Poste de Maître de Conférences susceptible d'être publié
Laboratoire Verimag et Grenoble INP/Ensimag
2018

De l'embarqué au distribué : validation et certification pour systèmes informatiques sûrs et sécurisés

http://www-verimag.imag.fr
http://ensimag.grenoble-inp.fr

Contact : Florence.Maraninchi@univ-grenoble-alpes.fr

1 Contexte : les systèmes cyber-physiques

Les systèmes cyber-physiques (CPS dans la suite) sont le résultat d'une intrication des aspects matériels et logiciels des systèmes informatiques, avec les aspects physiques des environnements dans lesquels ils sont amenés à fonctionner. Les CPS peuvent être conçus pour *contrôler* des processus physiques ; inversement leur fonctionnement peut être *contraint* par des phénomènes physiques, comme la consommation électrique ou des rayonnements dans le cas du spatial ; leur sécurité peut aussi être attaquée grâce à des observations physiques. De manière générale les CPS doivent fonctionner dans des environnements incertains, et être capables de tolérer des défauts ou des attaques intentionnelles.

Les domaines d'applications concernés sont très vastes : les véhicules autonomes, les grandes infrastructures comme les smartgrids ou les villes intelligentes, l'industrie 4.0, la santé, l'aéronautique, le spatial éventuellement à bas coût, le ferroviaire, etc.

2 Tendances du domaine

Des critères économiques poussent à diminuer le coût des systèmes informatiques omniprésents. Certains contextes particulièrement critiques ont accepté un coût plus élevé pour garantir les propriétés de sûreté/sécurité. C'est le cas depuis longtemps dans l'avionique et

e nucléaire par exemple, beaucoup moins dans l'automobile. Un certain nombre de cas très médiatisés (la prise de contrôle de voiture à distance, le virus WannaCry, les attaques sur la distribution électrique en Ukraine, etc.) font prendre conscience de la fragilité intrinsèque des infrastructures qui reposent sur des systèmes informatiques, et des risques associés pour les êtres humains ou l'environnement.

Être capable de garantir un bon niveau de sûreté et de sécurité des systèmes, à des coûts raisonnables, est donc un objectif central. De plus, si ces deux types de propriétés ont pu être abordés séparément par le passé, ce n'est plus le cas : une attaque de sécurité peut compromettre la sûreté, et les bugs d'un système peu sûr peuvent ouvrir la porte à des attaques. Aussi bien dans le cloud que dans les dispositifs embarqués de l'internet des objets, la cybersécurité est liée à la sûreté.

Par ailleurs les grands systèmes sont en fait des *systèmes de systèmes*, dont les parties ont été conçues indépendamment, et qui doivent fonctionner harmonieusement quand on les assemble. Cela demande de définir des interfaces, de se donner les moyens de raisonner sur des abstractions à différents niveaux, et de prendre en compte des composants hérités du passé.

Enfin l'arrivée de solutions basées sur l'apprentissage automatique, par exemple pour la maintenance prédictive ou la détection d'obstacle dans les véhicules autonomes, pose des questions sur les garanties de sûreté et sécurité qu'on peut espérer mettre en place, à terme, dans les domaines où ces solutions ont un impact critique. Le besoin de certifier de tels systèmes rejoint ici la préoccupation d' "explicabilité" des algorithmes.

3 Compétences du laboratoire Verimag

Le laboratoire Verimag s'intéresse depuis sa création aux principes, méthodes et outils qui permettent de concevoir directement des systèmes informatiques corrects, ou d'analyser des systèmes existants pour y découvrir des failles et les corriger. Cela s'applique aussi bien à la *sûreté* des CPS (capacité à fonctionner correctement dans des environnements physiques exigeants, robustesse, tolérance aux pannes, ...) qu'à la *sécurité* (résistance à des attaques intentionnellement malveillantes).

Le laboratoire Verimag développe des recherches fondamentales et appliquées sur les trois piliers nécessaires à ces objectifs : (1) Sémantique et vérification de propriétés des programmes et des systèmes cyber-physiques, aspects fondamentaux et développement d'outils utilisables en vraie grandeur ; (2) Méthodes et outils d'implantation correcte et efficace des systèmes cyber-physiques : langages de programmation dédiés, compilateurs, méthodes dirigées par les modèles, composants, parallélisation et distribution, optimisation, etc. ; (3) Méthodes et outils de modélisation fidèle, analyse et simulation efficace des comportements de l'ensemble cyber-physique : systèmes hybrides continus/discrets, architectures matérielles/logicielles, etc.

Ces recherches fondamentales et appliquées sont appuyées par de nombreuses collaborations académiques et industrielles qui permettent des expérimentations sur des applications réelles. Le laboratoire a des objectifs à long terme, produit des résultats fondamentaux et développe des outils pérennes dont certains sont transférés (exemple récent : startup argosim.com, 2013).

Le laboratoire maintient une vision globale des systèmes à construire et analyser, qui va de "tout en haut" (des modèles relativement abstraits, éventuellement hybrides continus/discrets, automates, logiques, algorithmique distribuée) à "tout en bas" (interface

logiciel/matériel, analyse de code binaire, temps-réel sur machines manycœurs, monitoring temporisé de systèmes de contrôle, implantation des systèmes distribués, etc.). La variété des études de cas abordées permet d'autre part de comprendre les problèmes dans toute leur généralité et de proposer des solutions applicables au-delà d'un domaine particulier.

4 Profil recherche du poste

Le profil proposé est : *De l'embarqué au distribué : validation et certification pour systèmes informatiques sûrs et sécurisés.*

Nous recherchons des candidats intéressés par l'étude de l'implantation des CPS et des modèles formels qui permettent de les comprendre, concevoir, analyser et corriger. Le ou la candidat(e) pourra contribuer aux thèmes suivants :

- La prise en compte de plateformes d'exécution diverses (architectures matérielles modernes et leurs systèmes d'exploitation, systèmes distribués, etc.) dans une démarche de **production d'implantations correctes par construction**, à partir de modèles et langages de haut niveau, en tenant compte de l'interface logiciel/matériel (compilateurs, code objet, systèmes temps-réel et calcul de temps d'exécution, ...).
- Les **vérifications de propriétés de sûreté/sécurité** des systèmes informatiques, et les démarches de **certification** associées. Il s'agit de connaître les méthodes de vérification (statique et dynamique), leurs applications et limites, afin de développer des outils et des démarches d'analyse adaptés à des classes de systèmes et de propriétés, prenant en compte l'environnement (propriétés du contexte d'exécution, modèles d'attaquant, ...)
- Le développement d'outils de suivi opérationnel de **systèmes complexes** qui comportent un part très significative de physique (automobiles, avionique, robotique, systèmes électriques, bâtiments intelligents, ...).