



The
University
Of
Sheffield.

Automatic
Control and
Systems
Engineering

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

Can Java Ever Be Safe?

Professor Ana Cavalcanti
Department of Computer Science
University of York

Wednesday 16th April 2014 at 14:00
LT01, Sir Frederick Mappin Building

Abstract

Safety-Critical Java (SCJ) is a novel version of Java that addresses issues related to real-time programming and certification of safety-critical applications. We present a technique that reveals the issues involved in the formal verification of an SCJ program, and provides guidelines for tackling them in a refinement-based approach. It is based on Circus, a combination of well-established notations: Z, CSP, Timed CSP, and object orientation. We cater for the specification of timing requirements and their decomposition towards the structure of missions and event handlers of SCJ. We also consider the integrated refinement of value-based specifications into class-based designs using SCJ scoped memory areas. We present a refinement strategy and a Circus variant that captures the essence of the SCJ paradigm.

Biography

Ana Cavalcanti is a Professor on Software Verification at the University of York (UoY) and a Royal Society - Wolfson Research Merit Award holder. In 2003, she was awarded a Royal Society Industry Fellowship to work with QinetiQ on formal methods. She has published more than 100 papers, and chaired the Programme Committee of various well-established international conferences. Her main research interest is the theory and practice of formal methods. She has a long-term interest in refinement and tools. She played a major role in the design and formalisation of a state-rich process algebra and its development and verification techniques.

(www-users.cs.york.ac.uk/~alcc).

*Refreshments will be available following the talk in the
Foyer of the Sir Henry Stephenson Building*