Analyse de sécurité de systèmes autonomes

Formalisation et évaluation en Event-B

Jean-Charles Chaudemar* — **Eric Bensana**** — **Christel Seguin****

* *ISAE-DMIA*
10 av. Edouard Belin, Toulouse, France
jean-charles.chaudemar@isae.fr

** *ONERA-DCSD*
2 av. Edouard Belin, Toulouse, France
{eric.bensana, christel.seguin}@onera.fr

RÉSUMÉ. *Cet article vise à décrire une architecture de sécurité de systèmes autonomes à l'aide de la méthode formelle Event-B. Le formalisme Event-B supporte une conception rigoureuse de ces systèmes. La technique de raffinement permet une modélisation progressive en vérifiant la correction et la pertinence des modèles par décharge de preuves. L'application de la méthode Event-B présente un intérêt dans la formalisation des relations entre couches qui assurent la cohérence d'un fonctionnement sûr ainsi que le respect des exigences de sécurité concernées par notre analyse. Par conséquent, la modélisation autour de ces relations fait apparaître en permanence un comportement nominal associé à des comportements en présence de fautes sous l'hypothèse d'une architecture intégrant des mécanismes de tolérance aux fautes.*

ABSTRACT. *This paper aims at describing safety architectures of autonomous systems by using Event-B formal method. The Event-B formalism well supports the rigorous design of this kind of systems. Refinement mechanism allows a progressive modelling by checking the correctness and the relevance of the models by discharging proof obligations. The application of the Event-B method is interesting in the formalisation of relations between layers which enable the safe functional consistency and the achievement of dependable requirements concerned by this analysis. Therefore, the modelling involving these relations emphasizes a nominal behaviour associated with faulty behaviours in assuming a fault-tolerant architecture.*

MOTS-CLÉS : *sécurité, architectures tolérantes aux fautes, Event-B, raffinement.*

KEYWORDS: *dependability, fault tolerant architectures, Event-B, refinement.*