S3P, UNE SOLUTION DE DÉVELOPPEMENT ET D'EXPLOITATION UNIQUE ET MODULAIRE POUR L'IoT

S3P
SMART, SAFE & SECURE PLATFORM

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES
DGE
DIRECTION GÉNÉRALE DES ENTREPRISES
INVESTIR L'AVENIR

Recueil et rédaction des témoignages : CAP'TRONIC

Nous remercions l'ensemble des personnes interviewées pour leur disponibilité et leurs avis éclairés.

Rédaction des chapitres : Eric BANTEGNIE (ANSYS), Claude BOUSCARLE (Thales), Fabrice DEREPAS (TrustInSoft), Yohann DESILES (CAP'TRONIC), Xavier FORNARI (ANSYS), Fabrice GRAIGNIC (STMicroelectronics), Pascal GRENELOT (SurTec), Chaînez HAMLAOUI (ANSYS), Mustapha IGUERDANE (Thales), Jean-Christophe JAMMES (Safran), Benoît LEBRAS (Altran), Yves MEYER (SYSGO), Christophe PAGEZY (Prove & Run), Salvatore PALMA (KRONO-SAFE), Charlotte PICHOT (Alstom), Maurice PITEL (Schneider Electric), Patrick RIGOT (Airbus), Fred RIVARD (MicroEJ), Richard SALVETAT (CAP'TRONIC), Margot SOULIER (MicroEJ), Jérémie TABOUTET (CEA List), Claude VITTORIA (CAP'TRONIC).

Imprimé en octobre 2018
Conception graphique Violaine Cleyet-Marrel.

Crédit photos : ©Shutterstock et nos contributeurs

INTRODUCTION

Eric Bantegnie,

Président d'ANSYS France

Coordinateur du Projet S3P

La Plateforme S3P vise à permettre le développement et l'exploitation commerciale rapide de services et de produits connectés à l'Internet des objets (IoT), combinant des caractéristiques uniques de sûreté de fonctionnement, de cybersécurité, d'agilité et de portabilité, tant pour des applications de nature industrielle que grand public.

Cette plateforme est désormais disponible commercialement, après un projet de développement de 3 ans et 45 M€, soutenu par l'initiative gouvernementale de la "Nouvelle France Industrielle".

L'originalité du projet de développement a été de valider les technologies et produits proposés au travers de cas d'utilisation en grandeur réelle et de mettre sur le marché des solutions immédiatement opérationnelles, couvrant la modélisation système, le développement automatisé de logiciels applicatifs embarqués, l'analyse de la cybersécurité des logiciels, la fourniture de plateformes d'exécution hautement performantes, sures, « cyber-secure » et agiles, ainsi qu'une réelle intégration entre les différents outils de la plateforme en facilitant une mise en œuvre productive et aisée.

Ce guide présente de manière conjointe les produits composant la Plateforme S3P et des cas d'usage emblématiques, dans des domaines aussi divers que l'avionique connectée, le « smart signalling » ou la « smart énergie », la santé connectée ou l'Industrie 4.0.

Vous en souhaitant bonne lecture...

1

PRÉSENTATION DU PROJET S3P

1

L'Internet des objets (IoT), un changement majeur

Les spécialistes s'accordent à dire que d'ici 2025, il y aura 35 milliards d'objets connectés en circulation dans le monde. Que ce soit dans le domaine industriel ou celui du grand public, toutes les entreprises sont impactées de près ou de loin par ce phénomène, considéré comme la troisième évolution de l'Internet : le Web 3.0.

Les avancées technologiques, la diversité des offres, l'accroissement de la demande et les standards émergents, sont autant de facteurs qui contribuent à l'accroissement de ce marché. Les acteurs majeurs que sont les GAFAM ou autre BATX déploient une énergie et des budgets faramineux pour asseoir leur place sur ce marché prospère. Des initiatives gouvernementales françaises ou européennes visent également à promouvoir et organiser ce secteur. La filière embarquée française, représente d'ailleurs 9% des emplois en France en 2015.

Comme tout secteur en développement, celui de l'Internet des objets a besoin de se structurer, notamment au niveau des solutions logicielles existantes. En effet, il existe actuellement une multitude de plateformes de développement et d'exécution dans la plupart des cas incompatibles entre elles ou accrochées à une solution matérielle qui nécessite d'utiliser le hardware et le software d'un fournisseur pas toujours adapté au besoin de l'entreprise.

C'est dans ce cadre que **le consortium S3P** a été créé.

S3P, proposer un ensemble de solutions modulaires dans des environnements de niveaux d'exigences variés (Smart, Safe & Secure)

Le consortium S3P a été créé en 2015, financé par le Programme d'Investissements d'Avenir (PIA), et constitué d'acteurs français de l'IoT :

- **Industriels :** Airbus, Alstom, Altran, Safran, Schneider Electric, SurTec, Thales
- **Fournisseur d'outils de conception logiciels :** CEA
- **Fournisseurs d'outils de modélisation et de développement :** ANSYS, MicroEJ, Thales, TrustInSoft
- **Fournisseurs de plateformes d'exécution :** KRONO-SAFE, MicroEJ, Prove & Run, SYSGO
- **Fournisseurs de couches de virtualisation :** Prove & Run, SYSGO
- **Fabricant de puces électroniques :** STMicroelectronics
- **Organisme d'accompagnement :** CAP'TRONIC
- **Partenaire technologique spécifique :** Telecom ParisTech
- **Organisme de diffusion des technologies de modélisation :** Fondation Eclipse

"Smart, Safe and Secure Platform"

La Plateforme S3P vise à permettre le développement et l'exploitation commerciale rapide de services et de produits connectés à l'Internet des objets, combinant des caractéristiques uniques de :

- **Portabilité et agilité (SMART)**

Etant donné qu'il est essentiel de permettre aux développeurs d'applications IoT de monétiser rapidement et efficacement de nouveaux services, la Plateforme S3P développe des solutions portables pour les architectures très économes en ressources matérielles, logicielles et de consommation dans des environnements réseaux et processeurs variés.

La Plateforme S3P intègre non seulement des capacités de développement et d'exécution de code mais aussi des outils de modélisation et de développement système et logiciel intégrés. Elle est compatible avec les différents standards et protocoles d'infrastructure IoT, ainsi que des plateformes cloud et analytics.

- **Sûreté de fonctionnement (SAFE)**

La Plateforme S3P permet le développement d'applicatifs logiciels critiques d'un point de vue de leur sûreté de fonctionnement et de leur intégration dans des systèmes industriels certifiables au titre des normes les plus exigeantes, comme des moteurs d'avion, des véhicules autonomes, des systèmes de production d'énergie, des systèmes médicaux, etc..

- **Cybersécurité (SECURE)**

La Plateforme S3P permet le développement et l'utilisation de logiciels applicatifs et de plateformes d'exécution sur les objets et les "Gateways" qui soient sûrs et certifiables du point de vue de la cybersécurité. Un des enjeux de ce projet est de créer une plateforme permettant de répondre aux besoins industriels tout en garantissant un niveau élevé de sécurité.

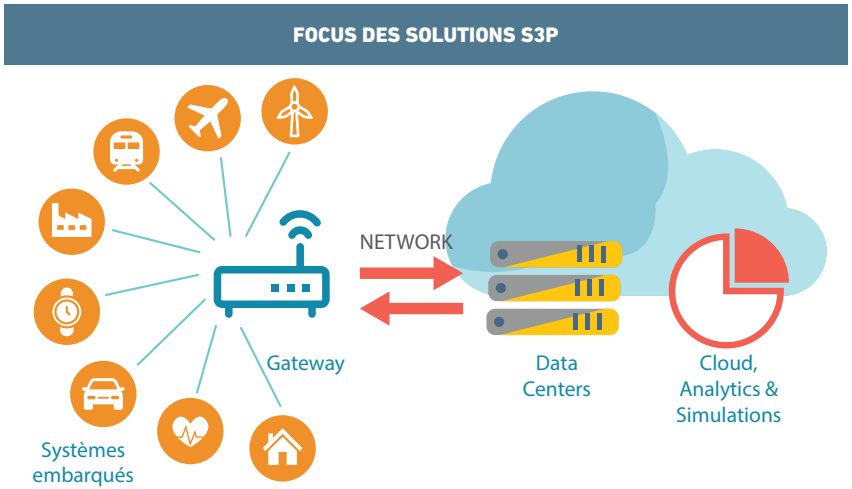
Industriellement parlant, l'objectif est que n'importe quelle entreprise puisse déployer rapidement des services innovants avec un investissement minimum et des garanties de sécurité des infrastructures et des données.

Le travail collaboratif au centre du projet

La Plateforme S3P vise la partie embarquée de l'infrastructure d'une application IoT avec une solution modulaire, construite autour d'un nombre réduit de fournisseurs de technologies. Cette plateforme propose un processus générique (pour l'industrie et le grand public) avec une attention particulière portée sur la partie sécurité (confiance numérique). Ainsi, la mobilisation de plusieurs fournisseurs de technologies, permet à l'utilisateur de choisir l'implémentation la plus adaptée en fonction de son besoin. Dans cet objectif, les fournisseurs de solutions du projet ont travaillé ensemble et en collaboration avec les industriels.

Une approche terrain par cas d'usage

Le projet a privilégié une approche pratique, en développant des solutions couvrant des cas d'usage retenus par de grands industriels français. Ces derniers ont été sélectionnés afin d'obtenir une bonne couverture des domaines d'application de l'IoT (aéronautique, automobile, domotique, santé...) et les contraintes et spécificités associées. Néanmoins, les solutions technologiques développées sont indépendantes des domaines métier et peuvent ainsi être réutilisées dans plusieurs cas d'usage.



1

L'Alliance S3P

L'Internet des objets crée une opportunité économique mondiale majeure qui impacte profondément la plupart des marchés. Parmi les enjeux majeurs de l'IoT on trouve d'un point de vue technologique le logiciel embarqué, notamment sur les aspects de sécurité, de sureté de fonctionnement et également l'efficience du modèle économique. Les acteurs de ce marché en forte progression, constatent que la sécurité et la sûreté de fonctionnement sont des problématiques communes à beaucoup d'applications quel que soit le secteur. Il y a par conséquent un enjeu stratégique à réutiliser des éléments logiciels pour un certain nombre de domaines que ce soit pour des objets connectés destinés aux chaînes de production industrielle ou pour des objets connectés grand public.

La France est très bien positionnée sur le marché des objets connectés, car elle possède de nombreux atouts scientifiques et techniques. Son excellence dans la sécurité et dans les systèmes embarqués est mondialement reconnue, n'oublions pas que la carte à puce est née en France. Il s'est créé tout un écosystème autour de l'école mathématique française pour définir des algorithmes et pour développer la cryptographie nécessaire à la sécurité informatique. De la même manière, de fortes compétences en sureté de fonctionnement industriel se sont développées en réponse aux demandes des grands industriels français et européens. Dans ce contexte, et suite à l'initiative de la Nouvelle France Industrielle un groupe de travail a été créé afin de pouvoir identifier à travers des secteurs très divers comme l'aéronautique, le ferroviaire, les systèmes énergétiques mais également la santé, l'électronique grand public, les besoins en matière de développement de logiciel embarqué critique et non critique. Au cours de cette évaluation, les industriels ont identifié des besoins communs. C'est à partir de cette demande industrielle de pouvoir développer des objets connectés industriels ou grand public de manière économique, sûre et fiable que le consortium S3P a été créé. De ce consortium est né le projet S3P qui a consisté à créer une plateforme de développement et d'exécution logicielle, performante, sûre et sécurisée.

La Plateforme S3P permet ainsi le développement, le déploiement et l'exploitation d'objets et systèmes connectés, de « Gateways » et d'applications, au meilleur coût et dans les meilleurs délais.

Dans le champ de l'intelligence embarquée, le projet S3P a permis de décloisonner les « SILOS » sectoriels et de faire dialoguer ensemble des industriels sur des besoins techniques dans des domaines différents afin de mieux comprendre ce qui était commun de ce qui ne l'était pas. L'analyse est allée de la génération de code extrêmement compact pour des systèmes qui disposent de très peu de ressources, jusqu'aux très grands systèmes dans lesquels il peut y avoir des millions de lignes de code et des architectures extrêmement puissantes, en passant par des systèmes hybrides comme « l'infotainment » (l'infodivertissement) automobile qui combine systèmes critiques et non critiques. Cette analyse fait ressortir que 70% des besoins sont communs et que la différenciation technique est essentiellement liée au coût et à l'usage de l'objet et du service.

Le projet S3P n'a pas vocation à rester national. En effet, beaucoup de partenaires du consortium sont multinationaux. Ceux-ci ont souhaité élargir le nombre de partenaires et permettre à des acteurs industriels intéressés par le projet de le rejoindre.

L'Alliance S3P s'est ainsi construite sous l'égide de l'association Embedded France, dans le but de faciliter le développement d'un écosystème national et international autour de l'initiative du consortium S3P et de développer l'utilisation de la Plateforme S3P auprès des autres leaders de l'industrie avec pour missions principales :

- **regrouper l'ensemble des utilisateurs de la Plateforme S3P et de ses utilisateurs potentiels, incluant ceux du Consortium S3P;**
- **assurer un lien avec les autres initiatives nationales et internationales (comme l'Industrial Internet Consortium, Industrie 4.0, etc..) au sein du domaine IoT et avec les autres solutions de la "Nouvelle France Industrielle";**
- **rassembler l'expression des besoins et les opportunités techniques et de marché;**
- **faciliter l'utilisation la plus large possible de la plateforme.**

L'Alliance S3P peut être rejointe en contactant :

- **Cedric Demeure :** Président du cluster Embedded France
  cedric.demeure@embedded-france.org
- **Chahinez Hamlaoui :** chef de file - coordination projet
  chahinez.hamlaoui@ansys.com

2

CONTEXTE ET PROBLÉMATIQUE, SOLUTION TECHNIQUE, RÉSULTATS ET BÉNÉFICES

- **A** Air Traffic Service Unit – Airbus
- **B** Passerelle d'interopérabilité multi-domaines sécurisée - Thales
- **C** Systèmes temps réel, physiquement distribués, et reconfigurables – Thales
- **D** Contrôle en temps reel pour les équipements aéronautiques – Safran
- **E** Plateforme nouvelle génération pour les systèmes de signalisation ferroviaire - Alstom
- **F** IoT Ready Device Architecture – Schneider Electric
- **G** Industrie 4.0 – Altran
- **H** Smart Home – SurTec
- **I** Connected Health – Altran
- **J** Domotique sécurisée – STMicroelectronics

LES CAS D'USAGE

2 A

AIR TRAFFIC SERVICE UNIT

AIRBUS

2A

Contexte et problématique

Le cycle de développement et de maintenance d'un logiciel avionique certifié s'étend sur plusieurs décennies. Après sa première mise en service, le logiciel avionique doit évoluer pour intégrer de nouvelles fonctions répondant à de nouvelles missions.

C'est particulièrement le cas de la fonction DATALINK, qui permet d'échanger des informations entre les avions et le sol en particulier dans les zones où les communications radio et la couverture radar sont difficiles comme les océans, et de la fonction Air Traffic Control (ATC) qui a pour but d'échanger de façon automatique des données liées au vol de l'avion avec les systèmes de contrôle du trafic aérien. L'accroissement du trafic aérien ainsi que la demande croissante des compagnies aériennes en services permettant l'optimisation de l'exploitation des aéronefs (changement de route pour optimiser le carburant, préparation des opérations de maintenance en escale etc.) requièrent une forte évolutivité de ces fonctions. L'accroissement des contraintes de sécurité sur l'échange des informations nécessitent également des fonctions supplémentaires de chiffrement et d'authentification.

Les plateformes actuelles conçues pour répondre aux besoins initiaux n'offrent pas les ressources matérielles répondant à ces nouveaux besoins. Les performances d'un microprocesseur développé dans les années 1990 ne sont pas au niveau de la puissance de calcul requise. De plus, les problèmes récurrents d'obsolescence de composants électroniques contraignent à des activités de redesign matériel incluant un changement de processeur qui, en plus d'être intrinsèquement très onéreuses (certification matérielle), entrainent des activités logicielles encore plus coûteuses dues au changement d'outils de développement et de validation logiciel attachés à ces nouveaux processeurs.

Les enjeux sont donc de préserver l'investissement logiciel des fonctions déjà développées et de permettre leur extension pour répondre aux nouvelles demandes de service.

Solution technique

L'architecture S3P, au travers d'une abstraction des couches matérielles va permettre un découplage entre le logiciel avionique et le matériel, assurant une capacité actuelle et future à disposer des puissances de calcul nécessaires tout en limitant l'impact sur le logiciel. La ségrégation des applications offerte par le système d'exploitation PikeOS de SYSGO permet de garantir la sécurité du protocole DATALINK dans sa globalité et l'assurance du respect du niveau de criticité requis par l'application ATC. Sur cette base, le partitionnement offert par PikeOS permet l'ajout progressif de nouvelles fonctions interconnectées entre elles et avec la fonction DATALINK.

La fonction DATALINK actuelle comporte une forte adhérence avec la plateforme matérielle existante et ne peut donc pas directement être relogée sur la nouvelle plateforme. L'application « legacy » étant basée sur des services du standard POSIX PSE53 (profil de système dédié à l'exécution temps réel), SYSGO a étendu dans le cadre du projet S3P sa personnalité POSIX, certifiée sur un périmètre PSE51 (profil de système minimaliste pour de l'exécution temps réel) pour inclure les services PSE52 (profil de système pour les contrôleurs temps réel) et PSE53 requis. Pour Airbus, l'enjeu est d'adapter cette application à l'environnement de la Plateforme S3P avec le minimum d'impact. Le choix retenu est de développer une couche d'abstraction qui limitera les impacts des évolutions matérielles et logicielles sur cette fonction afin de contribuer à conserver l'historique en service, de garantir un haut degré de fiabilité de la fonction DATALINK et d'éviter les phases de mise au point logiciel/logiciel.

Résultats et bénéfices

Les sous-ensembles plateforme nécessaires à l'accueil des applications DATALINK et ATC sont disponibles. Le portage de l'application ATC sur la nouvelle plateforme a été réalisé avec quasiment aucune modification de son code, à l'exception de quelques reprises liées à une moins grande permissivité du compilateur gcc. Des premiers tests de l'application sont fonctionnels dans l'environnement de simulation matériel offert par la Plateforme S3P (PikeOS sur QEMU).

L'abstraction entre couches matérielles et applications introduite dans ce cas d'utilisation permet d'offrir les mêmes services de la fonction DATALINK legacy que sur l'ancienne plateforme tout en permettant de suivre à moindre coût les évolutions futures des éléments de la Plateforme S3P : nouveaux processeurs, nouveaux services de sécurité, ...

L'ajout de nouvelles fonctions et services clients de la fonction DATALINK pourra se faire de façon modulaire, en s'appuyant sur la ségrégation offerte par PikeOS, sans entrainer de coûteuses activités sur cette dernière fonction ou les autres fonctions déjà présentes sur la plateforme.

2B

PASSERELLE D'INTEROPÉRABILITÉ MULTI-DOMAINES SÉCURISÉE

THALES

Contexte et problématique

Thales est un fournisseur mondial de premier rang dans le domaine des équipements avioniques ainsi que celui des systèmes de contrôle du trafic aérien. Thales Research & Technology, en tant qu'unité de recherche appliquée, apporte aux différentes unités de Thales son expertise de la connaissance de l'état de l'art académique et de la connaissance technique des verrous technologiques liés aux contextes métiers, notamment dans le domaine de l'aéronautique ou du contrôle du trafic aérien.

Aujourd'hui, plusieurs secteurs du monde de l'aéronautique sont confrontés à une demande de plus en plus croissante au niveau de la connectivité.

L'augmentation de la fréquentation des transports aériens est entrain de provoquer une mutation des communications au sein des systèmes de management et de contrôle. En effet, on constate que le besoin opérationnel en termes de communication au sens large ne cesse de se complexifier et a fait émerger des nouveaux besoins d'interopérabilités. On peut citer en exemple les fonctions de communication et de maintenance de l'aviation commerciale civile.

Les technologies de l'information grand public étant devenues omniprésentes auprès du grand public, les passagers souhaitent maintenant posséder une continuité de service au niveau de leur connectivité aussi bien au sein des aéroports qu'au sein des avions qu'ils empruntent pour leurs trajets réguliers. Ce défi technologique implique une connectivité omniprésente avec une demande de sécurité accrue et le respect rigoureux des normes appliquées dans le secteur aéronautique.

En effet, un avion possède de nombreux systèmes de bord communicants qui sont ségrégés principalement en trois domaines :

- **le domaine "contrôle et commande" qui inclut la conduite du vol, les fonctions sécurisées du cockpit ou de navigation ainsi que des moyens de communication "bord-sol";**
- **le domaine des systèmes d'information qui regroupe les fonctions de maintenance, les serveurs et réseaux cabine qui hébergent les services des compagnies aériennes ainsi que des moyens de communication "bord-sol";**
- **le domaine des communications et du "divertissement passagers" offrant des applications multimédias.**

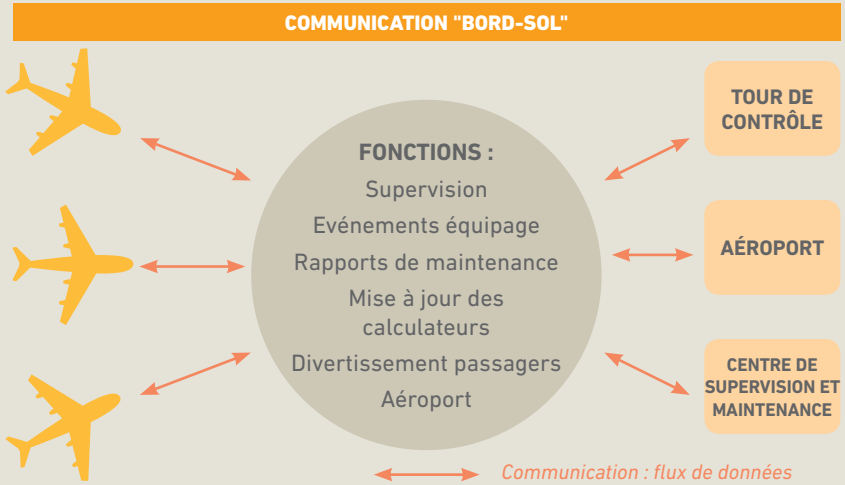
Ces domaines sont classiquement conçus comme autant de systèmes dédiés chacun possédant son propre niveau de sûreté et de sécurité. Néanmoins, les nouveaux besoins d'optimisation de l'aviation commerciale font que ces domaines seront amenés à héberger des applications de plus en plus communicantes et à échanger de plus en plus d'informations vers les autres domaines.

Pour Thales, un des enjeux majeurs est la migration vers une solution de plateforme unifiée respectant les exigences du secteur aéronautique tout en permettant la réutilisation des applications existantes souvent complexes et certifiées.

Cette plateforme doit apporter les bénéfices suivants :

- **une architecture interopérable offrant une sûreté inter-domaine tout en autorisant le partage de ressources : communications externes, passerelles sécurisées, réseaux embarqués partagés...**
- **le développement de services globaux : serveurs d'application critique, de maintenance, de synchronisation bord/sol...**
- **la réduction des coûts de développement d'application.**

De plus, ces nouvelles plateformes devront être compatibles des marchés de la gestion du trafic aérien. Elles devront permettre l'accroissement du niveau de sécurité des systèmes impliqués dans le contrôle de l'espace aérien et l'augmentation de leur niveau d'interopérabilité dans le but d'améliorer leur efficacité.



PASSERELLE D'INTEROPÉRABILITÉ MULTI-DOMAINES SÉCURISÉE

THALES

2 B

Parmi tous les points durs techniques, Thales s'est intéressé aux capacités de l'architecture S3 Platform, en une architecture ouverte et communicante, pour :

- **accueillir et permettre à un code métier, existant et déjà certifié, d'évoluer vers une architecture adaptée aux nouvelles technologies (i.e. multithread),**
- **cloisonner les logiciels applicatifs qui s'exécutent sur des plateformes multi-coeurs par niveaux de criticité;**
- **démontrer la possibilité de certifier les briques logicielles qui constituent l'architecture;**
- **garantir un haut niveau de confiance pouvant être soumis à des critères de certification en termes d'intégrité, d'authenticité et de confidentialité pour les logiciels et les données utilisateurs.**

Solution

Thales Reseach & Technology a appliqué une démarche de conception système au travers des outils de modélisation d'ANSYS. Ceci, afin de définir les configurations d'isolation et de communication de l'hyperviseur PikeOS de SYSGO. L'hyperviseur joue parfaitement son rôle en fournissant entre autre le cloisonnement et le partage de ressources, tel que le stockage, entre niveaux de criticité différents. Des fonctions de sécurité supplémentaires dédiées à notre architecture matérielle ont pu être développées dans le cadre du projet (gestion de la ségrégation fine des périphériques par exemple).

La complexité de la gestion du matériel (notamment la gestion de la sécurité de plus en plus présente) étant abstraite par l'OS/Hyperviseur ou confiée à des modules/drivers dédiés, les applications développées ne se concentrent donc uniquement sur les services à offrir.

Au travers de la JVM (Java Virtual Machine) de MicroEJ, Thales pourra augmenter la réutilisation d'applications sur plusieurs plateformes et architectures matérielles.

La sureté et la sécurité sont primordiales dans les applications réalisées. Pouvoir utiliser des outils de conception et des outils d'analyse de code ayant recours à des méthodes formelles, tel que TrustInSoft Analyzer, permet d'émettre les preuves du respect des exigences. Ceci est un enjeu important pour Thales.

Résultats et bénéfices

« S3P a permis à Thales de travailler avec des PME pour élaborer une plateforme d'avenir pour nos produits », affirme Claude BOUSCARLE de Thales. *« Nous avons pu évaluer un grand nombre de technologies et d'outils tout en arrivant à les intégrer aux flux de conception existant »* complète Mustapha IGUERDANE.

Thales a pu faire bénéficier aux PME partenaires, de son expérience et partager ainsi les contraintes liées aux marchés adressés. Par ailleurs, dans des secteurs d'activités où la confidentialité est très importante, la solution retenue permet une réalisation et une intégration des développements par le client (avec le support nécessaire) sans transmission de code source à un centre de service externe.

2

C

SYSTÈMES TEMPS RÉEL, PHYSIQUEMENT DISTRIBUÉS ET RECONFIGURABLES

THALES

Contexte et problématique

Thales a adressé une seconde problématique au sein du projet S3P. Devant le nombre grandissant de fonctions demandées à un système embarqué à l'activation très dynamique, de plus en plus de calculateurs sont nécessaires. Ces systèmes sont composés de calculateurs, souvent strictement dédiés à une tâche, ce qui aboutit à une intégration système de plus en plus complexe et coûteuse. L'utilisation de plusieurs instances homogènes d'un même calculateur permettant d'assurer différentes fonctions, est un enjeu majeur pour réduire le coût de ces systèmes.

Un autre avantage est de ne plus avoir de calculateur dédié à une fonction ou de réseau dédié à un flux et donc de faciliter son intégration, sa réutilisation et la réallocation des fonctions dans le système. Suivant le contexte opérationnel, certains de ces calculateurs sont utilisés ou non. On pourrait citer l'exemple de la caméra de recul qui n'est évidemment pas utilisée en marche avant. Le nombre de ces petits calculateurs dédiés croit. Certains éléments sont partagés (typiquement l'écran dans cet exemple), mais une réutilisation massive est difficile en raison de plusieurs barrières technologiques :

- **les propriétés temps réel strictes, sont garanties et vérifiées sur un matériel bien défini. La phase de conception nécessite donc la connaissance du matériel;**
- **des fonctions avec des niveaux de priorités différents, seraient en compétition sur le même matériel, amenant des comportements imprévisibles;**
- **des canaux de communication dédiés et un partitionnement souvent requis pour assurer la sureté ou la sécurité du système, rendent difficiles le partage du matériel.**

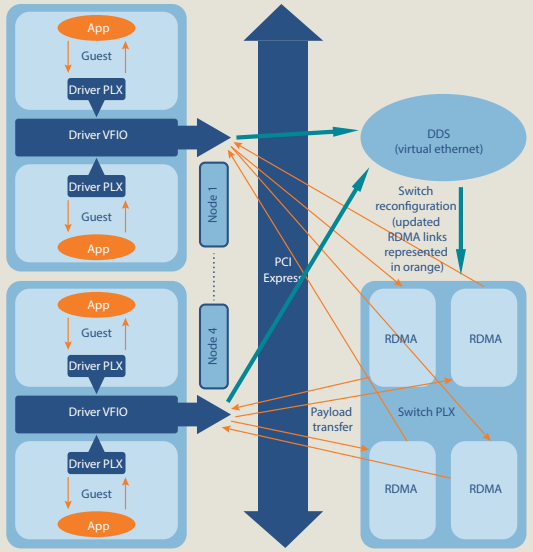
Ces contraintes amènent à la conception de systèmes où une part importante de la puissance de calcul n'est pas exploitée.

De plus, en cas de panne, la capacité d'un système à s'adapter automatiquement aux ressources matérielles encore disponibles serait facilité par l'homogénéité du matériel permettant une réallocation de l'exécution des applications.

Parallèlement à l'évolution des plateformes d'exécution, les outils de modélisation et d'ingénierie utilisés lors de la conception doivent aussi permettre de concevoir et de valider ces architectures utilisant les redéploiements dynamiques de fonctions et de flux.

L'approche consiste à considérer l'ensemble des ressources comme un cloud embarqué et à procéder dynamiquement à l'allocation des ressources. Toutefois, contrairement aux technologies du cloud, l'embarqué présente différents défis :

- **le respect de contraintes temps réel fortes et de niveau de criticité variable;**
- **l'optimisation des ressources matérielles : il est important d'utiliser au mieux les ressources matérielles et donc de partager;**
- **la redondance en cas de défaillance, d'une partie du système et donc la réallocation d'une fonction en garantissant sa criticité temporelle. Par exemple dans un traitement optronique visant à suivre un objet il est possible d'utiliser plus ou moins de ressources en fonction de la vitesse de l'objet suivi ou de la qualité recherchée. Néanmoins, le traitement des images de la caméra et l'asservissement de la navigation, impliquera des contraintes temps réel fortes. Lors du redéploiement sur d'autres calculateurs ces contraintes devront en permanence être respectées.**



SYSTÈMES TEMPS RÉEL, PHYSIQUEMENT DISTRIBUÉS ET RECONFIGURABLES

THALES

2C

Solution

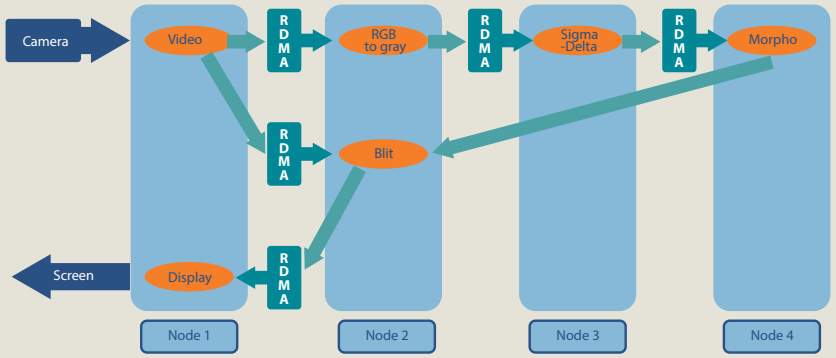
Le système est construit autour d'un réseau de type « PCI-Express ». Ceci se justifie par le besoin de bandes passantes de plusieurs dizaines de gigabits des capteurs radar et video et par le besoin d'une très faible latence des systèmes asservis. La topologie maillée est envisagée, justifiée par le besoin de redondance.

La pile logicielle intègre l'hyperviseur PikeOS de SYSGO, la DDS de PRISMTECH, le middleware à composant UCM basé sur le nouveau standard OMG développé par Thales et un mécanisme DMA zéro copie des flux vidéos entre les calculateurs.

Ce mécanisme, développé dans le cadre du projet, permet d'atteindre un débit important et une latence limitée. En effet, la bande passante réseau requise pour ce type d'application, interdit l'utilisation de solutions IP et de partitionnement logiciel.

Ainsi il est nécessaire de généraliser l'utilisation d'IOMMU (Input/Output Memory Management Unit) et d'étendre les concepts de virtualisation à l'ensemble des périphériques. Le réseau doit être partitionné matériellement de la même façon que le processeur !

La diminution de la couche protocolaire logicielle, pour se rapprocher du matériel, ne se traduit pas par une spécialisation de l'applicatif à un matériel spécifique. Pour cela, la couche middleware a été pensée dans le double but, antagoniste, d'abstraire au maximum le matériel tout en étant très proche de celui-ci !



Cette plateforme temps réel et reconfigurable a été validée avec un scénario de flux vidéo pour véhicule autonome. Pour ce faire, deux chaînes de traitement d'images temps réel sont distribuées sur 4 calculateurs. Une chaîne de traitement temps réel considérée critique, côtoie une chaîne de traitement non critique mais plus consommatrice en ressources.

Ce scénario permet de mesurer la performance réseau atteinte. Le débit des chaînes images a été cablé pour solliciter au maximum la bande passante réseau. La reconfiguration est validée en coupant aléatoirement un des calculateurs, et en procédant à la réallocation de la chaîne image.

Le démonstrateur permet de démontrer la continuité de séparation des flux de criticité multiple à travers le réseau et sa capacité à se reconfigurer

Résultats et bénéfices

Thales a pu intégrer une solution technologique relevant des défis techniques nouveaux. *« Nous avons mesuré l'importance de disposer de solutions maîtrisées : Switch réseau PCI-Express, middleware à composant UCM, logiciel de communication DMA zéro copie, Hyperviseur.*

Nous avons aussi profité de S3P pour faire évoluer notre environnement d'ingénierie et notre utilisation conjointe de CAPELLA et du logiciel Eclipse® Papyrus afin d'être efficaces et productifs dans le développement d'application » indique Claude BOUSCARLE.

Tous ces progrès seront utiles à Thales pour développer ses futurs systèmes distribués sur les véhicules d'intervention mais aussi dans les autres domaines d'application de Thales.

2D

CONTRÔLE EN TEMPS RÉEL POUR LES ÉQUIPEMENTS AÉRONAUTIQUES

Contexte et problématique

Safran est leader mondial, fournisseur de rang 1 en aéronautique, expert en électronique et logiciels critiques notamment pour les systèmes de commande du poste de pilotage, de navigation, de contrôle de vol et de régulation moteurs.

L'ampleur prise par l'électronique embarquée et les logiciels dans les systèmes aéronautiques en font un facteur de compétitivité déterminant pour les prochaînes générations d'équipements et de systèmes que Safran proposera à ses clients.

La mutation vers des systèmes de plus en plus connectés constitue en outre un défi pour Safran. « *Nous devons intégrer dans nos produits des fonctionnalités de surveillance et de communication plus élaborées que par le passé tout en conservant les fonctions premières de contrôle / commande* » explique Jean-Christophe JAMMES de Safran.

À ces défis font écho des technologies ou méthodologies émergentes telles que les langages formels ou semi-formels, les techniques de modélisation, les techniques d'ingénierie des systèmes et des équipements électroniques, les techniques de vérification et de démonstration de conservation de propriétés, les techniques de codage automatique des logiciels, les techniques de protection sécuritaire, les techniques de communication, etc.

Par ailleurs, il est à noter que l'ingénierie des systèmes embarqués est un domaine en développement rapide sous l'influence de nombreux secteurs industriels. L'aéronautique devra tirer les pleins bénéfices des avancées technologiques réalisées par ailleurs sur des secteurs grand public tels que les télécommunications.

Outre la conquête de nouveaux marchés qui sera facilitée par une meilleure compétitivité des solutions, un objectif fort est de développer et de monétiser une panoplie de services nouveaux liés à l'exploitation des équipements sur le terrain.

Safran travaille à l'élaboration d'architectures permettant de segmenter les fonctions de régulation moteur des fonctions de surveillance, et ceci entre autres dans l'objectif de pouvoir enrichir les niveaux de services offerts aux compagnies aériennes. Le pôle de compétences sur les électroniques et les logiciels embarqués met d'ores et déjà en œuvre un ensemble de technologies souches délivrées par des acteurs du projet S3P. Ces souches technologiques sont le plus souvent conçues et développées de manière indépendantes et leur intégration nécessite un effort important.

Par ailleurs, l'émergence des nouveaux services de maintenance des équipements nécessite d'introduire de nouvelles briques dont les OS à haut niveau de service et la cybersécurité. A noter que certaines technologies peuvent être issues du développement des « objets connectés » d'applications grand public.

Pour Safran, les innovations visées au titre du projet S3P portent sur deux points essentiels :

- **une meilleure intégration des ateliers de développement des logiciels applicatifs avec les plateformes d'exécution et ceci pour des équipements de contrôle / commande temps réel dur;**
- **une capacité facilitée à intégrer des fonctions critiques temps réel dur (exemple : régulation moteur) avec des fonctions périphériques de surveillance et d'optimisation de fonctionnement de l'équipement.**

Dans ce contexte, le projet S3P a été identifié comme un espace de concrétisation de certaines avancées technologiques.

Au sens S3P, les travaux ont été centrés sur l'ingénierie de :

- **une composante qui permet de contrôler un organe mécanique. A titre d'exemple les FADEC (régulation moteur), les contrôleurs de sous-ensemble ATA 32 (direction et freinage du train d'atterrissage), les contrôleurs d'actionneurs électriques, les électroniques de pilotage des capteurs, les systèmes de commande de vol, etc ... De manière générale, ces équipements appartiennent à la catégorie dite « temps réel dur », ils fonctionnent en environnement sévère et sont certifiés au plus haut niveau de sécurité des normes aéronautiques, DO178C – DAL A;**
- **une composante qui permet le contrôle de la "santé" du système. Ces fonctions sont complémentaires aux fonctions de contrôle / commande, elles sont d'un niveau de criticité plus faible et s'exécutent sur des OS à haut niveau de service.**

CONTRÔLE EN TEMPS RÉEL POUR LES ÉQUIPEMENTS AÉRONAUTIQUES

SAFRAN

2 D

Solution

Safran a profité de S3P pour évaluer des technologies prometteuses et leur compatibilité avec son atelier d'ingénierie système et logiciel.

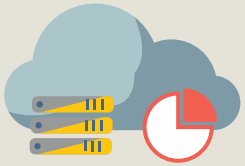
Les outils d'ANSYS ont permis d'assurer la gestion des exigences systèmes et leur traduction vers le logiciel avec une traçabilité garantie, ce qui est obligatoire pour des développements aéronautiques. Scade Suite a permis de générer du code pré-certifié répondant aux exigences établies pour le produit. La solution de KRONOSAFE avec son OS temps réel critique a permis d'isoler parfaitement les tâches critiques de contrôle commande de celles du monitoring de l'équipement pour les tierces parties. Le logiciel ASTERIOS qui permet de définir l'ordonnancement des tâches, grâce à S3P, a été intégré dans l'atelier d'ingénierie de Safran.

De plus, Safran est confronté depuis de nombreuses années au défi de la cybersécurité dans ses équipements. La solution Prove & Run a facilité l'utilisation des mécanismes de protection cyber des cœurs ARM et a garanti avec certitude l'efficacité des mesures déployées grâce aux méthodes formelles employées.

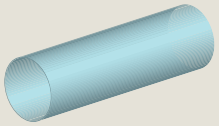
Résultats et bénéfices

Safran a engagé depuis quelques années une politique d'open innovation afin de détecter et de bénéficier des innovations provenant de start-up ou TPE/PME. "Les interactions avec les fournisseurs de solutions de S3P a permis de renforcer cette volonté" indique Jean-Christophe JAMMES. La participation à S3P a permis d'améliorer l'atelier d'ingénierie système et de proposer de nouvelles technologies à l'ingénierie de Safran. "Dès 2019, des nouveaux programmes bénéficieront des technologies évaluées sur S3P". Ce projet a permis d'évaluer une architecture à base de cœurs ARM avec des solutions logicielles répondant aux critères aéronautiques, ce qui permettra à l'avenir de proposer un choix de solutions élargies pour les architectures futures. Jean-Christophe JAMMES reconnait que

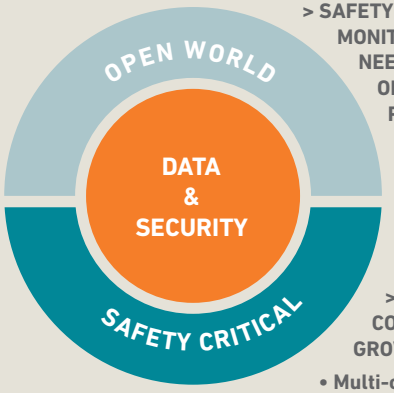
"S3P est un succès à la fois technique et stratégique, car une solution innovante et à fort enjeu commercial pour Safran a été réalisée dans les temps, et ce en établissant de nouveaux partenariats".



CLOUD



OPERATIONAL SYSTEM



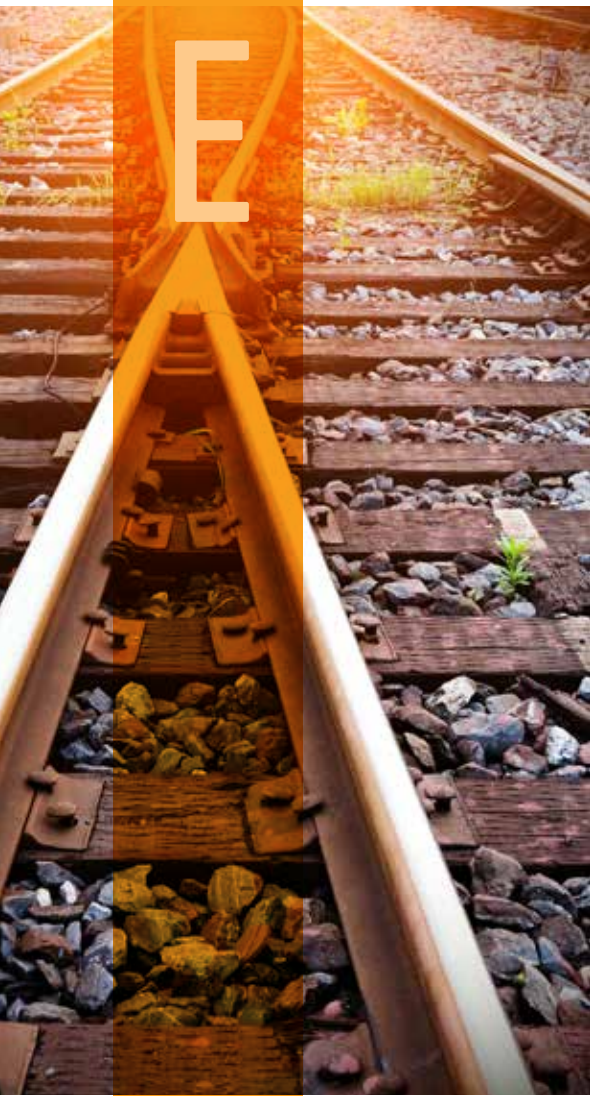
> SAFETY CRITICAL AND MONITORING FUNCTIONS NEED TO BE EMBBEDED ON THE SAME PLATFORM

- Cyber security becomes key driver

> SYSTEM COMPLEXITY STILL GROWING

- Multi-core
- Distributed platforms
- Efficients tools and methodology become mandatory

2 "SMART SIGNALLING"
SYSTÈME INTELLIGENT DE SIGNALISATION FERROVIAIRE



Contexte et problématique

Alstom est reconnu comme un des acteurs majeurs et des leaders mondiaux des systèmes, équipements et services pour le secteur du transport.

A l'échelle mondiale le processus d'urbanisation devrait atteindre probablement le seuil des 80% de la population habitant en zone urbaine à l'horizon 2050. Cette tendance induit des besoins grandissants de transport dans les zones urbaines mais aussi en connexion interurbaine. Le transport ferroviaire constitue de même une réponse aux problématiques d'éco-mobilité. Ce marché est donc particulièrement porteur et sa croissance est estimée à environ 5% par an.

Par ailleurs, le contexte économique mondial induit des réductions d'investissement de plus en plus fortes aux donneurs d'ordres qui sont le plus souvent des organismes publics. Ce contexte marché induit les spécifications des futurs systèmes de transport : sûreté, disponibilité, performance pour un coût de revient et d'exploitation bien moindre. C'est donc globalement ce que le projet développé dans le cadre du consortium S3P devait adresser en combinant les meilleures avancées technologiques et méthodologiques des plateformes d'exécution avec des approches nouvelles de conception et de déploiement des applications ferroviaires.

Les solutions ferroviaires doivent démontrer un niveau de sûreté de fonctionnement conforme à la norme CENELEC en Europe ou équivalent dans le reste du monde. Cette nécessité introduit une stratégie de sûreté de fonctionnement qui lie la plateforme d'exécution aux applications et services d'interopérabilité au regard du système global. De ce fait, le premier challenge résidait dans l'effort nécessaire pour faire la démonstration de sûreté de la solution, compte tenu que les contraintes de coûts orientent les choix de la plateforme vers des COTS basés sur des processeurs multi cœurs. Ceci induit des avancées auprès des OS-RT dans un contexte d'exécution multi- critique (SIL0-SIL4) devant apporter suffisamment de crédits de certification indépendamment des applications, et ce dans un contexte d'architectures redondées et sécurisées.

Les coûts de réalisation, d'intégration, de déploiement et de démonstration de sûreté des applications critiques (SIL2 à 4) doivent également être réduits. Si l'utilisation actuelle de méthodes formelles permet de garantir un résultat, l'effort nécessaire reste très important.

De même, si l'approche "composants" permet conceptuellement de garantir la réutilisabilité et la flexibilité, dans les faits, la construction et le déploiement d'applications de criticité mixte doivent pouvoir supporter aussi les briques logicielles existantes porteuses du patrimoine industriel.

"SMART SIGNALLING"
SYSTÈME INTELLIGENT DE SIGNALISATION FERROVIAIRE

2E

Solution

Pour Alstom, il s'agissait de mettre en œuvre une solution de signalisation existante sur une plateforme de nouvelle génération. Celle-ci devait introduire des évolutions majeures dans les outils de développement, de déploiement et de configuration des calculateurs.

La plateforme de nouvelles générations a été construite à partir de calculateurs COTS organisés en architecture 2 X 2oo2 (deux fois deux parmi deux) et munie de deux passerelles (en redondance). Ce sont au total 6 calculateurs banalisés qui sont associés pour animer la plateforme permettant ainsi d'atteindre les objectifs de disponibilité et de sûreté.

Plusieurs instances d'OS déterministes et supportant les processeurs multi-cœurs ont été mis en œuvre, y compris un mode hyperviseur PikeOS de SYSGO (en version 3.4) afin de permettre l'exécution d'applications non-critiques fonctionnant sous Linux. Un travail conséquent d'adaptation des intergiciels et passerelles avec l'architecture de la plateforme a été réalisé ; la validation de la solution a nécessité la démonstration de sûreté de fonctionnement.

Un des objectifs de ce projet fut d'identifier et de lever les risques techniques de non adéquation des briques technologiques retenues, en particulier sur l'aspect « passage à l'échelle ».

Les autres objectifs stratégiques du projet concernaient :

- **la réduction de l'effort de développement des systèmes et logiciels critiques et de l'effort de démonstration de sûreté de la solution;**
- **de pouvoir adresser un niveau de criticité allant du SIL0 au SIL 4 sur processeur multi cœur en minimisant les contraintes de déploiement sur les cœurs (plusieurs applications critiques, co-exécution avec niveaux de SIL différents);**
- **d'animer une plateforme basée sur des calculateurs COTS à base de processeurs multi-cœurs et de minimiser l'adhérence hardware;**
- **de réduire l'effort de démonstration de sûreté de la solution;**
- **de permettre l'intégration de logiciels spécifiques existants (encapsulation de codes existants voire sans toucher au binaire).**

Résultats et bénéfices

La chaîne complète a été testée et validée dans ses grandes lignes, les démarches de certification de l'applicatif sont en cours. Selon Charlotte PICHOT responsable du projet : *« Le niveau de maturité industrielle des outils et des solutions fournies par les partenaires du consortium est très satisfaisant. Le portage des applications critiques a été effectué avec un minimum de modifications. Les modifications apportées, l'ont été surtout pour tirer pleinement profit des fonctionnalités offertes par l'hyperviseur PikeOS ».*

En synthèse, le marché du transport guidé terrestre est porteur mais sera particulièrement concurrentiel et soumis à la pression des prix. Les industriels du secteur devront être dans les prix du marché et la différenciation sera apportée par la performance de l'offre. Les innovations apportées devront en particulier améliorer la qualité de service, réduire les coûts d'exploitation tout en garantissant la sûreté de fonctionnement. Ce contexte marché induit les spécifications des futurs systèmes de transport : sûreté, disponibilité, performance pour un coût de revient et d'exploitation bien moindre. C'est donc globalement ce que le projet a permis d'adresser en combinant les meilleures avancées technologiques et méthodologiques des plateformes d'exécution avec des approches nouvelles de conception et de déploiement des applications ferroviaires.

2

F

"SMART SPEED DRIVE" : DÉPART MOTEUR SÛR, INTELLIGENT ET FLEXIBLE

Contexte et problématique

Schneider Electric développe et commercialise des produits et solutions de distribution électrique destinées aux réseaux basse et moyenne tension.

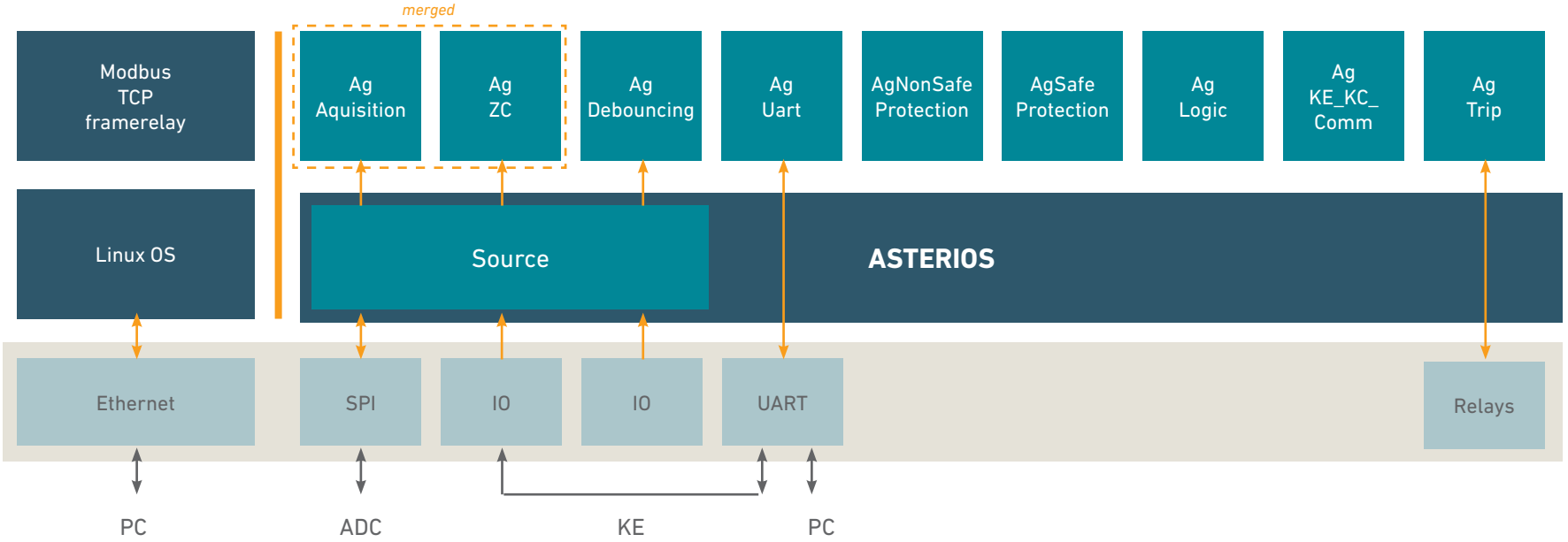
Les fonctions de base de ces équipements, qui ont déjà fait leurs preuves, ne sont plus, à l'heure actuelle, des éléments de différenciation pour Schneider Electric. Pour créer de la valeur à ces dispositifs, il faut utiliser les informations provenant de ces derniers afin de construire une vision globale de l'environnement utilisateur et proposer des axes d'amélioration à l'utilisation. Il faut donc rendre les équipements communicants pour assurer une meilleure gestion de la consommation, améliorer le confort, disposer de solutions plus rentables et plus écologiques. La plateforme logicielle devient donc le cœur du produit, qui doit répondre également à de nouvelles exigences en termes de sûreté et de sécurité.

L'enjeu pour Schneider Electric est de faire cohabiter sur une même plateforme d'exécution logicielle des fonctions critiques (exemple : détection de défaut de courant) et des fonctions annexes (exemple : rafraîchissement d'une IHM). En effet, si une fonction dysfonctionne, même annexe, elle peut entraîner soit la contamination des autres fonctions, soit bloquer les autres fonctions qui ne peuvent plus s'exécuter.

« Le produit a donc la solidité de la tâche la plus fragile », explique Maurice PITEL, Innovation Project Manager chez Schneider Electric. Il faudrait alors envisager d'utiliser une plateforme d'exécution par niveau de criticité de fonctions (partitionnement matériel), mais cela est coûteux et très rigide.

Dans ce cadre, ***comment arriver à concilier architecture ouverte et cybersécurité, flexibilité et sûreté de fonctionnement, et disponibilité ?***

Pour y répondre, Schneider Electric a choisi d'utiliser un cas concret de développement : un départ moteur. C'est le projet « Smart, Speed Drive ».



"SMART SPEED DRIVE" : DÉPART MOTEUR SÛR, INTELLIGENT ET FLEXIBLE

Solution

Schneider Electric a pu prototyper un départ moteur équipé de deux solutions développées par des membres du consortium S3P :

- **ASTERIOS de KRONO-SAFE un OS permettant de réaliser du cloisonnement spatio-temporel.**
- **Prove & Run qui fournit une solution répondant à des problématiques de sécurité avancées**

Dans un premier temps, les équipes de Schneider Electric ont travaillé avec KRONO-SAFE pour mettre en exécution les fonctions critiques et annexes ayant des fonctionnements réguliers ou variables sur une plateforme unique. Grâce au cloisonnement spatio-temporel, même si un tâche défaille, elle ne contamine pas les tâches à proximité et n'empêche pas les autres tâches prévues de s'exécuter. Ainsi la sûreté de fonctionnement est garantie, *« le produit est protégé contre lui-même »*, confirme Maurice PITEL.

Dans un second temps, il a fallu répondre à la partie cybersécurité de la problématique initiale. Il existe 2 types de cybersécurité :

- **au démarrage du produit pour s'assurer que le produit est bien celui qu'il prétend être;**
- **en utilisation pour vérifier que la communication extérieure ne soit pas dangereuse pour le produit.**

Ainsi a été développée une plateforme avec ASTERIOS répondant à des exigences de cybersécurité lors du démarrage et une avec Prove & Run gérant les fonctions variables en garantissant la cybersécurité lors de l'utilisation produit.

Résultats et bénéfices

Au travers de S3P, Schneider Electric a pu tester et prototyper un départ moteur utilisant une plateforme d'exécution gérant le cloisonnement spatio-temporel. Les fonctions critiques et annexes sont alors gérées ensemble sur la même plateforme, ce qui garantit la sûreté et la sécurité du produit pour ses utilisateurs et les équipements alentours. Par ce projet, les équipes de conception ont pris conscience de la nécessité d'intégrer la cybersécurité dès le départ du projet. Le fait de participer au projet S3P a facilité le choix de la solution de cybersécurité au travers du retour d'expériences des solutions utilisées par les autres grands industriels dans leur cas d'usage.

Pour une société industrielle, participer à un projet collaboratif permet d'entretenir le réseau de fournisseurs et de partenaires, et de maintenir les connaissances sur l'état de l'art d'une technologie.

Maurice PITEL reconnaît que des initiatives comme S3P permettent de mettre en valeur le savoir-faire des entreprises françaises, de maintenir et de créer des emplois, et de le valoriser à l'étranger, comme le prouve cet exemple.

Schneider Electric dispose ainsi d'un départ moteur Smart (connecté), Safe (sûreté de fonctionnement) et Secure (intégrant la cybersécurité).

2

"INDUSTRIE 4.0" :

PLATEFORME DÉDIÉE POUR CONNECTER UNE NOUVELLE CHAÎNE DE VALEUR

Contexte et problématique

Altran Connected Solution (ACS) World Class Center Internet of Things (WCC IoT) d'Altran, accompagne les industriels dans la création de produits autour des systèmes connectés.

Le développement et la diffusion des nouvelles technologies du numérique favorisent l'émergence d'un nouveau paradigme des systèmes de production : **l'Industrie 4.0.** Derrière ce concept se définit une nouvelle façon d'organiser les sites de production mettant en place une plus grande adaptabilité dans la production et une allocation plus efficace des ressources humaines. Dès aujourd'hui, les nouvelles ruptures technologiques, dont les systèmes connectés pourraient faire gagner en France, 1% de productivité chaque année. On pourrait réduire d'un tiers le taux d'absentéisme si on limite les absences dues aux désordres musculo-squelettiques. Cette ambition économique doit également intégrer deux importants volets : processus et humain, pour combiner la sécurité, la sureté et l'efficacité.

L'objectif du WCC IoT d'Altran est le développement et la mise en œuvre de plateformes dédiées, d'automates, d'ERP, d'opérateurs augmentés pour apporter une plus grande agilité et une amélioration substantielle des conditions de travail. Le challenge consiste à la fois à développer une plateforme permettant la gestion de produits et services communs sur toute la chaîne de valeur intégrée aux installations tout en prenant en compte la sécurisation des données et des informations.

"INDUSTRIE 4.0" :

PLATEFORME DÉDIÉE POUR CONNECTER UNE NOUVELLE CHAÎNE DE VALEUR

Solution

L'architecture S3P constitue la brique technologique absolument nécessaire pour optimiser la stratégie d'exploitation et de maintenance des usines (Smart & Safe) à l'abri des attaques (Secure & Safe).

Le développement de cette plateforme s'est appuyée sur les quatre éléments suivants :

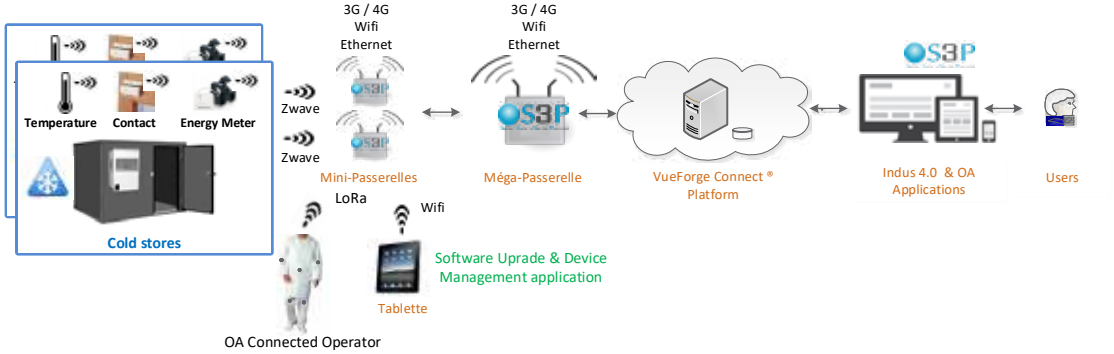
- **des objets connectés de mesure de l'exposition aux facteurs de pénibilité, intégrant dès leur conception l'ensemble des contraintes industrielles et environnementales, les problématiques d'acceptabilité sociale et les contraintes d'interopérabilité avec les systèmes d'information et de management de la santé et de la sécurité au travail;**
- **des mini-passerelles sécurisées utilisant les briques logicielles sécurisées du consortium. Ces mini-passerelles traitent et agrègent les données collectées des objets périphériques dans un rayon de couverture restreint;**
- **la passerelle (ou méga-passerelle) sécurisée est connectée via le réseau à des systèmes d'informations présents sur le cloud et mets les données collectées à disposition des différents acteurs/organismes concernés;**
- **le développement d'une application sur tablette qui permet de contrôler en temps réel les données remontées dans un environnement géographique restreint. Ce démonstrateur a été réalisé sur la base de plateformes matérielles de type ARM Cortex-A9, qu'on peut étendre à d'autres ARM Cortex A.**

L'OS de confiance Prove & Run est utilisé afin de sécuriser la connexion avec chaque client distant, pour isoler les différents modèles et pour communiquer avec les objets connectés et les différents systèmes d'informations. Un boot sécurisé a été également mis en place pour vérifier au démarrage l'authenticité des drivers, du boot et de l'OS, ce qui sécurise fortement l'ensemble du système. ProvenCore a permis de séparer l'OS (Linux) et les applications standards des applications métiers critiques. Les applications ont été développées en Java, en utilisant la plateforme MicroEJ. Celle-ci a eu le mérite de masquer la diversité des configurations matérielles-logicielles, en déconnectant l'application du processeur.

Résultats et bénéfices

La chaîne complète a été testée et validée dans ses grandes lignes sur des cas simples. Selon le chef de projet Benoît LEBRAS *«Par S3P, ACS a eu accès à des technologies matures pour mettre en place et opérer une plateforme sécurisée, notamment au travers de la mise en œuvre d'un boot sécurisé qui fut un élément clé du projet sur l'aspect Secure & Safe »*

Issu du retour d'expérience industriel du WCC IoT d'Altran, le développement de cette plateforme se place dans le contexte d'un acteur de la maintenance industrielle devant pouvoir analyser divers types de données au sein d'un site industriel (sidérurgie ou production d'électricité). Par conséquence, il justifie et définit les développements nécessaires pour les innovations de plateformes Smart, Safe and Secure pour l'Industrie 4.0.



2 H SMART HOME

Contexte et problématique

SurTec est une PME française basée en Bourgogne, concepteur de systèmes d'alarme dédiés aux télésurveilleurs professionnels (notamment bancassureurs) et installateurs. SurTec propose des systèmes d'alarme autonomes permettant la détection d'intrusion, connectés en IP et/ou par GSM-GPRS.

La société souhaite élargir son offre en proposant d'associer au système d'alarme, des solutions domotiques et des nouveaux services. Il s'agit d'interagir avec une grande diversité de capteurs et détecteurs nouvellement apparus sur le marché et à venir, afin de proposer une large variété de services additionnels aux utilisateurs finaux.

Les produits actuels sont sécurisés mais non interopérables avec des éléments tiers de captation d'information. Le projet de SurTec consiste à proposer à ses clients une plateforme d'alarme ouverte interopérable et sécurisée.

La création de valeur réside ainsi dans le développement d'une plateforme d'alarme :

- **ouverte sur des équipements tiers;**
- **interopérable;**
- **sécurisée;**
- **évolutive à moindre coûts.**

Le challenge de ce projet est donc d'interconnecter des équipements et services tiers de façon sécurisée tout en garantissant la sécurisation des fonctions déjà existantes telles que la détection d'intrusion ou la transmission d'alarme. Il faut aussi conserver les caractéristiques techniques inhérentes au produit telle que l'autonomie de 4 ans. Un élément majeur est de pouvoir adapter rapidement l'interface graphique utilisateur afin d'intégrer les nouveaux usages induits par les nouveaux éléments de mesure.

Dans cet environnement, comment concilier des besoins antinomiques telles que la sécurité et l'interopérabilité?

SMART HOME

Solution

SurTec a développé des prototypes de plateformes d'alarme en intégrant des solutions technologiques proposées par des membres du consortium S3P :

- **Prove & Run qui fournit des solutions répondant à des problématiques de sécurité;**
- **MicroEJ qui fournit une plateforme Java et des briques logicielles ad hoc pour microcontrôleur.**

La première étape a été d'intégrer des éléments provenant de MicroEJ. SurTec a développé des solutions spécifiques en mettant en oeuvre certaines solutions MicroEJ. De nouvelles solutions ont aussi été conjointement développées pour les besoins du projet. SurTec dispose désormais de solides compétences concernant la mise en oeuvre de l'environnement MicroEJ ainsi que le développement bas niveau sur microcontrôleur.

Le renforcement de la sécurité a été étudiée conjointement avec Prove & Run. Les solutions mises en place sur le démonstrateur sont satisfaisantes. Il reste à bien définir la position du curseur entre niveau de sécurisation et le supplément de prix. Une réflexion avec les clients est en cours pour la définir.

Résultats et bénéfices

Au travers de S3P, SurTec a pu concevoir un démonstrateur de plateforme d'alarme innovante comprenant des technologies avancées où coexistent une IHM évolutive, des solutions cybersécurité, et une grande interopérabilité.

SurTec a vu le bénéfice de s'appuyer sur des solutions technologiques permettant davantage d'ouverture et de sécurisation. Les contraintes fonctionnelles, sécuritaires et environnementales fortes ne pouvaient se suffire de solutions approximatives et fragmentaires. Le consortium S3P a permis la mise en place d'une solution « seamless » répondant aux exigences du produit.

Ce projet de R&D amont a permis d'être ambitieux et de parvenir à démontrer le fonctionnement réel de technologies nouvelles.

SurTec dispose ainsi de plusieurs démonstrateurs de plateformes d'alarme et d'acquisition Smart (connectée), Safe (sûreté de fonctionnement) et Secure (intégrant la cybersécurité).

Cela permet de réduire la prise de risque en amont des projets de développement de nouveaux produits.

2 "E-SANTÉ" :

SUIVI DE SANTÉ INDIVIDUALISÉ DES MALADIES CHRONIQUES

Contexte et problématique

La société de conseil en innovation et ingénierie Altran, qui accompagne les industriels dans la création de produits, a mis le cap sur les systèmes connectés par l'intermédiaire de son World Class Center Internet Of Things (WCC IoT), Altran Connected Solution (ACS).

En France, près de 15 millions de patients sont concernés par des affections de longue durée ce qui représente près de 70% des coûts de santé. Il est estimé que le marché mondial de l'E-santé devrait atteindre 20 milliards d'euros en 2018 et que plus de 500.000 cas de maladies chroniques pourraient être évités grâce à la santé mobile. Cela représenterait plusieurs milliards d'euros d'économie dans les dépenses annuelles de santé.

Le WCC IoT d'Altran souhaite mettre en place et opérer une chaîne complète d'E-santé qui permettrait un suivi de santé individualisé des maladies chroniques sur le long terme, dans une approche globale visant à terme à proposer des modèles de santé plus axés sur la prévention. L'enjeu est de parvenir à mettre en place, opérer et industrialiser à terme une plateforme à la fois ouverte et modulaire capable de supporter des produits et des services de santé allant de la télémédecine à l'automesure, tout en étant sécurisée, fiable et sûre. Cela de l'objet connecté au cloud, dans un contexte où la problématique de confiance liée à la confidentialité des données est critique et où la dimension humaine joue un rôle déterminant dans les produits et services.

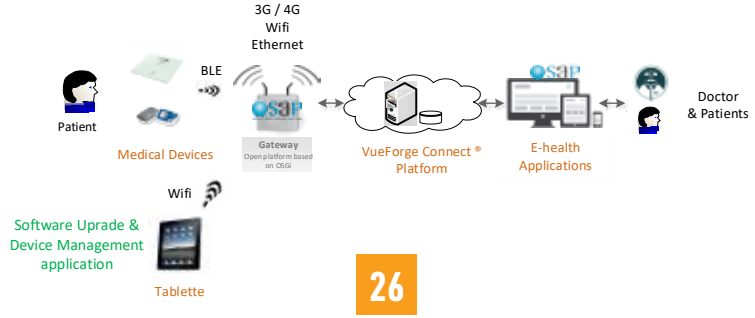
Pour le chef du projet, Benoît LEBRAS, « *L'avantage apporté par l'architecture S3P est la prise en compte dès la phase d'architecture des contraintes de sécurité, sûreté et fiabilité* ». L'hyperviseur et l'OS permettent de garantir intrinsèquement la sécurité des objets connectés et de la passerelle. La mise en place de solutions pour le maintien en condition opérationnelle et la prédictibilité de la performance permettent d'apporter une solution à un système dynamique en changement perpétuel : ajouts de nouveaux patients ; ajouts de nouveaux services ; mise à jour du système sans interruption de service; ajout aussi de nouveaux médecins (différents corps de métier possibles).

Une telle architecture, distribuée et ouverte est un avantage concurrentiel dans un monde aux besoins hétérogènes et en perpétuelle évolution.

La plateforme qui a été développée dans le cadre du projet S3P se compose des éléments suivants :

- **une passerelle sécurisée pour la santé à domicile traite les données collectées des dispositifs médicaux et les transfèrera vers les différents acteurs/organismes de santé concernés, le patient peut également accéder à ses données;**
- **de plusieurs périphériques (ou objets) connectés à la passerelle avec sécurisation de bout en bout, ainsi qu'une tablette;**
- **la passerelle sera elle-même connectée à des systèmes d'informations (médecins, autres) via le réseau et la plateforme VueForge Connect.**

Des alertes (emails) sont aussi envoyées au patient en cas de dépassements de certains seuils.



"E-SANTÉ" :

SUIVI DE SANTÉ INDIVIDUALISÉ DES MALADIES CHRONIQUES

ALTRAN

2

Solution

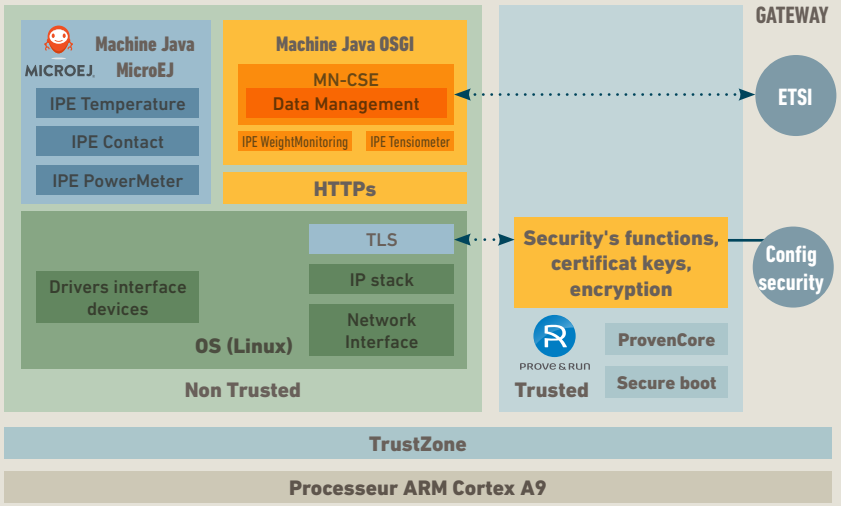
La plateforme devant être sûre, fiable et sécurisée. Son développement a fait appel à une architecture sécurisée grâce à l'utilisation d'un OS sécurisé (ProvenCore) délivré par Prove & Run.

Ce démonstrateur a été réalisé sur la base d'une plateforme matérielle de type ARM Cortex-A9 et ARM Cortex-A7. Cette base matérielle est complétée par une connexion à un réseau externe et des objets connectés médicaux. L'OS de confiance est utilisé pour sécuriser la connexion avec chaque client distant, pour isoler les différents modèles et pour communiquer avec les objets connectés et les différents systèmes d'informations. Un boot sécurisé a été également mis en place il vérifie au démarrage les clés et les certificats des éléments permettant de démarrer la gateway : boot, drivers et système d'exploitation, ce qui sécurise fortement l'ensemble du système. ProvenCore a permis de séparer l'OS (Linux) et les applications standards des applications métiers critiques. Les applications ont été développées en Java. Le WCC IoT d'Altran a utilisé la plateforme MicroEJ. Le mérite de cette plateforme fut de masquer la diversité des configurations matérielles-logicielles, en déconnectant l'application du processeur.

Afin d'offrir une grande souplesse de connectivité des périphériques la passerelle supporte plusieurs protocoles dont le BLE, le Wifi, la 2G/3G/4G et le Zwave. Deux versions du démonstrateur ont été échelonnées dans le temps. Ces deux versions reposent sur des cartes d'évaluation à base de ARM Cortex-A9. Chaque version permettant de lever successivement les verrous pour obtenir un démonstrateur sûr et sécurisé (v1) puis un démonstrateur intelligent (v2).

L'application de suivi du patient doit consister à :

- **mesurer le poids via un pèse-personne connecté et la tension via le tensiomètre connecté;**
- **monitorer ces données, afficher les diagrammes;**
- **envoyer un courriel et/ou un SMS au médecin et au patient si les valeurs seuils sont faibles et dépassées.**



Résultats et bénéfices

La chaîne complète a été testée et validée dans ses grandes lignes. Des tests de sécurité ont été essentiellement fait sur les aspects fonctionnels. Pour les tests plus poussés d'intrusion le WCC IoT d'Altran s'est appuyé en confiance sur les performances des solutions fournies par le consortium. Le développement des applications ayant été faites en JAVA, le WCC IoT d'Altran n'a pas pu bénéficier au début du projet d'outils de modélisation système, ni en cours de projet d'analyseur de code. En effet, les outils de modélisation proposés par le consortium S3P n'opèrent que sur des applications écrites en code C ou C++. Selon Benoît LEBRAS *« Au travers de S3P, ACS a eu accès à des technologies matures pour mettre en place et opérer une chaîne complète d'e-santé « smart, safe and secure » : de ce point de vue, le projet a atteint ses objectifs »*.

Enfin pour le WCC IoT d'Altran, le projet e-santé peut potentiellement donner lieu à des propositions de standards ou de normes (dont la Norme 13485), et ainsi permettre de développer la confiance numérique associée à ce secteur susceptible d'apporter des améliorations substantielles au système de santé.

2 DOMOTIQUE SÉCURISÉE

Contexte et problématique

STMicroelectronics est un leader mondial fournissant des semi-conducteurs qui contribuent de façon positive à notre vie quotidienne d'aujourd'hui et de demain.

Avec l'un des plus vastes portefeuilles de produits de l'industrie, STMicroelectronics fournit à ses clients des solutions innovantes couvrant toute la gamme des applications électroniques, dont l'Internet des objets. Par l'utilisation croissante de la technologie qui permet de mieux profiter de la vie, STMicroelectronics est synonyme de « life.augmented ».

STMicroelectronics permet de réaliser des prototypes rapidement et au meilleur coût, avec une offre complète d'écosystèmes de développement compatibles, parmi lesquels des outils de développement matériels et logiciels, des modules et des composants d'évaluation avec logiciels pré-embarqués pour applications verticales et compatibilité sur le cloud.

L'avenir de l'Internet des objets signifie que des milliards d'appareils doivent communiquer entre eux et avec les serveurs d'application via Internet, sans que les usagers n'aient besoin d'intervenir. Cela implique l'intégration d'une multitude de logiciels, de micro logiciels et de matériel afin que chaque appareil parle le même langage.

Les communications et la connectivité sont essentielles et influencent profondément l'architecture des solutions IoT, mais elles introduisent aussi de nouveaux défis.

Dans ce cadre, STMicroelectronics souhaite adresser les deux défis de la connectivité : l'interopérabilité et la sécurité dans l'IoT.

L'interopérabilité est un défi parce que l'IoT doit permettre aux appareils de parler différents langages à travers des protocoles de communication aussi variés que l'infrastructure ou le réseautage ad-hoc allant du WiFi, Thread, ZigBee et Bluetooth, au Sigfox, LoRaWAN et plus encore.

La sécurité est un défi largement illustré par les attaques basées sur l'IoT qui sont déjà une réalité. Une enquête récente de Gartner, a révélé que près de 20 % des organisations ont observé au moins une attaque basée sur l'IoT au cours des trois dernières années. Pour se protéger contre ces menaces, Gartner, Inc. prévoit que les dépenses mondiales pour la sécurité de l'IoT atteindront 1,5 milliard de dollars en 2018, soit une augmentation de 28 % par rapport à 2017 (1,2 milliard de dollars).

Les défis ont été adressés grâce à deux cas d'usage avec pour objectif de répondre à cette question :

Comment concilier des besoins antinomiques telles que la sécurité et l'interopérabilité?

DOMOTIQUE SÉCURISÉE

life.augmented

2 J

Solution

STMicroelectronics a prototypé deux plateformes matérielles pour STM32 :

- **un nœud IoT gateway;**
- **un nœud IoT connecté au cloud.**

Au départ, STMicroelectronics a développé une solution IoT flexible qui est capable de supporter différents protocoles tout en garantissant une flexibilité logicielle, une sécurité matérielle et une solution à faible coût.

Le nœud IoT gateway basé sur STM32 est un hub central qui est un concentrateur de nœuds IoT. Cette gateway interconnecte les nœuds IoT avec le cloud et traite les données de manière sécurisée et fiable. Elle fournit la traduction entre les différents protocoles et assurent le routage des données entre les nœuds IoT et le cloud.

Le nœud IoT connecté au cloud intègre une gateway simplifiée qui assure une connexion directe au cloud.

Ces plateformes matérielles ont permis d'intégrer la solution ProvenCore-M développée par Prove & Run qui fournit une solution répondant à des problématiques de sécurité avancées.

Les équipes de STMicroelectronics ont travaillé avec Prove & Run pour répondre aux problématiques de cybersécurité IoT :

- **au démarrage du nœud IoT, pour s'assurer que le produit est bien celui qu'il prétend être;**
- **lors de l'utilisation du nœud IoT, pour vérifier que la communication extérieure ne soit pas dangereuse pour le produit.**

Résultats et bénéfices

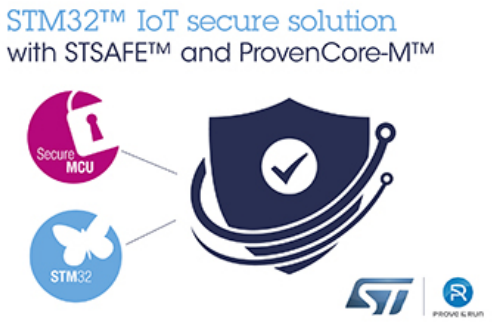
Grâce au portage de ProvenCore-M dans la solution STM32, les noeuds IoT basés sur STM32 offrent une sécurité renforcée.

ProvenCore-M est en effet un système d'exploitation sécurisé pour les dispositifs embarqués, dont STM32.

ProvenCore-M renforce ainsi les propriétés de sécurité sur STM32 et permet de garder un contrôle total sur toutes les situations de blocage et attaques de type DoS (attaques par déni de service) qui peuvent survenir dans un noeud IoT qui communique avec le cloud.

La nouvelle Plateforme S3P basée sur STM32 et ProvenCore-M facilite donc la création de produits IoT hautement sécurisés, tout en permettant aux clients de se concentrer sur le développement de la partie fonctionnelle de leur application.

Les développeurs de produits sans compétences particulières en matière de sécurité, bénéficieront de services déjà validés et éprouvés tels que l'isolation des applications, le démarrage sécurisé, la mise à jour sécurisée du firmware et le stockage des clés résistant aux attaques physiques.



3

A « Safe and Secure » coopération KRONO-SAFE et Prove & Run

B Gateway pour l'IoT – Prove & Run

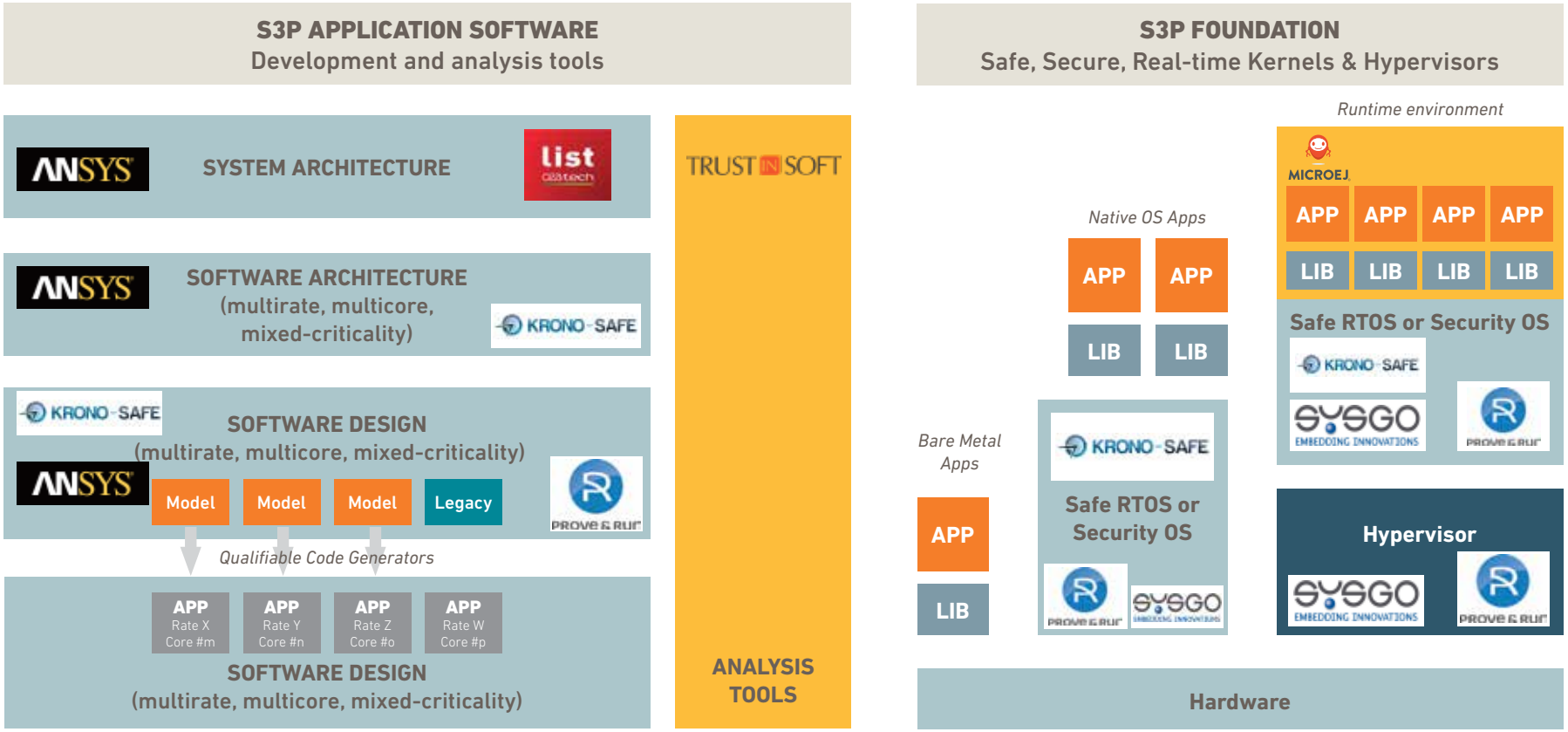
C Modélisation et génération des codes - ANSYS

D Safe, quick and low cost - MicroEJ

LES THÉMATIQUES TRANSVERSALES

LES TECHNOLOGIES S3P

Le projet S3P veut relever le défi de créer une plateforme pour l'embarqué, temps réel, critique et sécuritaire. Pour atteindre cet objectif, S3P fait plus que proposer un ensemble de réalisations, elle fournit également les outils nécessaires. En effet, S3P fournit des outils de conception pour mettre au point des modèles aussi bien systèmes que logiciels afin de garantir le plus haut niveau d'excellence et répondre aux normes les plus exigeantes, telles que celles des domaines avioniques, ferroviaires, distribution électriques... Au travers des cas d'usage, S3P s'est attaché à trouver des solutions techniques s'intégrant dans les processus les plus contraints. Le schéma ci-dessous détaille comment les solutions S3P, grâce à leur complémentarité, répondent aux différents enjeux métiers.



La complexité des systèmes et le réglementaire, inhérent à des secteurs où la sécurité entraîne des enjeux vitaux, imposent de passer par une phase de conception amont au développement logiciel : la phase de définition de l'architecture système.

Cette phase a pour but d'obtenir des modèles cyber-physiques et temporels du cycle de vie du produit qui permettent de mieux définir les exigences critiques.

Pour répondre à ces enjeux, S3P a utilisé des solutions logicielles permettant de définir les exigences systèmes et s'assurer que celles-ci soient respectées jusque dans le binaire produit.

S3P a rassemblé des solutions techniques allant du matériel à un environnement multiplateformes intégrant une solution de magasin d'applications, en incluant des solutions pour garantir la sécurité et la sureté de fonctionnement de ces applications.

3A

SAFE AND SECURE

Le secteur aéronautique est en train de vivre une mutation profonde : l'architecture électronique des avions doit s'ouvrir de plus en plus sur le monde extérieur pour échanger et exploiter toujours plus d'informations. Cela se traduit par l'utilisation de capteurs qui génèrent d'énormes quantités de données à chaque vol, des fonctions de maintenance au sol de plus en plus sophistiquées et des services aux passagers tel qu'un accès Internet pour un meilleur confort. En conséquence, les systèmes critiques embarqués dans les avions autrefois isolés et dédiés uniquement à assurer des fonctionnalités de sûreté, deviennent de plus en plus sensibles aux problématiques de cybersécurité.

Dans le secteur industriel, cela est associé au concept selon lequel les machines intelligentes, les systèmes d'information, les appareils et les personnes sont interconnectés. Cette connexion permet de prendre de meilleures décisions avec le support de grandes bases de données et d'analyses avancées. Cet aspect est très important pour les usines qui deviennent de plus en plus intelligentes. On assiste à une amélioration significative et croissante de la capacité à collecter, analyser et distribuer des données converties en informations importantes. Cela permet, tout particulièrement d'aider les usines dans l'optimisation de leurs opérations de maintenance grâce au partage et à l'analyse des données avec les différents services concernés.

Or jusqu'à maintenant, sûreté et sécurité sont adressées séparément au niveau physique en dupliquant les calculateurs (exemple : une passerelle mise en amont d'un calculateur de contrôle-commande). Une telle solution est la résultante de décisions historiques : afin d'éviter la gestion sécuritaire d'un système critique, ce dernier est isolé (non ouvert vers l'extérieur). Une telle approche est dorénavant obsolète. Un des enjeux des systèmes cyber-physiques de demain est de définir ce que deviennent les systèmes critiques dans un monde ouvert. Qu'est ce qui peut être autorisé sans impacter la sûreté ? Comment les contraintes de sécurité peuvent-elles être contrôlées en accord avec les exigences de sûreté ? Comment construire des systèmes à échelle industrielle tout en démontrant que les attaques sont inoffensives sur les fonctions critiques ? Toutes ces questions requièrent une réponse qui traite sécurité et sûreté simultanément.

Ainsi, dans le cadre du projet S3P, les deux sociétés KRONO-SAFE et Prove & Run ont été sélectionnées dans le but d'intégrer leurs technologies respectives, ASTERIOS et ProvenCore, et de délivrer une plateforme « Smart, Safe and Secure » (S3P) répondant aux défis des marchés aéronautiques et des objets industriels de l'Internet (Industrial IoT).

KRONO-SAFE développe et commercialise ASTERIOS, une solution d'ingénierie unique et innovante pour la conception, l'intégration et l'exécution d'applications embarquées temps réel complexes et critiques sur plateforme matérielle multi-cœur.

La solution **ASTERIOS** est constituée d'une suite d'outils logiciels intégrés et d'un noyau temps réel certifiable combinant trois innovations majeures :

- **un nouveau formalisme pour exprimer le parallélisme et le partitionnement;**
- **une nouvelle approche pour garantir le déterminisme et la performance;**
- **une nouvelle suite d'outils pour automatiser la génération des tables d'exécution.**

Prove & Run est un éditeur logiciel en pleine croissance dont la mission est d'aider ses clients à résoudre les défis de cybersécurité liés au déploiement à grande échelle des périphériques connectés et de l'Internet des objets.

La principale source des problèmes de cybersécurité peut être attribuée soit à des mesures de sécurité inappropriées, soit à des logiciels défectueux où les défauts d'architecture, de conception, d'implémentation ou de configuration créent des vulnérabilités potentiellement exploitables pour des attaques. Le défi est donc de produire un logiciel le plus proche possible du zéro défaut.

Prove & Run développe et commercialise les produits suivants :

ProvenCore : un micro-noyau formellement prouvé du point de vue sécurité (première mondiale) pour sécuriser les Smartphones, tablettes, passerelles, routeurs, concentrateurs et périphériques connectés ;

ProvenVisor : un hyperviseur formellement prouvé du point de vue sécurité pour les périphériques connectés et les solutions de virtualisation de l'Internet des objets (en cours de développement - bientôt disponible, sera également une première mondiale).

Safran Electronics & Defense et Schneider Electric, deux sociétés leaders respectivement sur les marchés de l'aéronautique et des objets industriels de l'internet, ont fourni chacun un cas d'utilisation employé comme banc d'essai pour le développement d'une Plateforme S3P.

SAFE AND SECURE

PROVE & RUN

KRONO-SAFE

3A

Cas d'utilisation Schneider Electric

La nécessité pour Schneider Electric de connecter ses équipements pour applications critiques au monde ouvert, pour la maintenance prédictive et/ou le contrôle à distance, a été un des cas d'utilisation proposé à KRONO-SAFE et Prove & Run pour le développement d'une Plateforme S3P.
Les deux sociétés ont collaboré à la mise au point de cette plateforme en utilisant un SoC propriétaire de Schneider Electric (LCES-2) basé sur une architecture hétérogène multi-cœur (ARM Cortex®-A7 et ARM Cortex®-M3).

Le choix a été d'assigner les cœurs selon le schéma ci-dessous :

- **Cluster ARM Cortex®-A7 dédié à l'interface avec le monde ouvert (« Open World »). ProvenCore est utilisé comme un système d'exploitation sécurisé (également appelé Trusted Execution Environment) à côté du système d'exploitation Linux : ProvenCore est isolé de Linux en s'appuyant sur le mécanisme matériel ARM TrustZone® et héberge les services de sécurité nécessaires pour protéger Linux et le système à base de ARM Cortex®-M3 avec ASTERIOS;**
- **ARM Cortex®-M3 isolé pour ASTERIOS (mission / temps réel / sûreté de fonctionnement).**

Cette solution repose sur l'isolation matérielle, garantie par la technologie ARM TrustZone® et des mécanismes de partitionnement spatial type MMU/MPU, afin d'isoler le composant cybersécurité de celui de la sureté de fonctionnement.

L'avantage de cette approche est que, puisqu'il n'y a aucune dépendance logicielle, le monde de la cybersécurité pourrait être certifié indépendamment du monde de la sûreté de fonctionnement.

Cas d'utilisation Safran Electronics & Defense

La nécessité pour Safran Electronics & Defense d'offrir des nouveaux services, comme par exemple la surveillance et l'optimisation des systèmes critiques de contrôle moteur (FADEC), et donc d'héberger des fonctions critiques (contrôle moteur) à côté d'autres fonctions non critiques (surveillance, optimisation), a été l'autre cas d'utilisation pour le développement d'une Plateforme S3P spécifique au monde aéronautique.

Les résultats attendus par l'utilisation d'ASTERIOS étaient les suivants :

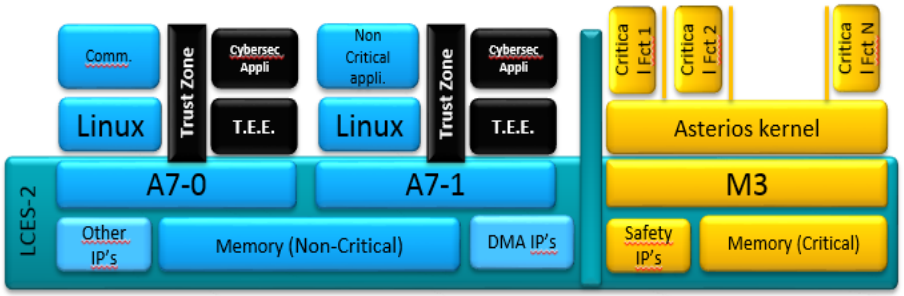
- **génération de codes entièrement automatisée;**
- **évaluation et démonstration des mécanismes de ségrégation pour différents niveaux de criticité.**

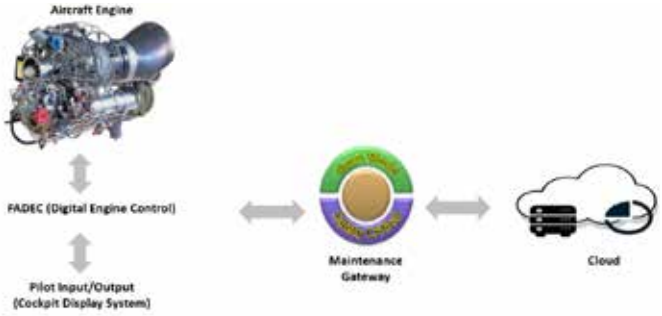
Le résultat attendu par l'utilisation de ProvenCore était le développement d'une passerelle de maintenance dédiée pour isoler le FADEC, critique en termes de sécurité, du monde extérieur.

La passerelle de maintenance dispose d'un processeur ARM Cortex®-A exécutant Linux et ProvenCore. Ce dernier agit comme un système d'exploitation sécurisé s'appuyant sur un mécanisme d'isolation matérielle ARM TrustZone®. ProvenCore héberge les services liés à la sécurité qui sont nécessaires pour protéger Linux et les opérations critiques de sécurité telles que :

- **démarrage sécurisé et résilience de la plateforme;**
- **protocoles de communication de confiance;**
- **filtrage des commandes.**

L'avantage de cette solution combinée est la disponibilité d'une pile technologique modulaire permettant l'intégration optimale des composantes sûreté de fonctionnement et cybersécurité au sein d'un calculateur unique.





3

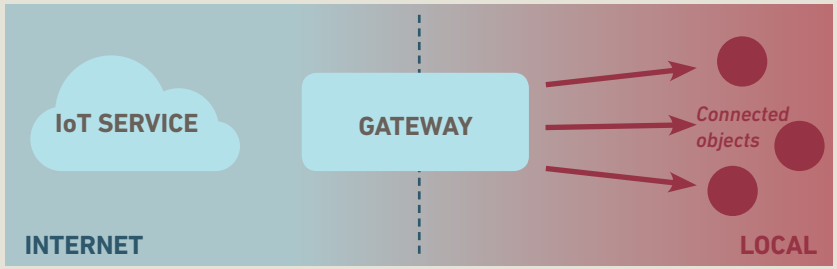
GATEWAY POUR L'IoT

PROVE & RUN

3 B

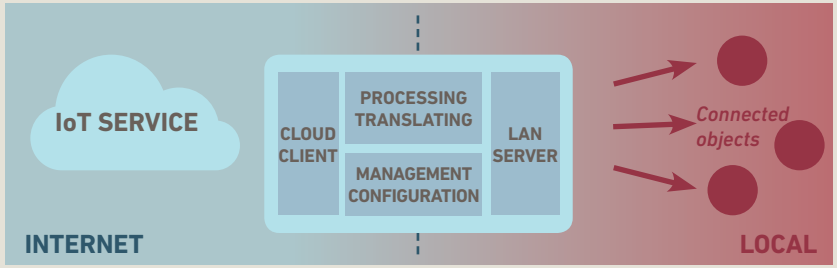
Description des Gateway IoT

Une passerelle physique IoT établit un pont entre les appareils IoT, les capteurs, les équipements, les systèmes et le cloud afin de faciliter leur communication comme représenté dans le schéma ci-dessous :



Comme leur nom l'indique, les passerelles IoT permettent donc d'établir un pont entre l'opérationnel et l'infrastructure informatique dans une entreprise. Elles s'appuient pour cela sur les données qu'elles collectent et traitent en temps réel « sur le terrain » et à la périphérie du réseau pour optimiser les performances du système.

En connectant de manière systématique « le terrain » avec le cloud, les passerelles physiques IoT remplissent plusieurs fonctions critiques que l'on peut décomposer en quatre groupes fonctionnels majeurs :



- **un client cloud** à travers lequel la passerelle se connecte à son service IoT dans le cloud et assure une protection contre les connexions non désirées. Le client cloud doit être la seule connexion à Internet et il inclut la totalité de la pile réseau qui gère cette connexion;
- **un serveur LAN et un gestionnaire de périphériques,** à travers lesquels la passerelle se connecte à ses objets connectés, en utilisant un certain nombre d'interfaces réseau LAN. Il inclut tous les pilotes pour les protocoles de bas niveau acceptés par la passerelle, ainsi que le code de base pour la gestion de ces objets;
- **certaines applications de traitement et de traduction** (« Processing Translating »), qui interfacent entre les objets connectés et le cloud, avec quelques transformations locales allant de la simple traduction de protocole réseau à un traitement de périphérie complexe spécifique au cas d'usage industriel;
- **certaines fonctions de gestion et de configuration** (« Management Configuration ») qui prennent en charge la gestion locale et à distance de la passerelle et des objets qui y sont connectés. Il s'agit d'une extension du client cloud, dédiée à la gestion, incluant certaines fonctions de gestion des périphériques telles que la mise à jour du firmware et la gestion des cycles de vie des périphériques.

En plus de ces quatre groupes, la passerelle comprendra une plateforme d'exécution fournissant des fonctions de base sur lesquelles tous les services sont construits.

3C

MODÉLISATION ET GÉNÉRATION DE CODE

ANSYS

Le projet S3P a pour but de définir une plateforme Smart, Safe and Secure en fournissant des briques inter-opérables. Dans ce chapitre, nous nous intéressons aux briques liées à la modélisation des applications et à la production de codes jusqu'à la cible finale.

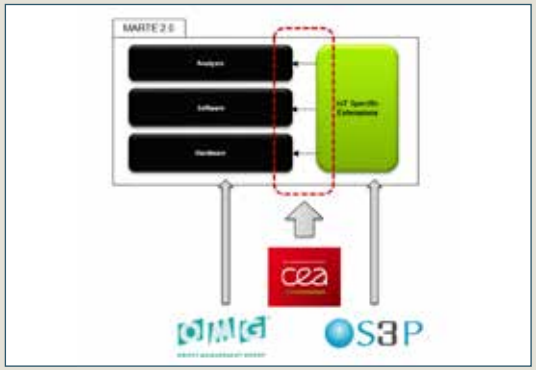
Un premier aspect très général de la modélisation est l'utilisation de modèles spécifiques. Plusieurs types de modèles selon les phases de développement peuvent co-exister et ont besoin de rester en cohérence. La technique de **co-évolution** répond à cette question.

Un second aspect concerne la diversité des ***frameworks*** dédiés et de nouveaux matériels qui apparaissent pour concevoir les systèmes IoT. Pour aider les concepteurs dans leur tâche, le projet contribue au développement d'un langage unifié, **IoTML** (Internet of Things Modeling Language).

Enfin, le projet S3P s'intéresse à la spécification détaillées des applications et à leur codage. Les applications sont **multi-fréquences** et **multi-coeurs**. Ces deux aspects introduisent un niveau de complexité supérieur par rapport à un développement mono-tâche ou mono-cœur. La solution proposée autour des outils **SCADE-ASTERIOS** facilite la tâche du concepteur et réduit les coûts et le temps de développement.

La technique de **co-évolution**, à laquelle participe Thales et qui est mise en œuvre dans l'outil Capella, permet la réalisation de ***bridges***.

Il est courant d'utiliser différents modèles qui peuvent évoluer de manière disjointe et parallèle, mais sont néanmoins reliés par les concepts qu'ils manipulent. Il est donc nécessaire de conserver cette relation conceptuelle et d'être en mesure de synchroniser les modèles à certains points de leurs cycles de vie. Il ne doit pas y avoir d'hypothèse sur les cycles de vie, mais il faut être en mesure de formaliser la relation par une association, ou mapping explicite.



Un bridge est donc un élément logiciel qui prend en compte l'association entre deux modèles et réalise la synchronisation. Cette technique de co-évolution renforce la stricte séparation entre la logique de mapping et la logique de mise à jour. Les travaux réalisés sont faits dans le cadre de la Fondation Eclipse.

Un mécanisme semblable est mis en œuvre dans l'outil SCADE Architect d'ANSYS afin de synchroniser les modèles représentant une architecture logicielle avec les modèles de conception réalisés avec l'outil SCADE Suite.

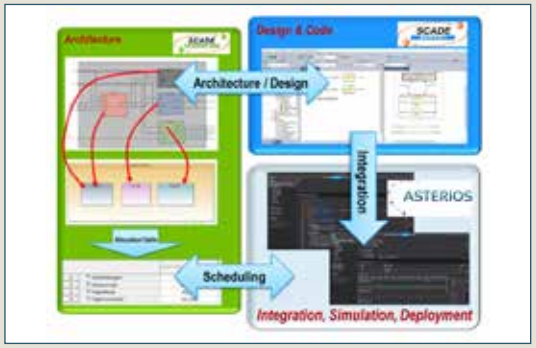
Un système IoT est un système cyber-physique. Ce type de système est fortement **distribué** (les nœuds de calculs sont physiquement répartis), **connecté** (accès à un ou plusieurs réseaux via les ondes radio ou un câblage) et **contraint** (puissance de calcul, énergie disponible, portée des télécommunications, etc.) par la plateforme physique sur laquelle il évolue. A l'heure actuelle, la conception de ces systèmes est principalement orientée par l'émergence de nouveaux ***frameworks*** de développement ainsi que de nouveaux matériels (***gateways***, capteurs, etc.) créés spécifiquement pour le domaine de l'IoT.

Afin d'affranchir les concepteurs de systèmes IoT d'une technologie ou d'une méthode de conception imposée par les outils disponibles, le consortium S3P (et plus spécifiquement le CEA) contribue au développement d'un langage unifié.

Ce langage, baptisé IoTML, identifie les concepts communément admis et utilisés dans le domaine de l'IoT. Il est également agrémenté d'un cadre architectural permettant aux concepteurs de se focaliser sur les préoccupations principales (description logicielle, description matérielle, sureté, sécurité, etc.) auxquelles doivent répondre ces systèmes.

Etant donné que les systèmes IoT relèvent très souvent du domaine des systèmes embarqués temps réel, le langage IoTML est défini comme étant une extension du profil UML MARTE (Modeling and analysis of Real –Time and Embedded Systems). MARTE est un standard OMG largement utilisé dans l'industrie, pour la conception et la spécification de modèles de conception et d'analyse pour les systèmes temps réel. Le langage IoTML fera partie intégrante de la version 2.0 de MARTE dont la définition a été initiée à l'OMG. Une implémentation du langage est fournie par l'outil de modélisation Papyrus, spécialisé pour le domaine de l'IoT. Cet outil est open source et peut directement être installé sur la plateforme Eclipse.

MODÉLISATION ET GÉNÉRATION DE CODE



La Plateforme S3P permet aussi de supporter des éléments IoT industriels qui peuvent être des moteurs d'avions, des éoliennes. Il s'agit d'objets avec lesquels le besoin de communication et de contrôle à distance devient important. La dimension **sûreté** et **déterminisme** est particulièrement critique pour ces objets. Les environnements SCADE Suite d'ANSYS et ASTERIOS de KRONO-SAFE permettent d'adresser efficacement ce type de développement en respectant les standards industriels (DO-178C, IEC 61508,...). Les plateformes finales utilisent des systèmes d'exploitation devant offrir des garanties, ce qui les cas de PikeOS de SYSGO et ASTERIOS RTK de KRONO-SAFE. Le projet S3P a permis l'assemblage de ces environnements.

L'architecture d'une application embarquée contient différentes fonctionnalités communiquant entre elles. Ces fonctionnalités ou groupe de fonctionnalités, s'exécutent de manière cyclique, avec des rythmes différents.

Ainsi, une fonctionnalité de pré-traitement des données devra opérer plus vite qu'une fonctionnalité de calcul qui elle-même opère plus vite qu'une fonction de surveillance. La difficulté consiste à trouver la bonne architecture temporelle (ou dynamique) et d'en faire une réalisation efficace en terme de communication et d'activation des tâches.

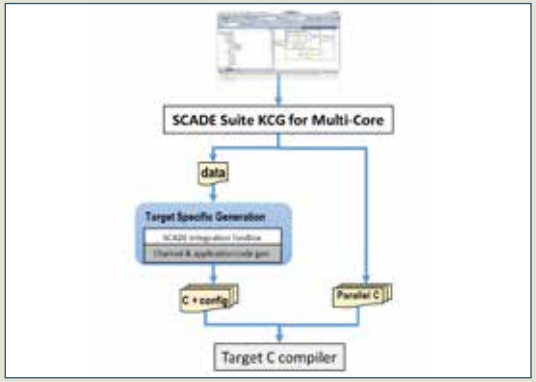
L'architecture fonctionnelle et dynamique est donc décrite en utilisant l'outil SCADE Architect, basé sur SysML/Papyrus. Les fonctionnalités, les communications et les différents délais ou cycles d'exécution sont ainsi définis à haut niveau. Des vérifications de cohérence peuvent déjà être effectuées (exemple : propagation des données).

Deux activités sont ensuite menées. D'une part, l'analyse d'ordonnancement avec ASTERIOS et d'autre part, la conception des fonctionnalités avec SCADE Suite. A partir des informations topologiques et temporelles décrites dans l'architecture, la faisabilité de l'ordonnancement et son optimisation sont faites dans l'environnement ASTERIOS. L'architecture est reliée avec la phase de conception grâce à la synchronisation entre les outils SCADE Architect et Suite, d'où une cohérence du flot de conception. Les fonctionnalités sont conçues comme des modèles Scade puis le code C certifiable est automatiquement produit. Les fonctions sont testées et validées à travers les outils de la chaîne SCADE.

La phase d'intégration est automatiquement assurée par l'outil ASTERIOS. Une simulation fonctionnelle et un réglage fin des budgets temps sont faits avant transfert sur cible.

Enfin, les applications peuvent être multi-cœurs. Le projet S3P réalise un générateur multi-cœurs de code C générique depuis Scade, qui a été mis en œuvre sur PikeOS. Le principe consiste à annoter les éléments de conception définis dans le modèle Scade. L'ingénieur fait ainsi un découpage de ce qu'il considère comme des éléments susceptibles d'être parallélisés. Son choix est validé par le générateur de code qui va produire à partir du modèle annoté, un code sous forme d'un réseau de Kahn de fonctions C. Ces fonctions communiquent par des canaux qu'il faut réaliser sur la plateforme finale. Les données produites sont consultables à travers une API en Python. Un fournisseur de plateforme peut donc compléter ces données avec ses informations sur la plateforme pour faire l'allocation des fonctions sur les cœurs, ainsi que la réalisation des communications. Le couplage avec PikeOS démontre la réalisation d'un flot depuis un modèle de conception indépendant de la plateforme jusqu'à sa réalisation effective. Ce travail fait suite à d'autres travaux menés sur les plateformes MMPA de Kalray ou Aurix d'Infineon et montre la pertinence de l'approche.

Un éco-système se met donc en place grâce au projet S3P. La modélisation de systèmes IoT ainsi que leur réalisation logicielle, bénéficient des liens entre les partenaires pour plus d'efficacité.



3D

SAFE, QUICK AND LOW COST - UN STANDARD POUR MONÉTISER À FAIBLE COÛT L'INTELLIGENCE DES APPAREILS ÉLECTRONIQUES DU QUOTIDIEN

MICROEJ

Réduisant la complexité des logiciels embarqués, les plateformes d'exécution structurent les écosystèmes logiciels et organisent les masses critiques économiques, produits et emplois, en étant la principale interface entre la puce électronique et le logiciel applicatif porteur d'une grande partie de la valeur et de la fonction à réaliser. La baisse drastique des coûts des composants de communications radio (Wifi, Bluetooth, LTE, Zigbee), permet de généraliser l'interconnexion des appareils électroniques du quotidien à la fois personnel et professionnel. Le premier écosystème qualifié d'Internet des objets (IoT) est l'écosystème des smartphones, tous différents du point de vue des matériels électroniques avec des millions d'applications indépendantes des matériels électroniques, et la virtualisation Android, qui fait l'interface entre ces applications simples à écrire et ces matériels électroniques.

Des processeurs bas coûts en milliards, des composants de communication bas coûts à foison, il ne manque, à coté de ce gigantesque champ des possibles technique, que la dimension économique : comment monétiser l'usage d'une flotte d'appareils hétérogènes, tous plus ou moins interconnectés à un cloud ?

C'est le thème central du projet S3P qui a pour but de définir une plateforme Smart, Safe and Secure pour les appareils constituant un écosystème IoT. Il s'agit de fournir les briques inter-opérables entre les différents fournisseurs de technologies pour baisser drastiquement les coûts de réalisation de ces écosystèmes IoT, pour permettre l'émergence rapide de flux de revenus data et/ou de management de flottes, ou encore de réaliser des économies d'usage par de meilleurs diagnostics.

Dans cet article, nous nous intéressons aux briques IoT liées à la modélisation des applications, sous formes de composants logiciels standards et assemblables afin de premièrement, définir une Plateforme S3P et deuxièmement, de permettre de définir une application IoT qui exécute sa logique applicative répartie sur les appareils de la Plateforme S3P, dans un cadre sécurisé et économiquement viable.

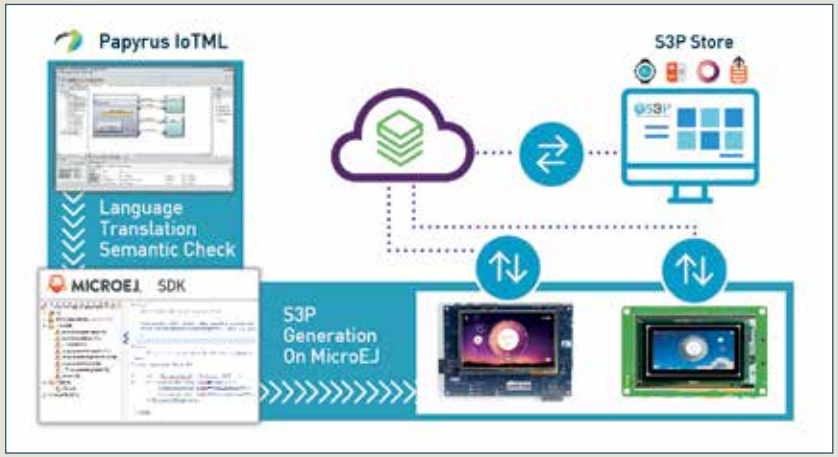


Figure 1: Plateforme S3P générée depuis sa description en IoTML.

La Plateforme S3P est générée, notamment ses communications implicites (en mode publish/subscribe) entre les différents constituants physiques qui exécutent la virtualisation sécurisée MicroEJ VEE. Les applications applicatives, comme une régulation de température, sont chargeables depuis un store d'applications compatibles S3P.

MicroEJ, avec ses partenaires au sein du consortium S3P et en s'appuyant sur plus de 15 études de cas représentatives de l'IoT dans de multiples domaines, a étudié et contribué à définir les briques sur étagère pour un IoT standard. Cela regroupe :

- **Les agents de communication, les différents formats de payloads, les divers protocoles de management, les moyens nécessaires pour réaliser des updates de code total et partiel Over The Air;**
- **Le domaine transversal de la sécurisation des données avec les outils de cryptographie, ainsi que la sécurité associée aux systèmes critiques (temps réel dur et déterminisme);**
- **Les outils de simulation du code, ainsi que la modélisation système ou ontologie IoT;**

SAFE, QUICK AND LOW COST - UN STANDARD POUR MONÉTISER À FAIBLE COÛT L'INTELLIGENCE DES APPAREILS ÉLECTRONIQUES DU QUOTIDIEN

MICROEJ

3 D

- **Le développement d'un langage unifié IoTML qui permet de bien séparer la construction des éléments d'infrastructure d'exécution, notamment l'usage de technologies de virtualisation comme Android et/ou MicroEJ VEE;**
- **La validation sur une grande variété de cibles matérielles MCU/MPU/SoC IoT économiques avec nos partenaires NXP, ST, Renesas, ainsi que les « System-on-Chip vendors » comme Espressif, Murata, Sony, pour accéder aux marchés très gros volumes, comme les Wearables, la maison, l'électroménager, l'industrie, l'automobile, les telecom, etc;**
- **La compatibilité de MicroEJ VEE avec les autres produits des éditeurs francais de l'embedded, comme ANSYS, Thales, KRONO-SAFE, TrustInSoft, SYSGO, Prove & Run.**

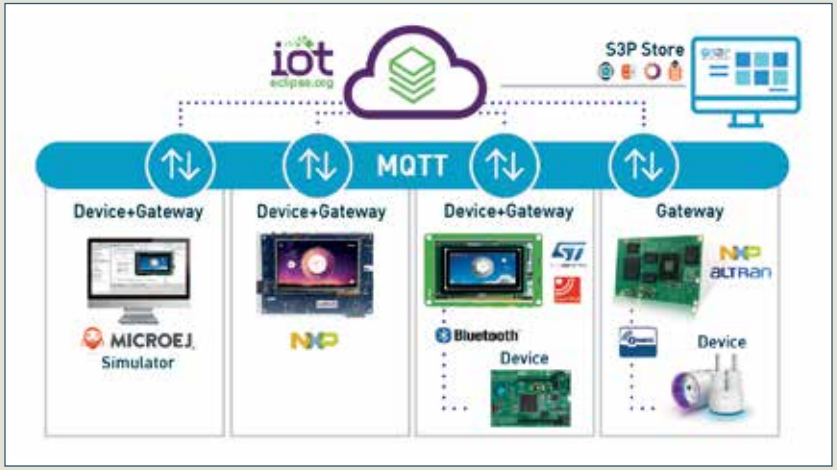


Figure 2 : Plateforme S3P typique avec plusieurs appareils connectés à un cloud.

Les appareils au sein d'une Plateforme S3P jouent parfois le rôle de gateway, plusieurs réseaux de transport peuvent cohabiter de manière transparente et les applications proviennent d'un même store d'applications. Bien que les appareils soient matériellement différents, la virtualisation MicroEJ VEE sécurisée permet leur exécution simplement dans un cadre compatible S3P.

Un écosystème IoT « cluster France » se met donc en place grâce au projet S3P, la modélisation de systèmes IoT, ainsi que les réalisations de briques standards, pour les plus grands bénéfices des acteurs et clients de la filière, faisant effet de levier sur les fertilisations croisées des partenaires du projet.

Ainsi, les acteurs du projet S3P, avec MicroEJ, ont pu réduire la complexité d'un système IoT pourtant basé sur un marché du hardware très fragmenté, en diminuant le coût du design et de la production des appareils électroniques destinés à la « monétisation IoT ». A travers S3P, et le renforcement de son positionnement IoT, MicroEJ a pu ainsi étendre sa plateforme logicielle VEE, et s'inscrire dans les traces de son ainé Android, un des champions de la virtualisation.

BESOINS DES ENTREPRISES	SOLUTION PROPOSÉE PAR MicroEJ ET S3P
Simplifier la conception • Rapidité de mise sur le marché et adaptation rapide au marché	**Processus simple** • Simulation de codes et dispositifs virtuels • Conception parallèle HW et SW • Tests automatiques massifs • Réutilisation entière du code et création d'actifs de logiciels binaires
Design-to-Cost & Design-to-Value • Augmenter le chiffre d'affaires et la marge	
Livraison dans les délais et dans les limites du budget. • Réduction des coûts de développement de l'équipe R&D	**Bibliothèques standards** • Interface utilisateur, IoT, Numérique, • Sécurité, Communication, HAL, Réseau, Fichier, ... • Toutes les architectures HW, tous les RTOS, tous les linkers ELF.
Innovation en matière de produits et de marques	
Innovation incrémentale et création d'actifs • De fortes synergies de coûts entre les lignes de produits. Avoir une interface commune de produits et de plateformes	**Couches sécurisées** • Couche de virtualisation, Crypto, mises à jour OTA

Coût R&D des appareils ➜ **20 à 50% de réduction des coûts R&D**
Bill of Material des appareils ➜ **10-15% de réduction des coûts unitaires des appareils**
Réduction du délai de mise sur le marché ➜ **-40% à -70% temps en moins**

À PROPOS

Développement de logiciels et de systèmes critiques embarqués

ANSYS est le leader mondial des solutions de génération de code, de vérification et de conception orientée modèle pour le développement de logiciels et de systèmes critiques embarqués, avec une gamme complète de produits **ANSYS SCADE® :**

- **SCADE Suite® pour le développement d'application de Contrôle et Logique;**
- **SCADE Display® pour le développement d'application de Conception Graphique et HMI;**
- **SCADE Architect pour le Design d'architecture de système;**
- **SCADE LifeCycle® pour le management du cycle de vie d'application critique;**
- **SCADE Test pour l'environnement de Test.**

ANSYS propose un environnement de développement et de simulation de logiciels embarqués basé sur des modèles et doté d'un générateur automatique de code intégré afin d'accélérer les projets de développement de logiciels embarqués.

Générateur de code certifié

Les générateurs de code SCADE ont été certifiés selon le plus haut niveau de sécurité dans six segments de marché différents par plus de dix autorités de sécurité dans le monde entier :

- **DO-178C jusqu'au niveau A - Applications de défense et aérospatiales par FAA, EASA, Transport Canada et ANAC;**
- **IEC 61508 jusqu'à SIL 3 – Applications industrielles et de transport par TÜV SÜD;**
- **EN 50128 jusqu'à SIL 3/4 – Applications de transport ferroviaire par TÜV SÜD, EBA et Certifer;**
- **Conformité à IEC 60880 démontrée – Applications nucléaires par les autorités de sûreté nucléaire;**
- **ISO 26262 jusqu'à ASIL D – Applications automobiles par TÜV SÜD.**

ANSYS SCADE accélère le processus de développement des logiciels embarqués :

- **alignement du processus de conception conformément aux objectifs des normes de sécurité;**
- **réduction des coûts de développement de 50 pour cent, en moyenne;**
- **accélération de certification par un facteur deux.**

PLUS D'INFOS
www.ansys.com

Contrôle-commande numérique

KRONO-SAFE est une société privée fondée en 2011 pour commercialiser des technologies logicielles hautement fiables développées et utilisées à l'origine pour des systèmes de contrôle-commande numériques employés à des fins de sûreté nucléaire.

KRONO-SAFE développe et commercialise **ASTERIOS®**, une solution d'ingénierie unique et innovante pour la conception, l'intégration et l'exécution d'applications embarquées temps réel complexes et critiques sur plateforme matérielle multi-cœur.

La solution ASTERIOS permet de réaliser des gains de productivité très significatifs, pouvant aller jusqu'à 90% lors de la phase d'intégration logicielle et matérielle (optimale et automatisée). Elle est constituée d'une suite d'outils logiciels intégrés et d'un noyau temps réel certifiable combinant 3 innovations majeures :

- **un nouveau formalisme pour exprimer le parallélisme et le partitionnement;**
- **une nouvelle approche pour garantir le déterminisme et la performance;**
- **une nouvelle suite d'outils pour automatiser la génération des tables d'exécution.**

KRONO-SAFE adresse les marchés en quête d'une solution plus sûre et plus efficace pour développer des applications complexes à criticité mixte, telles que : l'aéronautique, la défense, l'automobile, le transport, l'énergie et l'IoT industriel.

Avec une équipe d'une cinquantaine d'experts et de cadres chevronnés, KRONO-SAFE propose des solutions logicielles innovantes visant à servir efficacement ses clients. La société détient un portefeuille de brevets et poursuit activement ses activités d'innovation technologique et son déploiement à l'international.

PLUS D'INFOS
www.krono-safe.com

À PROPOS

Le List, institut de CEA Tech, focalise ses recherches sur les systèmes numériques intelligents. Porteurs d'enjeux économiques et sociétaux majeurs, ses programmes de R&D sont centrés sur le manufacturing avancé, les systèmes cyber-physiques, l'intelligence artificielle et la santé digitale. En développant une recherche technologique de pointe, avec des applications dans des domaines industriels variés (les transports, la défense et la sécurité, l'industrie, l'énergie, ...), le List permet à ses partenaires industriels d'améliorer leur compétitivité grâce à l'innovation et au transfert technologique.

Le List couvre tous les aspects du développement des logiciels et des systèmes embarqués en offrant des méthodes, des outils et des composants qui permettent d'optimiser la qualité et la performance des systèmes. Les aspects architecture, matériel et logiciel sont intégrés au service de la performance globale du système, quelle que soit sa complexité : système multifonctions, système critique, gestion du big data...

Les ingénieurs-chercheurs du List se consacrent à cinq sujets en intégrant les exigences de sûreté, sécurité, fiabilité et performance :

- **conception et analyse;**
- **validation et vérification;**
- **intégration de capteurs;**
- **composants et IPs pour la fiabilité, la sûreté et la sécurité;**
- **architectures de calcul.**

Grâce à la qualité de ses partenariats de recherche, le List est labellisé Institut Carnot depuis 2006 (Institut Carnot TN@UPSaclay).

Plus d'information sur : **@CEA_List | LinkedIn | YouTube.**

PLUS D'INFOS
www-list.cea.frn

MicroEJ est la seule Plateforme S3P applicative standard pour appareils électroniques économiques, potentiellement connectés, qui permet de concevoir des applications intelligentes à faible coût, et de déployer ces dernières n'importe où, sur n'importe quel dispositif électronique.

De même qu'Android a su transformer les téléphones en Smartphone, MicroEJ transforme les Things en Smart Things. Et déjà, plusieurs dizaines de millions d'appareils sont « Powered by » MicroEJ.

L'entreprise possède des bureaux en Europe et aux États-Unis et se déploie en Asie. MicroEJ est ainsi le leader des plateformes logicielles embarquées standard : appareils électroménagers, maison, automatisation, santé, télécommunications, industriel, énergie, imprimantes, éclairage, IoT, wearable, etc. sont parmi les secteurs utilisant le logiciel MicroEJ.

Les avantages perçus par les clients sont: des délais très courts de mise sur le marché des produits, des coûts de conception réduits, la possibilité de générer rapidement de nouveaux revenus dans le cadre de l'IoT, la création de réels actifs logiciels capitalisables, l'augmentation de la sécurité, ainsi que la création de véritables écosystèmes autour d'appareils hétérogènes interconnectés.

Aux industriels, MicroEJ offre une gamme complète et cohérente :

1. **MicroEJ Tools** pour la spécification, la conception et la simulation de logiciels embarqués;
2. **MicroEJ VEE** (Virtual Execution Environment), plus petit processeur 32-bit virtuel standard, véritable contenant sécurisé dédié à l'exécution de logiciels binaires, et applicable à tout type d'appareil électronique;
3. **Des bibliothèques gratuites et fiables :** Interface utilisateur graphique, capteurs et actionneurs, système de fichiers et réseau, protocoles IoT et communications série, matrices et numériques, gestion des ressources et des logiciels, sécurité et authentification, chargeur dynamique de composants logiciels;
4. **MicroEJ Store** en marque blanche pour capitaliser sur des actifs logiciels réutilisables pour la création de clients et partenaires écosystèmes.

PLUS D'INFOS
www.microej.com

À PROPOS

Editeur de logiciel

Prove & Run est un éditeur de logiciels permettant de protéger l'Internet des objets et les systèmes embarqués contre les attaques de cybersécurité, en particulier celles menées à distance.

La société commercialise 2 briques logicielles essentielles (COTS) prêtes à être intégrées :

- **ProvenCore :** un OS de sécurité dont les propriétés de sécurité sont formellement prouvées et dont l'objectif est d'offrir un environnement d'exploitation extrêmement robuste aussi proche possible du zéro-bug, sur lequel les fonctions les plus sensibles peuvent s'exécuter sans être sujettes aux attaques;
- **ProvenVisor :** un hyperviseur formellement prouvé pour la sécurité.

Ces briques logicielles, sans équivalent sur le marché, sont disponibles sur des architectures de processeurs ARM qui sont de très larges diffusions dans l'informatique connectée. Elles sont mises en œuvre soit individuellement, soit en combinaison pour sécuriser les architectures connectées telles que celles utilisées dans les secteurs cibles principaux que sont l'automobile, le ferroviaire, l'aéronautique, l'énergie, l'industrie, la téléphonie mobile et l'IoT.

Les compétences principales de Prove & Run sont dans la sécurité, les systèmes d'exploitation, les méthodes formelles et la certification de sécurité. Les solutions logicielles de Prove & Run améliorent considérablement le niveau de sécurité des objets connectés afin de les protéger contre les cyber-attaques à distance, à des coûts compatibles avec les contraintes industrielles.

Prove & Run a été fondée par Dominique Bolignano en 2009. Elle est indépendante et a son siège à Paris, en France.

PLUS D'INFOS
www.provenrun.cm

Quand sûreté de fonctionnement et sécurité sont requises

SYSGO est le leader européen des systèmes d'exploitation temps réel pour les applications embarquées critiques. Nos solutions disponibles depuis plus de dix ans sont développées dans le but de répondre au mieux aux exigences les plus élevées en termes de sûreté de fonctionnement et de sécurité. Nos clients, acteurs majeurs de l'industrie aéronautique, spatiale, automobile, du ferroviaire, du médical et de l'automatisation industrielle utilisent notre produit **PikeOS** comme Plateforme S3P stratégique de leurs systèmes critiques pour lesquels une certification conforme aux normes de sûreté et sécurité est nécessaire.

Filiale indépendante au sein du groupe Thales, SYSGO est implanté sur plusieurs sites en Allemagne, France et République tchèque. Notre réseau de partenaires inclut les principaux fournisseurs de technologies de l'embarqué ainsi que des distributeurs à valeur ajoutée couvrant l'Europe et l'Asie.

Nos produits étant principalement utilisés dans des environnements les plus critiques, SYSGO a mis en place une méthode de développement logiciel de haute qualité reconnue par l'obtention de certification ISO 9001 :2015 et ISO/IEC 27001:2013 en 2016. PikeOS quant à lui, a été le premier système d'exploitation certifié EN50128 SIL4 pour les processeurs multicœurs.

SYSGO propose à ses clients des contrats de maintenance sur l'ensemble du cycle de vie qui peuvent parfois excéder 20 ans. En tant que société européenne, nos solutions ne font l'objet d'aucune contrainte d'exportation et sont notamment libres par rapport à la réglementation ITAR.

PLUS D'INFOS
www.sysgo.com

À PROPOS

TRUST IN SOFT

TrustInSoft est le seul éditeur de solutions d'analyses de logiciel qui permet à ses clients d'avoir des garanties sur la sécurité et la fiabilité du code d'un logiciel sans devoir modifier le processus de développement.

TrustInSoft commercialise des outils et services d'analyse de code source permettant d'apporter des garanties fortes sur les logiciels de ses clients. Ses offres sont déployées chez les développeurs et les intégrateurs de composants logiciels issus des industries aérospatiales, ferroviaires, militaires, nucléaires, télécoms ou IoT. TrustInSoft propose une palette d'outils et de services déjà reconnus mondialement :

- **TrustInSoft Analyzer,** un outil d'analyse de code source C et C++ (vérification et validation) permettant de garantir mathématiquement la conformité à une spécification, l'absence de défauts et l'immunité de composants logiciels aux cyber-attaques les plus courantes.
- **TrustInSoft Advanced Software Audit,** un service outillé d'audit de logiciel réalisé par les experts de TrustInSoft en lien direct avec le client. Ces audits permettent d'évaluer la sécurité et la fiabilité de composants logiciels existants ou en cours de développement.
- **TrustInSoft Expertise,** un service d'expertise pour accompagner les clients dans le déploiement de TrustInSoft Analyzer ou de Frama-C avec des formations, du conseil méthodologique et de développements d'extensions spécifiques pour TrustInSoft Analyzer.

PLUS D'INFOS
www.trust-in-soft.com

À PROPOS

CAP'TRONIC
Systèmes électroniques et logiciel embarqué

Fondée par le CEA et Bpifrance, et financée par le ministère de l'Économie et des Finances, l'association JESSICA France est chargée de la mise en œuvre du **programme CAP'TRONIC**. Celui-ci a pour objectif d'**aider les PME françaises, quel que soit leur secteur d'activité, à améliorer leur compétitivité** grâce à l'intégration de solutions électroniques et de logiciel embarqué dans leurs produits.

Spécialistes en électronique et en logiciel embarqué, les 24 ingénieurs CAP'TRONIC sont présents sur l'ensemble de la France, **au plus proche des entreprises** et des défis qu'elles doivent relever au quotidien. Ils mettent en place, en toute neutralité, les expertises adaptées au projet, à l'entreprise et au marché, afin de parvenir rapidement à **une solution réaliste en termes de solution technologique, de délai et de coût.**

Les interventions prennent la forme de séminaires techniques et marché, de formations et de conseils. L'aide de CAP'TRONIC peut prendre ensuite la forme d'expertises cofinancées par le programme (choix technologiques, mise au point du cahier des charges...) et d'accompagnement du projet.

CAP'TRONIC mobilise de nombreux experts venant de centres de compétences publics et privés en électronique et en logiciel embarqué. Ces centres sont des laboratoires universitaires, des écoles d'ingénieurs, des sociétés d'études électroniques du secteur privé.

Chaque année, CAP'TRONIC aide plus de 3 500 PME, tous secteurs confondus, à conquérir de nouvelles parts de marché en faisant de l'électronique et du logiciel embarqué **le levier concurrentiel indispensable à leur croissance.**

PLUS D'INFOS
www.captronic.fr

Embedded France
L'EMBARQUÉ MADE IN FRANCE

Embedded France est l'association des acteurs français des logiciels et systèmes embarqués. Association loi de 1901, Embedded France est ouverte à tous les industriels fournisseurs et intégrateurs de systèmes et logiciels embarqués, ainsi qu'aux pôles et associations professionnelles représentatives de domaines développant ou intégrant des systèmes embarqués.

Embedded France a été créée à l'initiative de Syntec Numérique, de CAP'TRONIC et des pôles de compétitivité Aerospace Valley, Images & Réseaux, Minalogic et Systematic, avec pour objectif de développer l'emploi dans la filière française des systèmes et logiciels embarqués, et de contribuer à la compétitivité de l'industrie française.

Cet objectif est décliné en 5 missions :

- **Fédérer et développer la filière :** face à la forte croissance et aux mutations rapides de l'écosystème des systèmes connectés intelligents et des objets connectés, l'existence d'une entité fédératrice telle que Embedded France est essentielle;
- **Décloisonner les « silos » sectoriels :** Embedded France vise à partager les retours d'expériences et les solutions entre les nombreux acteurs, utilisateurs de logiciels et de systèmes embarqués, pour décloisonner le marché et contribuer à la compétitivité de l'industrie;
- **Développer les acteurs de la filière aux niveaux européen et international :** développer les actions d'Embedded France en coordination avec d'autres initiatives hors du seul territoire français;
- **Faciliter le recrutement et la formation :** les secteurs du logiciel et des systèmes embarqués ainsi que celui des objets connectés font face à une véritable pénurie de profils. Embedded France s'est fixé pour objectif d'apporter des réponses adéquates;
- **Communiquer** avec les acteurs du secteur, clients, investisseurs, pouvoirs publics, organismes de recherche et de formation, pour rendre la filière et les métiers visibles et en renforcer l'attractivité.

PLUS D'INFOS
www.embedded-france.org

LEXIQUE

API est une interface de programmation applicative, un ensemble normalisé de classes, de méthodes ou de fonctions qui sert de façade par laquelle un logiciel offre des services à d'autres logiciels.

ARM est un type de processeur particulier dont l'architecture permet une taille réduite. ARM est l'acronyme de Advanced Risk Machine elle est fortement inspirée des principes de conception RISC (processeur à jeu d'instructions réduit).

BATX pour Baidu, Alibaba, Tencent et Xiaomi, cet acronyme désigne l'équivalent chinois des GAFAM (Google, Apple, Facebook, Amazon).

Cloud connu sous le terme français de « nuage » est l'exploitation de la puissance de calcul ou de stockage de serveurs distants par l'intermédiaire d'un réseau, généralement l'internet.

Cluster (de serveurs) est un groupe de serveurs et d'autres ressources indépendantes fonctionnant comme un seul système, au sein d'un système informatique.

ARM Cortex est une famille de Processeur ARM à l'architecture SoC (System On Chip); on distingue les ARM Cortex-A pour les dispositifs portables (smartphones et tablettes), ARM Cortex-M pour le couplage à un microcontrôleur, ARM Cortex-R pour les microprocesseurs temps réel.

Criticité est la détermination du degré d'importance et de disponibilité d'un système d'information. On peut la quantifier comme le produit de la probabilité d'occurrence d'un incident, par la gravité de ses conséquences.

Cyber-physique est un système où des éléments informatiques collaborent entre eux pour le contrôle et la commande d'entités physiques.

DO-178C DAL-A est une norme qui fixe les conditions de sécurité applicables aux logiciels critiques de l'avionique, dans l'aviation commerciale et l'aviation générale. Elle précise notamment les contraintes de développement liées à l'obtention de la certification d'un logiciel avionique.

DoS est utilisé pour décrire un type d'attaque informatique dite "par déni de service" qui a pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser.

FADEC acronyme anglais de Full Authority Digital Engine Control, est un système qui s'interface entre le cockpit et le moteur d'aéronef. C'est un système de régulation numérique centré sur un calculateur à deux voies symétriques, redondantes et à pleine autorité.

Framework désigne en programmation informatique un ensemble d'outils et de composants logiciels à la base d'un logiciel ou d'une application.

Gateways désigne un dispositif permettant de relier deux réseaux distincts présentant une topologie différente.

GSM/GPRS est une norme (protocole réseau) pour la téléphonie mobile dérivée du GSM et complémentaire de celui-ci, permettant un débit de données plus élevé.

Hyperviseur est un logiciel de virtualisation qui est installé sur le système d'exploitation principal. Il permet la création d'environnements clos et indépendants sur lesquels seront installés d'autres systèmes d'exploitation (« systèmes invités »). Ces environnements sont des « machines virtuelles ».

LEXIQUE

IHM est l'acronyme d'Interface Homme Machine, c'est-à-dire l'ensemble des moyens utilisés par l'homme pour communiquer avec une machine.

IP pour Internet Protocole qui désigne le protocole de la couche réseau selon la classificaion OSI.

Middleware désigne un logiciel permettant la mise en relation de deux applications informatiques.

MPPA est un processeur à 256 cœurs développé par la start-up francaise Kalray.

MMU est un composant permettant de contrôler les accès qu'un processeur fait à la mémoire de l'ordinateur dans lequel il est intégré.

OMG-UCM pour Object Management Group (OMG) est un consortium américain à but non lucratif dont l'objectif est de standardiser et promouvoir le modèle objet sous toutes ses formes. L'UCM est un standard de modélisation utilisé sous Eclipse.

PCI Express dérivé de la norme PCI (Peripheral Component Interconnect), est un standard de bus d'extension série qui sert à connecter un ordinateur et un ou plusieurs périphériques.

Sûreté (de fonctionnement) désigne l'aptitude d'un système à remplir une ou plusieurs fonctions requises dans des conditions données ; elle traduit la confiance qu'on peut accorder à un système.

Sécurité en informatique représente une discipline qui se veut de protéger l'intégrité et la confidentialité des informations stockées dans un système.

SysML est l'acronyme de Systems Modeling Language, soit en français par Langage de Modélisation de Systèmes. SysML aborde la conception avec la notion de blocs qui deviendront des parties mécaniques, électroniques, informatiques ou autres : il est donc un langage graphique qui utilise des diagrammes.

Virtualisation est un mécanisme informatique qui consiste à faire fonctionner plusieurs systèmes, serveurs ou applications, sur un même serveur physique.

S3P

SMART, SAFE & SECURE PLATFORM

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES

DGE
DIRECTION GÉNÉRALE DES ENTREPRISES

INVESTIR L'AVENIR