PRIDA Track 1 (T1)

Les fondamentaux de l'IoT

24/08/2020

Qui suis-je?

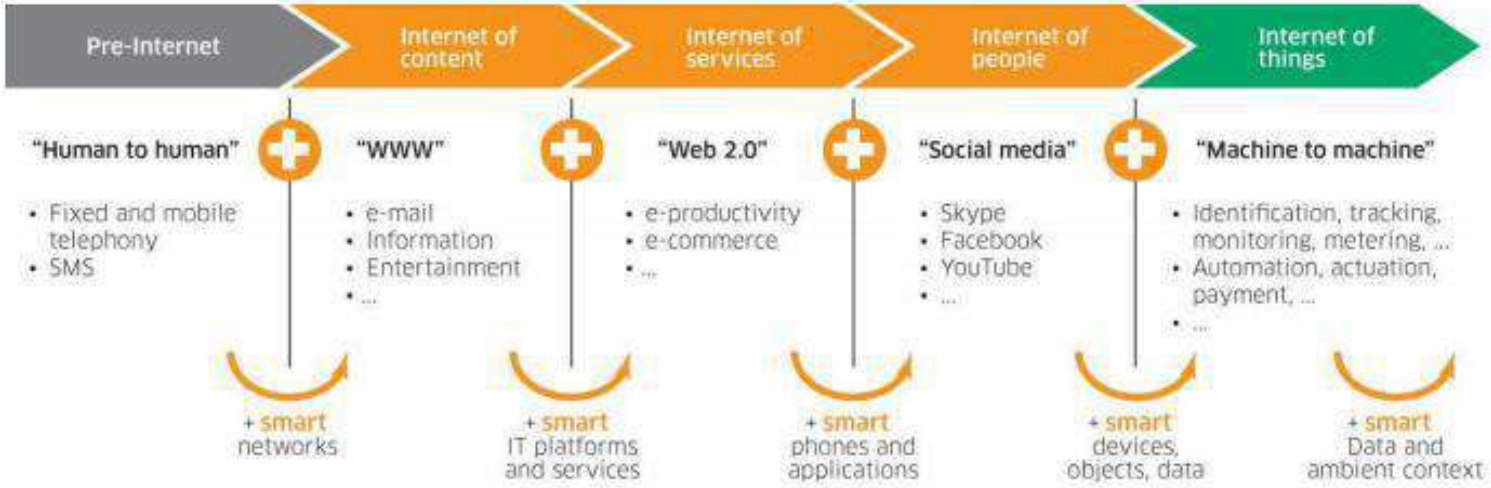
- **Hend Ben Hadji**
- **Ph'D, KAIST (Corée du Sud)**
- Directrice au Centre d'Etudes et de Recherche des Télécommunications (CERT), Tunisie.
- Hend.benhadji@tunsia.gov.tn
- IT Spécialiste
  - 18 ans d'expériences dans le domaine IT
  - Domaines d'activités:
    - PMO des projets stratégiques du plan numérique (projets sectoriels), Ministère (MTCEN)
    - Responsable du programme Innovation, Ministère (MTCTD)
    - Responsable du programme Smart City (MTCEN)
    - Point focal national de l'UIT et l'UAT
    - Membre de plusieurs consortiums internationaux (FP7 PROBE-IT, H2020 GEO-CRADLE, F7 BRAGMA, NIPA-CERT El-Ghazela Smart City, Smart Africa SDVN, …)

Plan de la formation

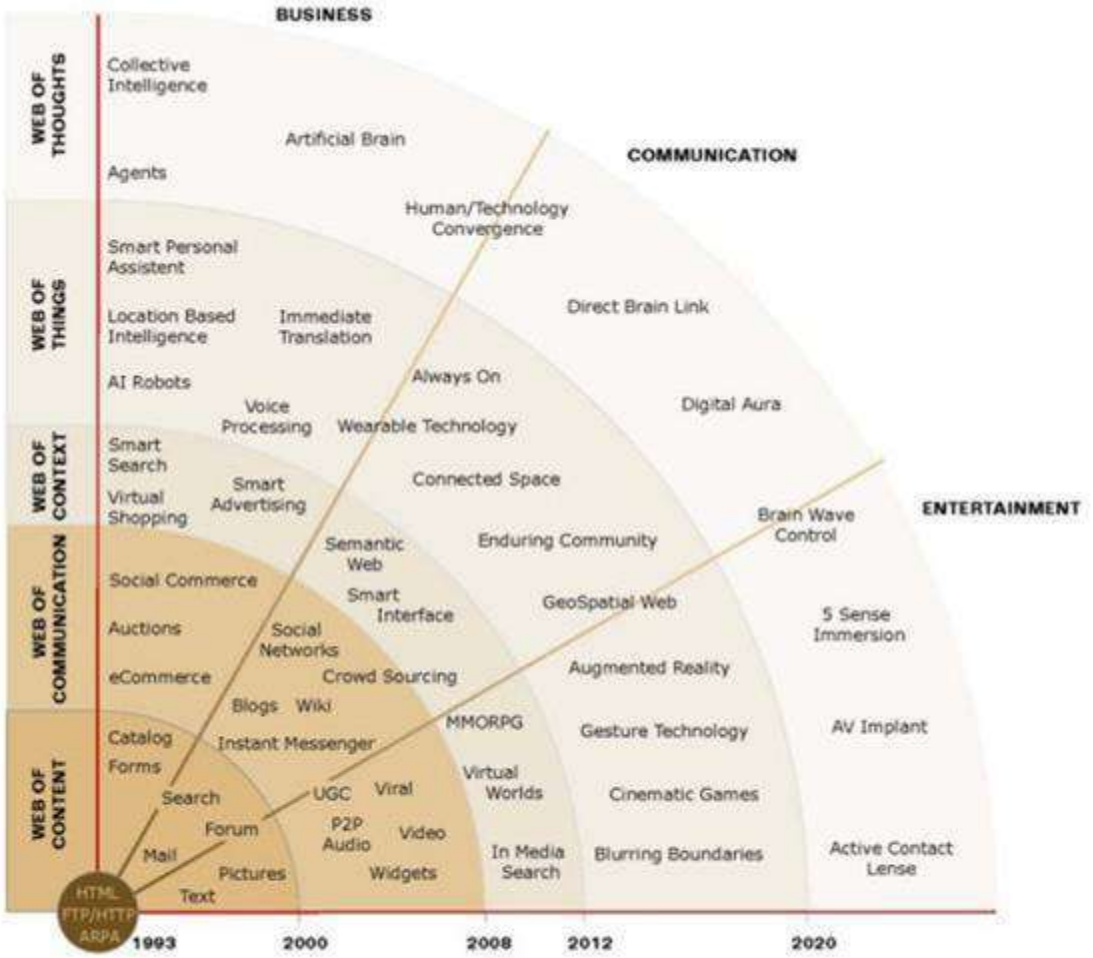
- Partie 1: Origine, définitions et motivations
- Partie 2: Marché, opportunités et challenges
- Partie 3: Modèles d'architecture et composants IoT
- Partie 4: Chaine de valeur IoT, connectivité et modèle d'affaires
- Partie 5 : Activités de normalisation

Partie 1 :
Origine, définitions et motivations

Evolution de l'internet

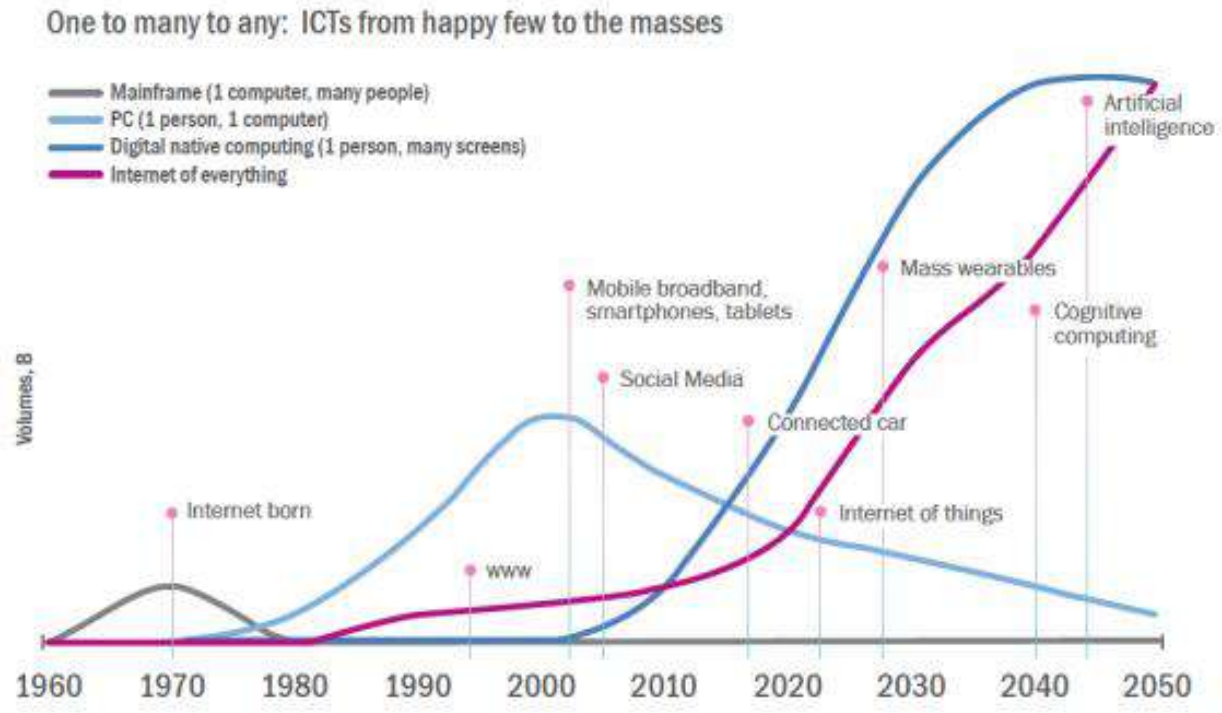


Source: Nokia Insight



Source: https://flatworldbusiness.wordpress.com/flat-education/previously/web-1-0-vs-web-2-0-vs-web-3-0-a-bird-eye-on-the-definition/

Histoire du futur



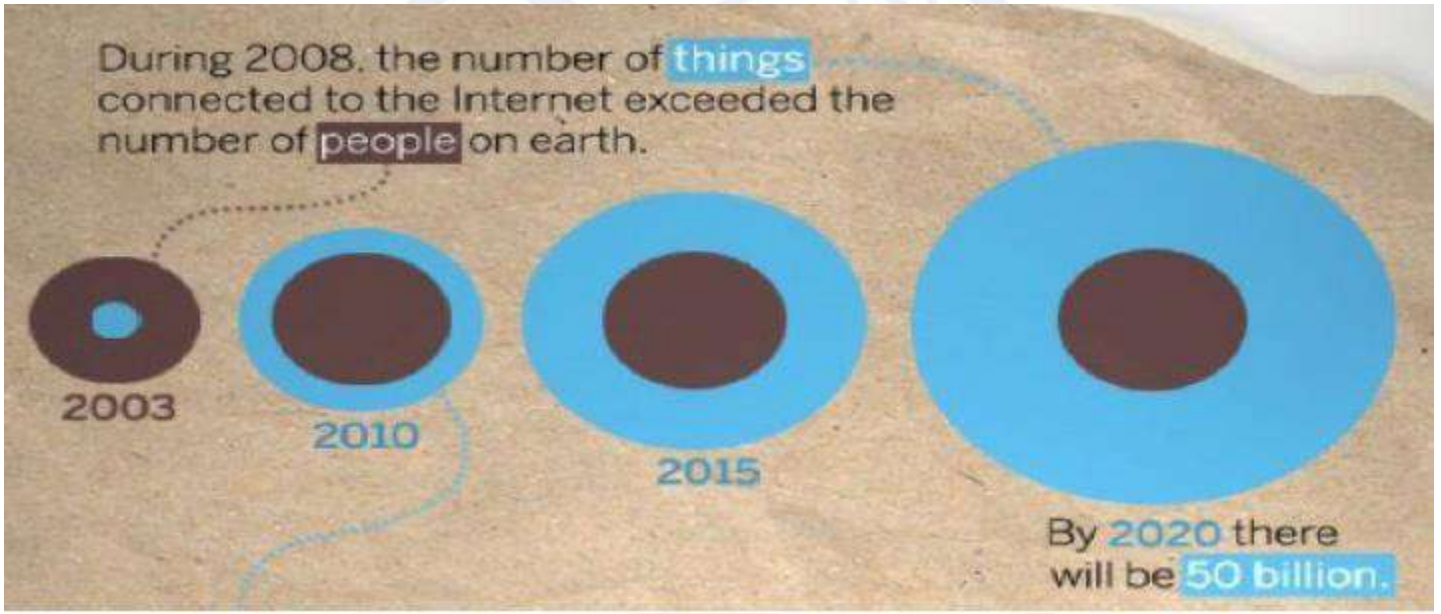
Source: Mario Maniewicz. Digital revolution: Are we ready? 14th Global Symposium for Regulators (GSR)

Origine

- Kevin Ashton : Le premier qui a utilisé le terme « Internet of Things » en 1999 pour décrire les micropuces d'identification par radiofréquence (RFID).

- Selon le groupe Cisco Internet Business Solutions (IBSG), l'Internet des objets est né entre 2008 et 2009, au moment où plus de «choses ou d'objets» étaient connectés à Internet que de personnes

Origine



Source : Cisco

Origine

- La première application IoT est née à l'université de Cambridge en 1991.
- Il s'agissait d'une caméra pointée sur une cafetière et connectée au réseau local de l'université.

- Chaque informaticien pouvait connaitre la disponibilité de café depuis son écran.

Définition UIT

- **Définition 1 :** Le groupe de travail « Internet of Things Global Standards Initiative » (IoT-GSI), piloté par l'Union Internationale des Télécommunications (UIT), considère l'IoT comme :

  « *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 existants ou en évolution* ». - **Recommandation UIT-T Y.2060 renommée Y.4000**

Définition – ISO/IEC

- **Définition 2** : “It is an infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react.”

Définition - IETF

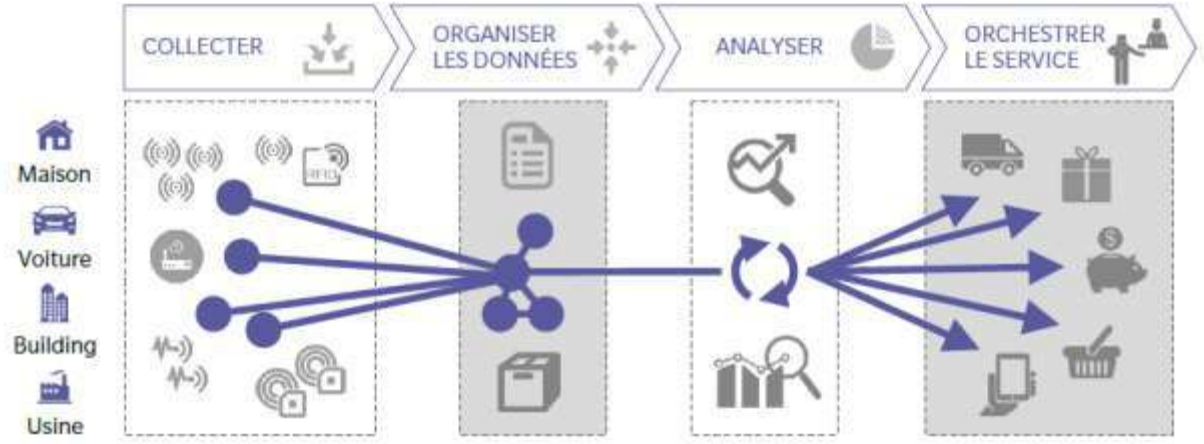
- **Définition 4 :** “The Internet of Things (IoT) refers to devices, that are often constrained in communication and computation capabilities, now becoming more commonly connected to the Internet, and to various services that are built on top of the capabilities these devices jointly provide. It is expected that this development will usher in more machine-to-machine communication using the Internet with no human user actively involved.“

Définition - IEEE

- **Définition 3 :** “Internet of Things envisions a self-configuring, adaptive, complex network that interconnects ‘things’ to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, a programmability feature and are uniquely identifiable. The representation contains information including the thing’s identity, status, location or any other business, social or privately relevant information. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability.“

Définition

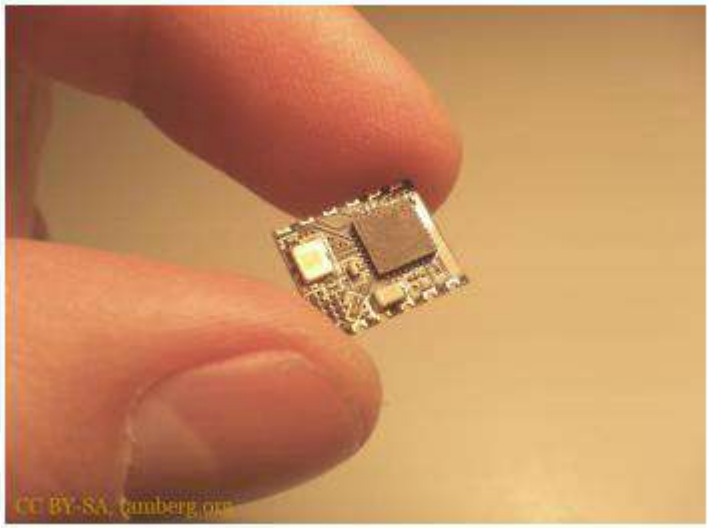
- **Objets physiques:** des capteurs, technologie de connectivité et intelligence;
- **Réseaux de communications :** utilisés pour transporter des données d'objets;
- **Cloud computing:** fournit les outils de stockage, de corrélation et d'analyse des données (processus décisionnels capables de remonter les objets physiques).



Motivations

- Miniaturisation des composants électroniques

RPi zero: 5 dollars



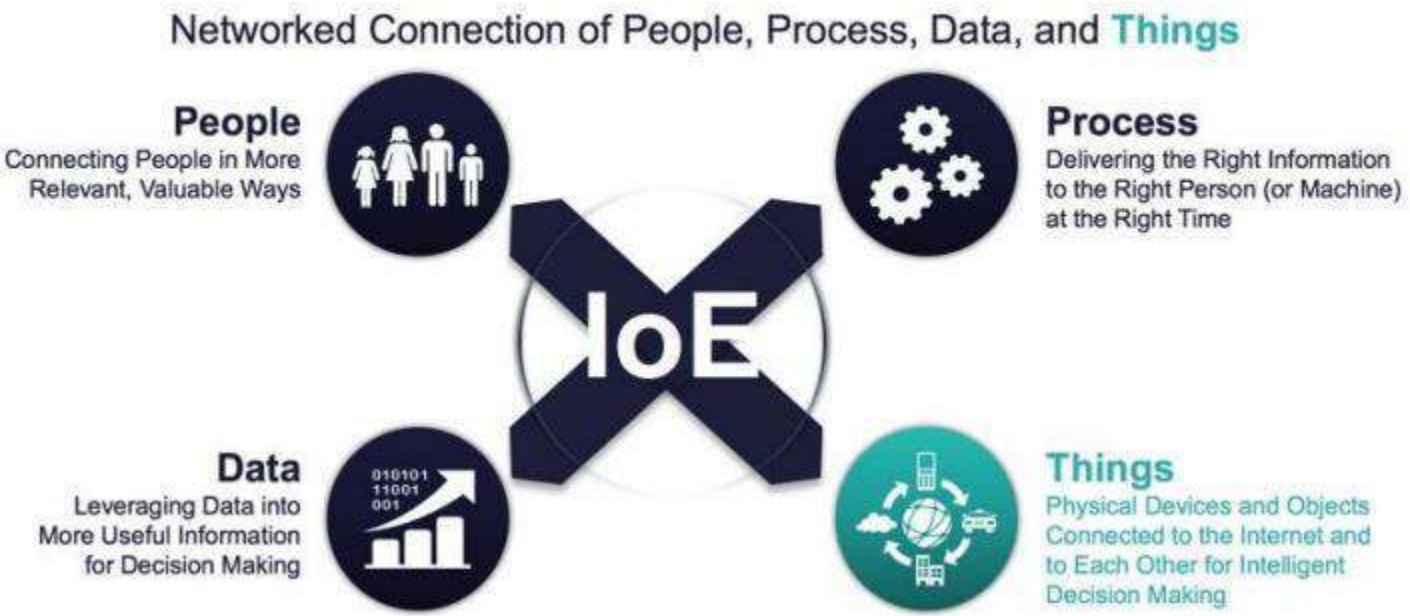
Motivations

- **Connectivité** omniprésente : diversité des solutions de connectivité sans fil, possibilité de connecter —tout‖.
- **Disponibilité et adoption généralisée de IP** (Internet Protocol).
- **Miniaturisation** et **coût faible** des composants électroniques.
- Progrès dans le **domaine Cloud Computing** : disponibilité des services qui permettent de bénéficier de capacités de calcul avec les objets physiques.
- Progrès dans le domaine **Big Data** : une multitude d'algorithmes sont disponibles pour collecter et analyser les données.
- Croissance du **marché de masse :** la vision du monde connecté a atteint une maturité et l'engagement est irréversible

Machine-to-Machine M2M

- M2M est une sous-classe de l'IoT.
- M2M : Machine to Machine, échange de données entre deux machines sans intervention humaine.
- M2M fait référence à des technologies permettant aux systèmes sans fil et câblés de communiquer avec d'autres périphériques du même type.
- M2M utilise un dispositif (capteur) pour capturer un événement (température, niveau de pollution, etc.) transmis via un réseau (sans fil, câblé ou hybride) à une application (logiciel) qui convertit l'événement capturé en données significatives.

Internet of Every Things



Source : The Internet of Everything | Plutomen Technologies

M2M versus IoT versus IoE

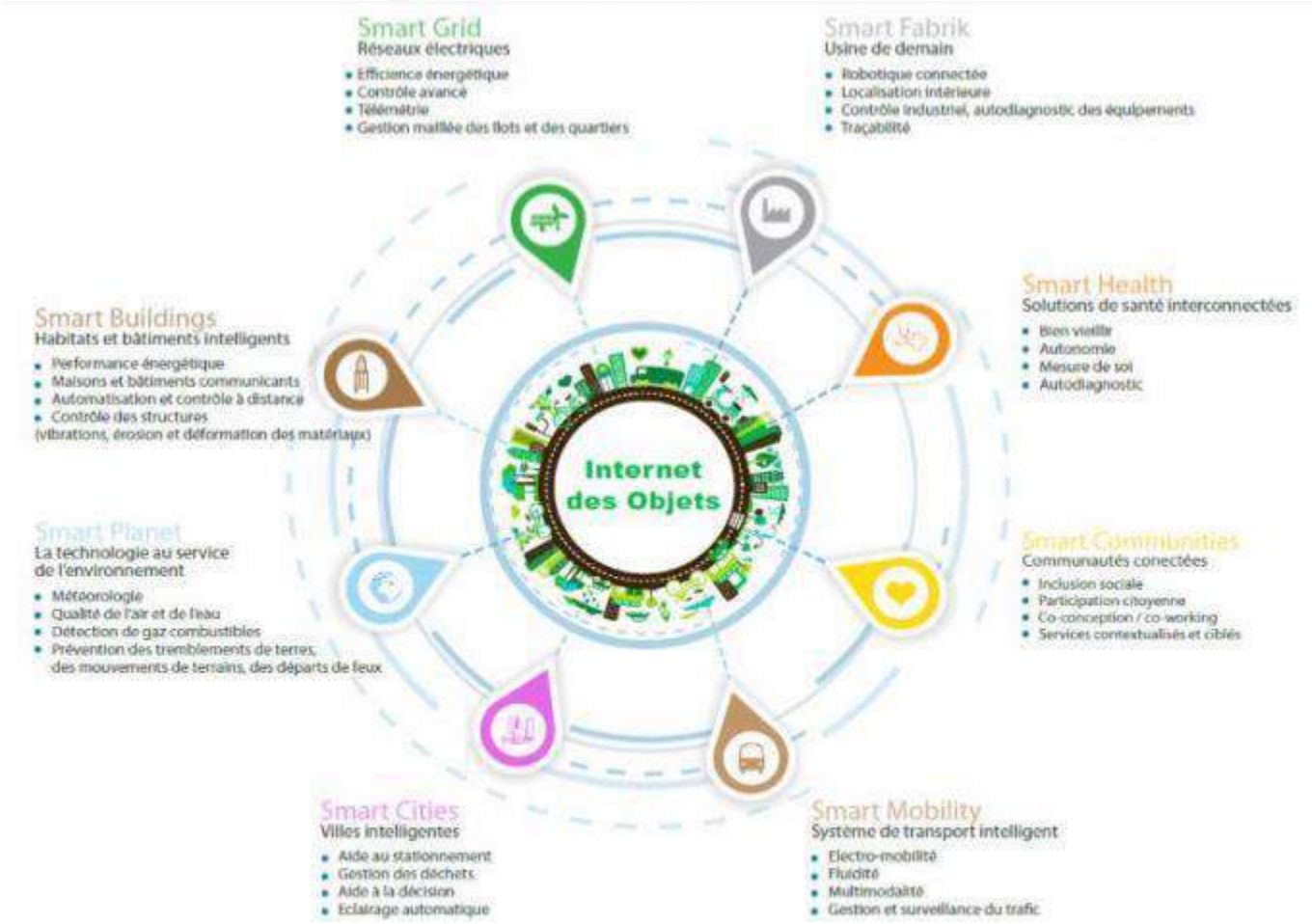
- M2M : Un périphérique qui capture un événement et le transmet sur le réseau à une application. L'application traduit l'événement en informations significatives.
- IoT : IoT Un réseau d'éléments identifiables de manière unique qui communiquent sans interaction humaine à l'aide de la connectivité IP.
- IoE Rassemble non seulement l'Internet des Objets mais également les processus, les données et les personnes (via smartphones et réseaux sociaux).

Quizz N°1

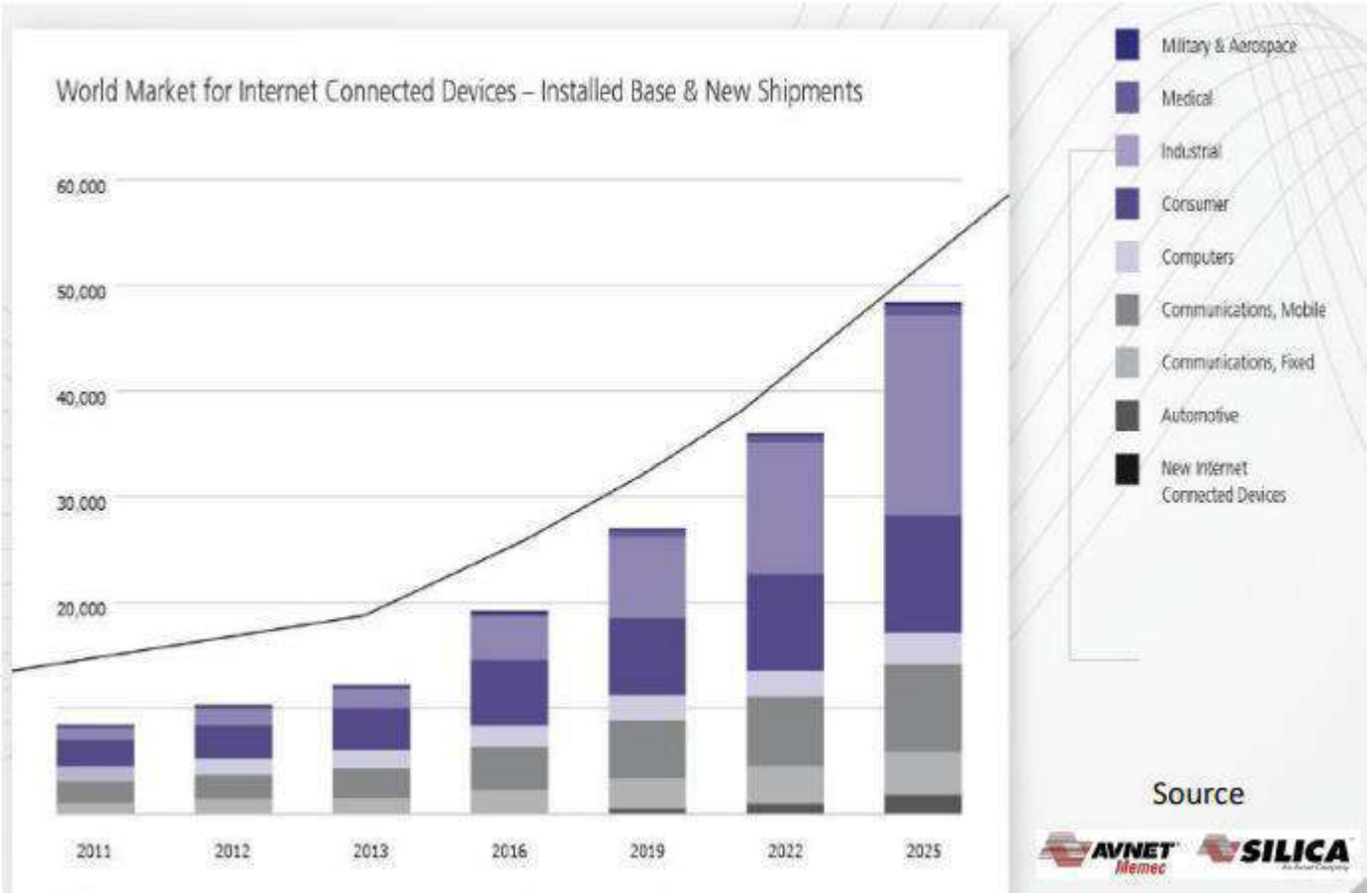
Quelles sont les caractéristiques d’un objet connecté?

Partie 2: Marché IoT, Opportunités et challenges

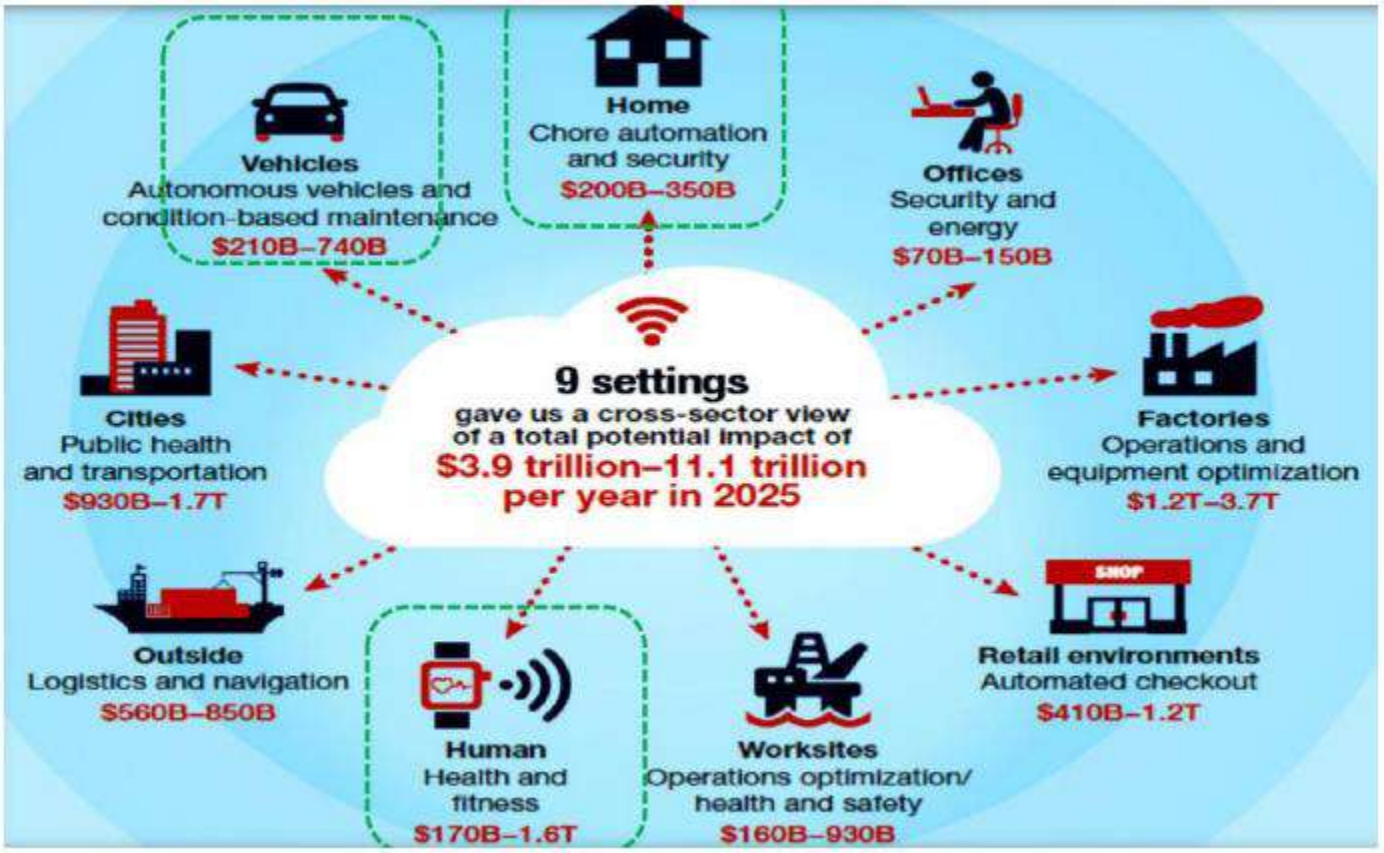
Marché IoT


Smart Grid
Réseaux électriques
• Efficience énergétique
• Contrôle avancé
• Télémétrie
• Gestion maillée des îlots et des quartiers
Smart Fabrik
Usine de demain
• Robotique connectée
• Localisation intérieure
• Contrôle industriel, autodiagnostic des équipements
• Traçabilité
Smart Buildings
Habitats et bâtiments intelligents
• Performance énergétique
• Maisons et bâtiments communicants
• Automatisation et contrôle à distance
• Contrôle des structures
(vibrations, érosion et déformation des matériaux)
Internet des Objets
Smart Health
Solutions de santé interconnectées
• Bien vieillir
• Autonomie
• Mesure de soi
• Autodiagnostic
Smart Planet
La technologie au service de l'environnement
• Météorologie
• Qualité de l'air et de l'eau
• Détection de gaz combustibles
• Prévention des tremblements de terres, des mouvements de terrains, des départs de feux
Smart Communities
Communautés conectées
• Inclusion sociale
• Participation citoyenne
• Co-conception / co-working
• Services contextualisés et ciblés
Smart Cities
Villes intelligentes
• Aide au stationnement
• Gestion des déchets
• Aide à la décision
• Eclairage automatique
Smart Mobility
Système de transport intelligent
• Electro-mobilité
• Fluidité
• Multimodalité
• Gestion et surveillance du trafic

Explosion du marché des objets connectés



Impact économique de l'IoT

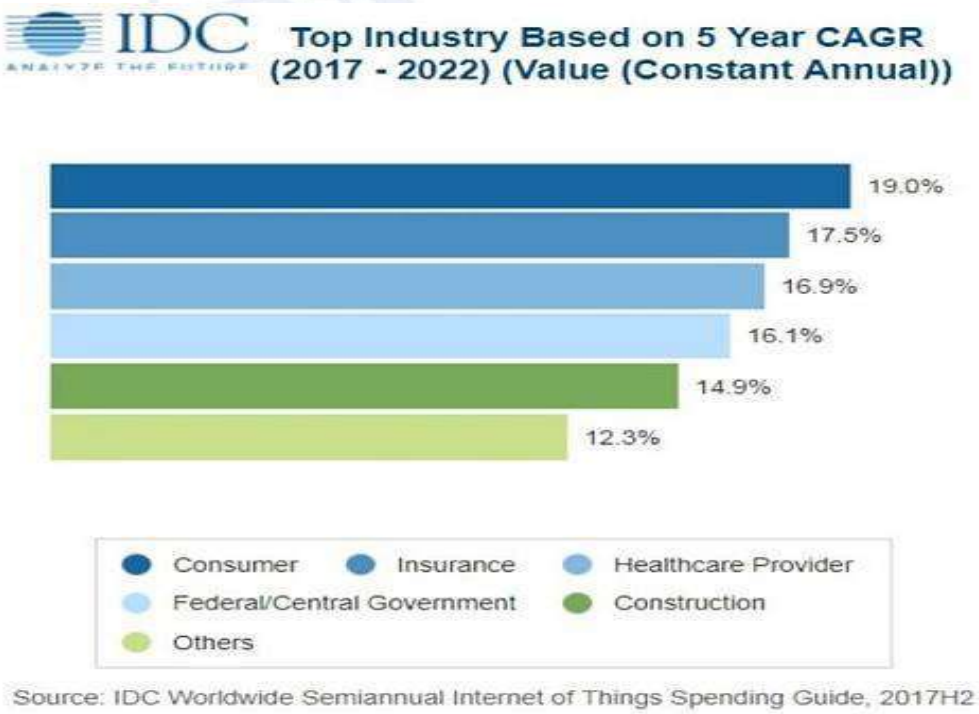


LPWAN will represent +26% of IoT Market

Source: McKinsey, June 2015

Estimation des dépenses dans l'IoT

Les dépenses dans l'IoT atteindraient 1 200 milliards de dollars en 2022

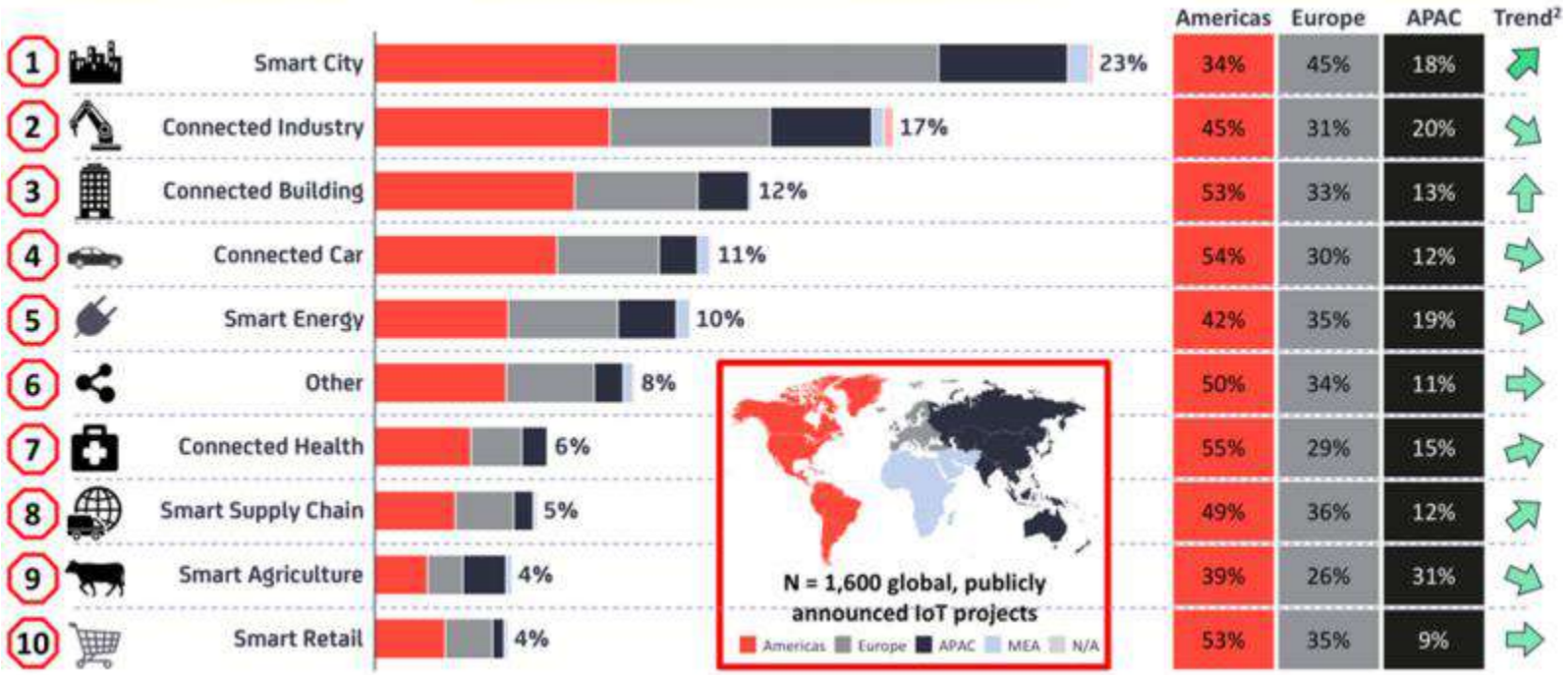


Part des projets IoT par secteur économique

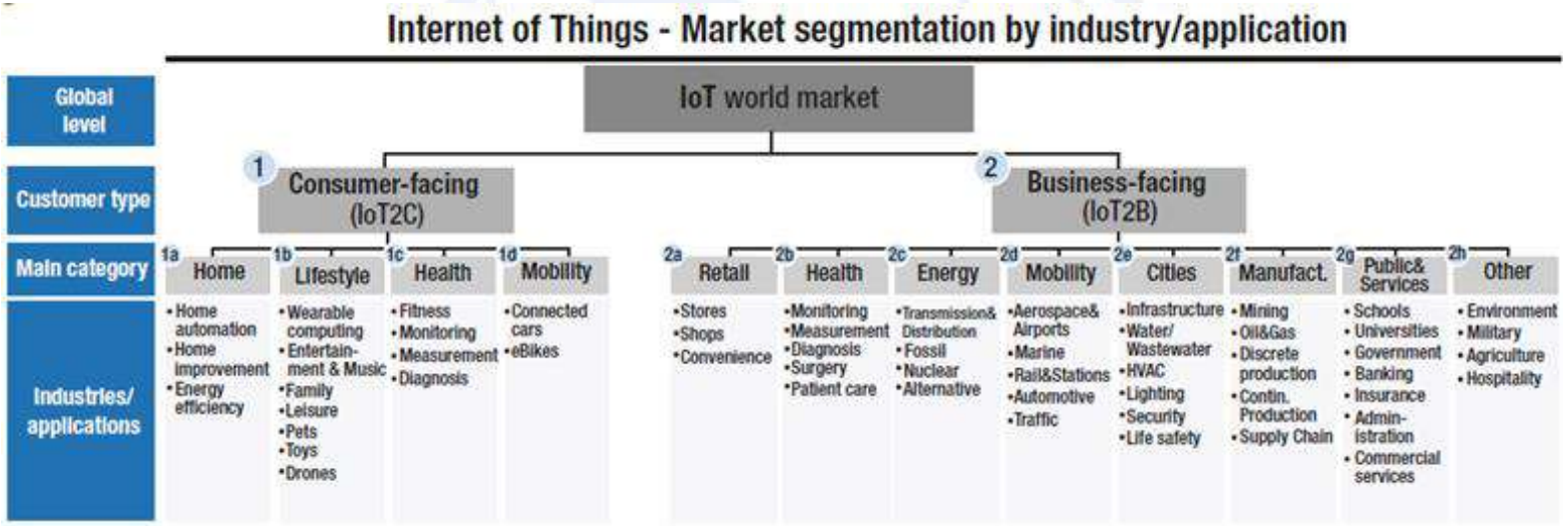
Segment IoT

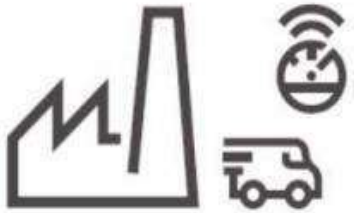
Part du marché mondial des projets IoT

Détails



Segmentation du marché par industrie/application



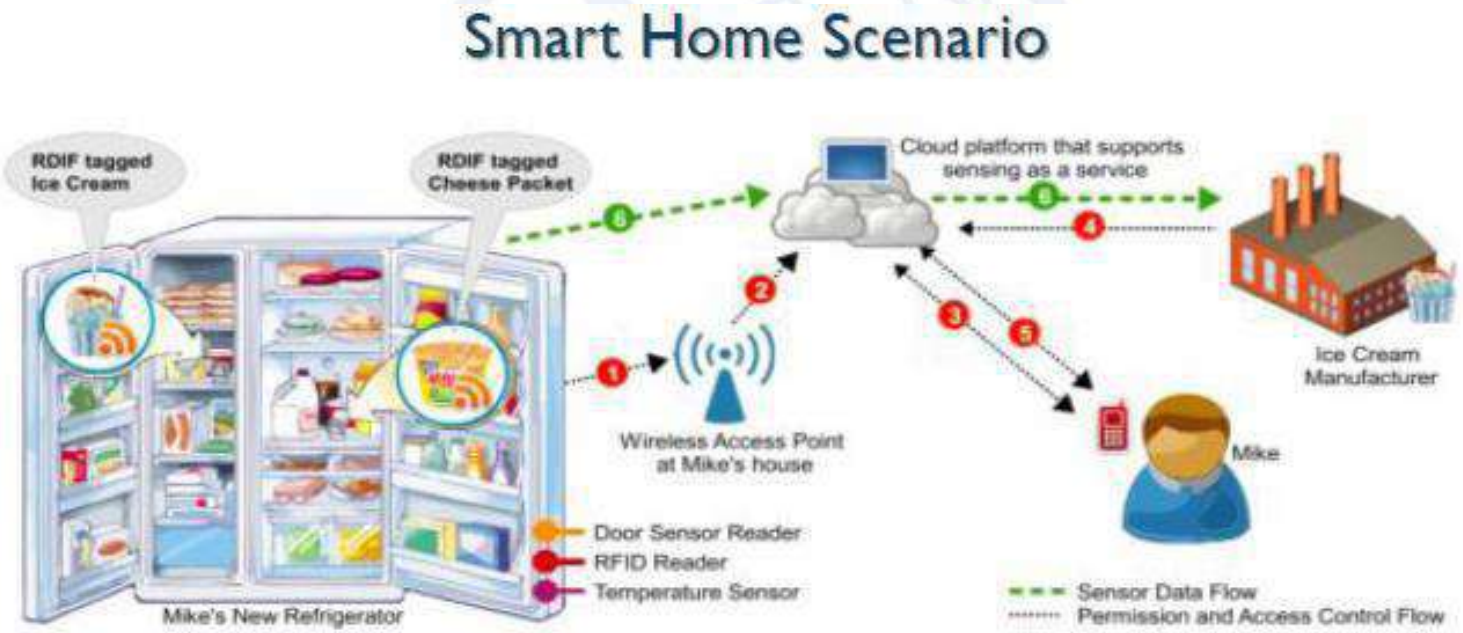
Category	Sub-category	
Consumer IoT	Consumer electronics	Smart TVs, home entertainment (games consoles, speakers), personal entertainment (MP3 players, portable gaming devices), set-top boxes
	Smart home	Home appliances (fridges, washing machines), home infrastructure (routers), home security (alarms), energy monitoring (thermostats)
	Wearables	Fitness trackers (including personal health trackers), smart watches
	Smart vehicles	Connected cars, connected bikes, insurance telematics
	Consumer – others	Trackers for children, the elderly and pets, as well as drones and robots
Industrial IoT	Smart city	Public transport, surveillance, electric vehicle charging, street lighting, parking, waste management
	Smart utilities	Energy, water and gas smart metering, smart grid
	Smart retail	PoS, digital signage, vending machines, ATMs
	Smart manufacturing	Inventory tracking, monitoring and diagnostics, warehouse management
	Smart buildings	Heating and air con, security, lighting, hot desks, office equipment
	Health	Remote monitoring of medical devices, emergency vehicle infrastructure
	Enterprise – others	Fleet management, applications in agriculture, oil, mining, construction

Segmentation du marché par industrie/application

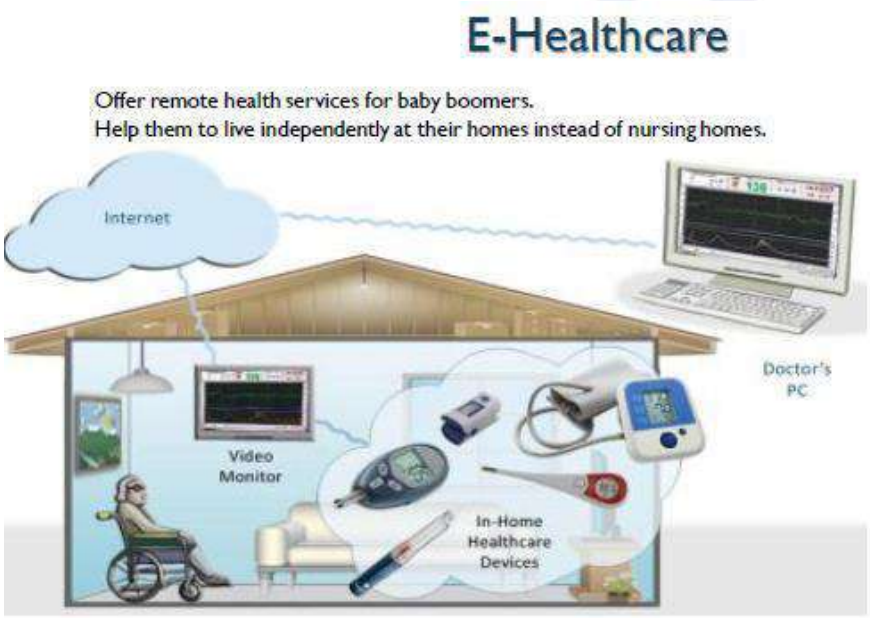
- Selon IoT analytics, les objets connectés sont classés en 2 catégories:
  - **Objets connectés Grand Public** sont des objets dédiés au grand public (wearables) : montre, bracelet, vêtement, etc. La vraie **valeur d'un objet connecté** est dans l'**usage** améliorée qu'il va apporter à son utilisateur.
  - **Objets connectés dans le B2B** sont **source de nouveaux business**. Gartner assure que les objets connectés à usage industriel se vendront moins que ceux destinés au grand public dans les années qui viennent, mais ils rapporteront plus d'argent.
- Les entreprises doivent passer d'une offre de produit à une **offre de service**, gage de plus de valeur.

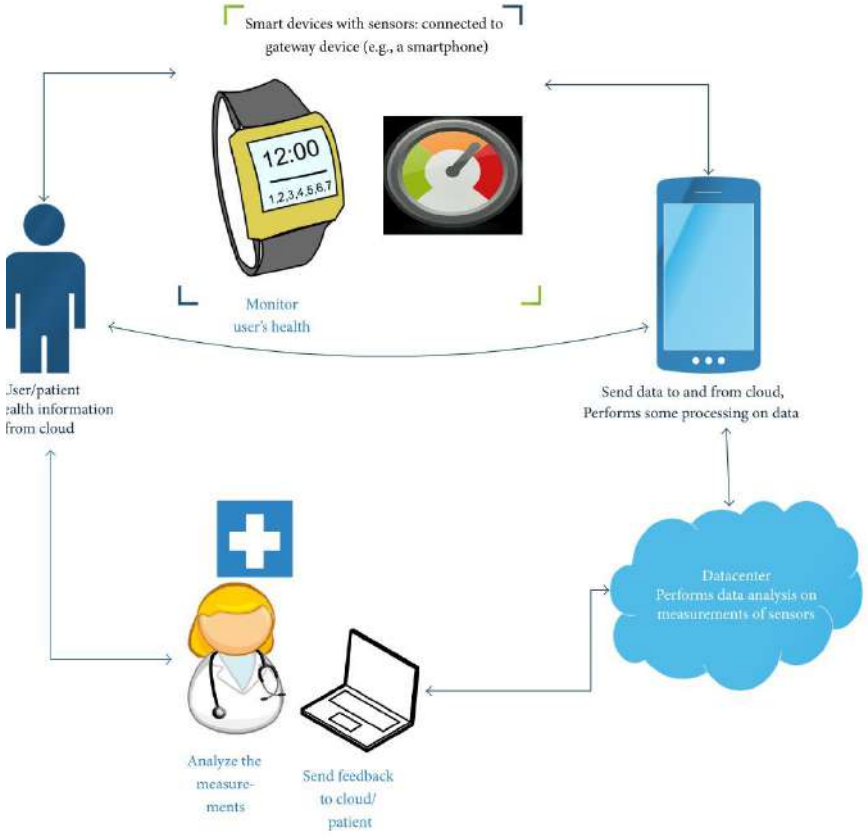
Maison intelligente

Maison intelligente



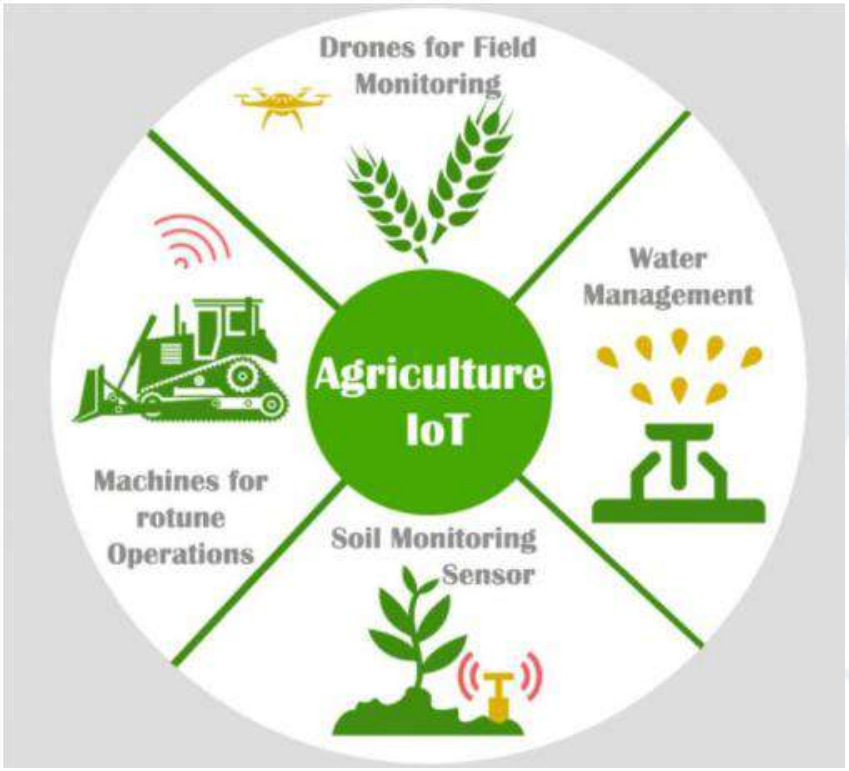
Santé et bien être



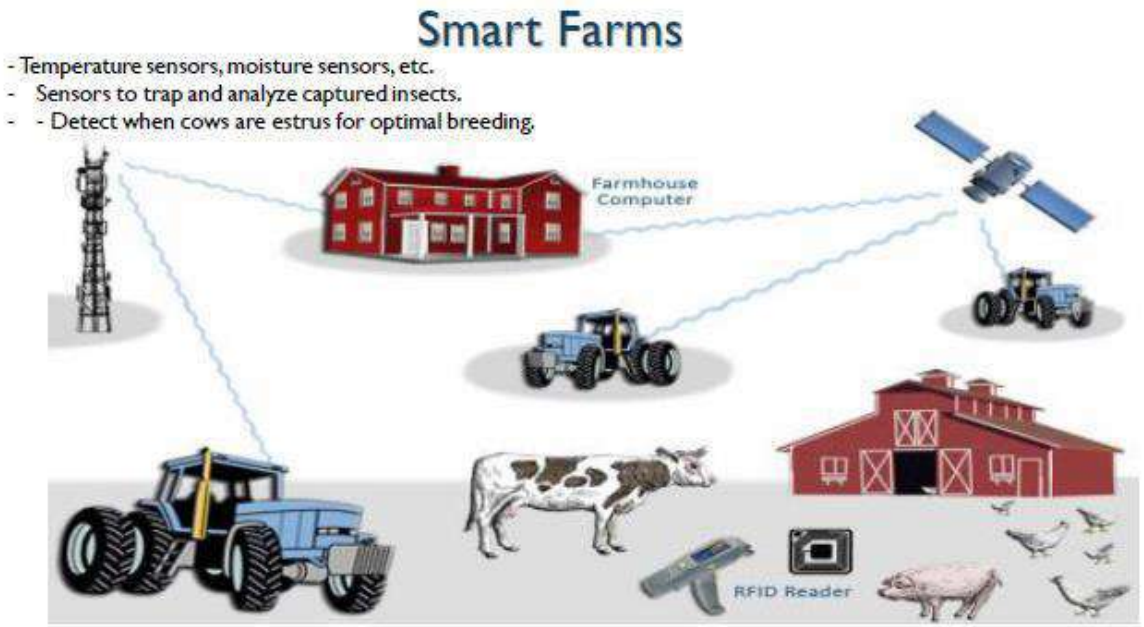


Gestion des déchets dans les vielles intelligentes

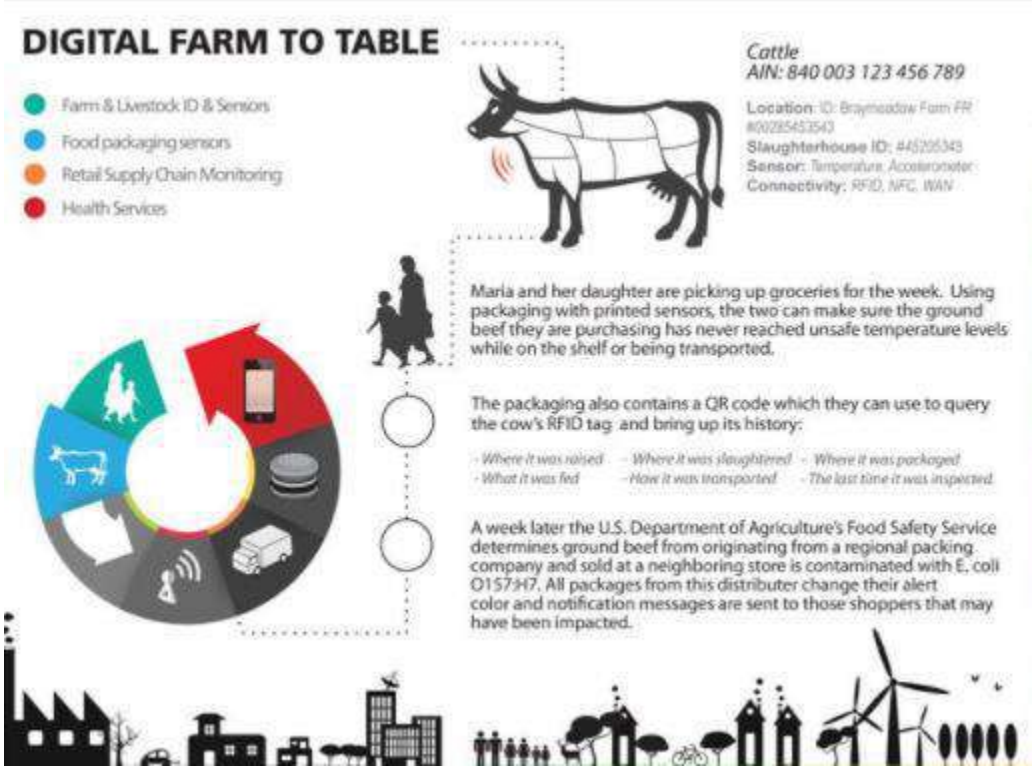
Agriculture intelligente



Ferme intelligente

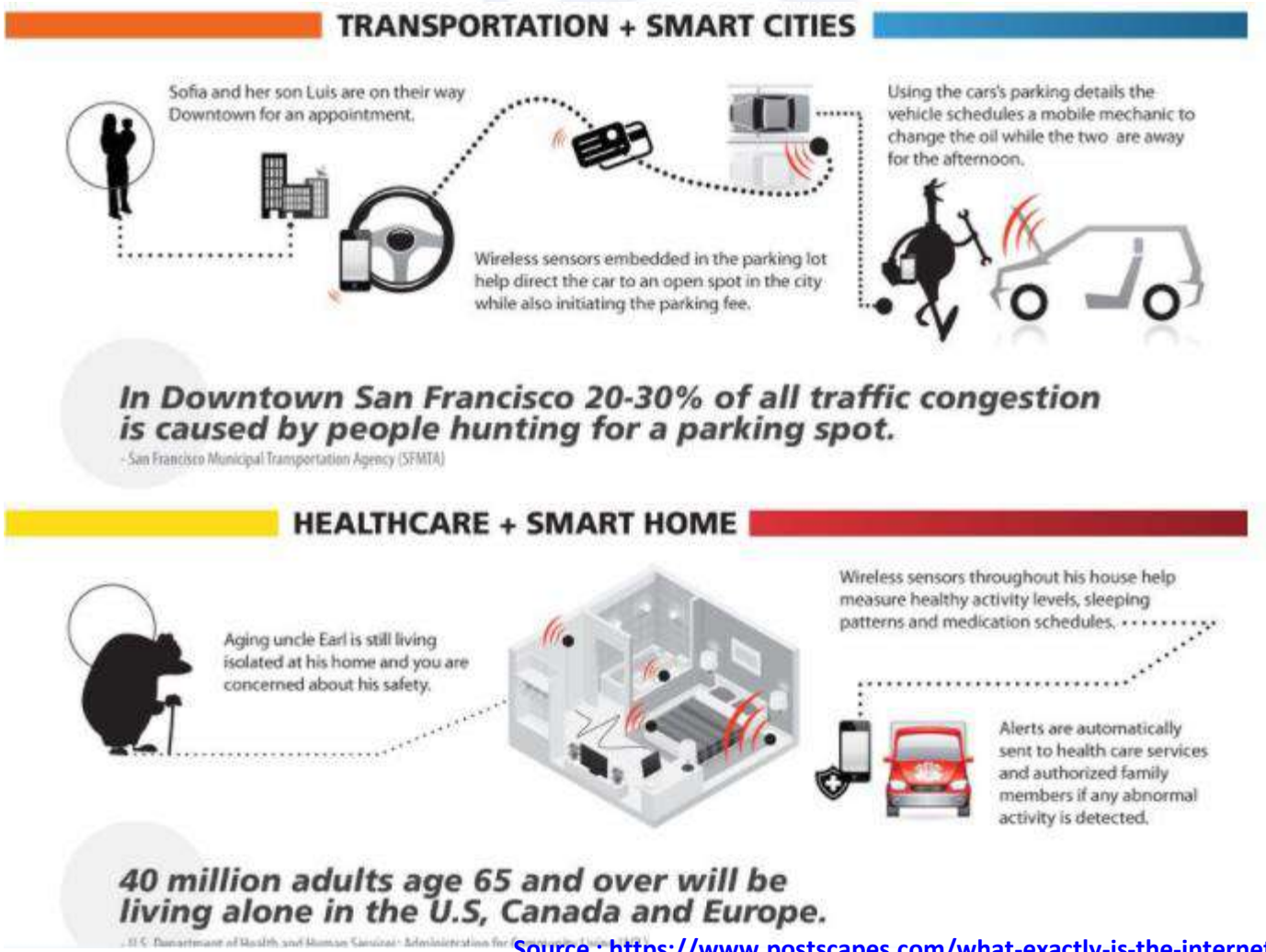


Ferme intelligente



Bâtiment intelligentes

Applications IoT



Source : https://www.postscapes.com/what-exactly-is-the-internet-of-things-infographic/

Valeur potentielle / niveau de risque de l'IdO par vertical

Source: OLIVER WYMAN

Technologies clés génériques

- L'IoT fonctionne avec le support de plusieurs technologies tels que les réseaux de capteurs sans fil, le Cloud Computing, les analyses Big Data, les protocoles de communication, les services web, etc.
  - Les réseaux de capteurs sans fil RCSF: (Wireless Sensor Network, WSN) Un RCSF se compose d'un nombre de Noeuds-Capteurs qui ont des fonctionnalités de capturer et traiter/transmettre les données.
  - Cloud Computing : fournit un espace de stockage de données IoT et offre des services de visualisation, analyse et archivage des données.
  - Big Data : offre des outils d'analyse avancées pour les données massives collectées par les objets IoT selon leurs caractéristiques : volume, vitesse, variabilité (forme de données : texte, audio, video, image).

Technologies clés génériques

- Les protocoles de communication : sont indispensables pour assurer la connectivité entre objets et applications. Les protocoles de communication définissent le format des données, taille paquets, adressage, routage, etc.
- Les systèmes embarqués : Les objets connectés sont formés essentiellement des cartes à microcontrôleur intégrant un microprocesseur, une mémoire et des ports d‘ E/S pour la connexion des capteurs.

Challenges

- Disponibilité et fiabilité : La méthode de collecte et de transmission des informations influence fortement la qualité des données fournies.
- Interopérabilité : l'hétérogénéité et la diversité des environnements logiciels et matériels des objets.
- Sécurité et confidentialité : nécessité de sécuriser et cloisonner les données échangées.
- Evolutivité et passage à l'échelle (Scalabilité) : trouver des solutions flexibles pour le passage à l'échelle dans un scénario d'objets dispersés et nombreux.

Challenges

- Politique réglementaire : la réglementation n’est pas adaptée pour des applications IoT spécifiques. Par exemple, les entreprises investissent énormément dans ce domaine, mais l’autorisation de circulation des voitures autonomes n'est toujours pas clair du point de vue réglementaire.
- Propriété intellectuelle : Une compréhension commune des droits de propriété entre les parties prenantes devrait être clairement défini pour libérer tout le potentiel de l'IoT. La question demeure ouverte, par exemple dans les dispositifs médicaux implantés dans le corps d'un patient, la question du droit sur le données générées, le patient ou le fabricant de l'appareil.

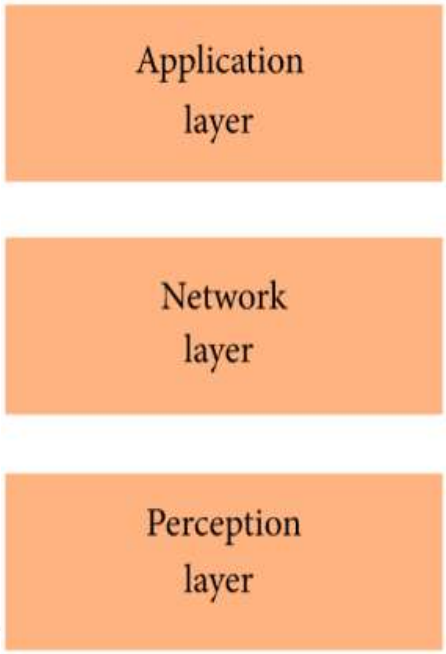
Quizz N°2

1. Quels sont les secteurs qui peuvent créer de la valeur économique en Afrique, à votre avis? Pourquoi?

Partie 3:
Architecture et composants de l'IoT

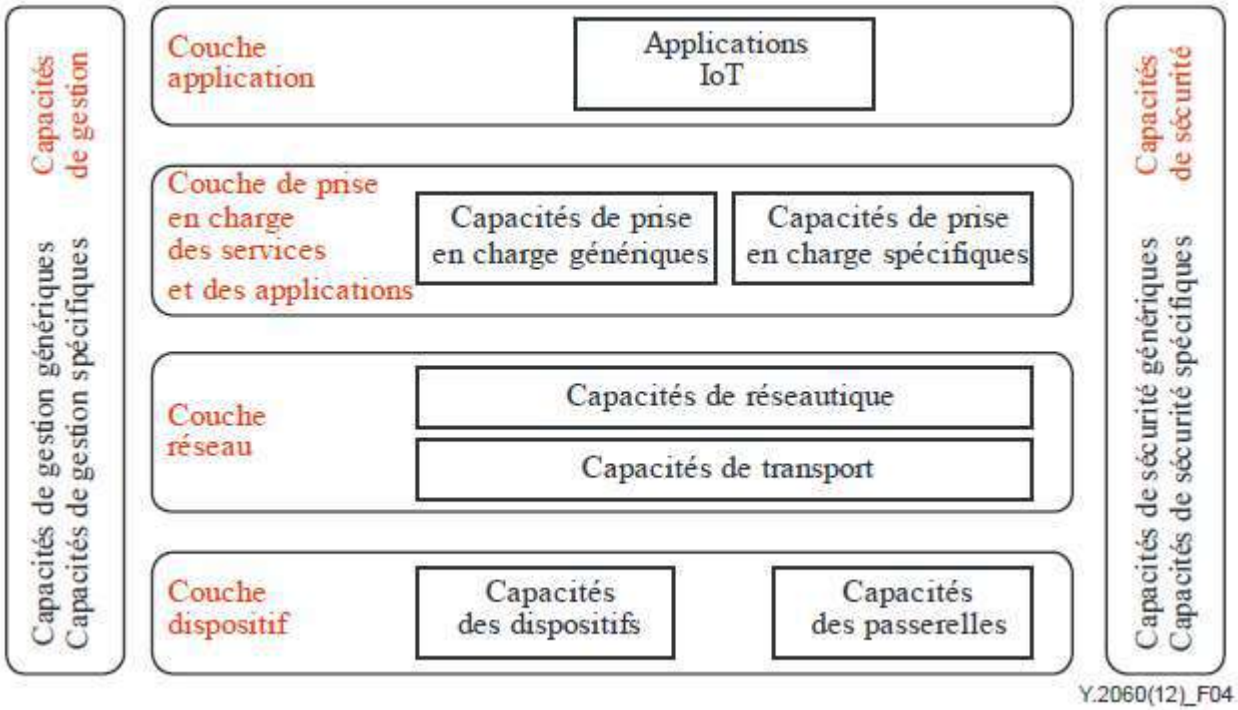
Architecture de l'IoT

- L'architecture d'une solution IoT varie d'un système à l'autre en se basant sur le type de la solution à mettre en place.
- L'architecture la plus élémentaire est une architecture à trois couches:
  - **La couche perception** possède des capteurs et actionneurs qui détectent et recueillent des informations sur l'environnement.
  - **La couche réseau** est responsable de la connexion, du transport et du traitement des données issues des capteurs et actionneurs.
  - **La couche application** est chargée de fournir à l'utilisateur des services spécifiques et applications intelligentes.



Modèle de référence de l'IoT

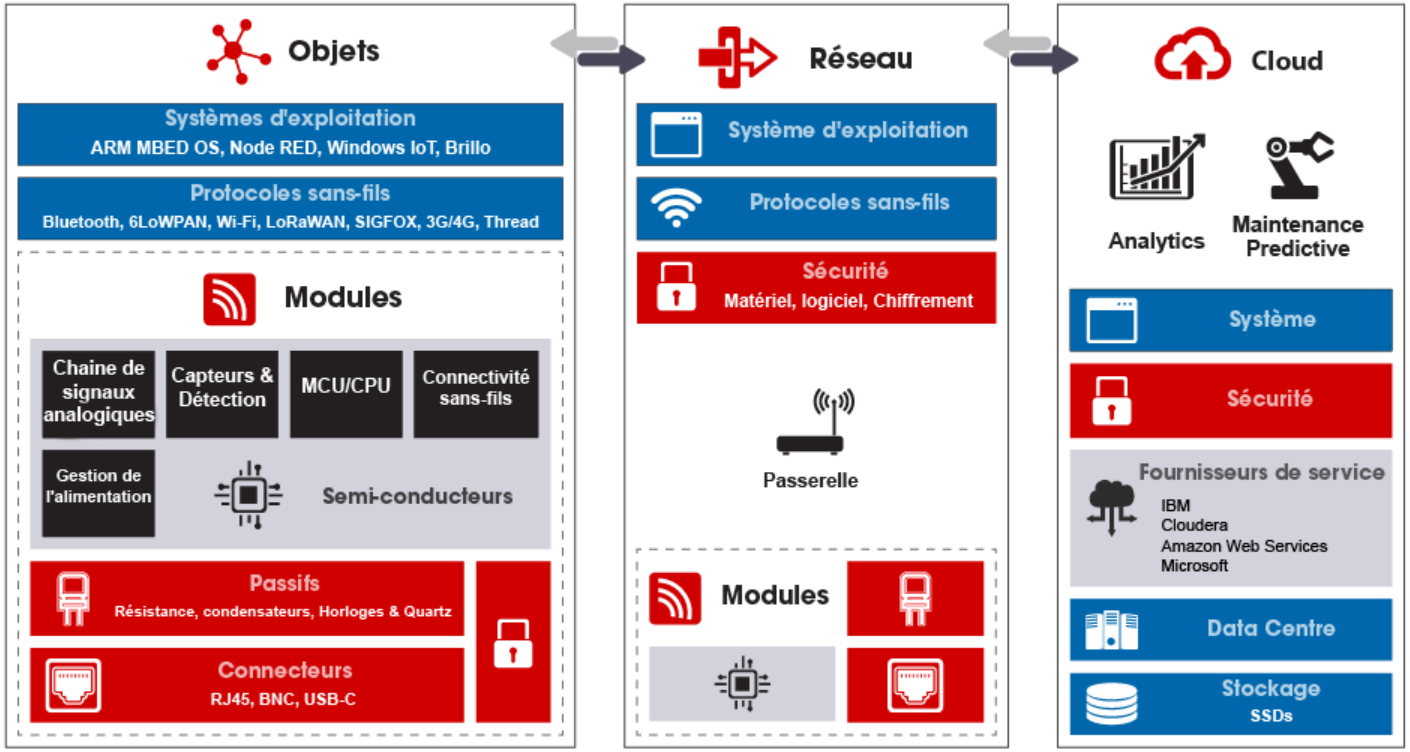
- Modèle de référence de l'IoT selon la recommandation UIT-T Y.2060



Composantes d'une solution IoT

- Généralement, une solution IoT est formée des composants suivants :
  - Objet (Module-capteur)
  - Capteurs, Actionneurs
  - Passerelle (Gateway)
  - Cloud (Informatique en nuage)

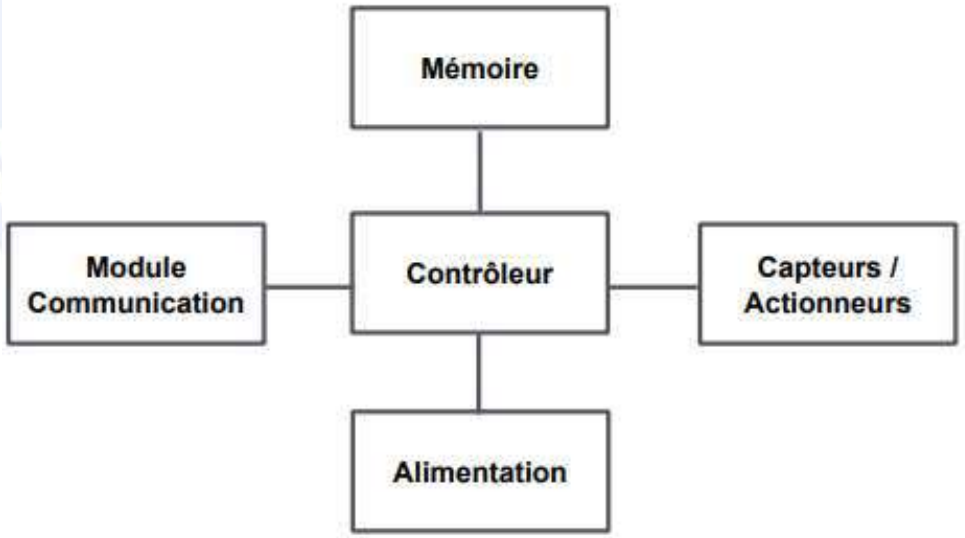
Architecture fonctionnelle d'une solution IoT



Source : https://fr.rs-online.com/web/generalDisplay.html?id=i/ido-internet-des-objets

Niveau 1 : Capteurs et actionneurs

- **Unité de détection :** Capteur/ Actionneur
- **Unité de traitement :** Contrôleur
- **Unité de communication** : Module RF
- **Alimentation**

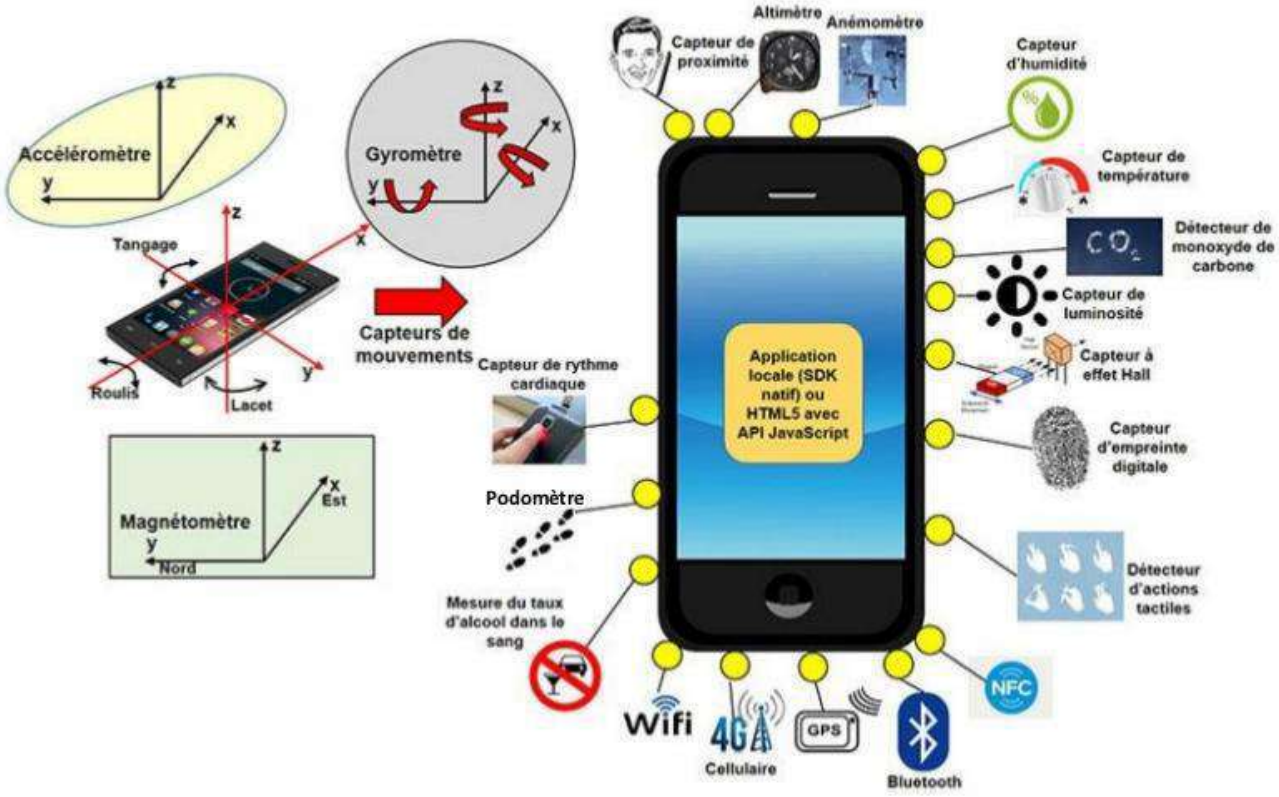


Niveau 1 : Capteur/actionneur

- Capteur : C’est un dispositif utilisé pour détecter un événement ou une grandeur physique, tels que luminosité, température, humidité du sol, pression, etc. et qui fournit un signal électrique correspondant.

- Les capteurs IoT sont généralement de petite taille, ont un faible coût et consomment moins d’énergie.
- Les signaux produits par un capteur sont traités par un microcontrôleur pour l‘interprétation, l‘analyse et la prise de décision.

Capteurs d'un smart phone



Niveau 1 : Capteur/actionneur

- Capteurs à air – Des capteurs qui détectent le niveau de pollution de l'air en milieu urbain et donnent des mesures pour protéger la santé des personnes.
- Bâtiments - Des capteurs qui surveillent les vibrations et les conditions des matériaux dans les bâtiments, les ponts et les monuments historiques et fournissent des «avertissements précoces» en cas de dommages.
- Véhicules de distribution - Des capteurs qui détectent l'allocation géographique de chaque véhicule dans un parc sont utilisés pour optimiser les itinéraires et créer des estimations précises des heures de livraison.
- Utilisation de l'énergie - Capteurs qui surveillent l'énergie, utilisée pour vérifier l'efficacité énergétique de la «construction verte» .
- Gaz dangereux - Des capteurs qui détectent les niveaux de gaz explosifs ou toxiques dans les environnements industriels et à l'intérieur, permettent une action immédiate pour garantir la sécurité des personnes.

Niveau 1 : Capteur/actionneur

- Santé - Les capteurs qui mesurent les données métriques vitales, la pression sanguine et la tension artérielle, sont utilisés pour surveiller les patients.
- Geo-localisation - Les capteurs qui détectent l'emplacement géographique d'un objet sont utilisés pour suivre les objets.
- Machines - Capteurs qui surveillent l'état des pièces de la machine, par exemple en mesurant la température, la pression, les vibrations et l'usure générée.
- Parking spaces - Capteurs qui sont utilisés pour détecter si un espace de stationnement est libre.
- Accès au périmètre - Les capteurs qui détectent la présence des personnes dans les zones non autorisées sont plus efficaces que les gardes de sécurité humains.

Niveau 1 : Capteur/actionneur

- Trafic - Des capteurs qui détectent la vitesse et le nombre de véhicules, sont utilisés pour détecter la congestion du trafic et suggèrent aux conducteurs d'autres itinéraires.
- Déchets - Capteurs qui détectent le nombre de contenants insuffisamment remplis, pour optimiser les itinéraires de collecte des ordures ménagères.
- Capteurs d'eau - qui détectent les fuites d'eau dans le réseau de distribution d'eau.
- Éclairage public - Capteurs qui détectent le mouvement des personnes et des véhicules dans une rue et règlent l'éclairage public au niveau requis.

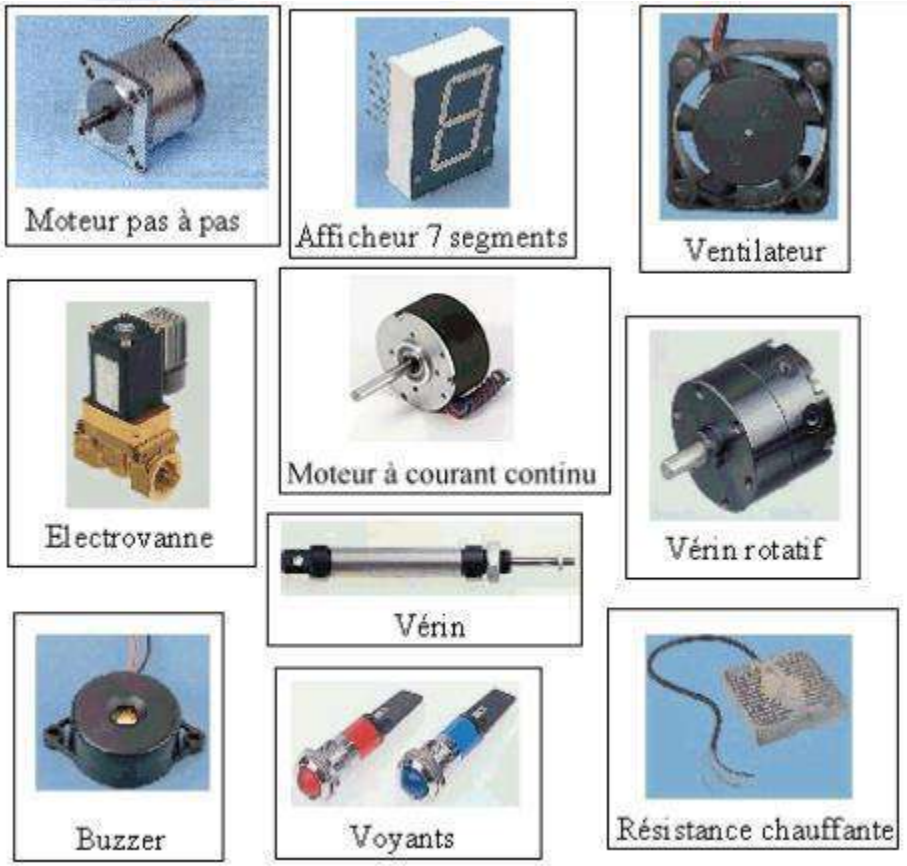
Niveau 1 : Capteur/actionneur

- Rivières – Capteurs qui détectent la pollution du conducteur.
- Conditions de stockage - Les capteurs qui surveillent les conditions de stockage des denrées périssables.
- Incompatibilité de stockage - Capteurs qui détectent des produits dangereux qui ne sont pas autorisés à être conservés ensemble; par exemple, des produits inflammables et des explosifs.
- Capteurs médicaux capables de mesurer différents paramètres tels que la fréquence cardiaque, le pouls, la pression artérielle, la température corporelle, la fréquence respiratoire, et la glycémie.

Capteurs de santé

Niveau 1 : Capteur/Actionneur

- Actionneur : une technologique complémentaire aux capteurs, convertit l'énergie électrique en mouvement ou énergie mécanique.
- Les actionneurs permettent de transformer l'énergie reçue en ur phénomène physique (déplacement, dégagement de chaleur, émission de lumière …).
- Exemple : Haut-parleurs qui convertissent les signaux électriques correspondants en sons ondes (acoustiques).l



Niveau 1 : Capteur/Actionneur

- Les actionneurs, qui induisent un mouvement, peuvent être classés en 3 catégories:
  - Les actionneurs hydrauliques facilitent le mouvement mécanique en utilisant un fluide ou une puissance hydraulique.
  - Les actionneurs pneumatiques utilisent la pression de l'air comprimé; et
  - Les actionneurs électriques utilisent l'énergie électrique.

Niveau 1 : Capteur/actionneur

- Un microcontrôleur (µc, MCU en anglais) est un circuit intégré et compact qui comprend un processeur, une mémoire et des périphériques d‘entrée et de sortie sur une seule puce.
- Un MCU est conçu pour traiter les données brutes capturées par les capteurs et extraire des informations utiles.

Niveau 1 : Capteur/actionneur

- Exemples de cartes à microcontrôleurs

Arduino

- Basé sur un µc Atmega (Single core, 16MHz)
- Connexion simple
- Programmation facile
- Bon choix pour les capteurs

STM32

- Basé sur un µc ARM 32 bits (24-400MHz)
- Bon choix pour les capteurs
- Bon choix pour le traitement local

NodeMCU

- Basé sur le µc ESP8266 (Single core, 80MHz)
- Programmation facile
- Intègre WiFi

Pycom Lopy4

- Basé sur le µc ESP32(Dual core, 160-180MHZ)
- Programmation facile
- Connectivité : WiFi, Bluetooth, Sigfox, LoRa

Source: https://fr.rs-online.com/web/generalDisplay.html?id=i/ido-internet-des-objets

Niveau 2 : Passerelle

- Une passerelle (gateway) est une combinaison de composants matériels et logiciels utilisés pour connecter un réseau à un autre.
- Les gateways permettent de relier les capteurs ou les nœuds de capteurs avec le monde extérieur.
- Les gateways sont donc utilisées pour la communication de données en collectant les mesures effectuées par les nœuds de capteurs et en les transmettant à l'infrastructure Internet.
- La gateway peut faire des traitements locaux sur les données avant de les relayer au Cloud.
- Exemples de gateways:

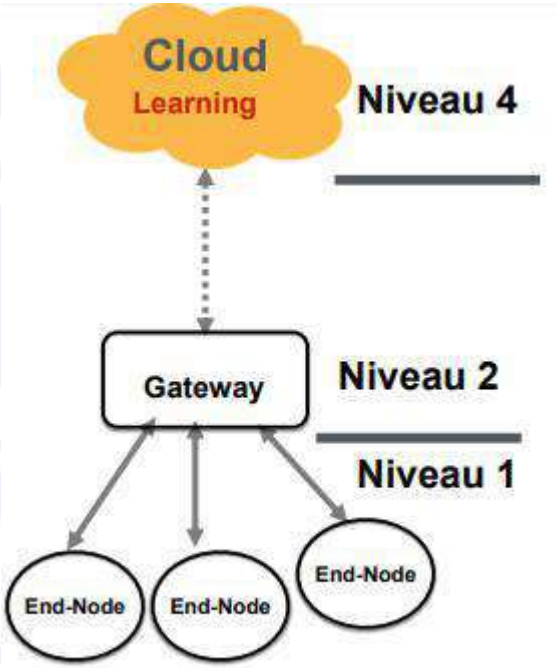
Raspberry Pi

Intel Galileo

Beaglebone Black

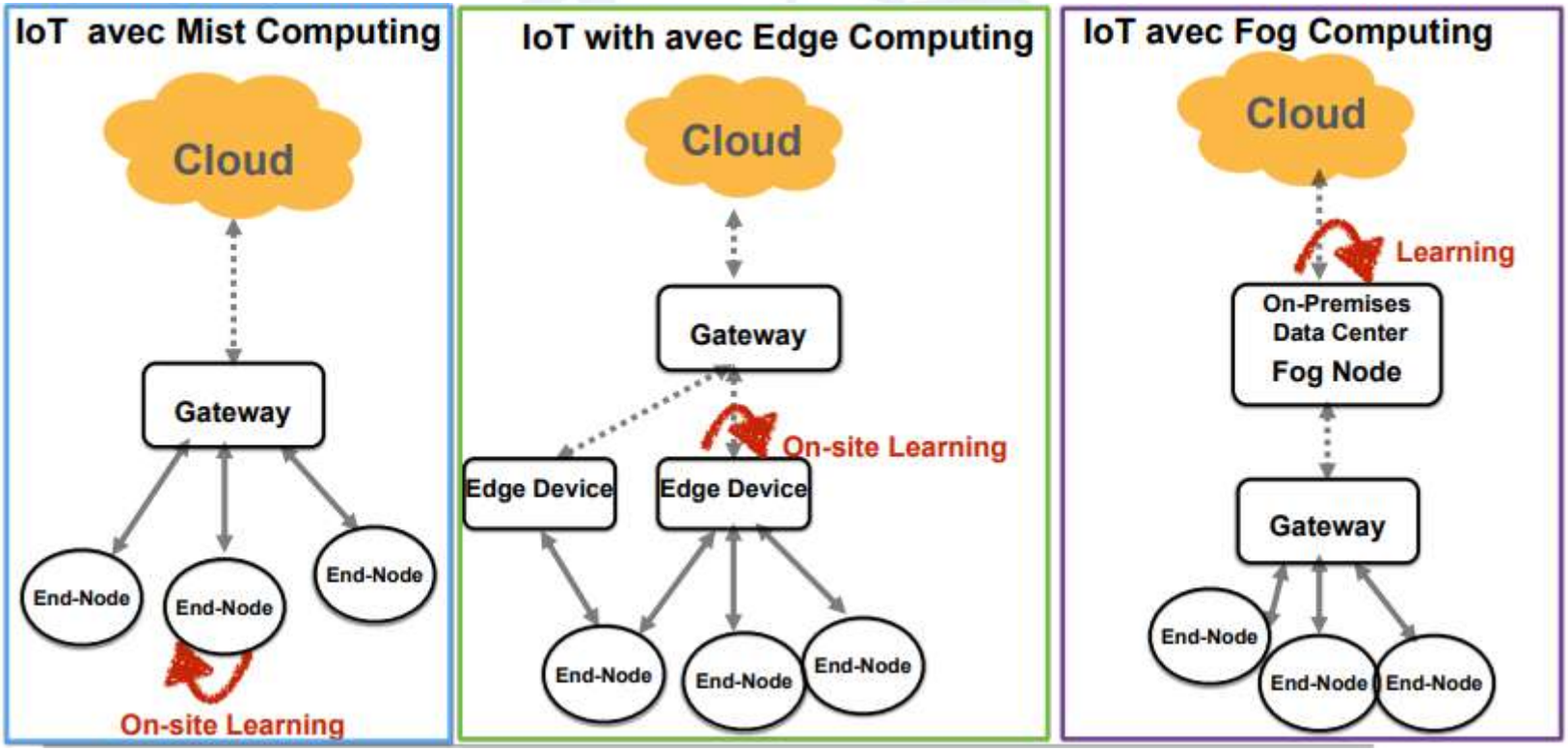
Niveau 3 : Cloud computing

- Le niveau 3 est un choix technologique (optionnel) qui permet d'alléger la charge du travail vers le Cloud et de faire des traitements locaux —on the Edge‖.
- Trois solutions techniques sont possibles pour l'implémentation du 3ème niveau :
  - Fog Computing : permet un calcul décentralisé en traitant les données IoT au niveau des noeuds locaux —Fog‖ avant de relayer l'information vers le cloud.
  - Edge Computing : le traitement des données IoT se fait à l'extrémité du réseau (Gateways ou des noeuds intermédiaires entre objets et gateways).
  - Mist Computing : le traitement des données se fait localement dans le noeud capteur.



Infrastructure IoT basique

Cloud Versus Fog Versus Edge



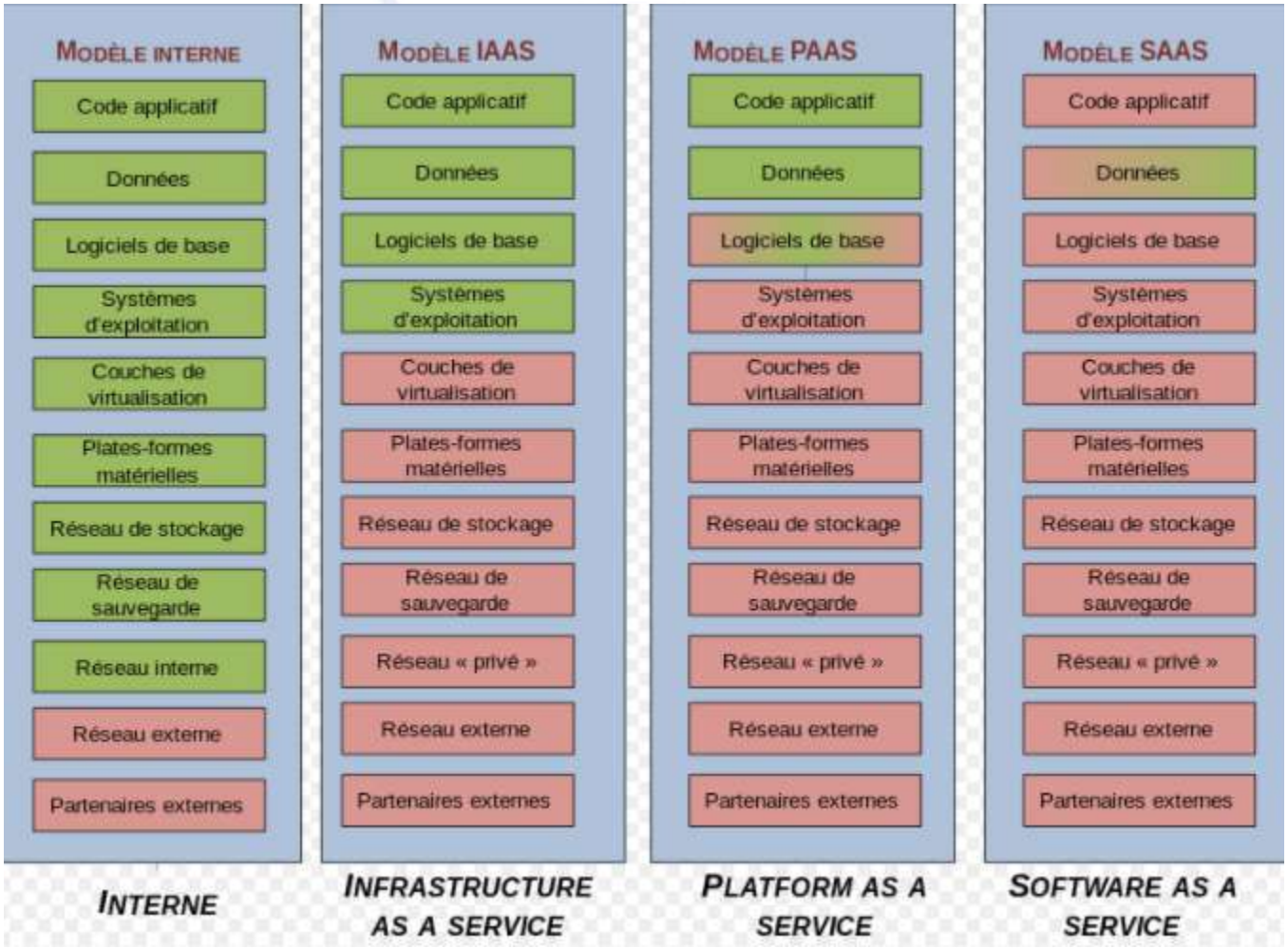
Niveau 3 : Edge Computing

- Avantages de l'architecture Edge
  - Le déploiement d'une architecture distribuée repose sur l'idée d'intégration de l'intelligence près des nœuds capteurs, on the « Edge », ce qui diminue par conséquence la dépendance au cloud computing.
  - L'idée est de rapprocher le plus possible le traitement des données et la prise de décisions des nœuds capteurs et réduire ainsi les temps de latence résultant de l'envoi des données au cloud.
  - Le traitement « Edge » des paquets de données brutes permet de renforcer la sécurité localement avant de les relayer au cloud.

Types de cloud IoT

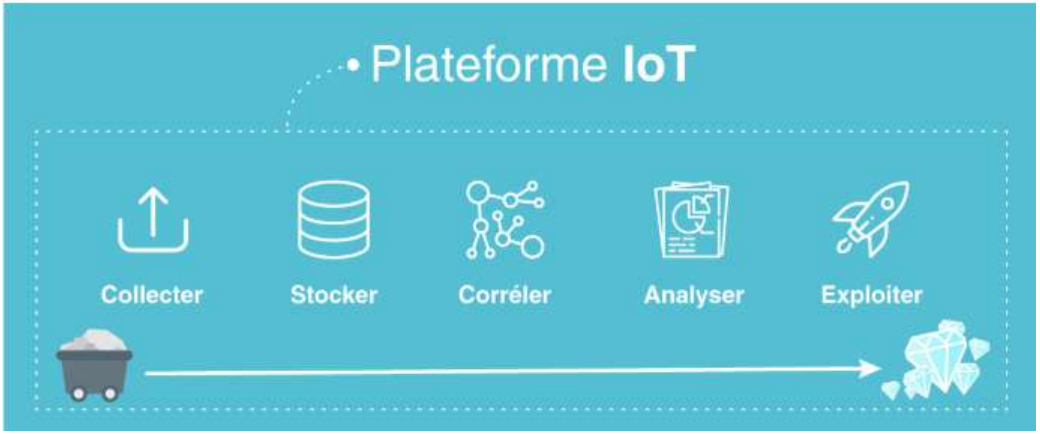
- 3 types de cloud IoT
  - IaaS: Infrastructure as a Service
  - PaaS: Plateforme as a Service
  - SaaS: Software as a Service

IaaS Versus PaaS versus SaaS

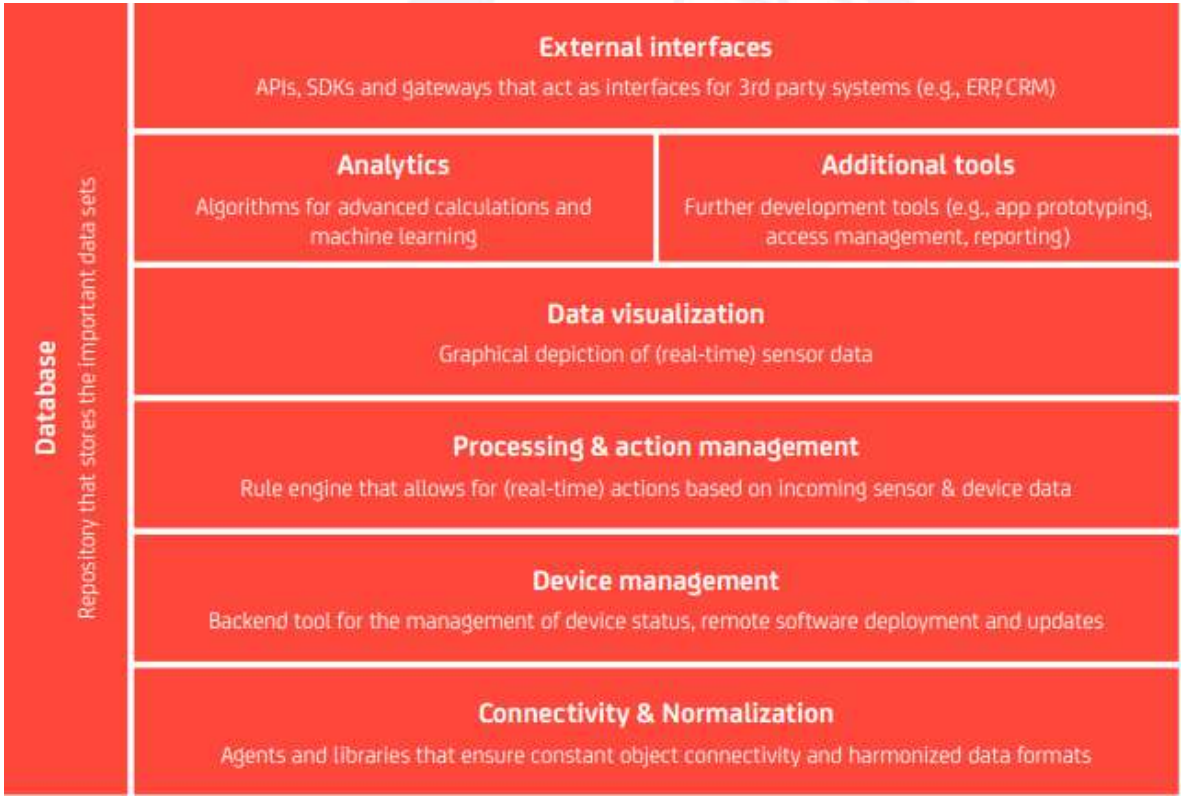


Niveau 4 : Plateformes IoT

- Une plateforme d'IoT est un ensemble de services permettant de collecter, stocker, corréler, analyser et exploiter les données.



Spécifications fonctionnelles d'une plateforme IoT



Source : https://iot-analytics.com/product/iot-platforms-white-paper/

Composants d’une plateforme IoT

Connectivité et normalisation :

- Elle a pour fonction d'apporter différents protocoles et différents formats de données dans une seule interface «logicielle».
- Les dispositifs IoT avancés fournissent généralement **une API** pour mettre en œuvre une interface de communication standardisée avec la Plateforme.
- Très souvent, **des agents logiciels** doivent être développés et installés sur le matériel afin de permettre à la plateforme IoT d'établir une connexion stable.

Composants d’une plateforme IoT

Module de gestion des périphériques

- Ce module s'assure que les objets connectés fonctionnent correctement et que ses logiciels et applications sont mis à jour et fonctionnent.
- Les tâches effectuées dans ce module incluent :
  - Le provisioning du périphérique
  - La configuration à distance
  - La gestion de mises à jour du micrologiciel / logiciel, et
  - Le dépannage.
- L'automatisation de ces tâches devient essentielle pour contrôler les coûts et réduire travail manuel.

Composants d'une plate-forme IoT

Stockage des données

- La gestion des données issues de différents dispositifs IoT apporte aux exigences des bases de données un nouveau niveau:
  - **Le volume.** La quantité de données à stocker peut être massive.
  - **Variété.** Différents dispositifs et différents types de capteurs produisent des formes de données très différentes.
  - **Rapidité**. De nombreux cas IoT nécessitent l'analyse des flux de données pour prendre des décisions instantanées.
  - **Véracité.** Dans certains cas, les capteurs produisent données ambiguës et inexactes.
- Une plate-forme IoT est donc généralement livrée avec une solution de base de données basée sur le cloud.

Composants d'une plateforme IoT

Gestion des actions et traitement

- Les données capturées par le module connectivité et normalisation et stockées dans la base de données, prend vie dans cette partie de la plateforme IoT.
- Le déclencheur événnement-action, basé sur des règles, permet de actions «intelligentes» basées sur des données de capteur spécifiques.
- Dans une maison intelligente, par exemple, un événement déclencheur d'action peut être défini de sorte que toutes les lumières s'éteignent lorsqu'une personne quitte la maison.
- La réalisation technique souvent se présente sous la forme d'une règle If-this-then-that (IFTTT): **Si** le signal GPS indique que le **smartphone de *Jason* est plus à moins de 5 mètres de sa maison**, **alors éteignez tous les lumières dans sa maison**.

Composants d’une plateforme IoT

Analytique

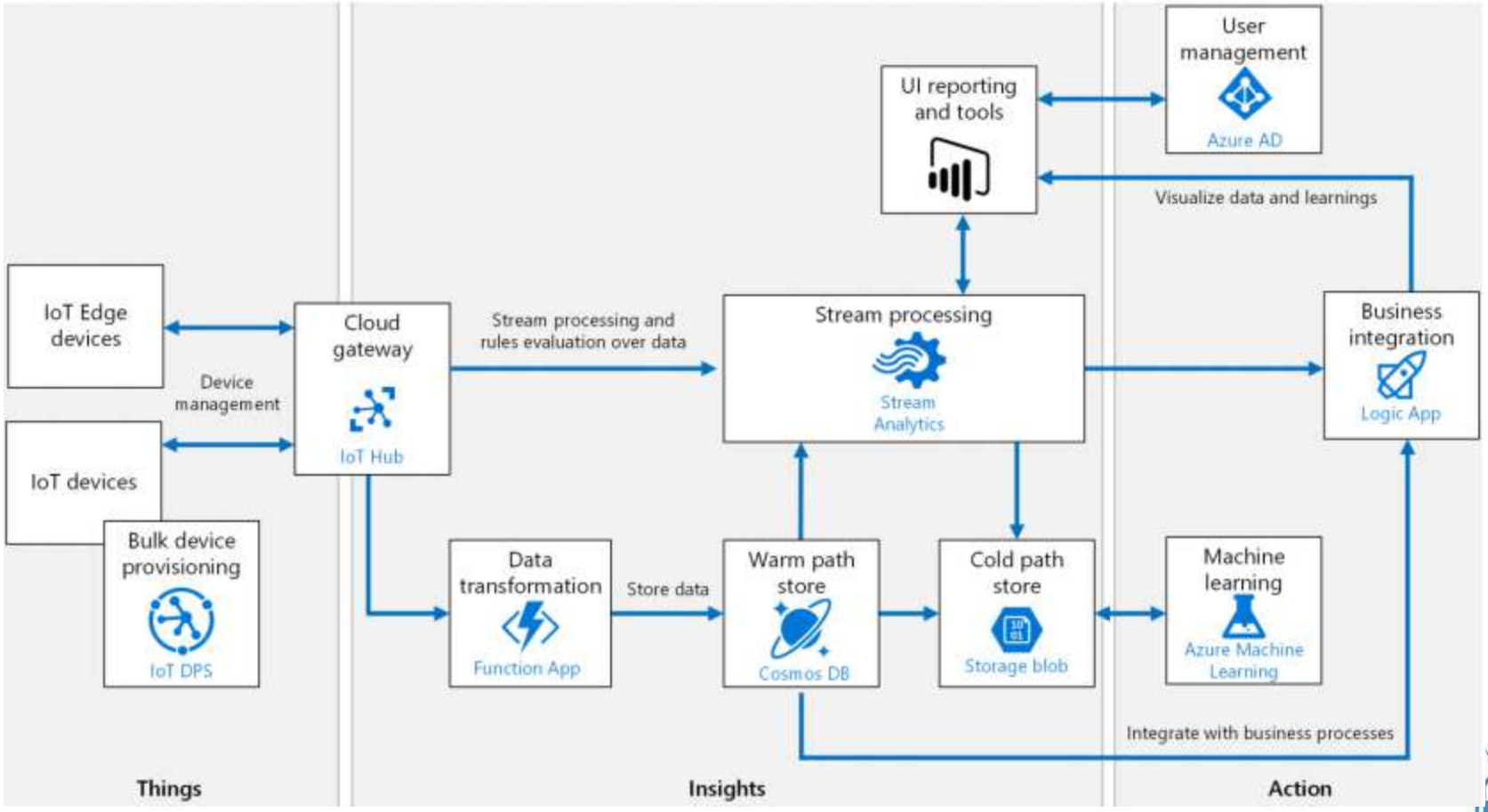
- De nombreux cas d'utilisation de l'IoT vont au-delà de la gestion des actions et nécessitent des analyses complexes pour tirer le meilleur profit des données IoT.
- Le moteur d'analyse prend en charge l’analyse des données des capteurs, à partir de la mise en cluster des données de base à l'apprentissage automatique en profondeur.
- Dans une maison intelligente, par exemple, le moteur d'analyse peut fournir les algorithmes qui permettent à la plateforme IoT de savoir quelle combinaison d'éclairage et de chauffage est préférée par l'utilisateur et à quelle heure de la journée en tenant compte des conditions météorologiques extérieures.

Composants d’une plateforme IoT

La visualisation

- La visualisation permet aux utilisateurs de voir les modèles et observer les tendances. Elle se présente sous la forme de lignes, empilées ou camemberts, modèles 2D ou même 3D.
- La visualisation des tableaux de bord mis à disposition du gestionnaire des plateformes IoT est souvent incluse dans les outils de prototypage qu'une plate-forme IoT avancée fournit.

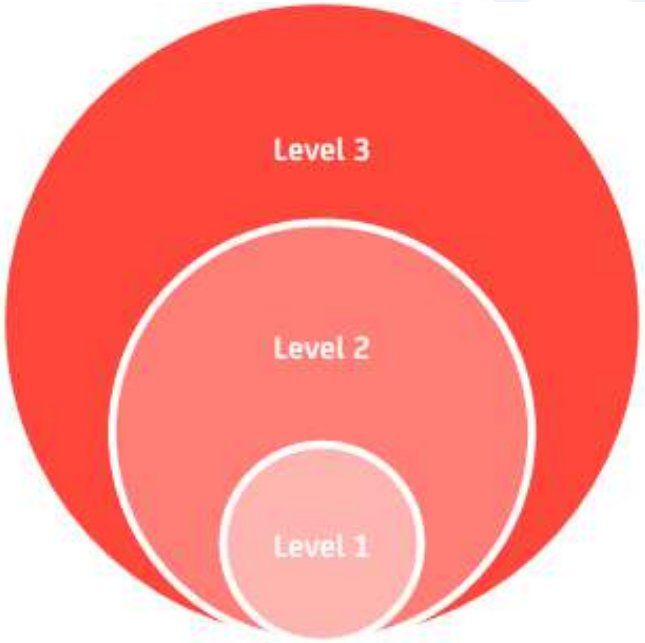
Microsoft Azure Cloud IoT



Types de plates-formes IoT

- Il existe deux types de plates-formes:
  - Plates-formes technologiques, et
  - Plates-formes focalisés sur le segment.

Plates-formes technologiques



- **Niveau 1: Plates-forme de connectivité (ou middleware)**
  - Collecte de données
  - Bus de messagerie
- **Niveau 2 : Plates-forme d'action**
  - Traitement des données
  - Gestion des événements-actions, par exemple basée sur des règles
- **Niveau 3 : Plates-forme de grande envergure**
  - Dispositif, protocole, normes indépendants
  - Back-end visuels multiformes
  - Interfaces externes sophistiquées (par exemple, API, SDK)
  - Solutions de base de données avancées, conçues pour le Big Data
  - Extensibilité de la plateforme: pour gérer un grand nombre d'appareils

Plates-formes avec un focus sur le segment du client final

- Les plates-formes B2C utilisent des mini-ordinateurs comme le Raspberry Pi ou l'Arduino. Ces plateformes sont souvent open-source et gratuits à utiliser dans leur version de base.
- Les plates-formes Smart Home prennent en charge les normes de connectivité domestique telles que WiFi, Zigbee, Z-wave et Bluetooth. Elles supportent souvent des applications visuelles prédéfinies qui permettent de surveiller et contrôler les appareils la maison.
- Les plates-formes de voiture connectées fonctionnent avec les normes automobiles et les protocole de communication de V2V. Elles donnent une attention particulière aux problèmes de sécurité car le piratage de cette plateforme peut causes des problèmes sérieux.
- Les plates-formes s'intègrent également aux services télématiques comme la gestion de flotte ou l'assurance basée sur l'utilisation.

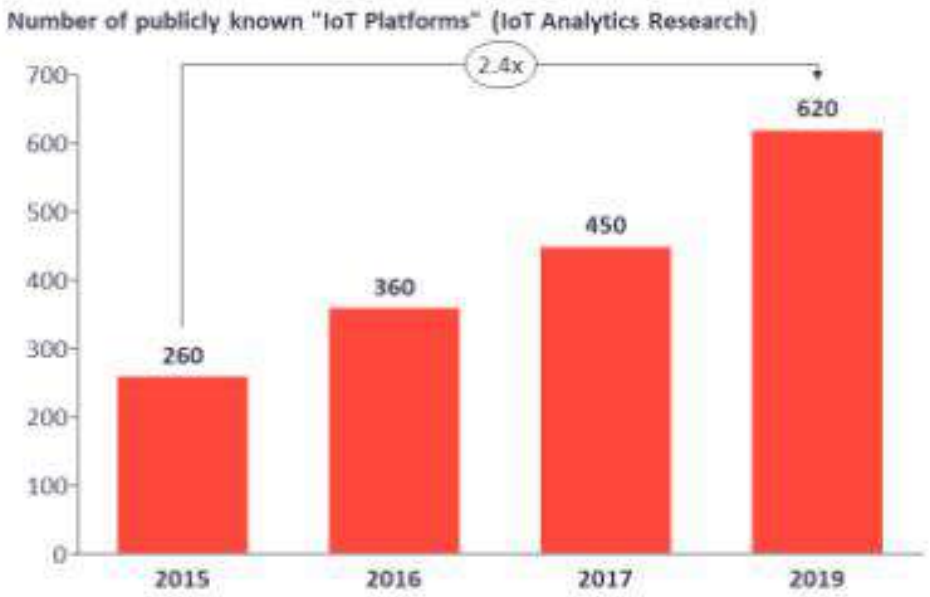
Plateformes avec un focus sur le segment du client final

- Les plateformes de ville intelligente. Les cas d'utilisation de la ville intelligente comme le stationnement intelligent ou la gestion des déchets connectés repose souvent sur des réseaux à faible puissance tel que réseaux étendus (LPWAN). Les plateformes sont également optimisée pour fonctionner avec les services de cartographie (par exemple, Google cartes) et des informations sur les rues locales.
- Les plates-formes IoT industrielles fournissent des passerelles spéciales à intégrer dans le SCADA et l'automatisation des systèmes existants. La sécurité renforcée constitue un souci majeur pour les entreprises qui craignent révéler des données sensibles aux clients ou concurrents involontairement.
- Autres plateformes spécialisées peuvent être trouvées dans des segments comme l'agriculture intelligente, la santé connectée ou la smart grid.

Principaux plateformes IoT

- Amazon Web Services IoT
- IBM Watson
- Microsoft Azure Cloud IoT
- Google Cloud IoT
- Oracle Integrated Cloud for IoT
- SAP Cloud Platform for the Internet of Things
- Cisco Jasper Control Center
- PTC ThingWorx Industrial
- GE Predix
- Cisco IoT Cloud

Marché des plateformes IoT (2015-2019)



Source: [IoT Platforms competitive Landscape & database 2020]

Marché des plateformes IoT (2015-2019)

- 620 fournisseurs de plateformes IoT, contre 450 en 2017.
- Le marché se concentre autour de quelques prestataires: les 10 premiers prestataires détenaient 58% de part de marché en 2019, contre 44% pour les 10 premiers en 2016.
- Les principaux fournisseurs continuent de croître à plus de 40%,
- L'industrie / la fabrication est la verticale n ° 1 - 50% des plates-formes s'y concentrent

Plateformes propriétaires vs plateformes open-source

- Deux types de plateformes sont à distinguer :
  - Les plateformes propriétaires permettent le partage des responsabilités, car le prestataire aura la charge du maintien opérationnel de tous les environnements.
  - Les plateformes open-source demandent plus de temps et de technique, vu qu'elles nécessitent le développement de l'ensemble des services, la maintenance des outils, de l'infrastructure et des applications.

Comparaison des plateformes IoT

	General Electric (GE)	Microsoft	Amazon	IBM
Platform Name	Predix	IoT Hub	AWS IoT	IBM Watson IoT
Deployment Models	Public, Private, On-Premise	Public	Public	Public
Pricing Models	Subscription, Pay-as-you-go (tiers) # of Services + usage	Subscription – different tiers based on total messages exchanged	Usage-based – messages published and delivered. (messages delivered to other AWS services are free)	Usage-based – Data exchange and analyzed
PaaS Platform	Cloud Foundry	Azure	AWS	IBM Bluemix, Cloud Foundry
Market Place	Extensive	Extensive	Extensive	Extensive
SDK / Languages	Yes	.NET, and UWP, Java, C, NodeJS	C, NodeJS	C#, C, Python, Java, NodeJS
API / API Libraries / Management	Yes	Yes (Extensive, Open)	Yes (Extensive, Open)	Yes
Ingestion Layer	Yes	Yes	Yes	Yes
Identity and Access Management	Yes	Yes	Yes	Yes
Workflow	Yes	Yes	Yes	Yes
Events Processing	Yes	Yes	Yes	Yes
Rules Engine	Yes	Yes	Yes	Yes
Audit	Yes	Yes	Yes	Yes

Comparaison des plateformes IoT

	General Electric (GE)	Microsoft	Amazon	IBM
Platform Name	Predix	IoT Hub	AWS IoT	IBM Watson IoT
CRM / ERP Integration	Manual	Manual	Manual	Manual
Field Service Integrations	ServiceMax	Manual/Partners	Manual/Partners	Manual/Partners
Visualization	Yes	Yes	Yes	Yes
Analytics - Hot Path	Yes	Yes	Yes	Yes
Analytics - Cold Path	Yes	Yes	Yes	Yes
Machine Learning	Yes	Yes/API(managed Service)	Yes	
BigData - Hadoop	Yes	Yes with HDInsight	Yes with Amazon EMR	
Notification and Alerts	Yes	Yes	Yes	
Device Lifecycle Mgmt	Yes	Yes	Yes	Yes
Device Security	Yes	X.509, TLS	X.509	TLS
Device – Device SDK	Yes	Open source SDK	Open SDK	Yes (limits - TBD?)
Device - Protocols	Yes	AMQP, MQTT, HTTP, WebSockets	MQTT, HTTP, Websockets	MQTT, HTTP
Device - Gateways	Yes	Yes	Yes	Yes
Object Storage	Yes	Yes	Yes	Yes

Quelle plateforme choisir?

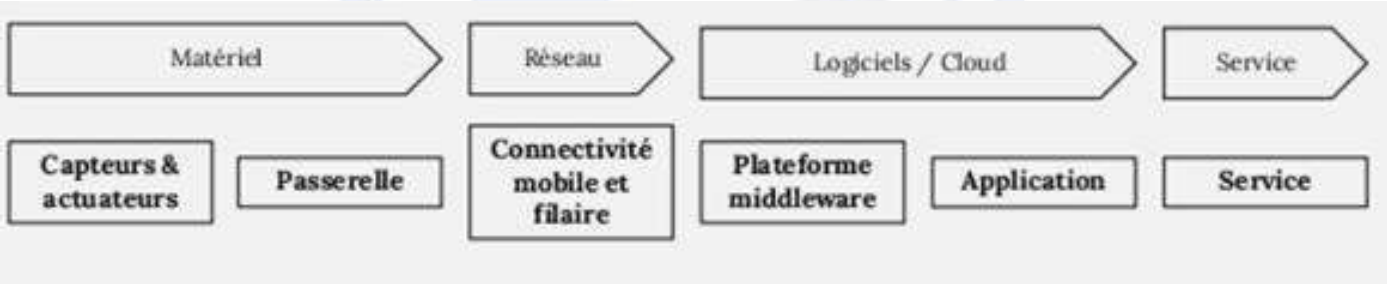
Ce qu'il faut retenir:

- Construire votre propre plateforme IoT prolonge la durée du projet de manière significative
- L'expertise interne est rare et coûteuse.
- Les projets IoT sont complexes - même avec une plateforme externalisée.

Quels sont les type de plateformes IoT et le quel domine le marché?

Partie 4:
Chaine de valeur IoT, connectivité et modèles économiques

Chaine de valeur de l'IoT



Fournisseurs de plateformes

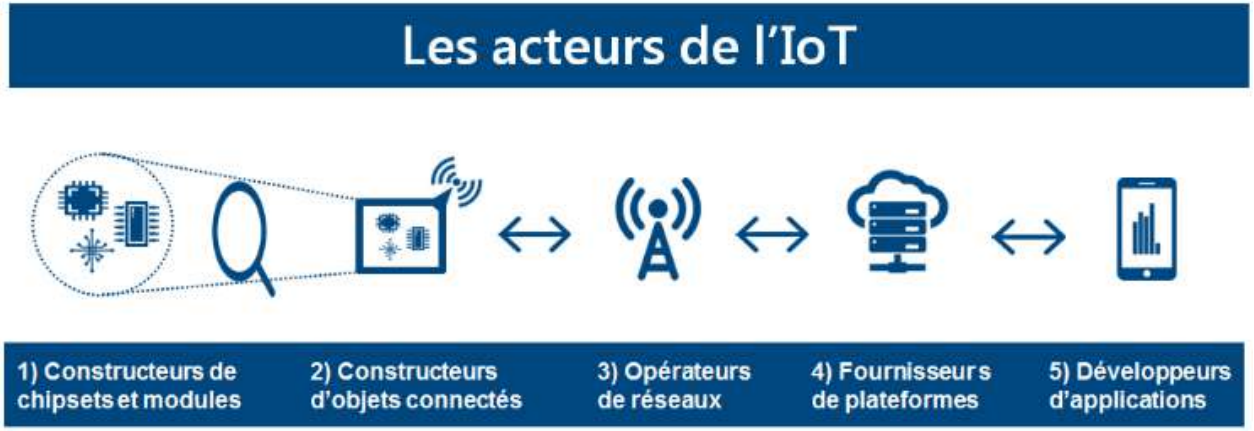
Constructeurs de matériel

- Microcontrôleurs et modules
- Constructeurs d'objets
- Constructeurs de passerelles

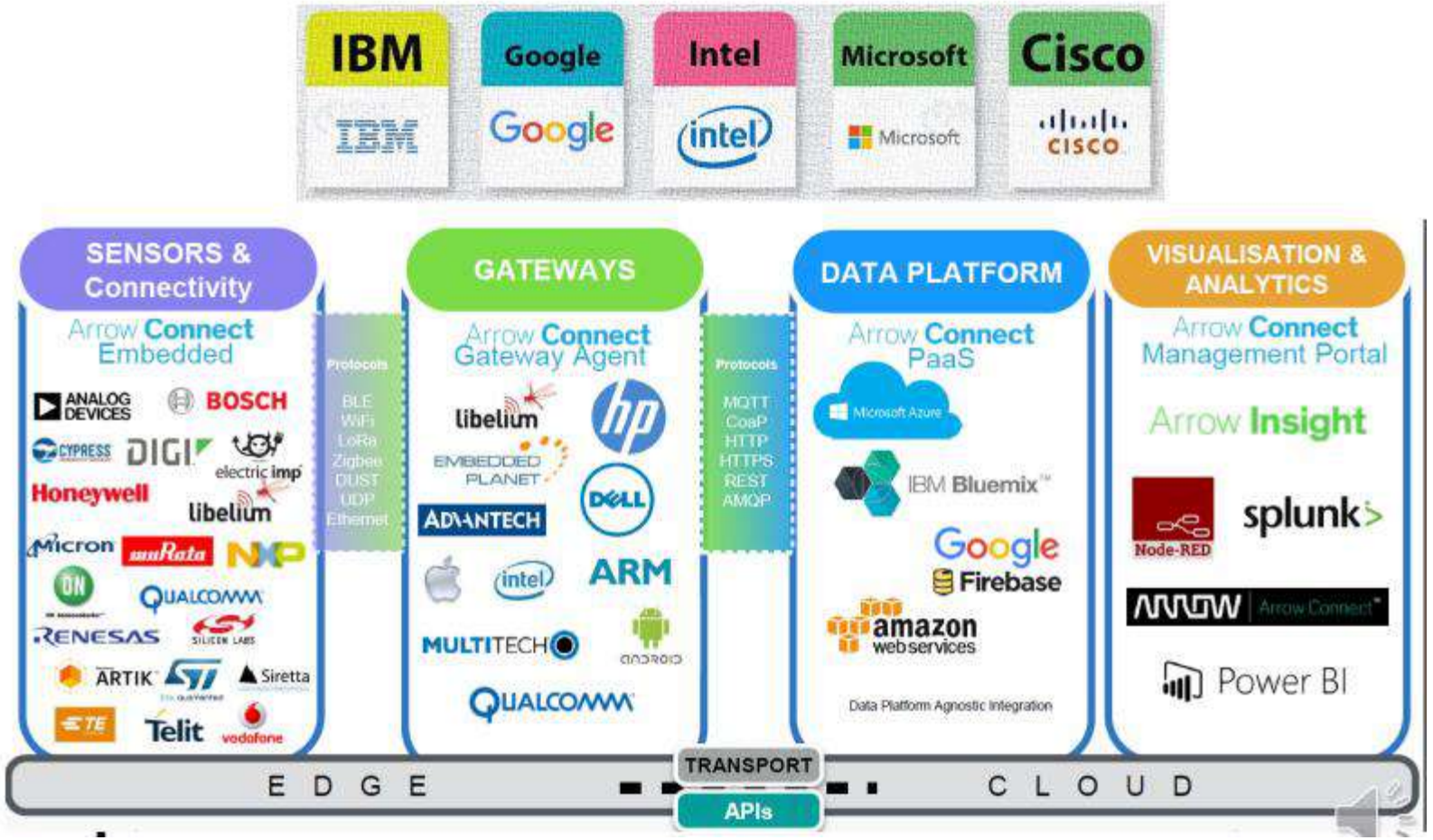
Opérateurs de réseaux

Développeurs d'applications

Décomposition des acteurs de l'écosystème IoT



Décomposition des acteurs de l'écosystème IoT



Constructeurs de chipsets et modules

- Les constructeurs de chipsets et modules produisent les capteurs et les transmetteurs électroniques qui, assemblés, composeront les objets connectés.
- Exemples de fabricants de puces et de modules électroniques : Texas Instrument, Semtech ou Sequans Communications.

Fabricants d'objets connectés

- Le fabricant d'objets connectés fait référence au constructeur du produit. Sa mission est d'assembler l'ensemble de composants issus du premier maillon, capteurs, puces, modules, antennes… afin de répondre aux mieux aux besoins.
- La stratégie des fabricants d'objets repose sur :
  - Un accroissement de chiffre d'affaires à court terme, et
  - Une amélioration de leur marge dans un second temps notamment autour de la vente de service, généralement plus rentable que la vente de produits.

Fabricants d'objets connectés

- La stratégie de « *servicisation* » des objets offre aux fabricants une opportunité pour:
  - La génération des revenus additionnels provenant de services ou encore de consommables liés à ces objets.
  - Une meilleure connaissance de leurs clients, en particulier autour des usages du produit. L'objet connecté devrait donc être considéré comme un bon outil de gestion de la relation client et de fidélisation de clientèle suivant les secteurs.

Fabricants d'objets connectés

- Les objets connectés sont fréquemment fabriqués par des start-ups, mais aussi par des filiales de grands groupes.
- Le positionnement des nouveaux entrants varie fortement selon le secteur :
  - ils optent pour des marchés où l'adoption est généralement la plus forte, comme la sécurité et la gestion de l'énergie ou de la domotique dans la maison ;
  - Ils évitent des marchés qui nécessitent une expertise métier très spécifique (et donc une image de marque installée).
  - Ils choisissent enfin des marchés peu concurrentiels comme la traçabilité d'animaux de compagnie.

Fabricants d’objets connectés

- Les fabricants historiques se focalisent essentiellement sur la vente d’objets et avancent très prudemment sur les services.
- Les nouveaux entrants orientent leur stratégie essentiellement sur la vente d’objets, mobilisant leurs équipes commerciales sur la distribution B2B2C pour vendre de plus gros volumes.
- Dans cette même optique, ils ouvrent le plus souvent un accès gratuit à leurs API afin de permettre à des tiers de proposer des services autour de leurs objets, pour en favoriser l’adoption et par suite accroître les nouveaux revenus qui en découlent.

Fournisseurs de connectivité

- Les fournisseurs de connectivité font référence en général aux opérateurs de télécommunications. Ils interviennent dans le marché IoT pour offrir des solutions de connectivité aux objets.
- Certains de ces acteurs se positionnent sur différents segments :
  - Fournisseurs de solutions (parfois de bout en bout incluant l'objet). Ils jouent un rôle plus actif dans la maison connectée puisqu'ils proposent des offres de bout en bout autour de leur « box », avec pour objectif de faire croître la facture mensuelle de leurs abonnés tout en maintenant un taux de désabonnement (*churn*) le plus faible possible.
  - Fournisseurs de connectivité. Leur rôle demeure principalement indirect, puisqu'une grande part des objets sont connectés en *Wifi/Bluetooth*.
  - Distributeurs. Ils sont également présents sur la distribution de ces objets (sport et bien-être notamment), en particulier s'agissant de la montre, considérée comme le deuxième écran du smartphone.

Fournisseurs de plateformes IoT

- Le fournisseur de plateforme fournit les outils techniques permettant de recueillir les données émises par les objets pour développer des applications métier et des services.
- Les fournisseurs de plateformes restent peu nombreux. Par définition, il leur est difficile de se positionner dans des secteurs où les fabricants d'objets ont une approche de bout en bout (ou verticale), quand eux ont une approche horizontale (indépendante du fabricant d'objets).
- La plupart des fournisseurs de plateforme font des offres en mode service (PaaS) mais chez certains fournisseurs comme Thingworx il est possible d'acheter uniquement la plateforme et de l'installer dans votre SI ou même chez un hébergeur Cloud si vous le souhaiter.

La dominance des GAFA

- Les GAFAs apparaissent très légitimes à se positionner sur ce segment puisqu'ils bénéficient de la maturité de leurs solutions technologiques.
- Certains d'entre eux ont verrouillé le marché de la domotique, l'e-santé et la voiture connectée:
  - Domotique : Google, Microsoft
  - L'e-santé : Apple, Google
  - la voiture autonome : Google, Apple

La dominance des GAFA

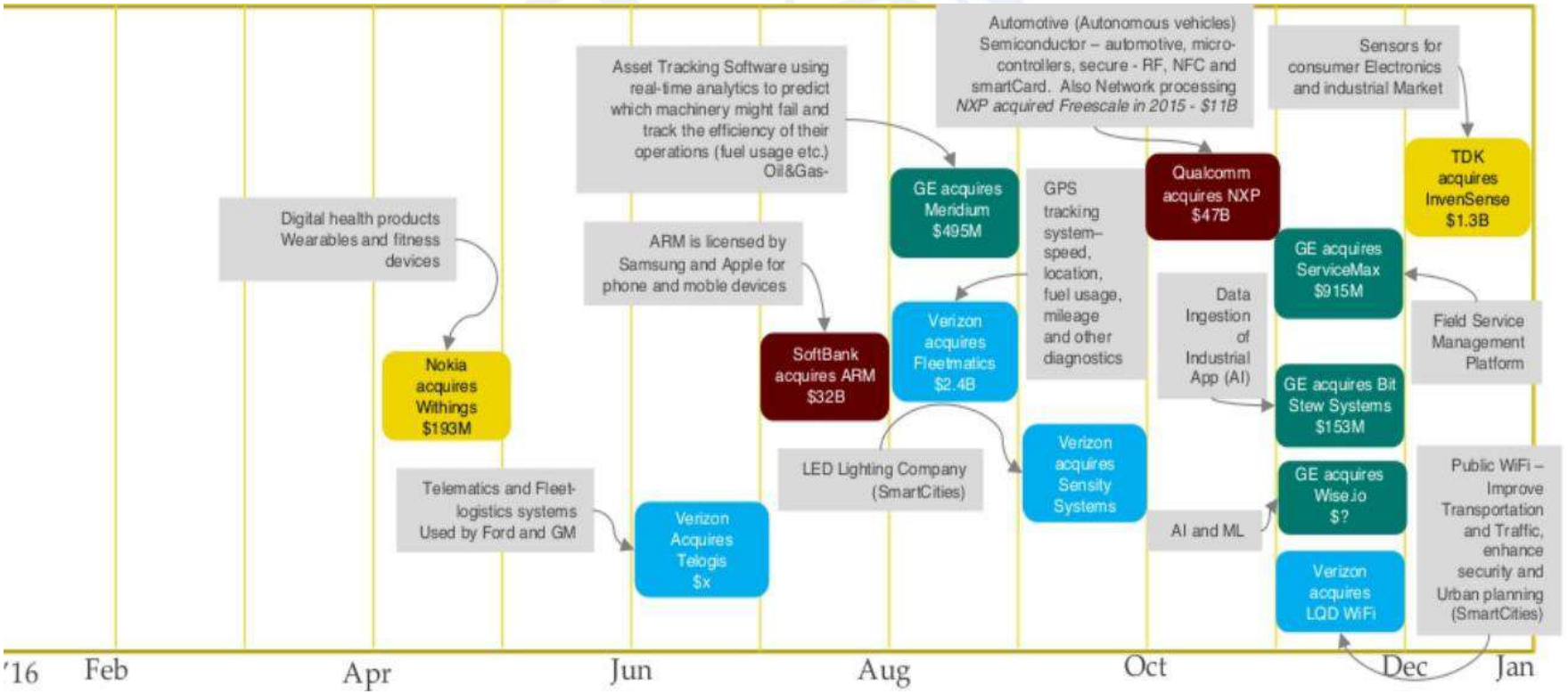
- Le foisonnement des start-ups, parfois rachetées par les grands du domaine, à l'image du récent rachat de Withings par Nokia en avril 2016, pour 170 millions de dollars US, est une constante de l'IoT.

Entreprise	Achetée par	Produit	Sous-secteur
Beats electronic	Apple	Audio grand public	Divertissement
LinX	Apple	Caméra	Tous
Coherent Navigation	Apple	Cartographie	Transports
AuthenTec	Apple	Biométrie	Sécurité
Didi Chuxing	Apple	VTC*	Transports
Revolv	Google	Domotique	Domotique
Lift Labs	Google	Suivi de santé	Santé
Drop Cam	Google	Caméra	Domotique
Sybox Imaging	Google	Cartographie	Transports
Nest Labs	Google	Domotique	Domotique
Oculus VR	Facebook	Réalité virtuelle	Tous
Face.com	Facebook	Reconnaissance faciale	Sécurité
Mobile Data Labs	Microsoft	Cartographie	Transports
N-Trig	Microsoft	Stylo connecté	Tous
Nokia	Microsoft	Terminaux	Tous
Id8 Groups	Microsoft	Domotique	Domotique
Perceptive Pixels	Microsoft	Capteurs	Tous

*Véhicules de transport avec chauffeur. Réalisation : Nicolas Mazzucchi.

Source : https://www.futuribles.com/fr/groupes/iot-2025/document/vers-une-industrie-integralement-40-2/

Principaux rachats en 2016



Fournisseurs d'applications métiers ou services

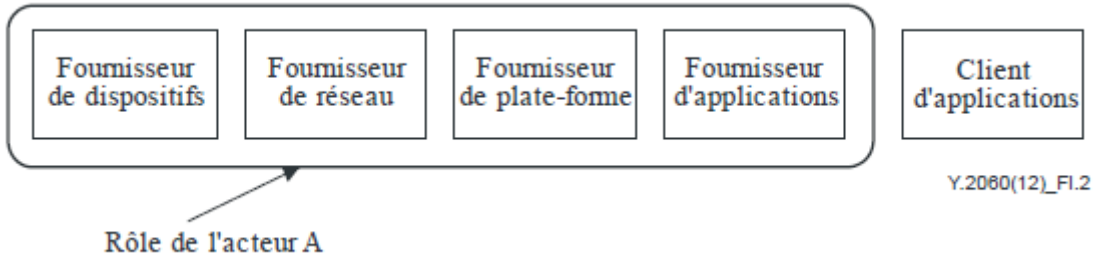
- Le fournisseur de services délivre les services à valeur ajoutée tirant parti des données générées par les objets.
  - Exemples : Services d'entraînement sportif ou minceur ou encore des services de sécurité.
- Les fournisseurs de services sont majoritairement les fabricants eux-mêmes compte tenu de leur approche de bout en bout.
- De nombreuses jeunes start-ups exploitent également les données à des fins spécifiques.

Modèles d’activités

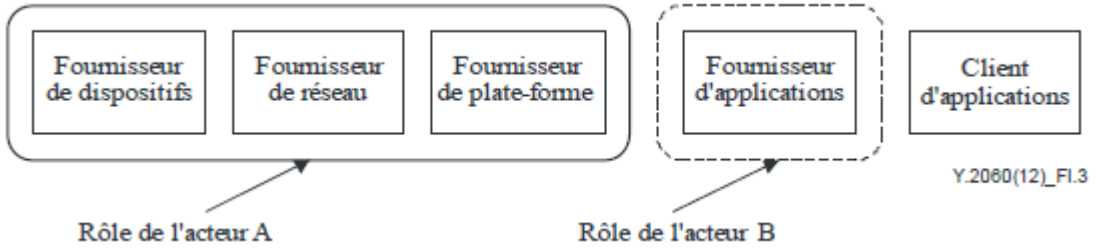
- Les acteurs de l'écosystème de l'IoT peuvent entretenir diverses relations dans le cadre de déploiements réels. La diversité de ces relations est présentée par des modèles d'activité.

UIT Recommandation 2060

Modèle 1

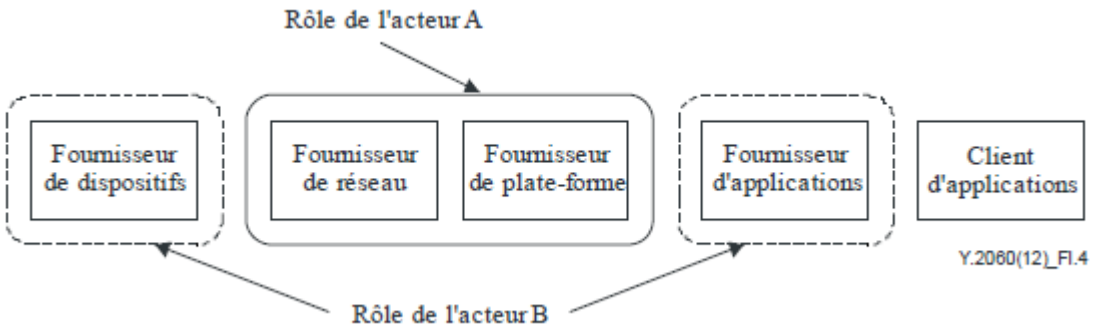


Modèle 2

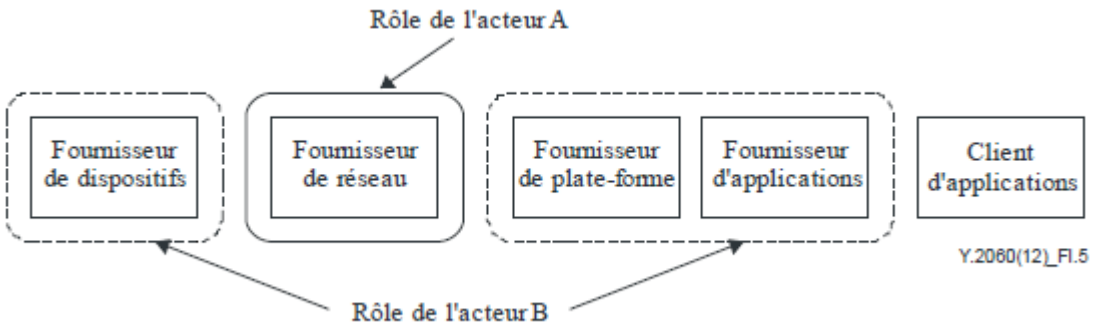


Modèles d'activités

Modèle 3

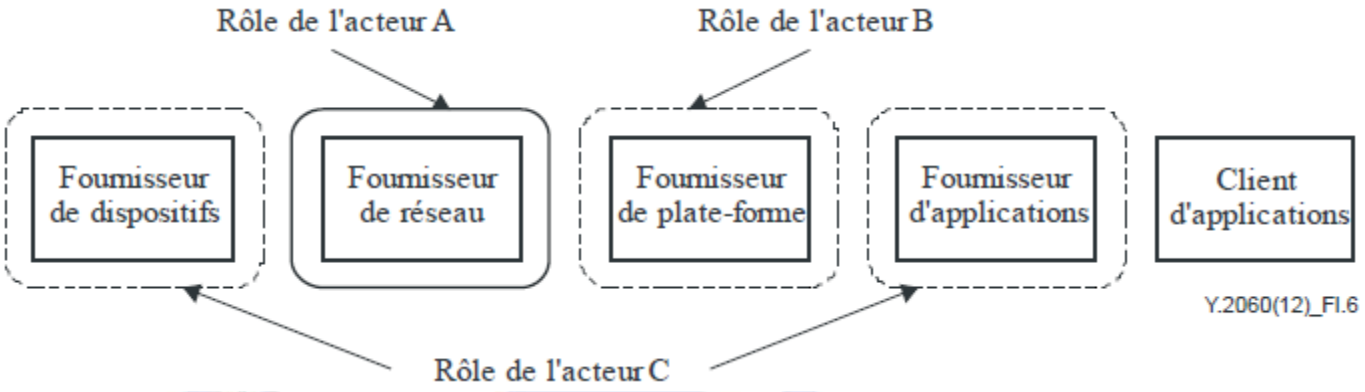


Modèle 4



Modèles d'activités

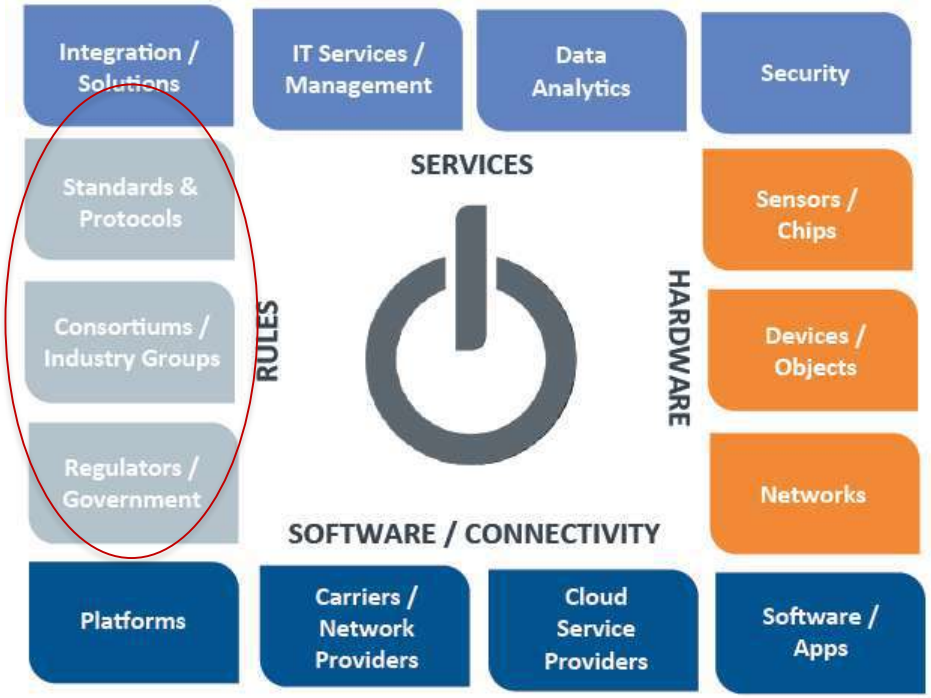
Modèle 5



Quizz N°3

Quel est le modèle d'activités le plus utilisé aujourd'hui par les startups?

Autres acteurs de l'écosystème de l'IdO



Partie 5:
Activités de normalisation

Thank you!

Structure et standards

Working Group	Reference and title	Scope	Status
WG 3 - IoT Architecture: standardization in the area of IoT vocabulary, architecture, and frameworks	ISO/IEC 20924, Definitions and vocabulary	This draft provides a definition of IoT along with a set of terms and definitions. It represents a terminology foundation for the IoT.	Under development
	ISO/IEC 30141, Internet of Things Reference Architecture (IoT-RA)	This draft specifies general IoT reference architecture defining system characteristics, a conceptual model, a reference model and architecture views of IoT.	Under development
	Technical Report (TR) on IoT Edge Computing	This draft provides basic concepts of IoT edge computing architecture, terminologies, values, characteristics, challenges, use cases and main technologies (including data management, coordination, processing, network functionality, heterogeneous computing, security, hardware / software optimization) of edge computing for IoT systems applications. It is also considered to assist in the identification of potential areas for standardization in edge computing for IoT.	Under development
	ISO/IEC 30147, Methodology for trustworthiness of IoT system / service	This draft provides a methodology to implement and maintain trustworthiness in IoT system/service. The methodology is not targeted to a certain application area of the IoT system/service but for a generic IoT system/ service common to various application areas.	Under development

Structure et standards

WG 4 - IoT Interoperability: standardization in the area of IoT interoperability, connectivity, conformance and testing.	ISO/IEC 21823-1, Interoperability for Internet of Things Systems - Part 1: Framework	This draft provides an overview of interoperability requirements and a framework for interoperability for IoT systems. It aims to enable IoT systems to be built in such a way that all the entities of the IoT ecosystem are able to exchange information and mutually use the information in an efficient way. The goal of this draft is to ensure that all parties involved in developing and using IoT systems have a common understanding of interoperability as it applies within and out of the various entities.	Under development
	ISO/IEC 21823-2, Interoperability for Internet of Things Systems - Part 2: Transport interoperability	This draft presents a conceptual model for network connection interoperability and requirements for interoperable IoT systems to enable information exchange, peer-to-peer connectivity and seamless communication within and out of the IoT systems.	Under development
	ISO/IEC 21823-3, Interoperability for Internet of Things Systems - Part 3: Semantic interoperability	This draft provides a basic concept of semantic interoperability for IoT systems, as described in the facet model of ISO 21823 Part 1. It also describes technologies supporting for semantic interoperability of IoT systems.	Under development

Structure et standards

WG 5 - IoT applications: standardization in the area of IoT applications, platforms, use cases, middleware, tools and implementation guidance.	ISO/IEC TR 22417:2017, IoT use cases	This TR is dedicated to identify IoT scenarios and use cases based on real-world applications and requirements as well as identification of potential areas of standardization to ensure easy operation and interoperability within and out of the IoT ecosystem. It comprises 25 use cases of the IoT applications.	Published

Commissions d'études et objectifs

Study Group	Objective
SG 7 - Wearables	This SG is to study market requirements of smart wearable devices, analyze the current standardization and research activities in this field, and identify standardization gaps.
SG 8 - Trustworthiness	This SG is responsible to propose a definition of trustworthiness. In addition, it is also responsible for investigating related standards and guidelines as well as to identify standardization gaps in the areas of security, privacy, safety, resilience and reliability.
SG 9 - Industrial IoT	This SG is responsible for analyzing market requirements and current standardization activities in the area of IIoT. One of the mission among other of this SG is to perform a comparison of reference architectures and models in the context of IIoT in order to avoid double works in future standardization developments.
SG 11 - Real-Time IoT	This SG is to provide an analysis of market requirements and a status of current standardization activities on real-time IoT. It will identify possible new projects within the area of SC 41.
SG 12 - Aspects of IoT Use Cases including Classification and Verification	The objective of this SG is to build a classification of use cases based on IoT scenarios identified in ISO/IEC TR 22417:2017 - IoT use cases. One of the objective among other of this SG is to propose an improved template for use case presentation as a part of the ISO/IEC 30141 - Reference Architecture.
SG 13 - Reference Architecture and Vocabulary	This SG is responsible for reviewing and analyzing a catalogue of reference architectures and assorted vocabulary, created by JTC 1/SC 41.

Caractéristiques d'un objet

- Identité unique : chaque objet connecté possède une identité unique.
- Dynamique & Auto-adaptatif : les objets connectés peuvent avoir la capacité de s'adapter aux changements de contexte et prendre des décisions basées sur les conditions de fonctionnement.
  - Exemple : changement automatique de résolution de caméra de surveillance lors de détection de mouvement.
- Auto-configuration : les objets connectés peuvent avoir des capacités d'auto-configuration pour permettre à un nombre large d'objets de fonctionner ensemble afin de fournir un service. Ces objets ont la capacité d'établissement de réseau, de mise à jour software, etc.
- Interopérabilité : les objets connectés sont des objets hétérogènes basés sur des plateformes matérielles différentes et peuvent supporter un nombre de protocoles de communication et communiquer ensemble et avec l'infrastructure.

Alliances IoT

- AIOTI
- OneM2M
- AllSeen
- Fondation Eclipse
- Consortium Internet industriel (IIC)
- Protocole Internet des objets intelligents (alliance IPSO)
- IoT alliance
- Oasis
- Open Interconnect Consortium (OIC)
- Thread Group
- Alliance ZigBee

Organisations internationales de standardisation

- L'Union Internationale des Télécommunications (UIT) élabore des lignes directrices qui serviraient de référence commune aux autres organisations de standardisation.
- L'Institut des Ingénieurs Electriciens et Electroniciens (IEEE) travaille sur la standardisation des réseaux de communication, des applications sectorielles (smart grid, industrie, agriculture et secteur minier).
- L'Internet Engineering Task Force (IETF) élabore des standards pour les systèmes de communication, notamment pour l'IPv6.

Organisations internationales de standardisations

- OASIS (*Organization for the Advancement of Structured Information Standards*) est un consortium sans but lucratif qui oriente les développements et l'adoption de standards ouverts pour la société de l'information. Les travaux de ce consortium sur l'internet des objets portent sur les technologies de réseau et de messagerie normalisées.
- 3GPP regroupe des organisations de normalisations télécoms produisant des spécifications pour la communication cellulaire par le biais de NarrowBand IoT (NBIoT)

Caractéristiques du support de service IoT

- Certains services IoT avancés devront collecter, analyser et traiter des segments de données brutes issus de capteurs et les transformer en information de contrôle opérationnel.
- Certains types de données issus de capteur peuvent avoir des tailles énormes (en raison du grand nombre de périphériques IoT).
- Des bases de données IoT seront nécessaires, qui seront prises en charge par le cloud.
- Un support Big Data sera nécessaire pour l'analyse des données IoT.
- Les Réseaux sociaux et la gestion des appareils mobiles joueront également un rôle dans la prise en charge de l'IoT.

Support : Hardware + Software + Protocoles de communications + Technologies (Big Data, data analytics, Cloud /Edge /Fog computing)

PRIDA Track 2 (T2)

Réglementation de l'IoT

25/08/2020

Agenda

- Partie 1: Sécurité de l'IoT
- Partie 2: Vie privée et responsabilité
- Partie 3: Normes et directives de sécurité, certification, et réglementation
- Partie 4: Identification et gestion des données
- Partie 5: Roaming et expériences régionales

Introduction

- L'Internet des objets (IoT) représente une révolution de l'Internet qui peut connecter presque tous les périphériques d'environnement sur Internet et partager leurs données pour créer de nouveaux services et applications et améliorer la qualité de vie.
- L'IoT apporte des avantages infinis; cependant, il crée plusieurs défis, notamment en matière de sécurité et de confidentialité.
- La sécurité et la confidentialité des produits et services IoT est une préoccupation de taille

Introduction

- Les utilisateurs doivent avoir confiance que les appareils IoT et les services associés sont sécurisés.
- La **sécurité** et la **vie privée** sont les enjeux majeurs liés au déploiement des objets connectés
- Les législateurs prévoient des textes juridiques pour réglementer l'IoT et protéger les individus contre les infractions.
- Cependant, les législateurs ont encore un long chemin à faire en ce qui concerne la **responsabilité** des objets connectés ou de leurs utilisateurs.

Partie 1: Sécurité de l'IoT

Pourquoi se préoccuper de la sécurité de l'IoT?

- IoT peut servir de base pour des attaques de grande envergure sur d'infrastructures qui sont critiques
- Quelques cibles:
  - Réseaux nationaux ou régionaux d'alimentation électrique
  - Système financier et de commerce
  - Automobile
  - Système industriel
  - Système d'alarme
  - Equipement médical
  - Surveillance audio et vidéo

Les récentes attaques IoT

Botnet Mirai (2016)

- Ce réseau de robots a infecté par de nombreux appareils IoT (anciens routeurs et caméras IP), puis s'en est servi pour saturer le serveur DNS de la société Américaine DYN par un flux gigantesque de requêtes (attaque de déni de service distribué).
- Le botnet Mirai a rendu a rendu une partie d'Internet inaccessible, dont certains sites très populaires: Twitter, Reddit, Netflix, Spotify, le *New York Times*, CNN, etc.
- Ce code malveillant a tiré profit d'appareils exécutant des versions obsolètes du noyau Linux et s'est appuyé sur le fait que la plupart des utilisateurs ne changent pas le nom d'utilisateur et le mot de passe par défaut sur leurs appareils.

Les récents attaques IdO

Vague de froid en Finlande (2016)

- Des cybercriminels ont coupé le système de chauffage de deux bâtiments dans la ville finlandaise de Lappeenranta.
- Il s'agit d'une autre attaque DDNS. Cette attaque a fait en sorte que les contrôleurs de chauffage redémarrent sans arrêt du système, empêchant le chauffage de se mettre en route.
- Comme les températures en Finlande descendent bien en dessous de zéro à cette période de l'année, l'attaque était loin d'être anodine.

→ Leçon à tirer : Le réseau IoT doit être régulièrement surveillé pour détecter les attaques par refus de service distribué.

Les récentes attaques IoT

Brickerbot

- Cette attaque fonctionne de façon similaire au botnet Mirai, elle s'appuie sur une attaque de déni de service distribué et sur le fait que les utilisateurs ne changent pas le nom d'utilisateur et le mot de passe par défaut de leurs appareils.
- La principale différence entre Brickerbot et le botnet Mirai est que Brickerbot détruit simplement l'appareil.

→ La leçon à tirer : Eviter l'utilisation des mots de passe par défaut.

Les récentes attaques IoT

Le barrage de botnets

- Verizon Wireless a publié un rapport évoquant une université dont le nom n'a pas été dévoilé où plus de 5 000 appareils IoT ont été attaqués.
- Lorsque des membres du personnel informatique du campus ont commencé à recevoir de nombreuses plaintes sur la connectivité réseau lente ou inaccessible, ils ont découvert que leurs serveurs de noms produisaient un volume élevé d'alertes et montraient un nombre anormal de sous-domaines liés aux fruits de mer.
- Il s'est avéré que plus de 5 000 systèmes distincts effectuaient des centaines de recherches DNS toutes les 15 minutes.
- Le botnet s'est propagé via une attaque en force brute pour casser les mots de passe vulnérables sur les appareils de l'‘l’IoT.

Source : https://www.zdnet.fr/actualites/5-attaques-cauchemardesques-qui-montrent-les-risques-lies-a-lasecurite-de-l-iot-39858896.htm

Quels sont les défis de la sécurité de l'IoT?

1. L'économie favorise la sécurité faible;
2. La sécurité est difficile; en particulier pour les nouvelles entreprises;
3. Les systèmes IoT sont complexes et chaque partie doit être sécurisée;
4. Le support de sécurité n'est pas toujours maintenu;
5. La connaissance du consommateur de la sécurité IoT faible;
6. Les incidents de sécurité peuvent être difficiles à détecter ou à résoudre pour les utilisateurs;
7. Les mécanismes de responsabilité légale existants peuvent ne pas être clairs.

Quels sont les défis?

1. L'économie favorise la sécurité faible

- Les pressions concurrentielles pour des délais de commercialisation plus courts et des produits moins chers incitent de nombreux concepteurs et fabricants de systèmes IoT à consacrer moins de temps et de ressources à la sécurité.
- Une sécurité forte est coûteuse et elle allonge le temps nécessaire à la mise sur le marché d'un produit,

Quels sont les défis?

1. L'économie favorise la sécurité faible

- Il n' y a pas de moyens crédibles permettant aux fournisseurs de signaler leur niveau de sécurité aux consommateur, par exemple les labels de confiance, certifications, …
  - Difficile pour les consommateurs de comprendre facilement la sécurité de différents systèmes IoT;
  - Réduction des pressions exercés par les consommateurs sur les fournisseurs
- La sécurité ne peut pas être un facteur de différenciation concurrentielle.

Quels sont les défis?

2. La sécurité est difficile, en particulier pour les nouvelles entreprises

- La mise en œuvre d'une sécurité renforcée dans les systèmes IoT nécessite une expertise;
- Les nouveaux acteurs de l'écosystème IoT peuvent avoir peu à as d'expérience en matière de sécurité,
  - Exemple : un fabricant peut savoir comment rendre un réfrigérateur sûr pour son usage initial (câblage électrique, produits chimiques), mais peut ne pas comprendre la sécurité informatique,

Quels sont les défis?

4. Les systèmes IoT sont complexes et chaque partie doit être sécurisée

- Les périphériques, applications et services IoT nécessitent des correctifs de sécurité et des mises à jour pour se protéger contre les vulnérabilités connues;
- La prise en charge des systèmes IoT est une tâche coûteus pour les fournisseurs de services IoT.

Quels sont les défis?

4. Les systèmes IoT sont complexes et chaque partie doit être sécurisée

- Les périphériques, applications et services IoT nécessitent des correctifs de sécurité et des mises à jour pour se protéger contre les vulnérabilités connues;
- La prise en charge des systèmes IoT est une tâche coûteus pour les fournisseurs de services IoT.

Quels sont les défis?

5. La connaissance du consommateur de la sécurité IoT faible

- Généralement, les consommateurs ont une connaissance limitée de la sécurité IoT, ce qui a un impact sur leur capacité à intégrer à intégrer dans leurs habitudes d'achats ou à configurer et maintenir la sécurité de leurs systèmes IoT.

Quels sont les défis?

6. Les incidents de sécurité peuvent être difficiles à détecter ou à résoudre pour les utilisateurs;

- Dans de nombreux cas, les effets d'un produit ou d'un service mal sécurisé ne seront pas évidents pour l'utilisateur.
  - Exemple, un réfréigrateur peut continuer à faire du bon boulot même s'il a été compromis et fait partie d'un botnet effectuant des attaques DDoS
- Les consommateurs n'ont également pas la capacité technique ou les interfaces utilisateur, d'implémenter les correctifs.
- Les utilisateurs peuvent ne pas savoir comment patcher leurs appareils.
- Les utilisateurs sont empêchés contractuellement de mettre à jour ou réparer les systèmes eux-mêmes ou les faire réparer par des spécialistes indépendants.

Hackers

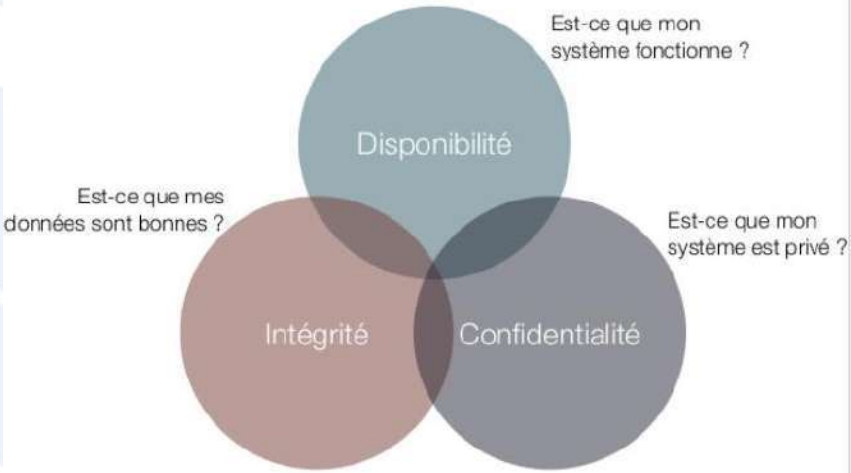
- L'essor de l'IoT a fait des heureux : les cybercriminels.
- De plus en plus de hackers s'appuient sur les failles de sécurité des objets connectés pour créer un botnet et mener une attaque à grande échelle.
- Ne pas transformer votre système IOT en passoir

Sécurité de l'information

- La sécurité de l'information regroupe l'ensemble des moyens organisationnels, technologiques, humains et juridiques permettant de gérer les risques et leurs impacts à l'égard de la disponibilité de l'information, de sa disponibilité et de son intégrité.
- De nombreux défis de l'IoT pourrait s'inscrire dans le cadre de la triade originale de la sécurité de l'information

Triade de la sécurité informatique

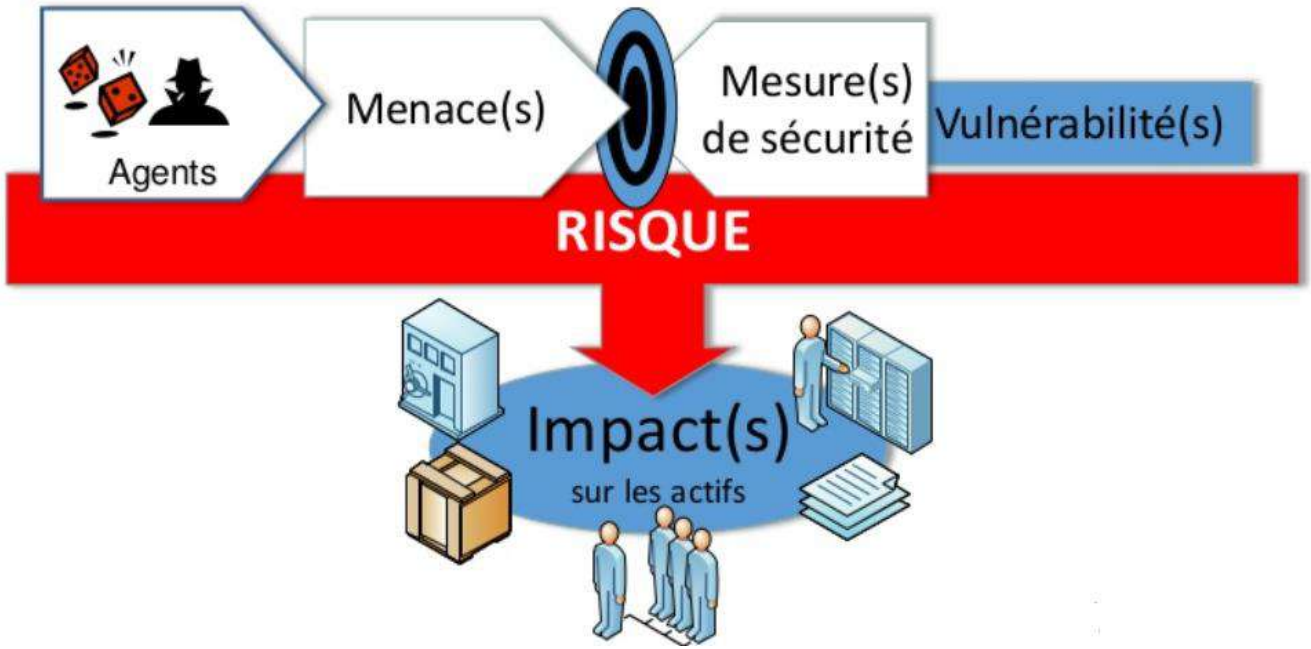
- La confidentialité : Seules les personnes autorisées avec les habilitations requises ont accès aux informations.
- L'intégrité : les données doivent être intactes, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante.
- La disponibilité : un système doit fonctionner sans faille durant les plages d'utilisation prévues et garantir l'accès aux services et ressources installées avec le temps de réponse attendu.



Sécurité des systèmes d'information

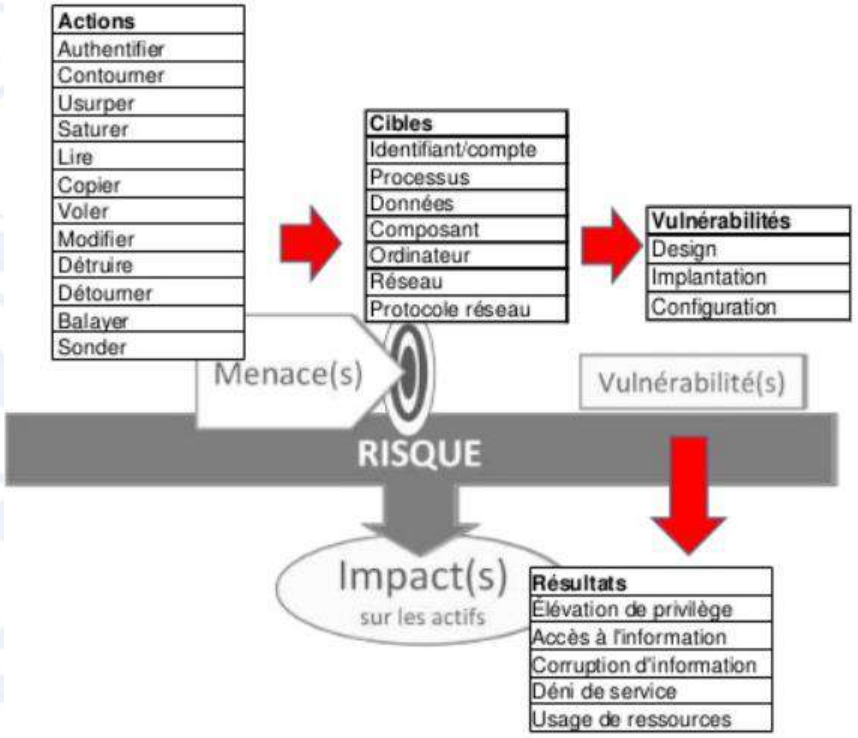
- D'autres aspects peuvent aussi être considérés comme des objectifs de la sécurité des systèmes d'information, tels que
  - La traçabilité : garantie que les accès et tentatives d'accès aux éléments considérés sont journalisés et que les journaux sont conservés et exploitables.
  - L'authentification : validation de l'identité des utilisateurs (et systèmes) afin de gérer les accès aux informations et les services et maintenir la confiance.
  - La non-répudiation (irrévocabilité): aucun utilisateur (ou système) ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées, et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

Risque : Menaces et mesures de sécurité



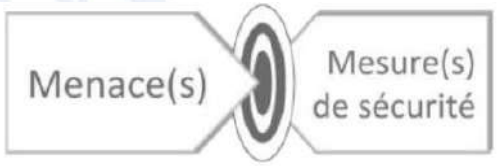
Risque : Menaces et mesures de sécurité

- Menace : Evénement potentiel et appréhendé, de probabilité non nulle, susceptible de porter attinte à la sécurité informatique
- Une menace exploite une ou plusieurs **vulnérabilités** afin d'atteindre une cible grâce à une action
- Lors que l'attaque est réussie, le résultat permet de produire un impact sur la cible (disponibilité, intégrité, et confidentialité)



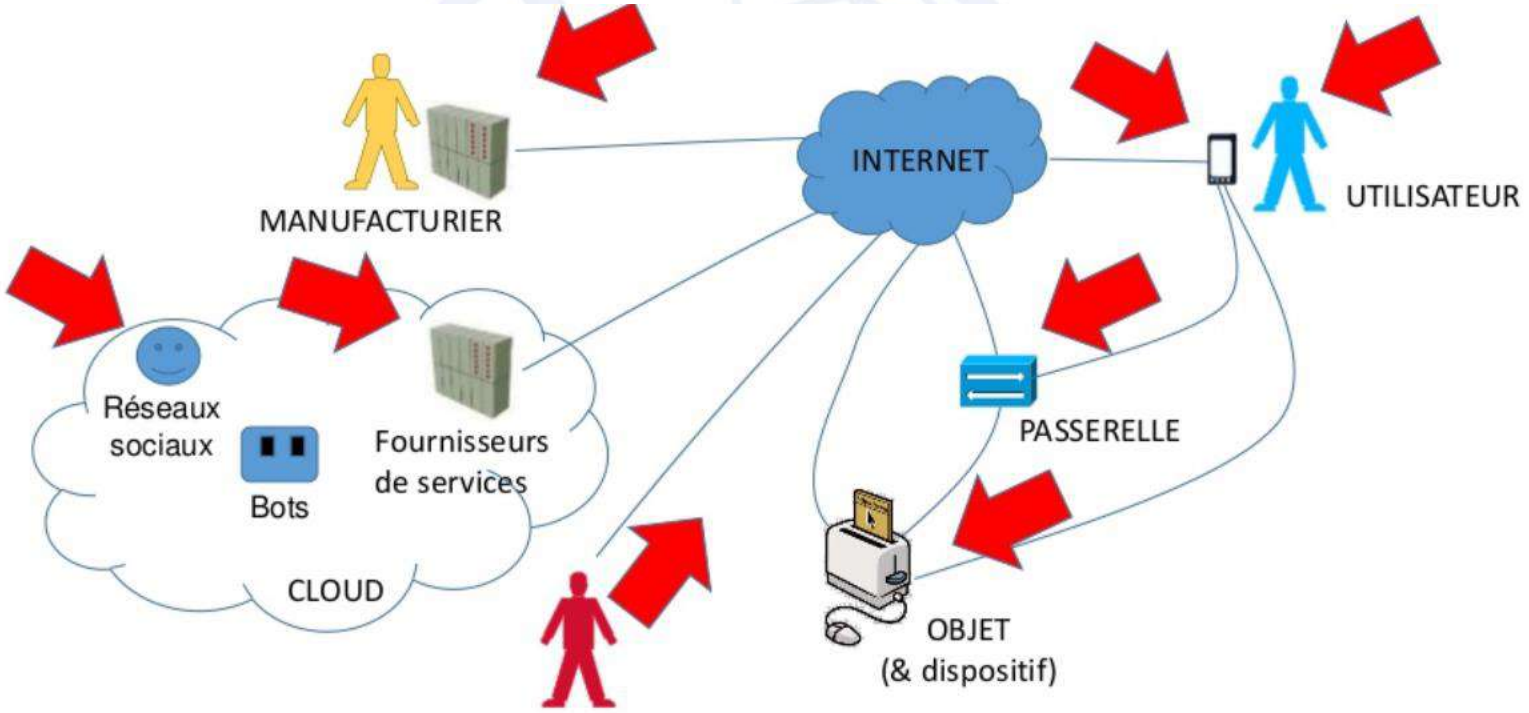
Risque : Menaces et mesures de sécurité

- Des mesures de sécurité sont mises en œuvre pour contrer une ou des menaces afin de contrôler, mitiger ou éliminer les risques

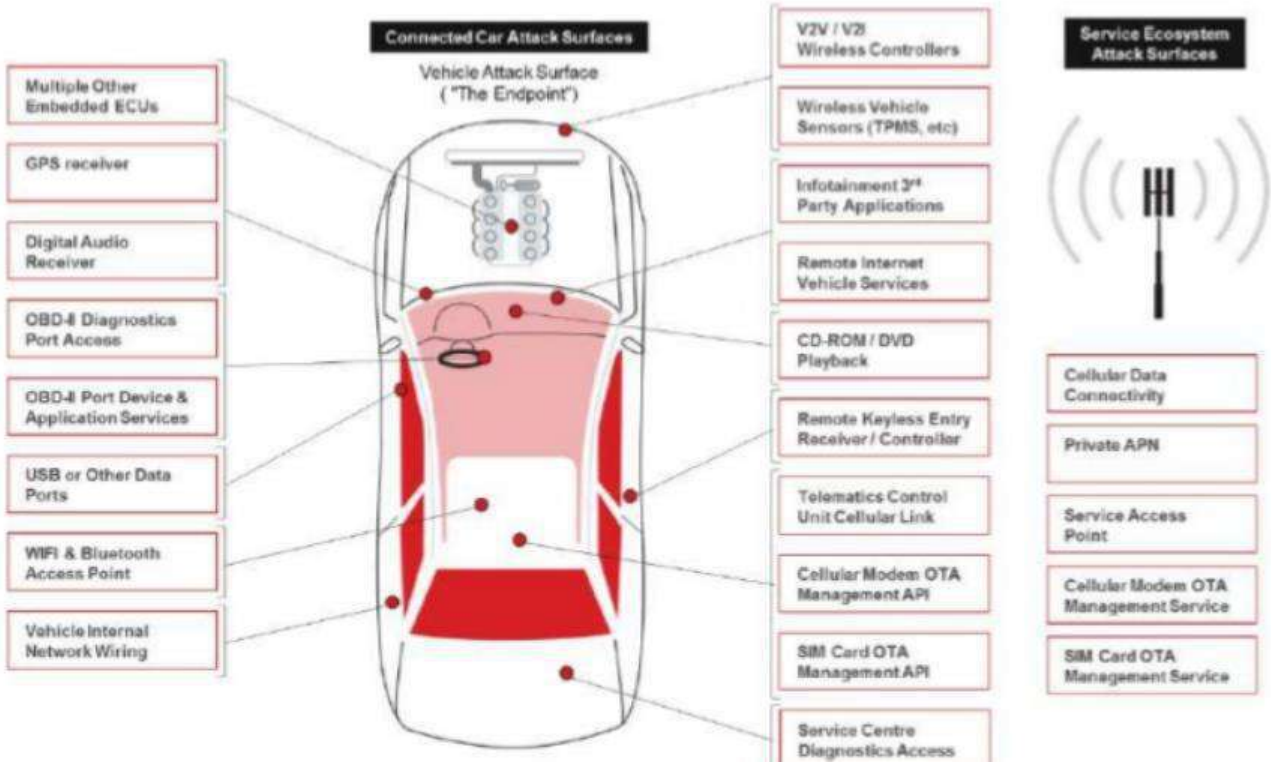


- Si malgré la mesure de sécurité, la menace réussit à atteindre un actif informationnel vulnérable, alors cette attaque est réussie. Il aura un impact sur sa disponibilité et/ou intégrité et/ou confidentialité de l'actif

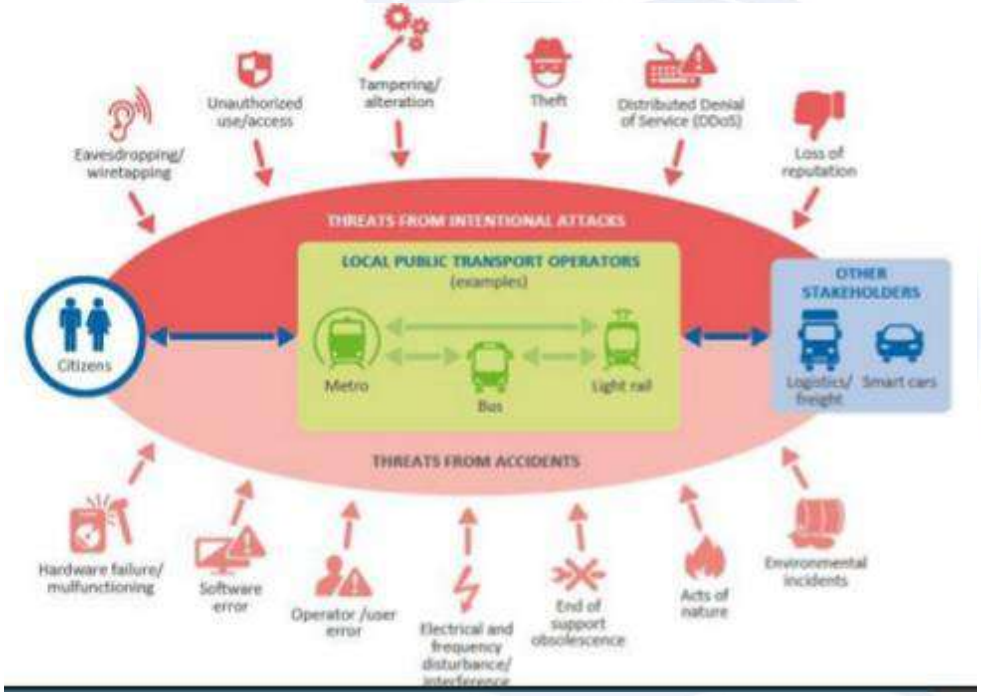
Surfaces d'attaque



Surface d’attaque de la voiture connectée



Surface d'attaque du système de transport intelligent



Menaces multiples

Nom de l'attaque	But et résultat de l'attaque	Menace	Active ou passive
DoS	- Saturer un serveur ou bloquer le trafic - Rendre un service non disponible	- Intégrité - Disponibilité - Confidentialité	Active
Man-in-the Middle	- Intercepter les communications entre deux parties contrôler la conversation - Écouter, modifier ou supprimer des données	- Intégrité - Confidentialité	Active
L'usurpation d'identité	- Vol d'identité - Réaliser des actions frauduleuses - Prendre délibérément l'identité d'une autre personne vivante,	- Confidentialité - Authentification	Active
Flooding	- Epuiser la mémoire et l'énergie des nœuds - Saturer le réseau	- Intégrité - Disponibilité	Active

Menaces multiples

Nom de l'attaque	But et résultat de l'attaque	Menace	Active ou passive
Les attaques de cartes à puces	- Pouvoir accéder aux informations et aux secrets contenus dans la carte (code PIN, clé(s) secrète(s) cryptographique(s), etc…)	- Physiques - Logicielles	Active
Wardriving	- Utilisé pour pouvoir accéder à internet au nom d'une autre personne, - Parcourir tous les lieux où le wifi est déployé afin de découvrir toutes les bornes Wifi existantes noter l'adresse géographique	- Confidentialité	Active
Snifling	- Capturer les trames circulent local et afficher les contenus entêtes des protocoles sur un réseau, id des users, MDP non crypté, etc…	- Confidentialité	Active

Menaces à différents niveaux

- Attaques sur l'ensemble de l'écosystème IoT
  - Capteurs / actionneurs
    - e.g. vider la batterie des stimulateurs cardiaques
  - Communications
    - e.g. intercepter la communication Bluetooth LE
  - Prise de décision (intégrité des données, etc.)
    - e.g. modification des messages pour modifier le comportement de la voiture intelligente
  - Confidentialité des informations
    - e.g. jouets intelligents exploités pour écouter les enfants

Vue générale des menaces

Client Web
- ❑ Code malveillant
- ❑ XSS (*cross site scripting*)

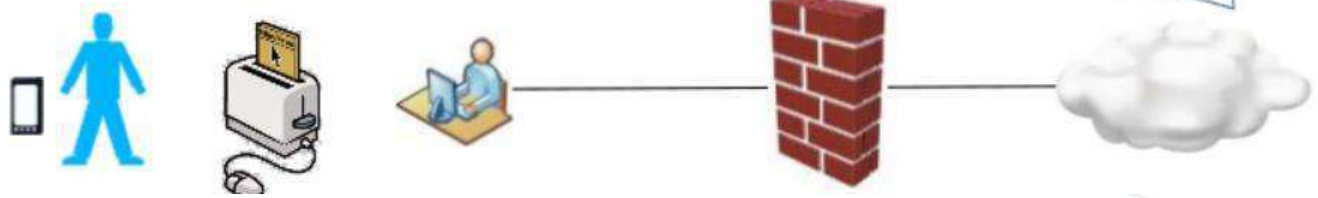
Accès à la ressource Web
- ❑ *Phishing*
- ❑DNS *poisoning*

Infrastructure télécom
- ❑Déni de service

Application & plate-forme
- ❑ Injection SQL
- ❑ Code malveillant
- ❑Déni de service
- ❑Attaque brute sur l'authentification

Infrastructure
- ❑ Code malveillant
- ❑Attaque brute sur l'authentification
- ❑Déni de service

Infrastructure télécom
- ❑Déni de service



Menaces propres aux capteurs/dispositifs

- **Détournement du dispositif:** s'applique à un dispositif qui est physiquement compromis ou pour lequel les clés sont perdues.
- **Attaque du puits (sinkhole):** désigne une attaque dans laquelle un dispositif compromis attire le trafic de communication pour former un trou noir ou mettre en place une retransmission sélective.
- **Attaque Sybil :** désigne une attaque dans laquelle un dispositif malveillant prend de multiples identités de manière illégitime.
- **Attaque par trou de ver:** une attaque par trou de vers se produit lorsque deux noeuds malveillants/compromis font croire que le trajet les reliant est très court.

Source : Rec. UIT-T X.1361 (09/2018)

Menaces propres aux capteurs/dispositifs

- **Attaques par inondation:** type d'attaque par déni de service (DoS) dans laquelle l'auteur de l'attaque envoie une succession de paquets "hello" à un dispositif visé afin de consommer une part suffisante des ressources du dispositif pour que celui-ci ne puisse plus répondre au trafic légitime.
- **Attaque par retransmission sélective:** attaque dans laquelle un nœud compromis filtre de manière aléatoire les paquets reçus et en retransmet certains au nœud suivant. On parle d'attaque par trou noir lorsque le nœud filtre (écarte) tous les paquets qu'il reçoit.
- **Usurpation de l'identité du capteur/dispositif:** désigne une attaque dans laquelle l'auteur de l'attaque réussit à se faire passer pour un capteur/dispositif légitime.

Source : Rec. UIT-T X.1361 (09/2018)

Menaces propres aux passerelles

- **Accès non autorisé:** l'accès non autorisé à une passerelle peut entraîner la divulgation d'informations sensibles, la modification de données, des dénis de service et l'utilisation illicite de ressources.
- **Passerelle malveillante:** même si toutes les passerelles hertziennes sont sécurisées, il est facile pour l'auteur d'une attaque de déployer sa propre passerelle malveillante et rassembler des informations confidentielles sur les connexions.
- **Attaque par déni de service:** une attaque par déni de service sature la mémoire et/ou la capacité informatique de sa cible afin que celle-ci ralentisse de manière significative voire interrompe la fourniture des services.

Source : Rec. UIT-T X.1361 (09/2018)

Menaces propres au réseau

- **Accès non autorisé:** l'accès non autorisé à un réseau de capteurs sans fil peut entraîner la divulgation d'informations sensibles, la modification de données, des dénis de service et l'utilisation illicite de ressources.
- **Reniflage des paquets:** dans le cas des réseaux de capteurs sans fil qui n'ont pas de capacités de chiffrement, il est généralement facile pour l'auteur de l'attaque d'écouter clandestinement les communications sur le réseau.

Source : Rec. UIT-T X.1361 (09/2018)

Menaces propres au réseau

- **Bluejacking:** il s'agit d'une attaque visant les dispositifs mobiles dotés d'une fonction Bluetooth, comme les téléphones cellulaires. Les messages envoyés n'endommagent pas le dispositif visé, mais peuvent amener l'utilisateur à répondre d'une certaine manière ou à ajouter de nouveau contact dans son répertoire.
- **Bluesnarfing:** cette attaque permet d'accéder sans autorisation à des informations contenues dans un dispositif sans fil cible grâce à une connexion Bluetooth, souvent entre téléphones et ordinateurs.

Source : Rec. UIT-T X.1361 (09/2018)

Attaques par type de technologie de connectivité	
Technologies	Risques de sécurité
WSN	• Attaque par déni de service (DoS) sur différentes couches du réseau, analyse du trafic, réplication des nœuds (attaque Sybil), problèmes de confidentialité généraux. • Attaques « black hole routing », dommages physiques / manipulation non autorisée.
RFID	• Attaques contre l'authenticité, c'est-à-dire désactivation de balises non autorisées; • Attaques contre l'intégrité, c'est-à-dire clonage de balises non autorisé; • Les atteintes à la confidentialité, c'est-à-dire le suivi non autorisé des tags; • Attaques sur la disponibilité; • Risques relatifs à la vie privée.
WiFi (802.11x)	• Attaques passives, telles que l'écoute clandestine armée d'antennes de réception appropriées; • Attaques actives, telles que les attaques de brouillage et de brouillage.
NFC	• Déni de service (DOS), fuite d'informations, détection du trafic (écoute clandestine) en mode actif.
Bluetooth	• Cryptage facultatif ou faible, paramètres par défaut non sécurisés, faible utilisation du code PIN, non sécuriséclés d'unité, protections d'intégrité défectueuses et génération de nombres prévisible; • Attaques Man-In-The-Middle, corruption de données et DOS.
ZigBee	• Traffic sniffing (écoute clandestine), décodage de paquets et manipulation de données /injection; • Dommages matériels et attaques sniffing key.
Z-Wave	• Attaque sur le cryptage codé en dur pour dévoiler la clé de contenu pour dévoiler le contenu; • Risque d'injection de paquets dans le processus d'échange de clés et prise de contrôle sur le dispositif.
	• Les attaques physiques, telles que la falsification, la destruction et le masquage des nœuds; • Plusieurs types d'attaques DOS sur plusieurs couches OSI; • Les attaques au niveau de la couche MAC comprennent les collisions, l'épuisement de la batterie et l'injustice; • Une attaque contre la couche de transport.

Menaces pour la sécurité des plateformes/services

- **Profilage:** processus d'exploration utilisé pour rassembler des informations sur la plate-forme/les services.
- **Déni de service:** attaque dans le cadre de laquelle la plate-forme/le service est submergé(e) par un très grand nombre de demandes de services et est de ce fait trop occupé(e) pour répondre aux demandes des clients légitimes.
- **Exécution d'un code arbitraire:** attaque consistant à tenter d'exécuter un code malveillant sur une plate-forme/un service afin de compromettre les ressources de la plate-forme/du service et de lancer ensuite d'autres attaques.
- **Exécution d'un code malveillant:** tout élément d'un système logiciel ou d'un script visant à causer des effets non désirés, des atteintes à la sécurité ou aux informations d'identification personnelles et des dégâts dans un système.

Source : Rec. UIT-T X.1361 (09/2018)

Mesures de sécurité

- Security by design vise à protéger la sécurité des appareils par les fabricants.
- La sécurité dès la conception peut aider l'utilisateur à comprendre les exigences de sécurité de l'IdO et l'encourage à prendre les bonnes décisions pour assurer sa sécurité et sa sûreté.
- Le gouvernement britannique exige la sécurité dès la conception dans les nouveaux produits pour répondre à la sécurité IoT, afin de garantir la sécurité des appareils connectés pendant la phase de conception et tout au long de la vie.

Mesures de sécurité

- Les solutions de cryptographie sont réputées comme des solutions sures qui répondent à l'ensemble des problèmes liés à la sécurité des données (confidentialité et intégrité).
- Les spécificités des réseaux de capteurs, à savoir une faible puissance de calcul et une mémoire limitée à laquelle se rajoute la problématique de préservation de l'´énergie, sont des freins considérables `a l'utilisation des systèmes cryptographiques courants réputes surs (SSL, RSA, etc.)
- Deux types de cryptographie :
  - la cryptographie symétrique à clé secrète et
  - la cryptographie asymétrique ou à clé publique.

Mesures de sécurité

- Un système IoT nécessite l'authentification et l'autorisation des utilisateurs et des périphériques.
  - L'authentification vérifie l'identité des utilisateurs ou des périphériques dans un système IoT
  - L'autorisation fournit les privilèges nécessaires à l'entité autorisée.

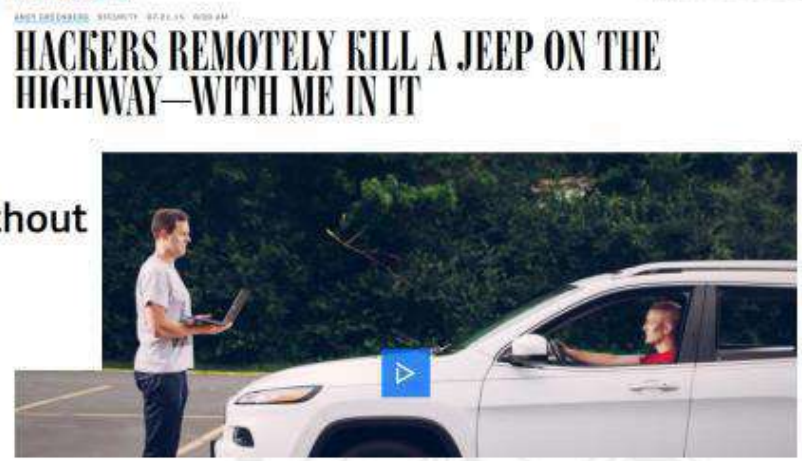
Partie 2: Vie privée et responsabilité

Vie privée

- L'une des caractéristiques importantes de l'IoT est la capacité des objets à percevoir et à ressentir leur environnement.
- Cette capacité induit à la violation de la vie privée des utilisateurs et entraînent de nombreux problèmes qui peuvent entraîner la mort de personnes.

Google Glass, le web sous vos yeux

Vie privée et menaces

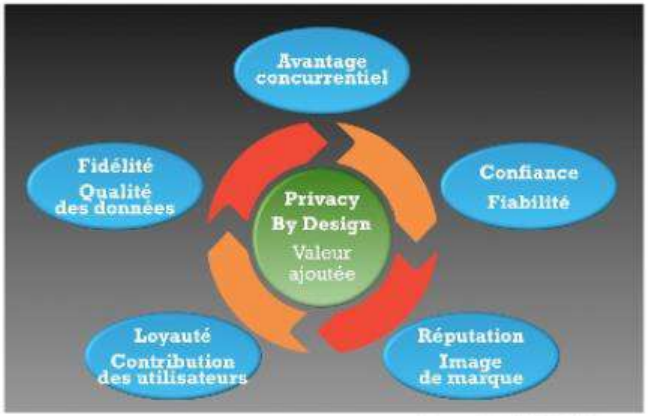


Menaces de l'IoT

- L'identification: est la menace d'associer un identifiant (par exemple, nom, adresse) avec des données privées sur un individu.
- La localisation et le suivi : sont les menaces liées à la spécification et à l'enregistrement de la position d'une personne dans le temps et dans l'espace par des moyens différents tels que la localisation du téléphone portable, le trafic Internet ou les données GPS.
- Le profilage : est le processus de collecte et de traitement de données sur les activités et les comportements des individus sur de longues périodes afin de les classer selon certaines caractéristiques et créer des profils plus complets.
- Le linkage : fait référence à la divulgation incontrôlée d'informations due à la combinaison de plusieurs sources de données séparées. L'intégration de divers types d'informations sur l'individu révèle des faits nouveaux auxquels le propriétaire ne s'attend pas.

Mesures de la protection de la vie privée

- Privacy by Design a pour objectif de garantir que la protection de la vie privée soit intégrée dans les objets dès leur conception.
- Les clients IoT doivent disposer des fonctionnalités requises pour contrôler leurs propres informations et définir qui peut y accéder.



Privacy by design au cœur de la réglementation européenne

- Privacy Awareness : L'un des principaux problèmes de violation de la vie privée est le manque de sensibilisation du public. Les utilisateurs de l'IoT doivent être pleinement conscients de la manière de se protéger contre tout type de menace pour la vie privée.
- La notification et le consentement consiste à fournir une explication et donner aux gens le choix de se décider sur la manière de traiter leurs données.

Mesures de la protection de la vie privée

- La minimisation des données consiste à collecter le moins d'informations personnelles possible.
- Les techniques de cryptographie: est l'une des principales solutions pour préserver la confidentialité des données. Cependant, avec des ressources de stockage et de calcul limitées dans les appareils IoT, cette solution reste difficile à réaliser.
- L'anonymisation des données: consiste à supprimer les éléments d'identification qui pourraient permettre un ré-identification aisée des personnes lors de traitement des données.
- Le contrôle d'accès: la mise en place d'un modèle de contrôle d'accès efficace est l'une des solutions pour protéger la vie privée des utilisateurs IoT.

Responsabilité des objets connectés

- La question de responsabilité est devenu un impératif face à l'explosion des objets connectés.
- En cas de dommages causés par un objet connecté, une plainte déposée par un tiers pourrait aboutir à un non-lieu »

→ ***D'où la nécessité d'élaborer un cadre de responsabilité propre aux objets connectés et des textes de loi qui s'adaptent à la nature des objets et leur évolution, et qui définissent sans l'ombre d'un doute la responsabilité de l'utilisateur ou encore du développeur d'un objet connecté en cas de défaillance.***

Enjeux juridiques

- L'objet est amené à posséder sa propre identité afin d'évoluer dans le réseau: Etre connu et reconnu
  - Mise en place de IPV6
    - Evolution de l'IPV4 ui ne peut couvrir structurellement l'IoT
  - Mise en place de l'ONS (Object Name Service)
    - Equivalent du DNS pour les objets
- Un objet qui est voué à agir seul et sous sa propre responsabilité
  - Ex Google Car : Quid de la responsabilité de l'accident

L'objet connect effectue des actions qui mène à la question de la responsabilité engagée

L’identité de l’objet : Futur débat?

Qand la voiture connectée va dans le mur?

Partie 3:
Normes et directives de sécurité, certification, et réglementation

Vers une normalisation

- Des normes et directives de sécurité sont requises pour le développement et opérations pour stimuler l'adoption de sécuriser les appareils IoT.
- La pérennité du marché passera par le respect des normes, des codes de conduite et l'obtention de certifications.
- Plusieurs travaux menés par de nombreuses organisations pour compenser le manque de standards (réseaux, protocoles, formats).
- Les consortiums : IISF (IoT industriel), IoT Cybersecurity Alliance, IoT-GSI de l'IUT, IEEE de l'IETF, GS1, Oasis, etc.

Le code de pratique de DCMS UK

- UK DCMS (Department for Digital, Culture, Media & Sport) a proposé un code de bonnes pratiques pour la sécurité des produits IoT grand public et des services associés.
- Le Code identifie que de nombreux problèmes de sécurité graves découlent d'une mauvaise conception de la sécurité et de mauvaises pratiques dans les produits vendus aux consommateurs:
  1. Aucun mot de passe par défaut.
  2. Mettre en œuvre une politique de divulgation des vulnérabilités,
  3. Gardez le logiciel à jour.
  4. Stockez en toute sécurité les informations d'identification et les données sensibles à la sécurité.

Source : https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

Le code de pratique de DCMS UK

5. Communiquez en toute sécurité.
6. Minimisez les surfaces d'attaque exposées.
7. Assurer l'intégrité du logiciel.
8. Veiller à ce que les données personnelles soient protégées.
9. Rendre les systèmes résilients aux pannes.
10. Surveiller les données de télémétrie du système.
11. Facilitez la suppression des données personnelles pour les consommateurs.
12. Facilitez l'installation et la maintenance des appareils,
13. Validez les données d'entrée.

Recommandations de sécurité de l'ENISA pour l'IoT

- Les recommandations de sécurité de base pour l'IoT de l'ENISA comprennent des mesures politiques, organisationnelles et techniques.
- Les mesures techniques comprennent l'utilisation d'une racine de confiance immuable basée sur le matériel et des fonctionnalités de sécurité telles que des puces/coprocesseurs de sécurité spécialisés qui intègrent la sécurité au niveau du transistor :
  - offrant un stockage fiable de l'identité de l'appareil,
  - offrant une protection des clés, et
  - empêchant les personnes non privilégiées accès au code de sécurité sensible.
- L'étendue et la profondeur de la couverture rendent cet inventaire impressionnant, mais en même temps peut-être difficile à mettre en œuvre dans la pratique.

Source : ENISA 'Baseline Security Recommendations for IoT', November 2017
https://ec.europa.eu/digital-single-market/en/news/

Recommandations de l'AIOTI

- Les exigences de base de l'AIOTI pour les dispositifs IoT incluent:
  - **Test et certification de la sécurité** - Utilisation de certifications reconnues comme étant à la pointe de la technologie niveau de risque évalué; introduction supplémentaire d'un système de classification pour certifier les dispositifs pour des scénarios d'utilisation en fonction du niveau de risque.
  - **Label de sécurité** - Labels éprouvés tels que «label d'efficacité énergétique» afin de classer l'IoT dispositif.
  - **Structures de sécurité prédéfinies et certifiées** – Exigence du cryptage d'identité, d'accès, et des canaux de communication ; et exigence du stockage sécurisé des clés et des données,

Recommandations de l'AIOTI

- **Justification de la sécurité** - Explication de la mise en œuvre des mesures de sécurité liées aux dangers coonus afin de définir un niveau acceptable de risques de sécurité à tout concepteur de dispositif IoT, auditable par une tierce personne indépendant.
- **Échange d'informations** - Partage d'informations entre fabricants sur les incidents et les vulnérabilités potentiels.
- **Fonctions définies** - Les dispositifs IoT devraient pouvoir exécuter des fonctions documentées, pour donner un sens aux appareils et services IoT
- **Normalisation** - Interopérabilité des composants et des protocoles de communication.

Programme de cybersécurité IoT de NIST

- Le programme de cybersécurité pour l'IoT du NIST entreprend des efforts pour identifier un ensemble de capacités de cybersécurité de base pour former une base de référence pour les disposiifs IoT.
- En septembre 2018, le NIST a publié une publication intitulée «Considérations pour la gestion de la cybersécurité et de la confidentialité de l'Internet des objets (IoT)» afin d'aider les agences fédérales et d'autres organisations à mieux comprendre et gérer les risques de cybersécurité et de confidentialité associés à leurs appareils IoT tout au long du cycle de vie des dispositifs.
- À partir de la mi-2019, le NIST se concentre sur l'engagement avec les parties prenantes via des ateliers et des séminaires afin de recueillir des commentaires pour un Core Référence des capacités de cybersécurité de l'IoT.

Source : https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

Guideline de la sécurité du GSMA

- Selon la GSMA, la fourniture de produits et services sécurisés est autant un processus qu'un objectif.
- Vigilance, innovation, réactivité et amélioration continue sont nécessaires pour garantir que les solutions répondent aux menaces.
- Afin de s'assurer que les nouveaux services IoT qui arrivent sur le marché sont sécurisé, la GSMA a créé un guideline au profit des prestataires de services qui cherchent à développer de nouveaux services IoT.
- Ce guideline permet aux fournisseurs de services et de produits IoT d'auto-évaluer la conformité de leurs produits, services et composants aux directives GSMA de sécurité IoT.
- La ckecklist d'évaluation permet à une entité de démontrer les mesures de sécurité qu'ils ont prises pour protéger leurs produits, services et composants issus de la cybersécurité des risques.
- Les déclarations d'évaluation peuvent être faites en soumettant une déclaration dûment remplie à la GSMA.

Source : https://www.gsma.com/iot/iot-security/iot-security-guidelines/

A retenir

- Un certain nombre de bonnes pratiques, lignes directrices et des recommandations existent, mais les efforts des organisations de normalisation telles que l'ETSI et Les NIST sont très récents.
- Les fabricants peuvent ne pas avoir l'expertise nécessaire pour utiliser les directives et recommandations disponibles. La convivialité des consignes de sécurité est un défi et nécessite plus de recherche.
- Harmonisation des directives de sécurité IoT et des recommandations sont nécessaires pour stimuler l'adoption.
- L'harmonisation doit être soutenue par des initiatives de recherche sur la cybersécurité.
- Il est important que les processus de normalisation restent aligné sur la technologie

Certification IoT

- Il y a un manque de labels pour informer les utilisateurs finaux sur la sécurité et les risques des appareils IoT. Cependant, des efforts pour créer un schéma de certification sont en cours dans diverses régions du monde.
- Il convient de veiller à ce que ces régimes soient alignés afin de créer des conditions de concurrence équitables pour les fabricants.

Cadre de certification de cybersécurité de l'UE

- Dans certains tels que la France, le Royaume-Uni et l'Allemagne, les producteurs de compteurs intelligents doivent actuellement subir des processus de certification.
- L'UE a identifié que la certification joue un rôle essentiel pour accroître la confiance et la sécurité dans les produits et services IoT essentiels pour le marché unique numérique de l'UE.
- De plus, sans un cadre commun de validité des systèmes de certificats de cybersécurité à l'échelle de l'UE, le risque croissant de la fragmentation et des obstacles dans le marché augmente.

IoT Security Foundation (IoTSF)

- Le cadre de conformité de la sécurité IoT vise à évaluer la sécurité d'un large éventail d'appareils IoT en adoptant une approche basée sur les risques dérivé de la triade CIA.
- Le cadre définit 5 classes de conformité. La classe d'un produit est définie sur la base d'une liste de contrôle des exigences. Cette liste de contrôle pourrait être rendu obligatoire par les parties contractantes afin de vérifier le respect des exigences.

Compliance class	Security objectives		
	Confidentiality	Integrity	Availability
Class 0	Basic	Basic	Basic
Class 1	Basic	Medium	Medium
Class 2	Medium	Medium	High
Class 3	High	Medium	High
Class 4	High	High	High

https://iotsecurityfoundation.org/wp-content/uploads/2016/12/IoTSecurity-Compliance-Framework.pdf

Cadre de certification de cybersécurité de l'UE

- UE a proposé un cadre de certification pour les produits de sécurité IT. Ce cadre fournit un ensemble complet de règles, exigences techniques, normes et procédures. L'ENISA est en charge de la mise en œuvre du processus de certification.
- Le résultant certificat est reconnu par tous les États membres, facilitant ainsi pour les entreprises le commercer au-delà des frontières et pour acheteurs pour comprendre les caractéristiques de sécurité du produit ou service.
- L'utilisation de la certification est volontaire pour le moment
- étant, le cadre évite la certification multiple processus dans différents États membres et crée un incitation à certifier la qualité et à vérifier la sécurité des les produits et services en question.

Common Criteria (CC)

- Le CC permet aux développeurs de produits de documenter leur les exigences fonctionnelles de sécurité (SFR) du produit dans un Cible de sécurité (ST).
- Un laboratoire indépendant peut évaluer son le produit par rapport aux SFR. La robustesse de l'évaluation dépend du niveau d'assurance de l'évaluation (EAL).
- En théorie, cette approche permet à un développeur de produit IoT de démontrer que son le produit répond aux exigences fonctionnelles de sécurité spécifiques.

Common Criteria (CC)

- Signataires de l'Accord de reconnaissance CC (ADRC) reconnaîtront la certification CC et en particulier les profils de protection collaboratifs (cPP).
- Le cPP pour
- Les périphériques réseau v2. semblent être le profil sur lequel s'appuyer pour la sécurité IoT; cependant, il est à noter que ce cPP manque de critères relatifs, par exemple, à la ressource de l'appareil les contraintes et l'hétérogénéité des équipements et du réseau environnements.
- La certification CC est un processus lent et coûteux pour les fabricants. Alors qu'il apparaît bien adapté pour tester les systèmes informatiques à vendre aux gouvernements, cela peut ne pas être aussi approprié pour les et un monde IoT à faible coût. Les alternatives non CC peuvent fournir une approche légère de la certification et peut
- s'avérer plus approprié.

https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V2.1.pdf

Politiques législatives et réglementation

- Le déploiement des systèmes IoT et leurs impacts potentiels sur les individus et les entreprises font émerger de nouvelles problématiques de réglementation avec un besoin d'adaptabilité à un domaine mouvant (protection des données, vie privée, sécurité…).
- Deux types d'initiatives réglementaires sont en cours :
  - Des initiatives sectorisées, portées par les acteurs industriels souhaitant établir un cadre réglementaire pour leurs activités sectorielles.
  - Des interventions des autorités publiques dans des domaines nécessitant des arbitrages entre les parties prenantes (industriels, société civile…).

Loi Américaine sur l'amélioration de la cybersécurité IoT de 2017

- Cette législation permet de définir les normes de sécurité applicables aux équipements IoT installés sur les réseaux de l'administration américaine.
- Elle vise à garantir la protection et l'absence de vulnérabilité des équipements en cas d'attaques, la conformité des produits avec les normes sectorielles ainsi que la possibilité de leur appliquer des correctifs.
- La loi interdirait également aux fournisseurs de vendre des équipements dont les mots de passe ne pourraient être modifiés.
- La législation obligerait également les agences américaines à établir et maintenir des inventaires des appareils IoT et des mettre à jour tous les 30 jours.

Loi no° 327 du Sénat de Californie

- Loi SB 327 de Californie, approuvée en septembre 2018, est entrée en vigueur en janvier 2020.
- Elle exige que tous les appareils connectés doivent être dotés d'une "sécurité raisonnable".
- Les experts en sécurité soulignent que la loi est bien intentionnée et même si cela ne résout pas réellement les problèmes qui nuisent à la sécurité IoT, elle est néanmoins largement considérée comme un bon début.

Loi de l'UE sur la cybersécurité

- En décembre 2018, l'UE a adopté la Loi sur la cybersécurité pour renforcer le mandat de l'Agence Européenne ENISA pour mieux soutenir les États membres qui luttent contre les menaces et les attaques de cybersécurité.
- Cette loi établit également un cadre européen pour la certification de cybersécurité, la cybersécurité des services en ligne et des dispositifs grand public.
- La certification est volontaire sauf si la future législation de l'UE prescrit un certificat UE comme une exigence obligatoire pour satisfaire un besoin de sécurité spécifique.

Directive NIS

- La directive sur la sécurité des réseaux et des informations systèmes a été adoptée par le Parlement Européen le 6 juillet 2016 et est entré en vigueur le Août 2016.
- La directive NIS prévoit des mesures juridiques pour accroître le niveau général de cybersécurité dans l'UE en garantissant
  - L'état de préparation des États membres en exigeant qu'ils soient équipé de manière appropriée, par ex. via une sécurité informatique Équipe d'intervention en cas d'incident (CERTE) et une autorité nationale NIS.
  - La coopération entre tous les États membres, en mettant en place un groupe de coopération, afin de soutenir et de faciliter la coopération stratégique et l'échange d'informations entre les États membres.

Règlement général sur la protection des données (RGPD)

- Le RGPD, entré en vigueur le 25 mai 2018, constitue aujourd'hui le texte de référence en matière de protection des données à caractère personnel pour l'UE.
- Les deux principes du RGPD vise renforcer le droit des personnes concernées par les traitements des données et accroitre la responsabilité des entreprises responsables des traitements de données personnelles
- Ce règlement s'applique à toute entreprise qui traite des données relatives aux résidents de l'UE, qu'elle soit établie au sein ou en dehors de l'UE.
- Ainsi les GAFA ou n'importe quelles entreprises qui s'adressent au marché européen sont concernées par ce règlement.

Règlement général sur la protection des données (RGPD)

- Le RGPD introduit 3 concepts novateurs :
  - **Privac*y by design***, prise en compte de la protection de la vie privée dès la conception d'un service ou d'un produit.
  - **Privacy by default,** principe de protection des données au plus haut niveau possible par défaut.
  - **Accountability**, logique de responsabilisation reposant sur l'auto-contrôle des mesures prises pour garantir la conformité des traitements de données et la prouver.

- En Europe : la réglementation axée sur la donnée
- En Amérique : la réglementation axée sur les objets

Partie 4 : dentification et gestion des données

Numérotation et adressage

- Plusieurs systèmes d'adressage sont utilisés pour identifier les objets connectés dans les réseaux :
  - Identifiants ouverts : numéros de téléphone mobiles, identifiants de cartes SIM, adresses IP (dans leurs variantes IPv4 ou IPv6), adresses MAC, identifiants OID (Object IDentifiers) de l'UIT, EPC, UID, etc.
  - Identifiants propriétaires : formats non standardisés.
- Le principal enjeu est d'éviter la pénurie d'identifiants ouverts face à un volume d'objets connectés toujours croissant. Mais également de permettre l'interopérabilité compte tenu des différentes modalités d'adressage.

Numérotation et adressage

Réseaux cellulaires

- Les normes 3GPP (GSM / UMTS / LTE) prévoient qu'à chaque ligne mobile soit affecté un numéro de téléphone mobile MS-ISDN compatible avec le standard E.164 de l'UIT.
- Ces numéros MS-ISDN sont également utilisés pour identifier les objets connectés dans le système d'information de l'opérateur de réseau mobile.
- Cependant, l'objet communique généralement avec l'application métier par le biais de protocoles de communications tels que l'IP, situé sur une couche réseau supérieure.

Numérotation et adressage

Réseaux cellulaires (Suite)

- Toutefois, les protocoles de communication voix et SMS, utilisant le numéro MS-ISDN comme identifiant d'adressage, sont utilisés dans le cadre de certaines applications spécifiques, telles que les actions de télé-relève commandées par un système central.
- Compte tenu de leur fonction d'identification du réseau mobile et de leur rareté, les codes MNC sont uniquement attribués aux opérateurs qui, au regard de leurs infrastructures et de leurs contrats, sont en mesure de les exploiter.
- En pratique, il s'agit à ce jour des opérateurs de réseaux mobiles (MNO) et des opérateurs de réseaux mobiles virtuels (MVNO).

Numérotation et adressage

Réseaux LPWAN

- Il n’existe à ce jour aucun plan de numérotation standardisé et unifié.
- Ces réseaux utilisent des identifiants privés, aux formats propriétaires, pour identifier les capteurs.

Numérotation et adressage

Identifiants RFID et NFC

- De nombreux objets disposent aujourd'hui d'un identifiant RFID ou NFC.
- L'identifiant RFID est constitué de plusieurs sous-identifiants, intégrés dans la mémoire de la puce électronique dès sa fabrication ou utilisés par l'opérateur final.
- L'autorité d'enregistrement (l'ISO) assure la cohérence d'ensemble et attribue des codes à une pluralité d'organismes, qui gèrent la mise à disposition de certaines sous-familles d'identifiants auprès des utilisateurs.
- L'ISO a publié la norme ISO/IEC 2916149 qui présente les différentes manières d'identifier les objets pour les applications de l'IoT.

Numérotation et adressage

Adressage IP

- Certains objets nécessitent d'être directement accessibles sur le réseau Internet et doivent disposer d'adresses IP publiques, accroissant ainsi la demande en ressources IP.
- Au niveau mondial, la gestion des adresses IP est assurée par l'ICANN qui partage les adresses IP en blocs, entre les différents registres régionaux, qui se chargent de les attribuer localement.
- Le RIPE NCC a annoncé le début de la distribution des adresses issues du dernier bloc d'adresses IPv4 (version du protocole définie en 1981) dont il dispose, alertant ainsi contre un risque de pénurie et appelant à la nécessaire migration vers le nouveau système d'adressage IPv6.

Partie 5: Roaming et réglementation

Introduction

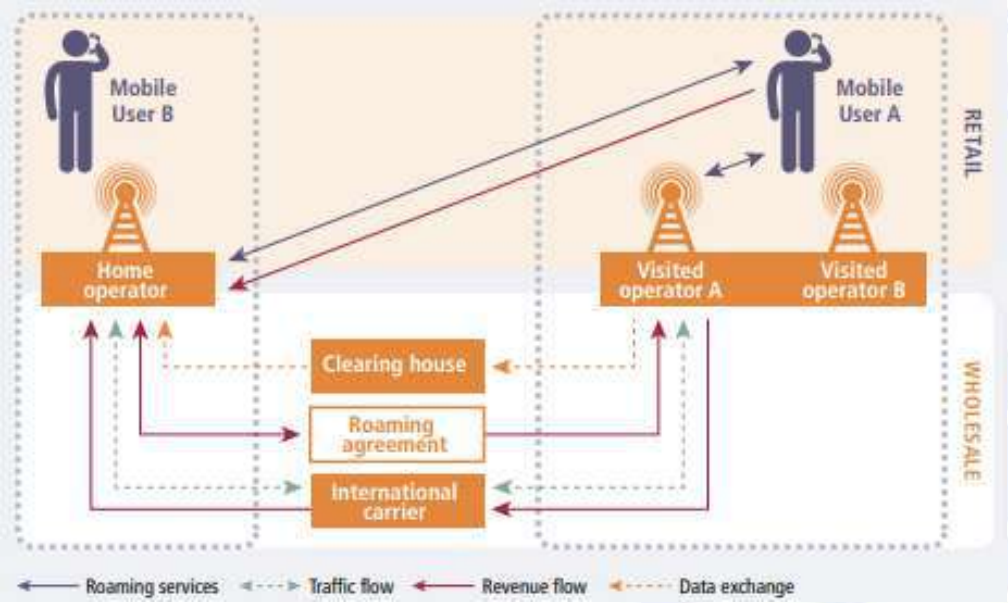
- Les tarifs des services de roaming (IMR) au niveau national, régional et international sont toujours la préoccupation des décideurs et autorités réglementaires nationales (recherche de solutions réglementaires et commerciales).
- Les discussions ne se concentrent pas uniquement sur le roaming de la voix ou des données, ou sur les principes liés au commerce international; mais aussi sur l'évolution des revenus du trafic et d'usage, les nouveaux modèles économiques ainsi que les nouvelles opportunités et innovations liées au roaming des communications IoT et M2M.

Concept IMR

- Le Roaming signifie littéralement itinérance en français.
- Ce service permet à l'abonné de continuer à utiliser son téléphone mobile et son numéro de téléphone pour accéder aux services vocaux et aux SMS, lorsqu'il qu'il se déplace dans un autre pays, par l'intermédiaire du réseau de l'opérateur mobile du pays visité.

Source: International roaming explained, GSMA

Concept IMR



Il existe 2 types de Roaming:

- Roaming entrant ou Inbound Roaming, désigne l'itinérance de clients étrangers
- Roaming sortant ou Outbound Roaming, désigne l'itinérance depuis l'étranger.

Source: International roaming explained, GSMA

Définition

Définition de l’UIT –T D.97

- L'IMR est un service (téléphonie, SMS/MMS, données) qu'un abonné à des services mobiles postpayés ou prépayés achète auprès d'un opérateur de téléphonie mobile de son pays d'origine.
- Il permet à l'abonné de pouvoir continuer à utiliser son numéro de téléphone mobile national et les services de téléphonie, de messages courts (SMS) et de données pendant un séjour à l'étranger, par le biais du réseau d'un opérateur de téléphonie mobile du pays visité, appelé le réseau de l'"opérateur visité", toutes les dispositions étant prises par l'opérateur d'origine.

Service roaming

- La réalisation du service Roaming passe par la mise en œuvre d'une structure qui doit permettre l'inter-connectivité des réseaux partenaires et garantir une bonne qualité de service pour les roamers.
- Cette structure est la suivante :
  - Connectivité entre réseaux mobiles : établissement des liens de signalisation (SS7, SIGTRAN ou MEDIATER) et d'interconnexion.
  - Accord (bilatéral ou unilatéral): Cet accord concerne essentiellement l'interconnexion des deux réseaux, la fixation des tarifs/prix, le format des données ainsi que le mécanisme qui régit l'échange de ces données. – Facturation: Génération de tickets d'usage par le réseau visité et établissement de factures
  - Test: Il s'agit de tests permettant la vérification de l'interfonctionnement et la qualité de service
  - Service de Roaming: Les services proposés dépendent des capacités de la station mobile, La liste des services spécifiés dans l'accord, le type de souscription, etc.

Challenges de l'IMR

- Accords bi/multilatéraux et initiatives régionaux
- Prix/Tarif de l'IMR
- Concurrence du marché
- Protection du consommateur

Source : ITU IMR Strategic Guidelines, 2018

Accords bi/multilatéraux et initiatives régionales

- Accord (bilatéral ou unilatéral): l'accord porte sur les aspects techniques et composants commerciaux nécessaires pour activer le service IMR. Il concerne essentiellement l'interconnexion des deux réseaux, la fixation des tarifs/prix, le format des données ainsi que le mécanisme qui régit l'échange de ces données.
- La multiplication des accords entre opérateurs permet à l'abonné de continuer à utiliser son téléphone portable dans la quasi totalité des pays de la planète.
- Cela s'avère un atout majeur pour les grands voyageurs ou les professionnels soumis à de nombreux déplacements, mais peut toutefois se révéler très onéreux lorsqu'on n'y prend pas garde.

Tarifs de l'IMR

- Les tarifs de gros et de détail de l'IMR sont les prix facturés pour le service IMR, à savoir:
  - les tarifs de gros de l'IMR sont les prix facturés par l'opérateur visité à l'opérateur d'origine pour permettre aux abonnés de l'opérateur d'origine d'utiliser le réseau de l'opérateur visité;
  - les tarifs de détail de l'IMR sont les prix que l'opérateur d'origine facture à ses abonnés pour utiliser les services IMR.

Tarifs de l'IMR

- La réglementation des tarifs de détail ou de gros de l'IMR pourrait suivre au moins l'un des principes suivants (Recommandation D.97):
  - Analyse comparative: basée sur la comparaison des tarifs de détail ou des tarifs ou coûts de gros pertinents, compte tenu des bonnes pratiques et expériences internationales.
  - Minoration au détail: les tarifs de gros de l'IMR sont estimés à partir des prix de détail pertinents, en retranchant un pourcentage.
  - Approche orientée vers les coûts: calcul du coût de gros de l'IMR en identifiant les coûts pertinents de fourniture de l'IMR, y compris tout taux de rentabilité raisonnable dont le niveau permet de favoriser l'investissement et l'innovation.

Tarifs de l'IMR

- Pour l'approche orientée coût, il convient de prendre en compte, au minimum, les éléments suivants lors de l'estimation de tarifs compétitifs et financièrement abordables pour l'IMR:
  - Coûts d'accès, de lancement et de terminaison au niveau local;
  - Coûts de la terminaison internationale, coûts des passerelles internationales; – coûts du transport local;
  - Coûts du transport international;
  - Frais propres à l'itinérance, y compris les frais d'établissement du contrat, de facturation et de signalisation;
  - Frais propres à la vente au détail, en particulier les coûts de facturation et de traitement international (y compris les relevés CDR et les tarifs IOT).

Concurrence du marché de services IMR

- Si la cherté du Roaming persiste dans nos pays, cela pourrait entraîner :
  - l'utilisation encore plus accrue et plus fréquente des SIM locales au détriment du Roaming, entraînant ainsi une perte de revenu non négligeable pour les opérateurs.
  - Une utilisation plus accrue des services OTTs (Skype, Viber, Facebook…) en remplacement du Roaming.

Free roaming

- Le free roaming est un service d'itinérance réglementé qui se caractérise par la suppression de toute surtaxe et surcharge sur les services de roaming.

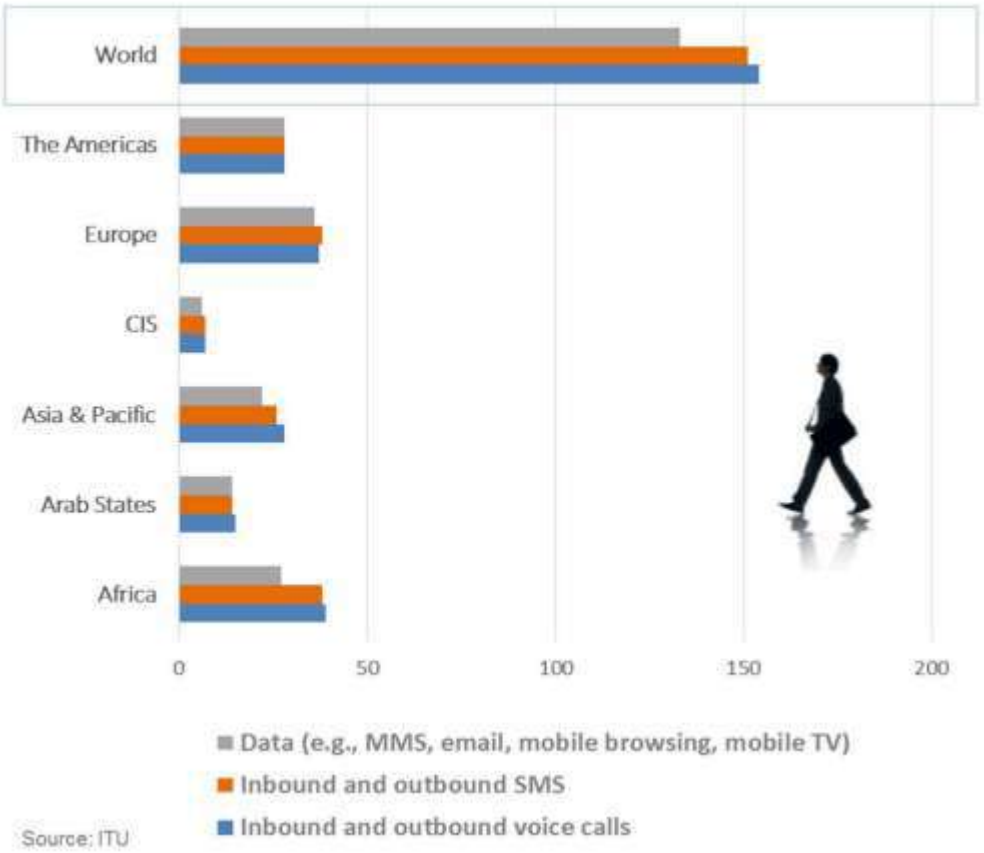
Activités de la CE3 de l'UIT-T

- A l'UIT, la Commission d'études 3 du Secteur de la normalisation des télécommunications (UIT-T) a élaboré une Recommandation sur les tarifs des services d'itinérance mobile.
- Un résumé des travaux de la Commission d'études a été soumis à l'OMC. Il est précisé dans le projet que les Etats Membres de l'UIT «devraient examiner comment protéger les consommateurs et leur donner les moyens de faire les meilleurs choix parmi les nombreuses options qui leur sont offertes sur le marché mobile en rapide évolution».

Activités de l'UIT sur le roaming

- Le règlement international des télécommunications (RTI) (v. 2012) stipule « Member states fostervmeasures to ensure that authorized oprating agencies provide free-of-free, transparent

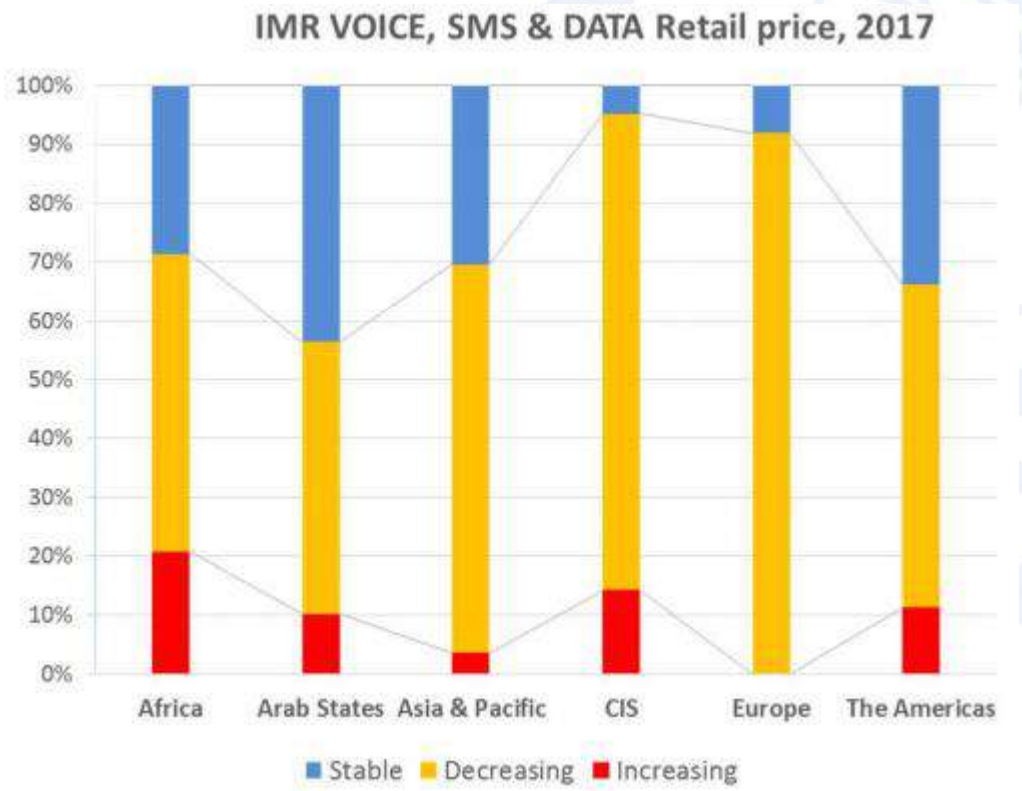
Disponibilité des services de roaming



- La disponibilité des services d'itinérance est en croissance dans tous les régions.
- Malgré cette augmentation mondiale, il y a encore des écarts sur la disponibilité de l'itinérance des données.

Source : ITU ICTEye

Le prix des services d'itinérance est en baisse… mais toujours pas assez

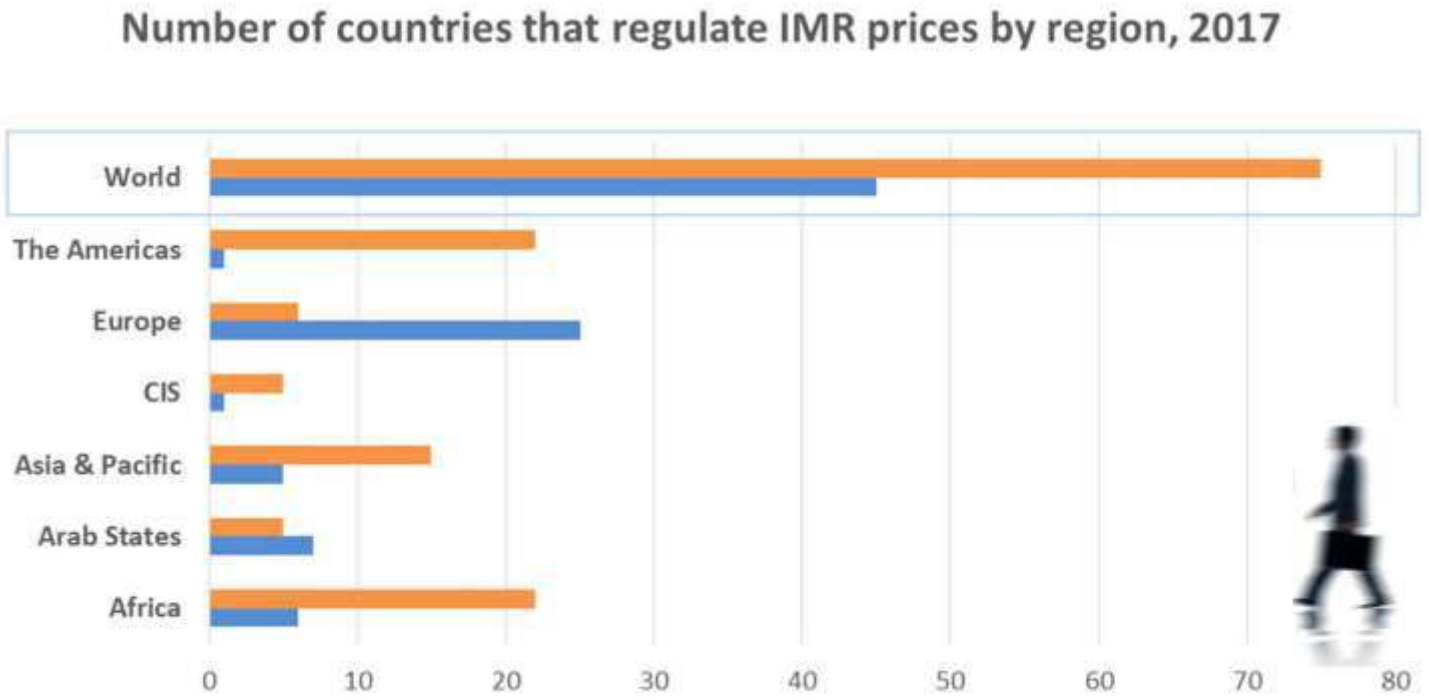


A global comparison of IMR and national prices showed that roaming calls and SMS prices were **three to six times higher** than the corresponding national tariffs[2].

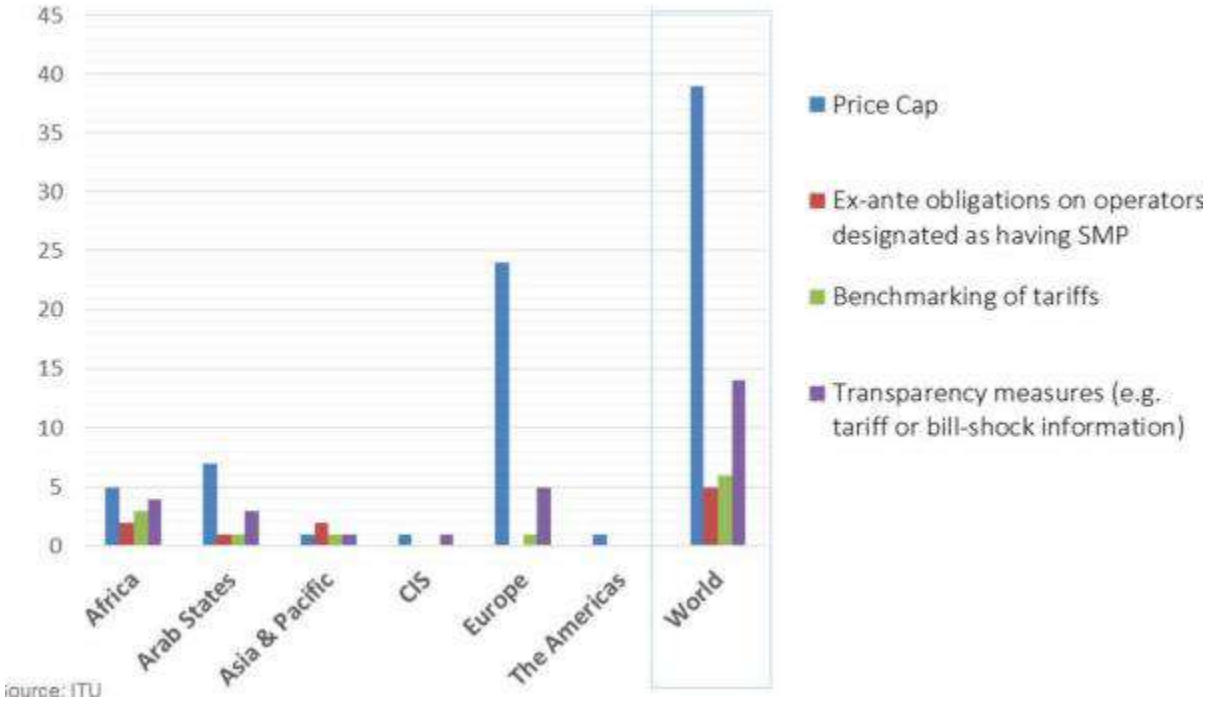
Source : ITU ICTEye

Réglementation du roaming

- Le nombre de pays appliquant la réglementation IMR, ciblant les prix de détail, est très faible dans toutes les régions, à l'exception de l'Europe.



Pratiques réglementaires appliquées par les ARN



Source: ITU

Intérêt d'un roaming régional

- Résoudre le problème du prix élevé des services d'itinérance
  - A travers la suppression de toute surtaxe et coûts artificiels sur les communications internationales
  - La fixation de tarifs plafonds par une approche règlementaire
  - A partir d' étude sur la chaine de valeur des coûts d'itinérance
  - En suivant les recommandations UIT-T D. (D.98 & D97)
- Déterminer les droits et devoirs des acteurs (opérateurs, régulateurs , fournisseurs de service, consommateurs) intervenants dans l'itinérance régionale.
- Offrir une alternative à l'utilisation des services OTTs
- Constituer un marché intérieur des services de communication mobile où convergent tarifs nationaux et tarifs de roaming communautaire.

Expériences dans le roaming régional : Exemple de l'UE

- Une initiative visant à limiter les tarifs de Roaming a été menée par l'UE.
- En Juin 2007 : l'UE a instauré un règlement de la Commission Européenne « N° EC 717/2007 », définissant « Eurotarif » ; il concerne la fixation d'un prix maximum des appels internationaux de téléphonie mobile dans l'UE lorsque l'abonné est en mode Roaming.
- Objectifs recherchés:
  - Mettre fin à l'opacité des tarifs et aux ententes entre opérateurs pour maintenir des prix élevés au détriment du consommateur, et instituer un « Eurotarif »;
  - Fixer au niveau communautaire, des redevances maximales par minute (pricecap) pour le prix de détail comme pour le prix de gros;
  - Refléter le plus fidèlement les coûts effectifs de fourniture du service,.

Expérience dans le roaming régional : Exemple de l'UE

- La fixation de prix Roaming en Europe pour les opérateurs européens laisse en outre des marges de manœuvre aux opérateurs pour se concurrencer avec des prix en-dessous des prix maxima.
- L'Eurotarif a connu des baisses significatives depuis sa mise en œuvre en 2010.
- En Juin 2017 : L'UE a mis en place un nouveau règlement sur le roaming, imposant la suppression des frais du roaming dans les 28 Etats membres, y compris au Royaume-Unis.

Expérience dans le roaming régional : Exemple de l'UE

- L'objectif de la suppression des frais d'itinérance n'est pas d'aboutir à une harmonisation des montants des forfaits téléphoniques dans l'UE, ni même de créer une concurrence entre tous les opérateurs européens.
- L'idée est plutôt de favoriser la mobilité des consommateurs, en leur assurant des communications mobiles sans surcoût lors d'un séjour en Europe et la nouvelle réglementation mise sur une utilisation raisonnable de l'itinérance.

Expérience dans le roaming régional : CEDEAO

- L'Afrique de l'Ouest a démarré officiellement le Free roaming en date du 31 mars 2017.
- Les premiers pays qui ont commencé sont : Burkina Faso, Côte d'Ivoire, Guinée, Mali, Sénégal, Togo, et Bénin.
- 16 décembre 2017: Règlement C/REG.21/12/2017 portant sur l'itinérance sur les réseaux de communications mobiles ouverts au public à l'intérieur de l'espace CEDEAO (Communauté Economique Des Etats de l'Afrique de l'Ouest)

Objectifs du règlement

- Définir un cadre juridique et tarifaire harmonisé pour l'itinérance sur les réseaux publics de communication mobile dans les États membres de la CEDEAO.
- Résoudre le problème du coût élevé des services d'itinérance dans la région CEDEAO, par la réduction, voire l'élimination, (en fonction du type d'appel / service)
- Déterminer les droits et obligations des fournisseurs d'itinérance communautaire, des régulateurs et des États membres de la CEDEAO.
- Fournir un minimum de garanties aux consommateurs de services d'itinérance

One Network

- Celtel a lancé le premier réseau sans frontière au monde, baptisé « One Network »
- Il couvre le Kenya, l'Ouganda et la Tanzanie.
- EAC (communauté d'Afrique de l'Est)
- En novembre 2007, Celtel a élargi ce réseau à neuf pays africains supplémentaires; le Burkina Faso, le Gabon, le Malawi, le Niger, le Nigeria, la RDC, la république du Congo, le Soudan et le Tchad se sont retrouvés ainsi connectés.
- Il permet à plus de 400 millions de personnes dans douze pays de communiquer à travers leurs frontières respectives sans payer de surprime pour frais d'itinérance.

One Network

- Un argument de poids à faire valoir auprès des autorités de régulation et des opérateurs pour motiver une baisse généralisée des tarifs du roaming.
- Deux problèmes menacent le développement des « One network »
  - Prolifération de taxes sur les communications internationales entrantes
  - Contrôle du volume de ce trafic, qui ont pour effet de relever de manière substantielle la taxe de terminaison vers ces pays.
- Cette inflation des coûts de terminaison d'appel vers ces pays (tels que le Congo Brazzaville, la Guinée, ...) remet au cause le modèle économique des réseaux uniques.

Expérience dans le roaming régional : CCG

- Les régulateurs du CCG ont adopté des politiques concertées pour faire baisser les prix d'itinérance dans les pays du Golfe:
  - d'abord pour les appels vocaux en itinérance (en juin 2010), et
  - Ensuite pour d'autres services d'itinérance (en juin 2015, avec entrée en vigueur au 1er avril 2016).

Activité de l'UIT-T

- A l'UIT, la Commission d'études 3 du Secteur de la normalisation des télécommunications (UIT-T) a élaboré une Recommandation sur les tarifs des services d'itinérance mobile qui sera soumise pour approbation en septembre 2012.
- Lignes directrices de l'UIT-T au travers de la D98: - obligation de transparence des opérateurs; - instauration de mesures de protection des consommateurs;
- encouragement d'une concurrence sur le service ; - interventions réglementaires: plafonnement des factures et/ou tarifs, présélection…
- Conclusions de la CE-3 de l'UIT de mai 2014, notamment le développement d'un modèle de coûts du Roaming.

Etude des incidences économiques des procédures d'appel alternatives

- Dans plusieurs Etats Membres en développement, différentes formes de procédures d'appel alternatives mises en œuvre grâce à des instances de routage du trafic et/ou des SIM Box se développent de manière exponentielle.
- Grâce à l'introduction de différentes surtaxes appliquées à la terminaison internationale et à la mise en œuvre d'initiatives visant à réduire les tarifs de l'itinérance mobile internationale, les conditions sont optimales pour procéder à un arbitrage.

→ Un nouveau sujet d'étude au titre de la Question 8/3, dont le principal objectif serait d'étudier les incidences économiques des procédures d'appel alternatives et d'élaborer des lignes directrices ou un projet de Recommandation UIT-T.

Thank you for your attention!

PRIDA Track 3 (T3)

Le spectre et les technologies IoT

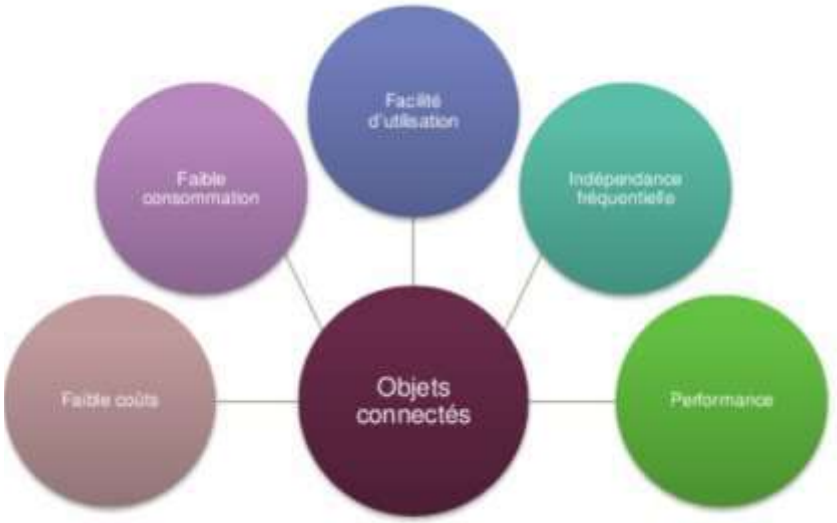
21/08/2020

Agenda

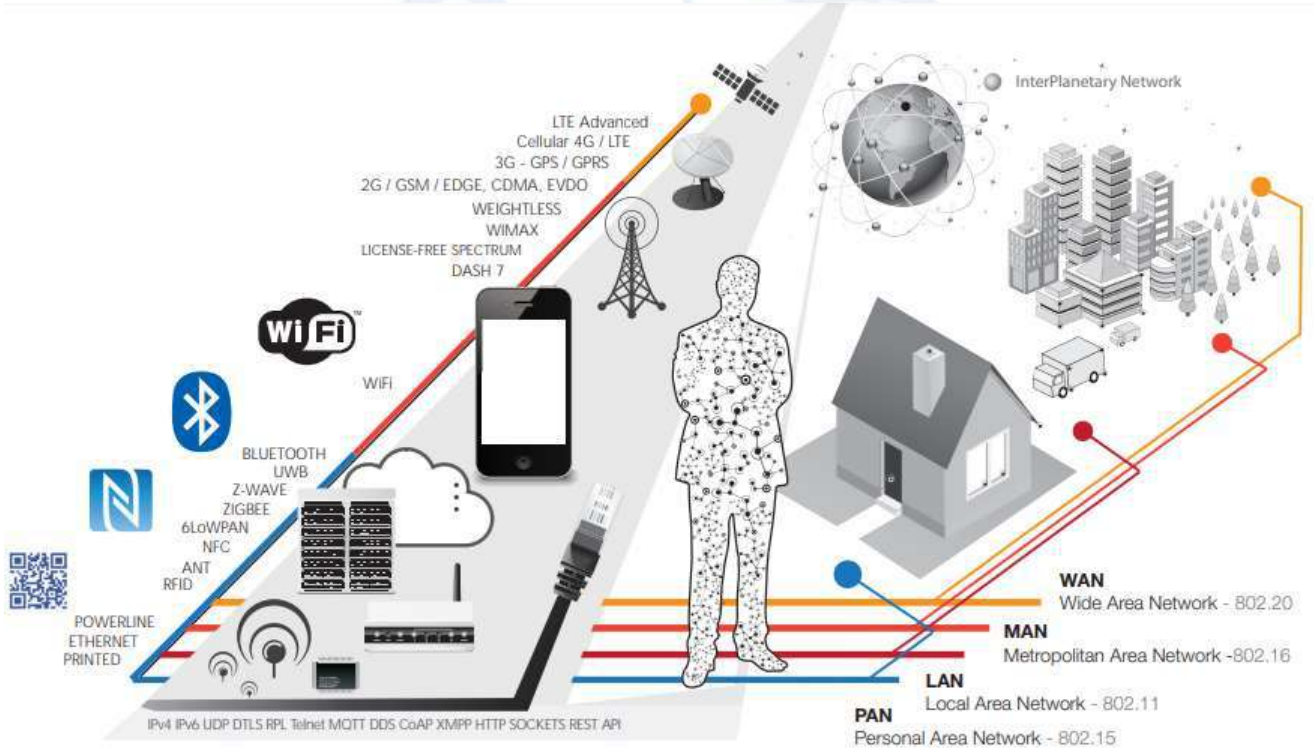
- Partie 1: Technologies à courte portée
- Partie 2: Spectre et technologies mobiles
- Partie 3: Spectre et technologies des satellites
- Partie 4 : Spectre et technologies 3GPP
- Partie 5 : Protocoles IoT

Caractéristiques des objets connectés

1. **Faible coût :**
   - *CAPEX : limiter les coûts*
   - *OPEX : facture télécom allégée*
2. **Faible consommation d'énergie :**
   Afin d'allonger l'espérance de vie de la batterie, réduire l'entretien, être indépendant du réseau électrique et de la localisation
3. **Facilité d'utilisation :**
   En ce qui concerne l'intégration dans les objets mais aussi en ce qui concerne la gestion et l'intégration avec les systèmes informatiques objet
4. **Independence fréquentielle :**
   Utilisation de fréquences sans licence, gratuites pour une universelle (Bandes ISM ou Lumière)
5. **Authentification embarquée :**
   Pour éviter des frais supplémentaires (et la gestion de cartes SIMs par exemple)
6. **Technologie performante :**
   - *Longue portée*
   - *Authentification embarquée*
   - *pénétration (eau/béton)*
   - *Utilisation des normes de transport/réseaux (IPv6)*
   - *Sécurisation*



Technologies de connectivité

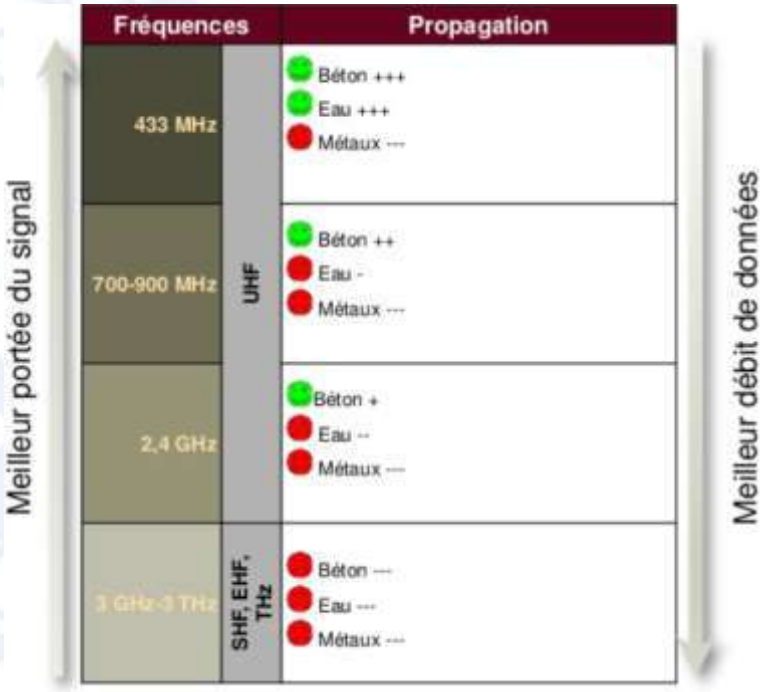


Critères de communication

- Bandes de fréquences
- Débit de transfert de données : dépend de la largeur de bande passante
- Topologies
- Portée
- Puissance consommée
- Appareils contraints
- Réseaux à nœuds contraints

Bandes de fréquence

- Choix de la bande de fréquence
- Plusieurs fréquences sont disponibles
- Chaque bande de fréquence possède ses propres qualités et contraintes



Sources: https://fr.slideshare.net/MartialAbissi/internet-des-objets-55908847

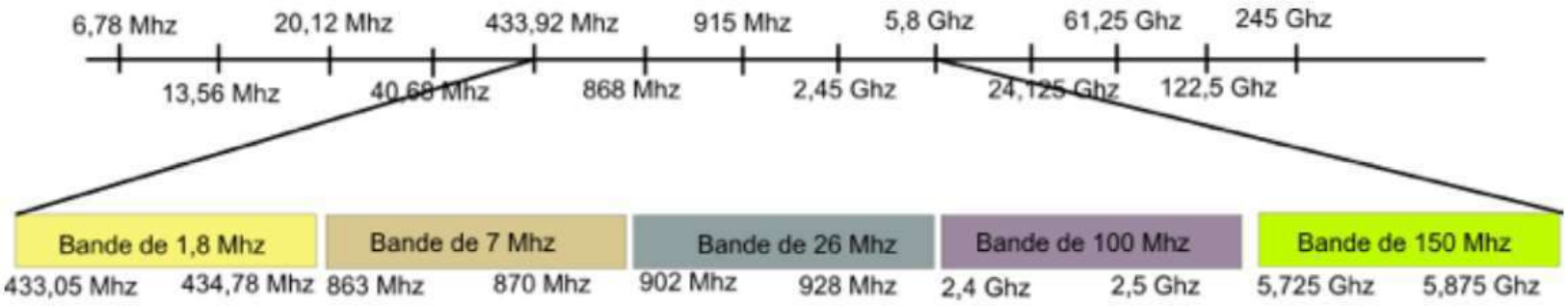
Bandes libres & bandes licenciées

- L'utilisation de l'onde radioélectrique (onde hertzienne) pour faire transiter des données dans l'espace est soumises à des régulations.
- Deux catégories : bandes libres et bandes licenciées)

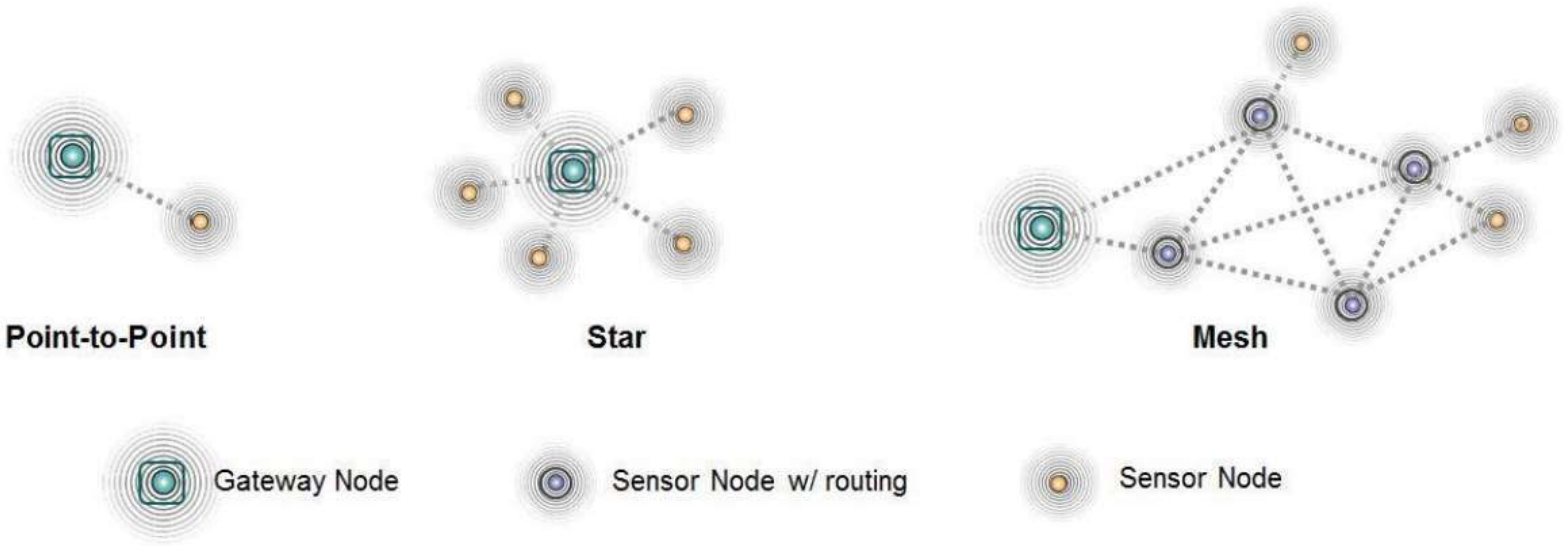
Bandes libres	Bandes licenciées
- Pas de demande d'autorisation - - Gratuité d'utilisation des fréquences - Droit collectif d'utilisation - Sans garantie de protection	- Autorisation individuelle préalable - Redevance d'utilisation des fréquences - Garantie exclusif d'utilisation - Garantie de protection

Les bandes libres ISM (Industriel, scientifique, et médical)

- Bandes de fréquences désignées par l'UIT
- Réservées pour des applications industrielles, scientifiques, médicales, domestiques, ou similaires.
- Les utilisations les plus courantes des bandes ISM: WiFi, Bluetooth, Zigbee, RFID, NFC.



Choix de la topologie



Choix de la topologie

Point à point

- Un réseau point à point établit une connexion directe entre deux nœuds de réseau : la communication ne peut avoir lieu qu'entre ces deux nœuds ou périphériques.
  - **Avantages :** simple et faible coût.
  - **Limitations :** ne permet pas le passage à l'échelle (évolutivité, scalabilité) . La portée du réseau est donc limitée à un saut

Choix de la topologie

Etoile (Star)

- Un réseau étoile se compose d'un seul concentrateur auquel tous les nœuds sont connectés.
- Ce concentrateur central agit comme un point de connexion commun à tous les autres nœuds du réseau : tous les nœuds périphériques peuvent ainsi communiquer avec tous les autres en transmettant et en recevant du concentrateur central uniquement.
  - **Avantages :** faible latence, haut débit, communications fiables.
  - **Limitations :** la portée du réseau est limitée à un seul saut.

Topologie des réseaux

Topologie Mesh

- Un noud est connecté à un ou plusieurs autres nœuds du même réseau. Cela forme un maillage dans lequel une donnée émise est relayée potentiellement par plusieurs nœuds avant d'arriver à destination, c'est ce qu'on appelle une route.
- Les nœuds peuvent établir de nouvelles routes en fonction de leurs états (par exemple en panne) et des caractéristiques du support physique (par exemple une diminution du bruit).

Topologie des réseaux

Topologie Cellulaire

- Elle repose sur un découpage d'un territoire en zones appelées cellules. Le rayon d'une cellule peut varier de quelques centaines de mètres (milieu urbain) à plusieurs kilomètres (milieu rural).
- Au cœur de la cellule, une antenne assure la liaison radio entre les objets et internet.
- Ce type de topologie est la base des réseaux mobiles (par exemple 2G/GSM, 3G/UMTS et 4G/LTE).

Topologie des réseaux

Topologie à diffusion (Broadcast)

- Dans ce type de topologie, un objet transmet un message sans préciser de destinataire en particulier. Ce qui fait que le message est analysé par tous les objets qui auront reçu correctement le message.
- Ce fonctionnement convient lorsque l'on souhaite atteindre plusieurs appareils sans distinction, c'est par exemple le cas des protocoles LoRaWAN et Sigfox.

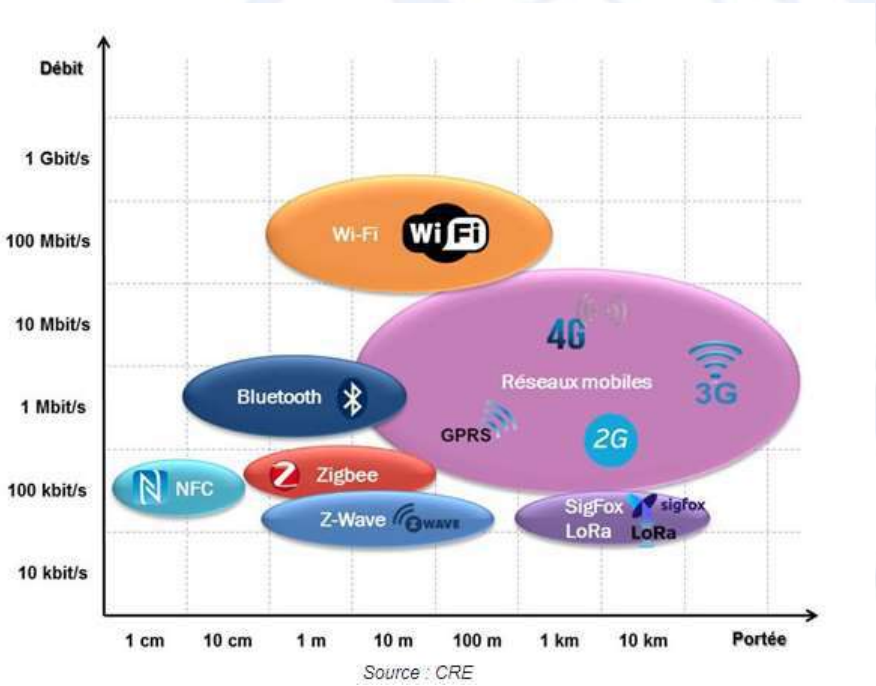
Portée des réseaux

- Il existe deux grandes catégories de réseaux qui permettent de transmettre des informations entre plusieurs objets connectés avec une consommation maîtrisée et minimale d'énergie :
  - Les réseaux à longue portée (Réseaux radio bas-débit (Sigfox, LoRa), réseaux cellulaires mobiles)
  - Les réseaux à moyenne portée (Bluetooth LE, Wifi, z-Wave)
  - Les réseaux à courte portée (RFID, NFC, Bluetooth,)

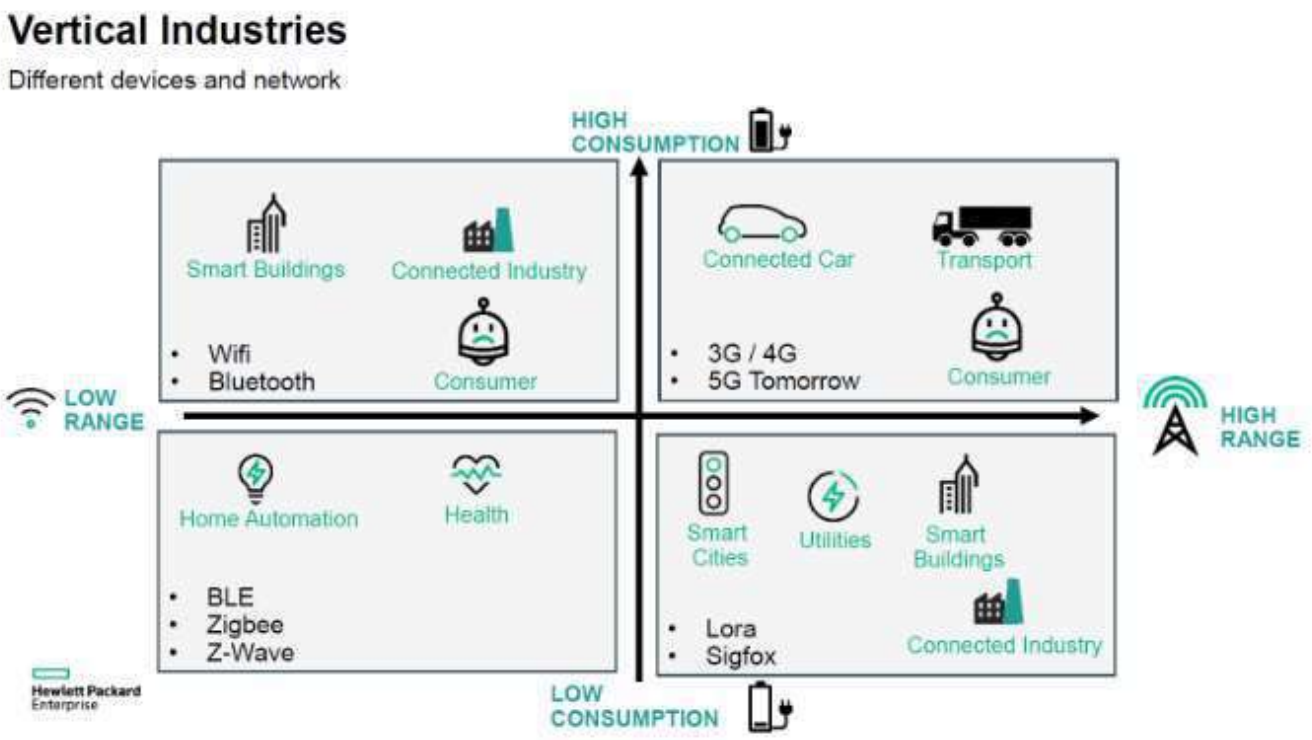
Choisir un réseau adapté à son besoin

- La diversité des technologies de radiocommunication répond à l'hétérogénéité des objets communicants :
  - pluralité des usages : domotique, maintenance prédictive, téléphonie, transfert et traitement de données, etc.
  - pluralité des publics visés : consommateurs résidentiels ou industriels, collectivités locales, etc.
  - pluralité des réglementations : bandes de fréquences d'utilisation libre ou sous licence, etc.

Portée des réseaux



Technologies de connectivité

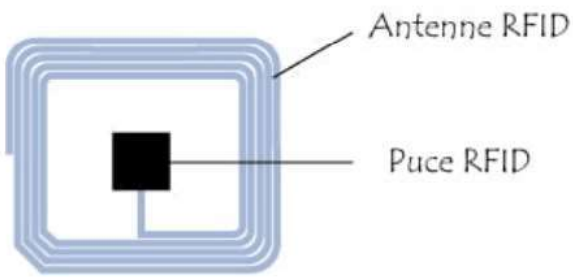


Source : **https://www.silicon.fr/hub/hpe-intel-hub/les-differentes-couches-dune-infrastructure-iot**

Partie 1: Technologies à courte portée

RFID

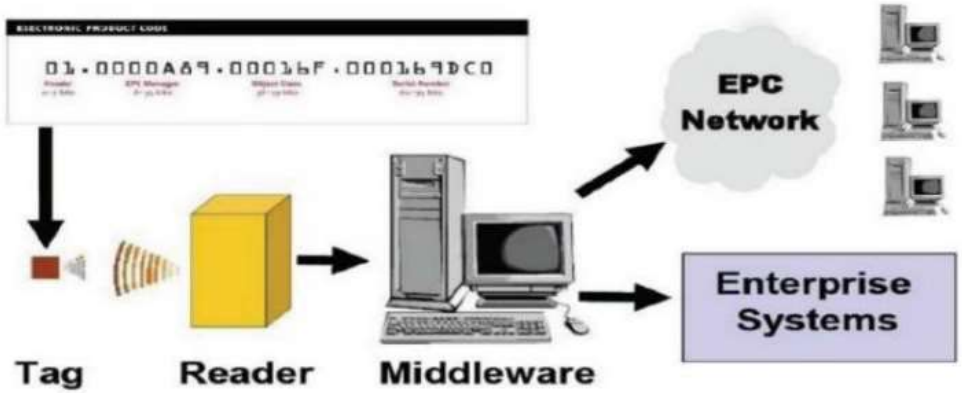
- La radio-identification ou les étiquettes (balises) RFID stockent les identifiants (UII Unique Item Identifier or EPC, Electronic Product Code) et les données et elles sont attachées aux objets.
- Exemple : les étiquettes autoadhésives, qui peuvent être collées ou incorporées dans des objets ou produits et même implantées dans des organismes vivants (animaux, corps humain).
- Les radio-étiquettes comprennent une antenne associée à une puce électronique qui leur permet de recevoir et de répondre aux requêtes radio émises depuis l'émetteur-réc
- L'étiquette RFID, qui est composée
  puce reliée à une antnne encapsulée dans u
  est lue par un lecteur qui capte puis transme
  l'information.



RFID

- On distingue deux types d'étiquette RFID :
  - **RFID passif :** alimentation RF depuis le lecteur. La durée de vie est illimitée. Et la portée 3-5m.
  - **RFID actif :** batterie interne incorporée dans la balise. la durée de vie est limité (approximativement 10 ans). Portée jusqu'à 100m. Les objets RFID sont lus par des lecteurs de carte (reader). Le lecteur passe le numéro à une application spécifique pour consulter les détails depuis une base de données.

- Technologie prometteuse pour IoT : ouverte, évolutive.
- Supporte les exigences IoT : identifiant objet, découverte service.



NFC

- NFC (Near Field Communication) est une technologie favorisant des interactions bidirectionnelles simples et sûres entre deux dispositifs électroniques (les smartphones en particulier), pour permettre aux consommateurs d'effectuer des transactions par paiement sans contact, d'accéder à des contenus numériques et de se connecter à des dispositifs électroniques.
- Norme : ISO/CEI18000-3
- Fréquence : 13,56MHz (ISM)
- Portée : 10 cm
- Vitesses de transmission : 100–420 Kbit/s

Bluetooth : 802.15.1

- Technologie basée sur la norme IEEE 802.15.1.
- La technologie Bluetooth est un acteur incontournable pour les réseaux de courte portée (WPAN). Low power, Low cost.
- Technologie évolutive : du Bluetooth classique vers le Smart Bluetooth.
- Fréquence : 2,4 GHz (ISM).
- Portée : 10 m (Téléphone mobile, écouteurs, équipement médical).
- Vitesses de transmission : 1 Mbit/s (version 1.2), 24Mbit/s (version 3.0).

https://www.ubuntupit.com/top-15-standard-iot-protocols-that-you-must-know-about/

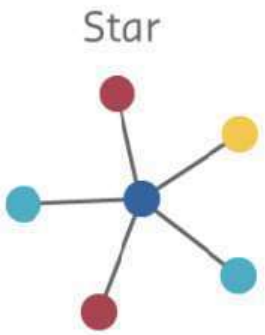
Bluetooth Low Energy (BLE) / Smart Bluetooth: 802.15.1

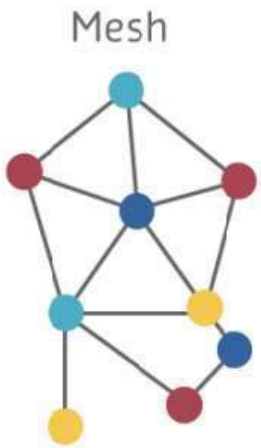
- Basée sur la norme IEEE 802.15.1
- Sous classe de la famille Bluetooth 4.0 mais issue d'une solution Nokia indépendante.
- Commercialisée sous le nom Smart Bluetooth.
- La norme BLE offre une consommation réduite d'énergie (Tx 2.9mW, Rx 2.3mW).
- Prise en charge d'IOS, Android, Windows et GNU / Linux.
- Utilisée dans les smartphones, tablettes, montres intelligentes, appareils de surveillance de la santé et de la condition physique.
- Les caractéristiques sont les suivantes :
  - **Portée : 50-150m (extérieur)** avec des temps de latence 15 fois plus courts que Bluetooth.
  - **Vitesses de transmission : 1 Mbit/s**
  - **Utilisation :** applications envoyant un volume réduit de données.
- BLE n'est pas compatible avec Bluetooth.

Bluetooth Low Energy (BLE) / Smart Bluetooth: 802.15.1

- La technologie Bluetooth a deux topologies : étoile et maillée.
  - **Topologie étoile (réseau piconet):** Consiste d'un nœud maitre (master) et des nœuds esclaves (slaves) sur un rayon de 10m. Les esclaves ne pe
  - **Topologie mesh (réseau sactterr**

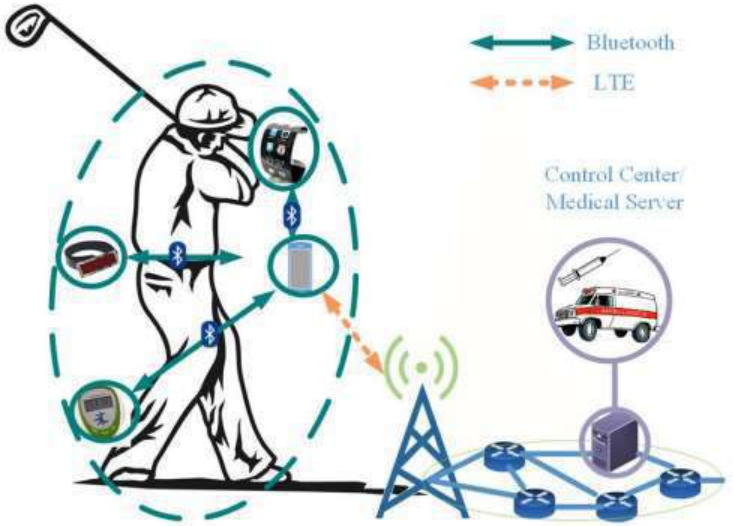
  Consiste en des interconnexions de
  Ces réseaux sont formés par des rés
  piconets reliés ensembles (les esclav
  peuvent avoir plusieurs maitres).





Bluetooth Low Energy (BLE) / Smart Bluetooth: 802.15.1

- Objets prêt-à-porter (shoes, glasses, belt, etc.) peuvent être utilisés pour détecter les information biométriqu
- Les objets communique centre de communicati un serveur médical.

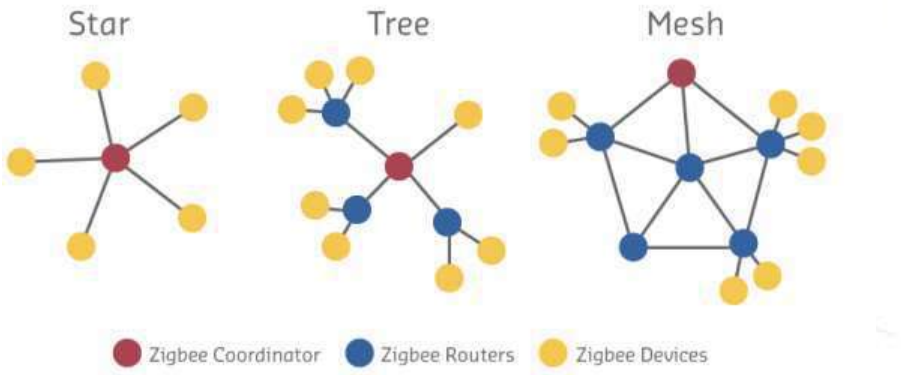


ZigBee

- Crée par Zigbee Alliance et est basée sur la norme IEEE 802.15.4.
- ZigBee est un protocole non IP cible les applications nécessitant des échanges de données relativement peu fréquents à de faibles vitesses de transmission sur un espace restreint et dans une portée de 100 m (résidence ou bâtiment, par exemple).
- Les caractéristiques sont les suivantes :
  - Fréquence : (2,4 GHz, 250 kbps), (868 MHz, 20 kbps), (915 GHz, 40 kbps) (ISM).
  - Portée : 10-100 m.
  - Vitesses de transmission : 250 Kbit/s (low data rates).

ZigBee

- Trois topologies sont possibles : étoile, maillée, cluster tree.
- Les objets connectés avec Zigbee prennent trois rôles : Coordinateur, routeur, client. Le coordinateur est responsable de la gestion des clients, la formation et la maintenance du réseau.
- Chaque coordinateur peut se connecter à 8 objets (clients & routeurs). Les routeurs jouent le rôle d'un pont de données entre le client et le coordinateur.



Z-Wave

- Z-Wave est une technologie télécoms RF à faible consommation, principalement conçue pour la domotique et les produits tels que les contrôleurs de lampe ou les capteurs.
- Les caractéristiques sont les suivantes :
  - **Norme:** Z-Wave Alliance ZAD12837/ITU-T G.9959.
  - **Fréquence :** 900MHz (ISM).
  - **Portée :** 30 m.
  - **Débit :** 9,6 / 40 / 100 Kbit/s.
  - **Topologie :** Mesh.

Partie 2: Spectre et technologies mobiles

Partie 3: Spectre et technologies des satellites

Partie 4: Spectre et technologies 3GPP

Standards LPWAN Cellulaires 3GPP

Standards IoT Cellulaires 3GPP

- Deux solutions LPWA (Low Power Wide Area) normalisées par le 3GPP sous forme de profils additionnels aux profils 4G LTE : LTE-M (LTE for Machine Type Communication) et NB-IoT (Narrowband IoT).
- **LTE-M (ou e-MTC)** : extension logicielle de la 4G LTE, dédiée au trafic M2M. LTE-M peut offrir un débit allant à 1Mbps.
- NB-IoT : intégrée dans la 4G LTE et utilisant une interface radio distincte. NB-IoT offre un débit, adaptée aux applications IoT, de quelques dizaines de Kbps.
- LTE-M et NB-IoT ont été développés avec les objectifs suivants :
  - Couverture intérieure améliorée
  - Coût du device ultra-faible
  - Faible consommation d'énergie du device
  - Architecture réseau optimisée
- Les technologies LTE-M et NB-IoT sont appelées CIoT (Cellular IoT) pour les distinguer des autres solutions LPWA.

NB-IoT

- NB-IoT pour Narrow Band IoT, Release 13 de 3GPP (Rel-13, Juin 2016). Prend en charge l'Internet des Objets (Cellular IoT: CIoT) à très faible complexité et à faible débit.
- Basée sur la spécification de la norme LTE : reprise de quelques fonctions LTE existantes avec suppression d'autres telles que : surveillance canal, transfert intercellulaire, etc. et ce pour optimiser la consommation de l'énergie et pour un coût minimal.
- Coexiste avec GSM et LTE sous les fréquences sous licence : 700 MHZ, 800 MHz, 900 MHz.
- Portée : NB-IoT permet d'atteindre des portées de 15 Km.
- Débit : débit limité à 200 kbps (downlink) et 20 kbps (uplink).
- Durée de vie batterie : 10 ans (200 octets par jour).

eMTC

- **eMTC (ou LTE-M)** qui est une extension logicielle de 4G LTE. Il requiert un canal de 1,4 MHz (à l'intérieur d'un canal LTE de 20 MHz) et permet des débits de 1 Mbit/s. C'est une solution adaptée au trafic M2M.
- **NB-IoT** qui est intégrée dans LTE mais utilise une interface radio spécifique. Le profil vient en compétition avec LoRa. Il requiert un canal de 200 kHz et permet des débits de quelques dizaines de kbit/s.

Partie 5: Protocoles IoT

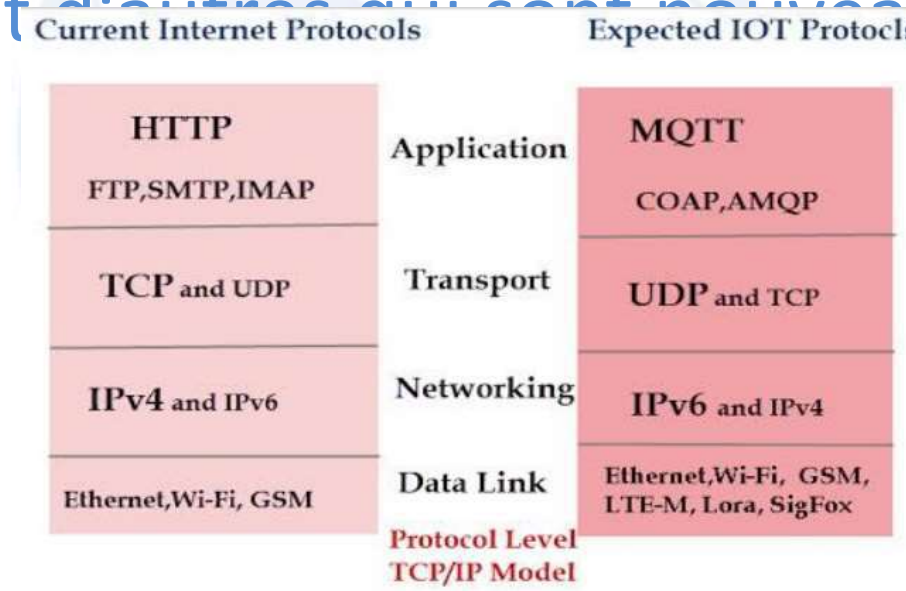
Protocoles IoT

- **Infrastructure** (ex: 6LowPAN, IPv4/IPv6, RPL)
- **Identification** (ex: EPC, uCode, IPv6, URIs)
- **Comms / Transport** (ex: Wifi, Bluetooth, LPWAN)
- **Discovery** (ex: mDNS, DNS-SD)
- **Data Protocols** (ex: MQTT, CoAP, AMQP, Websocket)
- **Device Management** (ex: TR-069, OMA-DM)
- **Semantic** (ex: JSON-LD, Web Thing Model)

https://www.postscapes.com/internet-of-things-protocols/

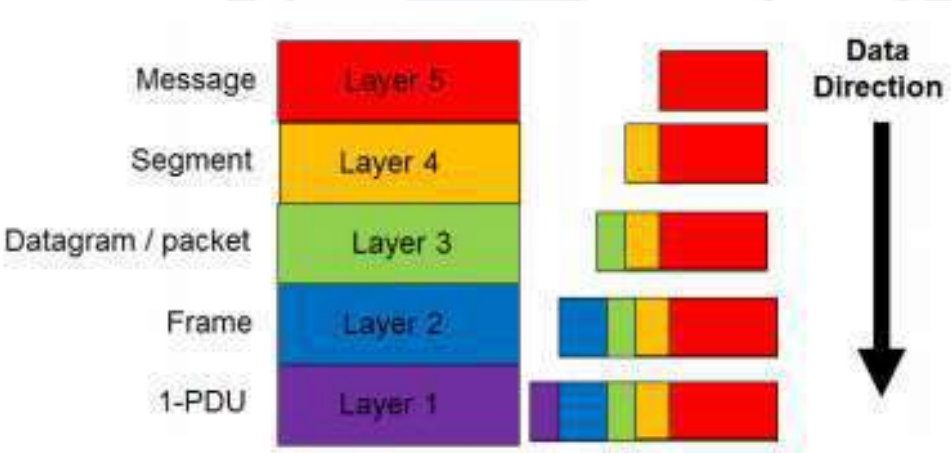
Modèle OSI Vs. Modèle TCP/IP

- L'IoT utilise des protocoles Internet existants et introduit d'autres qui sont nouveaux.

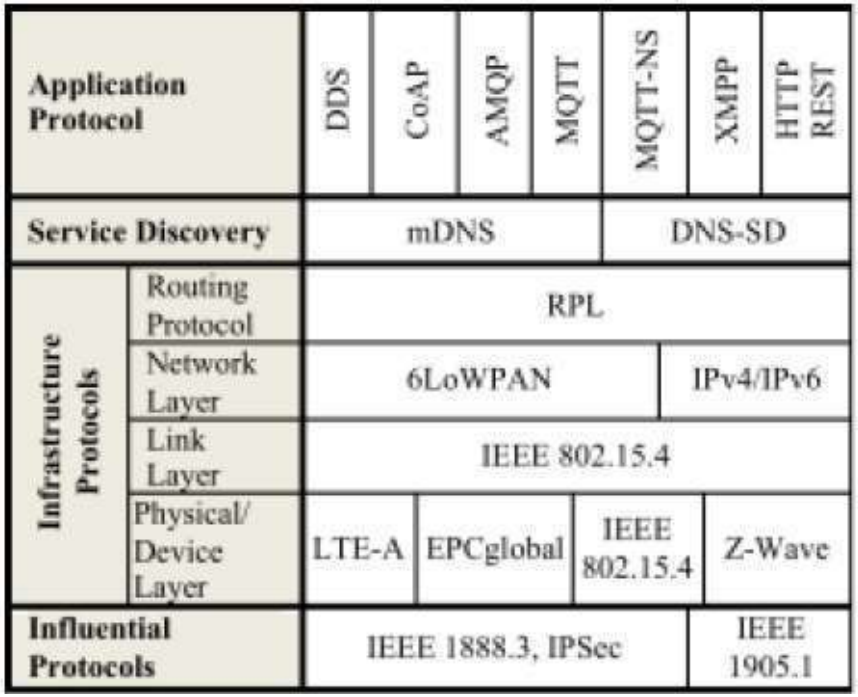


Encapsulation

- Flux de données dans la pile de protocoles



Pile de protocoles IoT



Protocoles de la couche application

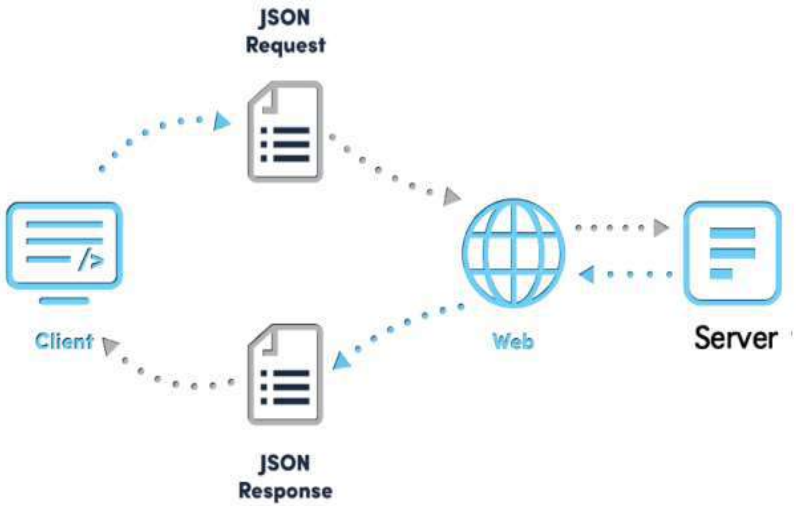
- Une application IoT permet aux objets connectés d'envoyer leurs données à un serveur Web Internet ou une plateforme Cloud.
- Les protocoles de la couche application permettent de transmettre des commandes depuis les applications utilisateurs aux actionneurs des objets connectés.
- L'infrastructure Web classique n'est pas adaptée à la majorité des applications IoT qui sont dotées d'équipements de faibles ressources : petits microcontrôleurs, petites quantités de mémoire RAM, énergie limitée, etc.
- Les protocoles applicatifs qui utilisent un nombre limité de messages de petites tailles sont utilisés pour les applications IoT, et sont classés en 4 familles:
  - Protocole de transfert web: Web REST, COAP
  - Protocole de messagerie: MQTT, XMPP et AMQ.
  - Protocole réseau: Websocket

Services Web REST

- REST (Representational State Transfer) n‘est pas un protocole mais plutôt un style d‘architecture Web client-serveur qui permettant de gérer, identifier et manipuler des ressources.
- Les capteurs, les actionneurs et les systèmes de commande en général peuvent être représentés comme des ressources et peuvent ainsi exposer leurs services via un service Web RESTful.
- Web REST est une interface de programmation d‘application qui utilise des requêtes HTTP avec les méthodes {GET, PUT, POST, DELETE} pour demander un service Web.
- L‘importance de REST découle de la simplicité de la communication et du fait qu‘il est complet : on peut réaliser n‘importe quel service Web avec l‘architecture REST.
- En plus REST est supporté par toutes les plateformes M2M Cloud.

Services Web REST (Representational State Transfert)

- Chaque ressource est définie par un unique URI (Uniform Resource Identifier).
- REST utilise plusieurs formats pour représenter les ressources : Text, JSON, XML. JSON est le format le plus utilisé.
- L'importance du REST découle de la simplicité de la communication et du fait qu'il est supporté par toutes les plateformes M2M Cloud.

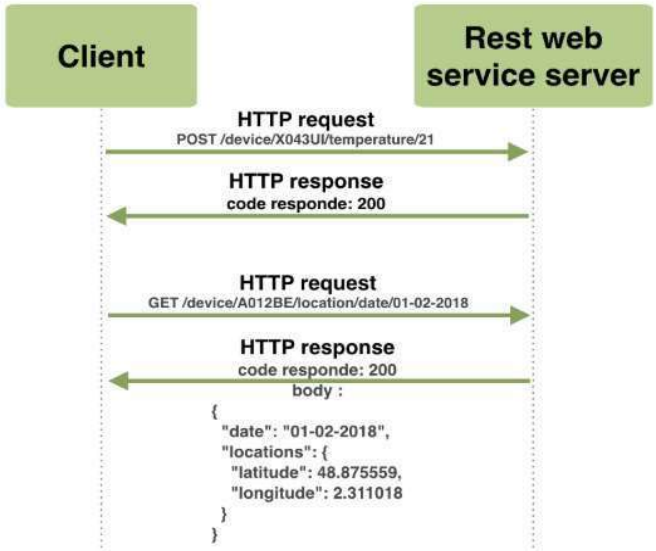


Source: Pietro Manzoni. Intro to MQTT. Workshop on Rapid Prototyping of IoT for Science (smr3268) – January 2019

Services Web REST

URI	Méthode	Signification
/device/:device/temperature/:temperature	POST	Effectuer un POST en spécifiant, pour l'objet `:device`, une nouvelle valeur de température `:temperature` en °C
/device/:device/location/date/:date	GET	Effectuer un GET pour obtenir la position GPS d'un objet `:device` à une date donnée `:date`

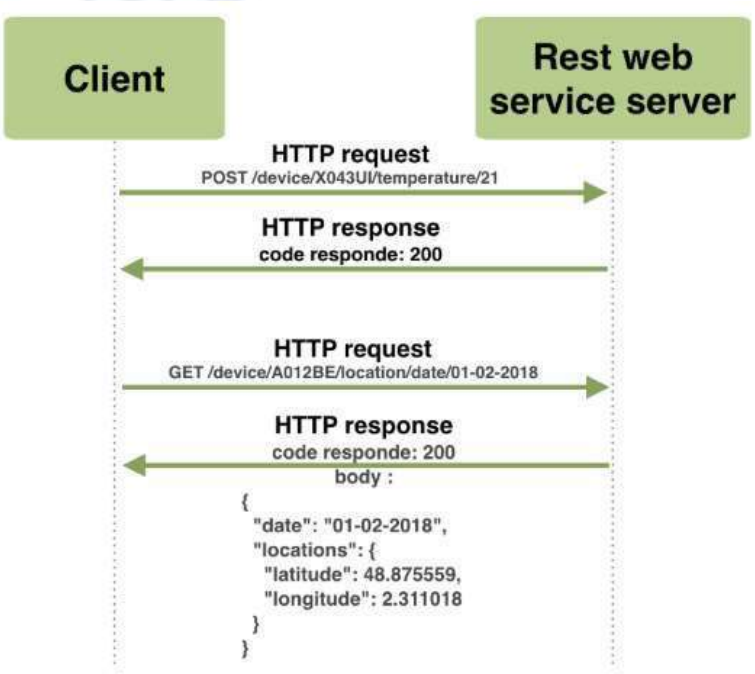
- Le client envoie une requête POST pour indiquer au serveur une nouvelle température de 21°C, pour l'objet X043UI.
- Le serveur lui répond avec un code de 200 pour indiquer que tout est OK.
- Le client envoie une requête GET pour demander la localisation de l'objet A012BE à la date du 01-02- 2018.
- Le serveur répond en envoyant les coordonnées.



Source: https://blog.engineering.publicissapient.fr/2018/04/16/internet-des-objets-quels-protocoles-applicatifs-utiliser-1-2/

Services Web REST (Representational State Transfert)

- Le serveur ajoute également un code réponse HTTP, à trois chiffres, afin d'indiquer l'état de la réponse dont la forme est comme suit :
  - 2xx indique le succès du traitement de la requête du client (exemple : 200 pour OK)
  - 3xx redirige le client vers un autre lien
  - 4xx indique une faute dans la requête du client (exemple : 404 pour Not Found)
  - 5xx indique une erreur de la part du serveur (exemple : 500 pour Internal Server Error)

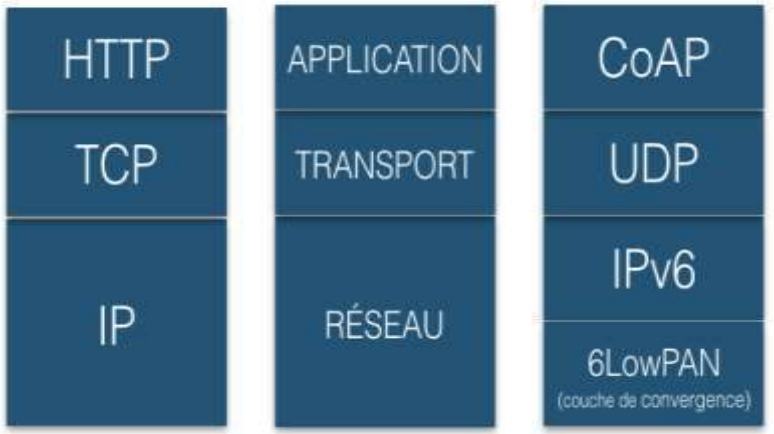


Source: https://blog.engineering.publicissapient.fr/2018/04/16/internet-des-objets-quels-protocoles-applicatifs-utiliser-1-2/

CoAP (Constrained Application Protocol)

- CoAP (Constrained Application Protocol) est un protocole web basé sur une architecture client/serveur.
- CoAP est une version légère de REST conçu pour des communications UDP.
- CoAP est destiné à l'utilisation sur des appareils électroniques à faible consommation d'énergie : —use with constrained nodes and constrained (e.g., low-power, lossy) networks.‖
- IETF CoAP utilise les URI pour identifier les ressources.
- HTTP est basé sur la suite TCP/IP alors que CoAP se base sur UDP/IPv6/6LoWPAN.

Suites TCP/IP et UDP/IPv6/6LowPAN



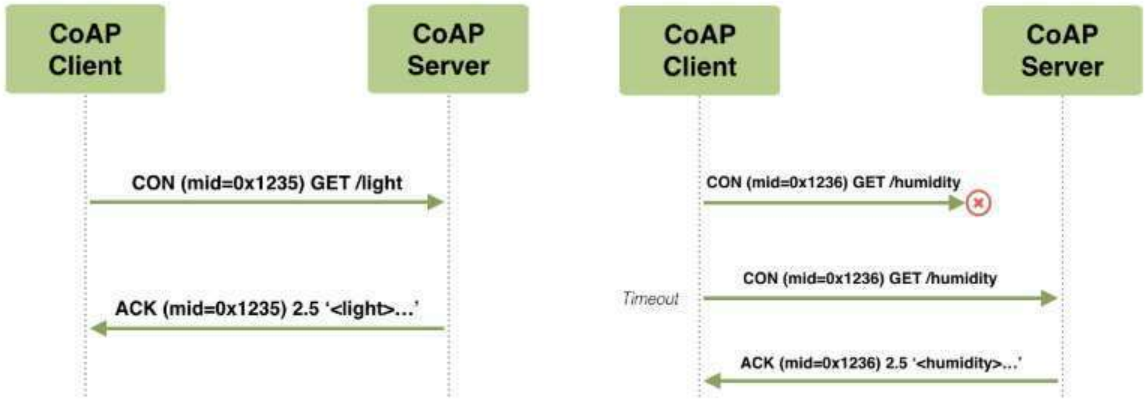
Source: http://www.efort.com/r_tutoriels/COAP_EFORT.pdf

CoAP (Constrained Application Protocol)

- Les requêtes CoAP sont équivalentes à celles de HTTP : un client envoie une requête à un serveur pour demander un service d'une ressource, identifiée par URI.
- CoAP utilise les méthodes HTTP {GET, PUT, POST, DELETE}.
- Les messages CoAP ont une taille (4 octets) allégée par rapport à celle des messages HTTP (variable).
- CoAP utilise quatre types de messages :
  - Confirmable (CON) : Message envoyé avec une demande d'accusé de réception.
  - Non-Confirmable (NON) : Message envoyé sans demande d'accusé de réception.
  - Acknowledgment (ACK) : Accusé de réception du message de type CON.
  - Reset (RST) : Accusé de réception d'un message qui n'est pas exploitable.

CoAP (Constrained Application Protocol)

- Si la requête est du type CON alors le serveur retourne une réponse dans laquelle se trouve ; le type du message (ACK), le même mid que celui de la requête et un code réponse (2.xx, 4.xx ou 5.xx) et une représentation de la ressource.



Source: https://blog.engineering.publicissapient.fr/2018/04/16/internet-des-objets-quels-protocoles-applicatifs-utiliser-1-2/

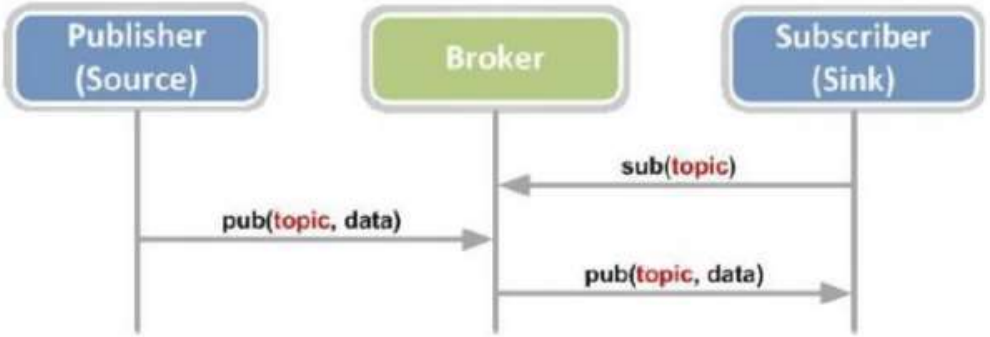
CoAP

- Le client (objet) envoie une requête CoAP, sur une ressource identifiée par une URI, au serveur en spécifiant : le type de message (CON, NON), l'identifiant du message (mid) et une action (POST, GET, PUT, DELETE).
- La signification du code réponse est la suivante :
  - 2.xx signifie que la requête a été correctement reçue et traitée
  - 4.xx signifie que une erreur a été rencontrée par le client
  - 5.xx signifie que le serveur n'est pas capable de traiter la requête

MQTT

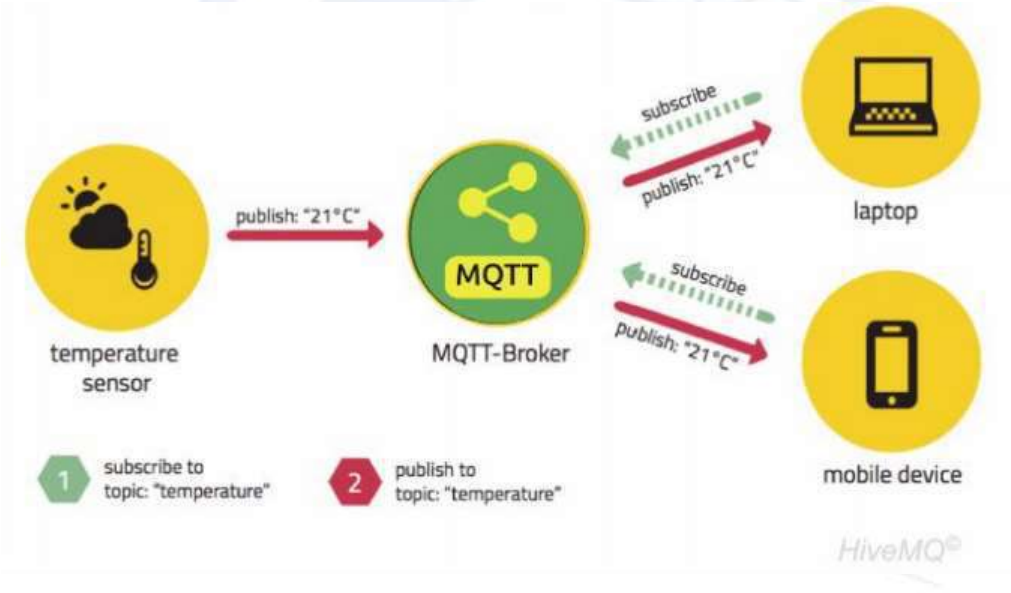
- MQTT (Message Qeuning Telemetry Transport) est un protocole de messagerie de publication et d'abonnement (publish/subscribe) basé sur le protocole TCP/IP.
- L'approche publish/subscribe classifie les messages par catégories (topics) auxquelles les destinataires s'abonnent (subscribe).
- Le client qui envoie un message (topic) est nommé publisher, celui qui reçoit le message est nommé subscriber.

- Un élément du réseau appelé broker, connu par le publisher et le subscriber, filtre les messages reçus et les distribue.

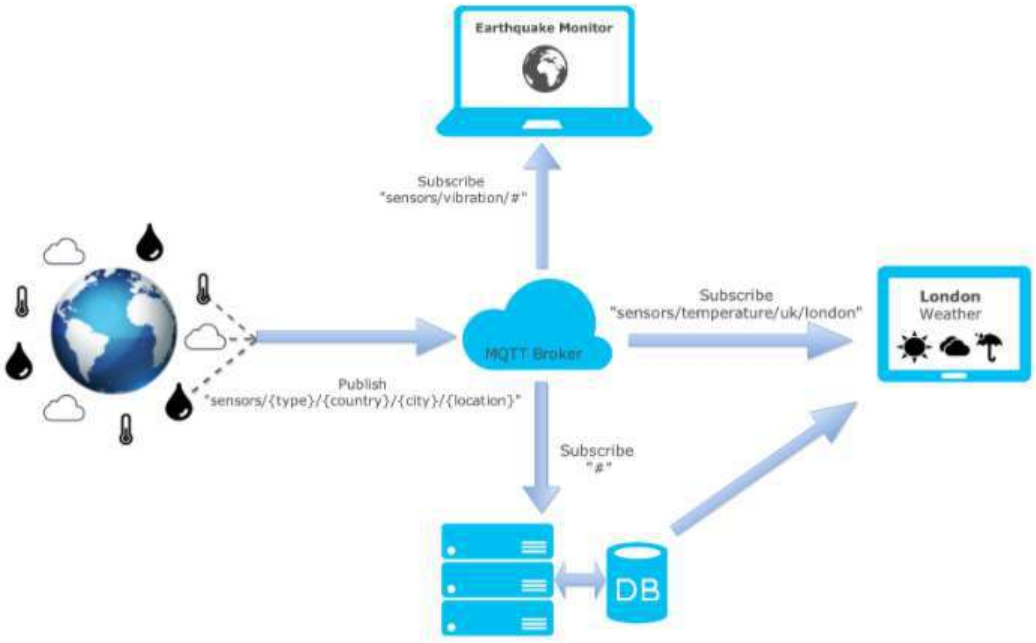


Source : Antonio Linan Colina et al. Internet of Things in 5 days-v1.1 2016

MQTT


publish: "21°C"
MQTT
temperature sensor
MQTT-Broker
subscribe
publish: "21°C"
laptop
subscribe
publish: "21°C"
mobile device
1
subscribe to topic: "temperature"
2
publish to topic: "temperature"
HiveMQ

MQTT



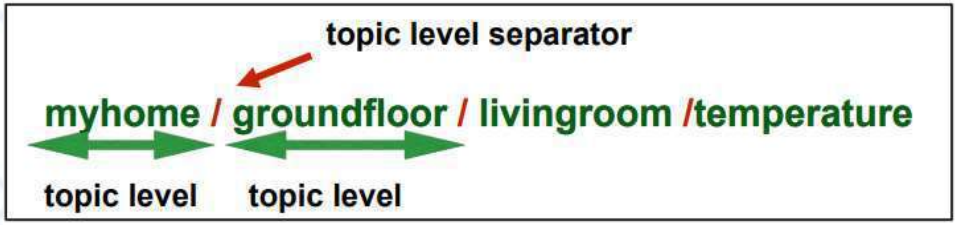
Source: https://zoetrope.io/tech-blog/brief-practical-introduction-mqtt-protocol-and-its-application-iot/

MQTT

- MQTT est caractérisé par :
  - faible consommation d'énergie
  - Entêtes compressées MQTT topics sont structurées d'une façon hiérarchique.
  - Les topics sont sensibles à la casse, codées en UTF-8 et doivent comporter au moins un caractère.
  - Les topics peuvent être génériques : possibilité de faire des souscriptions à des topics qui ne sont pas encore définies.

- « + » : correspond à tout à un niveau donné

- « # » : correspond à toute l'arborescence



MQTT

- Exemple:
  - La souscription à la topic house# couvre :
    - house/room1/main-light
    - house/room1/alarm
    - house/garage/main-light
    - house/main-door
  - La souscription à la topic house/+/main-light couvre :
    - house/room1/main-light
    - house/room2/main-light
    - house/garage/main-light

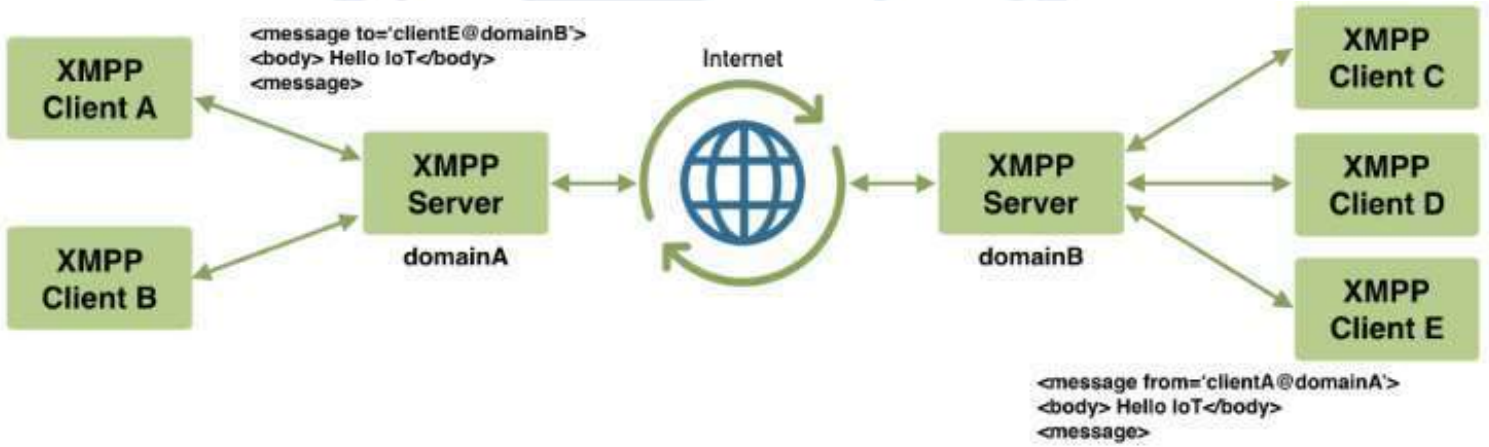
MQTT

- Les caractéristiques du protocole MQTT en font un protocole adapté aux réseaux IoT car il répond aux besoins suivants :
  - Adapté aux réseaux à faible bande passante
  - Idéal pour l'utilisation sur les réseaux sans fils grâce notamment à un nombre limité de messages de petite taille
  - Faible consommation en énergie car la publication et la consommation des messages est rapide
  - Nécessite peu de ressources de calculs et de mémoires
  - Transmet un message à plusieurs entités en une seule connexion TCP

XMPP

- XMPP (Extensible Messaging and Presence Protocol), est à l'origine un protocole de messagerie instantanée utilisé notamment dans les services Jabber et Google Talk.
- Grâce à son extensibilité, il est utilisé dans d'autres applications telle que la VoIP.
- Son fonctionnement est basé sur une architecture client/serveur où l'échange de données, au format XML.
- La communication entre deux clients est asynchrone et est réalisée au travers de serveurs XMPP.

Fonctionnement du protocole XMPP



XMPP

- Les principaux atouts de ce protocole sont son adressage avec identifiant unique, sa facilité de mise en place de la sécurité, son format de messages qui fournit des données structurées et son système de serveurs.
- Le protocole XMPP est plus adapté à l'IoT, contrairement au protocole MQTT (adaptés aux applications M2M):
  - il gère mieux l'intégration de nouveaux objets connectés, et
  - Il permet interopérabilité avec d'autres plateformes IoT et donc d'autres écosystèmes IoT.

AMQP

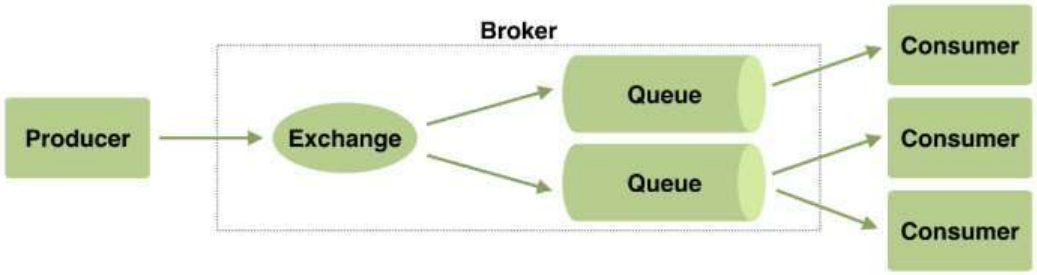
- Le fonctionnement du protocole AMQP est basé sur le même principe que celui de MQTT, toutefois la notion de *publisher*/*subsciber* est remplacée par celle de *producer*/*consumer*.
- En outre, grâce à un mécanisme interne noté « exchange », AMQP permet de router un message d'un producer vers plusieurs topics. Les critères de routage peuvent se faire de plusieurs façons ; inspection du contenu, de l'en-tête, clés de routage, etc. Ainsi, un même message peut être consommé par différents consumers via plusieurs topics.
- Par conséquent, AMQP est plus adapté aux situations exigeant la fiabilité, des scénarios de messageries plus sophistiqués, l'interopérabilité entre implémentations du protocole et la sécurité. Ainsi, il est plus destiné aux objets connectés avec des contraintes de communication faibles et des exigences de sécurités importantes.

AMQP

- Le fonctionnement du protocole AMQP est basé sur le même principe que celui de MQTT, toutefois la notion de *publisher/subsciber* est remplacée par celle de *producer/consumer*. En outre, grâce à un mécanisme interne noté « exchange », AMQP permet de router un message d'un producer vers plusieurs topics. Les critères de routage peuvent se faire de plusieurs façons ; inspection du contenu, de l'en-tête, clés de routage, etc. Ainsi, un même message peut être consommé par différents consumers via plusieurs topics.

AMQP

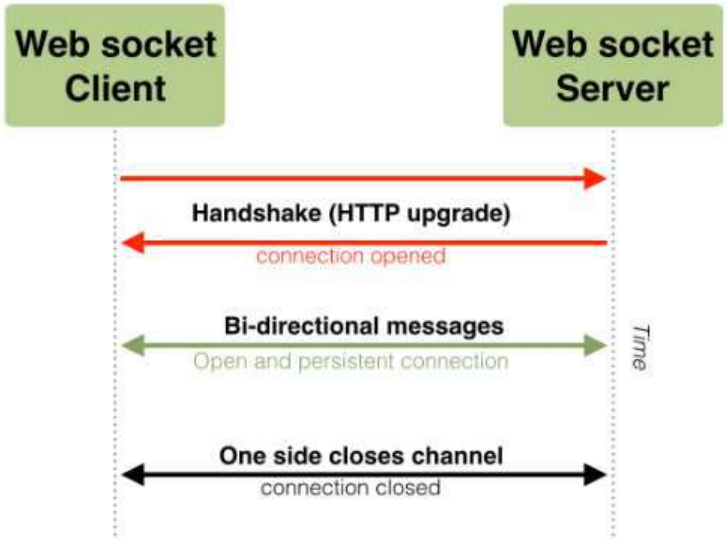
- Par conséquent, AMQP est plus adapté aux situations exigeant la fiabilité, des scénarios de messageries plus sophistiqués, l'interopérabilité entre implémentations du protoc[illegible]us destiné[illegible] contrai[illegible] et des exigences de sécurités importantes.



Fonctionnement du protocole AMQP

Protocole réseau (Websocket)

- Le protocole Websocket permet l'établissement d'un canal de communication full-duplex en une seule connexion TCP entre un client et un serveur.
- Les trois principales phases de la vie du canal :
  - la phase de connexion appelé «Handshake» initié par le client
  - la phase d'échange bidirectionnel de messages
  - la phase de clôture du canal initié par l'une des deux parties



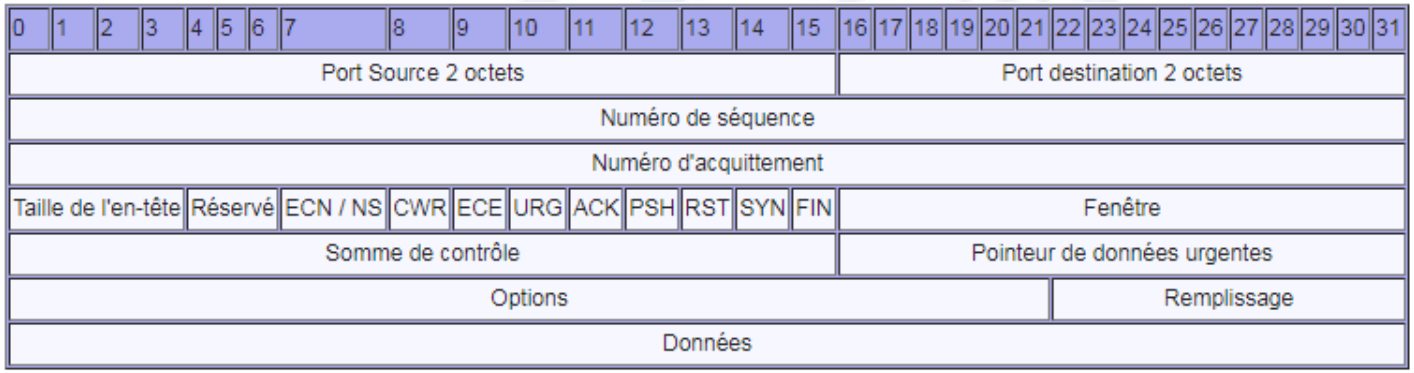
Protocole de transport TCP

- La couche Transport permet la communication et protège les données lorsqu'elles circulent entre les couches.
- Le protocole TCP (Transmission Control Protocol) est utilisé pour la majorité des connexions Internet.
- Il offre une communication d'hôte à hôte, en divisant de grands ensembles de données en paquets individuels, et en renvoyant et réassemblant les paquets en fonction des besoins.
- TCP n’est pas une bonne option pour la communication dans des environnements à faible consommation d’énergie car il a une surcharge importante en raison du fait qu’il s’agit d’un protocole orienté connexion.

Protocole de transport TCP

- Dans le modèle OSI, il correspond à la couche transport, intermédiaire de la couche réseau et de la couche session.
- L'établissement de la connexion se fait par un **handshaking en trois temps :**
  - l'établissement de la connexion ;
  - les transferts de données ;
  - la fin de la connexion.
- La rupture de connexion utilise un **handshaking** en quatre temps.

Structure d’un segment TCP



- **Port source :** numéro du port source
- **Port destination** : numéro du port destination
- **Numéro de séquence :** numéro de séquence du premier octet de ce segment
- **Numéro d'acquittement** : numéro de séquence du prochain octet attendu
- **Taille de l'en-tête :** longueur de l'en-tête en mots de 32 bits (les options font partie de l'en-tête)
- **Indicateurs ou *Flags***
- **Fenêtre** : taille de fenêtre demandée, c'est-à-dire le nombre d'octets que le récepteur souhaite recevoir sans accusé de réception
- **Somme de contrôle** : somme de contrôle calculée sur l'ensemble de l'en-tête TCP et des données, mais aussi sur un pseudo en-tête (extrait de l'en-tête IP)
- **Pointeur de données urgentes :** position relative des dernières données urgentes
- **Options :** facultatives
- **Remplissage :** zéros ajoutés pour aligner les champs suivants du paquet sur 32 bits, si nécessaire
- Données : séquences d'octets transmis par l'application

Protocole de transport UDP

- Le protocole User Datagram Protocol (UDP, en français protocole de datagramme utilisateur) est un des principaux protocoles de transport utilisés par Internet.
- Le protocole UDP assure la transmission de données transmission en mode non connectés. Il est donc non fiable (pas de garantie de protection quant à la livraison, l'ordre d'arrivée, ou la duplication éventuelle des datagrammes).
- Le protocole UDP est utile pour les applications en temps réel telles que la voix sur IP, les jeux en ligne, et de nombreux protocoles construits sur base du Real Time Streaming Protocol.

Structure d’un diagramme UDP

- L’entête UDP contient les champs suivants:
  - **Port source:** indique quel port a été envoyé
  - **Port destination :** indique à quel port le datagramme doit être envoyé
  - **Longueur:** indique la longueur totale (exprimée en octet) du segment UDP (entête et données). La longueur minimale est donc 8 octet (taille de l’entête)
  - **Source de contrôle:** celle-ci permet de s'assurer de l'intégrité du paquet reçu quand elle est différente de zéro. Elle est calculée sur l'ensemble de l'en-tête UDP et des données, mais aussi sur un pseudo en-tête (extrait de l'en-tête IP)

Port Source (16 bits)	Port Destination (16 bits)
Longueur (16 bits)	Somme de contrôle (16 bits)
Données (longueur variable)	

Protocole réseau IPv6

- La couche Réseau permet à des appareils individuels de communiquer avec le routeur.
- Le protocole IPv6 a été développé dans les années 1990 afin de succéder à l'IPv4 dont les capacités d'adressage sont aujourd'hui insuffisantes.
- IPv6 est devenu un standard officiel de l'IETF en 1998.
- La caractéristique principale de l'IPv6 est d'utiliser un format d'adresses sur 128 bits au lieu de 32 bits dans l'IPv4.

Adresses IPv6 Possible!

Le format générale d'une adresse IP

X:X:X:X:X:X:X:X/n

- X = 4 positions hexadécimales: X = hhhh oú h = [0 – 9, a – f]
- n = longueur de préfixe en décimale

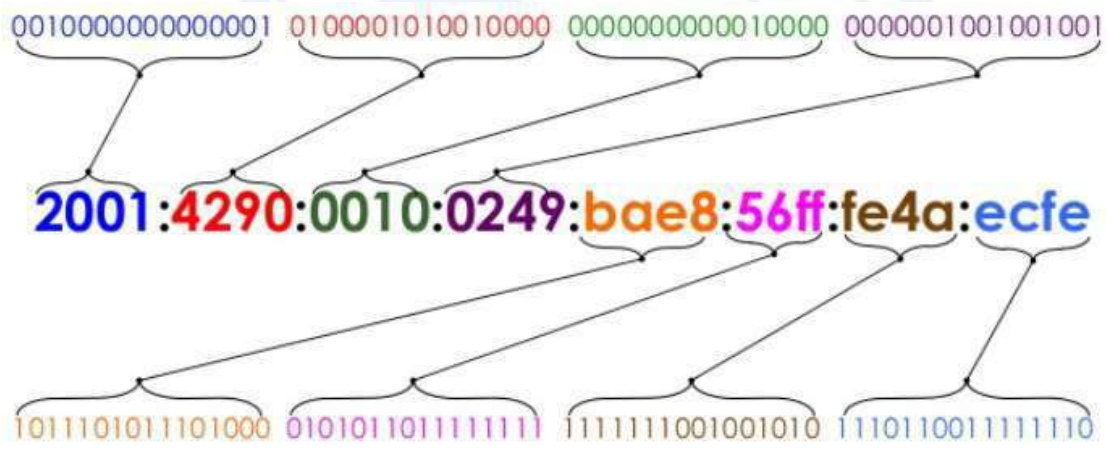
hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh/n

Comment écrire les adresses IP?

0010000000000001 0100001010010000
0000000000010000 0000001001001001
1011101011101000 0101011011111111
1111111001001010 1110110011111110

128 bits

Comment écrire les adresses IP?



6LoWPAN

Standard IETF – RFC 4944 : 6LoWPAN (2007)

- 6LoWPAN (IPv6 Low Power Wireless Personal Area Network) est une combinaison de deux protocoles : Internet Protocol version (IPv6) et Low-Power Wireless Personal Network (LoWPAN).
- 6LoWPAN a été conçu pour permettre à IPv6 d'intégrer les appareils contraints et les réseaux 802.15.4 qui les interconnectent
- Les paquets IPv6 ont des en-têtes de taille fixe à 40 octet : taille inconvenable pour les réseaux IEEE 802.15.4. 6LoWPAN permet a des objets 802.15.4 de communiquer sur les réseaux IPv6 de sorte que la connexion de bout en bout est adressable et qu'un routeur peut être utilisé pour le routage des tâches.

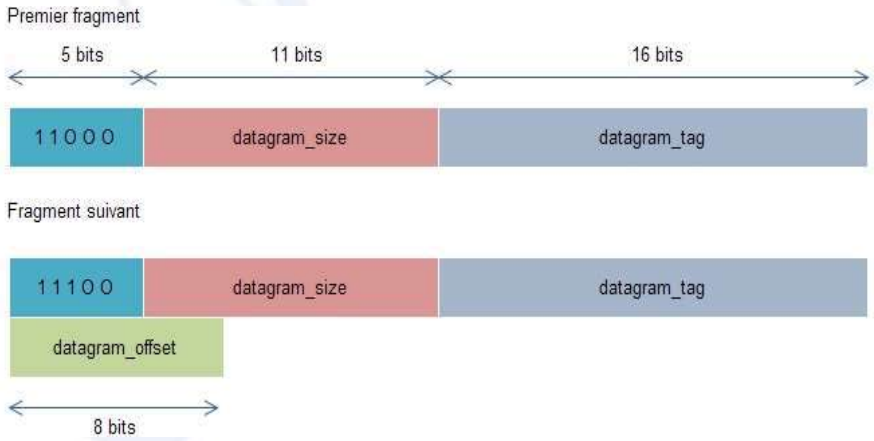
6LoWPAN

- 6LoWPAN est une couche d'adaptation qui réside entre la couche liaison de données et la couche réseau et réalise les fonctions suivantes :
  - **Fragmentation et rassemblements** des paquets.
  - **Compression des en-têtes**.
  - **Routage** (connexions multi-sauts).
- Le standard 6LowPan ne prévoit pas de fonctions de sécurité en plus de celles potentiellement mises en œuvre au niveau du 802.15.4 et de IP V6

6LoWPAN

Fragmentation et réassemblage

- La couche adaptation 6LoWPAN doit fragmenter les paquets IPv6 avant de les envoyer et les réassembler à la réception.
- Chaque fragment est précédé d'un en-tête de de **4 ou 5 octets** qui contient :
  - **5 bits :** permet d'identifier qu'il s'agit d'un fragment.
  - **8 bits :** position du fragment dans le paquet IP (uniquement présent dans les fragments suivant le premier).
  - **11 bits :** taille du paquet IP avant fragmentation ;
  - **16 bits :** identifiant commun à tous les fragments d'un même paquet IP ;

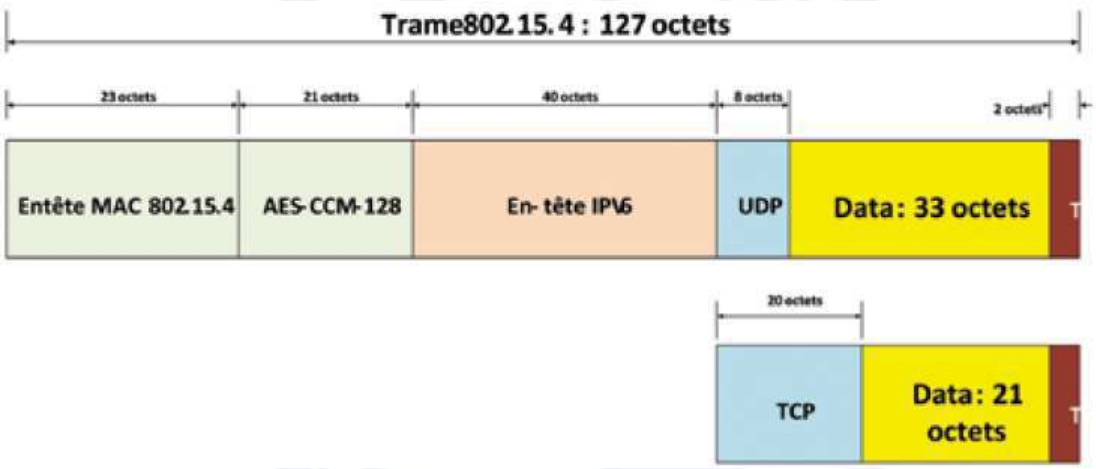


6LoWPAN

Routage

- La spécification RFC 49443 définit le mécanisme de compression des en-têtes IPv6 pour les réseaux LowPAN.
- L'utilisation de l'algorithme de compression LOWPAN_IPHC est recommandée par le groupe 6LoWPAN.
- L'en-tête IPv6s octets IPHC, résultante de la compression, intègre les informations :
  - de qualité de service,
  - des prochains en-têtes,
  - le nombre de sauts, et
  - les adresses source/destination compressées.

6LoWPAN


Trame802.15.4 : 127 octets
23 octets
21 octets
40 octets
8 octets
2 octets*
Entête MAC 802.15.4
AES-CCM-128
En-tête IPV6
UDP
Data : 33 octets
20 octets
TCP
Data : 21 octets

Protocole de routage RPL

- Un des enjeux de l'IoT est le routage des paquets IP. Les objets ont des ressources électriques limitées et sont souvent connectés par des liens radio de qualité médiocre.
- Les protocoles de routage traditionnels ne sont pas très adaptés à cette situation.
- Le groupe de travail ROLL de l'IETF a produit un protocole «officiel», RPL (Routing Protocol for LLNs (où un LLN est un Low power and Lossy Network), un réseau où mêmes les routeurs ont peu de courant et où pas mal de paquets se perdent en route).

Protocole de routage RPL

- RPL est un protocole de routage (routing), c'est-à-dire de construction de routes. Il utilise l'algorithme Trickle (basé sur la théorie des graphes pour distribuer l'information sur les routes et les routeurs.
- Pour optimiser les routes, RPL est paramétré avec une fonction nommée OF (pour Objective Function).
- Des réseaux différents peuvent utiliser des OF différents (une qui cherche le chemin le plus court, une qui cherche à ne pas utiliser comme routeur les machines n'ayant pas de connexion au courant électrique, etc), même s'ils utilisent tous RPL.

Protocole de routage RPL

Eléments de sécurité

- RPL est conçu pour des réseaux de machines ayant peu de capacités et il a par défaut peu de sécurité.
- Dans le mode de base, n'importe quelle machine peut se joindre au réseau et se faire désigner comme routeur.
- Dans le mode «pré-installé », les machines doivent connaître une clé pour joindre le réseau.
- Dans le mode de sécurité maximale, dit «authentifié », il y a deux clés, une pour devenir un nœud ordinaire et une pour devenir un routeur

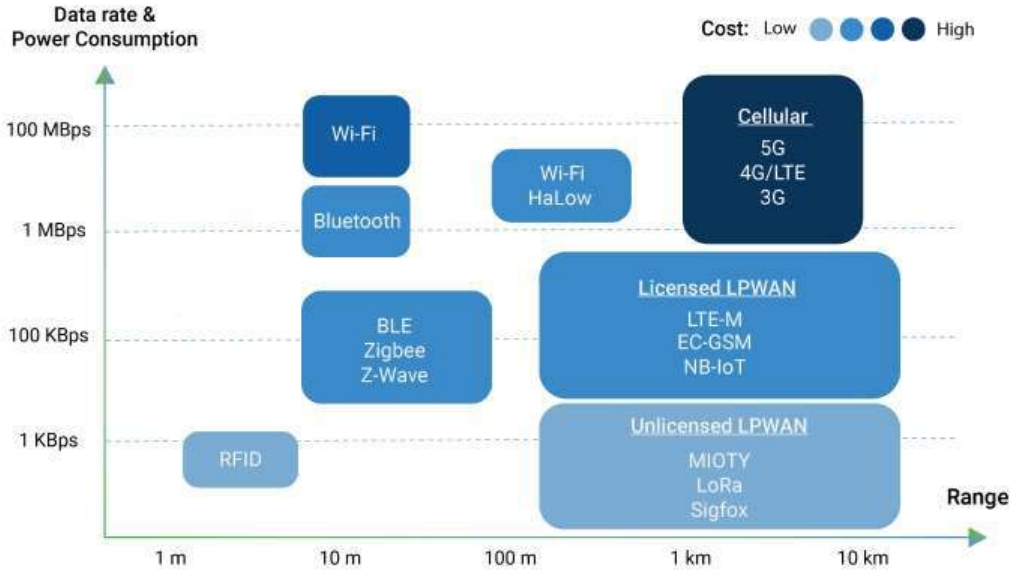
Positionnement des différentes technologies

Key IoT Verticals	LPWAN (Star)	Cellular (Star)	Zigbee (Mostly Mesh)	BLE (Star & Mesh)	Wi-Fi (Star & Mesh)	RFID (Point-to-point)
Industrial IoT	●	○	○			
Smart Meter	●					
Smart City	●					
Smart Building	●		○	○		
Smart Home			●	●	●	
Wearables	○			●		
Connected Car					○	
Connected Health		●		●		
Smart Retail		○		●	○	●
Logistics & Asset Tracking	○	●				●
Smart Agriculture	●					

● Highly applicable ○ Moderately applicable

Source : IoT for all

Positionnement des différentes technologies IoT : Portée, Débit, Energie



Source : BEHRTECH

Choix de la technologie

- La connectivité IoT exige l‘utilisation des normes spécifiques.
- Les technologies cellulaires héritées (2G, 3G, 4G) ne sont pas efficaces. Les normes cellulaires basées sur la release 13 traitent la plupart des lacunes, mais le coût est élevé et la disponibilité est limitée.
- WiFi, Zigbee et BLE ont une portée limitée.
- Plusieurs fournisseurs proposent des alternatives : LoRa et SigFox sont largement utilisés dans le monde pour des longues distances mais avec un débit de données limité.
- Les satellites pour l'IoT offriront des services dans des zones qui n'ont pas de connectivité Internet.

Réseaux propriétaires

- Certains grands groupes industriels, dotés de moyens financiers conséquents, préfèrent installer leur propre réseau de communication.
- Le déploiement de ces réseaux dits privés ou propriétaires est particulièrement intéressants en cas de déploiement à très grande échelle d'appareils communicants.
- C'est ainsi que m2ocity, filiale de Veolia Eau et d'Orange, a choisi d'installer son propre réseau de communication pour connecter les compteurs d'eau intelligents et réaliser des opérations de télé-relevé, de même que Suez.
- Le système de comptage évolué à destination des clients résidentiels de gaz naturel de GRDF se fonde également sur un protocole radio à longue portée spécifique et propriétaire : une bande de fréquence radio réservée (169 MHz) est utilisée pour assurer la communication des données entre les compteurs et les concentrateurs de données, eux-mêmes chargés de transmettre au système d'information central les informations qu'ils ont collectées.

Thank you!

Tableau de conversion du binaire-hexadécimal

Binaire	hexadécimal
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	A
1011	B
1100	C
1101	D
1110	E
1111	F

Les couches MAC définies par l'IEEE

Couche MAC	Utilisation	Bande
802.11	Wi-Fi	802.11, 802.11b, 802.11g, 802.11n : ISM 802.11a : U-NII
802.15.1	Bluetooth	ISM 2,4 GHz
802.15.4	ZigBee, 6LoWPAN	ISM 2,4 GHz dans le monde entier ISM 902–928 MHz aux USA 868,3 MHz dans les pays européens 802.15.4a : 3,1–10,6 GHz
802.16	Réseaux métropolitains sans fil (WMAN, *Wireless Metropolitan Access Network*) Technologie large bande mobile (BWA, *Broadband Wireless Access*), WiMax	802.16 : 10–66 GHz 802.16a : 2–11 GHz 802.16e : 2–11 GHz pour le fixe et 2–6 GHz pour le mobile

Technologies de connectivité

La connectivité WAN (réseau global)		La connectivité LAN (réseau local)	
Les liaisons filaires	Limité aux systèmes fixes pour les bâtiments d'entreprises, infrastructures publiques ou maisons connectées.	Wifi, Wifi Halow (traverse plus facilement les obstacles et consomme moins) et WiGig (débit ultra rapide)	Dédié aux objets alimentés sur secteur en raison de la consommation énergétiques
Les réseaux cellulaires traditionnels	GPRS, EDGE, 3/4G, LPWA (réseau "low power wide area" dédiés IoT)	LiFi (Light Fidelity) ou VLC (Visible Light Communication)	Pour utilisation de lumière entre bleue et rouge diffusée par LED (problèmes de malillumination)
Les réseaux radio basse consommation dédiés	LP-WAN (technologies LoRa, Sigfox et Weightless et Qowisio en développement)	BLE (Bluetooth Low Energy)	Utilisations multiples faible portée faible consommation.
Les réseaux par satellite	Pour les zones non couvertes par les réseaux terrestres (5% du globe)	ANT	Protocole unidirectionnel faible portée pour capteurs dans le domaine du sport.
Les approches hybrides	Combinaisons de plusieurs de ces solutions selon le contexte	Z-Wave	Pour la maison connectée, portée de 50m.
Les approches futuristes	Projet de Web global par ballons / satellites / drones	ZigBee	Pour plusieurs utilisations, portée de 100m.
		EnOcean	Portée de 300m, ultra basse consommation et capteurs autoalimentés. Utilisable pour la domotique (en développement).
		6LoWPAN	Standard permettant de diminuer la consommation d'énergie et rendre compatible le protocole IP avec le domaine IoT.

PRIDA Track 1 (T1)

Workshop Internet des objects

Agenda

- Partie 1: Les applications IoT en Afrique
- Partie 2: Workshop
- Partie 3 : Tutorial …

  Application Android avec Firebase

Workshop Internet des objets

Plan du workshop

- Objectif du workshop
- Démarche technique
- **Première partie :**
  Problématiques à résoudre
- **Deuxième partie :**
  Brainstorming
- **Troisième partie :**
  Démonstration pratique

Objectif du workshop

- Le premier but de cette formation pratique est de comprendre l'importance de l'IoT en tant que outil technologique moderne capable de résoudre des problématiques complexes.
- Le deuxième objectif est de permettre aux participants d'entamer une démarche technique de dimensionnement et de choix technologique d'une architecture IOT en utilisant des outils Open source
- Finalement, afin de pouvoir maitriser l'aspect pratique, nous ferons ensemble une démonstration de développement d'une solution IOT ayant pour objectif de résoudre une problématique d'actualité.

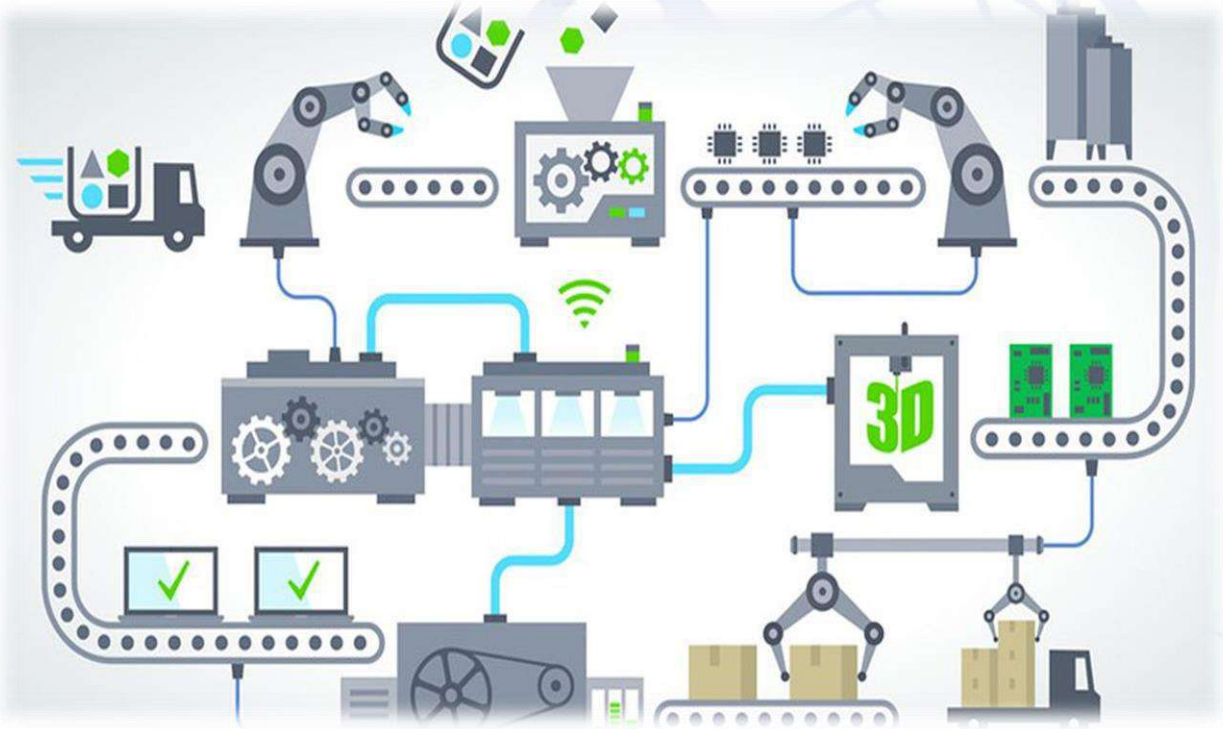
Démarche technique

Afin de maitriser l'aspect pratique et comprendre le principe de l'IOT, il est important de découvrir les différents secteurs d'applications de cette technologie.
Pour ce faire, nous allons évoquer des problématiques chroniques dans des secteurs vitaux et les participants seront invités à s'inspirer des anciennes formations théoriques pour définir les éléments de la solution à proposer.
En suite, nous allons échanger ensemble au tour des architectures présentées
Finalement nous ferons une application pratique d'une manière concrète.

Première partie : Problématique

Problématique 1: Industrie connectée 4.0

Le monde évolue avec la naissance de nouveaux besoins dans différents secteurs vitaux, principalement l'industrie moteur de l'économie.



Problématique 1: Industrie connectée 4.0

De nos jours le suivi de la production et le retour d'information en temps réel est devenue une nécessité pour assurer la compétitivité dans le secteur industriel. Ceci afin de réagir rapidement et afin de prendre les bonnes décisions.
Pour ce faire l'internet des objets s'affirme comme la convergence du monde virtuel, de la conception numérique, de la gestion avec les produits et objets du monde réel.

Cahier des charges

Sujet 1 :
La problématique consiste à concevoir une solution permettant aux industriels de suivre en temps réel et à distance la consommation énergétique de leurs parc machines
Sujet 2 :
La problématique consiste à développer une solution de supervision à distance d'une ligne de production industriel

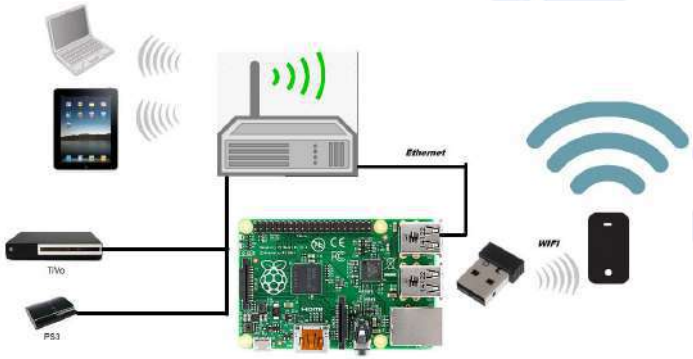
Outils Hardware : Industrie connectée 4.0

Centrale de mesure énergétique

Capteur de tension

Capteur de courant

Carte d'interface



Gateway à Base de carte Raspberry Pi

Gateway à Base de carte Arduino

Problématique 2: Agriculture intelligente

Le monde évolue avec la naissance de nouveaux besoins dans différents secteurs vitaux, notamment l'agriculture

Problématique 2: Agriculture intelligente

L'agriculture présente un secteur vital pour le pays. Actuellement l'intégration des nouvelles technologies est devenu une nécessité pour assurer le développement durable.

Cahier des charges

Sujet 1 :
La problématique consiste à concevoir une solution permettant aux agriculteurs de gérer leur système d'irrigation à distance.
Sujet 2 :
La problématique consiste à développer une solution de supervision à distance d'une station d'aquaculture.

Outils Hardware: Agriculture intelligente

Pompe à eau

Electrovanne

Capteur de température

Gateway

Capteur oxygène dissous

Station météo

Capteur humidité du sol

Problématique 3 : Télémédecine

Problématique

Grâce aux nouvelles technologies, la télémédecine permet l'accès à distance d'un patient à un médecin ou à une équipe médicale. Elle représente une autre manière de soigner, avec les mêmes exigences de qualité et de sécurité

Problématique 3 : Télémédecine

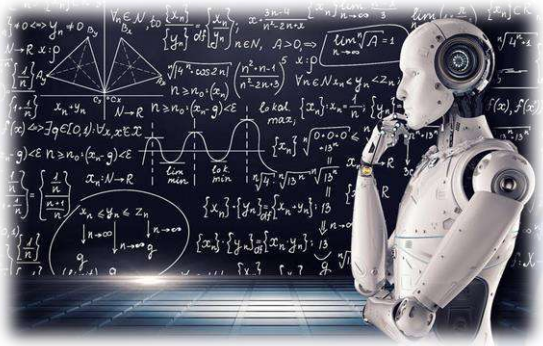
La télémédecine regroupe les pratiques médicales permises ou facilitées par les télécommunications. C'est un exercice de la médecine par le biais des télécommunications et des technologies qui permettent les prestations de santé à distance et l'échange de l'information médicale s'y rapportant.

Cahier des charges

Sujet 1 :
La problématique consiste à concevoir une solution permettant de dépister des symptômes et des signes évoquant de l'infection par covid-19 chez la population et permettant de suivre quotidiennement l'évolution clinique des symptômes de l'infection chez les utilisateurs

Sujet 2 :
La problématique consiste à développer une solution de supervision à distance les paramètres vitaux et le tracé ECG des patients hospitalisés .

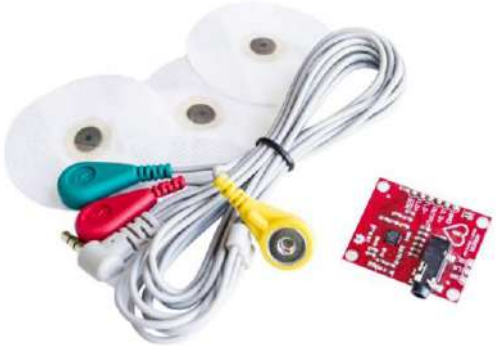
Outils Hardware & Software: Télémédecine



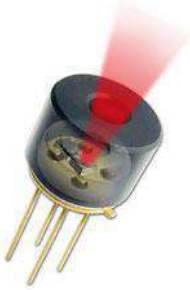
Intelligence artificielle

Base de données massives

Protection des données personnelles



Capteur ECG



Capteur température corporelle sans contact

Plateforme WEB/mobile

Problématique 4: Smart City

Problématique

Une ville intelligente est une ville utilisant les technologies de l'information et de la communication pour améliorer la qualité des services urbains.

Problématique 4: Smart City

Problématique

Une ville intelligente est une ville utilisant les technologies de l'information et de la communication pour améliorer la qualité des services urbains.

Cahier des charges

Sujet 1 :
La problématique consiste à concevoir une solution permettant aux municipalités de suivre en temps réel le pourcentage de remplissage des poubelles enterrés. Sujet 2 :
La problématique consiste à développer une plateforme WEB et mobile permettant au citoyens de valoriser leurs déchets ménagers triés.

Outils : Smart City

Capteur ultrason

Module GSM

Module GPS

Batterie Lithium

LoRa Node

LoRa Gateway

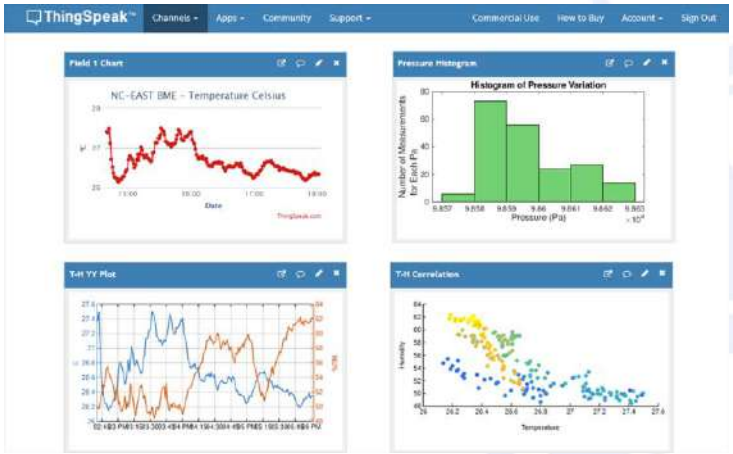
Firebase

NoSql Database

Les attentes de l'exercice de Brainstorming

- Choix de la problématique à résoudre
- Choix de l'architecture de la solution IoT
  - Exigences fonctionnelles (sécurité, disponibilité, …)
  - Composants de la solution
    - Capteurs
    - Passerelles
    - Technologies de connectivité (couverture, vie de batterie, bande passante, vie batterie, coût de connectivité, coût module, spectre)
    - Type de la plateforme de développement (middleware, cloud, …)
    - Application IoT (services métier à proposer, …)

Outils Software



Plateforme numérique

Base de données NoSql

Linux

Logiciel de développement

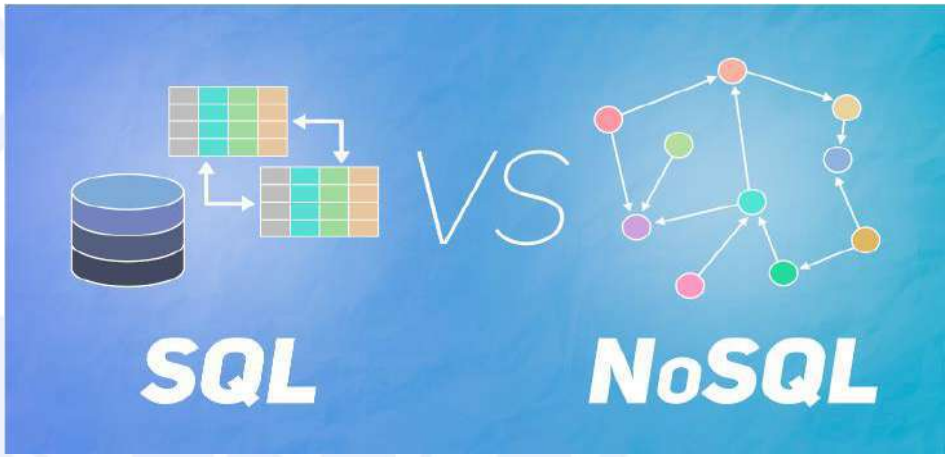
Partie 3:
Plateforme Firebase

Firebase est un ensemble de services d'hébergement pour n'importe quel type d'application. Il propose d'héberger en NoSQL et en temps réel des bases de données, du contenu, de l'authentification sociale, et des notifications, ou encore des services, tel que par exemple un serveur de communication temps réel.

Pourquoi Firebase pour IoT ?
Les principales enjeux de l'IoT sont:
a) Fournir un contenu à faible latence (Firebase Realtime Database)
b) Sécuriser la communication entre les appareils et le backend (Firebase Authentication).

Outils Software

Les bases de données SQL ont un schéma prédéfini alors que les bases de données NoSQL ont un schéma dynamique pour les données non structurées.

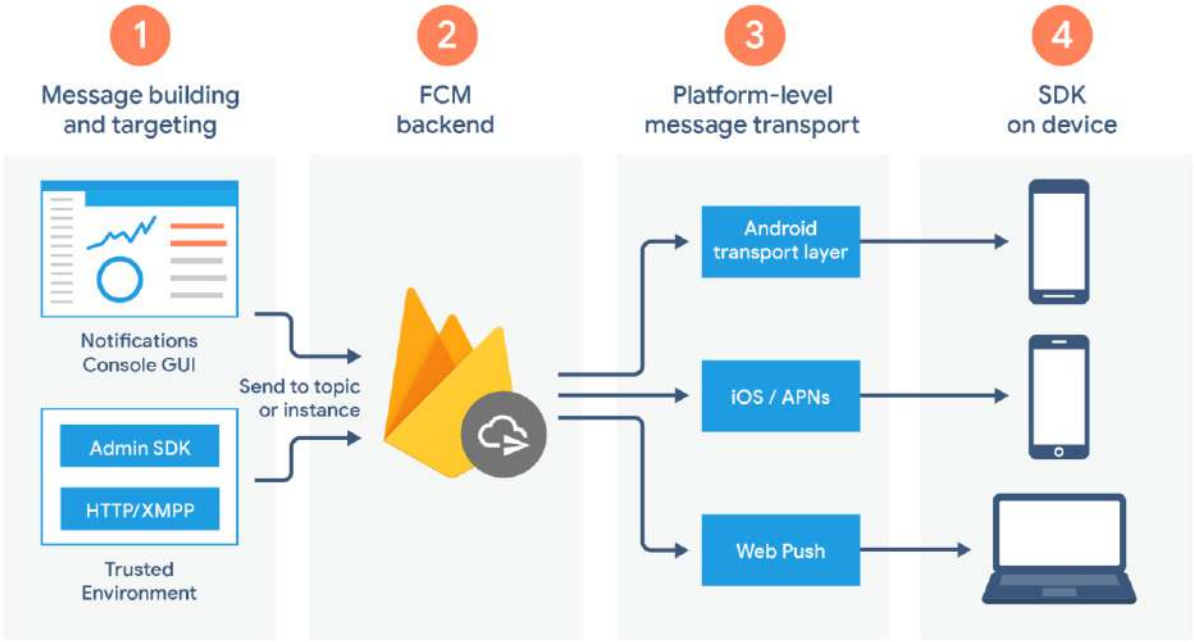


Les bases de données SQL sont évolutives verticalement, tandis que les bases de données NoSQL sont évolutives horizontalement. Les bases de données SQL sont mises à l'échelle en augmentant la puissance du matériel. Les bases de données NoSQL sont mises à l'échelle en augmentant le nombre de serveurs de bases de données dans le pool de ressources afin de réduire la charge.

Cela signifie que les bases de données SQL représentent des données sous la forme de tables composées de n nombre de lignes de données, tandis que les bases de données NoSQL sont la collection de paires clé-valeur, de documents, de bases de données graphiques, etc. qui ne possèdent pas de définitions de schéma standard.

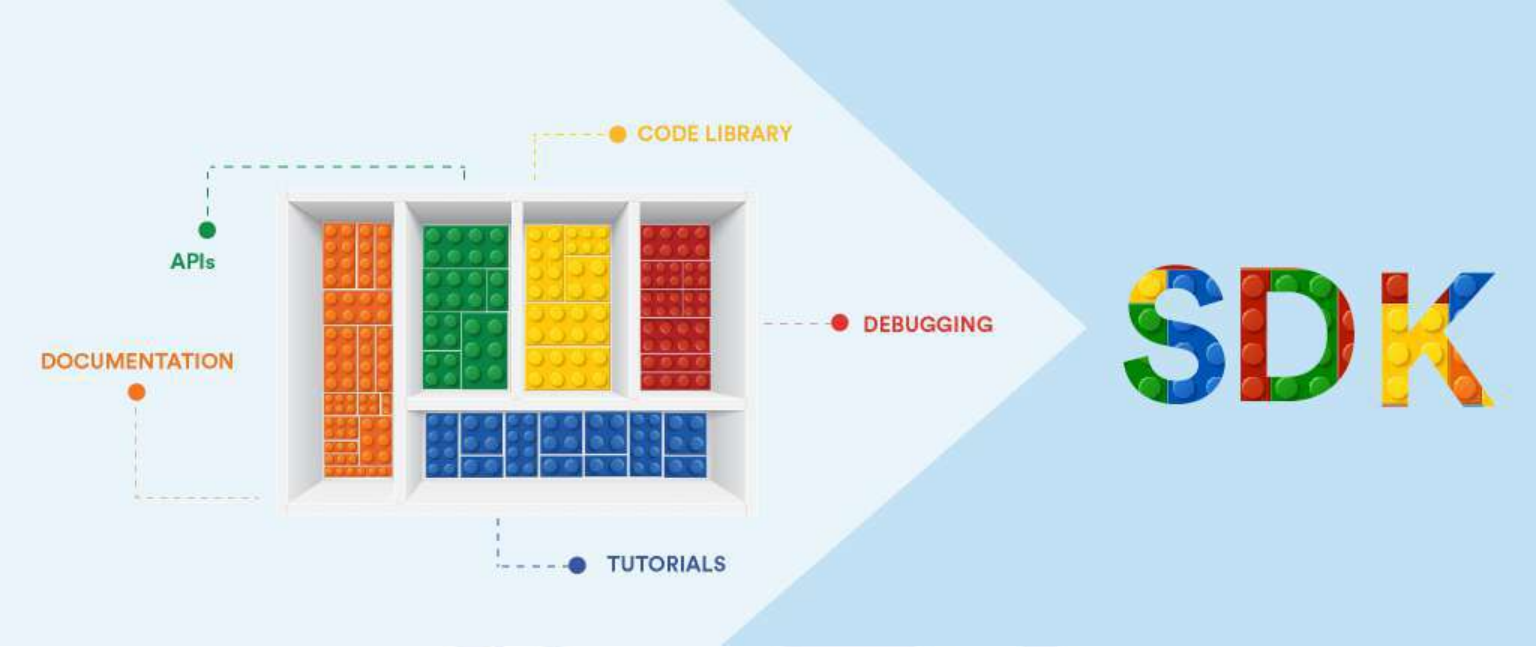
Outils Software

Firebase s'occupe d'une grande partie des services que normalement les développeurs eux-mêmes devraient les créer, comme par exemple l'authentification, les bases des données, les notifications, l'hébergement des serveurs etc.



Les services offerts par Firebase sont hébergé dans le Cloud et elles sont scalables avec peu ou pas d'effort de la part du développeur. Ces services ont des composants backend qui sont entièrement gérées et maintenues par Google. Firebase offre des SDK clients qui interagissent avec ces composants de façon directe sans besoin de placer un middleware entre l'application et les services

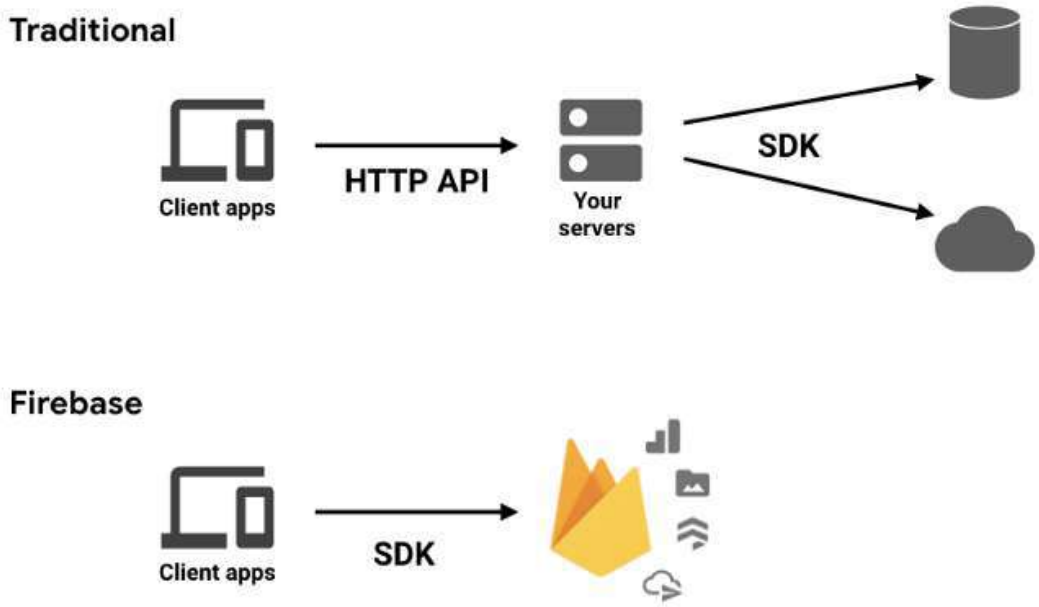
Outils Software



SDK (Software Developement Kit) désigne un ensemble d'outils utilisées par les développeurs pour le développement d'un logiciel déstiné à une plateforme déterminée (Android, iOS,…).
Un SDK peut avoir une seule ou plusieurs cibles comme un système d'exploitation, une application web, un serveur web, jeu vidéo, etc.
Pour développer une application Android, il faut le SDK client Android de Firebase. Pour développer une application web, il faut le SDK client web de Firebase, etc.

Outils Software

Le SDK de Firebase qui permet une interaction directe entre un client et les services Firebase importe une nouvelle notion de développent qui diffère de la méthode traditionnelle où une partie backend et une partie frontend doit être développée, alors que dans le cas de Firebase on contourne la partie backend et donc la logique d'exécution est placé chez le client (frontend). Voir figure suivante. L'accès administrateur est fournie par l'espace « Firebase console ».



Comparaison entre le développement classique et le développement avec Firebase

Les services de Firebase

Firebase Realtime Database et Cloud Firestore:
Ce sont les deux bases des données offertes par Firebase, elles se décrit comme des bases de données temps réel, hébergées dans le Cloud et NoSQL)

Les clients de multi plateforme partagent la même ressource dans la base des données. S'il a une modification, tout les clients reçoit automatiquement une mise à jour instantanée.

Firebase stockent les données sous la format JSON et elle utilise le type NoSQL pour ses bases des données, ce qui nous débrase du contrainte des tables de la base des données relationnelle (SQL par exemple), permettant ainsi de créer et dimensionner d'une façon plus libre et facile une base des données.

Firebase Realtime Database VS Cloud Firestore

Firebase Realtime Database	Cloud Firestore
Requêtes limitées	Requêtes plus riches et plus rapides
Latence plus faible	Latence plus élevée
Stockent les données dans une grande arborescence JSON	Stockent les données sous forme de collections des documents
Moins scalable	Facilement scalable
Idéale pour les synchronisations des données fréquentes.	Plus adéquates aux projet complexes

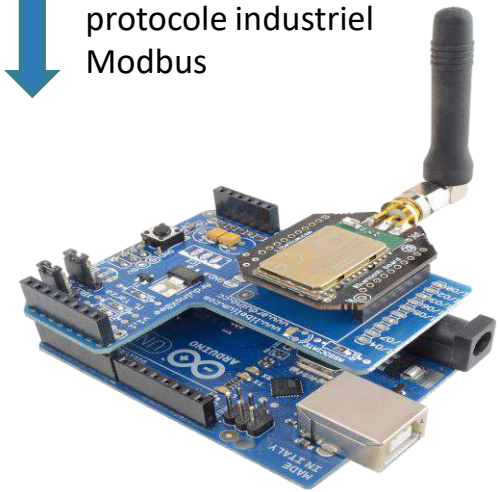
Cloud Storage fournit un stockage des fichiers massivement scalable, il permet aux clients (un client peut être un appareil IoT aussi!) de publier et de télécharger des fichiers (images, texte, etc.)

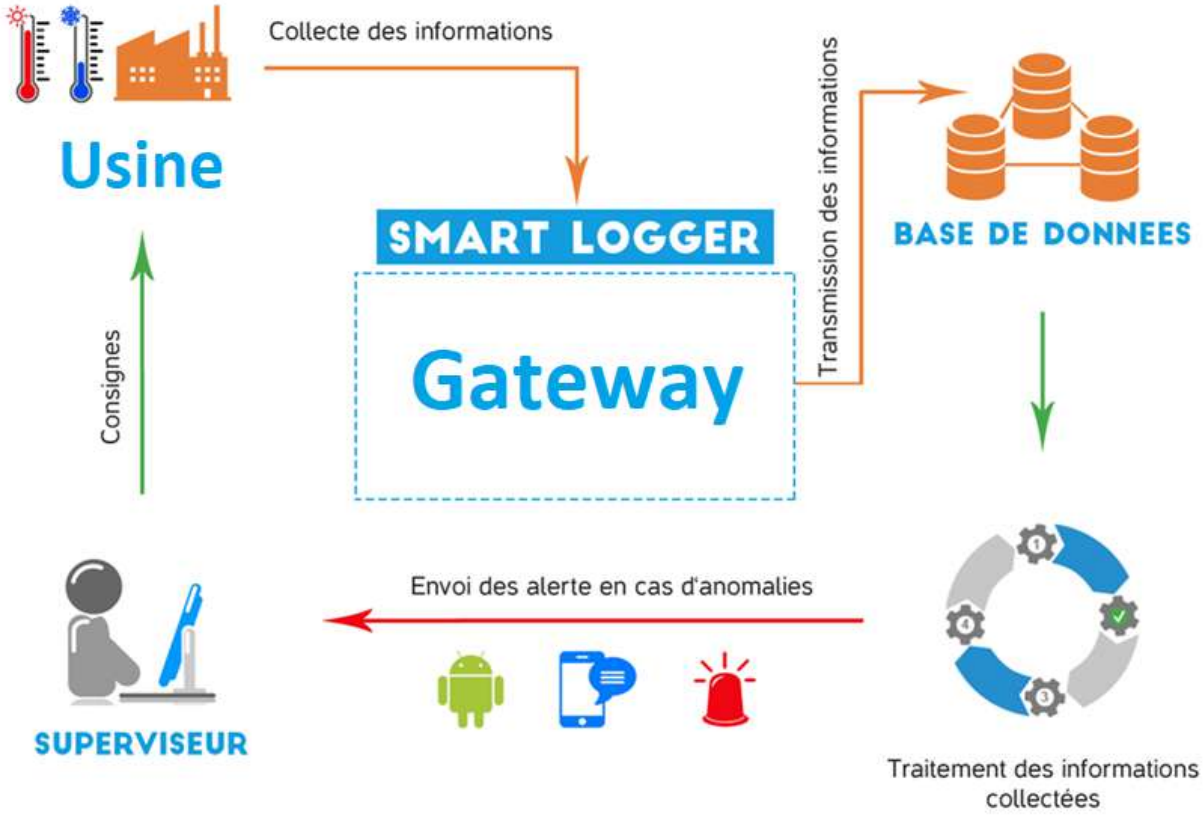
Cloud Functions:
En utilisant le service Cloud Functions de Firebase, on peut déployer un code exécutant sur les infrastructures serveur de Google qui répond automatiquement au événements arrivants d'autres service de Firebase.

Deuxième partie : Brainstorming

Eléments de la solution : Industrie connectée 4.0

Communication via le protocole industriel Modbus

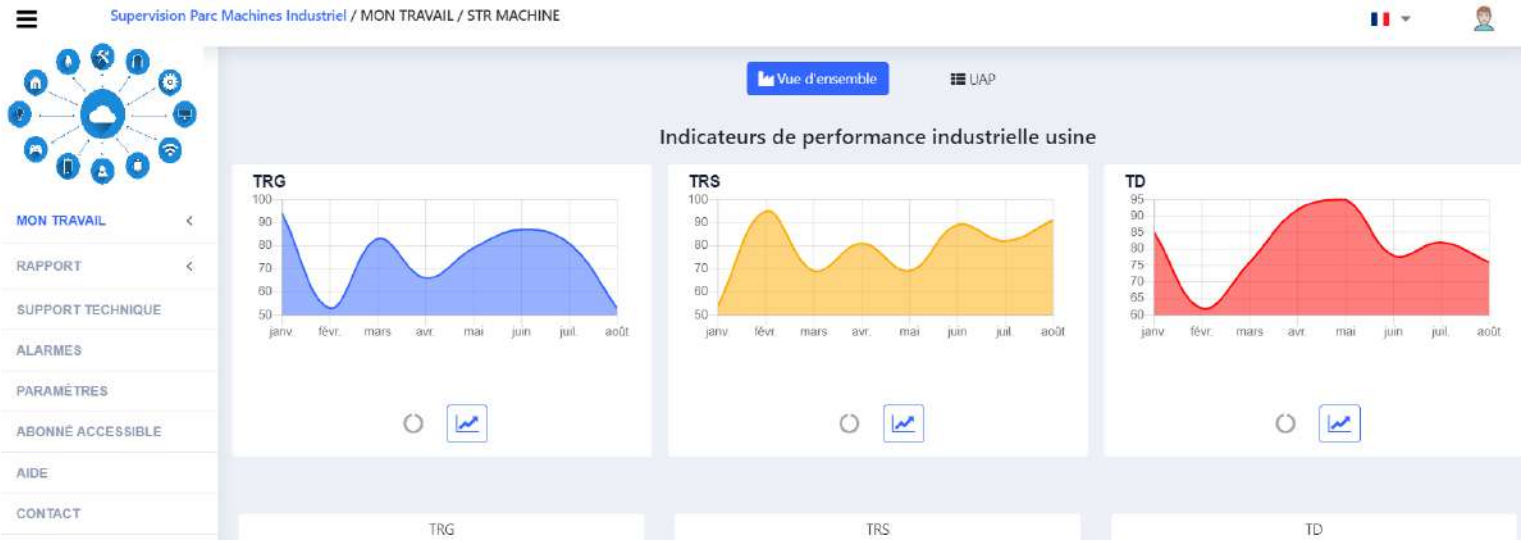




Technologie de connectivité : Wi-Fi, 4G

Eléments de la solution : Industrie connectée 4.0

Communication en temps réel entre la base des données et la plateforme



Eléments de la solution : Industrie connectée 4.0

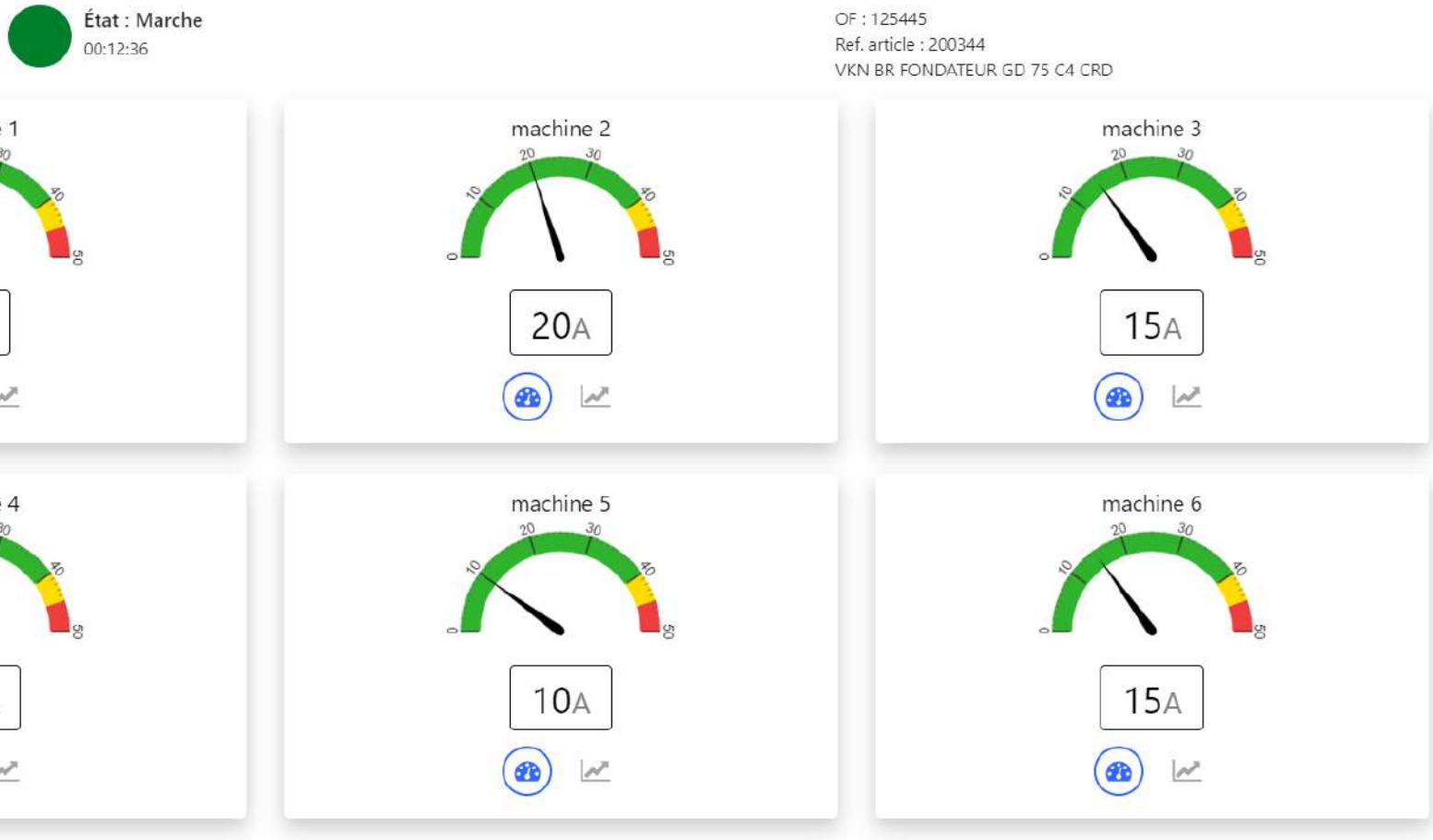


Tableau de bord accessible sur la plateforme

Eléments de la solution: Agriculture

Démonstration application SMART Irrigation

La solution contient principalement un kit de commande à distance des vannes d'irrigation et des motopompes via une application mobile. Cet outil permet à l'agriculteur d'épargner le déplacement sur site et il lui permet de définir des temps d'irrigations précis. La deuxième composante du projet c'est de faire de l'échantillonnage sur des différents niveaux de sols pour informer l'agriculteur sur le pourcentage d'humidité du sol. Ceci afin de savoir la quantité d'eau d'irrigation nécessaire.

Technologie de connectivité : 2G, LoRa

Eléments de la solution: Agriculture

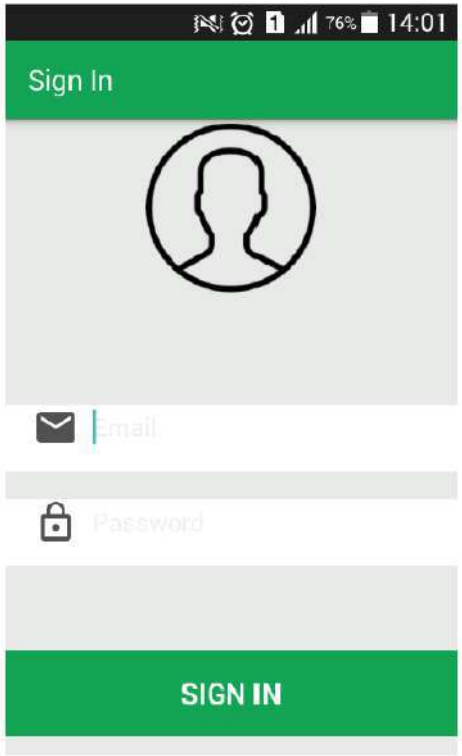


Figure 1: interface de login

Figure 2: Interface station météorologique

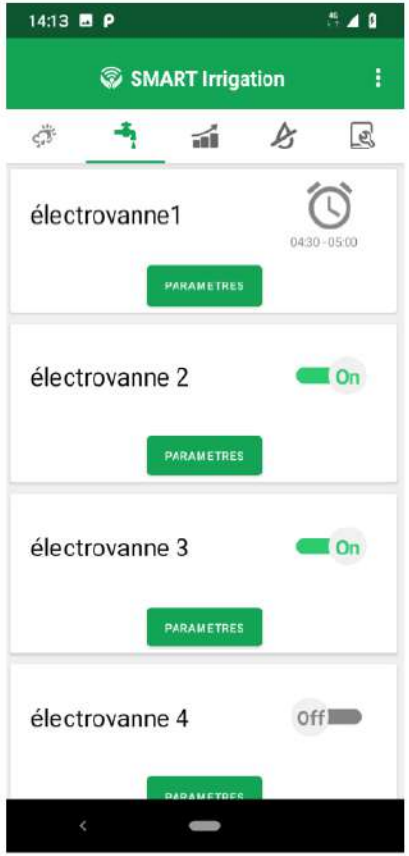


Figure 3: interface d'irrigation

Figure 8: fenêtre de configuration d'une pompe

Eléments de la solution: Agriculture

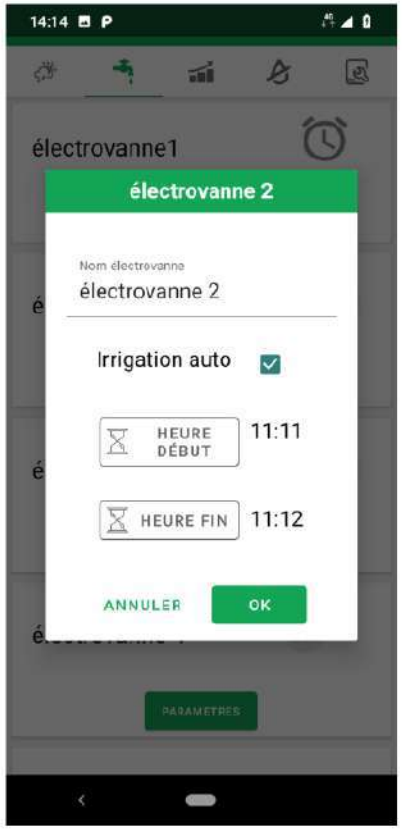


Figure 9: les paramètres de configuration d'une irrigation automatique.

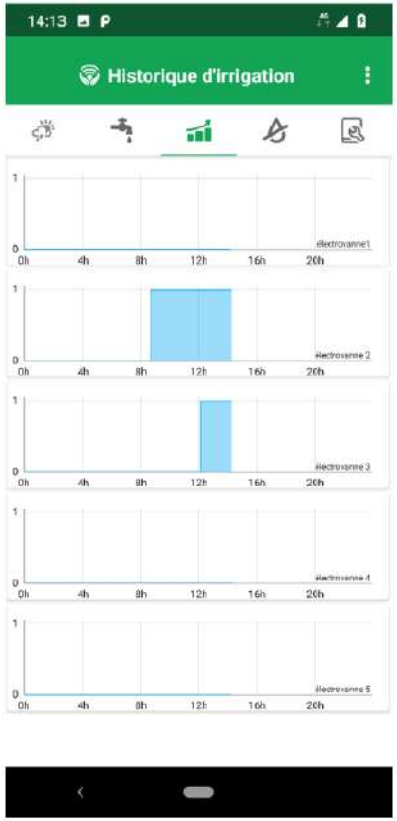


Figure 12: interfaces de l'historique d'irrigation.

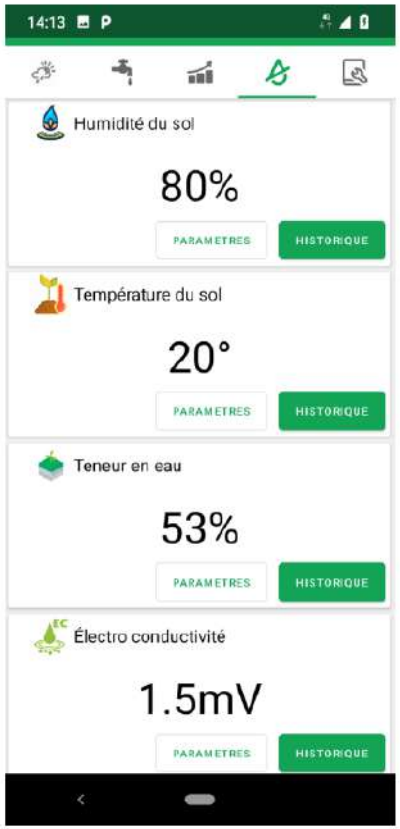


Figure 13: Interface des capteurs du sol

Figure 14: Définir des seuils

Eléments de la solution: Agriculture

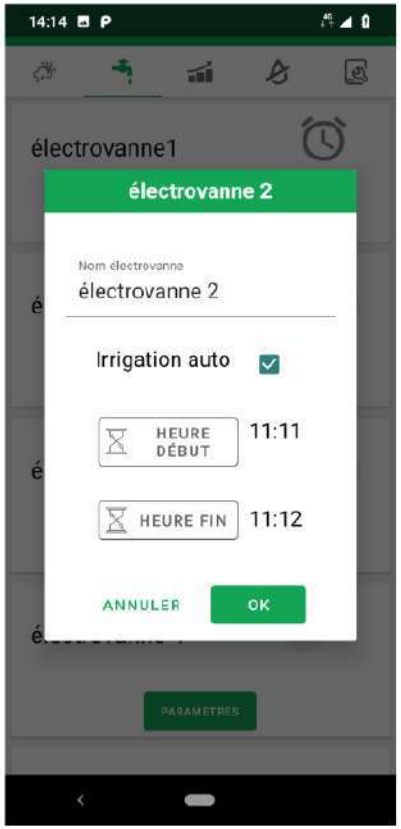


Figure 9: les paramètres de configuration d'une irrigation automatique.

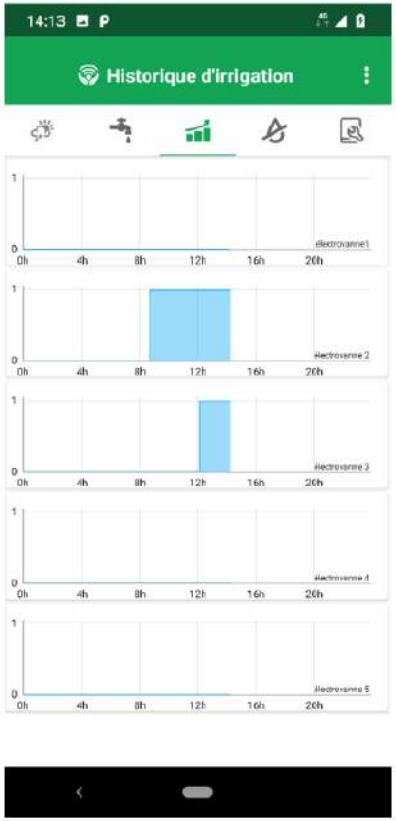


Figure 12: interfaces de l'historique d'irrigation.

Figure 13: Interface des capteurs du sol

Figure 14: Définir des seuils

Eléments de la solution : Télémédecine

Objectifs :

- ✓ Dépister les symptômes et signes évoquant de l'infection par covid-19 chez la population,
- ✓ Suivre quotidiennement l'évolution clinique des symptômes de l'infection chez les utilisateurs,

- ✓ Permettre au staff médical de détecter les patients suspects porteurs du covid-19,
- ✓ Permettre au staff médical d'indiquer la pratique du test de diagnostic du covid-19,
- ✓ Permettre au staff médical de sélectionner les patients à risque de développer des formes graves,
- ✓ Permettre au staff médical d'indiquer l'hospitalisation des patients,
- ✓ Permettre au staff médical de vérifier le respect du confinement des patients suspect par la géolocalisation,
- ✓ Permettre au ministère de la santé de générer des statistiques de l'évolution de l'épidémie,

- ✓ Sauvegarder et archiver tous les données et informations collectées des utilisateurs,
- ✓ Plateforme WEB accessible par plusieurs utilisateurs avec contrôle d'accès sécurisé,
- ✓ Séparer les informations à caractère personnelles de celle à utilisation anonyme,
- ✓ Dimensionner le serveur pour pouvoir gérer un nombre d'utilisateur simultané > 10 millions

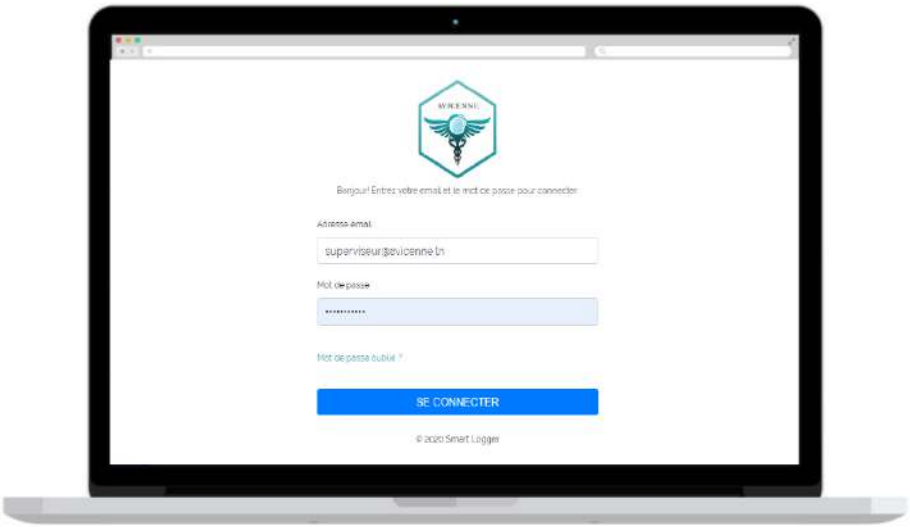
Eléments de la solution : Télémédecine

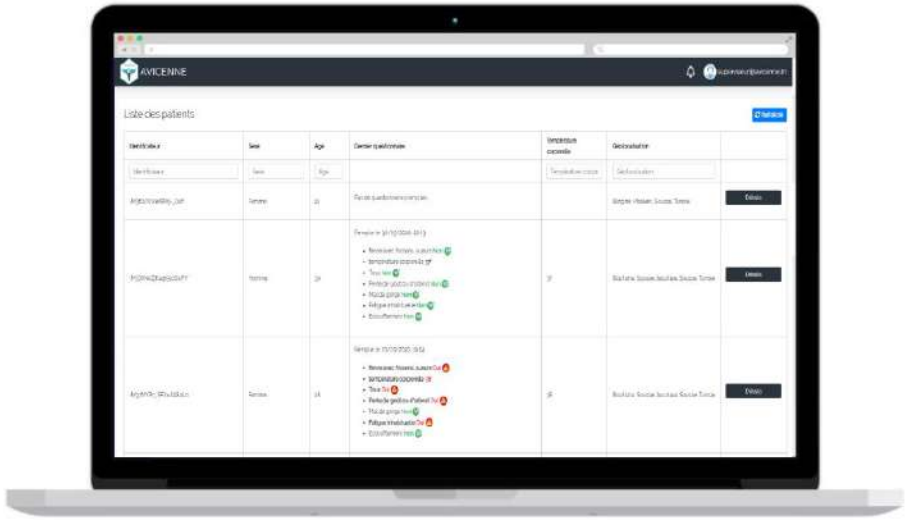
Technologie de connectivité : Wi-Fi, 4G

Eléments de la solution : Télémédecine

Le tableau de bord pour l'administrateur médical contenant un classement des utilisateurs de l'application mobile en indiquent leurs âges, dernière réponse au questionnaire, dernière prélèvement de la température corporelle.

Le staff médical peut trier les utilisateurs par catégorie d'âge, valeur de la température corporelle et zone géographique.

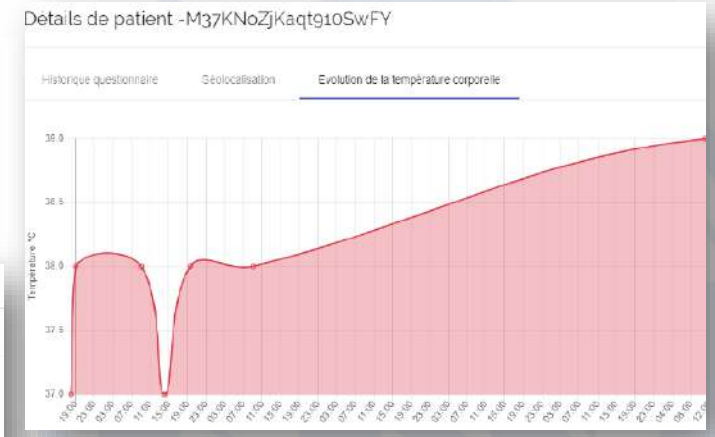




Plateforme WEB administrateur

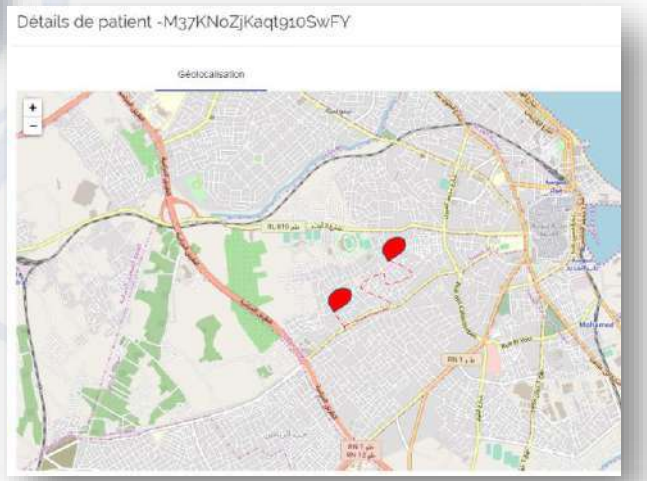
Eléments de la solution : Télémédecine

En cas d'urgence détecté, le staff médical peut visualiser l'historique des réponses du patient avec plus de détails sur l'évolution de sa santé.

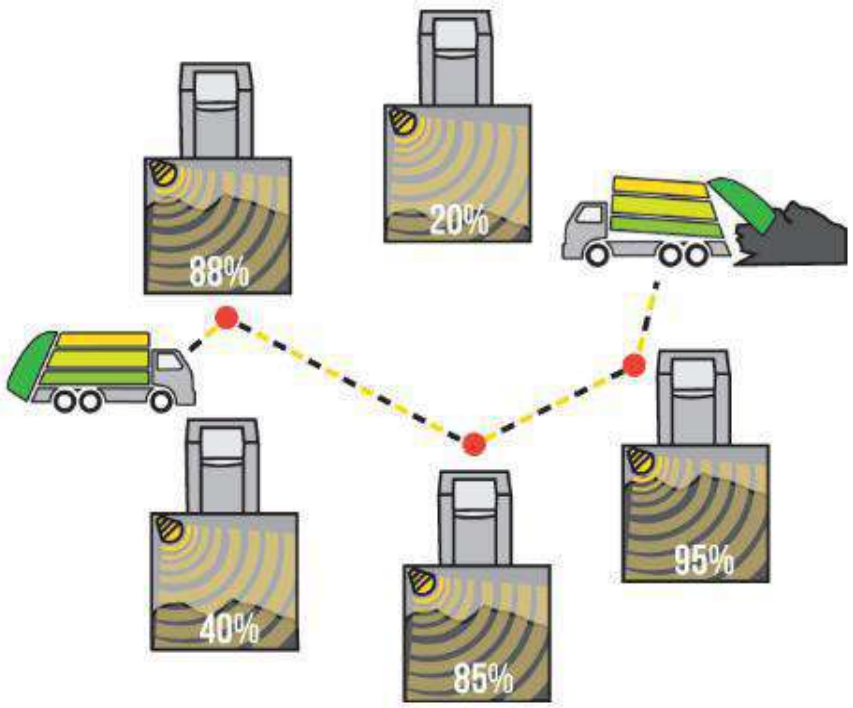


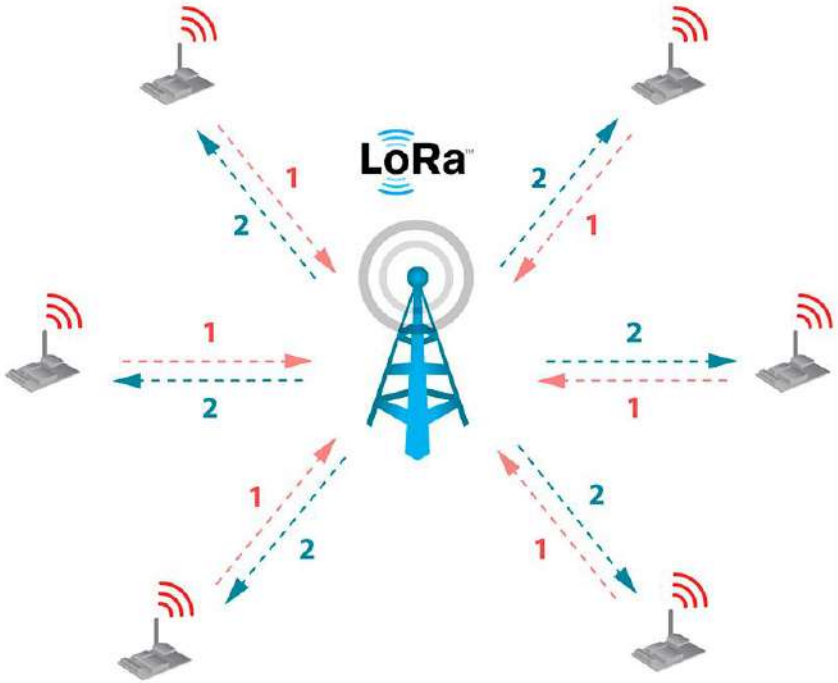
De même en cas de besoin le staff médical peut visualiser une lecture détaillée de l'évolution de la température corporelle du patient tout au long de son utilisation de l'application AVICENNE

Le tableau de bord **pour l'administrateur sécurité** contenant l'adresse approximative et un relevé de répartition géographique pour les patients porteurs du covid-19 misent obligatoirement en quarantaine.



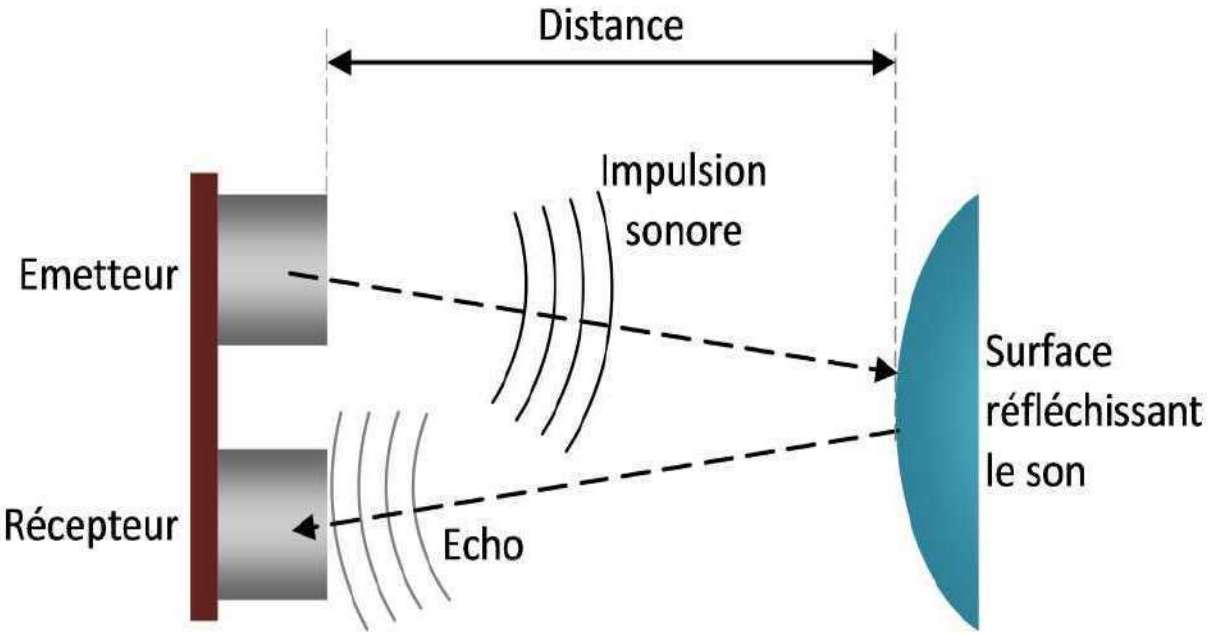
Eléments de la solution : Smart City





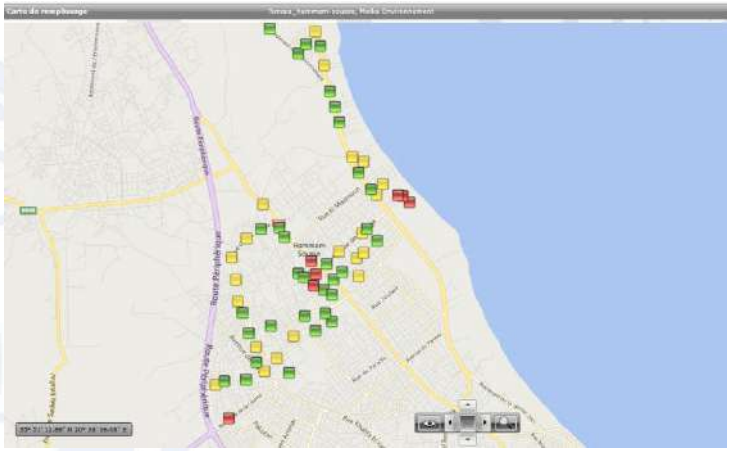
Technologie de connectivité : LoRa, 2G

Eléments de la solution : Smart City



Eléments de la solution : Smart City

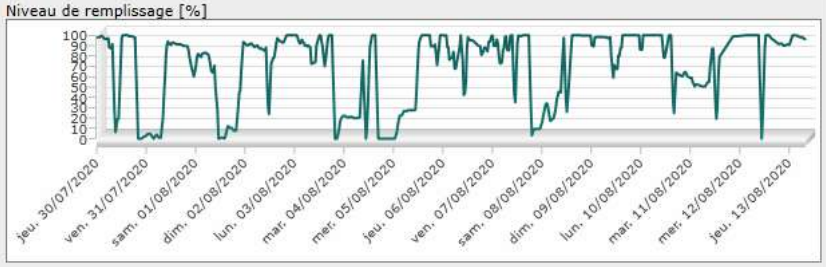
Statut	Fraction	Remplissage [%]	Conteneur ID	Rue	Code postal	Placer	Séquence ID	Geo ID
	OM	100	77	Boulevard Kantaoui Morjen	4011	Hammam-Sousse		
	OM	96	48	Route de la plage	4011	Hammam-Sousse		
	OM	96	74	Parking Maison de Jardin	4011	Hammam-Sousse		
	OM	93	30	Avenue de la république	4011	Hammam-Sousse		
	OM	88	1	Rue de la liberté	4011	Hammam-Sousse		
	OM	86	28	Route national 1	4011	Hammam-Sousse		
	OM	86	47	Résidence MonteCarlo	4011	Hammam-Sousse		
	OM	86	56	Rue de l'Océan Atlantique	4011	Hammam-Sousse		
	OM	85	61	Zone Touristique Port El Kantaoui	4089	Hammam-Sousse		
	OM	83	33	Rue Rmada	4011	Hammam-Sousse		
	OM	78	5	Rue El Yamni	4011	Hammam-Sousse		
	OM	78	78	Boulevard Kantaoui Morjen	4011	Hammam-Sousse		
	OM	75	2	Rue de la Victoire	4011	Hammam-Sousse		
	OM	75	24	Route national 1	4011	Hammam-Sousse		
	OM	75	29	Avenue de la république	4011	Hammam-Sousse		
	OM	75	69	Rue des Violettes	4011	Hammam-Sousse		
	OM	72	18	Boulevard abdelkader daghrir	4011	Hammam-Sousse		
	OM	72	19	Boulevard abdelkader daghrir	4011	Hammam-Sousse		
	OM	72	20	Rue Yasser Arafat	4011	Hammam-Sousse		
	OM	72	66	Passage el Mafa	4011	Hammam-Sousse		
	OM	72	82	Avenue 14 janvier	4089	Hammam-Sousse		
	OM	70	38	Boulevard alexandrie	4011	Hammam-Sousse		
	OM	70	52	Rue des sables	4011	Hammam-Sousse		
	OM	70	62	Passage la corallie	4011	Hammam-Sousse		
	OM	70	83	Route touristique El Kantaoui	4011	Hammam-Sousse		
	OM	68	9	Boulevard abdelkader daghrir	4011	Hammam-Sousse		
	OM	68	43	Route de la plage	4011	Hammam-Sousse		



Enregistrer | Minimiser les | Fermer | Déconnexion

Niveau de remplissage

Niveau de remplissage [%]



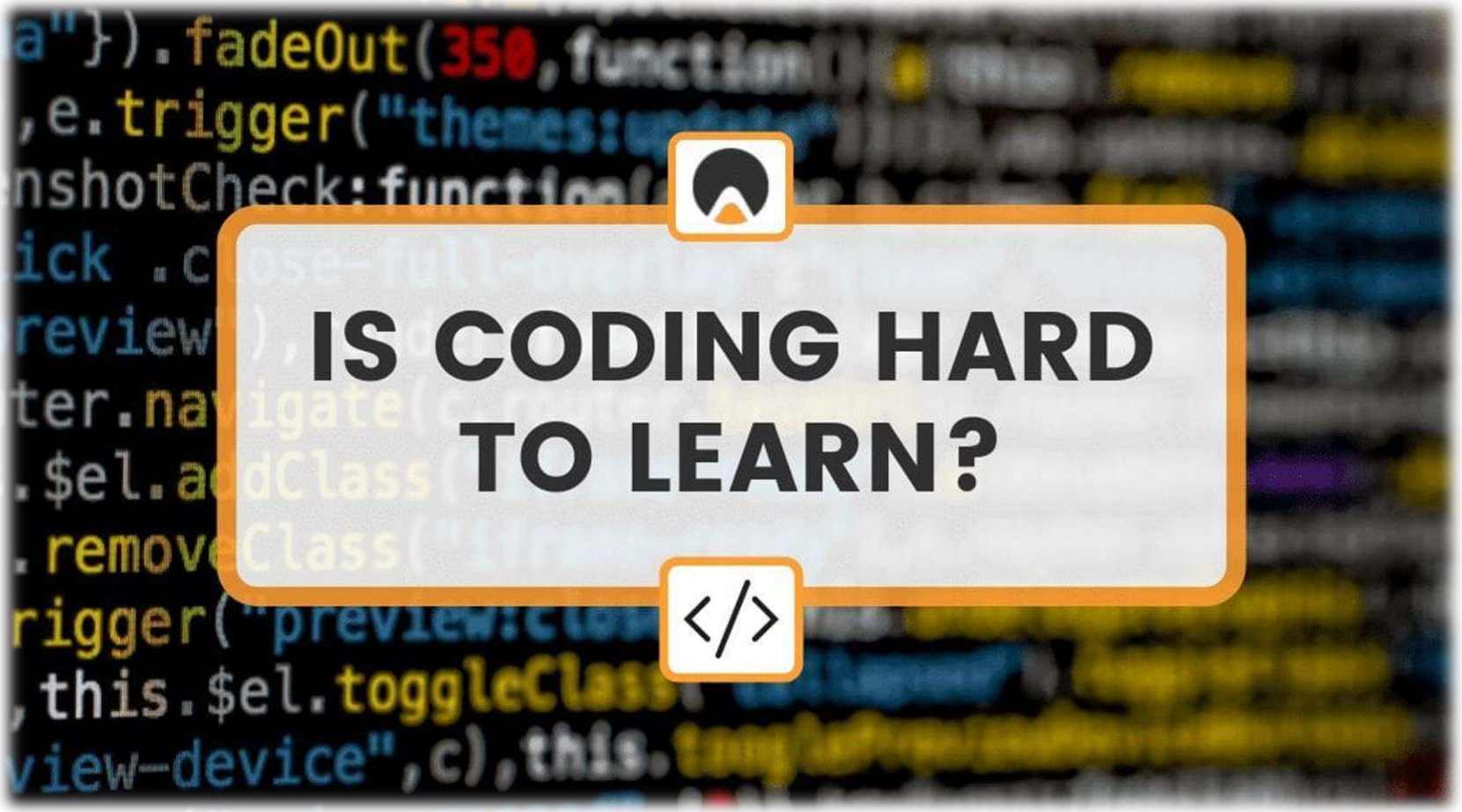
Des 30/07/2020 | Pour 13/08/2020 | Mise à jour

Rue

Désignation: Maison de jardin 1	Rue: Parking Maison de Jardin	ID Lieu: 135184492
Code postal: 4011	Placer: Hammam-Sousse	Visite ID:
Séquence ID:	Responsable:	La logistique de transport:

Journal

Troisième partie : Démonstration

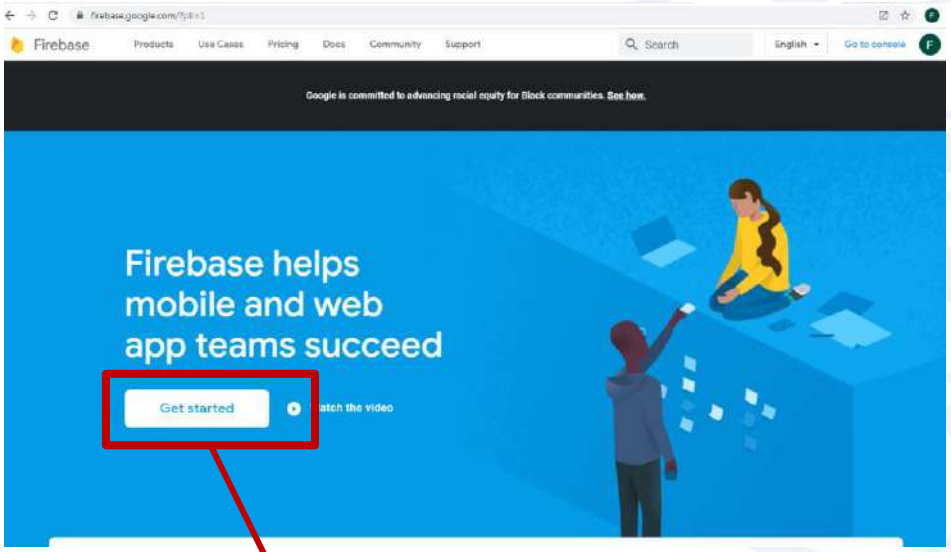


Application Android avec Firebase

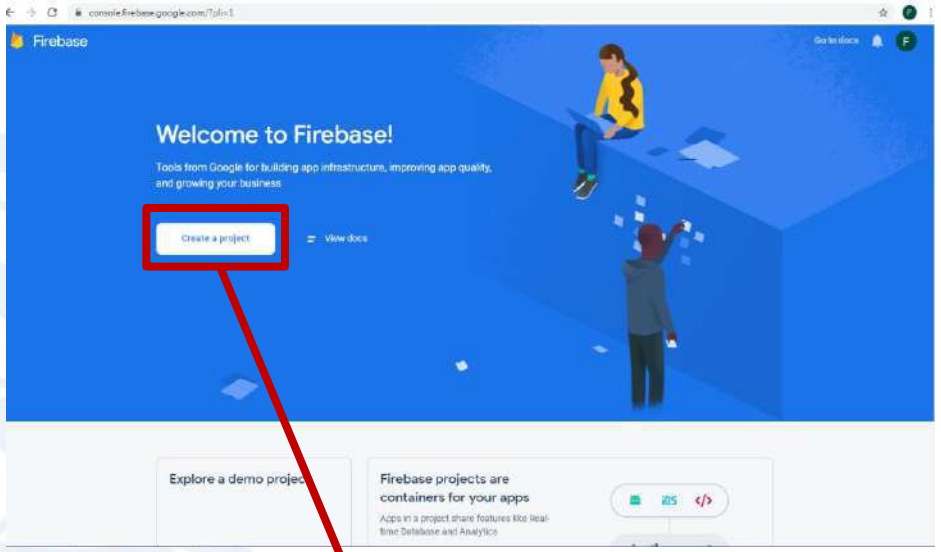
Il faut tout d'abord avoir un compte Google pour utiliser les service de Firebase, il suffit juste de créer un nouveau compte gratuitement. Ensuite, visitez le site web de Firebase:
https://firebase.google.com/

Pour développer une application sur Android, il nous faut un logiciel d'environnement de développement (IDE), nous allons utiliser l'IDE officiel de Google « Android Studio » téléchargeable sur ce lien:
https://developer.android.com/studio

Démarche de création d'une Application Android avec Firebase



Cliquez sur Get started

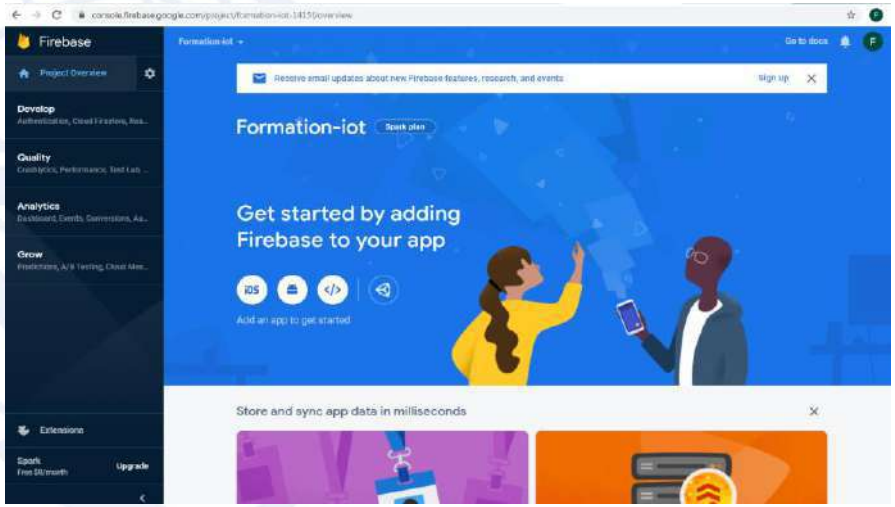


Cliquez sur Create project

Outils Software

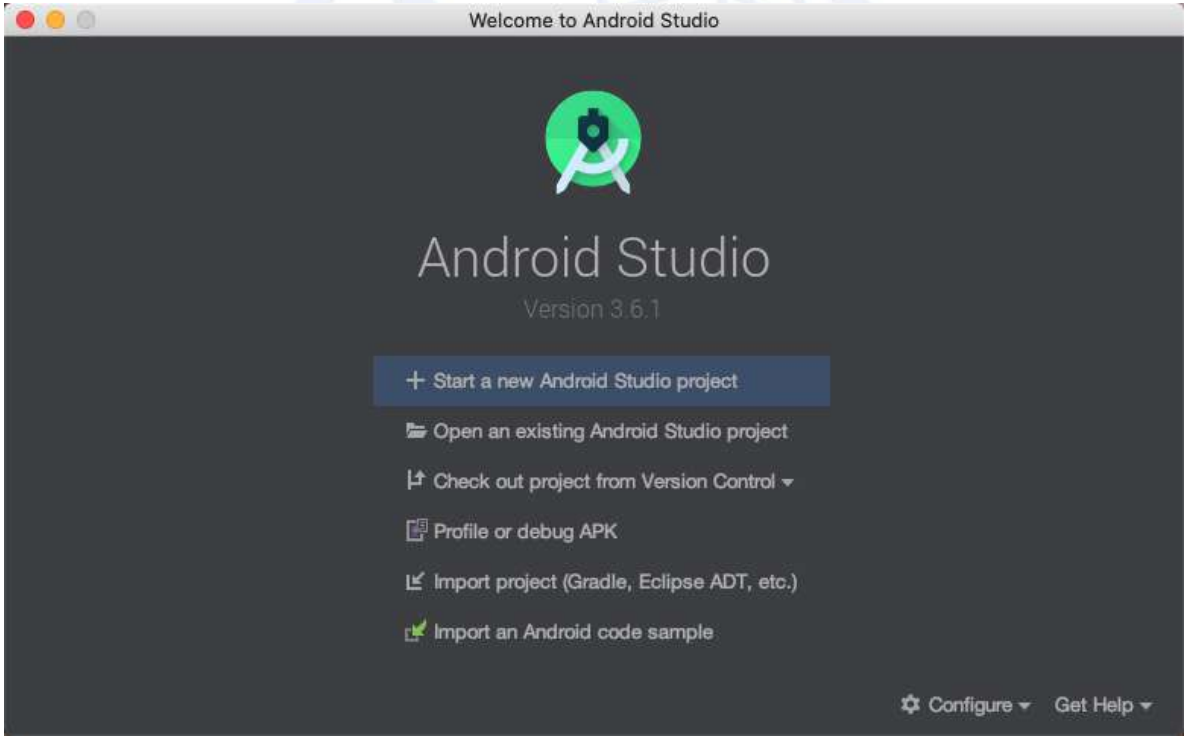
Entrez un nom de votre projet

Acceptez les termes de services de Firebase

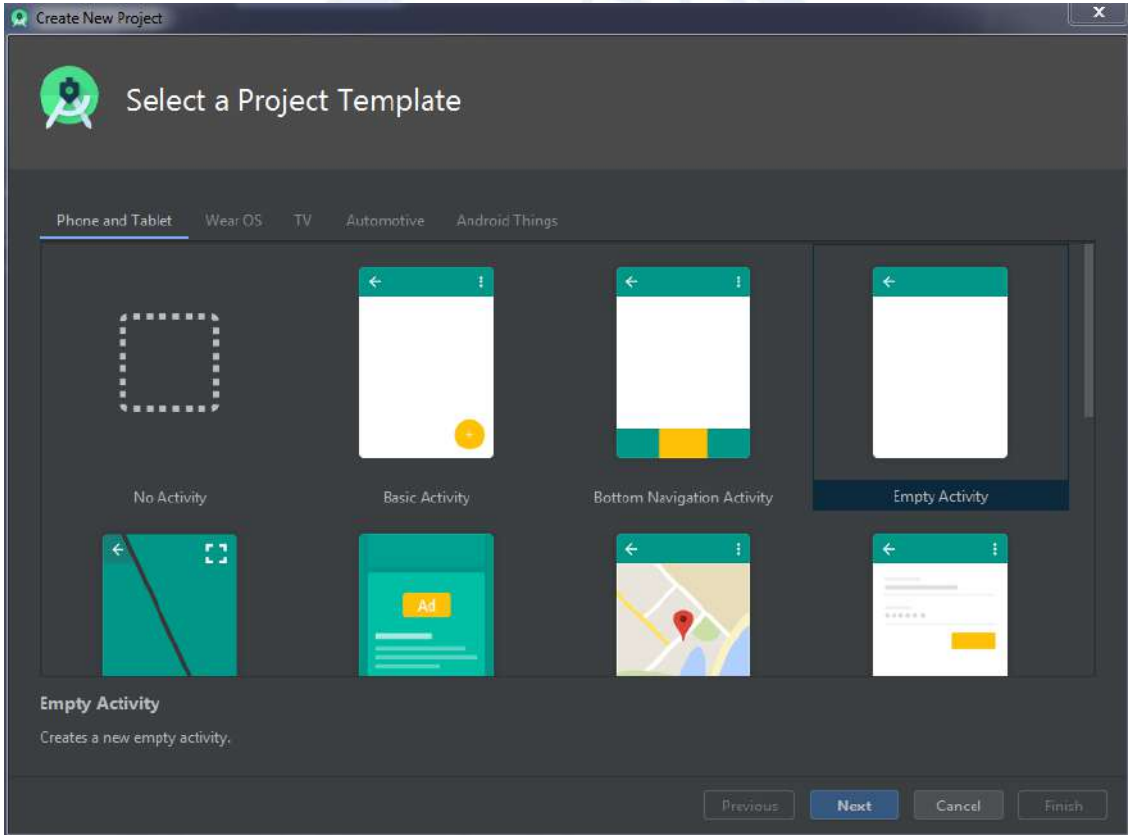


Vous êtes maintenant sur l'interface « Firebase console »

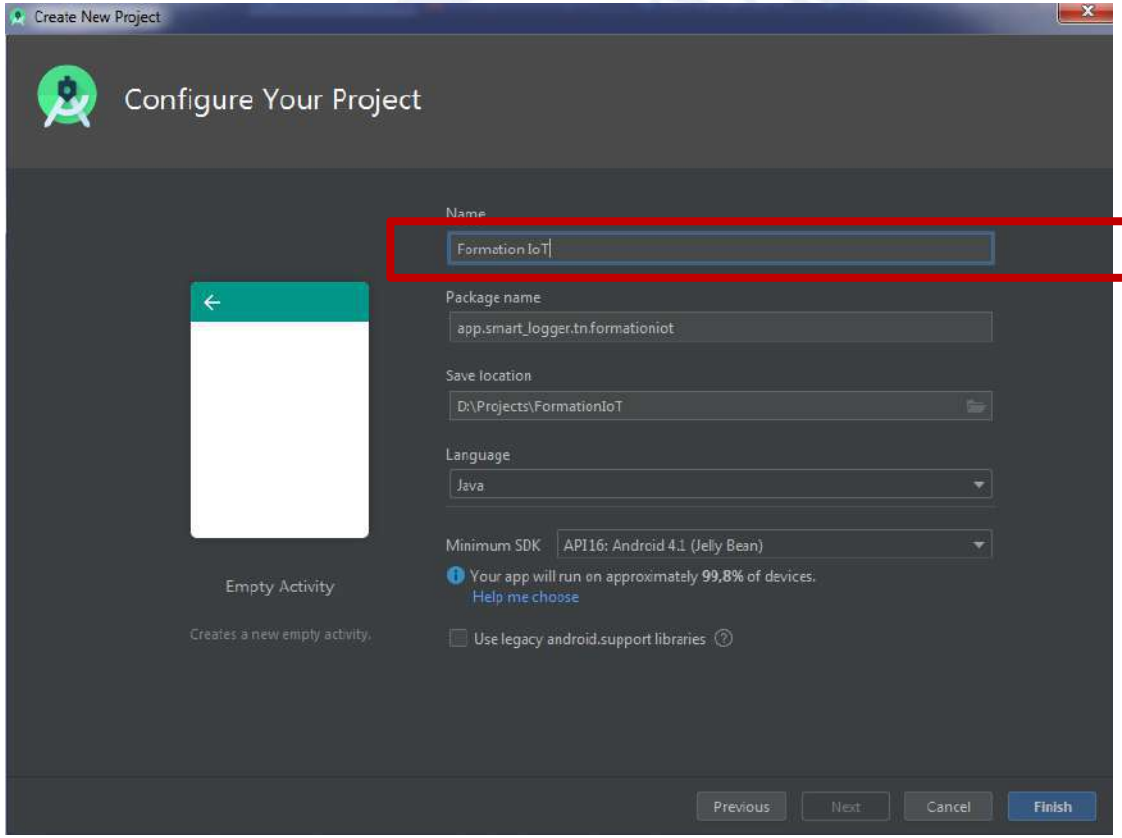
Ouvrez Android Studio et cliquez sur **Start a new Android Studio Project**



On nous demande de choisir un Template de notre projet, on va choisir « Empty Activity »



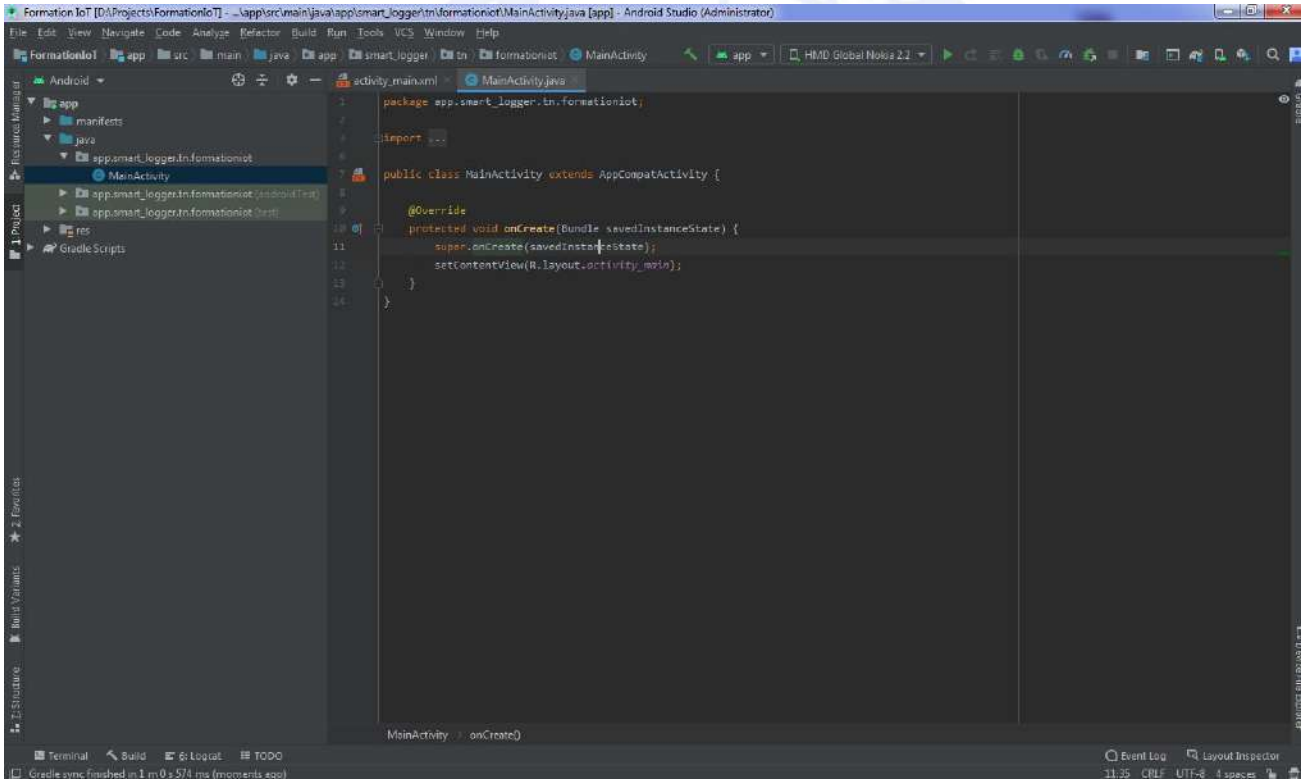
Attribuer un nom à votre projet et laisser tout les autre champs intacte et cliquez sur « Finish »



Nom du projet

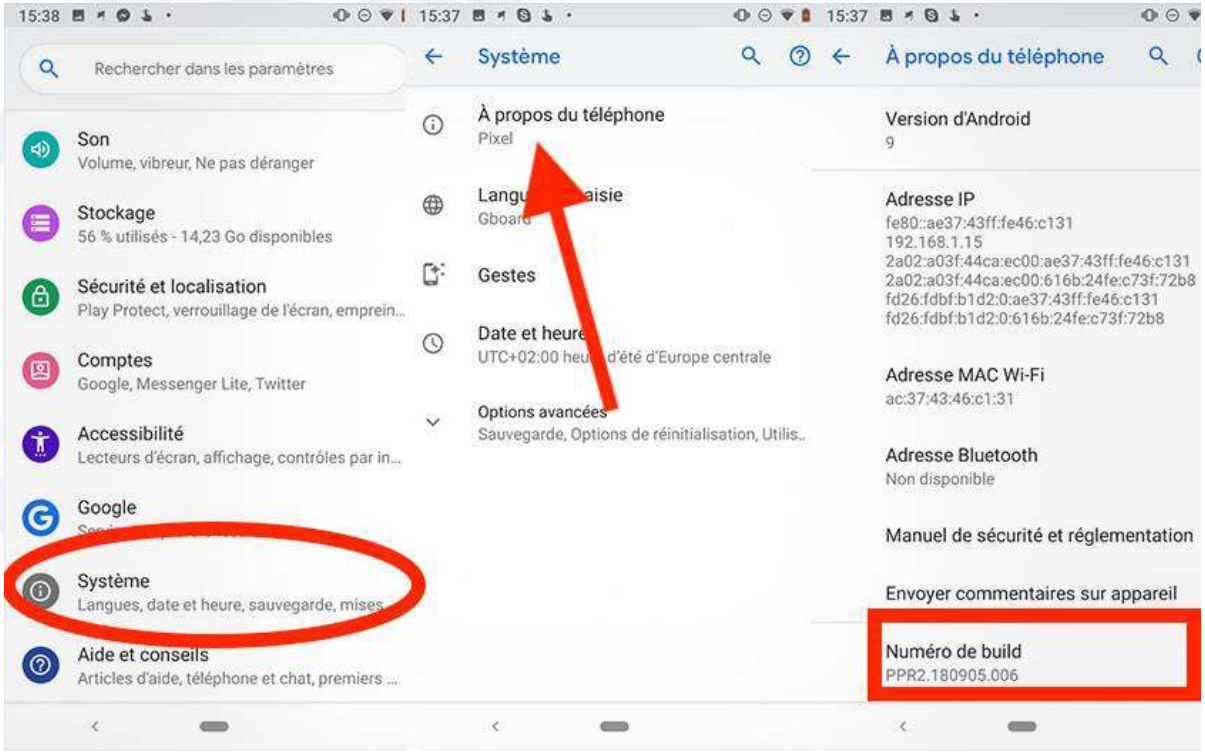
Outils Software

Votre projet est crée! L'interface doit être comme celle-ci:



Nous allons maintenant exécuter notre première application sur un Smartphone Android, mais avant il faut configurer son Smartphone en mode développeur.

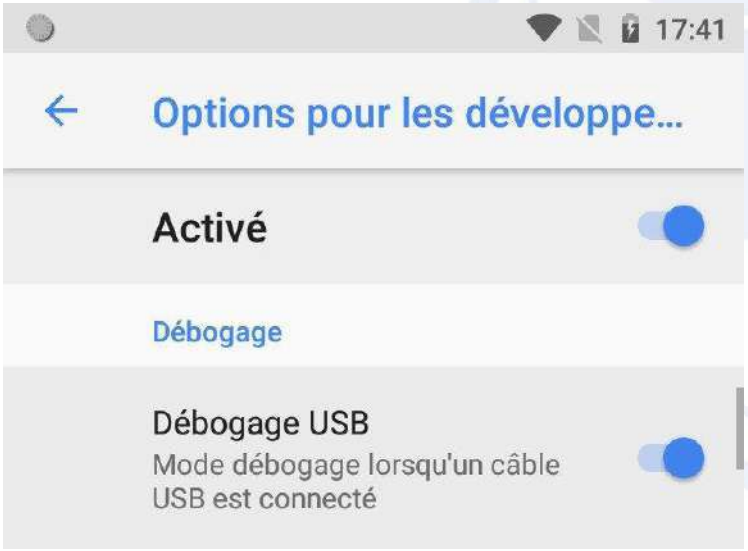
Remarque: On peut aussi utiliser le Smartphone virtuel de Android Studio, mais il est préférable de tester sur un appareil réel.



Accédez aux paramètres de votre Smartphone, puis **Système>A propos de téléphone>Numéro de build**

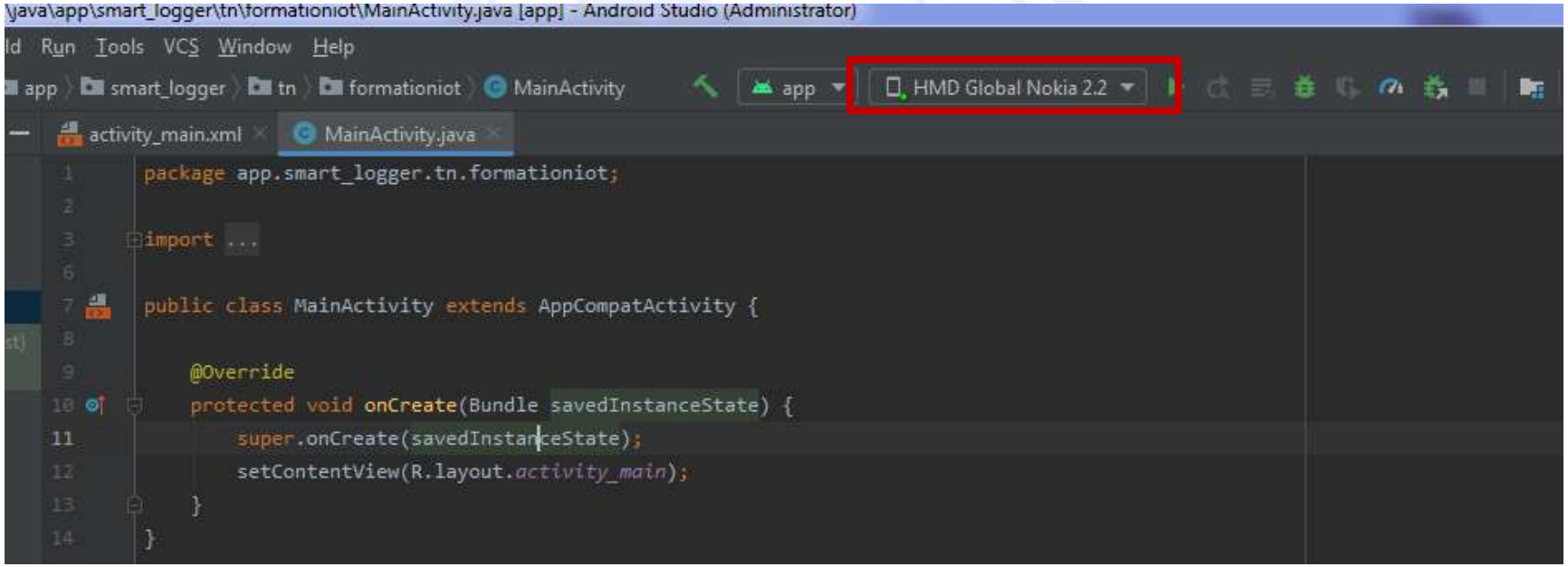
Outils Software

- Appuyiez successivement plusieurs fois sur le numéro de build jusqu'à que le système vous dit que la mode développeur est activée.
- Retournez au **système>Options pour les développeurs**, assurez vous que les Options pour développeur et le débogage USB sont activés.



Connectez votre Smartphone à votre PC a travers un câble USB, si un dialogue est apparu sur votre téléphone, cliquer sur « Toujours autoriser » puis « OK ».

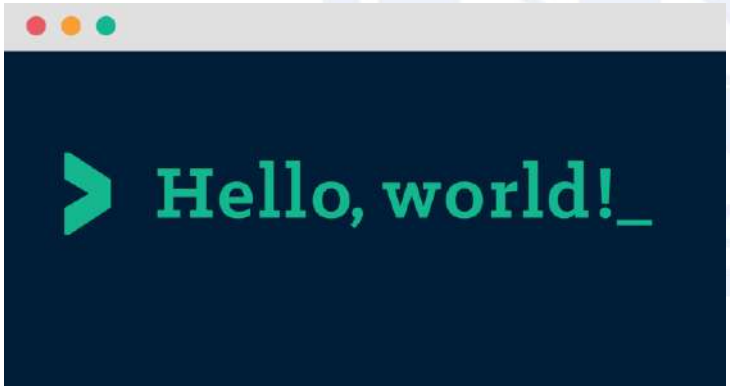
Le nom de votre Smartphone doit maintenant apparaitre sur Android Studio.
Cliquez sur « Run », l'icône vert juste au coté du nom.

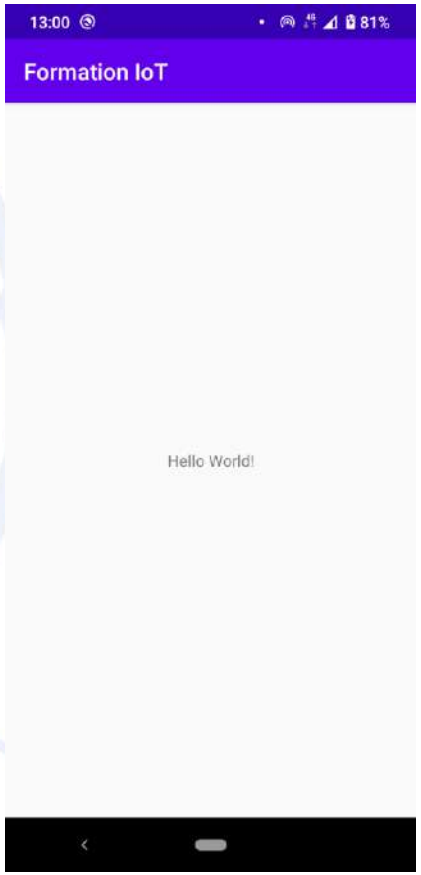


- Voici votre première application hello world!

Supposons qu'on veut contrôler une porte à distance via notre application, pour arriver à cet objectif nous allons ajouter un switch à l'interface.

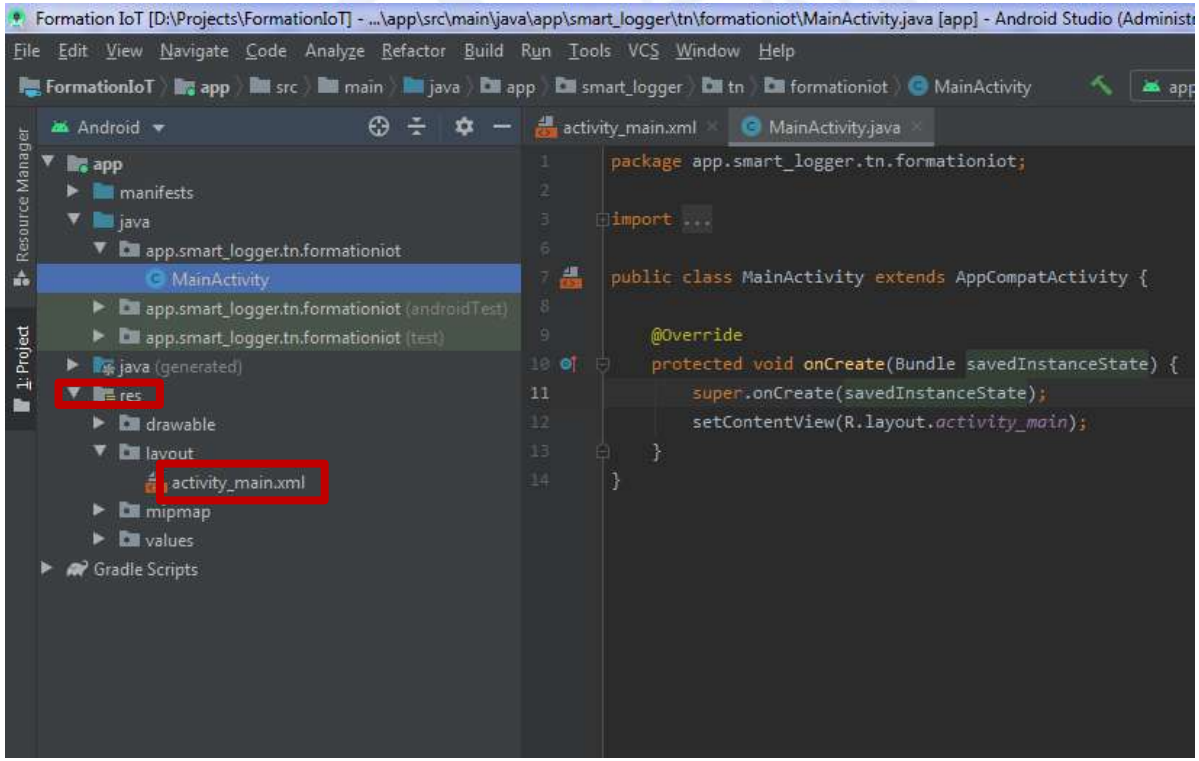
Si on active le switch, la porte concernée s'ouvre par contre si on le désactive la porte se ferme.



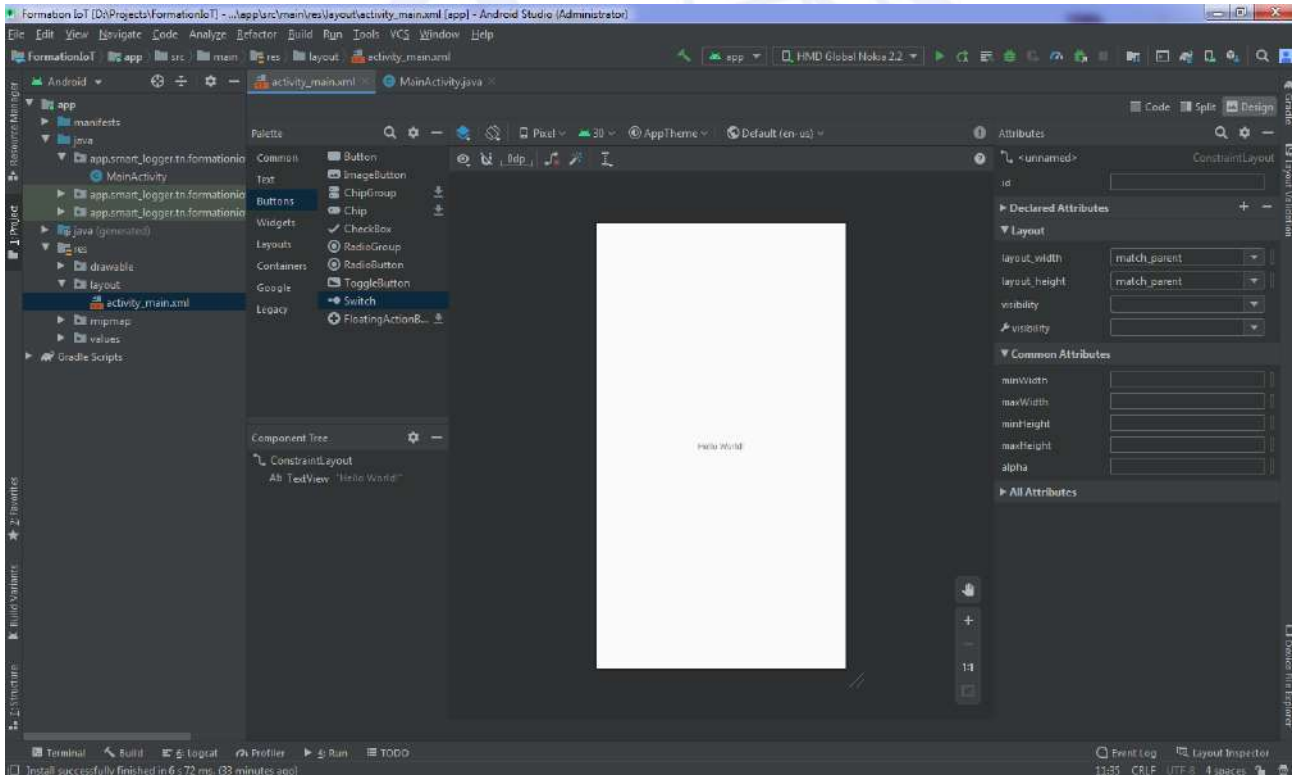


Outils Software

Pour ajouter un switch dans l'interface graphique de notre application, cliquer sur le dossier **res** dans l'arborescence de projet à gauche, puis **layout** et ensuite **activity_main.xml**

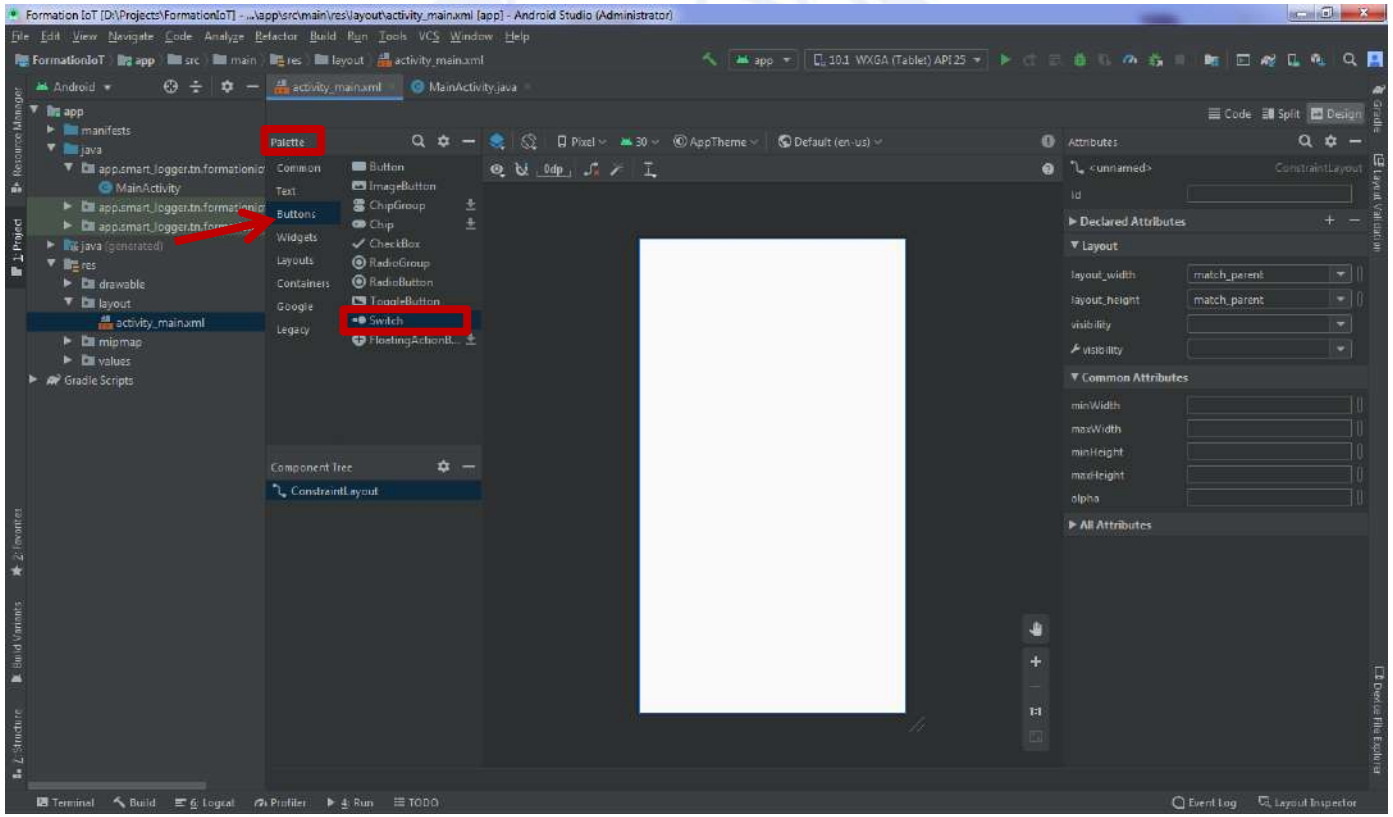


L'interface de ci-dessus est apparait, on remarque que c'est le même contenu que nous avons vu sur notre application tout à l'heure.



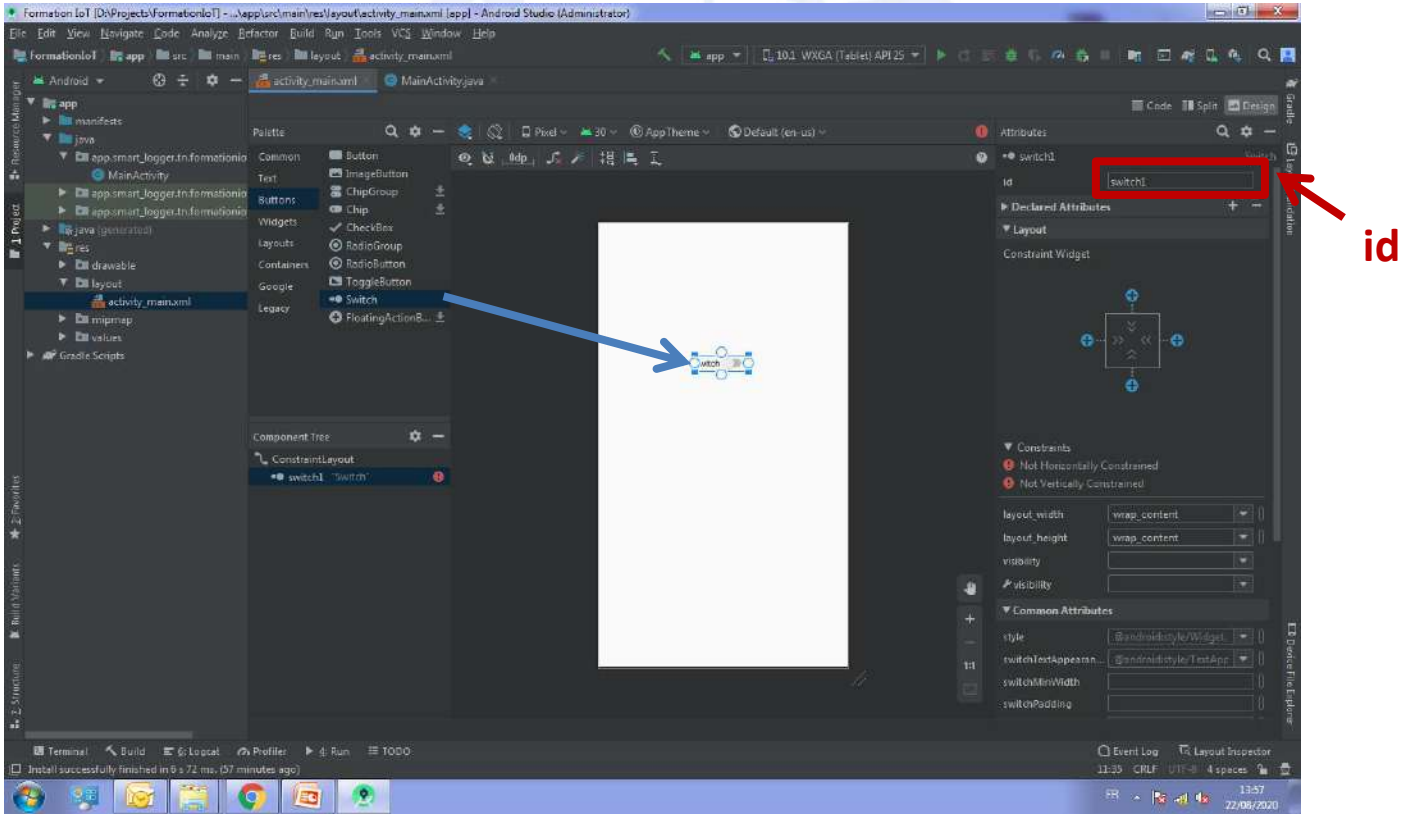
Outils Software

Pour ajouter un switch cliquez sur **Palette>Buttons>Switch**



Outils Software

Simplement, **glissez** le switch à l'interface de l'application, le switch est maintenant ajouté à l'interface, Veuillez noter l'**id** de notre switch.



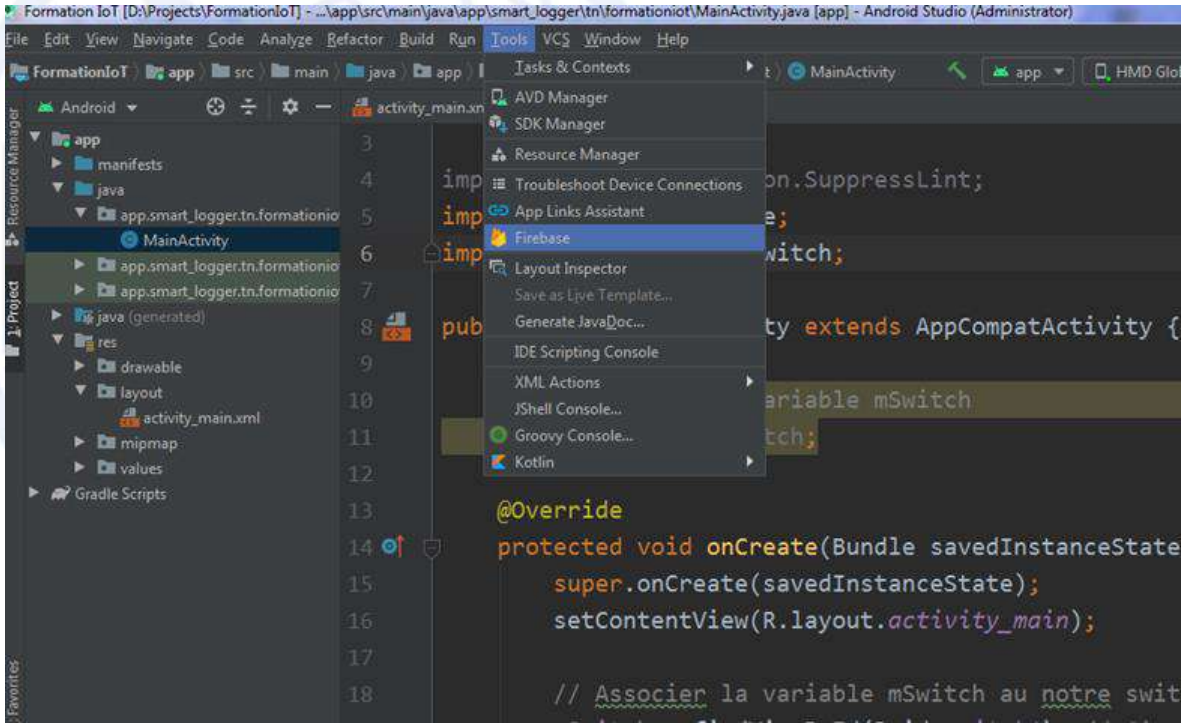
Pour que notre application connait les événements venant de switch, il faut créer une instance de switch dans le fichier MainActivity.java. le fichier doit sembler à l'image suivante

activity_main.xml | MainActivity.java

```java
package app.smart_logger.tn.formationiot;
import androidx.appcompat.app.AppCompatActivity;

import android.os.Bundle;
import android.widget.Switch;

public class MainActivity extends AppCompatActivity {

    // Instancier une variable mSwitch
    private Switch mSwitch;

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);

        // Associer la variable mSwitch au notre switch de l'interface graphique
        mSwitch = findViewById(R.id.switch1); // C'est l'id de notre switch vue précédemment!
    }
}
```

Cliquez sur **Tools>Firebase**

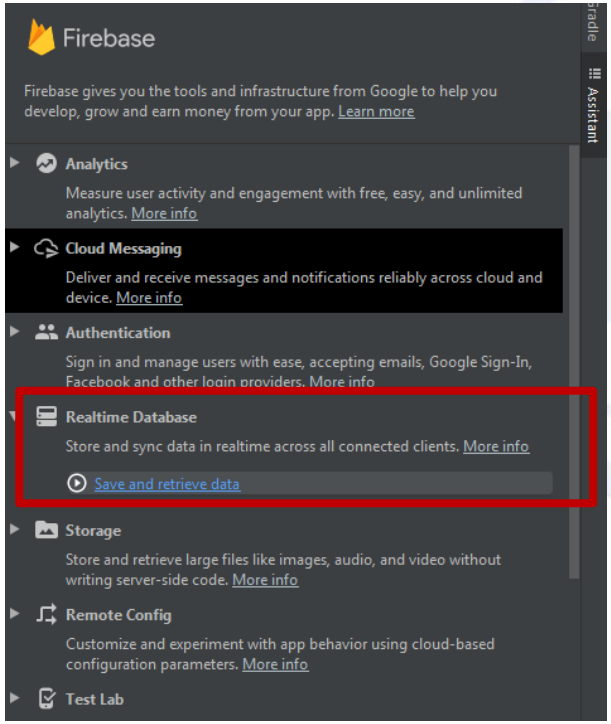
Maintenant, il faut associer notre projet Android au projet Firebase crée précédemment.
Android Studio fourni un outil qui facilite l'association de différentes services de Firebase.
Nous allons suivre les étapes suivantes pour utiliser la service Firebase Realtime Database dans notre projet Android

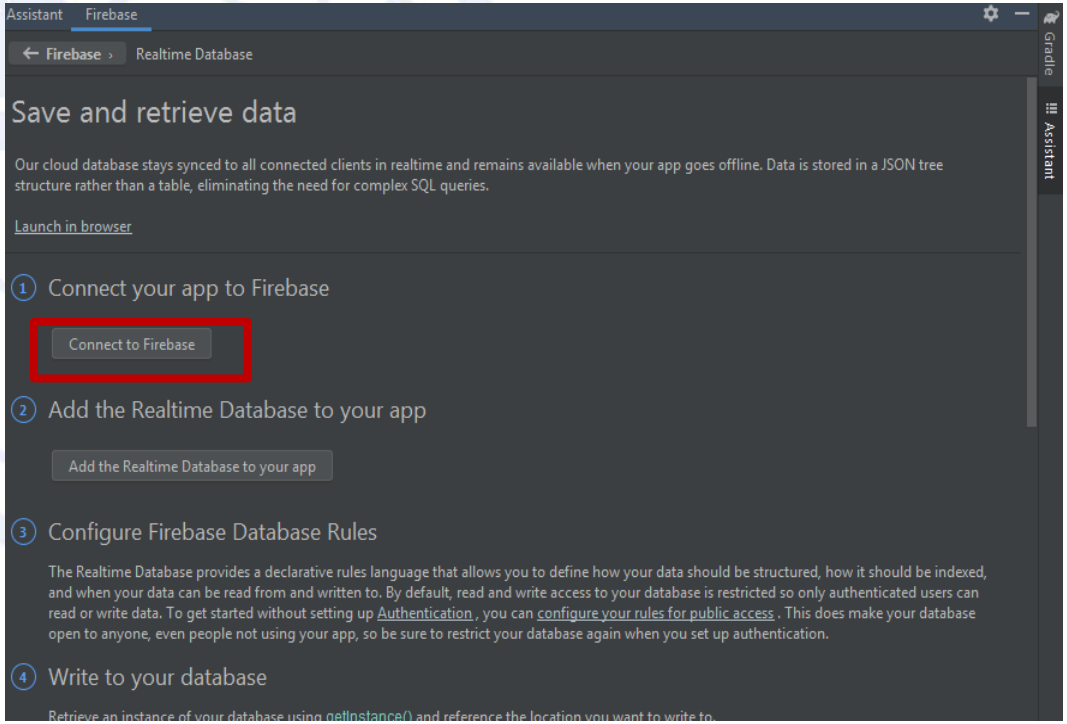


Outils Software

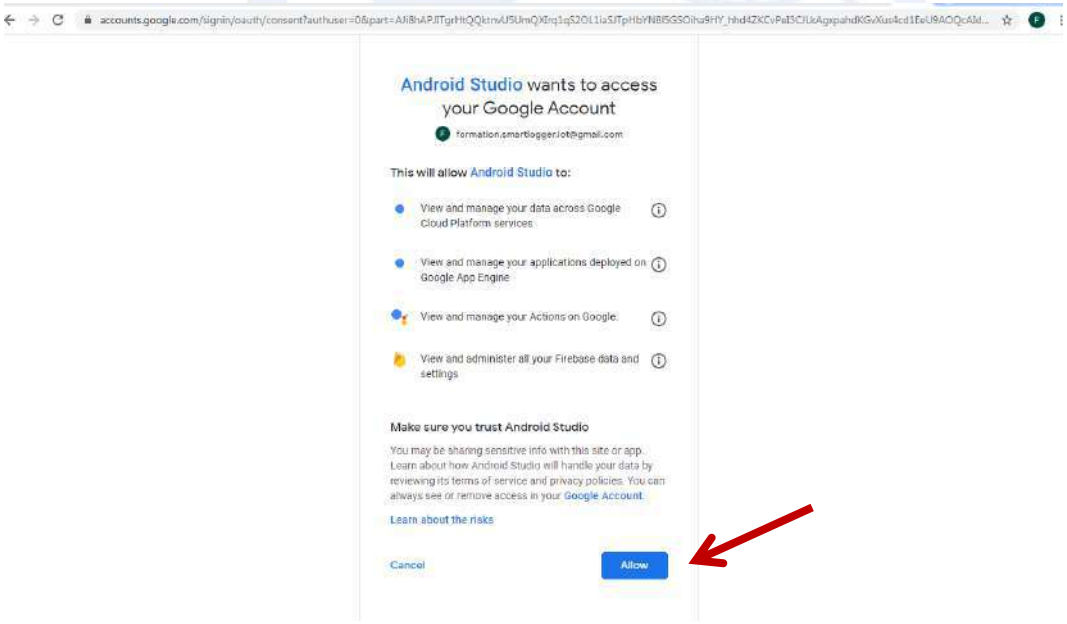
Choisir **Realtime Database>Save and retreive data**

Ensuite cliquer sur « Connect to Firebase »

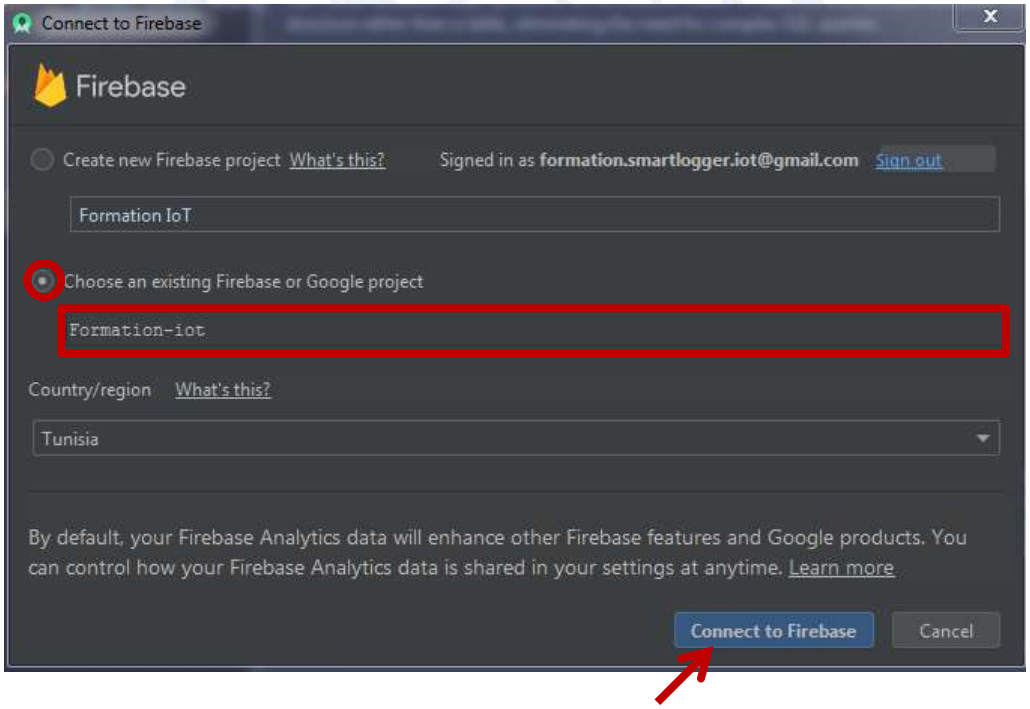




Votre navigateur va ce lancer, connectez vous au compte Google que vous avez utilisé lors du création du projet Firebase, puis cliquez sur autoriser.

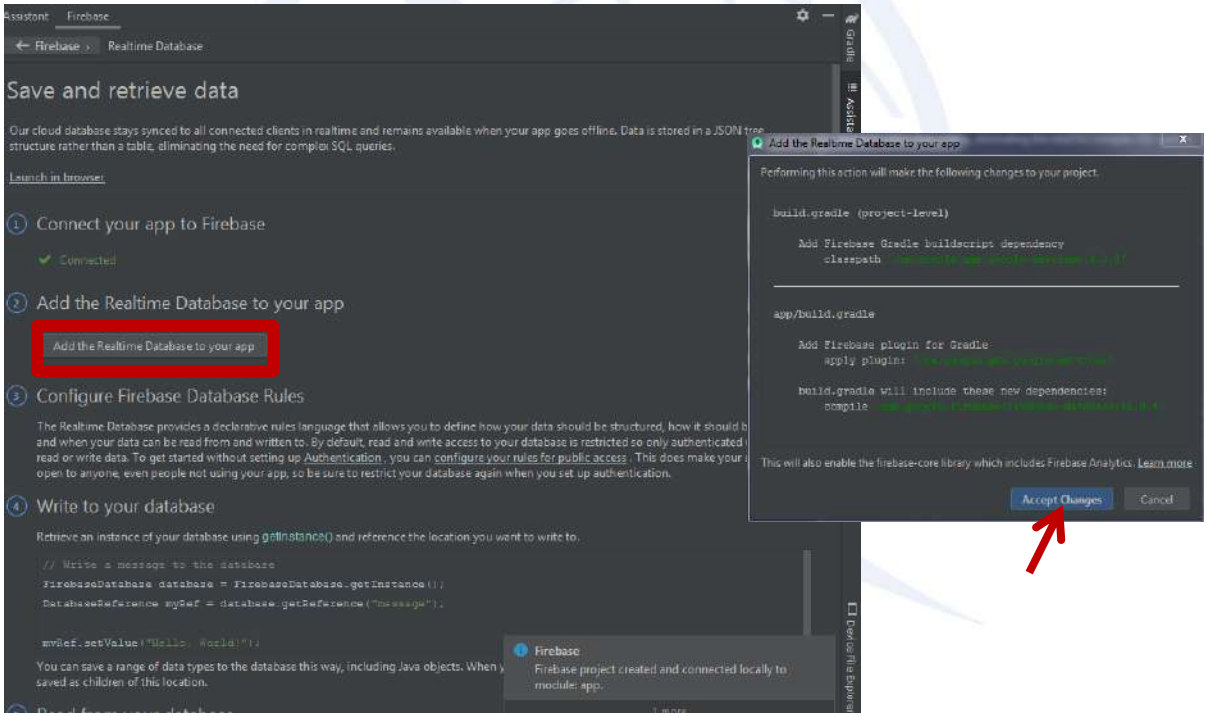


Revenons à Android Studio, et sélectionnez **Choose an existing Firebase on Google project** , choisir le projet et cliquez sur **Connect to Firebase**.

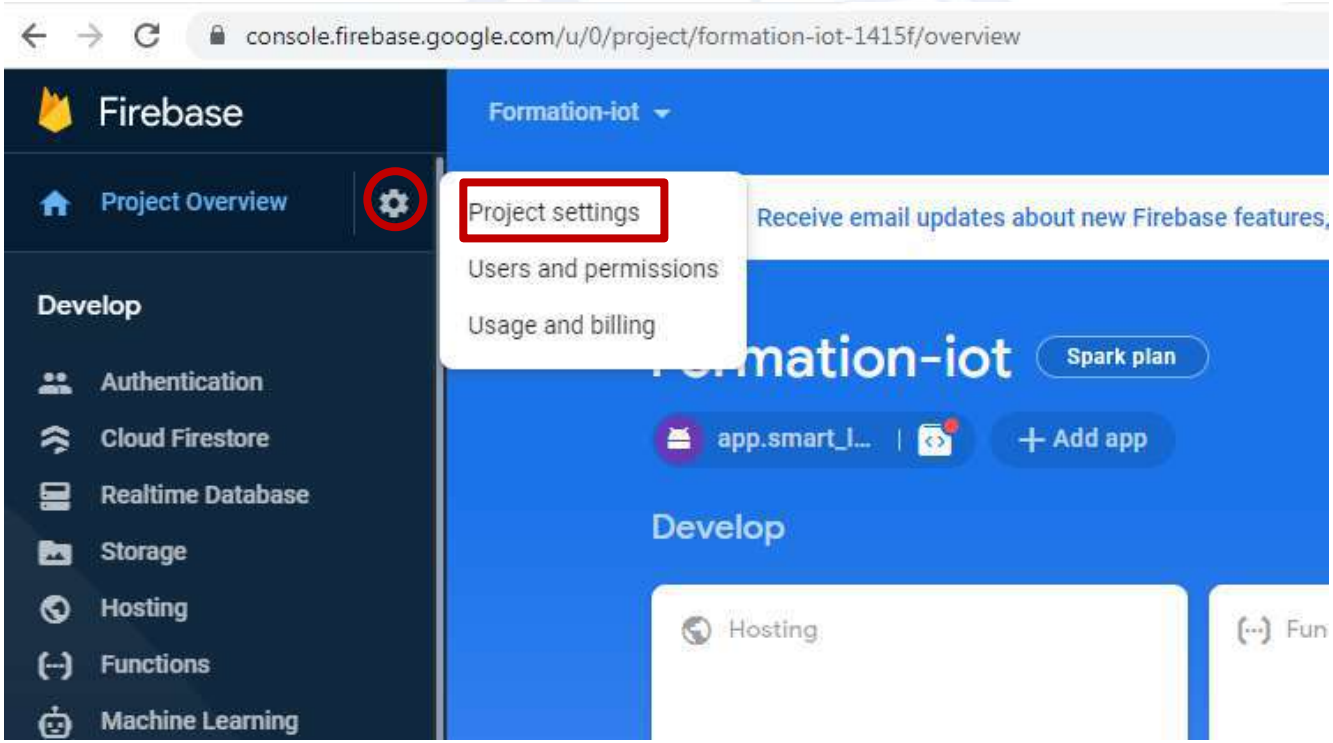


Outils Software

Cliquez sur **Add the Realtime Database to your app** et confirmez les changements dans le dialogue qui apparait.

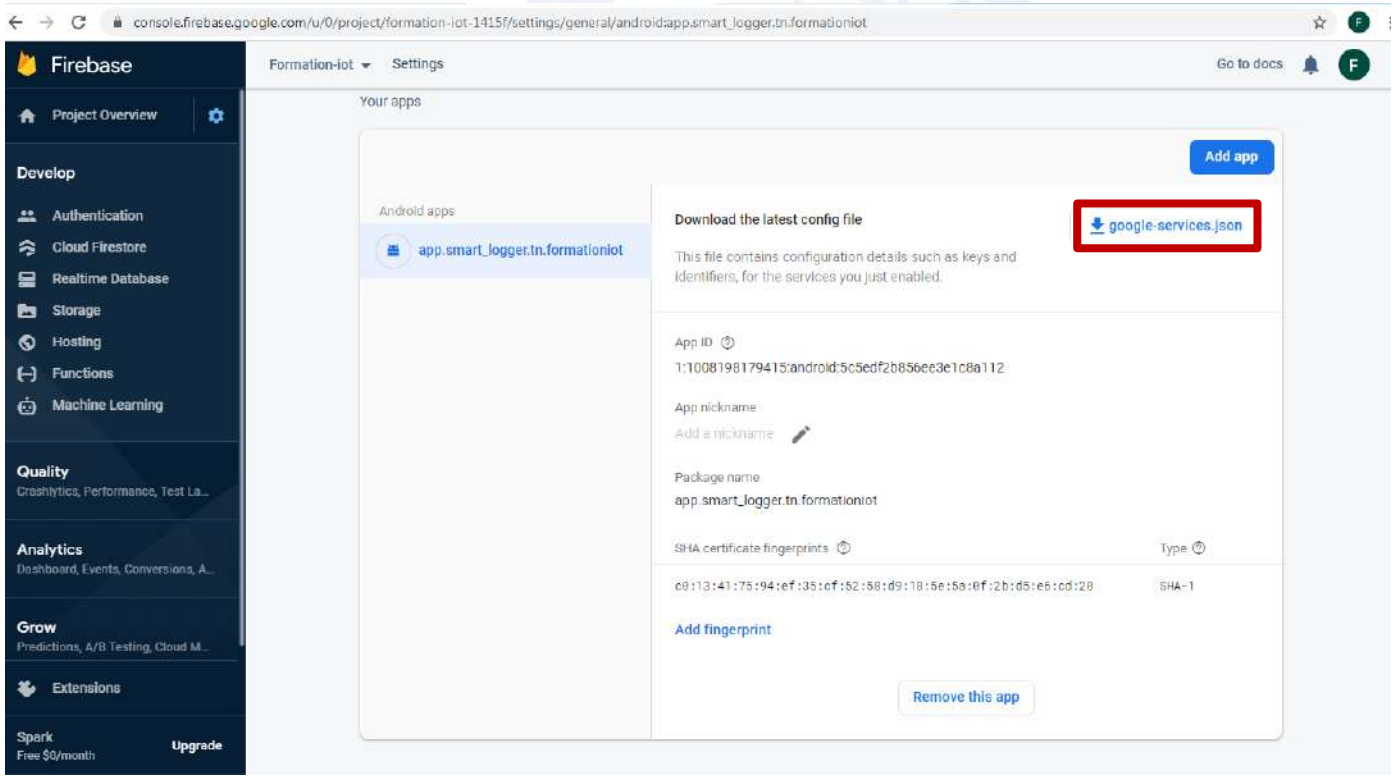


Revenons maintenant à Firebase console, cliquer sur « **Paramètres du projet**».

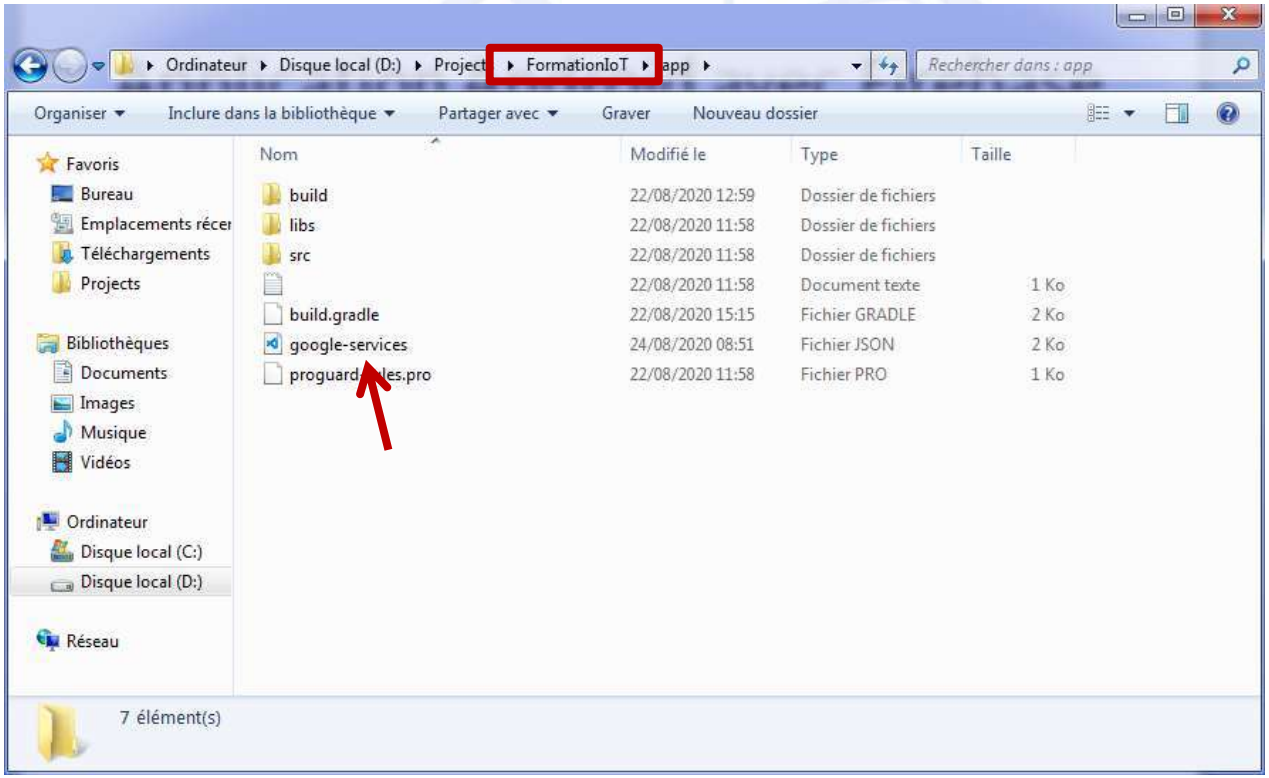


Outils Software

Cliquer sur « **google.services.json** » pour télécharger le fichier de configuration json de Firebase.



Copier le fichier google.services.json dans le dossier « **app** » de votre projet Android.



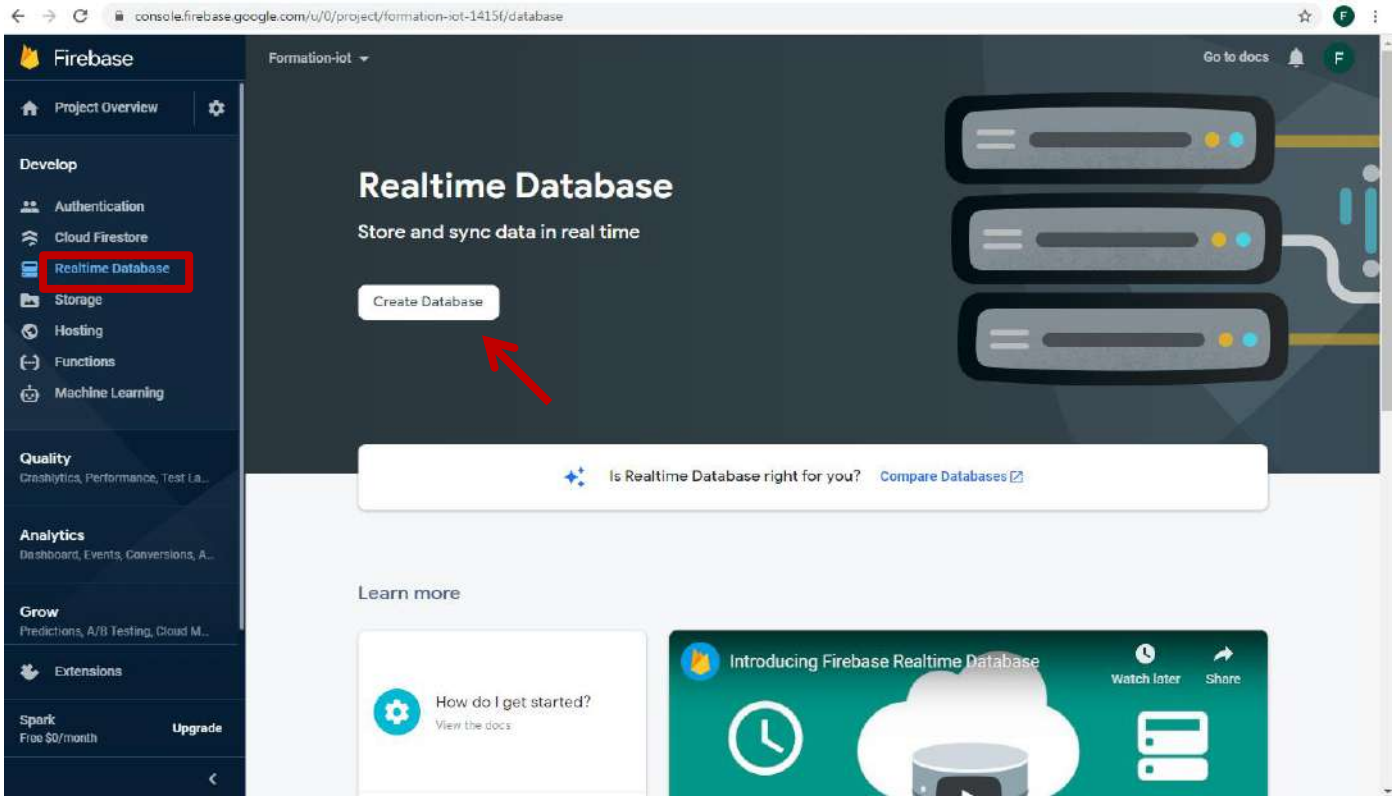
Le projet est maintenant associé à Firebase Realtime Database. Vous pouvez exécuter l'application sur votre téléphone pour vérifier qu'il n'y a pas des problèmes.

- Ajoutons une variable dans la base des données pour stocker la variable du porte.
- La porte a 2 états, soit ouverte, soit fermée donc on l'associe avec une variable booléenne:

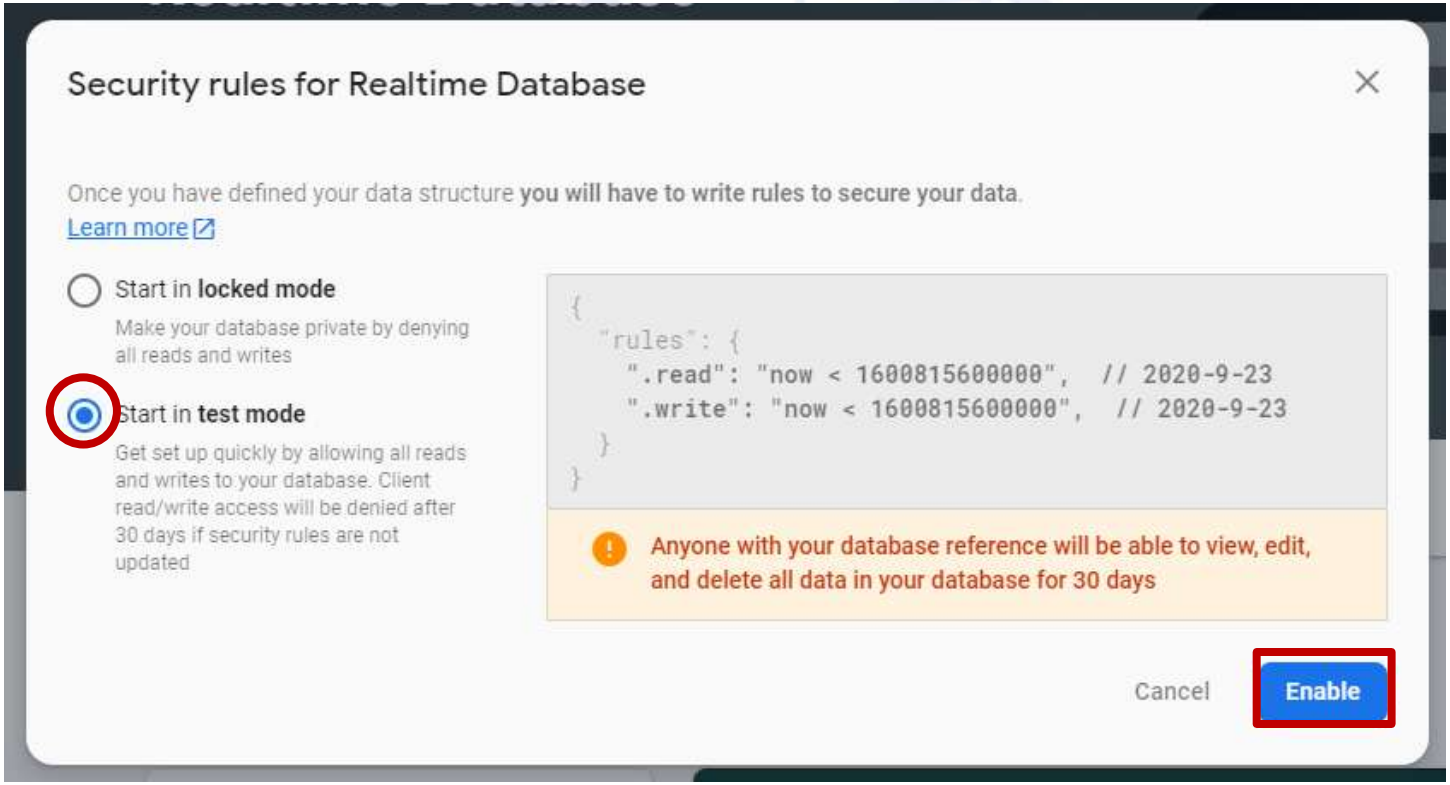
  true → porte ouverte

  false → porte fermée

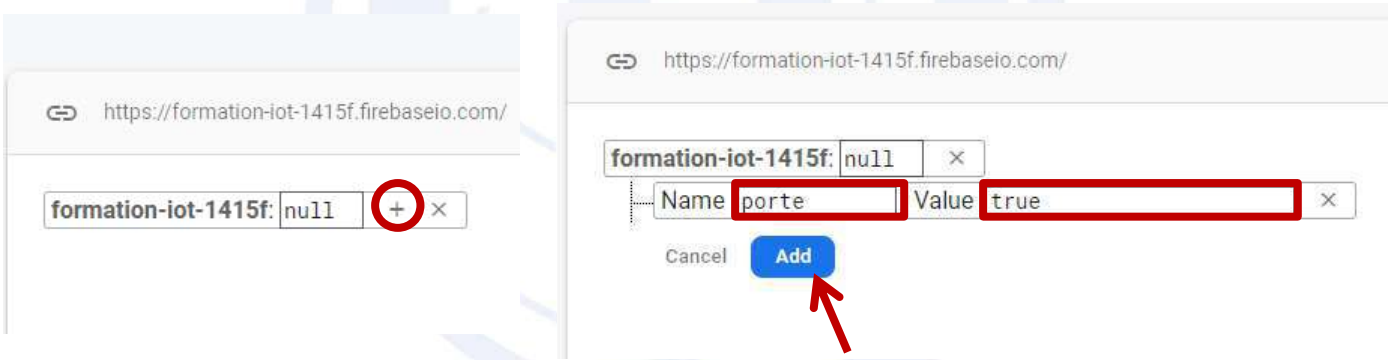
Dans la console de Firebase, choisir Realtime Database et cliquer sur Create Database.



Choisir l'option « test mode » et cliquer sur Enable



Pour créer une variable porte dans la base des données, cliquer sur « + », ensuite fournir le nom du variable (dans notre cas porte), attribuer une valeur booléene (true par exemple) et valider.



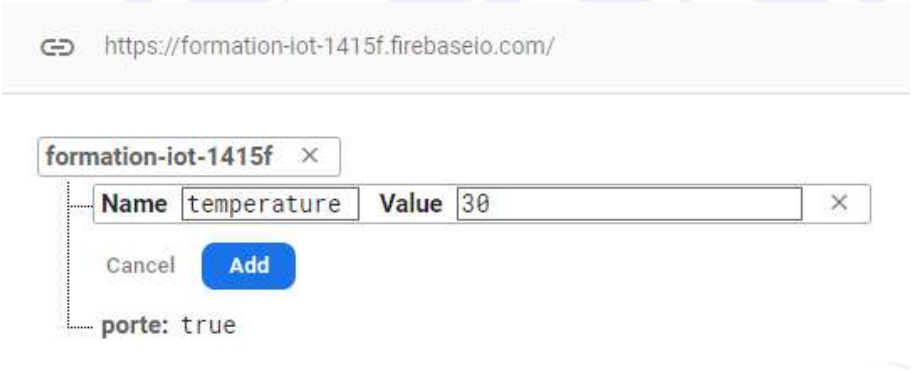
Initialiser l'état de switch selon la valeur de la variable porte stockée dans Firebase. Just à la fin de méthode Create dans le fichier MainActivity.java ajouter les lignes suivants:

```
// Initialiser le switch selon la variable porte stockée dans la base des données
FirebaseDatabase.getInstance().getReference( path: "porte")
        .addValueEventListener(new ValueEventListener() {
            @Override
            public void onDataChange(@NonNull DataSnapshot dataSnapshot) {

                mSwitch.setChecked((boolean) dataSnapshot.getValue());
            }

            @Override
            public void onCancelled(@NonNull DatabaseError databaseError) {

            }
        });
```

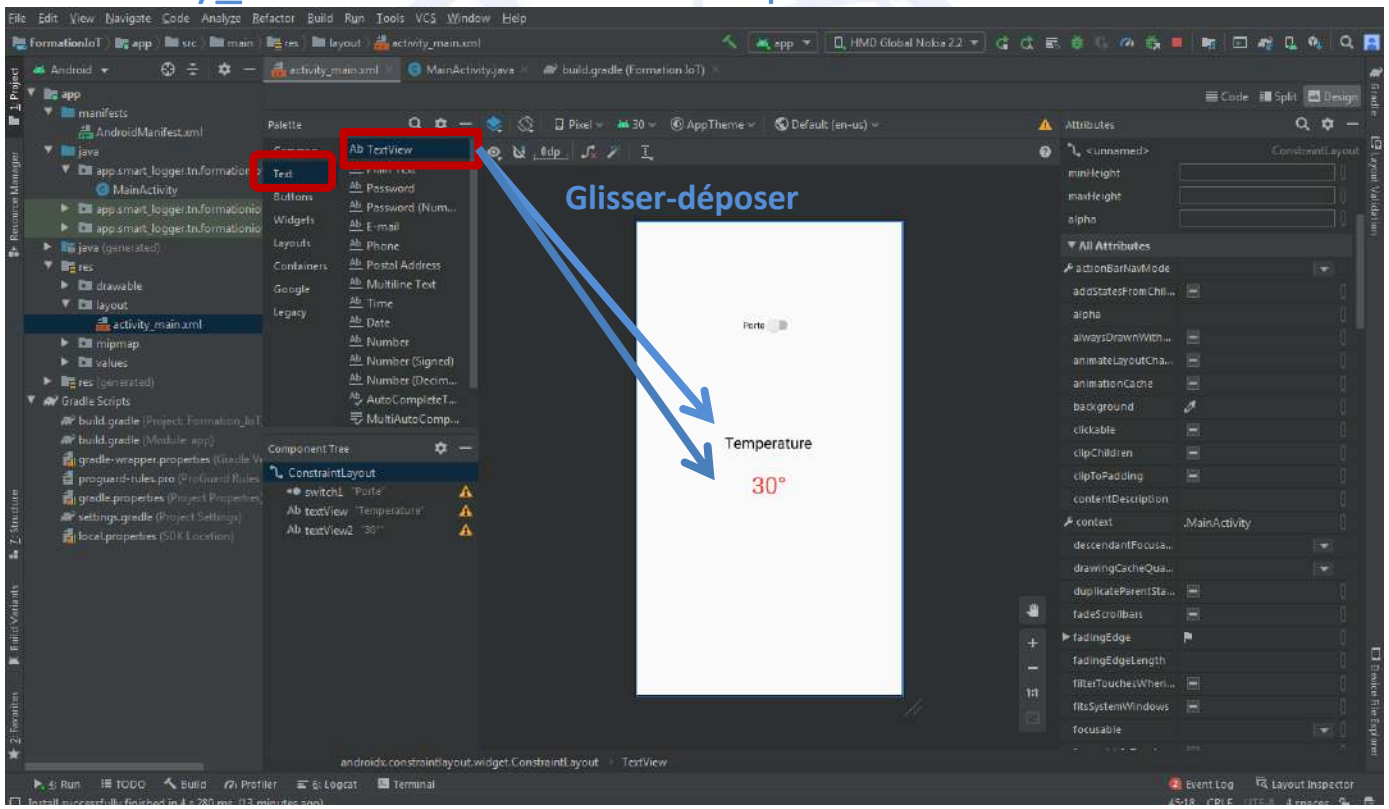
Maintenant, lire l'événement activer et désactiver du switch et l'enregistrer dans la base des données. Ajouter ces lignes après le code de l'étape précédente:

```
// Ecout sur les évenements du switch pour changer la variable porte
// dans la base des données en cas de changement d'état.
mSwitch.setOnCheckedChangeListener(new CompoundButton.OnCheckedChangeListener() {
    @Override
    public void onCheckedChanged(CompoundButton compoundButton, boolean b) {
        FirebaseDatabase.getInstance().getReference( path: "porte").setValue(b);
    }
});
```

- Exécutez votre application. Remarquez que tout changement effectué sur le switch se mémorise immédiatement dans la base des données et vice-versa
- Ajoutons une autre variable nommée température à notre base de donnée et attribuer une variable numérique quelconque.

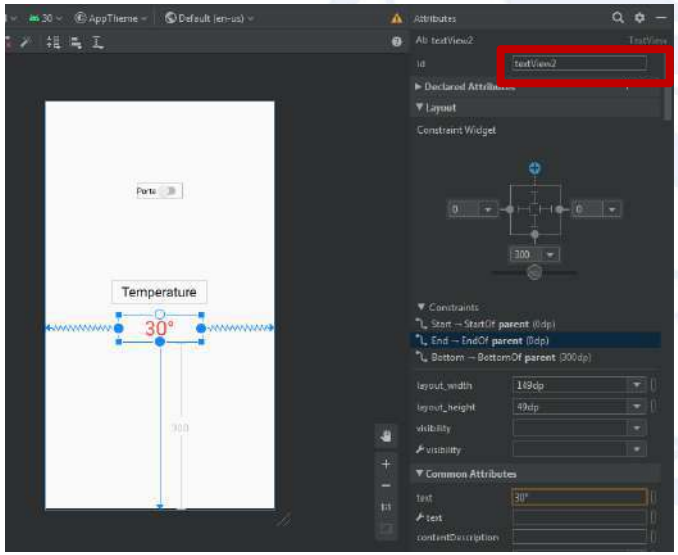


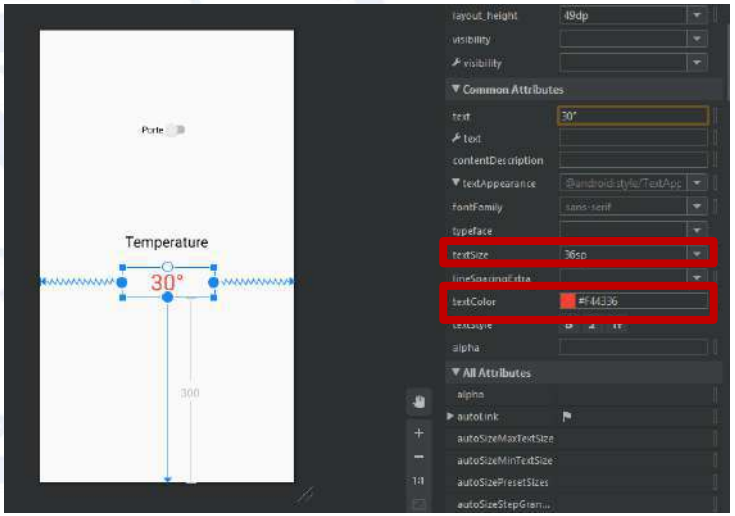
Ajouter deux « TextView » dans le fichier activity_main.xml: la labelle Température et sa valeur.



Outils Software

- Notez l'id de la valeur de la température.
- Changer la taille du texte et le couleur selon votre choix.





Instancier la variable température après la variable mSwitch

```
public class MainActivity extends AppCompatActivity {

    // Instancier une variable mSwitch
    private Switch mSwitch;

    // Instancier une variable temperature
    private TextView temperature;

    @Override
    protected void onCreate(Bundle savedInstanceState) {
```

Relier la variable temperature avec le TextView dans le layout (Interface graphique).

```
setContentView(R.layout.activity_main);

// Associer la variable mSwitch au switch de l'interface graphique
mSwitch = findViewById(R.id.switch1); // C'est l'id de notre switch vue précédemment!

// Associer la variable temperature au TextView de l'interface graphique
temperature = findViewById(R.id.textView2); // C'est l'id de notre TextView
```

Afficher la valeur de la température enregistrée dans Firebase en temps réel en ajoutant ces lignes à la fin de la méthode onCreate.

```
// Lire la valeur de la temperature stockée dans la base des données
// et l'afficher dans le TextView
FirebaseDatabase.getInstance().getReference( path: "temperature")
        .addValueEventListener(new ValueEventListener() {
            @Override
            public void onDataChange(@NonNull DataSnapshot dataSnapshot) {
                temperature.setText(dataSnapshot.getValue() + "°");
            }

            @Override
            public void onCancelled(@NonNull DatabaseError databaseError) {

            }
        });
```

Maintenant, si vous changez la température dans Firebase Realtime Database elle sera changé immédiatement sur l'interface de l'application!

Thank you!

PRIDA Track 5 (T5)

Villes intelligentes et applications IoT

28/08/2020

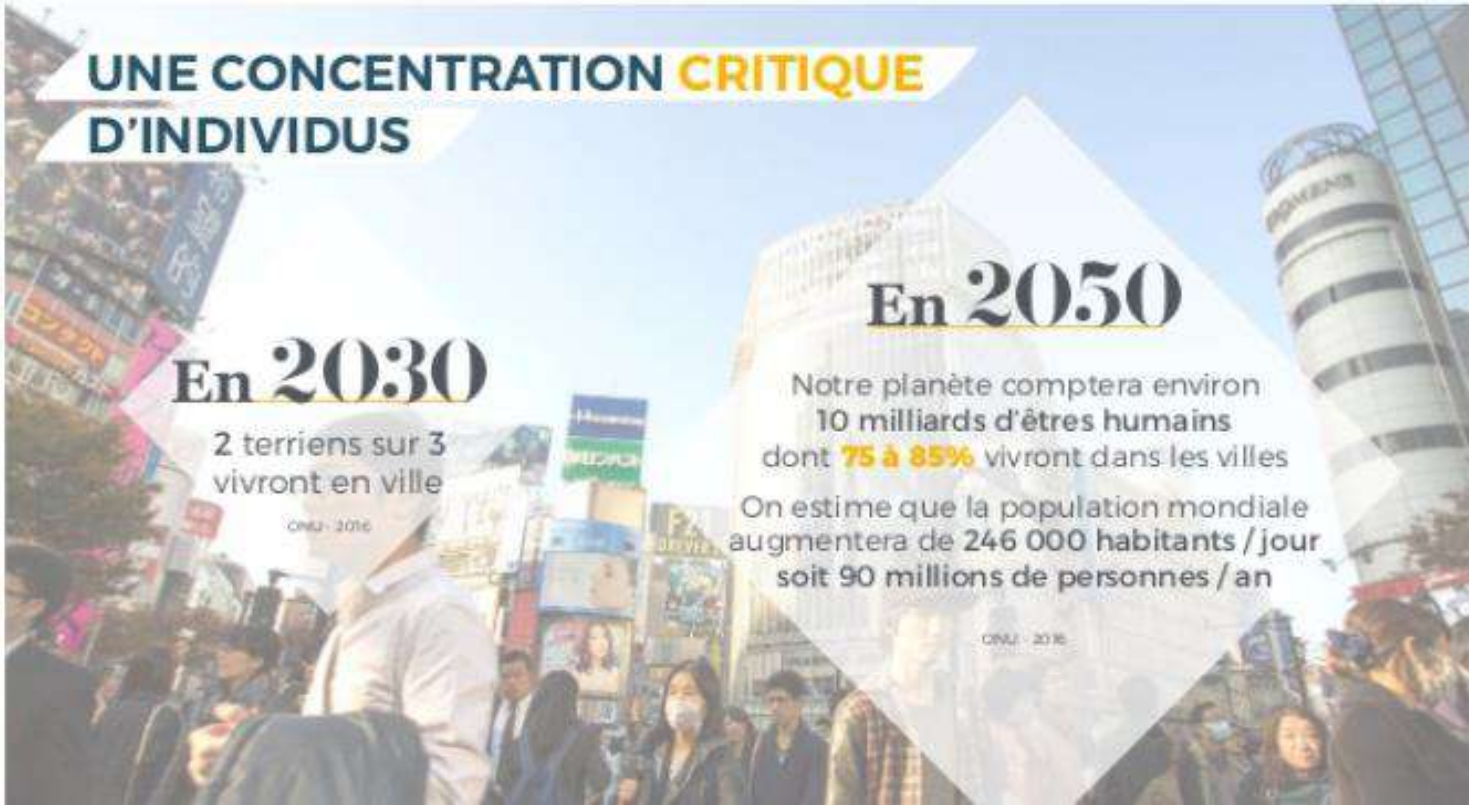
Partie 1 : Villes intelligentes

Agenda

- Pourquoi une ville intelligente?
- Définition de ville intelligente
- Visions et challenges
- Ecosystème et rôles des acteurs
- Technologies disruptives
- Modèles de gouvernance
- Chaine de valeur et modes de financement
- Sécurité
- Exemples

Défis globaux de la ville

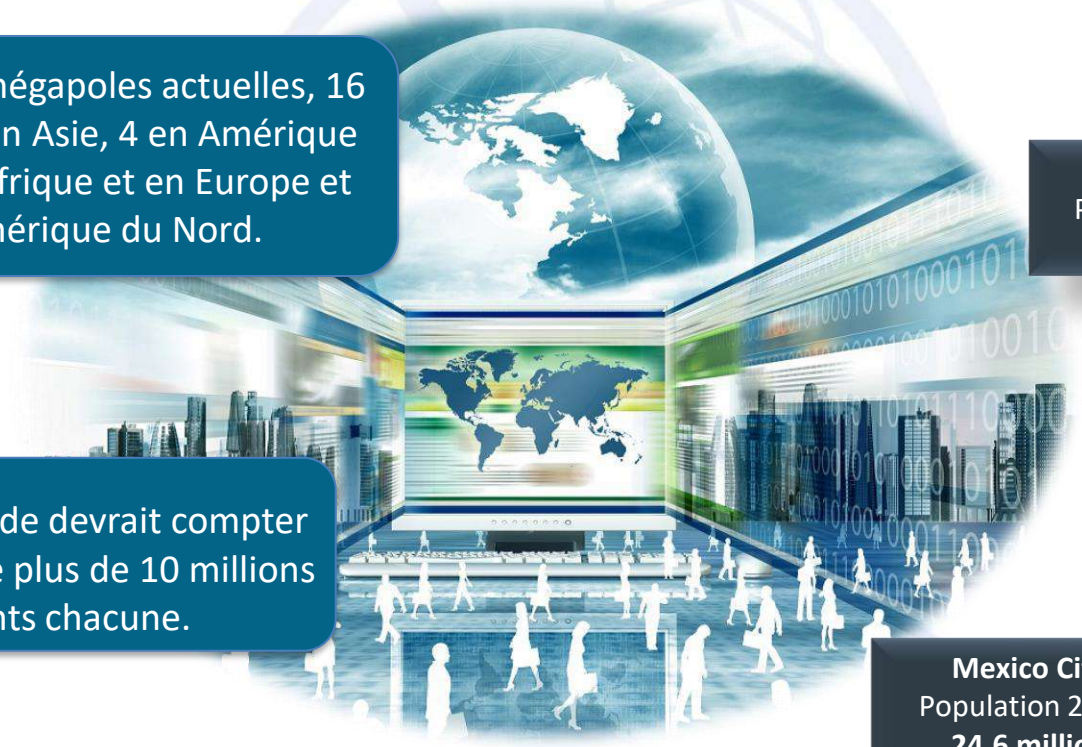
Augmentation de la population urbaine



Augmentation de la population urbaine

Parmi les 28 mégapoles actuelles, 16 sont situées en Asie, 4 en Amérique latine, 3 en Afrique et en Europe et 2 en Amérique du Nord.

En 2030, le monde devrait compter 41 mégapoles de plus de 10 millions d'habitants chacune.



Tokyo
Population 2030:
37 million

Delhi
Population 2030:
36 million

Mexico City
Population 2025:
24.6 million

Source: United Nations, Department of Economic and Social Affairs Statistics, Frost & Sullivan and other regional and country level statistics bureau

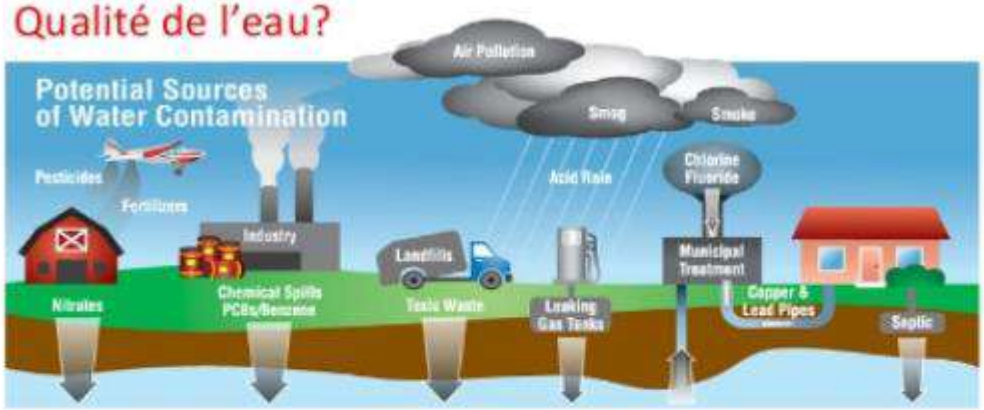
Défis de l’eau

La croissance de la population urbaine, ainsi que les exigences de l'industrie et de l'agriculture, exercent une immense pression sur les ressources en eau.

Près d'un milliard de personnes n'ont pas accès à l'eau potable

Défis de l'eau

Qualité de l'eau?



Les fuites:
20% dans le monde
50% dans certaines villes

Energie


LA CONSOMMATION CROISSANTE
D'ÉNERGIE
186%
La consommation énergétique mondiale a crû de 186 % en quarante ans
Rapport mondial des Nations Unies sur la mise en valeur des ressources en eau - 2014
10mds
Toutes les heures, 10 milliards d'e-mails sont envoyés, soit l'équivalent de 4000 aller-retours Paris/New-York en termes énergétiques
Reportage « Internet, la pollution cachée » 2013
Google
consomme autant d'énergie que la ville de Bordeaux pour faire fonctionner ses data centers
Reportage « Internet, la pollution cachée » 2013

Pollution


LE RÉCHAUFFEMENT CLIMATIQUE & LA POLLUTION ATMOSPHÉRIQUE
19cm
Depuis la fin du XIXe siècle, les océans se sont élevés de 19 centimètres. D'après le GIEC, leur niveau pourrait s'élever d'1 mètre d'ici à 2100 par rapport à la période 1986/2005
Groupe International des Experts sur le Climat (GIEC) - 2015
5 janv.
En 5 jours, Londres a franchi les limites annuelles de pollution atmosphérique
Station de surveillance de Brixton Road 2017
60%
Les émissions de carbone ont + que doublé depuis le début des années 1970 et représentent désormais 60% de notre empreinte écologique globale
Global Footprint Network 2016

Pollution


LA PRODUCTION EXCESSIVE DE DÉCHETS
3x
L'être humain jette 3 fois + de déchets dans l'océan qu'il ne pêche de poissons (alors que la surpêche fait des ravages)
150mns
Plus de 150 millions de tonnes de déchets plastiques flottent sur les océans & cette masse pourrait doubler d'ici 2050
Fondation Ellen MacArthur 2016
Si aucune mesure n'est prise pour lutter contre ce fléau, ce sera l'équivalent de 2 camions-poubelles jetés dans l'océan chaque minute en 2030 et 4 en 2050
Fondation Ellen MacArthur 2016

Défis de la gouvernance participative

Autres défis…

Alors quelles solutions pour ces défis?

La ville intelligente est un pas vers un meilleur cadre de vie pour les habitats et une meilleure durabilité pour la ville et pour la planète.

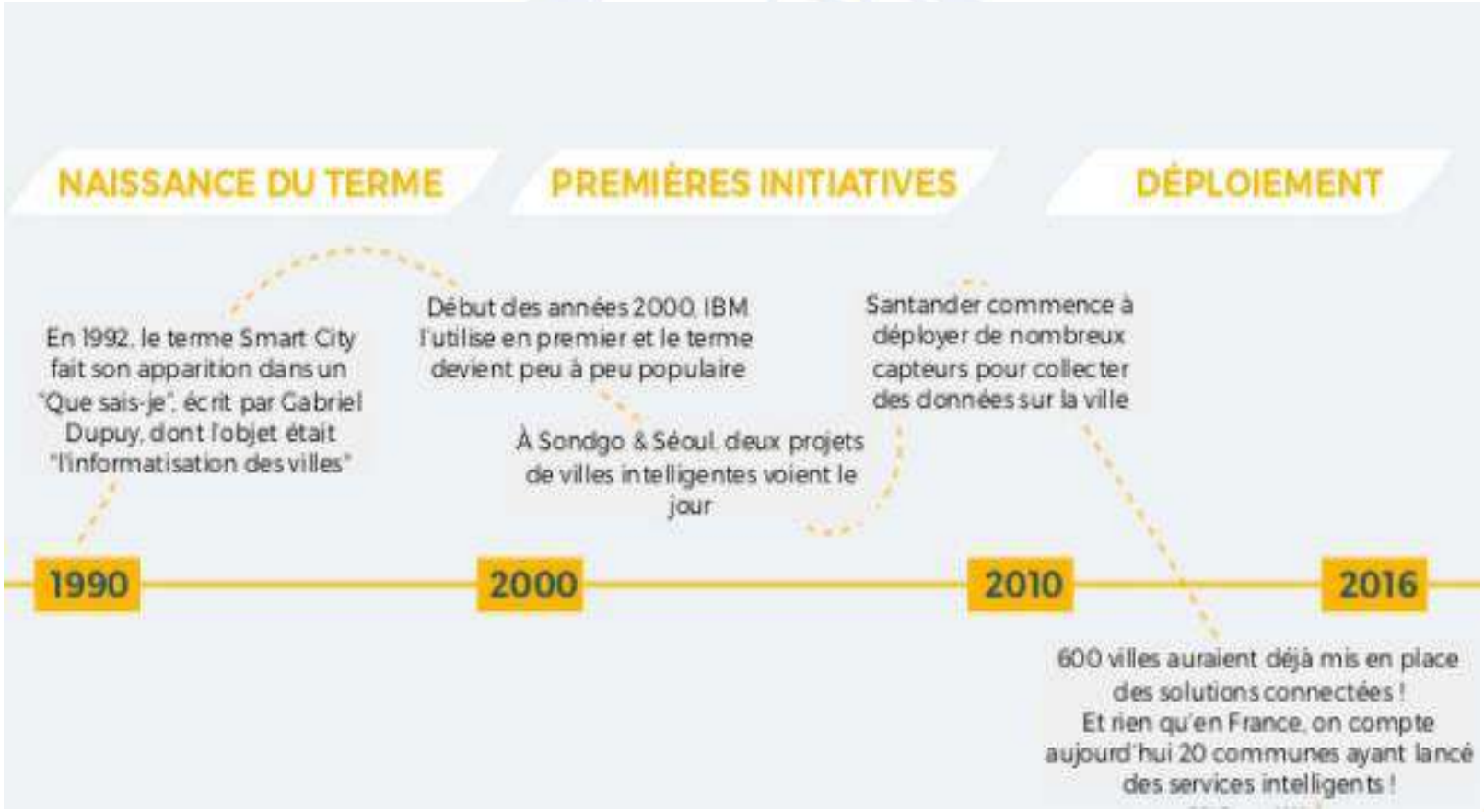
Quelques exemples de bénéfices apportés par les villes intelligentes

- Transport
  - Réduction de la congestion et de la pollution grâce à une utilisation optimale des infrastructures de transport (routes, parkings)
- Energie
  - Économies d'énergie grâce au suivi en temps réel de la consommation d'énergie.
  - Les appareils ménagers intelligents réagissent aux prix dynamiques de l'énergie pour ajuster la demande d'énergie à l'offre.
  - Transformation de déchets en énergie.
  - L'analyse des données fournies par les capteurs du réseau de distribution d'eau permet d'identifier les fuites et permet des réparations rapides.

Quelques exemples de bénéfices apportées par les villes intelligentes

- Sécurité et sureté de la ville
  - Réaction plus rapide aux menaces de la sécurité publique grâce à l'analyse en temps réel des données vidéo des capteurs et des caméras de surveillance.
- Santé
  - Un meilleur diagnostic et un traitement personnalisé grâce à l'utilisation de l'intelligence artificielle sur des volumes massifs de données patients.
  - Les personnes âgées peuvent être suives depuis leurs maisons grâce à la télémédecine et le robotique.
- Gouvernance
  - Des groupes dynamiques de citoyens s'organisent pour travailler ensemble sur des intérêts collectifs.
  - Co-création et prise de décision, nouvelles formes de démocratie numérique, et gouvernement participatif.
  - L'élaboration de politiques fondée sur les données.

Historique de la ville intelligente



La ville intelligente en chiffres

Définition - UIT

“Une ville intelligente et durable est une ville innovante qui utilise les technologies de de la communication et de l’information (TIC) et d'autres moyens pour améliorer la qualité de la vie, l'efficacité des opérations urbaines et des services, et la compétitivité, tout en veillant à répondre aux besoins des générations présentes et futures en ce qui concerne les aspects économiques, sociaux et environnementaux".

Qu’est ce qu’une ville intelligente?

- Qu’est ce qu’une ville intelligente?
  - Les villes intelligentes sont des espaces urbains qui utilisent les technologies de l'information et de la communication (TIC) pour fournir et transférer des informations afin de gérer efficacement les biens et les ressources et de fournir de meilleurs services aux citoyens de la ville.

- Quelles sont ses caractéristiques?
  - Infrastructures intelligentes (compétitivité)
  - Individus intelligents (capital social et humain)
  - Gouvernance intelligente (participation)
  - Mobilité intelligente (transports et TIC)
  - Environnement intelligent (ressources naturelles)
  - Mode de vie intelligent (qualité de vie)
  - Services intelligents (fiabilité)
  - Connectivité intelligente (prix abordable)
  - Sécurité intelligente (sureté)

Dimensions d'une ville intelligente

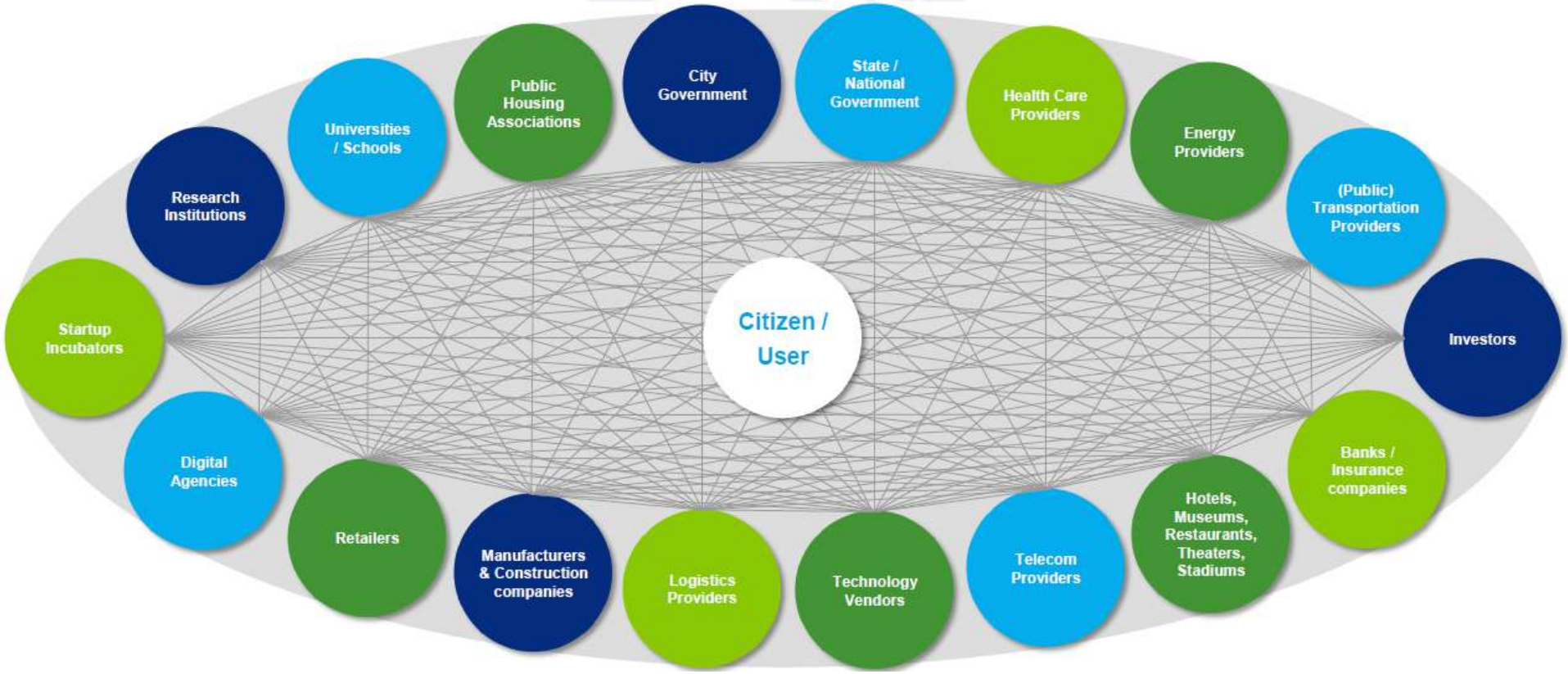
Infrastructures intelligentes (compétitivité)	Individus intelligents (capital social et humain)	Gouvernance intelligente (participation)
• Sûre et innovante • Disponibilité de l'infrastructure des TIC • Productivité • Capacité de transformation	• Niveau de qualification • Flexibilité • Créativité • Compétitivité • Ouverture d'esprit • Participation à la vie publique	• Participation à la prise de décision • Gouvernance transparente • Services publics et sociaux
Mobilité intelligente (transports et TIC)	**Environnement intelligent (ressources naturelles)**	**Mode de vie intelligent (qualité de vie)**
• Accessibilité locale • Disponibilité de l'infrastructure des TIC • Un système de transport durable, sûr et innovant	• Gestion durable des ressources • Protection de l'environnement	• Amélioration des conditions sanitaires • Équipements éducatifs • Équipements culturels

Dimensions d’une ville intelligente

Services intelligents (fiabilité)	Sécurité intelligente (sureté)	Connectivité intelligente (prix abordable)
• Disponibilité des services • Optimisation de la performance des ressources • Renseignement en temps réel • Prévention de la perte d'utilité	• Sécurité des femmes, des enfants et des touristes dans la ville	• Participation à la prise de décision • Disponibilité des services en ligne en tout endroit de la ville • Accessibilité locale

Technologies de rupture et d'innovations sociales

Cartographie des acteurs de la ville intelligente



Ecosystème de la ville intelligente

- L’écosystème de la ville intelligente est complexe en raison de la multiplicité des parties prenantes impliquées:
  - le maire, le conseil municipal, les municipalités de la ville, l'autorité des services publics, les prestataires de services, etc.
  - Les investisseurs
  - Les citoyens
- Une ville intelligente est le résultat des efforts de nombreuses parties prenantes, travaillant ensemble sous différentes formes de partenariat.
- Le citoyen/utilisateur est au centre de la carte, indiquant que les villes intelligentes qui réussissent sont toujours centrées sur l'utilisateur.

Rôle du gouvernement

- Définit une vision claire de la ville à construire, la stratégie pour y parvenir ainsi que les plans d'actions et d'investissements associés.
- Crée ou adapte des lois et des réglementations pour permettre de nouveaux modèles économiques tout en protégeant les intérêts des citoyens et des utilisateurs de la ville.
- Fédérer les acteurs de l'écosystème de la ville intelligente pour proposer de nouvelles solutions créatives et des modèles économiques innovants.
- Stimuler le développement des solutions innovantes en agissant en tant que client de lancement.
- Sécuriser les infrastructures de transport, les réseaux énergétiques et les réseaux de communication et veiller à prendre les mesures nécessaires pour rendre ces infrastructures résilientes et sûres.
- Créez un environnement favorable à l'innovation; par exemple en fournissant des «données ouvertes» et en soutenant le développement des startups.

Rôle du citoyen

- Le citoyen est au cœur de la ville intelligente. Il s'engage avec le gouvernement de la ville dans rôles différents:
  - Il paye les taxes et s'attend à ce que le gouvernement dépense l'argent des impôts à bon escient.
  - Le citoyen en tant que partenaire s'attend à être impliqué dans le processus d'élaboration de la politique et des choix judicieux en matière d'aménagement du territoire, de développement économique, de services sociaux et d'éducation.
  - Le citoyen en tant qu'électeur s'attend à être représenté par des politiciens élus, qui ont une vision claire et tiennent leurs promesses.
  - Le citoyen en tant que résident local s'attend à ce que son milieu de vie ait une certaine qualité: propre, écologique, et accessible.
  - Le citoyen en tant que résident s’attend à ce que sa ville soit sécurisée et résilente.

Capacités d'une ville intelligente

- Selon Deloitte, la construction d'une ville intelligente nécessite une stratégie claire et une maturité dans 7 dimensions:
  - Vision et stratégie
  - Partenariat Public-privé
  - Data
  - Technologie
  - Compétences
  - Innovation
  - Attractivité

Capacités d’une ville intelligente
Vision et stratégie

- Les villes intelligentes devraient avoir une vision claire de ce qu'elles veulent être et une stratégie pour réaliser cette ambition.
- Chaque ville a ses propres forces, défis et opportunités.
- Une ville intelligente exploite la puissance de la technologie et des innovations sociales pour accroître les forces existantes, pour résoudre les défis persistants et pour créer de nouvelles opportunités.
- Avoir une vision claire permet à une ville de concentrer son énergie et ses ressources sur ce qui apporte le plus de valeur à la ville, non seulement à court terme mais aussi à long terme.

Capacités d'une ville intelligente
Vision et stratégie

- Le développement des villes intelligentes est souvent motivé par trois objectifs stratégiques:
  - Sociétale: l'amélioration de la qualité de vie du citoyen et son bien être.
  - Economique: la croissance économique et l'attractivité du pays.
  - Environnementale : la protection de l'environnement.

Source: https://ant.cerema.fr/sites/ant/files/fichiers/2018/09/rapport_cgdd_villes_intelligentes_smart_agiles_-_copie.pdf

Capacités d'une ville intelligente

- Données - Une vraie ville intelligente émerge lorsque les données sont combinées à partir de plusieurs sources.
- Aptitudes et compétences - L'utilisation de technologies de rupture pour l'innovation nécessite de nouvelles aptitudes et compétences dans la ville, particulièrement dans le «data scientist» qui a été nommé comme le métier du 21e siècle.
- Ouverture à l'innovation et aux nouvelles idées - Réaliser une ville intelligente exige l'ouverture aux nouvelles idées créatives, la volonté d'expérimenter et prendre des risques calculés. Cela nécessite d'essayer de nouveaux types de collaboration entre différents départements du gouvernement et avec des parties prenantes extérieures au gouvernement.

Capacités d'une ville intelligente

- Attractivité des investisseurs et des talents - les villes doivent avoir une politique active pour attirer les investisseurs et les entreprises. Ils doivent aussi créer un climat dans lequel les startups peuvent se développer.
- Écosystèmes privé-public - Les villes intelligentes nécessitent des écosystèmes public-privé pour co-créer des solutions intelligentes et créatives.
- Projets et solutions - Innovations technologiques doivent être combinées avec des innovations sociales pour créer solutions. Des exemples de telles innovations sociales sont: la co-création et l'économie du partage

Stratégie de développement d'une ville intelligente

01 **Stratégie Institutionelle**

Au niveau national, un comité national de coordination des villes intelligentes peut être formé sous la forme d'un organe à vocation spécifique (SPV) au niveau de la ville.

02 **Stratégie de financement (Financing & Funding)**

Options traditionnelles - Financement par fonds propres, instruments de dette, Financement Mezzanine et Financement Public

Options non traditionnelles - Obligations Intelligentes, Actionnariat Dispersé, Financement participatif, Partenariat public-privé (PPP)

03 **Stratégie de Programmes & Projets**

Justification commerciale continue, Apprentissage par l'expérience, Rôles et responsabilités définis, Gestion par étapes & Exception, Focus sur les produits et Environnement de projet sur mesure

04 **Plan d'actions et plan d'investissments associé**

05 **Stratégie de management du changement**

Engagement avec les communautés locales, Engagement avec le secteur privé, Focus sur les femmes & jeunes, Pratique éthique, Image, Crédibilité & positionnement

Source: PWC Stratégie de développement de villes intelligentes, 2020

Stratégie institutionnelle

- Le Programme Ville Intelligente a besoin d'une structure institutionnelle et de gouvernance pour équilibrer les approches de gouvernance à la fois descendantes (bottom-up) et ascendantes (top-down).

- Il est important de gérer un bon équilibre de gouvernance au niveau des communes et au niveau national afin de briser les cloisonnements entre les différents services gouvernementaux et de tirer profit de la synergie entre les différentes parties prenantes (telles que les universités, le secteur privé, la société civile et les gouvernements locaux et municipaux).

  - Exemple : création d'un Comité National de Coordination des Villes Intelligentes qui a pour surmonter les barrières et les obstacles et de faire en sorte que les succès puissent être assimilés et reproduits.

Stratégie de financement

- Les projets de villes intelligentes nécessiteront des investissements à long terme pour le développement des infrastructures et des services basés sur les technologies de l'information.
- Il est peu probable que les gouvernements municipaux aient les ressources nécessaires pour financer et gérer les projets de villes intelligentes de manière indépendante.
- Il est donc de la responsabilité du gouvernement national d'assurer un flux de revenus substantiel et dédié aux projets de villes intelligentes, car ces projets créeront des infrastructures pour des résultats d'intérêt public.

Stratégie de financement

- Distinguer entre les termes :
  - « Financing » fait référence à l'étalement dans le temps des coûts impliqués.
  - « Funding » concerne la manière dont les coûts d'un projet seront remboursés
- Les sources de financing comprennent les banques, les obligations, les fonds de pension, les banques de développement, les prises de participation et le financement des fournisseurs.
- Les sources de funding comprennent les impôts fonciers, les taux d'activité, les péages et les droits d'utilisation, la cession des actifs, les allocations budgétaires et les subventions.

Stratégie de financement

Financement en fonds propres

Générer des fonds en émettant des titres en échange de liquidités aux institutions financières ou en accédant directement au marché

Instruments de dettes

Soit par une dette garantie par la mise en gage d'un collatéral, soit par l'obtention d'une dette sur le marché à un taux d'intérêt plus élevé s'il n'y a pas d'accord approprié avec les villes.

Dette Subordonnée et Financement Mezzanine

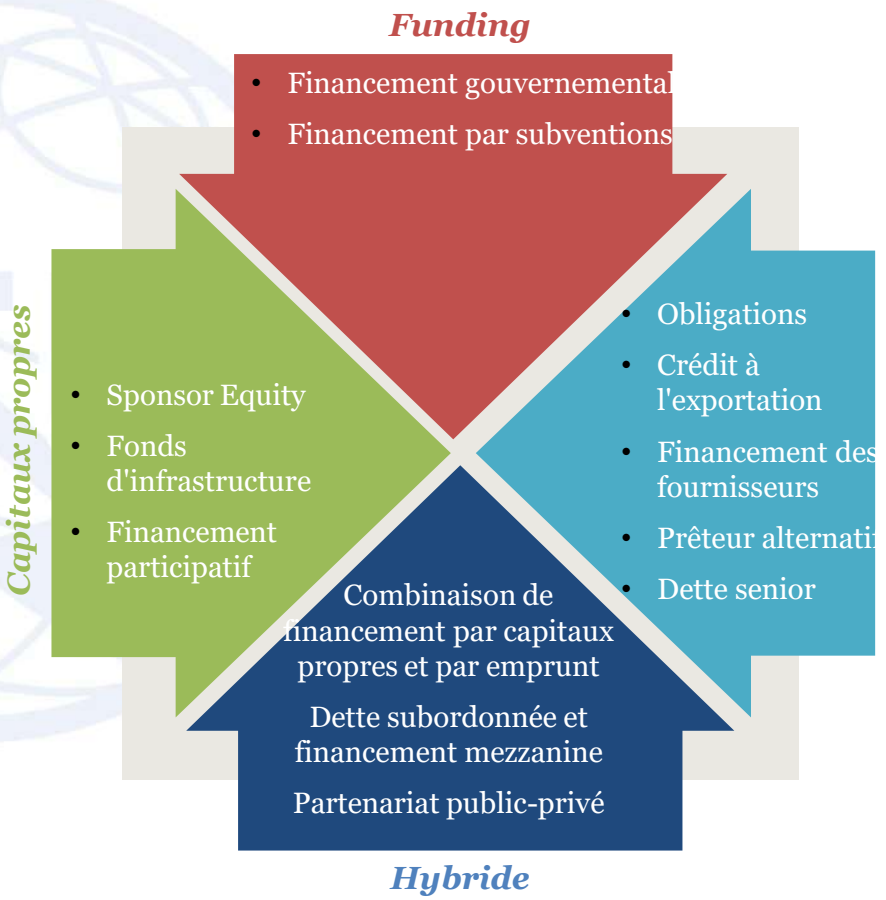
La dette subordonnée se situe à mi-chemin entre les instruments de fonds propres et de dette senior en termes de risque.

Le financement mezzanine est un mélange d'instruments de fonds propres et d'instruments de dette.

Partenariat public privé (PPP)

Le PPP est un instrument dans lequel des institutions du secteur public et des entreprises privées co-investissent dans le développement d'infrastructures publiques.

Les entreprises privées cherchent des moyens de faire progresser leurs propres intérêts commerciaux tout en réalisant un bien public fondé sur un défi commun. Ces dispositifs peuvent être basés sur des modèles commerciaux de partage des revenus après leur mise en œuvre.



Source: PWC Stratégie de développement de villes intelligentes, 2020

Stratégie de Programmes & Projets

Démarrage du Projet
- Déploiement des équipes
- Préparation du rapport de projet détaillé

Processus d'appel d'offres
- Publication de l'Appel d'Offres
- Evaluation des offres
- Séléction des fournisseurs

Excécution du Projet
- Etude de terrain
- Installation

Suivi de l'Avancement des Projets
- Progrès matériel
- Progrès financier

Processus de résolution
- Recherche de consensus
- Innovation

Cadre commun
- Directives & Conceptions de politiques publiques

Engagement des communautés
- Feedback & Suggestions durant les conceptions & excécution

Evaluation
- Evaluation externe

Etude de cas
- Documentation
- Séminaires
- Apprentissage

Achèvement du Projet
- Mise en ligne
- Mise en Operation & Maintenance
- Diffusion & Promotion

Structure ad hoc

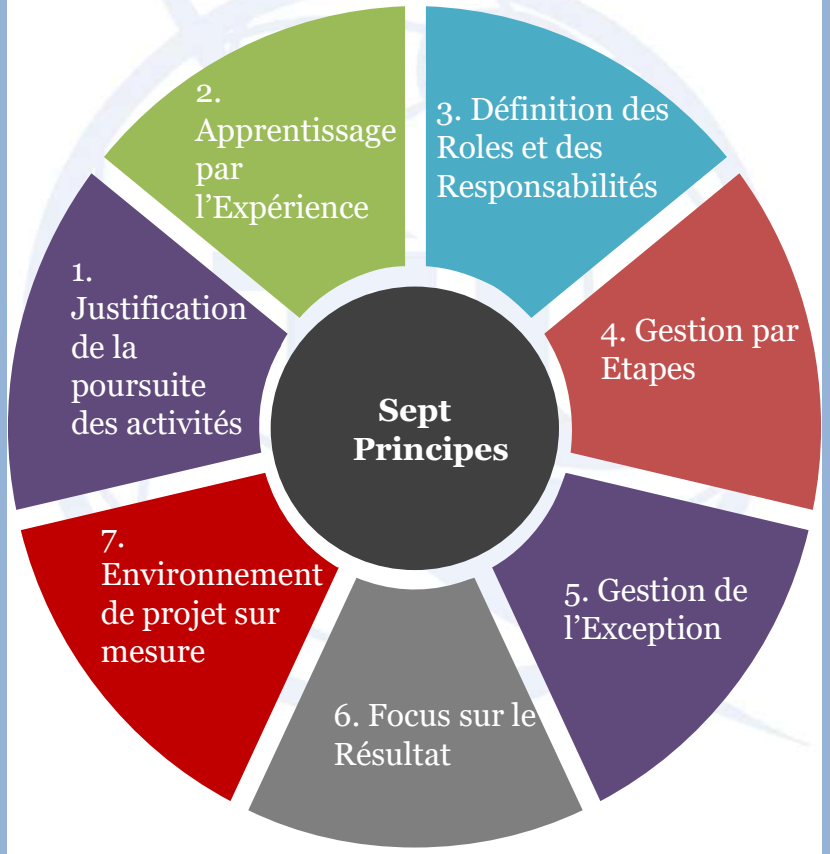
Communes municipales

Comité National de coordination

Source: PWC Stratégie de développement de villes intelligentes, 2020

Stratégie de Programmes & Projets

- ✓ Le dossier commercial est le document le plus important, et doit être mis à jour à chaque étape du projet.
- ✓ Chaque projet doit tenir un relevé des expériences acquises et doit être continuellement mis à jour
- ✓ Les rôles doivent être structurés en quatre niveaux (gestion de projet ou de programme, conseil de projet, gestionnaire de projet et équipe).
- ✓ Le projet doit être planifié et piloté étape par étape



- ✓ Le projet doit avoir des seuils de tolérance définis (6 aspects ci-dessus) pour chaque objectif du projet, afin d'établir les limites de l'autorité déléguée.
- ✓ Un projet doit se concentrer sur la définition et la livraison des résultats, en particulier sur leurs exigences de qualité.
- ✓ Chaque projet doit être conçu sur mesure pour s'adapter à l'environnement, à la taille, à la complexité, à l'importance, à la capacité de temps et au risque. L'adaptation est la première activité du processus de lancement d'un projet et elle est examinée à chaque étape.

Plan d’actions

- Pour que les programmes de villes intelligentes soient performants et durables, ils devront être agiles et se concentrer sur plusieurs aspects importants :
  - Être stable, mais pas en stagnation : Les villes doivent évoluer en permanence pour mettre en place des réglementations et des structures de gouvernance qui répondent aux besoins des parties prenantes, qui évoluent elles-mêmes à un rythme rapide.
  - Cultiver et encourager l'innovation : Les villes doivent expérimenter et adopter de nouvelles technologies et de nouveaux modèles commerciaux.

Plan d’actions

- Collaborer : Les villes doivent répondre aux besoins de tous les secteurs de la société et travailler avec les communautés, les ONG, les universités et le secteur privé ; ainsi, elles peuvent devenir durables, centrées sur les citoyens, économiquement dynamiques, accessibles, résilientes, réceptives et bien gouvernées.
- Créer un environnement propice aux affaires : Il est clair que les gouvernements municipaux auront besoin du soutien du secteur privé pour développer les villes. Les gouvernements municipaux devront comprendre et répondre aux besoins du secteur privé et créer des projets qui équilibrent les risques et les bénéfices
- Faire preuve de leadership : Les dirigeants municipaux doivent être à la fois visionnaires et pragmatiques pour faire avancer la transformation souhaitée. Ils devront prendre des risques calculés et bien informés et se garder d'assumer la position par défaut que constitue l'aversion pour le risque

Plan d'actions

1 Identification de la ville	2 Identification des défis principaux	3 Développement d'une Vision Partagée	4 Identification et Priorisation des Objectifs	5 Développement des Programmes
Chaque ville possède un ensemble unique de caractéristiques économiques et sociales. Il est important qu'une ville identifie ses caractéristiques uniques et s'appuie sur celles-ci.	Sur la base de la préparation du profil de la ville et grâce à l'engagement des parties prenantes, identifier les principaux défis auxquels la ville est confrontée. Une fois ces défis identifiés, établir un ordre de priorité.	Une ville doit développer une vision à long terme pour renforcer ses caractéristiques clés et surmonter les défis urbains.	Les priorités dépendront de facteurs tels que l'impact du défi, l'ampleur du défi, la transformation souhaitée, la capacité à conduire le changement, l'importance dans la vision globale, etc.	Lorsque les villes élaborent des programmes pour atteindre leurs objectifs, l'accent doit être mis sur les résultats des projets. La conception des solutions doit être laissée au secteur privé afin que des solutions innovantes puissent être introduites.

6 Révision des Régulations	7 Développement des Capacités	8 Financing et Funding	9 Objectifs de Quick Wins	10 Gestion des avantages et Suivi
Au moment où les villes se lancent dans le renouvellement urbain, elles tireront parti de modèles d'activités disruptives qui ne s'intègrent pas parfaitement dans le cadre réglementaire traditionnel.	Les capacités techniques et de gestion devront être renforcées par un soutien externe dans les cas où les capacités internes ne peuvent être développées en même temps.	Les villes devraient concevoir des programmes de renouvellement urbain qui sont financièrement viables.	Les méthodes agiles de développement de projets ou les projets pilotes peuvent aider à présenter des résultats intermédiaires. Ces résultats peuvent servir à attirer des investissements, des ressources humaines et des solutions innovantes.	Les projets doivent être suivis régulièrement pour s'assurer que les dépassements de coûts et de délais soient réduits au minimum et que la qualité souhaitée soit atteinte.

Stratégie de management du changement

Engagement avec les communautés locales
La consultation de la communauté dès la phase de planification permettra d'apaiser les inquiétudes et d'améliorer la conception du projet en tenant compte des préoccupations de la communauté.

Engagement avec le secteur privé
Les entreprises privées devraient favoriser un dialogue constructif avec le secteur public pour éviter la méfiance et présenter leur perspective.

Focus sur les Femmes & la Jeunesse
L'inclusion sociale dans la ville intelligente repose sur la sensibilisation et l'accès aux TIC, en particulier chez les femmes et les jeunes.

Pratique Ethique
Un comportement contraire à l'éthique est non seulement inacceptable, mais présente également un grand risque pour le succès du programme de Ville intelligente

Image, Crédibilité & Positionnement
Les projets de villes intelligentes sont développés dans une ville et ont un impact sur son image et sa crédibilité. Un mauvais classement ou une impression négative peuvent entraîner des changements dans son positionnement dans l'opinion publique.

Dimensions de la maturité de l'intelligence des villes durables

Leadership & Governance	• Level of Leadership Commitment • Effective City Mgt.- learning form best practices • Strategic and transformational mind-set for smart initiatives
Stakeholder Engagement and Citizen Focus	• Stakeholder engagement and citizen/customer focus • Support business, community & academic smart city activities • Social inclusion
Effective Use of Data	• Openness and sharing of data based on agreed regularity policies • Data interoperability (use of common standards)+ Availability of City data analytics • Data privacy and data security based on standard policies and processes
Integrated ICT Infrastructure	• Reliable ICT resource mapping and management • Progress in developing a city-wide ICT architecture • IOT Integration and Cloud computing
Levels of Smartness	• Smart core infrastructure smart management of water, gas, ICT, waste and energy • Smart Facilities and buildings • Smart core services (education, health, legal, safty,..)Environment

Joint ITU-UN KPI for Smart Sustainable Cities

Recommendation ITU-T
Y.4903/L.1603


How do we shape
Smarter and More
Sustainable cities

ITU KPI for SSK – Chemin pour des villes intelligentes et durables

Cycle de dévelop. de ville durable intelligent

1. Définir la vision de votre projet SSC
2. Identifier les objectifs du SSC
3. Assurer la cohésion politique
4. Construire votre SSC
5. Mesurer le propgrès de votre ville
6. S'assurer de la responsabilité

Pourquoi des KPIs for SSC ?

Comment savons-nous que notre ville est intelligente et durable?

KEY PERFORMANCE INDICATORS FOR SSC

3 Spécifications techniques et 1 Rapport technique sur les KPI pour SSC

Le projet KPI des villes intelligentes et durables de l'UIT

- Dubai
- Singapore
- & autres villes..

Mesurer le succès

Directives et recommandations de politiques

Index mondial des villes intelligentes et durables

Ces indicateurs de performance clés (KPI) sont des normes internationales

Structure IFP

54 indicateurs de base + 37 indicateurs avancés

20 intelligents + 32 structurels + 39 durables

132 points de collecte des données

Dimension	Economie	Environnement	Société et culture
Catégorie	▪ Infrastructure des TIC ▪ Eau et assainissement ▪ Drainage ▪ Approvisionnement en électricité ▪ Transport ▪ Secteur public ▪ Innovation ▪ Emploi ▪ Déchets ▪ Bâtiments ▪ Urbanisme	▪ Qualité de l'air ▪ Eau et assainissement ▪ Déchets ▪ Qualité environnementale ▪ Espace public et nature ▪ Energie	▪ Education ▪ Santé ▪ Culture ▪ Logement ▪ Inclusion sociale ▪ Sûreté ▪ Sécurité alimentaire
	Indicateurs de base: 22	**Indicateurs de base: 19**	**Indicateurs de base: 9**
	Indicateurs avancés: 16	**Indicateurs avancés: 7**	**Indicateurs avancés: 16**

Structures et propriétés des KPIs

- Simplicité: le concept de chaque indicateur devrait être simple et facile à comprendre par les parties prenantes.
- Mesurable: les KPI doivent être quantitatifs et les données historiques et actuelles devraient être disponibles ou facile à collecter.
- Intégralité: l'ensemble d'indicateurs devrait couvrir tous les aspects de SSC.
- Pertinent: les KPIs devraient donner un meilleur aperçu de la performance de la ville dans la réalisation de sa stratégie

IoT Applications

Mobilité intelligente

Systèmes de transport intelligent

- Systèmes de transport intelligent désigne l'application des Technologies d'Information et des Communication au domaine des transports

- Avantages apportés:
  - Réduire la congestion
  - Améliorer la qualité de
  - Economiser de l'énergie
  - Economiser du temps, et
  - Améliorer la sécurité et confort des conducteurs et piétons

Smart parking

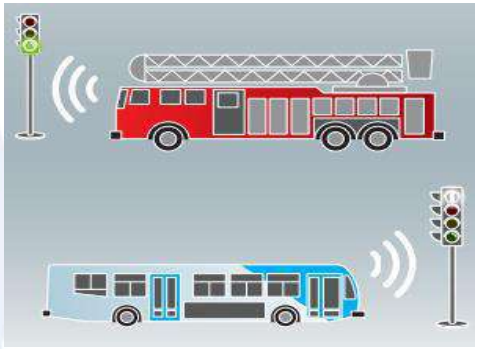
- Smart parking permet de fournir aux conducteurs des informations en temps réel sur les places de parking les plus proches et leur prix.
  - Elimine le besoin de conduire à la recherche d'une place de parking.
  - Recherchez d'autres options (par exemple, autre heure, transport public) en cas ou les places de stationnement de proximité sont occupées.

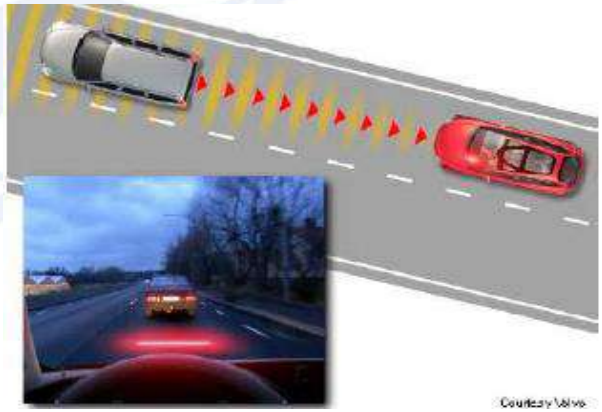
« Peer-to-peer ride service »

- « Peer-to-peer ride services » ce sont des services qui mettent en relation les conducteurs et les passagers.
- Elles utilisent des plates-formes numériques et des applications intelligentes pour permettre aux particuliers de vendre des trajets à des personnes nécessitant un transport.
- Uber et Lyft, sont de solutions qui ont connu une croissance exponentielle dans le monde .
  - Avantages: elles contribuent à la fois à la commodité et à la réduction de la congestion.

Gestion intelligente du trafic routier

- Cette application intègre divers sous-systèmes tels que CCTV, la détection des véhicules, … dans une interface unique cohérente pour fournir:
  - Un meilleur contrôle du trafic;
  - La gestion des accidents;
  - La gestion de maintenance des infrastructures,
  - Etc.





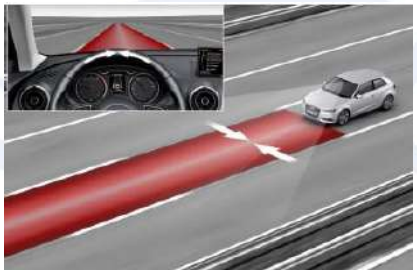
Quelques exemples d'équipements: Les capteurs intelligents

Caméra CCTV

Détecteurs de stationnement

LIDAR

RADAR

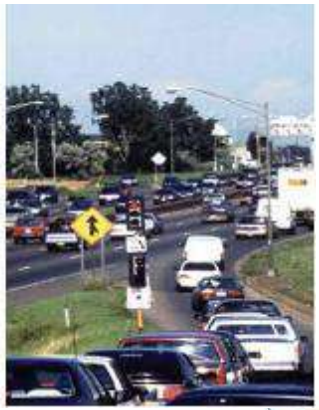


Caméra IP

- Le temps de réaction et les données à grain fin de la circulation dans la ville, créées par des capteurs dans les infrastructures et les véhicules, permettent aux systèmes intelligents d'optimiser le flux de circulation en ajustant les feux de signalisation et d'autres signaux.Les systèmes de contrôle de la circulation peuvent également être utilisés pour guider les services d'urgence comme les ambulances à travers le trafic en repérant les feux de circulation les plus rapides, en gardant les ponts fermés.

Système d'information multimodal pour les voyageurs (SIV)

- Avantages:
  - Obtenir en temps réel l'information sur les réseaux de transport ;
  - Estimer le temps de déplacement ;
  - Proposer des choix personnalisés de déplacement des voyageurs afin d'éviter la congestion.



Centre d’opération

- Plateforme de gestion de données (ou centre d’opération): C’est le cœur et le cerveau de tout SIT, il traite et analyse les informations provenant de divers équipements (feux de circulation, caméras, détecteurs de présence, …) et la présente aux opérateurs du centre de contrôle.

Partenaires internes

Partenaires externes

Environnement et bâtiment intelligents

Environnement intelligent

- Les compteurs intelligents ou Smart Metering:
  - Ils enregistrent la consommation d'énergie électrique à intervalles d'une heure et communique les valeurs à l'entreprise responsable de la gestion de l’élecricité.
  - Avantages:
    - Gérer votre établissement sans vous déplacer, et
    - Etablir un plan d’économie concret,

Environnement intelligent

- La reconstruction de l'éclairage public dans la ville comprend la modernisation des systèmes d'éclairage, l'implémentation de mesures d'efficacité énergétique, des nouvelles sources de lumière et systèmes de régulation de puissance plus efficace énergétiquement, ainsi que la modernisation d'autres éléments comme les lampadaires, les câbles etc.
- Les points principaux du projet comprennent la définition de modèles et des besoins pour l'implémentation d'un nouveaux système écologique et efficace énergétiquement qui devra être amélioré par l'implémentation d'un système de gestion de la lumière – capteurs, contrôleurs, etc.
- **Bénéfices:**
  - Gains en consommation électrique
  - Gains sur les coûts
  - Meilleure efficacité dans la maintenance

Maison connectée

- Une étude du cabinet Juniper Research prévoit un accroissement de 200 % du nombre d'objets connectés à l'intérieur des habitations d'ici fin 2021.
- Outre les objets de divertissement comme les télés intelligentes, la domotique s'intéresse à la sécurité et l'économie d'énergie au sein de l'habitat :
  - centrale domotique : contrôle et programmation de différentes interventions à l'intérieur du foyer
  - capteurs d'informations : système d'alarme, variations de température, etc.
  - Actionneurs : qui permettent la programmation et le contrôle des différents appareils électroniques du foyer, même à distance

Bâtiment intelligent

- Les habitations et les bâtiments se transforment et s'interconnectent entre eux mais également avec l'environnement, les habitants, le quartier et la ville.
- Maillon clé de la ville intelligente, le bâtiment intelligent est le lieu de nombreuses expérimentations ou se conjuguent le numérique et la durabilité.

Smart retail

Agriculture intelligente

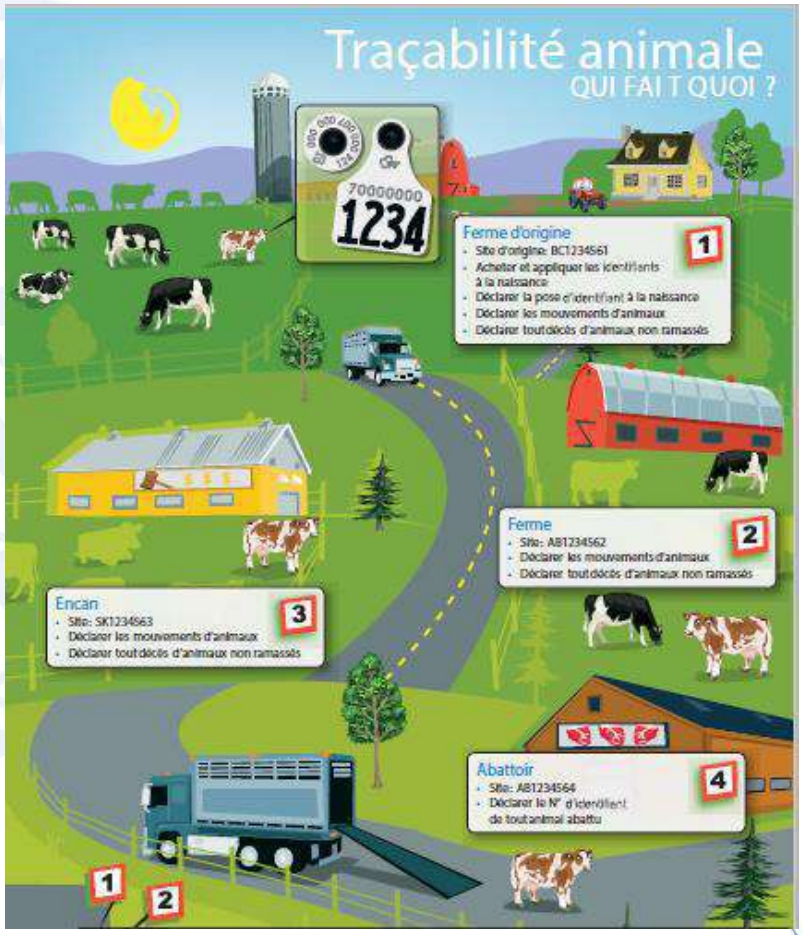
- Traçabilité des animaux
- Irrigation intelligente
- Drones

Agriculture intelligente

- La croissance rapide de la population mondiale et les perturbations climatiques sont deux grands facteurs, parmi d'autres, qui font de l'agriculture moderne un défi au quotidien.
- D'ici 2050, la productivité agricole devra avoir augmenté de 70 % pour répondre à la demande mondiale.
- Des drones sont aujourd'hui utilisés pour récolter en temps réel des informations essentielles à la gestion de l'exploitation :
  - humidité de la terre,
  - état des plantations,
  - climat,
  - Etc.

Traceurs GPS pour le bétail

- Surveiller plus finement l'état de santé du bétail et suivre leur mouvement en élevage depuis sa naissance.
- Les conditions nécessaires à la traçabilité :
  - Identification des animaux
  - Identification des sites
  - Localisation



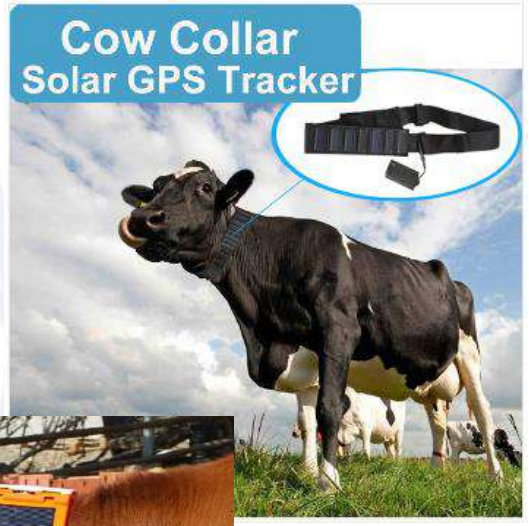
Moyen de géo-localisation

- Utilisation de la technologie GPS (Global Positioning System) pour la géo-localisation des animaux.

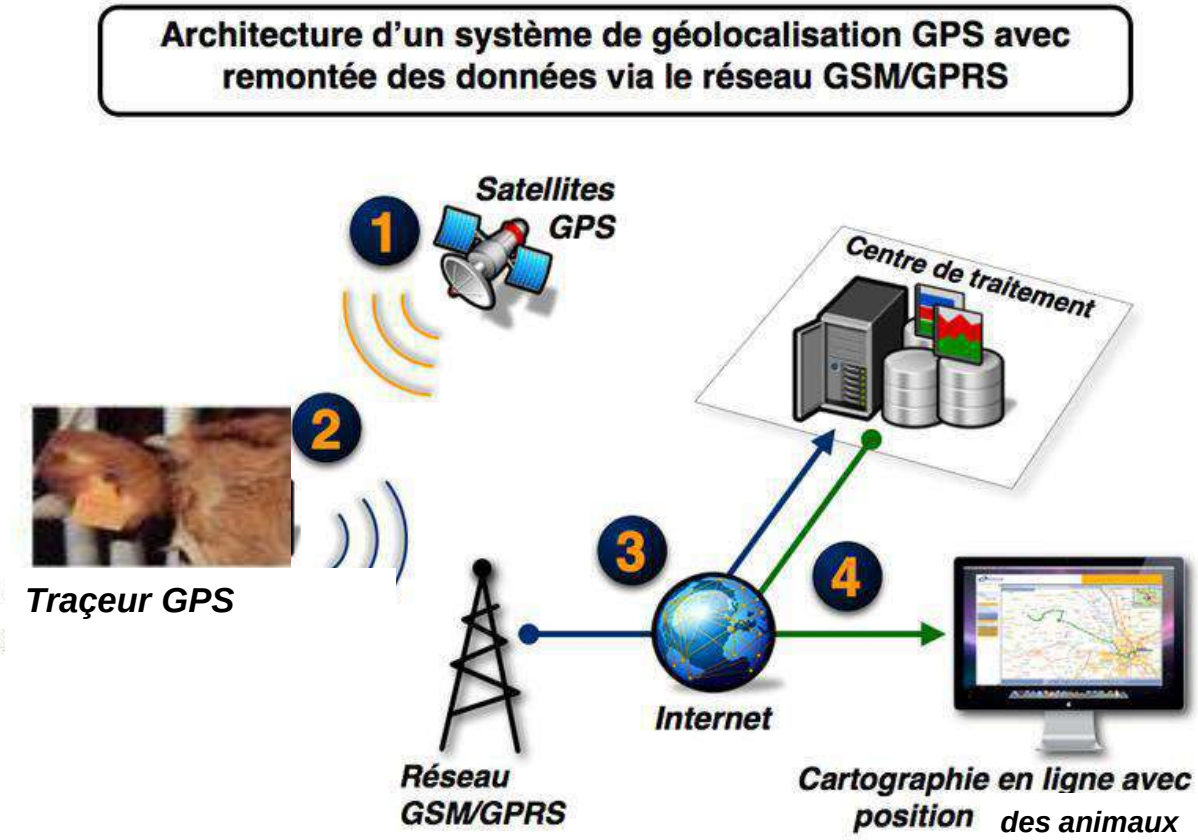
- Dispositif de traçabilité est un collier électronique équipé d'un récepteur GPS qui enregistre par satellite, de façon périodique, sa position au cours de ses déplacements.

Dispositifs de géo-localisation

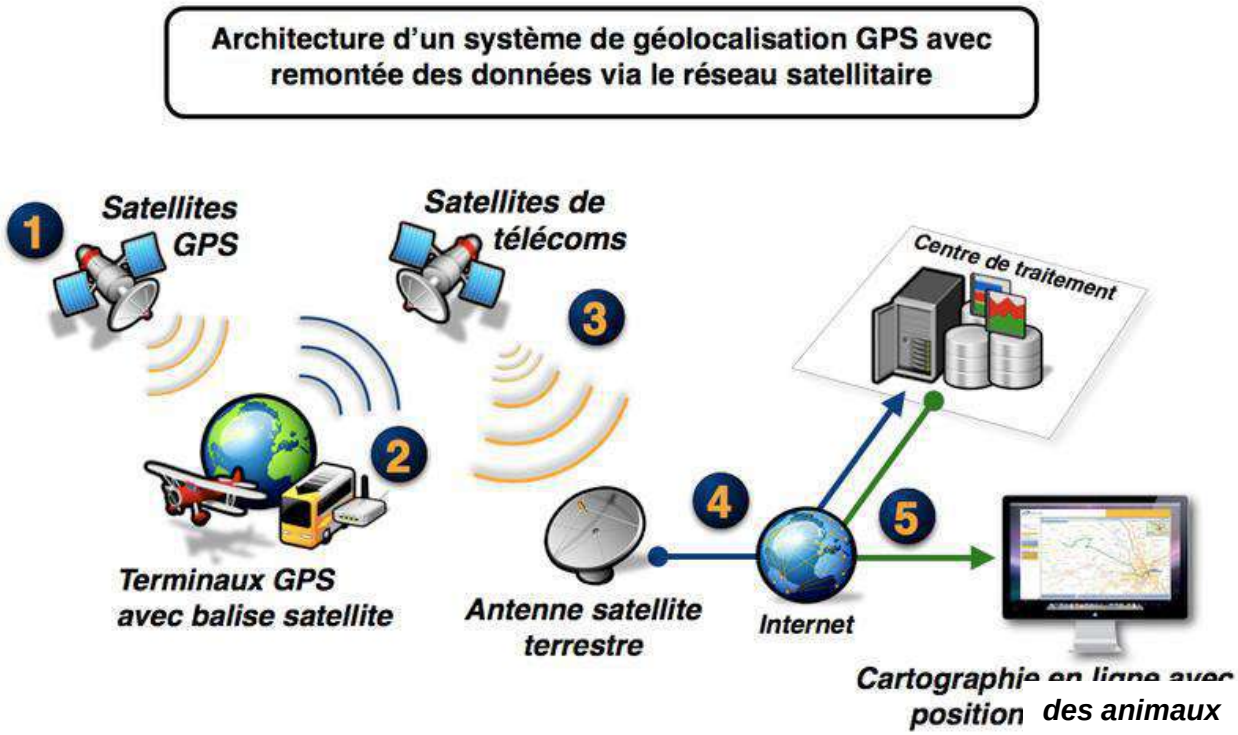
Collier GPS traceur bétail
Prix : 230 Euro
Sa batterie est de type: 5000mAh, soit 400 jours en veille.
Gps traceur : Son poids est de 190g et ses dimensions sont : 117*59*30 (mm)
Le collier : encolure : 1900(mm), son poids : 300g



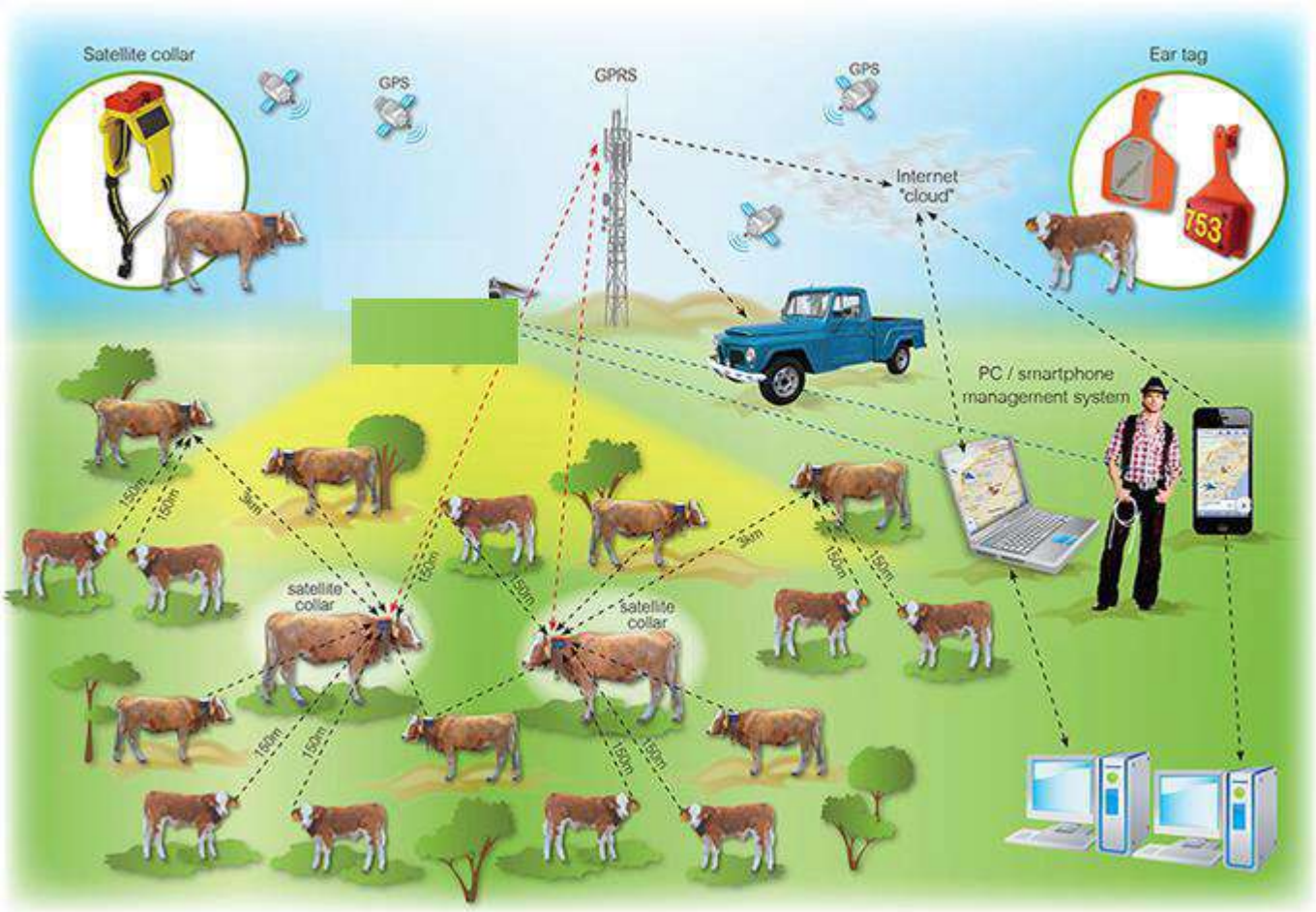
Principe de fonctionnement



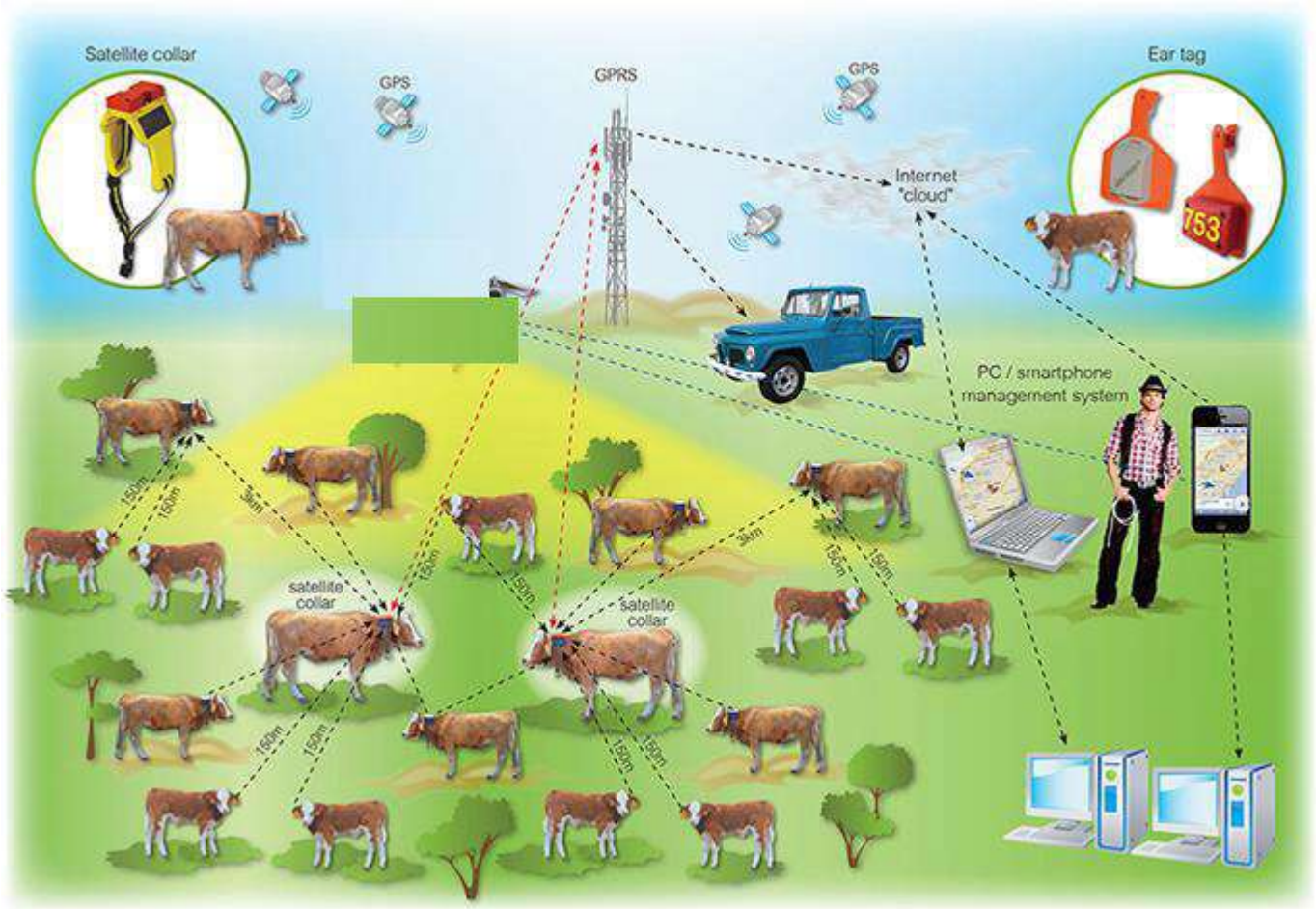
Principe de fonctionnement



Exemple de solutions existantes à base de GPRS



Exemple de solutions existantes à base de GPRS



Critères du choix du système de Géolocalisation

- Principaux critères pour le choix d'un système de Géolocalisation:
  - Le coût du système;
  - La couverture du réseau de communication;
  - L'autonomie: durée de vie de la batterie;
  - La facilité de déploiement: infrastructure nécessaire et encombrement du système;

Structure des coûts

- L'investissement dans une solution de suivi du cheptel engendre des coûts du matériel, des logiciels et d'abonnement.

Coté éleveur	Coté centre d'exploitation
Matériel: - Dispositif de traçabilité - Dispositif d'affichage Abonnement : -Abonnement GPRS ou satellite Autres coûts: - Formation à l'utilisation - Installation du matériel	Matériel: - Serveur - Routeur Licences: - Base de données - Logiciel d'exploitation - Cartographie - Interfaçage Abonnement : - Communication par GPRS ou satellite Autres coûts: - Paramétrages - Maintenance - Formation à l'utilisation - Installation du matériel

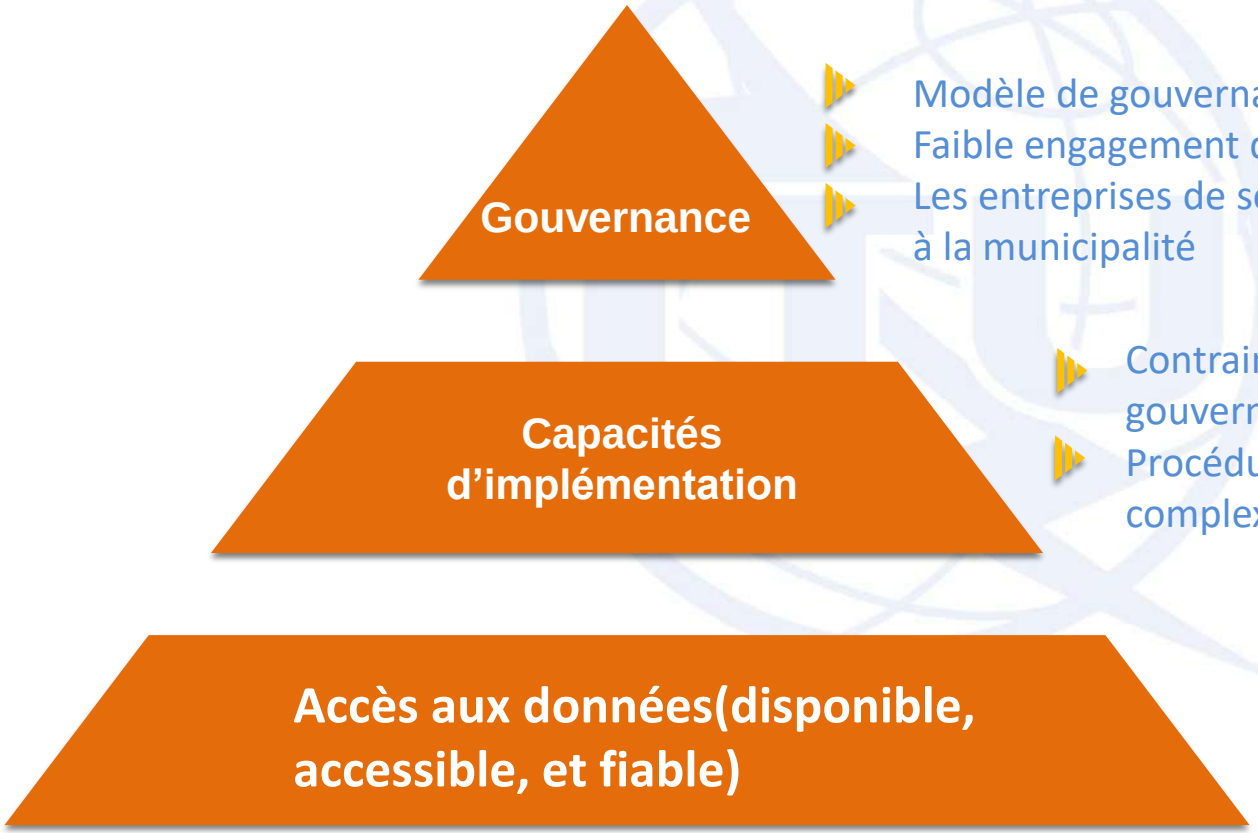

ITU

Industrie	Smart Cities	Retail	Santé	Transport	Assurance
					
▪Maintenance préventive ▪Sécurité du travailleur ▪Optimisation des stocks ▪Reassort automatique ▪Supervision des zones critiques	▪Contrôle d'accès au bâtiment ▪Éclairage intelligent ▪Optimisation du remplissage des parkings ▪Optimisation de gestion du trafic	▪Analyse zones chaudes et froides du point de vente ▪Prévention des ruptures de stocks ▪Offres personnalisées ▪Force de vente au bon endroit au bon moment	▪Monitoring des patients chroniques et des patients en sortie d'hospitalisation ▪Suivi de l'observance	▪Services d'information à valeur ajoutée pour les passagers (trafic) ▪Tele maintenance des véhicules	▪ Conduite vertueuse au volant ▪ Maintien à domicile et téléassistance nouvelle génération ▪ Sécurisation de la maison
l'usine connectée devient une réalité, la supply chain est révolutionnée	les premières villes intelligentes et les bâtiments connectés émergent	le parcours client est amélioré et les performances du distributeur décuplés	La télémédecine et la prévention santé se mettent en place	des transports publics optimisés, des véhicules plus sécurisés	déjà de nouveaux modèles de tarifications et nouveaux services

Quels sont les freins

- Multiplicité et variété des acteurs
  - De nombreux acteurs interagissent, outre les acteurs traditionnels des villes, de nouveaux acteurs apparaissent et prennent une place importante dans la construction de la ville intelligente de demain, les spécialistes des nouvelles technologies AI, IoT, etc.
- Une nouvelle forme de coopération Public/privée

Défis des villes intelligentes



- Modèle de gouvernance centralisé
- Faible engagement des parties prenantes de la ville
- Les entreprises de services publics n'appartiennent pas à la municipalité

- Contraintes budgétaires (budget gouvernemental limité)
- Procédure d'appel d'offres public complexe

- Les données ne sont pas ouvertes
- Problèmes de protection des données

Open data

- Les données ouvertes, générées par les villes, joueront inévitablement un rôle décisif dans les futurs projets de ville intelligente.
- en tirant parti de l'IoT pour promouvoir le déploiement de services urbains innovants sur les données publiques et créer de nouvelles sources de revenus.

Politique de données

- Cadre de politique des données.
- Malgré les avantages apportés par les données ouvertes, les obstacles sur le chemin empêchent les parties prenantes de la ville intelligente d'intervenir et de créer un marché des données, par exemple :
  - Quelle valeur peut-on tirer des données?
  - Comment peut-il être mieux capturé?
  - À qui appartiennent les données?
  - Quelle structure de gouvernance est responsable?

→ Une nouvelle politique de données est absolument nécessaire pour faire face à ces problèmes et se protéger contre les écoutes clandestines.

Modèles économiques

- Les modèles économiques traditionnels ne sont plus adaptés aux projets de la ville intelligente en raison de la complexité de l'écosystème IoT (multiplicité des parties prenantes).
- Des investissements importants sont désespérément nécessaires pour trouver des modèles économiques innovants qui traduisent la chaîne de valeur de la ville intelligente en quelque chose de finançable et répondre aux attentes des acteurs de l'écosystème de la ville intelligente.

Partenariat public-privé (PPP).

- Les PPP peuvent être bénéfiques tant pour le secteur public que privé.
  - Pour le secteur public, cela peut entraîner des économies importantes et peut être un moyen de renforcer l'attractivité de la ville.
  - Le secteur privé peut gagner une plus grande coopération gouvernementale et une meilleure compréhension des besoins locaux grâce à ces partenariats, accroître sa visibilité internationale et, par conséquent, accéder à de nouvelles opportunités commerciale

Acceptation de l'utilisateur

- L'acceptation des utilisateurs peut être obtenue grâce à l'engagement des citoyens dans le développement des services de la ville.
- Ceci est mieux illustré par la création de laboratoires vivants, où le développement des services de la ville repose sur la volonté des utilisateurs de contribuer et d'exploiter leurs connaissances et leur expérience spécifiques dans des domaines problématiques spécifiques.

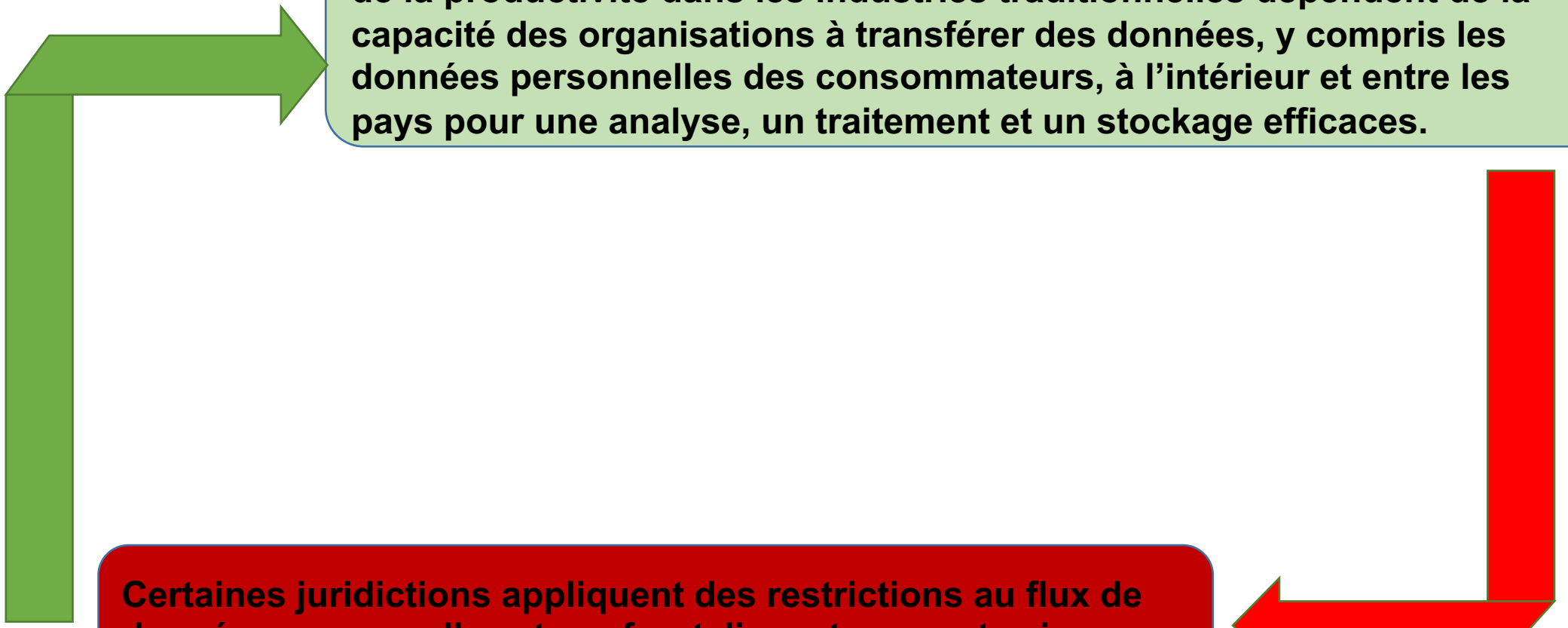
Gestion des données IoT (accès aux données, flux de données transfrontalier et localisation des données)

Seyni Fati – Senior Policy Manager GSMA

Août 2020

Flux de données transfrontaliers

Le développement de l'économie numérique et la croissance continue de la productivité dans les industries traditionnelles dépendent de la capacité des organisations à transférer des données, y compris les données personnelles des consommateurs, à l'intérieur et entre les pays pour une analyse, un traitement et un stockage efficaces.



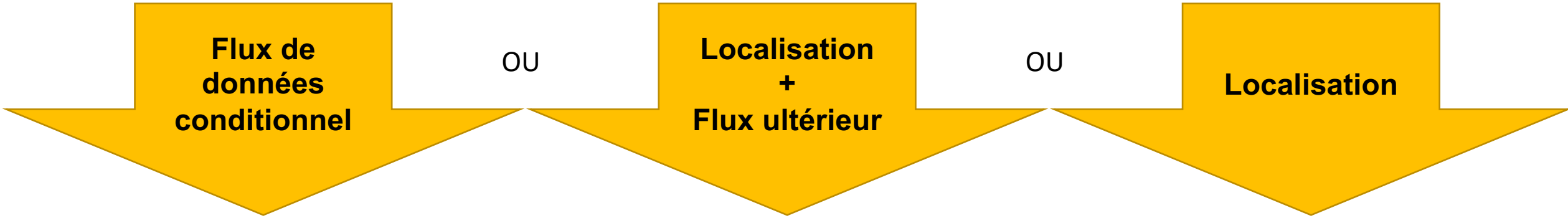
Certaines juridictions appliquent des restrictions au flux de données personnelles «transfrontalier» et peuvent exiger qu'elles soient situées dans un pays ou une région spécifique

Pourquoi restreindre le FDT?

Les raisons de l'introduction de restrictions diffèrent d'un pays à l'autre, mais comprennent généralement une ou plusieurs des justifications suivantes:

1. Confidentialité et protectiondes données
2. Surveillance étrangère
3. la sécurité nationale
4. Économie numérique nationale

Approches pour imposer un contrôle sur le FDT



IMPLICATIONS

Facilité administrative de faire des affaires

Coût de production des biens et services

Coût de fonctionnement global de l'entreprise

Développement et livraison de produits et services IoT

Comprendre les avantages de la libre circulation des données

La liberté de déplacer des données personnelles sans restriction entre les pays génère des résultats positifs non seulement pour les organisations, mais également pour les citoyens et les pays

Benefits to citizens

- accès à la vaste gamme de produits et services disponibles en ligne.
- profite particulièrement aux petites et moyennes entreprises qui n'ont pas d'empreinte internationale

Benefits to organisations

- des idées, des produits et des services de marketing et de livraison partout où les données peuvent circuler.
- permettre un fonctionnement efficace des organisations multinationales
- permet aux entreprises d'améliorer la qualité du service et de réduire les coûts et les prix clients

Benefits to countries and society

- Introduire davantage d'entreprises et de consommateurs nationaux dans le pli numérique
- permettant aux petites organisations spécialisées d'établir une présence Internet à la fois nationale et internationale
- Avantages pour les organismes du secteur public et les ministères

Approches politiques de la localisation des données et FDT

1 –S'engager à faciliter les flux de données transfrontaliers et à supprimer les mesures de localisation restrictives

2 – S'assurer que les cadres de confidentialité sont adaptés à l'ère numérique.

3 – Examiner les anciennes règles de confidentialité spécifiques au secteur.

4 – Encourager les initiatives régionales de confidentialité des données

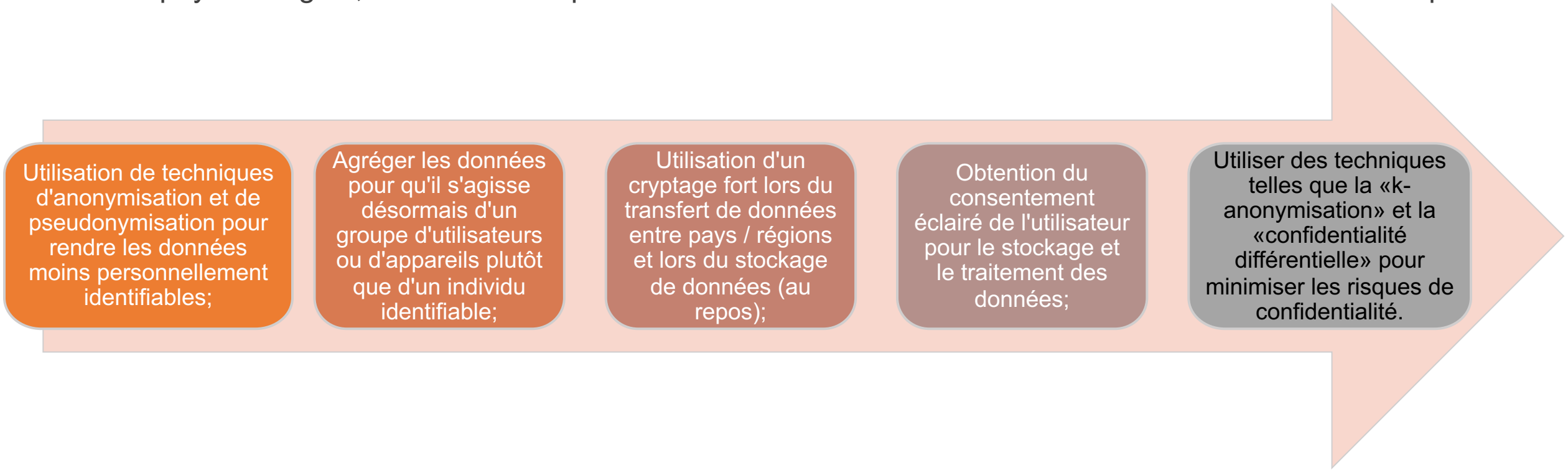
5 – Évitez la localisation en abordant les problèmes de surveillance étrangère de manière pragmatique.

6 – Évitez la localisation en abordant l'application de la loi et la sécurité naturelle de manière pragmatique.

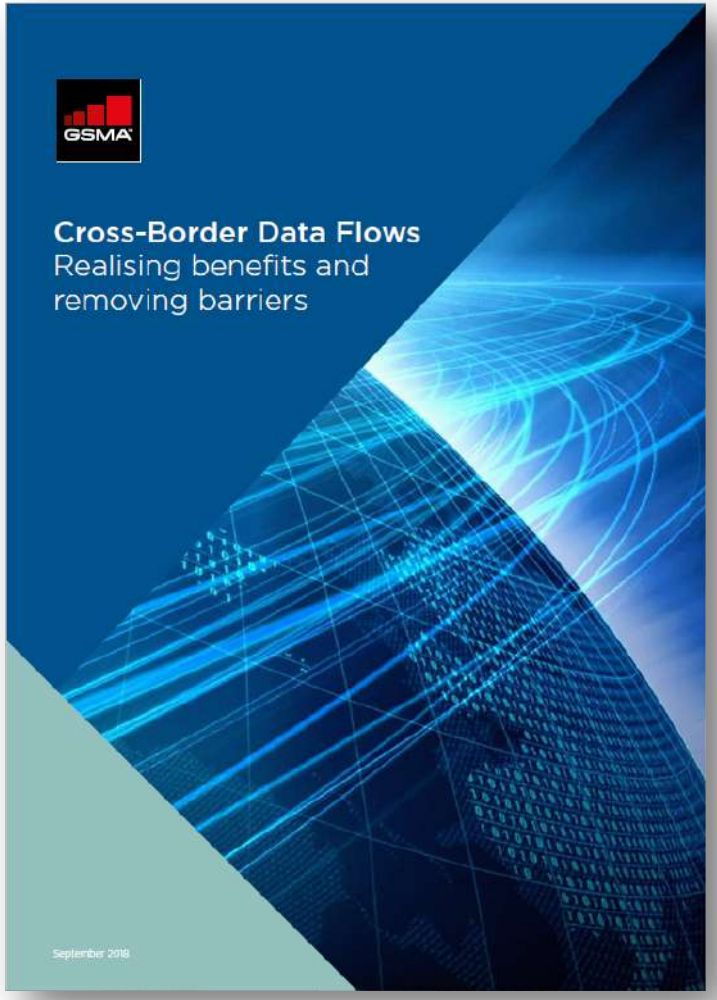
Mesures procédurales pour un FDT sûr

Les transferts de données en dehors du pays ou de la région peuvent raisonnablement encore avoir lieu s'ils sont contractuels et / ou techniques des mesures sont mises en place.

Pour les services IoT, avec une base de clients mondiale ou des appareils qui ne se limitent pas à rester dans un seul pays ou région, les restrictions peuvent être traitées avec un certain nombre de solutions techniques.



Documentations



FREQUENCES & TECHNOLOGIES IoT

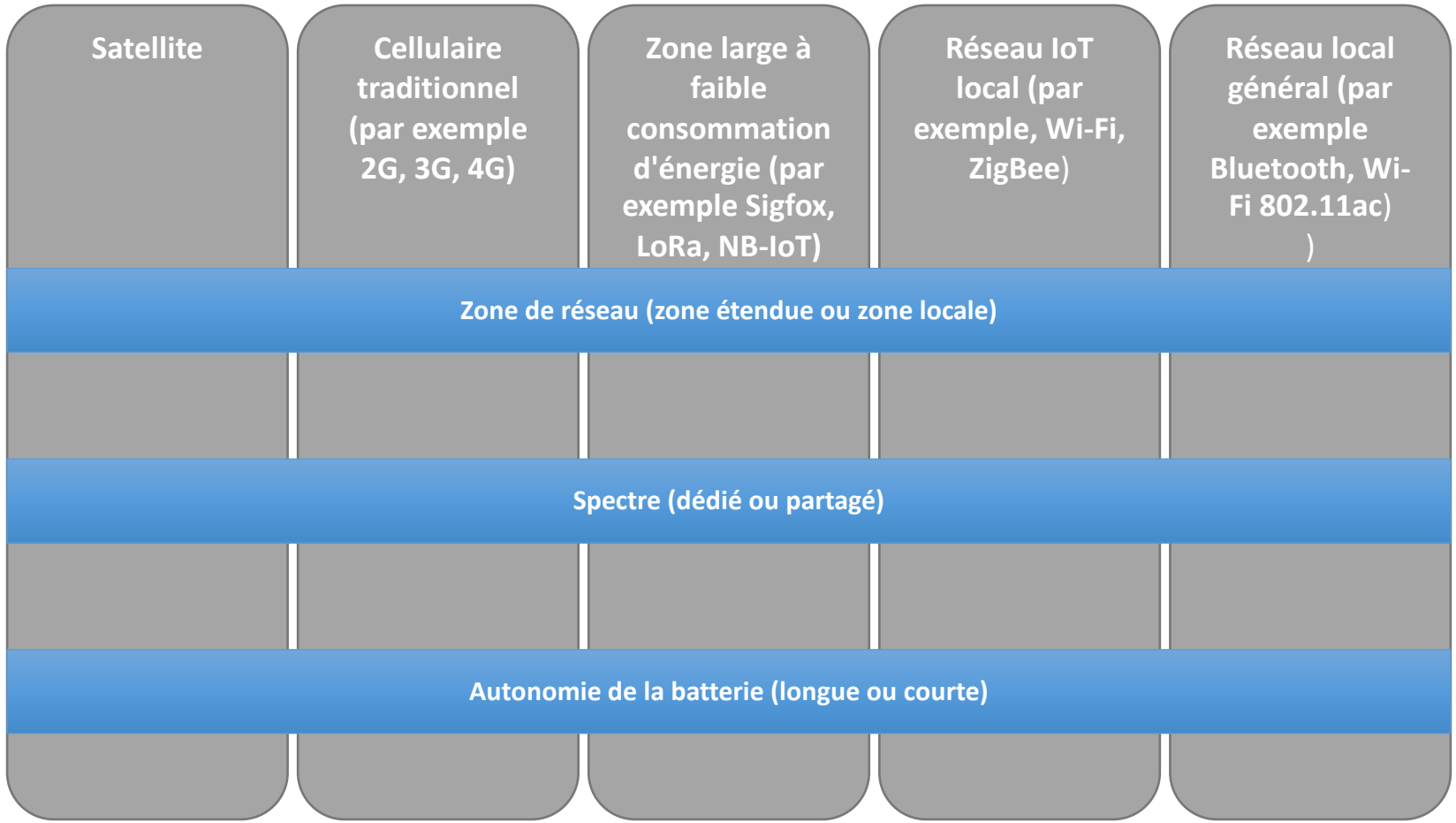
Seyni Fati, GSMA

Août 2020

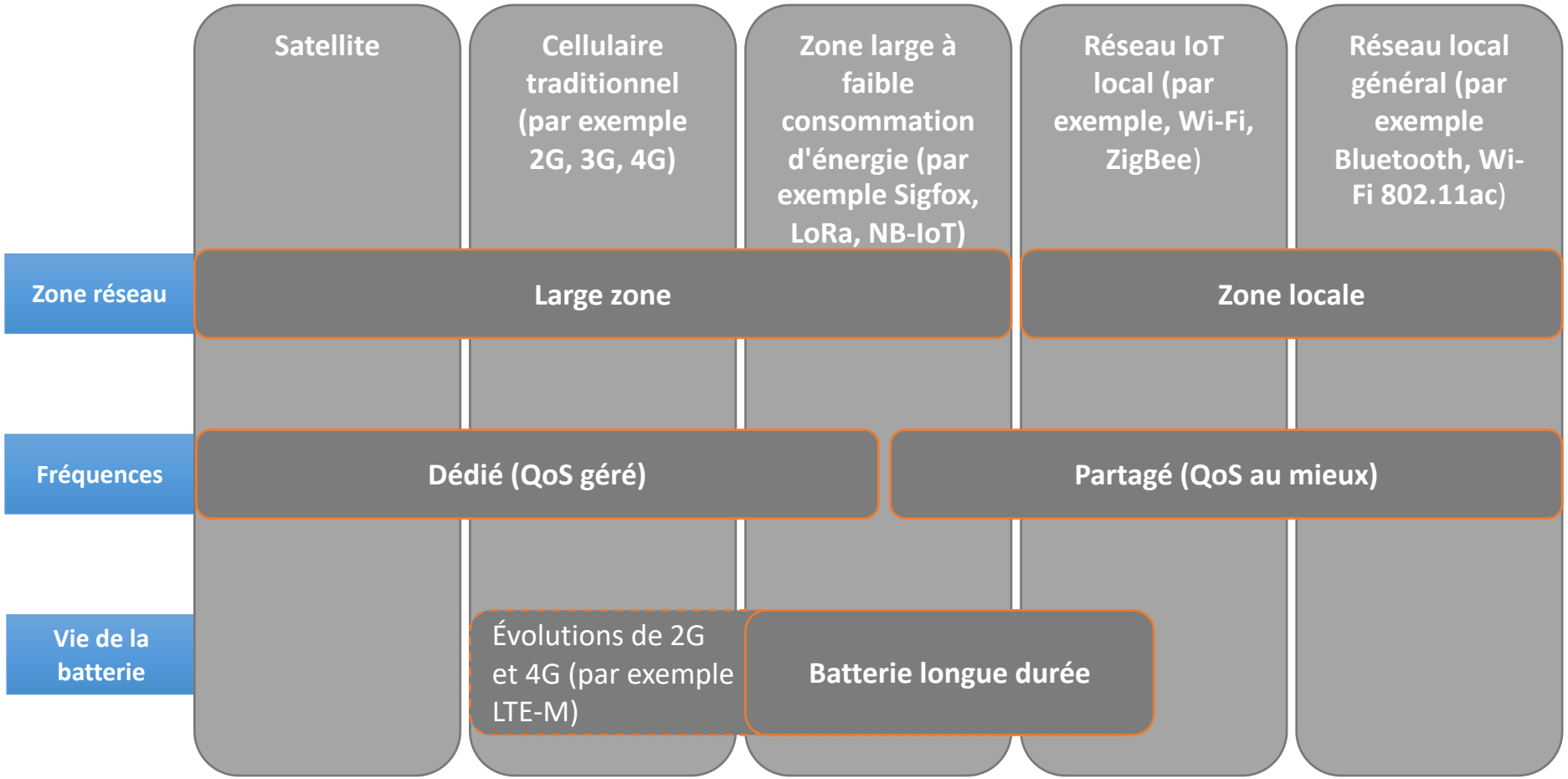
Principales caractéristiques des réseaux IoT

Satellite	Cellulaire traditionnel (par exemple 2G, 3G, 4G)	Zone large à faible consommation d'énergie (par exemple Sigfox, LoRa, NB-IoT)	Réseau IoT local (par exemple, Wi-Fi, ZigBee)	Réseau local général (par exemple Bluetooth, Wi-Fi 802.11ac)

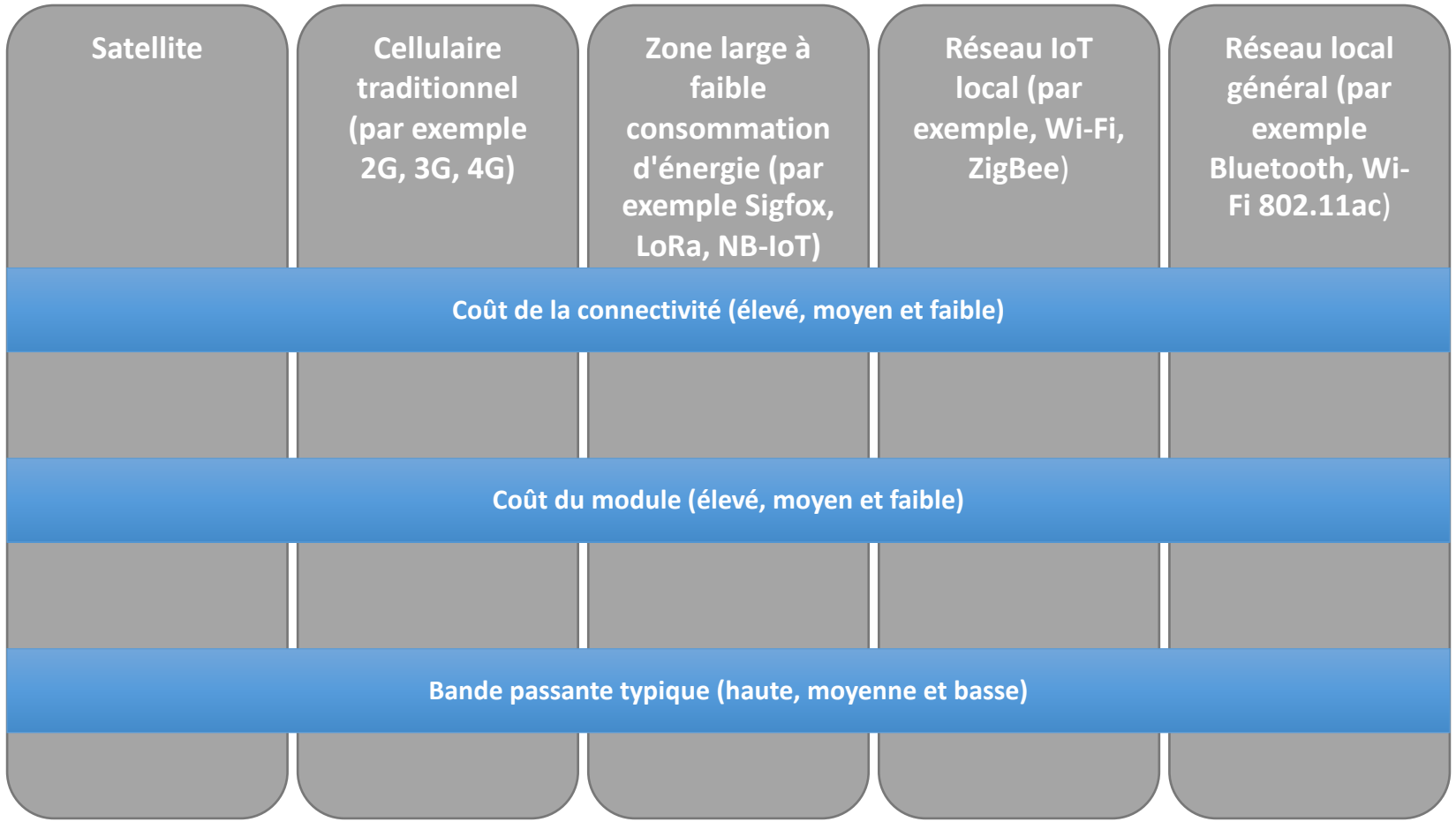
Dimensions du groupe technologique



Dimensions du groupe technologique



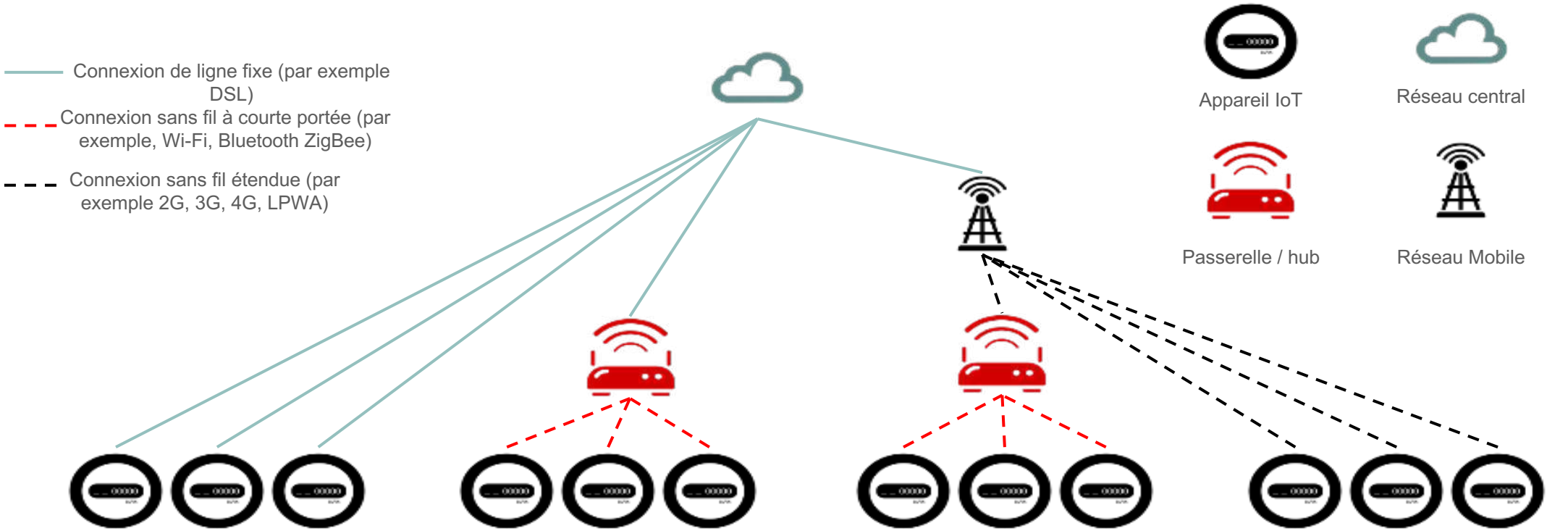
Dimensions spécifiques à la technologie



Dimensions spécifiques à la technologie

	Satellite	Cellulaire traditionnel (par exemple 2G, 3G, 4G)	Zone large à faible consommation d'énergie (par exemple Sigfox,	Réseau IoT local (par exemple, Wi-Fi, ZigBee)	Réseau local général (par exemple Bluetooth, Wi-Fi 802.11ac)
Coût de la connectivité	Élevé	*2G*: Moyen *3G*: Moyen *4G*: Moyen	Bas	Bas	Bas
Coût du module	Élevé	*2G*: Bas *3G*: Moyen *4G*: Élevé	Bas	Bas	Bas
Bande passante typique	Basse à Élevée	*2G*: Bas *3G*: Moyen *4G*: Élevé	Bas	*ZigBee*: Bas *Wi-Fi*: Élevé	*Bluetooth*:Bass *Wi-Fi 802.11ac* : Élevé

Il existe de nombreuses configurations pour les solutions IoT



Le spectre utilisé pour les solutions IoT peut être dédié (sous licence) ou partagé (sans licence)

Chaque option présente des avantages et des inconvénients

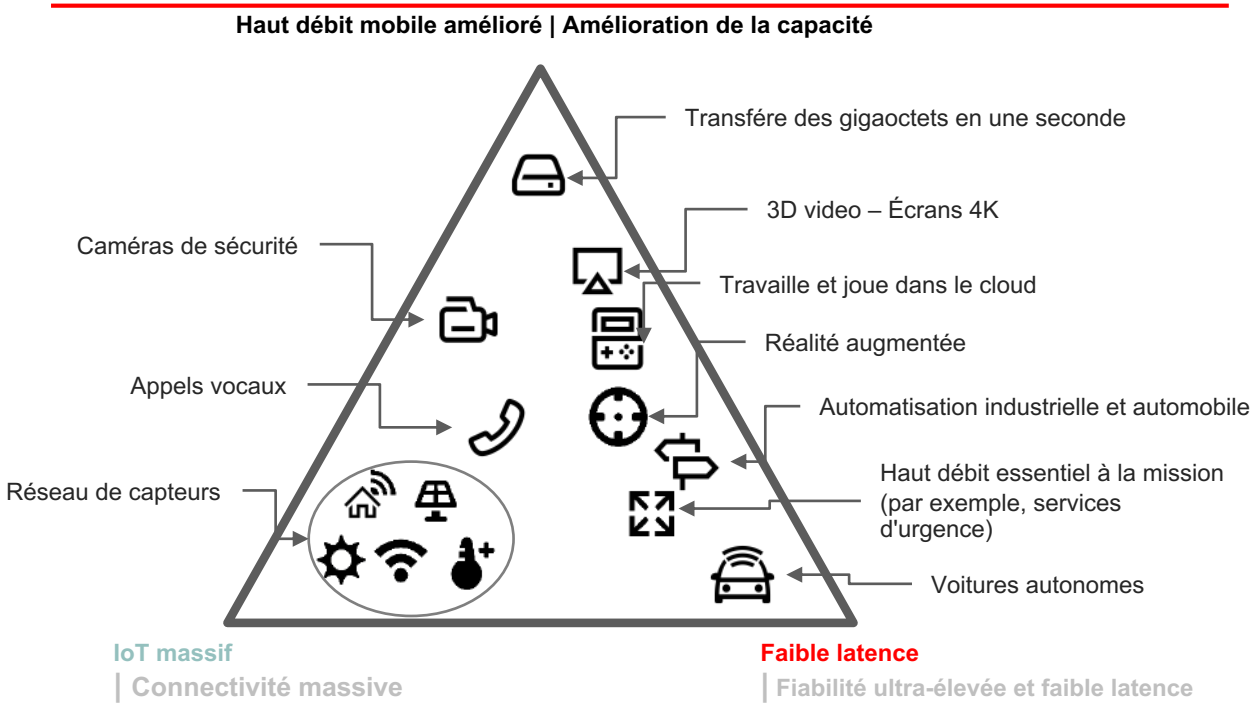
Spectre pour l'IoT		
Caractéristique	**Dédié**	**Partagé**
QoS	Prise en charge	Pas prise en charge
Coût	Plus élevé	Plus bas
Temps de commercialisation	Lent	Rapide

Technologies IoT: sous licence ou sans licence

Nom	LoRa	Sigfox	LTE-M	LTE NB-IoT
Description	Utilise la technologie à spectre étalé et est optimisé pour une longue durée de vie de la batterie.	Utilise la technologie Ultra Narrow Band pour offrir une longue durée de vie de la batterie et de faibles vitesses de transfert de données	Offre la plus large gamme de capacités IoT cellulaires	IoT cellulaire évolutif et ultra bas de gamme avec une couverture intérieure profonde
Fréquences	Sans licence	Sans licence	Avec licence	Avec licence
Déploiement	Bandes ISM	Bandes ISM	LTE en bande	LTE en bande et en bande de garde, autonome
Bandes	868/ 902-928Mhz	868/915 MHz	LTE bands 1, 2, 3, 5, 7, 8, 11,12, 13, 17, 18, 19, 20, 21, 26, 27, 28, 31(HD/FD – FDD) 39, 41 (TDD)	LTE bands 1, 2, 3, 5, 8, 12, 13, 17, 18, 19, 20, 26, 28, 66
Org standard.	LoRa Alliance	ETSI*	3GPP	3GPP
Couverture	153-161 dB	149-161 dB	155.7 dB (Classe de puissance 23 dBm) **	164 dB en mode autonome (classe de puissance 23 dBm) *
Max. Débit de données	50 kbps	100 bps	1 Mbps	~240kbps

La 5G et ses applications

Trois catégories de services activées par trois capacités



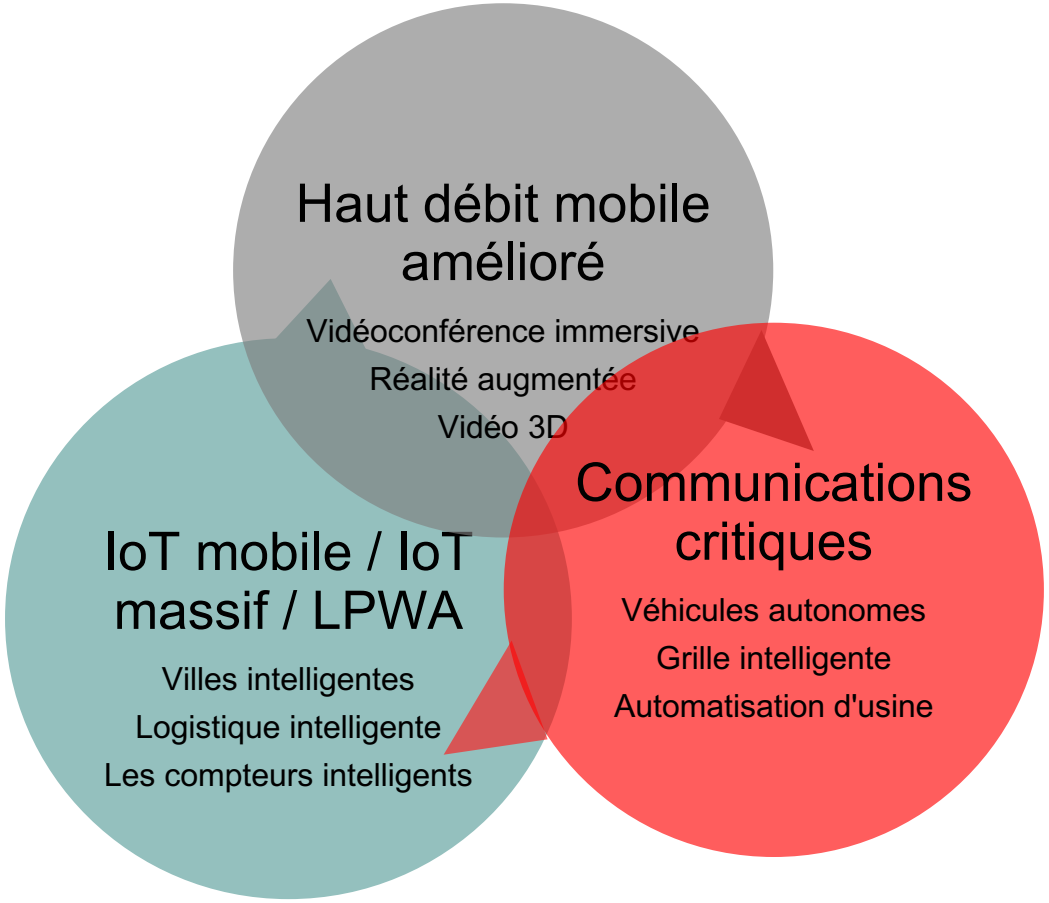
Source: ITU-R WP5D/TEMP/548-E: IMT Vision - "Framework and overall objectives of the future development of IMT for 2020 and beyond", February 2015

Les fondamentaux de la 5G

- Un «système de systèmes» répondant à une grande variété de cas d'utilisation
- Une nouvelle radio (par exemple, basée sur mmWave)
- Un nouveau cœur de réseau intégrant diverses technologies d'accès (HetNets)
- Un réseau flexible qui s'adapte au service (virtualisation)

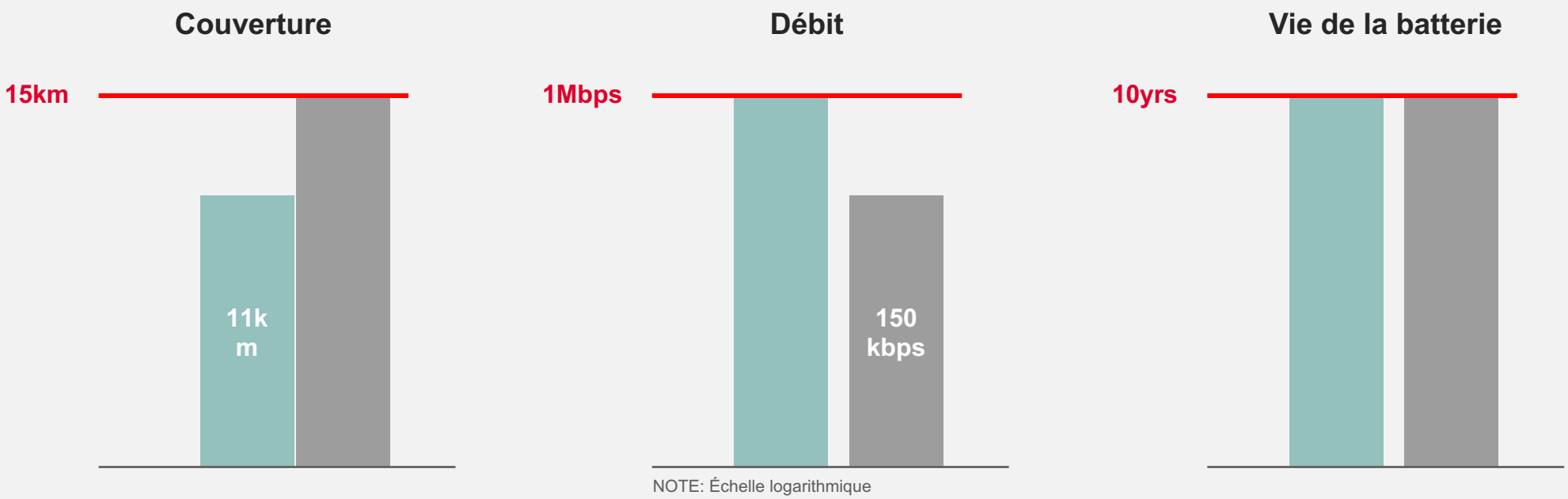
L'IoT mobile dans le futur de la 5G

- L'IoT mobile offre un IoT massif pour la 5G
- L'IoT mobile devrait coexister avec d'autres technologies 5G
- Le 3GPP continuera à traiter les cas d'utilisation LPWA par Mobile IoT dans les spécifications 5G
- Pour permettre une migration fluide des opérateurs vers les bandes 5G, 3GPP étudie comment le réseau central 5G prendra en charge le réseau d'accès radio mobile IoT.



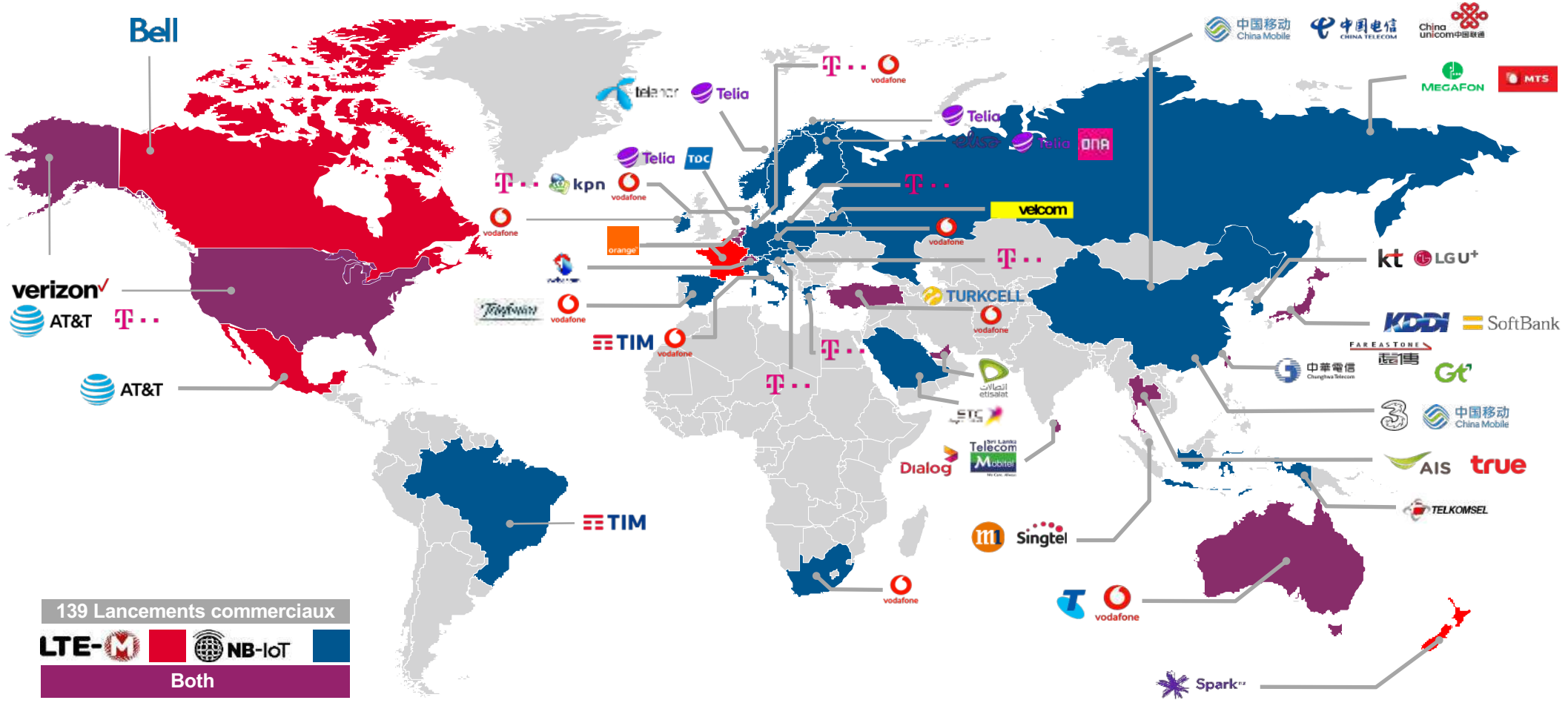
IoT et 5G

NB-IoT et LTE-M répondent déjà aux exigences 5G



Le 3GPP n'a pas l'intention de normaliser la technologie IoT spécifique à la 5G, mais pourrait le faire pour les applications IoT haut de gamme à l'avenir

Couverture IoT mobile



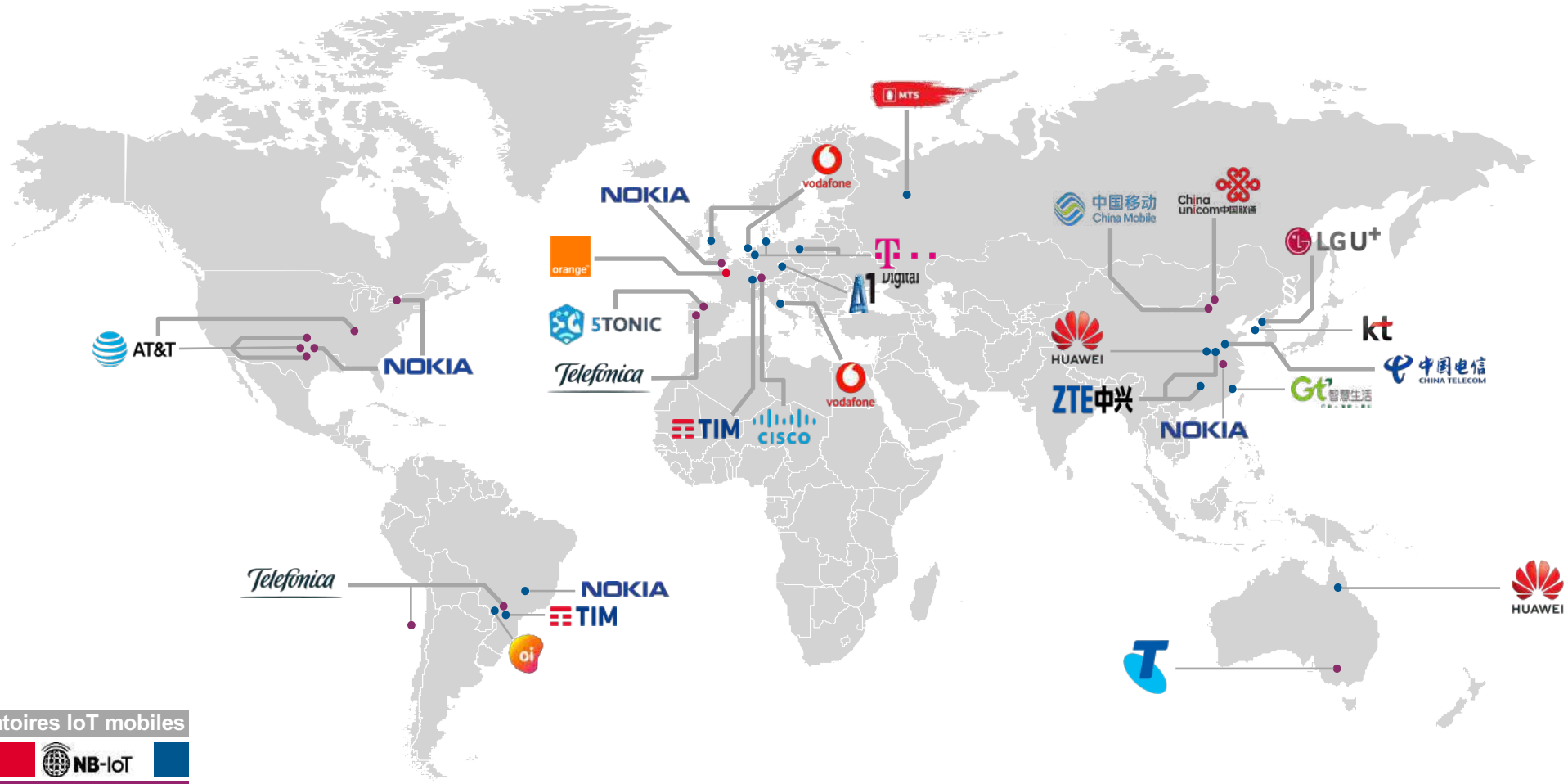
139 Lancements commerciaux

LTE-M NB-IoT

Both

*Au mois d'Août 2020

L'IoT mobile dans le futur de la 5G



Avantages socioéconomiques de l'IoT

Avantages sociaux

- 1 vie sur 9 sauvée dans des accidents de la route – GSMA
- 400 millions de personnes en plus nourries, en évitant les gaspillages de nourriture – GSMA
- 20 milliards de dollars d'économies par l'optimisation du trafic – PwC

Avantages économiques

- Impact économique en 2025 évalué entre 3 900 et 11 100 milliards de dollars – Mckinsey
- 14 400 milliards de dollars de revenus supplémentaires et de réductions de coûts – Cisco
- Plus de 5 600 milliards de dollars d'économies mondiales annuelles avec les voitures semi-autonomes et autonomes – Morgan Stanley

Applications et technologies IoT

Modèle d'étude de cas

Exigence d'application	Fonctionnalité de l'application
Zone réseau	▪ Large ▪ Local
Spectre	▪ Dédié ▪ partagé
Vie de la Batterie	▪ Longue ▪ Court ▪ N / A
Coût Connectivité	▪ Haute ▪ Moyen ▪ Faible
Coût Module	▪ Haute ▪ Moyen ▪ Faible
Largeur de Bande	▪ Haute ▪ Moyen ▪ Faible
Connectivity technology?	

Gestion à distance des ressources de l'industrie pétrolière

Fonctionnalité	Exigence
Zone réseau	▪ Large
Spectre	▪ Dédié
Vie Batterie	▪ N/A
Coût Connectivité	▪ Élevé
Coût Module	▪ Élevé
Bande Passante	▪ Basse à Élevée

Technologie de connectivité : **Satellite**

Autres technologies : 2G, 3G, 4G, LPWA

Laveuse intelligente

Fonctionnalité	Exigence
Zone réseau	▪ Locale
Spectre	▪ Partagé
Vie de la Batterie	▪ N/A
Coût Connectivité	▪ Bas
Coût Module	▪ Bas
Bande passante	▪ Moyenne

Technologie de connectivité : **Wi-Fi**

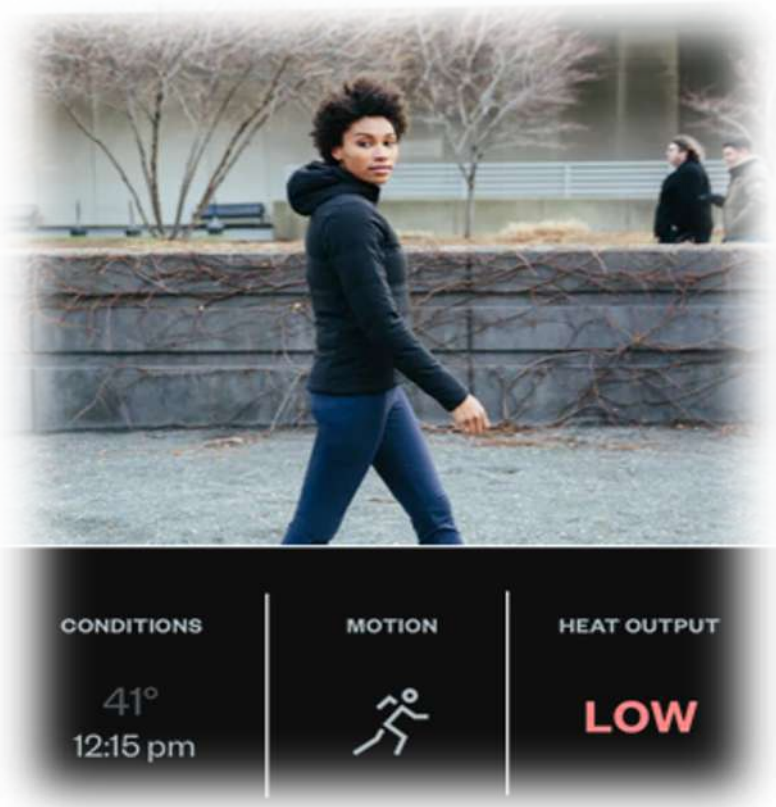
Autres technologies : 2G, 3G

Veste chauffante intelligente

Fonctionnalité	Exigence
Zone réseau	▪ Locale
Spectre	▪ Partagé
Vie Batterie	▪ Longue
Coût Connectivité	▪ Bas (ou pas)
Coût Module	▪ Bas
Bande Passante	▪ Basse

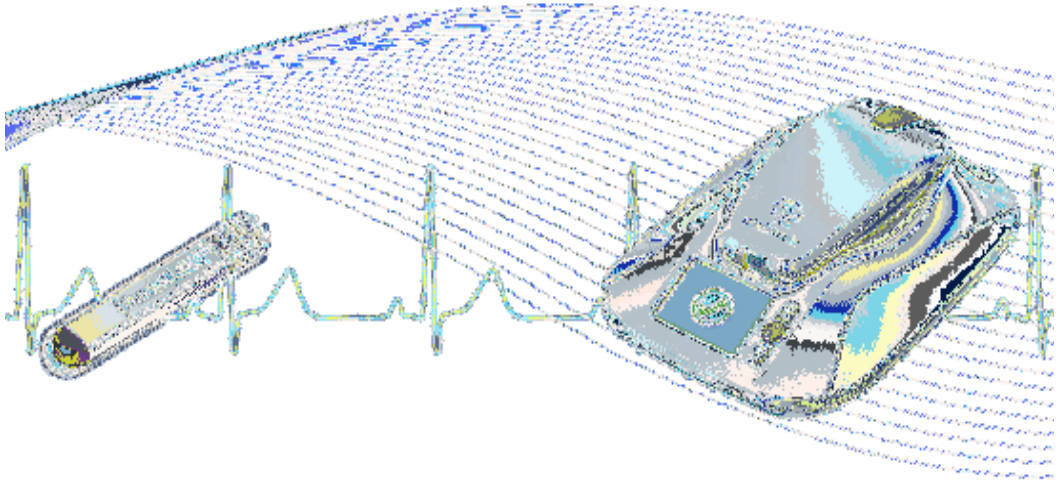
Technologie de connectivité : **Bluetooth**

Autres technologies : LPWA



Surveillance intelligente de la cybersanté

Fonctionnalité	Exigence
Zone réseau	▪ Large
Spectre	▪ Dédié
Vie Batterie	▪ N/A
Coût Connectivité	▪ Moyen
Coût Module	▪ Moyen
Bande Passante	▪ Moyenne



Technologie de connectivité : 3G

Autre Technologie: 4G

Caméra de surveillance HD

Fonctionnalité	Exigence
Zone réseau	▪ Large
Spectre	▪ Dédié
Vie Batterie	▪ N/A
Coût Connectivité	▪ Moyen
Coût Module	▪ Élevé
Bande Passante	▪ Élevée

Technologie Connectivité: 4G

Autres technologies: 3G, Wi-Fi

Pompe à eau intelligente

Fonctionnalité	Exigence
Zone réseau	▪ Large
Spectre	▪ Partagé
Vie Batterie	▪ N/A
Coût Connectivité	▪ Bas
Coût Module	▪ Bas
Bande Passante	▪ Basse

Technologie de connectivité : 2G

Autre technologie: LPWA

Capteurs de stationnement intelligents

Fonctionnalité	Exigence
Zone réseau	▪ Large
Spectre	▪ Partagé
Vie Batterie	▪ Longue
Coût Connectivité	▪ Bas
Coût Module	▪ Bas
Bande Passante	▪ Élevée

Technologie de connectivité : LPWA

Autres technologies: 2G, Wi-Fi

Activité

Capteurs contrôlant des paramètres de fonctionnement, comme la température et la pression

Champ pétrolier intelligent

Informe en cas de dégâts au niveau de la pompe

Pompe à eau intelligente

Capables de relever la fréquence cardiaque, l'emplacement GPS, l'itinéraire, la vitesse et l'altitude ; les données sont envoyées vers un téléphone mobile

T-shirt intelligent

Lave-linge intelligent

Lave-linge contrôlable à partir d'une application mobile

eSanté

Envoie les données sur le patient

Caméra de surveillance HD

Envoie la vidéo accessible via une application mobile

Surveille le niveau de remplissage de la poubelle

Poubelles intelligentes

Contrôle l'emplacement du parc et les habitudes de conduite

Système de suivi de parc

Leviers Réglementaires Spectraux pour soutenir l'IoT

1. Neutralité technologique

Les licences spécifiques à une technologie risquent d'empêcher les fournisseurs de services de déployer les dernières technologies IoT cellulaires.

2. Licence Spectrale

Le spectre sans licence a sa place dans l'écosystème IoT.

Mais le spectre sous licence est uniquement capable de fournir des garanties de qualité de service.

3. Spectre mis de côté

Mettre de côté le spectre pour l'IoT risque de gaspiller un spectre précieux.

4. Harmonisation du spectre

Des bandes de spectre largement harmonisées permettent de réaliser des économies d'échelle pour réduire le coût des appareils IoT.

5. La planification est la clé!

L'IoT jouera un rôle important dans la 5G et doit donc être inclus dans la planification continue du spectre.

MERCI POUR VOTRE ATTENTION

Études de l'UIT-R à l'appui de l'Internet des objets

L'Internet des objets

L'IoT **permet de détecter ou de contrôler à distance un large éventail de dispositifs** et **d'échanger des données via une connexion à l'infrastructure du réseau Internet**.

L'IoT a de **très nombreuses applications**, allant des **vêtements intelligents** aux **villes intelligentes**, en passant par les **systèmes de surveillance mondiaux**.

Pour répondre à ces nombreuses exigences, **des technologies d'accès, filaires et hertziennes, sont nécessaires** pour permettre l'accès au réseau.

Les connexions des applications IoT **utilisant des technologies filaires et des technologies hertziennes à courte portée** sont **désormais complétées par le déploiement de réseaux étendus à faible puissance et de systèmes mobiles cellulaires et à satellites optimisés**.

Accès hertzien

Les **besoins de spectre et les normes** pour les **technologies et techniques d'accès hertzien à l'IoT** sont **actuellement examinés au sein de l'UIT-R**, notamment :

- **la protection des services de radiocommunication** contre les émissions des systèmes de courants porteurs en ligne;
- **l'harmonisation des gammes de fréquences et les paramètres techniques et opérationnels** utilisés pour l'exploitation des **dispositifs à courte portée (SRD);**
- les normes pour les **systèmes de réseau étendu de capteurs et d'actionneurs (WASN);**
- Les besoins de spectre pour la mise en œuvre des **infrastructures de communication de type machine, à bande étroite et large bande;**
- la prise en charge des **communications massives de type machine** dans le cadre des **normes et des besoins de spectre pour les IMT évoluées (4G) et les IMT-2020 (5G);**
- l'utilisation des **communications du service fixe par satellite et du service mobile par satellite** pour l'IoT.

Résolution UIT-R 66-1: *Poursuite des études relatives aux systèmes et applications sans fil pour le développement de l'Internet des objets*

- **Différentes bandes de fréquences**, dont beaucoup permettent de mettre à disposition **des canaux de communication, des infrastructures et des capacités**, pourraient être utilisées afin **d'assurer un déploiement de l'IoT présentant un bon rapport coût/efficacité et une utilisation efficace du spectre des fréquences radioélectriques.**
- L'IoT est un **concept qui englobe diverses plates-formes, applications et technologies** qui sont, et continueront d'être, **mises en œuvre dans le cadre de plusieurs services de radiocommunication.**
- Pour mettre en œuvre l'IoT, **il n'est pas nécessaire actuellement de prévoir des dispositions réglementaires particulières dans le Règlement des radiocommunications.**

➢ L'UIT-R poursuit ses **études sur les aspects techniques et opérationnels** des **réseaux et systèmes de radiocommunication pour l'IoT.**

➢ Élaboration de Recommandations, de Rapports et/ou de Manuels UIT-R, selon le cas, sur la base des études.

Source: Résolution UIT-R 66 http://www.itu.int/pub/R-RES-R.66

Courants porteurs en ligne (CPL)

- Au titre de la Question **UIT-R 221-2/1**, il est demandé d'étudier les niveaux de rayonnements acceptables **émis par les systèmes de télécommunication utilisant le réseau d'alimentation électrique filaire** pour ne pas nuire à la qualité de fonctionnement des systèmes de radiocommunication.

- **Les Rapports UIT-R SM.2158 et UIT-R SM.2212 sur l'Incidence des systèmes CPL sur les systèmes de radiocommunication fonctionnant au-dessous de 80 MHz et dans les bandes d'ondes métriques et décimétriques au-dessus de 80 MHz.**
  - ✓ Illustrent les risques que des brouillages soient causés à divers services de radiocommunication en présence d'émissions/rayonnements émanant de systèmes et dispositifs CPL.
  - ✓ Décrivent les caractéristiques des émissions/rayonnements radioélectriques des systèmes CPL ainsi que les caractéristiques et les critères de protection des systèmes de radiocommunication.
  - ✓ Examinent les méthodes susceptibles d'atténuer les brouillages émanant des émissions CPL.

- Études en cours sur l'examen des risques de brouillage liés à **l'utilisation de techniques de diversité MIMO pour les systèmes de réseau domestique basés sur les CPL.**

Sources: Question UIT-R 221-2/1 http://www.itu.int/pub/R-QUE-SG01.221
Rapport UIT-R SM.2158 http://www.itu.int/pub/R-REP-SM.2158
Rapport UIT-R SM.2212 http://www.itu.int/pub/R-REP-SM.2212

Études menées principalement par le GT 1A de l'UIT-R

Réseau de distribution électrique et réseau intelligent pour services collectifs

- Au titre de la Question **UIT-R 236/1**, il est demandé d'étudier notamment:
  les débits de données, les largeurs de bande, les bandes de fréquences et les besoins de spectre **nécessaires pour** les systèmes de gestion des réseaux de distribution électrique **ainsi que** les problèmes de brouillage que la **mise en œuvre des technologies et dispositifs hertziens ou filaires** utilisés pour les **systèmes de gestion des réseaux de distribution électrique** pose pour les systèmes de radiocommunication.

- **Le Rapport UIT-R SM.2351 sur les systèmes de gestion des réseaux intelligents pour services collectifs**
  - ✓ Contient une description générale des systèmes de réseaux intelligents (technologies de réseau, objectifs et avantages, aperçu de l'architecture de référence, normes (y compris sans fil), etc.).
  - ✓ Aborde les problèmes de brouillages associés à la mise en œuvre de technologies hertziennes ou filaires de transmission de données utilisées dans les systèmes de gestion des réseaux de distribution d'électricité.
  - ✓ Traite des incidences du déploiement à grande échelle des réseaux filaires et hertziens utilisés pour les systèmes de gestion des réseaux de distribution d'électricité sur la disponibilité du spectre.

- Études en cours pour mettre à jour ce Rapport concernant **l'utilisation de technologies hertziennes à bande étroite et de technologies IMT large bande** pour la gestion des réseaux intelligents et les compteurs intelligents.

Sources: Question UIT-R 236/1 http://www.itu.int/pub/R-QUE-SG01.236
Rapport UIT-R SM.2351 http://www.itu.int/pub/R-REP-SM.2351

Dispositifs à courte portée (SRD)

- **Assurer l'harmonisation pour les SRD** pour permettre des économies d'échelle; des avancées technologiques/ des gammes d'accord; un partage de fréquences; une intégration dans des produits grand public qui franchissent les frontières.
  - ✓ Harmonisation des paramètres techniques et opérationnels (utilisation de technologies évoluées).
  - ✓ Procédures de mesure pour vérifier ces paramètres et assurer la protection des services de radiocommunication.
  - ✓ Déploiement dans des bandes spécifiques, harmonisées à l'échelle mondiale ou régionale (possibilité de faciliter l'utilisation de certaines bandes de fréquences/gammes d'accord, de préférence à l'échelle mondiale ou régionale).
  - ✓ Reconnaissance du rôle joué par certains SRD dans l'Internet des objectifs (IoT).
- Paramètres techniques et opérationnels et utilisation du spectre pour les SRD (Rap. UIT-R SM.2153).
- Gammes de fréquences harmonisées à l'échelle mondiale/régionale pour les SRD (Rec. UIT-R SM.1896)
  - Nouvelle gamme envisagée autour de 1,6 GHz pour les systèmes de correction auditive.
- Harmonisation mondiale des catégories de SRD (Rec. UIT-R SM.2103).
- Possibilités de contribuer à la prochaine réunion du GT 1B (24 nov.-2 déc. 2020)

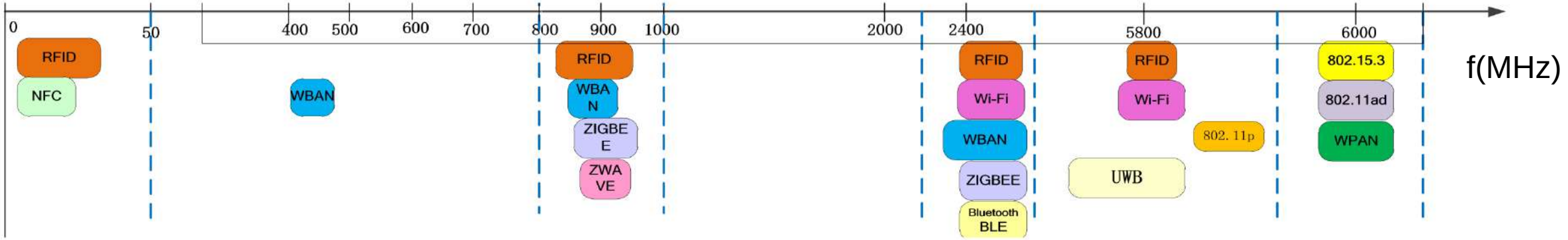
Source: Résolution UIT-R 54-2 http://www.itu.int/pub/R-RES-R.54

Études menées principalement par le GT 1B de l'UIT-R

Applications types prises en charge par les SRD

Catégorie	Applications	Technologies
Réseaux personnels (PAN)	Casques d'écoute, liaisons entre dispositifs (par exemple entre dispositif médical/sportif et iPhone)	Bluetooth®(2,4 GHz)
Réseaux domestiques (HAN)	Alarmes, domotique, éclairage intelligent (< GHz)	ZigBee® (2,4 GHz), KNX® (868-870 MHz), réseaux large bande tels que IEEE 802.11ah (< GHz)
RFID (voir le Rapport UIT-R SM.2255)	Lecture d'étiquette, tickets, cartes de paiement, péage	< GHz (plan à 4 canaux) et 2,4 GHz
Réseaux métropolitains (MAN)	Applications de détection et de commande	Réseaux étendus à faible puissance (LPWAN – LoRa™ et SigFox) (< GHz); Wi-SUN (< GHz) Réseaux de compteurs à faible débit (169 MHz)
Communications M2M par satellite	Suivi de camions, lecture de capteurs à distance	À l'étude dans la bande 862-863 MHz

Technologies SRD largement déployées dans des bandes au-dessous de 6 GHz



Source: Présentations lors de l'atelier de l'UIT sur la gestion du spectre pour le déploiement de l'IoT (www.itu.int/go/ITU-R/RSG1SG5-IoT-16)

LPWAN et VLC

- **Réseaux étendus à faible puissance (LPWAN) pour les communications de type machine et l'IoT dans des gammes de fréquences harmonisées exploités dans le cadre de la réglementation relative aux SRD** – Le Rap. UIT-R SM.2423:
  - ✓ Décrit certains **aspects opérationnels et techniques des LPWAN.**
  - ✓ Explique que la **réglementation relative aux SRD s'applique aux LPWAN (régime d'autorisation général**, ou **exemption de licence**).
  - ✓ Présente certaines applications utilisant les LPWAN pour les villes intelligentes, la fabrication, la domotique, l'environnement et l'agriculture, les transports et la logistique, l'énergie et les services publics (par exemple avec de nombreux dispositifs transmettant quelques messages par jour).
  - ✓ Indique certaines **gammes de fréquences** utilisées pour les LPWAN dans la **Région 1: 865-870 MHz**, la **Région 2: 902-928 MHz** et la **Région 3: 915-925 MHz**.

Études menées principalement par le GT 1B de l'UIT-R

- Rap. UIT-R SM.2422 sur la **lumière visible pour les communications large bande (VLC)** utilisant les **communications par capteur d'image ou par récepteur à photodiode à bas débit** convenant **pour différentes applications telles que l'IoT** (longueurs d'onde généralement comprises entre 390 et 750 nm).
- Possibilités de contribuer à la prochaine réunion du GT 1A (24 nov.-2 déc. 2020).

Sources: Rapport UIT-R SM.2423 http://www.itu.int/pub/R-REP-SM.2423 sur les LPWAN
Question UIT-R 238/1 http://www.itu.int/pub/R-QUE-SG01.238 sur la VLC
Rapport UIT-R SM.2422 http://www.itu.int/pub/R-REP-SM.2422 sur la VLC

Études menées principalement par le GT 1A de l'UIT-R

Systèmes de réseau étendu de capteurs et d'actionneurs (WASN)

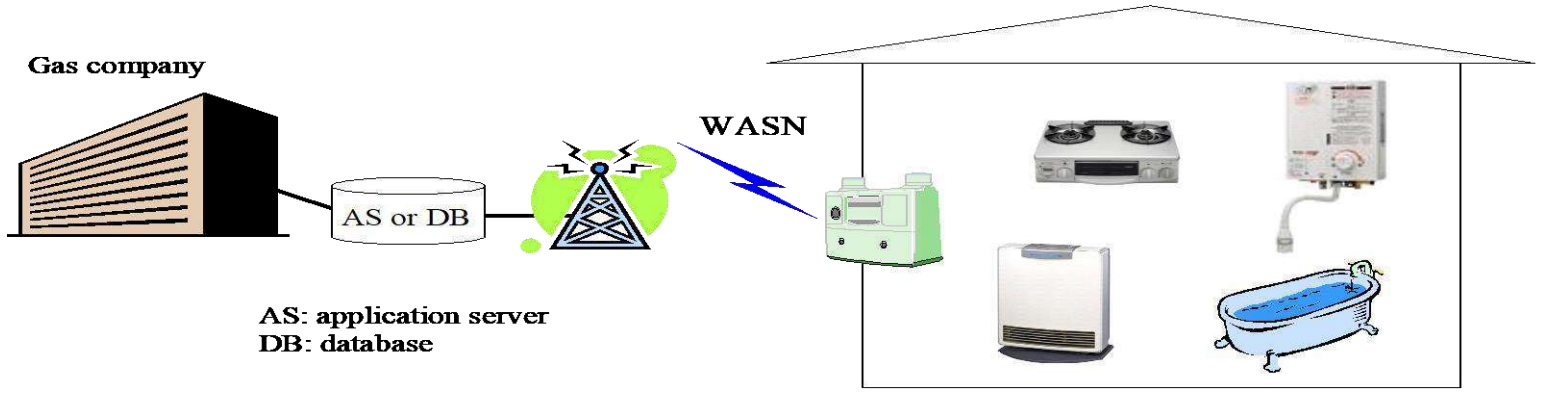
Les systèmes de réseau étendu de capteurs et/ou d'actionneurs (WASN) prennent en charge les communications de machine à machine vers un grand nombre de capteurs et/ou d'actionneurs.

- Recommandation UIT-R M.2002 *"Objectifs, caractéristiques et exigences fonctionnelles des systèmes de réseau étendu de capteurs et/ou d'actionneurs (WASN)"*. Le principal objectif des systèmes WASN est de prendre en charge des applications de service de machine à machine indépendamment de l'emplacement des machines.
- Rapport UIT-R M.2224 *"Lignes directrices concernant la conception des systèmes de réseau étendu de capteurs et/ou d'actionneurs (WASN)"*. Ce Rapport donne des informations détaillées concernant la politique de conception des systèmes, les applications hertziennes et des exemples de systèmes WASN pour le partage d'informations.

Études menées par le GT 5A de l'UIT-R

WASN – 2 fonctionnalités de réseau principales

- *Détection automatique et collecte d'informations*: recueille automatiquement les informations acquises par les capteurs et les envoie à des serveurs d'application (AS) ou à des bases de données (DB) via le réseau central.



- *Commande d'actionneurs à distance*: commande à distance les actionneurs en utilisant les serveurs d'application (AS) via le réseau central.

Applications MTC basées ou non sur les IMT

- **Les aspects techniques et opérationnels des réseaux et des systèmes radioélectriques utilisant la composante de Terre des IMT** pour prendre en charge **des applications de communications de type machine (MTC)**, ainsi que les besoins de spectre, y compris la possibilité d'une utilisation harmonisée du spectre pour permettre la mise en place des infrastructures et des dispositifs MTC à bande étroite et large bande, font l'objet du Rapport UIT-R M.2440.

- Le Rapport UIT-R M.2479 contient d'autres informations sur **diverses applications d'automatisation dans le secteur des communications hertziennes** (automatisation d'usine, automatisation de processus, interaction audiovisuelle, télécommande, robots mobiles et véhicules, allant d'applications à faible temps de latence (par exemple bras de robot) à des applications fiables et sécurisées (par exemple systèmes de transports autonomes sans conducteur). Il contient aussi des informations sur les applications MTC dans les réseaux électriques intelligents, par exemple le contrôle de la charge précis à la milliseconde près, l'automatisation de la distribution, l'acquisition d'informations relatives à l'électricité, la surveillance de la production décentralisée, les stations de recharge des véhicules électriques, ainsi que des exemples de bandes de fréquences utilisées pour les applications IoT/M2M.

Sources: Rapport UIT-R M.2440 http://www.itu.int/pub/R-REP-M.2440 sur les MTC basées sur les IMT
Rapport UIT-R M.2479 http://www.itu.int/pub/R-REP-M.2479 sur les MTC non basées sur les IMT

Études menées par le GT 5A et le GT 5D de l'UIT-R

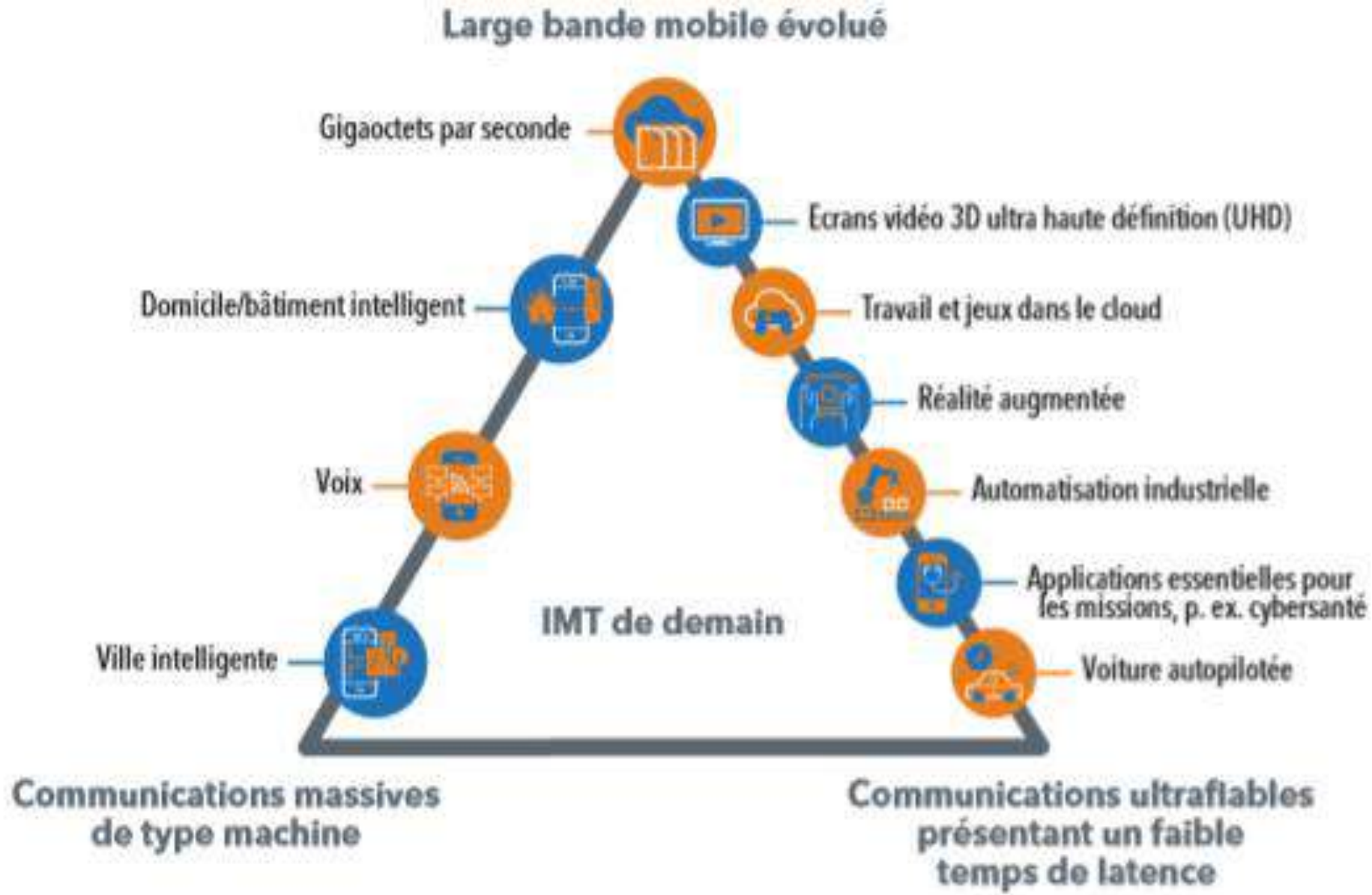
IMT – Télécommunications mobiles internationales

Prise en charge de l'IoT par les IMT:

- À court terme, la norme 4G (IMT évoluées) actuelle (Rec. ITU-R M.2012) est complétée afin d'inclure la prise en charge de l'IoT (par exemple les systèmes NB-IoT).
- À plus long terme, l'IoT est considéré comme faisant partie intégrante de la norme 5G (IMT-2020) en cours d'élaboration à l'UIT, ce qui permet d'étendre les avantages des IMT en termes d'économies d'échelle massives et de normes et de fréquences harmonisées au niveau mondial à tous les secteurs d'activité.
- Le cadre et les objectifs généraux du développement futur des IMT à l'horizon 2020 et au-delà sont décrits en détail dans la Recommandation UIT-R M.2083.

Études menées par le GT 5D de l'UIT-R

Scénarios d'utilisation de la 5G



Intégration des **systèmes à satellites** dans les technologies d'accès de prochaine génération

Les satellites permettent de couvrir une vaste zone et offrent souvent un débit élevé, ce qui rend possible:

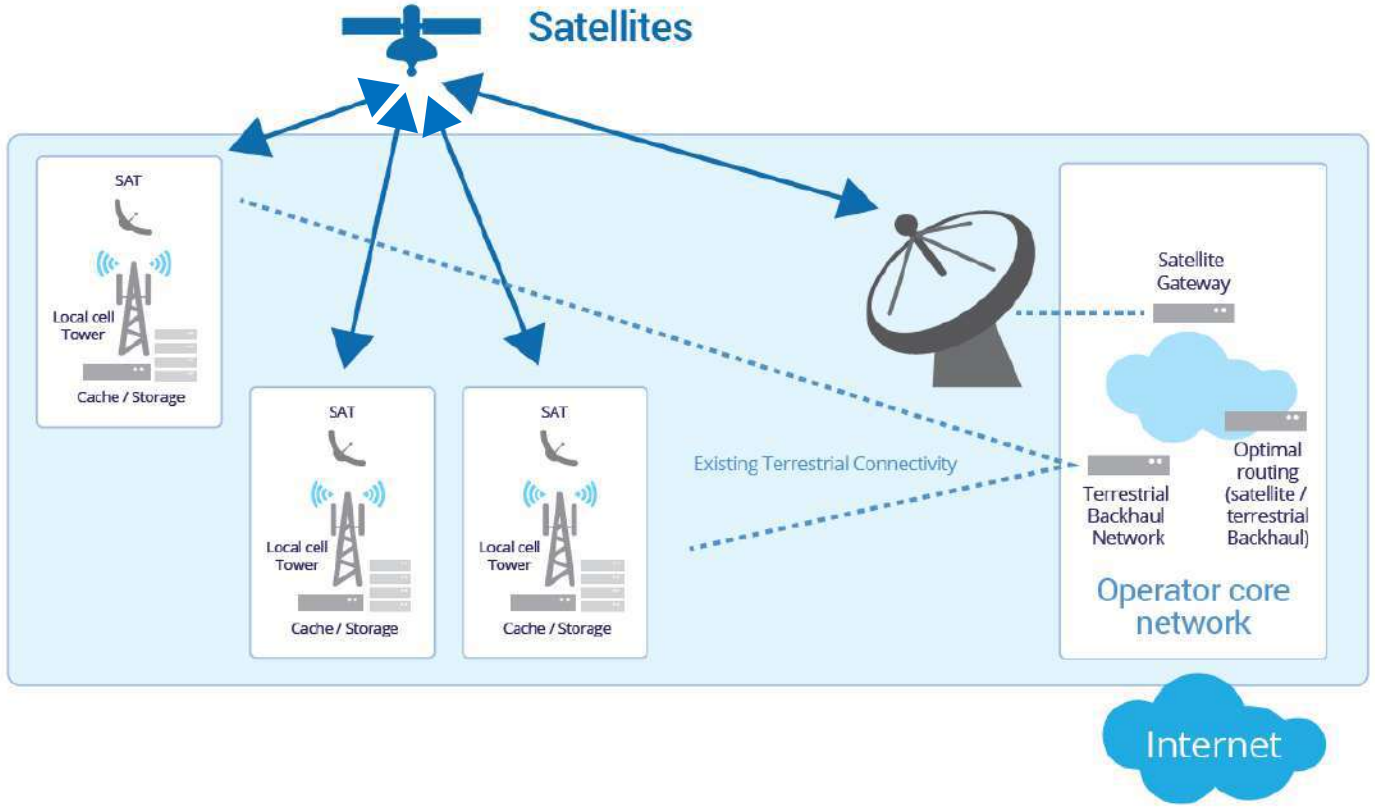
- La modulabilité: l'utilisation de capacités de multidiffusion sur une vaste zone avec mise en cache locale simultanée dans le nuage au plus près de l'utilisateur final permet d'obtenir des avantages importants liés au multiplexage statistique et d'assurer ainsi une plus grande efficacité d'utilisation de la bande passante globale et une plus grande fiabilité du service.
- Le déploiement rapide de la connectivité: les stations au sol de systèmes à satellites peuvent être déployées rapidement pour connecter n'importe quel endroit se trouvant dans la zone de couverture des satellites, permettant ainsi de connecter des villes, des villages, des entreprises et des foyers avec une qualité de service prévisible. En outre, les réseaux à satellite sont résistants en cas d'attaque physique ou de catastrophe naturelle, caractéristique qui permet de garantir des communications sécurisées.

Les satellites pourront ainsi contribuer à faciliter le développement des technologies d'accès de prochaine génération. Les systèmes à satellites géostationnaires ou non géostationnaires offrent des avantages uniques pour ce qui est des technologies d'accès de prochaine génération.

Source: Rapport UIT-R M.2460 http://www.itu.int/pub/R-REP-M.2460

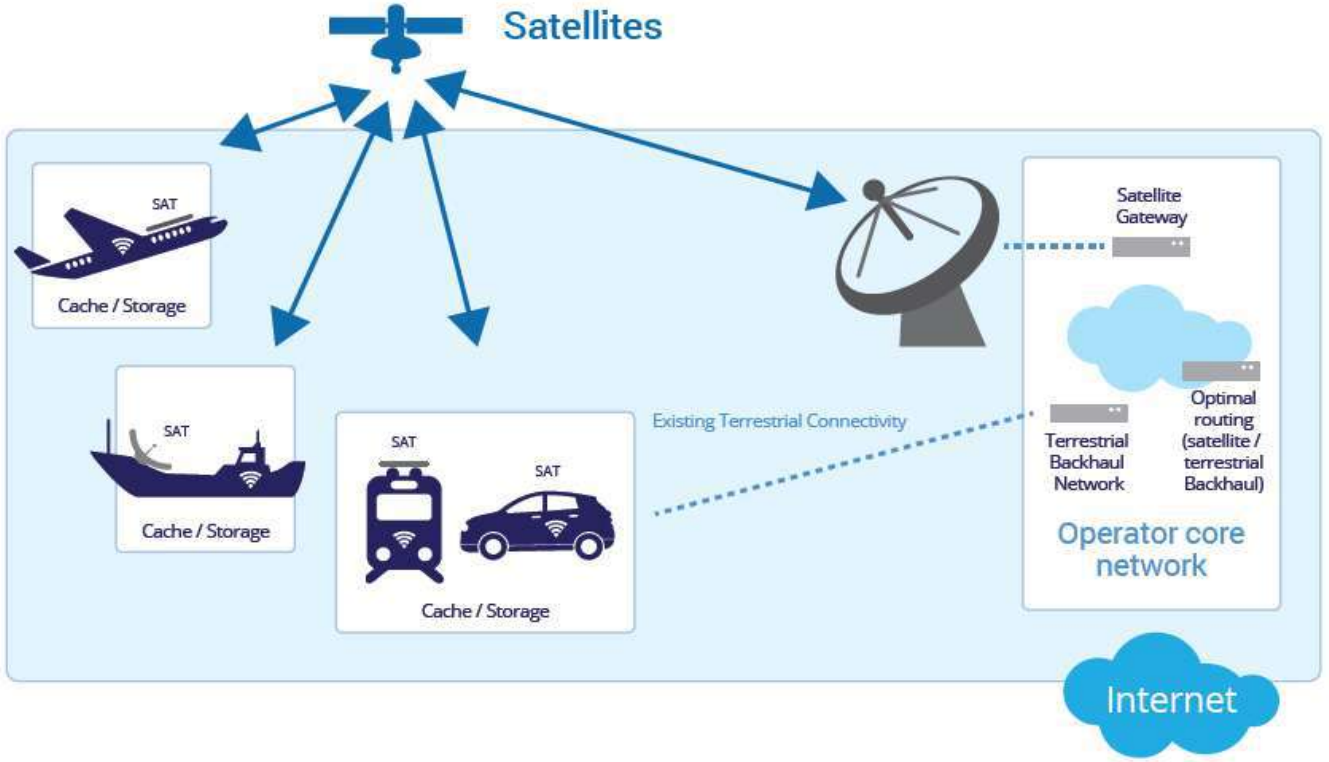
Études menées par le GT 4B de l'UIT-R

Exemple de cas d'utilisation – Station de base de raccordement et de multidiffusion



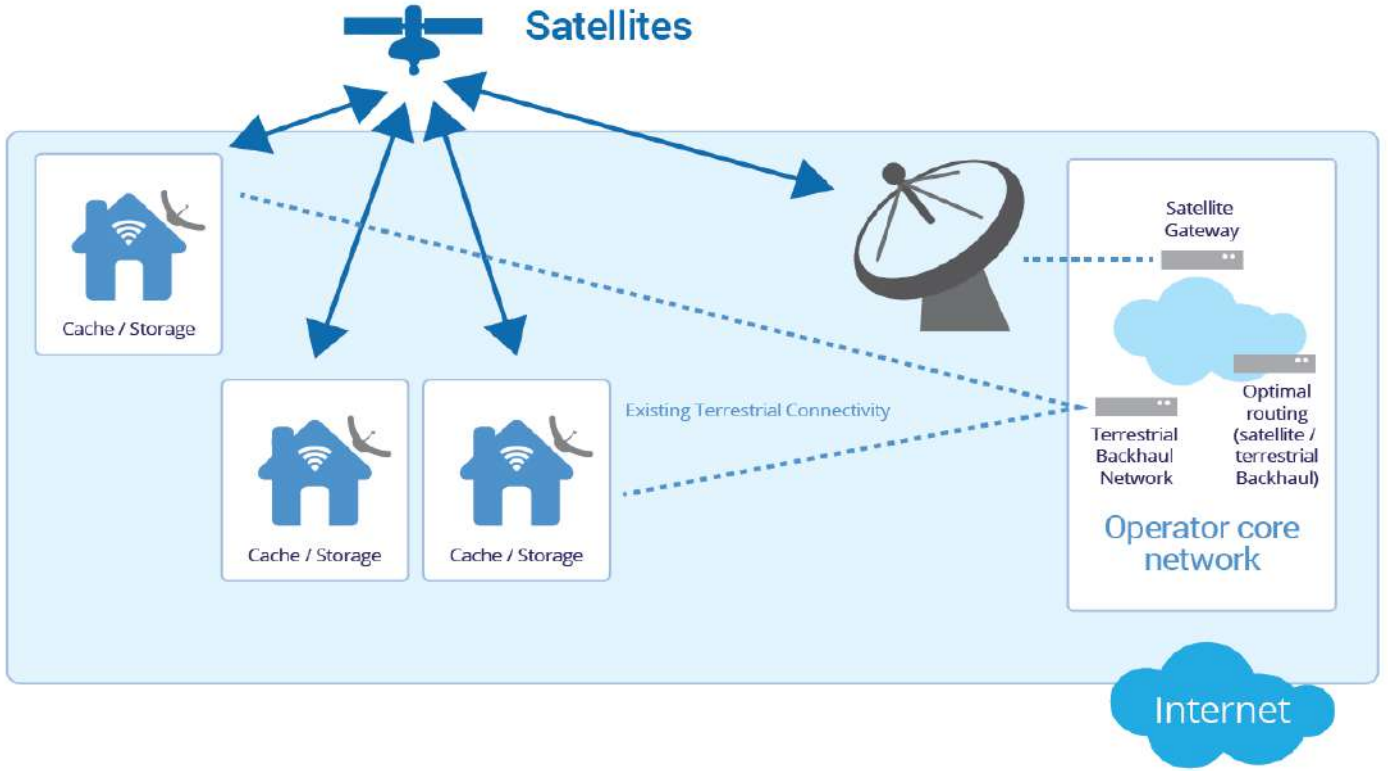
Une liaison directe à haut débit, de multidiffusion, entre des satellites géostationnaires ou non géostationnaires et des stations de base complète la connectivité de Terre existante pour assurer un raccordement vers différentes cellules avec la possibilité de multidiffuser le même contenu (par exemple vidéo, TV HD/UHD, données autres que vidéo) sur une vaste zone de couverture et assurer un raccordement efficace pour le trafic IoT agrégé provenant de plusieurs sites.

Exemple de cas d'utilisation - Communications en déplacement



Une liaison à haut débit, de multidiffusion, entre des satellites géostationnaires ou non géostationnaires et des avions, des véhicules, des trains et des navires (navires de croisière et autres navires transportant des passagers), permet de transmettre en unidiffusion un contenu à la demande (par exemple, TVIP over-the-top) ou de multidiffuser le même contenu (par exemple, vidéo, TV HD/UHD, données autres que vidéo telles que FOTA/SOTA) sur une vaste zone de couverture (par exemple pour le stockage local et la consommation). La même capacité permet également d'assurer une connectivité directe efficace pour les dispositifs des utilisateurs finals ou les capteurs et pour le trafic IoT agrégé provenant de ces plates-formes en mouvement.

Exemple de cas d'utilisation – Multiplay hybride



Une liaison à haut débit, de multidiffusion, via des satellites géostationnaires ou non géostationnaires permet de compléter la connectivité de Terre existante ou d'interagir avec elle, ainsi que d'assurer une connectivité large bande directe avec la possibilité de multidiffuser le même contenu (vidéo, TV HD/UHD, données autres que vidéo) sur une vaste zone de couverture (par exemple pour le stockage local et la consommation) pour la distribution au domicile ou au bureau par WiFi ou femto et nano-cellules, et la télévision par satellite DTH, intégrée dans le réseau IP au domicile ou au bureau. La même capacité permet également d'assurer une connectivité efficace pour les données IoT agrégées.

Systèmes du SMS à bande étroite à l'ordre du jour de la CMR-23 (point 1.18)

- Études portant sur les **besoins de spectre et d'éventuelles nouvelles attributions** au **service mobile par satellite (SMS)** pour le **développement futur des systèmes du SMS à bande étroite**, conformément à la Résolution **248 (CMR-19)**.
- **Bandes de fréquences à envisager** au titre de ce point de l'ordre du jour:
  - **1 695-1 710 MHz dans la Région 2** • **2 010-2 025 MHz dans la Région 1**
  - **3 300-3 315 MHz et 3 385-3 400 MHz dans la Région 2**.
- **Études actuellement menées par l'UIT-R** sur **les besoins de spectre et les exigences opérationnelles** ainsi que sur **les caractéristiques des systèmes à faible débit** pour la **collecte de données depuis des dispositifs de Terre du SMS et la gestion de ces dispositifs**.
- Le point 2.13 de l'ordre du jour préliminaire de la CMR-27, s'il est confirmé à la CMR-23, vise à permettre d'envisager une **éventuelle attribution à l'échelle mondiale au SMS** dans la gamme [1,5-5] GHz aux mêmes fins.

Sources:
Rés. 248 (CMR-19) https://www.itu.int/dms_pub/itu-r/oth/0c/0a/R0C0A00000D0018PDFE.pdf
Rés. 811 (CMR-19) – Ordre du jour de la CMR-23 https://www.itu.int/dms_pub/itu-r/oth/0c/0a/R0C0A00000D0041PDFE.pdf
Rés. 812 (CMR-19) – Ordre du jour préliminaire de la CMR-27 https://www.itu.int/dms_pub/itu-r/oth/0c/0a/R0C0A00000D0040PDFE.pdf

Études menées principalement par le GT 4C de l'UIT-R

Résumé

- **Diverses technologies radioélectriques seront utilisées pour mettre en œuvre l'Internet des objets**, allant des **dispositifs à courte portée** aux **réseaux étendus de capteurs** en passant par les **systèmes mondiaux IMT de Terre** et les **systèmes à satellites**.
- Les **Commissions d'études de l'UIT-R élaborent actuellement des normes techniques et opérationnelles** pour **faciliter le déploiement de l'IoT au niveau mondial**, et s'intéressent aux **bandes de fréquences harmonisées** et aux **régimes réglementaires appropriés.**
- Les aspects associés relatifs **aux attributions de fréquences et au cadre réglementaire pour les services de radiocommunication concernés seront également abordés** lors de la prochaine Conférence mondiale des radiocommunications de 2023 de l'UIT (**CMR-23**).

➢**Votre participation à ces activités est vivement souhaitée !**

Merci!

Commissions d'études de l'UIT-R : www.itu.int/ITU-R/go/rsg; Courriel: brsgd@itu.int

Commission d'études 1 de l'UIT-R – Gestion du spectre
www.itu.int/ITU-R/go/rsg1 ; Courriel: rsg1@itu.int

Commission d'études 4 de l'UIT-R – Services par satellite
www.itu.int/ITU-R/go/rsg4 ; Courriel: rsg4@itu.int

Commission d'études 5 de l'UIT-R – Services de Terre
www.itu.int/ITU-R/go/rsg5 ; Email: rsg5@itu.int

Complément d'information sur certains points et certaines questions à l'ordre du jour de la CMR-23

Point de l'ordre du jour	Résolution de la CMR	Groupe(s) responsable(s)	Thème du point de l'ordre du jour/de la question
1.1	Rés.223 (Rév.CMR-19)	GT 5B et GT 5D	examiner, sur la base des résultats des études menées par l'UIT-R, les mesures qui pourraient être prises pour assurer, dans la **bande de fréquences 4 800-4 990 MHz**, la protection des stations du service mobile aéronautique et du service mobile maritime situées dans l'espace aérien international et dans les eaux internationales vis-à-vis d'autres stations situées sur le territoire des pays, et examiner le critère de puissance surfacique figurant dans le renvoi **5.441B** conformément à la Résolution **223 (Rév.CMR-19)**
1.2	Rés.245 (CMR-19)	GT 5D	envisager l'identification des bandes de fréquences **3 300-3 400 MHz, 3 600-3 800 MHz, 6 425-7 025 MHz, 7 025-7 125 MHz et 10,0-10,5 GHz** pour les Télécommunications mobiles internationales (IMT), y compris des attributions additionnelles possibles au **service mobile** à titre primaire, conformément à la Résolution **245 (CMR-19)**
1.3	Rés.246 (CMR-19)	GT 5A	envisager l'attribution à titre primaire de la bande de fréquences **3 600-3 800 MHz** au **service mobile** en Région 1 et prendre les mesures réglementaires appropriées, conformément à la Résolution **246 (CMR-19)**
1.4	Rés.247 (CMR-19)	GT 5D	examiner, conformément à la Résolution **247 (CMR-19)**, l'utilisation de stations placées sur **des plates-formes à haute altitude en tant que stations de base IMT (HIBS)** dans le **service mobile** dans certaines bandes de fréquences **au-dessous de 2,7 GHz** qui sont déjà identifiées pour les IMT à l'échelle mondiale ou régionale
1.5	Rés.235 (CMR-15)	GA 6/1	examiner **l'utilisation du spectre et les besoins de spectre des services existants** dans la bande de fréquences **470-960 MHz** en Région 1 et envisager les mesures réglementaires qui pourraient être prises dans la bande de fréquences **470-694 MHz** en Région 1 compte tenu de l'examen effectué conformément à la Résolution **235 (CMR-15)**
1.10	Rés.430 (CMR-19)	GT 5B	procéder à des études sur les besoins de spectre, la coexistence avec les services de radiocommunication et les mesures réglementaires à prendre en vue de faire de **nouvelles attributions éventuelles au service mobile aéronautique** pour l'utilisation des **applications du service mobile aéronautique non liées à la sécurité**, conformément à la Résolution **430 (CMR-19)**
1.18	Rés.248 (CMR-19)	GT 4C	examiner les études portant sur les **besoins de spectre et envisager d'éventuelles nouvelles attributions** au **service mobile par satellite** pour le développement futur des systèmes mobiles à satellites à bande étroite, conformément à la Résolution **248 (CMR-19)**

Source: www.itu.int/go/rcpm-wrc-23-studies

SRD - Termes et définitions

Dispositifs (de radiocommunication) à courte portée

- Dans le cadre du Rapport UIT-R SM.2153, le terme SRD désigne les émetteurs radioélectriques qui assurent des communications unidirectionnelles ou bidirectionnelles et pour lesquels la probabilité de causer des brouillages à d'autres équipements de radiocommunication est faible.
- Les SRD sont autorisés à fonctionner à condition de ne pas causer de brouillage et de ne pas demander de protection, sous réserve des normes ou des réglementations nationales applicables.
- Il est possible d'appliquer des conditions simples d'octroi de licence (licences générales ou assignations générales de fréquence voire dispense de licence), mais il convient toutefois d'obtenir des informations sur les conditions réglementaires régissant la mise sur le marché et l'utilisation d'équipements SRD en prenant contact avec chacune des administrations nationales concernées.

Technologie à bande ultralarge (UWB): technologie destinée aux SRD, impliquant la production et l'émission volontaires d'énergie radioélectrique occupant une très large gamme de fréquences susceptible de couvrir plusieurs bandes de fréquences attribuées aux services de radiocommunication (voir par exemple la Rec. UIT-R SM.1755 et la Rec. UIT-R SM.1756).

Utilisation des SRD dans un grand nombre de pays et de régions

- Rapport UIT-R SM.2153 - Paramètres techniques et de fonctionnement des SRD et fréquences utilisées.
  - Définit les SRD et décrit brièvement différentes applications utilisant les SRD, par exemple: télécommande, télémesure, voix et vidéo, détection de victimes d'avalanche, RLAN, applications ferroviaires, télématique pour le transport et le trafic routiers, détecteurs de mouvements et équipements d'alerte, alarmes, commande de modèles réduits, applications inductives (par exemple accès aux voitures), microphones hertziens, RFID, implants médicaux actifs à ultra faible puissance, applications audio sans fil (par exemple haut-parleurs sans fil), indicateurs de niveau RF (radar), etc.
  - Indique les caractéristiques techniques types/limitations: gammes de fréquences communes; valeurs requises de puissance rayonnée ou de champ magnétique/électrique pour permettre un fonctionnement satisfaisant (pour les pays de la CEPT, USA(FCC)/B/CAN, J et KOR, etc.); exigences liées aux antennes.
  - Explique les obligations administratives: certification et vérification; conditions d'octroi de licences; accords mutuels entre pays/régions .
  - Fournit aussi des informations utiles sur les règles au niveau national/régional (y compris les paramètres techniques et opérationnels et l'utilisation du spectre).
- Rapport mis à jour régulièrement.

SRD – activités d'harmonisation (1/2)

- Rec. UIT-R SM.1896 – Gammes de fréquences pour une harmonisation mondiale ou régionale pour les SRD
  - Gammes de fréquences appropriées pour une harmonisation mondiale:

    9-148,5 kHz; 3 155-3 400 kHz (appareils de correction auditive sans fil de faible puissance, numéro **5.116** du RR);
    et les bandes ISM suivantes indiquées aux numéros **5.138** et **5.150** du RR:
    6 765-6 795 kHz; 13 553-13 567 kHz; 26 957-27 283 kHz; 40,66-40,7 MHz;
    2 400-2 500 MHz (jusqu'à 2 483,5 MHz dans certains pays); 5 725-5 875 MHz;
    24,00-24,25 GHz; 61,0-61,5 GHz; 122-123 GHz; 244-246 GHz.
    [proposition en cours d'examen pour l'ajout des bandes 3,7-4,8 GHz et 7,25-9 GHz (voir la note 1)]
  - Gammes de fréquences appropriées pour une harmonisation régionale*:

    (* bandes disponibles entièrement ou partiellement dans une Région ou seulement dans certains pays)
    7 400-8 800 kHz (dans les Régions 1 et 2 et dans certains pays de la Région 3);
    312-315 MHz (dans la Région 2 et dans certaines pays des Régions 1 et 3);
    433,050-434,790 MHz (dans la Région 1 et dans certains pays des Régions 2 et 3);
    862-875 MHz (pas dans la Région 2; dans la Région 1 et dans certains pays de la Région 3);
    875-960 MHz (dans la Région 2 en tant que gamme d'accord mais non disponible pour les SRD dans plusieurs pays en raison de l'utilisation de systèmes mobiles commerciaux; dans certains pays des Régions 1 et 3).
    [proposition en cours d'examen pour l'ajout des bandes 3,1-4,8 GHz et 6-9 GHz dans certains pays des Régions 1 et 3 (voir la note 1)]

Note 1: Pour les applications à bande ultra-large de communication, de géolocalisation et de radiorepérage, voir l'Annexe 13 du Doc. 1B/237

SRD – activités d'harmonisation (2/2)

- Rec. UIT-R SM.2103 – Harmonisation à l'échelle mondiale des catégories de SRD
  - Faciliter le processus d'harmonisation à l'échelle mondiale (par exemple identification à l'échelle mondiale de gammes de fréquences).
  - Avantages pour les utilisateurs finals, les fabricants et les régulateurs (par exemple économies d'échelle).
  - **Applications SRD non spécifiques** (toutes, permettent d'éviter toute fragmentation de l'utilisation du spectre et d'encourager l'innovation).
  - SRD aux fins de la **télématique pour le transport et le trafic** (par exemple entre voitures, entre voiture et infrastructure).
  - SRD pour le radiorepérage (par exemple détecteurs de mouvements et équipements d'alerte).
  - SRD pour les **alarmes sans fil** (applications SRD comprenant les alarmes pour la sécurité et la sûreté).
  - SRD pour la commande de modèles réduits (équipements visant uniquement à commander le déplacement du modèle réduit, dans l'air, sur terre ou au-dessus ou au-dessous de la surface de l'eau, par exemple les modèles réduits d'avion sont en principe soumis à des limites de poids et de hauteur au-dessus du sol par la réglementation nationale).
  - Applications de **microphones hertziens et applications audio**, y compris les appareils de correction auditive non assujettis à une licence.
  - **Applications utilisant l'identification par radiofréquence (RFID)** (par exemple identification automatique d'articles, suivi d'actifs, gestion des déchets, identification des personnes, contrôle d'accès, capteurs de proximité, systèmes antivol, etc., souvent désignés aussi comme l'«Internet des objets» ou les «communications de machine à machine»).
  - **Implants médicaux actifs à ultra faible puissance** (utilisés en règle générale pour aider les gens à améliorer leur qualité de vie, par exemple régulation du rythme cardiaque, administration de médicaments, traitement de tremblements d'origine neurologique, etc.).

- Rec. UIT-R SM.2104 – Lignes directrices relatives aux émetteurs-récepteurs de réseaux domestiques hertziens à bande étroite – Spécification des éléments liés au spectre.

Applications des réseaux étendus de capteurs et d'actionneurs (WASN)

- automatisation et amélioration de l'efficacité des processus d'activité, par exemple relevé à distance des compteurs pour les services collectifs (eau, gaz et électricité);
- observation météorologique, par exemple mesure de la température et de l'humidité dans l'air;
- observation, prévision et protection de l'environnement, par exemple observation de la pollution dans l'air, dans l'eau et dans les sols;
- prévention de la délinquance et sécurité, par exemple détection des intrusions, surveillance des enfants;
- soins de santé, applications médicales et amélioration de la qualité de vie, par exemple surveillance des paramètres vitaux (température corporelle, poids, rythme cardiaque, etc.);
- commande et surveillance à distance des machines industrielles et distribution de marchandises;
- prévention des catastrophes et mesures en cas de catastrophe, par exemple notification d'une catastrophe;
- commande des logements et des bâtiments commerciaux intelligents, par exemple mise en réseau des appareils électroménagers et des équipements de bureau;
- systèmes de transport et de gestion du trafic intelligents;
- surveillance des espèces aviaires qui peuvent être porteuses de la grippe aviaire.

PRIDA Composante 1

Atelier de renforcement des capacités sur Internet des objets (IdO) et services numériques

Atelier en Français en ligne: 24-28 août

The Internet of Things (IoTs)

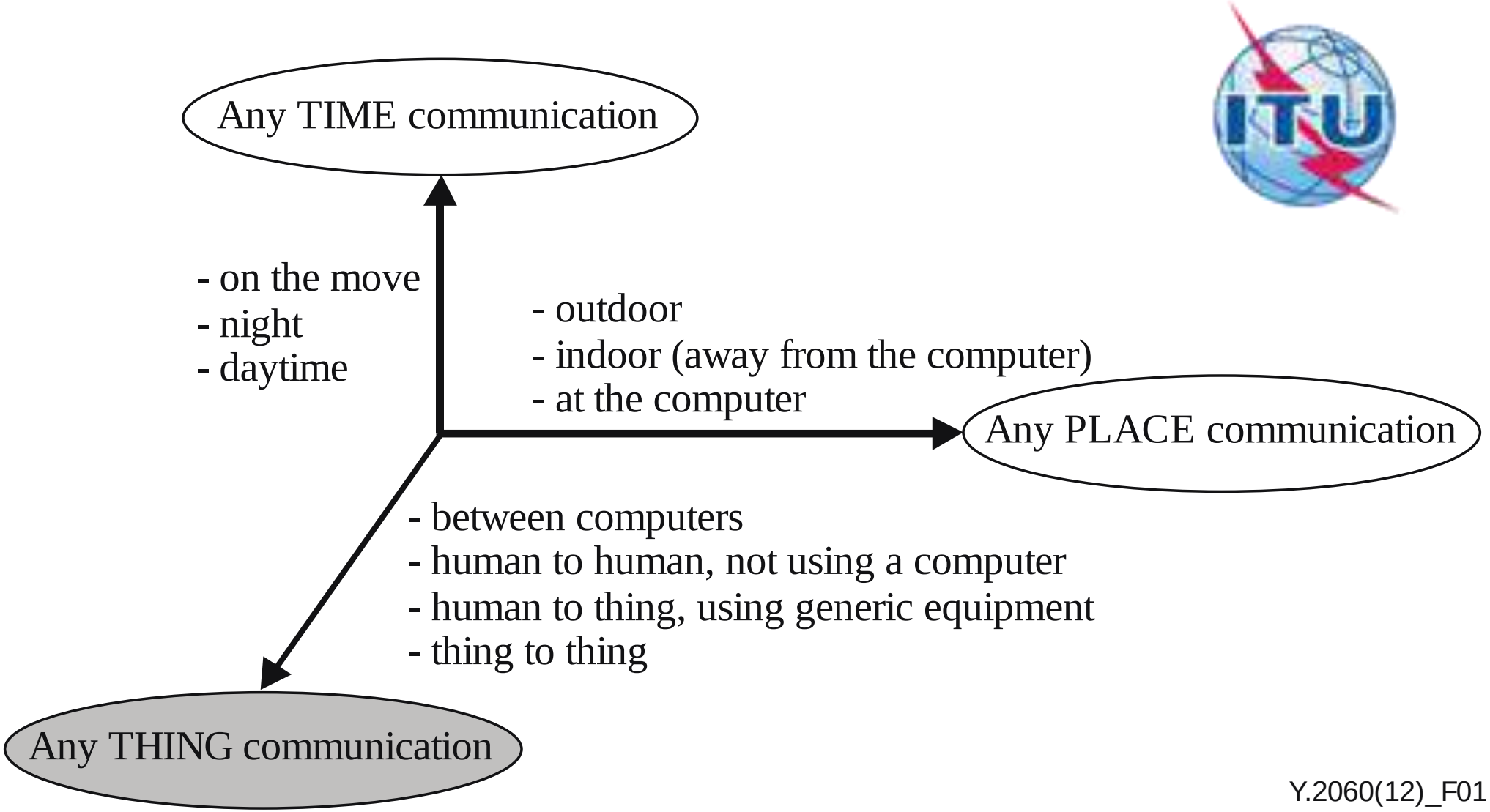
IoT ecosystem and business models

By Desire Karyabwite, Senior IP Coordinator, ITU

Geneva, 24-28 August 2020

ITU-T	Y.2060
TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU	(06/2012)

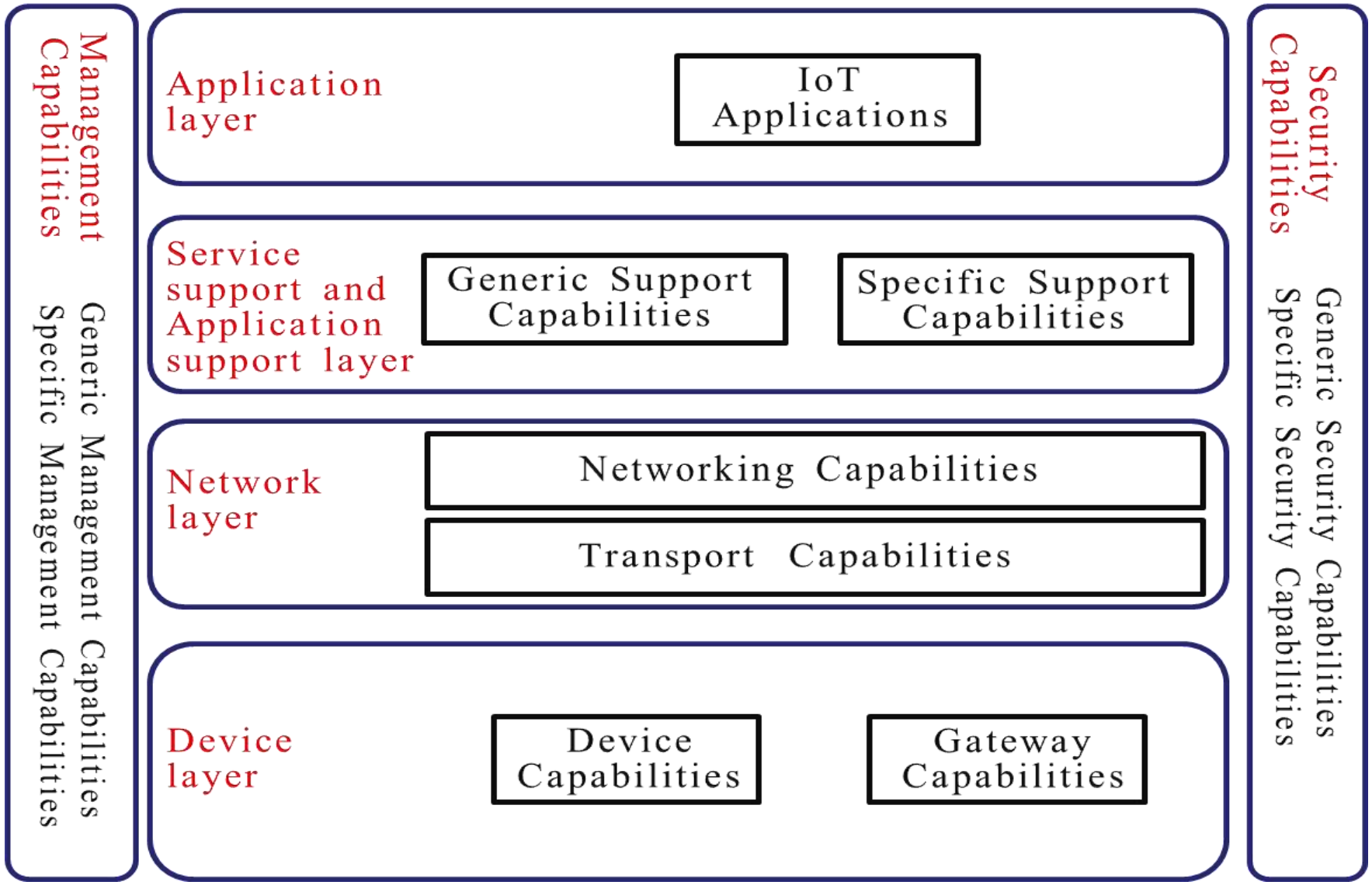
Internet of things (IoT): A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies



Y.2060(12)_F01

The new dimension introduced in the Internet of things

IoT reference model



ITU-T	Y.4416
TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU	**(06/2018)**

Architecture of the Internet of things based on next generation network evolution

ITU-T	Y.4806
TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU	**(11/2017)**

Recommendation ITU-T Y.4806 provides a classification of the security issues for the Internet of things (IoT) and examines how the security threats may affect safety, in order to determine which security capabilities specified in Recommendation ITU-T Y.4401/Y.2068 support safe execution of the Internet of things.

The appendices of this Recommendation consider how the joint analysis of threats and security capabilities mentioned herein may be used to establish security requirements for the different applications of the Internet of things

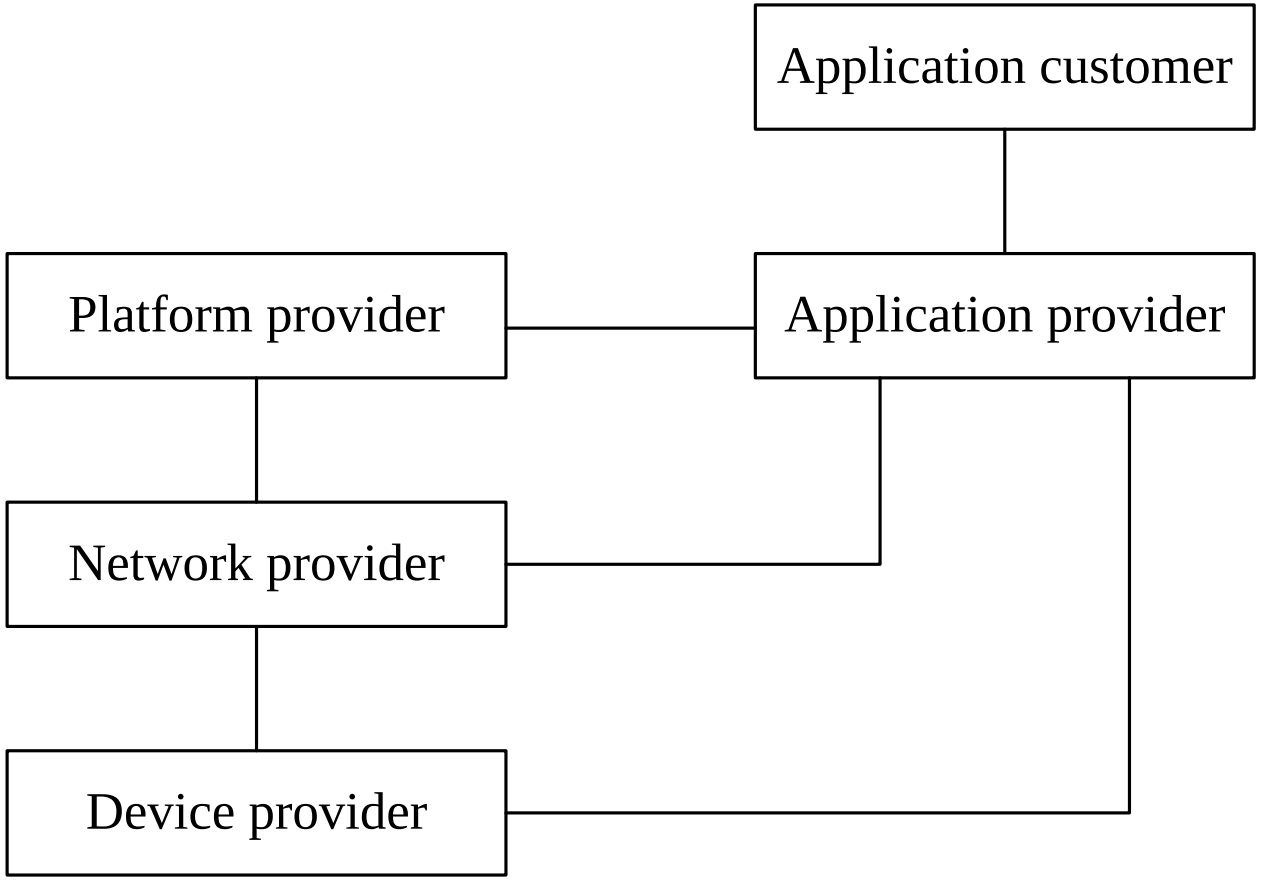
2019 ITU-T SG20 approved two Recommendations:

- *ITU-T Y.4556 "Requirements and functional architecture of smart residential community"*, which presents the key components and specifies requirements and the functional architecture of smart residential community (SRC).
- *ITU-T Y.4904 "Smart sustainable cities maturity model"* which contains a maturity model for smart sustainable cities. This maturity model helps identify the goals, levels and key measures that are recommended for cities to effectively examine their current situation and determine critical capabilities needed to progress toward the long-term goal of becoming SSCs.

SG20 also consented to 12 draft Recommendations (under approval):

- *ITU-T Y.4208 "IoT requirements for support of edge computing"*: This Recommendation provides an overview on related challenges faced by the IoT and describes how the IoT supporting edge computing may address these challenges. From the edge computing deployment perspective, service requirements for support of edge computing capabilities in the IoT are identified as well as related functional requirements.
- *ITU-T Y.4209 "Requirements for interoperation of the smart port with the smart city"*, which provides the requirements for Smart Port interoperation with Smart Cities and other smart elements. Additionally, these requirements are the foundation that enables the provision of enhanced smart services by the Smart Port.
- *ITU-T Y.4459 "Digital entity architecture for IoT interoperability"*, This Recommendation defines an architecture framework for information-oriented services that makes use of existing infrastructures, including the Internet infrastructure, to enhance, secure and manage information sharing over a distributed networking environment. This Recommendation can be used with different identification and addressing protocols (e.g. IP and/or non IP based networks).
- *ITU-T Y.4461 "Framework of open data in smart cities"*, which defines a framework of open data in smart cities. It clarifies the concept of open data in smart cities, analyses the benefits of open data in smart cities, identifies the key phases, key roles and activities of open data in smart cities and describes the framework and general requirements of open data in smart cities.

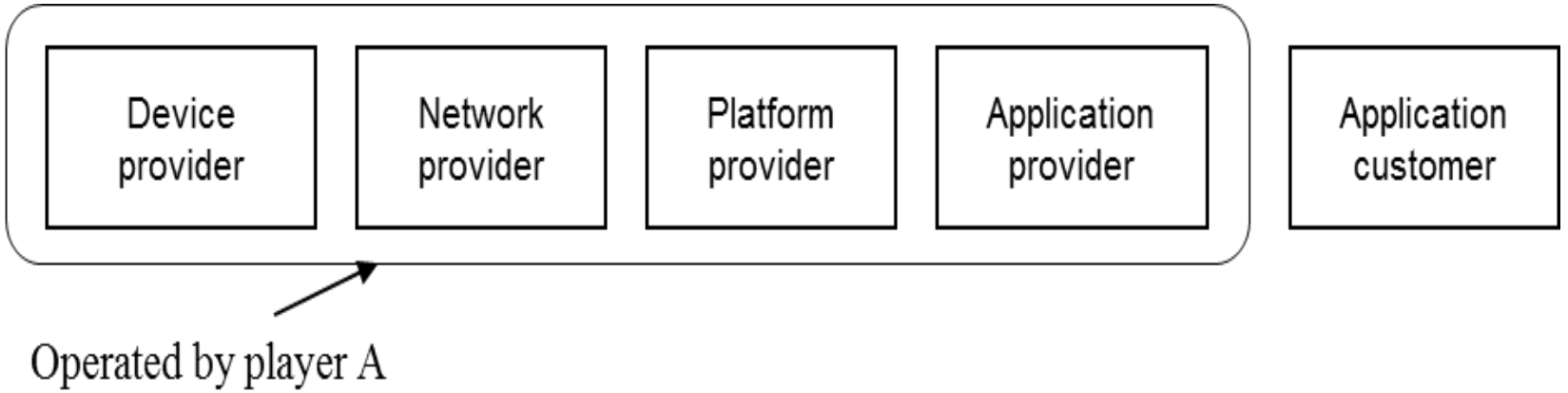
IoT ecosystem and business models



IoT ecosystem

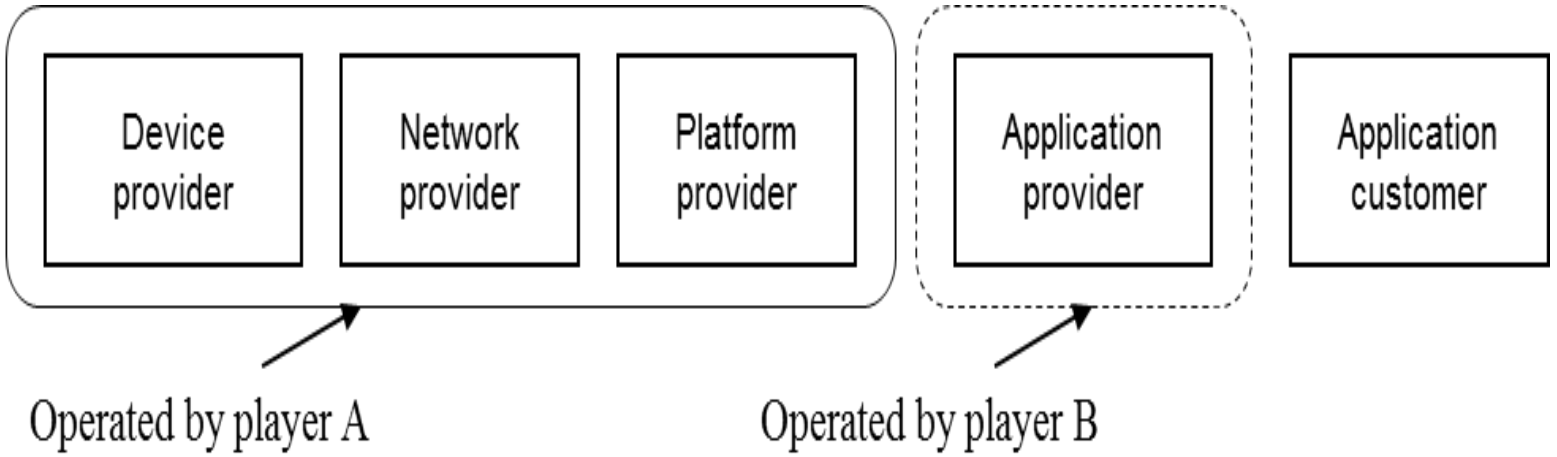
IoT Business models

IoT Business Model 1



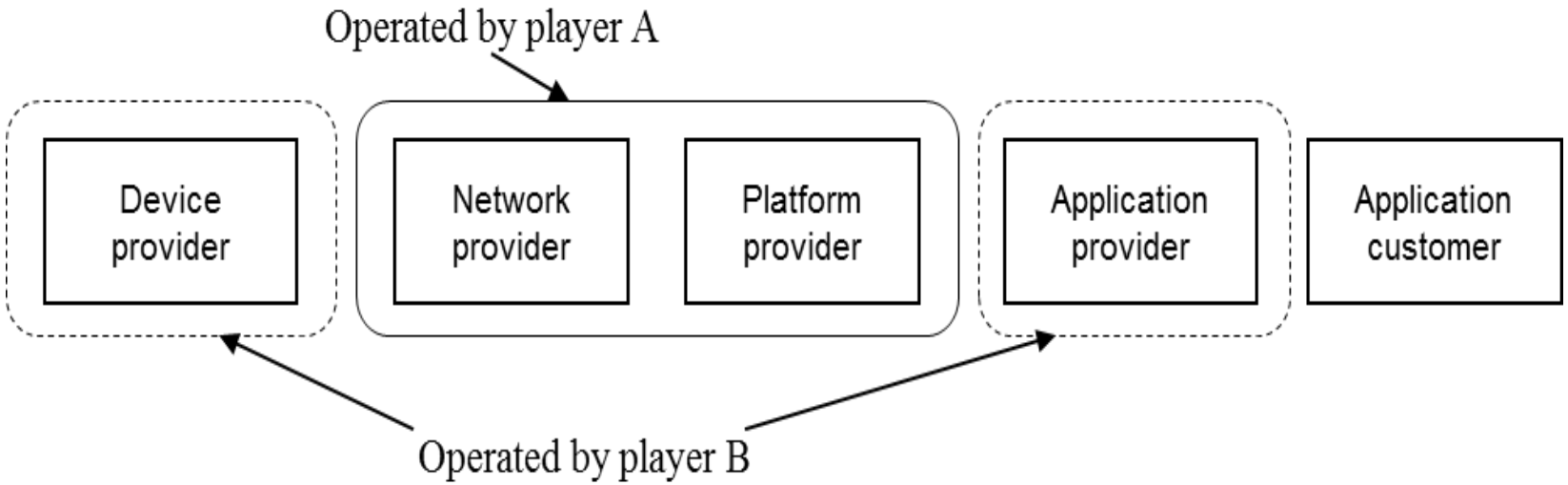
Telecom operators and some vertically integrated businesses (such as smart grid and intelligent transport systems (ITS) businesses) act as player A in model 1.

IoT Business Model 2



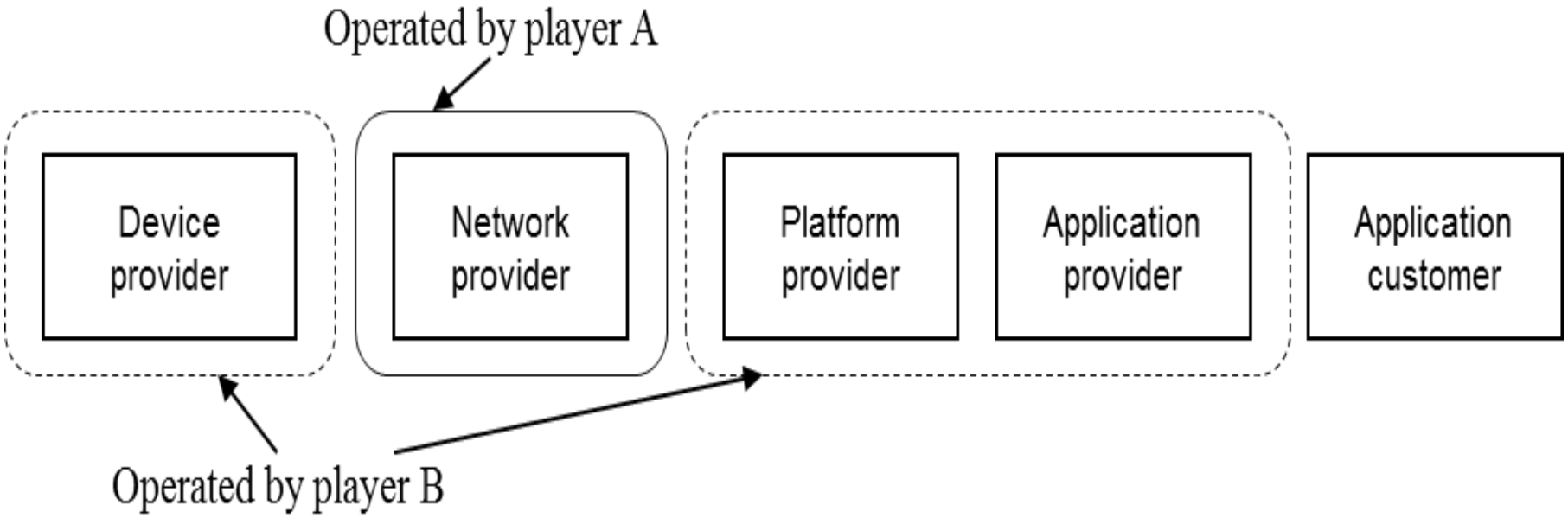
Telecom operators act as player A, other service providers as player B in model 2.

IoT Business Model 3



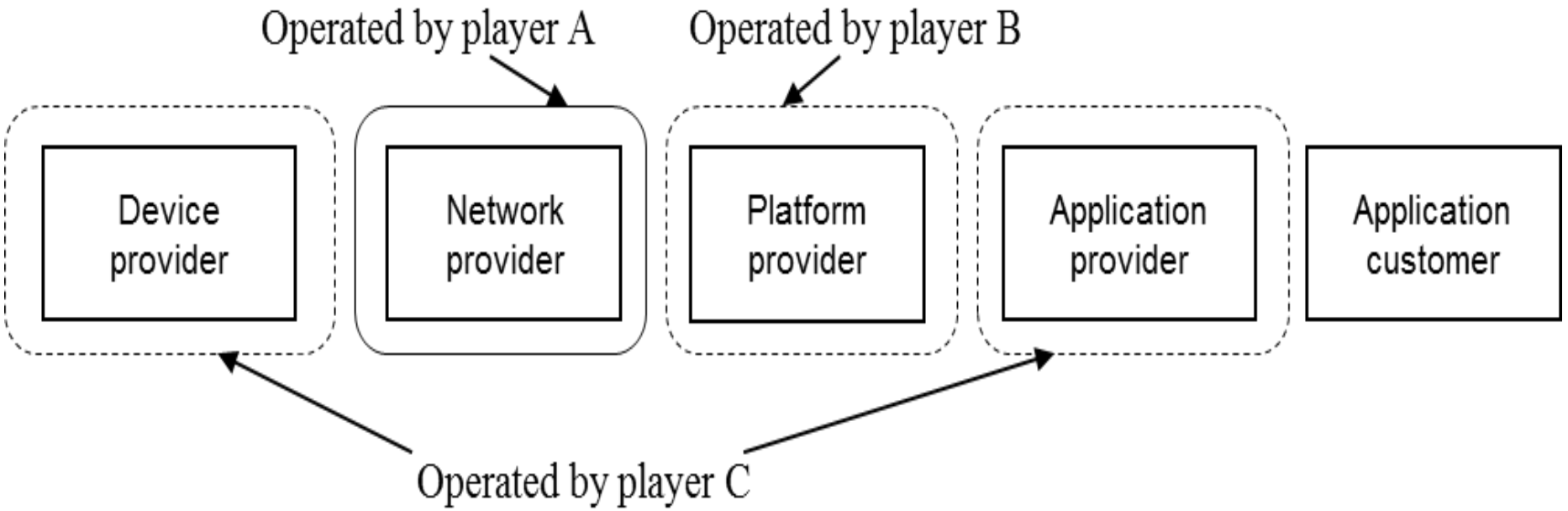
Telecom operators act as player A and other service providers act as player B

IoT Business Model 4



Telecom operators act as player A, other service providers and vertically integrated businesses act as player B in model 4.

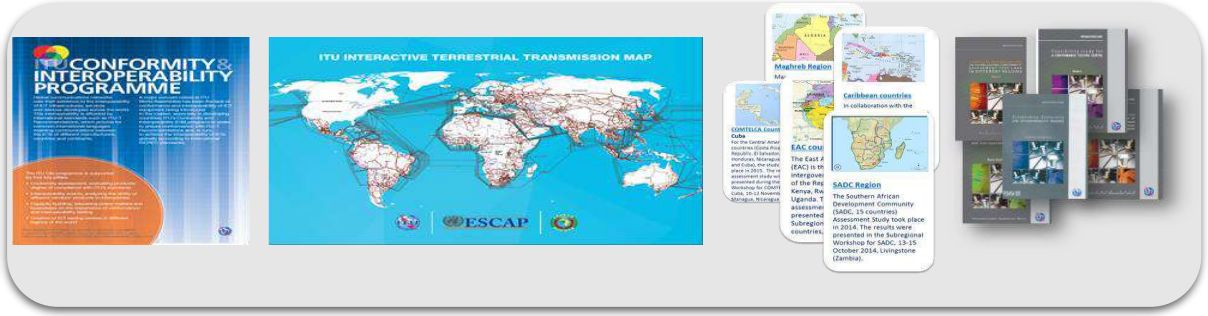
IoT Business Model 5



Telecom operators act as player A, other service providers act as player B, and vertically integrated businesses act as player C in model 5.

Telecommunication Networks

Our work is carried out by various means, including symposia, workshops, conferences, seminars and expert advice as well as information sharing, creation of tools and training material, direct assistance, partnership, publications and events. Our priority areas are as follows:



- **Next-Generation Networks:** assistance on planning, deployment, migration, interoperatbility, digitization and evolution of networks, network elements and applications
- **Broadband Networks (wired and wireless technologies):** assitance with planning, implementation and development of national ICT broadband networks, including promoting IXPs
- **Rural communications:** provision of information on access and backhaul technologies and source of power supply, latest technologies and best practice, implementation of projects on public community broadband access points
- **Conformance and interoperability (C&I):** assistance on the establishment of national, regional or subregional C&I programmes, assessment and feasibility studies, providing information and training to technicians, policy-makers and businesses on C&I, providing guidelines on C&I
- **ITU Broadband, IPv6 and Internet Exchange Implementations:** to provide broadband connectivity free or low cost digital access for schools, hospitals, underserved populations; IXPs to reduce transmission costs, optimize Internet traffic, improve QoS
- **ITU Interactive Transmission Maps:** cutting-edge ICT-data mapping platform to take stock of national backbone connectivity and other key ICT metrics.
- **Bridging the Standardization Gap**: Increasing the knowledge and capacity of developing countries for the effective application/implementation of standards
- **WSIS** ALC2 (Infrastucture)

For more information please visit: http://www.itu.int/en/ITU-D/Technology/Pages/default.aspx

Telecommunication Networks

ITU Broadband, IPv6 and Internet Exchange Implementations

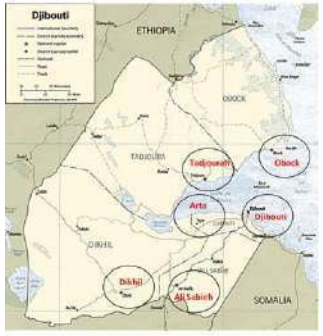
- **Broadband Wireless Networks Implementation**: To provide broadband connectivity free or low cost digital access for schools and hospitals, and for underserved populations in rural and remote areas in selected countries.
- **Internet Exchange Development**:

To bring the value of IXPs in leveraging the benefits of connectivity through potentially reduced transmission costs, optimized Internet traffic, improved Quality of Service.

Widely accepted best practices for the design, installation and operation of IXPs. peering as an effective way for Internet Service Providers (ISPs) to improve the efficiency of operations and interconnection business relationships

Broadband Wireless Projects

Djibouti - Mobile WiMax standard IEEE802.16e

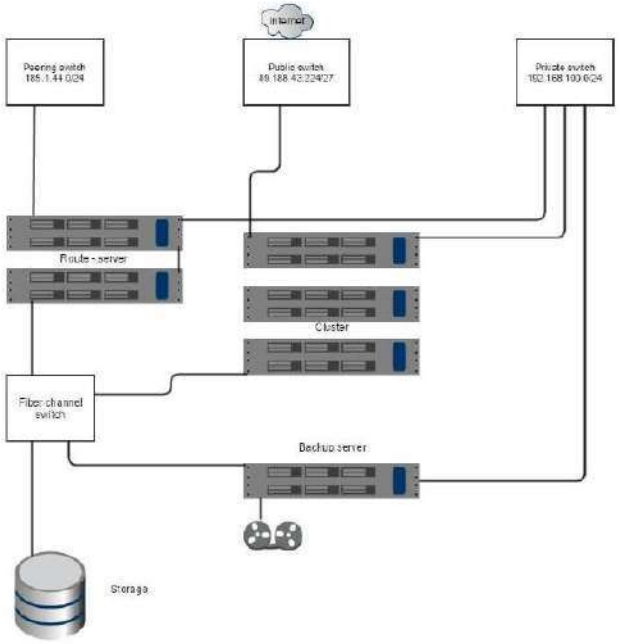


Swaziland Project Implementation - field Missions

Burundi Training & Network Installation

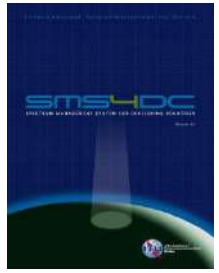
Burundi - Connecting Hospitals for E-Health

IXP In Montenegro



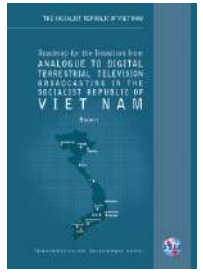
- Implemented and operational since July 2015

Spectrum Management and Broadcasting



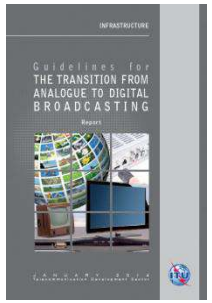
Spectrum Management Tool (SMS4DC)

- A computer program to assist the administrations of developing countries
- On technical and regulatory procedures for managing spectrum
- around 50 subscribers



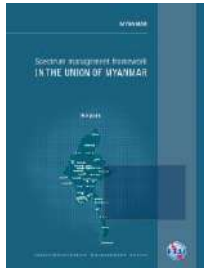
National Roadmaps for Digital Broadcasting Transition

- ITU has helped over 30 countries around the world since 2009 for establishing national goals, strategies, key activities and so forth



The Guidelines for DTTB Transition

- for the smooth transition to Digital Terrestrial Television Broadcasting (DTTB)
- On policy, technologies, network planning, customer awareness and business planning
- Worldwide revision published in 2014



Direct assistance in spectrum management

- Assistance in Cross Border Frequency Coordination (HCM4A in Africa)
- Spectrum management assessment
- Establishment of spectrum master plans
- Spectrum monitoring
- Consulting to specific issues (e.g. spectrum fee, NTFA)

Other Activities

- DSO database on status of the transition to Digital Terrestrial TV Broadcasting
- Spectrum Management Training Program (SMTP)
- ITU-D Study Group Questions (Q8/1, Resolution 9, Q7/2)
- WSIS Action Lines (C3, C7 e-science, C9)

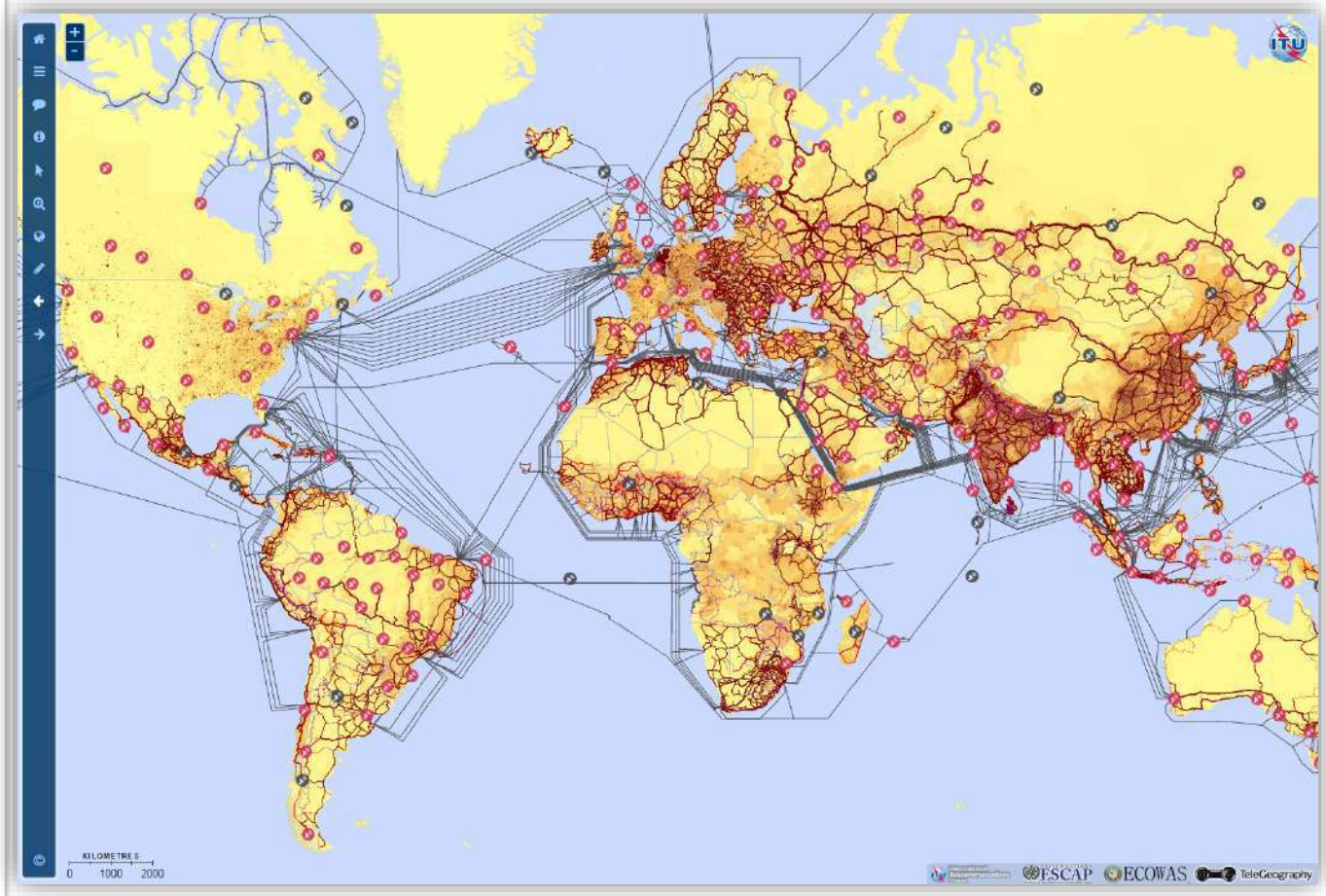
ITU Interactive Transmission Maps

The Interactive Transmission Maps are a cutting-edge ICT-data mapping platform to take stock of national backbone connectivity (Optical Fibres, Microwaves and Satellite Earth Stations) as well as of other key metrics of the ICT sector. Data concerning submarine cables are also included as provided by TeleGeography

- **The Scope** of this ITU project is to research, process and create maps of core transmission networks worldwide

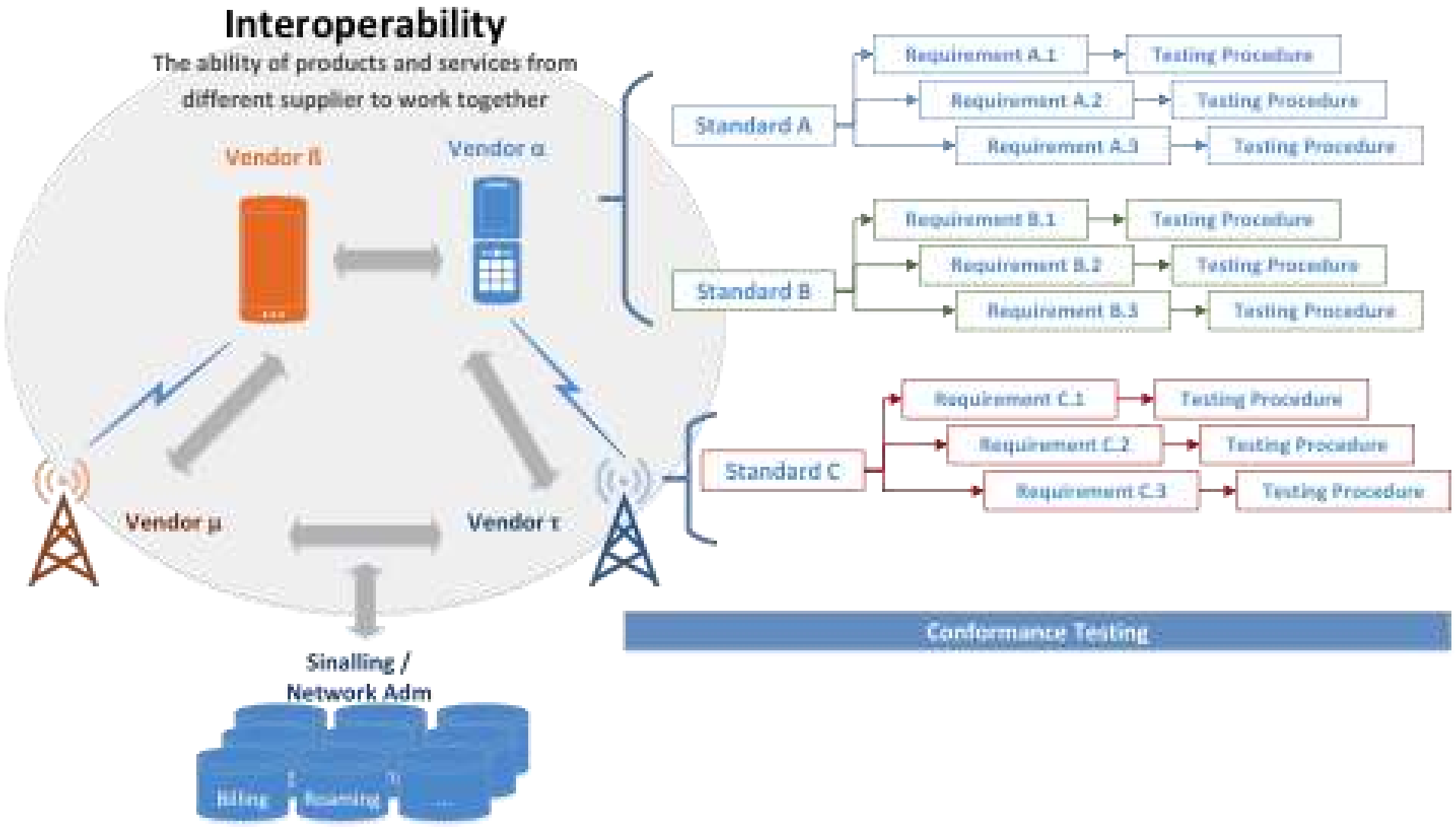
- **The Objectives** of this ITU project are:

- to assess the status of national connectivity and to identify gaps enabling the design of targeted strategies and implementation programs for increasing the use of broadband.
- to assess market opportunities, thus serving as a management tool for making investment decisions, promoting broadband and achieving universal connectivity.
- to be used as a source of abundant and current data on global ICT connectivity.



http://itu.int/go/Maps

Conformity and Interoperability

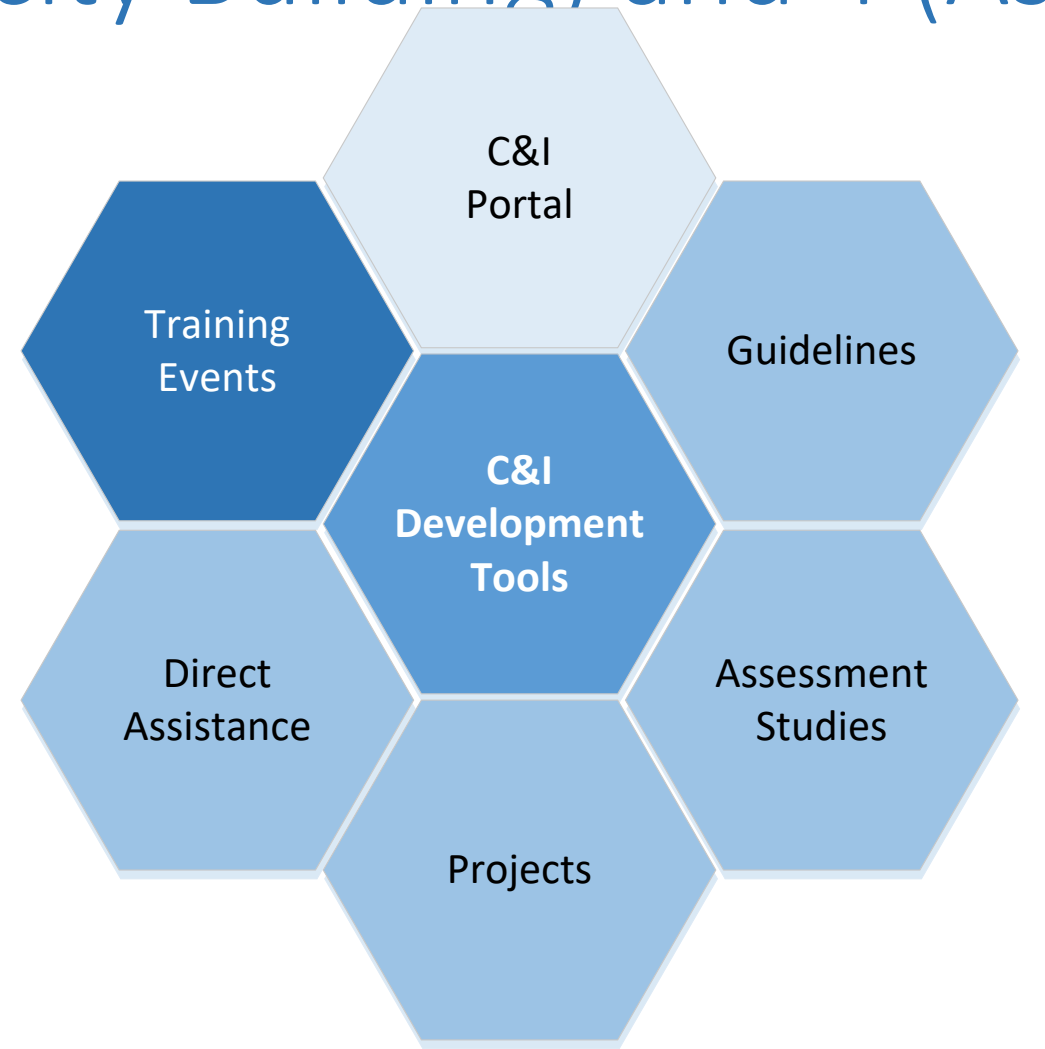


Conformity Assessment

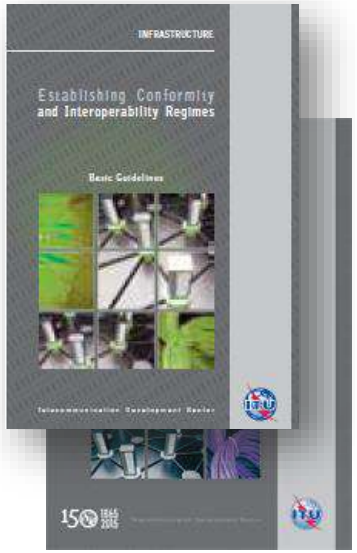
Demonstration that specified requirements relating to a product, process or system are fulfilled

ITU – C&I Programme

Pillars 3 (Capacity Building) and 4 (Assistance)

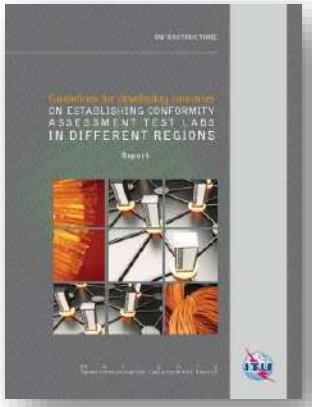


ITU C&I - Guidelines



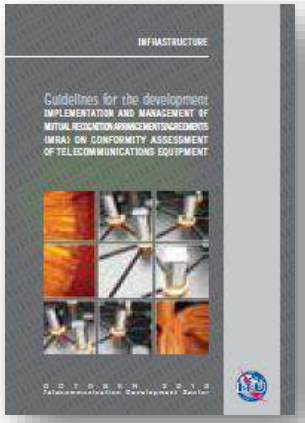
Establishing Conformity and Interoperability Regimes – Basic Guidelines (2014) and Complete Guidelines (2015)

These Guidelines address challenges faced by developing countries as they plan and review their own C&I regimes. Aspects covered by this publication include, inter alia, conformity assessment procedures; legislation to promote an orderly equipment marketplace; surveillance; coordination across regulatory agencies; and relevant international standards.



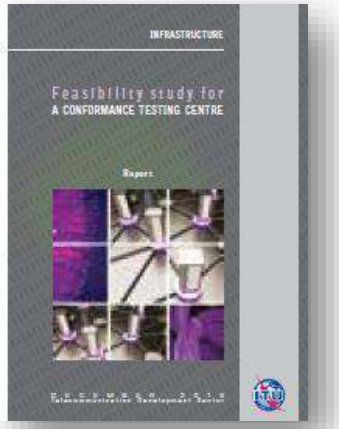
Guidelines for developing countries on Establishing Conformity assessment Test Labs in Different Regions (2012)

This set of guidelines is the first publication on C&I, its valuable content includes information concerning: The process required for building testing labs; A site analysis (e.g. existing testing labs, know-how);Collaboration mechanisms; Best practices; Reference standards and ITU Recommendations



Guidelines for the Development, Implementation and Management of Mutual Recognition Arrangements/Agreements on Conformity Assessment (2013)

These guidelines promote the understanding and establishment of Mutual Recognition Agreements (MRAs) on conformity assessment that are intended to promote efficiency and resource sharing as well as to streamline the flow of products among participating Parties such as ITU Member States and private sector organizations, such as testing laboratories



Feasibility Study for the establishment of a Conformance Testing Centre (2013)

This feasibility study describes environments, procedures and methodologies to be adopted to establish, manage and maintain a testing center covering different kinds of conformance and interoperability testing areas

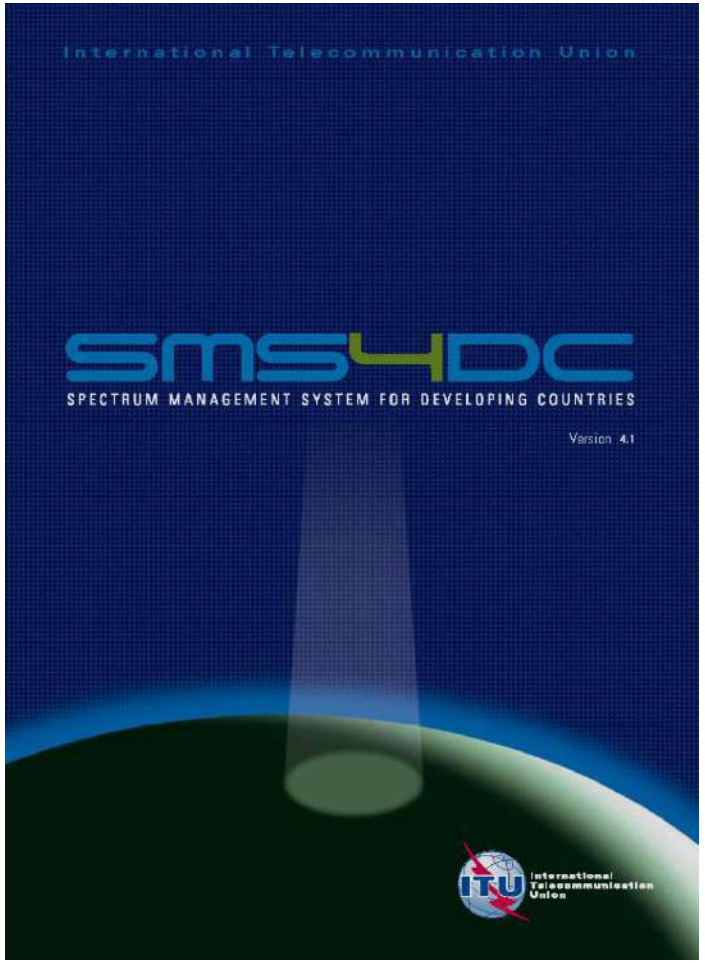
http://itu.int/go/CI_Guidelines

Spectrum Management

Spectrum Management and Broadcasting - summary

- Spectrum management
  - Spectrum Management Tool for Developing Countries (SMS4DC)
  - Assistance in Cross Border Frequency Coordination (HCM4A)
  - Spectrum Management Assessment, SM Master Plans
  - Spectrum Management Training Program (SMTP)
- Broadcasting
  - Guidelines for Transition to Digital Broadcasting (E, F, S)
  - Assistance for the preparation of national roadmap (more than 40 countries since 2009)
  - DSO database
- Others
  - ITU-D Study Group Questions (Q2/1, ex. 8/1, Q7/2)
  - WSIS Action Lines (C2, C3, C7 e-science, C9)

Spectrum Management Tool (SMS4DC)

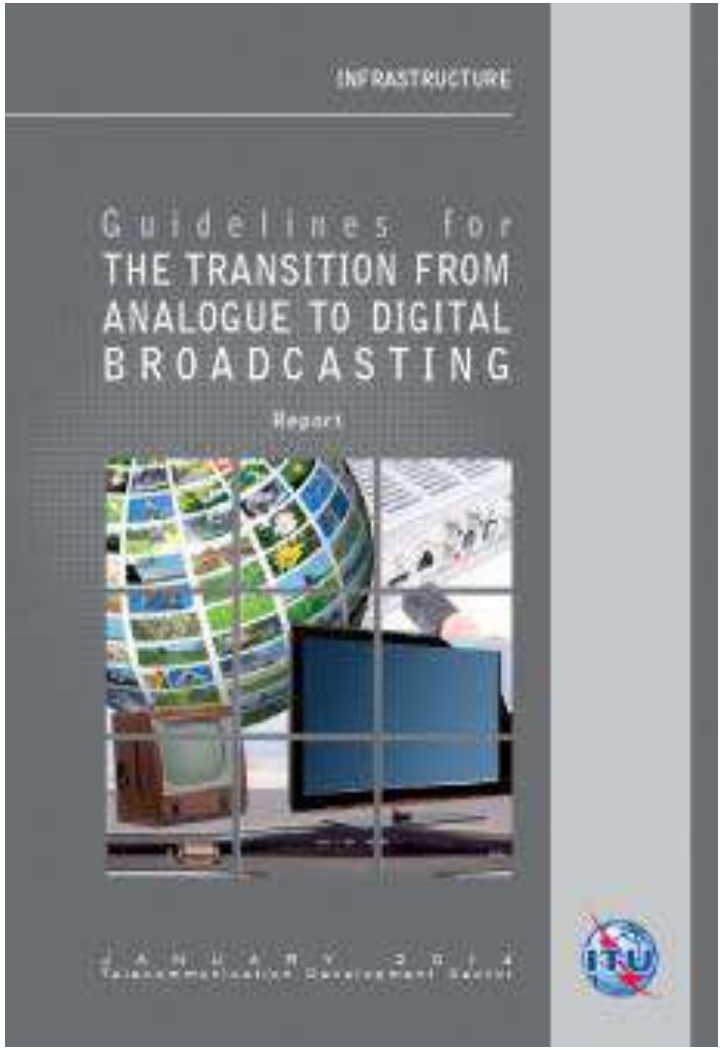


- A computer program to assist the administrations of developing countries
  - On technical and regulatory procedures for managing spectrum
  - A software package on CD containing a digital terrain map (only 1 km resolution!)
- Known as Spectrum Management System for Developing Countries (SMS4DC)
  - Made available in 2007, current version is 5.1
  - Subscribers: around 50 countries

Cross Border Frequency Coordination

- Harmonized Coordination Method for Africa (HCM4A)
  - Set a standard on a mutually beneficial approach by consensus
  - Provide a solid basis for bilateral and mutual agreements
  - Oblige each country to take account of other stations
- Implementation of HCM4A in four phases
  1. Assessment of existing administrative and technical procedures
  2. Multilateral agreement proposal by technical working group
  3. Validation workshop to adopt draft agreement
  4. Development of HCM4A software
- HCM4A involves 4 sub regions
  - Central, East, Southern and West Africa

The Guidelines for Transition to Digital Broadcasting



- Intended to provide information and recommendation
  - On policy, technologies, network planning, customer awareness and business planning
  - for the smooth transition to Digital Terrestrial Television Broadcasting (DTTB) and introduction of Mobile Television Broadcasting
- Prepared in 2010 for Africa
  - 1st Revision (2012) for ASP adding a section on archives migration
  - 2nd revision (2014) for global including Satellite TV, Cable TV, IPTV

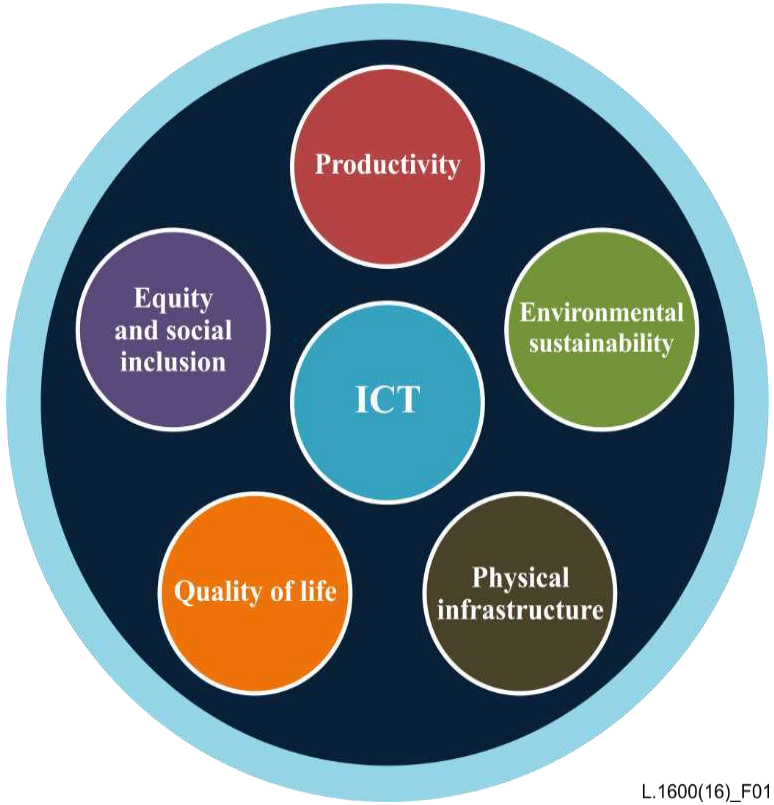
Key Performance Indicators in smart sustainable Environment

KPIs focuses specifically on a set of ICT-related indicators for smart sustainable Environment/Cities

The dimensions of KPIs can be categorized as shown :

- Information and communication technology
- Environmental sustainability
- Productivity
- Quality of life
- Equity and social inclusion
- Physical infrastructure

In the UN-Habitat prosperity index, ICT forms part of the general 'Infrastructure' category. ICT is defined as a separate category to highlight the focus of ITU.



L.1600(16)_F01

Thank you

Desire KARYABWITE
IP Coordinator / TNS/ Digital Networks & Society Department
Telecommunication Development Bureau (BDT)
International Telecommunication Union

Place des Nations
CH-1211 Geneva 20
E-mail: desire.karyabwite@itu.int
Tel: +41 22 730 5009
Fax: +41 22 730 5484
Cell. +41 79 249 4866
www.itu.int