THESE

présentée par

Thomas BOLUSSET

pour obtenir le grade de

DOCTEUR DE L'UNIVERSITE DE SAVOIE

(Arrêté ministériel du 30 mars 1992)

Spécialité :

Informatique

β-SPACE : Raffinement de descriptions architecturales en machines abstraites de la méthode formelle B

Soutenue publiquement le 30 septembre 2004, devant le jury composé de :

M. Alain HAURAT	Président du jury	Professeur à l'Université de Savoie
M. Jean-Jacques CHABRIER	Rapporteur	Professeur à l'Université de Bourgogne
M. François JACQUENET	Rapporteur	Professeur à l'Univesité Jean Monnet
M. Noureddine BELKHATIR	Examinateur	Professeur à l'Université de Grenoble II
M. Flavio OQUENDO	Directeur de thèse	Professeur à l'Université de Savoie

Thèse préparée au sein du Laboratoire d'Informatique, Systèmes, Traitement de l'Information et de la Connaissance – Ecole Supérieure d'Ingénieurs d'Annecy (ESIA) – Université de Savoie.

ABSTRACT

β-SPACE: Refinement of architectural descriptions into abstract machines of the B formal method

A software architecture describes its structure and behaviour in terms of components and connectors. Nevertheless, the architecture description languages do not support the complete development of complex software systems, from architectural design to the executable code. On the other hand, some formal development methods permit to refine a software specification in order to obtain another one closer to the implementation, or even to generate code, but without taking into account the system architectural description.

We propose, in this thesis, to use a refinement mechanism to transform the architectural description into a "classical" formal specification, which is already supported by tools allowing the development achievement.

The research problem that we are treating is the refinement of a software architecture description in π-SPACE, a software architecture description language based on a process algebra, towards an abstract specification, formed by abstract machines of the B method, which is supported by tools to help the formal development and the code generation.

We develop a formal system – named β-SPACE – to bring successive refinements into operation, leading from the starting architectural description (in π-SPACE) to a formal specification (a set of abstract machines of the B method) such as to make a formal development of the application possible, in the B method framework, while guaranteeing that each refinement step preserves the initial architectural description properties.

The formal definition of the software architecture refinement is based on the rewriting logic, in which the abstract architectural elements are represented, but the constructs of the target specification language too. This logic is also supported by a development and execution tool which permits to automate the transformations.

Our approach of the architectural refinement differs from the other existing methods, by being interested not only in the addition of details to the formal description, but also in the transformation of its control structure: the composition of components and connectors in the architecture is transformed to obtain a hierarchy of B abstract machines. This requires to change the way to control actions inside these different descriptions of the same system: from concurrent behaviours of components and connectors, synchronized by communications, to hierarchically organized abstract machines, related together by operation calls. However, we ensure the conservation of the interesting architectural properties.

This is an original approach both concerning its architectural range (structure but also behaviour), its formalisation and its connection with the classical formal methods.

Keywords: Software Engineering, Formal Refinement, Software Architecture, Formal Method.