
**Système de transports intelligents —
Systèmes coopératifs — Carte locale
dynamique**

*Intelligent transport systems — Co-operative ITS — Local dynamic
map*

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

[ISO 18750:2018](https://standards.itih.ai/catalog/standards/iso/d6b5ed8-7226-4a58-a66d-31721e327fa9/iso-18750-2018)

<https://standards.itih.ai/catalog/standards/iso/d6b5ed8-7226-4a58-a66d-31721e327fa9/iso-18750-2018>



iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ISO 18750:2018](https://standards.iteh.ai/catalog/standards/iso/d6b15ed8-7226-4a58-a66d-31721e327fa9/iso-18750-2018)

<https://standards.iteh.ai/catalog/standards/iso/d6b15ed8-7226-4a58-a66d-31721e327fa9/iso-18750-2018>



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO 2018

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en œuvre, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
Fax: +41 22 749 09 47
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos	v
Introduction	vi
1 Domaine d'application	1
2 Références normatives	1
3 Termes et définitions	2
4 Symboles et abréviations	3
5 Environnement architectural	4
5.1 Carte dynamique locale.....	4
5.2 LDM dans une ITS-S.....	5
5.3 LDM dans une ITS-SU.....	5
5.4 Processus liés à la LDM.....	7
5.4.1 Synchronisation des LDM.....	7
5.4.2 Archivage des objets de données de la LDM.....	8
5.5 LDM pour la sécurité routière et les applications de véhicule à véhicule.....	8
5.6 Perspective de sécurité.....	8
5.6.1 Accès autorisé à la LDM.....	8
5.6.2 Initialisation et installation d'applications dans le BSMD.....	8
5.6.3 Confidentialité.....	9
5.7 La LDM face à d'autres fonctionnalités similaires dans une ITS-SU.....	9
6 Fonctionnalités	10
6.1 Termes et conventions.....	10
6.2 Structure d'une LDM.....	12
6.3 Espace de stockage des données de la LDM.....	13
6.4 Services de la LDM.....	16
6.4.1 Enregistrement, désenregistrement et révocation des processus d'application ITS-S.....	16
6.4.2 Vérifications de sécurité dans les demandes d'accès.....	16
6.4.3 Gestion des demandes d'accès.....	16
6.5 Maintenance de la LDM.....	19
6.5.1 Zone de maintenance de la LDM.....	19
6.5.2 Gestion des données ayant expiré.....	19
6.6 Base de connaissances de la LDM.....	19
6.6.1 Métadonnées.....	19
6.6.2 Fonctions utilitaires.....	19
6.7 Interfaces.....	20
6.7.1 Types d'interfaces.....	20
6.7.2 Paramètres des fonctions d'interface.....	20
6.7.3 Interface de gestion de l'application de la LDM.....	23
6.7.4 Interface de données de la LDM.....	24
6.7.5 Interface de sécurité.....	28
6.7.6 Interface de gestion de la LDM.....	29
6.7.7 Points d'accès au service.....	29
7 Procédures	33
7.1 Services de la LDM.....	33
7.1.1 Enregistrement, désenregistrement et révocation des processus d'application ITS-S.....	33
7.1.2 Vérifications de sécurité dans les demandes d'accès.....	33
7.1.3 Gestion des demandes d'accès.....	33
7.1.4 Filtrage de deuxième niveau.....	35
7.2 Maintenance de la LDM.....	36
7.2.1 Gestion de zone.....	36
7.2.2 Retrait des données ayant expiré.....	36

ISO 18750:2018(F)

7.3	Base de connaissances de la LDM.....	36
7.4	Interfaces.....	36
7.5	Gestion de la LDM.....	37
7.5.1	Enregistrement de la LDM auprès de l'entité de gestion ITS-S.....	37
7.5.2	ITS-SCU multiples.....	37
Annexe A	(normative) Modules ASN.1	38
Annexe B	(normative) Dictionnaire de données de la LDM.....	50
Annexe C	(informative) Exemples de LDM-DO	52
Annexe D	(informative) Référencement spatial (localisation)	59
Annexe E	(informative) Référencement temporel.....	64
Annexe F	(normative) Formulaire de déclaration de conformité des mises en œuvre	65
Bibliographie	72

iTeh Standards (<https://standards.iteh.ai>) Document Preview

[ISO 18750:2018](https://standards.iteh.ai/catalog/standards/iso/d6b15ed8-7226-4a58-a66d-31721e327fa9/iso-18750-2018)

<https://standards.iteh.ai/catalog/standards/iso/d6b15ed8-7226-4a58-a66d-31721e327fa9/iso-18750-2018>

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO, participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (IEC) en ce qui concerne la normalisation électrotechnique.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient en particulier de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction définies dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/patents).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir le lien suivant: www.iso.org/iso/foreword.html.

Le comité chargé de l'élaboration du présent document est l'ISO/TC 204, *Système de transports intelligent*.

Cette première édition annule et remplace la première édition (ISO/TS 18750:2015), qui a été techniquement révisée.

Introduction

Les systèmes de transport intelligents coopératifs (C-ITS), voir l'ISO TR 17465-1,[15] possèdent une propriété essentielle: le partage des données entre différentes applications ITS fournissant divers services ITS aux utilisateurs. Cette démarche remplace l'approche traditionnelle selon laquelle chaque application est exploitée dans un environnement isolé, également nommée «approche cloisonnée». La démarche C-ITS permet de créer des synergies dans les composants d'une unité de station ITS, par ex. le partage des outils de communication, d'améliorer les performances et la fiabilité générales et de réduire les coûts globaux. Pour protéger les intérêts des différentes applications ITS, les C-ITS mettent en œuvre le concept d'une station ITS exploitée en tant que domaine délimité géré de manière sécurisée.

Les données sont partagées entre les applications via des dispositifs d'abonnement/de publication, dans lesquels on distingue au moins deux mécanismes: l'un permettant aux processus d'application ITS-S de s'abonner à des messages normalisés à partir d'ensembles de messages ITS (transfert direct à la réception de ces messages dans une unité de station ITS), l'autre utilisant une carte dynamique locale (LDM) en tant que référentiel d'objets de données normalisés. Ces objets de données stockés dans une LDM sont nommés Objets de données de la LDM (LDM-DO). Les LDM-DO fournissent des informations cohérentes sur les objets réels présents à une géolocalisation donnée durant un intervalle de temps déterminé. Les processus d'application ITS-S autorisés peuvent ajouter des LDM-DO à une LDM et récupérer des LDM-DO dans une LDM. Les LDM-DO peuvent être récupérés par le biais de requêtes et au moyen d'un abonnement. Un abonnement générera des notifications automatiques pour une sélection d'objets de données de la LDM, soit à intervalles de temps définis, soit dès l'occurrence d'un événement.

Ce document présente l'utilisation des LDM et spécifie la LDM pour une exploitation globale dans le cadre des C-ITS.

Les mises en œuvre initiales des LDM ont été réalisées dans le cadre des projets de recherche de l'UE CVIS[40] et Safespot[42].

Document Preview

[ISO 18750:2018](https://standards.iteh.ai/catalog/standards/iso/d6b15ed8-7226-4a58-a66d-31721e327fa9/iso-18750-2018)

<https://standards.iteh.ai/catalog/standards/iso/d6b15ed8-7226-4a58-a66d-31721e327fa9/iso-18750-2018>

Systeme de transports intelligents — Systemes cooperatifs — Carte locale dynamique

1 Domaine d'application

Ce document

- décrit la fonctionnalité d'une «Carte dynamique locale» (LDM) dans le contexte du «Domaine délimité géré de manière sécurisée» (BSMD).
- spécifie
 - les caractéristiques générales des objets de données de la LDM (LDM-DO) pouvant être stockés dans une LDM, notamment les informations sur les objets réels tels que les véhicules, les zones de travaux, les zones de ralentissement du trafic, les zones caractérisées par des conditions météorologiques particulières, etc. qui doivent, au minimum, posséder une référence spatiale (localisation) et une référence temporelle.
 - les fonctions des points d'accès au service fournissant des interfaces d'accès à une LDM dans une station ITS (ITS-S) pour,
 - les accès sécurisés d'ajout, de mise à jour et de suppression, pour les processus d'application ITS-S,
 - les accès sécurisés en lecture (requête), pour les processus d'application ITS-S,
 - les notifications sécurisées (lors de l'abonnement) aux processus d'application ITS-S.
 - la gestion des accès,
 - enregistrement, désenregistrement et révocation de manière sécurisée des processus d'application ITS-S au niveau de la LDM
 - abonnement et annulation des abonnements des processus d'application ITS-S de manière sécurisée,
 - les procédures d'une LDM tenant compte
 - des modalités de maintien du contenu et de l'intégrité du magasin de données,
 - les mécanismes soutenant plusieurs LDM dans une unité de station ITS unique.

2 Références normatives

Les documents de référence suivants, dans leur version intégrale ou partielle, ont un caractère normatif et sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO 21217, *Systemes intelligents de transport — Accès aux communications des services mobiles terrestres (CALM) — Architecture*

ISO/IEC 8824-1, *Technologies de l'information -- Notation de syntaxe abstraite numéro un (ASN.1): Spécification de la notation de base — Partie 1*

ISO/IEC 8825-2, *Technologies de l'information -- Règles de codage ASN.1: Spécification des règles de codage compact (PER) — Partie 2*

ISO/IEC 9646-7, *Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Essais de conformité — Méthodologie générale et procédures — Partie 7: Déclarations de conformité des mises en oeuvre*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

— ISO Online browsing platform: disponible à l'adresse <https://www.iso.org/obp>

— IEC Electropedia: disponible à l'adresse <http://www.electropedia.org/>

3.1

Intégrité des données

propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée

[SOURCE: ISO 24534-5]

3.2

Temps atomique international

temps s'écoulant depuis le 1^{er} janvier 2004, 00:00:00 UTC, identique au temps UTC hormis le fait qu'il n'est nécessaire d'ajouter aucune seconde intercalaire.

3.3

Zone d'intérêt de la LDM

exigence d'emplacement exploitée dans le processus de filtrage des requêtes et des notifications automatiques

3.4

Zone de maintenance de la LDM

Information sur la zone d'emplacement opérationnel d'une LDM utilisée par la maintenance de la LDM

Note 1 à l'article: L'ETSI EN 302 895[28] limite la Zone de maintenance de la LDM à la «zone géographique spécifiée par la LDM pour sa propre maintenance».

3.5

Permissions de la LDM

information précisant dans quelle mesure un processus d'application ITS-S spécifique est autorisé à utiliser une LDM

3.6

Objet de données de la LDM

représentation d'un objet réel, basée sur une référence spatiale (localisation) et une référence temporelle, explicite sans autre information de contexte

3.7

ID d'objet de données de la LDM

identificateur d'un objet de données unique dans une LDM

3.8

Dictionnaire de données de la LDM

dictionnaire de types d'objets de données de la LDM

3.9

Type d'objet de données de la LDM

identificateur du type d'information contenue dans un bloc de données de la LDM

3.10**Validité spatiale**

information indiquant un emplacement auquel un objet de données de la LDM est valide

3.11**Validité temporelle**

information indiquant un intervalle de temps durant lequel un objet de données de la LDM est valide

3.12**Temps d'intérêt de la LDM**

exigence de temps employée dans le processus de filtrage des requêtes et des notifications automatiques

3.13**Carte dynamique locale**

entité comprenant des objets de données de la LDM, avec les services et interfaces nécessaires à leur manipulation

3.14**Référence spatiale (localisation)**

description d'emplacement ou de zone identifiable de manière unique dans le monde réel

3.15**Métadonnées**

données concernant d'autres données

Note 1 à l'article: Le terme «métadonnées» est ambigu, car il est employé dans le cadre de concepts fondamentalement différents. Les métadonnées structurelles sont des informations liées à la conception et à la spécification de structures de données; elles sont également définies comme des «données concernant les conteneurs de données». Les métadonnées descriptives sont des informations sur les instances de données, c'est-à-dire le contenu des données; elles sont également définies comme des «données concernant le contenu des données».

3.16**Horaire de création**

horaire auquel un bloc de données de la LDM a été créé et mis à jour

3.17**Horaire de suppression**

horaire auquel un bloc de données de la LDM peut être supprimé et ne sera plus pris en considération par la fonctionnalité de recherche de la LDM

3.18**Horaire de génération**

horaire auquel le contenu du champ d'information de l'objet de données de la LDM a été créé

Note 1 à l'article: Cet horaire diffère de l'horaire auquel l'objet de données de la LDM a été écrit dans une LDM.

4 Symboles et abréviations

BSMD	<i>Bounded Secured Managed Domain</i> (Domaine délimité géré de manière sécurisée)
BSME	<i>Bounded Secured Managed Entity</i> (Entité délimitée gérée de manière sécurisée)
IAT	<i>International Atomic Time</i> (Temps atomique international)
ICS	<i>Implementation Conformance Statement</i> (Déclaration de conformité des mises en œuvre)
ITS	<i>Intelligent Transport Systems</i> (Systèmes de transport intelligents)
ITS-SCU	<i>ITS Station Communication Unit</i> (Unité de communication de station ITS)

ITS-SU	<i>ITS Station Unit</i> (Unité de station ITS)
IUT	<i>Implementation Under Test</i> (Mise en œuvre en cours d'essai)
LDM	<i>Local Dynamic Map</i> (Carte dynamique locale)
LDM-DD	<i>LDM Data Dictionary</i> (Dictionnaire de données de la LDM)
LDM-DT	<i>LDM Data Type</i> (Type de données de la LDM)
LDM-DAT	<i>LDM Data Attribute Type</i> (Type d'attribut de données de la LDM)
LDM-DATID	<i>LDM-DAT Identifier</i> (Identificateur du type d'attribut de données de la LDM)
LDM-DTID	<i>LDM-DT Identifier</i> (Identificateur du type de données de la LDM)
NdO	<i>Notification of Obligations</i> (Notification d'obligations)
OdC	<i>Obligation of Trust</i> (Obligation de confiance)
PMI	<i>Privilege Management Infrastructure</i> (Infrastructure de gestion des privilèges)
SAO	<i>Signed Acceptance of Obligations</i> (Acceptation signée des obligations)
SUT	<i>System Under Test</i> (Système en cours d'essai)
TPEG	<i>Transport Protocol Experts Group</i> (Groupe d'experts du protocole de transport)
UTC	<i>Universal Time Coordinated</i> (Temps universel coordonné)

5 Environnement architectural

Cette section contient des descriptions à caractère informatif de l'environnement architectural d'une LDM.

5.1 Carte dynamique locale

Une carte dynamique locale (LDM) est une entité comprenant des objets de données de la LDM (LDM-DO), avec les services et interfaces nécessaires à leur manipulation. Les LDM-DO se distinguent par leur type (LDM-DT). Les LDM-DT sont spécifiés par le biais d'un enregistrement dans le dictionnaire de données de la LDM (LDM-DD). Le concept du LDM-DD est présenté à l'[Annex B](#).

NOTE Dans l'ISO TR 17424,[\[16\]](#) les LDM-DO sont classés selon 4 types: Type 1 (objets de données permanents et statiques, par ex. les données de cartographie), Type 2 (objets de données temporaires et statiques, par ex. une aire de stationnement temporaire sur la route), Type 3 (objets de données temporaires et dynamiques, par ex. l'emplacement des travaux), et Type 4 (objets de données hautement dynamiques, par ex. localisation, orientation et vitesse des véhicules alentours). Le présent document n'utilise pas cette classification.

Un LDM-DO fournit des informations sur les objets réels (véhicules, événements routiers, etc.) localisés à un endroit défini, dans une zone géographique définie, dans un intervalle de temps défini. Dans le cas le plus simple, les informations fournies par un LDM-DO sont uniquement son type, sa géolocalisation et sa durée de validité. Ces informations peuvent être reçues dans une unité de station ITS via différents canaux, tels que

- DATEX II,[\[32\]](#) TPEG,[\[36\]](#) RDS-TMC (systèmes hérités);
- Ensembles de messages ITS CEN / ETSI / ISO / SAE selon CEN/ISO,[\[17\]](#) CEN/ISO TS 19321,[\[18\]](#) ETSI EN 302 637-2,[\[26\]](#) ETSI EN 302 637-3,[\[27\]](#) SAE J2735[\[37\]](#);

composés de différents jeux d'attributs, et présentés selon différents formats (encodages). Les processus d'application ITS-S capables de recevoir ces informations réalisent une cartographie à partir des LDM-DO et une conversion des formats d'attributs dans le format commun donné par les LDM-DT.

5.2 LDM dans une ITS-S

La spécification de carte dynamique locale (LDM) présentée dans ce document est conçue pour l'environnement architectural d'une station ITS exploitée en tant que domaine délimité géré de manière sécurisée (BSMD) spécifié dans l'ISO 21217:2014 et représenté dans la [Figure 1](#).

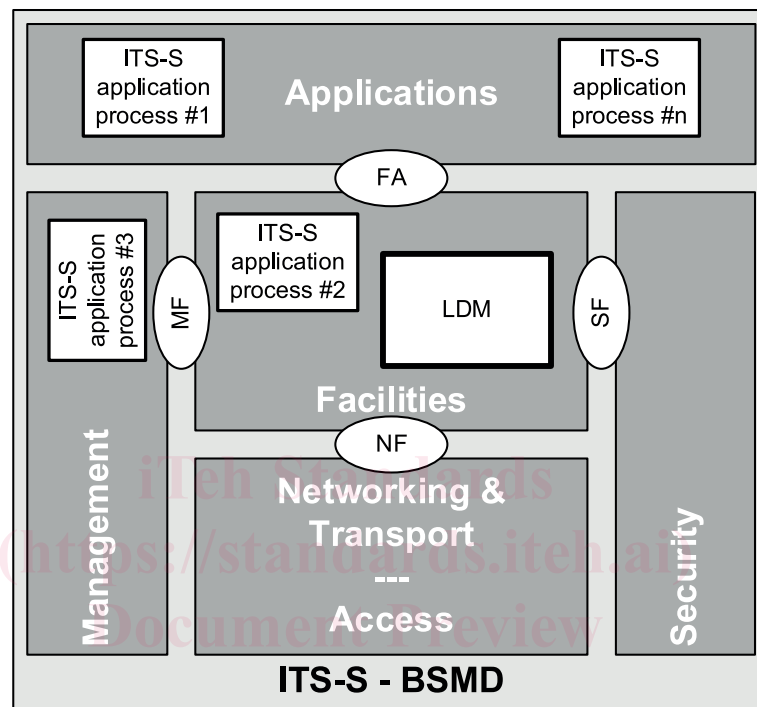


Figure 1 — LDM dans une ITS-S exploitée en tant que domaine délimité géré de manière sécurisée (BSMD)

La fonctionnalité LDM spécifiée dans la [section 6](#) est située dans la couche de dispositifs de l'ITS-S. Une LDM établit une interface avec les processus d'application ITS-S spécifiés dans l'ISO 21217:2014. La fonctionnalité d'interface est spécifiée au [paragraphe 6.6.2](#) par le biais de fonctions de services du FA-SAP et du MF-SAP; ces deux points d'accès au service (SAP) proposent des fonctions identiques à cette fin. Les services génériques des FA-SAP et MF-SAP sont spécifiés dans l'ISO 24102-3[9].

5.3 LDM dans une ITS-SU

La [Figure 2](#), la [Figure 3](#), la [Figure 4](#), et la [Figure 5](#) présentent divers exemples de configurations de mise en œuvre supportées.

[Figure 2](#) présente une configuration «monobloc» d'une unité de station ITS (ITS-SU) avec une seule LDM.

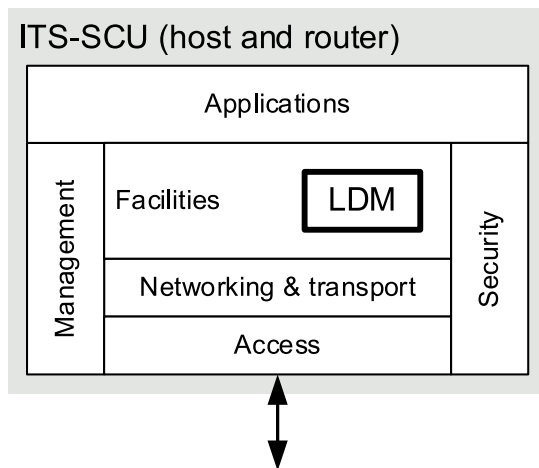


Figure 2 — Exemple de configuration de mise en œuvre a)

Figure 3 présente une configuration «monobloc» d’une ITS-SU avec deux LDM.

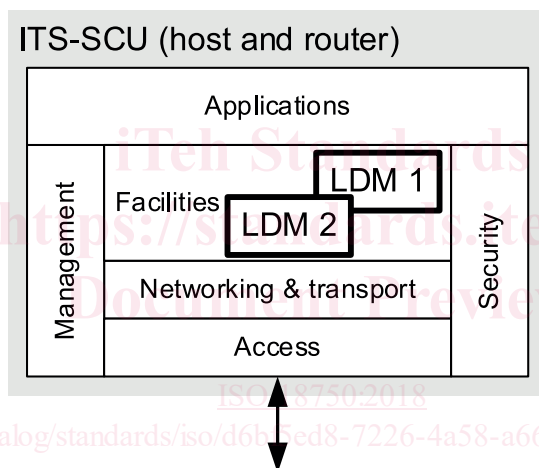


Figure 3 — Exemple de configuration de mise en œuvre b)

Figure 4 présente une configuration d’une ITS-SU avec deux unités de communication de station ITS (ITS-SCU). L’une de ces ITS-SCU a un rôle d’hôte uniquement, spécifié dans l’ISO 21217:2014, et contient une seule LDM. L’autre ITS-SCU a un rôle de routeur uniquement, spécifié dans l’ISO 21217:2014, et ne contient pas de LDM.

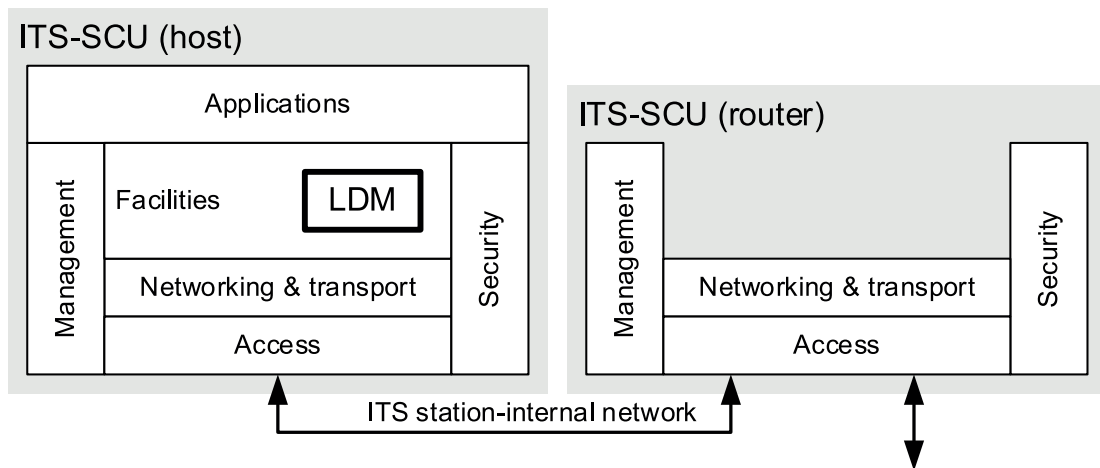


Figure 4 — Exemple de configuration de mise en œuvre c)

Figure 5 présente une configuration d'une ITS-SU avec deux unités de communication de station ITS (ITS-SCU). L'une de ces ITS-SCU a un rôle d'hôte uniquement, spécifié dans l'ISO 21217:2014, et contient une seule LDM. L'autre ITS-SCU a un rôle d'hôte et de routeur, spécifié dans l'ISO 21217:2014, et contient également une LDM.

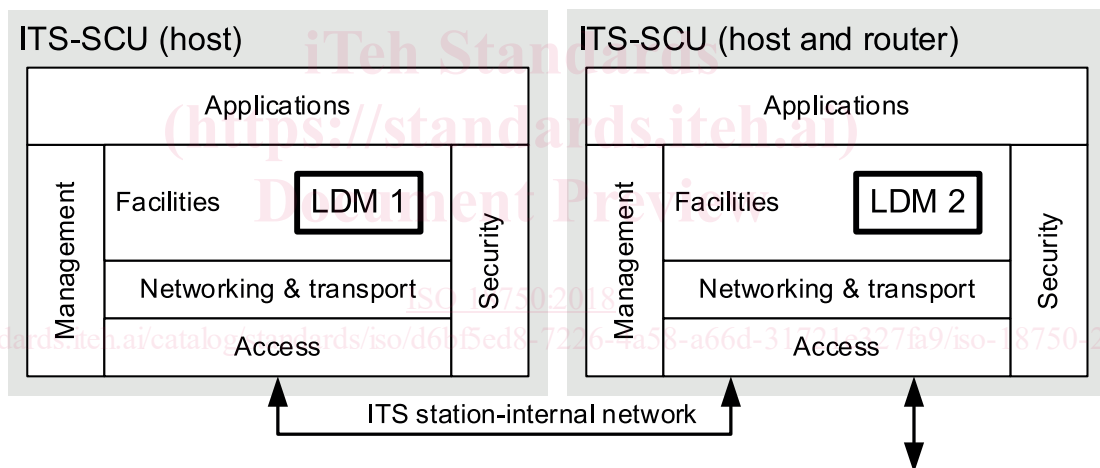


Figure 5 — Exemple de configuration de mise en œuvre d)

De nombreuses autres configurations de mise en œuvre sont réalisables.

NOTE Dans les ITS-SU composées de plusieurs ITS-SCU, la gestion de la station ITS peut exploiter le «protocole de communications de gestion interne à la station ITS» (IICP) spécifié dans l'ISO 24102-4[10] pour soutenir la gestion globale de la station.

5.4 Processus liés à la LDM

5.4.1 Synchronisation des LDM

Le concept de synchronisation des LDM est présenté par l'ISO TR 17424,[16] distinguant

- la synchronisation des LDM exploitées dans les unités de station ITS de différents véhicules;
- la synchronisation des LDM exploitées dans les unités de station ITS situées en bord de route, dans les bureaux centraux et dans les véhicules.

Il est fait référence aux moyens déjà exploités pour TPEG et DATEX.

Cette synchronisation implique la mise à jour d'une LDM par une LDM «maîtresse» autorisée. Étant donné que seuls les processus d'application ITS-S sont en mesure d'accéder aux LDM-DO, toute synchronisation doit être réalisée par les applications ITS. Les modalités détaillées sortent du domaine d'application du présent document.

NOTE La mise à jour des informations d'une ITS-SU peut être réalisée par le biais de la gestion à distance normalisée par l'ISO 24102-2[8].

5.4.2 Archivage des objets de données de la LDM

L'archivage des objets de données de la LDM est une fonctionnalité permettant de créer une sorte de fichier journal d'une LDM. Les informations de ce fichier journal peuvent être pertinentes pour différents usages, mais peuvent également faire l'objet de considérations ayant trait à la confidentialité.

Ce document ne spécifie ni fonctionnalité d'archivage, ni interface connexe. L'archivage peut être mis en œuvre de manière non normalisée.

5.5 LDM pour la sécurité routière et les applications de véhicule à véhicule

Une LDM dédiée au contexte de la sécurité routière et aux applications de véhicule à véhicule (horizon électronique) est spécifiée par l'ETSI dans l'EN 302 895.[28] Cette spécification de l'ETSI concernant la LDM constitue un sous-ensemble fonctionnel de la spécification du présent document.

5.6 Perspective de sécurité

5.6.1 Accès autorisé à la LDM

L'architecture d'une LDM dans le contexte du BSMD du point de vue de la sécurité permet de s'assurer que l'accès est réservé aux processus d'application ITS-S identifiés et autorisés. Les processus d'application non certifiés pour une exploitation dans un BSMD peuvent accéder à une LDM via une passerelle sécurisée décrite par l'ISO 21217:2014, dans laquelle le processus d'application ITS-S pare-feu de cette passerelle peut accéder uniquement en lecture à la LDM.

Tous les actifs fondamentaux doivent être considérés comme vulnérables et donc sous protection prenant la forme de mécanismes spécifiques. Le mécanisme de protection de la LDM est un système de contrôle d'accès basé sur une politique, dans lequel les processus d'application ITS-S doivent enregistrer au préalable leur politique auprès de l'ITS-S et, si cette politique est acceptée, tous les accès ultérieurs par le processus d'application ITS-S seront vérifiés et déclarés conformes à la politique.

5.6.2 Initialisation et installation d'applications dans le BSMD

Le noyau d'une ITS-SCU constitue le centre de confiance de la BSME et est identifiable en tant que tel vis-à-vis des processus d'application ITS-S tiers. Tout processus d'application ITS-S à ajouter à une ITS-SCU dans la BSME vérifie l'identité et les capacités de l'ITS-SCU avant l'installation. Si l'installation est autorisée, une ITS-SCU vérifie les justificatifs proposés par le processus d'application ITS-S. Avant la distribution, les fonctionnalités de chaque processus d'application ITS-S sont vérifiées et soumises à essai, et les affirmations de fonctionnalité requise, d'identité du développeur et d'identité du testeur, sont validées avant installation selon l'EN/ISO 17419[19].

Le modèle fondamental suit celui qui a été développé dans le cadre du projet i-Tour[39] en tant qu'extension d'un protocole d'«obligation de confiance» (OoT), dans le prolongement des modèles utilisés pour la distribution des midlets Java employés dans de nombreux référentiels d'applications, voir EN/ISO 17419.[19] Le cadre de protection est une forme d'Infrastructure de gestion des privilèges (PMI) basée sur un traitement et des modules cryptographiques communs selon lesquels l'autorisation est considérée comme un ensemble d'actions mutuellement convenues par l'attribution de permissions aux parties, c'est-à-dire la LDM et l'utilisateur de la LDM. Dans le protocole OoT, les parties prenantes échangent des engagements signés numériquement difficilement répudiables, également nommés «Notifications d'obligations» (NoO), qui énoncent de manière détaillée leurs exigences concernant l'envoi