BRAMA: a New Graphic Animation Tool for B Models

Clearsy - 2007 B Conference

Introduction

Clearsy is an engineering company specialized in system dependability.

It verifies the concepts and tools required to create secure systems and uses formal techniques to define, design and validate systems, then create critical software for their integration.

The principal formal tools used by Clearsy to create, refine and prove models are the *Atelier B and B4free*, and *CompoSys* to create formal system models and related documentation.

Based on our various experiments using formal tools in an industrial setting and our desire to disseminate formal methods, we have imagined a new approach to present models to our customers. The Brama tool supports this approach.

The objective of this document is to explain the approach and related Brama tool.

Context: the Need to Validate Models

Method B is often used in industrial settings to create proven secure software in the context of SIL 4 level certification pursuant to the 61508 standard.
It has now been used for a few years to model systems.
This new practice has revealed a deficiency.
When you want to specify a system, you need to:

- Know what you want
- Ensure the feasibility of what you want.

Modeling and proof activities reveal specification issues. This is the very point of modeling. An advantage of the B method is it is based on mathematics and therefore allows for specifications to be written with unparalleled precision.
However, we discovered that, when faced with a model, our customers, and in general those who did not write the model, have difficulty in understanding it, on the one hand, and, on the other, have difficulty in affirming that the model represents the system.
The completeness and quality of the model are therefore problematic.

Translation of Models into Natural Language

A first response to the issue of B model comprehension was provided by Clearsy with its offer of the CompoSys tool, allowing the modeler to prepare model documentation at the same time as the model. This allows the user to automatically produce a model translation, with various graphic views of dependencies between the different system components. The documentation in natural language is an accurate reflection of the model and may be read “easily” by all to ensure the model matches the system.

Animation to "Test" Models

The Brama model animation tool provides a further response as it may be used by the modeler throughout the modeling process. The animation functions allow him to “create” various model events, filters and properties; he can "test" the model.

Graphic Visualization of the System

A third means consists in using the model to graphically view the system in specific operational contexts.

This approach consists in offering the model’s author tools that allow for:

- The representation by graphic drawings and animations of the system and its different types of states
- “Linking” these drawings and animations to different events and B model B variables
- Representation by buttons of the various interactions of the elements external to the system and re-actualization of the system’s graphic representation in accordance with these interactions.

The model is therefore not shown to the client. The system’s graphic representation is presented, as it is based on the B model itself.

More Details on the Brama Tool

The modeler creates B models with Atelier B, B4free or the Rodin platform, then uses the Brama animation tool that in turn uses these models.

Brama was designed to communicate with Flash tools configured with a communication extension that is delivered with Brama.

The modeler’s task consists in representing his system with the Flash tools and configuring scripts that allow for communication with the Brama animation engine.

When the user is satisfied, Brama lets him export the finished animation in the form of files which, once saved on a CD, will launch the graphic animation without prior installation and on any PC using Windows or Linux.

Brama is presented as an Eclipse plug-in suite and Flash extension that can be used with Windows and Linux.
Brama contains the following principal modules: BtoRodin: an animation engine (predicate solver), event and B variable visualization tools, an automatic event linkage management module, a variable management module, observed predicates and expressions, and a Flash communication module.

Examples and Feedback

The first examples were developed on the basis of experimental models: mechanical press, island/continent road traffic, locks, switches, verification of Ariane’s nozzles.
The work on these samples demonstrated the deficiencies present in the analyzed models and confirmed the value of visualizing the system to better ensure model reliability.
This graphic representation work is not burdensome: approximately one week to perfect the animation of a model created over two months. The largest model represents 450 events and 17 refinement levels.

Distribution: in Beta Test on the Rodin Platform

Brama tools will be made available in Beta test. They can be used from the Open Source Rodin modeling platform.
A converter allows for the transformation of existing B models to this platform's format.

The Future

The model animation interface requires improvement. For the time being, the Brama tool is used most often to create graphic animations for existing models.