La fiabilité des systèmes devient un défi majeur

Hubert Garavel, Isabelle Bellin

Hubert Garavel, Isabelle Bellin (Technoscope) - 20/11/2012

La fiabilité des systèmes devient un défi majeur

Airbus A350. - *© Airbus*

En 20 ans, les systèmes informatiques (ordinateurs, logiciels, réseaux) ont envahi notre vie courante et sont désormais au cœur d'applications de plus en plus vitales. Leur complexité technique augmente sans cesse, alors que leur contexte de production est de plus en plus tendu, réductions de coûts et de délais obligent. Quelles conséquences en termes de qualité, sûreté et sécurité ? Eviter les défaillances informatiques représente un enjeu d'avenir, majeur pour l'industrie, sur la base des progrès scientifiques de ces dernières décennies.

Témoignage d'Hubert Garavel, lauréat du prix Gay-Lussac Humboldt en 2011, pionnier dans le développement de méthodes formelles et d'outils de vérification pour les systèmes industriels critiques.

La prise de conscience des enjeux de la fiabilité logicielle a eu lieu dès 1968 lors d'une conférence consacrée à la « crise du logiciel » : comment répondre aux besoins en produisant en quantité des logiciels de qualité ? De là est née la discipline du génie logiciel qui a considérablement amélioré la pratique industrielle. Mais le sujet a repris une nouvelle acuité ces vingt dernières années, car le paysage informatique a été profondément modifié par quatre changements majeurs :

- La diffusion massive des logiciels embarqués, devenus omniprésents dans les avions, les voitures, les téléphones, ou les télévisions, bien au delà de ce qu'on pouvait imaginer en 1968 ;
- La complexité croissante des systèmes informatiques, mesurée en nombre de lignes de code pour les programmes et en nombre de transistors pour les circuits électroniques ;
- La montée en puissance de la programmation parallèle — plus performante mais beaucoup plus difficile que la programmation séquentielle classique — indispensable aussi bien pour exploiter les processeurs multi-cœurs des ordinateurs grand public que les centaines de milliers de processeurs des supercalculateurs ;
- La mise en réseau généralisée de tous les ordinateurs et équipements, désormais interconnectés par Internet, ce qui pose de redoutables défis en termes de sécurité.

> *« On confie aux systèmes informatiques des missions de plus en plus critiques sans que leur sûreté et leur sécurité ne soient toujours à la hauteur »*

Ainsi, le bulletin « Risks Digest » recense chaque mois la liste des défaillances informatiques, souvent coûteuses et parfois mortelles, survenues dans le monde. Au delà d'accidents industriels très médiatisés (comme le bug du processeur Pentium en 1994 ou l'échec d'Ariane 5 en 1996), ces problèmes s'installent de manière discrète, mais lancinante, dans notre vie quotidienne. On les retrouve, par exemple, dans les pannes automobiles dues à l'électronique et au logiciel, les fraudes et les attaques sur Internet, ainsi que les usurpations d'identité. Globalement, on estime que le coût annuel des pannes logicielles pour l'économie mondiale avoisine aujourd'hui la centaine de milliards d'euros.

Pourtant, durant les 20 dernières années, les recherches en génie logiciel ont beaucoup progressé : les méthodologies se sont affinées, les langages se sont améliorés, les outils de vérification et de test sont devenus plus puissants, plus rapides et plus automatiques. Ces résultats sont déployés dans l'industrie, mais ils restent trop souvent réservés à certains domaines, soit lorsque des autorités de certification veillent à la sûreté publique (aviation civile, nucléaire, transports collectifs), soit lorsque la réparation d'éventuelles erreurs aurait un coût prohibitif (microprocesseurs et circuits électroniques à large diffusion). Malheureusement, trop de systèmes informatiques sont encore développés dans l'urgence sans mettre en œuvre les bonnes pratiques qui permettraient d'améliorer leur qualité.

Dans ce vaste domaine de recherche où beaucoup de questions restent à résoudre, plusieurs équipes d'Inria à Grenoble (Convecs, Mescal, Moais, Pop-art, Privatics, Sardes et Vasy) s'attaquent à des problèmes difficiles : systèmes distribués, systèmes embarqués, calcul parallèle, sûreté, sécurité et protection de la vie privée. Une attention particulière est portée aux systèmes embarqués qui doivent gérer en continu consommation énergétique, performance et disponibilité, ainsi qu'aux processeurs multi-cœurs, à la manière de les concevoir et de les programmer pour exploiter au mieux la puissance qu'ils fournissent. Depuis 20 ans, les progrès sont constants et ils sont transférés aux entreprises, souvent sous l'égide du pôle de compétitivité Minalogic.

CADP : des logiciels pour maîtriser le parallélisme

Les équipes Vasy et Convecs d'Inria et du LIG (Laboratoire d'Informatique de Grenoble) ont largement contribué au

développement de la boîte à outils CADP (*Construction and Analysis of Distributed Processes*). Lancée il y a 25 ans, cette plateforme de recherche rassemble désormais une cinquantaine d'outils dédiés à la modélisation, la vérification, le test et l'évaluation de performances pour les systèmes distribués et parallèles. De nombreux universitaires l'utilisent dans le monde pour enseigner ces sujets. Plus de 150 publications scientifiques traitent de problèmes résolus avec CADP et plus de 60 outils de recherche sont connectés à CADP.

Parmi les applications industrielles : la boîte à outils est reliée à la plate-forme de développement Topcased pilotée par Airbus, Bull s'est appuyé sur CADP pour valider l'architecture de ses supercalculateurs et STMicroelectronics et le CEA Leti l'ont utilisé pour vérifier des systèmes et réseaux sur puce et prédire leurs performances. Et de nouveaux partenariats ciblent les automates programmables, les interfaces graphiques et le cloud computing.

ET DANS 20 ANS ?

Hubert Garavel, directeur de recherche, équipe CONVECS

Hubert Garavel - © *Inria / Photo A.Eidelman*

« Les tendances actuelles vont certainement s'accentuer : les systèmes informatiques gèreront une part croissante de notre vie sociale, s'étendant à de nouveaux domaines tels que la distribution d'énergie et l'aide à la conduite automobile. La complexité matérielle et logicielle des systèmes embarqués ira en augmentant avec l'ajout de nouvelles fonctionnalités et l'évolution des architectures : généralisation du calcul parallèle, regroupement de multiples fonctions sur des processeurs multi-cœurs, interconnexion systématique à Internet et optimisation de la consommation énergétique. De tels changements risquent de rendre le fonctionnement des systèmes beaucoup plus difficile à prévoir.

Les scientifiques travaillent sur ces problématiques complexes pour lesquelles ils ont développé un vrai savoir-faire. Mais la diffusion de ces résultats et leur mise en œuvre par les industriels est un autre enjeu. Une prise de conscience aura-t-elle lieu à temps pour traiter en amont les problèmes de sûreté et de sécurité ? Ou bien des accidents imposeront-ils une régulation plus drastique, avec une responsabilité accrue pour les concepteurs de systèmes et, par exemple, l'obligation d'employer des développeurs spécialement qualifiés à cet effet, comme cela est la règle dans d'autres corps de métiers ? La question reste ouverte.»

Dates clés

- **1992** : Parution de la norme DO-178B (*Software Considerations in Airborne Systems and Equipment Certification*) qui fixe un cadre méthodologique pour le développement du logiciel embarqué.
- **1993** : Première version de l'atelier logiciel SCADE pour le langage synchrone Lustre (N. Halbwachs et P. Caspi) développé à Grenoble, désormais largement utilisé dans l'industrie aéronautique.
- **1999** : Création de la société Polyspace à Grenoble pour diffuser industriellement les avancées théoriques de l'interprétation abstraite (P. et R. Cousot).
- **2006**: Vérification mathématique d'un compilateur C garanti sans erreur pour les systèmes critiques (S. Blazy, Z. Dargaye, X. Leroy).
- **2012** : Parution de la norme révisée DO-178C et de son supplément DO-333 qui consacre l'utilisation des méthodes formelles pour la certification des systèmes critiques.

Numérique & société

- **1985-1987**: **le bug informatique le plus grave de l'histoire** : plusieurs patients sont décédés ou ont été gravement atteints dans leur santé suite à un surdosage en rayons X d'un appareil médical de radiothérapie.
Source Wikipedia.org
- **1996 : le bug informatique le plus coûteux de l'histoire** : l'échec du vol inaugural de la fusée Ariane 5 en raison d'un calcul erroné dans les appareils d'avionique
Source Wikipedia.org

1992 - 2012

- Collection "20 ans d'avancées et de perspectives en sciences du numérique" par les chercheurs d'équipes Inria de Grenoble et Lyon.
- www.inria.fr/20ansgrenoble