

Prise en compte de la validation dans l'ingénierie des exigences

29 mars 2021

Directrice de thèse : Jeanine Souquières

Equipe MOSEL-VERIDIS au LORIA (Ecole doctorale IAEM)

Contexte scientifique

Les méthodes formelles et l'introduction de modèles abstraits aident à maîtriser le développement et la complexité d'un système. La validation de ces modèles est une question cruciale pour la correction du logiciel final et tout au long de son développement. Pour de tels modèles abstraits, une approche raisonnable est de valider la partie limitée de l'espace correspond à la partie intéressante du modèle. Nos travaux récents nous conduisent à trois questions relativement à la validation :

- L'élicitation et formalisation des exigences du client. Les études de cas montrent le potentiel des outils tels que ProR utilisable sous la plateforme Rodin (<http://www.eventb.org>) pour lier exigences, modèles formels et raffinement [5, 2, 6, 7].
- L'introduction progressive des propriétés formelles dans une façon ordonnée, les niveaux d'observation guidant le raffinement.
- Les outils qui permettent d'exécuter les modèles abstraits durant le développement. Avec l'outil JeB [8], il est possible d'observer le comportement des modèles.

L'évolution du modèle lors de son raffinement prend en compte la dynamique du développement de la spécification. Le raffinement formel, tel que défini en B-événementiel permet de vérifier la spécification à chaque étape de son développement [1]. Il est ainsi possible d'assurer que le travail avance vers une solution sûre en prouvant les relations entre les états successifs du modèle. L'ambition de ce travail est d'offrir une telle assurance quant à la validité des modèles successifs [4, 5, 3]. Le principe de base est d'identifier une forme d'incrément de couverture des besoins, grâce notamment à la gestion des liens entre besoins et éléments du modèle formel, et de valider par rapport à cet incrément.

Sujet de thèse

Ce sujet s'inscrit dans la continuité directe des travaux cités ci-dessus en détectant les erreurs dans les exigences, et dans les modèles formels via les raffinements. Il concerne l'étude

de la validation dès les premières étapes du développement de systèmes complexes pour obtenir des systèmes de confiance. Quelques pistes du travail de thèse concernent :

- Apport des invariants et théorèmes à la validation.
- Extraction des éléments de validation et leur automatisation.
- Mémorisation et gestion de l'historique de la validation.
- Retours de la vérification relativement aux exigences.

La plateforme Rodin (<http://www.event-b.org>) sera mise à jour.

Connaissances et compétences requises

Le sujet se situe à la croisée de la définition des méthodes formelles et des outils pragmatiques. Pour cela, il convient de maîtriser les concepts mathématiques permettant d'utiliser efficacement les langages de spécifications formels tels B ou B-événementiel. La connaissance des outils comme Rodin (<http://www.event-b.org>) ou, plus généralement, les outils d'assistance à la preuve, serait appréciable.

Le travail se déroule dans le département *Méthodes Formelles* du LORIA.

Références

- [1] Jean-Raymond Abrial. *Modeling in Event-B : System and Software Engineering*. Cambridge University Press, 2010.
- [2] Fahad R. Golra, Fabien Dagnat, Jeanine Souquières, Imen Sayar, and Sylvain Guerin. Bridging the Gap between Informal Requirements and Formal Specifications Using Model Federation. In *SEFM 2018 International Conference on Software Engineering and Formal Methods, Toulouse, France*, pages 44–69, 2018.
- [3] Jean-Pierre Jacquot and Atif Mashkoor. The Role of Validation in Refinement-Based Formal Software Development. In Atif Mashkoor, Qing Wang, and Bernhard Thalheim, editors, *Models : Concepts, Theory, Logic, Reasoning and Semantics - Essays Dedicated to Klaus-Dieter Schewe on the Occasion of his 60th Birthday*, pages 202–219, 2018.
- [4] Atif Mashkoor, Faqing Yang, and Jean-Pierre Jacquot. Refinement-based Validation of Event-B Specifications. *Software and Systems Modeling*, 16(3) :789–808, 2017.
- [5] Imen Sayar and Jeanine Souquières. La validation dans les premières étapes du processus de développement. *Revue ISI-DAT, numéro spécial Décisions, argumentation et tracabilité dans l'Ingénierie des Systèmes d'Information*, 22(4) :11–41, 2017.
- [6] Imen Sayar and Jeanine Souquières. Bridging the Gap Between Requirements Document and Formal Specifications using Development Patterns. In *IEEE 27th International Requirements Engineering Conference Workshops (REW)*, pages 116–122, 2019.
- [7] Imen Sayar and Jeanine Souquières. Formalization of Requirements for Correct Systems. In *IEEE CPS, FORMalREquirements@RE'2020*, 2020.
- [8] Faqing Yang, Jean-Pierre Jacquot, and Jeanine Souquières. Proving the Fidelity of Simulations of Event-B Models. In *15th International IEEE Symposium on High-Assurance Systems Engineering, Miami Beach, FL, USA, January 9-11*, pages 89–96, 2014.