NATIONAL UNIVERSITY OF SINGAPORE

School of Computing

CS SEMINAR

Title:	**Model-Checking at Scale: Design space exploration of the next generation air traffic control system**
Speaker:	Dr Marco Gario Fondazione Bruno Kessler Italy
Date/Time:	13 May 2016, Friday, 03:00 PM to 04:00 PM
Venue:	SR7, COM1-02-07
Chaired by:	Dr Lee Jooyong, Senior Research Fellow, School of Computing (leejy@comp.nus.edu.sg)

Abstract:

In the early stages of design, there are often many competing candidate solutions that differ in the assumptions and implementations of the components in use. Deciding which solution to adopt requires considering several trade-offs. Model checking represents a possible way of comparing such designs, however, it faces major challenges. For a large number of designs, building and validating so many models may be intractable.

During our collaboration with NASA, we faced the challenge of considering a design space with more than 20,000 designs for the NextGen air traffic control system. To deal with this problem, we introduce a compositional, modular, parameterized approach combining model checking with contract-based design to automatically generate large numbers of models from a possible set of components and their implementations. Our approach is fully automated, enabling the generation and validation of all target designs. The 1,620 designs that were most relevant to NASA were analyzed exhaustively. To deal with the massive amount of data generated, we apply novel data-analysis techniques, that enable a rich comparison of the designs, including safety aspects. Our results were validated by NASA system designers, and helped to identify novel as well as known problematic configurations.

Biodata:

Marco Gario is a researcher at Fondazione Bruno Kessler (Italy). Marco obtained his PhD in Computer Science at University of Trento, working on Formal Methods for the design of Fault Detection components (FD). In particular, Marco introduced a formalism for the specification, validation, verification and synthesis of FD that is powered by an underlying

Temporal Epistemic Logic formalism. Marco was involved in projects from both ESA and NASA, aimed at applying formal methods to industrial problems.