INFORMATIQUE ET SÛRETÉ DE FONCTIONNEMENT

Ce n'est qu'un début...

La recherche en informatique, présente au LAAS dès sa fondation, a connu d'indéniables succès, tant sur le plan international que sur celui des relations industrielles. L'avènement des systèmes informatiques ubiquitaires présente nombre de défis, scientifiques et technologiques, qui offrent l'opportunité d'une riche feuille de route.

La recherche en informatique a été présente au LAAS dès sa fondation, avec comme centres d'intérêt l'architecture de calculateurs pour la commande et la surveillance de procédés ou d'objets, aérospatiaux en particulier, la synthèse, le test et l'auto-test de circuits logiques intégrés.

Le souci d'éviter que les défaillances informatiques n'affectent les procédés ou objets commandés a conduit très rapidement les recherches en architecture à s'insérer dans le mouvement alors naissant de la tolérance aux fautes, et, de là, à fortement contribuer à sa généralisation en termes de sûreté de fonctionnement. La modélisation du comportement de circuits séquentiels multiples a conduit à la description et à la validation de systèmes parallèles par des méthodes mathématiquement formelles, alliant systèmes de transition qui généralisent les machines à états, et logique mathématique, avec les réseaux de Petri comme outil privilégié. Ces deux évolutions ont été concrétisées par la fondation mi-années 70 de deux groupes de recherche : Tolérance aux fautes et sûreté de fonctionnement informatique, TSF, et Outils logiciels pour la communication, OLC. Afin de s'assurer de la pertinence des architectures tolérantes aux fautes, le groupe TSF s'est simultanément intéressé à l'évaluation probabiliste de leur comportement en présence de fautes. Le groupe OLC, pour sa part, se focalisant sur les protocoles de communication, au cœur des réseaux informatiques. Pour compléter cette genèse des recherches en informatique au LAAS, il convient de mentionner celles menées en robotique sur l'intelligence artificielle pour l'autonomie.

Les recherches menées par les groupes TSF et OLC l'ont naturellement été dans le style, alors original, qui caractérisait le LAAS, alliant spéculations scientifiques au meilleur niveau international et concrétisations technologiques par des relations industrielles. La formalisation de ce style, répandu depuis, peut être trouvée dans le modèle dit du *quadrant de Pasteur* [voir ci-contre], qui caractérise la recherche scientifique selon deux dimensions : quête de compréhension fondamentale, et considération d'utilisation. Augmenter les chances de succès des recherches, vu la complexité des problèmes abordés, passant par des collaborations, les deux groupes ont été présents dans les programmes européens dès leur début, par deux projets du programme ESPRIT *(European Strategic Programme for Research and Development in Information Technology)* du premier programme-cadre : coordination scientifique du projet Delta-4 *(Definition and Design of an open Dependable Distributed Architecture)* pour TSF, responsabilité d'ensemble du projet SEDOS *(Software Environment for the Design of Open Distributed Systems)* pour OLC.

Quête fondamentale et relations industrielles

Focalisant dans la suite sur la sûreté de fonctionnement informatique, nos travaux sont considérés comme pionniers selon plusieurs registres : construction et validation de modèles markoviens et non markoviens, extension de la théorie de la fiabilité aux systèmes matériels-et-logiciels, test statistique du logiciel, validation de la tolérance aux fautes par injection de fautes, étalonnage *(benchmarking)* de la sûreté de fonctionnement, notion de processeur à silence sur défaillance, tolérance aux malveillances (intrusions), sans oublier la formulation des concepts de base de la sûreté de fonctionnement et la terminologie associée, largement adoptée par l'ensemble de la communauté internationale. Le panorama serait incomplet sans mentionner nombre d'autres contributions significatives s'étalant sur plusieurs années, en évaluation tant théorique qu'expérimentale de la croissance de fiabilité du logiciel, en tolérance aux fautes logicielles, en algorithmique répartie pour la tolérance aux fautes, y compris en tenant compte de la mobilité, en tolérance aux fautes adaptative par des langages dits réflexifs, en politiques de sécurité au sens de l'immunité vis-à-vis des malveillances, en protection de la vie privée, en expression et maîtrise des interdépendances entre ce qui est devenu l'infrastructure informationnelle et les autres infrastructures essentielles, électrique en particulier.

Les résultats de ces travaux ont, pour la plupart, été concrétisés par des outils ou des démonstrateurs. Certains se sont avérés pérennes grâce au soutien d'ingénieurs du service d'informatique du laboratoire, tel le logiciel SURF pour l'évaluation de la sûreté de fonctionnement par réseaux de Petri stochastiques et chaînes de Markov.

Les collaborations européennes se sont poursuivies sans discontinuité au fil des programmes-cadre successifs, par 17 projets, avec la responsabilité de deux d'entre eux : le projet DBench *(Dependability Benchmarking)*, et le réseau d'excellence ReSIST *(Resilience for Survivability in Information Society Technologies)* encore en cours.

Notre position internationale de premier plan est avérée par, outre les articles et communications dans des revues et congrès au meilleur niveau, et les ouvrages écrits ou dirigés, les responsabilités exercées dans des sociétés savantes (IEEE et IFIP en particulier), et, liée à

ces responsabilités, l'organisation des conférences phares du domaine, comme les symposiums internationaux *Fault-Tolerant Computing* (par deux fois, en 1978 et en 1993) et *Software Reliability Engineering* (en 1995), ou, débordant largement la sûreté de fonctionnement pour embrasser l'ensemble de l'informatique, le *World Computer Congress* (en 2004).

Pour en revenir au quadrant de Pasteur, les paragraphes qui précèdent se rapportent essentiellement à la première de ses dimensions, la quête de compréhension fondamentale. La deuxième dimension, la considération d'utilisation, outre la référence à des outils diffusés comme le logiciel SURF déjà mentionné, est surtout caractérisée par les relations avec l'industrie. Ces relations ont toujours été présentes, sous diverses formes, informelles ou de partenariat, via des conventions de recherche ou des actions d'ingénieur-conseil, tant en France qu'à l'étranger. Pratiquement tous les secteurs d'activité économique étant devenus dépendants de l'informatique, nos relations industrielles ont, au fil du temps, concerné une vaste panoplie de secteurs applicatifs : aéronautique, espace, ferroviaire, automobile, production d'énergie, télécommunications, santé, sans oublier la construction informatique elle-même. Elles ont culminé lors de la création en 1992 avec Astrium (alors Matra Marconi Space) et Areva-TA (alors Technicatome) du LIS, le laboratoire commun d'ingénierie de la sûreté de fonctionnement ; à ces premiers partenaires se sont joints dans une deuxième étape Airbus, EDF et Thales.

Quid de l'avenir ? Les futurs systèmes informatiques tels qu'on les entrevoit seront d'immenses systèmes d'information, incorporant tout, depuis des super-ordinateurs et de gigantesques « fermes » de serveurs jusqu'à des myriades de petits ordinateurs mobiles et de minuscules objets dits embarqués (selon la maladroite, mais consacrée, traduction de l'anglais *embedded)*. De par leur insertion dans tous les actes de la vie, de tels systèmes peuvent être qualifiés de systèmes ubiquitaires. Au-delà de leur description par énumération, leur avènement s'accompagnera de profondes évolutions scientifiques et technologiques. Sans aucune prétention à la préfiguration de la structure de ces systèmes ubiquitaires, certaines évolutions drastiques sont déjà perceptibles, que ce soit dans le génie logiciel où l'agglomération de services existants découverts sur l'Internet a déjà commencé à remplacer le développement classique selon des étapes codifiées, dans la migration des systèmes d'exploitation vers le Web pour donner naissance au *network computing* (ou, familièrement, *cloud computing*), dans la convergence du Web et des objets embarqués, dans l'architecture même des réseaux, où la communication prend déjà bien souvent la forme d'essaims de contenus, qui ne vont plus d'un endroit à un autre, mais qui émanent comme des ondes générées en plusieurs points d'un étang, et deviennent disponibles pour une utilisation locale, sans oublier les capacités de mémorisation et les puissances de traitement qui seront amenées par les dimensions nanométriques des éléments de base du matériel. En liaison directe avec leur gigantisme et leur complexité, les systèmes ubiquitaires seront caractérisés par des changements incessants, dans leur composition, dans leur structure, qui rendront hors de portée l'analyse, la modélisation, la prévision de leur comportement avant déploiement opérationnel, sans même parler de l'anticipation des comportements émergents issus de la multitude des interactions.

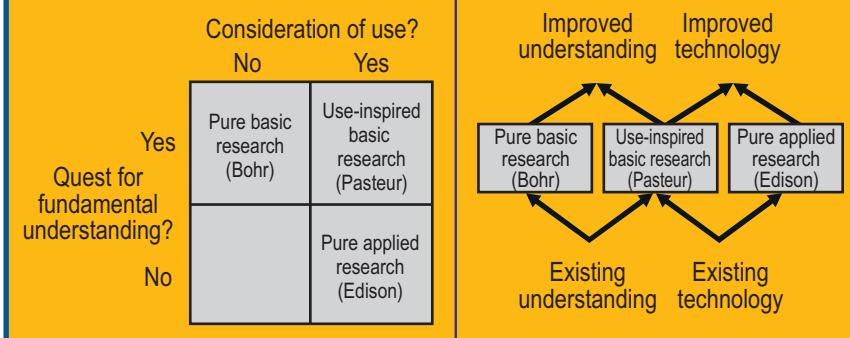
> **« Ces systèmes ubiquitaires feront partie du tissu même de notre société. A ce titre, leur sûreté de fonctionnement se devra d'être à la hauteur de celle des autres infrastructures essentielles de la société. »**

Ces systèmes ubiquitaires feront partie du tissu même de notre société. A ce titre, leur sûreté de fonctionnement se devra d'être à la hauteur de celle des autres infrastructures essentielles de la société, telles que les transports publics, la distribution d'électricité ou d'eau. Or, l'examen de la sûreté de fonctionnement des grands systèmes en réseau actuels, qui sont une (pâle) préfiguration des systèmes ubiquitaires, entraîne de sérieuses interrogations : par rapport aux systèmes informatiques critiques traditionnels, les grands sites Web souffrent statistiquement d'une chute de plusieurs ordres de grandeur, par exemple en termes de temps moyen jusqu'à défaillance. Il s'agit donc, à terme, d'un véritable problème de société, celui de l'infrastructure support de la « société de la connaissance » appelée de leurs vœux par les politiques de tous bords.

Les approches classiques de la sûreté de fonctionnement ont été essentiellement réactives, basées sur la détection d'anomalies, et sur la capacité des systèmes à se récupérer, via la détection des erreurs, la récupération s'effectuant par le traitement des erreurs et des fautes à l'origine des erreurs. Ces approches sont basées sur une hypothèse forte : l'existence de zones de confinement des erreurs à même limiter leur propagation. Que cette hypothèse ne soit plus vérifiée dans la structure des grands systèmes évolutifs en réseau est à l'origine de la piètre sûreté de fonctionnement constatée. Les évolutions brossées précédemment, jointes à une pression économique favorisant le court terme, ne favoriseront certainement pas la résurgence de la structuration des systèmes selon des zones de confinement d'erreurs. Les incessants changements qui caractériseront les systèmes ubiquitaires font, qu'à terme, le but doit être la persistance de la sûreté de fonctionnement lorsque confrontés à des changements, c'est-à-dire la résilience, et ce vis-à-vis des diverses causes de défaillance des systèmes informatiques : défaillances du matériel, erreurs logicielles résiduelles, erreurs d'interaction homme-système, attaques malveillantes. Les systèmes ubiquitaires verront ces sources classiques de défaillance évoluer, et de nouvelles sources sont prévisibles, comme des comportements émergents indésirables, résultant d'incompatibilités dans les évolutions continuelles caractéristiques de ces systèmes, y compris de nouvelles vulnérabilités. Un véritable changement de paradigme est donc nécessaire, par exemple en substituant aux approches réactives des approches *proactives*, c'est-à-dire permettant de détecter et de traiter les causes potentielles de défaillance quand elles sont encore précisément potentielles, avant qu'elles ne causent des anomalies dans la délivrance des services. La formulation des concepts et modèles permettant ce changement de paradigme, leur mise en œuvre par des architectures, algorithmes et mécanismes représentatifs, s'ils nécessiteront la même rigueur scientifique et le même souci technologique dont nous avons fait preuve au cours des quarante années écoulées, nécessiteront par contre encore plus d'imagination. ■

Jean-Claude Laprie
Directeur de recherche de classe exceptionnelle au CNRS
Directeur du LAAS de 1997 à 2002

Quadrant de Pasteur



[De Donald E. Stokes, Pasteur's Quadrant – Basic Science and Technological Evolution, Brookings, 1997]