Correct by Design Methodology for the Control of Safety-Critical Complex Reactive Systems

by

A. C. Vidanapathirana

This thesis was submitted to the Department Electrical & Electronic Engineering of the University of Peradeniya in partial fulfilment of the requirements for the Degree of Doctor of Philosophy

Research Supervised

by

Dr. S.D. Dewasurendra

Dr. S.G. Abeyratne

University of Peradeniya

Peradeniya, Sri Lanka

January 2019

Abstract

The objective of this thesis was to develop formal verification strategies suitable for model-based design of Complex Reactive Systems (CRS). Typical real scale CRS like automotive, power, avionic, rail transport and manufacturing systems require design techniques that facilitate continuous verification and validation of control software/hardware in their life cycles, which pose complex challenges due to their inherent complexity arising from concurrency, distribution, communication, rapid response, hybrid dynamics, hierarchy, modularity etc.

Since structurally flat models like Finite State Machines (FSMs) do not scale up well for representing real scale CRS we selected semantically rich statecharts to specify discrete event control.

Statecharts permit simulation from early stages of the design. Since simulation cannot guarantee correct behaviour, *formal* verification becomes necessary, and mandatory in some cases. However, the complex semantics of statecharts do not permit direct formal verification.

This led us to develop strategies for semantics preserving translation of statecharts into flat modules communicating through ports, to compositionally verify supervised and unsupervised discrete dynamics.

This thesis contributes through the incorporation of modular supervisory control, reconfigurabilty, redundancy and finally, integration of hybrid dynamics, to facilitate compositional formal verification, testing and runtime validation of Complex Hybrid Systems (CHS).

Verification and integration of modular non-blocking supervisory control have been automated. The verified controller models are then seamlessly translated automatically to executable software code and implemented in PLC (Telemechanique) and FPGA (Xilinx) hardware platforms with minimum debugging.

To capture errors at various integration levels, MiL and HiL testing was carried out. Continuous Variable dynamics were integrated and the formal verification strategy was elevated to Complex Hybrid Systems. Unlike in the traditional approach, testing was integrated with the formal verification.

Then safety invariants were defined for the CHS and differential dynamic logic was used to elevate verification logic to the hybrid dynamics. A runtime validation strategy was developed for capturing any un-modelled system behaviour.

To validate formal verification theories for this class of systems a prototype laboratory test-bed was built in the laboratory to perform research on CRS at various levels of system integration. All the theories developed in this thesis were implemented and tested on this test-bed.