



La thèse

"Etude des architectures de sécurité de systèmes autonomes : formalisation et évaluation en Event-B"

sera soutenue par Jean-Charles Chaudemar le 27 janvier 2012 à 10h00 à la salle des thèses de l'ISAE-Campus SUPAERO devant le jury composé de:

- M. Yamine Aït-Ameur, Professeur, IRIT et ENSEEIHT (rapporteur)
- M. Eric Bensana, Ingénieur de recherches, ONERA (co-directeur de thèse)
- Mme. Régine Laleau, Professeure, LACL et Université Paris-Est Créteil (examinatrice)
- M. Dominique Méry, Professeur, LORIA et Université Henri Poincaré Nancy 1 (rapporteur)
- Mme. Marielle Petit-Doche, Ingénieure, SYSTEREL (examinatrice)
- Mme. Christel Seguin, Ingénieure de recherches, ONERA (co-directrice de thèse)

Résumé de la thèse :

Etude des architectures de sécurité de systèmes autonomes : formalisation et évaluation en Event-B

La recherche de la sûreté de fonctionnement des systèmes complexes impose une démarche de conception rigoureuse. Les travaux de cette thèse s'inscrivent dans le cadre la modélisation formelle des systèmes de contrôle autonomes tolérants aux fautes. Le premier objectif a été de proposer une formalisation d'une architecture générique en couches fonctionnelles qui couvre toutes les activités essentielles du système de contrôle et qui intègre des mécanismes de sécurité. Le second objectif a été de fournir une méthode et des outils pour évaluer qualitativement les exigences de sécurité.

Le cadre formel de modélisation et d'évaluation repose sur le formalisme Event-B. La modélisation Event-B proposée tire son originalité d'une prise en compte par raffinements successifs des échanges et des relations entre les couches de l'architecture étudiée. Par ailleurs, les exigences de sécurité sont spécifiées à l'aide d'invariants et de théorèmes. Le respect de ces exigences dépend de propriétés intrinsèques au système décrites sous forme d'axiomes. Les preuves que le principe d'architecture proposé satisfait bien les exigences de sécurité attendue ont été réalisées avec les outils de preuve de la plateforme Rodin.

L'ensemble des propriétés fonctionnelles et des propriétés relatives aux mécanismes de tolérance aux fautes, ainsi modélisées en Event-B, renforce la pertinence de la modélisation adoptée pour une analyse de sécurité. Cette approche est par la suite mise en œuvre sur un cas d'étude d'un drone ONERA.

Mots clés : méthode formelle, Event-B, raffinement, architectures tolérantes aux fautes, sécurité

Abstract:

Model based safety of FDIR architectures for autonomous systems: formal specification and assessment with Event-B

The study of complex system safety requires a rigorous design process. The context of this work is the formal modeling of fault tolerant autonomous control systems. The first objective has been to provide a formal specification of a generic layered architecture that covers all the main activities of control system and implement safety mechanisms. The second objective has been to provide tools and a method to qualitatively assess safety requirements.

The formal framework of modeling and assessment relies on Event-B formalism. The proposed Event-B modeling is original because it takes into account exchanges and relations between architecture layers by means of refinement. Safety requirements are first specified with invariants and theorems. The meeting of these requirements depends on intrinsic properties described with axioms. The proofs that the concept of the proposed architecture meets the specified safety requirements were discharged with the proof tools of the Rodin platform. All the functional properties and the properties relating to fault tolerant mechanisms improve the relevance of the adopted Event-B modeling for safety analysis. Then, this approach is implemented on a study case of ONERA UAV.

Keywords: formal method, Event-B, refinement, fault tolerant architectures, safety, dependability