

# Comment améliorer la sécurité

## des systèmes embarqués en cinq étapes

Par Franz Walkembach, **Global Senior Product Manager Automotive Solutions, Wind River**

Apparu en 2010, le ver Stuxnet fut le premier programme malveillant conçu spécifiquement pour s'infiltrer au sein d'une infrastructure industrielle et propager du code malicieux au cœur-même des automates programmables. Une telle attaque virale souligne la nécessité de renforcer les mesures destinées à protéger la sécurité des systèmes embarqués critiques, et tout particulièrement ceux qui contrôlent les infrastructures vitales, les complexes industriels, les réseaux de renseignement, les réseaux militaires ou les équipements médicaux.

Pendant longtemps, les systèmes embarqués ont fonctionné dans une relative autarcie et, de ce fait, ils ont été protégés contre la plupart des menaces de sécurité. Mais ces mêmes équipements sont aujourd'hui reliés à des réseaux d'entreprises, à des *clouds* publics, voire même à Internet. Cette connectivité généralisée conduit à des gains substantiels en termes de fonctionnalités et d'ergonomie, mais elle rend les systèmes embarqués plus vulnérables aux attaques, aux intrusions et autres piratages. A l'heure du « tout-connecté », la sécurité qui fut loin d'être le souci principal des concepteurs par le passé se hisse au rang des caractéristiques fondamentales des équipements. Dès lors, les mécanismes de sécurité, ou plus exactement de cyber-sécurité, doivent protéger les systèmes embarqués de toute attaque malveillante qui pourrait entraver un fonctionnement correct et sûr, tout particulièrement lorsque des vies humaines sont en jeu. Ces mêmes mécanismes doivent garantir l'intégrité des données transmises ou stockées lorsque celles-ci sont considérées comme sensibles.

Dans ces conditions, comment les concepteurs peuvent-ils concilier des contraintes de sécurité de plus en plus strictes avec les exigences d'un marché concurrentiel où les délais de mise sur le marché et les budgets de développement sont constamment revus à la baisse ? En fait, les démarches qui visent à garantir aux systèmes embarqués un niveau de sécurité toujours plus élevé peuvent être déclinées selon cinq étapes couvrant l'ensemble du cycle de vie des produits, de leur conception à leur maintenance en passant par les phases de développement, de tests et de déploiement.

### **Etape 1 : Mener une évaluation des menaces de bout-en-bout**

L'amélioration de la sécurité d'un système embarqué commence par une bonne identification des menaces potentielles. Ces menaces doivent être évaluées en procédant à une analyse complète du cycle de vie du produit, en envisageant en amont toutes les conditions d'utilisation de ce même produit, et en prenant en compte l'impact que les développeurs, les fabricants, les opérateurs, les distributeurs, les revendeurs et les utilisateurs finaux peuvent avoir sur la sécurité globale du système. Ici, la difficulté principale est de prévoir les vecteurs d'infection (i.e. les diverses manières dont une attaque malveillante peut être perpétrée) et d'anticiper les vulnérabilités (i.e. les faiblesses ou défauts matériels ou logiciels exploitables par un programme malveillant).

## **Etape 2 : Tirer parti de mécanismes évolués de sécurité déjà existants**

Un certain nombre de technologies et de méthodes de conception ont déjà été élaborées pour contrer les menaces toujours plus sérieuses qui guettent les systèmes embarqués connectés. Dans ce cadre, les concepteurs ont tout intérêt à s'orienter vers des briques de base commerciales, éprouvées et disponibles sur étagère (COTS) qui ont la capacité d'améliorer la sécurité de leurs équipements sans grever les coûts de développement. Les plates-formes de virtualisation embarquées figurent au nombre de ces briques de base : elles permettent via des mécanismes de partitionnement de répartir et d'isoler les logiciels dans des environnements d'exécution virtuels.

## **Etape 3 : Choisir une plate-forme d'exécution appropriée**

Pour un système embarqué, le choix d'une plate-forme d'exécution commerciale est absolument crucial. L'implantation de composants logiciels COTS préalablement testés, validés et certifiés selon des critères stricts de sécurité et de sûreté fonctionnelle peut accroître la sécurité globale d'un système et réduire les coûts de développement afférents. Soigneusement sélectionnés en fonction de ces critères, les couches de support des composants matériels, les hyperviseurs, les systèmes d'exploitation temps réel, les piles de protocoles de communication, les plates-formes de simulation virtuelle, les outils de développement peuvent grandement contribuer à l'élaboration efficace d'un équipement embarqué sécurisé.

## **Etape 4 : Sécuriser les applications**

Les systèmes embarqués modernes hébergent de multiples applications et voient leurs fonctionnalités évoluer durant tout le cycle de vie de l'équipement grâce à des mises à jour et des mises à niveau matérielles et logicielles. Susceptibles, de ce fait, d'être les cibles de codes malicieux ou de vols de données, les applications doivent donc impérativement être sécurisées. Ceci peut être fait via la technique dite des « listes blanches », beaucoup moins gourmande en ressources que celles des « listes noires » et donc mieux adaptée aux contraintes propres à l'embarqué. Ce mécanisme autorise le téléchargement et l'installation des seules applications dont l'exécution est reconnue comme sûre.

## **Etape 5 : Opter pour un support couvrant l'intégralité du cycle de vie**

Les menaces de sécurité évoluent dans le temps, les parades aussi. Les systèmes embarqués doivent donc pouvoir être mis à niveau sur site, afin d'anticiper de futurs problèmes de sécurité. Aussi l'intégration d'une politique globale de sécurité dans la gestion du cycle de vie du produit s'avère-t-elle critique, ne serait-ce parce que les équipementiers doivent remédier aux nouvelles vulnérabilités dès qu'elles apparaissent, et si possible rapidement. Il est également nécessaire que leurs fournisseurs de briques de base COTS soient tout aussi réactifs en termes de sécurité.

En suivant ces cinq étapes, les entreprises peuvent réellement faire d'énormes progrès dans la minimisation des risques et des niveaux d'exposition aux menaces de sécurité qui affectent leurs produits embarqués à forte connectivité. L'intégration de mécanismes de sécurité dans les systèmes embarqués est devenue une exigence fondamentale qui requiert un investissement toujours plus important à tous les niveaux d'une entreprise.

**A propos de Franz Walkembach**

Franz Walkembach a rejoint Wind River en 2009. En tant que Global Senior Product Manager Automobile, il est responsable du développement et de la maintenance de la plateforme Wind River basée sur Linux pour l'infodivertissement, ainsi que de la gamme complète des logiciels tiers complémentaires. En outre, Franz Walkembach est un membre actif du Conseil Marketing de GENIVI Alliance.

Franz Walkembach dispose de 20 ans d'expérience sur le marché des accessoires automobiles et des produits d'infodivertissement et a occupé diverses postes dans le développement, les achats et la gestion de produits. Chez Siemens VDO, il était à la tête de la gestion produit et du développement du marché des accessoires automobiles d'infodivertissement. Avant de rejoindre Wind River, il était Directeur Marketing Produit et membre du conseil de gestion de MyGuide Deutschland GmbH responsable de la gestion de production et des nouvelles solutions. Franz Walkembach a étudié la mécanique de précision à Giessen en Allemagne, et possède un diplôme d'ingénieur Solutions Automobiles

[www.windriver.com](http://www.windriver.com)