7 Systèmes embarqués et distribués, sécurisés et sûrs

Loisirs & culture
ÉNERGIE, **MOBILITÉ**, **NUMÉRIQUE**
ENVIRONNEMENT, **HABITAT**, **SANTÉ ET BIEN-ÊTRE**, **SÉCURITÉ**
Alimentation

➤ Correspond à une technologie clé 2015

MOTS CLÉS

Sécurité, systèmes embarqués, fiabilité, robustesse, sûreté de fonctionnement, architecture distribuée, parallélisme, système de systèmes

© THALES B. Rousseau

Définition et périmètre

Les systèmes embarqués sont définis comme des ensembles matériels / logiciels intégrés dans le but d'effectuer des tâches fonctionnelles précises. Les systèmes et logiciels embarqués jouent un rôle majeur dans la quasi-intégralité des secteurs industriels et sont très présents au sein d'industries historiques : les transports terrestres et l'aéronautique, le nucléaire, la défense et l'espace, les télécommunications (téléphones portables, assistants personnels, applications internes chez les opérateurs).

Ils jouent et joueront un rôle de plus en plus important dans de nombreux autres secteurs comme :

- la production, la distribution et la gestion de l'utilisation de l'énergie,
- la production industrielle (automatique, systèmes discrets et continus),
- l'instrumentation médicale,
- le bâtiment (domotique),
- l'électronique grand public (terminaux mobiles, multimédia, jeux et loisirs numériques),
- la logistique (commerce et distribution),
- les infrastructures urbaines (eau, trafic, captation de la qualité de l'air),
- la sécurité (vidéosurveillance, moyens d'identification)
- les transactions bancaires et commerciales (terminaux de paiement, cartes à puce).

Les prochaines générations de systèmes embarqués regrouperont deux natures d'innovation:

- **Dans les systèmes embarqués** : adoption de processeurs à très haute performance programmables, connectivité à Internet, haut niveau de systèmes d'exploitation et autres intergiciels
- **Dans le réseau global digital** : adaptation à l'émission / réception de données et de services issus d'Internet

Santé

La sécurité constitue un enjeu fort, de la protection des données à la manipulation à distance des objets connectés. La majorité des équipements (IRM, scanners et autres) n'ont pas été conçus en faisant de la sécurité une priorité. La connectivité des composants des systèmes embarqués avec des couches supérieures ou d'autres systèmes (configuration « Systèmes de systèmes ») implique de sécuriser ces différentes couches. Pour exemple, il a été démontré en 2011 que les pompes à insuline pouvaient faire l'objet d'attaques à distance et délivrer une dose létale d'insuline au patient via la modification de ses paramètres d'injection.

Sécurité

Dans le domaine de la sécurité, la criticité de certaines applications demande un haut niveau de sécurité et de sûreté de fonctionnement tels que dans l'aéronautique (pilotage automatique), le nucléaire (contrôle-commande), l'aérospatiale et autres applications militaires (communications)… La connectivité à Internet, de plus en plus présente, demande de revoir les techniques de sécurité pour se prémunir de prises de contrôle à distance. Des failles ont été montrées quant aux communications échangées entre les stations de contrôle et des aéronefs. En 2015, le FBI enquête sur une éventuelle introduction d'un hacker sur un avion de ligne commerciale. Bien que faiblement probable à l'heure actuelle, l'interconnexion grandissante des systèmes informatiques à bord des avions de ligne augmente ce risque de scénario. À l'image du *Smart Specialization Platform* (S3P) « android industriel », des groupes de travail étudient les architectures permettant de maximiser la sécurité du logiciel de contrôle de vol, comme notamment les hyperviseurs de sûreté et de sécurité.

Énergie

De la production à la distribution, les technologies de l'embarqué sont présentes sur l'ensemble de la filière énergie (Contrôle-commande des centrales nucléaires, conversion d'énergie dans les éoliennes, supervision des réseaux de transport d'électricité). L'émergence des Smart Grids (réseaux intelligents) demandera de déployer de nombreux instruments déportés capables d'interagir avec des systèmes de supervision amont pour maîtriser la production et la fourniture d'énergie.

Mobilité

Les systèmes embarqués sont déjà présents dans les véhicules au travers de l'assistance au freinage (système ABS), des régulateurs de vitesse et autres fonctionnalités (Électronique de contrôle dans les systèmes de châssis, dans l'électronique des chaînes de traction, dans le corps électronique et de sécurité des systèmes).

Les nouvelles générations de véhicules en émergence, et déjà en développement chez Google, GM et

Nissan par exemple, sont de plus en plus connectés et communicants avec leur environnement (technologie V2I : *Vehicle to Infrastructure*) favorisant ainsi le développement de nouvelles applications ITS (*Intelligent Transport System*) pour l'amélioration de la gestion du trafic, de la sécurité routière et des services de mobilité et de confort. Cette révolution automobile engendre de nouveaux défis technologiques et économiques ; la conception de véhicules coopératifs interopérables, un système de management de la sécurité pour les communications, ainsi que la préparation de systèmes fiables et sécurisés pour les futurs véhicules autonomes connectés. Ces systèmes communicants V2V/V2I auront donc besoin de sécurité et confiance numérique ainsi qu'une définition fiable et robuste du partage des données qui seront générées.

Trains, tramways, métros et bus constituent aussi un autre terrain de prédilection pour les technologies de l'embarqué. Le système Traintracer d'Alstom, par exemple, permet de récupérer à distance les données de fonctionnement des rames pour optimiser leur maintenance. L'aviation civile et militaire embarque également un grand nombre de systèmes embarqués (pilotage automatique, connectivité internet, infotainment…).

■ Télécommunications

Les systèmes embarqués sont présents sur l'ensemble des infrastructures de communication et appareils terminaux (box Internet ou stations de base de réseaux mobiles). La sécurité des communications est un enjeu fort. Pour plus de détails, se référer à la fiche n°7 « Communications sécurisées ».

■ Loisirs & culture

Les systèmes embarqués se retrouvent dans un grand nombre d'articles électroniques (décodeurs), terminaux finaux d'accès à internet (tablette, *smartphone*), électroménager, matériel audio – vidéo. Bien que moins critiques, la sécurisation de ces éléments n'en demeure pas moins importante.

Liens avec d'autres technologies clés

Les technologies clés qui influencent les Systèmes embarqués distribués sécurisés et sûrs sont :	
2	Capteurs
4	Modélisation, simulation et ingénierie numérique
5	Internet des objets
6	Infrastructures de 5ème génération
13	Communications sécurisées
20	Nouvelles intégrations matériel-logiciel
34	Authentification forte

Les technologies influencées par les systèmes embarqués distribués sécurisés et sûrs sont :	
2	Capteurs
5	Internet des objets
10	Cobotique et humain augmenté
12	Robotique autonome
13	Communications sécurisées
22	Réseaux électriques intelligents
31	Dispositifs bio-embarqués
40	Systèmes énergétiques intégrés à l'échelle du bâtiment

Les marchés

Selon le cabinet International Data Corporation, le marché des systèmes embarqués intelligents (tout équipement architecturé autour d'un microprocesseur, d'une interface de connectivité et d'un système d'exploitation et/ou d'une interface utilisateur de haut niveau, à l'exception des PC, des *smartphones*, des serveurs et des tablettes) dépassera les 1 000 milliards de dollars en 2019[1] pour 8,5 milliards d'unités vendues (plus d'un quart du volume total adressable par les systèmes embarqués).

Les segments de marché à forte croissance attendue sont :

■ l'assistance à la conduite et la gestion de consommation d'énergie dans le domaine des transports,

1 – https://www.idc.com/getdoc.jsp?containerId=prUS25204914

■ les dispositifs portés sur soi et les systèmes d'éclairage intelligents dans le domaine de l'électronique grand public,

■ les systèmes de pathologie numérique et de métrologie virtuelle dans le secteur de la santé,

■ les passerelles dédiées dans le secteur industriel.

En France, en 2013, les systèmes embarqués représentaient un marché de 73,3 milliards d'euros (3,7 % du PIB)[2] avec une croissance annuelle prévisionnelle de 3,3 % jusqu'en 2017 (soit 83,6 milliards d'euros) selon une étude de l'OPIIEC (Observatoire Paritaire des métiers de l'Informatique, de l'Ingénierie, des Études et du Conseil).

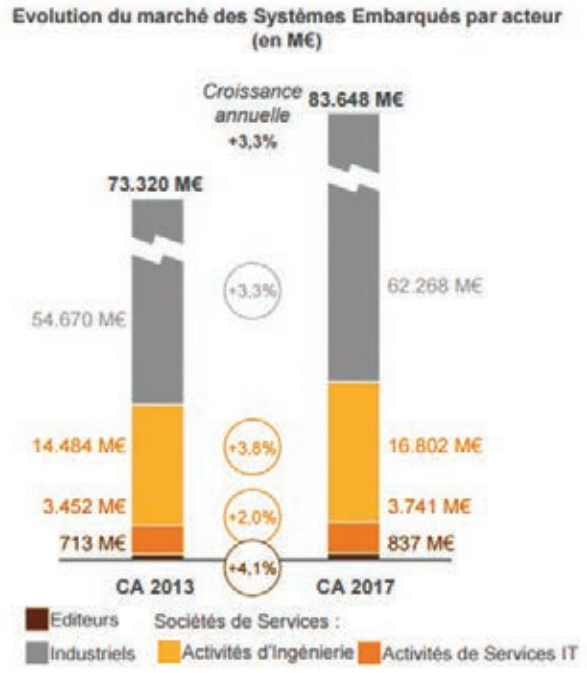

Figure 1: Rapport complet sur le développement des systèmes embarqués - OPIIEC 2014

Pourquoi cette technologie est-elle clé ?

Le caractère fortement diffusant de la solution, s'étendant à la quasi-intégralité des autres technologies, fait des systèmes embarqués une technologie clé. L'internet des objets accentue la place des systèmes et logiciels embarqués dans le quotidien et accroît plus que jamais la maîtrise des technologies de ces systèmes pour en faire un élément clé de la compétitivité industrielle.

Les défis technologiques à relever

Le caractère communicant des systèmes embarqués remet en cause les techniques actuelles de conception et de validation et conduit à de nouveaux défis, sur la sécurité en particulier[3].

Les principaux défis à relever sont:

■ **La sécurité et sûreté:** elles sont aujourd'hui traitées dans un environnement d'ingénierie des exigences, de modélisation des propriétés fonctionnelles et non fonctionnelles et d'approches formelles (ingénierie d'analyses statiques, preuves formelles, vérification, génération automatique de codes, de tests, analyse pour diagnostic). Les prochains défis seront de réussir à considérer l'incertitude de comportements, à réaliser des simulations hybrides mixant événements discrets et continus et à disposer de preuves de bons fonctionnements. L'évolution des règles et des pratiques de certification seront donc deux challenges à relever. La modélisation et le développement d'outils permettant de traiter conjointement la sécurité et la sûreté de fonctionnement deviennent nécessaires. Les nouveaux domaines d'application (informatique embarquée, intelligence ambiante, Internet des objets) et les nouvelles architectures (informatique dans les nuages, *Software as a Service* ou système de systèmes) font émerger de nouvelles propriétés ou contraintes (architectures reconfigurables, dynamique de l'environnement, évolution des usages), en plus des propriétés classiques. Un défi majeur consiste alors à revoir les méthodes de Validation et de Vérification (V&V) pour prendre en compte ces nouvelles architectures et les nouvelles propriétés associées, notamment par la simulation des systèmes cyberphysiques (Hardware in the Loop, Software in the Loop et Processor in the Loop – cf. Nouvelles intégrations matériel-logiciel). Dans ce cadre, la sécurisation des communications et l'authentification sont deux axes prioritaires. Il convient de développer les

2 – http://www.fafiec.fr/images/contenu/menuhaut/observatoire/etudes/2013/systemes-embarqu %C3 %A9s/SE-Developpement_economique_des_SE_-_20140606.pdf

3 – http://www.systematic-paris-region.org/sites/default/files/ROADMAP %20OCDS %20F %C3 %A9vrier %202015.pdf
https://ec.europa.eu/digital-agenda/en/embedded-systems
https://ec.europa.eu/digital-agenda/en/cyberphysical-systems-0
https://artemis-ia.eu/embedded-cyber-physical-systems.html
http://www.ecsel-ju.eu/web/index.php
http://www.smart-systems-integration.org/public/documents/presentations/presentations-at-the-ssi-2015-in-copenhagen-11-12-march-2015

algorithmes, outils ou méthodes permettant de les garantir, au niveau de ces infrastructures ;

■ La détection des attaques, la mise en place de modes résilients, autoréparables,

■ La gestion de l'hétérogénéité et de l'interopérabilité sécuritaire intra et inter-réseaux.

■ **L'Open source** représente une poche de productivité. Elle se développe depuis près de 25 ans mais reste en général minoritaire, toutefois pas en nombre d'utilisateurs, dans l'informatique et encore plus dans les systèmes et logiciels critiques embarqués à l'image d'OpenModelica, OpenCompute, OpenStack ou encore Android. L'ouverture peut être un facteur important de fiabilité et de sécurité : une utilisation à plus grande échelle des codes et la diversité des vérifications réalisées par des équipes aux techniques différentes contribuent à rendre optimale la détection de failles. Elle permettrait aux développeurs de disposer de bases communes ayant prouvé leur efficacité pour leur nouveaux développements. L'Open Source pourrait ainsi devenir un gage en termes de qualité et de sécurité des systèmes critiques.

■ **Le management des architectures distribuées et l'autonomie des systèmes** : La complexité croissante de notre environnement produit de très grands systèmes, le plus souvent concurrents, distribués à grande échelle et parfois composés d'autres systèmes appelés « Système de Systèmes » (résultat de l'intégration de plusieurs systèmes indépendants et interopérables, interconnectés dans le but de faire émerger de nouvelles fonctionnalités). La conception et la simulation de grands systèmes logiciels multi-niveaux et multi-échelles sont deux forts enjeux.

Le traitement en temps réel: la mise à disposition d'outils de développement pour les architectures orientées service et connectées au web permettra le traitement et la simulation en temps réel. Également présentes dans S3P, des recherches ont déjà été menées dans ce sens par le CNRS pour le compte de Schneider Electric (dont la valorisation des travaux est réalisée par la start-up Krono Safe[4]).

■ **Virtualisation, architecture multi-cœurs et algorithmes embarqués ;** la plupart des systèmes embarqués informatiques, des *smartphones* jusqu'aux accélérateurs de calculs (GPUs, FPGA, supercalculateurs) sont pourvus de systèmes multi-cœurs. Ces matériels mettent le parallélisme à portée de tous les acteurs bien qu'il reste d'une grande complexité. La mise en place de plateformes de plus en plus hétérogènes accroît cette complexité et le gain en performance se fait en utilisant des processeurs dédiés à des tâches définies. Il devient nécessaire de revisiter les langages (parallèles), mais également les moyens de construire les logiciels, tout en respectant des contraintes liées à l'espace et au temps et à la consommation de l'énergie en vue de diminuer les coûts de développement. Les systèmes embarqués devront également faire face à une demande de tolérance aux pannes de plus en plus exigeante et permettant une adaptabilité et une dégradation contrôlée des systèmes qu'ils régissent. L'évolution des principes de partitionnement, de reconfiguration, de dynamicité et d'évolutivité en sont donc les principaux enjeux.

■ **Le management de l'énergie** : certains secteurs opèrent dans des contraintes spécifiques dans lesquelles l'accès à l'énergie est limité. La consommation des systèmes embarqués est en grande partie due au mouvement et au stockage des données. Pour s'adapter à cette problématique, les compilateurs doivent prendre en compte la trace mémoire et les mouvements de données qui s'effectuent sur des unités de calcul différentes. La compilation à performances prédictives rend ce problème d'autant plus complexe et nécessite d'être abordé dans le futur.

■ **Les algorithmes embarqués** : ce sont des bibliothèques génériques utiles pour le traitement de signal et de l'image, le contrôle et la gestion de l'énergie embarquée. Cet axe prend place dans un contexte

4 – http://www-list.cea.fr/images/stories/decouvrir-le-cea-list/qui-sommes-nous/rapport-dactivite/Rapport-dactivite-CEA-2013_web.pdf
https://www.bitkom.org/files/documents/ES_Symposium_2011_Vortrag_Petrissans_IDC.pdf

d'exécution des algorithmes sur machines cibles. Les algorithmes doivent traiter de manière intensive les données générées dans des contextes variés (architectures homogènes ou hétérogènes, multi-cœurs), dans un contexte de tolérance aux pannes et de résistance au vieillissement. Les principaux défis sont d'obtenir la meilleure adéquation possible des algorithmes et des architectures de calcul et de garantir les propriétés opérationnelles : estimation exacte ou approchée des temps de réponse, gestion de l'énergie, mécanismes d'auto-surveillance et de reconfiguration inspirés des systèmes d'information, exploitation au niveau applicatif des mécanismes de bas niveau, tolérance aux SEU (*Single Event Upset*) et vieillissement avec dégradation contrôlée.

Les défis commerciaux à relever

Pour les secteurs « historiques » (défense, aéronautique, spatial, nucléaire...) : il s'agira d'effectuer la rénovation des solutions existantes. Pour les secteurs « Internet des objets »: l'exploitation de la croissance du secteur permettra d'accroître l'empreinte des acteurs français et européens dans les technologies de base.

La protection des éditeurs de technologies cœur présente ainsi un énorme effet levier sur les emplois indirects : elle permettrait l'éclosion d'usines pour logiciels embarqués sur des milliards de puces électroniques et la relocalisation des productions. En Europe il y a peu d'acteurs de taille moyenne (Kalray par exemple) mais on note la présence de startups avec des ambitions en France faisant de cet axe un enjeu stratégique.

Les mouvements participatifs fleurissent sur Internet et l'Open Source fait partie intégrante de ce nouveau modèle. Ce système économique permet de partager les coûts de développement, offrant ainsi un moyen à l'industrie de réduire ses dépenses en mutualisant les compétences. Cependant, le partage des sources demande de repenser les modèles économiques pour pallier la perte de l'avantage technologique d'un acteur sur son concurrent. Un des challenges est donc de trouver un business model viable pour les éditeurs de logiciels spécialisés dans ce type de développement puisqu'ils seront privés de licences propriétaires et de brevets.

Les enjeux réglementaires

Les architectures logicielles embarquées sont soumises à un processus de certification qui nécessite un développement très rigoureux pour assurer des fonctions critiques soumises à des contraintes très fortes. L'intégration des fonctionnalités de plus en plus complexes dans les logiciels embarqués rend à présent difficile la mise en œuvre des méthodes formelles. Les techniques de vérification souffrent également du problème d'explosion combinatoire du nombre de comportements des modèles, induite par la complexité interne du logiciel qui doit être vérifié. Les méthodes de preuve ou de vérification de programmes devront évoluer vers des certifications garantissant qu'un logiciel fournit les services attendus et définis par les utilisateurs, et pouvant prendre en compte, le cas échéant, la dimension « temps-réel » des systèmes embarqués.

Analyse AFOM

ATOUTS

Grand nombre d'acteurs français expérimentés

Excellence de l'école mathématique française

Pôles de compétitivité de référence

Association Embedded France

Leader mondial dans l'embarqué critique temps réel

FAIBLESSES

Décloisonnement des acteurs en cours

Excellence en langage distribué à renforcer

Passage d'une R&D industrielle à la production

Poids de l'écosystème national pour influencer les standards internationaux

OPPORTUNITÉS

Dialogues entre acteurs au travers de l'association Embedded France

Secteurs émergents (médical, bâtiments intelligents, objets connectés, usine du futur)

Relocalisation des productions

MENACES

Pénurie de talents disponibles

Concurrence des éditeurs américains, GAFA (Google, Apple, Facebook, Amazon)

Gestion de la diversité et de la variabilité à grande échelle

Sécurité des systèmes communicants

Facteurs clés de succès et recommandations

Réduire la pénurie de talents : une étude conjointe du Syntec Numérique et de l'OPIEEC publiée en 2013 indiquait que 40 000 emplois n'étaient pas pourvus dans la filière des systèmes embarqués. L'excellence reconnue de l'école mathématique française peut contribuer à la fuite de cerveaux vers l'étranger accentuant d'autant plus le manque de personnes compétentes. La formation initiale est une recommandation à considérer pour réduire cette pénurie.

Transposer l'excellence entre domaines d'applications: la France est leader mondial dans l'embarqué temps réel critique mais est moins présente dans l'embarqué non critique. Il est nécessaire de développer la recherche sur les langages pour la programmation distribuée et étendre le leadership sur le temps réel critique à des applications plus distribuées et vers des domaines plus variés.

Intégration des technologies liées à la sécurité : il s'agit en particulier d'aller vers des progiciel de gestion intégré (PGI) – *enterprise resource planning* (ERP) - de sécurité complets, assurant convergence de la sécurité dite « Physique » et « Logique » et la virtualisation de l'ensemble des composants de l'architecture, y compris capteurs et opérateurs.

Sécuriser le Cloud : n'étant applicables que sur des systèmes plutôt stables, statiques et fermés, les solutions techniques existantes ne sont plus du tout adaptées à ces nouvelles applications et nécessitent d'être repensées.

Renforcer l'ingénierie de « systèmes de systèmes » : la recherche de méthodes formelles pour la résilience des systèmes à logiciels prépondérants est un enjeu majeur de la prochaine décennie. À l'image de TrustinSoft, il s'agit de faire émerger des approches scientifiques mettant en œuvre des méthodes formelles et permettant de garantir sur ces logiciels le nombre grandissant de leurs propriétés de sécurité critiques.

Acteurs clés

Entreprises	Actia, Airbus, AKKA, Alstom Transport, Alten, Altran, Assystem, CapGemini, Dassault Aviation, Orange, Renault Technocentre, STMicroelectronics, Thales Research and Technology, Thales Communications & Security, Schneider Electric - Electropôle, Valéo…
IRT, ITE, IHU	B-COM, SystemX, IRT NanoElec, Railenium, IRT Saint-Exupéry…
Instituts Carnot	CEA LETI, CEA LIST, ESP, IRSTEA, INRIA, Logiciel et Systèmes Intelligents, M.I.N.E.S., LAAS CNRS, ONERA, TSN…
Autres centres de recherches	ENSTA, IFPEN, INSA, ISIR, LORIA, Mines ParisTech, UTC…
Pôles de compétitivité	Aerospace Valley, Images et Réseaux, Minalogic, Systematic, TES…
Autres (clusters, associations, fédération professionnelles, réseaux d'entreprises)	Cap'Tronic, CITC EuraRFID, Embedded France…

Position des acteurs français

Position des entreprises françaises dans la compétition mondiale	
En position de leadership	
Dans la moyenne	●
En retard	

Position des acteurs académiques français dans la compétition mondiale	
En position de leadership	●
Dans la moyenne	
En retard	