INTERNATIONAL STANDARD

ISO 21217

Second edition
2014-04-01

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

Systèmes intelligents de transport — Accès aux communications des services mobiles terrestres (CALM) — Architecture

Reference number
ISO 21217:2014(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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 on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 204, *Intelligent transport systems*.

This second edition cancels and replaces the first edition (ISO 21217:2010) which has been technically revised.

Introduction

"Communications Access for Land Mobile" (CALM) is the acronym used to refer to ISO TC204 WG16 work items. This acronym is used in the titles of the set of International Standards on communication for "Intelligent Transport Systems" (ITS). These International Standards focus on specifying open interfaces with regard to the functionalities required for all relevant layers and entities of the ITS station reference architecture specified in this International Standard. Note that these International Standards may also specify implementation details in situations where such specifications are deemed essential to interoperability of interface protocols.

The set of CALM International Standards is designed to allow interoperable instantiations of ITS stations which are based on the concept of abstracting applications and services from the underlying communication layers of the ITS station. This abstraction and the functionalities and services that can be easily implemented make the ITS station architecture described herein also well-suited to the development and deployment of ITS applications and services that share information amongst each other to improve the safety, sustainability and efficiency of transport systems.

The set of CALM International Standards include specifications for

— ITS station management,

— ITS communications 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.

This International Standard describes the common architectural framework around which ITS stations are instantiated and provides references to relevant International Standards, including access technology support standards, various networking and transport protocol standards, facilities standards, and ITS station management and security standards. It also describes the general architecture of peer-to-peer communications over various communication networks between ITS communication nodes. These nodes may be ITS stations as described in this International Standard or any other reachable nodes.

The set of CALM International Standards is complemented by ITS communication International Standards from other International Standards development organizations which together form the basis for implementation of ITS communications networks around the world.

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

1 Scope

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

This International standard 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, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

None.

3 Terms and definitions

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

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

3.2
application data unit
data unit exchanged between ITS-S application processes

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

3.4
communication interface
instantiation of a specific access technology 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 entity

3.7
IN interface
interface between the ITS-S access layer and the ITS-S networking and transport layer

3.8
in-vehicle network
generic term for a network in a vehicle which is not an ITS station-internal network

3.9
ITS application
instantiation of an ITS service that involves an association of two or more complementary ITS-S application processes

Note 1 to entry: Fragments of an application may also reside in nodes that are not ITS stations.

3.10
ITS message set
set of messages designed for an ITS-related purpose

3.11
ITS service
functionality provided to users of intelligent transport systems designed e.g. to increase safety, sustainability, efficiency, or comfort

3.12
ITS station
functional entity comprised of an ITS-S facilities layer, ITS-S networking and transport layer, ITS-S access layer, ITS-S management entity, ITS-S security entity, and ITS-S applications entity providing ITS services

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

3.13
ITS-S access layer
protocol layer in the ITS-S reference architecture containing the OSI physical and data link layer protocols for ITS communications

3.14
ITS-S access layer protocol data unit
protocol data unit exchanged between peer ITS-S access layers

3.15
ITS-S access layer service data unit
service data unit exchanged between ITS-S access layer and ITS-S networking and transport layer

3.16
ITS-S access router
ITS-S border router with additional functionality that provides other ITS communication nodes a point of attachment to an external network

3.17
ITS-S access technology
access technology dedicated to operation in an ITS-S

3.18
ITS-S application
ITS-S application process residing in the ITS-S application entity

3.19
ITS-S application process
element in an ITS station that performs information processing for a particular application and uses ITS-S services to transmit and receive information

3.20
ITS-S border router
ITS-S router with additional functionality that provides connectivity to other ITS communication nodes over external networks

3.21
ITS-S communication unit
physical unit in an ITS-SU containing a part or all of the functionality of an ITS-S

Note 1 to entry: In case an ITS-SU consists of a single physical unit, the ITS-SU and the ITS-SCU are identical. In case 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.

3.22
ITS-S facilities layer
layer in the ITS-S reference architecture containing OSI layers 5, 6, and 7 that connects applications to the ITS-S networking and transport layer

3.23
ITS-S facilities layer protocol data unit
protocol data unit exchanged between peer ITS-S facility layers

3.24
ITS-S facilities layer service data unit
service data unit exchanged between ITS-S facilities layer and ITS-S application entity

3.25
ITS-S facility application
ITS-S application process residing in the ITS-S facilities layer

3.26
ITS-S gateway
ITS-S node used to interconnect two different OSI protocol stacks at layers 5 through 7

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

3.27
ITS-S host
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

3.28
ITS-S internal router
ITS-S router that connects two or more ITS station-internal networks

3.29
ITS-S management application
ITS-S application process residing in the ITS-S management entity

3.30
ITS-S mobile router
ITS-S border router with additional functionality that allows a change of point of attachment to an external network while maintaining session continuity

3.31
ITS-S networking and transport layer protocol data unit
protocol data unit exchanged between peer ITS-S networking and transport layers

3.32
ITS-S networking and transport layer service data unit
service data unit exchanged between ITS-S networking and transport layer and ITS-S facilities layer

3.33
ITS-S networking and transport layer
layer in the ITS-S reference architecture containing OSI layers 3 and 4 that connects the ITS-S facilities layer to the ITS-S access layer

3.34
ITS-S node
node comprised of a set of functionalities in an ITS station unit that is connected to the ITS station-internal network or comprises an entire ITS station unit

3.35
ITS-S router
ITS-S node comprised of routing functionalities of an ITS station unit used to connect two networks and to forward packets not explicitly addressed to itself

3.36
ITS-S security application
ITS-S application process residing in the ITS-S security entity

3.37
ITS-S service
communication functionality of an ITS-S that provides the capability to connect to other nodes

3.38
ITS station unit
implementation of an ITS-S

3.39
MA interface
interface between the ITS-S management entity and ITS-S applications

3.40
medium
physical entity that supports the transmission of signals carrying information between ITS communication nodes, e.g. a set of wires supporting Ethernet signals or the space between two antennas that supports electromagnetic, optical, or acoustical transmissions

3.41
MF interface
interface between the ITS-S management entity and the ITS-S facilities layer

3.42
MI interface
interface between the ITS-S management entity and the ITS-S access layer

3.43
MN interface
interface between the ITS-S management entity and the ITS-S networking and transport layer

3.44
MS interface
interface between the ITS-S management entity and the ITS-S security entity

3.45
NF interface
interface between the ITS-S networking and transport layer and the ITS-S facilities layer

3.46
SA interface
interface between the ITS-S security entity and ITS-S applications

3.47
SF interface
interface between the ITS-S security entity and the ITS-S facilities layer

3.48
SI interface
interface between the ITS-S security entity and the ITS-S access layer

3.49
SN interface
interface between the ITS-S security entity and the ITS-S networking and transport layer

4 Symbols and abbreviated terms

ADU	Application Data Unit
API	Application Programming Interface
BSMD	Bounded Secured Managed Domain
BSME	Bounded Secured Managed Entity
CAL	Communication Adaptation Layer
CALM	Communications Access for Land Mobiles
CI	Communication Interface
C-ITS	Cooperative ITS
DSRC	Dedicated Short-Range Communication
ETSI	European Telecommunications Standards Institute
FA	name of interface between ITS-S facilities layer and ITS-S application entity
IN	name of interface between ITS-S access layer and ITS-S networking and transport layer
IP	Internet Protocol
IPv6	IP version 6
IR	Infra-Red
ISO	International Standards Organization
ITS	Intelligent Transport Systems
ITS-APDU	ITS Station Access layer Protocol Data Unit
ITS-ASDU	ITS Station Access layer Service Data Unit
ITS-FPDU	ITS Station Facility layer Protocol Data Unit
ITS-FSDU	ITS Station Facility layer Service Data Unit

ITS-NTPDU	ITS Station Networking and Transport layer Protocol Data Unit NOTE The deprecated term ITS-NPDU is in use in published standards with the same meaning as ITS-NTPDU.
ITS-NTSDU	ITS Station Networking and Transport layer Service Data Unit
ITS-S	ITS Station
ITS-SCU	ITS-S Communication Unit
ITS-SU	ITS-S Unit
IVN	In-Vehicle Network
LCH	Logical Channel
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 Channel
PDM	Probe Data Management; name of an ITS message set
PDU	Protocol Data Unit
POI	Point of Interest
PVD	Probe Vehicle Data; name of an ITS message set
SA	name of the interface between the ITS-S security entity and ITS-S applications
SAP	Service Access Point
SDU	Service Data Unit
SF	name of the interface between the ITS-S security entity and the ITS-S facilities layer
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
TOPO	name of an ITS message set used to carry information on digital maps covering the area of intersections
UMTS	Universal Mobile Telecommunication System

5 Requirements

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

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

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

This includes a minimum set of related security procedures and principles that can be verified by an appropriate ITS-related authority described in Reference [54]. These security procedures and principles are used to allow the BSME to assert a level of trust to other BSMEs in the communication network.

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.

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 e.g. application and message prioritization and logical channels.

6.2 ITS communication means

ITS communications involves communications between a wide variety of ITS communication nodes on different platforms, e.g. vehicles, roadside equipment, portable devices, control centres, using various means and methods as illustrated in Figure 1. 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. For example, any of the vehicles in Figure 1 connected to an RSE via 5 GHz or IR could communicate with the vehicle connected to the wireless LAN hotspot.

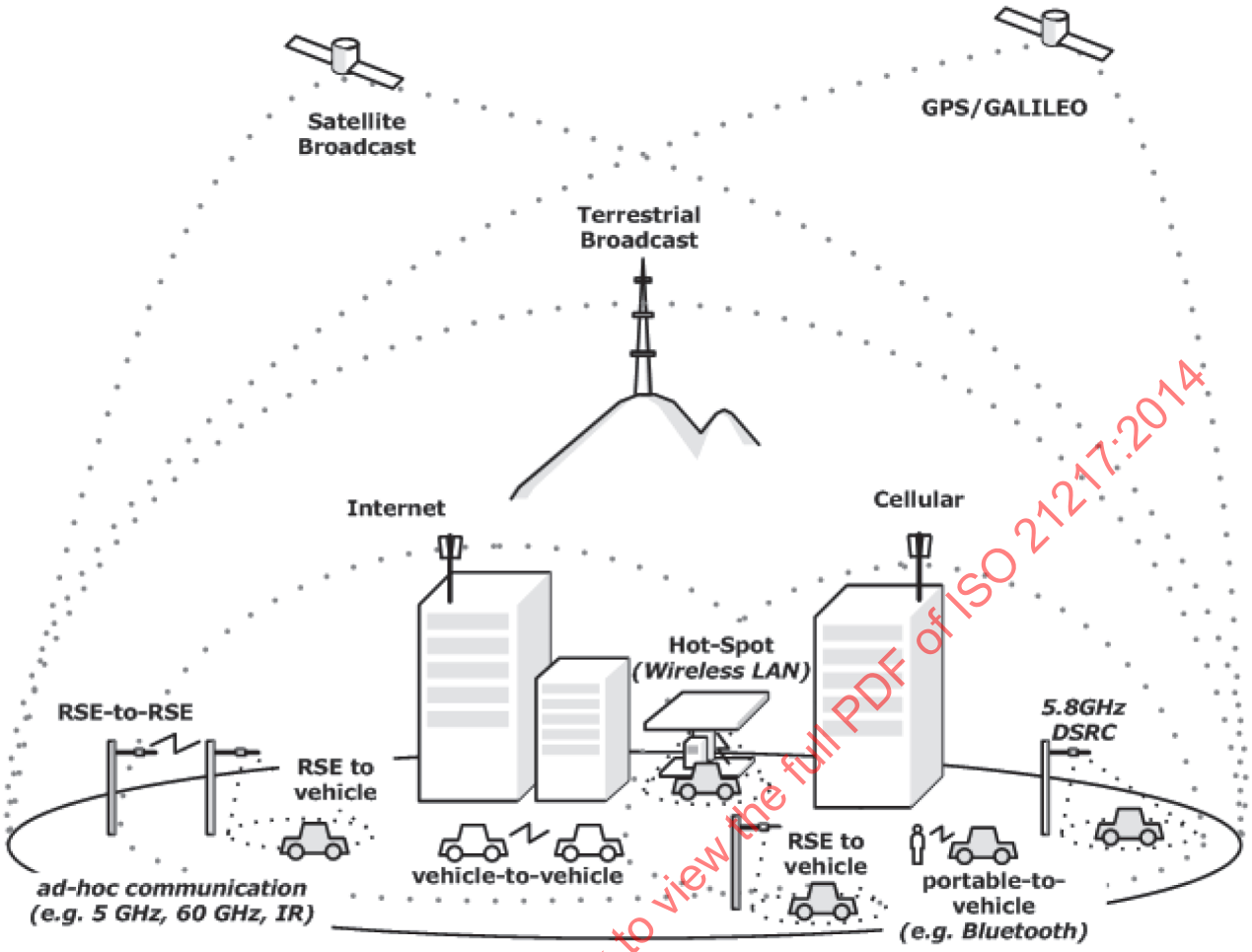

Figure 1 — Examples of ITS communications

6.3 ITS communication characteristics

Characteristics of ITS communications are presented in the following list:

— 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 WiFi, 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

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

— 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 ITS communication networks

An illustration of the various networks used in ITS communications is presented in Figure 2.

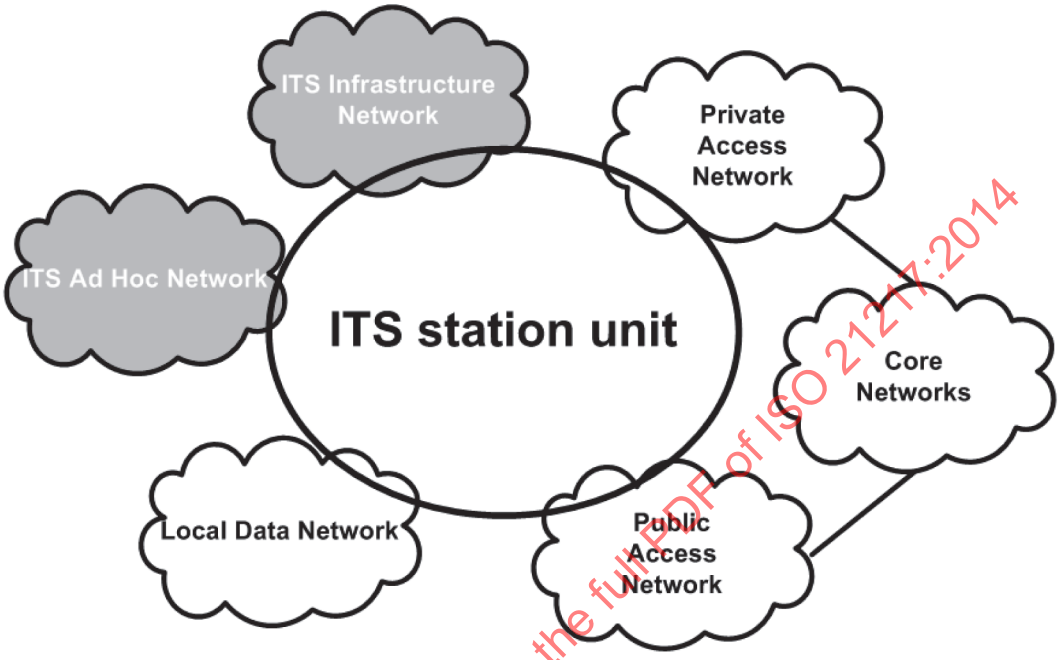

Figure 2 — Networking view of ITS communications

Figure 2 illustrates the following networks:

— 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. WiFi 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 An ITS station-internal network is not presented in Figure 2; however, it is necessary in implementations illustrated in Figures 14 and 15.

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 2. The concept of an ITS-SU is described in Clause 7.

6.5 ITS station interconnection scenarios

Four basic ITS station unit interconnection scenarios are identified as illustrated in Figures 3, 4, 5, and 6. The distinction between these scenarios is based on two criteria:

— whether ITS station units connect to peer stations with or without a network;

— 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.

Single-hop communication between two BSMEs is illustrated in Figure 3. 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 3 — BSME to BSME communication without an external network (single-hop)

Communication between two BSMEs over a network is illustrated in Figure 4. 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.

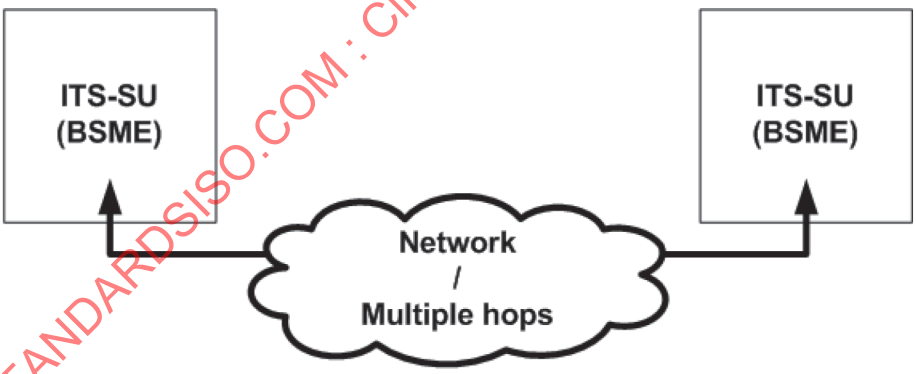

Figure 4 — BSME to BSME communication over an external network (multiple hops)

Single-hop communication between a BSME and an ITS station unit not implementing the principles of a BSMD is illustrated in Figure 5. This can represent, for example, a link between a 5,8 GHz DSRC on-board unit implemented in a vehicle BSME, as specified in Reference [43], and a 5,8 GHz DSRC roadside unit.

Figure 5 — BSME to ITS station unit (no BSME) communication without an external network (single-hop)

Communication between a BSME and an ITS station unit (no BSME) involving network connectivity is illustrated in Figure 6. 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 station unit is established.

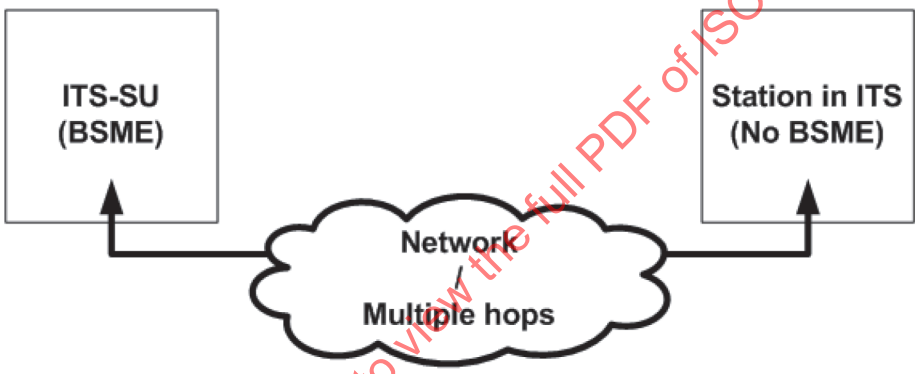

Figure 6 — BSME to ITS station unit (no BSME) communication over an external network (multiple hops)

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.

6.6 ITS concept of paths and flows

The concept of paths and flows in ITS is very beneficial in describing the abstraction of ITS-S application processes[55] from the communications services available in an ITS-S. This concept is based on similar concepts in IPv6 networking.[103] Procedures for ascertaining available communication paths and for mapping flows to those paths are divided into distinct functions within the ITS-S management as specified in Reference [35].

A **communication 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 could be multiple paths between a source and its destination.

A **flow type** is a set of communication requirements and characteristics associated with a specific flow.

A **flow** is an identifiable sequence of packets of a given flow type to be transmitted to one or more entities over a communication path. Each 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 communication 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.[55]

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

Figure 7 illustrates the architectural components (building blocks and management data flows) of the ITS-S which are involved in the path selection process. The same architecture applies to the communication profile selection process[55] introduced in 7.1.

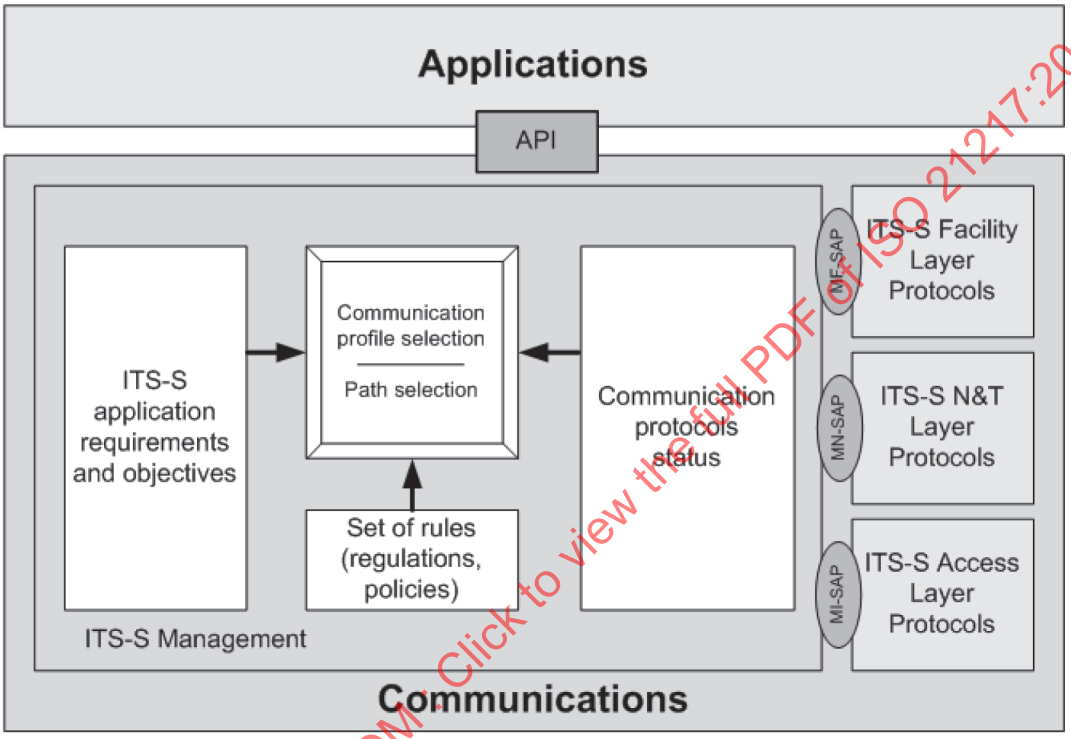

Figure 7 — Architecture of communication profile and path selection

"Communication protocols status" contains 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, and

— 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,[55] are maintained in "ITS-S application requirements and objectives".

NOTE The path selection process requires maintenance of further tables[35] not illustrated in Figure 7.

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 International Standard. 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 International Standard, 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 International standard. A general high-level description of communications in cooperative ITS is presented in Reference [14].

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[55] or specifying communication parameters on a packet-per-packet basis.[25][42][95]

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 means for (dynamically) assigning ITS-S application processes to communication media and networking and transport layer protocols is specified in References [25], [35], [54], and [55]. To exploit this flexibility, BSMD-compliant systems provide the ability to support handover of different types including

— those involving a change of "Communication Interface" (CI) (which may or may not involve a change of access technology) because ITS-SUs may have multiple communication interfaces using the same access technology,

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

— those involving both a change in communication interface and network reconfiguration.

The handover architecture is specified in Reference [8].

Finally, 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 bounded secured managed domains (BSMD).

7.2 ITS-S architecture

7.2.1 Generalized OSI model

The "ISO Open Systems Interconnect Reference Model"[47] is used in a number of figures within this International Standard with reference to the ITS-S communications architecture that embody the ITS station concept. Several levels of abstraction will be used to illustrate different points of view.

Figure 8 shows the general ITS-S reference architecture, including interfaces (IN, NF, FA, ;I, MN, MF, MA, SI, SN, SF, SA, MS, API) between the various blocks with informative details. Such interfaces may 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).

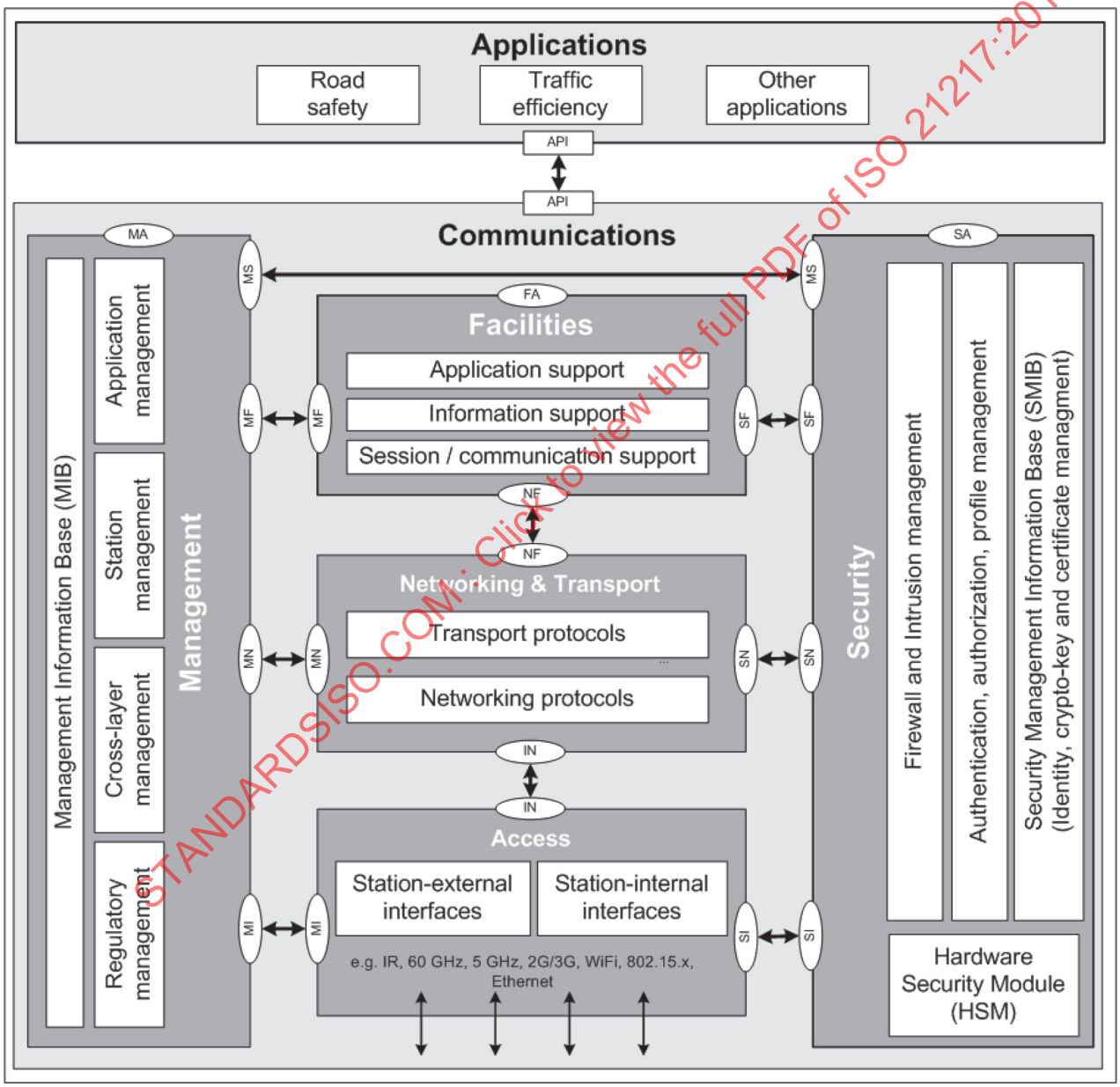

Figure 8 — ITS-S reference architecture

A simplified presentation of the ITS-S reference architecture is shown in Figure 9.

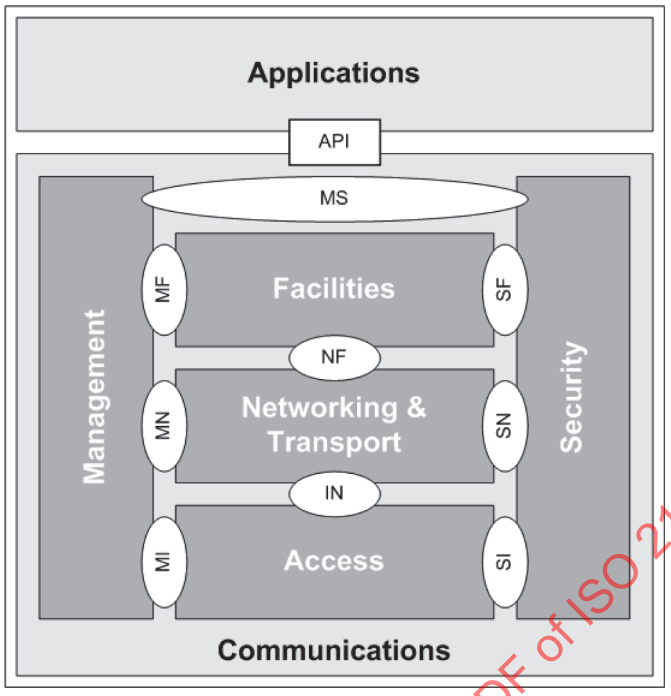

Figure 9 — Simplified ITS-S reference architecture

NOTE The interfaces MA, FA, and SA are not shown explicitly in Figure 9, as the functionality of these interfaces is provided in the API.

The blocks in Figures 8 and 9 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 8 and 9 are interconnected either via observable interfaces or via service access points (SAPs) as specified in e.g. References [25], [32], and [42] or via an API. The identifiers of these interfaces are shown in Figures 8 and 9.

Implementations of ITS stations, referred to as ITS station units (ITS-SU), 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 8 and 9 necessary for these ITS services . Some of the functionalities in the various blocks may not be applicable and therefore do not need to be implemented. For example, some ITS-S application processes might 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 International Standard.

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.

— 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 10 with the example of an ITS station-internal network and an external network B.

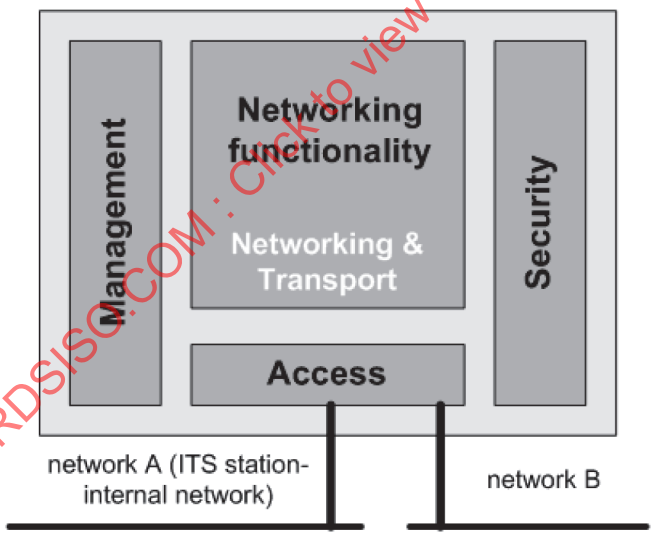

Figure 10 — ITS-S router

— 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 10).

— 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 obviously 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 11 is connected to the ITS station-internal network. The protocol stack on the left-hand side in Figure 11 is connected to an external network.

NOTE The external network may be a proprietary network, i.e. its technical specification may not be publicly available.

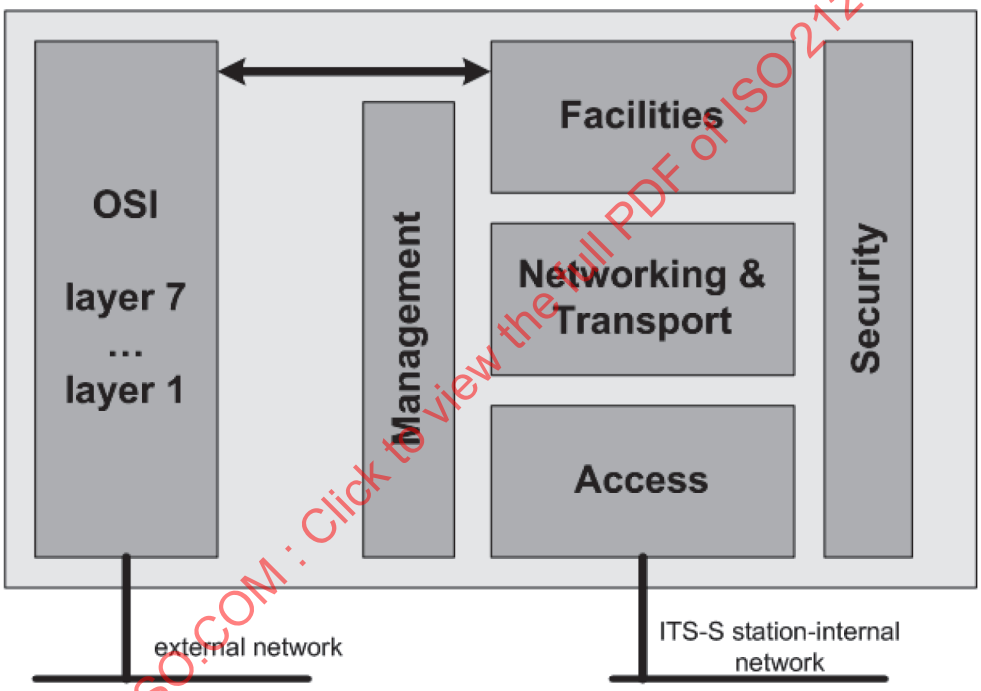

Figure 11 — Example of an ITS-S gateway at the ITS-S facilities layer

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

Figure 12 shows the data unit transfer, i.e. service data units (SDU) and protocol data units (PDU), 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 service data units (SDU) and protocol data units (PDU) follows the principles outlined in Reference [47].

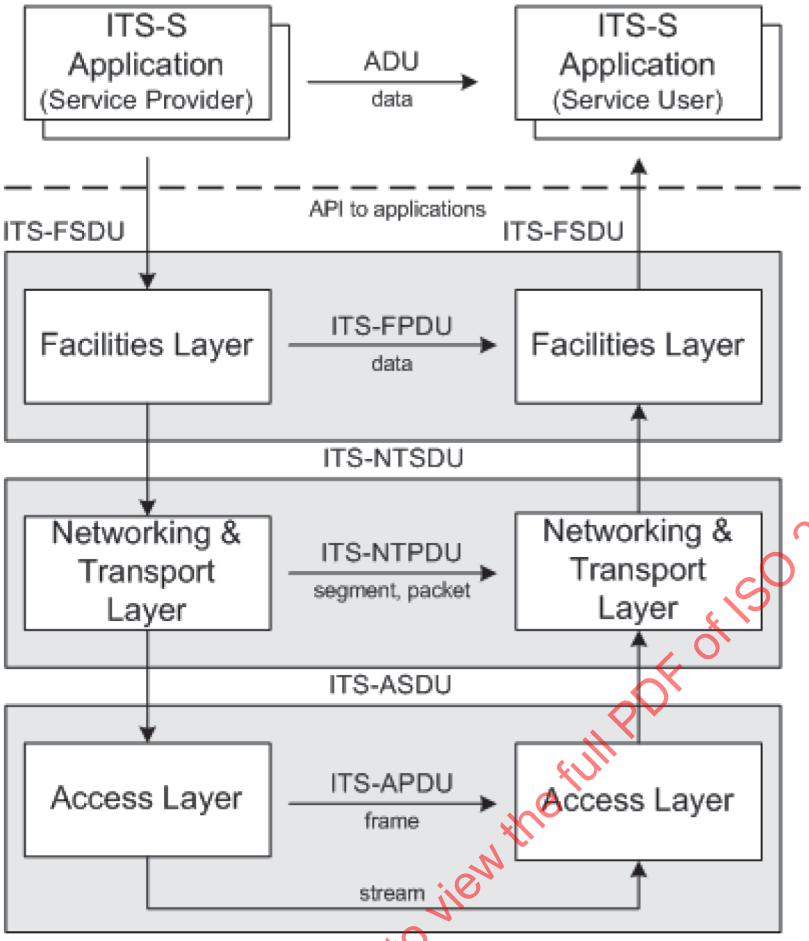

Figure 12 — OSI data unit transfer in an ITS station

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[1)]. PDUs exchanged between peer ITS-S facility layers are named ITS-FPDUs. Data units exchanged between ITS-S applications are named ADUs. Similarly, service data units are introduced for ITS communications with the names ITS-FSDU, ITS-NTSDU, and ITS-ASDU.

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 synonym 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 2. 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 e.g. an ITS-S host, an ITS-S router, an ITS-S gateway, an ITS-S border router, or a mixture of these functional elements, i.e. each ITS-SCU constitutes an ITS-S node specified in 7.2.2. Details of ITS-SCUs are specified in Reference [33].

Distributed and combined implementations of ITS-S roles are illustrated for the roles ITS-S host and ITS-S router in the following Figures 13, 14, and 15.

Figure 13 shows two ITS-SUs without ITS station-internal networks. The two ITS-SUs are interconnected via a wireless ITS link.

1) The deprecated term ITS-NPDU is in use in published standards with the same meaning as ITS-NTPDU.

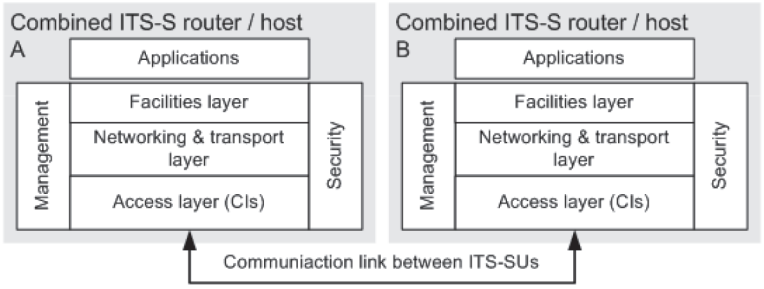

Figure 13 — Implementation architecture I

Figure 14 shows two ITS-SUs with ITS station-internal networks. The two ITS-SUs are interconnected via a wireless ITS link.

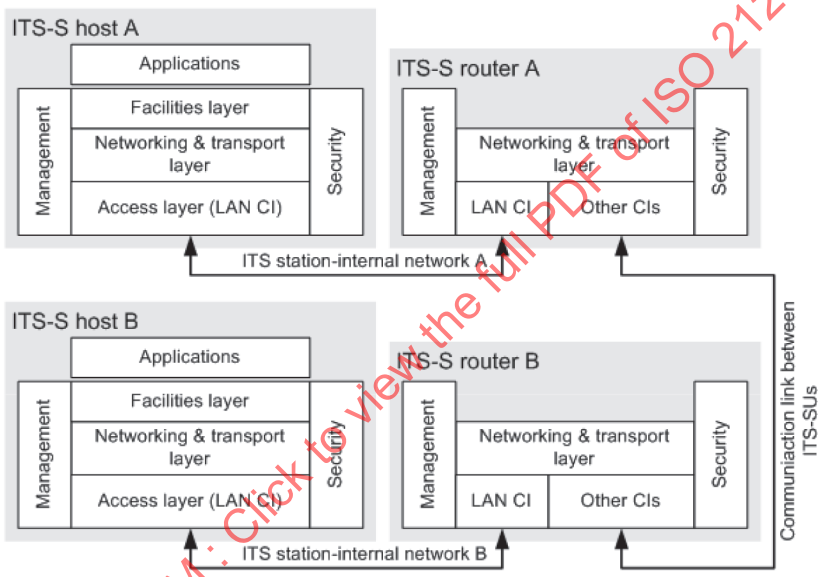

Figure 14 — Implementation architecture II

Figure 15 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.

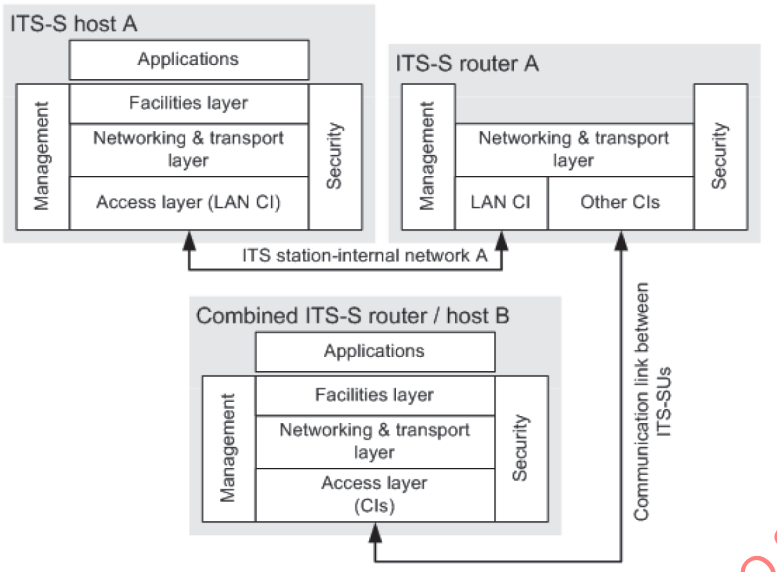

Figure 15 — Implementation architecture III

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 typically is implemented as an "Application Programming Interface" (API). All other interfaces typically are implemented as a "Service Access Point" (SAP).

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

8.1.2 ITS-S management interfaces

ITS-S management interfaces are specified in Reference [32], 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 Reference [25] and [42] and other standards 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 "Application Programming Interface" (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 16.

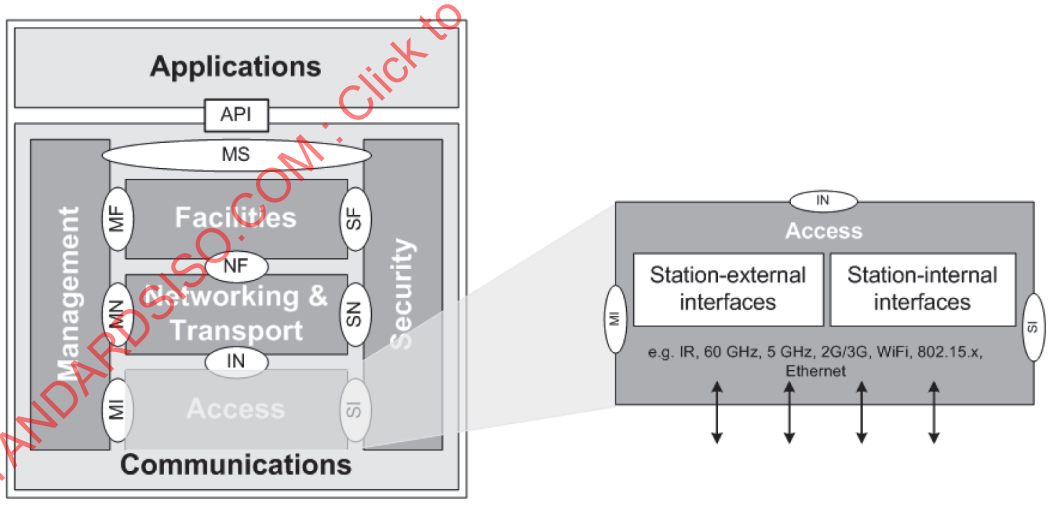

Figure 16 — ITS-S reference architecture - ITS-S access layer

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

— "Infrared light" (IR),[22]

— "Microwaves at 5 GHz, based on IEEE Std 802.11" (M5),[23] (ITS-G5),[64] (WAVE),[96] and

— "Millimeterwaves" (MM) at 60 GHz,[24]

shown in Figure 1 have been developed specifically for ITS applications and services and are specified in various ITS standards. Such access technologies are named "ITS-S access technologies".

Other access technologies shown in Figure 1 that are specified by reference to the standards according to which they operate are the following:

— Satellite networks;[3][44]

— 2G cellular systems;[20]

— 3G cellular systems (UMTS);[21]

— 4G cellular systems (LTE);[15]

— IEEE 802.16;[39]

— HC-SDMA;[40]

— IEEE 802.15.[99][100]

For these access technologies, an adaptation as specified in Reference [25] may be required 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 8).

Regionally specified DSRC systems may be supported in ITS-SUs as specified in References [36] and [43]. Services based on the DSRC standards[5][52] can be supported in the ITS environment as specified in Reference [43].

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 1, 8, and 16 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 17 shows details of the ITS-S access layer.

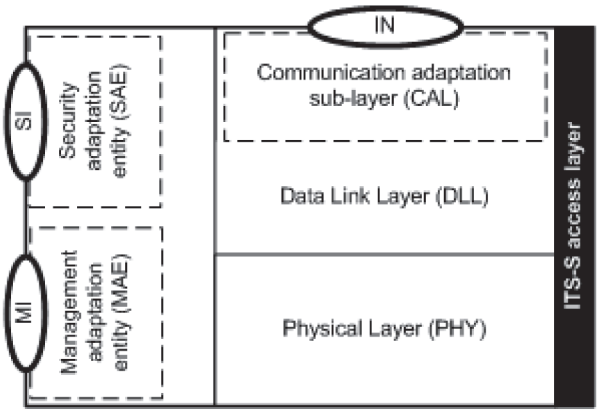

Figure 17 — Elements of the ITS-S access layer

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, and

— the following interfaces

  — MI to the ITS-S management entity,[32]

  — SI to the ITS-S security entity,[32] and

  — IN to the ITS-S networking and transport layer,[25]

as illustrated in Figure 17.

The data link layer consists of a MAC sub-layer and an LLC sub-layer, as specified in Reference [25]. 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 "Communication Adaptation Layer" (CAL) provides the IN-SAP as specified in Reference [25] for any instantiation of a data link layer. The CAL can be interpreted as an extension of an existing LLC or MAC protocol. The "Management Adaptation Entity" (MAE) provides the MI-SAP as specified in Reference [32]. Implementations of the CAL and MAE are access technology dependent.

The role of the security adaptation entity (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 communication interface (CI). The concept of a CI is specified in Reference [25]. 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 virtual communication interfaces (VCIs). Details of VCIs are specified in Reference [25].

8.2.3 Logical channels

CIs provide physical communication channels (PCHs) that are mapped to one or more logical channels (LCHs) by the station management. 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 advertisement channel (SaCH), where applications and services currently being offered are advertised by a station with service provider role;[34]

— 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.[54][55] For example, creation of a logical safety channel (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 6.6, 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

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 sublayer and the MAC sublayer, 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 sublayers 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 sublayers.

8.2.4.1 Station-internal contention

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

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 sublayer 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. Because there is no globally harmonized scheme for such prioritization, means for creating mappings between various prioritization schemes are necessary. For example, Reference [25] specifies a 256-level priority scheme in the ITS-S access layer, Reference [48] specifies an 8-level priority scheme for data transmission requests in the OSI data link layer, and Reference [97] specifies only four levels in the OSI medium access sublayer. 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 18.

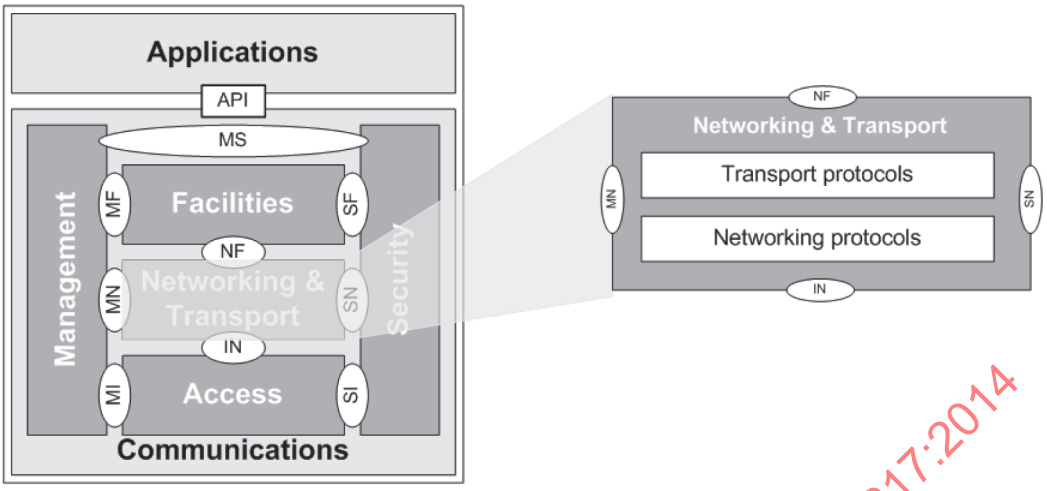

Figure 18 — ITS-S reference architecture - ITS-S networking and transport layer

Figure 19 shows details of the ITS-S networking and transport layer.

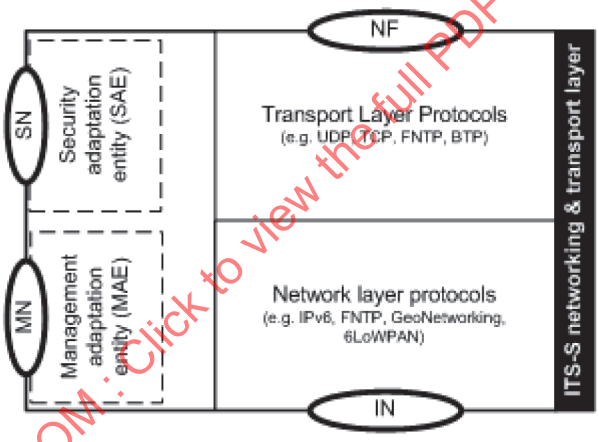

Figure 19 — Elements of the ITS-S networking and transport layer

The ITS-S networking and transport layer consists of

— an OSI network layer and an OSI transport layer,

— the adaptation elements (MAE, SAE), if necessary, e.g. an IPv6 adaptation agent,[12] and

— the following interfaces

  — MN to the ITS-S management entity,[32]

  — SN to the ITS-S security entity,[32]

  — IN to the ITS-S access layer,[25] and

  — NF to the ITS-S facilities layer,[42]

as presented in Figures 8, 18, and 19.

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 Reference [11], [12], [19], and [117].

  — To support communication with IPv4-based systems, IPv4 - IPv6 transition mechanisms can be used.

  — 6LoWPAN

— Other protocols

  — The "Fast Networking & Transport Layer Protocol" (FNTP)[42] 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 Reference [69]. 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 "WAVE Short Message Protocol" (WSMP)[95] 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 Reference [69].

  — GeoNetworking[75] uses geo-coordinates to identify target areas of possible destination stations. The basics of GeoNetworking were developed in the EU research project GeoNet.[116]

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.[75]

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, e.g.:

— "User Datagram Protocol" (UDP);

— "Transmission Control Protocol" (TCP);

— "Fast Networking & Transport Layer Protocol" (FNTP);[42]

— "Basic Transport Protocol" (BTP).[75]

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 20.

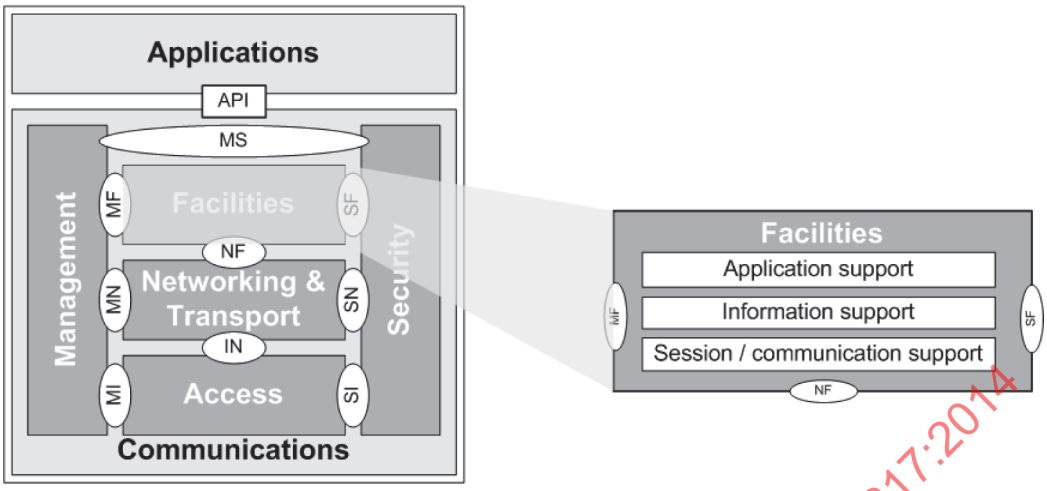

Figure 20 — ITS-S reference architecture - ITS-S facilities layer

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

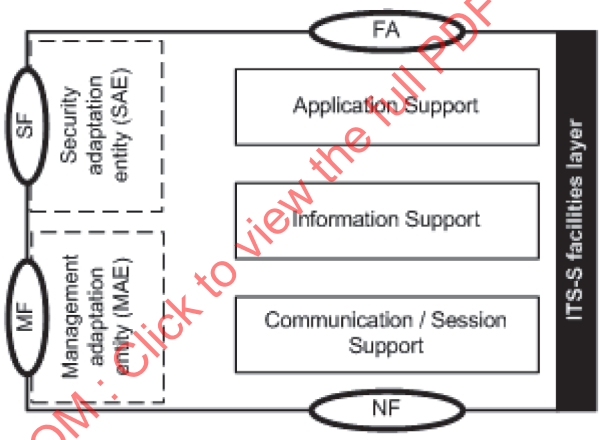

Figure 21 — Elements of the ITS-S facilities layer

The ITS-S facilities layer consists of

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

— the following interfaces

  — MF to the ITS-S management entity,[32]

  — SF to the ITS-S security entity,[32]

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

  — NF to the ITS-S networking and transport layer.[42]

8.4.2 ITS-S Facilities

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

— Support for:

  — 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).

  — Providing information on the geographical position (longitude, latitude, altitude) of an ITS-SU, and the actual time.

  — Location referencing and time stamping of data.

  — Local dynamic map (LDM)[53][56][65] 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.[54]

  — 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.[13]

  — 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 cancelation of event messages depend on specific events. Examples are

  — “Decentralized Environmental Notification Message” (DENM),[63]

  — “Transport Protocol Expert Group - Road Traffic Messages” (TPEG-RTM),[118]

  — “Signal Phase and Timing” (SPaT) message,

  — MAP and ToPo messages containing digital map information of intersections,

  — in-vehicle signage message,[57]

  — contextual speed message,[58]

  — “Probe Data Management” (PDM) message,

  — “Probe Vehicle Data” (PVD) message,

  — “Signal Request Message” (SRM),

  — “Signal Status Message” (SSM), and

  — messages from the Probe Data Message set[26][46]

— Messages to be sent periodically. Examples are

  — “Cooperative Awareness Message” (CAM),[62]

  - "Basic Safety Message" (BSM),[114]
  - "Service Advertisement Message" (SAM),[34] e.g. Point of Interest (POI) notifications,
  - "WAVE Service Advertisement" (WSA) message.[95]
- Messages to manage establishment of a session. Examples are SAM and CTX[34]
  - repetitive transmission of messages,
  - geodissemination of messages,[7] 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,[36][43] e.g. to enable efficient coexistent between DSRC wireless communciations[50][51][52] and ITS access technologies communications,[22][23][24] and by this supporting also smooth migration from DSRC communications to ITS communications, and
  - 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.
- Other functionality.

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 22.

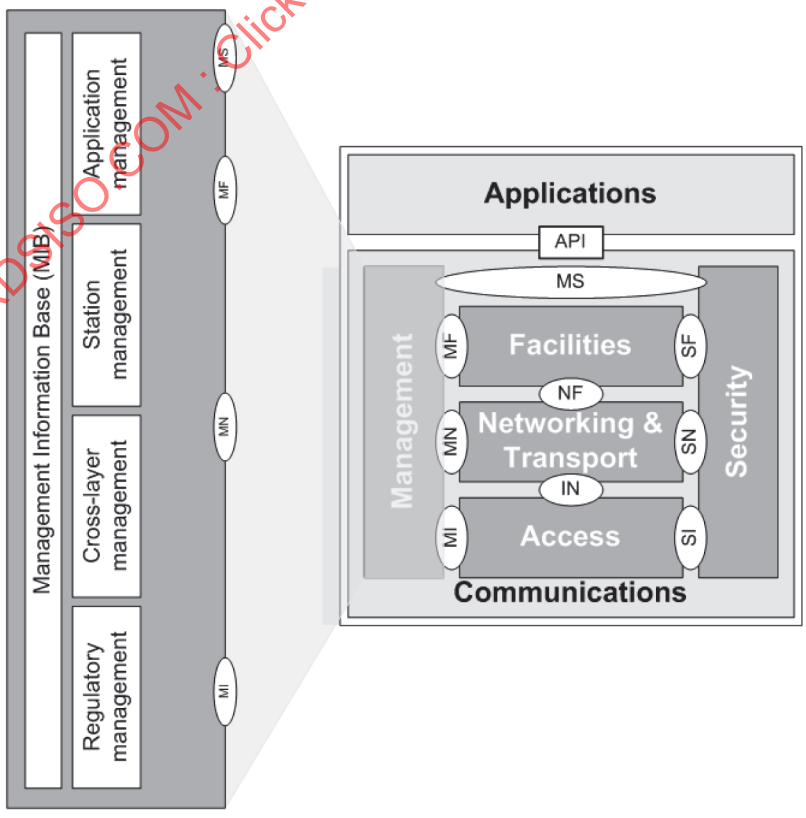

Figure 22 — ITS-S reference architecture - management entity

The ITS-S management entity consists of e.g.

— various management protocols as illustrated below,

— a “Management Information Base” (MIB),

— support of ITS station-internal management communications between ITS-SCUs,[33] and

— the following interfaces[32]

  — 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,[31] and

— local ITS-S management[30][35]

  — 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 “Regulatory Information” (RI) and policies[25][30][54] related to e.g. radio regulation, privacy issues,

— management of ITS-S application processes, e.g. installation, configuration, and station-internal registration[54][55] and update of ITS-S application processes, safeguard mechanisms alleviating harmful behaviours of ITS-S application processes,

— management of service advertisement,[34]

— communication system configuration and update management including communication profile selection and flow and path management,[35][54][55]

— management of communication interfaces (CIs) and VCIs,[25][30]

— management of channel congestion, e.g. “Distributed Congestion Control” (DCC),[92]

— “Radio Frequency” (RF) interference management,[30]

— protection of DSRC systems,[30]

— 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, and

— communications system performance recording.

Management protocols are specified e.g. in References [25], [30], [31], [32], [33], [34], [35], [54], [55], [90], and [92].

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 23.

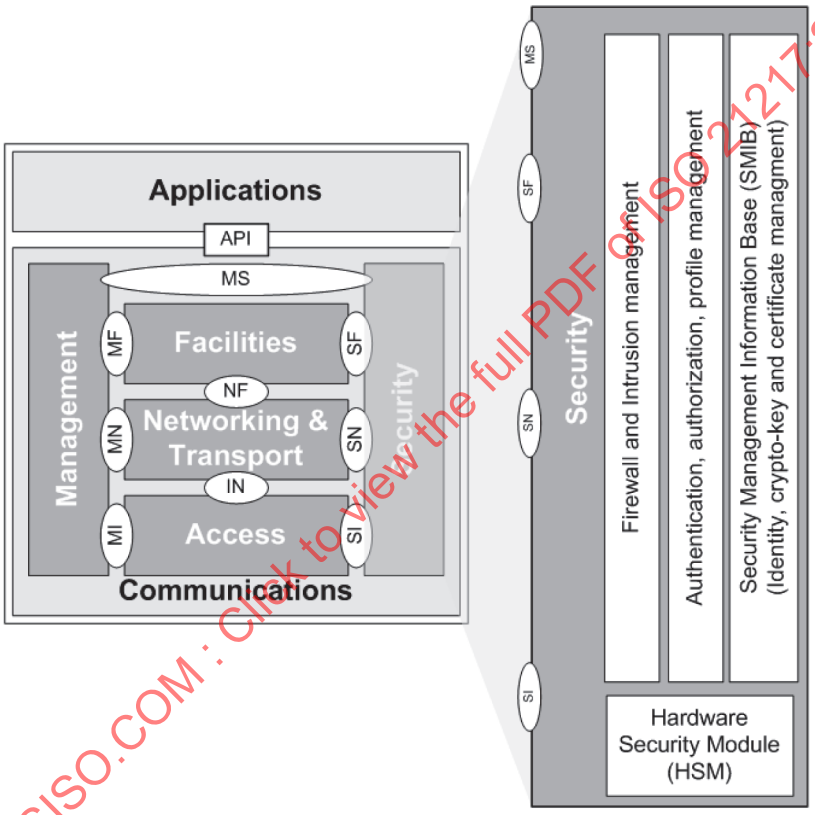

Figure 23 — ITS-S security entity as part of the ITS-S reference architecture

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,

— "Hardware Security Modules" (HSMs),

— a "Security Management Information Base" (SMIB), and

— the following interfaces

  — SI to the ITS-S access layer,[32]

— SN to the ITS-S networking and transport layer,[32]

— SF to the ITS-S facilities layer,[32]

— MS to the ITS-S security entity,[32] and

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

8.6.2 Functionality

The security entity provides

— security functionality

  — communication security and

  — system security

— and privacy functionality.

Communications between ITS-SUs, and ITS station internal management communications as specified in Reference [33], 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 may 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 24.

NOTE ITS-S applications are ITS-S application processes residing in the ITS-S application entity. Other ITS-S application processes may reside e.g. in the ITS-S facilities layer or in the ITS-S management entity, or in the ITS-S security entity.

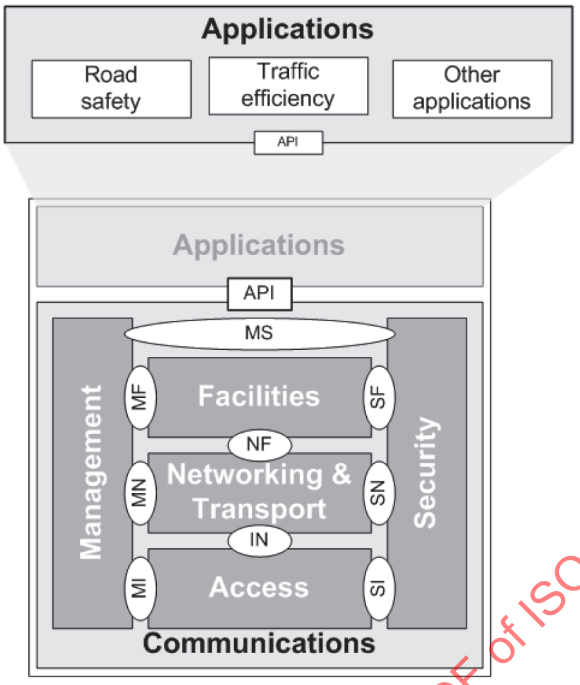

Figure 24 — ITS-S reference architecture - applications

The ITS-S applications entity consists of

— authorized ITS-S applications,[54] e.g. for

  — road safety,

  — traffic efficiency,

— permitted ITS-S applications,[54]

— an "Application Programming Interface" (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,[54][55] 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 functionality of an ITS-S via an application adaptation interface providing ITS-S gateway functionality. An example is the DSRC support specified in Reference [43] A general classification of sources of messages to be transmitted using the communications tools of an ITS-SU is specified in Reference [55].

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 may consists of two or more complementary ITS-S application processes. 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:

— User service discovery.

A client station actively tries to discover user services.

— User service notification.

A server station is actively broadcasting service advertisement messages (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 may depend on networking protocols used.

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

The "Fast Service Advertisement Protocol (FSAP) specified in Reference [34] which may use the "Fast Networking & Transport Layer Protocol" (FNTP) specified in Reference [42] provides service notification. A client station receiving an announcement message can 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 Application Identifier" (ITS-AID) specified in References [54] and [80].

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 to connect to one or more other ITS-S application processes or to other application processes. In implementations with more than one wireless communication interface, 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 station units

The four typical implementations of ITS station units that are illustrated in Figure 25 and further described in Annex A are the following:

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

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

— an ITS-SU installed in a portable device;

— an ITS-SU installed in an office, e.g. a traffic management centre.

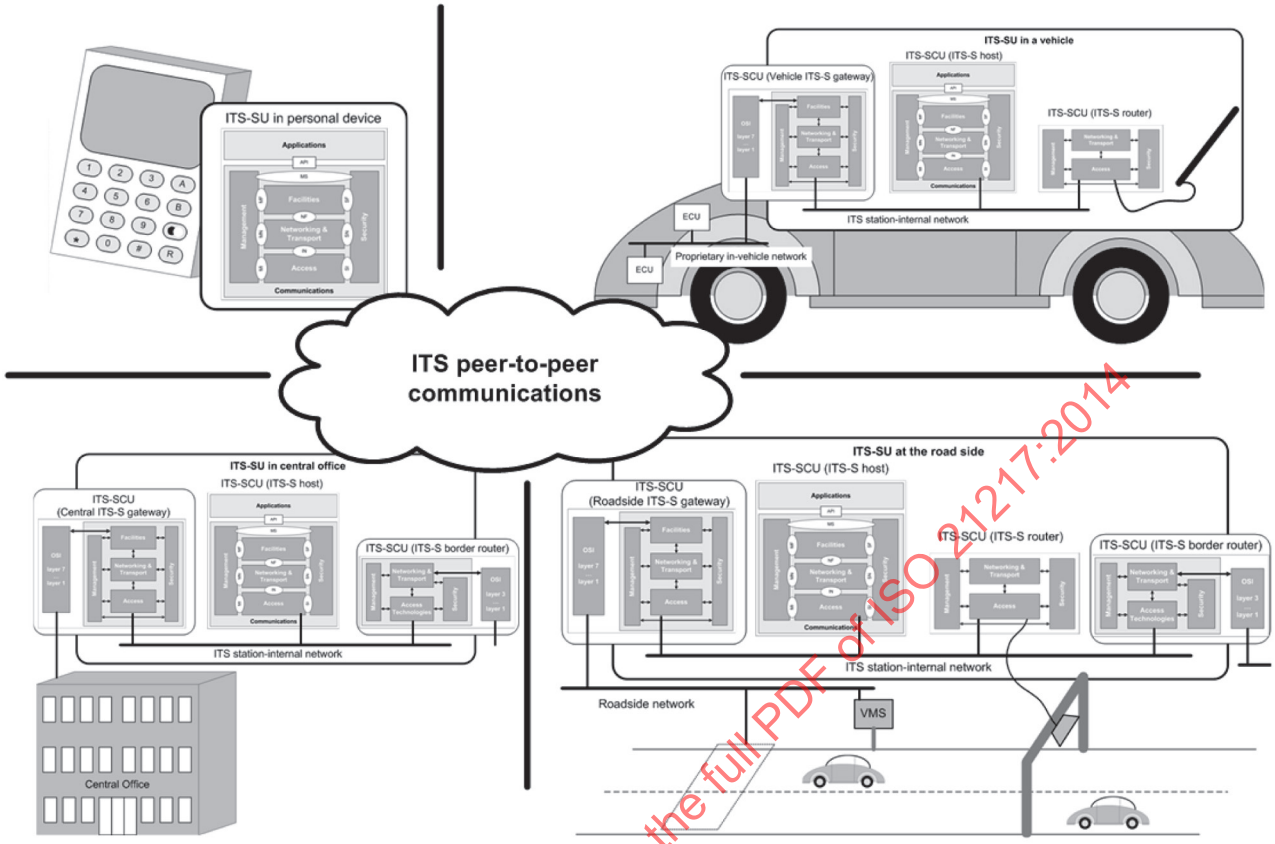

Figure 25 — Typical implementations of ITS station units

Annex A
(informative)

Illustration of typical ITS-SU implementations

Figures A.1, A.2, A.3, and A.4 illustrate the four typical ITS-SU implementations presented in Figure 25 and distinguish the split of an ITS-SU into ITS-S nodes with several roles specified in 7.2.2.

NOTE The ITS-SU implementations illustrated in this Annex may 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 International Standard.

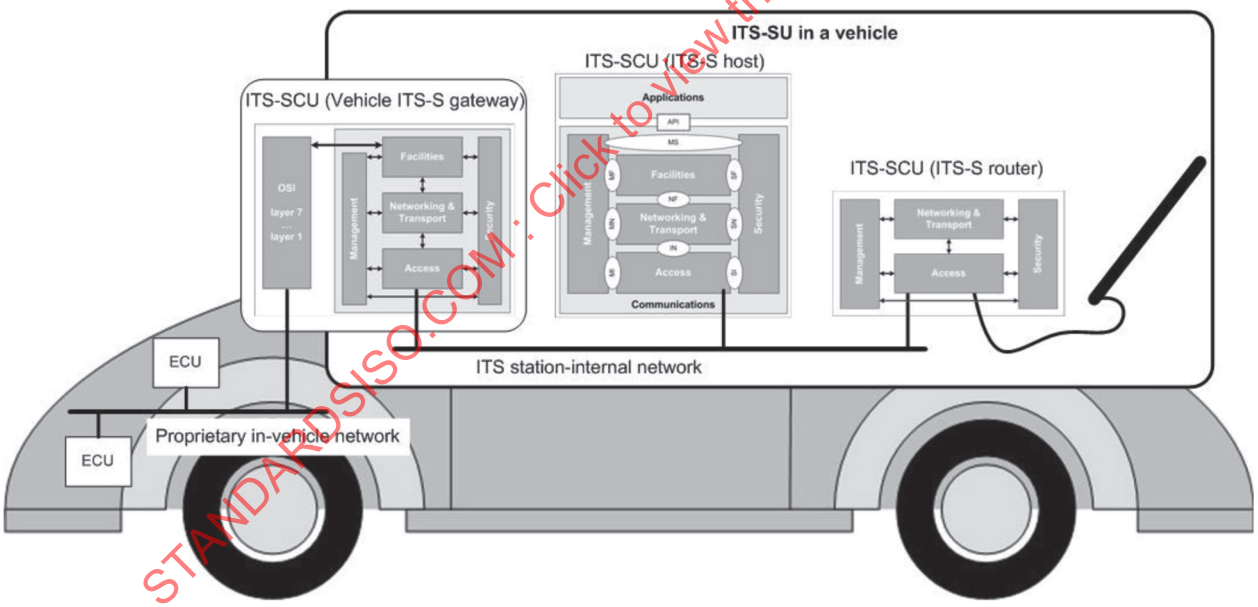

Figure A.1 — ITS-SU in a vehicle

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, e.g. trucks and buses, including motorcycles and special vehicles, e.g. military equipment.

A.2 Implementation at the road side

The implementation presented in Figure A.2 contains an ITS-SU at the road side which is physically split into an ITS-SCU with ITS-S host, an ITS-SCU with ITS-S router, an ITS-SCU with a roadside ITS-S gateway role, and an ITS-SCU with an ITS-S border router role.

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

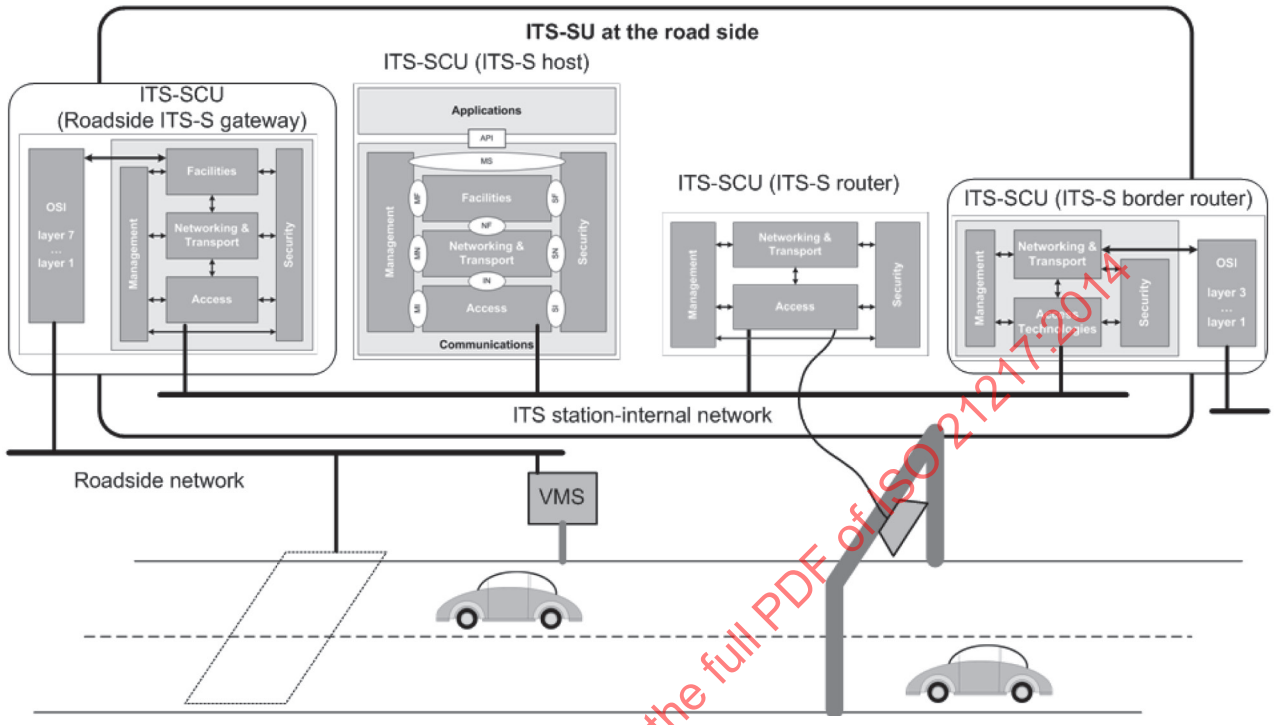

Figure A.2 — ITS-SU at the road side

A.3 Implementation in a personal device

The implementation presented in Figure A.3 provides the ITS-S functionality in consumer electronic devices such as PDAs and mobile phones. It contains a personal ITS-SU. Portable devices, e.g. PDAs, cellular phones, with ingress connectivity (provided by Bluetooth, for example), in addition to connectivity to public wireless network services, may be used as egress access technologies for ITS-SUs. Portable devices, e.g. laptops and media players, can use the vehicle as an access point for longer range connectivity. This is handled by the ITS-S router or gateway functionality and may use IPv6 protocols specified in References [11], [12], and [19].

Personal area network devices, such as those using Bluetooth,[98][99] may be used to provide local connectivity for portable devices.

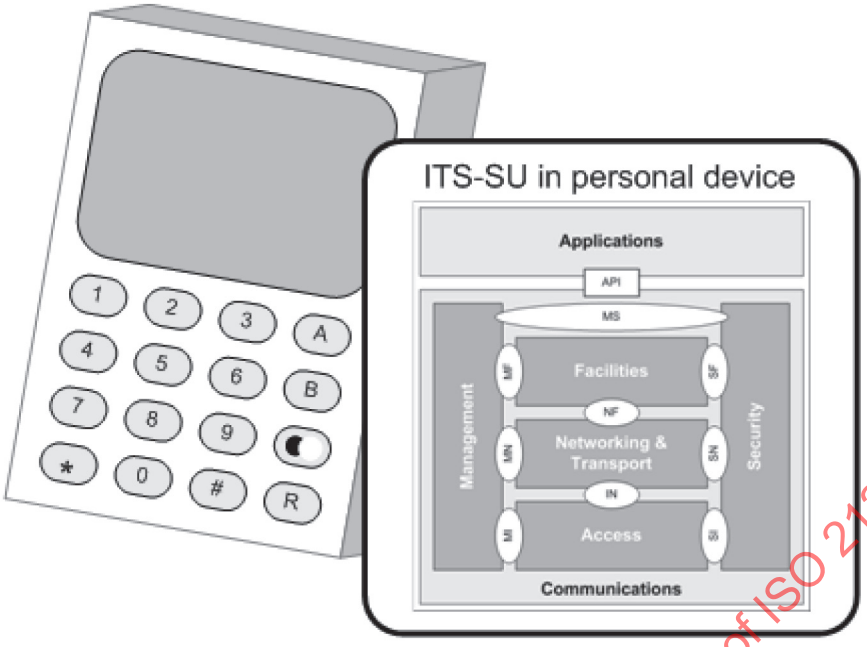

Figure A.3 — ITS-SU in a personal device

A.4 Implementation in an office

The implementation presented in Figure A.4 contains an ITS-SU in a central office which is physically split into an ITS-SCU with ITS-S host role, an ITS-SCU with a central ITS-S gateway role, and an ITS-SCU with an ITS-S border router role.

The ITS-SCU with central ITS-S gateway role connects the ITS station-internal network with a local data network presented in Figure 2. The part of the central ITS-S gateway which connects to the local data network is outside the scope of this International Standard.

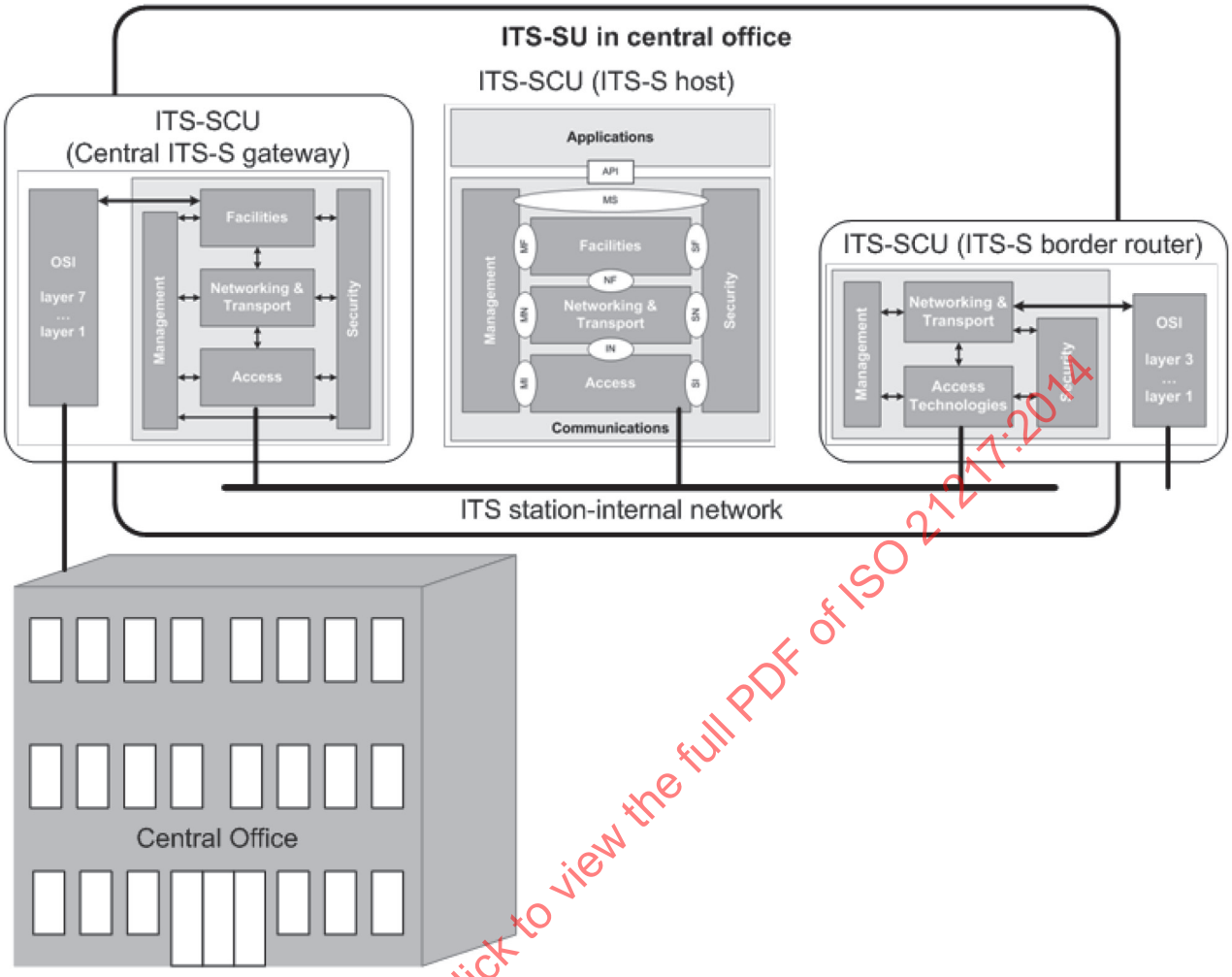

Figure A.4 — ITS-SU in an office

Annex B
(informative)

ITS-S configurations

B.1 General

This annex gives a non-exhaustive sequence of examples of differently configured implementations of ITS-SUs.

B.2 Advanced configuration in a vehicle

B.2.1 Building blocks

Figure B.1 shows an advanced ITS-S configuration in a vehicle, i.e. a simple vehicular ITS sub-system.

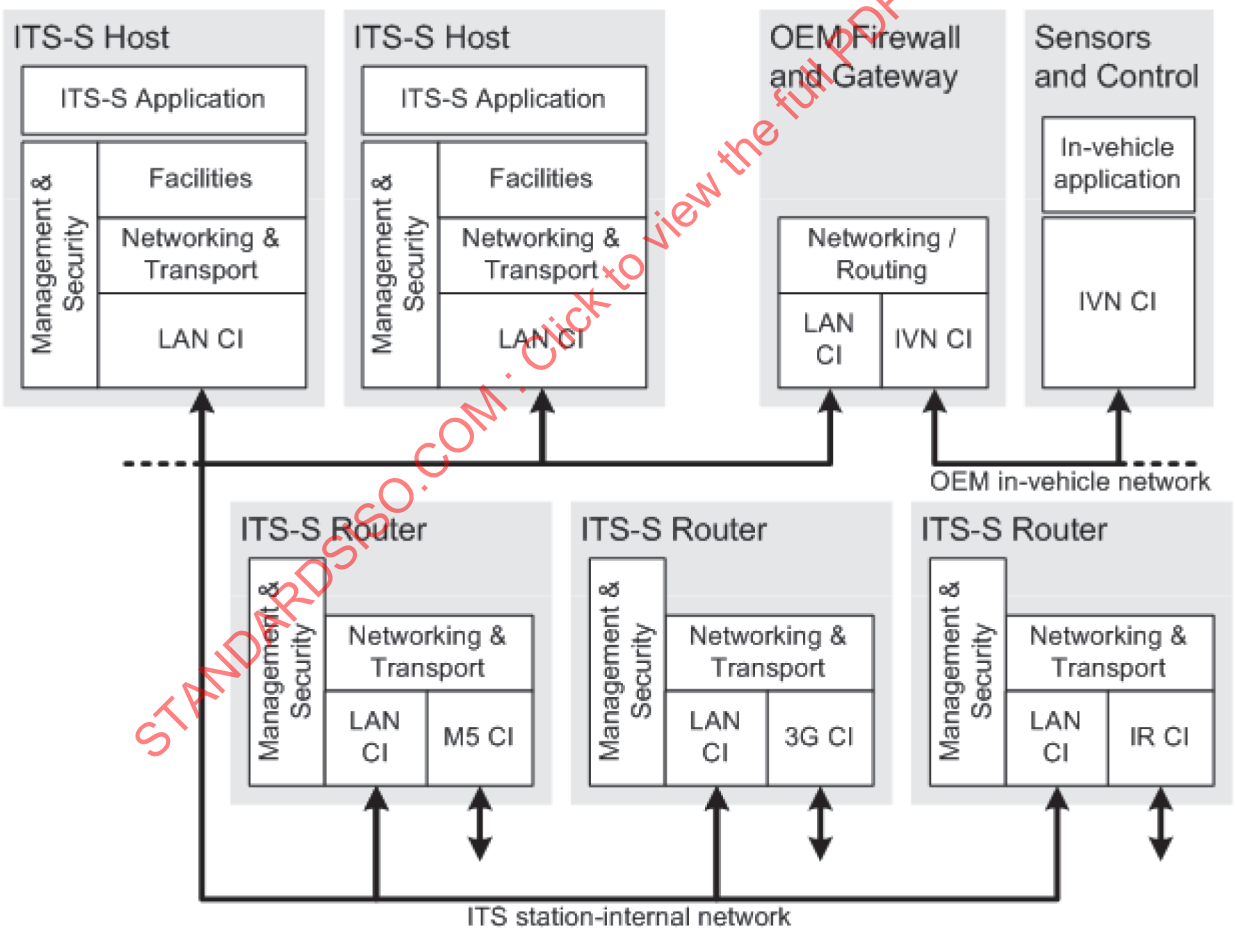

Figure B.1 — Advanced ITS-SU configuration in a vehicle