Master thesis defense on 3 February 2016 at 10.00 (Riskan)


Respondent: Joakim Gustafsson
Opponent: Adam Lundström

Abstract:

The complexity of electrical and electronic automotive systems have increased steadily over the previous decades, with modern vehicles containing as many as 50-70 Electronic Control Units, and several CAN-communication networks. In order to address the increasing complexity of these safety-critical embedded systems, safety standards such as ISO 26262 are making their way to the market, posing strong restrictions on the development process of automotive systems in order to ensure safety. With current automotive actors possessing large existing source code bases for their ECUs, primarily written in the C programming language, the demands posed on software architectural models by ISO 26262 are proving to be a challenge to meet given the difficulties of modelling low-level languages such as C.

This thesis aims to survey currently existing modelling formalisms with regards to their ability to model automotive embedded C source code in a way that ensures ISO 26262 compliance. A delimitation is made to the use of the MISRA-C:1998 subset of the C programming language, a safer subset commonly used in automotive industry. A short ontology is proposed, coupled with a metric for evaluating the completeness of a modelling formalism. Requirements are posed on suitable modelling formalisms, and AADL, Lustre, SysML and Promela are identified as promising candidates for modelling embedded C code. Semantic constructions present in the C language are identified, and a mapping between these constructions and semantic constructions present in the selected modelling formalisms is made and analyzed using the completeness evaluation framework that was proposed. Architectural Description Languages (ADL), such as AADL, are identified as being the most promising with regards to modelling embedded C code. Control Flow Graphs are identified as a promising augmentation to ADLs in order to deal with their lack of control flow semantics.