TECHNICAL REPORT

ISO/TR 21186-2

First edition
2021-02

Cooperative intelligent transport systems (C-ITS) — Guidelines on the usage of standards —

Part 2: Hybrid communications

Systèmes de transport intelligents coopératifs (C-ITS) - Lignes directrices sur l'utilisation des normes —

Partie 2: Communications hybrides

Reference number
ISO/TR 21186-2:2021(E)

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems,* in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/TC 278, *Intelligent transport systems,* in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

A list of all parts in the ISO 21186 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document is part of a family of deliverables from Standard Development Organizations (SDOs) for Cooperative Intelligent Transport Systems (C-ITS), which is a subset of standards for Intelligent Transport Systems (ITS).

ITS aims to improve surface transportation in terms of:

— **safety**

e.g. crash avoidance, obstacle detection, emergency calls, dangerous goods;

— **efficiency**

e.g. navigation, green wave, priority, lane access control, contextual speed limits, car sharing;

— **comfort**

e.g. telematics, parking, electric vehicle charging, infotainment;

— **sustainability**

by applying information and communication technologies (ICT).

In the European Union, the legal framework is given by the European Commissions Mandate M/453 on C-ITS[53], the European Commission Directive 2010/40[52], and the European Commission Mandate M/546[54].

The whole set of standards for deployment of C-ITS is difficult to understand by developers of equipment and software, especially ITS application software, and thus guidelines explaining a beneficial choice of standards (C-ITS Release), the purpose and interaction of standardized features, beneficial implementation approaches and guidance in developing ITS applications are a prerequisite for a fair and open market allowing early deployment of interoperable and future-proof solutions.

The ISO 21186 series provides necessary guidelines in multiple parts, each dedicated to a specific purpose:

— Part 1: Standardization landscape and releases[14];

— Part 2: Hybrid communications (this document);

— Part 3: Security[15].

This document can be complemented by further parts as required, for example:

— Usage of the service announcement protocol specified, for example, in ISO 22418;

— Dynamically extendable data and protocol parameters ("Information Object Classes" and "Information Object Sets"; based on ASN.1 type CLASS);

— Usage of the GTDM framework specified in ISO/TS 21184[1)].

The purpose of this document is thus to inform about relevant standards and to describe the functionalities of the ITS station architecture defined in support for hybrid communication technologies. It is intended to serve as a guideline to structure the development of new C-ITS standards and to harmonize the deployment of C-ITS services relying on the use of hybrid communication technologies. It also intends to give support to the developers of standards defining C-ITS services and to the developers of C-ITS solutions and ITS applications complying with the ITS station architecture and its set of functionalities supporting hybrid communications.

1) Under preparation. Stage at the time of publication: ISO/PRF TS 21184:2021.

At time of writing this document, no applicable Intellectual Property Rights (IPR) issues were known related to this document. However, this document references standards, for which IPRs are known. Information on such IPRs is expected to be provided in those respective standards, which might be from any one of the Standards Development Organisations working on ITS or C-ITS.

Referencing other SDOs and their respective deliverables in no way is to be understood as an endorsement, but rather as an informative piece of information.

More details on the C-ITS domain can be found in the Brochure cited in Reference [58].

Cooperative intelligent transport systems (C-ITS) — Guidelines on the usage of standards —

Part 2: Hybrid communications

1 Scope

This document serves as a guideline explaining the concept of hybrid communications and support functionalities for Cooperative ITS services deployed in conformance with the ITS station architecture and related Cooperative ITS standards.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
access technology
technology employed in a communication interface to access a specific medium

[SOURCE: ISO 21217:2020, 3.1]

3.2
communication adaptation layer
CAL
set of protocols and functions to adapt access technologies to the *ITS-S networking and transport layer* (3.20)

[SOURCE: ISO 21217:2020, 3.3]

3.3
hybrid communications
composition of multiple access technologies and communication protocols combined to provide complementary or redundant communication channels

[SOURCE: ISO 21217:2020, 3.7]

3.4
hybrid communication support
feature of an ITS station used to combine multiple access technologies and protocols

[SOURCE: ISO 21217:2020, 3.8]

3.5
hybrid ITS service
ITS service that relies on *hybrid communications* (3.3)

[SOURCE: ISO 21217:2020, 3.9]

3.6
ITS station
ITS-S
functional entity comprised of an *ITS-S facilities layer* (3.13), *ITS-S networking and transport layer* (3.20), *ITS-S access layer* (3.7), ITS-S management entity, ITS-S security entity and *ITS-S applications* (3.9) entity providing ITS services

Note 1 to entry: From an abstract point of view, the term "ITS station" refers to a set of functionalities. The term is often used to refer to an instantiation of these functionalities in a physical unit. Often, the appropriate interpretation is obvious from the context. The proper name of the physical instantiation of an ITS-S is ITS station unit (ITS-SU).

[SOURCE: ISO 21217:2020, 3.15]

3.7
ITS-S access layer
protocol layer in the ITS-S reference architecture containing the OSI physical and data link layer protocols for ITS communications

[SOURCE: ISO 21217:2020, 3.16]

3.8
ITS-S access technology
access technology (3.1) dedicated to operation in an *ITS station* (3.6)

[SOURCE: ISO 21217:2020, 3.20]

3.9
ITS-S application
ITS-S application process (3.10) residing in the ITS-S application entity

[SOURCE: ISO 21217:2020, 3.21]

3.10
ITS-S application process
element in an *ITS station* (3.6) that performs information processing for a particular application and uses ITS-S services to transmit and receive information

[SOURCE: ISO 21217:2020, 3.22]

3.11
ITS-S capability
uniquely addressable protocol or functionality that is part of an *ITS-S managed service entity* (3.19)

Note 1 to entry: Examples of ITS-S capabilities in the *ITS station* (3.6) facilities layer are generic *ITS-S facilities layer* (3.13) services specified in ISO/TS 17429 (Communication Profile Handler, Facilities Services Handler, Content Subscription Handler), the position and time service defined in ISO/TS 21176, the security services defined in ISO/TS 21177; examples of ITS-S capabilities in the *ITS-S networking and transport layer* (3.20) are IPv6 functionalities defined in ISO 21210 (IPv6 neighbour discovery, IPv6 forwarding, IPv6 mobility support, etc.), the fast service announcement protocol defined in ISO 22418, etc.

[SOURCE: ISO 21217:2020, 3.24]

3.12
ITS-S communication profile
ITS-SCP
parameterized ITS-S communication protocol stack (set of protocols composing all the *ITS station* (3.6) layers) that allows communication end points to communicate with one another

[SOURCE: ISO 21217:2020, 3.25, modified.]

3.13
ITS-S facilities layer
layer in the ITS-S reference architecture containing OSI layers 5, 6 and 7 that connects applications to the *ITS-S networking and transport layer* (3.20)

[SOURCE: ISO 21217:2020, 3.31]

3.14
ITS-S flow
identifiable sequence of packets of a given *ITS-S flow type* (3.16) transmitted between a source node and a destination node.

[SOURCE: ISO 21217:2020, 3.36]

3.15
ITS-S flow identifier
identifier, being unique within an *ITS station* (3.6) unit, that identifies an *ITS-S flow* (3.14)

[SOURCE: ISO 24102-6:2018, 3.9]

3.16
ITS-S flow type
set of characteristics describing a data flow

[SOURCE: ISO 21217:2020, 3.37]

3.17
ITS-S flow type identifier
identifier being unique within the *ITS station* (3.6) that identifies an *ITS-S flow type* (3.16)

[SOURCE: ISO 24102-6:2018, 3.11]

3.18
ITS-S host
ITS-S node (3.21) comprised of ITS-S functionalities other than the functionalities of an *ITS-S router* (3.23), ITS-S border router, ITS-S mobile router, or an ITS-S gateway

[SOURCE: ISO 21217:2020, 3.39]

3.19
ITS-S managed service entity
MSE
uniquely addressable entity in an ITS-S layer comprised of a set of related ITS-S capabilities

Note 1 to entry: Examples of ITS-S managed service entities are: a communication module in the ITS-S access technologies layer (M5, cellular, etc.), a protocol suite in the ITS-S networking & transport layer (IPv6, FNTP, GeoNetworking, 6LoWPAN, etc.), the generic facilities at the *ITS-S facilities layer* (3.13) (COH, FSH, CSH).

[SOURCE: ISO 21217:2020, 3.42]

3.20
ITS-S networking and transport layer
layer in the ITS-S reference architecture containing OSI layers three and four that connects the *ITS-S facilities layer* (3.13) to the *ITS-S access layer* (3.7)

[SOURCE: ISO 21217:2020, 3.46]

3.21
ITS-S node
node comprised of a set of functionalities in an *ITS station* (3.6) unit that is connected to the ITS station-internal network or comprises an entire ITS station unit

[SOURCE: ISO 21217:2020, 3.47]

3.22
ITS-S path
directed sequence of nodes connected by links starting at a source node, traversing a communication interface of the source ITS-S, an ITS-S ingress anchor node and an ITS-S egress anchor node, ending at a destination node

[SOURCE: ISO 21217:2020, 3.48]

3.23
ITS-S router
ITS-S node (3.21) comprised of routing functionalities of an *ITS station* (3.6) unit used to connect two networks and to forward packets not explicitly addressed to itself

[SOURCE: ISO 21217:2020, 3.49]

3.24
localized communications
communications with nearby stations without involving support of an infrastructure network

[SOURCE: ISO 21217:2020, 3.53]

3.25
networked communications
communications using support of an infrastructure network

[SOURCE: ISO 21217:2020, 3.60]

3.26
urban WiFi
short-range *networked communications* (3.25) WiFi *access technology* (3.1) used mostly in urban environments and in personal devices such as smartphones, tablets and laptops

Note 1 to entry: An example of urban WiFi is IEEE 802.11 Basic Service Set (BSS) for WLAN access used in 2,4 GHz or 5,4 GHz frequency range.

3.27
vehicular WiFi
short-range *localized communications* (3.24) WiFi *access technology* (3.1) specifically designed for vehicular localized communications

Note 1 to entry: An example of vehicular WiFi is IEEE 802.11 operating outside the context of a Basic Service (OCB), also known as IEEE 802.11p[51], used in the 5,9 GHz frequency range reserved for ITS services with profile standards named ITS-G5 (ETSI) in Europe and Australia, and US-DSRC in North America and their harmonization at ISO (ITS-M5).

4 Symbols and abbreviated terms

CAM	cooperative awareness message
C-ITS	cooperative intelligent transport systems
CPH	communication profile handler
CSH	content subscription handler
DENM	decentralized environmental notification message
DSRC	dedicated short-range communication
ETSI	European Telecommunication Standards Institute
FSH	facilities service handler
IEEE	Institute of Electrical and Electronics Engineers
IPv6	internet protocol version 6
ITS	intelligent transport systems
ITS-SU	ITS station unit
LDM	local dynamic map
LiFi	light fidelity
LoRA	long range
LTE-V2X	long term evolution based vehicle-to-everything
OCB	outside the context of a basic-service set
OSI	open systems interconnection
PVT	position, velocity and time
SDO	standards development organization
US-DSRC	american dedicated short range communication
V2X	vehicle-to-vehicle and vehicle-to-roadside
WiFi	wireless fidelity
WSMP	wave short message protocol

5 Motivations for hybrid communications support

5.1 Connected and cooperative mobility

Intelligent transport systems (ITS) services are traditionally ranged into three categories: road traffic safety, traffic efficiency and comfort (infotainment, value added services, etc.).

ITS services were initially deployed either in the roadside infrastructure (variable message signs, etc.), in vehicles (telematics) or nomadic devices (navigation, traffic alerts, etc.) with little or no interaction between the vehicles, other road users and the roadside infrastructure. With the advent of short-range communication technologies, ITS services using the exchange of data between vehicles and the roadside infrastructure then started to appear (electronic fee collection[2],[36]-[38], electric-vehicle charging[3], emergency call[39], etc.). These ITS services are specified to operate in a very controlled environment, with a very specific radio technology, and for a very specific purpose.

While recent generations of vehicles are deployed with built-in communication systems providing connectivity to remote platforms providing services (navigation, software update, telematics, electric vehicle charging, emergency call, etc.), the forthcoming generation of vehicles will cooperate with their surrounding environment (other vehicles, other road users, roadside infrastructure and urban infrastructure). This localized exchange of data improves road safety (crash avoidance, obstacle detection, etc.) and traffic efficiency (traffic information, green wave, lane access control, contextual speed limit, etc.).

Cooperative ITS (C-ITS) services, i.e. ITS services for connected and cooperative mobility that rely on the data exchanged between vehicles (cars, trucks, buses, etc.), other road users (pedestrians, cyclists, etc.), the roadside and urban infrastructure (traffic lights, road tolls, etc.) and control and services centres in the cloud (traffic control centre, service providers, map providers, etc.), and especially on the sharing of data amongst service domains and applications of the same service domain, are thus being developed. See Figure 1.

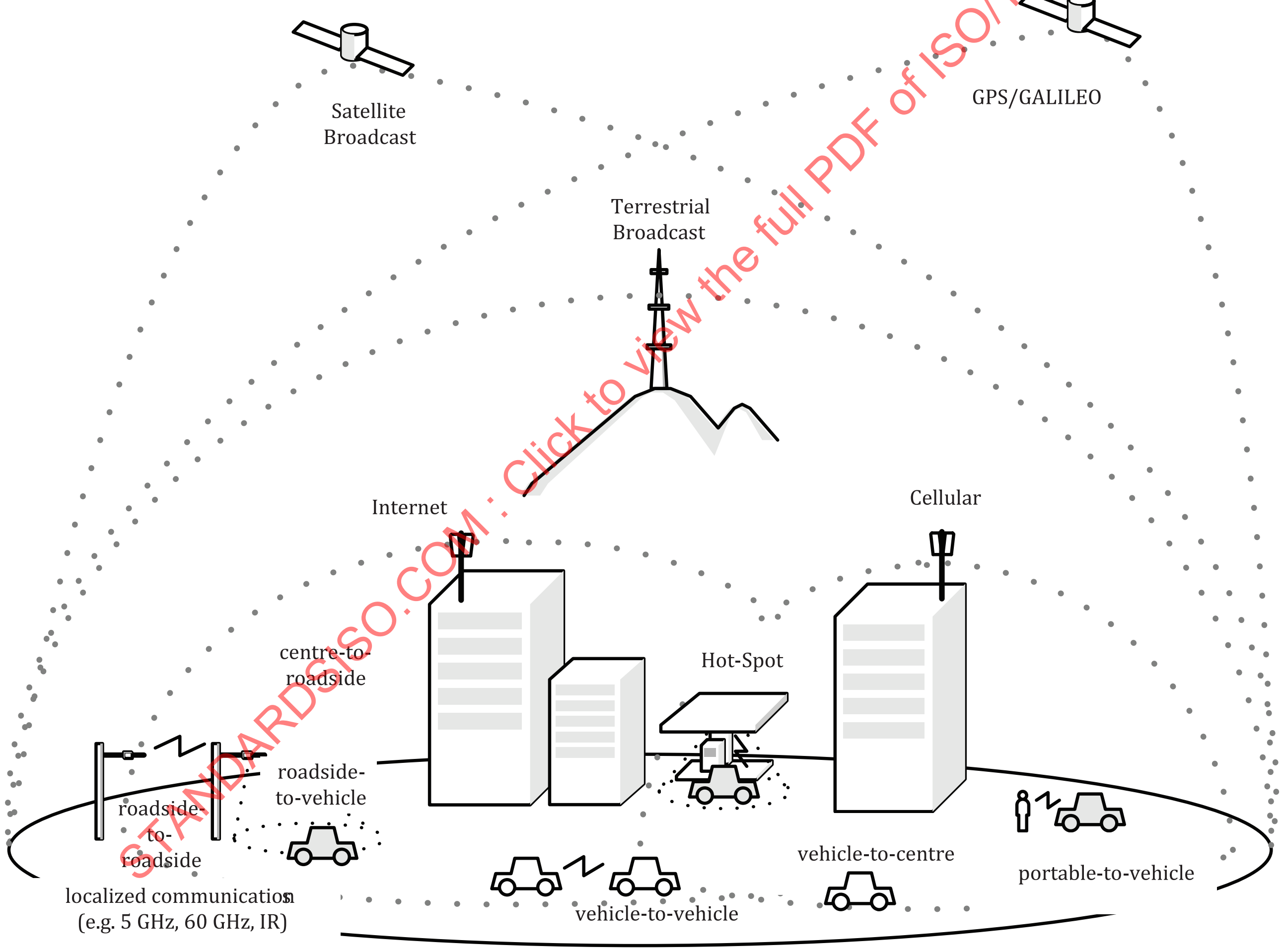

Figure 1 — Connected and Cooperative Mobility

However, distinct C-ITS services have diverging communication requirements (distribution area, amount of data, delivery delay, privacy, confidentiality, etc.). No single communication technology is able to fulfil all of these requirements at once.

Many communication technologies are available today on the market (cellular 3G/4G, infrared, LiFi, satellite, urban WiFi, vehicular WiFi, LoRA, etc.) and new promising technologies appear regularly. They have very different characteristics (radio coverage range, bandwidth, propagation delay, reliability, price, transmission power), and are more or less prone to security threats (denial of service, intrusion, impersonation, observation). Each of these access technologies has its own benefits and drawbacks with respect to the type of service that is to be delivered.

Due to their diverging characteristics, their geographic penetration, and regional regulations, the combination of several access technologies and protocols is beneficial or even necessary for ensuring reliability, interoperability and sustainable development of C-ITS services. This requires a common approach to the way security, communications and data are handled.

Before requirements for this common approach are discussed in 5.3, subclause 5.2 presents examples illustrating the need to combine a diversity of access technologies.

5.2 Examples of use cases requiring a diversity of access technologies

5.2.1 Road hazard notification (use case 1)

Road hazards present road safety risks that could be leveraged using localized communications (using vehicular WiFi in the 5,9 GHz frequency band, for example) and networked communications (using 3G/4G cellular technology, for example). A typical example is black ice on the road as illustrated on Figure 2.

A vehicle equipped with sensors can detect black ice. If it is equipped with localized communications capabilities it can inform subsequently following vehicles so that they reduce speed in due time and take other automatic actions to ensure safety. All equipped vehicles can relay this alert from vehicle to vehicle, but at some point, there will not be any vehicle able to relay this message further. Consequently, an approaching vehicle still kilometres away will not be informed.

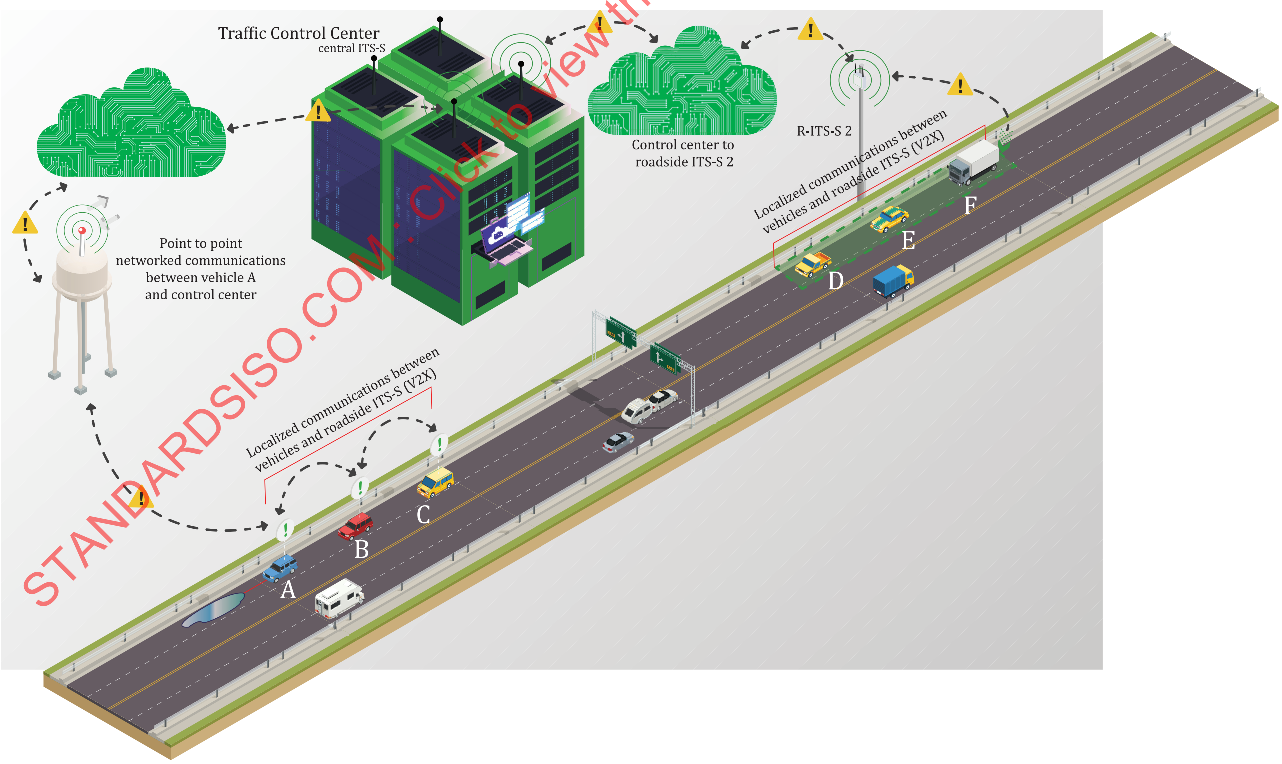

Figure 2 — Black ice notification using hybrid communications (FP7 GeoNet[64])

To ensure wide transmission of the alert, vehicles that detect the hazard could transmit a road hazard alert to the road traffic control centre, either directly using networked communications, or through a nearby roadside ITS station unit ("RSU" on Figure 2) using localized communications. The road traffic control centre can thus take necessary actions, like sending a patrol vehicle to secure the area, and inform road users.

In turn, the road traffic centre could inform vehicles approaching the risk area through a roadside ITS station unit located on the road upstream of the risk area that would repetitively broadcast the alert using localized communications or display the hazard through a variable message sign board. Alternatively, the road traffic centre could directly inform each of the vehicles subscribed to a road hazard alert service through networked communications. Such notification could be used to advise vehicles on alternative itineraries.

This example shows the value of using both localized and networked communications to inform vehicles and the control centres about road hazards so that the road hazard alert can be transmitted more widely and effectively. Localized communications are used to inform about an immediate time-critical danger, whereas networked communications are used to inform about dangers upstream of time and location.

5.2.2 Emergency call (use case 2)

A new series of vehicles are now placed on the market with an "emergency call" service which alerts public safety services in case of an accident.

At the time of writing this document, this road safety service relies on a 2nd generation cellular technology with limited capabilities and limited coverage. However, there will continuously be geographical areas not covered by the cellular network, either because there is no base station in the vicinity or because the service is disrupted or overloaded. In such a situation, the emergency call cannot be issued, although access technologies alternatives are available that could replace or complement the cellular network.

A case in which localized communications technologies could be useful is a situation in which a vehicle has driven off the road and has fallen into a canyon. The passengers are still alive, but unable to get out of the vehicle. There is no cellular coverage, so the emergency call cannot be transmitted. However, the vehicle is not far from the road and is in radio coverage using localized communications. If the emergency call could be supplied over that localized communications link in addition to the cellular network, passing-by vehicles could get the emergency call and relay it to public safety services as soon as they are in cellular radio coverage, or when they reach a roadside ITS station unit ("RSU").

A first related standard on "eCall via an ITS station" is CEN/TS 17182[39].

5.2.3 Public transport (use case 3)

Recent fleets of buses are deployed with communication technologies providing different types of services: buses are usually equipped with tracking capabilities to monitor the progress of the bus on the itinerary and inform passengers waiting at bus stops. They are also often equipped with a video capability in order to inform the control centre in an emergency situation; and sometimes with a system allowing priority of buses at crossroads. The newest generations of buses would of course also be equipped with with road safety services (see 5.2.1) and with emergency call (see 5.2.2).

As a consequence, buses are equipped with multiple communication systems. Each service is deployed using its own antenna, radio technology, hardware, software and screen, and has its own proprietary or standardized data format. These frequently duplicate one another, as there could be several communication systems deployed using the same access technology, e.g. cellular. This is not efficient in terms of cost, complexity and reliability. Overall, all of these communication systems are unable to exchange data between one another. An emergency call can thus not be transmitted using an alternative access technology if one fails or if the bus is out of cellular network coverage.

In this situation, a common reference communication architecture is needed to share data between the various communication systems and to combine multiple access technologies and protocols to provide more reliable and efficient services.

5.3 Hybrid communication technologies

As highlighted in the use cases described in 5.2, connected and cooperative mobility services cannot be achieved by a single type of communication technology. Multiple access technologies and protocols are needed and are preferably combined, for several reasons, including:

— to offer extended connectivity to an ITS service;

— to offer complementary or redundant communication channels;

— to address a diverse range of ITS services with varying communications needs;

— to allow future-proof development of specifications;

— to sustain environments with varying connectivity quality.

Combining multiple access technologies and communication protocols into a unified communication system (possibly duplicated for redundancy, or spread in multiple communication units complying to the same communication architecture) is sometimes referred to as "hybrid communications".

The term "hybrid communications" so far has no strict standardized definition and may be interpreted differently from different groups of stakeholders. Some views are:

— It merely means the combination of inter-changeable flavours of short-range access technologies used for localized communications with medium-range communication technologies used for connectivity to the cloud into a single communication system.

— It means the ability to deploy the same C-ITS services either using localized communications in some vehicles or cellular-based networked communications in other vehicles.

— It means having two independent systems integrated into a single platform, one with short range communications for a limited set of services (time critical road safety) and one with long-range communication capabilities for another limited set of services (infotainment, telematics, non-time critical road safety).

More generally, a hybrid communication system can be defined as a communication system combining various access technologies and protocols, used to support a range of applications with different and varying communications requirements.

In the context of C-ITS, the term hybrid communications is defined as multiple access technologies and protocols dynamically managed (combined) to provide complementary or redundant communication channels.

5.4 Unified communication and data management architecture

5.4.1 Requirements for the unified communication and data management architecture

Combining multiple access technologies and communication protocols as advocated in the previous sections requires a common approach on how communications and data are managed in a secure way, i.e. a unified communication architecture is needed.

The unified communication architecture should meet the following requirements:

— meet specific needs of ITS services;

— meet the need of data sharing between ITS service domains (such as public transport, road safety, freight and logistics, public emergency, electronic fee collection);

— meet the need of data sharing between vehicles of any kind, other road users, the roadside infrastructure, the urban infrastructure, control and services centres of any kind, etc.;

— be future proof, by:

  — allowing the future integration of new access technologies and protocols, new services and new data management schemes;

  — facilitating the migration from one earlier deployed technology to a new one;

  — scaling to support a large variety of ITS services;

  — adapting to locally applicable policies and regulations;

  — facilitating the integration of new capabilities (access technologies, communication protocols, mutualized services, etc.);

— to support multiple applications simultaneously, from any of the three categories for road safety, traffic efficiency, and comfort;

— to support hybrid communications in an optimized way, by;

  — meeting distinct and diverging communication requirements;

  — providing redundant or alternative communication channels;

  — combining both localized communications and networked communications.

The following sections of 5.4 detail the impact of supporting a diverse range of communication requirements and communication technologies.

5.4.2 Supporting a diversity of applications with diverging communication needs

Each application that needs to send and receive data has its own communication requirements, as was shown in the examples described in subclause 5.2.

An application is usually either engaged in a bidirectional exchange with known communication peers, or is repetitively broadcasting data to unidentified receivers. The nature of the data transmitted is known by the application and can thus be pre-determined at the communication system level. In addition, a given application may transmit different types of data flows, simultaneously, or in distinct sequences of exchanges over time. Communication requirements specific to the type of each data flow (ITS-S flow type) could thus be expressed in terms of bandwidth, end-to-end delay, security, packet size, etc.

For example, a video-conferencing application may need a voice data flow and a video data flow; a traffic hazard application may have a broadcast data flow (time-critical broadcast to nearby vehicles) and a unicast data flow (non-time-critical notification to a traffic control centre). These two data flows have completely different characteristics, including priority. In a video-conferencing application, the quality of the video data flow can easily be reduced without compromising a discussion, whereas any drop of quality in the voice data flow is prone to misunderstanding. The voice data flow would thus be given a higher priority with more transmission constraints than the video data flow.

5.4.3 Supporting a diversity of communication paths

The communication path (ITS-S path) is the itinerary taken in the network by data transmitted between the sender and the recipient. This itinerary can take an arbitrary number of intermediary steps, i.e. hops. It can be made of zero hop (e.g. transmission between a sender and a recipient installed in the same communication unit), a single hop (e.g. direct transmission between two vehicles), two hops (e.g. transmission between two vehicles via a roadside equipment) or an undefined number of hops (e.g. transmission between two vehicles via the Internet cloud).

Figure 3 illustrates a situation where a vehicle may be offered different communications paths in order to communicate with a communication peer. In this example, the communication peer is another vehicle. Data could be exchanged using localized or networked communication. One of the communication paths may be more appropriate, depending on the type of transmission (volume of data, latency, communication duration, etc.). For road safety like emergency breaking, low-latency localized communications (in broadcast mode) with repetition of the message a few times per second is probably best. For a short duration video transmission, networked communications using WiFi may be best, whilst the networked communications using a cellular link is probably the only option for a long duration session between the two vehicles, since the inter-distance between vehicles varies over time (for example vehicles may be split apart due to traffic congestion).

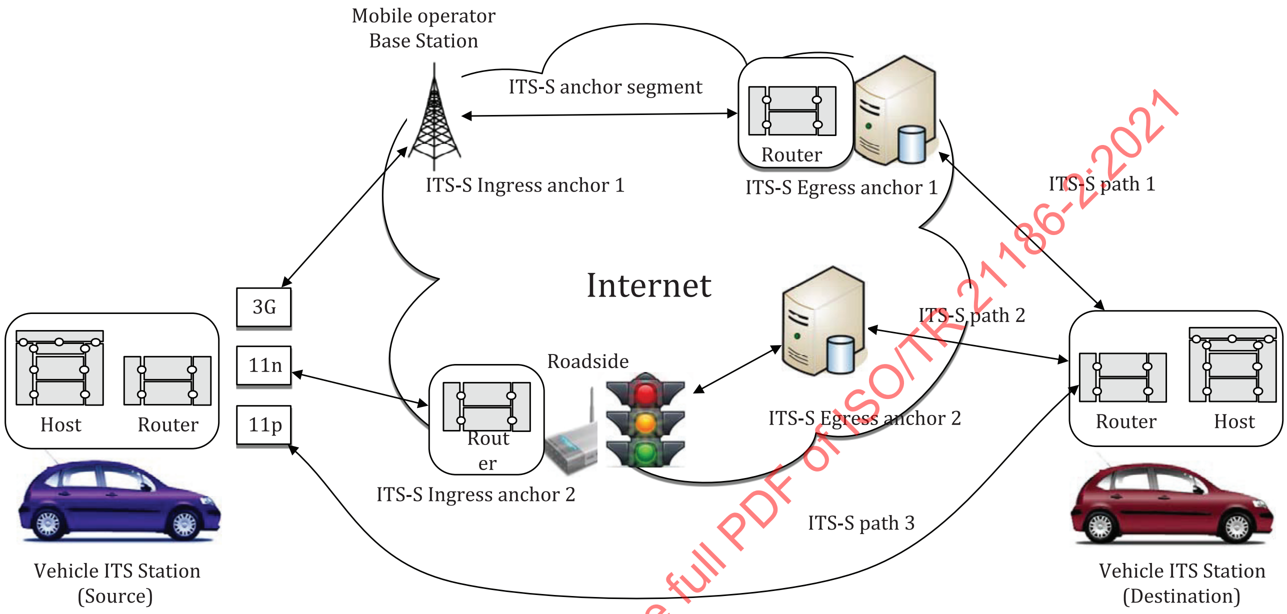

Figure 3 — Multiple communication paths (ISO 24102-6)

5.4.4 Supporting a diversity of access technologies and protocols

5.4.4.1 Networked communications in the ITS station

Networked communications refers to the use of communication technologies that rely on some form of infrastructure network.

Cloud-based services and all services through the Internet typically rely on networked communications. Cellular network access to Internet (ISO 17515-1) with IPv6 (ISO 21210) is an example of a protocol stack for networked communications.

5.4.4.2 Localized communications in the ITS station

One of the main pillars of C-ITS services is localized communications, i.e. communications used for the direct exchange of data between vehicles and their surrounding environment (other vehicles, other road users, roadside or urban infrastructure).

This term incorporates specific types of communications such as V2V (vehicle-to-vehicle) and V2R (vehicle-to-(roadside) infrastructure)[2)] short-range communications around a few hundred meters, and V2P (vehicle-to-pedestrian) using ultra short-range sensor-based communications. It is generally sufficient to use the term V2X, referring to localized communications around the vehicle, as there is no difference between localized communications involving only vehicles from localized communications involving both vehicles, the roadside infrastructure and other road users.

2) Vehicle-to-roadside communications are often referred to as V2I (vehicle-to-roadside infrastructure) but this term is confusing and may also refer to vehicle-to-(telecommunication) infrastructure, so it should be avoided.

In the literature, V2X is sometimes used with the meaning "vehicle-to-everything". However, this is confusing as it may imply that all types of communications technologies involving the vehicle, including networked communications over the cellular network or the satellite network (see sublause 5.4.4.1), which would dismiss any meaning for V2X. To remove confusion, this document uses the terms localized communications instead of using the term V2X.

It is worth noting that "localized communications" covers both broadcast and point-to-point communications.

In general, localized communications is considered as the means of communication when it comes down to road traffic safety and road traffic efficiency services that require real time transmission delays that cannot be met presently by any networked communication technology. As it involves safety aspects, the deployment of localized communications may be enforced by some form of regulation, by e.g. having dedicated frequency band(s) in most regions and continuously being harmonized at the global level.

The most mature localized communication technology is 5,9 GHz vehicular WiFi, i.e. a variant of the 802.11 WiFi technology specifically designed for ad-hoc communications for fast-moving vehicles. This WiFi variant for vehicular communications was originally specified in the IEEE 802.11p group, and is part of IEEE 802.11-2016; it is referred to as 802.11 "Outside the Context of a Basic service set" (802.11 OCB), and is fully integrated in the ITS station architecture.

Profiles of IEEE 802.11 OCB are known as ETSI ITS-G5 (mainly in the European Union and Australia), ITS-M5 (ISO), and US-DSRC (Dedicated Short-Range Communications) (North America). In Europe, CEN DSRC [38,37,36] applies to a 5,8 GHz short range communication technology used mostly for tolling[3].

Other short-range communication technologies such as IEEE 802.15.4 (6LoWPAN) can also be used as localized communications. The integration of 6LoWPAN and CoAP in the ITS station architecture is specified in ISO 19079 and ISO 19080, respectively, with communication profiles specified in CEN/TS 17496.

An emerging localized communications technology is LTE-V2X, specified in the 3GPP Release 14 specifications. This is a variant of cellular technology which, like 802.11 OCB, is specifically designed for ad-hoc communications for fast-moving vehicles. It has been profiled by ETSI TS 303 163 and is considered for China and the USA.

NOTE Whilst networked communications, e.g. cellular communications and access to Internet, can apply the principle of "Technology Neutrality" (allowing simultaneous usage of a mix of incompatible technologies), localized communications between ITS station units has to be based on a specific access technology per service (or service domain) in order to enable interoperability.

6 The ITS station architecture and functionalities in support of hybrid communications

6.1 Origins of the ITS station architecture

This subclause explains the origins of the standardized work that led to the development of a managed and secured harmonized communication and data platform, i.e. the ITS station architecture, illustrated in Figure 4.

3) The term DSRC is also confusing as it stands for different technologies in Europe (CEN DSRC for road tolling) and North America (DSRC for road safety). It should thus be avoided unless the context is precisely mentioned.

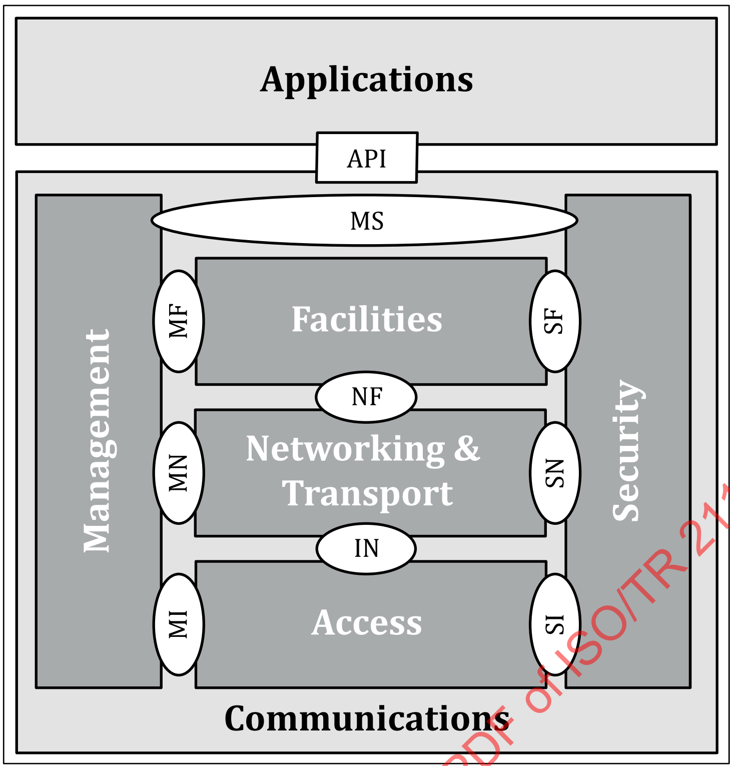

Figure 4 — Simplified ITS station architecture (ISO 21217)

The necessity to combine multiple access technologies and protocols for the benefit of ITS services has been advocated long before the ITS station architecture was revealed and standardized.

Earlier work on a standard communication architecture combining a variety of access technologies and protocols and suitable for a variety of ITS needs was initiated by ISO/TC 204 in the year 2000, simultaneously with work on communication technologies for ITS services. These activities became known under the acronym CALM (Communications Access for Land Mobiles).

From its initiation, the CALM initiative resulted in a communication architecture able to support multiple access technologies, and particularly infrared light[19], microwave communications[20], millimetre wave communications[21], satellite communications[1,32], all generations of cellular communications[7,17,18], visible light communications[25], and others, together with an interface standard ISO 21218 providing a common service access point to the ITS-S networking & transport layer. An essential property of this architecture is that access to data and the communications capabilities is managed and secured. Consequently, a set of station management standards in the series ISO 24102 (station internal management[26], remote station management[27], service access points[28], station-internal management communications[29], path and flow management[30]) was also developed.

Starting from 2006 under the European R&D 6th Framework Program, many research projects worked on similar issues, each of starting to define their own communication architecture, sometimes with their own specific focus e.g. focusing on time critical road safety for the SafeSpot (Cooperative vehicles and road infrastructure for road safety) project, or focusing on services within the interest of road authorities for the Coopers (Co-operative Systems for Intelligent Road Safety) project, while the CVIS (Cooperative Vehicle-Infrastructure Systems) project looked at communications from the perspective of aggregating the different types of ITS services into a common architecture in the same spirit as ISO/TC 204.

To put the development of diverging communication architectures to an end, harmonization between all of these different views was initiated within COMeSafety, a specific support action of the European Commission. The most significant contributors to COMeSafety were representatives from European Projects CVIS, Coopers, SafeSpot, GeoNet (IPv6 GeoNetworking), SeVeCom (Secure Vehicular

Communications) and the Car-to-Car Communication Consortium (C2C-CC), and several other European projects. Their work considered earlier architecture work performed within ISO/TC 204, the birthplace of many of the concepts behind the communication architecture before it was harmonized by COMeSafety. Some of the project participants, and particularly those involved in the CVIS got involved in ISO standardization activities.

The harmonization work conducted within COMeSafety resulted in a detailed list of use cases and the specification of a common communication architecture and terminology agreed between the different participating projects. This common communication architecture is largely inspired from the architecture initially designed by ISO TC/204, with some new concepts.

6.2 Detailed ITS station architecture

The ITS station architecture used in C-ITS standards is the result of the harmonization effort started in 2008. The *ITS station architecture* is a functional architecture defined to manage security, communications and data generically applicable to the three types of ITS services (road safety, traffic efficiency and others). It is specified in ISO 21217 and ETSI EN 302 665[42]. Details of the functional building blocks of the ITS station architecture are specified in a set of related standards.

Figure 5 provides a more detailed description of the ITS station architecture already shown in Figure 4.

The ITS station architecture updates the OSI 7-layer architecture[33] by merging the seven communication layers into three communication layers (*ITS station facilities layer, ITS station networking & transport layer, ITS station access layer*). Further on, it adds two vertical entities, i.e. the ITS station management entity and the ITS station security entity performing a number of cross-layer management and security functions, to explicitly express the high relevance of these management and security functionalities. A middle layer (*ITS station facilities layer*) provides common services to the applications (message handling, service discovery, selection of the communication stack, database of geo-localized events, maps, positioning, time stamping, etc.). Various network and transport protocols are grouped within a single *ITS station networking & transport layer* while the *ITS station access layer* can support any existing and forthcoming access technologies, including vehicular WiFi (ITS-G5 / ITS-M5 / US-DSRC), vehicular cellular technologies (LTE-V2X), urban WiFi (802.11n/ac), cellular (2G/3G/4G), infra-red, satellite, IEEE 802.15.4 (6LoWPAN), 60 GHz millimetre-wave, optical communications, and possibly new cellular-based ones (support for 5G is currently under investigation).

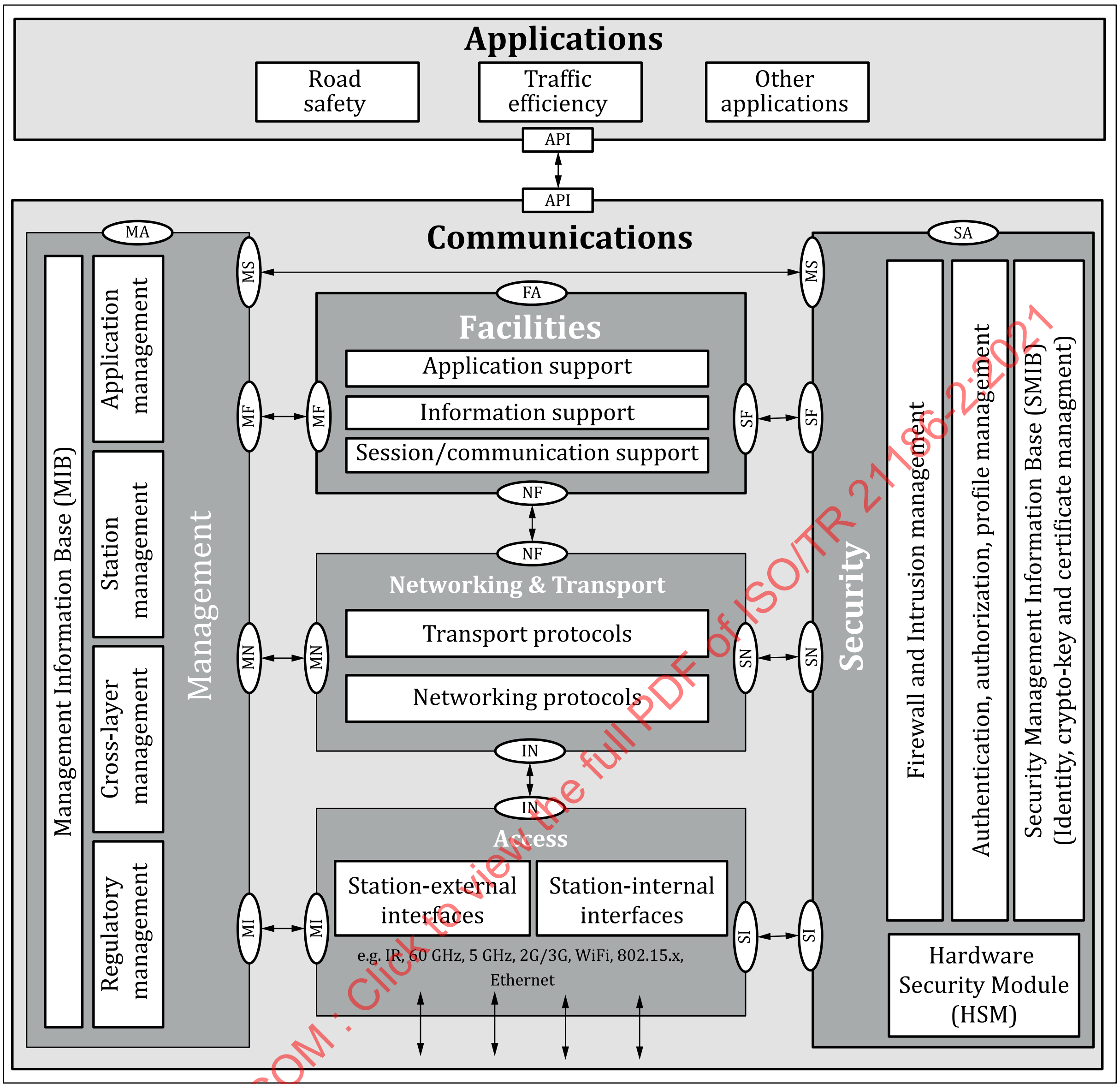

Figure 5 — Detailed ITS station architecture (ISO 21217)

It is worth mentioning that the ITS station supports both localized communications and networked communications:

— localized communications – also referred to as "ad-hoc communications" –, i.e. communications to nearby source and sink stations without involving networking through nodes of an infrastructure network;

— networked communications, i.e. communications using support of an infrastructure network, primarily supported using the Internet Protocol, preferably IPv6.

EXAMPLE ITS-M5 (ISO 21215) with FNTP (ISO 29281-1) and ITS-G5 with GeoNetworking[43,44,46] and BTP (Basic Transport Protocol)[45] are examples of protocol stacks specified for localized communications. Cellular network access to Internet (ISO 17515-1) and IPv6 (ISO 21210) is an example of a protocol stack for networked communications. Localized communications and networked communications can be combined using facility layer services (ISO 17429) and ITS station management functionalities (ISO 24102-6).

ISO/TC 204 has developed functional building blocks needed for:

— integrating various types of access technologies, including 5,9 GHz radio, cellular and satellite;

— ensuring harmonization between the European 5,9 GHz radio (ITS-G5) and the American 5,9 GHz radio (IEEE 1609) into a common abstraction sub-layer (ITS-M5 (ISO 21215);

— combining different protocol stacks for localized broadcast communications between ITS station units using the ETSI stack (BTP / GeoNetworking / ITS-G5) mostly used in European deployment pilots, the ETSI stack (BTP / GeoNetworking / LTE-V2X), the ISO stack (FNTP[31] /ITS-M5[20]) or the IEEE stack (WSMP / US-DSRC), and for end-to-end communications using the IETF stack (TCP/IP);

— developing technology-agnostic C-ITS services;

— managing ITS station units (identifiers, capabilities, communication units, etc.);

— developing generic facilities such as service announcement[24], position-velocity-time service[11], global transport data management service[40] enabling secure access to sensor and control networks, communication profile handler (CPH)[6] to manage the diversity of communication profiles[41], facilities service handler (FSH)[6] to provide generic amendments to APDUs, the content subscription handler (CSH)[6] to publish and subscribe to the reception of a specific piece of data, etc.

— developing security means for service sessions[12].

ISO/TC 204 is developing the communication standards, i.e. standards corresponding to the lower layers of the ITS station architecture and the ITS station management entities.

In 2010, ISO/TC 204 and CEN/TC 278 jointly set up new activities dedicated to the development of C-ITS standards related to data and services management, and particularly services provided by the ITS station facilities layer, and the interface allowing the subscription of services and data transmission between ITS applications and the ITS station facilities layer.

ISO/TC 204 and CEN/TC 278 are also developing other building blocks related to nomadic devices, i.e. standards allowing personal devices (e.g. smartphones) providing C-ITS services, and mobility integration, i.e. activities starting in 2018 to develop urban ITS services relying on C-ITS standards.

ETSI's version of the architecture specification has not been updated since its initial publication in 2010, while ISO's version has constantly been updated to add missing terms, to describe in more detail some of the design principles, and to clarify discrepancies and misinterpretations identified during the development of the standards and the deployment in pilot sites. In particular, the description of concepts and functionalities needed to support hybrid communication support have largely been improved in the ISO version.

6.3 Design principles of the ITS station architecture

The objective of the ITS station architecture is to support simultaneously a diversity of applications of the three usual categories (road safety, traffic efficiency and comfort / infotainment). The functionalities necessary in a given implementation can vary according to many factors: the environment of deployment, the services it provides, system architecture design choices, regulation, etc.

To accommodate the diversity of needs and solutions to meet these needs, the design principle of the ITS station architecture is to combine in a unified communication architecture communication protocols covering distinct modes of communications (localized and networked communications, wired and wireless communications, broadcast and point-to-point communications, mobile and fixed stations, etc.), relying on a diversity of access technologies with distinct characteristics (short, medium and long range wireless communications).

A fundamental advantage of this design principle over currently deployed systems is that applications are abstracted from the access technologies and the communication protocols used to transmit the information from the source to the destination(s). This means that ITS station applications are not limited to the availability and characteristics of a single access technology and protocol stack. Communication management functions make optimal use of all these resources transparently to the applications.

Thanks to this diversity of protocols and access technologies that can be combined simultaneously, the ITS station architecture is able to support a variety of communication modes (broadcast or point-to-point, localized or distant communications, etc.) for a variety of application types (road safety, traffic efficiency and comfort / infotainment).

Given these design principles, functionalities of the ITS station architecture have been developed to:

— manage the secure installation and operation of ITS applications;

— support technology-agnostic applications;

— manage diverse and varying communication requirements;

— manage simultaneously several access technologies and communication protocols;

— select the optimum communication profile for each data flow;

— manage priority of data flows;

— secure transmission, reception and access to data;

— remotely support the full life-cycle of an ITS station unit.

6.4 ITS station functionalities in support for hybrid communications

The ITS station architecture has been developed with the motivation to combine multiple access technologies in order to allow multiple data exchanges to happen simultaneously, on a single communication system (i.e. ITS station unit) gathering multiple access technologies and communication protocols, with priorities allocated to road safety over less time-critical data flows.

The set of functionalities of an ITS station specified to combine multiple access technologies and protocols is defined as hybrid communication support.

The concept of paths and flows is essential for abstracting ITS station applications from the communications services available in the ITS station and for selecting the most appropriate communication profile (i.e. protocol stack).

ISO/TC 204 initiated the development of cross-layer communication management functionalities for hybrid communications support. These functionalities are used by the ITS station management entity to select the appropriate communication profile, to maintain connectivity and to offer seamless or resilient connectivity. These tasks require the ITS station management entity to collect information about the quality of the surrounding access networks, the capabilities of the ITS station, and communication requirements for each data flow transmitted by the applications (ITS-S application process).

The functionalities are specified in a set of inter-related ISO standards (mainly ISO 24102-6, ISO 17423, and ISO/TS 17429). Most of these functionalities are inspired from earlier work conducted by the CVIS project[55], followed by the ITSSv6 project[57].

The functionalities specified in ISO 24102-6, ISO 17423 and ISO/TS 17429 allow:

— the applications (i.e. ITS-S application process) to inform the ITS station management about its communication requirements (communication profile) and other constraints for each data flow;

— the ITS station layers to provide various pieces of information about the capabilities of the layer (which functionalities are supported and their status) and about the conditions of the available surrounding networks;

— the ITS station management entity to determine which data flow can be transmitted over which available access networks (communication interface selection), using which protocol stack (communication profile selection) and to perform communication path handover (communication profile enforcement);

The specification of these functionalities requires the definition of architecture elements that are detailed in the following sections:

- The ITS station management entity;
- The ITS station capabilities;
- The ITS station managed service entity;
- The ITS station application process.

All these architecture elements need to be identified and managed, so globally unique identifiers have been created.

The following subclauses describe the process allowing for the development of technology-agnostic applications using hybrid communication technologies.

6.5 ITS station management entity

The ITS station management entity (SME) provides functionalities related to:

- Management of the communication protocol layers
- Management of the ITS security entity
- Management of the ITS applications
- Management of the ITS station communication units
- Management of the data flows

When there are multiple ITS-S flows and a range of ITS-S paths to choose from, it is useful to determine for each ITS-S flow:

- The most suitable ITS-S communication profile (facilities protocols, transport protocols, network protocols, access technologies and communication channels) to transfer data to the destination. This determination is not only necessary for the appropriate use of resources at the sending ITS station unit, but is also necessary to ensure both communication end points use a compatible set of protocols.
- The most suitable ITS-S path for routing a given ITS-S flow. This determination is not only necessary to route data packets but also to map ITS-S flows to the ITS-S path that best meets the communication requirements of the ITS-S application processes installed on the ITS station unit.

The selection of the ITS-S path implies the selection of the communication interface, the ITS-S ingress anchor node and ITS-S egress anchor node as shown in Figure 3.

Such selection is made by the ITS station management entity once it has gathered sufficient information of the following categories:

- Communication requirements of the applications installed in an ITS station unit that require communication resources of the ITS station unit (classified in operational, destination type, performance, monetary cost, energy cost, security, and protocol requirements as specified in ISO 17423).
- Capabilities of all layers of the ITS station unit (functionalities, technologies and protocols supported by the ITS station unit, characteristics of available access technologies, etc.);
- Capabilities of the access networks to which the ITS station unit is attached:
  - Network services provided by surrounding neighbour nodes (e.g. vehicle ITS station unit able to relay information to other vehicles, roadside ITS station unit providing Internet connectivity, etc.). The ITS station unit detects neighbour ITS station units and other legacy nodes through

  network services (neighbour discovery and other mechanisms including signalling protocols) and facilities services (CAM, DENM, SPaT, MAP, SAM, etc.);

  - Dynamic network conditions: various metrics of an access technology (bandwidth, packet loss), status of link (set up, in use, etc.), network load, reachability over that link (availability of Internet access);

  - Availability and characteristics of a communication interface,

  - The capabilities of neighbour ITS station units (functionalities, technologies and protocols) supported by the neighbour ITS station units;

- Capabilities of the peer communication end points as they must be able to support the same communication profiles;

- Capabilities of the ITS-S anchor nodes along the ITS-S path;

- Regulations and policies including local, national and regional rules (e.g. allowed access technologies and their transmission power; location privacy) and stakeholder rules (e.g. always prefer one access technology over another).

Figure 6 illustrates the architectural components of the ITS station management entity which are involved in the communication management process.

6.6 ITS station capabilities

The ITS station architecture supports multiple protocols and functionalities within each of the ITS station layers. These protocols, functionalities (or services) are provided by ITS-S capabilities.

Each ITS-S capability provides a well-identified function, with some specific characteristics. As such, each ITS-S capability has a unique identifier, recorded in a global registry, so that the functionalities provided by an ITS-S capability can be tested, and easily be recognized and managed by the ITS station management entity. Identifiers can be assigned to standardized ITS-S capabilities, or be reserved for private use.

Examples of ITS-S capabilities in each layer are:

- in the ITS-S facilities layer: generic services (communication handler, content subscription handler, generic message handler as specified in ISO/TS 17429), PVT (Position, Velocity and Time) as specified in ISO/TS 21176), service announcement specified in ISO 22418, CAM (Cooperative Awareness Message) specified in EN 302 637-2, DENM (Decentralized Environmental Notification Message) specified in EN 302 637-3, LDM (Local Dynamic Map) specified in ISO 18750 for general applicability and in ETSI EN 302 895, CoAP, and data distribution protocols such as the "Advances Message Queuing Protocol" (AMQP)[34] and the "Message Queuing Telemetry Transport" MQTT protocol[35].

- in the ITS-S networking & transport layer protocols: IPv6 (Internet Protocol version 6)[16], FNTP (Fast networking & transport layer protocol)[31], 6LowPAN, GeoNetworking[43,44,46], BTP (Basic Transport Protocol)[45], UDP, TCP, etc. and the functionalities they provide (broadcasting, multicasting, multihopping, geocasting, mobility management, multihoming, etc.) and their parameters;

- in the ITS-S access technologies, all instances of access technologies (IEEE 802.11(p), infrared, satellite, 2G / 3G, LTE, IEEE 802.15.4, etc.) and their characteristics (communication range, transmission delay, etc.).

Each ITS-S capability is given a globally unique ITS-S capability identifier.

6.7 ITS station service managed entity (ITS-S MSE)

The ITS station management entity is the architectural home of the central management of an ITS-SU. It is thus in charge of monitoring the installation and operation of all ITS-S capabilities in each layer or entity, and is piloting their behaviour.

In complex deployments, a given ITS station unit may implement different sets of inter-related ITS-S capabilities. The ITS-S managed service entity (ITS-S MSE) has thus been defined as a set of inter-related ITS-S capabilities available in a specific layer or entity of the ITS station unit. It is used to inform the ITS station management entity about ITS-S capabilities available in an ITS station unit and their status.

Each ITS-S MSE is given a globally unique ITS-S MSE identifier.

Table 1 — ITS-S MSEs at each layer of the ITS station

ITS-S layer or entity	ITS-S managed service entity (ITS-S MSE)[a]	
	Acronym	**Description**
ITS-S access layer	MSE-AT-ITSG5	5,9 GHz radio technology specified by ETSI (ITS-G5)
	MSE-AT-LTEV2X	LTE-V2X
	MSE-AT-USDSRC	5,9 GHz radio technology specified by IEEE
	MSE-AT-M5	ISO's harmonized 5,9 GHz radio
	MSE-AT-3G	3G cellular technology
	MSE-AT-4G	4G cellular technology
	MSE-AT-5G	5G cellular technology
ITS-S networking & transport layer	MSE-NT-TCPIP	MSE covering the ITS-S capabilities necessary for point-to-point communications and cloud connectivity, that is, the protocols providing network addressing (IPv6 Stateless Address Autoconfiguration), session continuity (IPv6 mobility support), security (IPsec), transport (UDP, TCP). ITS-S capabilities for IPv6 networking are defined in ISO 21210
	MSE-NT-IoT	MSE covering the ITS-S capabilities necessary for wireless constrained devices, that is 6LoWPAN and CoAP as defined in ISO 19079 and ISO 19080.
	MSE-NT-GN	MSE covering the ITS-S capabilities necessary for geo-localized broadcast that is the GeoNetworking protocol and the Basic Transport Protocol.
	MSE-NT-FNTP	MSE covering the ITS-S capabilities necessary for single-hop localized communication using FNTP (Fast networking & transport layer protocol)[31].
ITS-S facilities layer	MSE-FC-GEN	MSE covering the ITS-S capabilities providing general purposes services to ITS applications, that is, the facilities service handler (FSH), the content subscription handler (CSH), and the communication profile handler (CPH) specified in ISO/TS 17429); the position, time and velocity (PVT) service specified in ISO/TS 21176; the global transport data management (GTDM) specified in ISO/TS 21184; the Local Dynamic Map (LDM) specified in ISO 18750; CoAP specified in ISO 19080; and other currently undefined ITS-S capabilities.
	MSE-FC-BCAST	MSE covering legacy localized broadcast services specified by ETSI such as CAM and DENM.

[a] Most standards from ISO, CEN, IEEE and ETSI do not yet refer to functionalities of ITS stations as *ITS-S capabilities* nor do they yet refer to a set of inter-related ITS-S capabilities of *the ITS-S managed service entities* as this is a recent addition proposed to manage hybrid communications and associated communication profiles. For instance, the CAM and DENM services from ETSI are not yet defined as ITS-S capabilities, but from an ITS station management view point they can easily be encapsulated in ITS-S capabilities and be grouped together into an ITS-S MSE. By doing this, technology-agnostic ITS-S application processes could benefit from ITS services provided by legacy localized broadcast services.

Table 1 *(continued)*

ITS-S layer or entity	ITS-S managed service entity (ITS-S MSE)[a]	
	Acronym	**Description**
ITS-S security entity	MSE-SESSION	MSE covering services for secure sessions specified in ISO 21177 and for secure broadcast and location privacy specified in ETSI.
	MSE-SE-BCAST	MSE covering services for secure broadcast and location privacy specified in ETSI.

[a] Most standards from ISO, CEN, IEEE and ETSI do not yet refer to functionalities of ITS stations as *ITS-S capabilities* nor do they yet refer to a set of inter-related ITS-S capabilities of *the ITS-S managed service entities* as this is a recent addition proposed to manage hybrid communications and associated communication profiles. For instance, the CAM and DENM services from ETSI are not yet defined as ITS-S capabilities, but from an ITS station management view point they can easily be encapsulated in ITS-S capabilities and be grouped together into an ITS-S MSE. By doing this, technology-agnostic ITS-S application processes could benefit from ITS services provided by legacy localized broadcast services.

Each layer or entity of the ITS station architecture can contain multiple ITS-S managed service entities running simultaneously. This is particularly useful in the context of hybrid communications, as in the latter two implementation examples below:

— In the situation of an ITS station unit distributed into two ITS-S communication units as detailed in Table 2. This is an example of a communication system that supports hybrid communications in a non-optimized way.

— In the situation of a single ITS station communication unit designed to support hybrid communications (both localized communications and networked communications) as detailed in Table 3. This is an example of a communication system that supports hybrid communications in a more optimized way.

Table 2 — Example in an ITS-SU distributed into two ITS-S communication units

ITS-S layer or entity	ITS-S managed service entity (ITS-S MSE)	
	ITS-S MSEs in an ITS-SCU dedicated to localized communications for time-critical road safety	**ITS-S MSEs in an ITS-SCU dedicated to support networked communications for session-based cloud services**
ITS-S facilities layer	MSE-FC-BCAST	MSE-FC-GEN
ITS-S networking & transport layer	MSE-NT-GN	MSE-NT-TCPIP
ITS-S access layer	MSE-AT-ITSG5	MSE-AT-4G
ITS-S security entity	MSE-SE-BCAST	MSE-SE-SESSION

Table 3 — Example in an ITS-SU made of a single ITS-S communication unit

ITS-S layer or entity	ITS-S managed service entity (ITS-S MSE)
	ITS-S MSEs in a single ITS-SCU supporting both localized communications for time-critical road safety and networked communications for session-based cloud services
ITS-S facilities layer	MSE-FC-GEN
	MSE-FC-BCAST
ITS-S networking & transport layer	MSE-NT-TCPIP
	MSE-NT-GN
ITS-S access layer	MSE-AT-ITSG5
	MSE-AT-4G
ITS-S security entity	MSE-SE-SESSION

In all situations, the ITS-S management entity monitors the ITS-S capabilities provided by each ITS-S managed service entity and pilots the selection of the communication profile for each ITS-S flow, and thus the transmission through the appropriate ITS-S managed service entities.

6.8 Management of data flow types (ITS-S flow type)

In the common situation multiple ITS applications are running in parallel in a given ITS station unit. These ITS applications are competing towards the use of the same set of common ITS station unit resources (CPU, bandwidth, connectivity, etc.). In addition, each ITS application can be engaged in several data exchanges (ITS-S flow), of distinct nature (different ITS-S flow types), and possibly with multiple communication peers (multiple instantiations of the same ITS-S flow type). There could consequently exist multiple ongoing ITS-S flows, each with its own flow characteristics.

It is thus necessary to manage their needs and priorities. ISO 24102-6 and ISO 17423 specify a mechanism allowing ITS-S application processes to inform the ITS station management about their communication requirements for each ITS-S flow initiated.

ISO 17423 provides support for applications to define and provide a list of communication requirements for each type of data flow (ITS-S flow type).

At the ITS station management level, the ITS-S flow type allows the classification of data flows with the same characteristics, transmitted from distinct ITS station units or to distinct destination nodes.

If needed, a pre-defined Communication Profile (i.e. a specific list of protocols that have to be used precisely) may also be directly requested by the ITS-S application process following a regional regulation enforcement or specific design choices of the ITS application developer. Communication profiles and respective globally unique identifiers are specified in CEN/TS 17496 and in ISO/TS 21185.

NOTE CEN/TS 17496 builds on the earlier published ISO/TS 21185. Both documents contain the same technical specification of communication protocol stacks and communication profiles. The difference is that CEN/TS 17496 contains more examples of stacks and profiles for which globally unique reference identifiers are assigned.

Note that a high level of security is needed in order to prioritize the use of resources (CPU, energy, bandwidth) for which several applications are competing in parallel.

6.9 Management of communication paths (ITS-S path)

The ITS-S management entity monitors the available capabilities of the ITS station unit, the available access technologies and the capabilities of the access network.

The communication path is the itinerary taken in the network by data transmitted between the sender and the recipient. In the context of the ITS station architecture, the communication path is referred to as an ITS-S path.

An ITS-S path as defined in ISO 21217 starts at its source node and ends up at a destination node. There may be zero or more intermediate nodes in the ITS-S path between the source node and the destination node.

However, an ITS-S path towards a destination node always goes through "selectable communication nodes" that are pre-determined according to the peer nodes engaged in the communication. These "selectable communication nodes" are referred to as the 'ITS-S anchor nodes' (respectively the 'ITS-S ingress anchor node' and the 'ITS-S egress anchor node') and form the entry and exit end points of a controllable path segment ('ITS-S anchor segment').

Figure 3 illustrates a situation where a vehicle has several ITS-S paths to choose from in order to communicate with a communication peer.

6.10 Management of communication profiles (ITS-SCP)

The ITS station architecture is designed to support multiple protocols and functionalities within each of the ITS station layers. Available protocols and access technologies can be combined in various ways to transfer data to the destination. A collection of protocols used to transfer data to a destination is referred to as the ITS-S communication protocol stack (ITS-SCPS), and a parameterized ITS-SCPS is referred to as an ITS-S communication profile (ITS-SCP).

The ITS-SCP indicates the protocol stack, i.e. the protocols at the ITS station facilities layer, at the ITS station networking & transport layer, and at the ITS station access layer that are used for a given ITS-S flow.

Several communication profiles could exist to reach a given destination. Some communication profiles may not be appropriate to reach a given destination if the communication end points do not support a compatible set of protocols. The ITS station management is thus in charge of the determination of the most appropriate communication profile to be used for a given ITS-S flow.

This determination is made for each ITS-S flow according to the ITS-S flow type requirements provided by the ITS-S application process (or through an internal configuration), and known applicable regulatory requirements.

The ITS-S management entity is thus responsible for the selection of the best communication path (access technology, protocol stack, and communication path) according to the communication flow requirements expressed by the ITS-S application processes, pre-set policies, regulations, the capabilities and resources of the ITS station unit, the access technologies characteristics and the current network conditions.

The ITS-S management entity interacts with the ITS station layers and the ITS-S security entity in order to make this selection (see Figure 6).

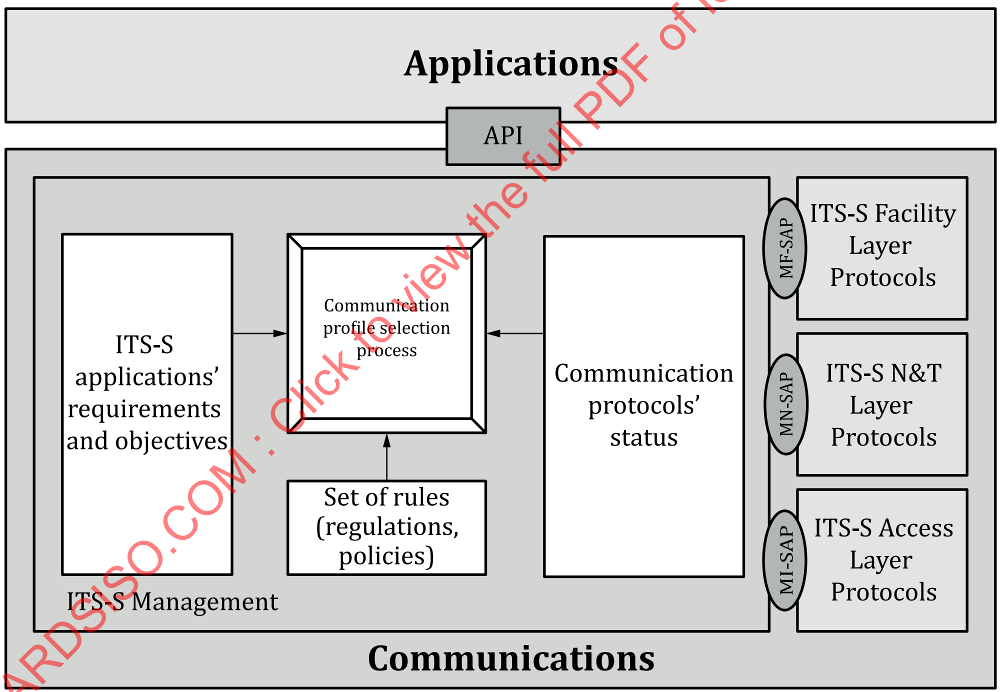

Figure 6 — Communication management (ISO 24102-6)

Based on this knowledge gathered through the management of communication requirements (6.8) and the management of communication paths (6.9), the ITS-S management entity selects the best communication profile (ITS-SCP) for each ITS-S flow.

This selection is notified to the ITS-S layers (facilities, networking and transport, access technologies) through an ITS-S internal unique identifier (ITS-S flow identifier) used as pointer to a list of parameters. This identifier allows each layer to map data ready for transmission (Application Data Unit) to a specific ITS-S flow ID. This is used to reserve specific resources and to process the Application Data Unit according to the protocol identified by the ITS-S flow ID, other actions such as adding a certificate for authentication purposes, or applying a time stamp or other type of information), and then pass the modified Application Data Unit to the next layer.

6.11 Management of communication handovers

The ITS-S management entity is able to maintain network connectivity under dynamic network environment conditions. Having multiple communication paths available, the ITS-S management entity can switch the transmission of an ITS-S flow from one communication path to another. This is referred to as "communication handover".

The ITS-S management entity supports different types of handover, including:

— Handovers involving a change of the point of attachment to the network without a change of access technology;

— Handovers involving a change of the point of attachment to the network with a change of access technology;

— Handovers involving reconfiguration or change of the network employed to provide connectivity;

— Handovers involving both a change of the point of attachment to the network and network reconfiguration;

— Handovers involving a change of the communication profile (different protocol stack).

Once the handover is performed, the ITS-S management entity informs the appropriate ITS-S MSE about the change of the communication profile for the given ITS-S flow.

6.12 Management of globally unique identifiers

The following objects, beyond others, require a globally unique identifier:

— Well-known ITS-S flow types;

— ITS-S capabilities (see 6.6);

— ITS-S services (provided by ITS-S capabilities) (see 6.6);

— ITS-S managed service entities (see 6.7);

— ITS-S application process.

Identifiers of ITS-S flows (ITS-S FlowId) do not need to be registered as they are dynamically allocated by the ITS-S management entity and are strictly internal to the ITS station unit.

6.13 Standards necessary in support of hybrid communications

Table 7 provides a list of key standards in support of hybrid communications; see also ISO/TR 21186-1.