Annexe : axe prioritaire Sécurité et sûreté
département STIC Paris-Saclay
(version du 01 septembre 2015)

Participants au GT : Daniel Augot (INRIA), Jean-Luc Danger (LTCI), Florent Kirchner (CEA LIST), Maryline Laurent (SAMOVAR), Laurent Pautet (LTCI), Renaud Sirdey (CEA LIST); Animateurs: Olivier Bournez (LIX), Laurent Fribourg (LSV), Christine Paulin-Mohring (LRI)

1) Objectifs

La révolution numérique que connaît notre société se traduit à de multiples niveaux : intégration croissante de logiciel de contrôle dans des domaines critiques (transport, santé, énergie, commerce); multiplication d'objets connectés collectant, échangeant et traitant de l'information de manière distribuée ; disponibilité de données massives multipliant les possibilités de prise de décisions par des programmes informatiques.

Les logiciels sont omni-présents, mais restent insuffisamment maitrisés. L'histoire (Ariane, anti-missile patriot) a d'ailleurs montré que des erreurs ponctuelles pouvaient avoir des conséquences économiques ou humaines catastrophiques. L'utilisation impropre des données personnelles (de l'indiscrétion à la cyber-criminalité en passant par les usages commerciaux) se développe également, rendant nécessaire de nouvelles stratégies de surveillance et de protection des données et des programmes. Plusieurs start-ups (TrustinSoft, Prove and Run, Internet of Trust, Secure-IC) dans le périmètre Ile-de-France ont été créées ces dernières années qui développent des solutions innovantes pour répondre à ces questions.
Les équipes de l'Université Paris-Saclay ont une expertise reconnue internationalement dans plusieurs domaines contribuant à cet enjeu : méthodes formelles, analyse statique, cryptographie, environnement de preuve, algorithmes de vérification, sûreté de fonctionnement, systèmes embarqués...Leurs compétences vont des aspects les plus fondamentaux qui font appel à des concepts avancés de mathématiques jusqu'aux applications réelles en passant par le développement d'outils.

Les objectifs de cet axe prioritaire sont de faire de Paris-Saclay un pôle scientifique de référence dans le domaine de la sûreté et de la sécurité logicielle et notamment :

- de créer de nouvelles synergies entre les équipes permettant de répondre à la complexité croissante des systèmes en combinant les approches et en attaquant de nouveaux problèmes;
- de faciliter le transfert des résultats fondamentaux vers les applications, en particulier au travers de plate-formes logicielles polyvalentes, également en développant le volet formation à des techniques avancées des ingénieurs de développement;
- d'accroitre l'impact des recherches en renforçant les compétences sur des aspects insuffisamment couverts ou transverses comme la cyber-sécurité.

2) Enjeux

La sûreté et la sécurité des systèmes logiciels sont des enjeux sociétaux majeurs : chaque faille révélée a un impact direct immédiat selon la gravité de l'accident mais aussi en terme d'image et de confiance. La nécessité de se préserver de possibles défaillances entraine également un surcoût important pour les entreprises. L'enjeu de cet axe prioritaire pour le département est multiple. Il s'agit de contribuer en amont aux grandes questions scientifiques difficiles du domaine

(modèles, langages, algorithmes…), de mobiliser les savoir-faire pour concevoir des méthodes, outils et composants qui répondent à la complexité des systèmes d'aujourd'hui et de demain tout en étant transférables vers les cycles de développement logiciel industriels afin de les déployer dans les secteurs critiques comme l'énergie, la santé..

La principale révolution de ces dernières années est l'ouverture des logiciels et données critiques sur le monde connecté. Les systèmes sont composés d'une multitude d'objets "intelligents" communicants qui manipulent des masses de données. Modéliser de tels systèmes complexes et être capables d'en contrôler le fonctionnement n'est que très partiellement couvert par les connaissances actuelles.

La sécurité et la sûreté est reconnue comme enjeu stratégique tant au niveau national qu'international.

La thématique sûreté et sécurité est en bonne position dans les recherches prioritaires des institutions du département STIC. Un des quatre programmes de recherche du CEA LIST porte sur les systèmes embarqués (conception et analyse, validation et vérification, composants et IPs pour la fiabilité, la sûreté et la sécurité). Dans son plan stratégique Objectif Inria 2020 (http://www.inria.fr/institut/strategie/plan-strategique), Inria identifie trois domaines de recherche prioritaires incluant 7 défis dont "la programmation des très grands logiciels prenant en compte les impératifs de fiabilité, de sûreté et de sécurité" et "une cyber-communication généralisée, sûre et respectueuse de la vie privée". Télécoms ParisTech identifie la "confiance numérique" (sécurité, sûreté et risques) comme un de ses 6 axes stratégiques. L'Ecole Polytechnique identifie "Vérifier la fiabilité des logiciels critiques" comme axe prioritaire dans le thème "Concept et méthodes pour la société numérique". L'implication des institutions dans ce domaine se traduit également par l'existence de chaires: Ingénierie des Systèmes Complexes (X-ENSTA-Télécom ParisTech-Dassault Aviation-DGA-DCNS-Thales) et "Systèmes embarqués robustes de la conception à l'architecture" (SAFRAN, Centrale Supélec).

Parmi les structures partenaires de l'Université Paris-Saclay, le pôle de compétivité systematic est organisé en 9 thématiques dont "Confiance numérique et sécurité" et "Outils de conception et de développement de systèmes". "Logiciels Critiques" est également un des quatre challenges de l'IRT SystemX.

Si on se place du point de vue des secteurs applicatifs qui ont un besoin fort en sûreté et sécurité, les transports, l'énergie et la santé sont trois axes forts soutenus par les institutions de l'Université Paris-Saclay et sur lesquels il est pertinent de se concentrer.

Au niveau européen, la sécurité est un des sept défis sociétaux du programme Horizon 2020 (cf http://www.horizon2020.gouv.fr/cid72619/le-defi-securite-dans-horizon-2020.html) avec entre autres objectifs d'améliorer la cyber sécurité et d'assurer le respect de la vie privée et les libertés individuelles. La protection des infrastructures (eau, énergie, transport, communication, santé et finance) est un enjeu majeur, qui passe obligatoirement par la protection des logiciels de ces systèmes. Un autre axe est la sécurité numérique qui inclut un volet "Privacy and Data Protection and Digital Identities".
En Allemagne, "Sécurité et sûreté" est l'un des 5 secteurs clés de la Hightech Strategy au même niveau que "climat et énergie" ou "santé et alimentation" (cf document SNR).

applicatifs comme l'énergie et la santé dans des approches transverses et pluri-disciplinaires.

3) Défis

Du fait de leur omniprésence en STIC, les questions de sûreté et sécurité ont été naturellement abordées à la fois par des initiatives d'excellence du plateau (comme dans le Lidex *Institut pour le Contrôle et la Décision (*http://www.icode-institute.fr/), le Lidex *Institut Société Numérique* (http://digitalsocietyinstitute.com/fr/), l'Equipex *Centre d'Accès Sécurisé Distant aux données* (https://casd.eu/index.php), l'axe SciLex du Labex Digicosme (http://labex-digicosme.fr/SciLex) ainsi que, de façon transverse, dans les autres axes prioritaires de la stratégie partagée (*Big Data*, *Interactions*, *Systèmes en réseaux*, *Modélisation*).
Un de nos objectifs au sein du département et plus largement de l'UPSaclay est de créer les conditions de collaborations avec les autres thématiques et départements permettant d'apporter des solutions innovantes aux problèmes soulevés par l'enjeu de sûreté et sécurité.

Nous présentons ici 4 défis majeurs tant sur le plan scientifique que technologique, au coeur de cette thématique. Une spécificité des forces présentes sur le plateau de Saclay est de couvrir l'ensemble du spectre de la sûreté de fonctionnement du logiciel qui inclut fiabilité, disponibilité, maintenabilité et sécurité avec une forte compétence en méthodes formelles.

3.1) **Sûreté et sécurité des systèmes cyber-physiques**

Le premier défi concerne la sûreté et la sécurité des systèmes cyber-physiques (SCP), c'est-à-dire des systèmes dans lesquels un réseau de processeurs embarqués interagit avec le monde physique pour réaliser certaines fonctionnalités complexes. Ces systèmes, qui incluent les systèmes embarqués, ont des applications dans des domaines très larges qui couvrent des domaines aussi variés que les communications, les transports, la domotique, la robotique, la production, les applications militaires ou industrielles, la santé, l'énergie, ou la conception d'infrastructures innovantes.

La complexité très grande qui provient de la combinaison intriquée des composants physiques et informatiques soulève de grandes difficultés. D'un côté, les systèmes digitaux opèrent d'une manière discrète, et les communications et calculs se déroulent en général en synchronisation avec les cycles de processeurs. D'un autre côté, les systèmes physiques évoluent et agissent en temps réel dans un environnement continu. Il s'ensuit que les SCP sont des systèmes complexes qui présentent des comportements *hybrides* (discrets et continus).

Le développement de méthodes de conception et d'analyse des SCP sûrs nécessite de contribuer aux points fondamentaux suivants:

- le développement de modèles hybrides incluant à la fois la sémantique des systèmes embarqués et le comportement des périphériques physiques connectés
- le développement de méthodes d'analyse et d'algorithmes permettant la vérification *quantitative* telles que "le système de contrôle de freinage d'un véhicule garantit d'amener la voiture à l'arrêt complet en moins de x secondes à partir d'une vitesse initiale de 100 km/h"

- le développement de méthodes de vérification *robuste*, c'est-à-dire telles que si la vérification est positive, on sait qu'elle le reste en présence de petites perturbations
- des méthodes pour garantir la sûreté de fonctionnement, et la sécurité des systèmes cyber-physiques en présence d'attaque.

Ce défi encourage naturellement l'approfondissement des interactions établies avec les équipes de Saclay étudiant les systèmes cyberphysiques d'un point de vue de la théorie du contrôle (groupe de travail GT SHY du Labex Digicosme qui réunit informaticiens et automaticiens, Séminaire d'Automatique du Plateau de Saclay du Lidex ICODE,...).

3.2) **Conception et vérification: du modèle au code exécuté**

L'objectif de ce second défi est de concevoir des applications qui exploitent pleinement les capacités des environnements actuels (par exemple code mobile, exécution dans un environnement ouvert sujet aux attaques, architectures cibles parallèles) tout en garantissant un haut niveau de sûreté de fonctionnement et de confiance en terme de disponibilité, fiabilité, maintenabilité, sécurité. La complexité des programmes actuels rend nécessaire une approche modulaire de décomposition des problèmes ainsi qu'une méthodologie largement automatisée pour réduire les temps et coûts de développement.

Les équipes de Saclay disposent de méthodes et d'outils variés se situant à différents niveaux du développement, les compétences allant des aspects les plus fondamentaux aux applications. Un enjeu du défi est de faire coopérer ces équipes de façon à s'attaquer aux questions fondamentales et verrous technologiques suivants:

- concevoir des formalismes (langages, modèles, preuves) adaptés au développement de systèmes garantis sûrs
- identifier des classes de problèmes pour lesquels on sait concevoir des solutions algorithmiques efficaces
- développer des méthodes d'analyse de schémas de code complexe (gestion du parallélisme, flots d'information, calculs en lien avec les composants physiques d'un système)
- développer des techniques et des langages de collaboration entre différentes méthodes de vérification (en particulier les synergies entre sûreté de fonctionnement et cyber-sécurité, les analyses statiques / dynamiques, ou encore les liens entre simulation et vérification)
- savoir concevoir des systèmes sûrs même en présence de composants non-fiables, ou incertains.

3.3) **Méthodes et outils utilisables par des non-spécialistes**

La conception et la réalisation de systèmes logiciels sûrs requièrent l'utilisation de méthodes rigoureuses pour l'ensemble du développement, s'intégrant dans les processus de développements propres de leurs utilisateurs. Cette interaction entre utilisateurs, outils et méthodes de mise en oeuvre nécessite de développer une base d'experts ayant une compréhension détaillée de leur fonctionnement et de leur utilisation dans des contextes variés. Les équipes de Saclay développent des outils qui ont comme cible d'être intégrés dans des cycles de développement de production.

L’enjeu de ce troisième défi est de contribuer à l’émergence d’une nouvelle génération de programmeurs qui maîtrise les techniques avancées de développement. Saclay du fait de son ancrage fort dans la formation en particulier en master a l’opportunité de contribuer fortement à ce défi en développant son offre d’éducation en particulier en l’ouvrant sur la formation continue.

La réalisation des objectifs de ce défi passe par la maîtrise des points suivants :

- savoir adapter les méthodes aux langages métiers cibles, en particulier pour les appliquer dans des projets inter-disciplinaires autour de l’énergie du transport et de la santé;
- fournir un ensemble de composants (librairies, preuves, etc) réutilisables;
- contribuer à automatiser les traitements et à faciliter leur composition, en lien avec le second défi pour les aspects fondamentaux;
- contribuer à intégrer des méthodes formelles dans le processus de certification;
- développer des techniques permettant le passage à l’échelle.

3.4) **Sécurisation des données et calculs distribués**

L’enjeu de ce quatrième défi est d’assurer la sécurité des données et des calculs distribués.

La cryptographie, qui consiste traditionnellement à assurer l’intégrité, l’authentification, la confidentialité et le contrôle d'accès, reste au cœur de la sécurité, avec les algorithmes de chiffrement, de signature, et hachage, qui peuvent être utilisés de nombreuses manières différentes et détournées.

Avec le cloud, et le déport des calculs et des données sur des ressources distances, qui ne sont pas automatiquement considérées comme sûres, des problématiques nouvelles apparaissent, selon que l'utilisateur d’un centre de calcul distant veuille protéger ses données, ce qui pose les questions de confidentialité, d’intégrité, d’anonymisation, de protection de la vie privée, de protection des consultations (Private Information Retrieval), mais aussi selon qu’il souhaite protéger ses traitements ou le résultat de ses traitements.

Une fois ces briques de base mises en place (chiffrement, signature, hachage), il reste à les assembler pour mettre au point des protocoles (vote électronique, monnaie électronique, certificat anonyme...) en veillant à ne pas introduire d’attaque logique (e.g., attaque par rejeu). Ces types d’attaque sont orthogonales à celles sur les briques de base et nécessitent des outils de vérification par méthodes formelles (déduction automatique, model checking).

Cela nécessite de contribuer aux points fondamentaux suivants:

- réaliser des progrès quantitatifs sur les primitives classiques (algorithmes de chiffrement, signature)
- concevoir des nouveaux mécanismes en présence de déport de calculs (signatures aveugles, calcul multipartite, cryptographie à seuil, protocoles de certification anonyme, chiffrement homomorphique, primitives d’obfusquation)
- développer de nouvelles techniques de preuve pour vérifier des propriétés de sécurité liées à la vie privée (e.g., anonymat, non traçabilité)

4) Forces en présence

Clairement le plateau de Saclay est très visible sur les thèmes de la sécurité et sûreté. Une des preuves de cela est le très grand nombre de publications, et le grand nombre de prix, ou records issus du plateau de Saclay (par exemple en cryptologie, ou via le financement de projets ERC junior et senior autour des méthodes formelles).

FRAMA-C

Frama-C est une plateforme d'analyse de codes sources issue de la collaboration des équipes d'Inria, de l'Université Paris-Sud et du CEA, et sur laquelle s'appuie la startup TrustInSoft. Elle met en œuvre des techniques d'interprétation abstraite, de vérification déductive et de résolution de contraintes dont la caractéristique commune est de reposer sur des méthodes formelles qui assurent que leurs résultats sont rigoureusement corrects. Dans une dynamique *open-source*, cette plateforme permet non seulement le développement d'approches variées par une communauté d'utilisateurs divers, mais aussi de combiner ces approches pour atteindre des objectifs de validation ambitieux. Elle est mise en oeuvre, au sein de processus de validation industrielle, dans des domaines où la confiance logicielle est un prérequis fondamental. Historiquement réservé aux domaines des gros équipements énergétiques, avioniques, ou ferroviaire, ces outils voient depuis quelques années leur adoption s'étendre à des applications médicales, ou de cybersécurité, à travers l'Europe, les États-Unis, et l'Asie.

Les projets ERC en sûreté et sécurité

ProofCert (https://team.inria.fr/parsifal/fr/proofcert/) est un projet sélectionné comme ERC Advanced Grant et financé pour la période 2012 à 2016. Coordonné par Dale Miller, DR Inria au LIX, son but est de concevoir un format pour des "certificats de preuves" qui soit capable de capturer la validité d'une preuve dans tous les outils majeurs de preuve informatique de théorèmes, tout en permettant d'être vérifié par un outil simple et déclaratif. La conception de tels certificats de preuve vise à terme à garantir une confiance dans les systèmes de preuve existants afin que les gens puissent échanger et partager des parties de preuves entre outils de preuve basés sur des logiques et paradigmes différents.
EQualIS (http://www.lsv.ens-cachan.fr/~bouyer/equalis/) est un projet sélectionné comme ERC Starting Grant et financé pour la période 2013 à 2018. Coordonné par Patricia Bouyer, DR CNRS LSV, il vise à développer une approche systématique pour l'analyse formelle de systèmes soumis à des contraintes quantitatives et à des interactions complexes entre composants (comme les réseaux de communication ou les contrôleurs embarqués). Les modèles développés s'appuient sur la théorie des jeux pour prendre en compte les interactions et permettent d'exprimer des aspects quantitatifs (probabilités, limite d'énergie) afin de garantir des propriétés de correction, de performance et de robustesse. Le noyau du projet consiste à développer des algorithmes pour synthétiser des systèmes interactifs à la qualité certifiée.

Prix ACM Software Award COQ
En 2013, l'assistant de preuve Coq a obtenu le SIGPLAN Programming Languages Software Award ainsi que la distinction la plus haute de l'ACM en matière de logiciel, le Software System Award. Ce prix, qui était remis pour la première fois à un logiciel développé en France, récompense un effort de développement de 30 ans coordonné par Inria en partenariat avec le CNRS, l'Université Paris Diderot, l'Université Paris-Sud et l'Ecole Polytechnique. Trois des neuf récipendiaires du prix (B. Barras, J-C Filliâtre et C. Paulin-Mohring) appartiennent au département STIC de Paris-Saclay. Coq repose sur un langage original de description de propositions logiques et de programmes et propose un environnement complet pour le développement de preuves interactives (bibliothèques, notations, procédures automatiques) tout en offrant un des plus hauts niveaux de confiance. Parmi les applications notables de Coq, on notera son utilisation dans un cadre industriel pour la certification de la sécurité des cartes à puce, le développement d'un compilateur C opérationnel et garanti sans erreur, ou encore les preuves avancées en mathématiques du théorème des 4 couleurs et du théorème de Feit et Thompson de classification des groupes finis. Coq reste un sujet de recherche et un outil pour les chercheurs du département STIC, en particulier dans les domaines de la preuve de programmes et des calculs en nombre flottants.

Une de nos forces est que nous couvrons de la recherche des aspects les plus fondamentaux aux plus appliqués. En particulier, il y a une grande expertise sur le développement d'outils logiciels pour les méthodes formelles sur le plateau. On peut citer par exemple les outils FRAMA-C (CEA), WHY (LRI), COQ (INRIA, LIX, LRI), et de nombreux prototypes disponibles et développés sur le plateau, avec des compétences très visibles en formalisation de preuves sur ordinateur et en cryptologie.

Nous nous appuierons sur les forces et les actions déjà mises en place via le Labex DIGICOSME. En particulier, les thèmes de cet axe prioritaire sont clairement reliés à l'axe Scilex du Labex. Plusieurs actions, comme la mise en place de groupes de travail autour des systèmes formels, ou des actions de formation ont été initiées par le Labex. Néanmoins l'objectif est plus ambitieux que celui du labex en proposant d'établir à Paris-Saclay un centre de référence tant sur le plan national qu'international dans le domaine de la sûreté et de la sécurité. Nous proposons également de développer des actions permettant d'intégrer la dimension sûreté et sécurité à la fois dans les autres domaines des STIC et dans les autres disciplines en lien avec les enjeux autour de l'énergie, de la santé et du transport. Le labex contribuera aux actions proposées dans une période transitoire jusqu'en 2020 (principalement école, groupes de travail, thèses, formation…) néanmoins ses moyens (qui restent limités de l'ordre de 1M€/an pour l'ensemble du labex qui comporte 2 autres axes) doivent être complétés dès la période transitoire en particulier pour accompagner le déploiement des logiciels (support ingénierie) et amplifier l'impact des recherches dans les autres disciplines qui nécessite d'avoir des experts ayant des compétences transverses.

Plusieurs chaires industrielles, communes à plusieurs établissements existent par ailleurs, et démontrent l'implication commune des établissements sur le plateau. Nous pouvons citer par exemple la chaire "Ingénierie des Systèmes Complexes" (X-ENSTA-Télécom ParisTech-Dassault Aviation-DGA-DCNS-Thales) et "Systèmes embarqués robustes de la conception à l'architecture" (SAFRAN, Centrale Supélec).

Plus généralement, les principaux laboratoires concernés par cet axe prioritaire sont les suivants:

LSV (ENS Cachan-CNRS), LIX (Ecole Polytechnique-CNRS),INRIA Saclay - Île-de-France, U2IS (ENSTA), CEA LIST, PRISM (UVSQ), LTCI (Télécom ParisTech-CNRS), SAMOVAR (Télécom SudParis-CNRS), LRI (Université Paris-Sud-CNRS), IBISC (UEVE), MAS (CentraleSupélec), LURPA (ENS Cachan)

Globalement, ces laboratoires comptent environ 200 chercheurs et enseignants-chercheurs permanents.

5) Recommandations d'actions

Construire un pôle de recherche coordonné autour de la sûreté et sécurité du logiciel
Une communauté importante forte d'environ 200 chercheurs offre aujourd'hui sur le plateau un spectre large de compétences méthodologiques en sûreté et en sécurité allant du fondamental aux applications. En particulier, ont été développés et disséminés des outils de vérification à haute valeur ajoutée (Frama-C, Coq, Orchids,…). Certaines de ces compétences sont cependant aujourd'hui dispersées géographiquement et structurellement. Un moyen d'augmenter leurs synergie et visibilité est de construire un grand pôle de recherche coordonné en sûreté et sécurité qui renforcera les coopérations entre équipes, organisera des conférences et écoles, mutualisera les plateformes et outils, facilitera à terme la reconfiguration d'équipes.

Contribuer à l'intégration des aspects liés à la sûreté et sécurité du logiciel dans des domaines d'applications prioritaires
La présence exponentiellement croissante de logiciel dans des applications prioritaires comme l'énergie, transport et santé, rend cruciale la vérification des propriétés de sûreté au fur et à mesure de leur intégration. L'expérience acquise dans le domaine du nucléaire ou aéronautique devrait être utile pour les domaines émergents concernant la santé et l'automobile. Ce processus nécessite de développer des partenariats avec des entreprises par exemple via des chaires industrielles, la proposition de projets communs type H2020 ou la création de laboratoires communs.

Accompagner le développement logiciel en vue de son transfert
La recherche académique fournit des outils novateurs qui restent trop souvent à l'état de prototype développé par un chercheur unique, puis abandonné après son départ. Un enjeu majeur est d'accompagner la production d'outils afin de pérenniser leur utilisation et préparer leur exploitation dans des contextes industriels. Cela peut être réalisé par le recrutement d'ingénieurs de soutien ou l'octroi de bourses de type « code consolidator » (voir Lidex CDS).

Coordonner l'offre de recrutement et de formation
La constitution d'une communauté forte thématiquement ciblée est une opportunité pour disséminer une culture en sûreté et sécurité du logiciel au travers d'une formation doctorale coordonnée et d'un catalogue d'offre commune de formation continue, en particulier au niveau des plateformes logicielles et de la cyber-sécurité.