Bluetooth devient plus SMART avec NFC intégré

Par Heiner Tendyck, Toshiba Electronics Europe

Bluetooth Smart étend la portée de l'Internet des objets (IoT) et, combiné au NFC (Near Field Communication, ou communicaion en champ proche), il constitue la technologie idéale pour connecter l'IoT aux smartphones et aux tablettes pour créer l'Internet de Tout.

La troisième vague de la révolution Internet

L'Internet des objets est parti pour éclipser la pénétration pourtant massive de l'Internet "classique" qui regroupe des ordinateurs de bureau et des dispositifs portables. Il y a désormais plus de 11 milliards de connexions Internet aux ordinateurs de bureau et aux mobiles, mais l'IoT pourrait connecter 28 milliards "d'objets" à Internet d'ici 2020 selon Goldman Sachs. D'autres estimations évoquent même près de 50 milliards de connexions.
L'IoT promet de formidables opportunités de supervision et de contrôle des environnements, d'amélioration de la productivité industrielle, et d'accroissement des standards de vie. Il s'agit de la troisième vague de la révolution Internet, après celle de l'Internet fixe et de l'Internet mobile, et elle commence vraiment à décoller. Grâce à cette dernière brique, on va assister à l'avènement ultime : celui de l'Internet de Tout (IoE ou Internet of Everything en anglais).
L'IoE permet aux utilisateurs d'accéder à l'intelligence issue de l'IoT où qu'ils se trouvent, à tout moment, avec n'importe quel dispositif, en offrant de tirer parti de tout le potentiel de la connectivité de l'ensemble de la société. Cependant, d'importants défis techniques tels que la facilité d'utilisation, la gestion d'énergie ou la sécurité doivent être surmontés, si cette vision doit devenir réalité.

Bluetooth et plus

L'IoE recouvre tous les domaines de la connectivité, comme les maisons intelligentes, les usines intelligentes, les "wearables" et les véhicules connectés, y compris les véhicules autonomes.
Avec l'extension de l'Internet, la connectivité sans-fil sera déterminante pour assurer la facilité d'utilisation et pour pouvoir se connecter n'importe où.
Pour la connectivité IP-adressable à proximité du backbone (épine dorsale d'Internet), le Wi-Fi constitue une norme haut-débit sécurisée et bien adaptée.
D'un autre côté, pour l'accès local à certains dispositifs comme des capteurs ou des actionneurs à la marge de l'IoT, plusieurs normes telles que Bluetooth® Low Energy (Bluetooth LE), ou certains protocoles tournant sur les couches radio IEEE 802.15.4, peuvent convenir selon les besoins de l'application.
Les normes à base Bluetooth ont le double avantage d'être bien maîtrisées par les communautés techniques, et d'être faciles à utiliser pour les consommateurs, et continueront donc d'être très largement supportées dans les environnements mobile et automobile, en particulier pour les applications audio ainsi que pour l'informatique personnelle.
Etant donné que le support Bluetooth est plus ou moins universel sur tous les smartphones actuels, un concentrateur de capteurs est déjà aux mains de millions d'utilisateurs du monde entier, et peut donc servir à toute une série d'applications grand-public ou professionnelles, allant de la domotique aux réseaux personnels.
L'ubiquité est sans aucun doute un atout majeur : les chiffres d'ABI Research indiquent que trois milliards de périphériques Bluetooth ont été livrés en 2014, et que la quantité annuelle devrait atteindre 4.6 milliards d'ici 2018. On estime que les téléphones mobiles représentent moins de 50% du total.

Bluetooth LE (Low Energy, ou basse énergie) a été introduit en version 4.0 et en est aujourd'hui à la version 4.2, qui intègre un certain nombre de mises à jour de sécurité et sert de support au trafic IP. Il est conçu pour répondre aux besoins des applications IoT, grâce en particulier à une très faible consommation et à l'établissement rapide de la connexion, qui permet aux noeuds d'un réseau sans-fil d'échanger de petits volumes de données.

Pour parvenir à cela, le Bluetooth LE optimise certains facteurs comme le débit, le nombre de canaux

radio et les temps de connexion/déconnexion. Le Bluetooth LE permet de configurer la connexion et d'être prêt à transférer des données dans la zone de sécurité multicast du dispositif, plusieurs dizaines de fois plus vite que le Bluetooth "classique".
Les modifications présentes dans Bluetooth LE réduisent sensiblement le courant consommé, de quelques milliampères pour une radio Bluetooth classique, à quelques microampères seulement.
Les noeuds IoT Bluetooth Smart peuvent fonctionner pendant des mois, voire même des années, à partir d'une petite pile plate type "pièce de monnaie" sans remplacement ni recharge.
Les applications Bluetooth LE typiques sont par exemple des noeuds de capteurs transmettant des données d'échantillonnage, des clapets intelligents transmettant des alertes au sein d'une usine, des dispositifs médicaux personnels transmettant les signaux vitaux d'un patient, des bio-détecteurs équipant des équipements de fitness, ou des vêtements de sport intelligents transmettant des données comme le niveau d'activité ou la fréquence cardiaque, ou encore un clavier transmettant ses données de frappe.
Les dispositifs supportant Bluetooth LE sont dits "Bluetooth Smart" par le groupe d'intérêt Bluetooth (SIG).
Par ailleurs, certains dispositifs peuvent supporter à la fois Bluetooth classique et Bluetooth LE, et dans ce cas sont dits "Bluetooth Smart Ready".
Il s'agit typiquement de smartphones ou de tablettes, qui jouent le rôle de concentrateurs et qui sont capables de se connecter à des dispositifs tels que des capteurs, comme illustré en Figure 1. Les futures versions de Bluetooth LE, telles que Bluetooth 5.0, permettront des débits plus élevés, sur des distances plus longues, avec un niveau de consommation de type Bluetooth Smart.



Figure 1.

Les dispositifs Bluetooth Smart Ready communiquent avec les dispositifs Bluetooth Smart ou Bluetooth classique.

Les dispositifs Bluetooth Smart et Smart Ready sont devenus plus faciles à implémenter avec l'arrivée de modules et de CI compacts.
Les concepteurs peuvent choisir l'approche répondant le mieux aux besoins de leur projet en termes de taille de circuit et de nombre de composants, de complexité technique, de temps de certification, et de "time-to-market" (délai de commercialisation).

Ajout de NFC pour un accès pratique et sécurisé
Bluetooth Smart intègre un cryptage AES-128, qui offre une résistance robuste à l'écoute illicite et au décryptage des paquets interceptés. D'un autre côté, la sécurité et la facilité d'utilisation peuvent être améliorées grâce au NFC (Near Field Communication, ou communication en champ proche) pour améliorer certaines tâches comme le "pairing" (appariement) (Figure 2).



Figure 2.

Profiter du NFC pour faciliter le pairing sécurisé du dispositif
Le NFC exige que les dispositifs se trouvent à proximité l'un de l'autre, typiquement distants de seulement quelques centimètres. Le NFC permet d'éviter les problèmes "d'intrus dans le passage" et évite que des dispositifs indésirables ne se connectent à l'insu de l'utilisateur en transmettant des informations de pairing comme les adresses des dispositifs Bluetooth hors de la bande et de la distance autorisées. Le pairing NFC est facile et évident, et se fait généralement en mettant les deux dispositifs brièvement en contact.
Le NFC simplifie aussi l'ajout de noeuds à un réseau maillé Bluetooth LE, par exemple pour étendre un réseau de capteurs sans-fil, ou pour ajouter de nouveaux éclairages à LED dans une zone contrôlée sans-fil. Avec certaines applications comme les compteurs intelligents qui peuvent être lus manuellement à intervalles de plusieurs semaines ou de plusieurs mois, le compteur peut rester hors-tension jusqu'à ce

qu'il soit interrogé en approchant un lecteur NFC ou un mobile doté d'une fonction NFC à proximité du compteur. L'énergie initiale est fournie par l'antenne NFC, et le dispositif BLE peut rester en mode sommeil profond pour minimiser la consommation. Une fois le dispositif lecteur identifié, une connexion peut être établie grâce à Bluetooth LE pour lire les données dans la mémoire du compteur.
En outre, il existe de nombreuses opportunités de contrôle d'accès sans-fil, pour répondre à la vision du marché de la sécurité, qui est demandeur de solutions d'authentification pratiques et sans-contact, offrant à la fois une sécurité et une souplesse accrues, et une meilleure expérience utilisateur.
Les leaders du contrôle d'accès électronique implémentent désormais des plateformes de sécurité bien connues comme SEOS, sur Bluetooth Smart et NFC à l'aide de techniques telles l'émulation de carte hôte. Ceci permet d'héberger des clés électroniques sur les smartphones et ainsi de surmontes certains points faibles des clés à carte à puce, tout en permettant d'imaginer de nouvelles applications à certains secteurs comme l'hôtellerie, le contrôle d'accès ou la sécurité domestique.
Les clients d'hôtels, par exemple, pourront s'enregistrer et se rendre directement à leur chambre, sans attendre que l'équipe de réception ne programme une carte d'accès.
Le smartphone du client est appairé de manière sécurisée avec la serrure de la porte par NFC, et la clé virtuelle est automatiquement détruite à l'issue du séjour. Pendant le séjour du client, des balises Bluetooth Smart peuvent fournir une assistance et envoyer des notifications de services et d'offres directement vers le smartphone du client, ou suivre ses dépenses à des fins de facturation et de marketing.
Parallèlement, les applis de sécurité domestique sur smartphone offrent aux propriétaires la possibilité d'envoyer des clés temporaires encodées numériquement à d'autres personnes comme des invités, une nounou ou des voyageurs de commerce, afin de permettre aux visiteurs d'utiliser leurs smartphones pour accéder à certaines zones de la propriété, à certaines heures. La clé peut être détruite à la discrétion du propriétaire, sans aucune crainte de perte, de mauvaise utilisation ou de vol.

Facteur essentiel au développement
Pour faciliter le développement de dispositifs tels que smartphones, capteurs intelligents, verrous, compteurs et autres matériels combinant la souplesse de connexion réseau du Bluetooth LE et la simplicité et la sécurité du NFC, Toshiba a développé le CI "tag" (étiquette) Bluetooth Smart + NFC, TC35670FTG.
Ce CI intègre un noyau CPU ARM et peut être utilisé en mode "host-less" (sans hôte) ou comme esclave connecté à une unité de traitement principale. Il fait partie d'une famille comprenant aussi le CI Bluetooth Smart, TC35667, permettant ainsi de réutiliser facilement de l'IP Bluetooth pour des projets sans tag. Cette famille bénéficie du support de micrologiciels embarqués certifiés Bluetooth, et d'un logiciel API portable et facile à utiliser.
Toshiba a également collaboré avec plusieurs partenaires pour produire des modules Bluetooth normalisés qui simplifient la conception et accélèrent le "time-to-market" (délai de commercialisation).
Le TC35670 intègre des circuits RF Bluetooth 2.4 GHz et bande de base, supportant les fonctions Bluetooth HCI (Host Control Interface, ou interface de commande d'hôte) et des fonctions de profil Bluetooth Low Energy, ainsi qu'une étiquette à la norme NFC Forum Type 3, combinant interface sans-fil, interface filaire I2C, et interface sans-contact compatible NFC Forum. Les passations douces du NFC au Bluetooth LE permettent au dispositif de supporter le pairing NFC, qui permet d'établir des connexions facilement.
Un dispositif contenant ce CI peut être mis en contact avec un autre dispositif compatible Bluetooth LE et NFC, comme un smartphone, pour transférer les clés de sécurité Bluetooth et l'adresse du dispositif, par l'intermédiaire de l'étiquette NFC, pour réaliser le pairing Bluetooth.

La transmission Bluetooth peut alors commencer immédiatement
En mode étiquette NFC, l'EEPROM embarquée sur la puce du CI peut être consultée à travers les interfaces filaire ou sans-fil. En outre, la RAM embarquée sur la puce autorise l'utilisation d'un mode "traversant", qui permet au processeur hôte de récupérer via l'interface filaire I2C, les données reçues par l'interface sans-fil et inversement.

Les Figures 3a, 3b et 3c comparent les modes filaire, sans-fil et traversant.

Pour passer en mode "traversant", le dispositif reçoit une commande Write (écriture) par l'interface sans-fil, puis stocke les données de bloc en RAM avant d'envoyer une réponse via l'interface sans-fil. Lors du passage en mode "traversant", l'interface sans-fil est désactivée et les données de bloc sont rendues disponibles via l'interface filaire.

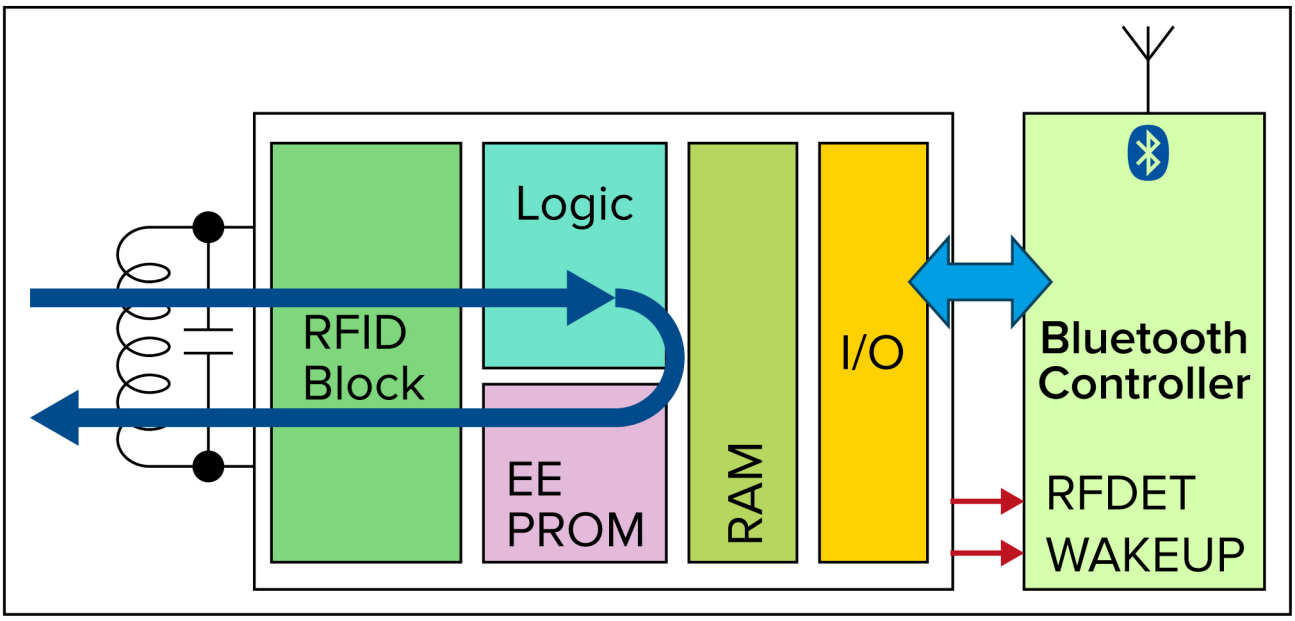


Figure 3a. TC35670 en mode sans-fil.

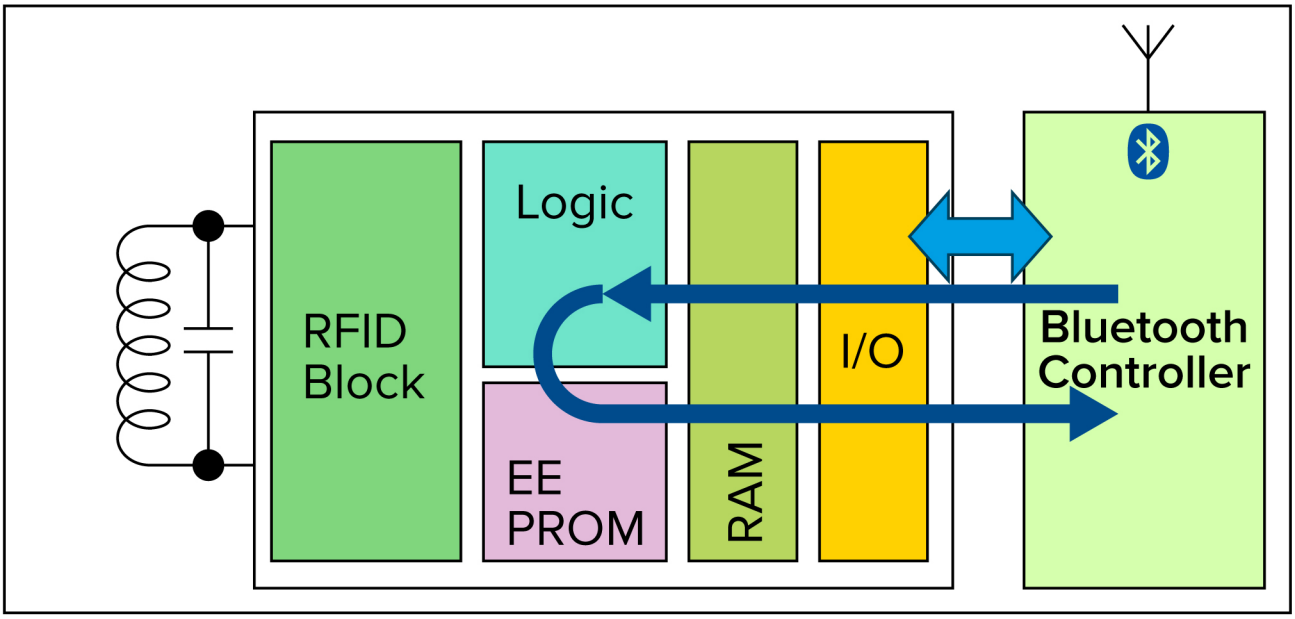


Figure 3b. TC35670 en mode filaire.

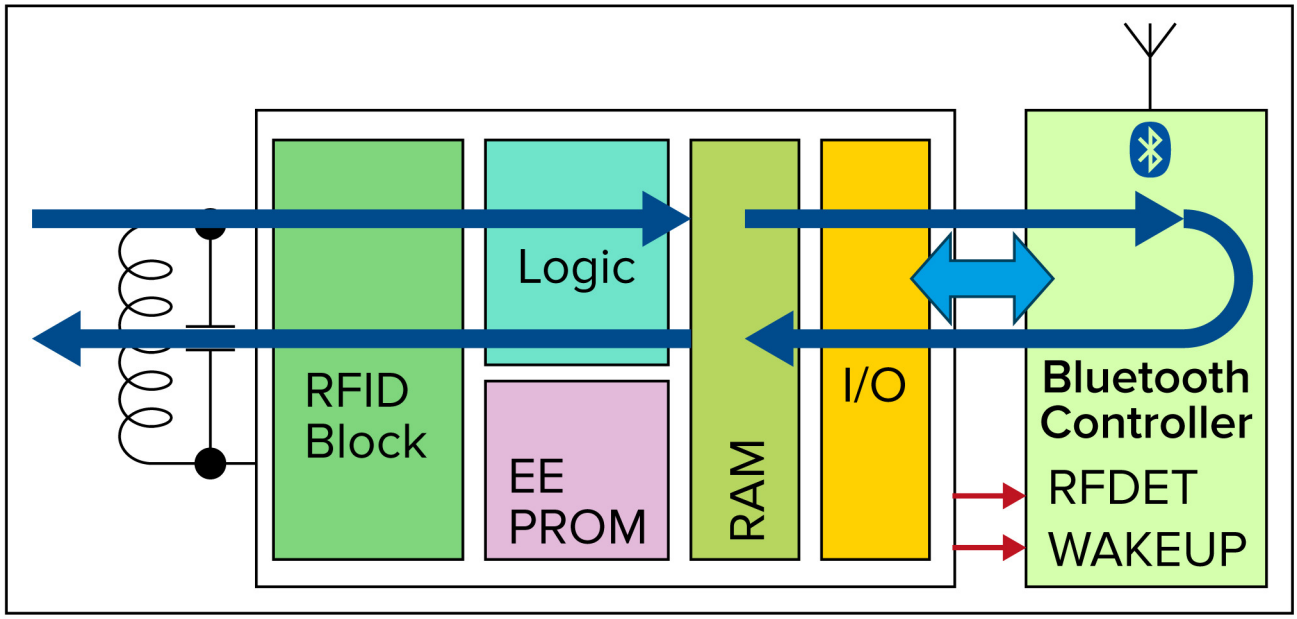


Figure 3c. TC35670 en mode traversant.

Le convertisseur DC-DC et le LDO intégrés permettent de minimiser le nombre de composants externes, et tout le dispositif ne consomme que très peu, avec un courant crête de 5.9 mA et un courant en mode sommeil profond extrêmement faible de seulement 0.1 µA. L'alimentation interne est capable de sortir du mode veille dès qu'un dispositif distant demande une connexion, ce qui permet un fonctionnement sans batterie.

Conclusion

Bluetooth Smart a été développé pour la génération IoT (Internet of Things, ou Internet des objets), et surmonte les problèmes critiques de consommation, qui ont jusqu'ici empêché le Bluetooth classique de séduire au delà des marchés grand-public et automobile.
Une fois combiné à NFC, Bluetooth Smart devient une solution encore plus puissante pour les applications où un pairing facile est nécessaire sans que la sécurité ne soit compromise.
Les dispositifs Bluetooth Smart et Smart Ready vont jouer un rôle majeur dans l'unification de l'IoT et de l'Internet "classique" pour aboutir à l'Internet de Tout.