**Statement regarding Nesredin Mahmud’s Ph.D. thesis titled ‘‘﻿Design of Assured and Efficient Safety-critical Embedded Systems”**

Nesredin Mahmud’s thesis deals with a timely and important topic both from the industrial and research perspectives that is, proposing solutions, supported by a sound method and a prototype implementation, for the specification and analysis of embedded systems requirements, formal large-scale Simulink analysis, and software-to-hardware mapping optimization in a distributed architecture.

The research in the thesis is conducted via a series of steps that rely on established research methods, such as identifying an overall research goal, formulating the research goals deemed to address the overall goal, proposing a design approach that considers assurance and resource by which answers to the research goals can be given, implementing the proposed solution, and validating and evaluating the implemented solution by using automotive use cases and benchmark. The research of the thesis pushes further the existing research safety-critical embedded software design by applying formal techniques at multiple levels of system development and optimization of power consumption of a distributed system. The thesis provides novel techniques based on logic-based reasoning (i.e., Boolean satisfiability, ontology) to formally analyze constrained natural language requirements, statistical model checking of large-scale Simulink models, and integer-linear programming model of software-to-hardware mapping which considers timing and reliability constraints, and formulation of the latter as metaheuristic problem (i.e., hybrid particle swarm optimization) to support large-scale software allocations. The prposed solution is validated on the brake-by-wire and adjustable speed limiter (ASL) automotive systems from Volvo Group Trucks Technology (VGTT), and engine management system benchmark from Bosch

The work focuses on a very difficult topic and the research results are of high quality. The main thesis results are: ﻿(i) a constrained requirements specifications language of embedded systems, *ReSA*; (ii) a formal analysis of ReSA specifications via SMT and Ontology; (iii) a statistical model checking of a software design, modeled in Simulink, via transformation to a network of stochastic timed automata; (iv) an integrated allocation of fault-tolerant software with end-to-end timing and reliability constraints via integer integer-linear programming and hybrid particle-swarm optimization. The results are found in the published work, which has targeted relevant real-time systems venues.

All the phases that make the thesis defendable are in place: crisply formulated research questions, a well-defined research methodology, well-presented and justified research results (mentioned above) as well as a comprehensive presentation of the limitations and validation of the research results, and comparison with related work.

In conclusion, I firmly state that the thesis is ready to be printed and publicly defended.

Sincerely,

Antonio Cicchetti

Associate Professor at Mälardalen University,

School of Innovation, Design, and Engineering, Västerås, Sweden.

Phone: ???

Email: antonio.cicchetti@mdh.se