Développement formel des Systèmes Complexes

Composante
École Nationale Supérieure d'Électrotechnique d'Électronique d'Informatique d'Hydraulique et des Télécommunications

En bref

- **Code Ametys:** N9EN12B
- **Ouvert aux étudiants en échange:** Oui

Présentation

Objectifs

Cet enseignement aborde la modélisation formelle de systèmes, avec pour but la preuve formelle de leur correction. L'emphase est mise sur l'utilisation des systèmes états-transitions ainsi que la théorie des ensembles et la logique du premier ordre afin de capturer les comportements et les propriétés potentiellement complexes de ces systèmes. La preuve par induction est abordée, pour établir la correction des systèmes au regard de propriétés de sûreté (safety). L'opération de raffinement est centrale ici, car permettant de décomposer la complexité du système et des preuves, et de concevoir des systèmes graduellement, d'une manière qui est correcte par construction, en préservant donc au niveau n+1 les propriétés établies au niveau n. Enfin, le lien est fait entre la conception formelle et la formalisation d'information de domaine à l'aide de théorie algébriques. Ces dernières sont utilisées par les modèles décrits dans le but d'introduire de nouveaux types.

Ces notions abstraites sont concrétisées au travers de l'utilisation de la méthode Event-B et de son outillage, la plateforme Rodin, qui permettent de mettre en pratique la théorie formelle de conception des systèmes tout au long de l'unité d'enseignement. L'UE est par ailleurs ponctuée par un projet substanciel de conception d'un système inspiré de ce que l'on trouve dans l'industrie, réalisé en équipe de 4 à 5.

Pré-requis obligatoires

logique, preuve par induction, systèmes formels, systèmes de transitions, langages formels et compilation,

Bibliographie

[1] J.-F. Monin, Introduction aux méthodes formelles, Hermès, 2000.

[2] J.-R. Abrial, The B-book : Assigning Programs to Meanings, Cambridge University Press, 1996.

[3] J.-R. Abrial, Modelling in Event-B: System and Software design, Cambridge University Press, 1996

[4] T. Hoare, Communicating Sequential Processes, Prentice Hall International, 1985.

[5] Jean-Raymond Abrial, Michael Butler, Stefan Hallerstede, Thai Son Hoang, Farhad Mehta and Laurent Voisin}, Rodin: an open toolset for modelling and reasoning in {Event-B}}, STTT journal, Vol 12, Num 6, Pages 447-466, 2010

[6] T. Hoare., An axiomatic basis for computer programming, Communications of the ACM, 12, pp. 576-583, October 1969.

[6] Floyd, R.W., Assigning meanings to programs', in Schwartz, J.T. (ed.), Mathematical Aspects of Computer Science, Proceedings of Symposia in Applied Mathematics 19 (American Mathematical Society), Providence, pp. 19-32, 1967

[7] Dijkstra, E.W., Guarded commands, non-determinacy and formal derivation of programs, Commun. ACM 18, 1975

[8] Dijkstra, E.W., A Discipline of Programming, Prentice-Hall, 1976.

[9] The Rodin platform Wiki, https://wiki.event-b.org/index.php/Main_Page