Sûreté de fonctionnement des systèmes critiques
Diagnostic et tolérance aux fautes
Ecole Centrale de Lille – Jeudi 25 octobre 2012

Diagnostic pour la commande sûre des systèmes embarqués critiques

Armand TOGUYENI
Professeur des Universités, Ecole Centrale de Lille/LAGIS
Cité Scientifique, 59651 Villeneuve d'Ascq, 03-20-33-54-49, armand.toguyeni@ec-lille.fr

Key-words: *critical embedded systems, modular diagnosability, diagnose, timed automata*

Year after year, the manufacturings of important volumes of numerical circuits' integrating more and more transistors with high integration and reduced costs have induced the development of embedded systems. Despite their many advantages, embedded systems are rarely used to control critical systems. This is due to industrial safety standards which compel manufacturers to use proven technologies such as those relay-based controls. It is in this context that we are participating in the project FerroCOTS. This project aims to design embedded systems for control and monitoring rolling systems in railways. The idea developed is the design of fault-tolerant architecture based on both active redundancy and fault diagnosis. We propose a diagnosis approach based on the technique of the diagnoser and the concept of diagnosability. The difficulty with this technique is the combinatorial explosion caused by the large number of inputs / outputs of such type of embedded systems.
We propose a methodology based on the modular diagnosability to avoid the combinatorial explosion of our models.

Mots clés : *systèmes embarqués critiques, diagnosticabilité modulaire, diagnostiqueur, automates temporisés*

La fabrication de plus en plus importante des circuits intégrés à forte intégration en transistors et la baisse de leurs coûts permet de les utiliser pour la mise en œuvre des systèmes embarqués. Malgré leurs nombreux avantages, les systèmes embarqués restent peu utiliser pour le contrôle des systèmes critiques. Cela est dû aux normes de sécurité industrielle qui contraignent les industriels à utiliser des technologies éprouvées comme celle basée sur les commandes à relais. C'est dans ce contexte que nous participons au projet FerroCOTS. Ce projet a pour objectif la conception de systèmes embarqués pour le contrôle-commande des systèmes roulants ferroviaires. L'idée développée est la conception d'architecture tolérantes aux fautes basées à la fois sur de la redondance active et sur diagnostic en lignes des fautes du système. Nous proposons une approche de diagnostic basée sur la technique du diagnostiqueur et le concept de la diagnosticabilité. La difficulté liée à cette technique est l'explosion combinatoire causée par le nombre important d'entrées/sorties de systèmes embarqués. Nous proposons une méthodologie basée sur la diagnosticabilité modulaire pour combattre l'explosion combinatoire de nos modèles.