BRAMA : un nouvel outil d'animation graphique de modèles B

Clearsy - Conférence B 2007

Introduction

Clearsy est une société d'ingénierie spécialiste en Sûreté de Fonctionnement des systèmes.

Elle maîtrise les concepts et outils nécessaires à la réalisation de systèmes sûrs, et utilise les techniques formelles pour spécifier, concevoir et valider les systèmes puis pour réaliser les logiciels critiques les intégrant.

Les outils formels utilisés par Clearsy sont principalement *l'Atelier B et B4free* pour réaliser les modèles, les raffinements et leur preuves et *CompoSys* pour réaliser les modèles formels systèmes et la documentation associée.

Nos différentes expériences d'utilisation d'outils formels en milieu industriel et notre volonté de dissémination des méthodes formelles nous a conduit à imaginer une nouvelle approche pour présenter les modèles à nos clients. L'outil Brama supporte cette approche.

Ce document a pour but d'expliquer cette approche et l'outil associé Brama.

Contexte : le besoin de valider les modèles

La méthode B est beaucoup utilisée en milieu industriel pour réaliser des logiciels sécuritaires prouvés, dans des contextes de certification à un niveau SIL 4 selon la norme 61508.
Elle est utilisée depuis quelques années pour modéliser des systèmes.
Cette nouvelle pratique a révélé un manque.
En effet, lorsque l'on souhaite spécifier un système il faut :

- savoir ce que l'on veut
- s'assurer de la faisabilité de ce que l'on veut

L'activité de modélisation et de preuve permet de découvrir des problèmes dans la spécification. C'est l'intérêt même de modéliser. En cela, la méthode B a l'avantage d'être basée sur les mathématiques, ce qui permet d'écrire la spécification avec une précision inégalée.
Mais nous nous sommes rendus compte que face à un modèle, nos clients et d'une manière générale ceux qui n'ont pas écrit le modèle ont du mal à le comprendre d'une part, et d'autre part ont du mal à affirmer que le modèle représente le système.
Se pose donc le problème de la complétude et de la qualité du modèle.

Traduction des modèles en langage naturel

Une première réponse au problème de compréhension d'un modèle B a été apporté par Clearsy en proposant l'outil CompoSys, qui permet au modélisateur de réaliser la documentation du modèle en même temps que le modèle. Cet effort permet à l'utilisateur de produire automatiquement la traduction du modèle, en y incluant différentes vues graphiques de dépendances entre les différents composants du système. Cette documentation en langage naturel est l'exacte reflet du modèle et peut être lue « facilement » par tous pour s'assurer de la fidélité du modèle au système.

L'Animation pour « tester » les modèles

Un autre réponse est apportée par l'outil d'animation de modèles de Brama. Cet outil peut être utilisé par le modélisateur au fur et à mesure de son travail de modélisation. Les fonctions d'animation lui permettent en effet de « mettre en œuvre » les différents évènements, gardes et propriétés du modèles ; il « teste » le modèle.

Visualisation graphique du système

Une troisème piste consiste à utiliser le modèle pour visualiser graphiquement le système dans le fonctionnement spécifié.

La démarche consiste à proposer à l'auteur des modèles des outils permettant de :

- représenter par des dessins et animations graphiques le système et ses différents états
- « relier » ces dessins et animations au différents évènements et variables B du modèles B
- représenter par des boutons les différentes interactions des éléments externes au système et réactualiser la représentation graphique du système en fonction de ces interactions

Le modèle n'est ainsi pas montré au client, c'est la représentation graphique du système qui est présenté, cette représentation s'effectuant sur la base du modèle B lui même.

Plus de détail sur l'outil Brama

Le modélisateur réalise ses modèles B avec l'Atelier B, B4free ou la plateforme Rodin, puis ensuite exploite l'outil d'animation Brama, qui exploite ces modèles.

Brama a été conçu pour communiquer avec les outils Flash que l'on configure avec une extension de communication livré avec Brama.

Le travail du modélisateur consiste à représenter son système avec les outils Flash et à configurer les scripts permettant de dialoguer avec le moteur d'animation Brama.

Quand l'utilisateur est satisfait, Brama lui permet d'exporter l'animation réalisée sous formes de fichiers, qui une fois gravés sur un CD permet de lancer l'animation graphique sans installation préalable et sur n'importe quel PC sous Windows ou Linux.

Brama se présente comme une suite de plugin Eclipse et d'une extension Flash, utilisables sous Windows et Linux.
Brama contient les modules principaux suivant : BtoRodin : un moteur d'animation (solveur de prédicat), des outils de visualisation des évènements et variables B, module de gestion de l'enchaînement automatique des évènements, module de gestion des variables, prédicats et expressions observées, et module de communication avec Flash.

Des exemples, retour d'expérience

Des premiers exemples ont été développés sur la base de modèles d'expérimentation : presse mécanique, trafic routier île/continent, écluse, aiguillage, contrôle des tuyères d'Ariane.
Le travail sur ces exemples a permis de montrer des défauts présents dans les modèles analysés, confirmant l'intérêt de visualiser le système pour mieux s'assurer de la fidélité du modèle.
Ce travail de représentation graphique n'est pas conséquent : une semaine environ pour mettre au point l'animation d'un modèle réalisé en deux mois. Le plus gros modèle représente 450 évènements et 17 niveaux de raffinements.

Distribution : en Beta test sur la plate-forme Rodin

Les outils Brama vont être mis à disposition en Beta test. Ils sont utilisables à partir de la plate forme de modélisation Open Source Rodin.
Un convertisseur permet de transformer les modèles B existants au format de cette plate forme.

Perspectives

L'interface d'animation de modèles est à améliorer. L'outil Brama est pour l'instant surtout utilisé pour réaliser des animations graphiques de modèles existants.