TECHNICAL REPORT

ISO/TR 17465-2

First edition
2015-08-15

Intelligent transport systems — Cooperative ITS —

Part 2:
Guidelines for standards documents

Systèmes intelligents de transport — Coopérative ITS —

Partie 2: Lignes directrices pour les documents normatifs

Contents

Page

Foreword

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

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

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

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

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information.

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

ISO/TR 17465 consists of the following parts, under the general title *Intelligent transport systems — Cooperative ITS*:

— *Part 1: Terms and definitions*

— *Part 2: Guidelines for standards documents*

— *Part 3: Release procedures for standards documents*

This includes an Annex that provides examples of the way that the guidance it contains should be applied to multi-part standards.

Introduction

As Cooperative-ITS involves many services provided using a large number of applications all communicating with each other and sharing data, it is very likely that some standards will become very large. This will be particularly true where a particular standard documents the requirements for a particular service or set of applications. It is thus likely that in some instances, multi-part standards will be required so that finding particular aspects of a standard can be made easier.

In order for users to quickly find the standard's information that they require in multi-part standards, this part of ISO/TR 17465 provides guidance on the common structure to be used for the parts in these multi-part standards. This will mean that a specific number is always used for each part, so that Architecture/Application will always be part 1, ITS-station Management will always be part 2, Security Set will always be part 3, etc. This part of ISO/TR 17465 also describes the relations between the different parts of these standards, e.g. the relationship between architectural elements and data sets.

The use by multi-part standards of the structure described in this Technical Report does not remove the obligation for those creating standards to involve other Technical Committees and/or Working Groups in the creation of a particular standard. Thus, for example, the part of the standard that describes the provisions for protection of privacy data and requirements for security of data and data transmissions should be created in explicit coordination with the CEN/ISO working group responsible for overall C-ITS Security and Privacy.

The need for the involvement of other Technical Committees and/or Working Groups will depend on the scope and contents of the multi-part standard. There might be need for this involvement to be identified in the New Work Item Proposal from which the multi-part standard is to be created and for a template to be created so that this is done in a consistent way for all multi-part standards.

This Technical Report is thus only for use with standards that relate to Cooperative-ITS. Its contents need not be applied to the ISO TC 204 and CEN TC 278 standards that do not specify information exchanges because they are not relevant to those standards (such as standards for stand-alone systems that acquire information only from sensors).

Intelligent transport systems — Cooperative ITS —

Part 2:
Guidelines for standards documents

1 Scope

This part of ISO/TR 17465 provides guidance for the structure that is to be used in multi-part ISO/CEN standards for particular services or applications to be included in Cooperative-ITS. The guidance in this part of ISO/TR 17465 may also be considered for use in multi-part standards for other ITS services and applications.

2 Terms and definitions

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

2.1
Cooperative-ITS
C-ITS
subset of overall *ITS* (2.2) that communicates and shares information between *ITS stations* (2.5) and *ITS applications* (2.3) to give advice or facilitate actions with the objective of improving safety, sustainability, efficiency, and comfort beyond the scope of stand-alone systems

Note 1 to entry: For further details and the justification of this definition, see ISO/TR 17465-1.

2.2
intelligent transport system
ITS
transport systems in which advanced information, communication, sensor and control technologies, including the internet, are applied to increase safety, sustainability, efficiency, and comfort

2.3
ITS application
instantiation of an *ITS service* (2.4) that involves an association of two or more complementary *ITS-S application processes* (2.6)

Note 1 to entry: Fragments of an application may also reside in nodes that are not *ITS stations* (2.5).

[SOURCE: ISO 21217:2014, 3.9]

2.4
ITS service
functionality provided to users of *intelligent transport systems* (2.2) designed to increase safety, sustainability, efficiency, or comfort

[SOURCE: ISO 21217:2014, 3.11]

2.5
ITS station
ITS-S
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* (2.4)

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)* (2.8).

[SOURCE: ISO 21217:2014, 3.12]

2.6
ITS-S application process
element in an *ITS station* (2.5) that performs information processing for a particular application, and uses *ITS-S service* (2.7) to transmit and receive information

[SOURCE: ISO 21217:2014, 3.19]

2.7
ITS-S service
communication functionality of an ITS-S that provides the capability to connect to other nodes

[SOURCE: ISO 21217:2014, 3.37]

2.8
ITS station unit
ITS-SU
implementation of an *ITS-S* (2.5)

[SOURCE: ISO 21217:2014, 3.38]

3   Symbols and abbreviated terms

API   application programme interface

ODP   Open Distributed Processing

OMA   Open Mobile Alliance

SDO   Standards Development Organizations

TC   Technical Committee, within a Standards Development Organization

4   Organization of multi-part Cooperative-ITS standards

4.1   Overview

It is envisaged that standards for ITS-S application processes in Cooperative-ITS will need to cover many aspects of their design and operation. This is because by its very nature, Cooperative-ITS will involve a number of actors, data from different sources, and information being sent to a variety or recipients, possibly needing to use more than one communications mechanism and a variety of interfaces. There will also be other standards relating to more generic issues such as roles and responsibilities that will be needed.

To aid the use of these standards, it will be advantageous if the standards that relate to a particular Cooperative-ITS service and/or application have a single number. Each standard would be made up of a number of parts, the number being dependent on the scope of the service and/or application. The parts

would each be a separate standards document, written using the ISO template. This type of approach is already quite common for large and complex standards in other areas of ITS, but as yet the parts do not always follow a common structure. Although this lack of a "common structure" enables a very flexible approach to be adopted for standards creation, it can actually make the task of finding the appropriate part of a standard very difficult for their users. This is because if a user is only interested in a particular aspect of a standard (e.g. interfaces, data used, architecture), all the parts have to be searched to find the one containing the aspect that is of interest. What would make the task of searching much easier is the application of a common structure for the numbering of the parts in each standard.

4.2 Structure of parts for Cooperative-ITS standards

4.2.1 Overview

The common structure of parts for the aspects that are to be included in multi-part standards for Cooperative-ITS services and/or applications is shown in Table 1.

Table 1 — Organization of the parts in a multi-part Cooperative-ITS standard

Content	Part number
Architecture/Application base standard	1
ITS station management	2
Privacy	3
Data	4
Interfaces	5
Network/protocols	6
Identifiers	7
Facilities/API's	8
Conformance testing	9
Security	10

The possible identities of the standards that relate to each part will be discussed in more detail in 4.3.

4.2.2 Use of annexes instead of parts

It should be noted that the need for separate parts will depend on the application being covered by the standard. For some applications, annexes may be created and added to part 1 (the base standard) instead of one or more of different parts shown above.

If the result of the use of annexes as just described is that none of the other parts are required, then there is no need to call the remaining single standard part 1. This means that only a single standards document will be produced.

4.2.3 Contents of part 1

The set of documents for each Cooperative-ITS standard will always have a part 1. This is the "base" standard and should provide all the basic information for the ITS application(s) that the standard covers. In addition, part 1 should also contain a short description of all the other parts in the standard. Each part will also, as a minimum, contain a table (see Table 1) so that if the user does not initially open part 1, they will realize that they are looking at a multi-part standard and can easily identify which other parts are relevant.

The following example shows the different lists of parts that would appear in part 1 of a multi-part Cooperative-ITS standard. It has been assumed that the Cooperative-ITS application to which this

particular multi-part standard relates to does not have a scope that necessitates the use of the full range of parts shown in Table 1.

<pre>
Part 1: Architecture/application base standard   this document
Part 2: ITS station management   ISO xxxxx–2
Part 3: Privacy   ISO xxxxx–3
Part 4: Data   not relevant
Part 5: Interfaces   ISO xxxxx–5
Part 6: Network/protocols   ISO xxxxx–6
Part 7: Identifiers   not relevant
Part 8: Facilities/API's   ISO xxxxx–8
Part 9: Conformance testing   ISO xxxxx–9
Part 10: Security   ISO xxxxx–10
</pre>

NOTE   The value "ISO xxxxx" represents a theoretical C-ITS standard that can be created.

4.2.4   Contents of part 2 to part 10

What needs to be defined for each of the other parts of the standard identified in Table 1 (part 2 to part 10) will be the subject of separate standards that are relevant to each part. Two examples of these standards are ITS Station Management, which will be defined in ISO 17423, and the identifier set which will be defined in ISO 17419.

The following example shows the different lists of parts that would appear in part 8 of a multi-part Cooperative-ITS standard. Again, it has been assumed that the Cooperative-ITS application to which this particular multi-part standard relates to does not have a scope that necessitates the use of the full range of parts shown in Table 1.

<pre>
Part 1: Architecture/application base standard   ISO xxxxx–1
Part 2: ITS station management   ISO xxxxx–2
Part 3: Privacy   ISO xxxxx–3
Part 4: Data   not relevant
Part 5: Interfaces   ISO xxxxx–5
Part 6: Network/protocols   ISO xxxxx–6
Part 7: Identifiers   not relevant
Part 8: Facilities/API's   this document
Part 9: Conformance testing   ISO xxxxx–9
Part 10: Security   ISO xxxxx–10
</pre>

NOTE   The value "ISO xxxxx" represents a theoretical C-ITS standard that can be created.

4.2.5   Further illustration of arrangement of parts

Three further illustrations of how the Parts in multi-part Cooperative-ITS standards would be numbered using the principles set out in Table 1 is shown in Table 2.

Table 2 — Part numbers for a set of different standards

	ISO xxxxx	ISO yyyyy	ISO zzzzz
Aspect	**Part numbers**	**Part numbers**	**Part numbers**
Architecture/application base standard	ISO xxxxx-1	ISO yyyyy-1	ISO zzzzz-1
ITS station management	ISO xxxxx–2	ISO yyyyy–2	ISO zzzzz–2
Privacy	ISO xxxxx–3	ISO yyyyy–3	not relevant
Data	not relevant	ISO yyyyy–4	not relevant
NOTE The values "ISO xxxxx", "ISO yyyyy" and "ISO zzzzz" represent theoretical C-ITS standards that may be created.			

Table 2 *(continued)*

Aspect	ISO xxxxx Part numbers	ISO yyyyy Part numbers	ISO zzzzz Part numbers
Interfaces	ISO xxxxx–5	not relevant	ISO zzzzz–5
Network/protocols	ISO xxxxx–6	not relevant	ISO zzzzz–6
Identifiers	not relevant	ISO yyyyy–7	ISO zzzzz–7
Facilities/API's	ISO xxxxx–8	not relevant	ISO zzzzz–8
Conformance testing	ISO xxxxx–9	ISO yyyyy–9	ISO zzzzz–9
Security	ISO xxxxx–10	ISO yyyyy–10	ISO zzzzz–10
NOTE The values "ISO xxxxx", "ISO yyyyy" and "ISO zzzzz" represent theoretical C-ITS standards that may be created.			

Again, it should be noted that the need for all of the separate parts shown above will depend on the application being covered by the standard. For some applications, annexes may be created and added to part 1 (the base standard) instead of one or more of different parts shown above. As noted in a previous clause, if a consequence of the use of annexes is that none of the other parts are required, then there is no need to call the remaining single standard part 1. This means that only a single standards document will be produced.

4.2.6   What if a particular part is very small?

If the content of a part happens to be very small, i.e. less than three pages, then its contents should be included as annex to part 1. This means that the contents of Table 1 and Table 2 would not reference a particular part but would point to the relevant annex in part 1, e.g. "See ISO xxxxx–1, Annex A". This will avoid the need to obtain a separate standard for less than three pages of content.

4.2.7   What happens if a particular part is not needed?

If a part is not needed because the aspect that it should cover is not relevant to a particular Cooperative-ITS application, then it should be omitted and shown as being "not relevant" in the list of parts. In this case however, the numbering of the parts would always remain the same. This means that part 8 will always be the "Facilities/API Set" in every multi-part standard for Cooperative-ITS applications even if some or all of part 3 to part 7 do not exist.

4.2.8   Need for coordination

The use of multi-part standards of the structure described in the clauses of this Technical Report, does not remove the obligation for those creating standards to involve other Technical Committees and/or Working Groups in the appropriate aspects of the creation of a particular standard. Thus, for example, part 3 and part 11 of the multi-part standard that describe the provisions for protection of privacy data and requirements for security of data and data transmissions should be created in explicit coordination with the CEN/ISO working group responsible for overall C-ITS security and privacy.

The need for the involvement of other Technical Committees and/or Working Groups will depend on the scope and contents of the application(s) for which the multi-part standard is being created. It may in fact be beneficial to identify the need for and scope of this involvement to be identified in the New Work Item Proposal that describes the need for the creation of a multi-part standard. As an aid to this, a modified version of the existing New Work Item Proposals template could be created so that the identification is done in a consistent way for all multi-part standards

4.3 Descriptions of the scope of each part of a Cooperative-ITS standard

4.3.1 Overview

In order to avoid confusion and to ensure that all the parts across all Cooperative-ITS standards are consistent in what they include, they should be based on the particular base standard that applies to the aspect that they describe. The following clauses provide descriptions of what should be the content of each part.

4.3.2 Part 1: Architecture/application

As will be expected from the definition given in ISO/TR 17465-1, Cooperative-ITS consists of a subset of the total scope of ITS services that shares necessary information across multiple ITS-S application process areas, e.g. information generated for safety purposes can be used for efficiency applications. The architecture showing the required ITS stations and the ITS-S application processes that they will host will be described in this part of the standard, together with a detailed description of the service, which, uses as its starting point, the list of ITS services provided in ISO 14813-1.

Using the ITS service description and the architecture as its starting points, this part of the standard will also provide an overall description of the functional requirements for the ITS-S application process(s) that are needed to deliver the ITS service(s). This description should be sufficient for readers to understand how the ITS-S application process(es) should work(s) and what data it(they) will need to exchange with functionality located elsewhere.

Other information about the ITS-S application process (e.g. organizational architecture and roles and responsibilities) should be included to enable the other parts (or lack of them) in the multi-part standard to make some sense. Again, this information should be based on what is available in the relevant standards, e.g. ISO 17427 for roles and responsibilities.

If particular parts are not included in a multi-part Cooperative-ITS standard, then the reasons for their exclusion should be stated in part 1. These reasons may include the fact that the required standards information is provided by another standard or that the information they could contain has been included in an annex to part 1, because it is insufficient to warrant the creation of a particular part for this standard.

4.3.3 Part 2: ITS station management

The basics of ITS communications and related management and security features based on the ITS station architecture is specified in ISO 21217:2014, 7.2.

Implementations of the ITS station architecture, i.e. ITS station units (ITS-SUs), need to be compatible and/or interoperable and operate within a common framework. ISO 21217:2014 specifies an overall architecture for ITS stations and their interactions. Other relevant standards are:

ISO 21218   complements ISO 24102–1 for management of communication interface;

ISO 24102–1   specifies local ITS station management;

ISO 24102–2   specifies remote ITS station management;

ISO 24102–3   specifies service access points in an ITS station related to station management and security issues;

ISO 24102–4   specifies ITS station-internal management communications for distributed implementations of ITS-SUs;

ISO 24102–5   specifies ITS service advertisement, especially the management of session set-up;

ISO 24102–6   specifies path and flow management, i.e. how to set up and maintain communication links;

ISO 17419   defines globally unique identifiers and addresses, related registries and functional usage of them to ensure trust and proper operation of ITS-SUs;

ISO 17423   defines ITS application requirements and objectives for communications in order to abstract ITS applications from communication tools in an ITS-SU, which complements ISO 24102–6.

This part will also need to discuss how the ITS station will need to be managed. This may need to take into account the possible need to distribute the ITS-S process applications over several physical "boxes" in its operation, or for it to be distributed across several ITS stations, e.g. collect data from multiple ITS stations in several vehicles, for each of them to transfer that data to a roadside ITS station which will fuse and extract the core data, before sending it back to (possibly different?) vehicle ITS stations and in the form of a report to a central ITS station.

4.3.4   Part 3: Privacy

Personal privacy protection will need to be protected in accordance with the local data privacy regulations applicable within any jurisdiction and must respect the international privacy regulations. Details of these can be found in ISO/TR 12859 (Privacy aspects in ITS standards and systems). Jurisdictions may impose regulations and carry out audits to protect personal privacy. Such measures are not defined within this Technical Report and will be included in another standard.

Guidance on privacy aspects and associated legislative requirements is again provided by ISO/TR 12859 and new standards for privacy are being produced. The privacy aspects that may need to be taken into consideration during the design and implementation of Cooperative-ITS applications include, determination or liability, PKI deployment, user authentication, Single Sign-On (SSO), trusted sharing of data (circle of trust), scalable trusted authenticated communication, any real-time communications constraints for V2V/V2I authentication, trusted execution, management of available resources, declaration of required resources in advance, protection against denial of service, provision of trusted policy management, use of Regime for Open Application Management (ROAM), and guaranteed secure communications with external applications.

4.3.5   Part 4: Data

Cooperative-ITS is focused around the sharing of data, which therefore means that the data used by the ITS-S application processes has to be organized consistently. One way of achieving this is by defining a Local Data Tree (LDT) which provides a uniform view of the data associated with any ITS station. For vehicles, it provides what is called "Essential Vehicle Data".

The use of a Local Data Tree enables the following:

— management of the ITS station database (discover, expand, or delete database elements) locally;

— provision of different access rights to all or parts of the data;

— ability to have different provisioning timings.

To populate a Local Data Tree, data will be required from the device that the ITS station is serving (e.g. vehicle, roadside unit, and mobile device), and the coding schema of status information generated by electronic control units and sensors is likely to be proprietary. Therefore, it will probably not be possible to harmonize this across all device manufacturers. However, it is believed that if a common set of status elements with status information of a defined type can be specified at ITS-S application process level, proprietary systems will be prepared in many cases to provide the data in that format, which will enable a device configuration independent access for safety-related and other ITS-S application processes.

The use of a Local Data Tree is not the only way of organizing the data that is used and shared by ITS-S application processes. For example, the data set can be described using ASN.1. Whatever method is selected, the reasoning behind the choice that has been made should be clearly explained in this part of the standard. This reasoning should take account of the types of devices in which the data will be used, such as vehicles, traffic signal controllers, and central systems

One way to establish a common definition of data elements is through the establishment of a Data Registry/Data Dictionary (DRDD). This is being actively pursued by both CEN and ISO, which are both requiring that a DRDD be created. It is envisaged that such a DR will not just be for data elements, but will also include definitions of terms so that these can be used and understood in a consistent manner.

Data, even where agreed and interoperable, can also appear or disappear dynamically. An example of when this can happen is when a sensor is plugged in or unplugged from the client system. The interfaces in the devices should be able to provide mechanisms to handle this dynamic behaviour.

It should also be a basic assumption that the same information will not be available in all devices of the same type, e.g. vehicle, roadside unit, and mobile device. This implies that a discovery mechanism will need to be supported in the ITS station or elsewhere in the device so that the client application can look up the available status items. The set of status elements can be accessed remotely, e.g. from a backend server by using the OMA device management specification.

The following three principle actors are involved with the workings of a Local Data Tree.

— **Local client**: a software component running on the client system that wants to access device status elements. The local client could represent a front-end component of an application service.

— **Local device information provider**: provides software components that contain information about the structure of the status element database and the mapping of the device data to this structure.

— **Remote client**: a software component running on the backend server that wants to access or manage device status elements.

Further information on the roles and responsibilities of these three actors will be found in ISO/TS 17427.

4.3.6 Part 5: Interfaces

This is where the standards for interfaces are specified or referenced for the lower layers in the OSI reference model. But it is important that any discussion about interfaces does not make any choice or express any preference about the actual medium(s) that is (are) to be used for communications between ITS stations, which in turn will dictate the interface requirements. This is being documented in ISO 21218, which includes the concept of the following two types of interface: Communication Interface and Virtual Communication Interface.

Communication Interface is a real communication equipment containing functionality of the ITS station access layer. On top of a Communication Interface, one or several Virtual Communication Interfaces for transmission to specific peer ITS stations, groups of ITS stations, or all ITS stations, and one or several receive Virtual Communication Interfaces may be created.

Further information on how these interfaces should be used is being provided in ISO 21218.

4.3.7 Part 6: Network/protocols

From a network perspective, Cooperative-ITS consists of a communications network that

— is dynamic and connects mutually reachable ITS stations,

— enables the implementation of the many services that Cooperative-ITS supports using multiple ITS-S application processes, and

— may link to traditional ITS networks, applications, and services.

This has already been illustrated and discussed in ISO/TR 17465-1.

In general and if possible, the communications means already available in the ITS station can be used. But if this is not possible, it should be remembered that IPv6 will be the basic network protocol for C-ITS, but other protocols may be needed in special circumstances, such as media dependent protocols and (possibly proprietary) protocols used in existing ITS implementations.

There are essentially two different networking approaches, i.e. using Internet Protocol IPv6 and using non-IP communications.

The basic use of IPv6 is described in ISO 21210. Other standards that will cover aspects such as networking security, optimization, multicast and IPv4-IPv6 interoperability are expected to be produced.

Non-IP communications mainly is for the purpose of very efficient single-hop communications, i.e. without real networking features:

— ISO 29281–1 specifies the "Fast Networking & Transport Layer Protocol" (FNTP), i.e. a port mapper protocol for single-hop communications with several features, e.g. N-hop broadcast, station-internal forwarding of packets, tunnelling of IP packets, support of DSRC technologies (e.g. ISO 15628);

— ISO 29281–2 specifies usage of FNTP to support ISO 15628 DSRC technologies.

4.3.8 Part 7: Identifiers

Proper and trusted operation of ITS station units (ITS-SUs) requires globally unique identifiers and addresses (ITS-S object identifiers) which are both internal and external to ITS-SUs.

ISO/TS 17419 identifies and specifies ITS-S object identifiers and describes how these are used for classification, registration, and management of ITS applications and for communications in ITS. The following are some important examples of such identifiers.

ITS-AID "ITS application identifier" identifying globally unique ITS application which provides ITS service by executing one or several complementary ITS-S application processes.

ITS-MsgSetID "ITS message set identifier" identifying globally unique ITS message set.

ITS-SCUID "ITS station communication unit identifier" identifying globally unique physical unit which contains either a part of or a complete ITS-SU.

ITS-PN "ITS port number" and ITS-S networking and transport layer address identifying an end-point of communications, e.g. in the ITS-S facilities layer or the ITS-S management entity.

ITS-LCHID "ITS logical channel identifier" allowing automatic selection of communication profiles by the ITS station management based on functional requirements set up by ITS-S application processes for each flow type as specified in ISO/TS 17423.

Automatic selection of communication profiles by the ITS station management based on functional requirements set up by ITS-S application processes for each flow type is specified in ISO/TS 17423. The following are set of requirements that distinguish mandatory requirements (examples listed below in bold) and optional requirements:

— operational requirements (logical channel);

— destination requirements (destination type, destination domain);

— performance requirements (maximum APDU size);

— security requirements;

— protocol requirements.

4.3.9 Part 8: Facilities/API's

In a connected world, the most effective business case for a vehicle subsystem is one where a single ITS station platform can support simultaneously a number of ITS-S application processes, some of which may be standalone and others cooperative. The means by which this is achieved is commonly referred to as a "facilities" layer, which manages how ITS-S application processes are loaded, operated, and

managed and how data are stored and accessed, together with the security required. In the wider world of Cooperative-ITS and particularly for safety related services, these aspects need to be clearly specified.

In order to provide Cooperative-ITS functionality in an open environment, specifying the architecture, selecting communications, and standardizing the ITS station is not enough. ITS-S application processes need to be loaded and run on-board the devices in which the ITS stations are located. These ITS stations should work in cooperation with each other and/or with other systems on-board the devices in which they are located. This requires a "facilities" layer which provides an open access, yet secure runtime environment for Cooperative-ITS-S application processes, on top of whatever else needs to be run.

This part should include a sufficiently detailed description so that the communication requirements of the application can be understood. The understanding should be sufficient for the communications provider(s) to be able to define the required communications profile(s) in order for the application to both send and receive the data it needs to exchange. Equally, the description of the API should recognize the profiles that are currently available for use by the application.

4.3.10 Part 9: Conformance testing

In order to ensure interoperability, conformance testing is a crucial component of Cooperative ITS. They should be written in combination with writing the functional requirements for the required ITS-S application processes. Standards exist that describe how to write these test standards that are available from SDO's such as ETSI, which also provides a test platform that implements test suites related to C-ITS (not restricted to base standards from ETSI).

This does not remove the need for a clause to be included in each part that defines what has to be done to conform to what is in the part.

4.3.11 Part 10: Security

Security is a crucial element of most ITS applications and particularly for Cooperative-ITS in the ITS-S application processes which are expected to exchange and reuse data and information. This can be largely with parties with whom the owner and/or operator of the sending or receiving ITS-S application process has no direct contractual relationship. Security is important both at the overall system level and in the management of the ITS station that is part of the in-vehicle subsystem which has specific security and privacy requirements for ITS-S application process and data pantry management.

The focus of security should be on the requirements as viewed from the ITS-S application process perspective. This includes the five basic data security requirements listed below that are often listed in discussions on this subject.

— **Data authenticity**: it is process needed to ensure that the data, transactions, communications, or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim to be.

— **Data availability**: for an ITS station to service its purpose, the information it provides should be available when it is needed. This means that the ITS station, the security controls used to protect it, and the communication channels used to access it should be functioning correctly. Those ITS stations that are classed as needing "high availability" should aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

— **Data confidentiality**: in its general form, this refers to preventing the disclosure of information to unauthorized individuals or systems. For ITS stations, mechanisms will be needed to apply confidentiality by encrypting data during transmission, by limiting the places where data might appear (in databases, log files, backups, printed records, and so on), and by restricting access to the places where the data is stored. If an unauthorized party obtains the data processed by an ITS station in any way, a breach of confidentiality has occurred. Confidentiality is necessary (but not sufficient) for maintaining the privacy of the travellers whose personal information an ITS station holds.