Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

Janvier 2009

Projet IMdR P06-1
Apport de la modélisation à la sûreté de fonctionnement de systèmes informatisés

Chef de Projet :
Monsieur Marc ANTONI – SNCF

Contractants :
SOCIETE APSYS

Le projet P06-1 de l'IMdR intitulé « Apport de la modélisation à la sûreté de fonctionnement de systèmes informatisés » a été réalisé en 2007-2008. Les souscripteurs qui y ont participé sont DGA-CEAT, INERIS, RATP, RENAULT et SNCF.

Synthèse

Ce projet a consisté à étudier l'apport de la modélisation dans la maîtrise de la Sûreté de Fonctionnement des systèmes informatisés; il a naturellement conduit les souscripteurs à analyser les modalités d'utilisation des méthodes, ou langages formels et semi-formels à travers les processus de développement des systèmes informatisés, notamment en ce qui concerne la maîtrise des composantes logicielles.

Le premier rapport constitue un état de l'art des différentes méthodes formelles et semi-formelles et applique différents points de vue de regroupement et de classification, pour fournir un éclairage sur les atouts et handicaps, cas d'utilisation ainsi que divers éléments d'analyse comparative.

Le deuxième rapport décrit les différents apports spécifiques susceptibles d'être assurés par les méthodes formelles et semi-formelles vis-à-vis des applications logicielles tout au long de leur cycle de développement et plus généralement de leur cycle de vie.

Le troisième rapport, quant à lui, présente un exemple de référentiel méthodologique permettant de procéder à une analyse multi-critère pour justifier le choix de méthode formelle ou semi-formelle dans le cadre d'un processus de développement particulier.

Enfin, le dernier rapport traite un certain nombre d'exemples concrets proposés par les souscripteurs et résolus à travers l'utilisation de différents langages et outils dont la mise en œuvre est décrite à titre d'exemple.

A l'issue de ce projet, il apparaît clairement que différentes considérations doivent être prises en compte, avant d'être en mesure de valider l'adoption d'une méthode formelle ou semi-formelle, et son intégration au cycle de développement d'une application:

- les atouts ou handicaps organisationnels de la société, du département ou du service ayant l'intention de mettre en œuvre des méthodes formelles : des déficits ou faiblesses organisationnelles importantes pourraient être bloquantes,

- les priorités performantielles présentées par l'application : la mise en œuvre des méthodes formelles semble particulièrement bien recommandée lorsque la sécurité des biens et des personnes semble impliquée dans la mise en œuvre de cette application,

- les bénéfices attendus au niveau des différentes phases du processus de développement : ils sont nombreux et divers; bénéfice économique et de maintenabilité du logiciel (réduction des temps de mise au point, réduction des temps de validation après évolution / modification…) notamment ; à termes, les méthodes formelles devraient se généraliser aux différentes phases du processus, tant elles constituent un support privilégié et rigoureux de formalisation de la connaissance de spécification, de conception, et de maîtrise du comportement de l'application logicielle à développer,

- les caractéristiques intrinsèques présentées par l'application et devant influer sur le choix de la technique formelle à cibler ; notamment son aptitude à être définie par les propriétés de sécurité fonctionnelles à vérifier et les postulats de fonctionnement dans lesquels la preuve est valide (environnement, règles d'usage…) : bien sûr, elles conditionnent largement le type de méthode, technique ou langage formel applicables à l'évaluation, et qui lui seront le plus profitables du point de vue des traitements d'évaluation et de démonstration,

- les contraintes de coûts et délais imposés par le projet : des modèles technico économiques d'aide à la décision peuvent s'avérer nécessaires, pour réduire les coûts liés aux essais habituels, le processus itératif d'essais d'outil rendant difficile la prédiction des temps ou coûts associés à la phase de validation. A ce titre, les méthodes formelles permettent aux concepteurs de substituer une obligation de résultat à une obligation de moyen pour les systèmes informatiques,

- les traitements formels ciblés apriori dans le cadre de ce choix, pour lesquels certaines techniques ou certains langages pourraient s'avérer plus pertinents que d'autres,

- les méthodes, techniques et outils disponibles sur le marché,

- les retours d'expérience sur leur mise en œuvre jusqu'à maintenant et qui permettront de valider une préférence d'un outil par rapport à l'autre.