

Que faut-il savoir au moment de spécifier un microcontrôleur avec des capacités Wi-Fi ?

Par Alex Li, Microchip Technology

Les objets connectés industriels sont en constante évolution. La tendance va vers davantage de fonctions sur un seul SoC plutôt que sur plusieurs composants discrets parce que cela permet, entre autres, une nomenclature plus réduite et diminue les risques liés à la conception tout en permettant une empreinte plus faible. Le microcontrôleur Wi-Fi illustre parfaitement cette tendance ; il intègre la connectivité Wi-Fi avec un processeur et les E/S à usage général requises pour répondre aux besoins d'un grand nombre d'applications diverses. Il existe différents facteurs à prendre en compte au moment de spécifier l'un de ces composants et il est important de bien les comprendre afin de minimiser les risques.

Il existe aujourd'hui des options de connectivité Wi-Fi économiques sur le marché, mais c'est souvent au détriment du nombre de périphériques et des performances globales. C'est pourquoi choisir le meilleur microcontrôleur Wi-Fi peut se révéler un véritable défi, et être risqué, car un microcontrôleur Wi-Fi ne doit pas seulement être doté d'une connectivité Wi-Fi robuste, mais doit aussi posséder des fonctionnalités de microcontrôleurs hautes performances. En l'absence de l'un ou de l'autre, le projet de conception pourrait être retardé voire échouer. En temps qu'élément central du système, le microcontrôleur est la partie la plus critique du microcontrôleur Wi-Fi, c'est pourquoi il est nécessaire d'analyser ses performances dès le début du projet, car s'il s'avère qu'il faille changer le composant par la suite, cela revient généralement à refaire toute la partie logicielle ainsi que la configuration du circuit y afférent.

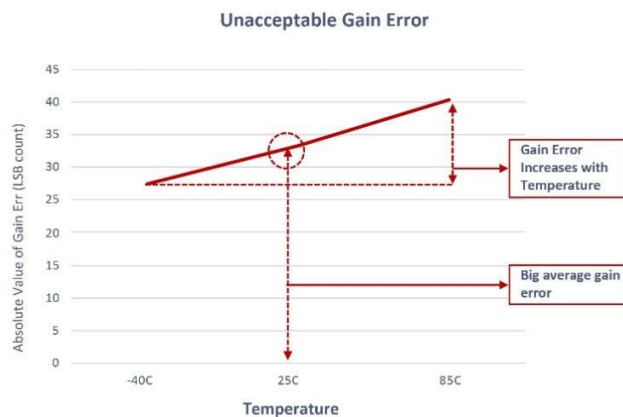
N'oubliez pas le convertisseur A/N

La conversion analogique/numérique est une fonction qui est trop souvent oubliée lors de la spécification d'un microcontrôleur Wi-Fi, bien que ce soit le premier composant de traitement dans la chaîne du signal après l'entrée analogique. Ses performances affectent donc l'ensemble du système, et c'est pourquoi il est important de comprendre les mesures clés concernant le convertisseur analogique/numérique (ADC) et comment le fabricant du microcontrôleur Wi-Fi devrait les gérer.

L'une des premières spécifications à laquelle les développeurs s'intéressent est le nombre de bits du convertisseur A/N. Cela peut s'avérer déconcertant car dans la pratique, le vrai nombre de bits est plus faible que celui indiqué dans les spécifications de la fiche de données (voire parfois beaucoup plus faible). Ce qui est donc plus important, c'est le nombre effectif de bits

(ENOB, *Effective Number of Bits*) dont dispose le convertisseur A/N pour effectuer la conversion. Ce nombre sera invariablement plus faible que celui inscrit dans la fiche de données, mais il est cependant très important que le chiffre ENOB soit le plus proche possible de celui de la fiche de données, car cet écart varie considérablement d'un convertisseur à l'autre. Moins il y aura de bits disponibles pour effectuer la conversion, moins le SoC représentera précisément le signal d'entrée.

De plus, comme tous les composants électroniques, les convertisseurs A/N « ajoutent » quelque chose au signal, qui affecte négativement leurs capacités, y compris des erreurs relatives à la quantification, l'horodatage, des variations d'offset et de gain ou de la linéarité. Les convertisseurs A/N sont également très connus pour leur sensibilité aux grandes variations de température, qui sont monnaie courante dans de nombreux environnements de fonctionnement pour les capteurs IoT industriels. Le fabricant de microcontrôleurs Wi-Fi peut limiter ce problème, c'est pourquoi il est important de contacter le fabricant de chaque microcontrôleurs Wi-Fi potentiel afin de déterminer leur ENOB, leurs performances en température, leur linéarité et leur précision. Si ces informations ne peuvent être obtenues, passez votre chemin.



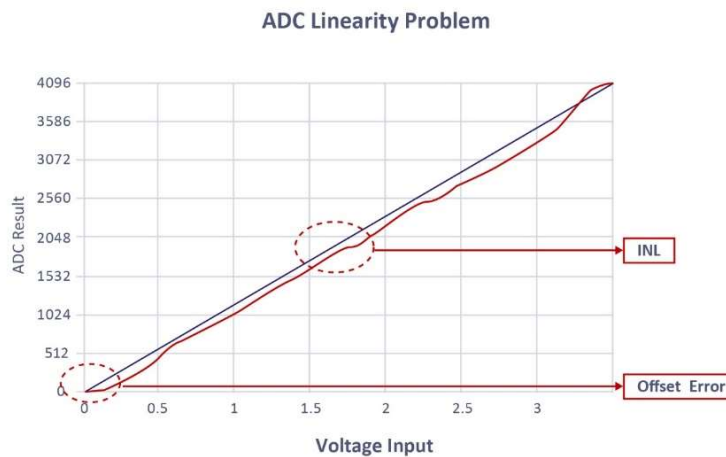


Figure 1. Les convertisseurs A/N de piètre qualité sont peu précis, affichent une faible linéarité et sont sensibles à l'environnement et à la température.

Compatibilités de périphériques

Tous les microcontrôleurs Wi-Fi supportent au minimum certaines interfaces standards, il arrive donc souvent de préférer supposer qu'il y en aura assez. Les ingénieurs regrettent souvent cette supposition quand ils essaient d'utiliser le même microcontrôleur Wi-Fi dans un autre système. Cela se produit très fréquemment lors de la construction ou de la modification de systèmes IoT industriels, car la plupart des équipements de production possèdent un large éventail de machines et de contrôleurs construits à divers moments, par des fabricants différents.

Et, au fur et à mesure que le système grandit, d'autres interfaces viennent encore s'y ajouter, de sorte qu'il arrive un moment où la compatibilité avec la détection tactile ou un écran LCD deviendra nécessaire. Si le SoC possède des E/S à usage général en surplus, il est possible alors de commander d'autres relais, commutateurs et autres composants sans avoir recours à un partage de broche (ou très peu). C'est pourquoi les interfaces prises en charge par le composant doivent au minimum inclure Ethernet MAC, USB, CAN CAN-FD, SPI, I²C, SSI, UART, et JTAG (et éventuellement prendre en charge la détection tactile et un afficheur) afin de parer à quasiment tous les scénarios possibles actuellement et anticiper sur l'avenir.

La sécurité commence à l'intérieur

La sécurité est capitale pour toutes les applications IoT, mais elle est absolument critique pour les cas d'utilisation dans l'industrie. Dès lors qu'une menace s'introduit dans un réseau IoT industriel, elle peut se répandre sur l'ensemble du site et potentiellement affecter l'entreprise entière. Le premier niveau où la sécurité est requise se trouve dans le moteur de chiffrement intégré au microcontrôleur, où le chiffrement et l'authentification s'effectuent de façon séquentielle ou en parallèle. Les codes doivent inclure le chiffrement AES, avec des clés allant jusqu'à 256 bits, DES et TDES, et l'authentification doit comprendre les standards SHA-1 et SHA-256, ainsi que MD-5.

Comme chaque fournisseur de service de Clouding possède son propre standard de certification et ses propres clés de chiffrement, le processus d'octroi de clé dans le composant s'avère complexe, nécessite de solides connaissances en cryptographie et représente l'une des tâches les plus difficiles pour les concepteurs. Heureusement, certains fabricants comme Microchip Technology facilitent ce processus en leur faisant gagner un temps considérable et par conséquent réaliser de sacrées économies. Le gain de temps et les problèmes évités ne sont pas à prendre à la légère ; plusieurs semaines au bas mot seront gagnées sur l'ensemble du développement tout en garantissant que toutes les conditions de sécurité et d'octroi de clé sont réunies, le tout en suivant une méthode vérifiable et ayant fait ses preuves.

Il est important de savoir que la plupart des microcontrôleurs Wi-Fi stockent les autorisations dans une mémoire Flash, où les données sont accessibles et vulnérables aux attaques logicielles comme physiques. La meilleure façon de sécuriser ces informations consiste à les conserver sur un élément sécurisé matériel, car les données qu'il renferme ne pourront ainsi être lues par aucun logiciel externe. Par exemple, les microcontrôleurs Wi-Fi de Microchip tels que le WFI32 (**figure 2**) utilisent cette méthode sur la plateforme Trust&GO de la société pour procéder en toute sécurité à l'octroi de clé dans ses microcontrôleurs en vue d'une connexion aux services AWS IoT, Google Cloud, Microsoft Azure ainsi qu'à tout autre réseau TLS tiers.

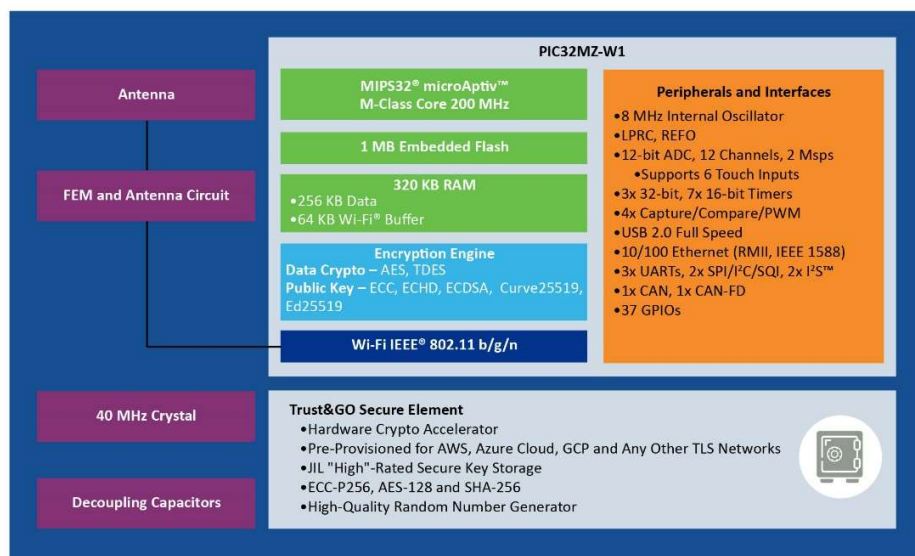


Figure 2. Le module Wi-Fi du WF132 isole les autorisations en les stockant sur un composant matériel, ce qui les rend quasiment invulnérables au piratage.

Les éléments sécurisés pré-configurés ou personnalisés stockent les autorisations générées dans des modules matériels sécurisés (ou HSM, *Hardware Secure Modules*) en usine, évitant ainsi toute exposition au cours de la production ou après. La plateforme Trust&Go ne nécessite qu'un kit de développement économique de Microchip, dans lequel le développeur va utiliser la suite de conception incluse en s'aidant des tutoriels et des exemples de code fournis, pour créer le fichier .manifest requis. Une fois que le code C pour l'élément sécurisé fonctionne sur l'application, le système peut être envoyé en production.

L'autre forme de sécurité requise est la toute dernière sécurité Wi-Fi certifiée par la Wi-Fi Alliance. La dernière version est la WPA3, qui s'inspire de la précédente WPA2, en y ajoutant des fonctionnalités qui simplifient la sécurité Wi-Fi, permettent une authentification plus robuste, offrent une puissance de chiffrement accrue et maintiennent la résilience du réseau. Tous les nouveaux composants doivent être certifiés WPA3 afin de pouvoir porter le logo de la Wi-Fi Alliance, de sorte que toutes les puces Wi-Fi et tous les microcontrôleurs Wi-Fi doivent en principe être certifiés pour une sécurité optimale. Néanmoins, il est prudent de s'assurer que le microcontrôleur Wi-Fi choisi est bien certifié WPA3.

Garantir l'interopérabilité

Il est possible que le microcontrôleur Wi-Fi ne puisse pas communiquer avec certains points d'accès sur le marché en raison d'une mauvaise adaptation RF, logicielle ou autre. Or, ne pas pouvoir se connecter à des points d'accès populaires peut sérieusement entâcher la réputation d'une société. Bien qu'il soit impossible de garantir qu'un microcontrôleur Wi-Fi fonctionnera avec absolument tous les points d'accès du globe, le problème peut tout de même être minimisé en s'assurant que le microcontrôleur Wi-Fi a passé avec succès des tests d'interopérabilité avec les points d'accès les plus populaires du marché. Cette information est disponible sur les sites Web des fabricants. Toutefois, si elle n'est pas accessible, vous pouvez appeler le fabricant en réclamant ces informations. En l'absence de réponse, optez pour un autre fournisseur.

Vous aurez besoin d'aide

Dernier point, mais loin d'être des moindres, vous aurez besoin d'une assistance à la conception. Sans une plateforme complète d'environnement de développement (IDE), le développeur en est réduit à faire du bricolage à partir de ressources trouvées sur le Web, qui peuvent s'avérer (ou non) utiles, simples ou fiables. Par exemple, certains fabricants de microcontrôleurs Wi-Fi fournissent les informations de base sur le produits et les instructions pour le prototypage, mais s'arrêtent là au lieu d'inclure des informations, pourtant importantes, expliquant comment passer de cette étape à la production.

Pour apporter un vrai plus, le fabricant devrait fournir un environnement de développement complet (**figure 3**) qui reprenne chaque fonction analogique et numérique réalisée par le microcontrôleur Wi-Fi, ainsi que tous les composants externes requis pour son implémentation sur des applications spécifiques. Il devrait fournir un moyen de visualiser comment les modifications apportés au système affectent ses performances globales tout comme la possibilité d'évaluer les performances RF du système ainsi que la conformité à la législation. Certains outils de base sont gratuits, tandis que d'autres sont disponibles à un coût abordable, y compris les cartes d'évaluation conçues pour être utilisées avec la famille de microcontrôleurs Wi-Fi.

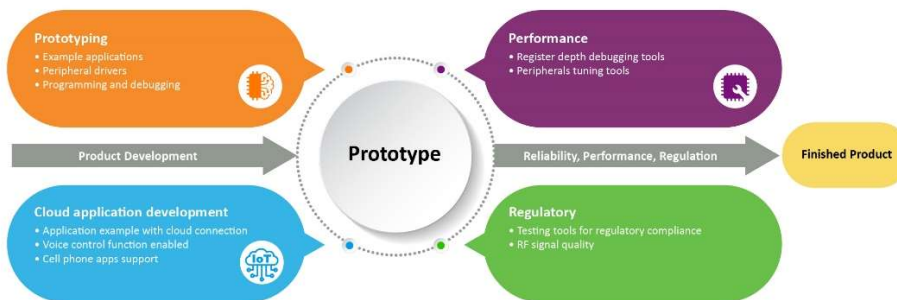


Figure 3. Un environnement de développement de ce type réduit les risques en offrant au développeur un outil de débogage, ainsi que d'autres outils utilisés pendant le cycle de production, du prototypage au produit fini.

Résumé

La tendance dans le monde de l'Internet des Objets consiste à placer davantage de puissance de calcul dans le réseau plutôt qu'uniquement dans les centres de données distants. Pour y parvenir, il faut intégrer le plus de fonctions possibles dans l'espace le plus réduit possible avec un nombre minimal de composants. Le microcontrôleur Wi-Fi est l'un des nombreux SoC qui contribuent à cet effort en intégrant de nombreuses fonctions dans un seul composant plutôt que dans plusieurs composants discrets dédiés à une fonction spécifique.

L'intégration de ce type de composant dans un sous-système IoT embarqué peut s'avérer relativement simple, à supposer que les ressources nécessaires sont disponibles auprès du fabricant du microcontrôleur Wi-Fi. Parmi ces ressources, il faut un haut niveau de sécurité, des moyens simples de procéder à l'octroi de clé répondant aux besoins des fournisseurs de service de Clouding, et un environnement de développement complet qui guide le développeur depuis le prototypage jusqu'à la production.