Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.4102/Y.2074

(01/2015)

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

Réseaux de prochaine génération – Cadre général et modèles architecturaux fonctionnels

Exigences relatives aux dispositifs de l'Internet des objets utilisés pour mettre en oeuvre les applications de l'Internet des objets lors des catastrophes

Recommandation UIT-T Y.4102/Y.2074

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.4102/Y.2074

Exigences relatives aux dispositifs de l'Internet des objets utilisés pour mettre en oeuvre les applications de l'Internet des objets lors des catastrophes

Résumé

La Recommandation UIT-T Y.2074 définit les exigences relatives aux dispositifs de l'Internet des objets (IoT) utilisés pour mettre en oeuvre des applications IoT en cas de catastrophe, qui viennent s'ajouter aux exigences communes relatives à l'Internet des objets, définies dans la Recommandation UIT-T Y.2066. Elle définit aussi les exigences relatives à la mise en oeuvre d'applications IoT en cas de catastrophe.

Il est nécessaire de spécifier ces exigences pour pouvoir utiliser les dispositifs IoT et les applications IoT en cas de catastrophe pour les opérations d'évacuation et de secours.

L'Appendice I décrit des méthodes permettant de s'assurer de l'intégrité et de la fiabilité des données produites par les dispositifs IoT en cas de catastrophe.

Cette Recommandation s'adresse aux concepteurs d'applications IoT et aux fournisseurs de services IoT ainsi qu'aux fournisseurs de services d'urgence.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	ITU-T Y.4102/Y.2074	2015-01-13	13	11.1002/1000/12421

Mots clés

Catastrophe, Internet des objets (IoT), application IoT, dispositif IoT, exigences, systèmes de sécurité.

* 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

		Page
1	Domaine d'application	1
2	Références	1
3	Définitions	2
3.1	Termes définis ailleurs	2
3.2	Termes définis dans la présente Recommandation	2
4	Abréviations et acronymes	2
5	Conventions	3
6	Exigences relatives aux dispositifs IoT en cas de catastrophe	3
6.1	Exigences générales se rapportant aux catastrophes	3
6.2	Exigences relatives aux dispositifs IoT	3
7	Exigences relatives à la mise en oeuvre des applications IoT en cas de catastrophe	4
7.1	Applications IoT avec un mode de mise en oeuvre dédié	4
7.2	Applications IoT fournissant provisoirement des ressources à des systèmes de sécurité extérieurs	5
7.3	Applications IoT avec commande de mise en oeuvre extérieure en cas de catastrophe	6
7.4	Alternance entre plusieurs stratégies de mise en oeuvre lors d'une catastrophe	7
Appendice I – Méthode permettant de s'assurer de l'intégrité et de la fiabilité des données produites par les dispositifs IoT en cas de catastrophe		8
I.1	Centres de surveillance et de commande des dispositifs IoT: présentation générale	8
I.2	Répartition des responsabilités du centre de surveillance et de commande entre des centres locaux	9
I.3	Scénarios de fonctionnement du centre de surveillance et de commande	9
I.4	Utilisation des données stockées	10
Bibliographie		11

Introduction

L'objet de chaque nouvelle technologie de l'information et de la communication (TIC) est de présenter un intérêt et une utilité pour les utilisateurs. Ainsi, même lorsqu'une catastrophe se produit, les TIC devraient avoir pour objet d'aider à secourir les utilisateurs en danger. Concrètement, les utilisateurs ne peuvent parfois pas attendre l'arrivée d'une équipe de secours ou d'une aide extérieure. Ils n'ont alors d'autre choix que de se débrouiller seuls et d'essayer de quitter la zone où s'est produite la catastrophe le plus vite possible. Il est par conséquent nécessaire d'élaborer des exigences relatives aux dispositifs de l'Internet des objets (IoT), ainsi que des exigences relatives à la mise en oeuvre des applications IoT en cas de catastrophe venant s'ajouter aux exigences relatives à leur mise en oeuvre en conditions normales. Dans les faits, les applications IoT sont généralement inutiles dans la pratique en cas de catastrophe, lorsqu'il est vital pour les utilisateurs de l'Internet des objets d'être secouru. Etant donné que l'infrastructure IoT est déjà largement déployée, les ressources techniques correspondantes pourraient être très utiles pour sauver des vies humaines.

D'un point de vue pratique, il est extrêmement difficile d'élaborer et de mettre en oeuvre efficacement un nouveau système de sécurité d'urgence, en raison des procédures complexes de normalisation et de certification devant être appliquées dans le domaine de la gestion des catastrophes. En revanche, il est assez simple d'améliorer les fonctionnalités des systèmes de sécurité existants en les dotant de capacités accrues pour la prise en charge des applications IoT en cas de catastrophe. De même, les systèmes fondés sur l'Internet des objets pourraient être associés aux systèmes de sécurité existants et utilisés par ces systèmes de sécurité lors des catastrophes.

Il faut bien comprendre que les nouveaux systèmes IoT intelligents ne remplaceront jamais les systèmes de sécurité testés et certifiés existants, qui ont fait leurs preuves depuis de nombreuses années; toutefois, ces nouveaux systèmes pourraient prendre en charge la capacité d'interaction avec les systèmes de sécurité existants. Il serait toujours possible sur le plan technique de gérer les applications IoT depuis le centre d'administration des systèmes de sécurité existants lorsqu'une catastrophe se produit.

L'interaction entre ces applications IoT améliorées et les systèmes de sécurité existants devrait être utile pour la mise en oeuvre des procédures de secours en cas de catastrophe, par exemple pour donner l'alerte et procéder aux évacuations.

Recommandation UIT-T Y.4102/Y.2074

Exigences relatives aux dispositifs de l'Internet des objets utilisés pour mettre en oeuvre les applications de l'Internet des objets lors des catastrophes

1 Domaine d'application

La présente Recommandation définit les exigences relatives aux dispositifs de l'Internet des objets (IoT) pouvant être utilisés pour mettre en oeuvre des applications IoT en cas de catastrophe, qui viennent s'ajouter aux exigences communes relatives à l'Internet des objets [UIT-T Y.2066]. Elle définit aussi les exigences relatives à la mise en oeuvre d'applications IoT en cas de catastrophe.

Le domaine d'application de la présente Recommandation couvre les exigences relatives:

- aux dispositifs IoT en cas de catastrophe;
- à la mise en oeuvre des applications IoT en cas de catastrophe (pour chacune des trois stratégies de mise en oeuvre identifiées).

L'Appendice I décrit des méthodes permettant de s'assurer de l'intégrité et de la fiabilité des données produites par les dispositifs IoT en cas de catastrophe.

La présente Recommandation s'adresse aux concepteurs d'applications IoT et aux fournisseurs de services IoT ainsi qu'aux fournisseurs de services d'urgence.

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. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Les Recommandations ou 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 énumérés 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 d'une Recommandation.

[UIT-T X.1303] Recommandation UIT-T X.1303 (2007), *Protocole d'alerte commun (CAP 1.1)*.

[UIT-T Y.1271] Recommandation UIT-T Y.1271 (2004), *Cadres généraux applicables aux spécifications et aux capacités de réseau pour la prise en charge des télécommunications d'urgence sur les réseaux à commutation de circuits et à commutation de paquets en cours d'évolution.*

[UIT-T Y.2066] Recommandation UIT-T Y.2066 (2014), *Exigences communes relative à l'Internet des objets*.

[UIT-T Y.2205] Recommandation UIT-T Y.2205 (2011), *Réseaux de prochaine génération – Télécommunications d'urgence – Considérations techniques*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 alerte [b-UIT-T X.674]: message d'avertissement ou d'alarme concernant l'imminence d'un danger ou d'un problème.

3.1.2 dispositif [b-UIT-T Y.2060]: 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.

3.1.3 télécommunications d'urgence (ET, *emergency telecommunications*) [UIT-T Y.2205]: tout service associé à une urgence qui nécessite un traitement spécial de la part du NGN par rapport aux autres services. Les télécommunications d'urgence comprennent les services de sécurité du public et les services d'urgence autorisés par les pouvoirs publics.

3.1.4 Internet des objets (IoT) [b-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, 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.

3.1.5 réseau de prochaine génération (NGN, *next generation network*) [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

Aucun.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

CAP protocole d'alerte commun (*common alerting protocol*)

ET télécommunications d'urgence (*emergency telecommunications*)

ICT technologies de l'information et de la communication (*information and communication technology*)

IoT Internet des objets (*Internet of Things*)

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

5 Conventions

Dans la présente Recommandation:

L'expression "il est obligatoire" indique 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 exigence 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 oeuvre 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.

L'expression "catastrophe" désigne tout type de situation critique ou d'urgence dû à un phénomène naturel ou causé par l'homme.

L'expression "dispositif IoT" désigne un dispositif dans l'environnement de l'Internet des objets.

6 Exigences relatives aux dispositifs IoT en cas de catastrophe

6.1 Exigences générales se rapportant aux catastrophes

Les Recommandations ci-après traitent des télécommunications dans le contexte des catastrophes:

– [UIT-T Y.1271] donne les exigences et les capacités de réseau pour les télécommunications d'urgence (ET).

– [UIT-T Y.2205] contient des considérations techniques qui peuvent être appliquées dans les réseaux de prochaine génération (NGN) pour la prise en charge des télécommunications d'urgence. En outre, cette Recommandation énonce les principes techniques sous-jacents associés à cette prise en charge.

Ces Recommandations portent sur les exigences et les aspects techniques pour les télécommunications d'urgence. Si l'on part du principe que les applications IoT utiliseront les NGN comme infrastructure de télécommunication lors d'une catastrophe, ces exigences leur sont pleinement applicables.

Conformément à [UIT-T Y.2205], il est recommandé d'utiliser le protocole d'alerte commun (CAP) défini dans [UIT-T X.1303] afin d'assurer les échanges d'informations entre les systèmes d'alerte.

6.2 Exigences relatives aux dispositifs IoT

Il est obligatoire de soumettre tous les dispositifs IoT fabriqués à des procédures de test.

Dans le cadre de ces procédures, les dispositifs IoT devraient être soumis à des tests dans des conditions allant au-delà de leur plage de fonctionnement (par exemple, température, pression, rayonnement), afin de vérifier qu'ils ne présentent aucun danger pour l'environnement et pour l'homme en cas de catastrophe. Les dispositifs IoT ne doivent pas provoquer de complications ou d'urgences d'un autre type.

Les conditions de test devraient être choisies sur la base des caractéristiques des situations d'urgence pouvant se produire dans la zone de déploiement.

Il est obligatoire de faire figurer, dans les caractéristiques techniques des dispositifs, les résultats des tests et les dangers que pourraient présenter ces dispositifs en dehors de leur plage de fonctionnement.

Il est recommandé de mettre au point de nouveaux dispositifs IoT dont les caractéristiques opérationnelles permettent une plus large plage d'utilisation (par exemple, température d'utilisation, humidité, pression). Cette exigence est essentielle pour les applications IoT qui pourraient présenter des défaillances, en raison de l'incertitude du comportement de l'environnement et des répercussions sur les dispositifs IoT en cas de catastrophe.

Il est recommandé de généraliser cette pratique aux types de dispositifs IoT très utilisés. La mise en oeuvre de dispositifs IoT fournissant des mesures pendant les catastrophes pourrait permettre de constituer une base de données de mesures de paramètres environnementaux effectuées lors de catastrophe de différentes natures. Ces mesures aideraient à tirer d'importantes conclusions concernant le déroulement des catastrophes dont il serait tenu compte lors de la phase de conception des dispositifs IoT.

7 Exigences relatives à la mise en oeuvre des applications IoT en cas de catastrophe

Les paragraphes ci-après décrivent les exigences relatives à la mise en oeuvre des applications IoT lors d'une catastrophe. En particulier, les § 7.1 à 7.3 décrivent les exigences pour chacune des trois stratégies de mise en oeuvre définies pour les applications IoT en ce qui concerne les catastrophes, tandis que le § 7.4 décrit les modalités permettant d'alterner entre ces stratégies lors d'une catastrophe.

En vue d'accroître l'efficacité des ressources d'infrastructure associées à la mise en oeuvre des applications IoT, il est recommandé que ces applications mettent en oeuvre une ou plusieurs des stratégies ci-après concernant les catastrophes.

Pour toutes les stratégies, on part du principe qu'au lieu de continuer, à fonctionner normalement lorsqu'une catastrophe se produit, les applications IoT effectuent uniquement des tâches visant à secourir des personnes.

Les fausses alertes sont possibles: un état d'urgence peut être annulé (par exemple, en cas de détection d'une fausse urgence) et, dans ce cas, l'application IoT revient à son fonctionnement normal. La période nécessaire pour décider s'il s'agit d'une fausse alerte (maintien du mode de mise en oeuvre ou retour au fonctionnement normal) est plus ou moins longue pour chaque mise en oeuvre particulière, en fonction de sa complexité.

7.1 Applications IoT avec un mode de mise en oeuvre dédié

Si elle dispose d'un mode de mise en oeuvre dédié pouvant être activé en cas d'urgence, une application IoT peut être utilisée sans intervention particulière ou commande extérieure. La Figure 1 montre le changement de mode de mise en oeuvre des applications IoT appliquant cette stratégie.

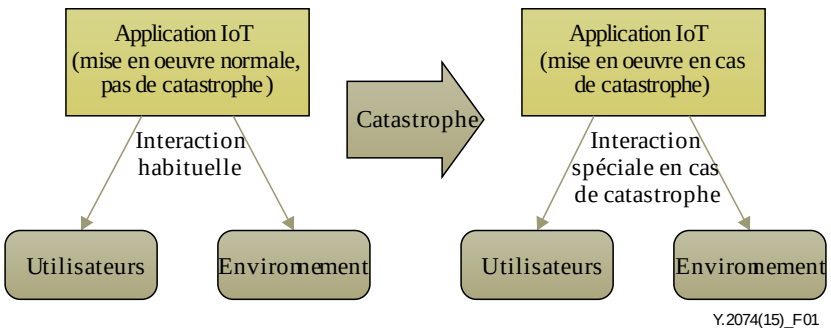

Figure 1 – Changement de mode de de mise en oeuvre des applications IoT ayant un mode de mise en oeuvre dédié activé en cas de catastrophe

Les applications fondées sur des réseaux de capteurs conçues pour donner la position des utilisateurs à l'intérieur d'un bâtiment et ayant des modes de mise en oeuvre dédiés activés en cas de catastrophe peuvent être particulièrement efficaces pour permettre l'évacuation d'un bâtiment sans intervention extérieure en cas d'incendie, de séisme ou d'autres catastrophes.

Autre exemple concernant cette stratégie de mise en oeuvre, l'une des applications IoT peut servir de système de sécurité.

NOTE – Il existe des prototypes de systèmes de sécurité de ce type fondés sur des technologies de capteurs hertziens (par exemple, ceux décrits dans [b-UIT-T Y.2222]), mais ils sont peu utilisés en raison de la longueur et de la complexité des procédures de normalisation et de certification applicables aux équipements de systèmes de sécurité.

Il est obligatoire que les applications IoT ayant un mode de mise en oeuvre dédié activé en cas de catastrophe respectent tous les textes réglementaires applicables.

7.2 Applications IoT fournissant provisoirement des ressources à des systèmes de sécurité extérieurs

Normalement, les applications IoT ont un but précis et, pour la plupart d'entre elles, n'ont pas pour vocation d'apporter une assistance ou une aide aux utilisateurs lors d'une catastrophe. Par conséquent, les ressources des applications IoT devraient être assistées par des systèmes de sécurité extérieurs afin d'accroître l'efficacité du processus de gestion des catastrophes. La Figure 2 montre le changement de mode de mise en oeuvre des applications IoT appliquant cette stratégie.

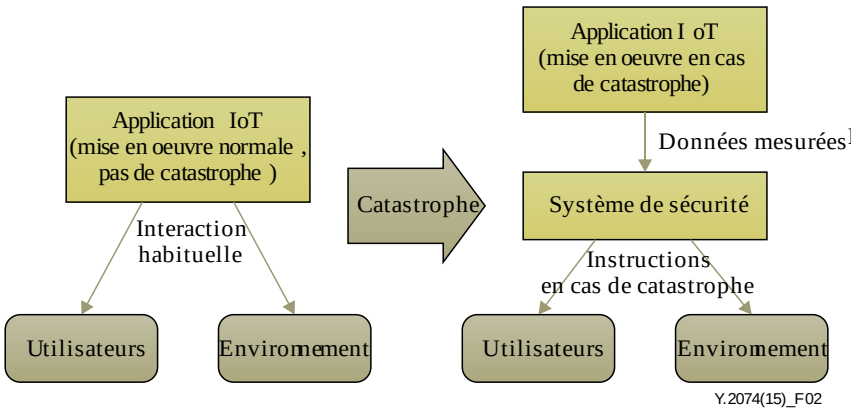

Figure 2 – Changement de mode de mise en oeuvre pour les applications IoT fournissant provisoirement des ressources à des systèmes de sécurité extérieurs

Les applications IoT conçues pour les utilisateurs se trouvent à l'intérieur d'un bâtiment ou dans un autre environnement doté d'un système de sécurité devraient provisoirement (pendant la durée de catastrophe) partager, avec ce système de sécurité, la capacité de commande de l'application IoT et tous les types de données mesurées. Ces ressources pourraient être utiles pour la mise en oeuvre du système de sécurité, par exemple, les données provenant des différents capteurs comme la température et l'humidité en cas d'incendie.

Pour simplifier l'intégration des applications IoT avec les systèmes de sécurité extérieurs, il est recommandé d'utiliser le protocole CAP [UIT-T X.1303] pour les échanges entre les applications IoT et les systèmes de sécurité extérieurs. Le protocole CAP est un protocole de communication bidirectionnelle qui peut permettre à la fois la transmission des données depuis les applications IoT

par les systèmes de sécurité et la transmission des messages d'alerte depuis les systèmes de sécurité vers les applications IoT.

Le principal inconvénient de cette stratégie de mise en oeuvre est que les composants fonctionnels de l'infrastructure IoT peuvent présenter des défaillances s'ils ne sont pas conçus pour fonctionner correctement lors d'une catastrophe. Ces défaillances peuvent avoir des conséquences négatives lorsqu'elles concernent des composants fonctionnels qui sont nécessaires lors des processus de gestion des catastrophes et s'expliquent par le fait qu'il n'existe, pour les composants fonctionnels de l'infrastructure IoT, aucune procédure de certification particulière permettant de garantir leur bon fonctionnement lors d'une catastrophe, comme c'est le cas pour les systèmes de sécurité.

7.3 Applications IoT avec commande de mise en oeuvre extérieure en cas de catastrophe

La troisième stratégie de mise en oeuvre des applications IoT en cas de catastrophe suppose un transfert total des capacités de commande et des données mesurées des applications IoT vers les systèmes de sécurité extérieurs ou des centres de commande extérieurs.

NOTE 1 – Le transfert complet des capacités de commande signifie que l'application IoT met fin elle-même au processus de gestion des ressources.

NOTE 2 – Un centre de commande extérieur peut être, par exemple, une organisation ou une initiée fonctionnelle d'une organisation qui a l'entière responsabilité sur les plans légal et administratif de la bonne gestion des catastrophes dans une zone donnée.

La Figure 3 montre le changement de mode de mise en oeuvre des applications IoT appliquant cette stratégie.

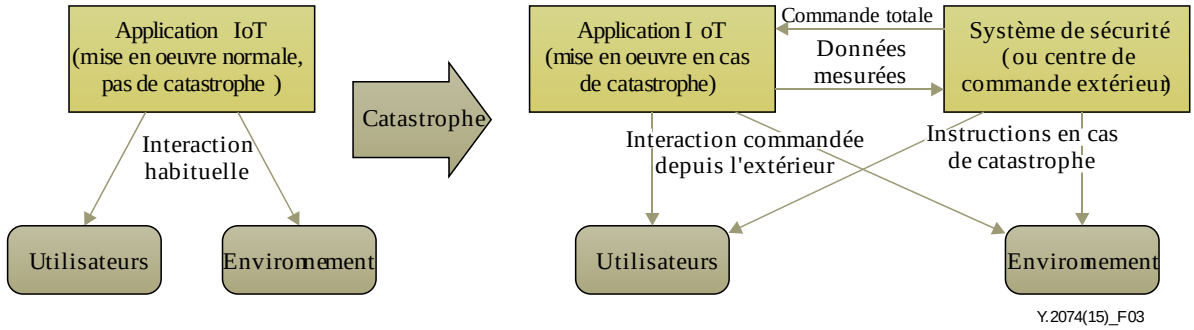

Figure 3 – Changement de mode de mise en oeuvre pour les applications IoT avec commande de mise en oeuvre extérieure en cas de catastrophe

Dans le cadre de cette stratégie, en ce qui concerne les applications IoT utilisant le mode de mise en oeuvre décrit au § 7.1, le comportement des utilisateurs pendant la catastrophe est entièrement commandé par des systèmes de sécurité et des alertes extérieurs.

Le principal objectif de cette stratégie de mise en oeuvre est de faire en sorte que les systèmes de sécurité ou les centres de commande extérieurs utilisent le plus efficacement possible toutes les ressources des applications IoT disponibles, grâce à leur bonne gestion.

L'Appendice I décrit des méthodes permettant de s'assurer de l'intégrité et de la fiabilité des données produites par les dispositifs IoT. Un centre de surveillance et de commande pour les dispositifs IoT, décrit dans l'Appendice I, peut être utilisé comme centre de commande extérieur pour les applications IoT utilisant cette stratégie.

Comme pour la stratégie de mise en oeuvre décrite au § 7.2, il est recommandé d'utiliser le protocole CAP [UIT-T X.1303] pour les échanges entre les applications IoT et les systèmes de sécurité extérieurs ou les centres de contrôle extérieurs.

7.4 Alternance entre plusieurs stratégies de mise en oeuvre lors d'une catastrophe

En fonction de l'objectif de l'application IoT et de ses capacités, une stratégie ou plusieurs stratégies combinées peuvent être mises en oeuvre dans l'application IoT, ce qui suppose que cette application a la capacité de changer de stratégie en fonction de certaines conditions extérieures, par exemple lorsqu'elle reçoit des signaux de commande ou en cas de dépassement d'un niveau prescrit dans les relevés des capteurs, etc.

Par exemple, la mise en oeuvre d'une application IoT peut se faire comme suit:

Prenons le cas d'une application IoT (à l'intérieur d'une zone géographique) dotée d'un système de sécurité (extérieur à l'application IoT). Si la surveillance des données recueillies par le dispositif IoT montre qu'une urgence se produit alors que le dispositif fonctionne normalement, l'application IoT passe automatiquement sur le mode de mise en oeuvre prévu en cas de catastrophe et applique la stratégie décrite au § 7.1.

Une fois que le délai prévu pour établir s'il s'agit d'une fausse alerte est écoulé, l'application IoT continue de fonctionner en mode dédié ou rétablit le mode de mise en oeuvre normal (en cas de fausse alerte). Si le mode de mise en oeuvre dédié est maintenu, avant la phase critique de la catastrophe, l'application IoT génère des informations personnalisées pour chaque personne concernée par la catastrophe, afin de gérer les modalités de secours.

Lors de la phase critique, lorsque l'application IoT n'est pas en mesure de gérer les secours du fait de capacités réduites, l'application IoT applique la stratégie de mise en oeuvre décrite au § 7.2 (surveillance et transmission des données recueillies au système de sécurité), ce qui peut aider à sauver des vies lors de la phase de sauvetage qui vient ensuite et permettra de suivre l'évolution de la situation.

Appendice I

Méthode permettant de s'assurer de l'intégrité et de la fiabilité des données produites par les dispositifs IoT en cas de catastrophe

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

Les dispositifs IoT ubiquitaires peuvent jouer un rôle important dans le quotidien des personnes, et influencer leurs décisions et leurs actions. Par conséquent, les personnes peuvent dépendre de leurs dispositifs IoT, en particulier des informations et des relevés de capteurs qu'ils fournissent, ainsi que des actions qui en découlent ayant des incidences sur l'environnement. Par conséquent, l'intégrité et la fiabilité des données produites par les dispositifs IoT sont des questions très importantes dans le contexte de l'Internet des objets en général.

La question de l'intégrité et de la fiabilité des données produites par les dispositifs IoT est d'autant plus importante en cas de catastrophe, qu'elle soit naturelle ou causée par l'homme, lorsqu'il se peut que l'intégrité des dispositifs IoT eux-mêmes ne soit pas garantie.

Pour préserver l'intégrité et la fiabilité des données produites par les dispositifs IoT, il est nécessaire d'instaurer un environnement de confiance pour la mise en oeuvre des dispositifs IoT. Pour ce faire, il est important de déterminer l'étendue de la responsabilité en ce qui concerne le fonctionnement des dispositifs IoT en général, par exemple dans le cas où des relevés de capteurs seraient incorrects. Pour y parvenir, il existe deux méthodes:

1) Le fabricant des dispositifs IoT a l'entière responsabilité de tout dysfonctionnement du dispositif IoT fabriqué et garantit le bon fonctionnement de ce dispositif.

2) Un centre autorisé indépendant a l'entière responsabilité de tout dysfonctionnement d'un dispositif IoT dont il a le contrôle (relevant de sa juridiction) et garantit le bon fonctionnement de ce dispositif.

La première méthode est moins efficace que la seconde en raison de l'interaction complexe entre les utilisateurs et les fabricants responsables des dispositifs IoT d'utilisateur, étant donné la grande diversité des dispositifs IoT des différents fabricants susceptibles d'être utilisés dans la même zone de déploiement. Ce problème mérite encore plus d'attention en cas de catastrophe, lorsque la protection de la vie humaine dépend en partie de l'intégrité et de la fiabilité des données produites par les dispositifs IoT. En cas de catastrophe, ni les utilisateurs, ni les services de secours, ni les dispositifs IoT ne seront en mesure de prendre contact avec le fabricant de chaque dispositif IoT donné afin d'obtenir l'assurance de l'intégrité et de la fiabilité de ces données.

La seconde méthode est bien plus simple à mettre en oeuvre, étant donné qu'elle consiste à créer des centres de surveillance et de commande pour les dispositifs IoT, qui seront chargés de la bonne mise en oeuvre des dispositifs relevant de leur juridiction.

I.1 Centres de surveillance et de commande des dispositifs IoT: présentation générale

Un centre de surveillance et de commande (le Centre) des dispositifs IoT est une organisation, ou une unité fonctionnelle d'une organisation, qui est pleinement responsable sur les plans légal et administratif de la bonne mise en oeuvre des dispositifs IoT relevant de sa juridiction. Il assure en outre la surveillance des dispositifs IoT et stocke les informations sur les opérations en cas de catastrophe. Le principal objectif d'un centre de surveillance et de commande des dispositifs IoT est de vérifier l'intégrité et la fiabilité des informations fournies par les dispositifs IoT relevant de sa juridiction. En outre, le Centre est chargé d'informer sans délai les utilisateurs et/ou propriétaires de dispositifs IoT dès lors qu'un dysfonctionnement d'un dispositif IoT quel qu'il soit est identifié.

Lorsqu'une catastrophe menace de se produire ou en cas de catastrophe, le Centre est chargé:

- de surveiller l'état des dispositifs IoT relevant de sa juridiction et des données que ces dispositifs produisent (par exemple, relevés de capteurs);
- d'identifier les dispositifs IoT qui ne fonctionnent pas correctement et d'informer sans délai les utilisateurs et/ou les propriétaires de ces dysfonctionnements;
- de déterminer la zone touchée par la catastrophe, ainsi que la nature et les caractéristiques de la catastrophe, compte tenu des informations obtenues auprès des dispositifs IoT relevant de sa juridiction et des sources d'informations extérieures (par exemple, organismes de secours);
- de gérer les dispositifs IoT relevant de sa juridiction afin de procéder en toute sécurité à l'évacuation des personnes se trouvant dans la zone touchée par la catastrophe;
- d'enregistrer et de stocker les informations obtenues pendant une catastrophe, ainsi que l'historique des opérations menées pendant la catastrophe.

I.2 Répartition des responsabilités du centre de surveillance et de commande entre des centres locaux

Les dispositifs IoT ubiquitaires sont présents en nombre dans les appartements, les maisons, les entreprises, les rues, les lieux publics, etc.

Dans le cas où il existe un centre de surveillance et de commande des dispositifs IoT, il est possible que tous les dispositifs IoT se trouvant dans une maison ou un bâtiment donné relèvent de la juridiction d'un centre local. De même, tous les dispositifs IoT situés dans d'autres zones, par exemple, dans une même rue, pourraient être gérés par d'autres centres locaux. Tous ces centres locaux pourraient être intégrés dans l'infrastructure du Centre principal.

L'infrastructure du Centre principal peut être organisée comme une hiérarchie à niveaux multiples contenant des noeuds de surveillance et de commande de plusieurs niveaux responsables des dispositifs IoT dans différents bâtiments (centres locaux), dans différentes villes (centres municipaux), dans différentes régions (centres régionaux) et dans différents pays (centres fédéraux).

En outre, les responsabilités des centres locaux peuvent être réparties sur la base des fonctions des dispositifs IoT. Par exemple, le Centre peut gérer plusieurs centres locaux, dont un est responsable des dispositifs IoT à vocation domestique, un autre des dispositifs IoT utilisés pour la gestion du trafic, un autre pour les dispositifs IoT utilisés pour le système de sécurité, etc.

Les paragraphes ci-après décrivent les scénarios de fonctionnement possibles pour le centre de surveillance et de commande.

I.3 Scénarios de fonctionnement du centre de surveillance et de commande

Le principal objectif du Centre est de vérifier l'intégrité et la fiabilité des informations fournies par les dispositifs IoT relevant de sa juridiction. Pour ce faire, il est possible de procéder selon les manières suivantes:

1) Comparer les relevés de capteurs des dispositifs IoT relevant de la juridiction du Centre avec les relevés de réseaux de capteurs autonomes (dupliqués).
2) Procéder à la surveillance intelligente des relevés de capteurs, sous la juridiction du Centre, en collectant des données et en effectuant des analyses mathématiques (exploration de données) des informations obtenues, ce qui permet d'identifier les dysfonctionnements des dispositifs IoT.

Ces deux méthodes peuvent être mises en oeuvre et utilisées en association de manière appropriée.

Les méthodes susmentionnées sont décrites plus en détail dans les § I.3.1 et I.3.2.

I.3.1 Réseau de capteurs autonome

Le Centre déploie des réseaux de capteurs autonomes mesurant divers paramètres physiques, qui permettent de doubler les capteurs des dispositifs IoT relevant de sa juridiction.

Il est obligatoire que le réseau de capteurs autonome couvre la totalité de la zone correspondant à la juridiction du Centre. Par exemple, un centre local situé à l'intérieur d'un bâtiment devrait déployer un réseau de capteurs qui couvre la zone située en intérieur qui contient les dispositifs IoT relevant du Centre.

On considère que les capteurs de ce réseau autonome sont des capteurs de référence, c'est-à-dire que les valeurs indiqués dans leurs relevés sont les valeurs de référence pour les paramètres physiques dans cette zone. Ces capteurs de référence sont normalement certifiés par une organisation de confiance dûment habilitée.

Le Centre recueille des données auprès des dispositifs IoT relevant de sa juridiction et les compare avec les valeurs de référence. Cette comparaison permet au Centre de prendre des décisions concernant l'intégrité et la fiabilité des données produites par les dispositifs IoT.

L'avantage de cette méthode est la fiabilité des capteurs de référence qui peut être très grande, quels que soient les dispositifs IoT. Par conséquent, les dysfonctionnements des dispositifs IoT sont identifiés avec une grande précision.

Les inconvénients de cette méthode sont le coût et la complexité du déploiement des réseaux de capteurs autonomes et les risques de défaillance des capteurs de référence en cas de catastrophe.

I.3.2 Surveillance intelligente

La surveillance intelligente concerne la collecte des informations et des relevés de capteurs transmis par les dispositifs IoT relevant de la juridiction du Centre, ainsi que l'analyse mathématique de ces informations. Elle comprend notamment les méthodes d'analyse statistique et le traitement des signaux de corrélation.

La surveillance intelligente permet d'identifier les dispositifs IoT ou les capteurs hors service à l'intérieur d'un groupe de dispositifs analogues.

L'avantage de cette méthode est son indépendance totale vis-à-vis des paramètres extérieurs de l'environnement, ce qui permet une mise en oeuvre à tout moment en cas de catastrophe.

L'inconvénient de cette méthode est qu'il est nécessaire de disposer d'un groupe de dispositifs IoT analogues pour identifier de manière plus fiable les dysfonctionnements.

I.4 Utilisation des données stockées

Le Centre procède à la surveillance, à l'enregistrement et au stockage des informations et des relevés de capteurs transmis par les dispositifs IoT relevant de sa juridiction, y compris ceux obtenus immédiatement avant et pendant la catastrophe.

Cette fonctionnalité permet au Centre de jouer le rôle de "boîte noire" en cas de situation d'urgence. Le Centre est censé aider à identifier les causes des situations d'urgence, comme le font les boîtes noires en cas d'accident d'avion.

Les données anciennes extraites de la mémoire de données du Centre peuvent être utilisées pour améliorer les méthodes de surveillance intelligente et définir des méthodes de gestion et de commande des dispositifs IoT lorsqu'une catastrophe est imminente ou se produit, afin d'assurer l'évacuation du plus grand nombre de personnes possible en toute sécurité.

Bibliographie

[b-UIT-T X.674] Recommandation UIT-T X.674 (2011), *Procédures d'enregistrement d'arcs d'identificateur d'objet en matière d'alerte*.

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

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

[b-UIT-T Y.2222] Recommandation UIT-T Y.2222 (2013), *Réseaux de commande de capteurs et applications connexes dans l'environnement 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	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	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, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects logiciels généraux des systèmes de télécommunication

Imprimé en Suisse
Genève, 2016