# Comment adapter une conception existante à l'IoT

Auteur : Arild Rodland, Directeur du Développement Commercial (EMEA), Microchip Technology Inc.

Pour beaucoup de gens, l'augmentation actuelle du nombre d'appareils électroménagers connectés rappelle la croissance des connexions d'ordinateurs personnels à Internet dans les années 1990. À l'époque, un débat similaire a existé pour savoir si cette technologie n'était qu'un gadget ou si elle allait effectivement avoir un impact durable sur la société. Les PC et les téléphones portables connectés sont aujourd'hui devenus incontournables, et nombre d'observateurs prévoient le même genre d'évolution au fur et à mesure de l'adoption mondiale d'appareils électroménagers connectés.

Pouvoir allumer une cafetière depuis n'importe quel point du monde n'est pas vraiment susceptible de changer votre vie, mais les cafetières ne sont que le début de la révolution IoT domestique. L'IoT va être à la base d'innovations et d'opportunités commerciales dans le secteur de l'électroménager. Les progrès réalisés par l'apprentissage automatique et l'intelligence artificielle ne vont faire qu'accélérer cette évolution. La capacité de recueillir des données brutes provenant de différents appareils et différents capteurs ouvre un tout nouveau monde de cas et d'opportunités d'utilisation.

Certains concepteurs ne sont pas sûrs de vouloir participer à la révolution IoT parce qu'ils craignent que la conception d'un produit intégré à connectivité IoT ne soit une tâche trop ardue. En réalité, cela reste assez simple à réaliser. Un produit compatible IoT est en général composé de trois éléments : un processeur ou microcontrôleur (l'élément "intelligent"), un contrôleur réseau (l'élément "connecté") et un moyen de sécuriser la communication avec le Cloud (l'élément "sécurisé").

Etant donné que la plupart des concepteurs ont déjà investi beaucoup de temps et d'efforts pour élaborer un bon produit, il est intéressant de pouvoir réutiliser la majeure partie du travail de conception existant. Souvent, il suffit d'ajouter les éléments de connectivité et de sécurité à une conception existante pour obtenir la connectivité IoT. Plutôt que de concevoir une solution en partant de zéro, il est possible de transformer rapidement certaines conceptions existantes pour la connexion à l'IoT**.** Ceci peut se faire de manière très efficace en utilisant des techniques éprouvées dans le monde du logiciel pour simplifier et accélérer le développement.

**Réduire la difficulté**

Il y a quelques astuces que les concepteurs de systèmes embarqués peuvent apprendre des programmeurs de logiciels quand ils entreprennent d'adapter un produit existant pour l'IoT. Les programmeurs confrontés à un défi de programmation complexe ont l'habitude de recourir à une approche de conception descendante, aussi appelée programmation modulaire. Cette méthode consiste à décomposer le problème en sous-problèmes plus petits et plus simples à gérer, qui peuvent eux-mêmes être scindés en plusieurs tâches plus faciles à traiter. Il s'agit d'une approche puissante et éprouvée permettant de résoudre des problèmes complexes, qui seraient difficiles à résoudre avec un code monolithique. Comment cela se traduit-il pour des systèmes embarqués ?

Il s'avère que les ingénieurs en systèmes embarqués peuvent profiter des mêmes avantages en "modularisant" le développement de leur système. En plus de poser de réels défis de programmation, les systèmes embarqués doivent souvent se conformer à des normes et subir des processus de certification rigoureux. Les modifications apportées au logiciel ou au matériel après

certification peuvent nécessiter une re-qualification du produit. Rien que pour cette raison, il y a un énorme avantage à séparer les différentes parties nécessitant une certification en plusieurs sous-systèmes. Ainsi, les bogues d'un certain sous-système n'affectent pas la performance des autres.

Par exemple, de nombreux concepteurs souhaitent ajouter une connexion Internet sécurisée à la nouvelle génération d'un produit existant, afin d'améliorer l'expérience utilisateur et de faciliter l'ajout de fonctionnalités telles qu'un diagnostic à distance, des fonctions de surveillance, des services automatisés ou la collecte de données statistiques pour planifier de futures améliorations du produit. Ce nouveau produit compatible IoT aura besoin de trois fonctions principales : 1) l'application originale ; 2) une connectivité Internet ; et 3) un moyen de sécuriser l'application. Comme illustré en Figure 1, l'application compatible IoT est essentiellement l'application d'origine, avec des fonctions de sécurité et de connectivité en plus.




*Figure 1: Une application compatible IoT se compose d'une application, et de fonctions de sécurité et de connectivité*

D'un point de vue implémentation, ce défi de conception peut être divisé en trois sous-tâches, dans lesquelles le code de l'application originale est réutilisé, et où seules les fonctions de sécurité et de connectivité sont rajoutées.

Cependant, la sécurité et la connectivité Internet sont toutes deux difficiles à mettre en oeuvre en partant de zéro. En outre, l'intégration de nouvelles fonctionnalités dans une application existante peut interférer avec la solution existante, et ainsi réduire la qualité de l'ensemble. Les développeurs travaillent souvent du code qui a été optimisé pour l'application existante. Par conséquent, il peut s'avérer difficile d'ajouter une connectivité à délai critique et une sécurité gourmande en puissance de calcul, tout en garantissant les mêmes niveaux de performance aux produits mis à jour.

La Figure 2 illustre cette approche combinée. Toutes les fonctionnalités sont implémentées comme une solution unique, ce qui augmente la complexité d'écriture et de débogage de l'application. Des bogues dans une partie du code peuvent affecter le timing et la performance d'autres fonctions critiques, ce qui augmente le risque qu'un simple bogue puisse avoir des effets secondaires, nécessitant une re-qualification.

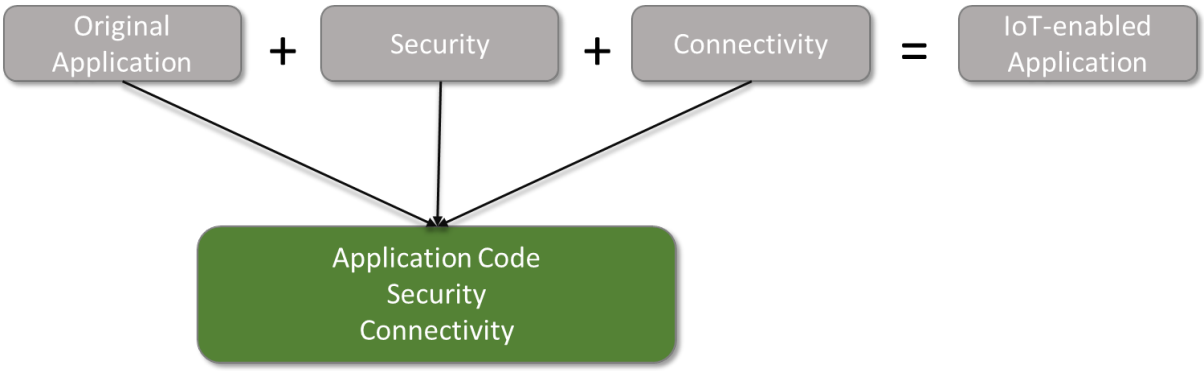



*Figure 2: Dans cette solution intégrée, tout le code et toutes les fonctionnalités sont intégrés dans un même dispositif, ce qui augmente la complexité du code et le temps de développement de celui-ci.*

Une approche modulaire permet aux concepteurs de conserver leur base de code et leur IP existants intacts, et simplement d'ajouter des fonctionnalités de connectivité et de sécurité en fonction des besoins.

Grâce à cette approche, les fonctionnalités de sécurité et de connectivité peuvent être mise en œuvre sous forme de tâches logicielles et matérielles distinctes, ce qui permet de gagner un temps considérable et de réduire le nombre d'ingénieurs nécessaires pour un produit donné. Cette approche favorise également la réutilisation du code et du système, ce qui offre plus de souplesse. Par exemple, un concepteur peut vouloir proposer à la fois une version Wi-Fi, et une version Bluetooth Low Energy (BLE) d'un même produit. L'approche modulaire permet d'innover rapidement et facilement au niveau de la conception IoT dans le cas d'un tel scénario.

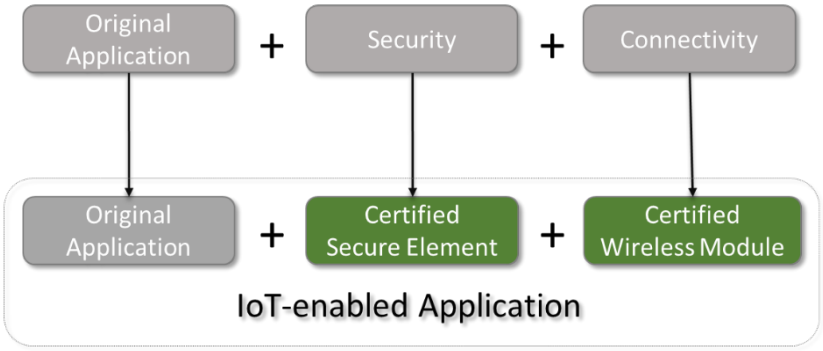



*Figure 3: Avec une solution modulaire, les concepteurs peuvent réutiliser l'application existante et isoler la sécurité et la connectivité comme des tâches de conception plus simples et plus faciles à gérer, indépendamment de l'application principale*

L'avantage de l'approche modulaire est que tout le travail axé sur l'optimisation et le "peaufinage" du système existant n'est pas perdu lorsque l'on ajoute la connectivité IoT au produit. Le concepteur peut facilement ajouter les fonctionnalités nécessaires sans affecter les autres parties du système.

Pour simplifier le processus, des modules certifiés peuvent être choisis pour la sécurité et pour la communication sans fil. Cela réduit considérablement le temps de certification, et le temps nécessaire au lancement du nouveau produit sur le marché. Un exemple d'un tel composant de sécurité certifié est l'ATECC608A de Microchip. Ce dispositif prend en charge toutes les tâches associées à l'authentification et au stockage sécurisé des clés et des certificats, et fournit ainsi une solution sécurisée, sans nécessiter d'écriture de code. De la même manière, les modules sans fil certifiés sont capables d'éxécuter toutes les opérations nécessaires pour se connecter en toute sécurité à un réseau sans fil.

L'utilisation de modules certifiés pour la sécurité et le sans-fil évite aussi au concepteur d'être un expert en sécurité et en communications. Les modules contiennent tous les éléments de code nécessaires, et sont généralement contrôlés par de simples commandes envoyées via une interface série de type UART, SPI ou I2C.

Pour simplifier encore la conception et accélérer le "time-to-market", des outils comme la carte de développement AVR-IoT WG de Microchip contiennent les modules nécessaires à une connectivité IoT sûre et facile à déployer. Avec de tels outils, il suffit de 30 secondes et de quelques clics à un ingénieur pour connecter un produit existant à Google Cloud IoT Core et commencer à transmettre des données.

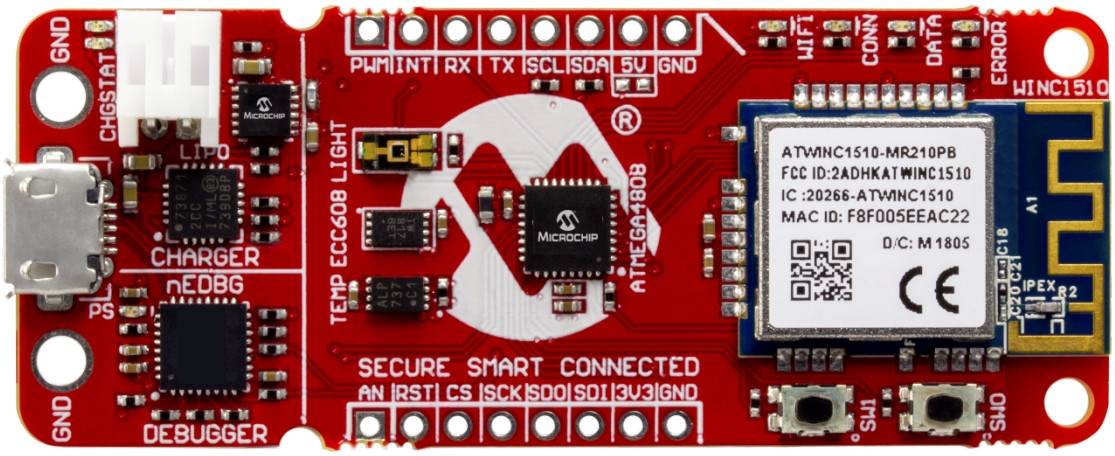



*Figure 4 : La carte de développement AVR-IoT WG combine un microcontrôleur AVR®, un CI de sécurité et un contrôleur de réseau Wi-Fi certifié, et permet aux concepteurs de prototyper des dispositifs connectés en quelques minutes*

La possibilité de connecter de l'électroménager ou des produits grand-public au Cloud permet aux concepteurs de produire une valeur ajoutée beaucoup plus élevée, que ce soit en fournissant des données importantes pour l'intelligence artificielle et l'apprentissage machine, ou simplement en offrant un moyen plus facile d'exécuter des mises à jour sécurisées de firmware à distance. La réduction de difficulté et l'utilisation de modules certifiés pour les fonctionnalités de sécurité et de communication, constituent pour les concepteurs un formidable raccourci pour adapter des conceptions existantes afin de tirer parti de nouvelles opportunités.