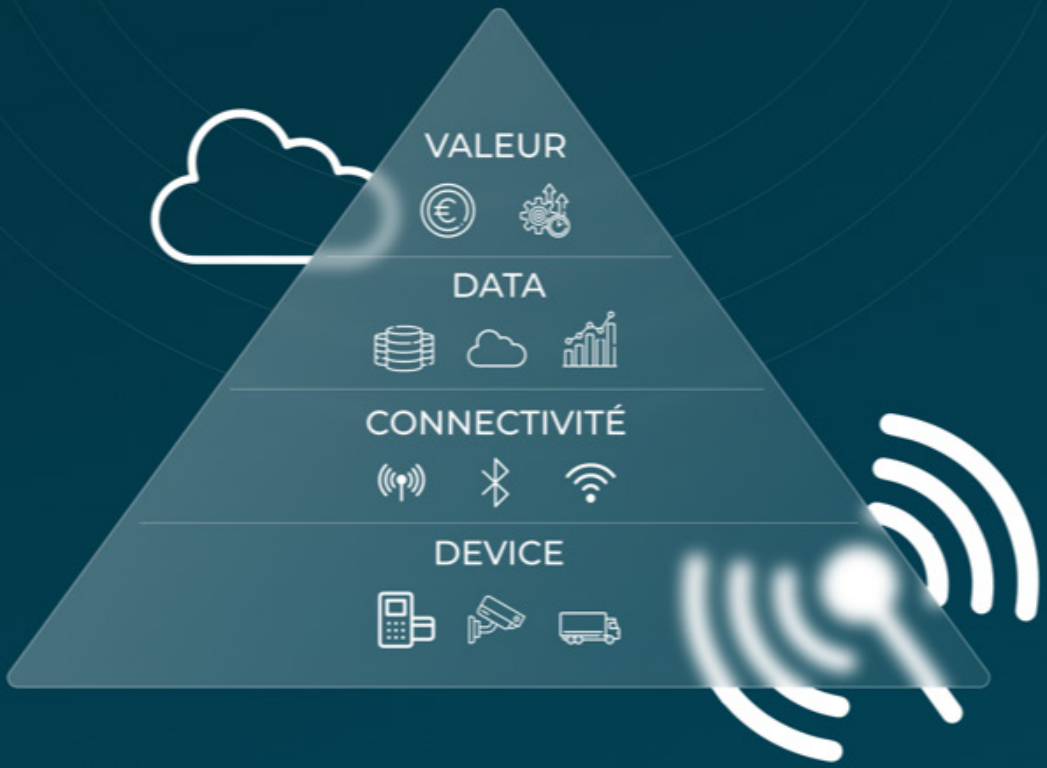
matooma
Wireless Logic Group

Le code de l'IoT

LES 4 ÉLÉMENTS D'UNE SOLUTION IOT À SUCCÈS



par Georges Dupont

Sommaire

Introduction

L'objectif de ce guide est de démystifier le fonctionnement d'une solution IoT et de comprendre les bases de son architecture.

Pour faciliter la compréhension, nous pouvons l'illustrer à travers une représentation pyramidale.

Ce guide s'adresse aussi bien aux dirigeants d'entreprise sans formation d'ingénieur, qu'aux product managers ou encore aux techniciens de terrain.

Nous avons vulgarisé chaque partie technique afin que tout un chacun puisse avoir une maîtrise des concepts de base.

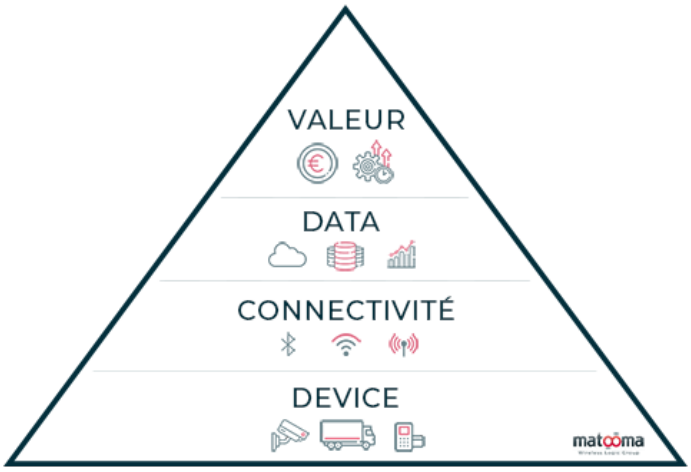
La pierre angulaire de cet article est de vous aider à atteindre votre objectif : **commercialiser une solution IoT qui apporte de la valeur pour vos clients** (réduction des coûts, augmentation des revenus, optimisation des process).

Il est naturel d'être intimidé par l'apparente complexité technique ou le jargon de l'univers IoT. A la fin de ce guide, vous aurez intégré les 4 éléments fondamentaux qui composent une architecture IoT, du device jusqu'à la monétisation de votre solution.

Les quatre piliers d'une solution IoT : une représentation pyramidale

Représenter une solution IoT sous cette forme permet de comprendre immédiatement à la fois son fonctionnement mais aussi la manière dont elle crée de la valeur.

Au-delà de son utilité pédagogique, la pyramide des besoins de l'IoT peut servir d'outil de communication au sein de votre organisation : aussi bien entre les différents services qu'avec vos clients et partenaires. Elle offre un cadre de référence et un lexique commun pour développer et marketer une solution IoT.



Pyramide de l'IoT, un outil pédagogique pour décortiquer une solution IoT

Notre pyramide peut être lue dans les deux sens.

Du bas vers le haut (bottom-up approach)

Approche destinée aux architectes réseaux IoT ou aux techniciens de terrain.

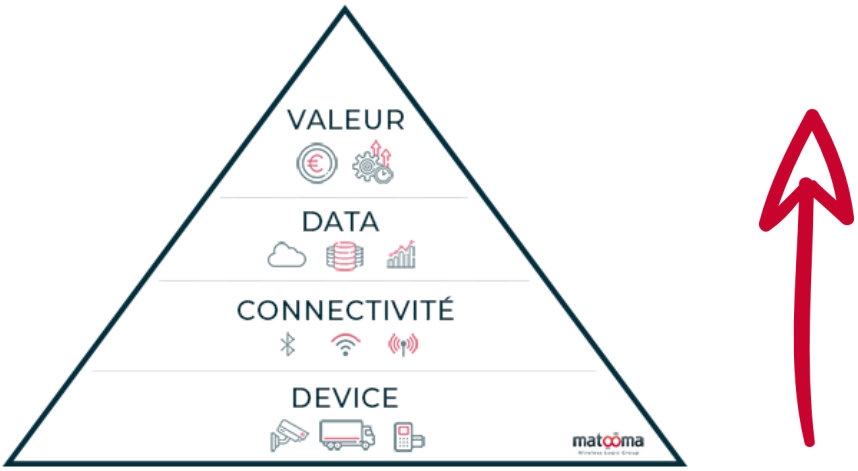
La base de la pyramide est constituée par les **capteurs** (devices), qui captent et collectent les données physiques environnantes. Cela peut être un taux d'humidité, une température, une présence, une pression…

Le niveau supérieur est celui de la **connectivité**, à savoir, comment cette donnée captée va être communiquée sur le réseau Internet. Vous connaissez sans doute déjà la plupart des différentes options de connectivité : le Wifi de votre foyer, le réseau cellulaire de votre téléphone, le Bluetooth de votre voiture, etc.

Nous verrons que d'autres technologies dédiées à l'IoT existent également.

Le troisième niveau est celui de la **data**. Les données arrivent à l'état brut. Ce sont des suites de chiffres qui doivent être triées, analysées, stockées.

Enfin, tout en haut de la pyramide, il s'agit de transformer ces données traitées pour leur donner du sens et de la **valeur**. Surtout, d'être en mesure de les présenter sous une interface compréhensible et utilisable : par exemple, l'application de votre téléphone qui communique la température de votre maison via les différents thermostats.



Du haut vers le bas (top-down approach)

Une approche customer-centric destinée aux product managers, marketeurs et spécialistes UX.

Nous partons cette fois-ci du sommet de la pyramide en identifiant la problématique à résoudre et de ce fait en définissant la proposition de valeur.

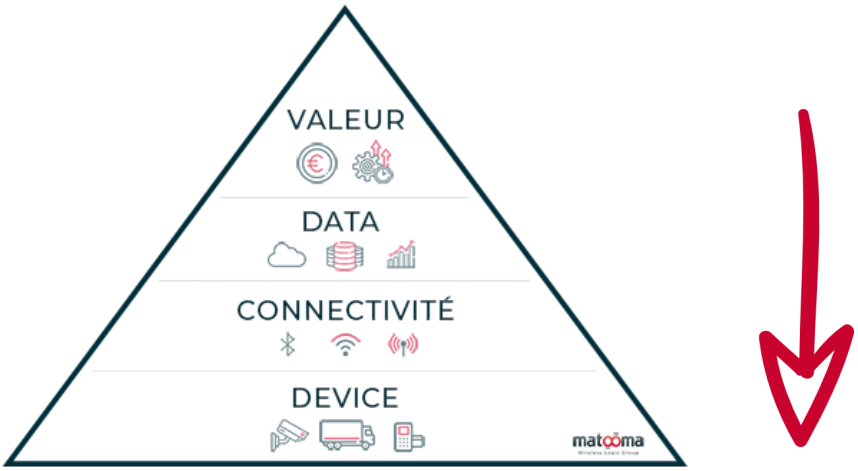
A titre d'exemple, une société produisant des vitrines réfrigérées reçoit, de manière récurrente de ses clients, des demandes pour alerter en cas de portes mal fermées. Cela entraîne des déperditions de fraîcheur et des risques de rupture de la chaîne du froid.

Il s'agit donc d'identifier quelles données vont être utiles pour résoudre ce problème. Dans notre exemple, il nous faut récupérer la température de chaque vitrine en temps réel et aussi savoir si la porte de chaque vitrine est bien fermée.

Pour remonter les données, il faut choisir la connectivité adéquate. Les vitrines étant statiques dans chaque magasin, il est possible de s'orienter vers du Wifi, chaque magasin ayant son réseau.

Vient enfin le choix des capteurs :

- pour la température, un capteur de type thermomètre connecté très résistant au froid
- pour savoir si la porte est bien refermée, un capteur infrarouge



1.

Le device

La partie **device** est la base réelle d'une solution IoT, sa brique physique. Il s'agit du boîtier installé sur un tableau électrique, du bracelet connecté que vous avez au poignet, ou de l'alarme d'urgence de votre ascenseur.

A l'issue de cette partie, vous saurez quels sont les composants principaux d'un device et quels critères prendre en compte dans son choix. Elle est principalement destinée aux acheteurs et aux product managers, avec une volonté de vulgariser l'ensemble des termes techniques.

Les composants d'un device IoT : le modèle 4+1

Nous pouvons isoler quatre composants principaux :

1. Le (ou les) capteur(s), qui capte(nt) les données
2. Le micro-ordinateur, qui traite les données
3. Le module de connectivité, qui transmet les données
4. L'alimentation électrique (continue ou sur batterie)

A ces quatre composants, nous ajoutons le logiciel qui gère la manière dont l'objet fonctionne et communique.
C'est la raison pour laquelle nous parlons de modèle 4+1.
Afin de mieux illustrer la manière dont fonctionne un device, nous ferons une analogie avec le corps humain.

1. Le capteur, les sens du device

Pour percevoir son environnement, le corps humain a cinq sens. Un device peut en avoir beaucoup plus.
Le capteur est le composant qui transforme une information physique (température, pression, débit...) en un signal électronique. Il en existe plusieurs types selon l'information que l'on souhaite récupérer. Parmi les types de capteurs les plus utilisés :

- **luxmètre** : mesure la luminosité (un éclairage public qui s'allume à la tombée de la nuit)
- **thermomètre** : mesure la température (un thermostat connecté qui rallume le chauffage en deçà d'un certain niveau)
- **hygromètre** : mesure l'humidité (pour savoir quand irriguer des cultures)
- **accéléromètre** : mesure la vitesse et les chocs (une alarme d'urgence se déclenche si votre voiture a eu un accident)
- **gyroscope** : mesure la rotation (permet à un drone ou une torpille de garder son cap)

Le capteur peut être physiquement séparé (juste relié par un câble) du "cerveau" du device, le micro-ordinateur.

2. Le micro-ordinateur, le cerveau du device

A la manière dont notre cerveau analyse les informations captées par nos sens, le micro-ordinateur héberge et fait fonctionner l'ensemble des programmes dictant le comportement de l'objet connecté.

Selon le cas d'usage, le type d'information et la complexité de celle-ci, il peut être plus ou moins miniaturisé.

Lorsque la tâche est basique ou requiert une action immédiate (une vanne se coupe en cas de détection d'une fuite de gaz), on parle de microcontrôleurs.

Lorsque la tâche requiert des actions plus élaborées, on parle de micro-ordinateurs. Ils sont comparables à un ordinateur dans leur fonctionnement mais réduits à la taille d'une carte bancaire. Parmi les fabricants les plus connus de ce type de composants, nous pouvons citer Arduino, Adafruit, Pololu et le plus célèbre Raspberry Pi

3. Le module de connectivité, la voix du device

Le capteur envoie un signal décodé par le micro-ordinateur, que l'on doit maintenant envoyer sur le réseau pour que la donnée soit récupérée et analysée à distance. C'est le rôle du module de connectivité, la voix du device.

Selon la connectivité choisie, le module de connectivité prendra des formes différentes. Il peut faire partie intégrante du micro-ordinateur (soudé dans la carte) ou prendre la forme d'un module séparé relié par un câble. Par exemple, un module Wifi peut être directement intégré dans la carte mère du micro-ordinateur ou bien prendre la forme d'une antenne déportée.

Le rôle de la gateway IoT

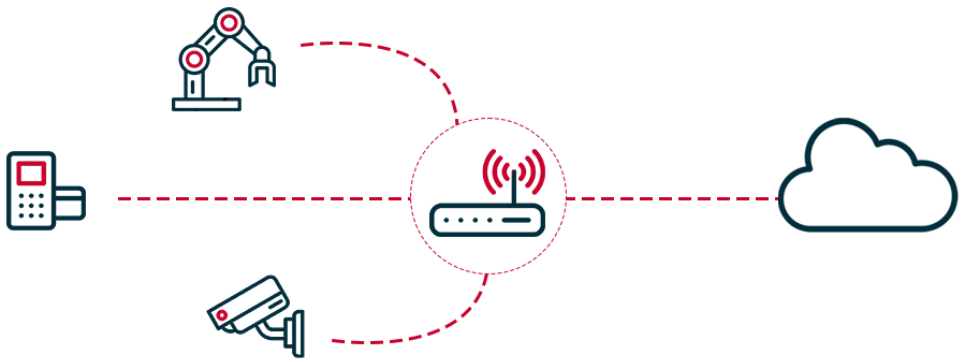
Le simple module de connectivité du device n'est pas suffisant pour établir une communication efficace avec le Cloud. De la même manière qu'un routeur Wifi domestique établit une connexion sécurisée entre votre ordinateur et internet, la gateway connecte les devices au réseau internet.

En revanche, le rôle de la gateway ne se limite pas qu'à cela.

Elle permet aussi de préparer les données issues des devices (consolidation, filtrage, nettoyage) avant de les transmettre aux plateformes cloud, où s'effectue le gros travail de transformation des données en intelligence significative. Cette étape préalable permet de réduire considérablement le volume de données à transmettre au cloud.

En envoyant moins de données, la gateway permet de réduire le coût de la connectivité et d'optimiser la durée de vie de la batterie.

Enfin, la gateway reçoit également des informations du cloud, renvoyées aux appareils pour permettre une gestion autonome des appareils sur le terrain.

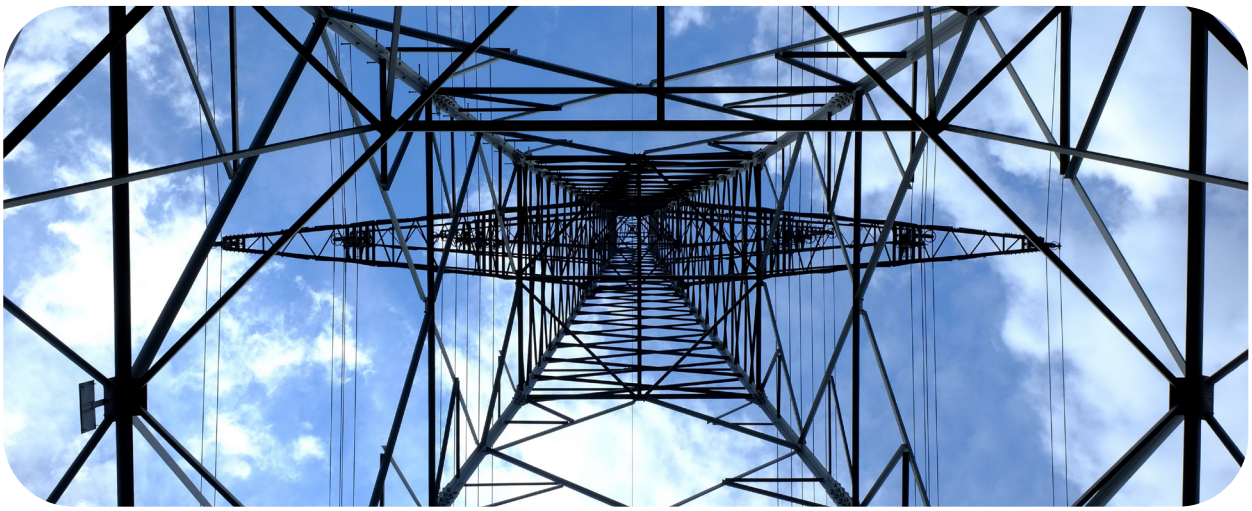


4. L’alimentation électrique, l’oxygène du device

Les possibilités d’alimentation électrique d’un objet connecté font partie des conditions prépondérantes dans le choix de la solution IoT. Selon qu’une alimentation électrique continue soit possible ou bien qu’une batterie soit nécessaire, cela impacte le choix de la connectivité, de la masse et de la fréquence de données pouvant être remontées.

Dans le cas de capteurs basiques qui ne font que remonter quelques octets par jour, une alimentation sur batterie est tout à fait envisageable. Elle peut durer une dizaine d’années voire plus. Si bien qu’au moment de l’épuisement de la batterie, les évolutions technologiques ont souvent rendu caduque le device en lui-même, qu’il vaut mieux remplacer.

Dans le cas de données massives ou continues, comme un flux vidéo, une alimentation électrique est nécessaire.



5. Le software, l'âme du device

Le software vient en quelque sorte donner vie au device en lui indiquant comment fonctionner.

Le système d'exploitation (OS) d'un objet connecté est assez éloigné de ceux fonctionnant sur ordinateur ou mobile. Il doit répondre à des challenges fondamentalement différents : mémoire, énergie et puissance limitées.

Parmi les critères de sélection d'un OS pour votre device il faut prendre en compte :

- le poids du système qui doit être le plus léger possible pour ne pas cannibaliser l'espace disponible
- la connectivité supportée
- la sécurité du système et sa fiabilité
- la modularité pour ajouter des fonctionnalités à la demande

Il n'existe pas encore de géant de l'OS IoT écrasant le marché (comme Microsoft ou Apple).

Les solutions sont multiples et souvent open-source. Nous pouvons citer parmi les plus utilisées :

- Contiki, qui existe depuis 2003
- FreeRTOS, créé par Amazon
- Mbed OS
- Embedded Linux
- TinyOS
- Raspberry Pi OS

Les points clés à vérifier avant de choisir votre device

Maintenant que nous avons détaillé les composants principaux d'un device et leur utilité, intéressons-nous aux critères de sélection.

Devez-vous développer vos propres composants ou acheter des solutions prêtes à l'emploi ?

Depuis une dizaine d'années, plusieurs fabricants ont développé des micro-ordinateurs si petits qu'ils peuvent convenir dans nombre de configurations IoT.

A titre d'exemple, une carte Raspberry pi Zero (qui inclut l'ensemble des composants d'un ordinateur) ne mesure que 65 sur 30 mm.

Une gamme complète de capteurs (détecteur de présence, thermomètre, caméra, micro) peut y être ajoutée facilement pour composer un ensemble prêt à l'emploi, sans connaissance technique particulière.

Ces solutions sont regroupées sous le terme Off-The-Shelf (OTS).

Cependant si cette solution est privilégiée dans le cas de prototypes ou de petites séries, elle devient beaucoup moins intéressante sur de gros volumes. Les limitations sont également bien présentes pour des dispositifs qui requièrent une miniaturisation accrue ou des fonctionnalités particulières.

Pour ces cas de figure, les solutions custom deviennent l'alternative obligée. Elles nécessitent évidemment beaucoup plus de ressources internes (supply chain, ingénieurs spécialisés).

Device fonctionnant avec batterie ou branché sur secteur ?

Si l'alimentation électrique continue est impossible, alors le recours aux batteries va influencer l'ensemble des choix du reste des composants, ainsi que le choix de la connectivité.

En effet, à l'exception des situations où le remplacement des batteries est aisé (des scanners dans un entrepôt que l'on recharge durant la nuit), nombre d'objets connectés doivent survivre des années avec la même batterie (comme des capteurs agricoles enterrés).

Utilisation intérieure ou extérieure ?

Les conditions d'utilisation de votre device jouent un rôle prépondérant dans le choix des composants et du boîtier.
Doivent-ils être résistants à l'humidité ? la chaleur ? la pression ?

Ces questions doivent être adressées dès la conception, ainsi que pour l'accès au réseau (device enterré ou à l'air libre).

Durée de vie

Pour quelle durée de vie est destiné votre device ? Par là, il faut comprendre que la vitesse des évolutions technologiques dans le domaine de l'IoT peut rendre caduque tout ou partie de votre solution. Il est donc nécessaire d'avoir cette donnée en tête afin de pouvoir ajuster le choix des matériaux et de la conception.

Rapport taille / poids

Le format de votre device répond-t-il à des exigences particulières ? Un device de type wearable (comme un bracelet connecté) doit rester léger et d'un format restreint. Doit-il répondre à une forme particulière, pour être intégré dans un véhicule ou une machine ?

Certifications

Enfin n'oubliez pas que les devices doivent répondre aux normes européennes et françaises, notamment en termes de sécurité et d'environnement. Celles-ci sont plus ou moins strictes selon les usages et les secteurs d'activité.

En conclusion

Un device IoT est probablement l'étape qui fait intervenir la plus grande hétérogénéité dans vos équipes. Ingénieur, électricien, informaticien; les ressources humaines à mobiliser et coordonner sont une étape essentielle dans la réussite de votre solution IoT.

2.

La connectivité

La connectivité de votre installation IoT est sans aucun doute la partie technique la plus importante dans la réussite de votre projet.

De ce choix va dépendre :

- la stabilité de la **communication entre les objets connectés** eux-mêmes,
- leur maintenance nécessaire,
- et la remontée des données vers vos centres d'analyse et de traitement.

Une erreur d'appréciation dans le choix du **réseau IoT** impactera le service que vous serez en mesure d'offrir à vos clients, d'un point de vue quantitatif et qualitatif.

Nous allons vous aider à comprendre les différents **protocoles de communication IoT** disponibles sur le marché et vous proposer un guide simple et efficace pour déterminer quel réseau IoT répond à vos besoins.

Brève introduction aux réseaux IoT

Cela va sans dire, la différence entre un objet quelconque et un objet connecté repose sur la connectivité de ce dernier.

Pour connecter un objet à Internet, plusieurs choix s'offrent à vous. Vous en connaissiez déjà certains : le Wifi, le Bluetooth, le réseau cellulaire (3G, 4G). Ce sont des modes de connexion extrêmement répandus et grand public.

Toutefois, certaines technologies comme le **LPWAN** ont été développées spécifiquement pour connecter les objets connectés. Elles ont pour but de minimiser la consommation énergétique, de maximiser la portée et de s'adapter au volume de données échangées.

Pourquoi le choix du réseau IoT est déterminant ?

Vous savez déjà que l'usage de vos objets connectés dépend grandement de leur mode de connectivité. Prenons un exemple du quotidien, le son de votre enceinte Bluetooth coupe au-delà de quelques mètres, ou bien le Wifi de votre appartement est moins fiable dans la chambre à coucher que dans le salon.

Pourquoi les enceintes de salon (type Sonos) sont connectées en Wifi alors que les enceintes portatives sans fil le sont en Bluetooth, et non l'inverse ?

Dans le premier cas, l'enceinte est uniquement faite pour être utilisée de manière immobile, branchée sur secteur, dans une pièce où le réseau Wifi est disponible.

Dans le second, l'enceinte Bluetooth peut être utilisée à la plage, recourant au réseau Internet de votre téléphone, par définition mobile.

Les trois éléments fondamentaux d'un réseau IoT

Chaque réseau dispose de ses points forts et de ses points faibles. Cependant, chaque technologie peut être considérée en fonction de trois critères :

- sa **consommation d'énergie** (combien d'énergie consommée pour envoyer 1 Mo),
- Sa **bande passante** (combien de temps nécessaire pour envoyer 1 Mo),
- Sa **portée** (sur combien de mètres ou kilomètres la connexion reste fiable).

A ces critères s'ajoute la fréquence à laquelle vous devez récupérer les données captées par votre objet (en temps réel, une fois par heure ou par jour).

Prenons l'exemple d'une caméra embarquée dans une voiture, appelée dashcam. Nous avons besoin de récupérer le film enregistré uniquement en cas d'accident.

Les dashcams connectées n'envoient donc le film à votre assureur qu'en cas de choc détecté, et suppriment les vidéos enregistrées au fur et à mesure le reste du temps.

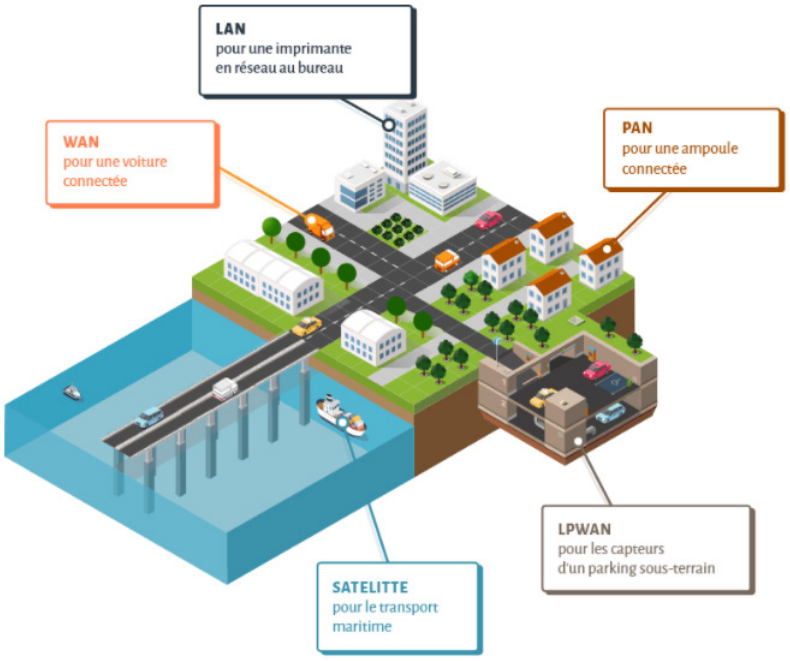
Quel réseau IoT choisir pour connecter vos objets ?

Passons en revue l'ensemble des technologies permettant à votre objet d'être connecté à Internet, en les classant en deux catégories :

1. Réseaux « **courte distance** » : de quelques centimètres à quelques mètres.
2. Réseaux « **longue distance** » : de quelques dizaines de mètres à plusieurs kilomètres.

Nous pouvons différencier les types de réseaux IoT selon cette typologie :

- **WAN** (Wide Area Network) : un réseau de plusieurs dizaines de kilomètres carrés
- **LPWAN** (Low Power Wide Area Network) : réseau de plusieurs dizaines de kilomètres carrés mais utilisant peu d'énergie (car peu de bande passante)
- **PAN** (Personal Area Network) : le réseau de quelques mètres (Bluetooth)
- **LAN** (Local Area Network) : le réseau Internet privé de votre domicile ou de votre entreprise (Wifi)
- **Satellite** : partout dans le monde pour peu de ne pas être dans un tunnel (GPS)



1. Les réseaux IoT courte distance

Bluetooth

Probablement la technologie la plus grand public, démocratisée depuis le début des années 2000. Sa consommation d'énergie est relativement faible ainsi que sa portée (environ **10 mètres**).

Le Bluetooth possède une bande passante intermédiaire (**entre 1 et 3 Mb/s**) mais amplement suffisante pour la plupart des utilisations classiques.

A titre d'exemple, vous pouvez streamer de la musique en MP3 mais difficile de relayer un film en HD. Le Bluetooth est un choix approprié pour beaucoup de **MedTech** (médecine).
Par exemple, la société **DiabNext** permet de surveiller son diabète à l'aide de capteurs connectés au téléphone en Bluetooth.

Zigbee

Le Zigbee est un **protocole de communication** similaire au Bluetooth mais dédié à l'IoT. Il consomme peu, et est fait pour envoyer de petits volumes de données (entre **20 et 250 Kb/s**). Il permet d'utiliser chaque objet comme "rallonge de connexion".

Par exemple, l'ampoule connectée de votre salon va permettre de connecter l'ampoule de votre chambre, comme un relai jusqu'au "hub", branché au réseau Internet. Les objets connectés de **Ikea** ou **Philips Hue** utilisent Zigbee.

Il s'agit d'envoyer en effet des ordres, tels que « **allumer la lumière** de la chambre», peu générateurs de données lourdes.

Wifi

Le Wifi permet un très important débit data (environ **400 Mb/s** pour les modems grand public récents), de manière fiable et sécurisée. Toutefois il consomme beaucoup d'énergie et sa portée est relativement limitée (**35 m**), d'autant plus au travers d'obstacles comme des murs épais.

Le **Wifi 6**, aussi appelé Wifi AX, nouvelle génération en cours de commercialisation, va permettre d'améliorer considérablement la connectivité des objets connectés.

Avec un débit de **10 Gb/s**, il permettra de gérer beaucoup plus d'appareils plus efficacement tout en consommant moins d'énergie : il s'agit de limiter le mode veille des objets en les "réveillant" lorsqu'un échange de données est nécessaire.

Le réseau Wifi très haut débit repose sur la couverture en fibre optique du territoire. Il est en effet nécessaire d'apporter le câble optique jusqu'à chaque terminal de chaque habitation ou entreprise.

Si c'est le cas dans la plupart des villes, nous en sommes très loin dans les zones rurales. En plus des **opérateurs télécoms,** plusieurs entreprises réalisent des poses de fibre optique à la demande, comme **Netiwan**.

RFID

Un mode de connexion particulier, dédié à l'identification. On pourrait le surnommer code-barre 2.0.

Une puce RFID permet d'identifier à distance, comme on le ferait en scannant un code-barre, mais jusqu'à **100 mètres**. C'est une technologie qui vient en complément d'autres types de connectivité.

Une société française comme **Ela Innovation** permet de faciliter considérablement la logistique des grands entrepôts grâce à l'**asset tracking**.

Pour aller plus loin

RFID, LoRa et cartes SIM-M2M : quand les technologies de connectivité deviennent complémentaires

NFC (Near Field Communication)

Son utilisation la plus connue est le paiement sans contact. Le NFC peut échanger un **très petit volume** de données sur une distance très rapprochée (quelques centimètres).

C'est une technologie largement répandue pour les ouvertures de portes dans les chambres d'hôtels. Elle permet aussi d'augmenter l'expérience utilisateur de manière ludique.

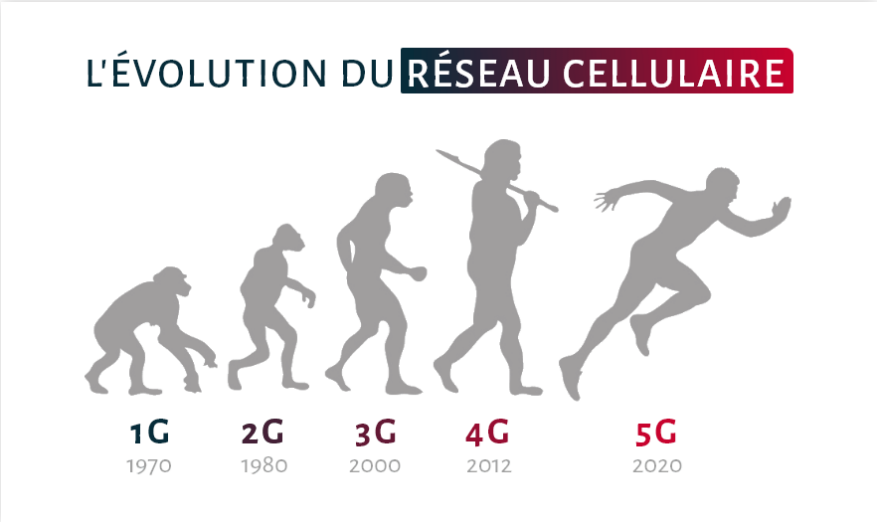
Par exemple la start-up **Yesitis** a développé des puces NFC dans des pochettes de disques vinyles, qui permettent à l'utilisateur d'accéder à la version numérique des titres, ainsi que d'autres contenus exclusifs.

2. Les réseaux IoT longue distance

Réseaux cellulaires

La technologie qui équipe nos téléphones portables depuis 30 ans. Plusieurs générations se sont succédé :

- **GSM :** supportant uniquement les appels et SMS
- **2G :** rendant possible l'envoi de MMS
- **3G :** initiant l'utilisation de l'Internet mobile
- **4G :** permettant le haut débit sur mobile, par exemple le streaming vidéo HD
- **5G** en cours de commercialisation (particulièrement adaptée à l'IoT très gourmand en data, comme les voitures autonomes).



Pour connecter votre objet au réseau cellulaire, il faut l'équiper, comme un téléphone, d'une carte SIM. Cependant, les **cartes SIM M2M** ne sont pas celles vendues pour le grand public. Elles sont appelées cartes M2M, **machine-to-machine**.

Elles ont plusieurs spécificités, par exemple de pouvoir résister à des températures extrêmes.

L'utilisation du **réseau cellulaire pour l'IoT** présente de nombreux avantages :

- les antennes sont déjà installées et dense;
- la couverture d'une antenne s'étend sur plusieurs dizaines de kilomètres;
- la configuration est minimale;
- la part de la connectivité dans le coût de l'IoT est beaucoup plus faible que pour d'autres technologies.

L'utilisation du réseau cellulaire par l'IoT est limitée par le fait qu'il est gourmand en énergie. Le choix du cellulaire est moins évident dans des zones sans accès au réseau électrique.

Les robots agricoles de la société **Naïo Technologies** sont équipés de cartes M2M pour pouvoir circuler à travers plusieurs hectares tout en restant connectés. Leur autonomie dure jusqu'à 10 heures et ils sont rechargés la nuit. Il ne s'agit donc pas d'avoir un branchement électrique continu mais un accès régulier à une recharge.

Enfin, le cellulaire est aussi un mode de connectivité **beaucoup plus sécurisé**. C'est donc une solution particulièrement adaptée aux services publics, comme la connexion de bornes de vélos en libre-service ou encore dans le **domaine de la santé** et de la **sécurité**.

LPWAN non cellulaire

Il s'agit d'envoyer de très petits volumes de données, entre **300 bits/s et 50 kbit/s**, sur une distance pouvant atteindre jusqu'à **40 kilomètres** et à travers des obstacles (murs, sous terre) en consommant le moins d'énergie possible.

La technologie IoT **longue distance** repose sur le fait que les normes et standards utilisés sont partagés par le plus d'acteurs possible. Il existe plusieurs systèmes concurrents, **sous ou sans licence**.

Les **technologies sans licence** sont présentes sur un spectre de fréquences "libres", à la manière des radios amateurs ou des **talkies-walkies**. Celles sous licence nécessitent une carte SIM, car les fréquences sont attribuées par les pouvoirs publics aux opérateurs (SFR, Bouygues, Free).

A noter que ce n'est pas parce qu'une technologie est sans licence qu'elle peut être utilisée de manière libre. Pour que votre objet soit connecté aux réseaux **Sigfox** ou **LoRa**, il est nécessaire d'avoir une puce compatible.

Sigfox (société française) est un réseau de communication ultra bas débit dans plus de 70 pays. Les objets connectés compatibles peuvent communiquer de très faibles volumes de data (12 octets) au maximum 140 fois par jour.

Le concurrent principal de Sigfox, **l'alliance LoRa**, est une association de plusieurs acteurs de l'IoT dans le monde, dont les objets sont connectés via la technologie **LoRaWan**, basée sur (et uniquement sur) une puce électronique Semtech.

Weightless est un standard open source. Son adoption est plus confidentielle que ses deux précédents concurrents, car son déploiement est plus récent. Il fait plus de sens pour des projets relativement sophistiqués ainsi que dans les cas où les débits ascendants et descendants sont tous deux importants.

Ces trois systèmes, parmi de nombreux autres LPWAN, sont principalement dédiés à l'Internet des objets de type capteurs et senseurs. Il s'agit d'envoyer de très faibles volumes de data (généralement entre **300 bits/s et 50 kbit/s**) :

- température dépassant un certain niveau
- changement anormal de pression dans une canalisation
- mouvement imperceptible sur une structure telle qu'un pont
- place de parking souterrain libre/occupée

La technologie LPWAN est donc parfaitement adaptée à ce type de mission, mais très limitée par la bande passante. S'il s'agit de communiquer des données plus lourdes (telles que des photos ou vidéos), le réseau cellulaire s'impose.

LPWAN cellulaire

Contrairement aux systèmes sans licence évoqués précédemment, les technologies **LTE-M et NB-IoT** consistent en une évolution de l'utilisation des antennes 4G existantes, et ne nécessitent pas la pose de nouvelles antennes.

Dans tous les cas, ces technologies permettent d'échanger sur le **réseau cellulaire,** donc avec une couverture réseau extrêmement solide et à travers plusieurs pays.

La batterie d'un capteur connecté grâce à ces technologies peut tenir entre **5 et 10 ans**.

La **technologie LTE-M** permet l'échange de faibles quantités de données pour une consommation énergétique très restreinte. Toutefois, c'est le dispositif LPWAN qui permet la plus grosse bande passante, en plus de la voix et le SMS.

Pour aller plus loin

Qu'est-ce que la technologie LTE-M pour les objets connectés ?

Le fait que la masse de données échangées est significativement supérieure aux autres dispositifs LPWAN, et qu'il intègre le **roaming,** en fait une solution de choix pour tous les dispositifs médicaux de surveillance et autres IoT wearables (montres et bracelets connectés).

Dispositif cousin du LTE-M, mais un débit data 4 fois plus faible (**0,24 kb/s contre 1 mo/s**), le **réseau Nb-IoT** correspond à un usage de type : capteurs de fuite d'eau, capteurs d'acidité pour les sols agricoles, capteurs de pollution de l'air.

C'est-à-dire l'envoi de données très légères (quelques chiffres) à intervalles régulières, et sur un capteur statique, qui peut être enterré sous plusieurs mètres (canalisations, parking souterrain, silo agricole, cave viticole...).

Satellite

Le réseau satellite reste encore l'unique solution pour les **zones reculées** (haute mer, désert, haute montagne), où il n'y a aucune alternative.

Les entreprises communément appelées du New Space (Space X, Blue Origin…) développent des projets de constellations qui ont pour but de **connecter toute la planète** à un réseau Internet haut débit.

Si la disponibilité commerciale de ce projet prend plusieurs années, la principale conséquence est d'avoir considérablement abaissé le prix du lancement de satellites, avec une répercussion sur le prix des services associés.

Les points à retenir

Si vous ne deviez retenir qu'un seul concept, il s'agit de la balance entre 3 critères : portée, bande passante et consommation d'énergie.

Le schéma ci-dessous illustre ce concept de manière très simplifiée.

La connectivité des objets connectés est assujettie à de constantes évolutions technologiques, économiques, politiques et normatives.

Si le choix du type de connexion (WAN, PAN, LAN ou LPWAN) s'impose à vous par les contraintes techniques de l'espace et de l'utilisation et de votre objet connecté, il existe des mouvements d'influence considérables pour imposer une norme particulière plutôt qu'une autre (entre Sigfox et LoRa par exemple).

A cela s'ajoutent les débats de société sur la **5G ou la robotisation**.

Le choix de la connectivité de votre gamme IoT dépasse donc un cadre purement technique, mais doit être associé à une **vraie réflexion stratégique**.

Pour aller plus loin

5 critères pour bien choisir son réseau IoT

3.

La data

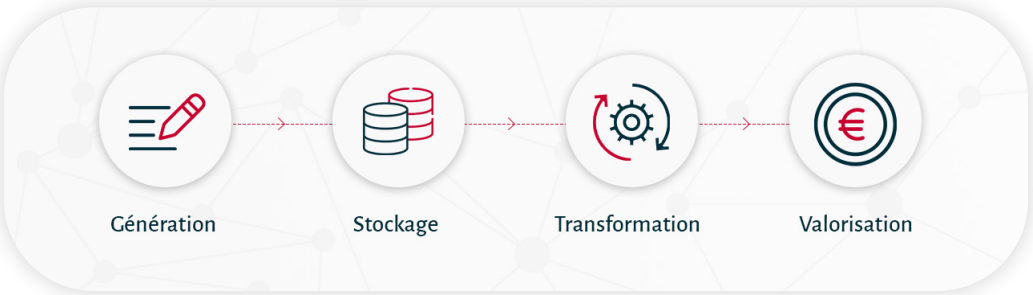
L'objectif principal d'une solution IoT est de transformer des données brutes en informations valorisables. Ces insights créent de la valeur soit en améliorant la productivité de l'entreprise soit parce qu'ils sont commercialisables.

Si les étapes précédentes de l'architecture IoT, qui consistent à capter puis remonter les données, sont primordiales, celle du traitement de la donnée l'est encore davantage. A la manière dont du pétrole brut va être transformé dans une raffinerie, les datas vont être disséquées, analysées, mélangées pour en extraire leur valeur.

Le cycle de vie d'une data : le data pipeline

Comme le serait une matière première dans n'importe quel cycle de production industriel, la data va cheminer dans un pipeline pour devenir exploitable. Ce pipeline peut être décomposé en quatre étapes successives : la génération, le stockage, la transformation et la valorisation.

Pour illustrer notre propos, nous prendrons l'exemple de données issues d'un ascenseur connecté.



1. Génération

Les datas sont générées par les **capteurs IoT** qui vont, par l'intermédiaire d'une gateway, les transmettre sur le réseau. Elles peuvent également avoir d'autres sources : base de données, CRM, données topographiques, etc.

A ce stade, ces données brutes, extraites du monde physique, ne sont pas utilisables en l'état. Leur lecture ne ferait aucun sens.

Dans notre exemple, les capteurs installés dans l'ascenseur communiquent la fréquence d'utilisation, les étages les plus fréquemment visités, le nombre de personnes (le poids calculé), la vitesse de l'ascenseur, les avaries plus le flux vidéo de la caméra de sécurité et l'utilisation de l'appel d'urgence.

2. Stockage

Les données générées par les capteurs vont être stockées, pour des durées variables selon le type de data, sur des serveurs géographiquement proches des capteurs.

Il est en effet inutile et coûteux d'envoyer la totalité des données brutes sur le Cloud. Une partie des données peut être conservée et même analysée localement, c'est ce que l'on appelle l'Edge Computing.

Dans notre exemple, les fichiers vidéo de la caméra de sécurité de l'ascenseur sont stockés sur un serveur situé dans le bâtiment, et automatiquement supprimés après une semaine. Pour des raisons de confidentialité et de coût, ils ne sont en aucun cas transmis sur Internet. Le reste des données, ne pesant que quelques octets par jour, est lui transmis en totalité sur le Cloud pour analyse au département Data de la société ascensoriste.

3. Transformation

C'est ici que la magie s'opère. Par une série d'opérations informatiques, les données vont être assemblées, dissociées, passées au crible des algorithmes pour en extraire des informations valorisables pour la société ou ses clients.

Pour cette société d'ascenseur, il s'agit d'identifier dans cette masse de données les signes d'une potentielle avarie avant qu'elle ne se produise. Pour cela, elle doit repérer des patterns, des éléments cachés dans les données qui sont les signes avant-coureurs d'une panne.

4. Valorisation

Les opérations de maintenance prédictive effectuées sur les ascenseurs durant le week-end ont permis de réduire considérablement les interruptions de service pour les clients de notre société ascensoriste. Elle peut commander les pièces à l'avance et réduire ses budgets de fonctionnement ainsi que les astreintes de ses équipes d'urgence.

Là réside la valeur principale d'une solution IoT, en pouvant, grâce à la data, à la fois améliorer ses services et réduire ses coûts.

A quel niveau faut-il analyser ses données ?

Qu'est ce que le Edge Computing ?

Au sein d'une architecture IoT classique, les données sont remontées dans leur ensemble sur le Cloud pour être analysées et transformées. Depuis quelques années, notamment grâce aux progrès techniques au niveau du hardware (ordinateurs moins onéreux et plus puissants), il apparaît parfois plus intéressant de traiter ces données localement.

Imaginons une entreprise fabriquant de la peinture, avec plusieurs sites de production disséminés sur des centaines de kilomètres. Si le siège souhaite connaître en temps réel les cadences de production, toute une série de données liées à chaque usine (consommation d'eau, d'électricité, vidéosurveillance) peut être analysée sur place.

L’intérêt du Edge Computing

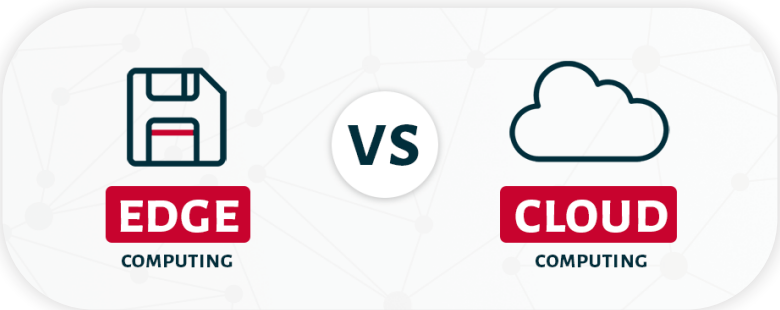
Traiter les données localement, sans passer par le Cloud, présente plusieurs avantages comme en premier, la vitesse de traitement. La latence s’en trouve réduite quasiment à zéro, ce qui, pour toute une série d’usages, est décisif (machines autonomes, VR/AR, hôpitaux).

Il est aussi moins coûteux et plus flexible de déployer de petites unités d’analyse en Edge qu’un seul énorme data center. Le ticket d’entrée pour ce type d’installation reste hors de portée pour la plupart des PME. De plus, il nécessite une infrastructure réseau colossale pour acheminer les données de l’ensemble des capteurs disséminés sur les différents sites de l’entreprise.

La démultiplication des points d’analyse rend la solution IoT dans son ensemble moins sensible aux failles de sécurité ou avaries techniques de grande ampleur. En effet, si l’un des sites est touché, il est bien plus envisageable de pouvoir le couper, le temps d’une intervention, que l’ensemble du réseau. Une installation en Edge computing améliore la maîtrise des impondérables de l’architecture IoT.

Edge computing VS Cloud computing

Les motivations à choisir le Edge peuvent être liées à la nature, à l’intérêt stratégique ou bien au volume des données en question. Reprenons notre exemple du fabricant de peinture. Si la direction nécessite d’avoir une vue d’ensemble sur la production et la livraison des commandes, pour améliorer sa productivité et son service client ; elle peut déléguer à chaque directeur d’usine la responsabilité d’améliorer les coûts et le fonctionnement de son propre site.



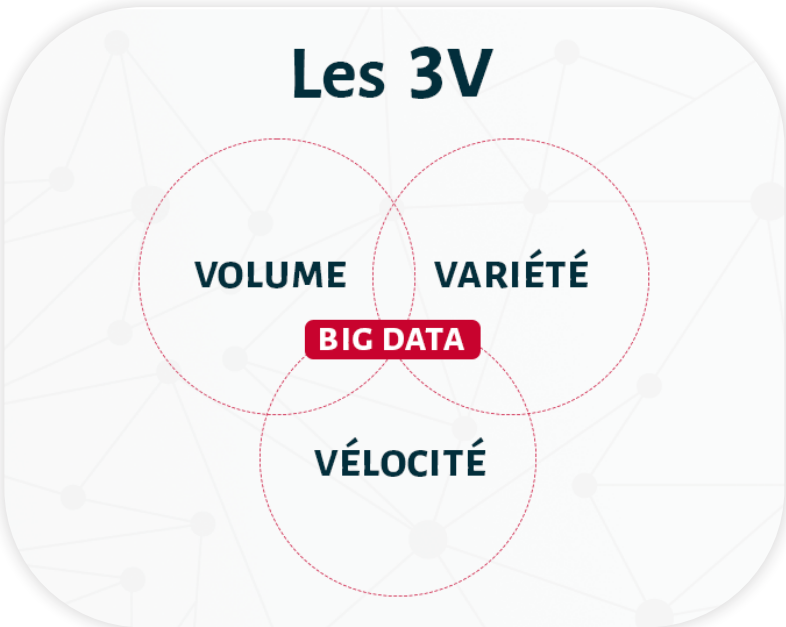
Faire face à l'hétérogénéité des données

Une installation industrielle, disons une usine automobile, remonte d'immenses quantités de données très hétérogènes, et ce sur plusieurs sites. Il est nécessaire de penser en amont, une véritable stratégie data pour savoir :

- quelles données méritent d'être captées
- quelles données méritent d'être remontées sur le cloud
- quelles données méritent d'être stockées pour une utilisation future potentielle

Selon la nature de la data, il sera nécessaire de la prétraiter pour la rendre compatible avec d'autres sources de données. Des capteurs sur une machine industrielle et une caméra thermique sont conjointement intéressants s'ils répondent au même timecode. Il sera donc nécessaire de combiner les deux sources de données à travers un programme informatique pour visualiser et comprendre les données.

Certaines données ont une utilité lorsqu'elles sont en temps réel, par exemple une balise géolocalisée sur un camion de livraison - d'autres uniquement sur un temps long, comme des capteurs environnementaux en forêt.



Le challenge du volume de données

Par définition, les données générées par les capteurs IoT s'accumulent sur une architecture réseau qui est, elle, limitée en capacité. Une installation permettant de stocker 10 terabytes de données sera vite saturée avec 1 terabyte supplémentaire uploadé chaque mois.

Nous observons généralement un biais qui consiste à remonter beaucoup plus de données qu'il serait utile, entraînant plusieurs conséquences néfastes :

- une saturation des espaces de stockage
- une impossibilité d'analyser efficacement les données
- une surconsommation des frais de communication

C'est ce que l'on appelle le data overload, pouvant résulter en l'échec du déploiement de la solution IoT et la destruction des données accumulées, leur stockage devenant trop coûteux.

Il convient donc d'effectuer les opérations adéquates pour traiter les données et réduire leur volume. Par exemple, les données d'un compteur de gaz peuvent être compressées en ne gardant qu'une moyenne quotidienne plutôt que les chiffres exacts heure par heure.

Conserver des données pour une éventuelle utilisation future révèle un manque de préparation dans le déploiement de la solution IoT. Chaque donnée captée doit répondre à un objectif précis : optimisation de la productivité, réduction des coûts, amélioration de la relation client.

Vélocité des données

Une question cruciale lors de la définition de la stratégie data consiste à déterminer la fréquence à laquelle la data doit être accessible. Un détecteur de fuite de gaz doit pouvoir communiquer ses données au plus vite, ce qui est moins le cas pour un compteur électrique.

Batch VS streaming

Le batch consiste à traiter de larges volumes de données sur un intervalle défini. Par exemple, chaque soir, les données des panneaux solaires d'un bâtiment sont relevées et analysées.

Le streaming, à la différence du batch, analyse les données en continu et en temps réel.

Le batch est moins onéreux et adapté aux larges volumes de données. Il n'est toutefois pas adapté à nombre de situations qui nécessitent une surveillance continue (sécurité, santé).

Les enjeux de la sécurité des données

Les données doivent faire l'objet d'une politique de sécurité à part entière. Elles peuvent être la cible de vol, de clé d'entrée dans le réseau d'une entreprise ou tout simplement de perte liée à une erreur humaine ou avarie technique.

Il faut ajouter à cela les risques liés à la confidentialité des données, quand celles-ci concernent des personnes physiques (dispositifs médicaux, géolocalisation).
La data fait l'objet de menaces différentes selon sa progression dans le data pipeline.

- au niveau des devices, via leur fragilité; qu'elle soit hardware ou software;
- au niveau des gateways, par une carence de mise à jour ou des interruptions de service (qui va impacter l'ensemble des devices connectés à cette gateway);
- au niveau de la connectivité, avec des interceptions des communications;
- au niveau du Cloud, par des fragilités des programmes informatiques;
- et enfin au niveau de l'application, par des failles sur l'authentification des utilisateurs.

L’impact du type de data sur le choix de la connectivité

Le type, l’hétérogénéité, la vélocité et le volume de data, tous ces facteurs vont venir impacter le choix de la solution IoT, et en particulier de la **connectivité**.

Si une connectivité **LPWAN** suffit pour remonter des batch de données techniques (relevés de compteurs, données météo), une connexion cellulaire ou haut débit câblé (fibre) est nécessaire pour des datas en streaming ou volumineuses (flux vidéo).

Avec l’arrivée des réseaux **5G privés**, principalement pour des solutions industrielles de grande ampleur, même des réseaux locaux (Edge) peuvent avoir recours à une connectivité cellulaire. Les nouveaux usages (robotique, drones, AR/VR, télémédecine), nécessitant des latences quasi nulles, devront pour répondre à ce challenge technique combiner l’Edge computing et la 5G.

4.

La valeur

Il s'agit du but ultime d'une solution IoT : créer de la valeur pour l'utilisateur final.

Selon **John Rossman**, qui décrit dans son livre la stratégie d'Amazon sur le marché de l'IoT, il y a principalement trois clés d'entrée :

- en réinventant l'expérience client
- en améliorant les process de production
- en concevant de nouveaux business models

Ces opportunités s'adressent autant aux start-ups qu'aux sociétés installées depuis des décennies. En connectant ses "objets" (machines, flotte automobile, outils, stocks), l'entreprise transforme ceux-ci en une vraie machine à générer des données et donc des informations qui, bien utilisées, peuvent être de véritables facteurs de croissance. Il y a, à ce jour, quatre principaux business models liés à l'Internet des objets.

Le business model “hardware”

Le meilleur exemple est celui des drones. Les fabricants s’adressent à la fois aux particuliers et aux professionnels, avec des gammes très larges. L’utilisateur final achète l’objet connecté (le drone) pour ce qu’il est.

Le business model “plateforme”

Comme le fait Amazon avec Alexa, ou Apple avec l’app store. L’objectif est autant, sinon plus, de générer des revenus avec la plateforme d’applications qu’avec l’objet en lui-même.

Amazon vend son boîtier Alexa a prix bas pour constituer une base d’utilisateurs très large et ensuite facturer l’utilisation de la plateforme aux sociétés qui l’utilisent (Uber, Dominos Pizza, etc.).

Le business model «outcome» (résultat)

Principalement utilisé dans le domaine des transports, et surtout des nouvelles mobilités. Lorsque vous louez une trottinette électrique en libre service, vous ne payez que pour vous déplacer d’un point A à un point B.

Cette approche repose sur l’élimination de toutes les frictions afin de proposer à l’utilisateur uniquement son besoin immédiat.

Le business model «data»

Notamment pour les sociétés de service ou de conseil. Il s'agit de n'utiliser que les données récupérées ou achetées à un tiers pour les transformer et revendre les fruits de cette analyse.

Pour illustrer cette création de valeur concrète, nous pouvons citer comme cas d'usage :

- un compteur d'eau connecté qui détecte les fuites et alerte dès les premières minutes d'un sinistre. L'usager évite ainsi les mauvaises surprises sur la facture et un dégât des eaux;
- des colliers GPS pour animaux de compagnie dont les données générées sont revendues à des laboratoires vétérinaires ou pharmaceutiques;
- le capteur géolocalisé d'un poids lourd qui permet d'ajuster en temps réel le parcours le plus rapide et d'avertir le client du délai exact de livraison.

Que retenir de ce guide ?

Si la complexité technique est réelle et les challenges permanents, votre proposition de valeur pour l'utilisateur final doit être limpide.

Chaque étage de votre architecture IoT doit être pensé et conçu en interaction, en amont et en aval du flux de données. Il est aisé de se perdre dans des solutions trop lourdes pour les besoins ou à l'inverse inflexibles dans un univers en évolution permanente.

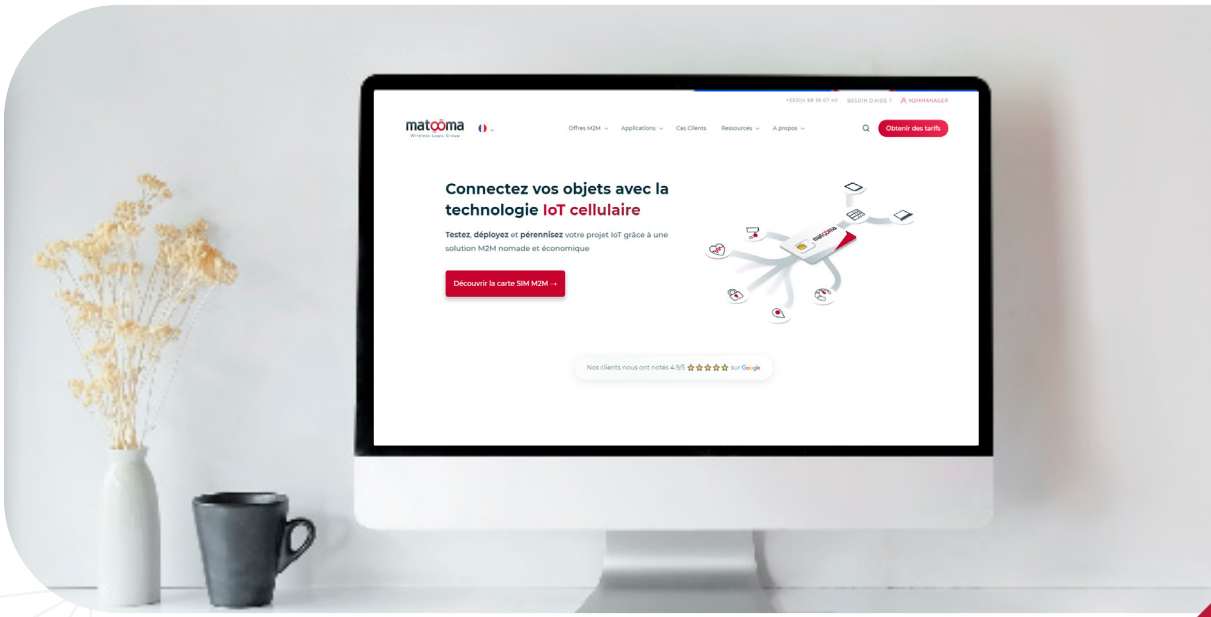
Qui est Matooma ?

Matooma est une société qui aide les professionnels à déployer leurs projets IoT/M2M en France et à l'international de façon simple, économique et rapide grâce à la mise en place d'un guichet unique made in France.

Fondée en 2012, Matooma rejoint le groupe international Wireless Logic, licorne européenne, en juillet 2019, afin de renforcer son expertise dans la fourniture de cartes SIM multi-opérateurs et de services M2M/IoT industriels.

Nous proposons des offres sur mesure de connectivité multi-opérateur ainsi qu'une plateforme de gestion, à destination des fabricants d'objets, exploitants de services, intégrateurs et distributeurs de solutions. Nos offres de connectivité sont adaptées, personnalisées et sans engagement afin de répondre aux besoins de chacun et notre équipe experte vous accompagne tout au long de votre projet. Leaders en France sur le marché de la sécurité des biens et des personnes (téléassistance, système d'alarme, vidéosurveillance...), nous permettons à nos clients de bénéficier d'une carte SIM unique couvrant 180 pays et des accords de roaming avec plus de 540 opérateurs partenaires.

Matooma, spécialiste dans son domaine pourra, à ce titre, vous fournir des conseils précis afin de vous orienter vers une solution IoT simple, économique et pérenne.



Inscrivez-vous à la MatooNews
et recevez nos infos IoT

Contact :

https://www.matooma.com/fr/contact

CONTACTEZ NOUS

Notre site Internet :

https://www.matooma.com/fr

VISITER LE SITE

Le pôle marketing et communication :

communication@matooma.com

ENVOYER UN EMAIL

matooma
Wireless Logic Group