Vers la génération de modèles de sûreté de fonctionnement

Xavier Dumas*, Claire Pagetti*, Laurent Sagaspe*, Pierre Bieber*, Philippe Dhaussy**

*ONERA-CERT - 2 av. E. Belin 31055 Toulouse
nom@cert.fr
http://www.cert.fr/
**ENSIETA - DTN - 2 rue F. Verny 29806 Brest
dhaussy@ensieta.fr
http://www.ensieta.fr/dtn/index.php

Résumé. La conception et le développement de systèmes embarqués critiques sont assujettis à la fois à des objectifs économiques mais également au respect des normes de sécurité. Dès lors, la qualité des analyses de sûreté de fonctionnement et des interactions entre les experts de sûreté de fonctionnement et les équipes de développement est primordiale. Partant du constat que les échanges entre ces équipes ne sont pas encore suffisamment automatisés, nous proposons des techniques de génération automatique de modèles de sûreté de fonctionnement à partir de spécifications exprimées sous forme de modèle. L'algorithme générique proposé a été implanté par un code de transformation de modèles AADL en AltaRica et une expérimentation a été réalisée sur une spécification d'un asservissement de gouverne avionique.

Summary

The development of highly critical embedded systems is accompanied with careful safety analyses. These analyses are performed on a *safety model* which is often constructed *by hand*. The purpose of the paper is to propose a first step in the development of a unified toolbox for specifying, modeling and analysing a system. Assuming that the specifications are written in a model, for instance an AADL model, then we describe an algorithm that generates the safety model in a formal language called AltaRica. This algorithm has been partially implemented in the KerMeta framework.