Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.2066

(06/2014)

SÉRIE Y: INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET, RÉSEAUX DE PROCHAINE GÉNÉRATION, INTERNET DES OBJETS ET VILLES INTELLIGENTES

Réseaux de prochaine génération – Cadre général et modèles architecturaux fonctionnels

Exigences communes relatives à l'Internet des objets

Recommandation UIT-T Y.2066

Union internationale des télécommunications

RECOMMANDATIONS UIT-T DE LA SÉRIE Y

INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET, RÉSEAUX DE PROCHAINE GÉNÉRATION, INTERNET DES OBJETS ET VILLES INTELLIGENTES

INFRASTRUCTURE MONDIALE DE L'INFORMATION	
Généralités	Y.100–Y.199
Services, applications et intergiciels	Y.200–Y.299
Aspects réseau	Y.300–Y.399
Interfaces et protocoles	Y.400–Y.499
Numérotage, adressage et dénomination	Y.500–Y.599
Gestion, exploitation et maintenance	Y.600–Y.699
Sécurité	Y.700–Y.799
Performances	Y.800–Y.899
ASPECTS RELATIFS AU PROTOCOLE INTERNET	
Généralités	Y.1000–Y.1099
Services et applications	Y.1100–Y.1199
Architecture, accès, capacités de réseau et gestion des ressources	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interfonctionnement	Y.1400–Y.1499
Qualité de service et performances de réseau	Y.1500–Y.1599
Signalisation	Y.1600–Y.1699
Gestion, exploitation et maintenance	Y.1700–Y.1799
Taxation	Y.1800–Y.1899
Télévision IP sur réseaux de prochaine génération	Y.1900–Y.1999
RÉSEAUX DE PROCHAINE GÉNÉRATION	
Cadre général et modèles architecturaux fonctionnels	**Y.2000–Y.2099**
Qualité de service et performances	Y.2100–Y.2199
Aspects relatifs aux services: capacités et architecture des services	Y.2200–Y.2249
Aspects relatifs aux services: interopérabilité des services et réseaux dans les réseaux de prochaine génération	Y.2250–Y.2299
Améliorations concernant les réseaux de prochaine génération	Y.2300–Y.2399
Gestion de réseau	Y.2400–Y.2499
Architectures et protocoles de commande de réseau	Y.2500–Y.2599
Réseaux de transmission par paquets	Y.2600–Y.2699
Sécurité	Y.2700–Y.2799
Mobilité généralisée	Y.2800–Y.2899
Environnement ouvert de qualité opérateur	Y.2900–Y.2999
RÉSEAUX FUTURS	Y.3000–Y.3499
INFORMATIQUE EN NUAGE	Y.3500–Y.3999
INTERNET DES OBJETS ET VILLES ET COMMUNAUTÉS INTELLIGENTES	
Considérations générales	Y.4000–Y.4049
Termes et définitions	Y.4050–Y.4099
Exigences et cas d'utilisation	Y.4100–Y.4249
Infrastructure, connectivité et réseaux	Y.4250–Y.4399
Cadres, architectures et protocoles	Y.4400–Y.4549
Services, applications, calcul et traitement des données	Y.4550–Y.4699
Gestion, commande et qualité de fonctionnement	Y.4700–Y.4799
Identification et sécurité	Y.4800–Y.4899
Evaluation et analyse	Y.4900-Y.4999

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T Y.2066

Exigences communes relatives à l'Internet des objets

Résumé

La Recommandation UIT-T Y.2066 définit les exigences communes relatives à l'Internet des objets (IoT). Ces exigences sont fondées sur les cas d'utilisation généraux de l'IoT et les acteurs de l'IoT, qui découlent de la définition de l'IoT contenue dans la Recommandation UIT-T Y.2060. Les exigences communes relatives à l'IoT sont indépendantes de tout domaine d'application particulier, à savoir des domaines de connaissance ou d'activité applicables pour une finalité économique, commerciale, sociale ou administrative particulière, par exemple le domaine d'application du transport et le domaine d'application de la santé.

S'appuyant sur la présentation générale de l'IoT (Recommandation UIT-T Y.2060), la présente Recommandation définit les exigences communes sur la base des cas d'utilisation généraux de l'IoT et des acteurs de l'IoT, en tenant compte des domaines importants à considérer du point de vue des exigences. Certains cas d'utilisation représentatifs de l'IoT, qui sont extraits de domaines d'application, sont également définis. Les exigences communes relatives à l'IoT spécifiées dans cette Recommandation sont classées dans différentes catégories: exigences non fonctionnelles, exigences relatives à la prise en charge d'applications, exigences relatives aux services, exigences relatives aux communications, exigences relatives aux dispositifs, exigences relatives à la gestion de données et exigences relatives à la sécurité et à la protection de la confidentialité.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T Y.2066	22-06-2014	13	11.1002/1000/12169

Mots clés

Exigences communes, exigences fonctionnelles, Internet des objets (IoT), exigences non fonctionnelles, cas d'utilisation.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et on considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T Y.2066

Exigences communes relatives à l'Internet des objets

1 Domaine d'application

La présente Recommandation définit les exigences communes relatives à l'Internet des objets (IoT). Ces exigences sont fondées sur les cas d'utilisation généraux de l'IoT et les acteurs de l'IoT, qui découlent de la définition de l'IoT contenue dans la Recommandation [UIT-T Y.2060]. Les exigences communes relatives à l'IoT sont indépendantes de tout domaine d'application particulier, à savoir des domaines de connaissance ou d'activité applicables pour une finalité économique, commerciale, sociale ou administrative particulière, par exemple le domaine d'application du transport et le domaine d'application de la santé.

S'appuyant sur la présentation générale de l'IoT (Recommandation [UIT-T Y.2060]), la présente Recommandation définit les exigences communes sur la base des cas d'utilisation généraux de l'IoT et des acteurs de l'IoT, en tenant compte des domaines importants à considérer du point de vue des exigences. Certains cas d'utilisation représentatifs de l'IoT, qui sont extraits de domaines d'application, sont également définis. Les exigences communes relatives à l'IoT spécifiées dans cette Recommandation sont classées dans différentes catégories: exigences non fonctionnelles, exigences relatives à la prise en charge d'applications, exigences relatives aux services, exigences relatives aux communications, exigences relatives aux dispositifs, exigences relatives à la gestion de données et exigences relatives à la sécurité et à la protection de la confidentialité.

Le domaine d'application de cette Recommandation couvre:

- les cas d'utilisation généraux de l'IoT;
- les acteurs de l'IoT;
- les domaines importants à considérer du point de vue des exigences;
- les exigences communes relatives à l'IoT.

Les exigences communes relatives à l'IoT sont résumées et numérotées dans l'Annexe A.

Certains cas d'utilisation représentatifs de l'IoT, qui sont extraits de domaines d'application, sont définis dans l'Appendice I.

NOTE – Les aspects réglementaires, juridiques et commerciaux sortent du cadre de la présente Recommandation. De même, les exigences relatives aux protocoles et aux interfaces (par exemple celles concernant les aspects de l'IoT relatifs au contrôle et à la gestion) sortent du cadre de la présente Recommandation.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document en tant que tel le statut de Recommandation.

[UIT-T Y.2060] Recommandation UIT-T Y.2060 (2012), *Présentation générale de l'Internet des objets*.

[UIT-T Y.2091] Recommandation UIT-T Y.2091 (2011), *Réseaux de prochaine génération: termes et définitions*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 application [UIT-T Y.2091]: ensemble structuré de capacités, qui constituent une fonctionnalité à valeur ajoutée acceptée par un ou plusieurs services, pouvant être pris en charge par une interface API.

3.1.2 client [UIT-T Y.2091]: le client achète à l'entreprise des produits et des services ou reçoit des offres ou des services gratuits. Il peut s'agir d'une personne ou d'une société.

NOTE – Il peut y avoir plusieurs utilisateurs pour un même client.

3.1.3 dispositif [UIT-T Y.2060]: dans l'Internet des objets, équipement doté obligatoirement de capacités de communication et éventuellement de capacités de détection, d'actionnement, d'acquisition de données, de stockage de données et de traitement de données.

3.1.4 Internet des objets (IoT) [UIT-T Y.2060]: infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution.

NOTE 1 – En exploitant les capacités d'identification, d'acquisition de données, de traitement et de communication, l'IoT tire pleinement parti des objets pour offrir des services à toutes sortes d'applications, tout en garantissant le respect des exigences de sécurité et de confidentialité.

NOTE 2 – D'un point de vue général, l'IoT peut être considéré comme un concept ayant des répercussions sur les technologies et la société.

3.1.5 service [UIT-T Y.2091]: ensemble de fonctions et de capacités offertes à un utilisateur par un fournisseur.

3.1.6 objet [UIT-T Y.2060]: dans l'Internet des objets, objet du monde physique (objet physique) ou du monde de l'information (objet virtuel), pouvant être identifié et intégré dans des réseaux de communication.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit le terme suivant:

3.2.1 domaine d'application: domaine de connaissance ou d'activité applicable pour une finalité économique, commerciale, sociale ou administrative particulière.

NOTE – Les domaines d'application du transport, de la santé et des pouvoirs publics sont des exemples de domaines d'application.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

2G deuxième génération

3G troisième génération

API interface de programmation d'application *(application programming interface)*

CAN gestionnaire de réseau de communication *(controller area network)*

DSL ligne d'abonné numérique *(digital subscriber line)*

IoT Internet des objets *(Internet of Things)*

ITS systèmes de transport intelligents *(intelligent transport systems)*

LTE évolution à long terme *(long term evolution)*

M2M machine à machine *(machine-to-machine)*

MOC communication orientée machine *(machine oriented communication)*

SDP plate-forme de fourniture de services *(service delivery platform)*

SLA accord de niveau de service *(service level agreement)*

UML langage de modélisation unifié *(unified modelling language)*

WiFi fidélité sans fil *(wireless fidelity)*

5 Conventions

Dans la présente Recommandation:

Les expressions "**il est nécessaire**" et "**doit**" indiquent une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité au présent document.

L'expression "**il est recommandé**" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire. Cette disposition n'est donc pas indispensable pour déclarer la conformité.

Les expressions "**peut, à titre d'option**" et "**peut**" indiquent une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Elles ne doivent pas être interprétées comme l'obligation pour le fabricant de mettre en œuvre l'option et la possibilité pour l'opérateur de réseau ou le fournisseur de services de l'activer ou non, mais comme la possibilité pour le fabricant de fournir ou non cette option, sans que cela n'ait d'incidence sur la déclaration de conformité.

6 Cas d'utilisation généraux de l'IoT et acteurs de l'IoT

Le présent paragraphe décrit les cas d'utilisation généraux de l'IoT, les acteurs de l'IoT, ainsi que les relations entre les cas d'utilisation généraux et les acteurs de l'IoT. Un acteur de l'IoT est défini dans la présente Recommandation comme une entité extérieure à l'IoT et interagissant avec l'IoT.

6.1 Cas d'utilisation généraux

Les cas d'utilisation généraux découlent de la définition de l'IoT contenue dans la Recommandation [UIT-T Y.2060].

D'après la définition de l'IoT indiquée dans la Recommandation [UIT-T Y.2060], l'IoT permet "de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution". Il en découle que l'IoT assure l'interconnexion d'objets, en vue de détecter ou d'actionner des objets et de fournir des services évolués, ce qui met en avant les cas d'utilisation généraux suivants: "détection ou actionnement par l'IoT" et "fourniture de services par l'IoT".

D'après la définition de l'IoT telle qu'elle est formulée dans la Recommandation [UIT-T Y.2060], "en exploitant les capacités d'identification, d'acquisition de données, de traitement et de communication, l'IoT tire pleinement parti des objets pour offrir des services à toutes sortes d'applications, tout en garantissant le respect des exigences de sécurité et de confidentialité". Il en découle que les capacités d'acquisition et de traitement de données peuvent être regroupées dans la catégorie des capacités de gestion de données et que la protection de la confidentialité doit être assurée. On peut déduire de ces considérations les cas d'utilisation généraux suivants: "gestion de données par l'IoT" et "protection de la confidentialité par l'IoT".

La Figure 6-1 illustre le modèle des cas d'utilisation généraux de l'IoT, décrit au moyen du langage de modélisation unifié (UML). Pour de plus amples informations concernant ce langage, voir [b-UML]. Ce modèle est constitué de quatre cas d'utilisation généraux: détection ou actionnement par l'IoT, gestion de données par l'IoT, fournitures de services par l'IoT et protection de la confidentialité par l'IoT.

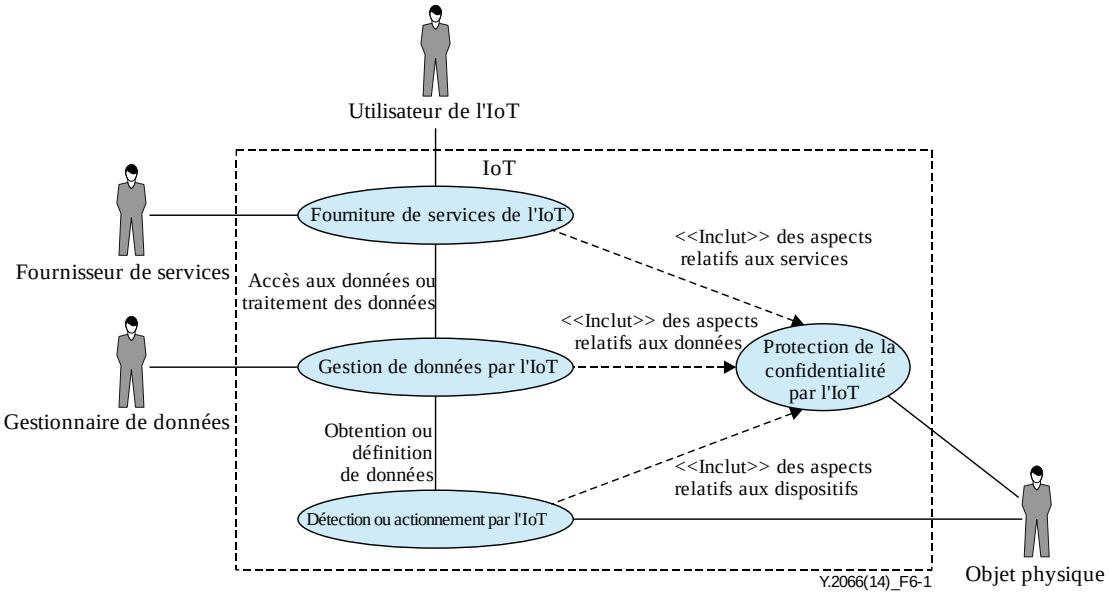

Figure 6-1 – Modèle des cas d'utilisation généraux de l'IoT

NOTE 1 – Dans [b-UML], un cas d'utilisation est défini comme une tâche élémentaire efficace d'un système. Il peut décrire un comportement observable par des entités à l'extérieur du système. Les cas d'utilisation peuvent être utilisés pour déterminer les exigences applicables à un système. Un modèle de cas d'utilisation (combinaison de tâches élémentaires) peut mettre en évidence les interactions entre le système et les entités extérieures au système. Ces entités extérieures sont appelées "acteurs" en langage UML. Par conséquent, l'IoT est le système modélisé en langage UML et les "acteurs de l'IoT" sont les entités extérieures à l'IoT qui interagissent avec l'IoT.

NOTE 2 – Certains cas d'utilisation découlant d'applications IoT (les cas d'utilisation représentatifs décrits dans l'Appendice I) peuvent être décomposés en cas d'utilisation généraux, comme décrits dans les paragraphes 6.1.1 à 6.1.4, afin de faciliter la définition des exigences fonctionnelles correspondant aux acteurs de l'IoT. Par exemple, le cas d'utilisation "surveillance vidéo", décrit au paragraphe I.1, peut être décomposé comme suit: acquisition vidéo (détection ou actionnement par l'IoT), transmission et stockage vidéo (gestion de données par l'IoT) et lecture et analyse vidéo (fourniture de services par l'IoT). Ces cas d'utilisation peuvent être utilisés pour définir les exigences fonctionnelles à partir des différents acteurs de la surveillance vidéo, notamment en matière de synchronisation temporelle pour assurer la transmission vidéo en temps réel et de stockage virtuel pour assurer le stockage d'une grande quantité de vidéos, provenant du fonctionnement continu de caméras vidéo.

6.1.1 Cas d'utilisation "détection ou actionnement par l'IoT"

Le cas d'utilisation "détection ou actionnement par l'IoT" est un cas d'utilisation général pouvant être appliqué à de nombreux domaines d'application. Ce cas d'utilisation comprend des activités de connexion avec des objets physiques, de détection de l'état d'objets physiques ou d'actionnement d'objets physiques.

6.1.2 Cas d'utilisation "gestion de données par l'IoT"

Le cas d'utilisation "gestion de données par l'IoT" est un cas d'utilisation général pouvant être appliqué à de nombreux domaines d'application. Ce cas d'utilisation comprend des activités d'acquisition, de transfert, de stockage et de traitement des données des objets physiques.

6.1.3 Cas d'utilisation "fourniture de services par l'IoT"

Le cas d'utilisation "fourniture de services par l'IoT" est un cas d'utilisation général pouvant être appliqué à de nombreux domaines d'application. Ce cas d'utilisation comprend des activités de fourniture de services pour les fournisseurs de services et d'utilisation de services pour les utilisateurs de l'IoT.

6.1.4 Cas d'utilisation "protection de la confidentialité par l'IoT"

Le cas d'utilisation "protection de la confidentialité par l'IoT" est un cas d'utilisation général pouvant être appliqué à de nombreux domaines d'application. Ce cas d'utilisation comprend des activités de sécurisation et de dissimulation des informations privées des objets physiques.

6.1.5 Relations entre les cas d'utilisation généraux

Les relations entre les cas d'utilisation généraux définis sont indiquées dans la Figure 6-1. Le cas d'utilisation "gestion de données par l'IoT" est lié aux cas d'utilisation "détection ou actionnement par l'IoT" et "fourniture de services par l'IoT". Le cas d'utilisation "protection de la confidentialité par l'IoT" est lié à tous les autres cas d'utilisation.

6.2 Acteurs de l'IoT

Les cas d'utilisation sont utilisés pour déterminer les exigences applicables à un système (voir [b-UML]). Chaque cas d'utilisation comprend les exigences fonctionnelles des acteurs impliqués.

D'après le modèle des cas d'utilisation généraux de l'IoT, illustré dans la Figure 6-1, quatre acteurs de l'IoT peuvent être définis: l'objet physique, le gestionnaire de données, le fournisseur de services et l'utilisateur de l'IoT. Ces quatre acteurs de l'IoT, décrits dans le présent paragraphe, sont des entités situées à l'extérieur de l'IoT et caractérisées selon le point de vue des exigences. Ils sont différents des rôles opérationnels décrits dans l'Appendice I de la Recommandation [UIT-T Y.2060], caractérisés selon un point de vue opérationnel.

NOTE 1 – L'acteur "objet physique" décrit dans la présente Recommandation correspond à l'objet physique tel que décrit dans la Recommandation [UIT-T Y.2060]. D'après le modèle des cas d'utilisation généraux de l'IoT, l'acteur qui correspondrait à l'objet virtuel tel que décrit dans la Recommandation [UIT-T Y.2060] n'est pas pris en compte dans la présente Recommandation, étant donné qu'un objet virtuel est une entité faisant partie intégrante de l'IoT.

NOTE 2 – Les correspondances entre les acteurs de l'IoT décrits dans la présente Recommandation et les rôles décrits dans l'Appendice I de la Recommandation [UIT-T Y.2060] sont les suivantes:

- L'acteur "utilisateur de l'IoT" correspond au rôle "client d'applications".
- L'acteur "fournisseur de services" correspond aux rôles "fournisseur d'applications", "fournisseur de plate-forme" et "fournisseur de réseau".
- L'acteur "gestionnaire de données" correspond au rôle "fournisseur d'applications" dans le cas où les applications fournies comprennent des fonctionnalités de gestion de données. Il peut aussi correspondre au rôle "fournisseur de dispositifs" dans le cas où les dispositifs fournis comprennent des fonctionnalités de gestion de données.

6.2.1 Acteur "objet physique"

L'acteur "objet physique" est un acteur de l'IoT doté d'un identifiant unique dans le monde physique. Un "objet physique" interagit avec l'IoT via des activités de détection ou d'actionnement.

NOTE – L'acteur "objet physique" peut être divisé en deux catégories, à savoir "objet artificiel" et "objet naturel". Un objet artificiel est un objet physique produit par l'homme et pouvant être identifié par un numéro de série. Un objet naturel est un objet physique généré par la nature et pouvant être identifié, par exemple, par sa catégorie et l'heure et le lieu auxquels il a été généré. La détection des objets naturels peut constituer un enjeu difficile dans le développement de l'IoT.

Il convient de noter que, dans les paragraphes suivants de la présente Recommandation, le terme "objet" désigne un "objet physique".

6.2.2 Acteur "gestionnaire de données"

L'acteur "gestionnaire de données" est un acteur de l'IoT chargé d'administrer l'acquisition, le stockage, le transfert et le traitement des données de l'IoT pour répondre aux besoins liés à la prestation de services IoT.

NOTE – L'acteur "gestionnaire de données" peut être divisé en deux catégories, à savoir "gestionnaire de données" humain et "gestionnaire de données" machine. Un "gestionnaire de données" humain réalise la gestion des données de l'IoT manuellement, tandis qu'un "gestionnaire de données" machine opère de manière automatique. Ces deux catégories de l'acteur "gestionnaire de données" sont associées à différents cas d'utilisation du type "gestion de données par l'IoT".

6.2.3 Acteur "fournisseur de services"

L'acteur "fournisseur de services" est un acteur de l'IoT fournissant tout type de services en rapport avec les objets, notamment des services de suivi, de localisation et de découverte de services.

NOTE – L'acteur "fournisseur de services" peut être divisé en deux catégories, à savoir "fournisseur de services" communs, qui fournit des services indépendants du domaine d'application, et "fournisseur de services" orientés application, qui fournit des applications conçues pour des domaines d'application particuliers.

6.2.4 Acteur "utilisateur de l'IoT"

L'acteur "utilisateur de l'IoT" est un acteur de l'IoT utilisant tout type de services en rapport avec les objets, notamment des services de suivi, de localisation et de découverte de services.

7 Domaines importants à considérer du point de vue des exigences

Il convient de prendre en considération plusieurs domaines importants pour la détermination des exigences relatives à l'IoT. Compte tenu des caractéristiques de l'IoT et des exigences de haut niveau figurant dans la Recommandation [UIT-T Y.2060], ainsi que des résultats des recherches des secteurs publics et universitaires portant sur l'IoT (par exemple [b-IoT-A D6.2]), les paragraphes ci-après décrivent des domaines importants qu'il convient de prendre en compte du point de vue des exigences.

7.1 Aspects liés à la mise en œuvre et à l'exploitation

Les aspects liés à la mise en œuvre et à l'exploitation de l'IoT constituent un domaine important qu'il convient de prendre en considération, par exemple pour assurer l'interopérabilité entre les mises en œuvre hétérogènes de l'IoT et garantir l'évolutivité suffisante pour la prise en charge d'un grand nombre de dispositifs connectés et une grande disponibilité pour la réalisation d'opérations automatiques au sein de l'IoT.

7.2 Connectivité ubiquitaire

Pour assurer la connectivité entre les objets et l'IoT, il est nécessaire de prendre en considération la connectivité ubiquitaire. Les capacités de connectivité doivent être indépendantes du domaine d'application et l'intégration de technologies de communication hétérogènes doit être prise en charge.

7.3 Intelligence de bout en bout

Il est nécessaire de prendre en considération l'intelligence de bout en bout, en particulier en ce qui concerne "l'intelligence des communications" et "l'intelligence des services", par exemple en vue de fournir des services sans intervention humaine. Cela comprend la prise en considération des communications fondées sur la localisation et des communications contextuelles (qui peuvent être considérées comme des communications intelligentes), des services prenant en compte le contenu et des services prenant en compte le contexte (qui peuvent être considérés comme des services

intelligents), ainsi que des services d'autoconfiguration, d'autorétablissement, d'auto-optimisation et d'autoprotection (qui peuvent être considérés comme d'autres services intelligents, regroupés sous le terme de services autonomes [UIT-T Y.2060]).

7.4 Synchronisation temporelle

Pour préserver la synchronisation temporelle entre les opérations des objets interconnectés lors de l'utilisation de capacités de communication et de service, il est nécessaire de prendre en considération la synchronisation temporelle.

7.5 Connectivité du corps humain

Pour fournir des capacités de communication liées au corps humain conformes avec les réglementations et législations en la matière, une attention particulière doit être accordée aux exigences relatives à la connectivité du corps humain. Il est nécessaire de spécifier une qualité de service particulière, de quantifier le niveau de fiabilité et de garantir la protection de la confidentialité.

7.6 Quantité importante des données des objets

Étant donné qu'un grand nombre de dispositifs seront connectés à l'IoT, un grand volume de données sera transmis depuis les objets vers l'IoT – on utilise généralement le terme "mégadonnées" pour désigner un volume important de données présentant une grande variété et une vitesse élevée. Pour permettre de classer, transférer, stocker, traiter, valider et interroger les mégadonnées en temps voulu, conformément à la demande des utilisateurs ou applications de l'IoT, il convient de prendre en considération l'évolutivité des ressources telles que la largeur de bande de communication ainsi que la capacité de stockage et de traitement.

7.7 Protection de la confidentialité liée aux objets

Les données provenant des objets peuvent contenir des informations confidentielles au sujet des propriétaires ou des utilisateurs des objets. Lorsque la confidentialité des données n'est pas respectée, celles-ci peuvent être utilisées pour localiser ou tracer les propriétaires ou les utilisateurs des objets. Il convient de prendre en considération la protection de la confidentialité lors de l'acquisition, du transfert, du stockage, de la validation et du traitement des données des objets. La protection de la confidentialité ne doit pas être utilisée pour faire obstacle à la validation des données des objets.

8 Exigences communes relatives à l'IoT

Les exigences communes relatives à l'IoT définies dans la présente Recommandation sont des exigences techniques et sont indépendantes de tout domaine d'application particulier. Les exigences concernant les protocoles et les interfaces (par exemple celles portant sur les aspects de l'IoT relatifs à la commande et à la gestion) sortent du cadre de la présente Recommandation.

8.1 Catégories des exigences communes relatives à l'IoT

Dans la présente Recommandation, on distingue deux types d'exigences communes relatives à l'IoT: les exigences non fonctionnelles et les exigences fonctionnelles.

Les exigences non fonctionnelles relatives à l'IoT renvoient aux exigences portant directement sur la mise en œuvre et l'exploitation de l'IoT.

Les exigences fonctionnelles relatives à l'IoT renvoient aux exigences portant sur les acteurs de l'IoT, autrement dit les entités extérieures à l'IoT qui interagissent avec l'IoT. Les exigences fonctionnelles relatives à l'IoT définies dans la présente Recommandation sont classées selon les catégories suivantes:

– exigences relatives à la prise en charge d'applications
– exigences relatives aux services
– exigences relatives aux communications
– exigences relatives aux dispositifs
– exigences relatives à la gestion de données
– exigences relatives à la sécurité et à la protection de la confidentialité.

Toutes les exigences définies dans les paragraphes ci-après sont listées et numérotées dans l'Annexe A. Dans ce qui suit, les numéros des exigences, tels qu'ils figurent dans l'Annexe A, sont indiqués entre crochets "[ ]" à la fin de chaque paragraphe décrivant la ou les exigences correspondantes.

8.2 Exigences non fonctionnelles

Les exigences de cette catégorie ne sont liées à aucun acteur de l'IoT et ne découlent pas des cas d'utilisation généraux de l'IoT décrits au paragraphe 6.

8.2.1 Interopérabilité

Il est nécessaire de garantir l'interopérabilité entre les mises en œuvre hétérogènes de l'IoT [N1].

NOTE – Pour assurer l'interopérabilité dans l'IoT, il est nécessaire d'établir un modèle d'architecture de référence normalisé pour l'IoT.

8.2.2 Évolutivité

Il est nécessaire de prendre en charge l'évolutivité dans l'IoT, afin qu'un grand nombre de dispositifs, d'applications et d'utilisateurs puissent être gérés [N2].

NOTE 1 – Pour respecter l'exigence relative à l'évolutivité portant sur la gestion d'un grand nombre de dispositifs, il est nécessaire qu'un grand nombre de données (mégadonnées) puissent être gérées dans l'IoT.

NOTE 2 – Pour respecter l'exigence relative à l'évolutivité portant sur la gestion d'un grand nombre d'applications et d'utilisateurs, il est nécessaire de disposer d'une grande quantité de ressources de traitement de de stockage. Cette exigence peut être respectée au moyen de l'intégration dans l'IoT de technologies de l'informatique en nuage.

NOTE 3 – Il convient de tenir compte du principe d'équité pour la gestion d'un grand nombre de dispositifs, d'applications et d'utilisateurs.

8.2.3 Fiabilité

Il est nécessaire d'assurer la fiabilité des capacités de l'IoT, par exemple la fiabilité des capacités de l'IoT relatives aux communications, aux services et à la gestion de données [N3].

NOTE – Il convient de tenir compte de la résilience lorsqu'il s'agit d'assurer la fiabilité.

8.2.4 Grande disponibilité

Une grande disponibilité est nécessaire pour la fourniture de services, la gestion de données, la communication, la détection et l'actionnement des objets de l'IoT [N4].

8.2.5 Adaptabilité

L'adaptabilité de l'IoT aux nouvelles technologies qui verront le jour dans l'avenir est nécessaire [N5].

NOTE – Les normes techniques utilisées dans le domaine de l'IoT devraient imposer des contraintes minimales en matière d'adaptabilité aux nouvelles technologies.

8.2.6 Facilité de gestion

L'IoT doit pouvoir être géré, afin de garantir un fonctionnement normal. En règle générale, le fonctionnement de l'IoT est automatique et ne nécessite pas d'intervention humaine. Néanmoins, les processus régissant ce fonctionnement doivent pouvoir être gérés [N6].

NOTE 1 – Il convient de tenir compte de la gestion des dispositifs dans l'IoT, notamment la gestion des états des dispositifs, la gestion de la connectivité des dispositifs, la gestion de la consommation d'énergie, etc. Les contraintes pesant sur les ressources des dispositifs, telles que celles relatives à l'énergie, à la mémoire et à la largeur de bande, doivent être prises en compte dans la gestion des dispositifs.

NOTE 2 – Il convient de tenir compte de la gestion automatique des défaillances dans l'IoT, notamment le compte rendu préventif des défaillances, diagnostic des défaillances, le retour à la normal, etc.

NOTE 3 – Il convient de tenir compte de la gestion de la configuration automatique dans l'IoT, notamment la configuration automatique des paramètres des dispositifs.

8.3 Exigences relatives à la prise en charge d'applications

Les exigences relatives à la prise en charge d'applications renvoient aux exigences fonctionnelles portant sur la mise au point d'applications IoT dans différents domaines d'application. Ces exigences concernent uniquement l'acteur "fournisseur de services".

8.3.1 Interfaces de programmation

Des interfaces de programmation normalisées sont nécessaires, afin de fournir un accès ouvert aux capacités de prise en charge d'applications [A1].

NOTE – Les interfaces de programmation permettent de prendre en charge les applications IoT de façon programmable.

8.3.2 Gestion des groupes

La gestion des groupes doit être prise en charge dans l'IoT, y compris l'affichage, la création, la modification et la suppression de groupes IoT, ainsi que l'affichage, l'ajout, la modification et la suppression de membres de groupes IoT [A2].

NOTE – Un groupe IoT peut contenir des utilisateurs de l'IoT et/ou des dispositifs IoT.

8.3.3 Synchronisation temporelle

Une synchronisation temporelle fiable est nécessaire, afin de pouvoir assurer l'horodatage global dans l'IoT [A3].

NOTE – L'horodatage permet la fourniture de services à temps critique de manière sûre et sécurisée.

8.3.4 Collaboration

La collaboration est nécessaire entre les services ou entre les dispositifs qui accèdent aux applications IoT avec un même objectif, afin que l'IoT puisse permettre la collaboration autonome entre ces services ou dispositifs, sur la base de cet objectif [A4].

NOTE – La collaboration entre les dispositifs qui accèdent aux applications IoT doit être activée par les dispositifs eux-mêmes, afin qu'une collaboration évolutive à commande répartie entre les dispositifs concernés puisse être assurée dans l'IoT.

8.3.5 Gestion des utilisateurs

La gestion des utilisateurs est nécessaire, notamment la création, l'authentification, l'autorisation et la comptabilisation des utilisateurs de l'IoT [A5].

8.3.6 Comptabilisation de l'utilisation des ressources

La comptabilisation de l'utilisation des ressources de l'IoT est nécessaire et doit être réalisée pour chaque application considérée individuellement [A6].

8.4 Exigences relatives aux services

Les exigences présentées dans cette section concernent les acteurs "fournisseur de services", "utilisateur de l'IoT" et "objet".

NOTE – Conformément à la définition générale de "service" comme un ensemble de fonctions et de capacités offertes à un utilisateur par un fournisseur [UIT-T Y.2091], les exigences relatives aux services concernent tant l'acteur "utilisateur de l'IoT" que l'acteur "fournisseur de services". Cela n'exclut toutefois pas le cas où un service est directement offert à l'acteur "objet".

8.4.1 Hiérarchisation des services

La hiérarchisation des services est nécessaire pour répondre aux exigences relatives aux services, propres aux différents groupes d'utilisateurs de l'IoT [S1].

NOTE – La différenciation des services doit être prise en charge, afin que l'IoT puisse respecter différents accords de niveau de service (SLA).

8.4.2 Services fondés sur la sémantique

Les services fondés sur la sémantique sont nécessaires dans l'IoT, afin de permettre la prise en charge de la fourniture autonome de services. Les mécanismes de mise en œuvre de services fondés sur la sémantique incluent l'annotation sémantique des services, l'accès sémantique aux services ainsi que l'échange sémantique entre les services [S2].

NOTE – L'annotation sémantique des services peut permettre la description sémantique des services. L'accès sémantique aux services peut être utilisé pour accéder aux services à travers des interfaces sémantiques. L'échange sémantique entre les services peut permettre de transmettre et d'échanger des informations sémantiques entre les services, afin de prendre en charge la création automatique de nouveaux services.

8.4.3 Composition de services

La composition de services est nécessaire pour prendre en charge la création flexible de services dans l'IoT [S3].

NOTE 1 – Les services primaires constituent un ensemble d'opérations de base qui ne peuvent pas répondre directement aux exigences applicables aux applications IoT. La composition de services est l'une des méthodes de création de services pouvant être utilisées pour créer automatiquement des services plus complexes à partir des services primaires, afin de satisfaire l'ensemble des diverses exigences auxquelles sont soumises les applications IoT.

NOTE 2 – Les techniques de fourniture de services flexibles existantes, telles que les plates-formes de fourniture de services (SDP), peuvent notamment assurer le respect des exigences relatives à la composition de services.

8.4.4 Services de mobilité

Des services de mobilité sont nécessaires pour que l'IoT puisse prendre en charge la mobilité des services, des utilisateurs et des dispositifs, du point de vue de la fourniture de services. Par exemple, la fourniture de services n'est pas soumise à des contraintes liées à l'emplacement depuis lequel l'accès au service est réalisé lorsque la mobilité des services est prise en charge [S4].

8.4.5 Services de connectivité du corps humain fiables et sécurisés

Une fiabilité et une sécurité élevées sont nécessaires lorsque des services de connectivité du corps humain sont fournis [S5].

NOTE – Les exigences juridiques et réglementaires concernant ces services peuvent varier d'un pays à l'autre.

8.4.6 Services autonomes

Des services autonomes sont nécessaires, afin que l'IoT puisse permettre l'acquisition, le transfert et le traitement automatiques des données des objets, sur la base de règles établies par les fournisseurs de services ou personnalisées par les utilisateurs de l'IoT [S6].

NOTE – Les commandes centralisée et décentralisée des services autonomes doivent toutes les deux être prises en charge, afin que l'IoT puisse permettre la réalisation d'activités automatisées centralisées ou décentralisées.

Des services fondés sur la localisation et des services prenant en compte le contexte sont nécessaires, afin que l'IoT puisse permettre le fonctionnement de services flexibles, personnalisés par l'utilisateur et autonomes, fondés sur les informations de localisation des objets et/ou des utilisateurs ainsi que sur leur contexte [S7].

8.4.7 Gestion des services

La gestion des services est nécessaire pour que la fourniture de services soit assurée avec une grande disponibilité et de façon très fiable [S8].

NOTE – La gestion des services comprend, entre autres, la gestion du cycle de vie des services et la vérification de l'intégrité des services. La gestion du cycle de vie des services peut contribuer à accroître la disponibilité des services et la vérification de l'intégrité des services peut participer au renforcement de leur fiabilité.

8.4.8 Services de découverte

Des services de découverte sont nécessaires pour que des utilisateurs, services, dispositifs et données des objets de l'IoT puissent être découverts par les fournisseurs de services ou les utilisateurs de l'IoT [S9].

NOTE – Un fournisseur de services ou un utilisateur de l'IoT peut découvrir des utilisateurs, services, dispositifs ou données des objets de l'IoT spécifiques, en fonction de certains critères, portant par exemple sur les informations de localisation, le type de dispositifs, etc.

8.4.9 Prise en charge de l'abonnement aux services

La prise en charge de l'abonnement aux services est nécessaire, afin que l'IoT puisse permettre aux utilisateurs de l'IoT de s'abonner aux services dont ils ont besoin et aux données des objets associées [S10].

8.4.10 Nommage et adressage

Il est nécessaire d'utiliser une procédure de nommage et d'adressage des objets et des services normalisée [S11].

8.4.11 Stockage et traitement virtuels

Des capacités de stockage et de traitement virtuels sont nécessaires pour qu'une grande quantité de données (mégadonnées) puissent être stockées et traitées [S12].

8.5 Exigences relatives aux communications

Les exigences relatives aux communications renvoient aux exigences fonctionnelles portant sur l'échange de messages entre les acteurs "utilisateur de l'IoT", "fournisseur de services", "gestionnaire de données" et "objet". Ces exigences concernent tous les acteurs de l'IoT.

8.5.1 Modes de communication

Les modes de communication entre les dispositifs ou entre les utilisateurs de l'IoT ci-après doivent être pris en charge: mode fondé sur des événements, mode périodique et mode automatique [C1].

La prise en charge du mode de communication monodiffusion est nécessaire (par exemple pour les communications entre les utilisateurs ou les dispositifs de l'IoT). La prise en charge des modes de communication multidiffusion, radiodiffusion et unidiffusion est nécessaire, afin que l'IoT puisse fournir divers services de communication au sein d'un groupe d'utilisateurs ou de dispositifs de l'IoT (par exemple pour assurer la collaboration entre les utilisateurs ou les dispositifs de l'IoT) [C2].

NOTE – Il est recommandé que les modes de communication entre les dispositifs ou entre les utilisateurs de l'IoT susmentionnés (mode basé sur des événements, mode périodique et mode automatique) soient pris en charge tout en préservant la qualité de fonctionnement du réseau au moyen de mécanismes permettant d'éviter que des encombrements du trafic ne surviennent.

La prise en charge des communications déclenchées par les dispositifs est nécessaire pour satisfaire les exigences relatives aux communications automatiques [C3].

8.5.2 Contrôle des communications

Le contrôle d'erreur pour les communications doit être pris en charge pour que l'IoT soit en mesure, par exemple, de faire face aux brouillages entre les dispositifs [C4].

Les communications à temps critique doivent être prises en charge, de sorte que l'IoT puisse assurer la gestion et la transmission de messages à temps critique [C5].

8.5.3 Communications intelligentes

Les exigences relatives aux communications intelligentes comprennent des exigences concernant la réseautique autonome [UIT-T Y.2060], les communications prenant en compte le contenu et les communications fondées sur la localisation.

La réseautique autonome est nécessaire dans l'IoT pour que les capacités d'autoconfiguration, d'autorétablissement, d'auto-optimisation et d'autoprotection au niveau du réseau soient prises en charge, afin de pouvoir s'adapter à des domaines d'application et à des environnements de communications différents ainsi qu'à des dispositifs nombreux et variés [C6].

Les communications prenant en compte le contenu sont nécessaires, de sorte que, par exemple, l'IoT puisse prendre en charge la sélection du trajet et le routage des communications sur la base du contenu [C7].

Les communications fondées sur la localisation sont nécessaires, afin que l'IoT puisse prendre en charge les interactions fondées sur la localisation entre les acteurs de l'IoT [C8].

NOTE – L'acquisition et le traçage des informations de localisation doivent être réalisés de façon automatique.

8.5.4 Prise en charge des communications hétérogènes

Les communications peuvent avoir lieu dans la couche dispositif (voir [UIT-T Y.2060]) à l'aide de différentes technologies filaires ou hertziennes, par exemple à l'aide d'un bus gestionnaire de réseau de communication (CAN), du protocole ZigBee, du Bluetooth, du WiFi, etc. La prise en charge des technologies de communications hétérogènes relatives aux dispositifs est nécessaire [C9].

Les communications peuvent avoir lieu dans la couche réseau (voir [UIT-T Y.2060]) à l'aide de différentes technologies, par exemple les réseaux de deuxième génération/troisième génération (2G/3G), les réseaux LTE, les réseaux Ethernet, les lignes d'abonné numérique (DSL), etc.

La prise en charge des technologies de communications hétérogènes relatives aux réseaux est nécessaire [C10].

8.6 Exigences relatives aux dispositifs

Les exigences relatives aux dispositifs renvoient aux exigences fonctionnelles portant sur les équipements connectés avec des objets. Ces exigences concernent les acteurs "utilisateur de l'IoT" et "objet".

8.6.1 Connectivité des objets

L'IoT doit prendre en charge l'établissement de la connectivité entre un objet et l'IoT sur la base de l'identifiant de l'objet [D1].

NOTE – Les identifiants hétérogènes des objets doivent être traités de manière uniforme (voir [UIT-T Y.2060]).

8.6.2 Commande et configuration des dispositifs

La prise en charge de la surveillance, de la commande et de la configuration à distance des dispositifs est nécessaire, afin d'accroître la facilité de gestion des dispositifs dans l'IoT [D2].

L'IoT doit offrir une capacité de connexion immédiate (*plug and play*), afin de permettre de générer, composer ou acquérir de manière instantanée des configurations fondées sur la sémantique, de sorte que les objets soient parfaitement intégrés aux applications et coopèrent avec elles sans discontinuité apparente et que les exigences propres à ces applications soient respectées (voir [UIT-T Y.2060]) [D3].

8.6.3 Surveillance des objets

La notification automatique du statut des objets et de ses changements est nécessaire, afin d'assurer la surveillance des objets en temps voulu [D4].

8.6.4 Mobilité des dispositifs

La mobilité des dispositifs est nécessaire, de sorte que l'IoT puisse prendre en charge la mobilité des objets connectés avec des dispositifs [D5].

8.6.5 Vérification de l'intégrité des dispositifs

La vérification de l'intégrité des dispositifs est nécessaire, afin de contribuer à assurer une grande disponibilité des dispositifs [D6].

8.7 Exigences relatives à la gestion de données

Les exigences relatives à la gestion de données renvoient aux exigences fonctionnelles portant sur le stockage, l'agrégation, le transfert et le traitement des données de l'IoT. Ces exigences concernent les acteurs "gestionnaire de données" et "utilisateur de l'IoT".

8.7.1 Stockage des données

Le stockage des données des objets fondé sur des règles et des politiques définies au préalable doit être pris en charge [DM1].

8.7.2 Traitement des données

La fusion et l'exploration des données fondées sur des règles et des politiques définies au préalable doivent être prises en charge [DM2].

8.7.3 Interrogation des données

L'interrogation de l'historique des données des objets stockées doit être prise en charge, afin que l'IoT puisse fournir l'historique des informations concernant les objets [DM3].

8.7.4 Contrôle de l'accès aux données

Le contrôle de l'accès aux données par leur propriétaire doit être pris en charge dans l'IoT, afin que les utilisateurs de l'IoT aient la possibilité de contrôler la visibilité de leurs données par d'autres utilisateurs de l'IoT [DM4].

8.7.5 Échange des données

L'échange des données avec des entités à l'extérieur de l'IoT doit être pris en charge, afin que l'IoT soit en mesure de donner l'accès à des sources de données externes, par exemple des bases de données relatives à la santé situées à l'extérieur de l'IoT [DM5].

8.7.6 Validation des données

La vérification de l'intégrité des données des objets et la gestion de leur cycle de vie doivent être prises en charge, afin que l'IoT soit en mesure d'assurer une disponibilité et une fiabilité élevées pour les données des objets [DM6].

8.7.7 Annotation sémantique des données des objets et accès sémantique à ces données

L'annotation sémantique des données des objets est nécessaire. L'accès sémantique aux données des objets est nécessaire, afin que les objets puissent être interrogés de manière automatique [DM7].

8.7.8 Stockage, transfert et agrégation sémantiques des données des objets

Le stockage, le transfert et l'agrégation sémantiques des données des objets sont nécessaires, afin que le stockage, le transfert et l'agrégation des données des objets puissent être réalisés de manière automatique, conformément aux exigences des utilisateurs ou des applications de l'IoT [DM8].

8.8 Exigences relatives à la sécurité et à la protection de la confidentialité.

Les exigences relatives à la sécurité et la protection de la confidentialité renvoient aux exigences fonctionnelles à respecter lors de l'acquisition, du stockage, du transfert, de l'agrégation et du traitement des données des objets, ainsi qu'à la fourniture de services faisant intervenir des objets. Ces exigences concernent tous les acteurs de l'IoT.

8.8.1 Sécurité des communications

Une capacité de communication sécurisée et sûre avec protection de la confidentialité est nécessaire, afin de pouvoir interdire l'accès non autorisé au contenu des données, garantir l'intégrité des données et protéger le contenu des données à caractère confidentiel lors de la transmission ou du transfert des données dans l'IoT [SP1].

8.8.2 Sécurité de la gestion de données

Une capacité de gestion de données sécurisée et sûre avec protection de la confidentialité est nécessaire, afin de pouvoir interdire l'accès non autorisé au contenu des données, garantir l'intégrité des données et protéger le contenu des données à caractère confidentiel lors du stockage ou du traitement des données dans l'IoT [SP2].

8.8.3 Sécurité de la fourniture de services

Une capacité de fourniture de services sécurisée et sûre avec protection de la confidentialité est nécessaire, afin de pouvoir interdire l'accès non autorisé au service et la fourniture de services frauduleux et protéger les informations à caractère confidentiel des utilisateurs de l'IoT [SP3].

8.8.4 Intégration des politiques et des techniques de sécurité

Il est nécessaire de pouvoir intégrer différentes politiques et techniques de sécurité, afin de garantir des contrôles de sécurité cohérents sur les différents dispositifs et réseaux utilisateurs dans l'IoT [SP4].

8.8.5 Authentification et autorisation mutuelles

Avant qu'un dispositif (ou un utilisateur de l'IoT) puisse accéder à l'IoT, une authentification et une autorisation mutuelles entre le dispositif (ou l'utilisateur de l'IoT) et l'IoT doivent avoir lieu selon les politiques de sécurité définies au préalable [SP5].

8.8.6 Audit de sécurité

Les audits de sécurité doivent être pris en charge dans l'IoT. L'accès aux données et les tentatives d'accès aux applications IoT doivent être parfaitement transparents, traçables et reproductibles, conformément aux réglementations et législations pertinentes. En particulier, l'IoT doit prendre en charge les audits de sécurité concernant la transmission, le stockage et le traitement des données, et l'accès aux données par les applications [SP6].

Annexe A

Liste des exigences communes relatives à l'IoT

(Cette annexe fait partie intégrante de la présente Recommandation.)

Les exigences décrites au paragraphe 8 "Exigences communes relatives à l'IoT" sont listées et numérotées dans le tableau suivant.

Numéro de l'exigence	Catégorie de l'exigence	Description de l'exigence	Résumé de l'exigence
N1	Non fonctionnelle	Il est nécessaire de garantir l'interopérabilité entre les mises en œuvre hétérogènes de l'IoT.	L'interopérabilité est nécessaire.
N2	Non fonctionnelle	Il est nécessaire de prendre en charge l'évolutivité dans l'IoT, afin qu'un grand nombre de dispositifs, d'applications et d'utilisateurs puissent être gérés.	L'évolutivité est nécessaire.
N3	Non fonctionnelle	Il est nécessaire d'assurer la fiabilité des capacités de l'IoT, par exemple la fiabilité des capacités de l'IoT relatives aux communications, aux services et à la gestion de données.	La fiabilité est nécessaire.
N4	Non fonctionnelle	Une grande disponibilité est nécessaire pour la fourniture de services, la gestion de données, la communication, la détection et l'actionnement des objets de l'IoT.	Une grande disponibilité est nécessaire.
N5	Non fonctionnelle	L'adaptabilité de l'IoT aux nouvelles technologies qui verront le jour dans l'avenir est nécessaire.	L'adaptabilité est nécessaire.
N6	Non fonctionnelle	L'IoT doit pouvoir être géré, afin de garantir un fonctionnement normal.	La facilité de gestion est nécessaire.
A1	Prise en charge d'applications	Des interfaces de programmation doivent être normalisées, afin de fournir un accès ouvert aux capacités de prise en charge d'applications.	Des interfaces de programmation normalisées sont nécessaires.
A2	Prise en charge d'applications	La gestion des groupes doit être prise en charge dans l'IoT, y compris l'affichage, la création, la modification et la suppression de groupes IoT, ainsi que l'affichage, l'ajout, la modification et la suppression de membres de groupes IoT.	La gestion des groupes est nécessaire.
A3	Prise en charge d'applications	Une synchronisation temporelle fiable est nécessaire, afin de pouvoir assurer l'horodatage global dans l'IoT.	Une synchronisation temporelle fiable est nécessaire.
A4	Prise en charge d'applications	La collaboration est nécessaire entre les services ou entre les dispositifs qui accèdent aux applications IoT avec un même objectif.	La collaboration est nécessaire.

Numéro de l'exigence	Catégorie de l'exigence	Description de l'exigence	Résumé de l'exigence
A5	Prise en charge d'applications	La gestion des utilisateurs est nécessaire, notamment la création, l'authentification, l'autorisation et la comptabilisation des utilisateurs de l'IoT.	La gestion des utilisateurs est nécessaire.
A6	Prise en charge d'applications	La comptabilisation de l'utilisation des ressources de l'IoT est nécessaire et doit être réalisée pour chaque application considérée individuellement.	La comptabilisation de l'utilisation des ressources est nécessaire.
S1	Services	La hiérarchisation des services est nécessaire pour répondre aux exigences relatives aux services, applicables aux différents groupes d'utilisateurs de l'IoT.	La hiérarchisation des services est nécessaire.
S2	Services	Les services fondés sur la sémantique sont nécessaires dans l'IoT, afin de permettre la prise en charge de la fourniture autonome de services.	Les services fondés sur la sémantique sont nécessaires.
S3	Services	La composition de services est nécessaire pour prendre en charge la création flexible de services dans l'IoT.	La composition de services est nécessaire.
S4	Services	Des services de mobilité sont nécessaires pour que l'IoT puisse prendre en charge la mobilité des services, des utilisateurs et des dispositifs.	Des services de mobilité sont nécessaires.
S5	Services	Une fiabilité et une sécurité élevées sont nécessaires lorsque des services de connectivité du corps humain sont fournis.	Les services de connectivité du corps humain doivent être très fiables et sécurisés.
S6	Services	Des services autonomes sont nécessaires, afin que l'IoT puisse permettre l'acquisition, le transfert et le traitement automatiques des données des objets, sur la base de règles établies par les fournisseurs de services ou personnalisées par les utilisateurs de l'IoT.	Des services autonomes sont nécessaires.
S7	Services	Des services fondés sur la localisation et des services prenant en compte le contexte sont nécessaires, afin que l'IoT puisse permettre le fonctionnement de services flexibles, personnalisés par l'utilisateur et autonomes, fondés sur les informations de localisation des objets et/ou des utilisateurs ainsi que sur leur contexte.	Des services fondés sur la localisation et des services prenant en compte le contexte sont nécessaires.
S8	Services	La gestion des services est nécessaire pour que la fourniture de services soit assurée avec une grande disponibilité et de façon très fiable.	La gestion des services est nécessaire.

Numéro de l'exigence	Catégorie de l'exigence	Description de l'exigence	Résumé de l'exigence
S9	Services	Des services de découverte sont nécessaires pour que des utilisateurs, services, dispositifs et données des objets de l'IoT puissent être découverts par les fournisseurs de services ou les utilisateurs de l'IoT	Des services de découverte sont nécessaires.
S10	Services	La prise en charge de l'abonnement aux services est nécessaire, afin que l'IoT puisse permettre aux utilisateurs de l'IoT de s'abonner aux services dont ils ont besoin et aux données des objets associées.	La prise en charge de l'abonnement aux services est nécessaire.
S11	Services	Il est nécessaire d'utiliser une procédure de nommage et d'adressage des objets et des services normalisée.	Il est nécessaire d'utiliser une procédure de nommage et d'adressage normalisée.
S12	Services	Des capacités de stockage et de traitement virtuels sont nécessaires pour qu'une grande quantité de données (mégadonnées) puissent être stockées et traitées.	Des capacités de stockage et de traitement virtuels sont nécessaires.
C1	Communications	Les communications fondées sur des événements, périodiques et automatiques entre les dispositifs ou entre les utilisateurs de l'IoT doivent être prises en charge.	Les modes de communication ci-après doivent être pris en charge: mode fondé sur des événements, mode périodique et mode automatique.
C2	Communications	La prise en charge du mode de communication monodiffusion est nécessaire (par exemple pour les communications entre les utilisateurs ou les dispositifs de l'IoT). La prise en charge des modes de communication multidiffusion, radiodiffusion et unidiffusion est nécessaire, afin que l'IoT puisse fournir divers services de communication au sein d'un groupe d'utilisateurs ou de dispositifs de l'IoT (par exemple pour assurer la collaboration entre les utilisateurs ou les dispositifs de l'IoT).	La prise en charge des modes de communication monodiffusion, multidiffusion, radiodiffusion et unidiffusion est nécessaire.
C3	Communications	La prise en charge des communications déclenchées par les dispositifs est nécessaire pour satisfaire les exigences relatives aux communications automatiques.	La prise en charge des communications déclenchées par les dispositifs est nécessaire.
C4	Communications	Le contrôle d'erreur pour les communications est nécessaire pour que l'IoT soit en mesure, par exemple, de faire face aux brouillages entre les dispositifs.	Le contrôle d'erreur pour les communications doit être pris en charge.
C5	Communications	L'IoT doit pouvoir assurer la gestion et la transmission de messages à temps critique.	Les communications à temps critique doivent être prises en charge.

Numéro de l'exigence	Catégorie de l'exigence	Description de l'exigence	Résumé de l'exigence
C6	Communications	Les capacités d'autoconfiguration, d'autorétablissement, d'auto-optimisation et d'autoprotection au niveau du réseau doivent être prises en charge dans l'IoT.	La réseautique autonome est nécessaire.
C7	Communications	Les communications prenant en compte le contenu sont nécessaires, de sorte que, par exemple, l'IoT puisse prendre en charge la sélection du trajet et le routage des communications sur la base du contenu.	Les communications prenant en compte le contenu sont nécessaires.
C8	Communications	Les interactions entre les acteurs de l'IoT fondées sur la localisation doivent être prises en charge dans l'IoT.	Les communications fondées sur la localisation sont nécessaires.
C9	Communications	Les communications peuvent avoir lieu dans la couche dispositif [UIT-T Y.2060] à l'aide de différentes technologies filaires ou hertziennes, par exemple à l'aide d'un bus gestionnaire de réseau de communication (CAN), du protocole ZigBee, du Bluetooth, du WiFi, etc.	La prise en charge des technologies de communications hétérogènes relatives aux dispositifs est nécessaire.
C10	Communications	Les communications peuvent avoir lieu dans la couche réseau [UIT-T Y.2060] à l'aide de différentes technologies, par exemple les réseaux de deuxième génération/troisième génération (2G/3G), les réseaux LTE, les réseaux Ethernet, les lignes d'abonné numérique (DSL), etc.	La prise en charge des technologies de communications hétérogènes relatives aux réseaux est nécessaire.
D1	Dispositifs	L'IoT doit prendre en charge l'établissement de la connectivité entre un objet et l'IoT sur la base de l'identifiant de l'objet.	La connectivité entre un objet et l'IoT fondée sur l'identifiant est nécessaire.
D2	Dispositifs	La prise en charge de la surveillance, de la commande et de la configuration à distance des dispositifs est nécessaire, afin d'accroître la facilité de gestion des dispositifs dans l'IoT.	La surveillance, la commande et la configuration à distance des dispositifs sont nécessaires.
D3	Dispositifs	L'IoT doit offrir une capacité de connexion immédiate (*plug and play*), afin de permettre la configuration instantanée fondée sur la sémantique des dispositifs.	Une capacité de connexion immédiate est nécessaire.
D4	Dispositifs	La notification automatique du statut des objets et de ses changements est nécessaire, afin d'assurer la surveillance des objets en temps voulu.	La surveillance des objets en temps voulu est nécessaire.
D5	Dispositifs	L'IoT doit prendre en charge la mobilité des objets.	La mobilité des dispositifs est nécessaire.
D6	Dispositifs	La vérification de l'intégrité des dispositifs est nécessaire, afin d'assurer une grande disponibilité des dispositifs.	La vérification de l'intégrité des dispositifs est nécessaire.

Numéro de l'exigence	Catégorie de l'exigence	Description de l'exigence	Résumé de l'exigence
DM1	Gestion de données	Le stockage des données des objets fondé sur des règles et des politiques définies au préalable doit être pris en charge dans l'IoT.	Le stockage des données des objets doit être pris en charge.
DM2	Gestion de données	La fusion et l'exploration des données fondées sur des règles et des politiques définies au préalable doivent être prises en charge.	Le traitement des données des objets doit être pris en charge.
DM3	Gestion de données	L'IoT doit pouvoir fournir l'historique des informations concernant les objets.	L'interrogation de l'historique des données des objets doit être prise en charge.
DM4	Gestion de données	Le contrôle de l'accès aux données par leur propriétaire doit être pris en charge dans l'IoT, afin que les utilisateurs de l'IoT aient la possibilité de contrôler la visibilité de leurs données par d'autres utilisateurs de l'IoT.	Le contrôle de l'accès aux données par leur propriétaire est nécessaire.
DM5	Gestion de données	L'IoT doit être en mesure de donner l'accès à des sources de données externes, par exemple des bases de données relatives à la santé situées à l'extérieur de l'IoT.	L'échange des données avec des entités à l'extérieur de l'IoT doit être pris en charge.
DM6	Gestion de données	L'IoT doit assurer la vérification de l'intégrité des données des objets et la gestion de leur cycle de vie, afin d'être en mesure d'assurer une disponibilité et une fiabilité élevées pour les données des objets.	La vérification de l'intégrité des données des objets et la gestion de leur cycle de vie sont nécessaires.
DM7	Gestion de données	L'annotation sémantique des données des objets est nécessaire. L'accès sémantique aux données des objets est nécessaire, afin que les objets puissent être interrogés de manière automatique.	L'annotation sémantique des données des objets et l'accès sémantique aux données des objets sont nécessaires.
DM8	Gestion de données	Le stockage, le transfert et l'agrégation des données des objets doivent être réalisés de manière automatique, conformément aux exigences des utilisateurs ou des applications de l'IoT.	Le stockage, le transfert et l'agrégation sémantiques des données des objets sont nécessaires.
SP1	Sécurité et protection de la confidentialité	L'IoT doit prendre en charge une capacité de communication sécurisée et sûre avec protection de la confidentialité.	La sécurité des communications est nécessaire.
SP2	Sécurité et protection de la confidentialité	L'IoT doit fournir une capacité de gestion de données sécurisée et sûre avec protection de la confidentialité.	La sécurité de la gestion de données est nécessaire.
SP3	Sécurité et protection de la confidentialité	L'IoT doit fournir une capacité de fourniture de services sécurisée et sûre avec protection de la confidentialité.	La sécurité de la fourniture de services est nécessaire.
SP4	Sécurité et protection de la confidentialité	L'intégration de différentes politiques et techniques de sécurité relatives aux différents dispositifs et réseaux utilisateurs dans l'IoT est nécessaire.	L'intégration de différentes politiques et techniques de sécurité est nécessaire.

Numéro de l'exigence	Catégorie de l'exigence	Description de l'exigence	Résumé de l'exigence
SP5	Sécurité et protection de la confidentialité	Avant qu'un dispositif (ou un utilisateur de l'IoT) puisse accéder à l'IoT, une authentification et une autorisation mutuelles sont nécessaires, selon les politiques de sécurité définies au préalable.	Une authentification et une autorisation mutuelles sont nécessaires.
SP6	Sécurité et protection de la confidentialité	L'accès aux données et les tentatives d'accès aux applications IoT doivent être parfaitement transparents, traçables et reproductibles, conformément aux réglementations et législations pertinentes.	Les audits de sécurité doivent être pris en charge dans l'IoT.

Appendice I

Cas d'utilisation représentatifs de l'IoT

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

Le présent appendice contient la description de certains cas d'utilisation représentatifs de l'IoT. Ces cas d'utilisation sont décrits et classés en fonction de leur application dans un ou plusieurs domaines d'application.

I.1 Surveillance vidéo

La surveillance vidéo est une catégorie de cas d'utilisation type présente dans de nombreuses applications IoT. Par exemple, dans les applications relatives aux villes intelligentes, des caméras sont utilisées pour observer les déplacements de la population dans la ville, pour des raisons de sécurité. En matière de surveillance de la pollution, la surveillance vidéo est utilisée pour repérer les rejets d'eau polluée par des usines. Les hôpitaux utilisent la surveillance vidéo pour surveiller à distance l'état des patients.

La surveillance vidéo nécessite généralement un grand nombre de ressources, notamment une grande largeur de bande pour le transfert des vidéos, une grande quantité de ressources de stockage pour la conservation de copies des vidéos et de puissants processeurs pour les recherches effectuées sur les vidéos ainsi que leur traitement.

I.2 Alerte d'urgence

L'alerte d'urgence est présente dans un grand nombre de cas d'utilisation, notamment pour la transmission d'un message de secours lorsqu'un patient déclare une maladie cardiaque, la transmission d'un message d'alerte avant qu'un véhicule cesse de fonctionner normalement, ou après, lorsqu'un accident de la route survient, ainsi que pour la transmission d'un message d'alerte lorsque la pression artérielle dépasse un certain seuil.

Ces cas d'utilisation nécessitent une grande priorité ainsi qu'un transport de données fiable, présentant un temps de propagation minimal. Ils nécessitent en outre des capacités de communications déclenchées par les dispositifs.

I.3 Acquisition de données

Cette catégorie comprend de nombreux cas d'utilisation, tels que le téléchargement de données provenant de compteurs de gaz, de compteurs d'eau, de dispositifs de surveillance de la qualité de l'eau, de compteurs électriques, de terminaux de tickets de bus, etc. Dans ces cas d'utilisation, les communications de données sont réalisées à des intervalles de temps réguliers.

Ces cas d'utilisation nécessitent des mécanismes permettant la transmission périodique de données. L'opération de transmission peut être activée de manière automatique, conformément à une politique définie. En général, la plupart de ces cas d'utilisation présentent un faible débit de transmission de données.

I.4 Contrôle à distance

Cette catégorie comprend des cas d'utilisation qui s'inscrivent dans plusieurs domaines d'application, tels que la domotique, la fabrication et les systèmes de transport intelligents (ITS). Dans ces cas d'utilisation, l'application IoT doit permettre à l'utilisateur de contrôler à distance les dispositifs.

Pour cette catégorie de cas d'utilisation, les communications de données visant à contrôler à distance les dispositifs ne sont pas continues et ne sont pas nécessairement réalisées à des intervalles de temps réguliers. Ces cas d'utilisation nécessitent des mécanismes permettant aux

contrôleurs et aux dispositifs d'établir la connectivité entre les contrôleurs et les dispositifs distants, uniquement lorsqu'une transmission de données est nécessaire.

I.5 Transfert d'événements entre différents domaines d'application

Dans de nombreuses applications IoT telles que celles relatives aux villes intelligentes et à la gestion des situations d'urgence, les événements qui se produisent dans un domaine d'application sont transférés à d'autres domaines d'application concernés. En fonction des événements transférés entre les différents domaines d'application, des applications peuvent fonctionner en collaboration, afin de fournir davantage de fonctionnalités et de services, par rapport à un domaine d'application donné fonctionnant seul. Ces cas d'utilisation comprennent notamment le transfert d'événements entre les applications d'entretien des routes et les applications d'entretien des ponts, entre les applications de gestion du trafic et les applications de conduite, entre les applications de prévision météorologique et les applications de prévention des inondations, etc.

Pour ces cas d'utilisation, il est nécessaire que les événements soient décrits dans un format normalisé, afin qu'ils puissent être compris par les différentes applications IoT concernées. De plus, les événements devraient être transférés de manière fiable et sécurisée.

I.6 Partage de données entre différents domaines d'application

Certaines données revêtent une importance non seulement pour l'application IoT dans laquelle elles sont recueillies, mais aussi dans d'autres applications IoT. Il s'agit notamment de données relatives à la position géographique, de données concernant le trafic routier, etc. Conformément aux réglementations et législations applicables, les données peuvent aussi être partagées entre différents domaines d'application, permettant ainsi de fournir davantage de fonctionnalités et de services. Par exemple, des données relatives à la position géographique des téléphones mobiles peuvent être utilisées pour calculer le trafic routier.

Ce type de cas d'utilisation nécessite l'utilisation par les différents domaines d'application de l'IoT de formats de données normalisés, afin que les données puissent être partagées entre différents domaines d'application.

I.7 Centre opérationnel intégré pour ville intelligente

Les villes intelligentes développées sur la base d'une infrastructure IoT constituent une nouvelle tendance dans le développement des villes dans le monde entier. Dans le futur, les villes auront besoin d'un système de "cerveau" intelligent pour analyser les différents types de données recueillies par les dispositifs IoT et agir en fonction de cette analyse ou prendre les mesures qui en découlent. On peut appeler ce système de cerveau d'une ville un "centre opérationnel intégré pour une ville intelligente".

Un tel centre opérationnel intégré nécessite des fonctionnalités de partage, d'agrégation et de traitement de données couvrant plusieurs domaines d'application. Par exemple, la mise en œuvre d'un centre opérationnel intégré nécessite en général l'intégration d'informations opérationnelles relatives au statut urbain en temps réel, avec des fonctionnalités de surveillance des événements, d'analyse de données, d'alerte avancée et de diffusion d'informations intelligentes, de prise de décision intelligente et de commande et de distribution intégrées.

I.8 Cas d'utilisation détaillé: Collecte d'informations relatives à un accident de la route

Une station ITS située à bord d'un véhicule directement impliqué dans un accident ou qui passe à proximité de cet accident détecte l'événement et lance automatiquement une procédure de signalement d'accident. Elle tente de se connecter à l'IoT pour envoyer un rapport d'accident. L'IoT réceptionne et vérifie le rapport d'accident et le résultat de l'analyse est transmis aux abonnés au service, autrement dit un poste de police et un centre de secours.

Les abonnés au service peuvent demander à l'IoT de recueillir davantage d'informations concernant l'accident. L'IoT reçoit ces demandes de service et sollicite les stations ITS, afin qu'elles recueillent d'autres informations, en fonction des demandes des abonnés. Les stations ITS se trouvant à proximité du lieu de l'accident reçoivent ces instructions, les vérifient, les analysent et les exécutent, par exemple en prenant des photos, en évaluant l'état courant du trafic, en générant des rapports, en les signant puis en les envoyant à l'IoT. L'IoT réunit et vérifie les rapports téléchargés par les stations ITS et génère un rapport contenant des informations visuelles concernant l'accident, à l'intention du centre de secours, ainsi qu'un rapport concernant l'état du trafic aux abords du lieu de l'accident. Ces rapports sont transmis respectivement au centre de secours et au poste de police.

Le centre de secours analyse le rapport concernant le lieu de l'accident et élabore en conséquence un plan de secours adéquat. Le poste de police analyse le rapport concernant l'état du trafic et élabore en conséquence un plan de gestion du trafic approprié.

Ce cas d'utilisation nécessite une capacité de communications déclenchées par les dispositifs, une capacité de communications sûres et sécurisées et une collaboration fondée sur les événements entre les différentes applications.

Bibliographie

[b-UIT-T Y.2061] Recommandation UIT-T Y.2061 (2012), *Exigences relatives à la prise en charge des applications de communication orientée machine dans l'environnement des réseaux de prochaine génération*.

[b-IoT-A D6.2] The Internet of Things Architecture – IoT-A (2011), *Project Deliverable D6.2 – Updated Requirements List*.
http://www.iot-a.eu/public/public-documents/documents-1

[b-UML] ISO/CEI 19505-2:2012, *Technologies de l'information – Langage de modélisation unifié OMG (OMG UML) – Partie 2: Superstructure*.
http://www.iso.org/iso/catalogue_detail.htm?csnumber=52854

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	**Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes**
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2019