Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.2060

(06/2012)

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

Réseaux de prochaine génération – Cadre général et modèles architecturaux fonctionnels

Présentation générale de l'Internet des objets

Recommandation UIT-T Y.2060

RECOMMANDATIONS UIT-T DE LA SÉRIE Y

INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET ET RÉSEAUX DE PROCHAINE GÉNÉRATION

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

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

Recommandation UIT-T Y.2060

Présentation générale de l'Internet des objets

Résumé

La Recommandation UIT-T Y.2060 présente un aperçu général de l'Internet des objets (IoT). Elle précise le concept et la portée de l'IoT, dont elle définit les caractéristiques fondamentales ainsi que les exigences de haut niveau et décrit le modèle de référence. L'écosystème de l'IoT ainsi que différents modèles d'activité sont en outre présentés dans un appendice donné à titre d'information.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	ITU-T Y.2060	2012-06-15	13	11.1002/1000/11559

Mots clés

Dispositif, Internet des objets, modèle de référence, objet, objet physique, objet virtuel.

* 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 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.2060

Présentation générale de l'Internet des objets

1 Domaine d'application

La présente Recommandation vise à donner un aperçu général de l'Internet des objets (IoT), l'objectif premier étant de mieux faire connaître ce système appelé à occuper une place importante dans les futures activités de normalisation.

La présente Recommandation traite plus précisément des points suivants:

– termes et définitions applicables à l'IoT;

– concept et portée de l'IoT;

– caractéristiques de l'IoT;

– exigences de haut-niveau de l'IoT;

– modèles de référence applicables à l'IoT.

On trouvera dans l'Appendice I des informations au sujet de l'écosystème et des modèles d'activité de l'IoT.

2 Références

Aucune.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise le terme suivant défini ailleurs:

3.1.1 réseau de prochaine génération (NGN) [b-UIT-T Y.2001]: réseau en mode paquet, en mesure d'assurer des services de télécommunication et d'utiliser de multiples technologies de transport à large bande à qualité de service imposée et dans lequel les fonctions liées aux services sont indépendantes des technologies sous-jacentes liées au transport. Il assure le libre accès des utilisateurs aux réseaux et aux services ou fournisseurs de services concurrents de leur choix. Il prend en charge la mobilité généralisée qui permet la fourniture cohérente et partout à la fois des services aux utilisateurs.

3.2 Termes définis dans la présente Recommandation

Les termes suivants sont définis dans la présente Recommandation:

3.2.1 dispositif: dans l'Internet des objets, équipement doté obligatoirement de capacités de communication et éventuellement de capacités de détection, d'actionnement, de saisie de données, de stockage de données et de traitement de données.

3.2.2 Internet des objets (IoT): 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, de saisie 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 – Dans une optique plus large, l'IoT peut être considéré comme un concept ayant des répercussions sur les technologies et la société.

3.2.3 objet: 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.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

2G Deuxième génération

3G Troisième génération

AAA Authentification, autorisation et comptabilité (*authentication, authorization and accounting)*

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

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

FCAPS Dérangements, configuration, comptabilité, qualité de fonctionnement et sécurité (*fault, configuration, accounting, performance, and security*)

IoT Internet des objets (*Internet of things*)

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

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

NGN Réseau de prochaine génération (*next generation network*)

RTPC Réseau téléphonique public commuté

TCP/IP Protocole de commande de transmission/protocole Internet (*transmission control protocol/Internet protocol*)

TIC Technologies de l'information et de la communication

5 Conventions

Aucune.

6 Présentation de l'IoT

6.1 Le concept d'IoT

L'Internet des objets (IoT) peut être considéré comme un concept ambitieux ayant des répercussions sur les technologies et la société.

Au plan de la normalisation technique, on peut se représenter l'IoT comme une 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 (TIC) interopérables existantes ou en évolution.

En exploitant les capacités d'identification, de saisie 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 – L'IoT devrait associer étroitement certaines technologies de pointe – telles que la communication évoluée de machine à machine, la réseautique autonome, l'exploration de données et la prise de décision, la protection de la sécurité et de la sphère privée et l'informatique en nuage – avec des technologies offrant des capacités avancées en matière de détection et d'actionnement.

Comme l'illustre la Figure 1, l'IoT donne aux TIC une nouvelle dimension en ce sens que, grâce à lui, la communication est non seulement possible en tout LIEU et à tout MOMENT, comme c'était déjà le cas, mais aussi avec n'importe quel OBJET.

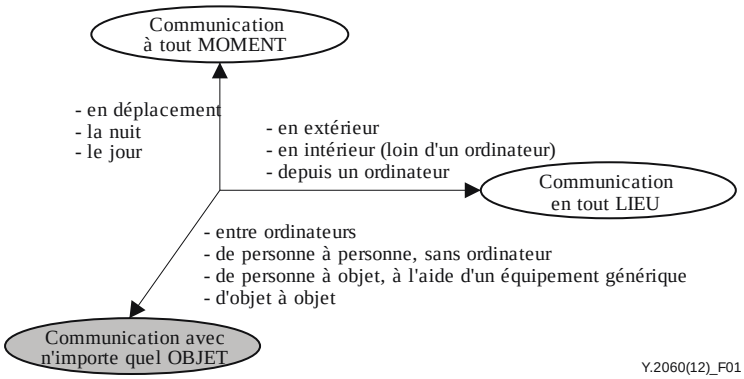

Figure 1 – La nouvelle dimension introduite par l'Internet des objets [b-UIT Rapport]

Dans l'IoT, les objets s'entendent d'objets du monde physique (objets physiques) ou du monde de l'information (objets virtuels), pouvant être identifiés et intégrés dans des réseaux de communication. Des informations leurs sont associées, qui peuvent être statiques ou dynamiques.

Les objets physiques appartiennent au monde physique et peuvent être détectés, commandés et connectés. L'environnement qui nous entoure, les robots industriels, les biens et les équipements électriques sont autant d'exemples d'objets physiques.

Les objets virtuels appartiennent au monde de l'information; on peut les stocker, les traiter et y accéder. Ces objets sont par exemple des contenus multimédias ou des logiciels.

6.2 Aperçu technique de l'IoT

On trouvera dans la Figure 2 un aperçu technique de l'IoT.

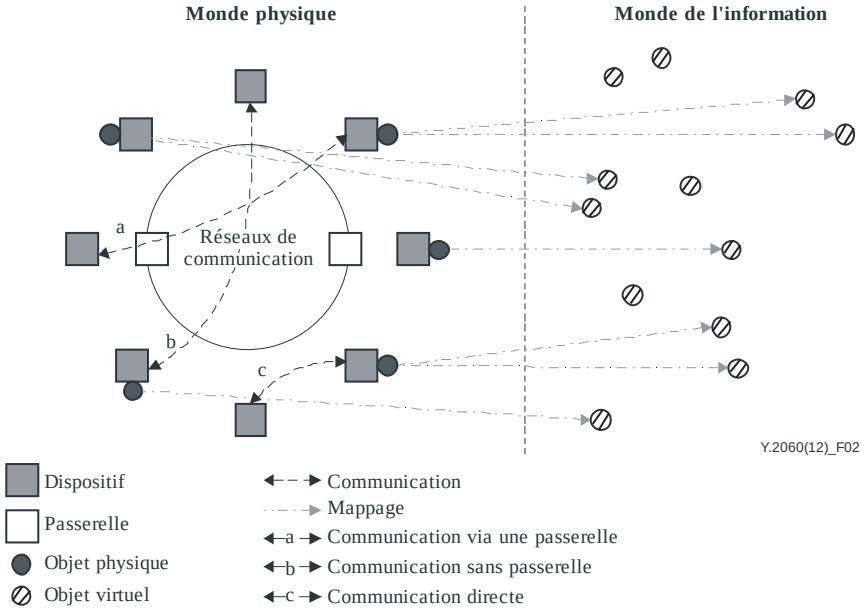

Figure 2 – Aperçu technique de l'IoT

Un objet physique peut être représenté dans le monde de l'information par l'intermédiaire d'un ou de plusieurs objets virtuels (mappage) mais un objet virtuel peut tout aussi bien n'être associé à aucun objet physique.

Un dispositif est un équipement doté obligatoirement de capacités de communication et éventuellement de capacités de détection, d'actionnement, de saisie de données, de stockage de données et de traitement de données. Il recueille des informations de différents types, qu'il transmet aux réseaux d'information et de communication en vue d'un traitement approfondi. Certains dispositifs peuvent également exécuter des opérations à partir des informations reçues des réseaux d'information et de communication.

Les dispositifs communiquent entre eux soit par l'intermédiaire du réseau de communication, via une passerelle (cas a) ou sans passerelle (cas b), soit de manière directe, c'est-à-dire sans passer par le réseau de communication (cas c). Il est également possible de combiner les cas a et c ou les cas b et c; des dispositifs peuvent par exemple communiquer avec d'autres dispositifs au moyen d'une liaison directe sur un réseau local (c'est-à-dire un réseau assurant une connectivité locale entre les dispositifs eux-mêmes et entre ceux-ci et une passerelle, comme un réseau ad hoc) (cas c) puis d'une liaison sur le réseau de communication via une passerelle de réseau locale (cas a).

NOTE 1 – Bien que la Figure 2 ne présente que les interactions qui se produisent dans le monde physique (communications entre dispositifs), des interactions ont également lieu dans le monde de l'information (échanges entre objets virtuels) et entre les deux mondes (échanges entre objets physiques et objets virtuels).

L'IoT prend en charge des applications très diverses, ayant trait par exemple aux "systèmes de transport intelligents", aux "réseaux électriques intelligents", à la "cybersanté" ou au "logement intelligent". Les applications IoT peuvent être installées sur des plates-formes propriétaires mais aussi sur une ou plusieurs plates-formes de service/d'application communes dotées de capacités génériques (par exemple, authentification, gestion de dispositifs, taxation et comptabilité).

Les réseaux de communication transfèrent aux applications et aux autres dispositifs les données saisies par les dispositifs, de même que les instructions que les applications adressent à ceux-ci. Ils sont à même d'assurer le transfert des données de manière fiable et efficace. L'infrastructure réseau de l'IoT peut être mise en place sur la base des réseaux existants, tels que les réseaux TCP/IP conventionnels, ou sur la base de réseaux en évolution, tels que les réseaux de prochaine génération (NGN) [b-UIT-T Y.2001].

La Figure 3 présente les différents types de dispositifs ainsi que les relations entre ceux-ci et les objets physiques.

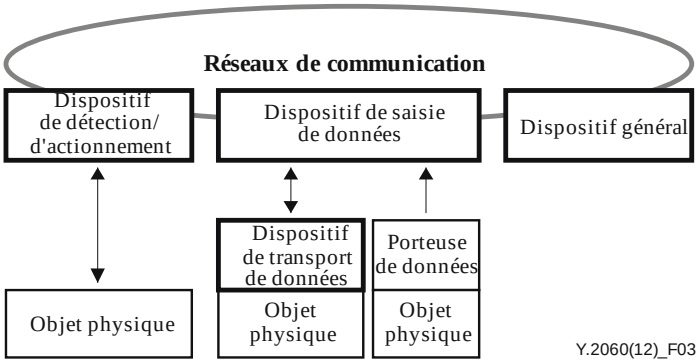

Figure 3 – Les différents types de dispositifs et leurs relations avec les objets physiques

NOTE 2 – "Dispositif général" peut également désigner un objet physique ou un ensemble d'objets physiques.

L'exigence minimale en ce qui concerne les dispositifs IoT est la prise en charge de capacités de communication. Il existe différentes catégories de dispositifs, à savoir:

– Dispositifs de transport de données: il s'agit de dispositifs rattachés à un objet physique pour assurer une connexion indirecte entre celui-ci et les réseaux de communication.

– Dispositifs de saisie de données: il s'agit de dispositifs de lecture/écriture à même d'interagir avec des objets physiques. L'interaction peut être indirecte, par l'intermédiaire de dispositifs de transport de données, ou directe, via des porteuses de données rattachées aux objets physiques. Dans le premier cas, le dispositif de saisie de données lit les informations sur un dispositif de transport de données et peut aussi, éventuellement, y écrire les informations fournies par les réseaux de communication.

  NOTE 3 – Les interactions entre les dispositifs de saisie de données et les dispositifs de transport de données ou les porteuses de données sont notamment assurées au moyen de commandes radioélectriques, infrarouge, optiques ou par courant galvanique.

– Dispositifs de détection et d'actionnement: il s'agit de dispositifs capables de détecter ou de relever des informations concernant leur environnement immédiat et de les convertir en signaux électronumériques. Ils peuvent également convertir les signaux électronumériques reçus des réseaux d'information en opérations. En règle générale, les dispositifs de détection et d'actionnement des réseaux locaux communiquent entre eux à l'aide de technologies filaires ou hertziennes et se connectent aux réseaux de communication via des passerelles.

– Dispositifs généraux: il s'agit de dispositifs dotés de capacités de traitement et de communication, qui sont à même d'interagir avec les réseaux de communication au moyen de technologies filaires ou hertziennes. Cette catégorie de dispositifs recouvre les équipements et appareils utilisés dans différents domaines d'application de l'IoT (machines industrielles, appareils électroménagers, smartphones, etc.).

7 Caractéristiques fondamentales de l'IoT et exigences de haut niveau

7.1 Caractéristiques fondamentales

Les caractéristiques fondamentales de l'IoT sont les suivantes:

– Interconnectivité: dans l'IoT, tout objet peut être connecté à l'infrastructure mondiale de l'information et de la communication.

– Services liés aux objets: l'IoT est à même de fournir des services liés aux objets tenant compte des exigences inhérentes à ceux-ci (par exemple protection de la sphère privée et cohérence sémantique entre les objets physiques et les objets virtuels qui leurs sont associés). Pour que de tels services puissent être fournis dans le respect de ces exigences, les technologies utilisées seront amenées à changer, aussi bien dans le monde physique que dans le monde de l'information.

– Hétérogénéité: les dispositifs utilisés dans l'IoT sont hétérogènes puisqu'ils ne font pas appel aux mêmes plates-formes matérielles ni aux mêmes réseaux. Ils peuvent interagir avec d'autres dispositifs ou plates-formes de service par l'intermédiaire de réseaux différents.

– Changements dynamiques: l'état des dispositifs (par exemple veille/réveil, connecté/déconnecté) change de façon dynamique, de même que le contexte dans lequel ces dispositifs fonctionnent (emplacement, vitesse, etc.). Par ailleurs, le nombre de dispositifs peut lui aussi évoluer de façon dynamique.

– Très grande échelle: les dispositifs qui devront être gérés et qui communiqueront entre eux seront au moins dix fois plus nombreux que ceux connectés à l'Internet à l'heure actuelle. Le rapport entre les communications établies par des dispositifs et celles établies par des personnes deviendra nettement plus favorable aux premières. La gestion des données générées et leur interprétation pour les besoins des applications seront d'autant plus critiques. Cette question est en lien avec la sémantique et le traitement efficace des données.

7.2 Exigences de haut niveau

On trouvera ci-après les exigences de haut niveau applicables à l'IoT:

– Connectivité fondée sur l'identification: la connexion entre un objet et l'IoT doit pouvoir être établie sur la base de l'identificateur de l'objet en question. Cela implique par ailleurs que les identificateurs des différents objets, potentiellement hétérogènes, soient traités de manière uniforme.

– Interopérabilité: il est nécessaire d'assurer l'interopérabilité de systèmes hétérogènes et répartis afin de permettre la mise à disposition et l'utilisation d'un large éventail d'informations et de services.

– Réseautique autonome: la réseautique autonome (y compris les techniques ou mécanismes d'autogestion, d'autoconfiguration, d'autorétablissement, d'auto-optimisation et d'autoprotection) doit être prise en charge dans l'IoT par les fonctions de contrôle de la réseautique 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.

– Fourniture de services autonomes: les services doivent pouvoir être fournis à travers la saisie, la transmission et le traitement automatiques des données concernant les objets conformément aux règles établies par les opérateurs ou définies par les abonnés. La fourniture de services autonomes pourra dépendre des techniques de fusion et d'exploration automatiques des données.

– Capacités de localisation: L'IoT doit prendre en charge des capacités de localisation. Les communications et services liés à un objet quelconque seront fonction des informations relatives à l'emplacement des objets ou des utilisateurs. Ces informations devront être détectées et actualisées de manière automatique. Les communications et services de localisation peuvent être limités en vertu des lois et règlements en vigueur et devraient satisfaire aux exigences de sécurité.

– Sécurité: dans l'IoT, chaque objet est connecté, de sorte qu'il existe d'importants risques pour la sécurité, notamment en ce qui concerne la confidentialité, l'authenticité et l'intégrité des données comme des services. L'un des meilleurs exemples d'exigences de sécurité que l'on puisse donner est la nécessité de tenir compte des politiques et techniques de protection liées aux différents types de dispositifs et de réseaux d'utilisateur existant dans l'IoT.

– Protection de la sphère privée: la sphère privée doit être protégée dans l'IoT. De nombreux objets ont des propriétaires et des utilisateurs et les données détectées relatives aux objets peuvent receler des informations confidentielles concernant ces propriétaires et utilisateurs. L'IoT doit assurer la protection de la confidentialité lors de la transmission, de l'agrégation, du stockage, de l'exploration et du traitement des données. Cette protection ne devrait pas empêcher l'authentification de l'origine des données.

– Fourniture de services de qualité hautement sécurisés concernant le corps humain: l'IoT doit prendre en charge des services concernant le corps humain offrant un niveau de qualité et de sécurité élevé. Différents pays ont adopté leurs propres législations et réglementation concernant de tels services.

NOTE – Les services concernant le corps humain désignent les services fournis moyennant la saisie, la transmission et le traitement, avec ou sans intervention humaine, des données relatives aux caractéristiques statiques et dynamiques d'une personne.

– Plug and play: l'IoT doit offrir des capacités de connexion immédiate (Plug and play) permettant de générer, composer ou acquérir de manière instantanée des configurations sémantiques, de sorte que les objets interconnectés soient parfaitement intégrés aux applications et coopèrent avec elles sans discontinuité apparente et que les exigences propres à ces applications soient respectées.

– Gérabilité: l'IoT doit pouvoir être géré de manière à garantir un fonctionnement normal des réseaux. En règle générale, les applications IoT fonctionnent de manière automatique, sans intervention humaine, mais leur processus global d'exploitation devrait néanmoins pouvoir être géré par les parties concernées.

8 Modèle de référence de l'IoT

La Figure 4 présente le modèle de référence de l'IoT. Ce modèle comprend quatre couches auxquelles sont associées des capacités de gestion et de sécurité.

Ces quatre couches sont les suivantes:

– couche application;

– couche de prise en charge des services et des applications;

– couche réseau;

– couche dispositif.

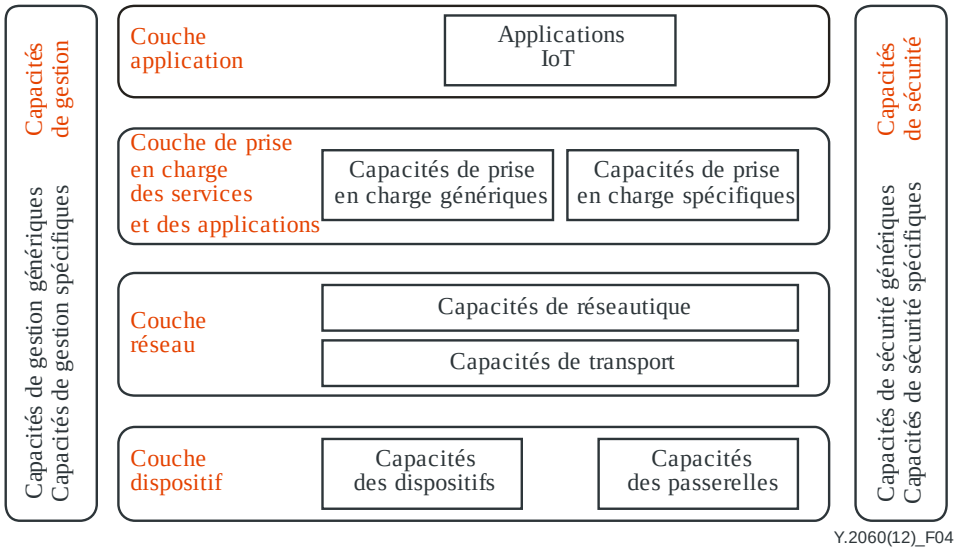

Figure 4 – Modèle de référence de l'IoT

8.1 Couche application

La couche application contient les applications IoT.

8.2 Couche de prise en charge des services et des applications

La couche de prise en charge des services et des applications contient les deux ensembles de capacités suivants:

– Capacités de prise en charge génériques: il s'agit de capacités communes pouvant être utilisées par différentes applications IoT, par exemple de capacités de traitement ou de stockage de données. Des capacités de prise en charge spécifiques peuvent également faire appel à ces capacités génériques, par exemple pour créer de nouvelles capacités spécifiques.

– Capacités de prise en charge spécifiques: il s'agit de capacités particulières répondant aux besoins d'applications diversifiées. Elles peuvent en effet être constituées de différents ensembles de capacités bien précis afin d'assurer des fonctions de prise en charge différentes pour des applications IoT distinctes.

8.3 Couche réseau

Cette couche comprend deux types de capacités, à savoir:

– des capacités de réseautique, qui assurent les fonctions de contrôle pertinentes concernant la connectivité au réseau, telles que le contrôle d'accès et le contrôle des ressources de transport, la gestion de la mobilité ou l'authentification, l'autorisation et la comptabilité (AAA);

– des capacités de transport destinées essentiellement à assurer la connectivité nécessaire pour le transport des informations propres à chaque service ou application IoT ainsi que pour le transport des informations de contrôle et de gestion relatives à l'IoT.

8.4 Couche dispositif

Les capacités de la couche dispositif peuvent être réparties de manière logique en deux catégories:

– **Capacités des dispositifs**:

Les capacités des dispositifs sont entre autres les suivantes:

Interaction directe avec le réseau de communication: les dispositifs sont à même de collecter des informations et de les télécharger sur le réseau de communication de manière directe (c'est-à-dire sans avoir recours pour ce faire aux capacités des passerelles) et peuvent recevoir des informations (par exemple des commandes) provenant directement de celui-ci.

Interaction indirecte avec le réseau de communication: les dispositifs sont à même de collecter des informations et de les télécharger sur le réseau de communication de manière indirecte (c'est-à-dire en ayant recours pour ce faire aux capacités des passerelles). De même, ils peuvent recevoir des informations (par exemple des commandes) provenant indirectement du réseau de communication.

Etablissement de réseaux ad hoc: les dispositifs peuvent être en mesure de créer des réseaux ad hoc dans certains cas de figure nécessitant une modularité accrue et un déploiement accéléré.

Veille et réveil: les capacités des dispositifs peuvent inclure des mécanismes de mise en veille et de réveil permettant de réaliser des économies d'énergie.

NOTE – Un même dispositif ne prendra pas nécessairement en charge et les capacités d'interaction directe et les capacités d'interaction indirecte.

– **Capacités des passerelles**:

Les capacités des passerelles sont entre autres les suivantes:

Prise en charge d'interfaces multiples: au niveau de la couche dispositif, les capacités des passerelles prennent en charge des dispositifs connectés 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 ou du Wi-Fi. Au niveau de la couche réseau, les capacités des passerelles peuvent communiquer par divers moyens, notamment en utilisant le réseau téléphonique public commuté (RTPC), les réseaux de deuxième ou de troisième génération (2G et 3G), les réseaux LTE, les réseaux Ethernet ou les lignes d'abonné numérique (DSL).

Conversion de protocole: les capacités des passerelles s'avèrent nécessaires dans deux cas de figure, le premier étant lorsque des protocoles différents (par exemple ZigBee et Bluetooth) sont utilisés pour les communications au niveau de la couche dispositif, le second lorsque des protocoles différents sont utilisés pour les communications impliquant à la fois la couche dispositif et la couche réseau (par exemple ZigBee au niveau de la couche dispositif et 3G au niveau de la couche réseau).

8.5 Capacités de gestion

Tout comme dans les réseaux de communication traditionnels, les capacités de gestion de l'IoT couvrent les dérangements, la configuration, la comptabilité, la qualité de fonctionnement et la sécurité (FCAPS), c'est-à-dire qu'elles assurent la gestion de ces différents aspects.

Les capacités de gestion de l'IoT peuvent être classées en capacités génériques et capacités spécifiques.

Les capacités de gestion génériques essentielles dans l'IoT sont notamment les suivantes:

– gestion de dispositif (activation/désactivation à distance, diagnostic, mise à jour logicielle/micrologicielle, gestion du mode de fonctionnement);

– gestion de la topologie du réseau local;

– gestion du trafic et de l'encombrement (détection des débordements sur le réseau, réservation de ressources pour les flux de données à temps critique ou vitaux, etc.).

Les capacités de gestion spécifiques sont étroitement liées aux besoins propres à une application donnée, par exemple pour le contrôle des lignes électriques utilisées dans les réseaux électriques intelligents.

8.6 Capacités de sécurité

Les capacités de sécurité sont de deux ordres: génériques ou spécifiques. Les capacités de sécurité génériques sont indépendantes des applications. Elles comprennent:

– au niveau de la couche application: l'autorisation, l'authentification, la confidentialité des données d'application et la protection de leur intégrité, la protection de la sphère privée, les audits de sécurité et les anti-virus;

– au niveau de la couche réseau: l'autorisation, l'authentification, la confidentialité des données utiles et des données de signalisation et la protection de l'intégrité de la signalisation;

– au niveau de la couche dispositif: l'authentification, l'autorisation, la validation de l'intégrité du dispositif, le contrôle d'accès, la confidentialité des données et la protection de l'intégrité.

Les capacités de sécurité spécifiques sont étroitement liées aux besoins propres à une application donnée, par exemple les exigences de sécurité associées aux paiements sur mobile.

Appendice I

Ecosystème de l'IoT et modèles d'activité

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

I.1 Rôles opérationnels

Différents acteurs interviennent dans l'écosystème de l'IoT, chacun d'eux étant investi d'un rôle opérationnel, parfois même de plusieurs. Les rôles opérationnels identifiés en ce qui concerne l'IoT sont représentés dans la Figure I.1.

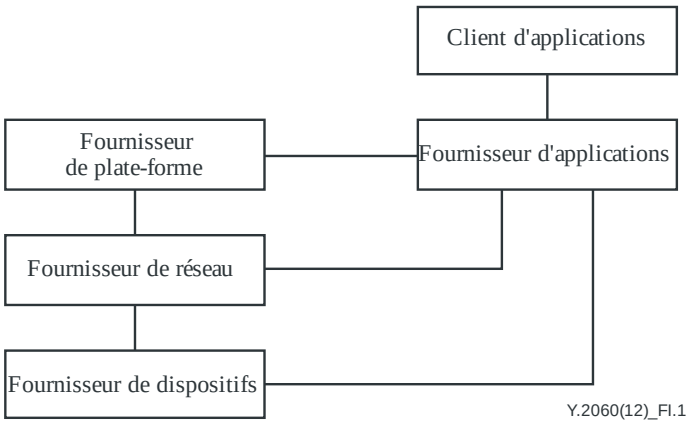

Figure I.1 – Ecosystème de l'IoT

NOTE – Les rôles opérationnels identifiés dans cet écosystème et les relations entre eux ne sauraient rendre compte de l'ensemble des rôles et relations pertinents que l'on pourra rencontrer lors des déploiements réels de l'IoT.

I.1.1 Fournisseur de dispositifs

Le fournisseur de dispositifs doit veiller à ce que les dispositifs livrent des données/contenus bruts au fournisseur de réseau et au fournisseur d'applications conformément à la logique de service.

I.1.2 Fournisseur de réseau

Le fournisseur de réseau joue un rôle central dans l'écosystème de l'IoT. Ses principales fonctions sont notamment les suivantes:

– accès aux ressources mises à disposition par d'autres fournisseurs et intégration de ces ressources;

– prise en charge et contrôle de l'infrastructure de capacités de l'IoT;

– offre de capacités liées à l'IoT, y compris de capacités et de ressources de réseau, à d'autres fournisseurs.

I.1.3 Fournisseur de plate-forme

Le fournisseur de plate-forme propose des capacités d'intégration ainsi que des interfaces ouvertes. Des plates-formes différentes peuvent offrir des capacités différentes aux fournisseurs d'applications. Les capacités des plates-formes sont notamment des capacités d'intégration ainsi que des capacités concernant le stockage et le traitement de données ou la gestion de dispositifs. La prise en charge de différents types d'applications IoT est également possible.

I.1.4 Fournisseur d'applications

Le fournisseur d'applications utilise les capacités ou les ressources mises à sa disposition par le fournisseur de réseau, le fournisseur de dispositifs et le fournisseur de plate-forme pour proposer des applications IoT aux clients d'applications.

I.1.5 Client d'applications

Le client d'applications est l'utilisateur d'une ou de plusieurs applications IoT mises à sa disposition par le fournisseur d'applications.

NOTE – Un client d'applications peut représenter plusieurs utilisateurs d'applications.

I.2 Modèles d'activité

Les acteurs de l'écosystème de l'IoT peuvent entretenir diverses relations dans le cadre de déploiements réels.

La diversité de ces relations s'explique par la multiplicité des modèles d'activité envisageables. Dans la suite du présent appendice, seuls cinq de ces modèles applicables à l'IoT sont étudiés du point de vue des opérateurs de services et de réseau de télécommunication.

I.2.1 Modèle 1

Dans le modèle 1, l'acteur A est fournisseur à la fois de dispositifs, de réseau, de plate-forme et d'applications et dessert le client d'applications de manière directe (Figure I.2).

En règle générale, dans le modèle 1, l'acteur A désigne les opérateurs de télécommunication et certaines entreprises intégrées verticalement (par exemple, opérateurs de réseaux électriques intelligents et de systèmes de transport intelligents (ITS)).

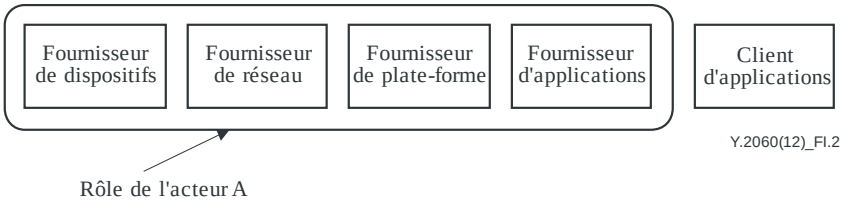

Figure I.2 – Modèle 1

I.2.2 Modèle 2

Dans le modèle 2, l'acteur A est fournisseur à la fois de dispositifs, de réseau et de plate-forme, tandis que l'acteur B est fournisseur d'applications et dessert le client d'applications (Figure I.3).

En règle générale, dans le modèle 2, l'acteur A désigne les opérateurs de télécommunication et l'acteur B d'autres fournisseurs de services.

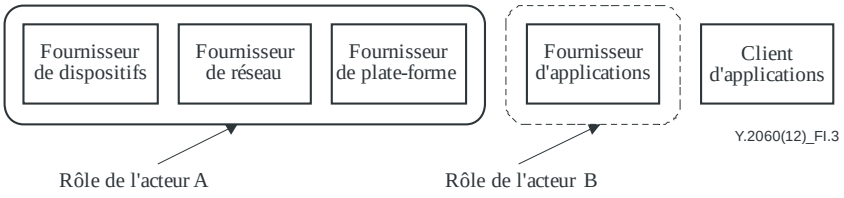

Figure I.3 – Modèle 2

I.2.3 Modèle 3

Dans le modèle 3, l'acteur A est fournisseur à la fois de réseau et de plate-forme, tandis que l'acteur B est fournisseur de dispositifs et d'applications et dessert le client d'applications (Figure I.4).

En règle générale, l'acteur A désigne les opérateurs de télécommunication et l'acteur B d'autres fournisseurs de services.

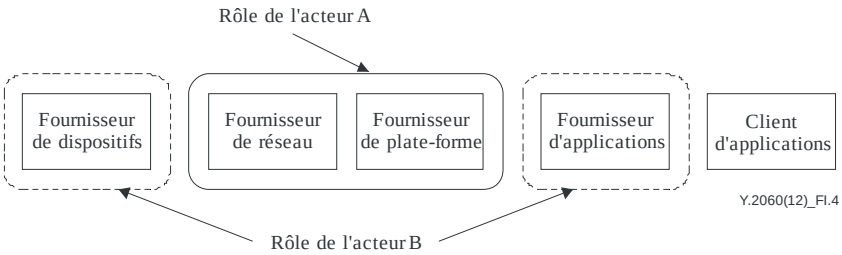

Figure I.4 – Modèle 3

I.2.4 Modèle 4

Dans le modèle 4, l'acteur A est uniquement fournisseur de réseau, tandis que l'acteur B est fournisseur de dispositifs et de plate-forme et fournit des applications au client d'applications (Figure I.5).

En règle générale, dans le modèle 4, l'acteur A désigne les opérateurs de télécommunication et l'acteur B d'autres fournisseurs de services ou des entreprises intégrées verticalement.

NOTE – Il existe une variante à ce modèle, qui ne comprend ni fournisseur de plate-forme ni fonctionnalités de plate-forme associées (l'acteur B fournit uniquement des applications).

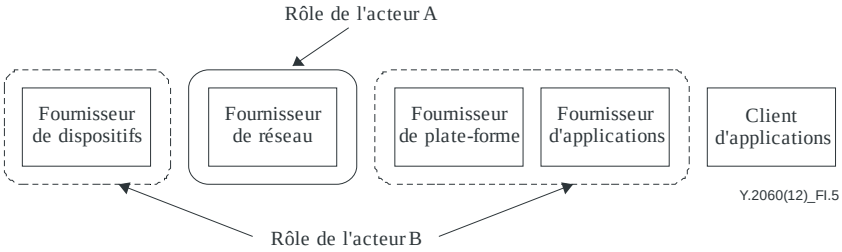

Figure I.5 – Modèle 4

I.2.5 Modèle 5

Dans le modèle 5, l'acteur A est uniquement fournisseur de réseau, l'acteur B est fournisseur de plate-forme, tandis que l'acteur C est fournisseur de dispositifs et fournit des applications au client d'applications (Figure I.6).

En règle générale, dans le modèle 5, l'acteur A désigne les opérateurs de télécommunication, l'acteur B d'autres fournisseurs de services et l'acteur C des entreprises intégrées verticalement.

NOTE – Il existe une variante à ce modèle, qui ne comprend ni fournisseur de plate-forme ni fonctionnalités de plate-forme associées (l'acteur C fournit uniquement des applications).

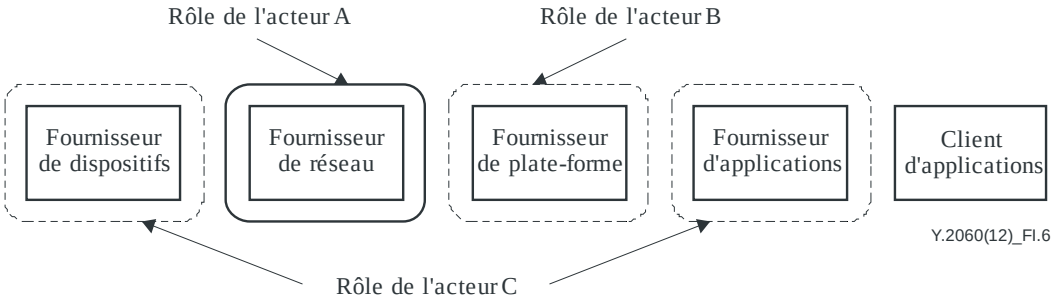

Figure I.6 – Modèle 5

Bibliographie

[b-UIT Rapport] ITU Internet Reports (2005), *The Internet of Things*.

[b-UIT-T Y.2001] Recommandation UIT-T Y.2001 (2004), *Aperçu général des réseaux de prochaine génération*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
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	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	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
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 et réseaux de prochaine génération**
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2014