les défis de la commercialisation des **solutions IdO**

Problématiques de sécurité, d'évolutivité et de concurrence

Figure 1. La Commission européenne a examiné si les grands acteurs du secteur des assistants vocaux, interface utilisateur préférée des maisons intelligentes, étouffaient la concurrence. (Source : ShutterStock/Gorodenkoff)

Stuart Cording (Elektor)

L'Internet des objets (IdO) existe depuis plus de 20 ans, et une multitude de technologies sans fil ont émergé pour favoriser son déploiement. À la maison, les assistants vocaux sont devenus la principale interface utilisateur de nombreux appareils intelligents. Malgré ces progrès, plus d'un tiers des projets IdO ne dépassent jamais la phase de démonstration de la faisabilité. En outre, la Commission européenne craint que l'absence de concurrence dans certains espaces d'application n'empêche l'entrée sur le marché des entreprises de l'UE. Alors, quels sont les véritables défis, et comment se déroule le déploiement d'une solution IdO en Europe ?

Si vous souhaitez vous familiariser avec les technologies de l'Internet des objets (IdO), vous pouvez trouver facilement un grand nombre de projets adaptés. Il suffit de rechercher « IdO » avec votre plateforme de prototypage préférée, et vous serez submergé par des pages de projets, de plateformes en cloud, de comparaisons technologiques et de listes d'idées. Elektor est également une excellente source d'informations. Depuis que le terme IdO a été introduit il y a plus de 20 ans, notre site web a rassemblé plus de 600 articles sur l'IdO ou liés à ce sujet [1].

Cependant, il existe un fossé entre la démonstration du concept de base d'une solution IdO à l'aide d'une plateforme prototype et le déploiement d'une version réelle. Le rapport *IoT Insights* de Microsoft [2] est basé sur des entretiens avec plus de 3 000 professionnels de l'IdO en 2021. Ils ont constaté que 35 % des projets IdO connaissaient un échec pendant la phase d'essai ou de démonstration de faisabilité, soit une augmentation de 5 % par rapport à l'enquête réalisée un an plus tôt. Le coût élevé de la mise à l'échelle (déploiement) est la raison la plus citée pour expliquer l'échec à ce stade. Parmi les autres causes, figurent le grand nombre de plateformes à tester, la multitude de cas d'utilisation à étudier et le manque de ressources. Une autre étude réalisée par Cisco [3] a révélé que seulement 26 % des entreprises participantes pensaient que leurs initiatives IdO avaient été couronnées de succès. Les réponses à cette étude ont montré que, même si la plupart des projets IdO semblent bien conçus sur le papier, ils s'avèrent plus complexes que prévu dans la pratique.
En dépit de ces impressions négatives sur l'IdO, il existe des secteurs où cette infrastructure fait d'énormes progrès et génère des revenus croissants.

La Commission européenne examine le secteur de l'IdO grand public

Les citoyens de l'UE ont accueilli favorablement les solutions IdO grand public proposées ces dernières années. À tel point qu'un rapport sur le marché des maisons intelligentes publié par Statista [4] prévoit que le chiffre d'affaires associé doublera, passant d'environ 17 milliards d'euros en 2020 à environ 38,1 milliards d'euros en 2025. Préoccupée par le fait que la concurrence dans ce secteur pourrait être étouffée, la Commission européenne a réalisé une enquête dans le cadre de sa stratégie numérique [5]. Le rapport, publié en janvier 2022, a recueilli les contributions des fabricants de technologies portables, d'appareils grand public connectés utilisés dans la maison intelligente et de ceux qui fournissent des services par le biais de ces appareils intelligents. En outre, la Commission a demandé la contribution d'organismes de normalisation. Cependant, on constate à la lecture que de nombreux points de leur analyse sont consacrés aux assistants vocaux (*voice assistants* - VA) qui constituent l'interface utilisateur de nombreux produits et services IdO (**figure 1**).
Après avoir analysé le paysage de la maison intelligente, le rapport montre clairement qu'en Europe, Google Assistant de Google, Alexa d'Amazon et Siri d'Apple sont les principaux assistants vocaux polyvalents. D'autres sont disponibles, mais ils ont tendance à disposer de fonctionnalités plus limitées et à se concentrer sur la prise en charge d'un seul produit ou de l'application d'un fournisseur de services. Selon ZDNet, parmi les solutions des trois grands groupes, c'est Amazon qui offre le plus haut niveau de compatibilité, en prenant en charge environ 7 400 marques [7]. En comparaison avec Google qui en reconnaît environ 1 000, Apple reste le plus exclusif avec une cinquantaine de marques.

Si l'on examine le paysage de l'IdO, il est clair que les opportunités commerciales s'offrent à vous, et ce, qu'il s'agisse de solutions pour les consommateurs ou à l'industrie.

Peu de place pour les nouveaux venus dans le domaine des assistants vocaux

Avec de tels acteurs industriels puissants et déjà présents sur le marché, il y a peu de place pour les nouveaux venus, et la courbe technologique pour développer un VA compétitif est importante. Ainsi, si vous voulez tirer parti du contrôle vocal pour votre solution IdO, vous devez jouer selon les règles établies par les trois géants. Une approche alternative serait d'accorder une licence à un VA. Cependant, certains fabricants ont signalé que les conditions d'octroi des licences restreignaient leurs choix. Ces limitations pouvaient aller de l'exclusivité ou de restrictions empêchant l'utilisation simultanée de plusieurs VA jusqu'à des licences imposant l'intégration d'autres types de logiciels ou d'applications, ce qui signifie que la technologie VA ne peut pas être utilisée de manière autonome.
Une autre grande préoccupation est l'accès aux données. En tant que tiers recourant à un VA, vous n'avez qu'un accès limité aux données collectées. Le fournisseur de VA a accès aux enregistrements audio et sait également combien de tentatives ont échoué pour exécuter les commandes sélectionnées pour votre appareil. Cependant, votre équipe n'aura pas cet accès, et il vous faudra plus probablement attendre les retours des utilisateurs pour découvrir que votre choix de commandes vocales est sous-optimal par rapport au groupe plus expansif que celui utilisé pour les tests. En outre, comme le fournisseur de VA peut analyser tout ce qui est dit, il pourrait éventuellement utiliser ces données pour développer une solution concurrente à la vôtre ou tirer parti de l'expérience des utilisateurs fournie par votre solution IdO pour améliorer ses propres services.
Un autre problème se pose lorsque le fournisseur de VA propose également des services de publicité. En théorie, les données vocales fournies par vos utilisateurs pourraient aider le fournisseur à améliorer le ciblage de la publicité en fonction de la population représentée par votre base de clients. Enfin, il y a la diminution de la reconnaissance de la marque et de l'expérience. Votre solution soigneusement élaborée est à la merci des VA. Toute modification importante, telle que la voix utilisée, le mot d'appel ou même le déploiement de fonctions entraînant une baisse du nombre d'utilisateurs et aura inévitablement des conséquences pour vous.
Le rapport examine également de nombreux autres domaines pertinents, notamment les interfaces de programmation d'applications (API), les normes, l'interopérabilité, le déséquilibre de puissance entre de nombreux développeurs tiers de dispositifs IdO et les grands fournisseurs de services de plateforme en cloud, ainsi que les clauses de résiliation de contrat.
Le rapport ne contient aucune recommandation. Toutefois, les conclusions précisent que le contenu du rapport contribuera à la stratégie de normalisation de la Commission et enrichira le débat de la législation sur les marchés numériques (DMA).

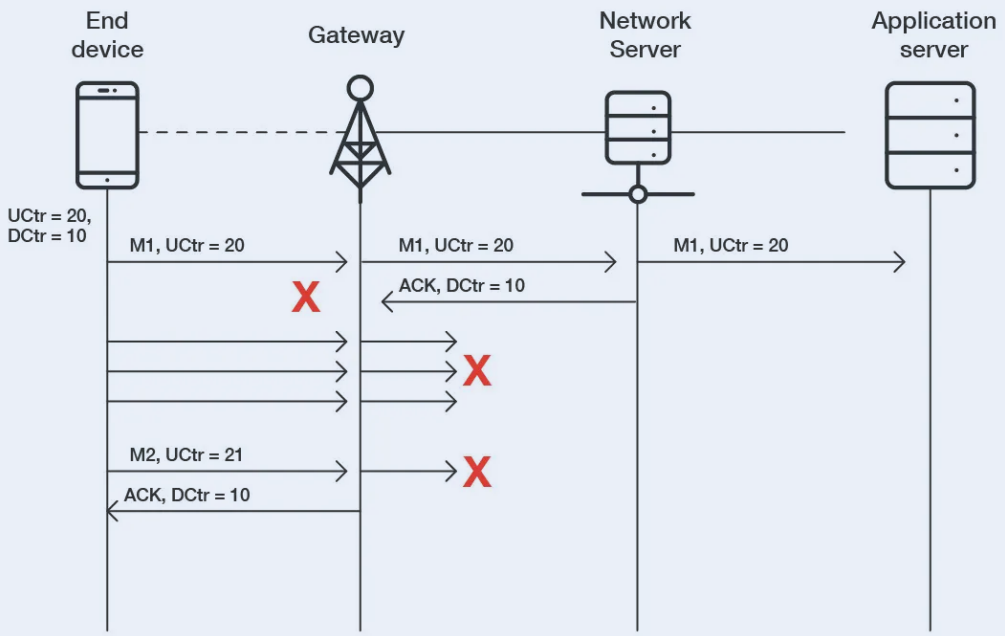

Figure 2. Les chercheurs ont découvert une attaque par déni de service (DoS) dans LoRa 1.0. En répétant un précédent transfert de données réussi, un nœud LoRaWAN est empêché d'envoyer d'autres paquets de données. (Source : Trend Micro)

Les préoccupations en matière de sécurité inquiètent les concepteurs de solutions IdO

À l'examen des données recueillies dans le rapport *IoT Insights* de Microsoft, on constate que la sécurité de l'IdO est en tête de la liste des préoccupations, notamment pour ceux qui envisagent des solutions IdO. 29 % d'entre eux ont indiqué que les risques de sécurité associés les empêchaient d'utiliser davantage l'IdO. Le rapport explique également qu'environ un tiers des organisations sont préoccupées par les risques de sécurité de l'IdO, notamment les violations de données. Pour lutter contre cela, l'externalisation est considérée comme le meilleur moyen de gagner en sérénité.

Même si de nombreux ingénieurs connaissent la notion de « sécurité par l'obscurité » (non-divulgation d'informations relatives au procédé considéré), peu d'entre eux sont qualifiés dans ce domaine pour garantir qu'une solution est sécurisée de bout en bout contre les attaquants. Et si les fournisseurs de semiconducteurs proposent toute une gamme de solutions de sécurité monopuces, les développeurs doivent encore comprendre comment les utiliser correctement afin d'éviter de créer par inadvertance de nouvelles failles de sécurité.

Au cours des dernières décennies, les solutions de réseaux étendus à basse consommation (LPWAN) telles que LoRa et Sigfox se sont imposées comme des technologies IdO sans fil clés prenant en charge les communications longue distance. Avec des portées de plusieurs dizaines de kilomètres, elles constituent une alternative au réseau cellulaire sans fil tel que le LTE Cat-M1 et le NB-IoT grâce à leurs performances exceptionnelles à basse consommation pour de faibles volumes de données [8]. Pour autant, à quel point sont-ils sécurisés ?

LoRaWAN à la loupe

Les protocoles LoRa et LoRaWAN ont fait l'objet d'une attention particulière de la part de la communauté de la sécurité et du piratage. Sébastien Dudek, de Trend Micro, entreprise spécialisée dans les solutions de sécurité informatique, est l'un des nombreux chercheurs qui ont écrit de manière approfondie sur certains des problèmes potentiels. Dans une série de trois notes techniques (brief1, brief2, brief3), il évoque un ensemble de problèmes de mise en œuvre et d'attaques potentielles. Celles-ci vont du déni de service (DoS) (**figure 2**) et de l'écoute clandestine au basculement binaire (**figure 3**) et à la mystification des accusés de réception (**figure 4**). Les conséquences de ces attaques vont de l'impossibilité de communiquer avec les nœuds jusqu'à l'altération des données des applications, en passant par la réduction de l'autonomie de la batterie. Un grand nombre des vulnérabilités signalées ont été résolues entre les versions 1.0.2 et 1.1 de la norme LoRaWAN. Cependant, d'autres défis se posent lors de l'exploitation de nœuds LoRaWAN avec des passerelles utilisant différentes versions de la spécification. Dans de tels cas, il est nécessaire d'apporter des modifications pour assurer une rétrocompatibilité sécurisée entre les dispositifs finaux et le back-end, comme le souligne un article de 2018 de Tahsin C. M. Dönmez [12].

Le problème ne se limite pas au piratage de la liaison sans fil. Le risque que de mauvais acteurs volent et attaquent directement le matériel existe aussi. Sébastien Dudek étudie également cet aspect de la sécurité. Dans le cas du protocole LoRaWAN, de nombreuses solutions utilisent un microcontrôleur et un module sans fil de Semtech. Comme ceux-ci sont connectés via SPI, les données passant entre les deux peuvent être facilement acquises et analysées.

En outre, il faut également tenir compte de la sécurité du microcontrôleur lui-même. Une méthode d'attaque consiste simplement à extraire le micrologiciel de la mémoire flash, ce qui permet d'analyser le code. Si les clés de sécurité se trouvent également dans le programme, un attaquant peut les utiliser pour développer des nœuds qui usurpent des dispositifs finaux authentiques. Pour lutter

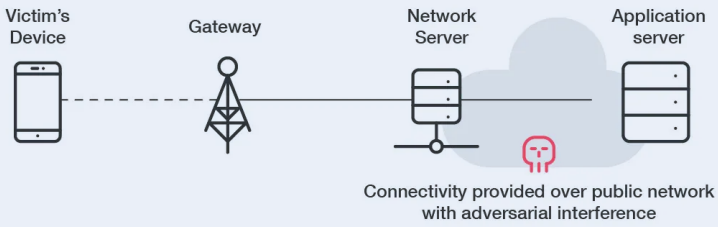

Figure 3. En raison de la structure fixe connue des paquets de données LoRaWAN, il est possible d'inverser les bits (attaque par basculement binaire) dans le contenu sans avoir à décrypter le message. Cela nécessite un accès au serveur du réseau recevant les données. (Source : Trend Micro)

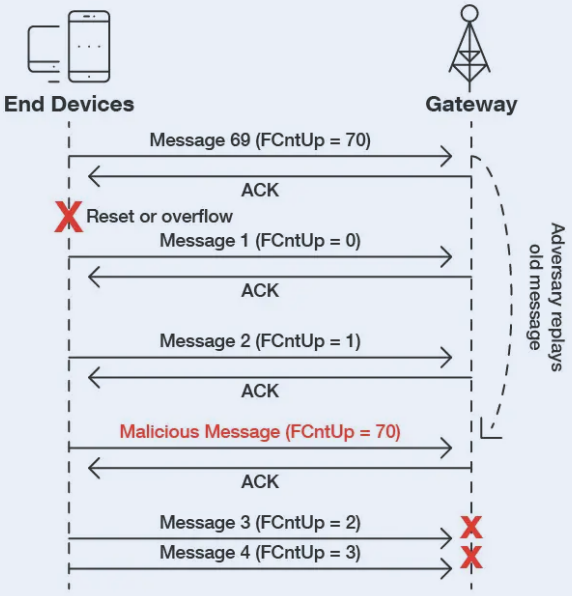

Figure 4. Le brouillage de la liaison sans fil amène le nœud LoRaWAN à répéter le transfert de paquets jusqu'à sept fois, ce qui réduit l'autonomie de la batterie. Si l'attaquant collecte et répète également les paquets d'accusés de réception (ACK), le nœud estime que la liaison est toujours fonctionnelle, car les paquets ACK ne déclarent pas la réception du message. (Source : Trend Micro)

contre ce risque, il est recommandé d'utiliser des Secure Elements (SE), des dispositifs d'authentification à puce unique qui stockent en toute sécurité les clés de cryptage. L'approche utilisant le composant ATECC608A de Microchip [13] est l'une des nombreuses configurations possédant un exemple de code. Bien que les exemples de projet montrent comment protéger les clés cryptographiques, la fonction de démarrage sécurisé de ce dispositif d'authentification n'est pas utilisée. Ainsi, si la même approche était utilisée pour un produit, le dispositif d'authentification pourrait être éliminé et utilisé comme SE (Secure Element) avec un microcontrôleur différent et un nouveau micrologiciel.

Problèmes de sécurité en général

Les terminaux LoRaWAN n'offrent qu'une bande passante de données limitée. De plus, n'ayant pas d'adresse IP comme un module Wi-Fi, ils ne sont pas adressables. En tant que tels, ils présentent un risque minimal pour les réseaux d'entreprise. Cependant, les applications basées sur ces technologies sans fil présentent des risques potentiels. En cas de problème, cela peut avoir des conséquences sur les vies et l'environnement. Par exemple, dans le cadre d'un réseau de ville intelligente, les capteurs LoRa peuvent être chargés de surveiller le niveau des eaux pour éviter les inondations. Si les données des capteurs sont bloquées, les systèmes de défense contre les inondations risquent de ne pas réagir. À l'inverse, de fausses données injectées pourraient amener ces systèmes à réagir à un événement inexistant, ce qui pourrait avoir des conséquences tout aussi désastreuses.

Nous avons évoqué ici les protocoles LoRa et LoRaWAN. Mais de nombreux chercheurs se penchent sur d'autres technologies LPWAN, notamment Sigfox et NB-IoT. Dans un article de Florian Laurentiu Coman et ass. [14], sont décrites plusieurs attaques de démonstration de faisabilité sur des réseaux sans fil autres que LoRaWAN. Dans une note technique publiée par Deutsche

Figure 5. Les capteurs de particules DEUS POLLUTRACK recueillent des données à partir d'unités IdO fixes et mobiles. Les données sont transmises au back-end à l'aide des réseaux cellulaires 4G et 5G. (Source : DEUS POLLUTRACK)

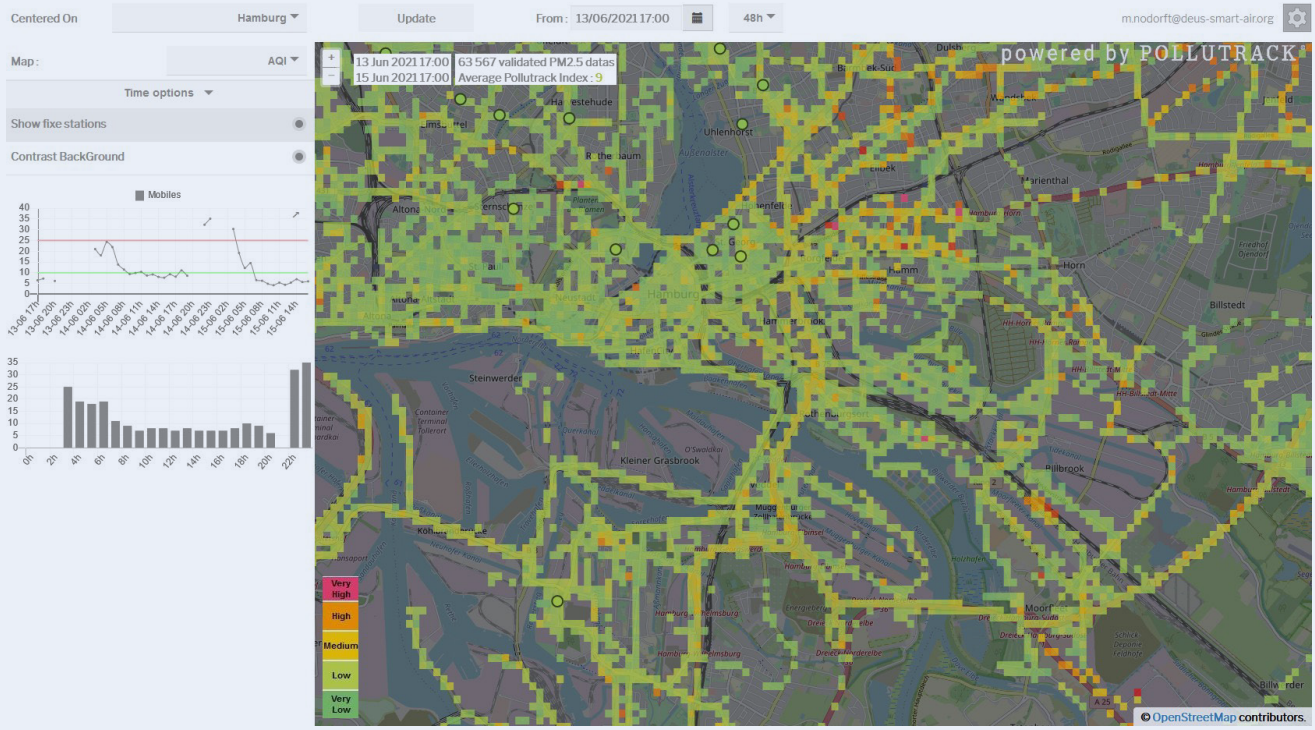

Figure 6. Un tableau de bord basé sur le cloud montre le niveau des polluants atmosphériques, comme illustré ici pour la ville allemande de Hambourg. Les autorités locales utilisent ces données pour élaborer des décisions sur les solutions de transport. (Source : DEUS POLLUTRACK)

Telekom [15], il est indiqué que la mise en œuvre de Sigfox et LoRaWAN « sans [un SE] peut [même] rendre inutile le chiffrement de bout en bout ». Le document explique qu'en revanche, le protocole NB-IoT bénéficie de fonctions de sécurité LTE éprouvées, telles que l'authentification et la génération, et l'échange de clés sécurisées. Cependant, il précise également que le chiffrement de bout en bout n'est pas standard et que, s'il est jugé nécessaire, il doit être discuté avec l'opérateur réseau.

Offrir des solutions IdO à l'échelle de la ville

Les problématiques relatives à la sécurité des réseaux LPWAN ont influencé les choix technologiques de DEUS POLLUTRACK Smart City GmbH i.G. pour sa plateforme IdO [16]. Leur équipe développe depuis plus de dix ans des réseaux de capteurs IdO pour surveiller les particules dans les villes. La technologie étant déployée dans plus de 15 villes européennes, elle permet aux responsables locaux des municipalités de prendre des décisions environnementales éclairées concernant la pollution atmosphérique. Leurs compteurs optiques de particules (OPC) brevetés sont capables de surveiller jusqu'à la classification des particules ultrafines (UFP) (moins de 0,1 µm). Alors que les particules plus volumineuses, comme les PM_{10}, sont considérées comme dangereuses pour les poumons, les UFP peuvent pénétrer dans la circulation sanguine et passer à d'autres organes par l'air inhalé.

La technologie de capteurs de DEUS (**figure 5**) utilise une combinaison de capteurs fixes et mobiles, reliés à des tableaux de bord en back-end qui visualisent les données collectées. Des villes comme Marseille et Paris utilisent 40 capteurs fixes ainsi que 300 capteurs mobiles [17]. Les capteurs mobiles sont installés sur les véhicules des partenaires, tels que les fourgons de livraison de DPD, qui circulent régulièrement dans la ville cible. Ces capteurs se réétalonnent en fonction des données acquises par les capteurs fixes qu'ils croisent pour garantir la précision requise sur la base. Tout cela nécessite un choix de réseau LPWAN robuste, fiable et sécurisé. Le cofondateur Marc Nodorft a expliqué que les normes Sigfox et LoRaWAN ont l'une et l'autre été considérées lors des premières étapes du développement. Sigfox offrait une infrastructure de connectivité, ce qui simplifiait le déploiement du système, mais aucun des deux ne fournissait le débit de données requis. Le protocole LoRaWAN, à l'époque, n'était pas suffisamment sécurisé et, en l'absence de partenaires d'infrastructure dans les villes où la technologie devait être déployée, il était nécessaire de mettre en place des passerelles qui se connectaient au back-end via des réseaux cellulaires. La 4G et, plus tard, la 5G cellulaire, ont donc été choisies, résolvant ainsi les problèmes de couverture, de fiabilité et de sécurité selon les niveaux requis.

Marc Nodorft nous explique également que, bien qu'il existe de nombreuses solutions électroniques bon marché pour l'IdO, celles-ci ne sont pas suffisamment robustes pour un déploiement à long terme dans les environnements où leurs produits sont installés. C'est pourquoi le choix s'est porté sur un développement conforme aux normes industrielles, une autre considération pour ceux qui planifient leurs propres produits IdO.

Autre aspect, les activités de back-end, développées spécifiquement selon les besoins de leur implémentation IdO (**figure 6**). Pour progresser, il est nécessaire de prendre en charge des tableaux de bord de reporting open source pour permettre aux organismes publics utilisant le système et aux citoyens d'accéder aux données, ce qui nécessite un fournisseur de services dans le cloud. Et, bien que les choix soient nombreux, la sélection du fournisseur est

aussi importante que la solution technique. Il faut donc chercher un fournisseur capable d'offrir une assistance personnelle, bien au-delà d'un chatbot de service client impersonnel.
Avec mon expérience dans des déploiements IdO importants et ayant beaucoup appris sur les défis techniques, je me suis demandé quels autres conseils Marc Nodorft pourrait donner à ceux qui cherchent à mettre en œuvre des solutions IdO. « Nous sommes toujours restés fidèles à notre vision, répond-il, ce qui nous a souvent obligés à modifier notre approche. » Cela a impliqué l'évaluation de différentes technologies, la collaboration avec différents partenaires et la modification de la stratégie de vente sur leur chemin vers le succès.

Équipes d'experts et partenariats nécessaires

Si l'on examine le paysage de l'IdO, il est clair que les opportunités commerciales s'offrent à vous, et ce, qu'il s'agisse de solutions pour les consommateurs ou l'industrie. Cependant, du concept au déploiement, le parcours est parsemé de défis. Si les développeurs de systèmes embarqués peuvent être bien versés dans le développement de matériel et de micrologiciels, et peuvent même avoir de l'expérience dans les technologies sans fil, l'IdO et ses défis en matière de sécurité et d'évolutivité peuvent être trop importants pour qu'une organisation s'y attaque toute seule.
Selon le rapport de la Commission européenne, les grandes organisations dominent également les relations commerciales en matière de services et de plateformes. Les petits opérateurs et les jeunes pousses (start-up) auront du mal à obtenir le soutien dont ils ont besoin dans ces relations asymétriques s'ils font cavalier seul. Sans aucun doute, l'expertise, au travers d'embauches ou de financements, est essentielle pour aller au-delà des exemples d'applications, des tableaux de bord de démonstration et des tests de services IdO. Enfin, il est vital de fixer votre vision, mais en restant agile dans tous les domaines de la mise en œuvre, depuis les choix technologiques jusqu'au marché visé, pour la concrétiser.

220053-04

Contributeurs

Texte : **Stuart Cording**
Rédaction : **Jens Nickel, C. J. Abate**
Traduction : **Asma Adhimi**
Mise en page : **Harmen Heida**

Des questions, des commentaires ?

Envoyez un courriel à l'auteur (stuart.cording@elektor.com) ou contactez Elektor (redaction@elektor.fr).

LIENS

[1] Articles d'Elektor sur l'IdO : www.elektormagazine.com/select/internet-of-things-IoT
[2] « IoT Insights, Edition 3 », Microsoft/Hypothesis, octobre 2021: https://bit.ly/3rxMk3a
[3] « The Journey to IoT Value », Cisco, mai 2017: https://bit.ly/3GzdJWS
[4] J. Lasquety-Reyes, « Smart Home - revenue forecast in Europe from 2017 to 2025 », Statista, juin 2021: https://bit.ly/3LlGiuG
[5] « Sector inquiry into the Consumer Internet of Things », Commission européenne, janvier 2022 : https://bit.ly/3Lgw9iE
[6] « Final report - sector inquiry into consumer Internet of Things », Commission européenne, janvier 2022 : https://bit.ly/3B2Htu9
[7] «The best voice assistant », ZDNet, septembre 2021 :: https://zd.net/3rxf6Rt
[8] L. Tan, « Comparison of LoRa and NBIoT in Terms of Power Consumption », Institut royal de technologie KTH : https://bit.ly/3JafsUb
[9] S. Dudek, « Low Powered and High Risk : Possible Attacks on LoRaWAN Devices », Trend Micro, janvier 2021 : https://bit.ly/3rA02Tg
[10] S. Dudek, « Gauging LoRaWAN Communication Security with LoraPWN », Trend Micro, février 2021 : https://bit.ly/3LhV0T5
[11] S. Dudek, « Protecting LoRaWAN Hardware from Attacks in the Wild », Trend Micro, mars 2021 : https://bit.ly/3rxquge
[12] T.C.M. Dönmez, « Security of LoRaWAN v1.1 in Backward Compatibility Scenarios », Elsevier, 2018 : https://bit.ly/3GtzKq0
[13] Page du produit Microchip - ATECC608A :: https://bit.ly/3B7zIms
[14] F.L. Coman et ass., « Security issues in internet of things : Vulnerability analysis of LoRaWAN, sigfox and NB-IoT », IEEE, juin 2019 : https://bit.ly/3uwhUQX
[15] « NB-IoT, LoRaWAN, Sigfox : An up-to-date comparison », Deutsche Telekom AG, avril 2021 : https://bit.ly/3uyUydj
[16] Site web de DEUS Pollutrack : https://bit.ly/3sHL9O5
[17] Réseau de mesure des capteurs DEUS : https://bit.ly/3Gzjbcc