

NATIONAL UNIVERSITY OF SINGAPORE

School of Computing

C S S E M I N A R

Title: A Correct-by-construction system recovery model

Speaker: Professor Yamine AIT-AMEUR,
IRIT/INPT-ENSEEIH

Date/Time: 11 March 2016, Friday, 10:30 AM to 12:00 PM

Venue: SR3, COM1-02-12

Chaired by: Dr Dong Jin Song, Associate Professor, School of Computing
(dongjs@comp.nus.edu.sg)

Abstract:

The substitution of a system by another one occurs in several cases like adaptation, failures, resilience, reconfiguration, self-healing, etc. System substitution consists in replacing a running system by another one when a given condition holds. In this talk, we present a generic formal model for system substitution.

In our approach, a system is defined as being a transition system. Each state is characterised by a set of variables and transitions denote state changes. We consider that each system refines a global specification (another system). A set of systems, namely substitute systems, can be associated to a global specification. By system substitution, we mean the capability of a system to be replaced by another system, each of these two systems refine the same global specification. Preserving the properties of the original system is a key point to be addressed during substitution.

In this talk, we present a stepwise formal approach for system substitution. Substitute systems are formalised by Event-B machines, which refine a shared Event-B machine defining the global specification. State recovery is performed when a failure in the running system occurs. In that case, modes are changed and control is transferred to the selected substitute system. The transfer of the control shall 1) preserve safety of the properties expressed as invariants in the Event-B model and 2) identify the recovery state in the substitute system. Proof obligations associated to this substitution operation are defined. They guarantee invariant preservation. We show how different substitution modes are handled: equivalent degraded or upgraded. Finally, specific case studies of system substitutions are discussed.

Biodata:

Yamine AIT AMEUR is Full Professor since 2000 at ENSEEIHT (Ecole Nationale Supérieure d'Electronique, Electrotechnique, Informatique, Hydraulique et Telecommunications) in Toulouse (France). Previously he was at ENSMA (National School of Mechanics and Aeronautics) in Poitiers (France) between 2002 and 2011, and he has been the head of LISI/ENSMA (Laboratory of Industrial and scientific computer science at ENSMA). He got his HDR (Habilitation to conduct research) in 2000, and his PhD in Computer Science in 1992 at ENSAE-SUPAERO.

His Research topics concern: i) Formal methods for validation and verification, ii) Ontology based modeling and ontology based databases, iii) Application domains: embedded systems, interactive systems, semantic web, PDM databases, etc. Two main important aspects characterize his research activities. On the one hand the fundamental aspects through the use of formal modeling techniques based on refinement and proof, explicit formalization of semantics using formal ontology models. On the other, hand, practical aspects, through the development of operational applications, allowing to validate the proposed approaches. Embedded systems in avionics, engineering, interactive systems, CO2 capture are some of the application domains targeted by this work.