The University Of Sheffield.

Automatic Control and Systems Engineering

The Department of Automatic Control & Systems Engineering
is pleased to announce the following seminar:

Verification of FMI Cosimulations

Dr Frank Zeyda
Department of Computer Science
University of York, UK

Wednesday, 29 November 2017 at 14:00
LT02, Sir Henry Stephenson Building

Abstract

Cosimulation techniques are popular in the design and testing of cyber-physical systems. Such systems are typically composed of heterogeneous components and specified using a variety of languages and tools that adopt complementary modelling paradigms. The industrial standard FMI (Functional Mock-up Interface) has been developed to address challenges of coupling different simulators and simulations. It defines an API used to implement master algorithms that mitigates issues of interoperability.

Whereas simulation is currently the predominant approach to analyse CPS, such cannot provide universal guarantees of correctness and safety. This is due to the complexity of CPS in considering continuous behaviours as well as real-world interactions, and the impracticality of running an exhaustive number of simulation test scenarios. Moreover, simulations depend on parameters and algorithms, and are software systems (with possible faults) in their own right.

To overcome the above issues, this talk will present a verification technique for FMI cosimulations that was developed as part of the INTO-CPS project (http://projects.au.dk/into-cps/). Our technique captures the FMI paradigm in its purest form, and shows how Hoare logic and refinement can be employed to verify universal properties of cosimulations. As part of this, we present both an abstract and concrete model of FMI, using a state-rich reactive language (Circus). The technique will be illustrated by way of an example from railways, provided by our INTO-CPS industrial partners. All theories have been mechanised in Isabelle/UTP - a proof system that we developed for Hoare and He's "Unifying Theories of Programming" framework.

Biography

Dr Zeyda completed his PhD in 2007, investigating the application of the B Method for formal software development to reversible computations. From 2007-2014, he worked as an RA at the University of York (UK) on two EPSRC projects, that targetted the development of novel (refinement-based) verification techniques both for Simulink control systems and Safety-Critical Java (SCJ). After lecturing for two years at Teesside University (UK), he rejoined York in Nov. 2016 to work on the INTO-CPS EC project (http://projects.au.dk/into-cps/); his interest therein was the development and application of novel verification techniques for cosimulations of cyber-physical systems, also considering industrial case studies.

His research focus and expertise is in both theoretical foundations, considering the mathematical underpinning of languages used to describe various kinds of software systems, as well as practical applications that involve verification strategies and the use of theorem provers such as Isabelle/HOL to rigorously apply and automate them.

Light refreshments will be served in the foyer of
the Sir Henry Stephenson Building