Réseau Thématique Pluridisciplinaire CNRS/STIC n°21
Sûreté de fonctionnement des systèmes informatiques complexes ouverts
[http://www.laas.fr/RTP21-SdF]

Journée de travail du 5 novembre
Compte rendu

— ◊ — ◊ —

Cette journée a réuni 35 personnes (23 académiques et 12 industriels) — voir la liste des participants pour le détail des coordonnées.

Exposés de la matinée

Lors de son exposé à caractère introductif, Jean Arlat a rapidement présenté le comité de pilotage du réseau et l'organisation de la journée de travail. Après avoir demandé à chacun des participants de se présenter brièvement, il a présenté quelques transparents destinés à préciser les objectifs du réseau et d'identifier les spécificités et relations avec d'autres RTPs. Il a également présenté les quatre Actions Spécifiques rattachées au RTP21 : l'AS 23 est maintenant terminée, les trois autres ASs sont en cours.

Enfin, il a brièvement présenté les activités menées dans le cadre du Réseau d'Ingénierie de la Sûreté de fonctionnement (RIS) <www.ris.prd.fr>. En particulier, l'exposé de Philippe David illustre les résultats obtenus dans le cadre du groupe de travail du RIS sur le thème « logiciel libre et la sûreté de fonctionnement ».

Quatre exposés ont suivi :

- Évolution de la conception des "systèmes sur une puce" à l'ère des nanotechnologies
  par *Jean-Pierre Schoellkopf (ST Microelectronics, Crolles)*
- Développement de systèmes critiques intégrant des logiciels libres
  par *Philippe David (ESA-ESTEC, Noordwijk, Pays-Bas)*
- L'intégration du facteur humain dans la conception des systèmes à risques
  par *Hubert Guillermain (Technicatome, Aix en Provence)*
- Nouvelles architectures avioniques et sûreté de fonctionnement
  par *Pascal Traverse (Airbus France, Toulouse)*

Ils ont été très denses et instructifs. Ils ont aussi suscité de nombreuses questions de la part de l'audience qui ses sont traduites par des réactions et des interactions tout à fait explicites de la part des orateurs. Ils ont été unanimement appréciés par les participants.

Groupes de réflexion de l'après-midi

Un sondage rapide ayant fait état d'un petit nombre de participants (6 personnes) désirant explicitement contribuer au groupe de réflexion sur le thème 1, il a été décidé de ne pas se séparer en deux groupes. Une seule session, rassemblant tous les participants, a donc eu lieu. Néanmoins, les deux thèmes ont été successivement abordés dans le même ordre que celui indiqué sur le programme.

Infrastructures informationnelles sûres de fonctionnement : confiance à hauteur des enjeux ?

Jean-Claude Laprie a fait une courte présentation (*Secure Ambient Intelligence Landscape Needs Dependable Information Infrastructures*) au cours de laquelle il a mis l'accent sur principaux points suivants :

L'**ouverture** sans frontière des systèmes et le corollaire à cette ouverture : l'impact croissant des fautes de type malveillance.

L'**évolutivité** exemplaire des systèmes, qui s'applique tant au niveau des fonctionnalités, ce qui se traduit par la disparition de la notion de « système final », qu'au niveau de la prise en compte de dysfonctionnements, ce qui peut être rapproché de l'émergence de l'autogestion des systèmes pour

l'adaptation autonome de leur configuration à différents facteurs d'évolution de leur environnement (par ex. *autonomic computing* d'IBM).

La **mobilité** dynamique à la fois des agents et des infrastructures de communication.

Plusieurs problèmes majeurs ont également été identifiés :

- l'accroissement quasi-exponentiel des **vulnérabilités** liées à l'informatique et les coûts considérables induits par les défaillances partielles, voire les abandons de projets logiciels aux USA.
- l'augmentation significative de l'**indisponibilité** des systèmes à partir de deux catégories de systèmes : d'une part, l'Internet par rapport aux systèmes transactionnels et d'autre part, les systèmes de communication téléphoniques mobiles par rapport au cas des postes fixes.
- l'existence d'un **décalage** important entre les **risques perçus** et les **risques réels** : la perception se focalise sur les risques liés aux virus, alors que d'autres risques (tels que ceux liés à la perte de services de base offerts par les grandes infrastructures ou à une mauvaises utilisation des systèmes) sont bien présents.

Bernard Pavard a ensuite mis l'accent sur les problèmes posés par la robustesse des systèmes socio-techniques en situation de crise. Il s'agit là de grands systèmes ouverts et hétérarchiques, faisant intervenir différents réseaux tant technologiques que liés aux service d'urgence (SAMU, pompiers, etc.,) et à l'équipement du territoire (réseau électrique, réseaux de communication,...). Des études sont actuellement initiées afin d'analyser le fonctionnement nominal de ces réseaux afin d'anticiper les problèmes éventuels et de mieux préparer les situations de crise. Ils s'appuient sur la théorie du contrôle et l'anticipation des collectifs.

La discussion a porté sur plusieurs aspects de la problématique, en particulier, sur l'identification des **interdépendances** existant entre les différents infrastructures et réseaux mis en jeu. Jean-Claude Laprie a notamment précisé que lors de l'accident de l'usine AZF à Toulouse en septembre 2001, seul le réseau Internet était resté disponible : les autres réseaux de communication (par ex. téléphonies mobile et fixe) avaient été rapidement saturés.

Bernard Pavard a indiqué qu'une des solutions actuellement envisagées était de prévoir une certaine bande passante prioritaire (par exemple, au niveau des communications satellitaires).

Cette session, en dépit de sa brièveté, a néanmoins permis d'échanger des idées mêlant les problématiques technologiques et organisationnelles bien en phase avec les objectifs de croisement de domaines de compétences que le réseau désire favoriser. De plus, ces discussions dénotent de façon tout à fait explicite que ce thème a reçu un intérêt marqué de la part de plusieurs participants.

Systèmes embarqués et systèmes enfouis : impact de la prise en compte de la sûreté de fonctionnement ?

En guise d'introduction, Marie-Claude Gaudel a présenté quelques planches. Elle a tout d'abord rappelé les thèmes des différentes Actions Spécifiques associées au RTP21. Ceci a notamment permis aux animateurs des Actions en cours d'intervenir brièvement pour expliciter les thèmes développés au sein de leur AS. Elle a ensuite rappelé les orientations scientifiques que le réseau entend favoriser afin d'identifier quelques pistes possibles pour la mise en place de nouvelles actions.

Bernard Courtois est ensuite intervenu pour demander aux participants de bien vouloir se situer suivant les aspects « matériel », « logiciel » et « système » de la problématique. La distribution des réponses est relativement bien équilibrée et se situe comme suit[1] :

Matériel : 8 Logiciel : 15 Système : 12

Marie-Claude Gaudel a noté une proportion significative d'industriels dans la catégorie « système ».

[1] Bien que le total soit égal à 35, il est important de noter que :
- cinq participants à la journée, n'ayant pu rester jusqu'à cet instant, ils n'ont donc pas pris part à ce « sondage ».
- des réponses multiples étaient permises.

Trois principaux points ont été abordés au cours de la discussion : la prise en compte de l'impact croissant des *« soft-errors »*, les incertitudes induites par les nouvelles architectures de processeurs sur les comportements temporels, les relations/différences entre preuve et test.

Prise en compte des « soft errors »

Bien que le problème de l'impact des radiations sur les circuits intégrés soit connu depuis longtemps dans le contexte spatial, en raison de la réduction des dimensions géométriques et des niveaux de tensions impliqués, l'acuité du problème est que ces effets sont maintenant perceptibles au niveau atmosphérique et aussi au niveau du sol.

La discussion qui s'est engagée a permis d'identifier les principaux points suivants :

1) Les conséquences essentiellement transitoires de telles fautes sont à rapprocher des conséquences des effets de couplage au niveau physique ou bien des fautes du logiciel.
2) Ces fautes induisent des comportements byzantins transitoires qui soulèvent de nouveaux problèmes au niveau des algorithmiques de tolérance aux fautes.
3) Les circuits modernes intègrent de plus en plus de fonctions afin de répondre aux exigences des applications, ce qui justifie donc pleinement le souci d'intégration et de complexification des comportements.
4) Les solutions technologiques spécifiques (circuits durcis) sont trop onéreuses et ne sont pas viables.
5) C'est donc au niveau de l'architecture et des comportements des circuits qu'il semble nécessaire de chercher des solutions.
6) Une solution pour faciliter l'analyse de ces problèmes peut passer par la simulation : les architectures de certains processeurs décrits en VHDL (ou tout au moins certaines parties) ainsi que certaines bibliothèques relatives à des circuits complexes (par ex. FPGA) pourraient être mises à disposition (*Open Source*), comme l'a fait par exemple l'ESA pour le processeur LEON.

Un intérêt marqué est à signaler sur ce point tant au niveau des participants académiques qu'industriels. Un groupe de travail du RIS est en train de se mettre en place sur cette problématique ; il serait bon de pouvoir associer les deux démarches.

Impact des architectures de processeurs sur les comportements temporels

La présence de mémoires cache, et le parallélisme croissant des activités se traduisent par des comportements temporels non déterministes. En effet, ces éléments architecturaux ne sont la plupart du temps pas accessibles aux utilisateurs, ce qui pose de plus en plus de problèmes quant à la possibilité de prédire de façon fiable les comportements temporels.

Il devient de plus en plus difficile de déterminer des bornes — par ex. le WCET (*Worst Case Execution Time*) — qui soient représentatives et donc utiles, c'est-à-dire pas trop pessimistes.

Dans ce cas encore, il semble que la simulation de ces éléments architecturaux puisse permettre d'obtenir de meilleurs résultats. Ceci est également à rapprocher de la remarque relative au point 6) du thème précédent.

Plusieurs participants — académiques et industriels — ont exprimé un vif intérêt sur ce thème.

Preuve vs. test

La discussion a porté sur les bienfaits respectifs et complémentarités des techniques de preuve et de test en dégageant les principaux points suivants :

- L'utilisation plus généralisée de techniques de preuves analytiques et prédictives permettrait de modifier le processus de développement en réduisant les efforts et les coûts associés aux tests effectués dans les phases aval.
- Dans quelle mesure les types de preuves mathématiques considérées se distinguent elles des techniques de type vérification de modèles (*model checking*).
- C'est au niveau « système », et ce dès les étapes initiales du développement (juste après le recueil des exigences du système) que doivent être effectuées ces preuves et pas seulement au niveau du logiciel. Ce n'est pas l'implémentation qui pose le plus de problème, c'est surtout au niveau des spécifications du niveau « système ».

- Néanmoins, il est à noter que tout n’est pas encore résolu au niveau de l’implémentation : il existe un manque entre la spécification et la mise en œuvre.
- Il a été noté que dans le contexte du ferroviaire, l’objectif est de faire évoluer l’utilisation de la « méthode B », depuis le logiciel vers le niveau « système ».

À l’issue de cette discussion fort animée, il semble justifié que toute réflexion sur les notions de preuve et de vérification, en particulier dans le contexte des systèmes enfouis/embarqués doivent être associées avec le RTP 19 (Systèmes embarqués complexes et contraints).