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.

1 Introduction

Contexte. La conception et le développement de systèmes embarqués critiques sont assujettis à la fois à des objectifs économiques, telle la réduction des coûts et du temps de développement, mais également au respect des normes de sécurité. Dans le contexte aéronautique, par exemple, ces contraintes sont amplifiées puisque le processus de développement doit répondre à une certaine fiabilité pour passer l'étape de certification. De ce fait, le cycle de développement est soumis à davantage de validation et de vérification ainsi qu'à une plus grande traçabilité. Dès lors, les activités d'évaluation liées à la *sûreté de fonctionnement* [1], où l'on établit le niveau de confiance justifié qu'il est possible d'attribuer à un système lorsqu'il est utilisé correctement, occupent une place prépondérante. Une représentation schématique d'un cycle de développement d'un système critique est donnée dans la figure 1. Ce cycle est le résultat de l'imbrication d'un cycle de développement que l'on pourrait qualifier de *classique* et d'un cycle de sûreté de fonctionnement.

La première étape est l'analyse des besoins qui permet ensuite de définir les grandes fonctionnalités attendues du système. Ces fonctions de haut niveau sont étudiées d'un point de

[1] Pour rappel, selon [Laprie (1989)], la sûreté de fonctionnement englobe outre la sécurité innocuité -non occurrence de défaillance à caractère catastrophique -, la disponibilité, la maintenabilité, la fiabilité, l'intégrité et la confidentialité.