A Proof and Refinement based Development for Cyber-Physical Systems

.....

Overview

Cyber-physical systems (CPS) are dependable critical systems that refer to the tight integration and coordination between computational and physical resources, which fuel many industrial sectors like aerospace, railway, medical, nuclear and automotive domains. The growing demand for CPS increases vulnerabilities that could lead to devastating system failures. Such a failure can result in injuries or loss of life, including reputation and economical damage. Design errors are a major source of the defects that are introduced during the system development process. Traditional validation and verification techniques such as simulation and testing are effective methods for detecting these defects, but are seriously limited in that they cannot guarantee to find all existing defects. Formal methods provide a complementary alternative to testing and simulation, and, although we do not yet have a 'theory of coverage' when combining formal validation and verification techniques with testing and simulation, the combination provides better coverage than any one of them on its own.

This course provides the necessary background in formal methods, including specifying, designing and implementing complex CPS. We introduce Event-B modeling language and refinement principle. The refinement allows modeling a system gradually by introducing safety properties at various refinement levels. Rodin is an integrated development environment (IDE) for Event-B modeling language based on Eclipse. It supports project management, stepwise model development, proof assistance, model checking, animation and automatic code generation.

In the lectures, we will discuss modeling techniques (discrete and continuous), refinement and proofs, model checking, code generation and several complex examples. In the tutorials, we will provide introduction of the Rodin Platform and other associated tools and instructions for solving exercises. The given course material provides scientific basis for modeling complex systems using a correct by construction and may help to meet the certification standards by providing proof evidences. Moreover, it will meet industrial requirements to tackle current challenges for designing large complex critical systems safer and secure.

Objectives

The main objectives of the course are as follows:

- Introduce fundamental discrete and continuous modeling concepts for CPS using refinement.
- Introduce domain modeling and system modeling for designing and verifying closed-loop systems.
- Formal verification & validation, simulation and implementation for building prototypes.
- Exposure of several complex case studies from different domains.

Modules	**June 20 – July 01, 2022 (except Saturday & Sunday) covering 24 hours lectures and 18 hours tutorials.**
You Should Attend If…	• Executives, engineers and researchers from software industries, service and government organizations including R&D laboratories. • Student students at all levels (BTech/MSc/MTech/PhD) or Faculty from reputed academic institutions and technical institutions.
Fees	The participation fees for taking the course is as follows: **Participants from abroad : USD 200** **Industry/Research Organizations: INR 4,500** **Faculty from Academic Institutions: INR 2,500** **Indian Students: INR 1,500** The course will be conducted in online mode.

The Faculty

Dr. Neeraj Kumar Singh is an Associate Professor in computer science at INPT-ENSEEIHT and member of the ACADIE team at IRIT. Before joining INPT, Dr. Singh worked as a research fellow and team leader at the Centre for Software Certification (McSCert), McMaster University, Canada. He worked as a research associate in the Department of Computer Science at University of York, UK. He also worked as a research scientist at the INRIA Nancy Grand Est Centre, France, where he received his PhD in computer science. He leads his research in the area of theory and practice of rigorous software engineering and formal methods to design and implementation of safe, secure and dependable critical systems. He is an active participant in the "Pacemaker Grand Challenge". He is the author of a book "Using Event-B for Critical Device Software Systems" published by Springer. His main research interests include formal methods, refinement and proof, software certification, requirement analysis, code generation, domain engineering, hybrid systems, human machine interface, etc.

Dr. Raju Halder currently working as an Assistant Professor in the Dept. of Comp. Sc. and Engg. at IIT Patna since 2012. Dr. Halder did his PhD in Computer Science from Ca' Foscari University of Venice (Italy) in 2012, and received B.Sc., B.Tech. and M.Tech. Degrees from University of Calcutta in the years 2002, 2005 and 2007 respectively. Before joining IIT Patna, he served as a post doctoral researcher with Macquarie University, Australia. He worked with the Robotics team at HASLab (University of Minho), Portugal, in 2016. Prior to his PhD, he had also worked as an associate system engineer with IBM India Pvt. Ltd. during 2007-2008. His areas of research interests include Formal Methods, Blockchain and Smart Contract, Program Analysis and Verification, Information Systems Security, etc.

Course Co-ordinator

Dr. Raju Halder
Phone: +91 612 3028009
E-mail: halder@iitp.ac.in
https://www.iitp.ac.in/~halder

Detailed Course Plan

Day	Session	Topic
20 June 2022 (Monday)		Inauguration
	Lecture-1	Motivation; Propositional Calculus; First order predicate calculus; Event-B modeling language
	Lecture-2	Continue Event-B modeling language; Set Theory; Relation and functions
	Tutorial-1	An introduction to the Rodin Platform; Simple examples from different domains (thermostat, lift and bank transactions etc.)
21 June 2022 (Tuesday)	Lecture-3	System modeling; Machine, Context, Witness, Invariant, Variant, Theorems and Proofs
	Lecture-4	Natural Deduction; Sequent Calculus; Backward and Forward reasoning; Proof strategies
	Tutorial-2	Case studies on Cardiac Pacemaker (1-electrode and 2-electrodes)
22 June 2022 (Wednesday)	Lecture-5	Refinement in Event-B; Proof Obligations; Proof Structure
	Lecture-6	Development process; Simulation and co-simulation; Animation and ProB model checker
	Tutorial-3	The Automatic Rover Protection; Landing Gear System
23 June 2022 (Thursday)	Lecture-7	Requirement Analysis; Tabular Expressions; Completeness and Disjointness; Automatic Refinement
	Lecture-8	Stateflow to Tabular Expressions; Transformation rules
	Tutorial-4	Development of Insulin Infusion Pump (IIP) using Tabular Expression
24 June 2022 (Friday)	Lecture-9	Environment Modeling; Heart model; Glucose Homeostasis model (GHM)
	Lecture-10	Explicit Implicit Modeling; Model refactoring
	Tutorial-5	Closed-loop modeling of heart and pacemaker
27 June 2022 (Monday)	Lecture-11	Continuous and Discrete Modeling in Event-B; Theories in Event-B; Modeling ODE in Event-B
	Lecture-12	Generic refinement for continuous system; Controller modelling
	Tutorial-6	Automatic Brake and Signalized Left-Turn Assist (SLTA)
28 June 2022 (Tuesday)	Lecture-13	Code Generation; Certifying code generation process
	Lecture-14	Verifying medical protocol: Electrocardiogram (ECG)
	Tutorial-7	Introduction of EB2ALL code generator; Case studies: Cardiac Pacemaker and Multisite pacing devices
29 June 2022 (Wednesday)	Lecture-15	Model Checking; Computational Tree Logic (CTL); Linear Temporal Logic (LTL)

	Lecture-16	Applications of LTL and CTL; Verification Algorithms; SAT and SMT solvers
	Tutorial-8	Demonstration of NuSMV and Uppaal model checker using suitable examples
30 June 2022 (Thursday)	Lecture-17	Static analysis, Abstract Interpretation: Galois Connection, Fix-point Abstractions, Widening and Narrowing
	Lecture-18	Deductive Vs. Model-based verification, Model abstraction and counterexample guided refinement
	Tutorial-9	Case study on the verification of temporal properties of ROS-based Kobuki Robot
01 July 2022 (Friday)	Lecture-19	Testing and Test Cases Generation, Possible Research Directions
		Course Assessment Test and Certificate Distribution

* NS: Dr. Neeraj Singh, RH: Dr. Raju Halder