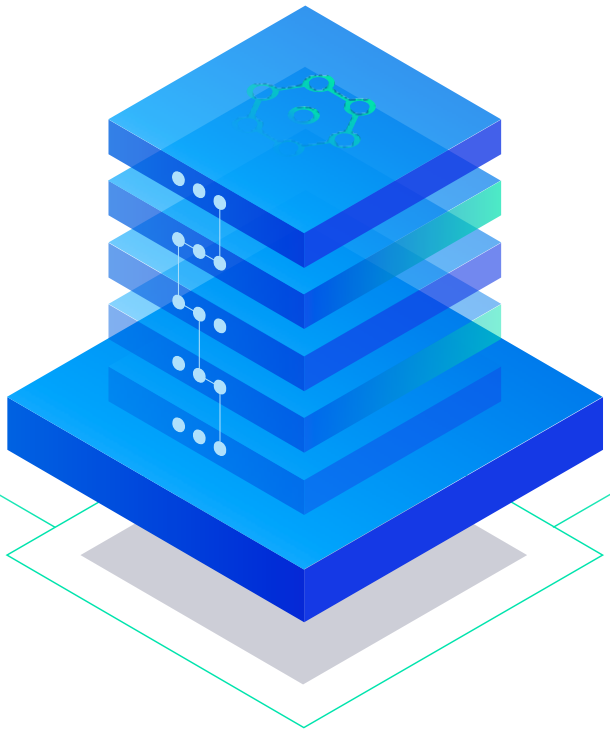
Livre blanc #2

S'orienter dans les technologies IoT

IT LINK
Accélérateur d'innovation

SOMMAIRE



Chef de rédaction : IT LINK
Réalisation : Voyez Large
Crédit Photo : Adobe Stock
Avril 2021

De l'Internet des écrans à l'Internet des objets

1. Aux prémices de l'Internet des objets
2. Fonctionnement global d'une solution IoT

1. Aux prémices de l'Internet des objets

L'Internet des objets (IoT - Internet of Things) connecte une immensité d'objets et des milliards d'êtres humains. Depuis une dizaine d'années, il permet d'améliorer de manière progressive et à la fois considérable **nos capacités à rassembler, analyser, et restituer des données** pour les transformer ensuite en informations et en connaissances pertinentes afin de répondre aux enjeux cruciaux de l'industrie.

Pour décrire et comprendre cette technologie, il est utile de revenir sur son évolution.

À partir de 1968, **la nécessité de partager, de diffuser et d'échanger de l'information sans l'intervention de l'Homme**, notamment dans le monde industriel, conduit à la création du concept de **Machine-to-Machine (M2M)**. Dans ce contexte, de nouveaux systèmes apparaissent comme la technologie des contrôleurs logiques programmables dite PLC (Programmable Logic Controller) permettant d'automatiser des commandes, de collecter de la donnée et d'exécuter des opérations en temps réel.

Avec sa liaison de capteurs, de données et de réseaux, le M2M a généré au fur et à mesure de nombreux usages tant dans l'industrie que dans la logistique telles que **la télésurveillance, la mise à jour à distance d'écrans d'affichage ou l'automatisation des chaînes de production industrielle**. Certaines entreprises étaient donc déjà familières d'un concept proche de l'IoT.

La notion **d'objet connecté** est quant à elle **introduite sur le réseau IP à partir des années 1980-1990**. Elle cible en particulier le grand public. Plusieurs expériences voient le jour, avec la création de **technologies innovantes capables d'établir des passerelles entre le monde virtuel et des objets physiques**, comme des distributeurs de boissons reliés à distance pour contrôler le stock de boissons fraîches ou une lampe connectée émettant des messages vocaux ou lumineux présentée en 1994 par la société française Violet. Quelques visionnaires s'intéressent sérieusement au sujet, à l'image de Paul Saffo qui publie un article en 1997 sur les capteurs, à l'origine d'une nouvelle vague d'innovation du secteur informatique.

L'appellation **Internet des objets (IoT), apparaît en 1999**. Employée par Kevin Ashton, directeur du centre Auto-ID au MIT (Massachusetts Institute of Technology) lors d'une conférence, ce dernier présentait l'avantage d'intégrer des micropuces dans tous les produits du géant de la consommation Procter & Gamble, afin de contrôler leur chaîne d'approvisionnement.

L'essor de l'IoT s'explique par **le développement des réseaux de communication, permettant des applications beaucoup plus étendues dans la récolte de données**. Si l'Internet des objets s'inscrit dans la continuité du M2M, il se différencie notamment grâce à une machine ou un objet doté de capteurs permettant d'être autonome et de s'adapter à un environnement donné, tout en étant perceptible par d'autres machines ou objets. Il permet ainsi d'élargir le champ des possibles.

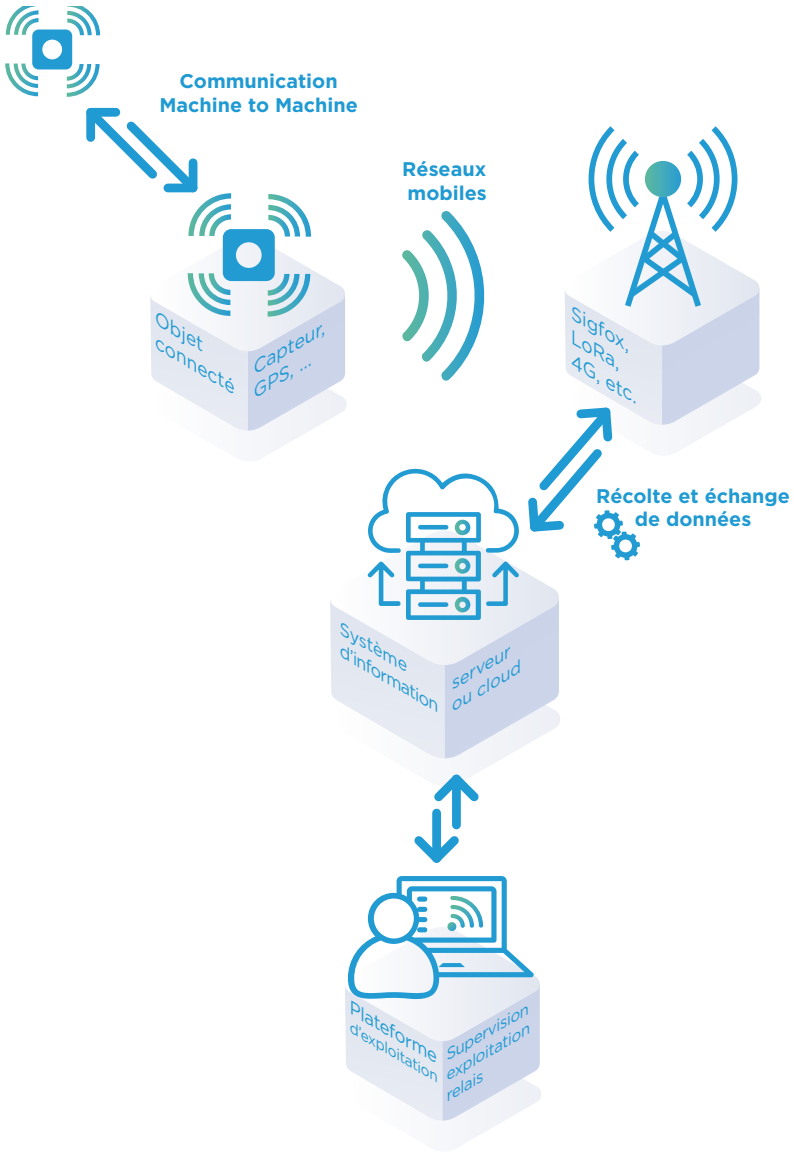
Ce n'est qu'en 2010 que l'IoT va s'intégrer plus concrètement dans **la stratégie globale des entreprises**. Dès lors, les réflexions sur le sujet et ses applications seront focalisées sur **la réduction des coûts, le gain de productivité et la création de nouveaux modèles économiques**. C'est désormais « l'ordinateur qui va générer de la nouvelle information et non plus les humains » (Conrad Wolfram). Au fil du temps, les systèmes vont générer de plus en plus de données que **des technologies de plus en plus pointues vont pouvoir traiter plus facilement**.

Aujourd'hui, l'Internet des objets est devenu **un levier puissant dans le monde professionnel**. De multiples solutions IoT devenues incontournables dans les entreprises et industries sont alors proposées pour répondre aux problématiques de demain.

Point de vue IT Link

« Depuis le début de sa démocratisation il y a 30 ans, internet a permis de connecter plus de 4,5 milliards d'humains au même environnement. Aujourd'hui, ce chiffre est multiplié par 10 lorsqu'on parle d'objets connectés. »

2. Fonctionnement global d'une solution IoT



Un panel d'options techniques disponibles pour des contextes et des enjeux très variés

1. Analyser un projet IoT
2. Répartir les traitements et les données
3. Choisir une technologie de communication
4. Définir l'architecture de la plateforme d'exploitation

1. Analyser un projet IoT

À première vue, les projets IoT partagent une architecture commune : des objets communicants déployés sur le terrain, un réseau de communication et une plateforme de stockage, d'analyse et d'exploitation des données.

En réalité, la diversité des contraintes techniques et d'enjeux spécifiques impose à chaque fois des choix techniques très différents. La première étape consiste donc à bien identifier les différentes caractéristiques qui doivent guider un projet IoT vers les bonnes solutions.

Les contraintes directes sur l'objet portent principalement sur :

- L'encombrement
- L'alimentation électrique
- Le raccordement à un réseau d'entreprise et l'accès à internet

À celles-ci s'ajoutent les contraintes induites sur la puissance de calcul et la capacité de stockage local, directement impactées par les contraintes d'encombrement et d'alimentation.

Il est également essentiel d'étudier les contraintes relatives aux transferts de données :

- Quel est le volume des données à transmettre des objets vers le serveur ?
- Est-il nécessaire de prévoir l'envoi de données de configuration ou de commandes de la plateforme vers les objets ?
- Les données contiennent-elles des données personnelles, voire des données sensibles soumises à des réglementations spécifiques (vidéo sur un espace public par exemple) ?
- L'envoi des données et leur exploitation doivent-ils se faire en temps réel ou pseudo-réel (quelques minutes de délai maximum) ? Un délai de plusieurs heures ou plusieurs jours entre l'acquisition et le traitement reste-t-il compatible avec l'usage attendu ?

De la même manière pour les contraintes sur la plateforme d'exploitation :

- Quelle est la volumétrie globale des données qui seront conservées et analysées ?
- Quelle est la nature des données reçues ? Des données générées ? Quel est leur niveau de confidentialité et de criticité ?
- Quelles sont la puissance de calcul et la bande passante nécessaires pour gérer l'ensemble du parc ?
- Quels sont les utilisateurs de la plateforme ? Comment s'y connectent-ils (PC, mobile, tablette, ...) ?
- Quels sont les autres systèmes avec lesquels la plateforme doit collaborer, les interfaces à prévoir, etc. ?

L'analyse sur les fonctions « métiers » de la solution IoT (« Data management ») doit être complétée en prenant en compte les contraintes liées à la gestion des objets eux-mêmes, telles que la supervision de leur fonctionnement, la mise à jour logicielle/firmware, etc. (le « Device management »).

La diversité des cas d'usage de l'IoT a conduit à l'émergence de nombreuses briques technologiques, qui permettent chacune de pallier efficacement à une ou plusieurs contraintes spécifiques de chaque projet. Il s'agit de correctement les identifier et savoir quand et comment les utiliser à bon escient.

2. Répartir les traitements et les données

Les contraintes et les coûts liés à la transmission de gros volumes de données ont fait émerger le concept de « Edge Computing », ou « Processing des données au plus proche du capteur » **pour limiter les données envoyées au serveur à des informations déjà consolidées ou pré-traitées**.

L'objet déployé sur le terrain n'est plus un simple capteur. **Il embarque des ressources en CPU, mémoire, stockage, etc. qui lui permettent de transformer la donnée brute issue des capteurs en une information synthétique**. Par exemple, l'analyse d'un signal vibratoire permanent pour superviser un moteur permettra de détecter une séquence anormale et d'envoyer dans ce cas un message d'alerte vers le serveur. Sans un traitement local, le signal doit être intégralement et continuellement transféré vers le serveur. Avec une détection **par traitement local du signal, la communication se limite à quelques messages, lorsqu'une anomalie est effectivement détectée**.

Les solutions de « Edge Computing » peuvent également s'imposer pour éviter le transfert de données personnelles ou sensibles. Par exemple, dans le cadre de solutions d'analyse de flux d'individus dans un lieu recevant du public, les données pouvant revêtir un caractère personnel (vidéos, traces WiFi…) sont traitées en local afin d'être « anonymisées » avant d'être transmises à la plateforme d'exploitation.

La contrepartie à l'utilisation du « Edge Computing » se traduit par **une plus grande complexité matérielle de l'objet sur site**, avec un encombrement plus important, une consommation électrique accrue, et éventuellement une durée de vie plus faible.

Edge Computing

⊕ minimise les transferts de données, diminue les coûts et les enjeux techniques liés à la communication

⊖ augmente la complexité et la taille de l'objet, sa consommation énergétique et son coût global

La partie « Edge Computing » peut parfois être localisée dans un équipement intermédiaire, situé sur le terrain à proximité des capteurs. On parle alors d'équipement passerelle ou « Gateway ».

La « Gateway » est connectée aux capteurs par une solution de communication locale, qui peut être filaire comme Ethernet ou radio en utilisant une solutions adaptée WiFi, LoRA, ou autre. Elle est capable d'héberger des traitements, et dispose d'une solution de communication vers le serveur 4G, Lora, SigFox ou autre. Des équipements de ce type sont maintenant disponibles de façon standard chez de nombreux constructeurs (Reliagate Eurotech, GenPro Ercogener, etc.), avec différentes caractéristiques permettant d'adresser une grande diversité de contextes.

Gateways

Relais entre un réseau de capteur et la plateforme d'exploitation

⊕ permet de simplifier les capteurs en déplaçant la gestion des communications et du « Edge Computing » dans un composant spécialisé

⊖ complexifie l'architecture

Certains traitements resteront dans tous les cas localisés sur la partie plateforme, soit parce qu'ils nécessitent une puissance de calcul trop importante, soit parce qu'ils consolident des données en provenance de plusieurs sites terrain.

Les traitements sur le serveur

⊕ disponibilité de ressources, traitements corrélés entre plusieurs objets émetteurs, capacité à mettre en place de la scalabilité horizontale pour gérer la montée en charge

⊖ impose de transférer au serveur toutes les données nécessaires au traitement

3. Choisir une technologie de communication

Le développement récent de l'IoT est également lié à l'apparition de nouvelles technologies de communication, qui permettent de répondre à des enjeux et de prendre en compte des contraintes qu'il était difficile d'adresser auparavant.

L'évolution des réseaux mobiles « grand public » pour le transfert de données (3G, 4G, 5G…), aussi bien du point de vue du débit utilisable que de la couverture territoriale, facilite le déploiement de systèmes connectés sur tout le territoire.

En complément à ces réseaux initialement destinés à la téléphonie mobile, sont apparues de nouvelles solutions, qui ciblent spécifiquement les enjeux des objets connectés :

- La couverture maximale d'un territoire avec une infrastructure minimale.
- Un faible coût d'accès au réseau, lorsque le volume de données à transmettre est réduit.
- L'optimisation de la consommation électrique dans les échanges avec le réseau.

Ces nouvelles solutions, regroupées sous l'acronyme de LPWAN (Low Power Wide Area Network), dont font partie par exemple les technologies SigFox et LoRa, ont contribué à l'apparition d'objets connectés à faible coût, avec une consommation électrique suffisamment faible pour permettre un fonctionnement sur batterie pendant plusieurs années. De nouveaux cas d'usage ont ainsi pu être adressés et déployés massivement (traceurs GPS autonomes, conteneurs connectés, ...).

Lors de la conception d'un système IoT, la technologie de communication doit être sélectionnée en fonction du niveau d'autonomie de l'objet communicant, et du volume de données qu'il doit transmettre.

Les principales options à envisager sont :

- Le raccordement à un réseau local, qui peut permettre un routage vers internet si nécessaire. C'est la solution la plus simple quand un accès LAN est disponible et lorsque la technologie de communication est compatible avec la consommation électrique de l'objet.
- L'utilisation d'un réseau de téléphonie mobile (3G/4G/5G) offre un débit important et une faible latence (les données sont transmises à la demande, en temps réel). Elle induit cependant une consommation électrique élevée, et un coût d'abonnement de l'ordre de quelques euros par objet et par mois.
- L'utilisation d'un réseau LPWAN qui permet d'optimiser la consommation électrique et le coût de l'abonnement par objet. Cette option limite toutefois le volume de données échangées, et induit un délai (quelques minutes à quelques heures) entre l'émission des données et leur réception par le serveur.

4. Définir l'architecture de la plateforme d'exploitation

La première chose à définir, concernant la plateforme d'exploitation d'un système IoT, concerne l'infrastructure d'hébergement. Deux options sont envisageables : privilégier un déploiement sur le Cloud, ou installer les serveurs sur une infrastructure interne à l'entreprise (déploiement « On Premise »).

Plusieurs aspects sont à prendre en compte dès le départ : les contraintes liées à la sécurité, et le dimensionnement du système à moyen et long terme.

Concernant la sécurité :

Une solution Cloud, paradoxalement, ne signifie pas forcément « moins de sécurité ». Les systèmes IoT sont caractérisés par le fait d'avoir de nombreux objets communicants déployés sur le terrain, qui communiquent avec le serveur.

Les objets déployés sont susceptibles d'être attaqués ou compromis beaucoup plus facilement qu'un poste informatique installé dans des locaux sécurisés.

Connecter tous ces objets à un serveur situé sur le réseau de l'entreprise représente donc un risque important, et nécessite la mise en place de solutions de cybersécurité complexes (Firewall réseau, Firewall applicatif, DMZ...).

Lorsque la plateforme est déployée sur le Cloud, avec un accès sécurisé du SI interne vers cette plateforme pour consulter ou récupérer les données générées par le système IoT, le risque sur le réseau de l'entreprise est beaucoup moins important. Toutefois, les données spécifiques à la solution IoT sont hébergées chez un tiers.

Concernant le dimensionnement :

Les solutions Cloud offrent une souplesse et une adaptabilité qu'il est quasiment impossible d'obtenir avec une solution « On Premise ». Les infrastructures Cloud permettent de déployer un serveur avec un dimensionnement réduit pour un coût réduit, et le faire évoluer simplement vers de la très haute capacité ; à condition évidemment de définir une architecture interne capable de monter en charge en profitant de la scalabilité horizontale offerte par le Cloud (les traitements sont répartis sur un nombre de ressources qui augmente automatiquement avec la charge).

Plateforme Cloud

Connectée aux objets, isolée du réseau d'entreprise

⊕ scalabilité
⊕ permet de connecter des objets déployés « dans la nature » sans ouvrir une brèche de sécurité sur le réseau interne

⊖ délègue à un tiers une partie de la cybersécurité

Plateforme « On Premise »

⊕ Maîtrise complète de l'infrastructure et des données récupérées

⊖ Nécessite la mise en place d'un canal de communication avec l'extérieur

⊖ Coût et complexité importants pour supporter une forte montée en charge

⊖ Scalabilité complexe à maîtriser

D'autres options technologiques peuvent être envisagées en fonction du contexte, comme le fait de s'appuyer sur des briques technologiques existantes (COTS : Component On The Shelf). De nombreuses « Plateformes IoT » offrent des solutions clé en main de recueil de données et de supervision d'équipements. Il existe également de nombreux composants logiciels qui couvrent certains aspects de la communication, des échanges ou des traitements de données et permettent de simplifier la mise en œuvre d'une nouvelle solution.

Cas d'usages

1. HéroDot : Solution de comptage de flux de passagers
2. Sécuriser des infrastructures sensibles avec Astao IoT
3. L'IoT au service de la maintenance prédictive

1. HéroDot : Solution de comptage de flux de passagers

Le challenge

Mesurer, prévoir et réguler l'affluence de passagers en situation de crise sanitaire ; piloter les flux piétons dans une zone de passage en période de travaux ; réduire le temps d'attente aux stations de taxis en sortie de gare…

Les opérateurs de services de transports ont de plus en plus besoin de connaître le comportement des usagers en mobilité au sein de leurs infrastructures pour garantir leur sécurité, offrir une expérience voyageurs augmentée et optimiser l'exploitation de leurs ressources.

L'usage de Gateways IoT simplifie la conception d'un capteur capable de traiter localement un grand volume de données pour communiquer en temps réel des informations opérationnelles.

La Solution IoT

Pour répondre à ces enjeux, il a fallu développer une solution de comptage et d'analyse de flux de personnes déployable sur des engins roulants, dans des bâtiments ou encore capable d'être exploitée de manière légère et autonome en énergie.

Basée sur l'analyse des traces WiFi environnantes, cette solution permet la visualisation temps réel et géoréférencée de la fréquentation sur un parcours défini ou sur un site et apporte l'analyse du comportement d'un flux de personnes (Origine/Destination et Temps d'attente et/ou de parcours).

Les principales contraintes :

- **L'objet** doit être capable de compter de manière fine le nombre de personnes dans une zone définie et d'en analyser les comportements.

  Sa conception doit être adaptée aux différents usages et lieux (norme matériels roulants, alimentation externe ou batteries) auxquels la solution est destinée.

- **Les données** recueillies ont une volumétrie variable et potentiellement très importante en période de pic de trafic.

  D'autre part, ces données doivent permettre d'isoler les individus étudiés pour pouvoir en analyser les comportements. Elles revêtent donc un caractère personnel et leur exploitation est soumise à la réglementation en vigueur.

  Afin d'anonymiser les données recueillies et d'en réduire **le volume à transmettre par l'objet**, un pré-traitement doit être opéré au niveau de l'objet.

- Une fois pré-traitées, les données n'ont plus aucun caractère critique et **leur exploitation** ne requiert plus que des mesures de sécurité « standards ».

Caractéristiques clés :

- Hardware adapté aux matériels mobiles
- Edge Computing pour garantir l'anonymisation des données recueillies et limiter le volume de données à envoyer
- Protocole de communication 3G/4G
- Plateforme Cloud
- Remontée d'information temps réel 24/7

2. Sécuriser des infrastructures sensibles avec Astao IoT

Le challenge

Le vol d'équipements au sein d'infrastructures sensibles nécessite la mise en place d'une solution de bout en bout couvrant à la fois la détection des incidents, leur caractérisation en tant que « vol confirmé », la mobilisation des équipes d'intervention, et la mise à disposition des informations et outils leur permettant de réagir efficacement.

Avec l'IoT et l'apparition d'objets communicants autonomes, il devient très simple d'intégrer à des équipements existants la fonctionnalité de traçage GPS et d'alerting.

La Solution IoT

ASTAO IoT est une solution de sécurisation des matériels et infrastructures sensibles capable d'offrir une couverture fonctionnelle complète :

- Un traceur capable de détecter une mise en mouvement, de géolocaliser l'objet, et de communiquer toutes les informations pertinentes vers une plateforme opérationnelle.
- La plateforme de gestion des Alertes : un serveur chargé de réceptionner et analyser les messages envoyés par les traceurs, et de déclencher des alertes vers les équipes de télésurveillance.
- Le centre de télésurveillance : ce service, assuré 24h/24 et 7j/7, assure le traitement des alertes, pour réaliser une levée de doute et si nécessaire la mobilisation des équipes d'intervention lorsqu'une alerte est déclenchée.

Les principales contraintes :

- L'objet (traceur) doit pouvoir être fixé sur les matériels à risque, être robuste et autonome en énergie. De plus, ce type de traceurs doit être déployable à grande échelle.
- Les données de géolocalisation recueillies doivent être disponibles 24h/24 et 7j/7 quelle que soit leur position géographique.
- La plateforme d'exploitation doit disposer de canaux de notification efficaces pour garantir une réaction rapide en cas d'incident (mail, sms, appel vocal...). Elle doit également être interopérable avec le système d'information de l'entreprise afin de fournir un accès aux alertes et à l'information associée permettant de réaliser les opérations de levée de doute, et de guider les équipes d'intervention.

Caractéristiques clés :

- Traceurs robustes et frugaux en énergie
- Couverture réseau étendue et consommation minimale grâce aux réseaux Sigfox et Lora
- Plateforme Cloud permettant d'offrir le service en mode SaaS

3. L'IoT au service de la maintenance prédictive

Le challenge

Toute machine est soumise à des risques de panne pouvant conduire à une perte de productivité voire, pour les équipements les plus critiques, à des accidents graves. La maintenance des infrastructures est donc un élément essentiel des processus industriels et représente un poste de coût important.

Les solutions IoT permettent aux équipements industriels d'être connectés en permanence à des plateformes de maintenance chez l'exploitant ou le fabricant. Données d'usage, défauts et pannes peuvent être traités en temps réel et analysés par des algorithmes de maintenance prédictive.

La Solution IoT

Prédire les risques de panne et agir au plus vite en cas de risque de dysfonctionnement permet de réduire la fréquence des défaillances et d'organiser les opérations de maintenance de manière plus efficiente.

La solution développée assure la collecte et le traitement intelligent de données provenant d'équipements IoT situés sur des zones étendues afin de mettre en place un process de maintenance prédictive.

Elle est capable de gérer l'acquisition et le transfert de mesures provenant de multiples capteurs situés sur des infrastructures sensibles. Grâce à un algorithme de machine learning, elle analyse les historiques et détecte les signaux incohérents révélateurs de risques de dysfonctionnement, avant de déclencher des actions de maintenance préventive.

Les principales contraintes :

- **L'objet** à surveiller est en général un équipement déjà intégré à un réseau local. Il faut pouvoir extraire des mesures et les envoyer vers une plateforme dédiée à la maintenance, qui peut se trouver sur le même réseau local ou être accessible via internet.
- Lorsque la supervision est mise en place par un constructeur, sur des systèmes déployés dans des contextes clients, **la solution de communication** doit pouvoir s'adapter à de nombreux contextes différents.

Caractéristiques clés :

- Ce type de solution peut souvent s'appuyer sur des Gateways IoT qui viennent se connecter localement au système à superviser, et prennent en charge l'envoi des données vers la plateforme de maintenance.
- Le fait de déployer un système communicant chez un client impose d'apporter des garanties très fortes sur tous les aspects de cybersécurité.
- La communication peut s'appuyer dans la plupart des cas sur une infrastructure de réseau local, qui offre un routage vers internet.

LEXIQUE

COTS (*Component On The Shelf*) : solution clé en main de développement de logiciel qui répond aux besoins de plusieurs clients en termes de recueil de données et de supervision d'équipement.

CPU (*Central Processing Unit*) : unité centrale de traitement en charge des opérations de manipulation des données dans un système informatique.

Data management : ensemble des processus déployés pour collecter, structurer, gérer et utiliser les données. Il englobe également la manière dont les données vont être intégrées au système d'information de l'organisation.

Device management : prise en compte des contraintes liées à la gestion des objets, telles que la supervision de leur fonctionnement et la mise à jour logiciel.

Edge Computing : traitement des données au plus proche du capteur plutôt que sur un serveur centralisé ou dans le cloud.

Gateway : dispositif permettant le relais entre un réseau de capteurs et la plateforme d'exploitation. Il est connecté aux capteurs par une solution de communication locale. La Gateway est capable d'héberger des traitements, et dispose d'une solution de communication vers le serveur.

IoT (*Internet of Things*) : Internet des objets.

LAN (*Local Area Network*) : réseau local permettant à des machines de communiquer entre elles en utilisant des connexions filaires (Ethernet) ou des technologies Radio de proximité (WIFI).

LPWAN (*Low Power Wide Area Network*) : nouvelles solutions de communication, regroupées sous l'acronyme de LPWAN, dont font partie par exemple les technologies SigFox et LoRa. Elles contribuent à l'apparition d'objets connectés à faible coût, avec une consommation électrique suffisamment faible pour permettre un fonctionnement sur batterie pendant plusieurs années.

Machine Learning : concept d'Intelligence Artificielle où une machine est capable d'apprendre par elle-même et de se corriger.

Machine-to-Machine (*M2M*) : concept, créé en 1968, permettant la communication entre machines sans intervention de l'Homme.

Maintenance prédictive : maintenance réalisée par anticipation, grâce à des capteurs connectés qui peuvent détecter en temps réel une anomalie de fonctionnement ou une usure prématurée.

Plateforme Cloud : Plateforme hébergée dans un datacenter, en utilisant des technologies de virtualisation permettant de déléguer totalement la gestion des ressources matérielles physiques.

Plateforme « On Premise » : plateforme hébergée sur un serveur local.

PLC (*Programmable Logic Controller*) : contrôleur logique programmable utilisé dans l'industrie permettant d'automatiser les processus électromécaniques.

Scalabilité horizontale : capacité de l'architecture à évoluer en cas de montée en charge en ajoutant des serveurs d'un type donné.

Pour en savoir plus sur la mise en place de solutions IoT, contactez-nous :

contact@itlink.fr

www.itlink.fr