# Sécurité et sûreté, les deux piliers des dispositifs médicaux embarqués

Auparavant, la sécurité et la sûreté des dispositifs médicaux embarqués faisaient généralement l'objet de réflexions à l'issue du processus de conception. Il n'est désormais plus acceptable de procéder ainsi. C'est dès la conception d'un dispositif médical que la sécurité et la sûreté de ces produits doivent être analysées, comme l'explique ici Microchip.

Tous les jours on apprend que des attaques informatiques ont eu lieu ou que de nouvelles vulnérabilités ont été découvertes dans tout type d'équipements connectés. Malheureusement, les dispositifs médicaux ne sont pas plus à l'abri que les autres de ces attaques. Alors qu'ils constituent ce que l'on appelle l'IoMT (Internet of Medical Things ou Internet des objets médicaux), leur vulnérabilité, et donc la vulnérabilité des données des patients, ne font que croître. Les inquiétudes concernent la responsabilité juridique ainsi que la protection de la marque, de la propriété intellectuelle, des revenus des entreprises concernées et, bien entendu, des données personnelles médicales. A ce niveau, les mesures de sécurité qui doivent être intégrées par conception dans un dispositif médical embarqué dépendent de l'application et des exigences relatives à son utilisation.

La mise en œuvre de conceptions assurant la surveillance de patients à distance et le bon suivi de leurs traitements font partie des premières raisons pour connecter les dispositifs médicaux au cloud. Malheureusement, une fois le dispositif connecté à des applications dans le nuage, il peut devenir une cible pour les pirates informatiques. Deux exemples de menaces de piratage informatique courantes pour ces appareils médicaux sont l'attaque par déni de service (DoS) et l'attaque dite « man-in-the-middle » ou attaque de l'homme du milieu.

Une attaque par déni de service se produit lorsque des pirates informatiques prennent le contrôle d'un système connecté de télésurveillance de patients et inondent un serveur cloud d'une avalanche de requêtes redondantes pour le saturer et ainsi l'empêcher de répondre aux requêtes légitimes. Le pire scénario est une attaque par déni de service distribué. Un exemple d'une telle attaque est le cas où tous les moniteurs connectés des patients au sein d'un hôpital sont piratés et envoient tellement de demandes redondantes qu'ils saturent le seul serveur cloud censé prendre en charge les moniteurs.

Un exemple d'attaque de l'homme du milieu apparaît lorsqu'un pirate informatique accède par exemple à une pompe à perfusion connectée servant à administrer de la morphine au goutte-à-goutte à un patient. Le pirate peut alors intercepter les communications entre la pompe et le serveur et ainsi envoyer de fausses informations à l'un ou à l'autre. En d'autres termes le hacker, en prenant le contrôle de la pompe, se trouve en mesure de ne pas administrer le médicament au patient, ou au contraire de provoquer une overdose. Ces deux scénarios s'avérant bien évidement tragiques pour le patient et la réputation de l'hôpital (photo A) Traditionnellement, les mesures pour contrer ces attaques reposaient entièrement sur des solutions logicielles. Toutefois aujourd'hui, ces mesures anti-piratage sont plutôt mises en œuvre à l'aide de solutions matérielles, à la fois plus rapides et plus économiques.

Pour cela, il faut installer des puces de sécurité. Dans ce cadre, les concepteurs de dispositifs médicaux doivent décider très tôt dans le cycle de conception quelles fonctions et quels niveaux de sécurité sont nécessaires à leur conception, et ensuite sélectionner les puces de sécurité capables de mettre en œuvre ces fonctions. Les circuits qui assurent cette sécurité sont en premier lieu des microcontrôleurs et des microprocesseurs à chiffrement, couplé à des éléments sécurisés et à un micrologiciel intégré. Cet ensemble lié à une architecture de sécurité gérée dans le cloud procure des fonctions de sécurité et des mesures anti-piratage assurant la confidentialité et l'intégrité des données, ainsi que l'authentification des dispositifs médicaux connectés (voir encadré).

Un type de puce capable de réduire à la fois les risques d'attaque par déni de service et de l'homme du milieu est généralement appelé composant sécurisé ou dispositif de crypto-authentification (authentification chif-

AUTEUR

Marten L. Smith, responsable du développement commercial, groupe Produits médicaux, Microchip Technology.

## EXEMPLES DE MICROCONTRÔLEURS À SÉCURITÉ FONCTIONNELLE

■ Des caractéristiques sont potentiellement importantes pour détecter les défaillances de conception d'un dispositif médical :

■ Une bibliothèque de diagnostic fonctionnant aussi bien à la réinitialisation qu'en cours d'exécution, pour s'assurer de l'absence de défaillances dans le système.

■ Des outils de développement de microcontrôleurs qui peuvent être considérés comme sûrs, afin de ne pas introduire de défaillances dans le système. La qualification des outils de développement par rapport aux normes de sécurité fonctionnelle est un élément important de tout cela.

■ La conception à l'aide de microcontrôleurs dotés de périphériques intégrés et intelligents permet de renforcer la fiabilité et la capacité de surveillance des applications critiques au niveau sécurité.

frée). Typiquement, il s'agit de petits circuits – en boîtier UFDN ou SOIC à 8 broches– que l'on peut ajouter à la conception d'un dispositif médical connecté. Cette puce à éléments sécurisés fonctionne comme un compagnon du microcontrôleur utilisé.
Ces puces à éléments sécurisés disposent généralement de fonctions comme un générateur de nombre aléatoire de qualité, un système de chiffrement matériel, un stockage sécurisé des clés et une fonction d'amorçage sécurisé du microcontrôleur. Elles proposent en plus des mesures anti-piratage comme la protection contre les attaques par canal auxiliaire ou encore l'antieffraction active, qui réduisent les risques potentiels dus à des « portes dérobées » liées à des faiblesses logicielles (ports ouverts). Une bonne image pour imaginer ces puces à éléments sécurisés est de penser à un coffre-fort qui protège des secrets, secrets qui sont placés dans ce coffre an moment de la fabrication de la puce.

## Les clés, le cœur de la sécurité

Dans le domaine des puces à éléments sécurisés, les secrets s'appellent des clés. Les clés peuvent être vues comme les identifiants de la puce qui autorisent ou non l'accès au serveur ou lui indiquent qu'il peut autoriser la connexion au dispositif médical. Ce processus de consentement à la connexion est appelé authentification.
Le processus d'insertion des clés dans la puce est appelé « attribution de clés ». Cette phase d'attribution peut être considérée comme une préprogrammation. Elle est réalisée dans une installation sécurisée du fabricant de puces. Ce processus d'attribution sécurisée ne permet à aucun humain d'accéder aux clés. Celles-ci ne sont donc jamais exposées.Conséquence, le dispositif médical est physiquement sécurisé lors de son utilisation à l'hôpital, dans les cliniques ou au domicile du patient. L'attribution sécurisée élimine également le risque qu'un fabricant de cartes électroniques tiers puisse voler les clés stockées dans la puce à éléments sécurisés.
Lorsque le dispositif médical est en service et qu'il veut se connecter au cloud, il passe aussi par un processus d'authentification avec le serveur. Au cours de ce processus, le serveur cloud envoie une énigme à la puce à éléments sécurisés qui, à son tour, propose une réponse calculée à l'aide d'une clé secrète qu'elle est seule à détenir. Si la réponse du composant sécurisé est correcte, l'accès au serveur lui est accordé.

● A. Lorsqu'un hacker prend le contrôle d'équipements médicaux en fonctionnement, une pompe par exemple, il peut mettre les patients en danger de mort.

L'authentification sécurisée à un serveur cloud est un processus complexe que les concepteurs de dispositifs médicaux devant les mettre en œuvre ne connaissent pas toujours bien. Pour répondre à cela, la puce à éléments sécurisés peut aussi être préconfigurée et se voir attribuer, avant de quitter l'usine du fournisseur de puces sécurisées, les identifiants qui lui permettront de s'authentifier auprès des services cloud les plus populaires comme Amazon Web Services (AWS) IoT Core, Microsoft Azure IoT Hub ou Google IoT Core. Le recours à un service d'attribution évite ainsi aux concepteurs la complexité, les retards de conception et les coûts élevés, souvent associés à une implantation ultérieure des clés par leurs propres soins.

## La sûreté de fonctionnement, le second cœur des dispositifs médicaux embarqués

Parallèlement, les exigences de sûreté et de sécurité fonctionnelle se sont renforcées. Ici les processus et les fonctions liés à la sûreté de fonc-

● B.- Garantir la sûreté des dispositifs médicaux est essentiel pour les concepteurs car ces systèmes peuvent avoir un impact direct sur la santé des patients qui en sont tributaires. Tout comme la sécurité, la sûreté doit, elle aussi, être prise en compte dès le début de la conception de tout dispositif médical.

tionnement détectent les défaillances de systèmes ou de produits électriques et/ou électroniques afin d'éviter les risques de blessure, de dommage et d'événements potentiellement dangereux pour la vie des utilisateurs. Ceci peut se faire de deux manières. La première est de réduire les risques de défaillance systémique au moment de la conception. La seconde est de permettre à la conception de détecter les défaillances aléatoires et de passer en mode protégé.

Une chose à garder en tête est que la sécurité fonctionnelle ne réduit pas le taux de panne global. Cet aspect est pris en compte par les processus de qualité de conception et de fabrication des différents composants utilisés, tant pour la conception que pour le dispositif médical lui-même. L'objectif d'une conception selon les normes de sécurité fonctionnelle est de transformer les défaillances dangereuses en défaillances sûres. Il s'agit également d'un processus permettant au concepteur de définir un niveau tolérable de défaillances dangereuses.

Les problèmes de sûreté d'appareils médicaux ont fait la part belle à des gros titres à caractère négatif dans la presse. Avec, comme avec la sécurité, des conséquences fortes en termes d'image. Garantir la sûreté des dispositifs médicaux est donc essentiel pour les concepteurs, car ces systèmes peuvent avoir un impact direct et immédiat sur la santé des patients qui en sont tributaires. Tout comme la sécurité, la sûreté doit elle aussi être prise en compte dès le début de la conception de tout dispositif médical (photo B).

Il existe de nombreuses normes de sécurité fonctionnelle applicables à différents secteurs. La sécurité de conception d'un dispositif médical intégré peut dépendre de sa conception selon une ou plusieurs de ces normes. Par exemple, les concepteurs d'appareils médicaux ont constaté qu'ils devaient non seulement concevoir leurs produits sur la base de la norme CEI 62304 relative au cycle de vie des logiciels, mais aussi intégrer la norme industrielle de sécurité fonctionnelle CEI 61508 à leur processus de conception. En fait, la norme CEI 62304 encourage tous ceux qui conçoivent selon cette norme à s'appuyer également sur la norme CEI 61508 comme source de bonnes pratiques, de techniques et d'outils logiciels.

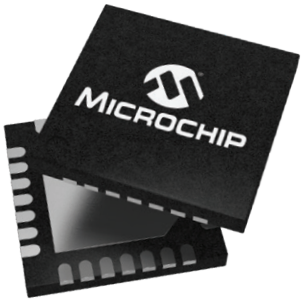
Il faut bien garder en tête que la sécurité fonctionnelle ne concerne pas seulement le matériel et le logiciel du dispositif médical, mais qu'elle englobe aussi l'ensemble du processus de conception et de l'écosystème pour que la conception soit sûre. Par exemple, les microcontrôleurs conçus pour les applications à sécurité fonctionnelle s'appuient sur des fonctions intégrées au niveau matériel, des bibliothèques de tests de diagnostic logiciel, des manuels de sécurité et des rapports FMEDA (Analyse des modes, effets et diagnostics des défaillances) selon la norme et le niveau de sécurité qu'ils doivent assurer. Les caractéristiques de cet écosystème aident non seulement à respecter les normes de sécurité, mais peuvent également jouer un rôle important dans la détection des défaillances lors de la mise au point de la conception. Les considérations de sécurité fonctionnelle doivent jouer un rôle important dans la sélection des microcontrôleurs que les concepteurs utilisent pour concevoir des dispositifs médicaux sûrs (voir encadré). ■

# Votre partenaire d'expérience pour concevoir vos dispositifs médicaux embarqués

## Un support de classe mondiale en ces temps difficiles

Depuis de nombreuses années, Microchip est le partenaire de confiance et d'expérience de tous les concepteurs et fabricants de dispositifs médicaux embarqués. Vous fournir les composants et le support pour vos dispositifs médicaux embarqués FDA Classe 1, 2 et 3 est notre seconde nature.

Si vous concevez ou fabriquez des dispositifs médicaux diagnostiques, thérapeutiques ou de soins intensifs, nous pouvons vous aider. Nous nous engageons à assurer l'avancement de votre conception et la continuité de votre fabrication. Donc, si vous vous souciez de questions d'approvisionnement ou si vous avez besoin de l'aide de nos spécialistes en conception embarquée ou en solutions médicales, nous sommes là pour vous aider.




**www.microchip.com/MedicalDeviceSupport**

MICROCHIP