The Positive Way

WAVESTONE

CYCLE DE VIE DES OBJETS CONNECTÉS :

QUEL IMPACT SUR LA VIABILITÉ D'UN PROJET IOT ?

De nombreuses entreprises considèrent aujourd'hui l'*Internet of Things* (IoT) comme un vecteur de transformation, pour créer de nouvelles offres, accroître l'excellence opérationnelle, ou encore répondre à de nouvelles réglementations. Mais l'industrialisation et le passage à l'échelle des projets IoT, pouvant aller jusqu'à plusieurs millions d'objets connectés, induisent la nécessité d'anticiper la gestion du cycle de vie des objets connectés pour garantir la pérennité des solutions mises en place. Le maintien en conditions opérationnelles et en conditions de sécurité s'avère d'autant plus complexe que les volumes et la diversité d'objets connectés sont élevés, car tous les scénarios peuvent se produire dès l'instant où l'on considère des flottes de millions d'objets connectés.

Pour réussir l'industrialisation de leurs projets IoT, les entreprises doivent se poser les bonnes questions. Quelles sont les étapes du cycle de vie des objets connectés ? Quels impacts ont-elles sur l'ensemble d'un projet IoT ? Quelles sont les équipes concernées ? Quel est le niveau d'intégration avec le SI existant et plus largement avec l'écosystème du projet ? Cette publication vise à donner les clés d'un passage à l'échelle réussi.

CONTACTS

Alice MORIZE
alice.morize@wavestone.com

Romain POINTEREAU
romain.pointereau@wavestone.com

Cette publication a été réalisée avec l'appui de Maximilien Bouilly, Julia Franco, Taha-Mahmoud Gaidi, Maxime Gérard, Kévin Guerin et Benoit Tanguy.

Quelques définitions

- Un **capteur** est un instrument de mesure qui peut communiquer les données relevées grâce à un réseau de connectivité. Dans cette publication, le terme capteur peut faire référence à un simple capteur, à un système composé d'une passerelle et de plusieurs capteurs ou à un système plus complexe avec des capacités de *Edge computing*.
- Un objet est connecté lorsqu'il est équipé d'un capteur communicant. Un **objet connecté** désigne donc l'ensemble du capteur et de l'équipement ou environnement auquel il est associé.
- L'**IoT** correspond à un ensemble d'objets connectés qui peuvent communiquer avec une plateforme IoT[2].

OBJETS CONNECTÉS : UN CYCLE DE VIE PONCTUÉ DE NOMBREUSES ÉTAPES

Différentes étapes ponctuent le cycle de vie des objets connectés, et concernent à la fois le parcours physique de l'objet connecté et le parcours logique des informations qui le caractérisent. Il convient d'anticiper ces étapes dans leur globalité dès la phase de cadrage du projet IoT pour en garantir la viabilité économique, opérationnelle et le maintien en conditions de sécurité[1].

Étapes caractéristiques du cycle de vie des objets connectés

Prototypage

Le capteur est conçu en fonction des besoins et des contraintes métiers. Les choix technologiques doivent prendre en compte la criticité de l'usage final et les enjeux du cycle de vie.

Fabrication

Le capteur est produit en série. À sa sortie d'usine, le capteur est fonctionnel mais n'est pas encore connecté. Il est indispensable de définir au préalable un contrôle qualité de bout-en-bout, et ce aussi bien sur l'objet physique que sur ses attributs digitaux.

Provisioning

L'identité du capteur est créée dans la plateforme IoT. Elle comprend ses caractéristiques, un identifiant unique et d'éventuelles données secrètes telles que des certificats ou des clés cryptographiques.

Installation

Le capteur est physiquement installé dans son environnement. Selon les cas d'usage, il peut par exemple s'agir d'un bâtiment, d'un réseau électrique, d'un véhicule, ou encore d'un équipement que l'on souhaite géolocaliser.

Début de vie

Revente ou changement d'utilisateur

Dans le cas d'une revente ou d'un changement d'utilisateur, la complexité est de cadrer la revente pour permettre au nouveau propriétaire de l'objet connecté d'être également propriétaire du service associé. D'une entreprise à l'autre, les réponses apportées à cette problématique diffèrent. Dans certains cas, la revente est interdite, dans d'autres elle se base sur les déclarations des utilisateurs ou sur la détection d'évènements spécifiques.

Changement d'objet associé au capteur

Un changement d'objet associé au capteur implique de désinstaller physiquement le capteur et de le réinstaller. Un choix s'impose entre deux processus logiques : un décommissionnement suivi d'un nouveau provisioning, ou une simple mise à jour de l'appairage en gardant l'identifiant unique. Cette deuxième option permet une meilleure traçabilité.

Fin de vie & recyclage

Recyclage

Enfin, le recyclage des capteurs est une pratique émergente. Depuis 2005, une norme impose à tous les fabricants de DEEE (Déchets d'Équipements Électriques et Électroniques) professionnels de prendre en charge ou de déléguer leur récupération. Pour autant, cette pratique reste marginale pour les capteurs IoT et les éco-participations ne sont pas encore généralisées.

Désinstallation

Le capteur est physiquement désinstallé de son environnement. La protection des données et des éventuels secrets industriels que contient le capteur est alors essentielle pour prévenir le risque de perte ou de fuite d'informations.

Révocation

En complément du décommissionnement, les droits et associations liés au capteur doivent être révoqués. Elle correspond à la suppression de l'appairage.

1- Plateformes IoT : la clé de voûte d'une stratégie IoT réussie : https://www.wavestone.com/app/uploads/2019/04/Plateformes_IoT.pdf

2- Une approche par le cycle de vie pour la sécurité de l'IoT : https://www.riskinsight-wavestone.com/2019/09/cycle-vie-securite-iot/

Étapes relatives au parcours physique de l'objet connecté

Étapes logiques relatives à l'information associée à l'objet connecté

Appairage

Il correspond à l'association entre le capteur et l'objet auquel il est lié et à la nomination du responsable. Cette étape permet de savoir que la donnée reçue caractérise un objet en particulier.

Enrôlement

L'objet est dorénavant connecté et peut communiquer avec la plateforme IoT. Il est nécessaire de s'assurer que le capteur qui requiert une connexion est légitime.

Supervision

La plateforme IoT doit permettre un suivi des états de l'objet connecté. Il peut s'agir de son état de fonctionnement, son niveau de batterie, sa configuration, ou encore sa version.

Alertes

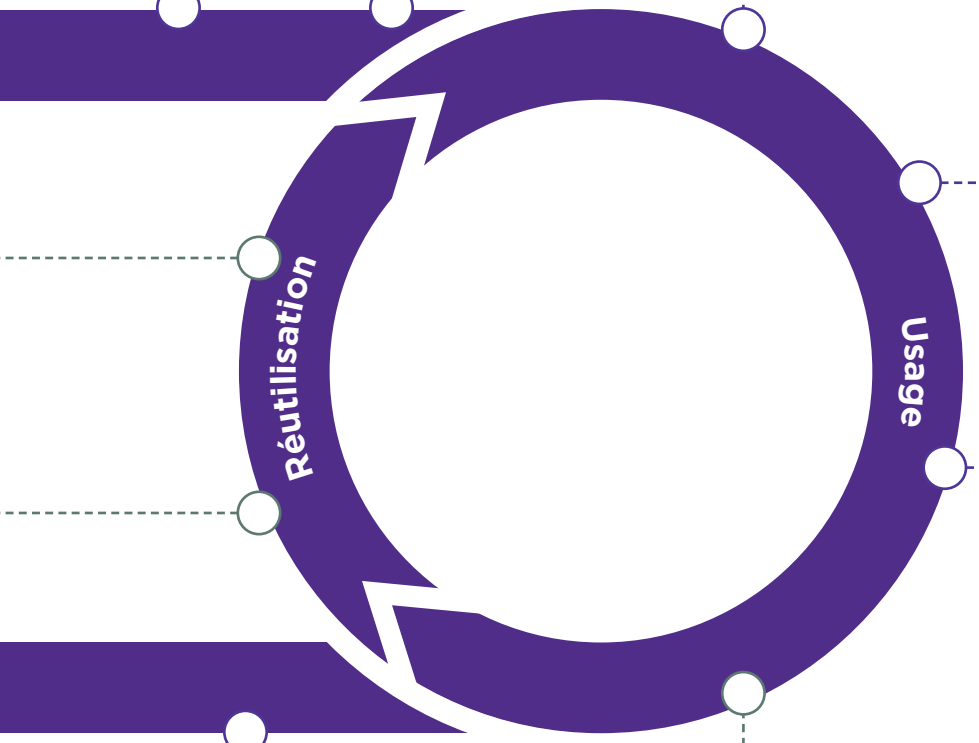
La remontée d'alertes est à paramétrer selon les évènements à risque que l'on souhaite détecter, comme l'émission de données erronées.

Mises à jour Over The Air

Cette fonctionnalité communément appelée OTA permet de mettre à jour à distance les objets connectés sans fil. Elle est un levier important et complexe de la gestion du cycle de vie des objets connectés[3].

Opérations de maintenance

La détection du dysfonctionnement d'un capteur engendre une opération de maintenance. Elle peut impliquer une intervention physique, par exemple la réparation ou le remplacement d'un composant, ou une intervention à distance, comme par exemple la recalibration OTA d'un capteur.



Décommissionnement

Il correspond à la désactivation sur la plateforme du caractère connecté de l'objet, de façon à enregistrer la fin de son utilisation.

3- Cette fonctionnalité est détaillée dans l'encart « L'œil de l'expert sur l'OTA » (pages 6 et 7).

L'INTÉGRATION DES ÉCOSYSTÈMES, UN LEVIER POUR UNE GESTION RÉUSSIE DU CYCLE DE VIE

En complément de la définition du cycle de vie des objets connectés, il est nécessaire d'identifier les parties prenantes. À titre d'exemple, les acteurs suivants peuvent jouer un rôle essentiel :

- **Les fabricants de capteurs** sont les premiers détenteurs des informations relatives aux capteurs, telles que leur identité ou leurs caractéristiques ;
- **Les équipes logistiques** assurent la gestion des stocks de capteurs, depuis leur approvisionnement jusqu'à leur envoi vers les responsables de l'installation ou vers les utilisateurs finaux eux-mêmes ;
- **Les équipes terrain** sont responsables des opérations physiques à appliquer aux objets connectés, comme leur installation, leur maintenance ou leur désinstallation ;
- **Les équipes en charge de la plateforme IoT** sont notamment en charge des actions logiques telles que l'appairage, le provisioning, ou encore les mises à jour.

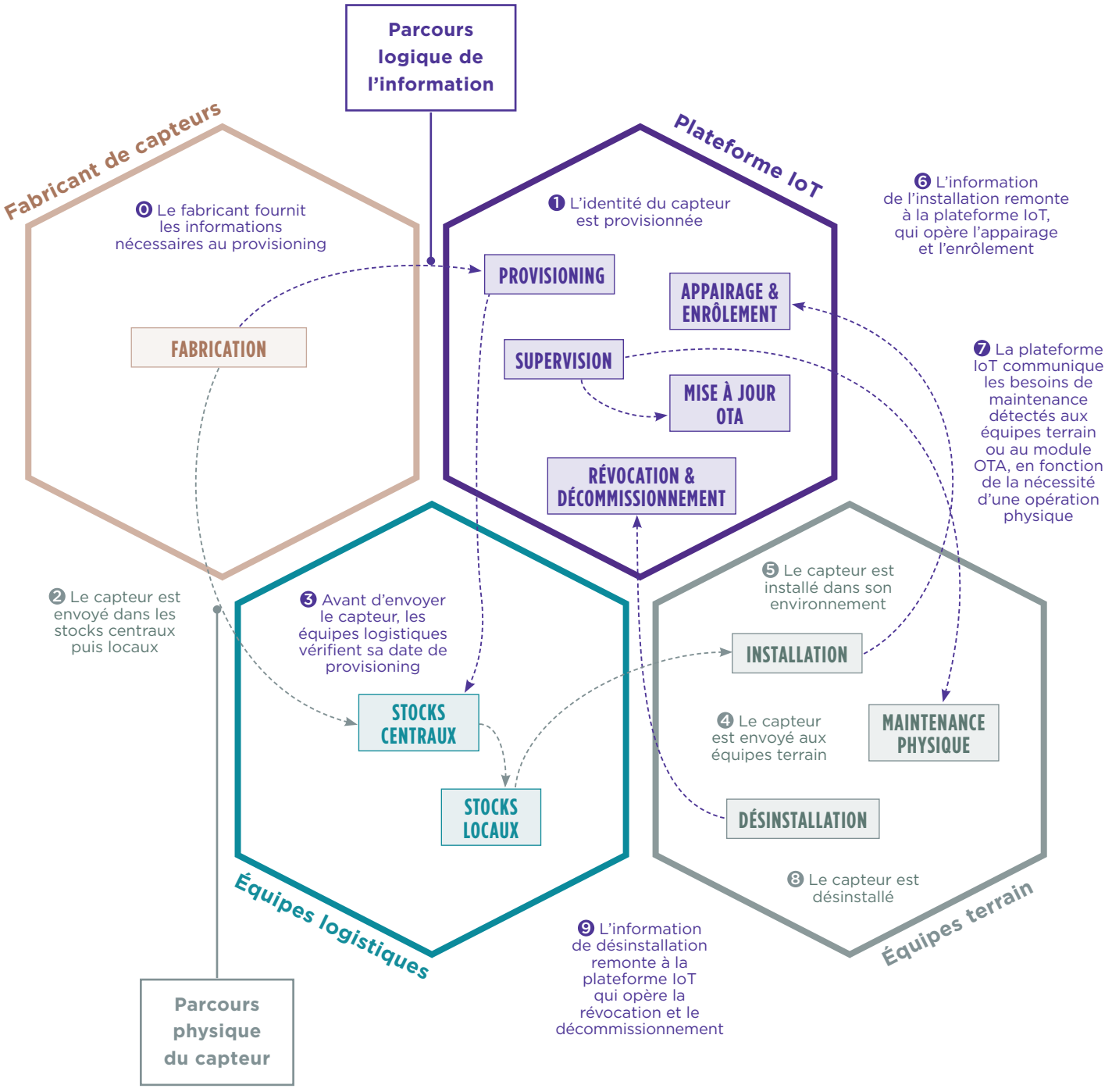
La gestion d'ensemble du cycle de vie des objets connectés requiert donc la consolidation des informations détenues par chacune des parties prenantes.

Il est essentiel de formaliser **les contributions et les interactions attendues de la part de chacun** des acteurs sur les étapes physiques ou logiques du cycle de vie.

À titre d'exemple, un processus clé à sécuriser est la synchronisation entre la réception physique du capteur et la réception des données qui composent son jumeau numérique. Il convient d'appliquer les mêmes engagements pour la livraison des données numériques que pour la livraison physique. La même recommandation s'applique pour le support et la maintenance.

Un modèle de répartition possible est proposé en page suivante.

Contribution des équipes au cours du cycle de vie de l'objet connecté



Une fois ces contributions définies, l'intégration des différents écosystèmes associés à ces équipes est nécessaire.

Les équipes impliquées pouvant évoluer, par exemple en cas de changement de fournisseur ou d'évolution du périmètre, il est nécessaire d'adopter **une manière standard d'intégrer ces nouveaux composants**. De la mise en place d'une architecture modulaire composée de micro-services indépendants, jusqu'à l'exposition des services au travers d'API, ou encore à l'utilisation de protocoles ouverts, une architecture évolutive doit être pensée.

En parallèle, pour assurer la cohérence des informations, il est recommandé de mettre en place **un référentiel unique des objets connectés et de leurs statuts**. Ce référentiel doit être alimenté par les référentiels métiers des objets et par les statuts que possède chaque équipe précédemment citée. Il peut se matérialiser par une ou plusieurs bases de données : c'est le portail d'accès aux informations qui se doit d'être unique. La nomination d'un responsable du référentiel des objets connectés est requise pour garantir la cohérence d'ensemble.

Enfin, certaines entreprises font le choix de **stocker tout ou une partie de l'historique des statuts pour alimenter des fiches de vie des objets connectés**. Si une telle pratique améliore la traçabilité, ses bénéfices sont à évaluer au cas par cas, en fonction de la pertinence des statuts à garder et du délai associé.

L'ŒIL DE L'EXPERT SUR *LES UPDATES OVER THE AIR* (OTA)

L'OTA permet d'effectuer des actions à distance sur un objet connecté et peut être décliné en trois catégories, de la plus basique à la plus complexe :

- **Le COTA** (*Configuration Over The Air*) permet de modifier le paramétrage des objets connectés, comme leur fréquence de connexion ou leur plage nominale de valeurs ;
- **Le SOTA** (*Software upgrade Over The Air*) permet de mettre à jour les couches hautes du logiciel de l'objet connecté, comme des applications ;
- **Le FOTA** (*Firmware upgrade Over The Air*) permet de mettre à jour les couches basses du logiciel de l'objet connecté, comme un système d'exploitation.

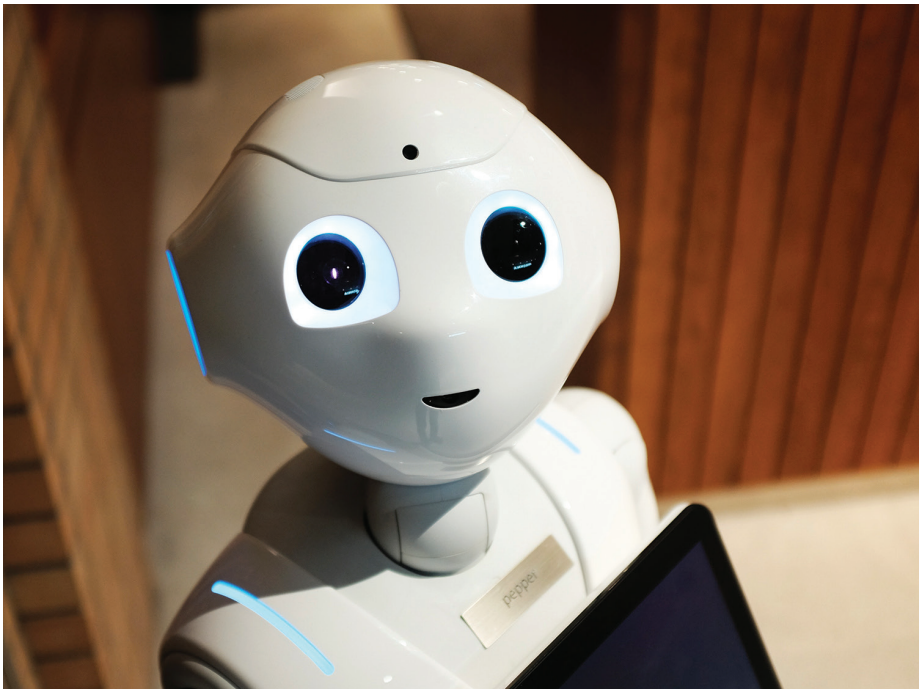
Des bénéfices à plusieurs niveaux sont attendus de l'OTA

Entre la fabrication d'un capteur et son premier usage, il peut s'écouler une durée importante. Il est pertinent dans ce cas d'utiliser l'OTA pour le **mettre à jour avec la dernière version disponible**, et ainsi éviter un reconditionnement avant sa mise en service. Cette flexibilité permet de commander des volumes importants et facilite donc la scalabilité.

L'OTA permet également de **fixer les défauts logiciels des objets connectés** déjà déployés, en évitant les options coûteuses comme le rappel de masse ou les interventions manuelles via un opérateur.

Par ailleurs, de nombreux objets connectés présentent des failles de cybersécurité dans leur couche logicielle, comme par exemple des mots de passe trop faibles ou l'absence de protocole de chiffrement des données. La surface d'exposition au risque est donc considérable pour les entreprises qui souhaitent multiplier leur volume. L'intégration d'une capacité de mise à jour SOTA ou FOTA dès la conception de l'objet connecté est fortement recommandée pour soutenir **son maintien en condition de sécurité**.

Enfin, une **réduction notable du *time-to-market*** est rendue possible par l'OTA. Dans ce cas, ce sont les mises à jour OTA qui serviront ultérieurement à enrichir l'aspect logiciel de l'objet connecté.



L'OTA n'en demeure pas moins une solution complexe qui soulève des questions spécifiques

Le premier dilemme concernant l'OTA est la stratégie de mise à jour. Pour ne pas devoir gérer une diversité de capteurs et de versions et pour accroître la cybersécurité, **une politique de mise à jour systématique vers la dernière version disponible** peut être envisagée. Cette stratégie nécessite toutefois une fréquence élevée de mises à jour sur des volumes importants. Il est donc nécessaire de concevoir une infrastructure OTA adaptée et d'en assumer les coûts.

Les **limitations physiques liées au *hardware*** doivent aussi être prises en compte. Par exemple, la mémoire RAM ou la CPU étant limitées, le capteur doit être dimensionné en anticipant au mieux les futures mises à jour.

Le **choix d'une plateforme OTA** est également déterminant. Elle peut être distincte de la plateforme IoT. Elle doit être sélectionnée en vérifiant sa compatibilité avec les SI existants, les objets connectés et la plateforme IoT lorsque c'est applicable.

Par ailleurs, selon les cas d'usage, une **mise à jour incrémentale ou totale** peut être retenue. Si la mise à jour incrémentale est plus rapide et moins onéreuse compte tenu de sa taille limitée, elle est également plus complexe à mettre en place lorsque des versions multiples coexistent dans le parc. Une mise à jour totale présente également des risques en cas de dysfonctionnement de la nouvelle version si la précédente n'est pas conservée après installation.

Le choix du moment de l'installation du nouveau package doit également être réfléchi en fonction du cas d'usage et de l'impact d'une interruption de service. Le lancement de l'installation peut se faire lors de la phase d'extinction de l'appareil, comme c'est le cas pour les véhicules connectés et pour les PC, mais peut aussi se faire par action humaine, comme pour les smartphones.

Enfin, **l'interaction entre la plateforme OTA et l'objet connecté** doit être sécurisée de bout en bout pour éviter les attaques de type *man-in-the-middle*, DoS, DDoS ou package pirate.

En conséquence, pour ne pas faire de l'OTA une source de vulnérabilité, **le processus de mise à jour doit faire l'objet d'une attention particulière** et être étudié dès le cadrage d'un projet IoT.

De manière générale, le taux de réussite de l'OTA est maximisé par l'anticipation des cas particuliers sous-jacents à la diversité des situations. Pour autant, il reste utopique d'anticiper l'intégralité des scénarios possibles. **L'OTA ne dispense pas de prévoir des actions correctives de proximité.** Il ne faut pas opposer ces deux moyens, ils doivent pouvoir cohabiter de façon asynchrone. Cela implique d'investir d'une part dans une solution OTA robuste avec l'ambition de couvrir un maximum de cas, et d'autre part dans un accès local et sécurisé au capteur. Le retour sur investissement découlera de la réduction des coûts de maintien en conditions opérationnelles et de sécurité.

Sur le marché, des fournisseurs spécifiques de solutions OTA se démarquent

En observant les écosystèmes IoT des grands comptes, il apparait que les fonctionnalités de COTA sont souvent portées par la plateforme IoT, alors que les fonctionnalités de SOTA et de FOTA, plus complexes, sont souvent portées par des plateformes OTA distinctes fournies par des acteurs spécialisés.

Ainsi, **les principaux fournisseurs de COTA demeurent les éditeurs de plateformes IoT** fréquemment utilisées par les grands comptes, comme Azure IoT ou AWS IoT par exemple, ce qui rend les solutions COTA relativement standards.

À l'inverse, **ce sont des acteurs spécifiques qui proposent l'essentiel des technologies SOTA et FOTA**. Ces solutions de mises à jour à distance sont plus complexes à implémenter car elles dépendent de l'objet connecté choisi. En effet, elles consistent à mettre en place un agent de la plateforme OTA dans l'objet connecté. Le rôle de cet agent est de gérer l'interaction avec la plateforme et l'installation du *software* ou du *firmware*, à la fois au niveau de l'objet connecté et de la plateforme OTA. Cette forte dépendance avec la solution embarquée explique que des acteurs verticaux et spécialisés se démarquent. On retrouve notamment Airbiquity ou Uptane spécialisés dans le secteur de l'automobile, l'industriel Bosch, Redbend issu du monde de la téléphonie ou encore des solutions open sources telles que HawkBit et Mender. Cette dépendance entre l'objet connecté et la plateforme OTA a une conséquence sur la réversibilité quant à la plateforme choisie.

CONCLUSION

Ainsi, chacune des étapes du cycle de vie des objets connectés conditionne la viabilité des solutions IoT. Il est donc primordial d'anticiper l'intégralité de ce cycle dès la phase de cadrage, jusqu'à collaborer étroitement avec les fabricants de capteurs pour garantir la prise en compte de tous ces enjeux lors de leur conception.

Pour garantir le succès de cette gestion d'ensemble, l'adoption de référentiels communs, la définition de règles de gouvernance et le choix de méthodes d'intégration des systèmes d'informations ouvertes et évolutives sont à privilégier.

La réussite passe également par une collaboration aussi anticipée que possible entre les métiers et les DSI. Elle évite aux projets IoT d'être rattrapés au moment du passage à l'échelle par des sujets qui nécessitent l'expertise de la DSI. Les entreprises se doivent de définir des modèles organisationnels autour de l'IoT adaptés à leurs ambitions.

Le focus OTA est une illustration des solutions technologiques qui peuvent renforcer la gestion du cycle de vie des objets connectés. L'OTA est un gain considérable pour le maintien en conditions opérationnelles et de sécurité, dès lors que les mises à jour peuvent avoir lieu de façon industrielle et planifiée. Ce serait une erreur de ne pas considérer l'OTA comme un prérequis à la validation d'une solution IoT qui ambitionne un passage à l'échelle.

Il existe d'autres solutions technologiques, à l'instar du jumeau numérique, qui promet par exemple de faciliter la gestion à grande échelle des aspects plus complexes du cycle de vie, comme les simulations lors du prototypage des capteurs ou encore la maintenance prédictive. Autant de sujets qui seront au cœur des préoccupations des projets IoT ces cinq prochaines années.