TECHNICAL SPECIFICATION

ISO/TS 18750

First edition
2015-05-15

Intelligent transport systems — Cooperative systems — Definition of a global concept for Local Dynamic Maps

Systèmes intelligents de transport — Systèmes coopératifs — Définition d'un concept global pour cartes dynamiques locales

Reference number
ISO/TS 18750:2015(E)

Contents

Page

Foreword

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

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

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

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

For an explanation 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.

ISO/TS 18750 was prepared by the European Committee for Standardization (CEN) in collaboration with ISO/TC 204, *Intelligent transport systems*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

Introduction

An essential property of cooperative intelligent transport systems (C-ITS)[16] is the sharing of data between different ITS applications providing different ITS services to the users. This approach replaces the traditional approach where each application is operated in an isolated environment, i.e. referred to as "silo approach". The C-ITS approach enables synergies in components of an ITS station unit, e.g. sharing of communication tools, improves overall performance and reliability, and reduces overall cost. In order to protect the interests of the various ITS applications, C-ITS implements the concept of an ITS station (ITS-S) operated as bounded secured managed domain.

The sharing of data between applications is achieved by subscribe/publish mechanisms, where at least two mechanisms are distinguished, i.e. one allowing ITS-S application processes to subscribe to standardized messages from ITS message sets (direct forwarding upon reception of such messages in an ITS station unit) and one using a Local Dynamic Map (LDM) as repository of standardized data objects. Such data objects stored in an LDM are named LDM Data Objects (LDM-DOs). LDM-DOs provide self-consistent information on real objects existing at a given geo-location during a given lifetime-interval. Authorized ITS-S application processes may add LDM-DOs to an LDM and may retrieve LDM-DOs from an LDM. Retrieval of LDM-DOs may be performed in queries and by means of subscription. A subscription will result in automatic notifications of selected LDM-DOs either in defined time intervals or event driven.

This Technical Specification introduces the usage of LDMs and specifies the LDM for global usage in C-ITS.

Initial implementations of LDMs were in the EU research projects CVIS[32] and Safespot[34].

Intelligent transport systems — Cooperative systems — Definition of a global concept for Local Dynamic Maps

1 Scope

This Technical Specification

- describes the functionality of a “Local Dynamic Map” (LDM) in the context of the “Bounded Secured Managed Domain” (BSMD), and
- specifies
  - general characteristics of LDM Data Objects (LDM-DOs) that may be stored in an LDM, i.e. information on real objects such as vehicles, road works sections, slow traffic sections, special weather condition sections, etc. which are as a minimum requirement location-referenced and time-referenced,
  - service access point functions providing interfaces in an ITS station (ITS-S) to access an LDM for
    - secure add, update, and delete access for ITS-S application processes,
    - secure read access (query) for ITS-S application processes,
    - secure notifications (upon subscription) to ITS-S application processes, and
    - management access,
      - secure registration, de-registration, and revocation of ITS-S application processes at LDM, and
      - secure subscription and cancellation of subscriptions of ITS-S application processes,
  - procedures in an LDM considering
    - means to maintain the content and integrity of the data store, and
  - mechanisms supporting several LDMs in a single ITS station unit.

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.

ISO 21217, *Intelligent transport systems — Communications access for land mobiles (CALM) — Architecture*

ISO/IEC 8824-1:2008, *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation — Part 1*

ISO/IEC 8825-2:2008, *Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER) — Part 2*

ISO 24102-3, *Intelligent transport systems — Communications access for land mobiles (CALM) — ITS station management — Part 3: Service access points*

3 Terms and definitions

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

3.1
data integrity
property that data has not been altered or destroyed in an unauthorized manner

[SOURCE: ISO 24534-5]

3.2
International Atomic Time
time since 00:00:00 UTC, 1 January, 2004, identical with UTC except that no leap seconds need to be added

3.3
LDM area of interest
location requirement used in the filter process of queries and automatic notifications

3.4
LDM area of maintenance
information on the operational location area of an LDM used by LDM maintenance

Note 1 to entry: Reference [22] restricts the LDM Area of Maintenance to "geographical area specified by the LDM for LDM maintenance"

3.5
LDM permissions
information on how a specific ITS-S application process may use an LDM

3.6
LDM data object
location-referenced and time-referenced representation of a real object that is self-explanatory without any further context information

3.7
LDM data object ID
identifier of an LDM data object which is unique in an LDM

3.8
LDM data dictionary
dictionary of LDM data object types

3.9
LDM data object type
identifier of the type of information contained in an LDM data record

3.10
location validity
information indicating a location at which an LDM data object is valid

3.11
time validity
information indicating a time interval during which an LDM data object is valid

3.12
LDM time of interest
time requirement used in the filter process of queries and automatic notifications

3.13
Local Dynamic Map
entity consisting of LDM data objects, services, and interfaces for manipulating these LDM data objects

3.14
location reference
uniquely identifiable description of position or area in the real world

3.15
metadata
data about data

Note 1 to entry: The term "metadata" is ambiguous as it is used for fundamentally different concepts. Structural metadata are information related to the design and specification of data structures; it is also referred to as "data about the containers of data". Descriptive metadata are information on instances of data, i.e. the data content; it is also referred to as "data about data content".

[SOURCE: ISO 19115]

3.16
time of creation
time when an LDM data record was created and updated

3.17
time of deletion
time when an LDM data record may be deleted and will no more be considered by the LDM search functionality

3.18
time of generation
time when the content of the LDM data object information field was created

Note 1 to entry: This is different to the time when the LDM data object was written into an LDM.

4 Symbols and abbreviated terms

BSMD	Bounded Secured Managed Domain
BSME	Bounded Secured Managed Entity
IAT	International Atomic Time
ICS	Implementation Conformance Statement
ITS	Intelligent Transport Systems
ITS-SU	ITS Station Unit
IUT	Implementation Under Test
LDM	Local Dynamic Map
LDM-DD	LDM Data Dictionary
LDM-DT	LDM Data Type
LDM-DAT	LDM Data Attribute Type
LDM-DATID	LDM-DAT Identifier
LDM-DTID	LDM-DT Identifier
NoO	Notification of Obligations
OoT	Obligation of Trust

PMI	Privilege Management Infrastructure
SAO	Signed Acceptance of Obligations
SUT	System Under Test
TPEG	Transport Protocol Experts Group
UTC	Universal Time Coordinated

5 Architectural environment

5.1 General

This Clause contains informative descriptions of the architectural environment of an LDM.

5.2 Local Dynamic Map

A Local Dynamic Map (LDM) is an entity consisting of LDM Data Objects (LDM-DO), services, and interfaces for manipulating these LDM Data Objects. LDM-DOs are distinguished by means of their LDM Data object Type (LDM-DT). LDM-DTs are specified by registration in an LDM Data Dictionary (LDM-DD). The concept of the LDM-DD is specified in Annex B.

NOTE In Reference [17], LDM-DOs are classified into Type 1 (static permanent data objects, e.g. cartographic data[5]), Type 2 (static transitory data objects, e.g. temporary parking lot on the road[5]), Type 3 (dynamic transitory data objects, e.g. works location), and Type 4 (highly dynamic data objects, e.g. location, orientation, and speed of surrounding vehicles). This classification is not used in this Technical Specification.

An LDM-DO provides information on real objects (cars, road events, etc.) that are existent at a defined location, e.g. in a defined geo-area and within a defined time interval. In the uppermost simple case, the information provided by an LDM-DO is just its type, its geo-location, and its time interval of validity. Such information may be received in an ITS station unit via different channels such as

— DATEX II, TPEG, RDS-TMC (legacy systems),[30][26] and

— CEN/ETSI/ISO/SAE ITS message sets,[22][21]

composed of different sets of attributes, and presented in different formats (encodings). ITS-S application processes capable to receive this information perform a mapping on LDM-DOs and a translation of attribute formats into the common format given by the LDM-DTs.

5.3 LDM in an ITS-S

The Local Dynamic Map (LDM) specification provided in this Technical Specification is designed for the architectural environment of an ITS station operated as a Bounded Secured Managed Domain (BSMD) specified in ISO 21217 and illustrated in Figure 1.

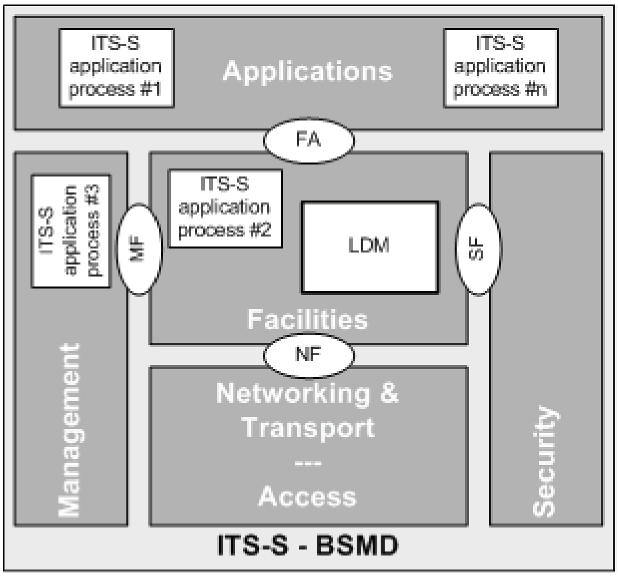

Figure 1 — LDM in an ITS-S operated as a Bounded Secured Managed Domain (BSMD)

The LDM functionality specified in Clause 6 is located in the ITS-S facilities layer. An LDM interfaces with ITS-S application processes specified in ISO 21217. The interface functionality is specified in 6.6.2 by means of functions of services of the FA-SAP and the MF-SAP; both service access points (SAPs) offer identical functions for this purpose. The generic services of FA-SAP and MF-SAP are specified in ISO 24102-3.

5.4 LDM in an ITS-SU

Various examples of supported implementation configurations are illustrated in Figure 2, Figure 3, Figure 4, and Figure 5.

Figure 2 illustrates a “single-box” configuration of an ITS station unit (ITS-SU) with a single LDM.

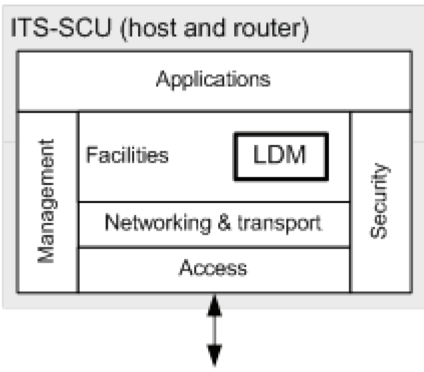

Figure 2 — Implementation configuration example a)

Figure 3 illustrates a “single-box” configuration of an ITS-SU with two LDMs.

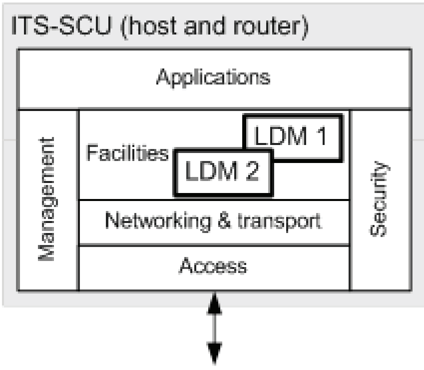

Figure 3 — Implementation configuration example b)

Figure 4 illustrates a configuration of an ITS-SU with two ITS station communication units (ITS-SCU). One of these ITS-SCUs has a host-only role specified in ISO 21217 and contains a single LDM. The other ITS-SCU has a router-only role specified in ISO 21217 and does not contain an LDM.

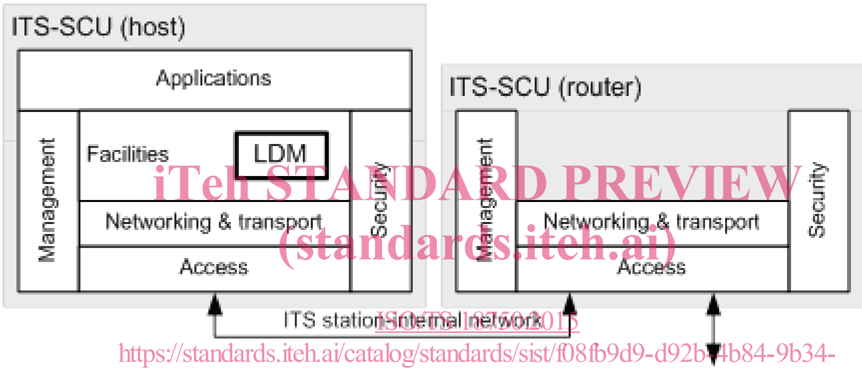

Figure 4 — Implementation configuration example c)

Figure 5 illustrates a configuration of an ITS-SU with two ITS station communication units (ITS-SCU). One of these ITS-SCUs has a host-only role specified in ISO 21217 and contains a single LDM. The other ITS-SCU has a host-and-router role specified in ISO 21217 and contains also an LDM.

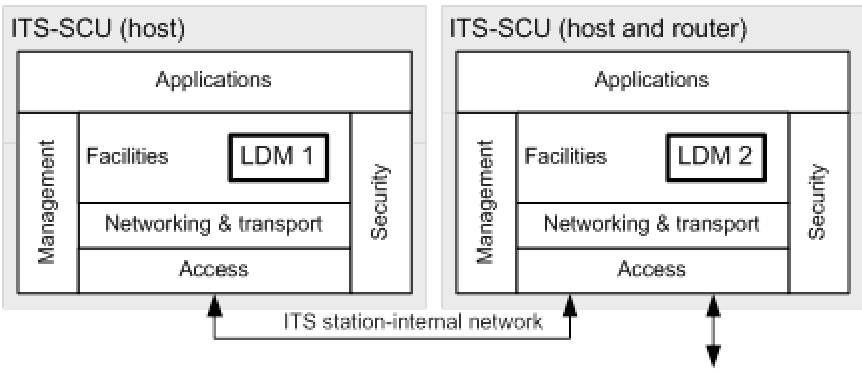

Figure 5 — Implementation configuration example d)

Many other implementation configurations are feasible.

NOTE In ITS-SUs composed of several ITS-SCUs, the ITS station management can use the "ITS station-internal management communications protocol" (IICP)[11] to support overall station management

5.5 LDM-related processes

5.5.1 Synchronization of LDMs

The concept of synchronization of LDMs is introduced in Reference [17], distinguishing

— synchronization of LDMs operated in ITS station units of different vehicles, and

— synchronization of LDMs operated in ITS station units at the roadside, in central offices, and in vehicles.

Reference is made to means which are already in use for TPEG and DATEX.

Such synchronization means updating of an LDM by an authorized “master” LDM. As only ITS-S application processes can access LDM-DOs, any synchronization is to be realized by ITS applications. Details are outside the scope of this Technical Specification.

NOTE Updates of information in an ITS-SU can be performed using remote management standardized in Reference [10].

5.5.2 Archiving of LDM Data Objects

Archiving of LDM Data Objects is a feature that produces a kind of log-file of an LDM. Such log-file information might be of interest for different purposes, but might also be subject to privacy considerations.

This Technical Specification specifies neither an archiving functionality nor related interfaces. Archiving can be implemented in a non-standardized way.

5.6 LDM for road safety and vehicle-to-vehicle applications

An LDM dedicated to usage for road safety and vehicle-to-vehicle applications (electronic horizon) is specified by ETSI in Reference [22]. This ETSI LDM specification constitutes a functional sub-set of the specification provided in this Technical Specification.

5.7 Security perspective

5.7.1 Authorized access to LDM

The architecture of an LDM in the context of BSMD from a security perspective is to ensure that access is restricted to identified and authorized ITS-S application processes. Application processes not certified for operation in a BSMD may access an LDM via a secure gateway described in ISO 21217, where the firewall ITS-S application process of this gateway is authorized for read-access to the LDM.

All the core assets are to be considered as vulnerable and therefore subject to protection, where protection takes the form of specific guards. The guard mechanism used in protecting the LDM is a policy-based access control scheme where ITS-S application processes will pre-register their policy with the ITS-S, and if that policy is agreed, all future access by the ITS-S application process will be verified as being consistent with the policy.

5.7.2 Initialisation and installation of applications to the BSMD

The kernel of an ITS-SCU forms a trust centre of the BSME and is identifiable to third-party ITS-S application processes as such. Any ITS-S application process to be added to an ITS-SCU within the BSME verifies the identity and capability of the ITS-SCU prior to installation. If installation is allowed, an ITS-SCU verifies the credentials offered by the ITS-S application process. Prior to distribution, each ITS-S application process is functionally verified and tested and assertions of required functionality, of developer identity, and of the tester are validated prior to installation.[18]

The core model follows that developed in the i-Tour project[33] as an extension of an “Obligation of Trust” (OoT) protocol, extending the models used for Java midlet distribution used in many common application stores.[18] The protection framework is a form of a Privilege Management Infrastructure (PMI) based on common cryptographic modules and processing where authorization is viewed as a set of mutually agreed actions through the assignment of permissions to the parties, i.e. the LDM and the LDM user. In the OoT protocol, the participating parties exchange difficult-to-repudiate digitally signed obligating constraints, also referred to as “Notification of Obligations” (NoO), which detail their requirements for sending their sensitive information to the other party, and proof of acceptances, also referred to as “Signed Acceptance of Obligations” (SAO), which acknowledge the conditions they have accepted for receiving the other party’s sensitive information. The required capabilities of the LDM user, i.e. an ITS-S application process, to be installed will be declared and the application restricted to use only those capabilities by means of a policy enforcement engine acting in the role of a Policy Enforcement Point in the LDM itself.

For protection of data, the data objects identified below capture the primary policy elements:

— PrivacyPolicyDirective;

— SecurityPolicyDirective;

— SignedPrivacyPolicy;

— SignedSecurityPolicy;

— CounterSignedPrivacyPolicy;

— CounterSignedSecurityPolicy.

The privacy policy directive is a set of policy statements that identify the identity of the data controller. The privacy enforcement point agrees to implement the policy and to indicate that in the Signed Privacy Policy where the signature is of the data processor (acting as policy enforcement point).

Acceptance of the privacy policy is notified by the client in the Countersigned Privacy Policy where the signature is given by the client using the pseudonymous identity agreed during registration. The retention of the countersigned policy agreement provides the basis of non-repudiation of consent.

NOTE The data privacy legislation in Europe assumes the presence of a number of entities in a system dealing with private data. These are the data controller, data processor and data subject, and a contract of consent. In an all-informed C-ITS, there is no a priori consent establishment between the transmitting ITS-SU and any of the receiving ITS-SUs, thus, the security model attempts to minimize the possibility of any personal data being made known to a receiving ITS-SU. The model therefore virtualizes the functionality of data controller, data processor, and consent by use of verifiable proofs of authority to act on data.

Permissions resulting from policy are of type “Permit” and “Deny” based on authorization, i.e. after application of the policy, the request is either permitted or denied. Requests themselves may contain specific access requests, e.g. read data from the LDM, write data to the LDM.

Every incoming command to the LDM is associated with a set of claims that are checked against the local policy at the PEP in the LDM. If any data access attempt from an application is made post-registration and post-acceptance of the policy that does not comply with the policy, it is denied.

5.7.3 Privacy

The C-ITS enforces pseudonymity capabilities through the security functions described in ETSI/TS 102 940[24] and ETSI/TS 102 941[25] which maintains privacy control of data entered into the LDM.

5.8 LDM versus other similar functionalities in an ITS-SU

The sharing of data between ITS-S application processes in an ITS-SU can be achieved by subscribe/publish mechanisms, where at least two mechanisms are distinguished, i.e.

a) one allowing ITS-S application processes to subscribe at the ITS-S facilities layer to standardized messages from ITS message sets as specified in[19] without using an LDM, and

b) one using a Local Dynamic Map (LDM) as repository of standardized data objects.

The approach a)[19] standardizes an ITS-S facility layer message handler which can

— directly forward complete received messages to subscribed ITS-S application processes without storing these messages, and

— present LDM Data Objects to an LDM in case these LDM Data Objects are contained in messages that follow the message format convention of this message handler.

There may be also other data storages, which are basically different to an LDM, i.e. which may store data objects that are not following the definition of an LDM-DO.

6 Functionality

This Clause contains informative descriptions of the functionality of an LDM.

6.1 General definitions and conventions

As explained in 5.2, an LDM deals with information on real objects that are existent at a defined location (geo-area) and within a defined time interval. Such information on a real object is identified in an **LDM Data Record** (see Figure 7). Every LDM Data Record is identified with a unique LDM Data Record ID; the value zero indicates an "unknown record".

Different location and time definitions are used to define the functionality of an LDM.

— Definitions related to the information on the real object:

— **Location Validity**

Information at which geo-location or in which geo-area the LDM-DO applies.

— **Time Validity**

Information in which time interval(s) the LDM-DO applies.

— **Time of Generation**

Information on the time when the LDM-DO information was generated, e.g. time when a perception system (e.g. a sensor) detected the event "slippery road".

— **Time of Mandatory Deletion**

Information on time after which the LDM record will no longer be returned in a query.

— Definitions used in queries:

— **LDM Area of Interest**

Geo-location(s) or geo-area(s) that are of interest for the querying ITS-S application process.

— **LDM Time of Interest**

Time instant or time interval(s) that are of interest for the querying ITS-S application process.

— **Age of Interest**

Age of LDM record as required by the querying ITS-S application process. The age is calculated with a numerical operator presented by the ITS-S application process against the time of generation of an LDM-DO, if available, or alternatively against the time of last update of an LDM-DO.

