Ordonnanceur vérifié pour un générateur de code automatique qualifiable

Nassima Izerrouken[†‡] — **Marc Pantel**[†] — **Xavier Thirioux** [†]

[†] *Laboratoire IRIT Site ENSEEIHT- UMR CNRS 5505*
2 Rue Charles Camichel, BP 7122 Toulouse Cedex
nom.prenom@enseeiht.fr

[‡] *Continental Automotive, Toulouse, France*

RÉSUMÉ. *Cette contribution présente une expérience d'utilisation d'une approche à base de méthodes formelles pour la conception et la vérification de certains composants d'un générateur automatique de code séquentiel impératif (du code C pour l'instant) qualifiable pour les systèmes embarqués critiques. Le générateur de code accepte un sous ensemble du langage de modélisation* SIMULINK*/Stateflow et produit du langage C. Nos travaux se situent dans le cadre du projet européen ITEA GeneAuto. Nous présentons l'ordonnanceur de blocs Simulink spécifié, développé et vérifié, en utilisant l'assistant de preuves Coq. Une implantation correcte par construction a été extraite et intégrée dans la chaîne des composants du générateur de code. L'ordonnanceur vérifié a été expérimenté pour des modèles industriels réels et fait partie de l'outil open source actuellement disponible.*

ABSTRACT. *This paper relies on a formal approach to the design of a correct by-construction code generator for embedded systems, within the GeneAuto project. We present a machine-checked scheduler of the code generator. We present a verified scheduler for critical embedded code generator using proof assistant Coq. A correct executable Caml scheduler was automatically extracted from the specification of the scheduler, integrated as a certified part into the code generator GeneAuto and applied to industrial models.*

MOTS-CLÉS : *Générateur de code, vérification formelle, Simulink, ordonnancement de circuits, assistant de preuve Coq*

KEYWORDS: *Code generator, formal verification, validation, circuit scheduling, theorem proving Coq*