

Anatomie des microcontrôleurs de sécurité pour les applications IoT

Rich Miron, Applications Engineer at Digi-Key Electronics

L'implémentation de la sécurité dans les conceptions embarquées peut sembler être une tâche colossale. C'est là que les microcontrôleurs spécialisés dans les fonctionnalités de sécurité entrent en jeu pour activer la sécurité dès le début de la conception embarquée. C'est une bonne chose, car il ne fait aucun doute qu'une nouvelle génération de solutions embarquées est nécessaire pour sécuriser les applications Internet des objets (IoT).

D'après une étude d'ABI Research, on estime que moins de 4 % des dispositifs IoT vendus l'an passé intégraient des fonctionnalités de sécurité embarquée. Dans le même temps, la société d'études de marché prévoit que, d'ici 2020, près de 25 % des cyberattaques cibleront les dispositifs IoT, faisant des microcontrôleurs de sécurité un sujet brûlant.

Mais qu'est-ce qu'un microcontrôleur de sécurité ? Nombre de ces dispositifs prétendent offrir des fonctionnalités de sécurité, mais à y regarder de plus près, cela semble être de belles paroles. Cet article explore en détail ce qui définit un microcontrôleur de sécurité. Il s'intéresse aux propriétés et aux fonctionnalités qui distinguent un microcontrôleur véritablement sécurisé d'un dispositif qui prétend l'être.

Commençons par la quête des fournisseurs de microcontrôleurs qui cherchent à compléter leurs solutions matérielles de sécurité avec une couche supplémentaire de sécurité afin de renforcer la défense contre les vulnérabilités logicielles et les attaques basées sur le réseau.

Récit de deux collaborations avec des microcontrôleurs

L'avènement des dispositifs de points d'extrémité fonctionnant à la périphérie du réseau demande des mises à jour micrologicielles sécurisées sans fil (OTA). Les microcontrôleurs [RX651](#) de [Renesas](#) répondent à cette exigence de reprogrammation en intégrant la technologie Trusted Secure IP (TSIP) et la protection de zone Flash de confiance, qui active les mises à jour micrologicielles Flash sur le terrain grâce à des communications réseau sécurisées.

La technologie TSIP offre une gestion solide des clés, la communication cryptée et la détection des intrusions afin d'assurer une sécurité forte contre les menaces externes comme l'écoute illicite, les altérations et les virus (Figure 1). De la même manière, la mémoire Flash à deux bancs intégrée facilite l'exécution sûre et fiable des mises à jour micrologicielles sur site pour les fabricants de dispositifs.

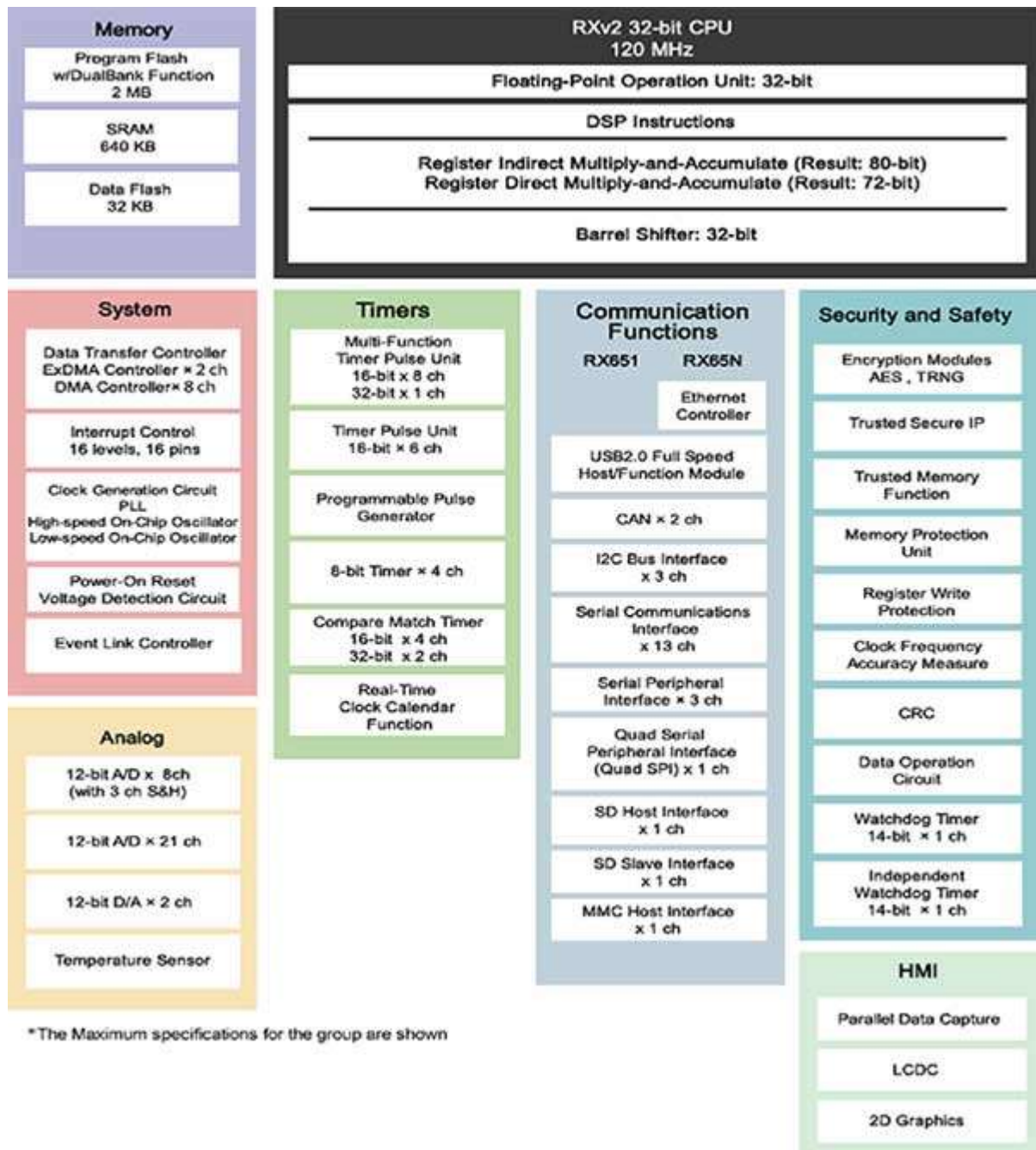


Figure 1. Aperçu des éléments de sécurité (au milieu à droite) du microcontrôleur RX651. (Source de l'image : Renesas Electronics)

La mémoire Flash à deux bancs permet aux concepteurs de systèmes embarqués d'atteindre les niveaux élevés d'une base fiable grâce à la combinaison de la technologie TSIP pour la protection des clés de cryptage et d'accélérateurs matériels de cryptage comme AES, 3DES, RSA, SHA et TRNG. La protection de zone Flash réservée au code permet ensuite de sécuriser le code d'amorçage contre la reprogrammation non autorisée.

Renesas a décidé de collaborer avec Secure Thingz, un expert en matière de sécurité des systèmes embarqués, pour le provisionnement sécurisé de sa gamme RX de microcontrôleurs 32 bits. Pour ce faire, Renesas va prendre en charge l'architecture Secure Deploy que Secure Thingz a créée pour simplifier les implémentations de sécurité dans les chaînes de valeur de conception et de fabrication.

Autre fournisseur de microcontrôleurs qui s'est associé à un fournisseur de solutions de sécurité embarquée : [STMicroelectronics](#). Le fabricant de puces collabore avec Arilou Information Security Technologies pour créer une configuration de sécurité multicouche où matériel et logiciels se complètent pour surveiller les flux de données et détecter les anomalies de communication.

La série [SPC58](#) Chorus de microcontrôleurs automobiles 32 bits de STMicro embarque un module de sécurité matériel (HSM) qui protège les informations de sécurité sensibles comme les clés cryptographiques, assurant ainsi une protection contre les intrusions via les bus de communication dans les applications de carrosserie automobile et de passerelle. Les modules HSM offrent la base matérielle fiable pour faciliter les communications sécurisées, les mises à jour sans fil et le démarrage sécurisé.

ST a ajouté le logiciel Intrusion Detection and Prevention System (IDPS) d'Arilou à sa série de microcontrôleurs automobiles SPC58 Chorus afin de détecter les anomalies de trafic et de former une couche supplémentaire de protection contre les cyberattaques (Figure 2). IDPS est une solution logicielle conçue pour surveiller le bus de données (CAN) et détecter les anomalies dans les schémas de communication des calculateurs (ECU) dans les conceptions automobiles.

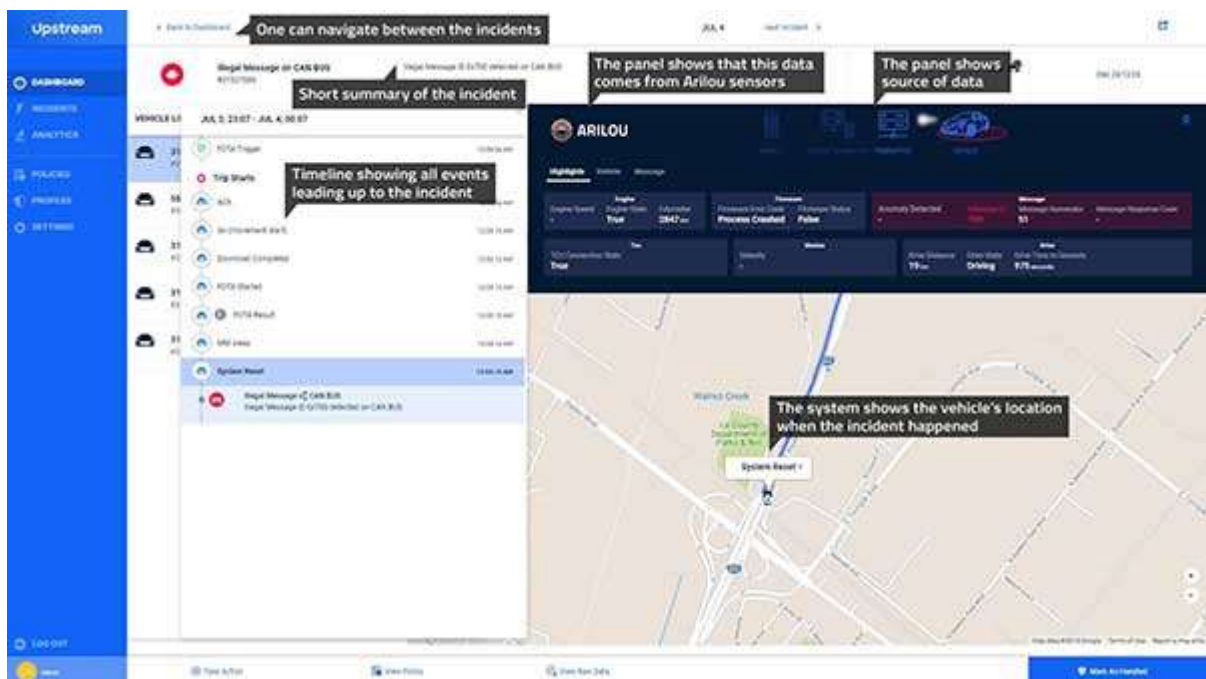


Figure 2. Manière dont le logiciel IDPS détecte les anomalies de trafic et d'autres anomalies sur la route. (Source de l'image : Arilou)

Microcontrôleurs de sécurité spécialisés

La section ci-dessus a donné un aperçu des microcontrôleurs qui intègrent des capacités de sécurité pour contrer les attaques physiques et distantes. Cette section va expliquer le fonctionnement des microcontrôleurs de sécurité spécialisés, souvent appelés « éléments sécurisés », qui agissent comme une puce auxiliaire du microcontrôleur principal tout en étant reliés via une interface I²C ou à un fil.

Les éléments sécurisés, qui prennent en charge les microcontrôleurs sans fonctionnalités de sécurité, s'appuient sur du matériel spécialement conçu afin d'offrir une structure de sécurité contre un large éventail de menaces. Simples et abordables, ces éléments déchargent le microcontrôleur ou le processeur principal des tâches liées à la sécurité, comme le stockage de clés, l'accélération cryptographique, etc. C'est pourquoi ils sont également connus sous le nom

de « coprocesseurs de sécurité ».

Dans un élément sécurisé, tous les blocs modulaires de sécurité fonctionnent avec une limite commune, qui isole les clés d'authentification des logiciels et empêche ainsi les pirates informatiques de mener des attaques visant le cycle d'alimentation, les horloges ou encore les canaux auxiliaires. L'importation de clés et de certificats de sécurité dans des éléments sécurisés en usine prévient également le vol d'IP, le clonage de conceptions et la contrefaçon de produits. Prenons, par exemple, l'élément sécurisé [ATECC608A](#) de [Microchip](#) (Figure 3), qui présente un générateur de nombres aléatoires (RNG) pour générer des clés uniques tout en respectant les dernières exigences du National Institute of Standards and Technology (NIST). Il inclut également des accélérateurs cryptographiques comme AES-128, SHA-256 et ECC P-256 pour l'authentification mutuelle.

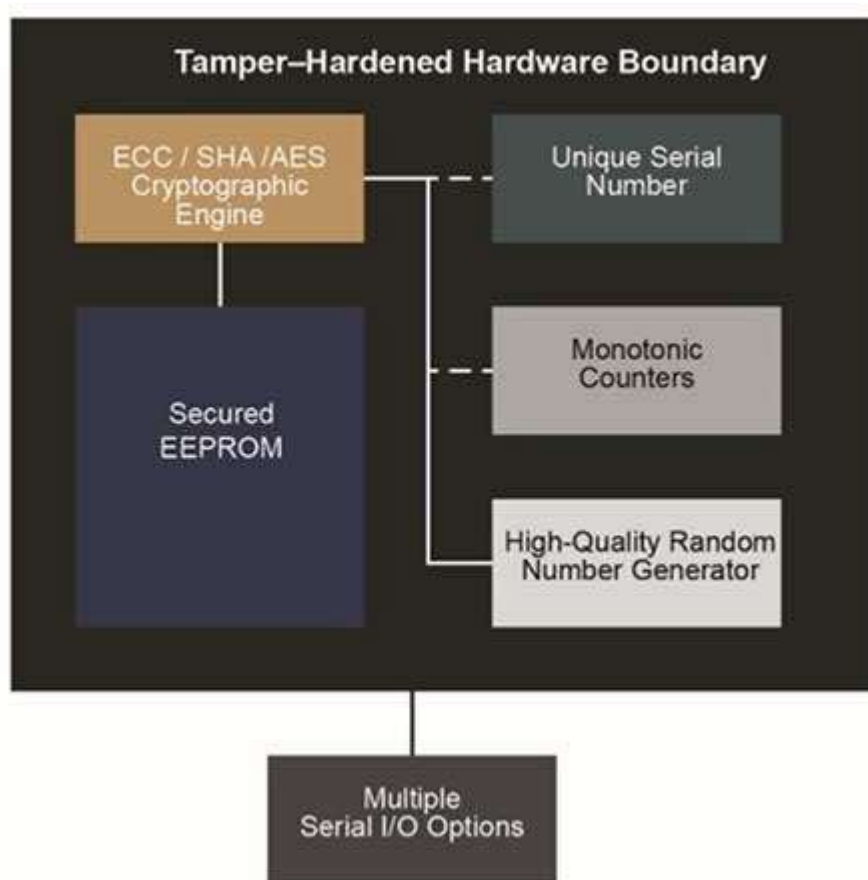


Figure 3. Schéma fonctionnel de l'élément sécurisé ATECC608A. (Image : Microchip Technology)

Enfin, la mémoire ROM sécurisée pour le stockage de clés permet de créer un environnement immuable qu'il est difficile pour les pirates informatiques et les usurpateurs d'identité d'altérer, ce qui empêche les intrusions et les attaques par canal auxiliaire. Collectivement, l'élément sécurisé ATECC608A offre des services allant du démarrage sécurisé à la validation sans fil pour sécuriser le stockage et le transfert de clés pour l'IoT et l'authentification des services cloud.

Le microcontrôleur [SAM L11](#) de Microchip (Figure 4) est un autre dispositif à faible coût spécialisé dans les implémentations de sécurité, qui protège les nœuds IoT soumis à des contraintes de puissance contre les menaces comme l'injection de défauts et les attaques par canal auxiliaire. Il extrait les détails de sécurité de faible niveau à l'aide d'une interface utilisateur graphique (GUI) modulaire qui permet aux développeurs de choisir les fonctionnalités de sécurité pertinentes. L'implémentation de la sécurité embarquée est ainsi facilitée.

SAM L11 Use Cases

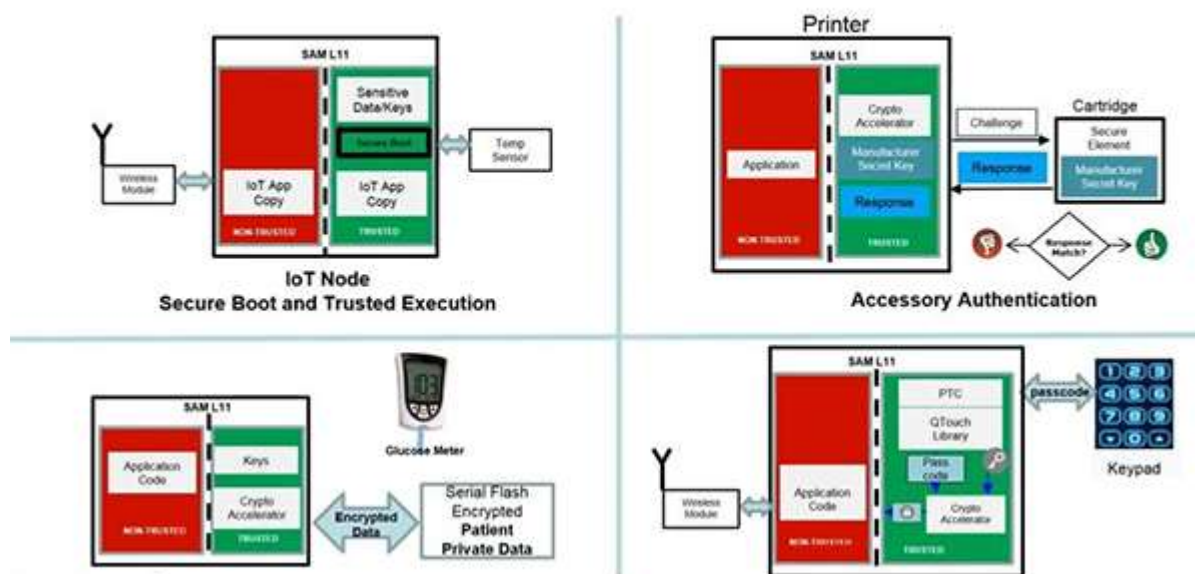


Figure 4. Quatre cas d'utilisation de sécurité employant le microcontrôleur de sécurité SAM L11. (Image : Microchip Technology)

Les fonctionnalités de sécurité que le SAM L11 extrait incluent des services de provisionnement tiers. Il intègre également la technologie TrustZone d'Arm qui isole le code sécurisé et non sécurisé dans un microcontrôleur. Par ailleurs, le SAM L11 rationalise les besoins de sécurité du nœud IoT tout en se connectant aux services cloud comme Amazon Web Services (AWS). Le microcontrôleur [LPC5500](#) de [NXP](#), spécialement conçu pour les applications périphériques IoT, constitue un autre exemple de microcontrôleur basé sur la sécurité. Il utilise des clés uniques au dispositif pour créer une base matérielle fiable immuable. Les clés peuvent être générées localement par une fonction physique inclonable (PUF) basée sur SRAM qui permet des transactions en boucle fermée entre l'utilisateur final et le fabricant OEM. Cette opération élimine le besoin de manipuler des clés tierces.

Outils de sécurité spécialisés

Même si les microcontrôleurs centrés sur la sécurité comme l'ATECC608A englobent des éléments de sécurité permettant de créer un écosystème fiable, ils ne répondent pas à l'isolement logiciel. Aujourd'hui, alors que la quantité de logiciels s'exécutant sur des microcontrôleurs ne cesse de croître, les développeurs doivent protéger une importante base de codes contre les attaques malveillantes.

Les dispositifs IoT, par exemple, ont des piles de protocoles pour Wi-Fi, Bluetooth, TLS, etc., et la corruption des piles de protocoles peut impacter le fonctionnement des dispositifs sans que les pirates informatiques volent les clés de sécurité. Cela requiert une séparation entre le code stratégique et le code non stratégique, afin de placer les logiciels stratégiques dans un environnement sécurisé.

L'environnement [TrustZone](#) d'[Arm](#) (Figure 5) sépare le code stratégique et les piles de protocoles des logiciels de systèmes d'exploitation (OS) complexes et des bases de codes importantes, ce qui empêche les portes dérobées de micrologiciels donnant accès aux zones de stockage de clés de sécurité. Il crée plusieurs domaines de sécurité logicielle pour restreindre l'accès à la mémoire, aux périphériques et aux composants E/S spécifiques dans le microcontrôleur.

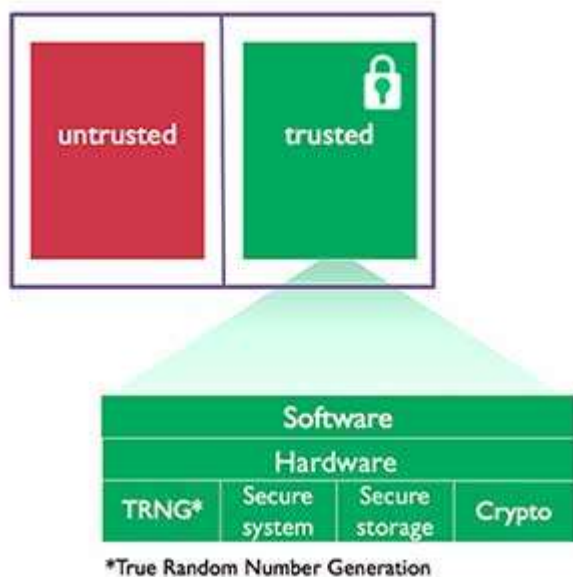


Figure 5. Structure de base de la technologie TrustZone pour isoler les logiciels dans des zones sécurisées et non sécurisées. (Source de l'image : Arm)

Les trois microcontrôleurs de sécurité mentionnés ci-dessus, l'ATECC608A, le SAM L11 et le LPC5500 (Figure 6), intègrent la technologie TrustZone pour séparer le code sécurisé et le code non sécurisé. En outre, l'élément sécurisé ATECC608A peut fonctionner avec n'importe quel microcontrôleur équipé de la technologie TrustZone.

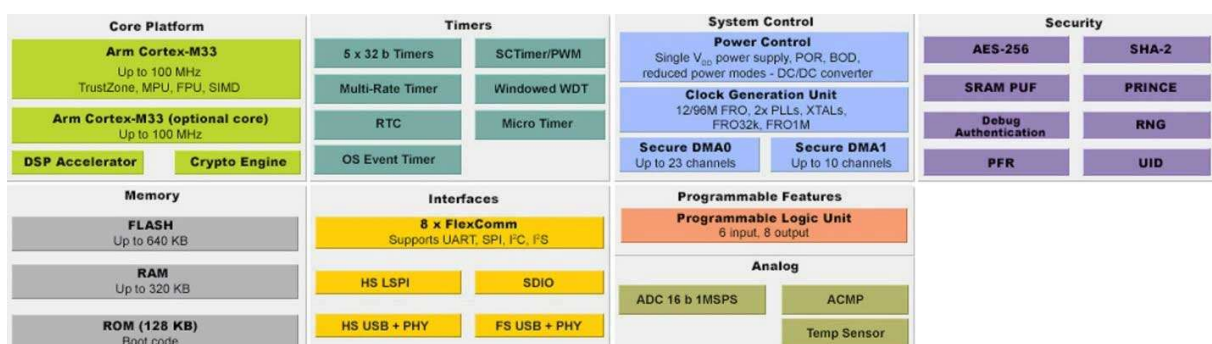


Figure 6. La technologie TrustZone dans le microcontrôleur LPC5500 est fournie avec le processeur Arm Cortex M-33, illustré en haut à gauche du schéma. (Source de l'image : NXP)

Il est aussi bon de mentionner ici que les microcontrôleurs de sécurité et la technologie TrustZone se complètent dans le sens où TrustZone requiert une protection matérielle, et les microcontrôleurs comme l'ATECC608A et le SAM L11 facilitent cela dans un contexte de conception IoT. D'autre part, TrustZone aide à créer un environnement logiciel compact dans les conceptions embarquées centrées sur les microcontrôleurs.

Conclusion

L'anatomie des microcontrôleurs de sécurité illustre la manière dont ils simplifient l'implémentation de la sécurité embarquée pendant la phase de conception, et comment ils permettent de contourner la rude courbe d'apprentissage en termes d'expertise en technologies de sécurité. Ces microcontrôleurs spécialisés réduisent également les coûts et la consommation énergétique, deux considérations majeures dans les conceptions IoT soumises à de nombreuses

contraintes.

Alors que le lancement des dispositifs IoT est plus rapide que le déploiement sécurisé de ces conceptions connectées, les microcontrôleurs de sécurité offrent une solution viable pour faire face aux cybermenaces sur plusieurs fronts. Ils fournissent une solution simplifiée équipée d'un écosystème de conception de sécurité pour faciliter les environnements de développement de type pointer-cliquer.