The MDM operates with authentication according to X.509 certificates.

NOTE: X.509 certificates are digital documents that bind a public key to an identity, such as a user, device, or website, and are a standard used in many security protocols like TLS/SSL. Issued by a Certificate Authority (CA), they are used to authenticate identities, enable secure communication (like HTTPS), and verify the integrity of data through digital signatures. These certificates contain information like the public key, the identity's name, the issuer's name, and a validity period. It is IP networking (internet) security protocol.

The DFRS ecosystem, is an ITS ecosystem based on the IP protocols (internet) "Open ICT ecosystems Framework". At present the DFRS ecosystem is an B2B platform where partners can make bilateral agreements about data conformity and interoperability on the data interface between the partners, there is no general platform data conformity and interoperability guarantied. DATEX II use guidelines defined. On the B2B interface different security mechanisms could be used. Only to the MDM there is a DFRS platform common security defined.

At present the DFRS ecosystem does not make use of ETSI ITS standards but refers to other standards from other SDOs.

4.4.2.4 The NAPCORE ecosystem

The National Access Point Coordination Organisation for Europe (NAPCORE) [i.15] project started in 2022, to work on a better alignment of the implementation of EU specifications in the European Member States. NAPCORE is a Programme Support Action co-funded by the EU under the Connecting Europe Facility.

NAPCORE [i.15] has been launched as coordination mechanism to improve interoperability of the National Access Points as backbone of European mobility data exchange. NAPCORE [i.15] improves the interoperability of mobility data in Europe with mobility data standard harmonisation and alignment. Also, NAPCORE [i.15] aims at increasing access to and expanding availability of mobility related data by coordinated data access and better harmonisation of the European NAPs. It is intended by increasing the accessibility to traffic information available at the various European road authorities from member state to city level to improve Traffic Safety and road efficiency.

The CEN/TS 17268:2018 [i.28] defines the content specification for the exchange of road-related spatial data and especially updates thereof. Based on the content specification, this document defines also a physical exchange format (structure and encoding) for the actual data exchange. In addition, it defines web services needed to make the coded data on updates available. This technical specification addresses specifically static data in the remit of Commission Delegated Regulation (EU) 2015/962 [i.26] and Commission Delegated Regulation (EU) 2022/670 [i.27], and aims at helping to keep digital maps for ITS up to date. Although the focus of this technical specification is on providing information on updates, the technology described in this document in principle also enables the exchange of full data sets.

NAPs are intended to make safety related traffic information and real time traffic information strategically available at authorities available for anyone to use. At present related information expected to be made available in the DATEX II [i.18] format. As DATEX II [i.18] is metadata based it is not interoperable by itself. To overcome this, there are European reference profiles for Commission Delegated Regulation (EU) No 886/2013 (SRTI) [i.25] and Commission Delegated Regulation (EU) 2015/962 (RTTI) [i.26] profiles defined, by DATEX II [i.18].

At present, specifications about the trustworthiness of the information provided can be found and no security mechanism are defined. It is intended that related information is made available at member state specific IP network references. Information is freely available. As it can be assumed that it makes use of the general capabilities of the Open ICT ecosystems Framework and has no specific requirements. It can be seen as another ICT ecosystem.

At present the NAPCORE ecosystem does not make use of ETSI ITS standards but refers to other standards from other SDOs.

4.4.2.5 The MirrorLink® ITS ecosystem

At present, MirrorLink® is an ITS Ecosystem which was specified by the Car Connectivity Consortium (CCC). It is a smartphone-to-vehicle integration system that works similarly to other systems such as Android Auto® and Apple CarPlay®. A smartphone can be linked to the vehicle's infotainment display using MirrorLink®. Once the smartphone display function is integrated into the infotainment system, the driver can interact with the apps using voice control, dashboard buttons, steering wheel buttons, or touchscreens.

For the interoperable operation between devices a standardized interface is specified the ETSI ITS-Ecosystem MirrorLink® ETSI TS 103 544 parts 1 to 25 [i.21], an ITS Ecosystem focussed on the HMI interface between Vehicular and Mobile phone equipment. It is an ITS Ecosystem which has a different objective compared to the ITS transport related Ecosystems and does not make use of the ITS Release components and functionalities. It therefore has to be seen separate from the ITS framework.

4.5 ITS Services

At present there is a large base of ITS services operational such as process or information management related services (Logistics) but also safety related services. Each of these ITS service classes have their own dynamics, functional and technical requirements. Some of these services encompasses both management as well as safety related services such as road navigation (MAP) services.

In the context of the ETSI ITS standardization, the focus is to specify all interoperability and conformity aspects related to "safety related" services which does not mean that other services cannot be supported by ITS releases but at present is not in focus.

An essential aspect of ITS services compared to other services that these are always operational in a time and locations context and therefore relate information to time and location. Among these ITS services, traffic safety related and traffic efficiency (in ITS as group referred to as "safety related") are distinguished from the other ITS services by having some, mostly timing, communication predictability and liability related advanced requirements.

Safety related is everything which can have a direct or indirect impact on the safety situation.

As already identified in clause 4.4.2.2, a service can be of a strategic or a tactical nature and as tactical information fulfils higher qualitative requirements, it can also be used for strategic related use cases, while strategic information generally cannot be used for tactical related use cases.

ITS services can be of a private nature, or of a cooperative nature. Private services are characterized by their B2B nature and restricted access for use. Data is not openly accessible unless there is a contract with a specific service provider. An example of a private service is a logistic service to manage truck fleets, DFRS or MAP provider services.

Cooperative ITS (C-ITS) and NAPCORE services have to be available to everybody without any restrictions. To ensure the trustworthiness and quality of the information for the C-ITS ecosystem a C-ITS trust mechanism is specified and referenced by the European Directive (EU) 2023/2661 [i.9]. NAPCORE as it has to comply with other security regulations then C-ITS, it is expected to have its own IP internet-based security mechanism, probably similar to DFRS.

4.6 ITS Systems and ITS Stations

As clarified in clause 4.2, different ITS Systems are and further can be realized in the ITS Domain.

ITSs are Information and Communications Technology (ICT) systems with an ITS purpose. An ITS is formed by more than one piece of equipment's communicating to each other. ITS in which the software and hardware in these equipment's work together to accomplice a specific communication ITS task of set of tasks.

ITS equipment generally consists of many components to realize not only communication tasks but also other task it is function specific. A bike does different things then a Vehicle. As such, the ITS related component of equipment is identified as the Station (ITS-S) and consists of a set-up of hardware, software, data, it can be autonomous but can also interfaces with other systems in the equipment of directly with the user, depending on the purpose of the equipment.

As such, ITS-Ss communicate to other ITS-Ss to realize an ITS specific service or set of services in the ITS Domain.

As there are various ITS Ecosystems there can be various ITS systems active at the same time e.g. C-ITS, DFRS and NAPCORE. As illustrated in clause 4.4, ITS Systems use different communication concepts. Two different communication concepts can be recognized.

- Dynamic networking configuration based. A method in which there is a process of assigning network settings, polities, flows and controls. This process could be physically or virtual. IP networks are configuration based e.g. DFRS and NAPCORE.
- Networking Constellation based. A method in which there is no dynamic configuration process but there are only static network settings, policies, flows and controls are commonly agreed e.g. C-ITS.

The later method is used there where there is no time or no reason to negotiate about the network access possibilities. This concerns typically sensor networks, AdHoc networks, often broadcast oriented networks. C-ITS direct communications is principally constellation based and typically used for tactical information exchange.

Tactical information can also be shared over configured networks, but this often leads to limited strategic use of the data. In any case to comply to the C-ITS trust and privacy requirements the information should be sealed in an envelope when shared over IP networks to comply to these C-ITS ecosystem requirements. Figure 5 provides a perspective on the present transport safety and transport efficiency related ITS Ecosystems. For DFRS [i.14] and NAPCORE [i.15] see the references.

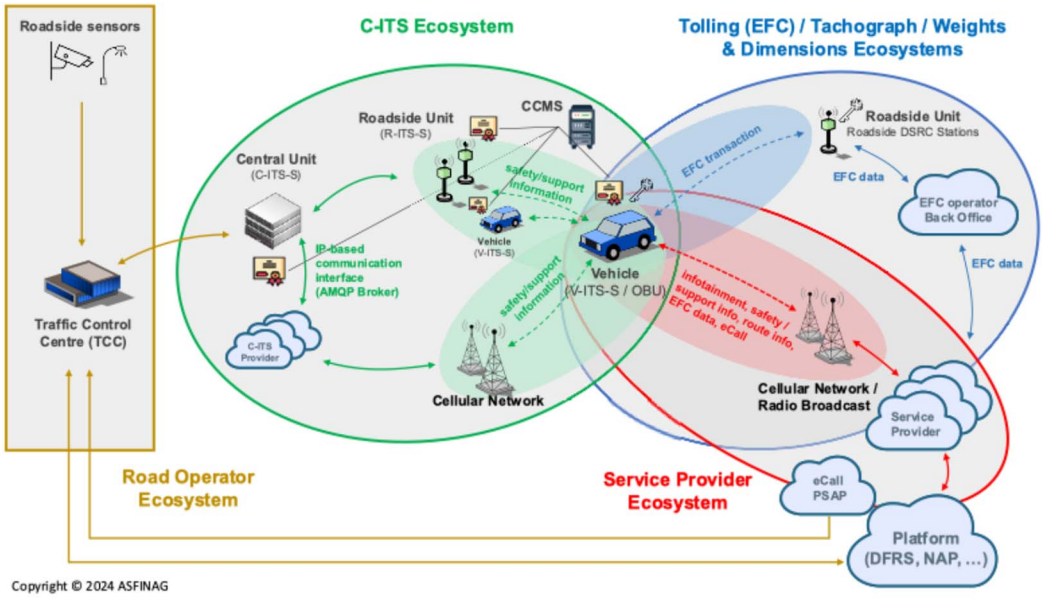

Figure 5: Existing EU ITS Ecosystems (including C-ITS, DFRS and NAPCORE) (Source: ASFINAG©)

5 ITS technical architectures

5.1 Introduction

As described in clause 4.3, a Technical Architecture (TA) provide a detailed view that specifies the technical design, technology standards, protocols, and products, used to implement functions and layers of an ecosystem. Technical architectures are used to implement and realize equipment. In general TAs specify specific stakeholder equipment or is B2B related e.g. consortia, to ensure interoperability and conformity on an interface between the B2B partners. In the latter case often, related documents are identified as profiles as they profile general specification and standards. Such profiles can additionally be standardized and then called profiling standard.

ETSI ITS provides a toolbox of ITS standards allowing stakeholders to define their own systems and profiles. Some of these profiles e.g. C2C-CC profile Basic System Profile (BSP)) are maintained in the C2C-CC organization. Cellular profiles e.g. LTE sidelink and 5G-NR sideling are profiles which are maintained at ETSI TC ITS and part of the Release 2 set of ETSI ITS specifications, but they are not part of the toolbox itself.

Only at the equipment implementation specification or profiling level, there are architectural requirements. Therefore, when it is not about implementation specification or profiling, architecture illustrations only provide guidance on how components and their interfaces are related to each other. This means that, for all toolbox documents architectures, architectures are informative.

The following clauses only provide architectural views about how components, protocols, interfaces, data structures relate, providing guidance in how these components related.

5.2 ITS implementation architectures

In the ITS domain, ITS-Ss exchange information via various implementation communication architectures. The overall architecture as illustrated in Figure 6 shows the collection of presently implemented or envisioned ITS ecosystems for the EU.

The following aspects are recognized:

- The Service Provider (SP) ITS strategic indirect information exchange based on provider specific security. Depending on the SP Ecosystem selected business model(s) and system solutions any interested party can participate.
- National Access Points (NAPs) are an EU commission initiative for the exchange of strategic indirect information in which all member states have their own NAP being interoperable with other NAPs. It is intended to be an intercloud based system for indirect information exchange of Safety Related Traffic Information (SRTI) based on standardized DATEX II [i.18] data exchange. An approached being managed by NAPCORE [i.15]. NAPCORE is expected to have its own ITS Ecosystem.
- Data For Traffic Safety (DFRS) [i.14] is expected to be similar to the SP with focus on the exchange of strategic indirect information, but could move more to the NAPs approach or be combined with the NAPs based business model(s) and system solutions. Details are not known at present. At present DFRS refers to the Safety Related Traffic Information ITS Ecosystem.
- Safety priority service (Netherlands specific), realizes the exchange of strategic indirect information based on Probe Vehicle Data (PVD) and SRTI and provides navigation type information via data protocol suite for traffic and travel related information and is TPEG (Transport Protocol Experts Group) based (see TISA https://tisa.org/). An exchange of data based on a Dutch specific safety priority ITS Ecosystem and related security.
- C-Roads [i.16] Hybrid approach realizes the EU C-ITS Ecosystem requirements laid down by EU regulations for sharing safety related information basically both as tactical and as strategical information exchange. It follows C-Roads and Car2Car Communication Consortium (C2C-CC) [i.17] profiles for the realization of Traffic Safety and Road Efficiency and exchanges information I2X over a tactile direct (AdHoc) communication network. Besides it shares this I2X safety information in a closed so-called brown envelop over the indirect IP based network so that the information is protected and can only be accessed when it returns into a C-ITS Ecosystem certified ITS-S. See for more detail Annex C.
- The C-ITS tactile direct V2X communication follows the EU C-ITS Ecosystem requirements laid down by Directive 2010/40/EU [i.24] and Directive (EU) 2023/2661 [i.9] for sharing safety related information. In principle direct communication information sharing based on C-Roads and/or Car2Car Communication Consortium (C2C-CC) [i.17] profiles. See Annex C for more details.
- Besides exchanging the information by means of direct V2X, some of the information exchange can also be shared via IP networks as long as the C-ITS ecosystem trust and security is maintained. This means that unpacking of the information shared between ITS-Ss is not possible at the IP protocol level but only at ITS-S stations which are C-ITS certified.

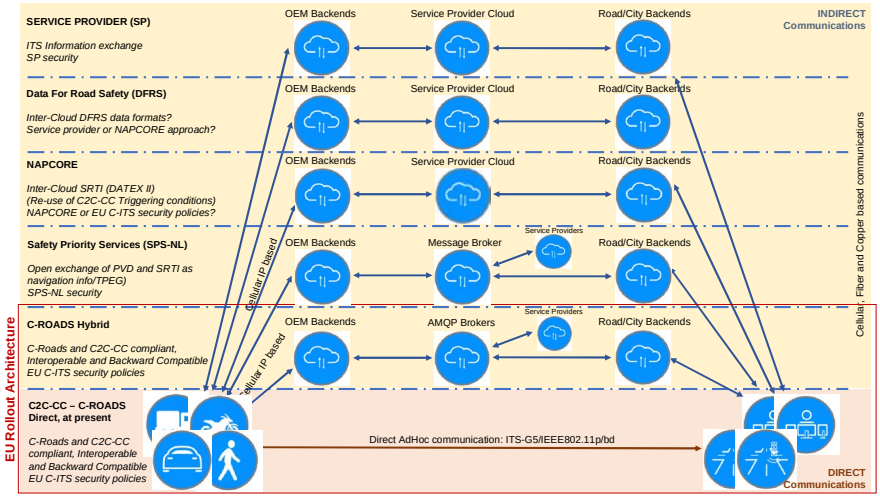

Figure 6: The ITS communication architectures used to realize ITS services

Figure 6 shows that in general indirect V2X and direct V2X communications are being linked to different Ecosystems e.g. Service Provider (SP) specific, DFRS, NAPCORE, SPS-NL, C-ROADS Hybrid and C2C-CC/C-Roads direct.

In general, these ecosystems offer partly overlapping, but also different information dissemination possibilities. Figure 6 shows the complementary possibilities they together give. As coexisting ITS ecosystems are being able to evolve separately, they can use the same security mechanisms as long as the credential and certificate management are kept separate for each of the ecosystems to ensure being able to identify the uniqueness of the received information because, coexisting ITS ecosystems could provide similar information which could still differ in usability depending on e.g. source, time or other various conditions.

5.3 Technical architectures in ITS standardization

5.3.1 Introduction

As explained in clause 5.1, although profiles can be part of ETSI ITS releases, TAs in ETSI ITS standards of a release are informative or illustrative only. However, a basic ITS architecture identifying the basic ITS communication between ITS-Ss (sometimes also referred to as ITS nodes) can be defined. This ITS basic architecture is shown in Figure 7. It identifies the ITS-S as a component of equipment. ITS-Ss communicate to each other, so one ITS-S provides information to other ITS-Ss and vice versa.

In principle in ITS compliant equipment, one of the components is an ITS-S as illustrated in Figure 7. This is simple and clear for a Vehicle, PTW, bike of any other road user but in road infrastructure this is a bit more complicated.

The medium in Figure 7 is not always the same. In case of C-ITS ecosystem, in principle direct V2X, it is the air interface, in case of the other ITS ecosystems referenced in the present document, it is generally realized based on IP communications and internet protocols.

Figure 7 provides a very general overview of the ITS domain, identifying that an ITS-S is only a component of an equipment and that there can be other components from which some could provide information to the ITS-S functionality and vice versa.

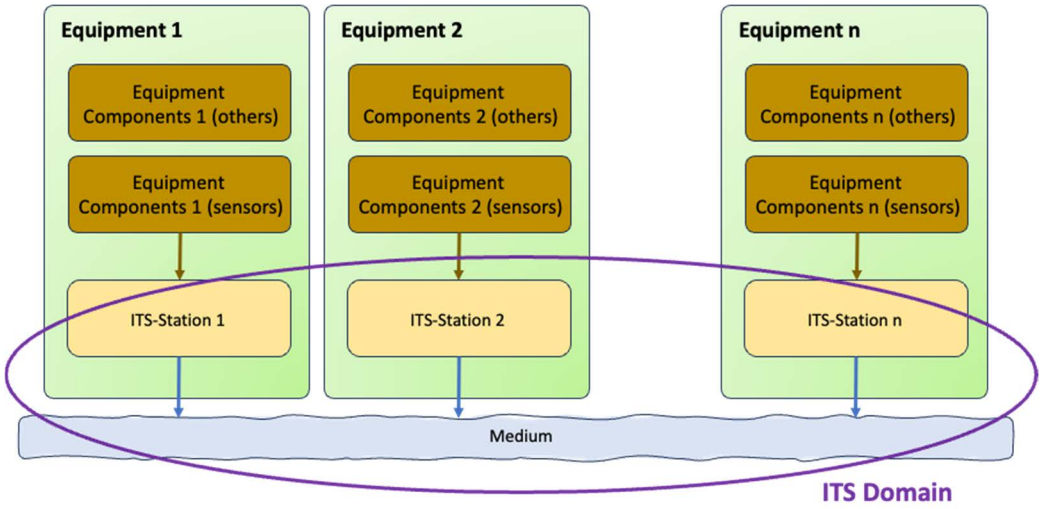

Figure 7: ITS basic architecture (high-level example)

Figure 8 illustrates a more complex setup, a road infrastructure equipment setup with traffic management centre and some roadside units. This figure is a possible result of the illustrations of Figure 5 and Figure 6. What can be recognized is that, from an system configuration point of view, the C-ITS and other ITS processing may be mixed as well as that the authority internal network can be just one, but that care has to be taken that the system complies to the different data trust and data ownership aspects which are generally different for different ITS ecosystems. Aspects such as that different regulations could apply for different ITS ecosystems, as well as that different security mechanisms can apply. As illustrated in Figure 8 at the Trust Critical location care should be taken in order to address these issues.

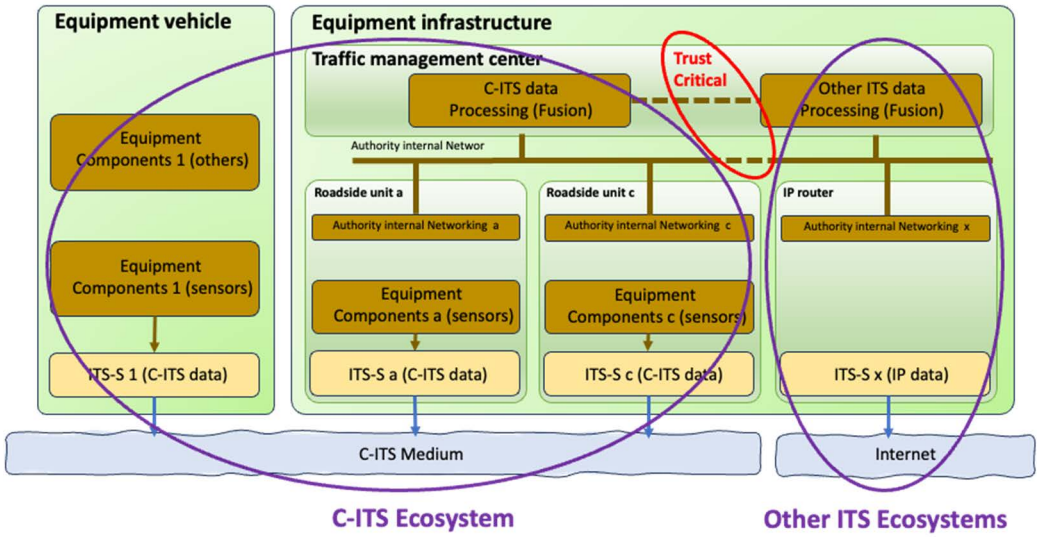

Figure 8: Infrastructure oriented ITS basic architecture (high-level example)

5.3.2 The ITS-S technical architecture

The ITS-S architecture is a simplified model derived from the ISO Information Basic Model (ISO-IBM, ISO/IEC 7498-1 [i.12]) and is provided in Figure 9. This architecture is intended to provide a structure in which components can relate to each other. Information flows between components belonging to the same layer or to different layers can be characterized as Management (Control) Data flow, Functional Data flow and when required as Security Data flow. Within the architecture these flows are identified respectively on the Management Plane, the Data Plane and the Security Plane as illustrated in Figure 9.

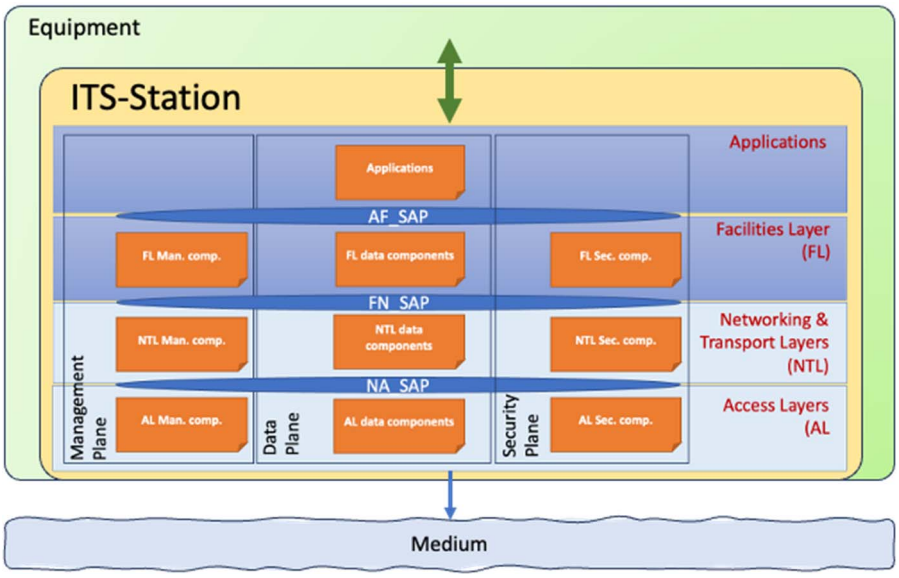

Figure 9: ITS-S architecture

Depending on the complexity of the functionality, Data and Management flows can be included in one figure or can be separately presented in multiple figures. In other systems the Management Plane is recognized as the Control Plane.

In the ITS-S architecture, the Access Layer (AL) represents the OSI layers 1 and 2, the Networking & Transport Layers (NTL) represent the OSI layers 3 and 4, the Facilities Layer (FL) represents the OSI layers 5, 6 and 7. The Applications are on top of the OSI layer 7.

Functionality architectures could be presented in a simplified way in a single drawing such as the one presented in Annex A.

In ETSI EN 302 665 [i.10] (Release 1 ITS communication architecture), the term Service Access Point (SAP) was defined but was identified as an interface. As over a SAP (between the layers) many interfaces may exist and those interfaces are a functionality and not system specific, these interface specifications are part of the functionality specification they are defined in and not in a separate SAP specification.

5.3.3 Other Architectural models (UML)

Components can be realized in soft- and hardware or be realized by a mixture of soft- and hardware. In principle, the higher the component is placed in the ITS-S architecture the more it will be realized by software. In case component descriptions could be used to realize software solutions, UML is often used to specify the functionality. Further it should be recognized that more and more software is also used at lower layers e.g. Software Defined Radio.

In ETSI ITS specifications UML visualization methods can be used e.g. UML design models, UML flow models and UML behavioural models, for the modelling and illustrations of designs, flows and behaviour. Some examples are illustrated in Annex B.

5.3.4 Common Layer aspects

The common aspects are mainly related to the use of terminology. The terminology is dependent on the layer. Figure 10 provides an overview.

Data are bits whose meaning is not directly of relevance or not known. Information is data from which the meaning is known. At the applications and Facilities Layer (FL), it is about Information and within the protocol it is about data. At the FL, messages can be collected from lower layers or disseminated to lower layers. At the Networking and Transport Layer (NTL) packages are transferred and on the Access Layer frames are transmitted or received (see Figure 10).

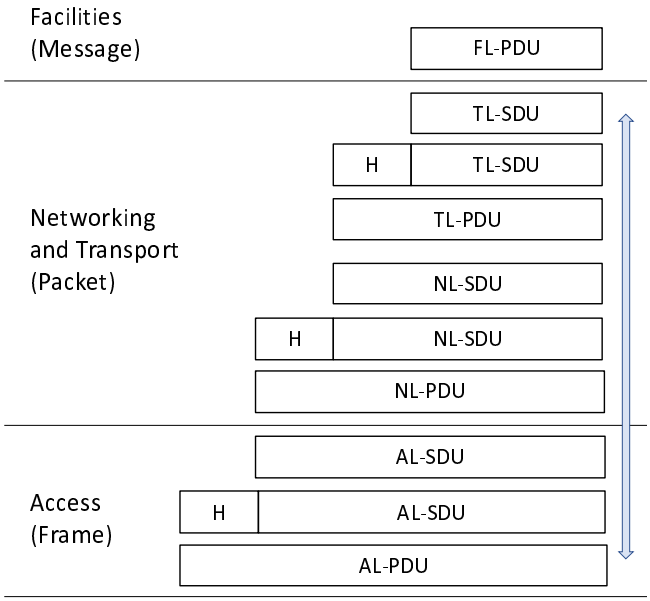

Figure 10: Layer dependent terminologies

In ICT communications, a Protocol Data Unit (PDU) is s single unit of information disseminated or transmitted (depending on the layer) between peer entities. It is composed of protocol-specific control information (the Header) and user data. So, at the Facilities Layer there is the FL-PDU including all the facility layer aspects relevant for the receiver of the information. To inform other layers about the intent of the use of the forwarded information a Service Data Unit (SDU) can be exchanged between layers. Each Layer PDU forms the payload for the next layers PDU.

5.3.5 ITS Applications

This clause defines general ITS application possible additional aspects, e.g. classification, prioritization and channel assignment, registration and secure maintenance, in the context of ITS.

An ITS application can be a single functionality above the FL in one ITS-S, making use of collected information received from another ITS application active in one or more other ITS-Ss to realize an ITS service. An ITS application can also be realized as a set of applications active in multiple ITS-Ss, combined providing a specific ITS service.

At present two types of service models can be recognized.

- The client service model which is traditionally used in networked communication systems based on having the security at the facilities layer. In this case one of the functionalities active in one particular ITS-S will be the server part and the other ones will represent the client parts. In such case the server part should manage the proper operation of the application and be responsible to ensure the ITS service is properly realized. It is therefore responsible for the correct operation of its functionalities active in all ITS-Ss.

- The C-ITS service model in which information is shared based on having no knowledge of the presence of any receiving ITS-Ss. A sensor-based data sharing model with no expectation about what the receiving ITS-S will do with the data. A model in which the security is handled at the Networking & Transport layers as this layer should be able to forward messages.

At present three classes of ITS Applications are considered: "Traffic Safety", "Traffic Efficiency" and "Other Applications". Depending on the ecosystem at hand, different functional requirements can be applicable for each of the classes. Depending on how many applications rely on communication services, application classes impose communication requirements on the ITS-S as identified for each ecosystem to be implemented, with respect of e.g. reliability, security, latency, and other performance parameters.

Whilst the reliability of communication systems can be optimized, communication systems will never be 100 % reliable as radio transmissions are not 100 % reliable. Developers should design their applications and systems to operate safely even when a problem with the communications system occurs.

Improvement can be realized by enabling the applications to be informed about the communication capabilities ahead of their decision making. It can be of interest for ecosystems to install interoperable mechanisms to realize this. Within C-ITS Resource Management (RM) is one such mechanism.

For C-ITS, it should be ensured that information sourced by an ITS-S can be received by sinking ITS-Ss. A sinking ITS-S needs to know in advance how the information is disseminated by the sourcing ITS-S in case the sourcing ITS-S is not aware of the presence of ITS-Ss. This means that the channel assignment and prioritization of the messages in a given channel or spectrum are one of the aspects which are required to be use case or ITS-S service specifically set to ensure an interoperable behaviour. This is generally part of the ecosystem requirements mostly specified as part of a system profile.

In such C-ITS profile, for each of the C-ITS services related messages disseminations, it is required to set the communication requirements e.g. logical channel or spectrum, priority and possibly modulation parameters, to ensure that sinking ITS-Ss can receive, and process received data.

Maintenance of ITS applications, i.e. installation, de-installation, activation, de-activation and management of updates, should be performed in a secure way in order to support protection of ITS stations from attacks by malicious applications. As this is a system aspect, this is an Ecosystem requirement and should be specified in a profile.

Each ITS application is unique and needs to be uniquely identified. It is therefore required to register ITS applications and message ITS-S services at a registration authority, to receive a unique ITS application ID (ITS-AID).

The Service Specific Permissions (SSP) is a field that indicates specific sets of permissions within the overall permissions indicated by the ITS-AID.

ITS System security aspects are typically governed by an Information Security Policy. Such security policy is a document that outlines the requirements and guidelines an organization or a group of organizations will use to manage their IT systems and protect its/their data. The policy explains the strategy and the reasons behind the proposed security measures and defines the general expectation and approach to information security. A security policy is often based on the three principles of the CIA triad: Confidentiality (C), Integrity (I), and Availability (A).

ITS System also may need to use security credentials, such as cryptographic keys and/or associated certificates issued by external systems, to ensure protected relevant information. Security aspects of Security Credentials Management Systems (SCMS) such as Public Key Infrastructures, i.e. dedicated IT systems that issue security credentials for use by data processing IT systems, are typically regulated by a Certificate Policy. Such a Certificate Policy defines the requirements for the issuing of certificate by the SCMS and usage of certificates and associated key material by End Entities.

The present document recognizes the C-ITS Application ID (AID), the Service Specific Permissions (SSPs) and Port-Numbers are defined.

5.3.6 Access Layer

As shown in Figure 11, the Access Layer (AL) identified as part of the ITS-S architecture in clause 5.4, is decomposed into the Data Link Layer (DLL) and the Physical Layer (PHY). The DLL can be further decomposed into a Media Access Control (MAC) which manages the access to the communication medium, and below it, the Logical Link Control sub-layer (LLC).

At the AL multiple radio technologies can coexist in parallel while having their own management components.

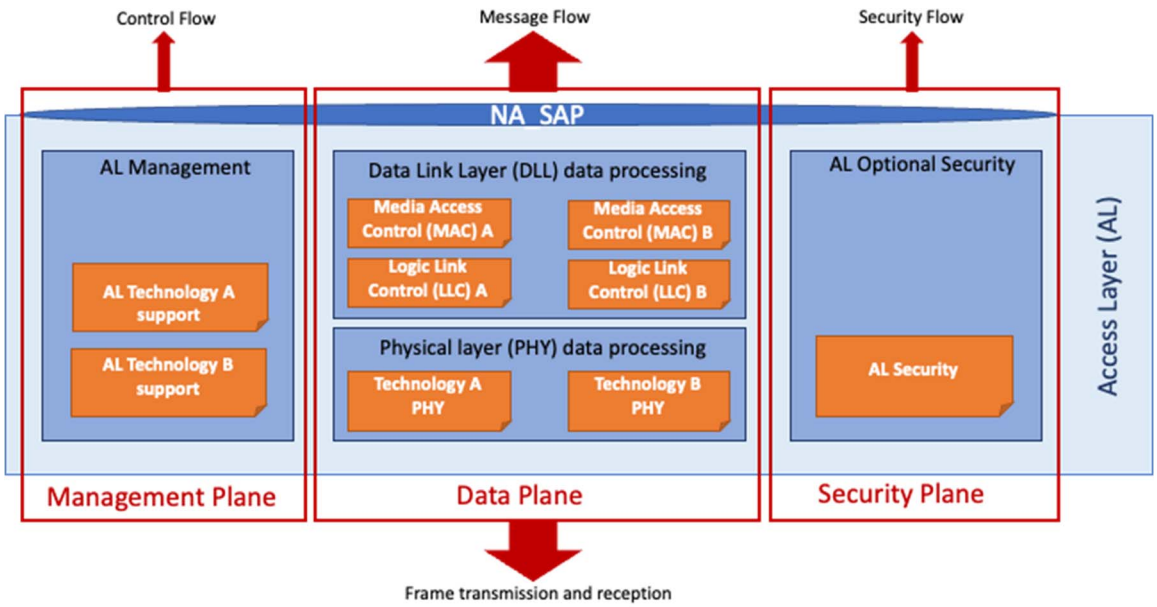

Figure 11: The generalized Access Layer composition

Each of the technology specific AL management and data plane components can interface to higher layer components independently but also via a generalized interface. At present, for C-ITS there are no interfaces between Access Layer components and security components at the security plane specified.

Figure 11 illustrates that single or multiple channels can be realized by means of several technologies simultaneously.

To allow flexible physical channel assignment, the concept of virtualisation can be used. A mapping of logical channels onto physical channels can be performed in compliance with the related standards dedicated to the AL technologies. This allows a virtualisation concept such as an Access Layer Instance (ALI) concept in which channels are configured virtually for one specific usage at one moment and one other use at one other moment.

5.3.7 Networking & Transport Layer

The Networking & Transport Layer (NTL) is shown in Figure 12.

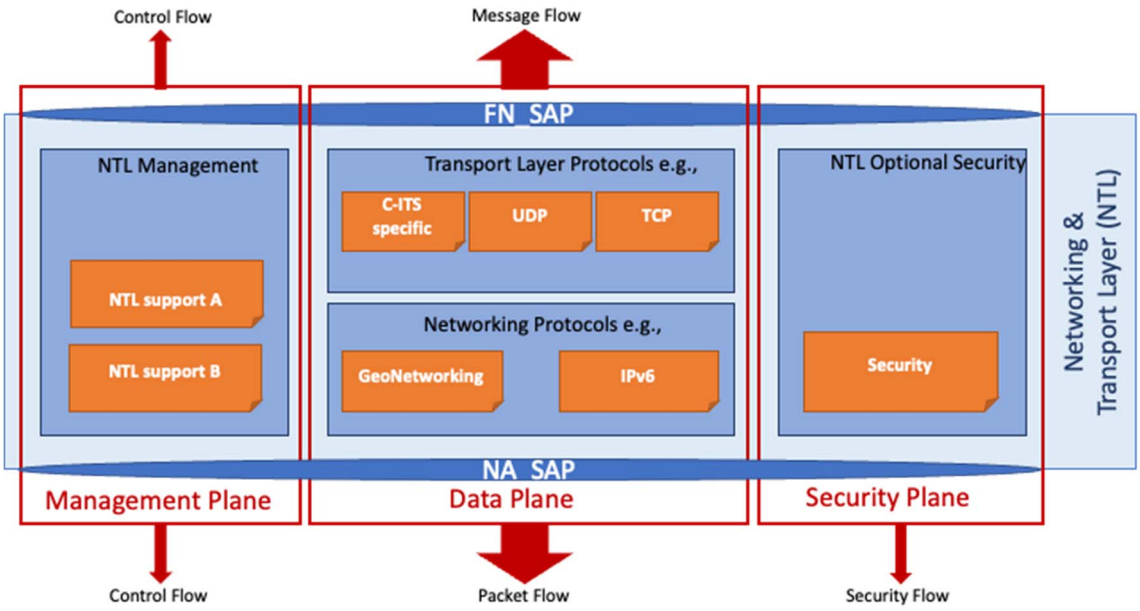

Figure 12: The generalized Networking & Transport Layer composition

The NTL contains components from the OSI network layer and the OSI transport layer. It can include one or several networking protocols, one or several transport protocols, as well as, generally, some network and transport layer management components at the management plane and could include some security components at the security plane.

In case the concept of Access Layer Instances (ALIs) is used, the NTL routes the package to the AL or, if virtualisation is implemented, to the appropriate Access Layer Instances (ALI), and provides received packages from the ALI or ALIs to the higher layers.

Additionally, the NTL can be used to exchange NTL and AL parameters with other ITS-Ss.

5.3.8 Facilities Layer

The Facilities Layer (FL) is shown in Figure 13.

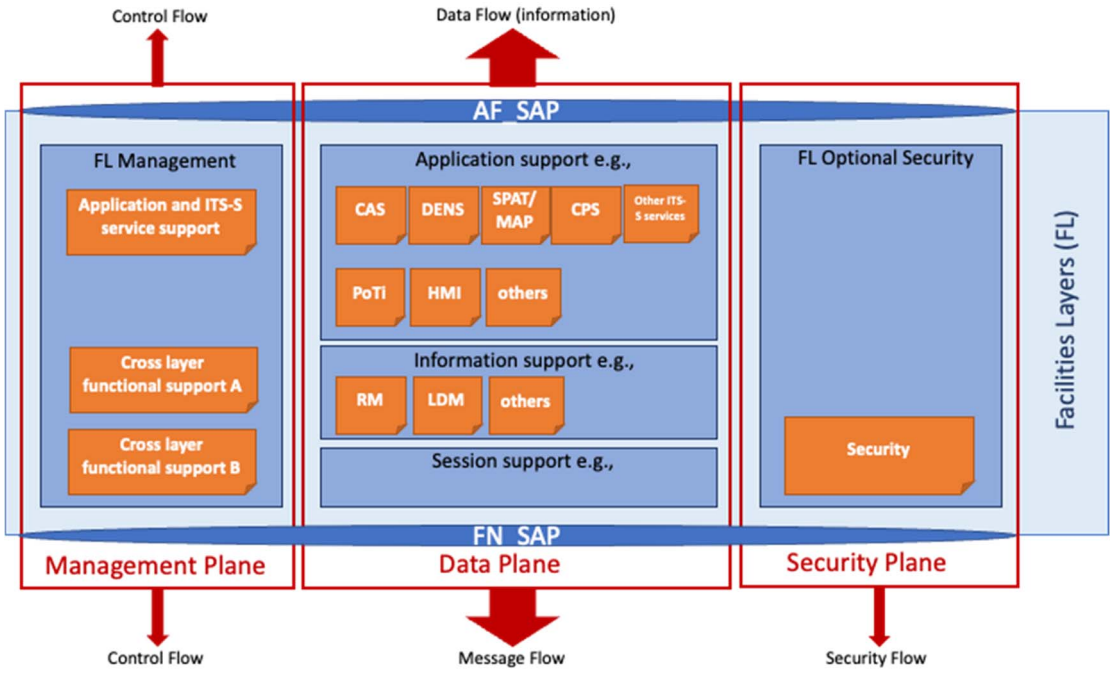

Figure 13: The generalized Facilities Layer composition

The basic components of the FL are application support, information support and application/FL management. Security related component can additionally reside at the FL layer depending on the ITS ecosystem. The FL includes an OSI presentation layer (e.g. ASN.1 encoding and decoding, and encryption) and can include an OSI session layer (e.g. inter-host communication) with amendments dedicated to ITS. At present the latter is not required for C-ITS but could be required for other ITS ecosystems.

The FL is providing support to ITS applications which can share generic functions and data according to their respective functional and operational requirements. A non-exhaustive list of generic ITS specific functions from which some are illustrated in Figure 13 are the following:

- Generic Human Machine Interface (HMI) support. This functionality presents information to the user of the system, e.g. to the car driver, via the HMI hardware and firmware.
- Support for data presentation. Data presentation is a basic functionality of the OSI presentation layer. Its function is to code and decode messages according to formal language being used (e.g. ASN.1).
- Addressing support. This functionality supports selection of the addressing mode at lower layers.
- Position and Time (PoTi) support. This functionality provides information on the geographical position (longitude, latitude, altitude) of the ITS station, and the actual time. It provides support for location referencing and time stamping of data and can be composed out of several components deriving information from different other equipment subsystems.

- Local Dynamic Map (LDM). A cooperative system for Traffic Safety critical applications benefits from using digital maps. Such maps used in ITS may include lane-specific information including curbs, pedestrian walking, bicycle paths and road furniture such as traffic signs and traffic lights. Furthermore, all dynamic objects that are directly sensed or indicated by other road users by means of cooperative awareness and collective awareness can be referenced in such LDM. Essential for C-ITS, all objects are time-stamped. An LDM containing the location of dynamic objects might also be provided for vehicles that do not have a geographic digital map available.

- Support for maintenance of ITS-S applications. This functionality could support the download and activation of new application software and the update of already installed software.

- Service-Oriented Architecture (SOA) application protocol support. This functionality could support the operation of loosely coupled business-aligned and networked services. An implementation example are SOA-based web services. It can support applications using backend services with features such as establishing a session with the backend, handling unexpected session losses due to the mobility of the ITS station and maintenance of a session during handover.

- Support for station capabilities management. This functionality could manage information on station type, e.g. vehicle profile or roadside unit profile, station capabilities, e.g. supporting ITS communication channels and other static or variable information related to the station itself.

- Support for combining and fusing data from different sources and keeping them up to date.

- Support for station data provision. This functionality provides static and dynamic information from the ITS-S as required by ITS applications and other facilities.

- Support for common message management for data exchange between ITS-S applications:

    - Event messages: Event messages are triggered by applications following the detection of some events. They are repeated as long as the event is perceived by the ITS-S which is detecting it. Events are signalled using broadcasting capabilities. Rules to define the signalling coverage, stop to repeat it or cancel it depend on a specific event.

    - Periodic messages: Awareness Messages are an example of periodic messages. Periodic messages are disseminated periodically, signalled using broadcasting capabilities.

    - Service messages. Service messages are messages to manage sessions. There are two parts: the service announcement allowing other ITS-S to be aware of possible ITS services which can be provided by a specific ITS-S and a reply message to answer the service announcement when applicable.

- Support of repetitive transmission of messages. This functionality could be in charge to repetitively request transmission of messages according to the requirements set up by the ITS-S application.

- Channel selection. This functionality could support the selection of the proper communication interface for transmission of messages.

NOTE: The different functionalities as presented above often do not need to be interoperable and may be already part of the Operating System or supported by other sub-systems of the equipment and therefore are not necessarily standardized.

5.3.9 Predictable ITS Communication behaviour

In a communication system the communication is always limited by the limited availability of radio spectrum or by interference of any kind and therefore is characterized by having a certain level of predictable behaviour of being able to transmit or receive information. To realize higher levels of predictability in ITS-Ss, the transmission of frames should possibly be controlled to allow all ITS-Ss to realize their tasks predictably. It depends on the Ecosystem requirements which mechanisms to include.

It is common for communication technologies to limit the transmission of frames at the Access Layer for the realization of acceptable access. These mechanisms are generally specified by the related AL technology.

NL mechanisms can be used for improvement but are generally not responsible for the limitation of the transmissions. Improvement mechanisms could require to be interoperable depending on the Ecosystem requirements.

Generally, no other limiting mechanisms are needed. However, as defined by C-ITS Ecosystem requirements, for C-ITS it is of importance to be able to make functional decisions based on the dynamic communication capabilities. Therefore, in C-ITS, besides the basic limitation at the AL, congestion level information as detected at the AL can be forwarded to higher layers to enable higher layer functionalities to make better message dissemination decisions insuring more predictable ITS behaviour.

NOTE: With a limited fixed set of applications active in a single channel, predictability could be manageable, however even for a single channel ITS-S system it could be of interest to add resource management mechanism. Such mechanisms are a necessity when multiple channels and/or multiple technologies are being used.

5.3.10 ITS-Station management

5.3.10.1 Introduction

ITS-S management is an ITS-S internal aspect and therefore mostly an implementation aspect. Depending on the ecosystem required communication architecture, it could be important to realize some of the management functionalities in an interoperable way and therefore it could be of relevance to standardize those functionalities. Most of ITS-S non interoperable management functionalities are supported by Operating System (OS) components.

It is possible that an interoperable ITS management functionality is realized by several management components residing on different layers, while exchanging information over the management plane as clarified in clause 5.4.

The following management functionalities could be considered in case interoperability is required: Cross-interface management, Networking management, Communications service management, ITS application management, Station management, Resource management, Management of Service Advertisement management, Radio Spectrum Congestion management and Radio spectrum interference management.

In the following clauses a number of these functionalities are considered which could require interoperability for a specific Ecosystem.

5.3.10.2 Application management

ITS application management manages the installation and configuration of ITS-S applications and is responsible for the updating of these applications. The application management supports the error handling of ITS-S applications. It can include safeguarding mechanisms alleviating harmful application behaviours.

In general, ITS application management in an ITS-S is generally seen as a station internal aspect and for the support of managing the application operation often OS mechanisms can be used, or additional mechanisms are implemented which do not require any interoperability. It can include functionality revision control from outside of the ITS-S via Internet protocols including the management of security mechanisms.

Only in case the application is realized by components which are located in various ITS-Ss and that these various components are owned by various parties/stakeholders, could interoperability be required. In such case, the interoperability is possibly not managed by a functionality in the ITS-S itself but could be managed by both having interoperability requirements on the ITS-S application itself or by having ecosystem agreed interoperable installation and activation processes in place for this application to ensure the proper operation as a hole.

The interoperability of ITS-S applications and ITS-S services is laid down in the application and service specifications. The interoperable process evaluation specification should be part of validation of an ecosystem.

Application management aspects which could be of interest to realize interoperability and conformity could be, for instance, Service Advertisement (SA), application mapping and Management Information Base (MIB) in case they are network based managed.

In ITS push and pull mechanisms can be introduced allowing ITS-Ss to identify existence or presence of ITS services. The push mechanism is realized by a "Service Advertisement Service" (SAS). The pull mechanism is known e.g. from internet protocols.

SAS could be implemented optionally in different ways and may differ for each of the ecosystems. One option on how to advertise ITS services is through a single-hop wireless links.

A SA manager active in a sinking ITS-S collects the SAMs and can forward them to service provider specific applications active in this ITS-S. Within C-ITS, it is not envisaged to forward SAMs.

A SAS is generally managed by a service provider. Sourced SAMs are mostly periodic disseminated.

5.3.10.3 Resource management

In ITS, information exchange possibilities could be limited by the available radio or spectrum resources. At present in ITS it is recognized being of interest to manage these radio resources. In future, possibly also other resources could be managed.

In internet communication, the routing of data is managed at the Networking & Transport Layer. Applications are not informed about the underlaying dynamics, source and sink can only be connected, and the sourcing station can only be informed about whether a package has been delivered or not. It allows the sourcing station only to correct afterwards but not proactively take actions based on communications current dynamics. For most applications this highly best effort approach is sufficient, but for safety related information exchange this is often not enough, leading to higher performance requirements being put onto the communication system.

For more time critical safety related applications, it could be of importance to know the communication possibilities in advance so that they can make decisions depending on the availability of the communications.

For those applications where it is important to understand these communication capabilities, these capabilities should likely not depend on randomly made choices at a nonfunctional layer such as realized in Internet (IP) communications at the NTL. It could be of relevance that the dissemination and the influence of other applications are managed at the FL.

The Cooperative ITS (C-ITS) methodology is an ecosystem in which the dissemination (i.e. passing PDU to lower layer) and the scheduling of the dissemination is realized at the FL where Resource Management (RM) takes place when applicable. This allows the applications to make decisions based on a better knowledge of the communication capabilities. This methodology does result in routing limitation at the NTL to ensure that the FL is able to predict the channel usage.

Although forwarding or rerouting of information, whether this is realized at the FL or at the NL, has influence on the RM, the message collection is handled by separate components which have an interface to the RM.

RM is technology agnostic and its main functionality is realized at the FL. RM has to be interoperable because in case it is dynamically assigning and routing message dissemination, it can have dynamic influence on the use of the communication resources and therefore on the performance of other ITS-Ss.

5.3.10.4 Message forwarding

Message forwarding is a mechanism which is helpful in direct (AdHoc) communication environments as the source could possibly not reach the destination. In such case an ITS-S which sinks packets from other ITS_Ss can source the packets toward the final destination. This is not applicable for internet-based communications as the destination should always be known.

Message forwarding can be realized at different layers depending on the control over the dissemination of the information. At present there are two ways recognized and generally, it is up to the ecosystem to identify which to use.

First of all, forwarding can be realized at the NTL which is commonly used in C-ITS. For some message types, each message disseminated includes a specified message relevance area value. This information provides the means by which a sinking ITS-S can determine whether or not the messages should be forwarded. In ITS Release 1 this is realized only for specific messages which are initiated by road authorities and realized by relevant functionalities at the NTL. As this forwarding is only initiated by road operator equipment, the influence on the performance of the communications is limited and therefore is not expected to be an issue for any RM.

The consequence of realizing the forwarding at the NTL, is that also the security has to be handled at the NTL.

Forwarding at the FL is more flexible, provides more dissemination control at the FL and gives more flexibility in making technical choices and introduction of new technologies. It could be part of a RM functionality.

5.3.10.5 Network management

Message forwarding at the NTL is a functionality which directly forwards packages without providing knowledge about the forwarding to the FL. In case a RM functionality is implemented at the FL, the RM gets only aware about the forwarding of packets at the NTL in a reactive manner via the ALI dynamic collection component, when an ALI concept is used.

Message forwarding at the NTL has the advantage that it is a faster forwarding process tailored for fast decision making, however it requires that security measures are handled at the NTL and not at the FL for massages which could be forwarded.

In case, in an ecosystem, it is required to manage the components in the communication system, this could be done with a Management Information Base (MIB). The MIB is usually associated with the Simple Network Management Protocol (SNMP). A MIB is often used in OSI/ISO Network management models.

5.3.11 ITS security

5.3.11.1 Introduction

The type of security that needs to be implemented is defined by the ecosystem requirements and therefore the security requirements often differ from ecosystem to ecosystem.

In many cases the security is covered by a commonly agreed model and authority. For example, in the C-ITS ecosystem, this is covered by European security policies laid down in the European Security Credential Management System (EU CCMS) [i.23].

The following clauses identify some ITS related security aspects to be considered.

5.3.11.2 Security related ecosystem dependencies

A security solution depends on various requirements related to trust, data privacy, safety or functional impact and system security impact requirements. Some of these requirements are part of national or regional regulations. A number of these aspects are system specific and could be seen as static requirements, however there is the functional dependency coming from the services to be supported. This last aspect is dynamic as at any time a new service could possibly provide additional security requirements.

As result, whenever a significant change in these requirements can be recognized, a risk assessment is required to identify the security technical requirements.

In addition to these requirements having an influence on the security technical requirements, there could also be requirements coming from security system threats which also could result in additional risk assessments.

For each ecosystem, risk assessments should be realized whenever identified situations occur.

5.3.11.3 Security in the ITS architecture

As identified, the required security mechanism depends on the ecosystem to be supported. In principle security functionalities could exist at any layer of the ITS architecture. At present there are no general architectural considerations being identified. The security architecture should be considered as an ecosystem implementation related aspect. Considering the present listed ecosystems, in addition to the aspects identified in clause 5.3.11.2, regulations have an impact on the architecture. According to several EU regulations, C-ITS has to comply with additional elements of these regulations, and therefore different security requirements are applicable and have to be considered.

5.3.11.4 Security functionalities

The ITS-S security includes security functionalities related to the ecosystem specific ITS communication protocol stack, the ITS-S and ITS applications, e.g.:

- firewall and intrusion management;
- authentication, authorization and profile management;

- identity, crypto key and certificate management;
- a common Security Information Base (SIB);
- Hardware Security Modules (HSM).

5.3.12 Local Dynamic Map

For the purpose of direct traffic manoeuvrer and traffic safety services, the knowledge about the presence of other ITS-Ss in the direct neighbourhood is essential for manoeuvrer and safety decision making. Relevant information about the equipment's ITS-S kinematic state, e.g. position, speed and heading can be captured in a Local Dynamic Map (LDM).

Depending on the ecosystem, additionally communication parameters such as MAC addresses and networking addresses could be added depending on ITS service requirements.

5.4 ITS Radio Spectrum

5.4.1 Introduction

In the context of ITS, there are ITS ecosystems which make use of IP networks and ITS ecosystems which make use of specific ITS allocated spectrum. This clause concerns only those ITS ecosystems which make use of specific ITS allocated spectrum.

Radio spectrum is a scarce resource and therefore ITS applications should use it efficiently.

Two aspects should be considered:

- The presence of several ITS applications and ITS message services requires to consider the impact of their information dissemination on other ITS applications and ITS message services.
- The presence of other systems active in the same spectrum. In general, this should be arranged by spectrum regulation but should be reviewed and may lead to additional measures such as mitigation.

Both aspects are out of scope of basic standards (toolbox) since they are ecosystem issues and need to be covered by profiling.

In the context of direct V2X some related aspects are considered in the following clauses.

5.4.2 Congestion management

Physical communication channels have limited bandwidth. In operational environments, a large number of directly communicating ITS-Ss accessing the ITS spectrum can lead to excessive load on the physical channel. Mechanisms avoiding such excessive load should therefore be considered to ensure proper operation of ITS.

Such means are referred to as "Congestion Control" (CC) and impacts all communication layers of the ITS-S architecture.

Congestion management is usually realized with functionalities at the applications, the FL and/or the AL through means such as:

- By informing the applications about the channel CC so that applications can limit message dissemination.
- By resource management functionalities at the FL which dynamic re-route information to appropriate channel resources. Dynamic modification of repetition rate of periodic/repetitive messages.
- By modification of AL parameters, on a frame-by-frame basis.

In addition, it is quite common that there are mechanisms implemented at the AL as part of technology specific specifications and are unique for those specific technologies.

For the definition of application and /or FL layer CC related functionalities such as RM, the influence of these AL CC mechanisms should be considered.

5.4.3 Interference management

In general, any radio system should comply with all the spectrum related requirements which are applicable for the used spectrum. Equipment should therefore comply with all applicable world, regional and national spectrum regulations and avoid any unwanted interference with other existing systems in and outside of the frequency band used. In case harmful interference could occur, mitigation methods could be applicable.

Tolling systems realize their information exchange by means of Dedicated Short-Range Communication (DSRC) technologies, at the time of implementation not hampered by any spectrum receiver parameter requirements in regulations with the effect that related OBUs are sensitive for transmissions in adjacent channels. As ITS communications became later active in related adjacent channels, ITS equipment should ensure not to interfere with DSRC Tolling systems. As such it could be required to implement mitigation techniques

At present service provider specific urban rail technical systems are deployed in restricted areas which can be adjacent to roads. This means that mitigation from R-ITS to Urban rail ITS (U-ITS) needs to be considered.

6 ITS Standards Releases

6.1 Introduction

A product has its lifecycle, from research and product definition to development, production to maintenance. When the product definition changes, this can be seen as a product upgrade but also as a new product. Often this is recognized as going from one generation to the next generation products. This shift can be backward compatible or not. For ITS this is not different. ETSI ITS standards are based on Releases, Release 1 being already frozen while Release 2 work has not been completed at the time of writing the present document.

NOTE: While the Release 2 documents can be recognized by "Release 2" appearing in the title, Release 1 documents have no Release statement in their titles.

The development of Release 1 focused on C-ITS realization, and the C-ITS extension in Release 2 do have to be backward compatible (see clause 6.3) with Release 1 according to EU regulation Directive 2010/40/EU [i.24] and Directive (EU) 2023/2661 [i.9].

Based on the experiences with Release 1 ITS specifications as identified in ETSI TR 101 607 [i.1], an updated Release 2 of the ETSI TR 101 607 [i.1] includes all Release 2 documents. ETSI TR 101 607 [i.1] is part of the set of framing documents.

6.2 Release 1 findings

The restructuring into Releases was initiated when going from Release 1 to Release 2. In Release 1 there were circular references which basically defined a system and limited the use of the Release 1 specifications. As result in following releases, normative referencing is limited to only the functionality specific components.

Re-use analyses of Release 1 documents for use in Release 2 showed the following misunderstandings:

- There is back and forth (up and down) normative referencing. To avoid issues only one direction (downwards) normative referencing should be used. In case it can be proven that it is required for clear understanding and avoids errors informative referencing bottom up could be used.

- Normative referencing is realized between different functionalities. Normative referencing to other functionalities should be avoided. In case one functionality could have an interface with another functionality this should only be generally identified and not specified. Only in case parameters which are defined in one functionality specification should be set in another functionality specification, can it be specified conditionally normative so that other possibilities are kept open.

- Consciously functionality specifications and sub-system specification should be kept separate and referenced one way or another.

- There can only be normative references between functionality specifications in case those specifications are a subpart of one larger functionality. These specifications are entity specifications which together specify a functionality. In most cases such set of specifications is kept together by a functionality architecture specification specifying the overall operation and architecture of the functionality and therefore it will reference normatively to all other specifications of that functionality. Each of the entity specifications can informatively reference to the architecture specification. They should not reference to the other entity specifications.

6.3 Release principles

To support going from one release to another, some release principles for the ITS Domain are needed.

The following ITS release related principles are defined:

- Maximize the technology neutrality within and between releases and only be specific when this is strictly required for the realization of interoperable and conform implementations.

- A Release includes a set of specifications by which any user can realize an ITS implementation, possibly in combination with other specifications.
  A release should be seen as a toolbox by which any stakeholder, group of stakeholders or other organizations can realize an ITS system which realizes a specific set of ITS services in accordance with a specific set of ecosystem requirements in mind.

- Functionality specifications should not reference to other functionality specifications except when in a functionality specification there are parameter values which are specified in other functionality specifications. In that case a normative reference to the specifications in which the parameters are specified could be made.

- In addition to functionality specifications, sub-system specifications can exist. Sub-systems often are defined by combining several functionality specifications. As such, in sub-system specifications, normative referencing to functionality specifications is allowed, but circular referencing should be avoided.

- A functionality can also be specified by a set of specifications, generally this happens when the functionality has components at more than one layer. In that case a top, often architectural normative specification is the leading document for that functionality which can have normative references to layer specific specifications.

- A release could include ecosystem profiles in separate clauses and identified as examples in case there are also other profiles defined elsewhere.

ITS Domain related principles:

- For any functionality, the spectrum efficient use should always be considered at the ecosystem level and therefore in the related profile, to avoid the influence on other functionality operations in the same spectrum.

- In case multiple ecosystems make use of the same spectrum, agreements are needed between those ecosystems to ensure correct operation of each of them.

- A specific release is the extension of the previous release. It includes all elements which support the realization of ITS services as supported in the previous release(s). For the sale ITS services, A release is backward compatible with all previous releases.

An ITS-S based on Release x+1 (Rx+1) is backward compatible with an ITS-S based on Release x (Rx) when:

- Rx+1 is able to obtain the same level of services of Rx in an environment based on Rx (see also Figure 14); and

- Rx+1 is specified in a such a way that Rx is able to maintain its full functionality in an environment based on Rx+1 (see also Figure 15). For C-ITS this is a regulatory requirement. At present there are no Backward compatibility regulatory requirements for other Ecosystems.

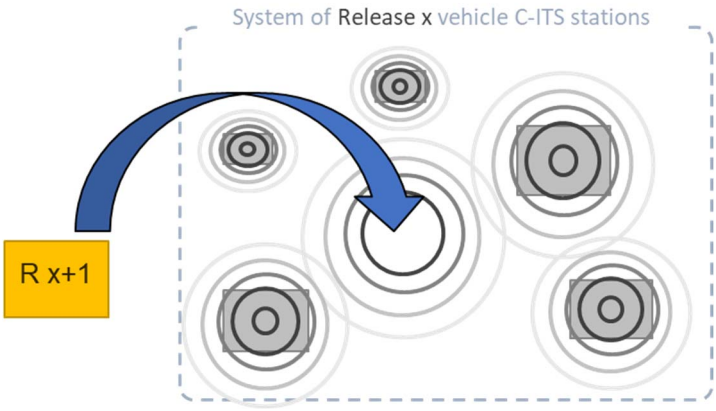

Figure 14: ITS stations implemented based on Release X+1 obtains the same level of services of a Release x station

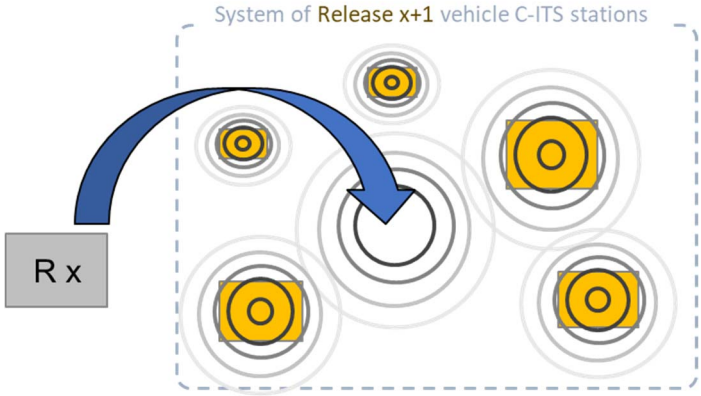

Figure 15: ITS stations implemented based on Release x maintains its full functionality in an environment based on Rx+1

6.4 Release management

A Release represents a toolbox including functionality, cross-layer sub-system and testing specifications as well as context and study reports. Besides the toolbox, system specifications and system profiles could complement the toolbox as system implementation specifications.

All the specifications part of a Release are listed in ETSI TR 101 607 [i.1] which is one of the framing documents. For Release 1 this is ETSI TR 101 607 [i.1] V1.x.x (for maintenance reasons the present document could still be updated in future) while for Release 2 this will be in ETSI TR 101 607 [i.1] V 2.x.x (the first digit of the version number is in accordance with the release, so 2 is for Release 2)

6.5 Release processes

Release management consists of two main processes:

a) The development process in which specifications part of a release are developed and updated following test and validation.

b) The maintenance process once a given release is "frozen" in which corrections are included with Change Requests (CRs). These CRs, once approved by the Technical Committee (TC), are included in an ERRATA document. An ERRATA document is release specific, but it is required to check all releases to see whether the CRs are applicable to a document part of any other release, in which case the CRs could affect ERRATA documents of other releases. The ERRATA documents are always publicly available.

7 ETSI ITS deliverables

7.1 Introduction

ETSI deliverables have different purposes within the equipment development process, see ETSI drafting rules [i.3]. These documents follow the standard template formats. For users of the standards, it gives a recognizable format allowing easy reading. For standardization experts the template complemented with the ETSI Drafting Rules [i.3] provide the bases for qualitative standard creation.

Within ETSI ITS, mainly the following types of documents are in use: European Norms (EN), Technical Specifications (TS) and Technical Reports (TR). The first 2 are normative specifications which provide requirements for specific functionalities, sub-systems or systems. The TR is an informative document type which can be used for clarifications of aspects specified in one or more TSs or ENs. It can also be used to reflect the results of a study to explain why a specification included specific requirements. ENs are specific for Europe and are always transposed at national level..

In addition, there are some ETSI ITS specific aspects which complement the ETSI Drafting Rules [i.3] and are added for quality and consistency reasons.

Clause 7.2 provides a perspective on how the ETSI ITS deliverables should be seen as part of the equipment development process and how they relate to each other. The following clauses provide a guidance on how to look at the purpose of each of the clauses in the ETSI ITS deliverables in addition to the document templates as provided by ETSI.

It should be noted that, in general a standard specification only includes interoperability and conformity requirements to allow each interested enterprise or consortium or group to create its own system specification and to allow them to differentiate in an open market following, for instance in Europe, the open market Regulation (EU) 2022/2065 [i.4].

Although a standard is a technical specification and therefore is technology specific, it should allow to add additional technical possibilities and maximize the technology neutrality. This technology neutrality does not need to be specific for a standard itself, but it is required in general, meaning that as long as it is possible to create another standard allowing other technologies, each of these standards can be considered technology agnostic. ETSI ITS standards follow the ETSI drafting rules [i.3] and by that comply with Regulation (EU) 2022/2065 [i.4].

7.2 ITS documents in the development process

In the equipment realization process, the V-model identifies the definition, testing and possibly integration specifications (profiles). A single or a set of specifications could define a single functionality up to a complete system. Equipment in general is vendor specific while the realization can be based on proprietary specifications only, standards or both of them.

In case the equipment of one vendor needs to be interoperable with the equipment of one or more other vendors, they can form a group to come to common interoperable specifications, often called profiles. Profiles can be managed by such groups themselves or be realized as a standard via an SDO such as ETSI. An example of ETSI ITS related Ecosystem profiles are the HMI ITS-Ecosystem MirrorLink® [i.5]specifications and the ITS Profiles for the sidelink LTE-V2X and sidelink 5G-NR profiles as captured in ETSI TS 103 723 [i.13].

Equipment could include a number of ICT systems from which several ITS related sub-systems. For instance, there is equipment which includes a C-ITS Eco-sub-system, ICT sensor sub-system and a DFRS Eco-sub-system.

Four system interoperability levels can be distinguished.

- **Party specific equipment implementation specifications:**

  All specifications up to the system architecture specification are proprietary, which means that solution and technical architectural requirements and exclusive for the specific party. They are not shared with other parties.

- **Private and/or public partnership system interoperability profiles:**

  If applicable, related specifications are often realized in so called system design profiles based on common interest between the contributing parties. Such profiles can be maintained by a specific stakeholder in common agreement, by a defined organization, a Standardization Development Organization (SDO) or by an authority.

- **Sub-system design specifications:**

  Sub-system specifications have the objective to realize interoperability and conformity at a sub-system level. A sub-system is a specific composition of 2 or more functionalities (building blocks) which together realize a specific higher-level functionality which as a hole cannot operate by itself as it is not a system by itself. Sub-system specifications are technical specific and as much as possible technology agnostic to enable the use in different system configurations.

- **Functionality design specifications:**

  Functionality specifications have the objective to realize interoperability and conformity at a building block level for a specific functionality so they can be used to realize private and public partnership profiles or be used in sub-system specifications. Functionality specifications are technical specific and as much technology agnostic as possible to enable the use in different system configurations.

NOTE: In the above the terms system and sub-system are used the context of ITS-S system definition.

To ensure that sub-system and functionality specifications can be combined without a specific system in mind some specific parameters should commonly be agreed. Within ETSI ITS at present the following supporting layer related specifications have been identified: Common Data Dictionary (CDD), encoding rules, AIDs, port-numbers and geographical area definitions. These common specifications can be normatively referenced in the functionality specifications. See clause 7.3 below.

For the test and integration specifications there are 3 levels.

- **Party specific equipment testing specifications:**

  For the verification and validation of equipment a party specifies system, sub-system and functionality testing specifications. These specifications are based on the party specific design specifications.

- **Private and/or public partnership system interoperability testing:**

  If applicable, these testing specifications are based on the related system design profiles and are meant to test the system or sub-system aspects. Such testing specifications can be maintained by a specific stakeholder in common agreement, by a defined organization, a Standardization Development Organization (SDO) or by an authority.

- **Sub-system and functionality testing specifications:**

  Sub-system testing and functionality testing specifications are directly linked to the related design specifications. In this case, compliance with the testing specifications implies compliance with the related interoperability and conformance requirements.

Within the context of ETSI ITS, sub-system and functionalities are specified in TSs and ENs.

7.3 ITS documents - purpose in perspective

The various documents in a release all have a specific role in the development process. The most basic difference is identifiable in the development process V-model. In the V-model the design specifications are separated from the testing (verification and validation) related compliance specifications. Further at the design side of the V-model, framing, layer studies and specifications can be recognized.

Framing documents provide context to the standards within the ITS domain. They provide information about how these standards could be used. Framing documents provide a general perspective and how the different aspects relate and should be seen in relation to each other.

Part of a set of specifications are various study documents. Layer studies and specifications follow the ITS-S architecture structure as illustrated in clause 5.3.2.

From a document perspective besides layer specific documents there are also cross layer functionalities which may reside at any layer depending on the implementation.

Figure 16 provides an overview of the document purposes and relations. Except for the contextual framework and system profiles, the other specifications and supporting documents are part of the ITS-Toolbox. A toolbox is a set of specifications to support the realization of ETSI based ITS ecosystem profile. Profiles can be part of the ETSI list of ITS release specifications or can be realized by other organizations such as C2C-CC [i.17] and C-Roads [i.16].

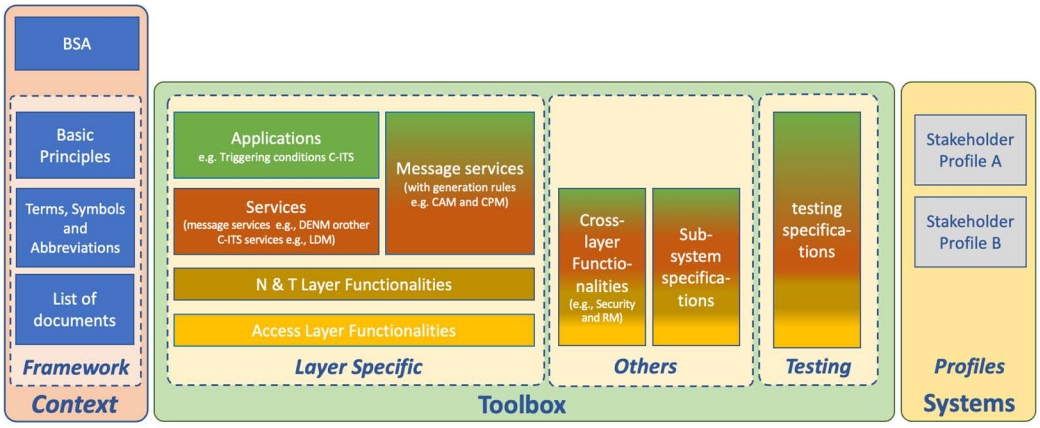

Figure 16: ITS Document purposes

7.4 ETSI ITS standards structure

7.4.1 Introduction

This clause provides a structure of the ITS standards documents. There are several types of ETSI standard documents [i.19], but the main documents used in ITS are European Norms (EN), Technical Specifications (TS), and Technical Reports (TR). See ETSI drafting rules [i.3].

For the purpose of the framework in the following clauses the document approach within ITS is generally addressed.

7.4.2 Document Title

The following structure for the title should be used for ETSI ITS deliverables:

1) Intelligent Transport Systems (ITS);
2) the document purpose (for clarification see clause 7.3):
   a) Framework;
   b) Access Layer, Networking & Transport Layer, Facilities Layer and Applications;
   c) Cross-Layers;
   d) Sub-System;
   e) Testing (identify whether this is profile, sub-system or functionality specific);
   f) Profile (which could be system and communication profiles);
3) the core functionality title;
4) the sub-functionality title (Sub-Part);
5) the sub-sub-functionality title (Sub-Sub-Part); and
6) Release x.

The numbers 4 and 5 are not applicable for TRs.

7.4.3 The table of contents

All ETSI ITS documents should include an introduction (see clause 7.4.4). Except for Technical Reports, the ETSI ITS documents should not include a summary. A summary should be included in a Technical Report to sum up the results of the study.

The following clauses are expected to be included in an ETSI ITS deliverable:

1) Scope.

2) Informative and/or Normative references as applicable.

3) Definitions of terms, symbols, and abbreviations.

   Generic ITS terms, symbols and abbreviations are defined in ETSI TR 103 902 [i.2]. Therefore, this clause should contain only terms, symbols, and abbreviations which are specific for the document.

4) Service introduction clause

   This clause is intended to provide a view of the service provided by the functionality/sub-system specified, context and/or background information. The context identifying the relation of the specified functionality or sub-system within one or several system configurations in which is expected to operate should be included. No requirements should be added in this clause.

5) Service description clause

   This clause is intended to describe the functionality/sub-system specified and its possible relation with other functionalities/sub-systems. The description is expected to be informative and could include general aspects of interfaces for which the requirements are expected to be specified elsewhere.

6) Requirements clause(s)

   The document should include at least one clause specifying mandatory/optional service specific interoperable requirements such as the component behavioural requirements and interface(s) requirements which are specific for the specified functionalities/sub-systems. Data formats, protocols etc, should also be included as applicable. It is advised to use separate clauses for the different items to be addressed.

7) Informative and Normative Annexes, as applicable.

ETSI ITS Technical Reports (studies) cannot include any requirements, normative references or normative Annexes being, by definition, informative reports (see ETSI drafting rules [i.3]).

More information on the content of the clauses is provided below.

7.4.4 The Introduction

The introduction should provide a clarification of the intent of the document and how it relates to other ITS documents. It should not reflect the scope or the context as this is content related and should be part of the "body" of the document.

7.4.5 Service introduction clause (the context)

This clause provides the user of the document an overview of the context in which the content of the document can be used and where to look for possible related documents.

The context can consist of aspects like background, the origin or reason of having this document. Often in this part Ecosystem aspects relevant for the implementation are expressed. Enterprise or Solution architecture illustrations can be used to show such context. Further possible relations with other functionalities or systems from a general perspective can be of relevance to the user of the document. When it is relevant to indicate multiple architecture illustrations, Annexes should be used.

The content of this clause should be limited to only those aspects which are required for the understanding of the implementation of the standard. Technical architecture illustrations are not applicable.

If the document intends to specify a specific part of a functionality while the whole functionality is specified in a set of documents, this set of documents has a leading architectural document including a normative functionality architecture specification. This document is the main one and should reference to the other documents normatively. The document specifying a part of the functionality (not the main one) should therefore clarify that it is part of a functionality "in an informative way".

7.4.6 Service description clause (the functional description)

This clause should be seen as the introduction to the subsequent technical clauses of the study or specification and should provide a general explanation of the studied or specified functionality, of what it is composed and how it in general behaves.

In case of normative specifications (EN or TS), the following should be considered for this clause:

1) Depending on whether functionality or sub-system specified is hardware or software dependent, specific terminology can be used.

2) In case the functionality being specified is software-oriented, UML modelling should be used to describe the internal components and interfaces. It can include UML flow diagrams to present behaviour.

3) In case the functionality is hardware oriented a hardware architecture could be used as illustration. Often UML flow diagrams are used to illustrate the possible behaviour. See clause 5.3.3 for more details.

4) In case a functionality specified includes both software and hardware both 2. and 3. above apply as long as it is ensured that the result is implementable.

In case of Technical Reports (TR):

Technical Reports are not normative and are mostly realized to provide study results and potential standardization items (pre-standardization). A TR therefore only includes descriptive clauses while the results are provided in a summary.

7.4.7 Requirement clauses (functional specification)

For an EN or TS, these clauses define and specify the interoperable requirements.

If a functionality consists of components or entities having internal and external interfaces, their behaviour, and data- and management flows should be defined. For readability the different aspects should be defined in separate clauses.

Only when the internal interfaces are testable, should the requirement on these interfaces be included .

In case the functionality is specified in a single specification, there should not be any normative or informative references to other ITS functional specifications. There can only be normative references to prescriptive documents such as the CDD, port-numbers or AIDs specifications. See clause 7.2 for more details.

In case the functionality is specified in a set of specifications (and therefore a single specification defines only a part of the functionality), normative references to other specifications on the same set are possible (see clause 7.4.5).

7.4.8 Annexes

See the ETSI drafting rules [i.3] for more information on Annexes.

Annex A:
Example of an ITS functionality architecture representation

As an example, Figure A.1 shows what is expected in functionality specifications for the Cooperative Awareness Service. For that an implementer should use the appropriate specification. The architecture illustration allows the implementer to verify in the system specifications whether or not to support those interfaces identified and what related behaviour on these interfaces is expected.

In Figure A.1, a system concept is presented identifying possible relations with other functionalities within the same and other layers. Interfaces could exist but not necessarily.

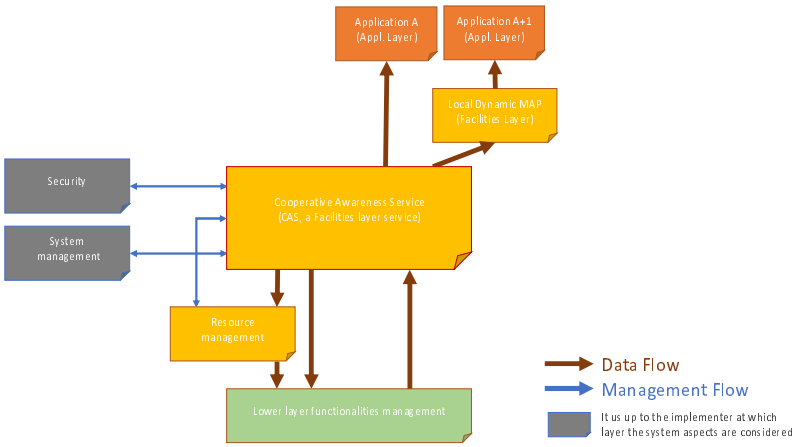

Figure A.1: An example - CAS architecture

A facilities layer service could be part of a communication system which includes a Management Information Base (MIB). In case an MIB exists, or possible other system management functions and system management interface can exist. A Management system is a functionality which can reside at any layer and is characterized being active at the management plane. Alternatively, communication aspects can be statically configured.

In case there is no MIB, no RM and no LDM, the CAS has only data flow interfaces directly going to application layer sinking information and have sourcing and sinking interfaces to lower layers, all depending on the system configuration.

As can be seen the layers are not drawn but are made clear in the descriptions included in the body text or the figures to realize simple diagrams. This way of illustrating functionality behaviour is similar to the processes in other SDOs.

Annex B:
UML models

The Unified Modelling Language (UML) is a general-purpose visual modelling language that is intended to provide a standard way to visualize the design of a system. It delivers a standard notation for various types of diagrams e.g. behaviour diagrams, interaction diagrams, and structure diagrams.

UML offers a way to visualize a system's architectural blueprints in a diagram, including elements e.g. activities (jobs), components of the system, how the system will operate, entities interact with each other and external interfaces.

UML is not a development method by itself. UML provides a standardized partial graphical representation of a functionality or system. UML has many diagrams but the main three usable for standardization are the Component diagram, the Flow (or State) diagram and the Sequence diagram model.

Specific for Use case descriptions, UML Use case diagrams are used and are also called actors diagrams.

UML can be used at different abstraction levels. Within ETSI TC ITS documents UML drawing tools should be used to keep conformity among the different ETSI ITS deliverables.

A component diagram illustrates the different entities part of a functionality and their relations internally and/or externally. See for an example Figure B.1. In standards the internal relation is only reflected in case there is an interoperability concern.

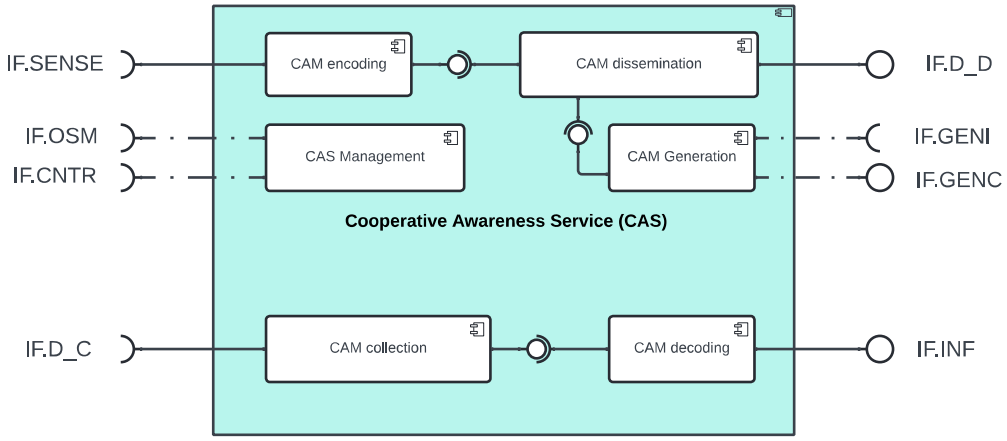

Figure B.1: A CAS component diagram example

A flowchart (see Figure B.2 for an example), shows the flow from one activity to another in a system or process. It is used to describe the different dynamic aspects of a system and is referred to as a 'behaviour diagram' because it describes what should happen in the modelled system.

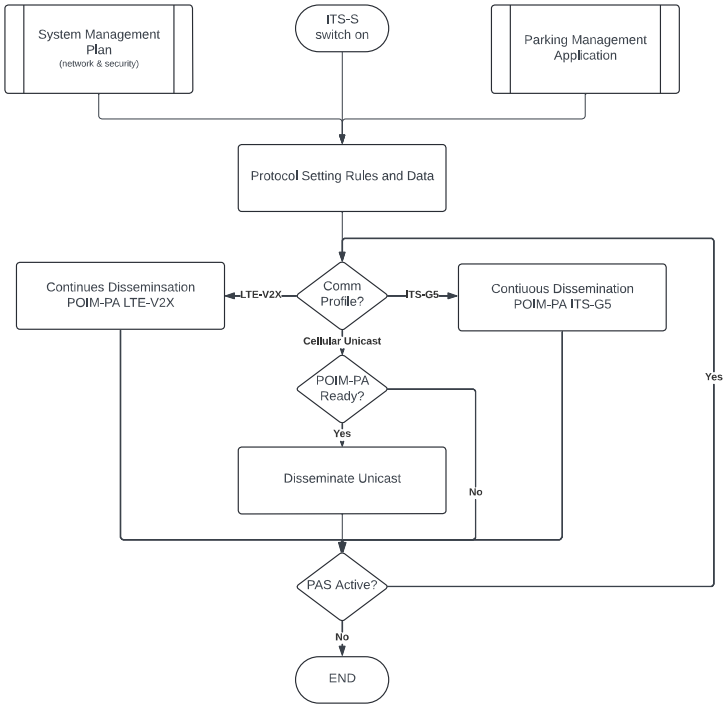

Figure B.2: A PAS Flow (State) diagram example

A sequence diagram(see Figure B.3 for an example) shows process interactions arranged in time sequences. A sequence diagram depicts the processes and actors involved and the sequence of messages exchanged as needed to realize a use case or carrying out a functionality.

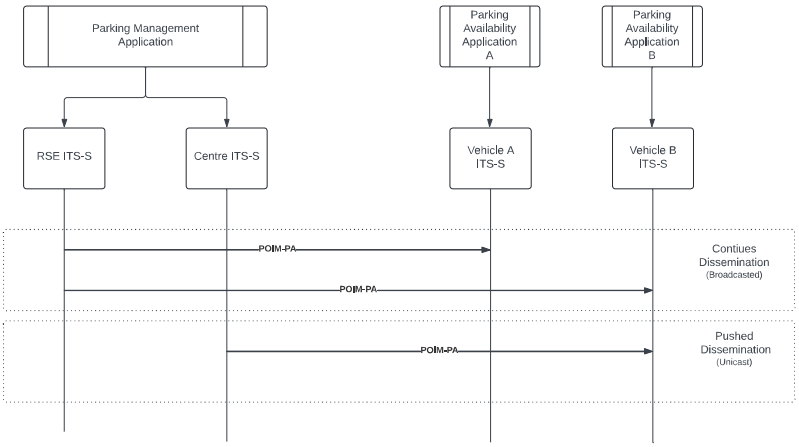

Figure B.3: A PAS service Sequence diagram example

A use case diagram (see Figure B.4 for an example), is a graphical depiction of the actors' interactions. The processes are generally represented by either circles or ellipses and the actors are often shown as stick figures.

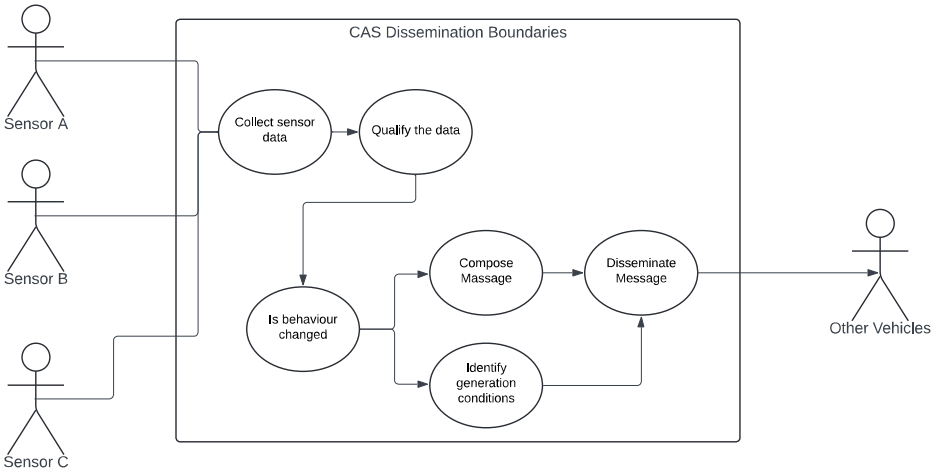

Figure B.4: A CAM dissemination Use case diagram example

Annex C:
C-ITS Communication Architecture

For the exchange of information between ITS stations, any communication method can be used as long as it satisfies the functional, operational, and legal requirements defined by the ITS services it should support.

Figure C.1 shows the C-ITS communication architecture including information sharing via direct AdHoc communications and infrastructure-based cellular 3G, 4G, and 5G communications to enable also the information exchange via cellular networks within the same C-ITS Ecosystems. Figure C.1 shows that the information managed at the traffic management centre may use direct ad-hoc communication and/or cellular networks for its information distribution depending on the ITS service to be provided.

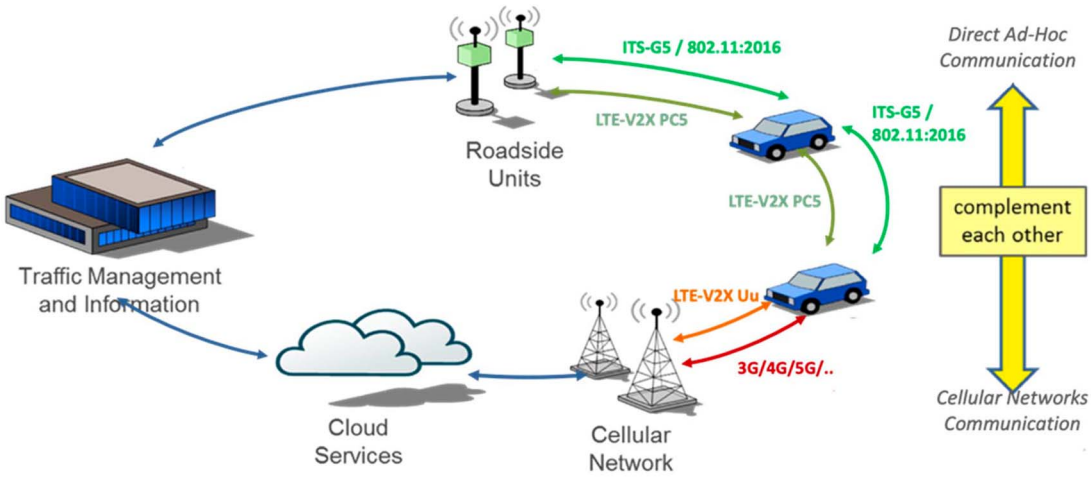

Figure C.1: C-ITS Communications

History

Version	Date	Status
V2.1.1	March 2026	Publication