

L'IOT C'EST QUOI ?



nicolas KAKOURIDIS
EPHIKAS 20620 BIGUGLIA



1. Qu'est-ce que l'IoT ?

L'**IoT** est l'acronyme de **Internet Of Things** (IdO Internet des Objets en français).

Selon l'UIT (Union Internationale des Télécommunications), l'Internet des Objets est défini comme « *une infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physique ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution* ».

Au fil du temps, le terme a évolué et il englobe maintenant tout **l'écosystème des objets connectés**. Cet écosystème englobe, des fabricants de **capteurs**, des éditeurs de **logiciels**, des **opérateurs** historiques ou nouveaux sur le marché, des **intégrateurs**...

2. Les 5 composantes de l'IoT

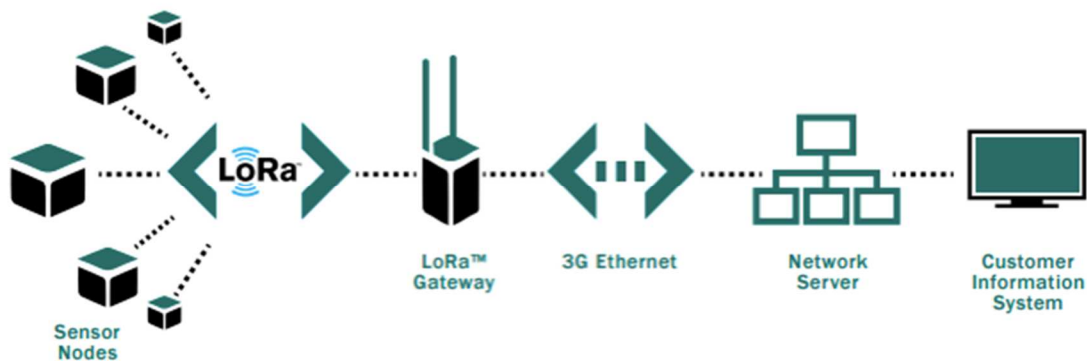
Une solution d'IoT s'articule autour de 5 composants essentiels que sont :

- Les objets (capteurs),
- Le réseau (connectivité),
- Les données,
- Les informations,
- Les applications d'exploitation.

2.1 Les objets pour capter des données de valeur

Les objets sont tous les **équipements actifs ou passifs** pouvant **générer de la donnée exploitable et créatrice de valeur** pour les utilisateurs. Les objets sont composés d'éléments passifs : les capteurs, et pour certains, d'éléments actifs les rendant capables de traitements d'enrichissement des données et de transmission de celles-ci.

Les données sont aussi diverses que les métiers. Nous pouvons aussi bien avoir des données de température, d'humidité, de positionnement, de temps de fonctionnement, de niveau, d'alerte...



Exemple avec LoRA

2.2 Les réseaux pour transmettre les données

Les **réseaux** sont le maillon prépondérant d'un **projet d'IoT**, ils doivent répondre à un critère d'usage :

- La **couverture de la zone** d'usage des objets :
 - Sur un campus,
 - Sur une ville,
 - à l'ensemble de la planète.

Et ils doivent répondre à une contrainte : l'objet disposera-t-il d'une **source d'énergie en permanence** ?

Cela conditionne :

- L'**architecture** de la solution,
- La **conception** de l'objet,
- Le **cycle de vie** de la solution

En effet, toutes les technologies ne sont pas adaptées à tous les cas d'usages et leur déploiement. Nous vous proposons ici de faire un rapide tour d'horizon de quelques technologies.



2.2.1 Les LPWAN : Sigfox et LoRaWAN

Dans cette catégorie, nous retrouvons entre autres deux technologies d'origine française bien connues du monde de l'IoT que sont **SIGFOX** et **LoRaWAN** (Low Range Wide Area Network). Il s'agit de 2 technologies à longue portée et faible consommation.

Si ces deux technologies se retrouvent dans la même catégorie, elles ne sont pas pour autant identiques. Je vous propose donc de faire un bref comparatif.

Les points communs

Tout d'abord, il s'agit de réseaux permettant d'**envoyer des messages de petite taille** de l'ordre de l'Octet (12 pour Sigfox et 24 pour LoRa). D'autre part, ce sont des **réseaux à fort taux de pénétration**.

Les points forts du LoRa

LoRa est plus qu'un réseau, il s'agit d'une **technologie « standardisée »** basée sur 2 bandes de fréquences libres (868 MHz en Europe et 915 MHz en Amérique).

Ce réseau peut être déployé de manière « privé » ou « opéré ».

Privé :

Opéré :

C'est d'ailleurs parce qu'il s'agit d'une technologie standardisée que ce type de réseau est **rapidement déployé** par la plupart des opérateurs de téléphonie.

Les points forts du Sigfox

Sigfox est un réseau opéré par un seul et unique opérateur, qui est son concepteur, Sigfox. Cette technologie tout comme le LoRa utilise les bandes de fréquence 868 MHz et 915 MHz).

D'autre part, l'ensemble des **modules de communication** Sigfox sont nécessairement **certifiés** et validés par l'opérateur, ainsi que chaque référence d'objet.



2.2.2 Le M2M

Avec le M2M (Machine to Machine), il s'agit tout simplement d'utiliser des réseaux télécom existants à savoir de la 2G jusqu'à la 4G. Majoritairement, il s'agit d'abonnements souscrits auprès des opérateurs de téléphonie pouvant donner accès uniquement à des volumes de données.

Le modèle économique actuel, avec un volume de données mensuel limité, commence à évoluer vers un service de type « Pay As You Use » soit un paiement à l'usage.



2.2.3 La RFID

Nos n'aborderons pas cette technologie ici.

Ephikas lot



2.2.4 Le Bluetooth

Le **Bluetooth**, est une technologie connue et maîtrisée par tous depuis maintenant une dizaine d'années. Il s'agit d'une technologie radio de moyenne portée (environ 10m) qui permet d'envoyer **des messages de grande taille et en grande quantité**. Cependant, cette connectivité ne se suffit pas à elle-même car elle **nécessite une tierce technologie** pour **transférer et stocker les données**. D'autre part, il s'agit d'un moyen de communication disposant d'un grand débit, puisqu'il repose sur la bande de fréquence 2,4 GHz tout comme le Wifi.



2.2.5 Résumé des technologies de réseau

Technologie	Points forts	Points Faibles	Type de cas d'usage
LoRa	<ul style="list-style-type: none"> Faible consommation énergétique Longue portée Un standard opérable 	<ul style="list-style-type: none"> Couverture mondiale encore faible Taille et volume de données 	<ul style="list-style-type: none"> Relève de compteurs d'énergie Envoi d'informations ponctuelles (géolocalisation,
Sigfox	<ul style="list-style-type: none"> Faible consommation énergétique Longue portée Un opérateur unique 	<ul style="list-style-type: none"> Couverture mondiale encore faible Taille et volume de données 	<ul style="list-style-type: none"> Relève de compteurs d'énergie Envoi d'informations ponctuelles (géolocalisation,
M2M	<ul style="list-style-type: none"> Couverture mondiale importante 	<ul style="list-style-type: none"> Consommation d'énergie Portée 	<ul style="list-style-type: none"> Terminaux de paiement Application avec de gros volumes de données ou d'envoi de données sur incident
RFID	<ul style="list-style-type: none"> Pas d'émission d'ondes Pas besoin d'énergie 	<ul style="list-style-type: none"> Faible portée Nécessité d'une passerelle 	<ul style="list-style-type: none"> Géolocalisation de zone Identification (contrôle d'accès, autorisation,...)
Bluetooth	<ul style="list-style-type: none"> Taille et volume des messages Débit 	<ul style="list-style-type: none"> Faible portée Nécessité d'une passerelle 	



3 Pourquoi mener une stratégie d'IoT ?

Aujourd'hui, afin de rester compétitives, les entreprises sont dans l'obligation de créer de la valeur soit pour :

- Développer et augmenter le **chiffre d'affaires**,
- Rationnaliser ses processus afin d'améliorer la **rentabilité**.

Dans de nombreux cas, les métiers des entreprises pourraient être optimisés ou développés en ayant à disposition des informations qui jusqu'alors n'étaient pas disponibles.

Mener seul une **stratégie d'IoT** n'est pas chose aisée. Il est nécessaire de constituer une **équipe pluridisciplinaire** et de bien s'entourer afin d'optimiser les délais de mise en production. En effet, dans le secteur de l'IoT on voit fleurir de plus en plus d'entreprises que l'on peut classer suivant deux catégories :

- Celles qui développent leurs **solutions** et créent de **nouveaux marchés**, il s'agit plutôt des start-up,
- Celles qui se positionnent uniquement dans le **conseil** afin d'aider leurs clients à mettre en œuvre des solutions d'IoT en adéquation avec les besoins du marché.

EPHIKAS, à travers ses compétences pluridisciplinaires, ses expériences dans la GTC et GTB, et son réseau de partenaires, se positionne dans une autre catégorie qui permet d'apporter une solution globale d'IoT à nos clients à travers l'accompagnement, de la définition de l'idée jusqu'à l'exploitation et le maintien en condition opérationnelle des installations :

Capteurs – réseaux - monitoring

4 Quelques exemples d'application IoT

- **L'Industrie** avec la maintenance prédictive, la gestion automatisée d'alerte, l'optimisation de processus, l'amélioration des rendements et des approvisionnements...
- Les **villes** avec la gestion des stationnements, optimisation des flux de circulation, la gestion de l'éclairage public, la gestion des consommations énergétiques...
- Le **Transport** avec l'optimisation de flux de passager, l'optimisation des tournées de livraison...
- Le **Retail** avec la réduction de la fraude, l'optimisation d'inventaire, la gestion de stock automatisée...

Si vous avez un projet IoT, voici les 9 questions à vous poser.



1. Les acteurs côté métier ont-ils des idées de services et les moyens (humains) de les mettre en œuvre ?

A terme, c'est le service qui va donner toute sa valeur à un projet IoT. Ainsi, la première chose à faire est de réfléchir et de collecter diverses idées de services qui ont le potentiel d'offrir de réelles perspectives, ainsi qu'aux modèles économiques associés.

Pour cette phase de *brainstorming*, l'entreprise peut aussi bien solliciter ses collaborateurs en interne que ses partenaires ou ses clients. Il faut ensuite détailler les cas d'usages afin de sélectionner les plus prometteurs. Là aussi, l'entreprise peut faire appel à des partenaires internes ou externes afin de les aider à choisir les pistes les plus intéressantes.

2. Possédons-nous les compétences en électronique nécessaires pour concevoir l'objet, et sinon, où les trouver ?

La manière dont sera conçu l'objet dépendra bien évidemment du service que l'entreprise souhaite offrir. Par exemple le degré de fiabilité, la durée de vie et le niveau de précision souhaités de l'objet vont fortement influencer sur le choix des capteurs. La localisation des objets va, quant à elle, nécessiter de s'interroger sur leur degré d'autonomie, leur alimentation en énergie et le type de réseau de communication.

Chaque élément de l'objet devra être pensé lors de cette phase de conception/prototypage et il faudra également, durant cette phase, tenir compte du coût de production que cela impliquera. Une chose est sûre, la conception d'objets connectés nécessite des compétences variées. Dans la conception d'un objet, on distingue 2 composantes essentielles :

L'électronique pour le design et l'assemblage des différents composants (capteurs, actionneurs, processeurs, etc.),

L'intelligence embarquée, qui retranscrit les signaux reçus des capteurs pour les rendre compatibles avec les spécifications des réseaux de communication. On peut également y retrouver des algorithmes de chaînes d'actions.

Heureusement, des solutions existent pour compléter les compétences manquantes.

Pour accompagner ses clients EPHIKAS a sélectionné des fabricants, validé et testé les différents réseaux et méthodes et même développé des prototypes.

3. Comment allons-nous gérer les objets (déploiement, maintenance, etc.) ?

Un autre enjeu essentiel concerne la gestion des réseaux. En effet, du fait de leur nature même, les réseaux IoT multiplient les dispositifs et donc le nombre de points d'entrée et de connexions à gérer. Il est donc impératif de prévoir une architecture adaptée pour ainsi simplifier le déploiement et la maintenance des objets et du réseau.



Une plateforme d'accueil des objets, qui regroupe les différents services nécessaires à l'administration d'un réseau IoT, permettra de faciliter leur enregistrement, leur localisation, leur identification, ainsi que la gestion et la sécurisation des connexions.

4. Qui va développer les applications qui supportent le service ?

Les services se concrétisent toujours à travers diverses applications. Ces applications reçoivent les informations produites par les objets et les utilisent pour déclencher des actions ou soutenir la prise de décision. Elles sont un maillon clef pour la qualité globale du service.

Une application mal conçue ou trop lente pourrait remettre en cause l'efficacité du dispositif dans son ensemble. Il faut donc y accorder un soin particulier et optimiser l'expérience utilisateur, celle-ci pouvant à elle seule conditionner le rejet ou l'adoption d'un service.

5. Où et comment gérer la masse de données générées par les objets ?

Une fois en place, les objets vont commencer à envoyer des données. L'entreprise aura besoin de pouvoir collecter ces données afin de les traiter et d'en extraire de l'information utile. La plateforme d'accueil des objets servira de passerelle entre les objets et le système de traitement de ces données, en automatisant la collecte.

Afin de répondre aux besoins d'évolutivité, d'optimisation de l'expérience utilisateur, d'accessibilité et de sécurité, la plateforme EPHKAS est hébergée dans un environnement de type *Cloud* chez MICROSOFT.

Dans le cas où les services envisagés le nécessitent (ex : services de surveillance médicale, de prévention des incendies ou de détection d'intrusion, etc.), le système de capture et d'analyse des données doit être capable d'effectuer des traitements en temps réel et de façon parfaitement sécurisée.

6. Sommes-nous capables de traiter ces données en temps réel ?

Les projets d'IoT nécessitent deux types de traitements de données en fonction des applications et des usages. Par exemple, pour un usage de maintenance préventive, l'exploitant est informé des modes de fonctionnement incohérents. Ainsi, l'exploitant pourra intervenir au moment opportun pour procéder à ses opérations.

Lorsque l'on travaille dans des domaines qui nécessitent de la réactivité, nous pouvons mettre en place des algorithmes qui vont traiter les données et apporter des actions correctives en temps réel. Typiquement, dans le domaine de la maintenance prédictive, il est important d'analyser les informations afin d'informer les exploitants d'une panne probable et de sa cause.



7. Les réseaux en place sont-ils à même de permettre la communication avec les objets ?

Un autre aspect fondamental des projets IoT est la mise en place et la gestion d'un réseau d'objet qui permettra la communication d'un système à l'autre. Le premier point est le choix du réseau lui-même. Il existe plusieurs familles de technologies utilisables dans le cas de projets IoT :

- Des réseaux radio classiques (LTE, LPWAN, GSM...), en passant par le Wi-Fi,
- Des réseaux qui reposent sur des standards ouverts comme LoRa ou les réseaux IP,
- Des réseaux développés par des opérateurs comme Sigfox.

Il existe d'importantes différences entre ces technologies, c'est pourquoi une étude précise des cas d'usages est nécessaire afin de choisir la plus adaptée. Par exemple sur les réseaux de type LPWAN (LoRaWAN, Sigfox), il est impossible de faire du temps réel. La raison repose sur les spécifications technologiques de basse consommation, longue portée et basse fréquence. Cependant, pour de la télémétrie, ils trouvent tout leur sens. De plus, pour certains, ils sont unidirectionnels.

8. Comment pouvons-nous garantir la sécurité et la confidentialité de la chaîne de valeur de l'IoT (objet et infrastructure) ?

La sécurisation du réseau nécessite une adaptation des processus et des outils.

Si les objets collectent des données sensibles, l'entreprise doit également se soucier de leur protection aussi bien à la source (dans l'objet) que pendant leur circulation, jusqu'à leur stockage.

Aujourd'hui, les acteurs de l'IT sont conscients des enjeux de la sécurisation des infrastructures de l'IoT. Cependant, peu d'objets communicants sont aujourd'hui sécurisés. Pour cela, certains fabricants travaillent pour produire des composants de sécurité que l'on appelle « *SecureElement* ». Ainsi, la chaîne de valeur de l'IoT est entièrement sécurisée.

9. Avons-nous anticipé les contraintes liées à l'intégration avec le système d'information et à la sécurité des informations ?

Il est important de bien travailler en amont afin de bien identifier ses enjeux et ses processus. Ainsi, nous pourrions aisément concevoir un système qui serait compatible avec les outils décisionnels existants. Notre expertise des bases de données nous permet de nous interconnecter avec ces systèmes de gestion (ERP, GMAO, MES, LIMS, etc.)

La sécurisation des données faisant partie de l'ADN de Digora, nous tenons bien évidemment compte de cette composante.



Pour vous aider à répondre à ces 9 questions et vous aider à la mise en œuvre de votre projet, nous sommes à votre disposition pour un rendez-vous.

Contactez-nous pour que nous étudions ensemble votre projet IoT.

iot@ephikas.fr

<http://www.ephikas.fr>

<https://oit.ephikas.fr>

Ephikas IoT





Notre plateforme de services



L'Internet des objets ESP (Ephikas platform Services pour l'IoT) est une collection de services cloud gérés par EPHIKAS qui permettent de connecter, superviser et contrôler des ressources IoT. Plus simplement, une solution IoT est constituée d'un ou plusieurs appareils IoT et d'un service back-end exécuté dans un cloud qui communiquent entre eux.

Cette plaquette présente les principes de base de l'IoT, aborde les cas d'usage et décrit brièvement les différents services disponibles. En comprenant ce qui est à votre disposition, vous arriverez à savoir ce que vous souhaitez étudier de plus près pour vous permettre de concevoir votre environnement IoT.

Introduction

Les principaux éléments d'une solution IoT sont : les appareils, les services back-end et les communications entre les deux.

Appareils IoT

Les appareils sont généralement constitués d'un circuit avec des capteurs attachés qui se connectent à Internet. De nombreux appareils communiquent via une puce Lora ou SigFox. Voici quelques exemples d'appareils IoT :

- capteurs de pression sur une pompe
- capteurs de température et d'humidité dans une salle climatisée
- panne dans un ascenseur
- capteurs de présence dans une salle

Communication

Votre appareil peut communiquer avec les services back-end dans les deux sens. Voici quelques exemples de modes de communication de l'appareil avec la solution ESP.



Exemples

Votre appareil peut envoyer la température d'un camion réfrigéré mobile à un hub IoT toutes les 5 minutes.

Le service back-end peut demander à l'appareil d'envoyer la télémétrie plus fréquemment pour aider à diagnostiquer un problème.

Le back-end peut commander l'ouverture ou la fermeture d'une relais afin d'éteindre un éclairage ou de réarmer un disjoncteur ouvert.

Votre appareil peut envoyer des alertes basées sur les valeurs lues de ses capteurs. Par exemple, si vous surveillez un bâtiment de bureaux, vous souhaitez peut-être envoyer une alerte quand la température dépasse une certaine valeur.

Votre appareil peut envoyer des informations à un tableau de bord pour que des opérateurs humains puissent les analyser. Par exemple, relever la consommation électrique des différents services d'un bâtiment communal, les débits journaliers d'une pompe d'eau potable ou encore le suivi de température extérieur dans la cour d'un établissement scolaire.

Ces tâches, et d'autres, peuvent être implémentées à l'aide de la plateforme ESP.

Considérations relatives à la connexion

La connexion sécurisée et fiable des appareils est souvent le défi le plus important dans les solutions IoT. Cela est dû au fait que les appareils IoT ont des caractéristiques différentes de celles d'autres clients tels que les navigateurs et les applications mobiles. Plus précisément, les appareils IoT :

- sont souvent des systèmes intégrés, qui ne font appel à aucun opérateur humain (contrairement à un téléphone) ;
- peuvent être déployés sur des sites distants avec un accès physique coûteux ;
- sont accessibles uniquement via le serveur principal de la solution ; Il n'existe aucun autre moyen d'interagir avec l'appareil.
- peuvent avoir des performances et/ou des ressources de traitement limitées ;
- peuvent avoir une connectivité réseau intermittente, lente ou coûteuse ;
- peuvent nécessiter l'utilisation des protocoles d'application personnalisés, propriétaires ou spécifiques à un secteur.

Services back-end

Voici quelques-unes des fonctions que peut fournir notre service back-end.

Recevoir des données de télémétrie à grande échelle de vos appareils et déterminer comment traiter et stocker ces données.



Analyser la télémétrie pour fournir des insights en temps réel ou en différé.

Envoyer des commandes depuis le cloud à un appareil spécifique.

Présenter les données relevées, les rendre accessibles visuellement à l'aide de vues graphiques animées.

Monitorer les données recueillies, faire des calculs, construire des tableaux d'analyses.

Archiver les tendances (archives de grandeurs physiques horodatées) et les présenter sous forme graphique, courbes, camemberts, tableaux.

Gérer des événements, des alarmes, et informer des utilisateurs, par email ou par sms.

Contrôler l'état de vos appareils et surveiller leurs activités.

Par exemple, dans un scénario de maintenance prédictive, le back-end stocke les données de télémétrie historiques. La solution utilise ces données pour identifier un comportement anormal potentiel au niveau de pompes spécifiques avant qu'un problème réel ne puisse survenir. À l'aide de l'analyse des données, on peut identifier que la solution préventive consiste à envoyer une commande à l'appareil pour effectuer une action corrective. Ce processus génère une boucle de rétroaction automatisée entre l'appareil et le cloud qui augmente considérablement l'efficacité de la solution.

Démarrez

Démarrez rapidement grâce aux accélérateurs de solution et aux offres PaaS. Pour créer une solution entièrement personnalisable, choisissez parmi les solutions préconfigurées disponibles, celles permettant d'activer des scénarios IoT types (par exemple, la surveillance à distance, la maintenance prédictive et l'amélioration de l'efficacité énergétique).

