

SoC sans fil pour dispositifs de soins de santé connectés

Auteur : Rolf Horn, ingénieur d'applications chez Digi-Key Electronics

Au cours des deux dernières décennies, le secteur des soins de santé a adopté une utilisation accrue des technologies numériques. La pandémie de COVID-19 a contribué à accélérer cette évolution. L'accès à distance aux soins de santé, rendu nécessaire par la pandémie, a mis en évidence plusieurs autres avantages, notamment des soins de santé plus efficaces et un suivi continu des patients. Les avancées technologiques ont donné naissance à l'Internet des objets médicaux (IoMT), où des réseaux de patients équipés de capteurs et de dispositifs médicaux portables et/ou corporels, et les fournisseurs et les systèmes de soins de santé correspondants, sont connectés via Internet. Les dispositifs de surveillance du taux de glycémie en continu et les moniteurs cardiaques sont des exemples d'appareils largement adoptés. Les dispositifs IoMT aident à automatiser le transfert de données, réduisant ainsi les erreurs humaines. Grâce aux progrès en matière d'analyse de données prédictive et d'intelligence artificielle (IA), les dispositifs IoMT sont encore plus puissants en permettant des diagnostics basés sur les données avec une détection précoce des anomalies, un plus grand engagement personnel des patients et une réduction des coûts de santé.

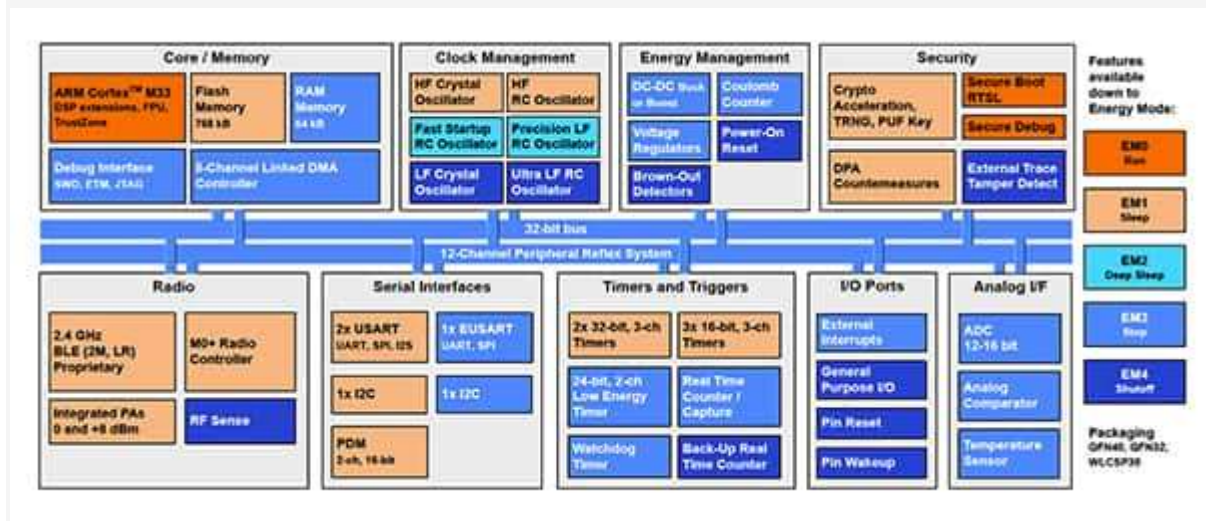
Exigences clés pour les dispositifs IoMT

- **Sécurité :** Le caractère sensible des informations médicales transférées exige un haut niveau de sécurité. La norme de chiffrement avancé (AES) et la cryptographie par courbes elliptiques (ECC) peuvent chiffrer et déchiffrer le transfert de données à l'aide de clés sécurisées et ainsi authentifier les données. Les clés basées sur un générateur de nombres véritablement aléatoires (TRNG) dans le dispositif contribuent à la génération sécurisée de ces clés. Les attaques par usurpation peuvent être minimisées grâce à l'identification du dispositif à l'aide de fonctions physiques inclonables (PUF) uniques au sein du dispositif semi-conducteur. Les protocoles matériels de démarrage sécurisé, ainsi que les mécanismes inviolables qui empêchent l'accès aux régions protégées de la mémoire du dispositif contribuent à améliorer la sécurité du dispositif.
- **Consommation d'énergie :** Les dispositifs corporels et portables fonctionnent généralement sur batterie. Des protocoles de communications basse consommation tels que Bluetooth LE 5.x, des modes d'économie d'énergie lorsque le dispositif est inactif et une architecture efficace qui optimise les performances opérationnelles par rapport à la consommation d'énergie sont quelques-unes des fonctionnalités essentielles pouvant maximiser la durée de vie de la batterie.
- **Riche ensemble de fonctionnalités dans un format compact :** Les dispositifs compacts et légers peuvent être utilisés dans les applications médicales portables et corporelles. Les nouvelles applications, telles que les implants dentaires intelligents, requièrent des facteurs de forme miniatures. Le concept de système sur puce (SoC) offre un haut niveau d'intégration multifonctionnelle sur une seule puce. Il peut s'agir d'un ensemble de fonctionnalités périphériques fournissant la détection, la mesure, la transformation des données et la communication analogiques et numériques haute vitesse. D'autres exigences essentielles incluent la connectivité sans fil, le traitement des données haute vitesse avec de grandes mémoires Flash et RAM, des temporisateurs et des horloges basse fréquence/basse consommation de précision, la régulation de tension CC/CC, etc.

Famille de SoC Wireless Gecko EFRBG27 de Silicon Labs pour applications IoT

En mars 2023, [Silicon Labs](#) a annoncé le lancement d'une nouvelle famille de dispositifs écoénergétiques sécurisés, étendant leur portefeuille de produits Wireless Gecko. Cette famille inclut notamment la série BG27 de dispositifs SoC Bluetooth LE, parfaitement adaptés aux applications IoT.

Un schéma fonctionnel montrant le riche ensemble de fonctionnalités inclus dans les SoC BG27 est présenté à la Figure 1. Vous trouverez ci-dessous quelques détails sur les fonctionnalités clés.



Processeur et mémoire : Le cœur RISC ARM Cortex®-M33 de 76,8 MHz et 32 bits avec instruction DSP et unité en virgule flottante permet une capacité de traitement des signaux hautes performances à 1,50 Dhrystone MIPS/MHz. Il inclut la technologie de sécurité ARM TrustZone. La mémoire Flash est de 768 Ko, tandis que la mémoire de données est de 64 Ko de RAM. Le contrôleur d'accès direct à la mémoire (LDMA) permet au système d'effectuer des opérations de mémoire indépendantes du logiciel, réduisant ainsi la consommation d'énergie et la charge de travail du logiciel.

Modes basse consommation : L'EFR32BG27 inclut une unité de gestion de l'énergie (EMU) qui gère les transitions des modes d'énergie (EM0 à EM4) du SoC. Avec l'unité EMU, les applications peuvent minimiser dynamiquement la consommation d'énergie pendant l'exécution du programme. Le mode EM0 offre le plus grand nombre de fonctionnalités, telles que l'activation du processeur, de la radio et des périphériques à la fréquence d'horloge la plus élevée. Les périphériques peuvent être désactivés dans les modes actifs basse consommation EM2, EM3. La mise à l'échelle de la tension est utilisée par l'unité EMU lors de la transition entre les modes d'énergie afin d'optimiser le rendement énergétique en fonctionnant à des tensions plus basses lorsque cela est possible. EM4 est l'état inactif à la plus basse consommation qui permet au système de s'activer en mode EM0.

Conversion CC/CC : La famille EFR32BG27 comprend des convertisseurs intégrés en modes abaisseur et élévateur, pouvant fournir la tension interne requise de 1,8 V. Les dispositifs en mode élévateur, tels que l'[EFR32BG27C230F768IM32-B](#), ont la capacité de fonctionner à seulement 0,8 V, permettant l'utilisation de batteries alcalines à une cellule, oxyde d'argent et autres batteries basse tension. Le convertisseur élévateur peut être arrêté à l'aide d'une broche BOOST_EN dédiée, économisant ainsi l'énergie de la batterie système pendant le stockage et

l'expédition. Dans ce mode, la consommation de courant maximum n'est que de 20/50 nA, en fonction de l'alimentation de certaines broches. Dans les dispositifs en mode abaisseur, tels que l'[EFR32BG27C140F768IM40-B](#), une tension maximum de 3,8 V peut être fournie en externe. Un moniteur d'alimentation intégré signale lorsque l'alimentation est suffisamment faible pour permettre de contourner le régulateur et d'étendre la plage à 1,8 V. Le mode de dérivation permet également au système de passer en mode d'économie d'énergie EM4. Un bloc de compteurs de coulombs est intégré au convertisseur CC/CC. Il inclut deux compteurs 32 bits utilisés pour mesurer le nombre d'impulsions de charge délivrées par le convertisseur CC/CC, permettant un suivi précis du niveau de la batterie pour améliorer la sécurité de l'utilisateur.

Mise en réseau Bluetooth 5.x : Le protocole sans fil Bluetooth Low Energy (LE) est pris en charge par cette famille de SoC. Le récepteur radio utilise une architecture Low-IF composée d'un amplificateur à faible bruit et d'un convertisseur abaisseur I/Q. Le module de commande automatique de gain (CAG) ajuste le gain du récepteur pour éviter la saturation et améliorer la sélectivité et les performances de blocage. La radio 2,4 GHz est étalonnée en production pour améliorer les performances de réjection d'image. La famille inclut un choix de puissances de transmission s'étendant de 4 dBm à 8 dBm. L'atténuation du bruit RF inclut le fonctionnement du convertisseur CC/CC en mode de commutation douce au démarrage et les transitions de régulation CC/CC à dérivation pour limiter la vitesse de balayage d'alimentation maximum et atténuer le courant d'appel. Le bloc RFSENSE permet au dispositif de rester en mode d'économie d'énergie EM2, EM3 ou EM4 et de s'activer lorsqu'une énergie RF supérieure à un seuil spécifié est détectée.

Sécurité : La famille de SoC EFR32BG27 comprend une variété de fonctionnalités de sécurité, comme le montre la Figure 2.

FONCTIONNALITÉS	SECURE VAULT MID (SVM)
Générateur de nombres véritablement aléatoires (TRNG)	Oui
Démarrage sécurisé avec RTSL (racine de confiance et chargeur sécurisé)	Oui
Débogage sécurisé avec verrouillage/déverrouillage	Oui
Contre-mesures DPA	Oui
Anti-violation	Altération externe (ETAMPDET)
Attestation sécurisée	Avec TrustZone
Gestion des clés sécurisée	Avec TrustZone

Chiffrement symétrique	<ul style="list-style-type: none"> • AES 128 bits/192 bits/256 bits <ul style="list-style-type: none"> ◦ ECB, CTR, CBC, CFB, CCM, GCM, CBC-M
Chiffrement à clé publique - ECDSA/ECDH/EdDSA	<ul style="list-style-type: none"> • p192 et p256
Dérivation de clé	<ul style="list-style-type: none"> • ECJ-PAKE p192 et p256
Hachages	<ul style="list-style-type: none"> • SHA-1 • SHA-2/256

Figure 2 : Fonctionnalités de sécurité de la famille de SoC Wireless Gecko EFR32BG27. (Source de l'image : Silicon Labs)

Le démarrage sécurisé avec RTSL authentifie un micrologiciel de confiance qui démarre à partir d'une mémoire morte (ROM) immuable. L'accélérateur cryptographique prend en charge le chiffrement et le déchiffrement AES et ECC. Il inclut également des contre-mesures DPA (Differential Power Analysis) pour protéger les clés. Le générateur TRNG récupère l'entropie d'une source thermique et inclut des tests d'état de démarrage pour cette source, comme l'exigent les normes NIST SP800-90B et AIS-31, ainsi que des tests d'état en ligne comme requis par la norme NIST SP800-90C. L'interface de débogage, verrouillée lorsque le composant est déployé sur le terrain, dispose d'une fonction de déverrouillage sécurisé qui permet un accès authentifié basé sur la cryptographie à clé publique. Côté matériel, un module ETAMPDET (External Tamper Detect) permet de détecter toute altération externe telle qu'une ouverture non autorisée du boîtier. Il peut générer une interruption pour avertir le logiciel et permettre de prendre des mesures au niveau du système.

Riche ensemble de périphériques : Les SoC incluent des convertisseurs analogique-numérique hybrides qui combinent les techniques SAR et Delta-Sigma. Le mode 12 bits peut fonctionner à des vitesses jusqu'à 1 Méch./s, tandis que le convertisseur 16 bits peut fonctionner jusqu'à 76,9 Kéch./s. Le module de comparateur analogique peut utiliser des références internes ou externes et peut également être utilisé pour détecter la tension d'alimentation. Les modes de communication série SPI, USART et I2C sont tous pris en charge. Le module de capture et d'horloge temps réel (RTCC) fournit un chronométrage 32 bits jusqu'aux modes de puissance EM3 et peut être cadencé avec l'oscillateur basse fréquence interne. Le temporisateur basse consommation (LETIMER) fournit une résolution de 24 bits et peut être utilisé pour la temporisation et la génération de sortie lorsque la majeure partie du dispositif est hors tension, permettant ainsi d'effectuer des tâches simples avec une consommation d'énergie minimale. Le système PRS (Peripheral Reflex System) est un réseau de routage des signaux qui permet la communication directe entre les modules périphériques sans impliquer le processeur. Cela réduit la surcharge logicielle et la consommation de courant.

Boîtiers à empreinte réduite : L'[EFR32BG27C320F768GJ39-B](#) est un dispositif de la famille EFR32BG27. Ce dispositif est fourni en boîtier WLCSP avec des dimensions de seulement 2,6 mm x 2,3 mm, et il peut fonctionner en modes de régulateur abaisseur ou élévateur. Les autres dispositifs de la famille de produits sont disponibles en boîtiers QFN32 de 4 mm x 4 mm ou QFN40 de 5 mm x 5 mm dans des modes de régulateurs spécifiques de type abaisseur ou élévateur.

Conclusion

L'EFR32BG27 offre une capacité de traitement écoénergétique de pointe et une connectivité Bluetooth Low Energy. Ces SoC à facteur de forme compact, dotés d'une variété de fonctionnalités de sécurité, sont parfaitement adaptés aux applications IoMT.

www.digikey.fr