SURVEILLANCE, SECURITE ET SURETE DES GRANDS SYSTEMES

Le thème de la sécurité est très vaste et concerne, par exemple, aussi bien l'économie, l'environnement que la santé. La concurrence dans ce domaine est de niveau mondial et ce sera une priorité du 7ème PCRD. Dans ce contexte, les quatre laboratoires constituent un centre de compétences important dans la maîtrise des risques informatique et industriel, en s'appuyant sur les méthodes formelles et probabilistes, la vérification de logiciels, l'évaluation de performances, la détection d'événements ou la commande tolérante aux fautes.

Les problèmes de fiabilité et de sécurité des systèmes informatiques sont abordés par les équipes des laboratoires sous différents aspects complémentaires: conception de logiciels sûrs, vérification des systèmes et services critiques, embarqués ou enfouis, l'étude de protocoles et de services distribués, la cryptographie (sous ses aspects classiques issus par exemple de la théorie des nombres, mais aussi sous des aspects novateurs utilisant les systèmes chaotiques), la sûreté de fonctionnement, et la qualité de services.

Le CRAN et le LORIA sont, via leurs établissements de rattachement, partenaires du GIS Surveillance, Sûreté et Sécurité des Grands Systèmes (3SGS). Deux projets associant les deux laboratoires viennent d'être retenus par le conseil scientifique du GIS. Le premier concerne la co-conception de systèmes contrôlés en réseau sûrs de fonctionnement et vise à intégrer de façon coordonnée les caractéristiques qui expriment la qualité de contrôle au sens de l'automatique, les propriétés de la sûreté de fonctionnement et les paramètres d'ordonnancement temps réel des tâches et des messages. Le second, qui associe également un département de recherche d'EDF vise à spécifier les besoins en information des différents métiers (démarrage de tranche, production, maintenance, arrêt de tranche) en vue d'exploiter une centrale de production d'énergie à son optimum. L'objectif scientifique consiste à poser les fondements d'un langage de modélisation des informations d'exploitation qui permette la description du fonctionnement d'une tranche indépendamment de toute répartition homme/système et de tout choix technologique à partir des connaissances et besoins des exploitants.

Parmi les problèmes qui ont déjà donné lieu à des collaborations fécondes entre chercheurs de nos quatre laboratoires, citons :

- La méthodologie de modélisation formelle d'un système fait l'objet d'une collaboration entre le CRAN et le LORIA depuis une dizaine d'années et s'est poursuivie dans le cadre du PPF IAEM. La difficulté scientifique est d'allier des techniques formelles, telle que la méthode B, avec des techniques qui le sont moins, telles que SysML, afin de vérifier certaines propriétés d'un système, par exemple sécuritaires, à partir de l'expression in extenso de l'ensemble des propriétés et services attendus. Ces travaux ont pour objectif de faciliter l'ingénierie de systèmes dirigée par les modèles en complémentarité des approches normatives pratiquées dans l'industrie (les échanges et confrontations des points de vue académique et industriel se déroulent notamment dans le cadre des groupes de travail de l'association française d'ingénierie système - AFIS, http://www.afis.fr/ - auxquels nous contribuons).

- Les algorithmes de cryptographie basés sur les propriétés des nombres entiers (nombres premiers, entiers friables ...). L'équipe de Théorie des Nombres de l'IECN collabore ainsi étroitement avec le projet Cacao du LORIA sur ces questions. Cette collaboration s'est formalisée récemment par le projet ANR Cado porté par le LORIA et l'IECL.

- Le cryptage de signaux sonores ou vidéo en utilisant les propriétés chaotiques des systèmes dynamiques. Cette approche a été initiée par une collaboration entre chercheurs du CRAN et de l'IECL et elle a déjà donné lieu à plusieurs publications et expériences concluantes.