INTERNATIONAL STANDARD

ISO 21217

Third edition
2020-12

Intelligent transport systems — Station and communication architecture

Systèmes de transport intelligents — Architecture du station et du communication

Reference number
ISO 21217:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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.*

This third edition cancels and replaces the second edition (ISO 21217:2014), which has been technically revised.

The main changes compared to the previous edition are as follows:

— many general alignments with other standards (e.g. on terms and abbreviations, and on references) revised or developed since the publication of the second edition of this document;

— prioritization in the receive path added;

— more details on hybrid communications included;

— details on security requirements added.

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 provides the intelligent transport systems (ITS) station and communication reference architecture that is referenced in a family of deliverables from standard development organizations (SDOs) for cooperative intelligent transport systems (C-ITS), which is a subset of standards for 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; and

— **sustainability**,

by applying information and communication technologies (ICT).

ITS specifications are in general developed to address a specific ITS service domain (see ISO 14813-1), such as public transport, road safety, freight and logistics, public emergencies or electronic fee collection.

To support interoperability, C-ITS specifications are developed to exchange and share information amongst ITS applications of a given application domain and even between application domains.

C-ITS services are based on the exchange of data between vehicles of any category (cars, trucks, buses, emergency and specialized vehicles, etc.), the roadside and urban infrastructure (traffic lights, road tolls, variable message signs, etc.), control and services centres (traffic control centre, service providers, map providers, etc.), and other road users (pedestrians, cyclists, etc.).

Some ITS services require cooperation by vehicles with their surrounding environment (other vehicles, other road users, roadside and urban infrastructure, etc.) while other ITS services require connectivity to remote service platforms (road traffic control centres, map providers, service providers, fleet managers, equipment manufacturers, etc.).

In order to support:

— a large variety of C-ITS services with diverging requirements, and

— efficient sharing of information maintained by individual service applications,

it is necessary to combine multiple access technologies and communication protocols with distinct performance characteristics (communication range, available bandwidth, end-to-end transmission delay, quality of service, security, etc.); see Figure 1.

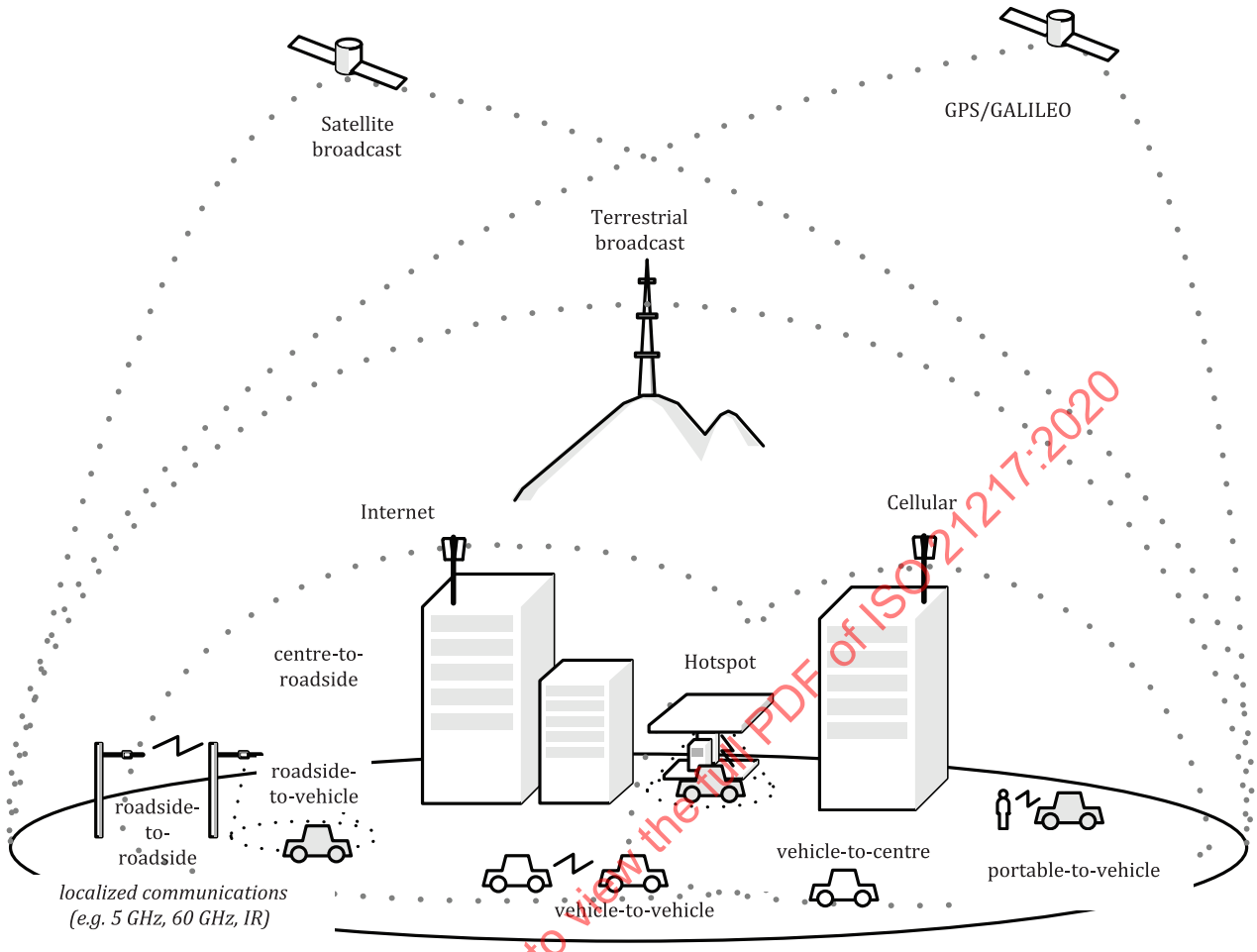

Figure 1 — Examples of ITS communications

Combining multiple access technologies and communication protocols requires a common approach to the way communications and data are securely managed, which is specified in this document (see Figure 2).

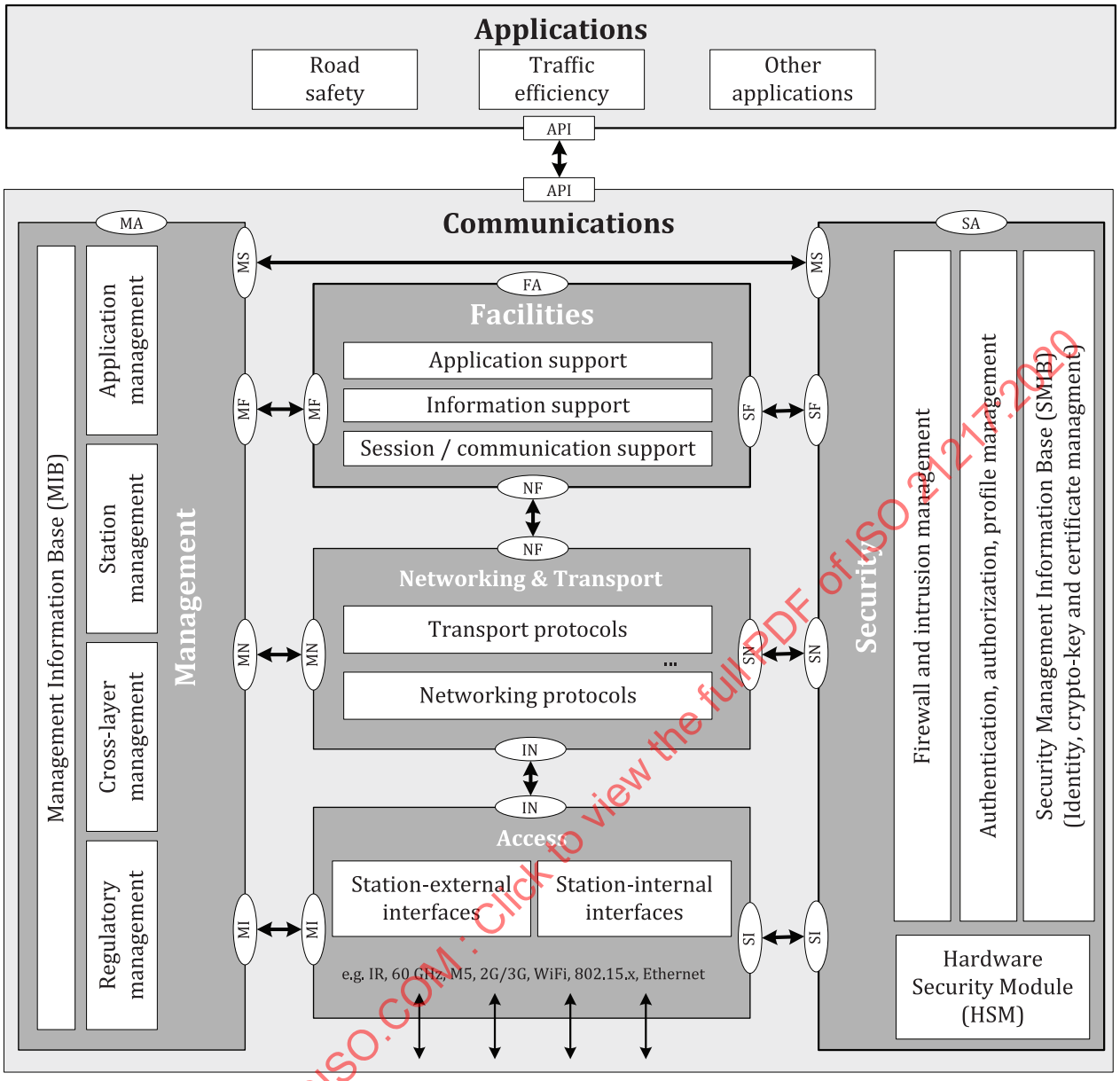

Figure 2 — ITS-S reference architecture

Similarly to the ISO Open Systems Interconnection (OSI) 7-layer architecture, the ITS station architecture is divided into three independent communication layers (namely the ITS station access layer, the ITS station networking and transport layer and the ITS station facilities layer) on top of which the ITS Applications entity is located. Additional cross-layer entities in charge of the management activities (management of ITS station units, of communications and security) support communications and applications.

An implementation of this ITS station architecture is referred to as an “ITS station unit" (ITS-SU). The functionalities available in an ITS-SU can be implemented in one or multiple physical units, referred to as “ITS station communication units” (ITS-SCUs). The various ITS-SCUs of one single ITS-SU may even be split over a large geographical area, e.g. along a motorway several tens of kilometres in length.

ITS-SUs conformant with this document may be deployed in various environments, including vehicles of any kind (vehicle ITS station), on the roadside infrastructure (roadside ITS station), in data centres (central ITS station) or in nomadic devices (personal ITS station), as illustrated in Figure 3.

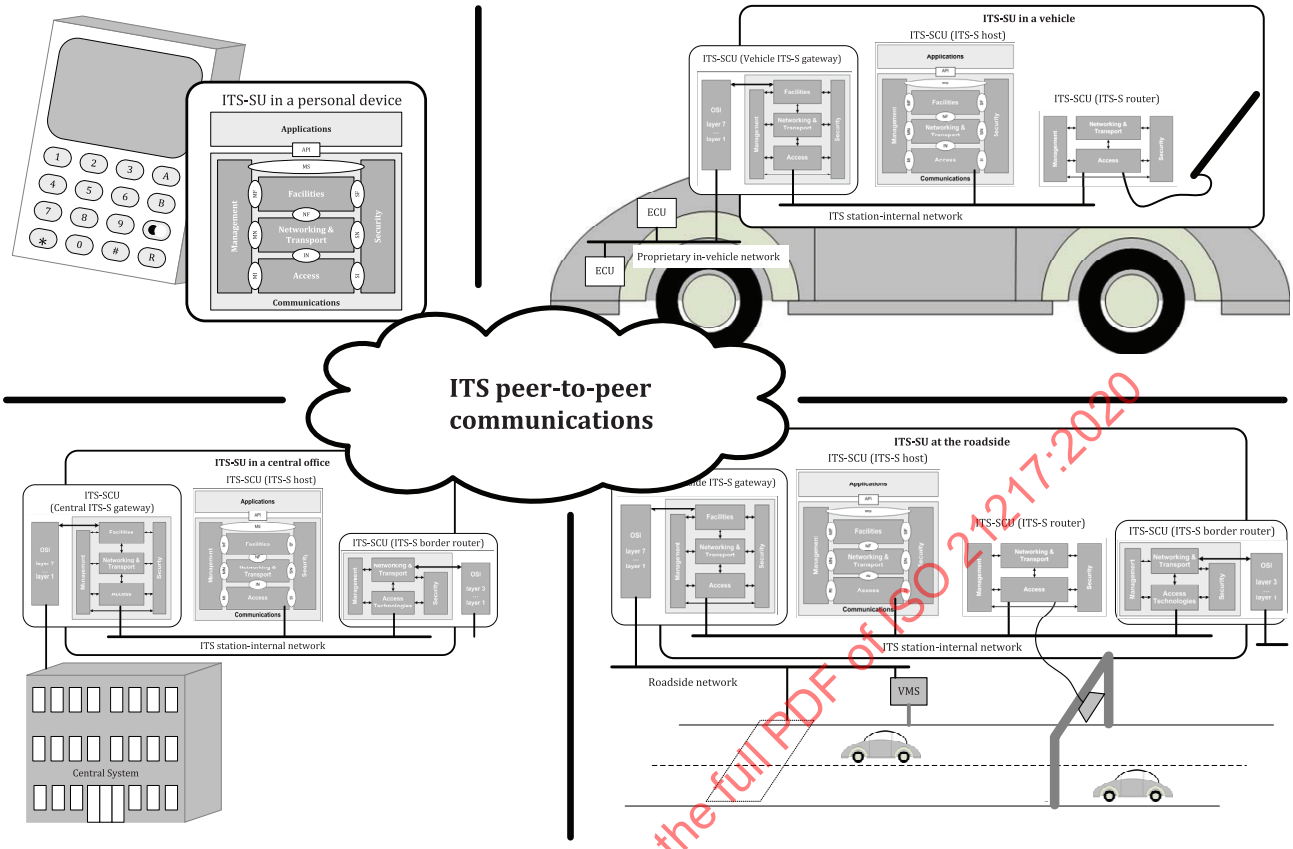

Figure 3 — Typical implementations of ITS station units

Details of the following functional building blocks of the ITS station architecture are specified in a set of related standards:

— ITS station management,

— ITS communication, application (service) and station security,

— ITS station facilities layer protocols,

— ITS station networking and transport layer protocols,

— communication interfaces (CIs) designed specifically for ITS applications and services such as those designed specifically for safety of life and property,

— interfacing existing access technologies into ITS stations,

— distributed implementations of ITS stations, and

— interfacing ITS stations to existing communication networks and communicating with nodes thereon.

As C-ITS deals with safety of human life and property, ITS station units are designed for supporting the secure provision of the C-ITS services and secure allocation of resources with prioritized access. Security means covering the two essential operational modes:

a) Authentication of the sender of a broadcast message used for information dissemination.

b) Secure session establishment and maintenance.

Due to the diverging requirements from the multiplicity of already known and continuously emerging ITS applications, multiple communication technologies that are fundamentally different may be

supported in a specific ITS-SU. Supporting multiple access technologies and communication protocols, also referred to as "hybrid communications", is a design principle of the ITS station architecture. The ITS station architecture is thus specified with no pre-defined mandatory communication technologies. It can support any type of existing and forthcoming technology, on the condition that:

1) it respects the same design principles;

2) its integration into the ITS station architecture is specified in a support standard, and

3) it preserves backward compatibility with existing standards.

Presently, specifications have been developed to support a number of access technologies, for example:

— all kinds of cellular access technologies (e.g. specified at 3GPP with profile standards from other SDOs tailoring them to the ITS station reference architecture);

— satellite communications;

— other technologies such as infrared, millimetre wave (ultra wideband communications), vehicular Wi-Fi (ITS-G5/US-DSRC/ITS-M5: all profiles of IEEE 802.11 OCB) and optical light communications;

and several flavours of communication protocol suites:

— GeoNetworking / Basic Transport Protocol from ETSI;

— FNTP from ISO;

— WSMP from IEEE; and

— the suite of IPv6 protocols from IETF with supporting specifications from ISO.

The ITS station architecture actually combines:

a) localized communications,

i.e. communications to nearby stations without involving networking from a source station through nodes of a network to a final destination station – also referred to as "ad-hoc communications", and

b) networked communications.

NOTE While 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 access technologies), it is necessary for localized communication between ITS station units to be based on a specific access technology per service (or service domain) in order to enable interoperability.

EXAMPLE ITS-M5 (ISO 21215) with FNTP (ISO 29281-1) is an example of a protocol stack for localized communications. Cellular network access to internet (ISO 17515-1) with IPv6 (ISO 21210) is an example of a protocol stack for networked communications.

Unlike many legacy applications, the choice of the access technology and communication protocol can be made transparent to the applications, i.e. ITS applications are technology-agnostic. This is achieved through a number of functionalities across the ITS station architecture in support of hybrid communications, and is illustrated in Figure 4.

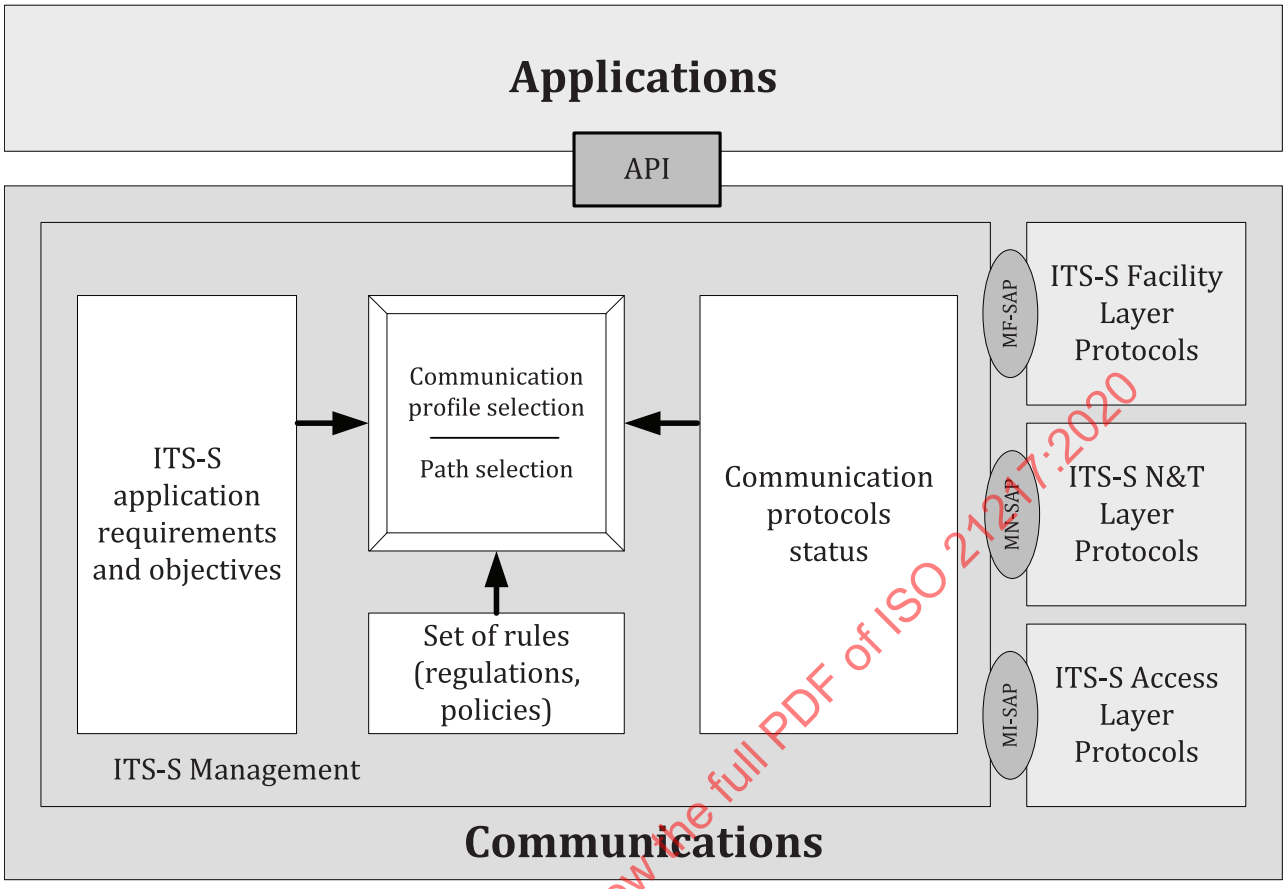

Figure 4 — Architecture of communication profile and path selection

Before transmitting data, applications provide their communication requirements (level of priority, amount of data to be transmitted, expected level of security, expected end-to-end transmission delay, etc.) to the management entity of the ITS-SU for each type of communication flow. In the meantime, the management entity maintains various elements of information (local regulation enforcing the use of a specific communication profile, existing capabilities of the ITS-SU and their status, characteristics and load of available radio technologies, current load of the ITS-SU, etc.). Based on the communication requirement and the current view of the management, the uppermost relevant communication profile (uniquely identified by an ITS-S communication profile identifier) is selected and ITS station resources are securely committed for identified communication flow.

The ITS station architecture serves as a reference for numerous C-ITS services developed around the world, and more particularly, in Europe. Early deployments of C-ITS services conforming to the ITS station architecture have been initiated in Europe under the framework of the C-ROADS[115] and InterCor initiatives supported by the European Commission. National pilot deployments are underway all across Europe (for example, SCOOP in France, NordicWay in Scandinavia, the C-ITS corridor project between The Netherlands, Germany, and Austria) and in other regions such as Austroads in Australia and New Zealand, and in Israel. These early deployment projects are typically focused on road safety and traffic efficiency services that rely on the exchange of data between vehicles and the roadside infrastructure. This data exchange is performed through both localized communications and networked communications.

In these European deployments, localized communications, also known as V2X, are performed using the ITS-G5 access technology within the 5.9 GHz frequency band, a Wi-Fi profile designed for vehicular communications. Networked communications are typically performed using a cellular technology (e.g. LTE). Other technologies may of course be used in the future (e.g. 5G, infrared, etc.) provided that they conform to the ITS station architecture and related standards defining technology building blocks.

Early deployments have proven the need to deploy C-ITS services using a range of access technologies, for example either ITS-G5 or LTE, or a combination of both. For instance, the French pilot deployment (SCOOP) uses ITS-G5 between vehicle and roadside ITS stations to inform about immediate dangers (CAM, DENM) and LTE is used by patrol vehicles to provide information to road control centres. In Scandinavia, the scarce population has driven NordicWay to deploy roadside ITS stations only at critical locations and to rely on LTE to deliver environmental information (DENM) from road control centres to vehicles.

Further on, at the early stage of deployment of C-ITS services, the density of vehicle ITS stations equipped with ITS-G5 capabilities is scarce, whereas roadside ITS stations are only deployed in critical areas. Similarly, many areas anywhere in the world do not have the benefit of sufficient cellular network coverage. While some time critical road safety C-ITS services are best served by localized communications (e.g. notification of immediate danger requiring emergency breaking), there are not always vehicles equipped with the ITS-G5 technology or roadside equipment in the vicinity able to relay the notification immediately to nearby vehicles. In such a situation, using networked communications (e.g. cellular) to provide the information to road control centres, and then from them back to vehicles in a specific area, prevents the successive occurrence of road accidents.

All of these experiences, gained through early deployments, demonstrate that it is not possible to provide the same level of services to all vehicles in all locations. The type of service and the performance of the service depends on national decisions, the local road environment, the density of population, the density of vehicles equipped, cellular coverage, and numerous other factors. In addition, and importantly, the roadside infrastructure equipment and vehicles have a life expectancy that far exceeds the innovation cycle of new radio and communication technologies. Equipment at the roadside and in vehicles is therefore likely to have to accommodate new communications technologies during its lifetime.

The ITS station and communication architecture specified in this document and its functionalities in support of hybrid communications provide an answer to these concerns and enable a future-proof and sustainable deployment of C-ITS services.

This architecture document is complemented by:

— a business-oriented architecture specified in ISO 17427-1;

— testing architectures specified in ISO/TS 20026 and ETSI EG 202 798; and

— data registration procedures for ITS safety and emergency messages specified in ISO 24978.

Further on, guidelines on the topics related to this document are provided in the ISO 17427 series and in the ISO 21186 series.

The Bibliography at the end of this document provides information on standards, draft standards and new standard work items from various SDOs, and about other documentation relevant to ITS. The information given there does not claim to be complete. There can be further standards and documentation relevant to ITS, either already in existence, or available in the future.

Intelligent transport systems — Station and communication architecture

1 Scope

This document describes the communications reference architecture of nodes called "ITS station units" designed for deployment in intelligent transport systems (ITS) communication networks. The ITS station reference architecture is described in an abstract manner. While this document describes a number of ITS station elements, whether or not a particular element is implemented in an ITS station unit depends on the specific communication requirements of the implementation.

This document also describes the various communication modes for peer-to-peer communications over various networks between ITS communication nodes. These nodes can be ITS station units as described in this document or any other reachable nodes.

This document specifies the minimum set of normative requirements for a physical instantiation of the ITS station based on the principles of a bounded secured managed domain.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/TS 21177, *Intelligent transport systems — ITS station security services for secure session establishment and authentication between trusted devices*

NOTE Document also available as CEN/TS 21177.

ETSI TS 103 097, *Intelligent Transport Systems (ITS); Security; Security header and certificate formats*

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* (3.4) to access a specific *medium* (3.55)

3.2
application data unit
ADU
data unit exchanged between *ITS-S application processes* (3.22)

3.3
communication adaptation layer
CAL
set of protocols and functions to adapt access technologies to the ITS-S networking & transport layer

3.4
communication interface
CI
instantiation of a specific *access technology* (3.1) and ITS-S access layer protocol

3.5
communication path
directed sequence of nodes connected by links, starting at a source node and ending at one or more destination nodes

3.6
FA Interface
interface between the ITS-S facilities layer and the *ITS-S applications* (3.21) entity

3.7
hybrid communications
composition of multiple access technologies and communication protocols combined to provide complementary or redundant communication channels

3.8
hybrid communication support
feature of an *ITS station* (3.15) used to combine multiple access technologies and protocols

3.9
hybrid ITS services
ITS service that relies on *hybrid communications* (3.7)

3.10
IN Interface
interface between the ITS-S access layer and the ITS-S networking & transport layer

3.11
in-vehicle network
IVN
generic term for a network in a vehicle which is not an ITS station-internal network

3.12
ITS application
instantiation of an ITS service that involves an association of two or more complementary *ITS-S application* (3.21) processes

Note 1 to entry: Fragments of an application can also reside in nodes that are not *ITS stations* (3.15).

3.13
ITS message set
set of messages designed for an ITS-related purpose

3.14
ITS service
functionality provided to users of intelligent transport systems designed to increase safety, sustainability, efficiency, or comfort, for example

3.15
ITS station
functional entity comprised of an ITS-S facilities layer, ITS-S networking & transport layer, ITS-S access layer, ITS-S management entity, ITS-S security entity and *ITS-S applications* (3.21) entity providing *ITS services* (3.14)

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 physical instantiation of an ITS-S is *ITS station unit (ITS-SU)* (3.52).

3.16
ITS-S access layer
protocol layer in the ITS-S reference architecture containing the OSI physical and data link layer protocols for ITS communications

3.17
ITS-S access layer protocol data unit
ITS-APDU
protocol data unit exchanged between peer *ITS-S access layers* (3.16)

3.18
ITS-S access layer service data unit
ITS-ASDU
service data unit exchanged between *ITS-S access layer* (3.16) and ITS-S networking & transport layer

3.19
ITS-S access router
ITS-S border router (3.23) with additional functionality that provides other ITS communication nodes a point of attachment to an external network

3.20
ITS-S access technology
access technology (3.1) dedicated to operation in an *ITS station* (3.15)

3.21
ITS-S application
ITS-S application process (3.22) residing in the ITS-S application entity

3.22
ITS-S application process
element in an *ITS station* (3.15) that performs information processing for a particular application and uses *ITS-S services* (3.51) to transmit and receive information

3.23
ITS-S border router
ITS-S router with additional functionality that provides connectivity to other ITS communication nodes over external networks

3.24
ITS-S capability
uniquely addressable protocol or functionality that is part of an *ITS-S managed service entity* (3.42)

Note 1 to entry: Examples of ITS-S capabilities in the *ITS station* (3.15) facilities layer are generic ITS-S facilities layer 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 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.

3.25
ITS-S communication profile
parameterized *ITS-S communication protocol stack* (3.28)

3.26
ITS-S communication profile identifier
globally unique, registered reference number identifying an *ITS-S communication profile* (3.25)

3.27
ITS-S communication protocol
protocol used in a communication protocol stack of an *ITS station* (3.15)

3.28
ITS-S communication protocol stack
consistent set of *ITS-S communication protocols* (3.27) enabling communications between an *ITS-SCU* (3.30) and other nodes which may be identified by a registered globally unique reference number

3.29
ITS-S communication protocol stack identifier
globally unique, registered reference number identifying a non-parameterized communications protocol stack

3.30
ITS-S communication unit
ITS-SCU
physical unit in an *ITS station unit* (3.52) containing a part or all of the functionality of an *ITS station* (3.15)

Note 1 to entry: If an ITS-SU consists of a single physical unit, the ITS-SU and the ITS-SCU are identical. If an ITS-SU consists of more than one ITS-SCU, then these ITS-SCUs are interconnected via the ITS station-internal network of the ITS-SU.

3.31
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 & transport layer

3.32
ITS-S facilities layer protocol data unit
ITS-FPDU
protocol data unit exchanged between peer ITS-S facility layers

3.33
ITS-S facilities layer service data unit
ITS-FSDU
service data unit exchanged between *ITS-S facilities layer* (3.31) and *ITS-S application* (3.21) entity

3.34
ITS-S facilities service
ITS-S capability (3.24) of the *ITS-S facilities layer* (3.31) providing a service that may be applied to *ADUs* (3.2) at the request of the source ITS-S-AP

3.35
ITS-S facility application
ITS-S application process (3.22) residing in the *ITS-S facilities layer* (3.31)

3.36
ITS-S flow
identifiable sequence of packets of a given *ITS-S flow type* (3.37) transmitted between a source node and a destination node

3.37
ITS-S flow type
set of characteristics describing a data flow

3.38
ITS-S gateway
ITS-S node (3.47) used to interconnect two different OSI protocol stacks at layers 5 through to 7

Note 1 to entry: An ITS-S gateway can convert between different protocols

3.39
ITS-S host
ITS-S node (3.47) comprised of ITS-S functionalities other than the functionalities of an ITS-S router, *ITS-S border router* (3.23), *ITS-S mobile router* (3.43), or an *ITS-S gateway* (3.38)

3.40
ITS-S internal router
ITS-S router (3.49) that connects two or more ITS station-internal networks

3.41
ITS-S management application
ITS-S application process (3.22) residing in the ITS-S management entity

3.42
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 and transport layer (IPv6, FNTP, GeoNetworking, 6LoWPAN, etc.), the generic facilities at the *ITS-S facilities layer* (3.31) (CPH, FSH, CSH).

3.43
ITS-S mobile router
ITS-S border router (3.23) with additional functionality that allows a change of point of attachment to an external network while maintaining session continuity

3.44
ITS-S networking & transport layer protocol data unit
ITS-NTPDU
protocol data unit exchanged between peer ITS-S networking & transport layers

Note 1 to entry: The deprecated term ITS-NPDU is in use in published standards with the same meaning as ITS-NTPDU.

3.45
ITS-S networking & transport layer service data unit
ITS-NTSDU
service data unit exchanged between *ITS-S networking & transport layer* (3.46) and *ITS-S facilities layer* (3.31)

3.46
ITS-S networking & transport layer
layer in the ITS-S reference architecture containing OSI layers three and four that connects the *ITS-S facilities layer* (3.31) to the *ITS-S access layer* (3.16)

3.47
ITS-S node
node comprised of a set of functionalities in an *ITS station* (3.15) unit that is connected to the ITS station-internal network or comprises an entire *ITS station unit* (3.52)

3.48
ITS-S path
directed sequence of nodes connected by links starting at a source node, traversing a *communication interface* (3.4) of the source ITS-S, an ITS-S ingress anchor node and an ITS-S egress anchor node, ending at a destination node

3.49
ITS-S router
ITS-S node (3.47) comprised of routing functionalities of an *ITS station unit* (3.52) used to connect two networks and to forward packets not explicitly addressed to itself

3.50
ITS-S security application
ITS-S application process (3.22) residing in the ITS-S security entity

3.51
ITS-S service
communication functionality of an *ITS station* (3.15) that provides the capability to connect to other nodes

3.52
ITS station unit
implementation of an *ITS station* (3.15)

3.53
localized communications
communications with nearby stations without involving support of an infrastructure network

3.54
MA Interface
interface between the ITS-S management entity and *ITS-S applications* (3.21)

3.55
medium
physical entity that supports the transmission of signals carrying information between ITS communication nodes

EXAMPLE A set of wires supporting Ethernet signals or the space between two antennas that supports electromagnetic, optical or acoustical transmissions.

3.56
MF Interface
interface between the ITS-S management entity and the *ITS-S facilities layer* (3.31)

3.57
MI Interface
interface between the ITS-S management entity and the *ITS-S access layer* (3.16)

3.58
MN Interface
interface between the ITS-S management entity and the *ITS-S networking & transport layer* (3.46)

3.59
MS Interface
interface between the ITS-S management entity and the ITS-S security entity

3.60
networked communications
communications using support of an infrastructure network

3.61
NF Interface
interface between the *ITS-S networking & transport layer* (3.46) and the *ITS-S facilities layer* (3.31)

3.62
SA Interface
interface between the ITS-S security entity and *ITS-S applications* (3.21)

3.63
SF Interface
interface between the ITS-S security entity and the *ITS-S facilities layer* (3.31)

3.64
SI Interface
interface between the ITS-S security entity and the *ITS-S access layer* (3.16)

3.65
SN Interface
interface between the ITS-S security entity and the *ITS-S networking & transport layer* (3.46)

4 Symbols and abbreviated terms

API	application programming interface
BSM	basic safety message
BSMD	bounded secured managed domain
BSME	bounded secured managed entity
BTP	Basic Transport Protocol
CAM	cooperative awareness message
CCH	control channel
CEN	European Committee for Standardization (Commission Européenne de Normalization)
C-ITS	cooperative ITS
C-ITS-SU	central ITS-SU
DCC	distributed congestion control
DENM	decentralized environmental notification message
DLL	data link layer (OSI)
DSRC	dedicated short range communication
ETSI	European Telecommunications Standards Institute
FA	name of interface between ITS-S facilities layer and ITS-S application entity
FlowID	identifier, being unique within an ITS station unit, that identifies an ITS-S flow
FNTP	Fast Networking & Transport Layer Protocol
FSAP	Fast Service Announcement Protocol
HMI	human machine interface
HSM	hardware security modules

IN	name of interface between ITS-S access layer and ITS-S networking and transport layer
IP	internet protocol
IPv6	internet protocol version 6
IR	infrared
ISO	International Standards Organization
ITS	intelligent transport systems
ITS-AID	ITS application identifier
ITS-M5	access technology specified in ISO 21215
ITS-S	ITS station
ITS-S-AP	ITS-S application process
ITS-SU	ITS-S unit
IVI	in-vehicle information
LCH	logical channel
LDM	local dynamic map
LTE	long term evolution
MA	name of the interface between the ITS-S management entity and ITS-S applications
MAE	management adaptation entity
MAP	name of an ITS message set used to carry information on digital maps covering the area of intersections.
MF	name of the interface between the ITS-S management entity and the ITS-S facilities layer
MI	name of the interface between the ITS-S management entity and the ITS-S access layer
MIB	management information base
MN	name of the interface between the ITS-S management entity and the ITS-S networking and transport layer
MS	name of the interface between the ITS-S management entity and the ITS-S security entity
NF	name of the interface between the ITS-S networking and transport layer and the ITS-S facilities layer
PCH	physical communication channel
PDM	probe data management. Name of an ITS message set.
PDU	protocol data unit
PHY	physical layer (OSI)
POI	point of interest

PVD	probe vehicle data. Name of an ITS message set.
P-ITS-SU	personal or portable ITS-SU
RF	radio frequency
RI	regulatory information
R-ITS-SU	roadside ITS-SU
SA	name of the interface between the ITS-S security entity and ITS-S applications
SaCH	service announcement channel (also called service advertisement channel)
SAE	security adaptation entity
SAM	service announcement message
SAP	service access point
SCH	service channel
SDU	service data unit
SF	name of the interface between the ITS-S security entity and the ITS-S facilities layer
SfCH	safety channel
SI	name of the interface between the ITS-S security entity and the ITS-S access layer
SMIB	security management information base
SN	name of the interface between the ITS-S security entity and the ITS-S networking and transport layer
SOA	service oriented architecture
SPaT	signal phase and timing. Name of an ITS message set.
SRM	signal request message. Name of an ITS message set.
SSM	signal status message. Name of an ITS message set.
TCP	Transmission Control Protocol
TOPO	name of an ITS message set used to carry information on digital maps covering the area of intersections.
TPEG-RTM	Transport Protocol Expert Group - Road Traffic Messages
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System
VCI	virtual CI
V-ITS-SU	vehicle ITS-SU

V2X	localized communications between a vehicle and its surrounding environment
WSA	WAVE service advertisement
WSMP	WAVE Short Message Protocol

5 Requirements

A physical instantiation of an ITS-S shall provide as a minimum:

— the functionality of an ITS-S host as specified in 7.2.2, i.e. acting as a terminal only, or

— the functionality of an ITS-S host and ITS-S router as specified in 7.2.2,

with station management functionality as specified in ISO 24102-1 (local station management) and ISO 24102-2 (remote station management).

This includes a minimum set of related security procedures and principles that can be verified by an appropriate ITS-related authority described in ISO 17419. Security means, as a minimum, are needed for:

a) secure sessions between trusted devices;

b) signing broadcast messages for information dissemination;

c) securing station-internal access to facilities as identified in, for example:

   — ISO 18750 for the local dynamic map (LDM);

   — ISO 24102-4 for station-internal management communications.

As a variety of appropriate security means exist, particularly considering different ITS application domains and different regional approaches or even regulations, this document cannot normatively require a specific set of security means. However, if no other appropriate and testable security means are selected for an implementation, the applicable means to secure hybrid communications shall be:

— those specified in ISO/TS 21177, applicable, for example, in support of secure sessions; or

— those based on specifications provided in ETSI TS 103 097 for signing broadcast messages for information dissemination.

These security procedures and principles are used to allow the BSME to assert a level of trust to other BSMEs in the communication network.

This includes support of hybrid communications and hybrid ITS services, where appropriate optional tools may be:

— presentation of application requirements specified in ISO 17423;

— path and flow management specified in ISO 24102-6;

— access technology support specified in ISO 21218;

— generic facilities specified in ISO/TS 17429.

6 Overview of ITS communications

6.1 ITS services and applications

The wide variety of services and applications to be deployed in the ITS sector and the global time-varying nature of transportation itself lead to challenges in the design of communication systems to support these services and applications. One of the challenges is to support widely disparate communication

requirements with respect to reliability, security, latency and other performance parameters. Another challenge is to support widely disparate access technologies and communication protocols with respect to communication range (short, medium, long), communication mode (broadcast or point-to-point, localized communications or networked communications) and performance parameters (latency, throughput, etc.). These challenges are best addressed by specifying ITS services and applications independently of the available access technologies and communication protocols, i.e. technology-agnostic ITS services and applications.

Furthermore, the possibility of having multiple applications in an ITS station unit (ITS-SU) simultaneously competing for communication resources leads to the need for a controlled access to these resources. Useful means for addressing this issue are, for example, application and message prioritization and logical channels and selection of the most appropriate communication protocol stack (identified by a globally unique ITS-S communication protocol stack identifier) and communication route for data transmission.

6.2 ITS communication technologies

ITS communication involves communication between a wide variety of ITS communication nodes on different platforms, for example, vehicles, roadside equipment, portable devices and control centres, using various means and methods, as illustrated in Figure 5. The various access and networking technologies illustrated are used to interconnect stations on a peer-to-peer basis, serving a range of ITS service domains.

The multiplicity of access technologies supported by design in this document expresses basic support of the general principle of "neutrality of technology" typically applied in the ICT service domain; further on this enables several technical features for improving overall efficiency and reliability of communications.

NOTE Neutrality of technologies is never applicable to broadcast services, where all peer entities need to use the same technology to ensure interoperability. Neutrality of technologies is typically applicable for scenarios with private (unicast) communications for services that are provided by various service providers where each service provider selects their supported communication technologies. An end-user can thus select a preferred communication technology by selecting the appropriate service provider; consequently, interoperability between end-user's devices from different service providers can be technically impossible.

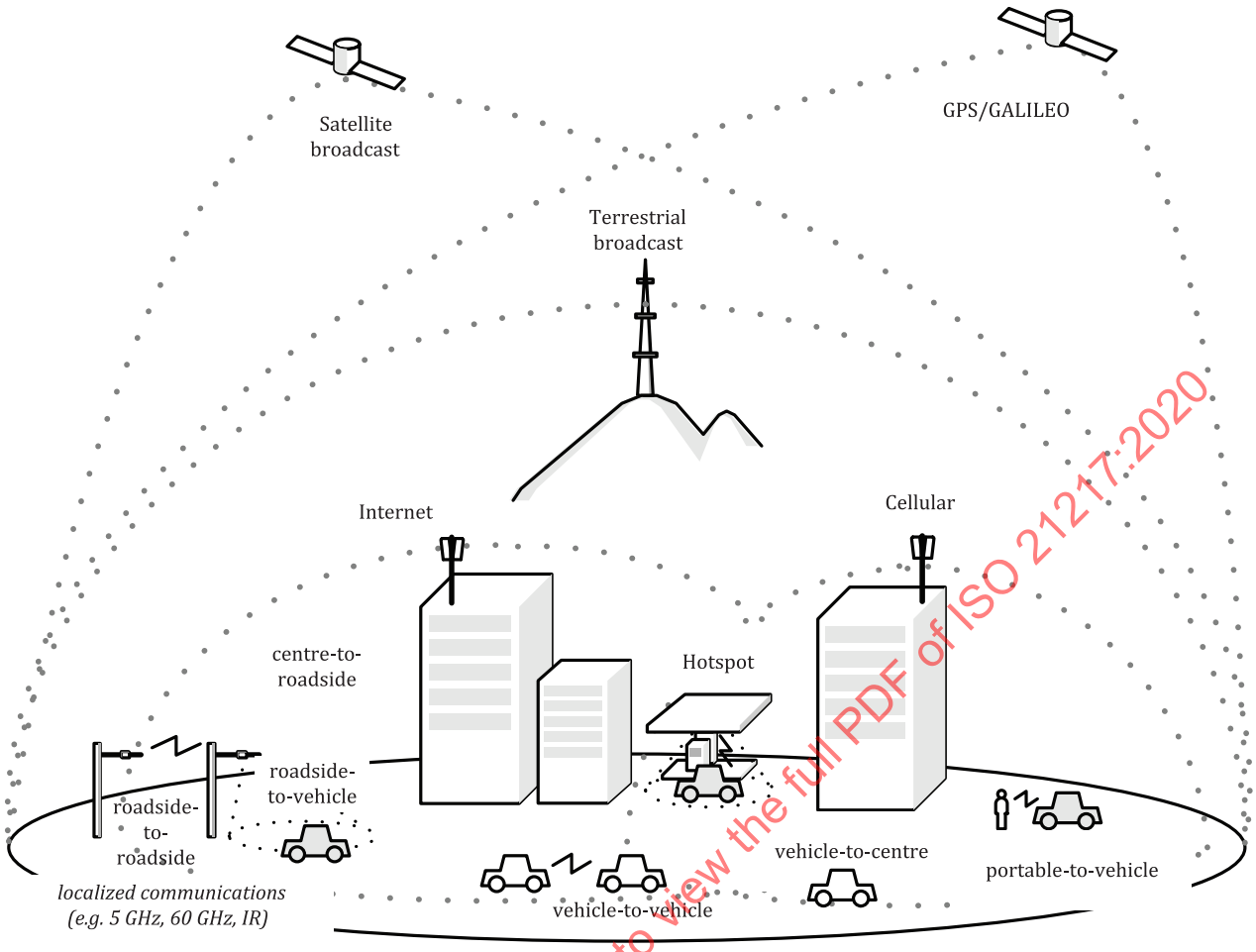

Figure 5 — Examples of ITS communications

6.3 ITS communication characteristics

ITS communication has the following characteristics:

— station mobility leads to complex time-varying networking topologies, and time-varying properties of wireless communication channels (fading, hidden-nodes, etc.);

— variety of stations connected via various networking and access technologies including the internet, various public and private networks, Bluetooth and Wi-Fi, dedicated technologies, such as 5.8 GHz DSRC for road tolling;

— a station with multiple access and networking technologies can maintain session continuity through a change of either or both;

— two stations with different access technologies can establish end-to-end connectivity, e.g. via internet;

— variety of communication requirements resulting from different ITS applications with different priorities, (e.g. road safety, traffic efficiency, mobility and infotainment), with respect to communications capacity (data rate), communications reliability, communications availability, for example;

— variety of communication requirements resulting from user needs, e.g. with respect to communications cost (in terms of money), communications privacy, communications security;

— variety of communication requirements resulting from regional regulations and policies;

— global applicability, where intended.

6.4 Localized and networked communications

ITS communications can be divided into two types of communication modes:

— Localized communications, also referred to as “ad-hoc communications”, are communications between nearby communication nodes without involving the support of an infrastructure network;

— Networked communications are communications using the support of an infrastructure network.

Localized and networked communications can either be:

— single-hop or multi-hop communications, or

— point-to-point or multipoint communications.

NOTE 1 Broadcast communications refers to a particular type of multipoint communications where all nodes in a “network” receive the data transmitted.

NOTE 2 Localized communications are more commonly associated with broadcast dissemination of data for time-critical road traffic. However, services that require point-to-point sessions between nearby nodes without network infrastructure support are also qualified as “localized communications”.

NOTE 3 Localized broadcast dissemination of information can be targeted to a specific geographic area. For this purpose, ETSI developed a “GeoNetworking” protocol, see ETSI EN 102 636. Due to physical constraints in the 5.9 GHz communication channels, GeoNetworking is mainly used for single-hop communications.

6.5 Hybrid communications

ITS services in general, and cooperative ITS services particularly, have different communication requirements and implementation contexts. There is no single access technology nor communication protocol that can fulfil all communication requirements at once, in all situations and all environments. It is thus necessary to use a variety of access technologies and communication protocols in a complementary sense or to provide redundant communication channels.

Hybrid communication support is a feature that allows the combination of multiple access technologies and communication protocols, in particular for:

— localized and networked communications;

— IP-based and non-IP based communications; and

— broadcast-based and session-based communications.

This requires knowledge about the communication requirements of all ITS services and knowledge about the characteristics of all available access technologies and communication protocols. It also requires capabilities for dynamic determination and enforcement of the most appropriate communication profile.

NOTE 1 The basic idea of hybrid communications was developed by the CVIS project[111] without using this term and was already implemented in the first edition of this document. See the ISO 21186 series for a thorough explanation on hybrid communications.

NOTE 2 See ISO/TS 21185 and CEN/TS 17496 for globally unique identification of communication profiles for cooperative ITS.

6.6 ITS communication networks

An illustration of the various networks used in ITS communications is presented in Figure 6.

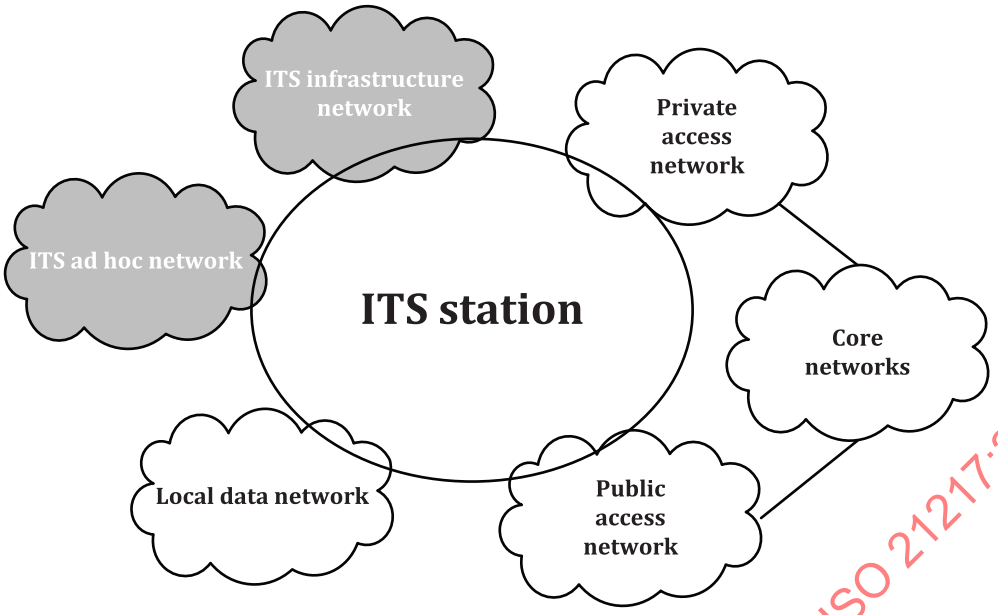

Figure 6 — Networking view of ITS communications

Figure 6 illustrates the following "networks" for localized communications and networked communications (see 6.3):

— An ITS infrastructure network comprised of ITS-SUs with a (quasi-)static topology, e.g. a collection of roadside stations connected via a fibre backbone.

— An ITS ad hoc network comprised of ITS-SUs in which the topology may change rapidly, e.g. a mesh network of (vehicle) stations connected via microwave technologies.

— A local data network, e.g. a proprietary in-vehicle network based on CAN bus technology or a 6LoWPAN wireless sensor network.

— A public access network, e.g. Wi-Fi hotspot or cellular networks.

— A private access network, e.g. a proprietary road operator network.

— A core network, e.g. the internet, a virtual private network.

NOTE 1 The collection of communication nodes that are interconnected with localized communications (see 6.4), in a strict sense does not represent a network, as network routing is not necessary even in situations where localized communications are based on IP.

NOTE 2 An ITS station-internal network is not presented in Figure 6; however, it is necessary in implementations illustrated in Figures 18 and 19.

ITS infrastructure and ITS ad hoc networks are networks specifically designed to accommodate and implement ITS services and applications. They are connected to each other, and to public access, private access and local data networks through an ITS-SU as shown in Figure 6. The concept of an ITS-SU is described in Clause 7.

6.7 ITS station interconnection scenarios

Four basic ITS-SU interconnection scenarios are identified as illustrated in Figures 7, 8, 9 and 10. The distinction between these scenarios is based on two criteria:

— Whether ITS-SUs connect to peer stations with a managed network (networked communication) or without a managed network (localized communication); see 6.1 and 6.4.

— Whether a peer station unit is a BSME presented in 7.1 or not.

This classification of scenarios does not consider any details of the network(s) between the peer station units.

Localized communication (i.e. typically single-hop communication) between two BSMEs is illustrated in Figure 7. This can represent, for example, a link between two vehicle BSMEs, or between a vehicle BSME and a roadside BSME, or between a personal BSME and a vehicle BSME.

Figure 7 — BSME to BSME communication without an external network (single-hop)

Communication between two BSMEs over a managed network (i.e. networked communication; see 6.4) is illustrated in Figure 8. This can represent, for example, a peer-to-peer communication involving a single-hop link from a BSME to a base station of a cellular network which is connected to the internet through which connection to a central BSME is established.

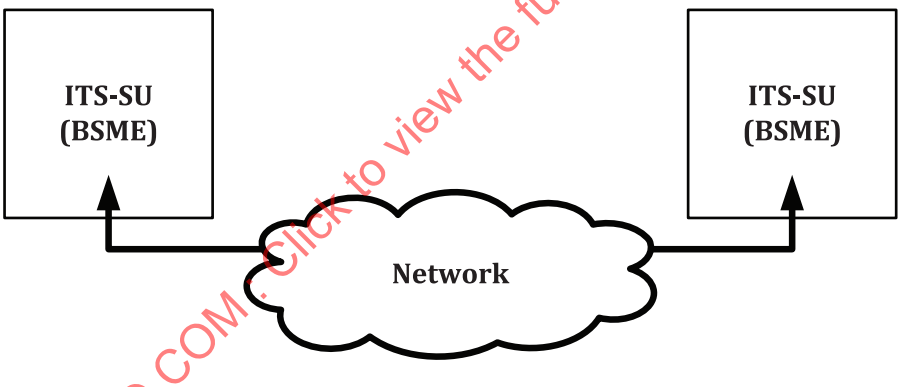

Figure 8 — BSME to BSME communication over an external network (multiple hops)

Single-hop communication between a BSME and an ITS-SU not implementing the principles of a BSMD is illustrated in Figure 9. This can represent, for example, a link between a 5.8 GHz DSRC on-board unit implemented in a vehicle BSME, as specified in ISO 29281-2 and a 5.8 GHz DSRC roadside unit.

Figure 9 — BSME to other node (no BSME) communication without an external network (single-hop)

Communication between a BSME and an ITS-SU (no BSME) involving network connectivity is illustrated in Figure 10. This can represent, for example, a single-hop link from a BSME to a base station of a cellular network which connects to the internet through which connection to an ITS-SU is established.

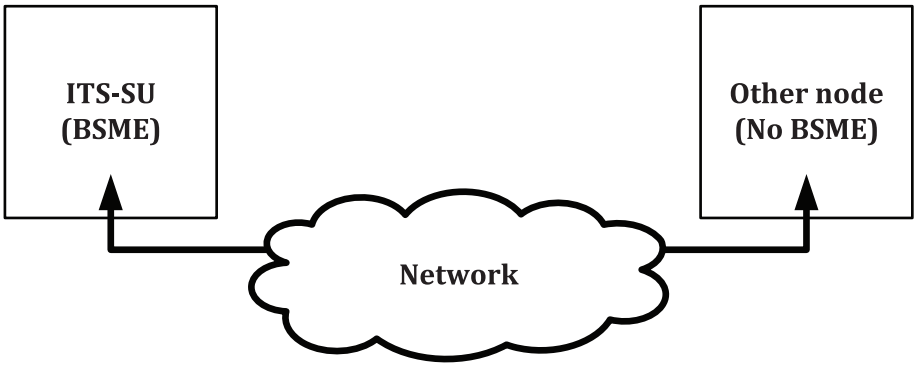

Figure 10 — BSME to other node (no BSME) communication over an external network (multiple hops)

An ITS-SU (with or without implementing the principles of a BSMD) may have multiple simultaneously active sessions involving any or all of these basic communication scenarios.

6.8 Communication paths and data flows

The concept of communication paths and data flows in ITS is very beneficial in describing the abstraction of ITS-S application processes (ITS-S-APs); see ISO 17423 from the communications services available in an ITS-S. This concept is based on similar concepts in IP networking; see RFC 3917. Procedures for ascertaining available communication paths and for mapping data flows to those communication paths are divided into distinct functions within the ITS-S management entity as specified in ISO 24102-6. Path and flow management is a feature in support of hybrid communications.

An **ITS-S path** is defined as a directed sequence of nodes connected by links, starting at a source node (VCI which connects to the next hop node) and ending at one or more destination nodes. Note that for bidirectional communications, two such paths exist, i.e. one at each peer station. Note further that there can be multiple paths between a source and its destination.

An **ITS-S flow type** is defined as a set of communication requirements and characteristics associated with a specific flow.

An **ITS-S flow** is defined as an identifiable sequence of packets of a given ITS-S flow type to be transmitted to one or more entities over an ITS-S path. Each ITS-S flow is identified by a **FlowID** which is unique in an ITS-SU and is mapped to a given communication path or a set of available ITS-S paths.

Categories of communication requirements and objectives requested by an ITS-S application process to select an appropriate communication profile and communication path include e.g. operational, destination type, performance, financial, security, and protocol requirements; see ISO 17423.

In general, it cannot be ensured that the communication requirements will be met all along a communication path as there can be no knowledge of the capabilities of all the nodes along a particular path.

Figure 11 illustrates the architectural components (building blocks and management data flows) of the ITS-S which are involved in the ITS-S path selection process. The same architecture applies to the communication profile selection process introduced in 7.1 and specified in ISO 17423.

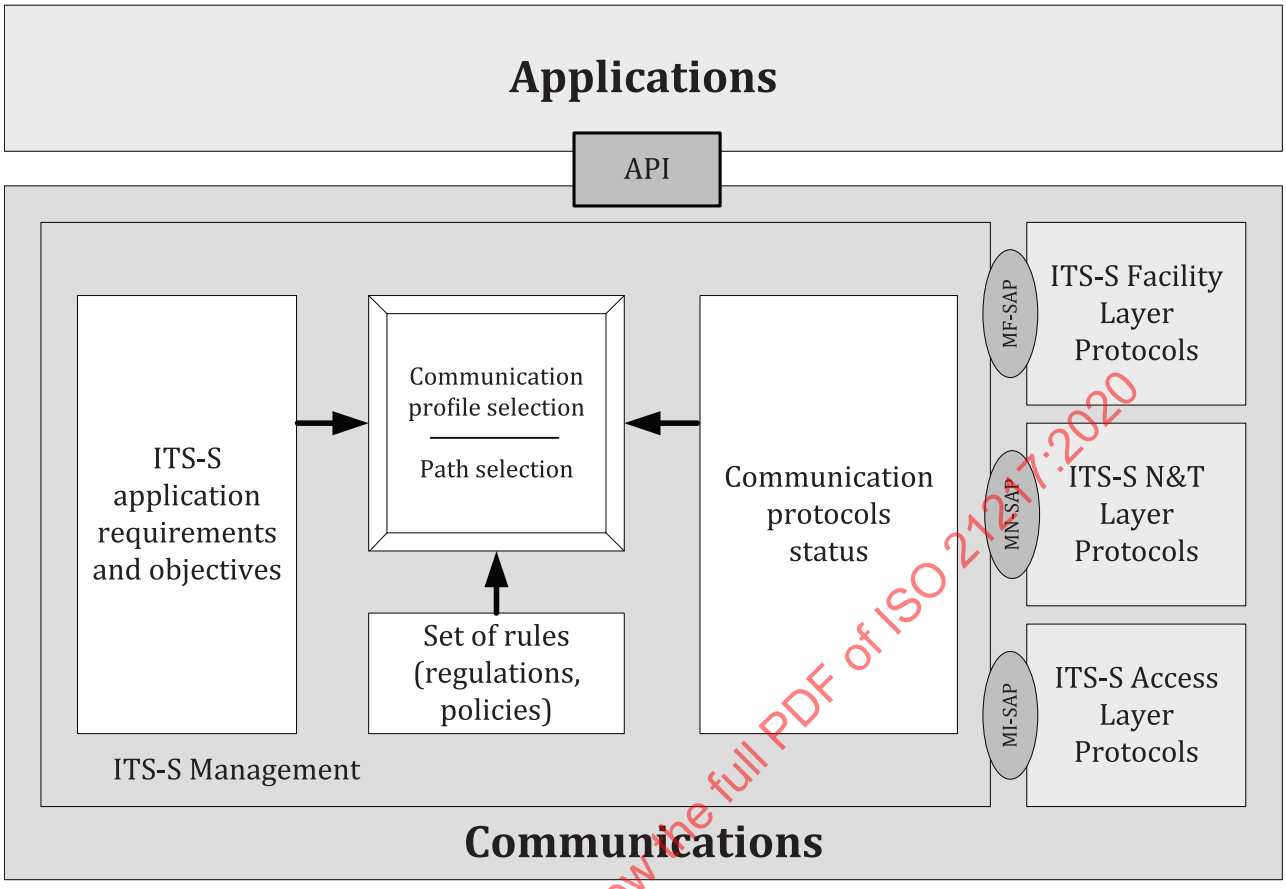

Figure 11 — Architecture of communication profile and path selection

"Communication protocols status" contains the continuously updated properties and status of:

— the various CIs and VCIs in the ITS-S access layer,

— protocols and parameters in the ITS-S networking and transport layer,

— protocols, functions and parameters in the ITS-S facilities layer.

It is updated via MI-SAP, MN-SAP and MF-SAP.

Requirements and objectives obtained from ITS-S application processes (e.g. from ITS-S applications via the API or from ITS-S facility applications via the MF-SAP) are maintained in "ITS-S application requirements and objectives".

NOTE The ITS-S path selection process requires maintenance of further tables presented in ISO 24102-6 that are not illustrated in Figure 11.

7 ITS station — overview

7.1 ITS station — concept

The ITS station concept is based on the abstraction of ITS application processes from communication protocols serving these ITS application processes along with the ability to securely manage those application processes and communications. It is embodied in the abstract definition of an ITS station (ITS-S) as a "Bounded Secured Managed Domain" (BSMD), i.e. a trusted ITS-S described in this document. An instantiation of a trusted ITS-S is referred to as a "Bounded Secured Managed Entity"

(BSME) if the trust nature of the implementation is relevant. In general, an instantiation of an ITS-S is referred to as an "ITS station unit" (ITS-SU).

NOTE In this document, the acronym ITS-S is used to indicate an ITS station based on the principles of the BSMD. A general classification of stations used in ITS is outside the scope of this document. A general high-level description of communications in cooperative ITS is presented in ISO/TR 17465-1.

The salient feature of the ITS-S concept that distinguishes it from the concept behind traditional communication systems is that application processes are abstracted from both the access technologies that provide the wireless connectivity and the networks that transport the information from the source to the destination(s). ITS-Ss are not limited to either a single access technology, or to a specific networking and transport protocol. ITS-SUs can implement any of those technologies that are supported through appropriate adaptation specifications.

While the aforementioned abstraction is generally useful for most application processes, this abstraction does not prevent application processes from requesting a specific communication profile to be considered in the communication profile selection process as specified in ISO 17423, or specifying communication parameters on a packet-per-packet basis as specified in ISO 21218, ISO 29281-1, and IEEE Std 1609.3(TM)

The flexibility that ITS-S management has to make optimal use of all available ITS-S resources (communication media and higher-layer protocols) is one of the key enabling features of ITS communications and applications.

The ITS-S management continuously identifies the available ITS-S capabilities provided by all ITS-S MSEs in the ITS-S layers (see also ISO 24102-6).

EXAMPLE An example of ITS-S capabilities are ITS-S facilities services.

The means for (dynamically) assigning ITS-S application processes to communication media and networking and transport layer protocols are specified in ISO 24102-6, ISO 21218, ISO 17419 and in ISO 17423. To exploit this flexibility, BSMD-conformant systems provide the ability to support handover of different types including:

— those involving a change of CI (which can or can not involve a change of access technology, since ITS-SUs may have multiple CIs using the same access technology),

— those involving reconfiguration or change of the network employed to provide connectivity, and

— those involving both a change in CI and network reconfiguration.

The handover architecture is specified in ISO 24102-6.

Finally, in order to be able to meet the stringent security requirements of ITS application processes related to safety of life and property, the ITS-S concept provides for secure peer-to-peer communications between entities that are themselves capable of being secured and remotely managed. While this is an abstract definition, it has very specific physical consequences. The bounded nature is derived from the requirement for ITS-Ss to be able to communicate amongst themselves, i.e. peer-to-peer, as well as with devices that are not secured. Realizing that to achieve this in a secure manner often requires distribution and storage of security-related material that must be protected within the boundaries of the ITS-S, leads to the secured nature of the entity. As there is great flexibility to achieve desired communication goals, there is a requirement that this flexibility be managed. Thus, ITS-Ss are referred to as BSMDs.

7.2 ITS station architecture

7.2.1 Generalized OSI model

The "ISO Open Systems Interconnect Reference Model" specified in ISO/IEC 7498-1 is used in a number of figures within this documents with reference to the ITS-S communications architecture that embodies the ITS station concept. Several levels of abstraction are used to illustrate different points of view.

Figure 12 shows the general ITS-S reference architecture, including interfaces (IN Interface, NF Interface, FA Interface, MI Interface, MN Interface, MF Interface, MA Interface, SI Interface, SN Interface, SF Interface, SA Interface, MS Interface, API) between the various blocks with informative details. Such interfaces can be partly non-observable and thus non-testable service access points (SAPs), or observable and testable interfaces (e.g. plug-and-play), or application programming interfaces (APIs).

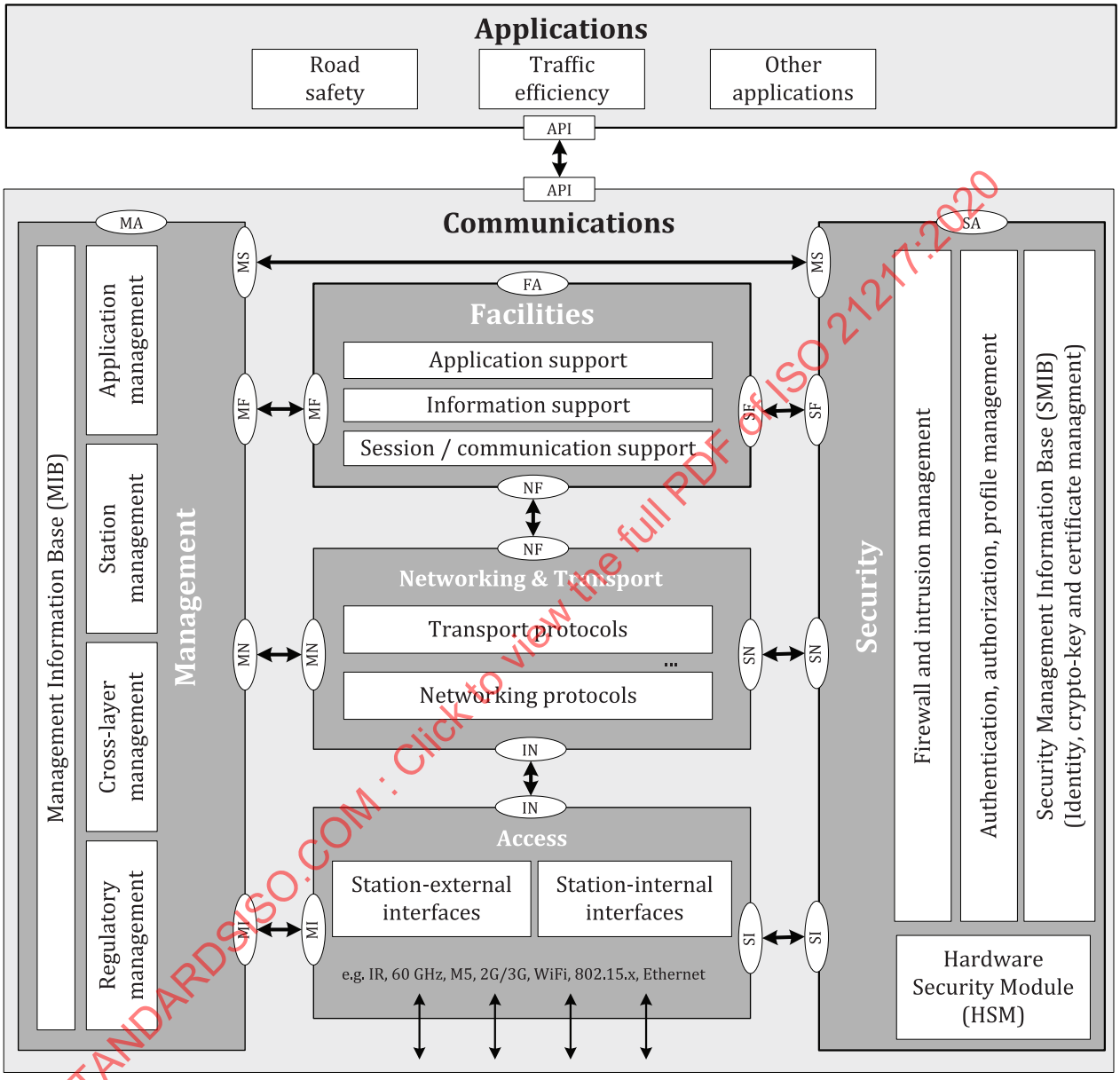

Figure 12 — ITS-S reference architecture

A simplified presentation of the ITS-S reference architecture is shown in Figure 13.

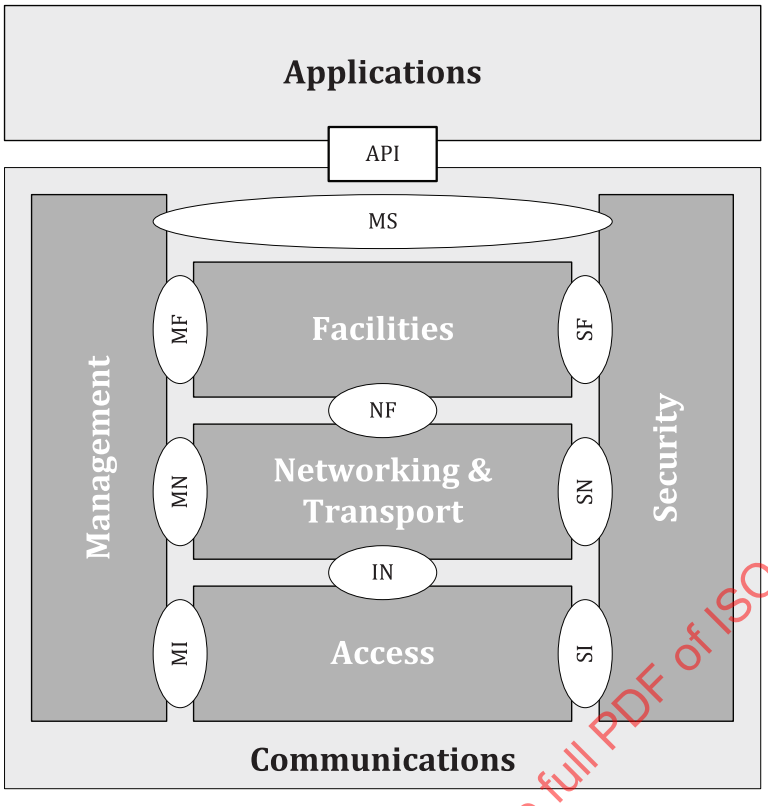

Figure 13 — Simplified ITS-S reference architecture

NOTE The MA, FA and SA interfaces are not shown explicitly in Figure 13, as the functionality of these interfaces is provided in the API.

The blocks in Figure 12 and Figure 13 contain the following functionality:

— ITS-S access layer, referred to as "Access", comprised of OSI layers 1 (Physical) and 2 (Data Link) of the OSI communication protocol stack,

— ITS-S networking and transport layer, referred to as "Networking & Transport", comprised of OSI layers 3 (Network) and 4 (Transport) of the OSI communication protocol stack,

— ITS-S facilities layer, referred to as "Facilities", comprised of OSI layers 5 (Session), 6 (Presentation) and 7 (Application) of the OSI communication protocol stack,

— ITS-S management entity, referred to as "Management", containing station management functionalities,

— ITS-S security entity, referred to as "Security", comprised of security services provided to the OSI communication protocol stack and to the ITS-S management entity,

— ITS-S application entity, referred to as "Applications", which make use of the OSI communication protocol stack.

The functional blocks presented in Figures 12 and 13 are interconnected either via observable interfaces or via SAPs, as specified in ISO 24102-3, ISO 21218, and ISO 29281-1, for example, or via an API. The identifiers of these interfaces are shown in Figures 12 and 13.

Implementations of ITS stations, referred to as ITS-SUs, constitute "endpoints" of a communication path. An ITS-SU designed and configured to provide one or several specific ITS services to its user is expected to provide those functionalities of the blocks in Figures 12 and 13 that are necessary for these ITS services. Some of the functionalities in the various blocks can not be applicable and therefore do not need to be implemented. For example, some ITS-S application processes can not require specific support

from the ITS-S facilities layer or from the ITS-S security entity. The requirement to instantiate certain functionalities does not imply anything about the actual implementation. These functionalities (blocks) may be spread over several physical devices, or they may be implemented inside a single device, as illustrated in this document.

7.2.2 ITS station nodes

An ITS-SU comprises ITS-SCUs connected via an ITS station-internal network as illustrated in 7.2.4. The functionality contained in an ITS-SCU may be expressed by the functionalities of one or several ITS-S nodes as illustrated in Annex B. The following ITS-S nodes are identified:

a) ITS-S router

   1) ITS-S border router

      — Access router

      — Mobile router

   2) ITS-S internal router

b) ITS-S host

c) ITS-S gateway

The following definitions apply (see also Clause 3):

— An **ITS-S router** is an ITS-S node comprised of routing functionalities of an ITS-S used to connect two networks and to forward packets not explicitly addressed to itself as illustrated in Figure 14 with the example of an ITS station-internal network and an external network B.

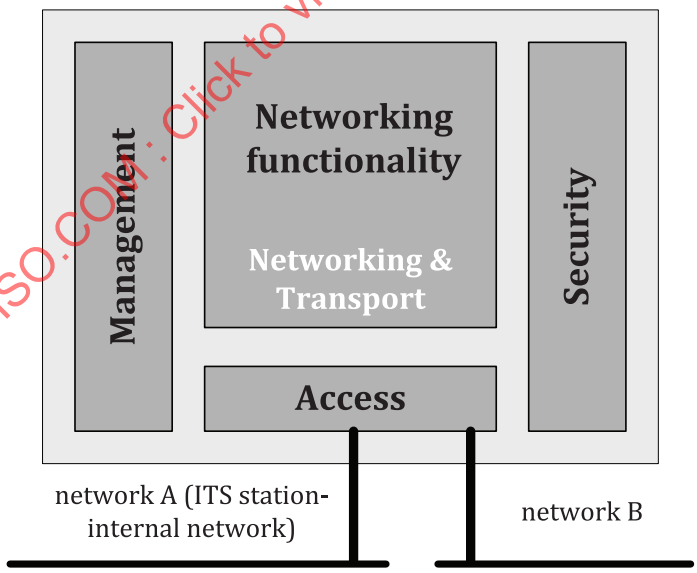

Figure 14 — ITS-S router

— An **ITS-S border router** is an ITS-S router with additional functionality that provides connectivity to other ITS communication nodes over external networks (network B in Figure 14).

— An **ITS-S access router** is an ITS-S border router with additional functionality that provides other ITS communication nodes a point of attachment to an external network.

— An **ITS-S mobile router** is an ITS-S border router with additional functionality that allows a change of point of attachment to an external network while maintaining session continuity.

— An **ITS-S internal router** is an ITS-S router that connects two or more ITS station-internal networks.

— An **ITS-S host** is an ITS-S node comprised of ITS-S functionalities other than the functionalities of an ITS-S router, ITS-S border router, ITS-S mobile router, or an ITS-S gateway, i.e. not capable to forward packets not explicitly addressed to itself.

NOTE Being an ITS-S node, an ITS-S host contains the communication functionality to connect to at least one network, although routing functionality is not part of the ITS-S host functionality.

— An **ITS-S gateway** interconnects an "external protocol stack" to the ITS-S management entity, or to the ITS-S facilities layer, or to the ITS-S networking and transport layer, and thus supports also direct routing on a default path to internet which enables end to end communications. An ITS-S gateway may convert between different protocols. The protocol stack on the right-hand side in Figure 15 is connected to the ITS station-internal network. The protocol stack on the left-hand side in Figure 15 is connected to an external network.

NOTE The external network can be a proprietary network based on a technical specification that is not publicly available. Data management details of an ITS-S gateway are specified in ISO/TS 21184, for example. Details on how to establish secure sessions between ITS-SCUs (see 7.2.4), and between an ITS-SCU and an external network are specified in ISO/TS 21177.

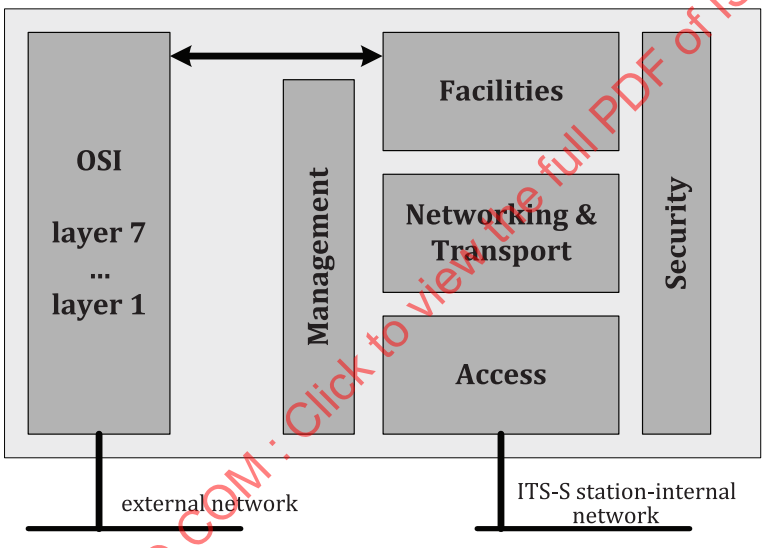

Figure 15 — Example of an ITS-S gateway at the ITS-S facilities layer

7.2.3 Protocol and service data units in the ITS-S protocol stack

Figure 16 shows the data unit transfer (i.e. SDUs and PDUs) through the ITS-S communication stack of two peer ITS stations communicating with each other, and the grouping of protocol layers as used in ITS:

— Session, presentation and application OSI layers 5 through 7 comprise the ITS-S facilities layer.

— Network and transport OSI layers 3 and 4 comprise the ITS-S networking & transport layer.

— Physical interface and link control OSI layers 1 and 2 comprise the ITS-S access layer.

The naming and usage of SDUs and PDUs follows the principles outlined in ISO/IEC 7498-1.

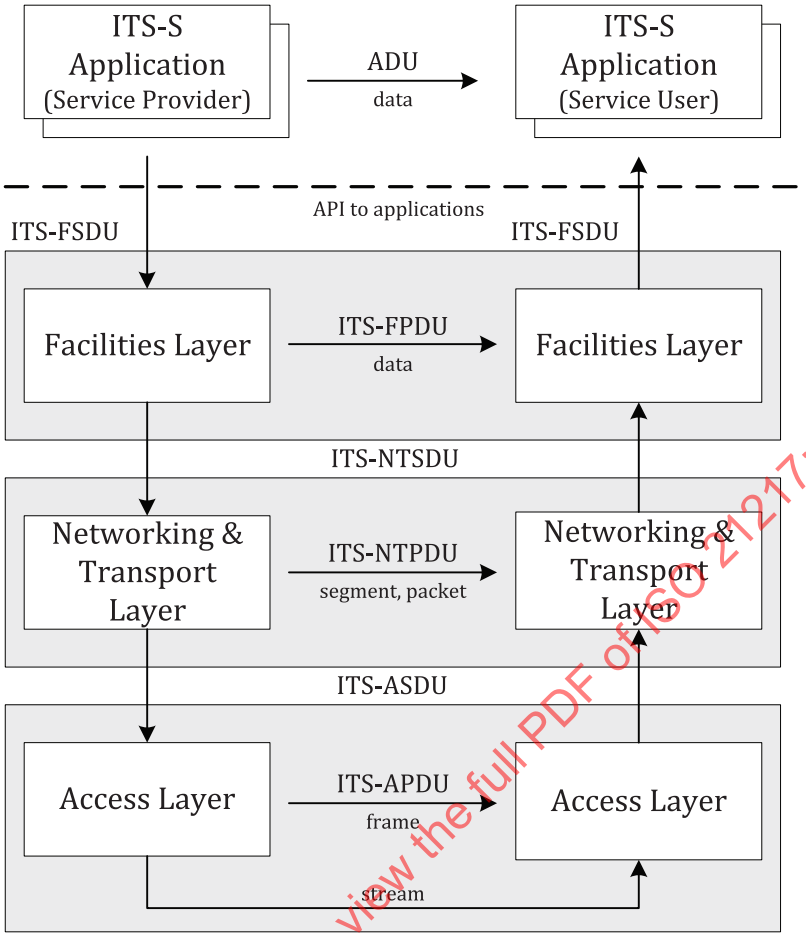

Figure 16 — OSI data unit transfer in an ITS station

PDUs exchanged between peer ITS-S access layers are named ITS-APDUs. PDUs exchanged between peer ITS-S networking and transport layers are named ITS-NTPDUs. PDUs exchanged between peer ITS-S facility layers are named ITS-FPDUs. Data units exchanged between ITS-S applications are named ADUs. Similarly, SDUs are introduced for ITS communications with the names ITS-FSDU, ITS-NTSDU and ITS-ASDU.

NOTE The deprecated term ITS-NPDU is in use in published documents with the same meaning as ITS-NTPDU.

7.2.4 Distributed implementations of ITS-S roles

An implementation of the functionality of an ITS station is named “ITS-S Unit” (ITS-SU).

NOTE The term ITS-S quite often is used synonymously to ITS-SU.

The roles of an ITS-S can be implemented in physical units, which are interconnected via an ITS station-internal network presented in Figure 6. Such a physical unit is named “ITS station communication unit” (ITS-SCU). Every ITS-SCU can be addressed uniquely inside an ITS-SU. Typically, an ITS-SCU is an implementation of, for example, an ITS-S host, an ITS-S router, an ITS-S gateway, an ITS-S border router or a mixture of these functional elements. This is to say that each ITS-SCU constitutes an ITS-S node specified in 7.2.2. Details of ITS-SCUs are specified in ISO 24102-4.

Distributed and combined implementations of ITS-S roles are illustrated for the roles ITS-S host and ITS-S router in the following Figures 17, 18 and 19.

Figure 17 shows two ITS-SUs without ITS station-internal networks. The two ITS-SUs are interconnected via a wireless ITS link.

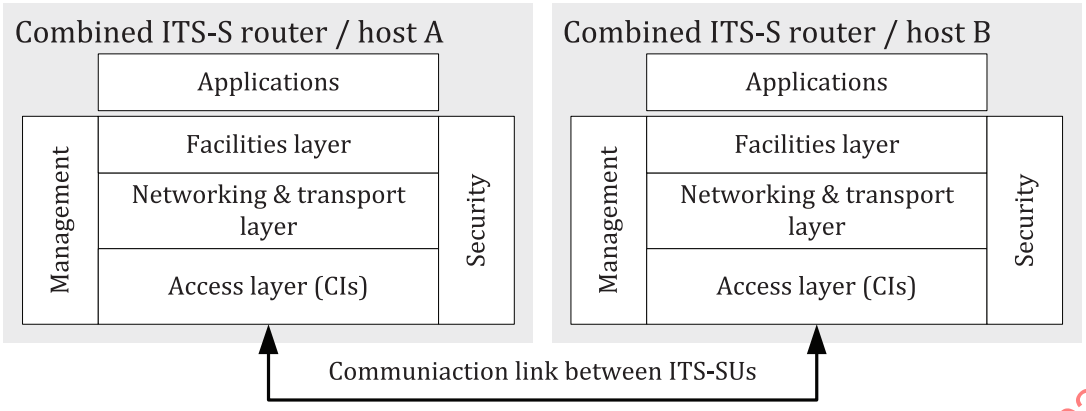

Figure 17 — Implementation architecture I

Figure 18 shows two ITS-SUs with ITS station-internal networks. The two ITS-SUs are interconnected via a wireless ITS link.

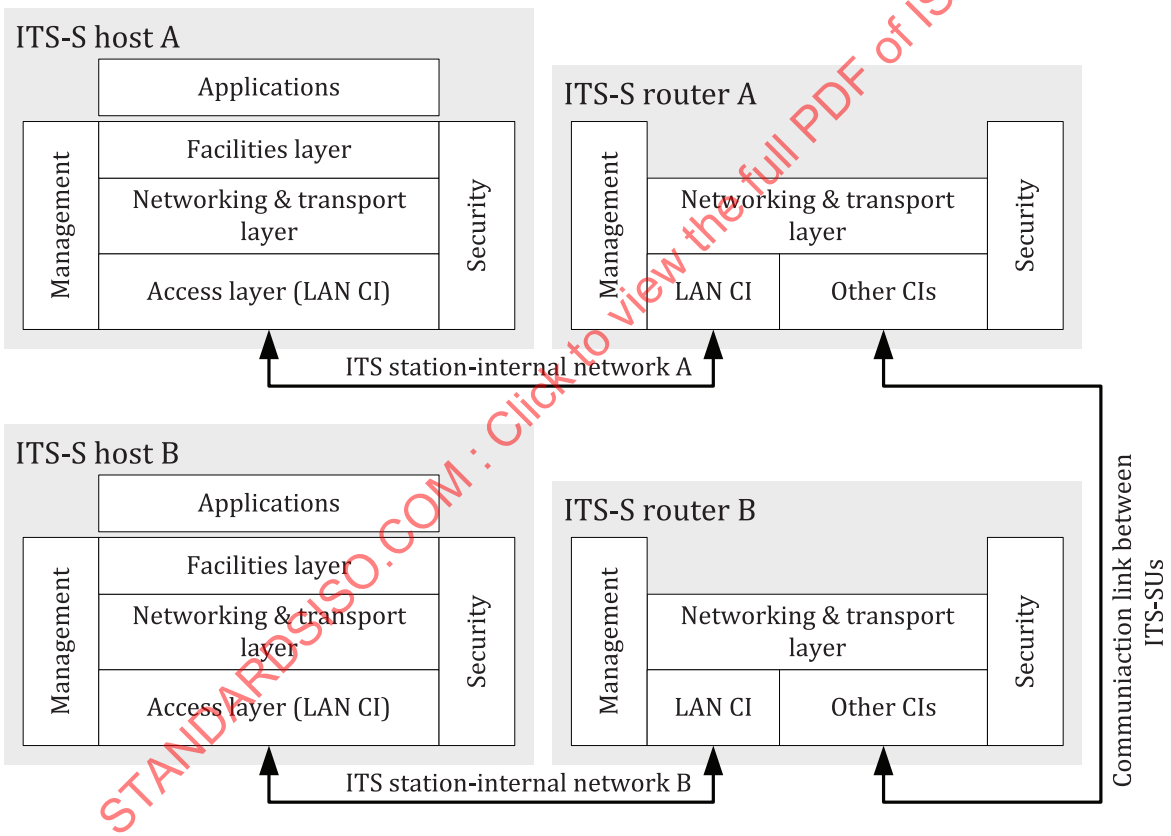

Figure 18 — Implementation architecture II

Figure 19 shows two ITS-SUs, where the ITS-SU A has an ITS station-internal network, and where ITS-SU B has no ITS station-internal networks. The two ITS-SUs are interconnected via a wireless ITS link.

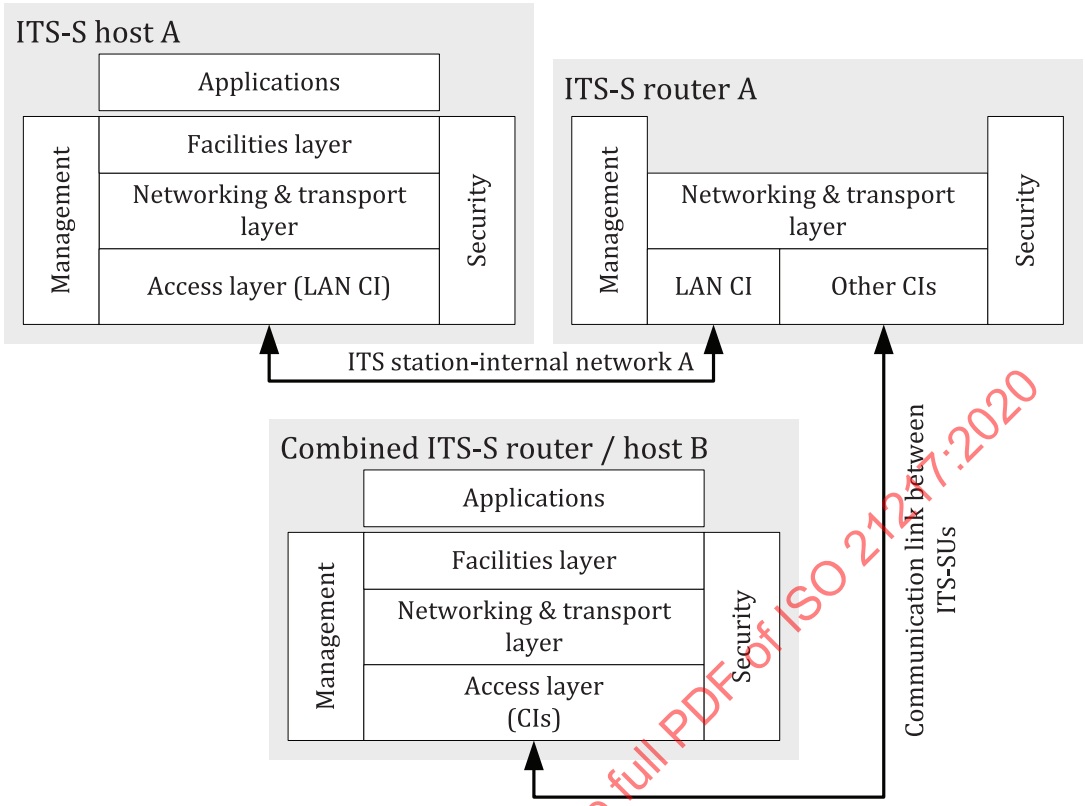

Figure 19 — Implementation architecture III.

More detailed illustrations of implementation details are provided in Annex B.

8 Details of elements of ITS-S reference architecture

8.1 ITS-S interfaces

8.1.1 Implementation habits

The interface towards the ITS-S applications is typically implemented as an API. All other interfaces typically are implemented as an SAP.

NOTE An API depends on the operating system for which it is designed.

8.1.2 ITS-S management interfaces

ITS-S management interfaces are specified in ISO 24102-3 and are listed below:

— MI: Enables the ITS-S management entity to interact with the ITS-S access layer (OSI layers 1 and 2).

— MN: Enables the ITS-S management entity to interact with the ITS-S networking and transport layer (OSI layers 3 and 4).

— MF: Enables the ITS-S management entity to interact with the ITS-S facilities layer (OSI layers 5 through to 7).

— MS: Enables the ITS-S management entity to interact directly with the ITS-S security entity.

— MA: Enables the ITS-S management entity to interact directly with the ITS-S application entity.

8.1.3 ITS-S security interfaces

ITS-S security interfaces are listed below.

— SI: Enables the ITS-S security entity to interact with the ITS-S access layer (OSI layers 1 and 2).

— SN: Enables the ITS-S security entity to interact with the ITS-S networking and transport layer (OSI layers 3 and 4).

— SF: Enables the ITS-S security entity to interact with the ITS-S facilities layer (OSI layers 5 through to 7).

— SA: Enables the ITS-S security entity to interact with the ITS-S application entity.

8.1.4 ITS-S communications interfaces

ITS-S communications interfaces are specified in ISO 21218 and ISO 29281-1 and other documents on communication protocols, and are listed below.

— IN: Allows the ITS-S networking and transport layer and the ITS-S access layer to interact with each other.

— NF: Allows the ITS-S facilities layer and the ITS-S networking and transport layer to interact with each other.

— FA: Allows the ITS-S facilities layer to interact with ITS-S applications.

8.1.5 ITS-S application programming interface

An API is an implementation of the MA, FA and SA interfaces which connect ITS-S applications to the ITS-S facilities layer and the ITS-S security and management entities.

8.2 ITS-S access layer

8.2.1 Access technologies

The ITS-S access layer is part of the ITS station reference architecture as illustrated in Figure 20.

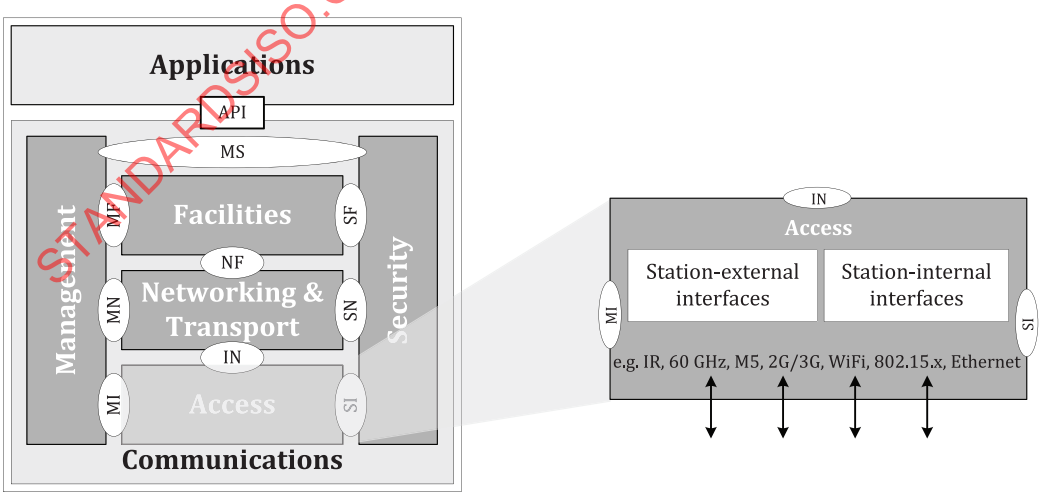

Figure 20 — ITS-S reference architecture — ITS-S access layer

The ITS-S access layer provides means for communication between entities both inside and outside a station through interfaces. The following four classes of interfaces are distinguished:

a) Wireless interfaces out of an ITS-S.

b) Wired interfaces out of an ITS-S.

c) Wireless interfaces for station-internal communications.

d) Wired interfaces for station-internal communications.

The following wireless access technologies shown in Figure 5 have been developed specifically for ITS applications and services for localized communications, and are specified in various ITS standards. Such access technologies are named "ITS-S access technologies":

— "Infrared light" (IR); see ISO 21214,

— "Microwaves at 5 GHz, based on IEEE Std 802.11" (ITS-M5; see ISO 21215), (ITS-G5; see ETSI EN 302 663 and ETSI TS 102 724), (WAVE; see IEEE Std 1609.0(TM) and IEEE Std 1609.4(TM)),

— "Millimetre waves" (MM) at 60 GHz; see ISO 21216,

— "Optical camera communications" (OCC); see ISO 22738.

Other access technologies for localized or networked communications shown in Figure 5 are specified by reference to the standards according to which they operate:

— Satellite networks; see ISO 13183 and ISO 29282,

— 2G cellular systems; see ISO 21212,

— 3G cellular systems (UMTS); see ISO 21213,

— 4G cellular systems (LTE); see ISO 17515-1, ISO 17515-2 and ISO 17515-3,

— IEEE 802.16; see ISO 25111 and ISO 25112,

— HC-SDMA; see ISO 25111 and ISO 25113,

— IEEE 802.15; see IEEE Std 802.15.4(TM) and IEEE Std 802.15.5(TM).

For these access technologies, an adaptation as specified in ISO 21218 can be required in order to interface to the ITS-S management entity, to the ITS-S security entity and to the ITS-S networking and transport layer; see the ITS station reference architecture illustrated in Figure 12.

Regionally specified DSRC systems may be supported in ITS-SUs as specified in ISO 24103 and ISO 29281-2. Services based on the DSRC standards (see ISO 15628 and CEN EN 12834) can be supported in the ITS environment as specified in ISO 29281-2.

Positioning data from satellite networks such as GPS, GALILEO or GLONASS may be received and provided to the related ITS-S application processes.

The access technologies illustrated in Figures 5, 12 and 20 and listed above are examples of technologies well suited for ITS-Ss. The ITS station architecture is compatible with a wide variety of other access technologies which are not mentioned herein.

8.2.2 Details of the ITS-S access layer

Figure 21 shows details of the ITS-S access layer.

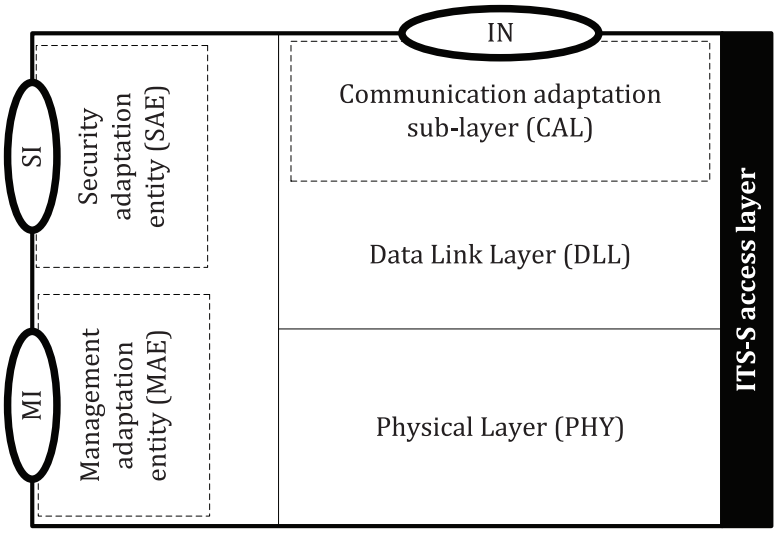

Figure 21 — Elements of the ITS-S access layer

The ITS-S access layer consists of:

— an OSI physical (PHY) layer and an OSI data link layer (DLL),

— the adaptation elements (MAE, SAE, CAL), if necessary,

— the following interfaces:

  — MI to the ITS-S management entity; see ISO 24102-3,

  — SI to the ITS-S security entity; see ISO 24102-3, and

  — IN to the ITS-S networking and transport layer, see ISO 21218,

as illustrated in Figure 21.

The data link layer consists of a MAC sub-layer and an LLC sub-layer, as specified in ISO 21218. There is generally a dedicated MAC sub-layer for every PHY layer. Details of MAC sub-layers are generally specified together with the associated PHY layer standards.

The CAL provides the IN-SAP as specified in ISO 21218 for any instantiation of a DLL. The CAL can be interpreted as an extension of an existing LLC or MAC protocol. The MAE provides the MI-SAP as specified in ISO 24102-3. Implementations of the CAL and MAE are access technology dependent.

The role of the SAE is to provide a common interface to the security entity. Implementations of the SAE are access technology dependent.

An instantiation of an access technology is called a CI. The concept of a CI is specified in ISO 21218. An ITS-SU contains one or more CIs.

The need to support single-hop links with different physical characteristics (e.g. transmit power) over the same CI leads to the concept of VCIs. Details of VCIs are specified in ISO 21218.

The ITS-S access layer supports prioritization of the processing of received frames (see Figure 16), and the configuration and management of prioritization by the ITS-S management entity through the MI-SAP.

8.2.3 Logical channels

CIs provide PCHs that are mapped to one or more LCHs by the station management; see ISO 17419. Mapping of LCHs to PCHs depends on the requirements of the logical channels, and properties of the physical channels. Multiple LCHs can be mapped to a single PCH.

The following is a list of some potentially useful LCHs in a communication system:

— control channel (CCH) on which basic channel control information, communication and application management information is disseminated or exchanged,

— service announcement (also referred to as “service advertisement”) channel (SaCH), where applications and services currently being offered are advertised by a station with service provider role; see ISO 22418,

— service channels (SCHs), where peer to peer ADU exchanges take place, and message dissemination may take place,

— safety channels (SfCHs), where safety of life and property critical information is disseminated or exchanged.

The concept of logical channels provides increased flexibility in application and message prioritization; see ISO 17419 and ISO 17423. For example, creation of a logical SfCH allows a regulatory agency to specify that such a channel is reserved for safety-related exchanges only, and then give characteristics of the physical channels to which the SfCH can be mapped (e.g. dedicated to safety only), providing system designers the flexibility to maximize channel capacity by appropriately configuring the RF parameters.

As described in 6.8, ITS-S application processes are assigned one or more flows that are used to identify the communication resources to be used when transmitting a data packet (PDU). A given flow may be mapped to only one logical channel.

8.2.4 Prioritization of transmission requests

Prioritization of transmission requests in the ITS-S access layer is used to handle multiple flows associated with ITS application processes in an ITS-S contending for access to the same physical communication channel in an ITS-S. In an ITS-S, prioritization can take place in the CAL, the LLC sub-layer and the MAC sub-layer, and where it takes place depends on the details of the ITS-S access layer and the implemented CAL. Implementation inside the CAL is necessary when neither the MAC nor LLC sub-layers provides a prioritization mechanism. Nothing prevents prioritization from occurring in multiple layers. The cumulative effect is equivalent to (possibly multiple layer) buffering of packets for transmission, with possibly different criteria for packet transfer between the buffers in the sub-layers.

8.2.4.1 Station-internal contention

Station-internal contention for resources is largely an implementation issue. In distributed implementations of ITS-Ss, there can be contention for access to a medium (station-internal ethernet) used to exchange information between ITS-S nodes and there can be limited ability to store data (buffers full). The resolution of such issues is implementation dependent and can use various standards.

Station-internal contention can also occur in the receive path, for example, if too many signed messages are received in a time unit such that the necessary crypto-procedure cannot be applied to all of them in due time. Consequently, prioritization in the receive path is a way to manage such contention.

8.2.4.2 Station-external contention

The final arbiter in the chain of prioritization mechanisms from the CAL to the PHY is the one ultimately responsible for mediating physical channel access. Generally, this will occur in the MAC sub-layer of a given access technology because therein, information about the current activity on the physical channel is made available. Furthermore, prioritization of PDUs being sent by ITS-S application processes must also be considered. Since there is no globally harmonized scheme for such prioritization, means for creating mappings between various prioritization schemes are necessary. For example, ISO 21218 specifies a 256-level priority scheme in the ITS-S access layer, ISO/IEC 8802-2 specifies an 8-level priority scheme for data transmission requests in the OSI DLL, and IEEE Std 802.11(TM) specifies only four levels in the OSI medium access sub-layer. Mapping of the 256 and 8 levels to the 4 levels is implementation dependent (though defaults are given).

8.3 ITS-S networking and transport layer

8.3.1 ITS-S networking and transport layer details

The ITS-S networking and transport layer is part of the ITS-S reference architecture as illustrated in Figure 22.

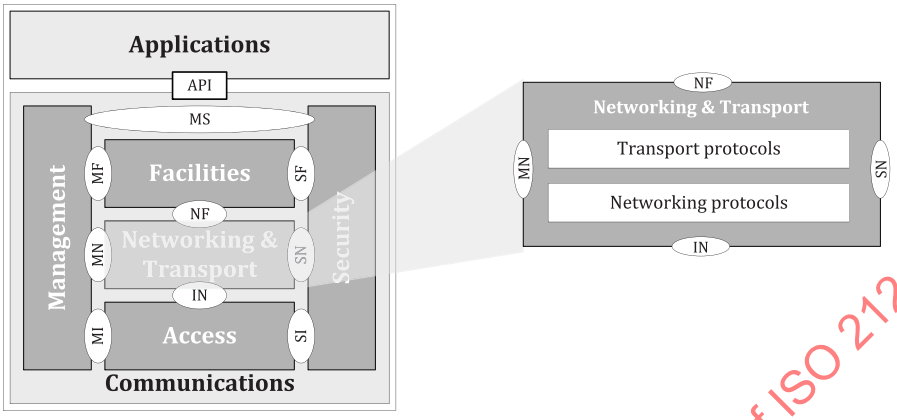

Figure 22 — ITS-S reference architecture — ITS-S networking and transport layer

Figure 23 shows details of the ITS-S networking and transport layer.

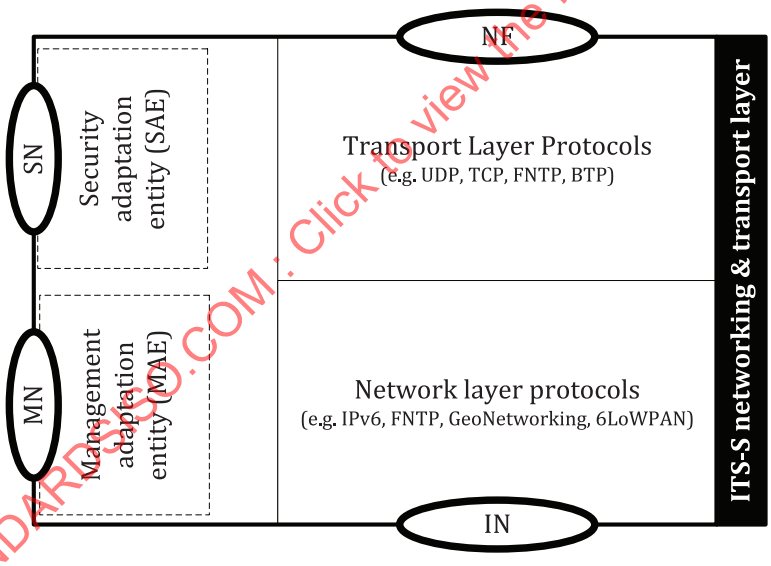

Figure 23 — Elements of the ITS-S networking and transport layer

The ITS-S networking and transport layer consists of the following elements, as presented in Figures 12, 22, 23:

— an OSI network layer and an OSI transport layer,

— the adaptation elements (MAE, SAE), if necessary, and

— the following interfaces:

  — MN to the ITS-S management entity; see ISO 24102-3,

  — SN to the ITS-S security entity; see ISO 24102-3,

  — IN to the ITS-S access layer, see ISO 21218, and

— NF to the ITS-S facilities layer; see ISO 29281-1 amongst others,

The ITS-S networking and transport layer supports prioritization of received packets (see Figure 16), and the configuration and management of prioritization by the ITS-S management entity through the MN-SAP.

8.3.2 Networking protocols

The OSI network layer connects the OSI data link layer to the OSI transport layer. Multiple optional and complementary network protocols running independent of each other may be supported.

Two classes of network protocols are identified.

— Internet protocols:

  — IPv4 is the IP protocol version most widely deployed. However, the IPv4 address space is exhausted, and IPv4 does not fully meet deployment requirements of Cooperative ITS.

  — IPv6 provides features in support of Cooperative ITS requirements and has a practically unlimited address space. Details on usage of IPv6 for ITS are found in ISO 21210 and in the ITSSv6 project [113]. Same base specifications from IETF are e.g. RFC 2460, RFC 3587, RFC 3917, RFC 3963, RFC 4291, RFC 4294, RFC 4493, RFC 4861, RFC 4862, RFC 5648.

  — In order to support communication with IPv4 based systems, IPv4 — IPv6 transition mechanisms can be used.

  — 6LoWPAN; see ISO 19079 and ISO 19080.

— Other protocols:

  — The FNTP, specified in ISO 29281-1 is designed for ITS-S application processes with severe time constraints and low latency requirements, e.g. time-critical safety related applications as illustrated in ETSI TR 102 638. FNTP does not provide networking capabilities at the ITS-S networking and transport layer, but uses MAC addresses of access technologies for identifying nodes in the network.

  — The WSMP, specified in IEEE Std 1609.3(TM) is designed for ITS-S application processes with severe time constraints and low latency requirements, e.g. time-critical safety related applications as illustrated in ETSI TR 102 638.

  — GeoNetworking specified in ETSI EN 102-636 uses geo-coordinates to identify target areas of possible destination stations. Geographical area definitions are provided in ETSI EN 302 931. The basics of GeoNetworking, beyond other methods of geo-dissemination of information, were developed in the EU research project GeoNet [112].

A priori, nothing prevents the tunnelling of networking protocol A over networking protocol B, equivalently encapsulating networking protocol A into networking protocol B, e.g. tunnelling IPv6 over GeoNetworking as specified in ETSI EN 102-636.

8.3.3 Transport protocols

The OSI transport layer connects the OSI network layer with the ITS-S facilities layer and provides transparent transfer of data between the communicating entities.

Various transport protocols may be used to meet ITS-S communication requirements, for example:

— UDP

— TCP

— FNTP; see ISO 29281-1

— BTP; see ETSI EN 102-636.

8.4 ITS-S facilities layer

8.4.1 ITS-S facilities layer details

The ITS-S facilities layer is part of the ITS-S reference architecture as illustrated in Figure 24.

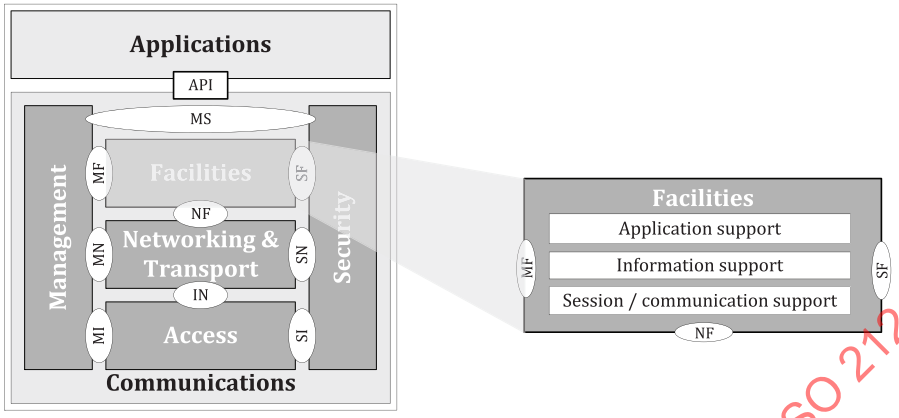

Figure 24 — ITS-S reference architecture — ITS-S facilities layer

Figure 25 shows details of the ITS-S facilities layer.

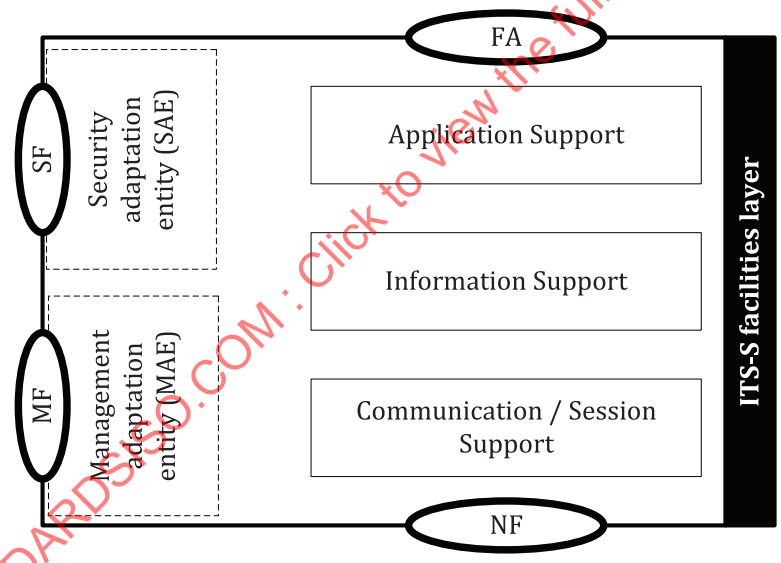

Figure 25 — Elements of the ITS-S facilities layer

The ITS-S facilities layer consists of:

— an OSI session, presentation and application layer, providing application support, information support, communication support and session support,

— the following interfaces

— MF to the ITS-S management entity; see ISO 24102-3,

— SF to the ITS-S security entity; see ISO 24102-3,

— FA to the ITS-S application entity (via an API), and

— NF to the ITS-S networking and transport layer; see ISO 29281-1 and others.

8.4.2 ITS-S facilities services

ITS-S facilities services can include the following functions that map to the OSI application layer, presentation layer and session layer:

— Support for:

  — Generic packet header and message handling; see ISO/TS 17429.

  — Data and service publication and subscription; see ISO/TS 17429.

  — Generic HMI for presentation of information to a human user of the system, e.g. to the car driver, via the HMI hardware and firmware.

  — Data presentation to encode and decode messages according to a formal language being used (e.g. ASN.1).

  — Globally unique data presentation; see ISO/TS 21184 and ISO 18750.

  — Flexible and future-proof method of message definitions by means of configuration information, see ISO/TS 21184.

  — Providing information on the geographical position (longitude, latitude, altitude) of an ITS-SU, speed and velocity, the actual time, and other parameters of the kinematic state vector of the ITS-SU; see ISO/TS 21176.

  — Location referencing and time stamping of data; see ISO/TS 21176 and ISO/TS 17429.

  — LDM (see ISO 18750 and ETSI EN 302 895) which involves a cooperative system for road safety critical applications, and involves support for combining and fusing data from different sources and keeping them up to date.

  — Maintenance of ITS-S application processes including the download and activation of new application software and the update of installed software; see ISO 17419.

  — SOA application protocols for loosely coupled, business-aligned and networked services, e.g. SOA-based web services. This facility supports applications using backend services with features such as establishing a session with the backend, handling unexpected session losses due to the mobility of an ITS-SU, and maintenance of a session during handover.

  — Processing and transfer of information between ITS stations; see ISO/TS 17429.

  — Common message distribution by ITS-S application processes residing in the ITS-S facilities layer (ITS-S facility applications).

— Event messages are triggered following the detection of some events. Rules to define dissemination coverage, repetition or cancellation of event messages depend on specific events. Examples are:

  — DENM; see ETSI EN 302 637-3,

  — TPEG-RTM; see TISA 12017,

  — SPaT message; see ISO/TS 19091,

  — MAP and ToPo messages containing digital map information of intersections; see ISO/TS 19091,

  — In-vehicle signage message; see ISO/TS 17425,

  — IVI message; see ISO/TS 19321,

  — Contextual speed message; see ISO/TS 17426,

  — PDM message,

  - PVD message,
  - SRM; see ISO/TS 19091,
  - SSM; see ISO/TS 19091,
  - Messages from the Probe Data Message set; see ISO 22837 and ISO/TS 29284).

NOTE Further standards related to probe data are ISO 16461, ISO 19414, ISO 24100, ISO/TS 25114.

- Messages to be sent periodically. Examples are:
  - CAM; see ETSI EN 302 637-2,
  - BSM; see SAE J2735,
  - SAM; see ISO 22418, e.g. POI notifications,
  - WSA message; see IEEE Std 1609.3(TM).
- Messages to manage establishment of a session. Examples are SAM and SRM; see ISO 22418.
- Repetitive transmission of messages.
- Geo-dissemination of messages, i.e. dissemination of messages to a defined geographical location rather than a physical device address or addresses.
- Relevance checking of received information.
- 5.8 GHz DSRC based services (see ISO 29281-2 and ISO 24103) to enable efficient coexistence between DSRC wireless communications (see CEN EN 12253, CEN EN 12795, and CEN EN 12834) and ITS access technologies communications (e.g. ISO 21214, ISO 21215, and ISO 21216) and by this supporting also smooth migration from DSRC communications to ITS communications.
- Selection of addressing modes at lower layers.
- Connecting to the ITS-S application entity by providing the FA Interface to the API.
- Connecting to the ITS-S networking and transport layer by using services of the NF-SAP.
- Support for dynamic selection of a communication profile in relation with the ITS-S management.
- Other functionality.

The ITS-S facilities layer supports prioritization of received data, and the configuration and management of prioritization by the ITS-S management entity through the MF-SAP.

8.5 ITS-S management entity

8.5.1 Management entity details

The ITS-S management entity is part of the ITS-S reference architecture as illustrated in Figure 26.

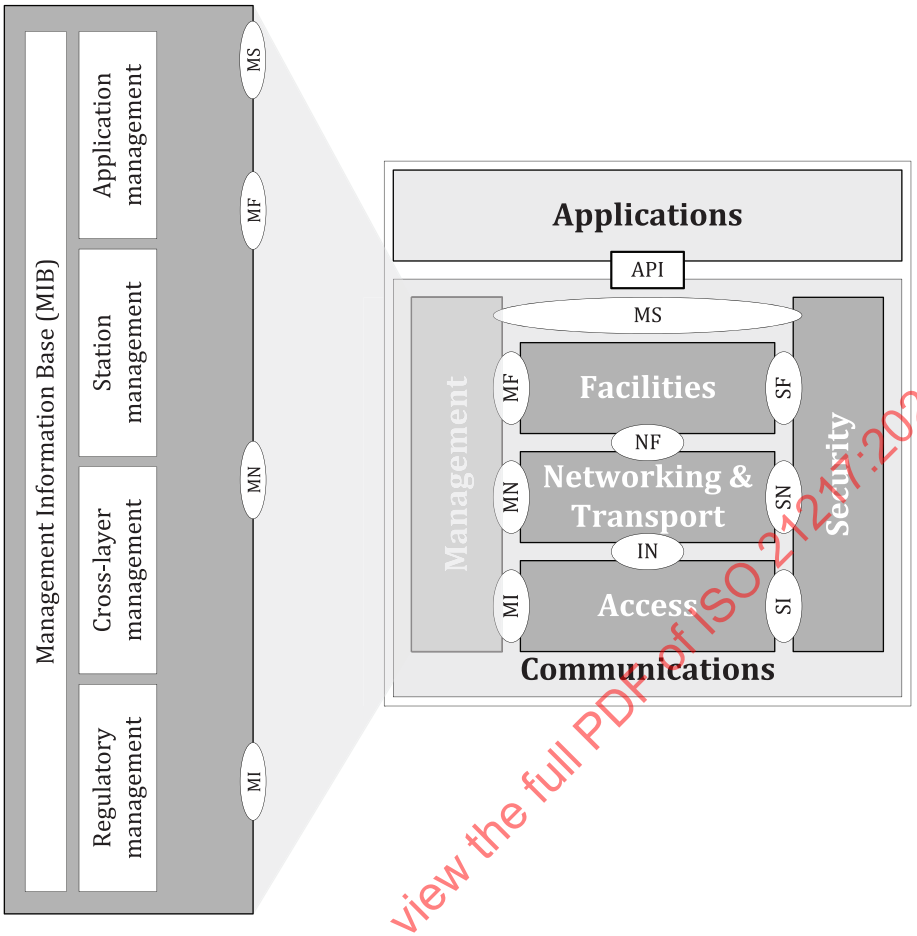

Figure 26 — ITS-S reference architecture — management entity

The ITS-S management entity consists of, for example:

— various ITS-S management applications as illustrated below,

— an MIB,

— support of ITS station-internal management communications between ITS-SCUs; see ISO 24102-4,

— the following interfaces; see ISO 24102-3:

  — MI to the ITS-S access layer,

  — MN to the ITS-S networking and transport layer,

  — MF to the ITS-S facilities layer,

  — MS to the ITS-S security entity,

  — MA to the ITS-S application entity (via API).

ITS-S management distinguishes:

— remote ITS-S management; see ISO 24102-2,

— local ITS-S management; see ISO 24102-6 and ISO 24102-1,

— management inside an ITS-SCU,

— management in a whole ITS-SU, covering several ITS-SCUs.

8.5.2 Management functionality

Management includes protocols for:

— management of RI and policies (see ISO 21218, ISO 17419, ISO 24102-1) related to, for example, radio regulation or privacy issues,

— management of capabilities of ITS-SCUs,

— management of ITS-S application processes (e.g. installation, configuration, station-internal registration specified in ISO 17423 and ISO 17419) and update of ITS-S application processes, safeguard mechanisms alleviating harmful behaviours of ITS-S application processes,

— management of service advertisement; see ISO 22418,

— communication system configuration and update management including communication profile selection and data flow and communication path management specified in ISO 17423; see ISO 24102-6, ISO 17419, ISO/TS 21185, and CEN/TS 17496,

— management of CIs and VCIs; see ISO 21218 and ISO 24102-1,

— management of channel congestion, e.g. DCC; see ETSI TS 103 175, ETSI TS 687, and ETSI TS 103 175,

— RF interference management; see ISO 24102-1,

— protection of DSRC systems; see ISO 24102-1 and ETSI TS 102 792,

— maintenance of a local node map containing information on neighbouring stations, e.g. communications parameters (e.g. MAC addresses, networking addresses), kinematic state vector of stations (e.g. position, speed and heading),

— recording and forwarding of usage billing events, particularly for third party usage of chargeable communication services accessed vehicle to vehicle communications, and holding of license agreements to confirm that an ITS-SU is authorized to use a communications service,

— fault management, e.g. to deactivate a local faulty communications system,

— monitoring of service level,

— communications system performance recording, and

— the configuration and management of prioritization functions of the ITS-S access layer, the ITS-S networking and transport layer, the ITS-S facilities layer, and the ITS-S security entity.

Management protocols are specified e.g. in ISO 21218, ISO 22418, ISO 24101-1, the ISO 24102 series, ISO 17419, ISO 17423, ETSI TS 103 110, ETSI TS 103 175.

8.6 ITS-S security entity

8.6.1 Security entity details

The ITS-S security entity is part of the ITS-S reference architecture as illustrated in Figure 27. Details of security in ITS are specified by in ETSI TS 102 731, ETSI TS 102 867, ETSI TS 102 940, ETSI TS 102 941, ETSI TS 102 942, ETSI TS 102 943, ETSI TS 103 097 and by IEEE Std. 1609.2.

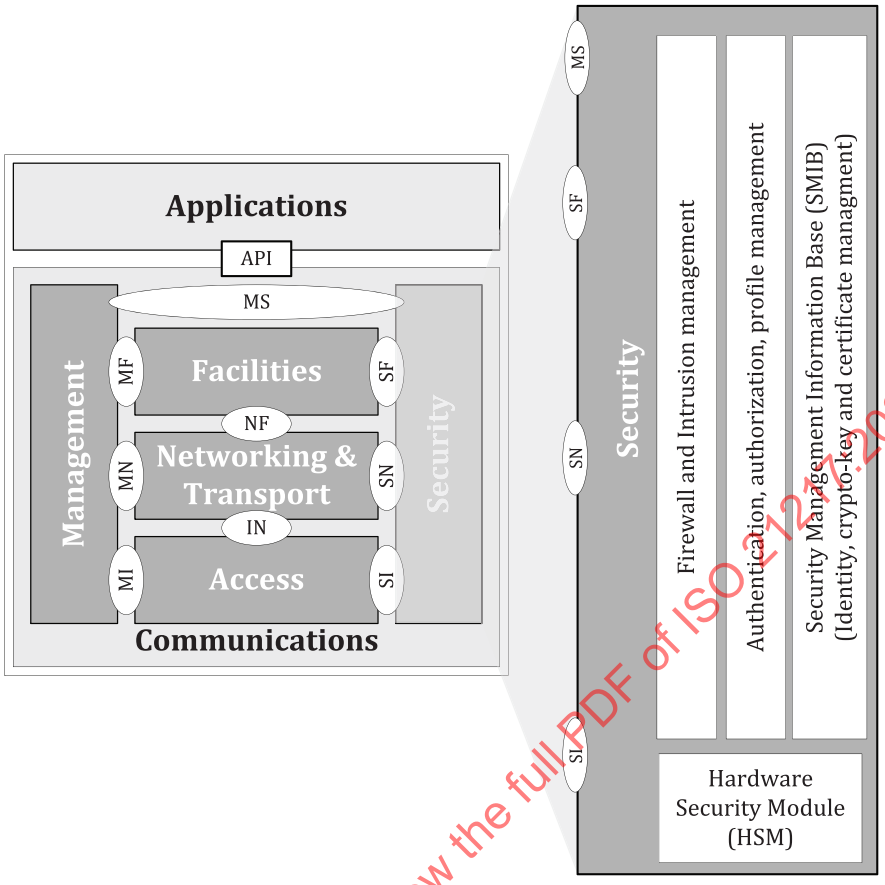

Figure 27 — ITS-S security entity as part of the ITS-S reference architecture

ITS-S security entities may consist of:

— various security and privacy functionalities,

— firewall and intrusion management,

— authentication, authorization and profile management,

— identity, crypto-key and certificate management,

— HSMs,

— functionality in support of prioritization of received messages, and the configuration and management of prioritization by the ITS-S management entity through the MS-SAP,

— an SMIB,

— the following interfaces:

  — SI to the ITS-S access layer; see ISO 24102-3,

  — SN to the ITS-S networking and transport layer; see ISO 24102-3,

  — SF to the ITS-S facilities layer; see ISO 24102-3,

  — MS to the ITS-S security entity; see ISO 24102-3,

  — SA to the ITS-S application entity (via API).

8.6.2 Functionality

The security entity provides:

— security functionality,

— communication security for:

  — information dissemination (broadcast or multicast communications);

  — sessions (unicast communications).

— system security, and

— privacy functionality.

Communications between ITS-SUs and ITS station internal management communications as specified in ISO 24102-4 may be secured at various OSI layers. End-to-end security built into the standards and specifications for applications allows usage of non-secured communication channels.

System security essentially is lifecycle management. It covers means to ensure proper secure configuration and operation of an ITS-SU.

Functionality to ensure privacy of data are provided according to regional regulation.

There can be ITS-S security application processes.

8.7 ITS-S applications

8.7.1 ITS-S applications details

ITS-S applications are part of the ITS-S reference architecture as illustrated in Figure 28.

NOTE ITS-S applications are ITS-S application processes residing in the ITS-S application entity. ITS-S application processes can also reside, for example, in the ITS-S facilities layer or in the ITS-S management entity, or in the ITS-S security entity.

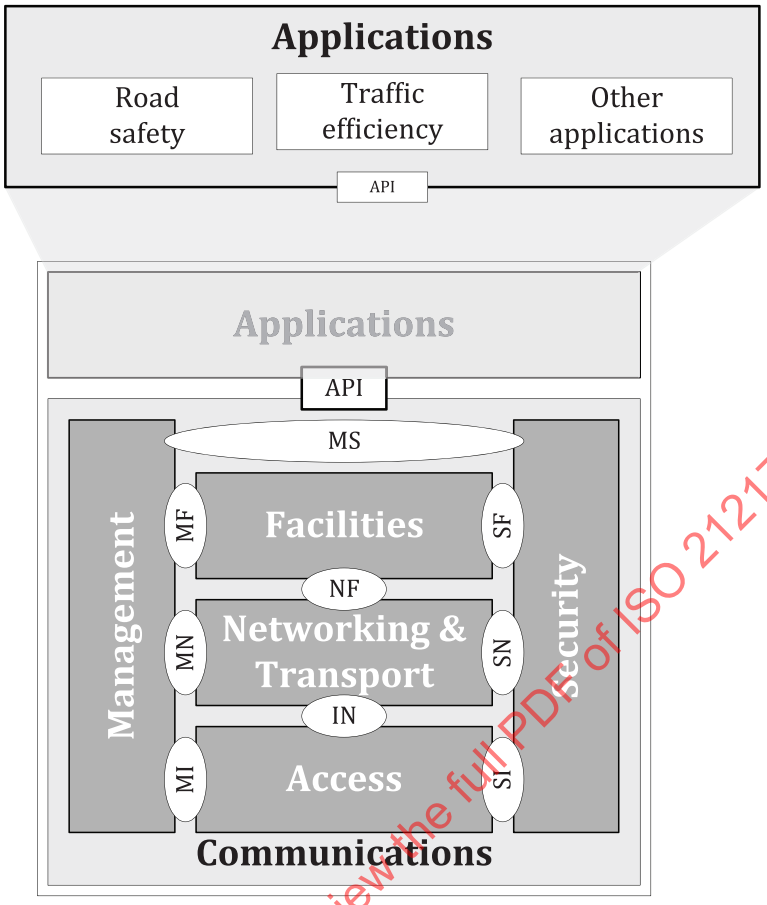

Figure 28 — ITS-S reference architecture — applications

The ITS-S applications entity consists of

— authorized ITS-S applications (see ISO 17419), e.g. for:

  — road safety; see ETSI TS 101 539-1, ETSI TS 101 539-2, ETSI TS 101 539-2, for example,

  — traffic efficiency,

  — permitted ITS-S applications; see ISO 17419,

  — an API.

All interactions of an ITS-S application with:

— the ITS-S management entity

— the ITS-S security entity, and

— the ITS-S facilities layer

go via the API. Details are defined by standards related to the ITS-S management entity, (e.g. ISO 17423 and ISO 17419), the ITS-S security entity and the ITS-S facilities layer.

Applications which are not designed to operate in a BSMD may use some restricted communication functionalities of an ITS-S via an application adaptation interface providing ITS-S gateway functionality. An example is the DSRC support specified in ISO 29281-2. A general classification of sources of messages to be transmitted using the communications tools of an ITS-SU is specified in ISO 17423.

8.7.2 ITS service

The term “ITS service” refers to a service provided by an ITS application to a user of an ITS-SU. The ITS application itself typically may consist of two or more complementary ITS-S application processes, for example:

— a message-parser ITS-S application process and an ITS-S application process in the same ITS-SU that provided the final ITS service;

— two ITS-S application processes residing in different ITS-SCUs of the same ITS-SU, or in different ITS-SUs.

Pairs of ITS-S application processes may be classified, for example, as client applications and server applications.

A client station can identify available user services in the two following ways:

1) User service discovery. A client station actively tries to discover user services.

2) User service notification. A server station is actively broadcasting SAMs to notify user services. These service advertisements are managed through various processes, including application registration and announcement requests, and construction of such announcement messages is to be transmitted over the air with an appropriately chosen access technology.

Details can depend on networking protocols used.

NOTE The term “service announcement message” is used synonymously to the term “service advertisement message”.

The FSAP specified in ISO 22418 which may use the FNTP specified in ISO 29281-1 provides service notification. Service advertisement based on the message specification of ISO/TS 16460 is also specified in IEEE Std 1609.3 and by ETSI in EN 302 890-1. Using the same ITS communication profile (see ISO/TS 21185 for globally unique identification of communication profiles) for transmission of the service announcement message, and limiting the functionality to the common denominator, the implementations conformant with any one of the three specifications (ISO/IEEE/ETSI) are interoperable. FSAP provides the full set of functionalities.

A client station receiving an announcement message may either:

— use this announcement message as an information message, in case it already contains the complete service information (e.g. traffic situation alert message),

— reply to the notification with a privately addressed frame containing service context information, upon which the server runs the service transaction in the correct context, or

— run the service transaction directly.

ITS applications are identified by a globally unique ITS-AID, specified in ISO 17419.

NOTE ITS-SUs communicate in a peer-to-peer mode where, once the application association has been made, data exchanges between applications occur until such time as the session is complete or the link between the applications is broken.

ITS-S application processes use ITS-S services in order to connect to one or more other ITS-S application processes or to other ITS-S application processes. In implementations with more than one wireless CI, quasi-simultaneous provision of ITS-S services with data streams via different CIs is supported. The term “ITS-S service” refers to a communication functionality of the ITS-S provided to ITS-S application processes. Parts of this ITS-S service are under direct control of an ITS-S application process. Other parts run autonomously without control by or feedback to the ITS-S application process.

9 Typical implementations of ITS-SUs

Four typical implementations of ITS-SUs are illustrated in Figure 29 and further described in Annex A:

— an ITS-SU installed in a vehicle, e.g. passenger car, bus, truck or motor-cycle; referred to as V-ITS-SU,

— an ITS-SU installed at the side of a road, e.g. on a gantry; referred to as R-ITS-SU,

— an ITS-SU installed in a portable (personal) device; referred to as P-ITS-SU, and

— an ITS-SU installed in a central station; referred to as C-ITS-SU, e.g. a traffic management centre.

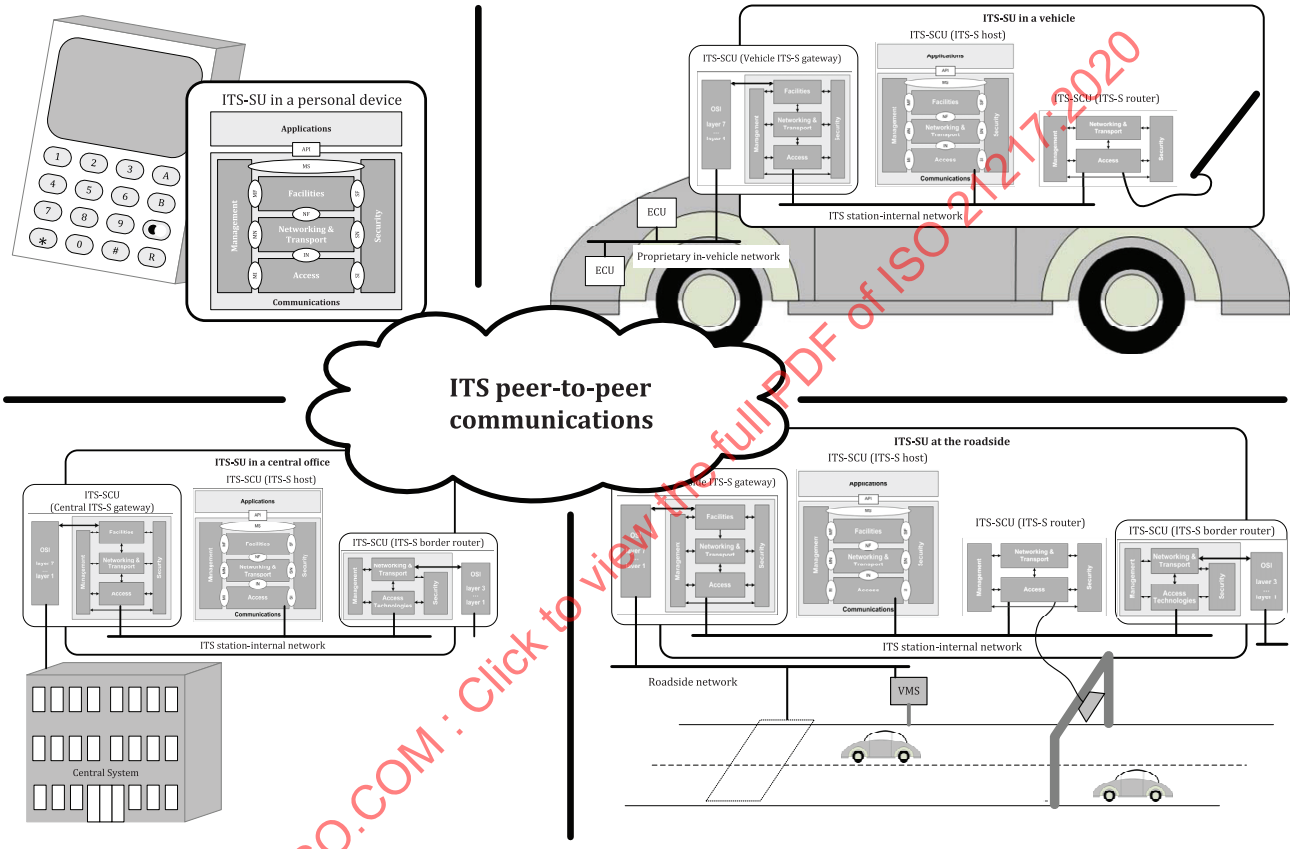

Figure 29 — Typical implementations of ITS station units

Annex A
(informative)

Illustration of typical ITS-SU implementations

Figures A.1, A.2, A.3 and A.4 in this annex illustrate the four typical ITS-SU implementations presented in Figure 29 and distinguish the split of an ITS-SU into ITS-S nodes with several roles as specified in subclause 7.2.2.

NOTE The ITS-SU implementations illustrated in this annex can have different roles (private usage, police usage, military usage etc.).

A.1 Implementation in a vehicle

The implementation presented in Figure A.1 contains an ITS-SU in a vehicle which is physically split into:

— an ITS-SCU with ITS-S host role,

— an ITS-SCU with ITS-S router role, and

— an ITS-SCU with a vehicle ITS-S gateway role.

A passenger may use a personal ITS-SU, as presented in Figure A.3, which uses an HMI and forms an integral part of the vehicle ITS-SU.

The ITS-SCU with vehicle ITS-S gateway role connects the ITS station-internal network with a proprietary in-vehicle network. The part of the vehicle ITS-S gateway which connects to the proprietary in-vehicle network is outside the scope of this document.

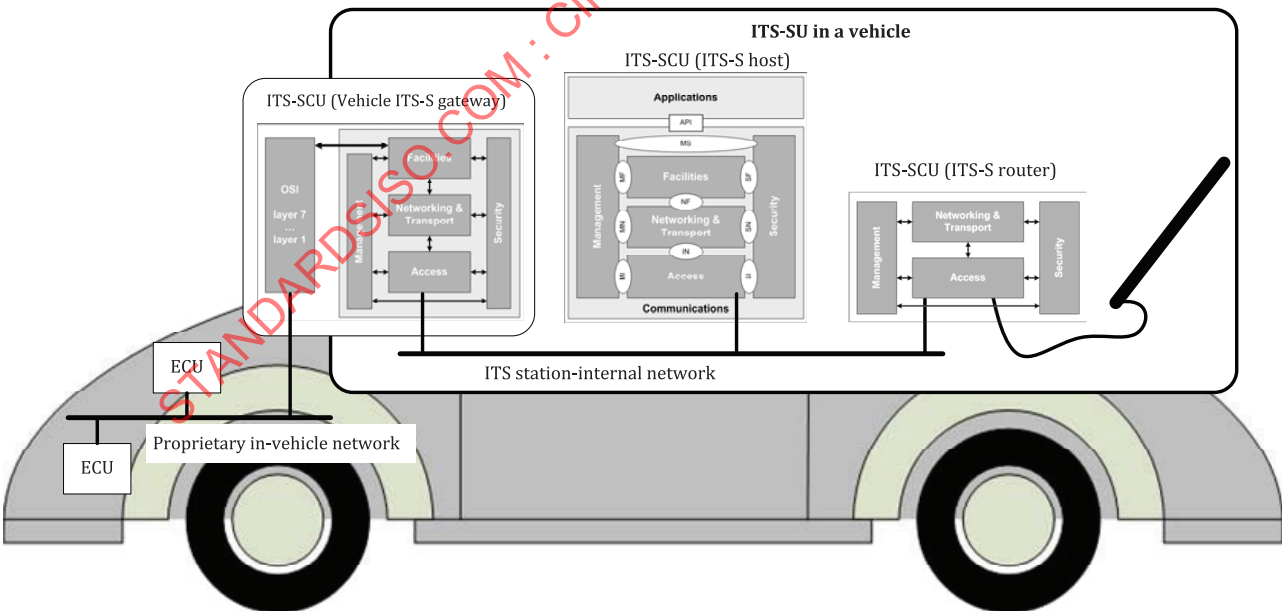

Figure A.1 — ITS-SU in a vehicle (V-ITS-SU)

NOTE The presentation in Figure A.1 does not imply a restriction to passenger cars. A vehicular ITS sub-system is also given for any other kind of vehicle, for example, trucks and buses, including motor-cycles and special vehicles, e.g. military equipment.