DEPARTMENT OF ELECTRICAL & COMPUTER ENGINEERING
The University of Auckland

COMPSYS705 Formal Methods for Engineers – Formal Methods for Medical Device Validation

COURSE OUTLINE & REQUIREMENTS — 2017

Partha Roop

Staff

Dr Partha Roop
Room: Building 903, Room 258, EMAIL: p.roop@auckland.ac.nz
Responsibilities: *Course coordinator, Course Lecturer*

Dr. Avinash Malik
Room: Building 1.401, Room —, EMAIL: avinash.malik@auckland.ac.nz
Responsibilities: *Course Lecturer*

Questions about the lecture material should be directed to the lecturer concerned. General problems and questions about the course should be directed to the course coordinator. Please approach the TA for any programming assignment / verification related questions. The TA for 2017 is yet to be decided.

Course Details

This is a inter-disciplinary course inspired by software engineering and formal methods. However, this course has been adapted for applicability for computer systems engineering, mechatronics, bio-engineering and medical devices domains. Executable biology refers to executable computational models that mimic biological processes. In this course we will present a range of executable models inspired by formal methods especially for medical device validation. The range of formal methods considered here include a synchronous Statechart called SCChart for pacemaker modelling, a tool called Uppaal for pacemaker verification and a tool called Piha for the design of the cardiac conduction system, which will be validated using the SPIN model checker.

Our research group (http://pretzel.ece.auckland.ac.nz/bio) has proposed a refinement for real-time executable biology, where human organs can be transformed into executable models such that these models can operate in real-time with medical devices. The main motivation for such models is that they can be used for the validation of medical devices in a closed-loop without using live human organs. This has significant implications in medicine, biology, computer science, and also biomedical engineering. There are obvious implications for educational software related to this approach.

Globally, medical device validation using formal methods is a exciting research area involving many medical device companies and leading institutes such as Oxford university (see: EU funded project http://qav.cs.ox.ac.uk/projects/veripace/) and many leading US universities funded by the National Science Foundation (See: https://cybercardia.cs.stonybrook.edu). You may also get a glimpse of our research on these topics by watching this video of the heart on chip at: http://pretzel.ece.auckland.ac.nz/bio.

Learning Goals

The learning goals for this course are as follows:

- To understand the need for mathematical modelling of complex, software intensive control systems.
- To apply the concepts learned to design and verify a realistic system.
- Comprehensive understanding of the models for biological systems such as the electrical conduction system of the human heart.
- Creating an awareness of the major challenges in the design of such systems, in particular the issues related to the cyber-physical nature of such systems.
- The use of formal methods and synchronous programming languages in the design of cyber-physical systems.
- Providing practical exposure to current design and research challenges of CPS, particularly related to executable biology.
- Provide an inter-disciplinary focus where computer systems engineers, software engineers, cardiac physicians, bio-engineers and electrical engineers can cooperatively learn topics of immense interest for the design and verification of safety-critical systems used in medicine.

Course Details

The course is taught in two parts:

Part 1-*Fundamentals of model-based design founded on formal methods.*

- Automatic verification of *closed* and *open* systems using *model* checking and *module* checking.
- Modelling and verification of a pacemaker using UPPAAL.
- Run-time verification and enforcement of medical devices.
- Formal modelling and verification using *process algebras* and *bisimulation.*
- Introduction to Cyber-Physical Systems (CPS).

Part 2-*Industrial successes of formal methods*

- Model of the cardiac conduction system.
- Explicit state model-checkers: primarily the SPIN model-checker will be covered.
- SPIN for verification of industrial scale safety critical software.
- The Boolean satisfiability problem – SAT and related solving algorithms.
- Case study of the cardiac conduction system and the associated verification.

Assessment

The coursework component of this course is 100% consisting of two assignments. :

Component	Weighting	When
Assignment1	50%	Monday, Week 8
Assignment2	50%	Friday, Week 12

Schedule

Formal lectures will be held twice a week in weeks 1-12. After this, we will have consultation hours for discussions on the projects. Some more lectures may be scheduled when needed.

Academic Integrity

The University of Auckland will not tolerate cheating or assisting others to cheat, and views cheating in course work as a serious offense.The work that a student submits for grading must be the student's own work, reflecting his or her learning. Where work from other sources is used, it must be properly acknowledged and referenced. This requirement also applies to sources on the world-wide web. A student's assessed work may be reviewed against electronic source material using computerized detection mechanisms. Upon reasonable request, students may be required to provide an electronic version of their work for computerized review.

References

1. Fisher, Jasmin, and Thomas A. Henzinger. "Executable cell biology." Nature biotechnology 25.11 (2007): 1239-1249.
2. Z. Jiang, M. Pajic, S. Moarref, R. Alur, and R. Mangharam. Modeling and verification of a dual chamber implantable pacemaker. In TACAS, pages 188203. Springer, 2012.
3. Allen, Nathan, et al. "Modular code generation for emulating the electrical conduction system of the human heart." Proceedings of the 2016 Conference on Design, Automation & Test in Europe. EDA Consortium, 2016.
4. Yip, E., Andalam, S., Roop, P. S., Malik, A., Trew, M., Ai, W., & Patel, N. (2016). Towards the Emulation of the Cardiac Conduction System for Pacemaker Testing. arXiv preprint arXiv:1603.05315.
5. R. Sinha, P. S. Roop and S. Basu,
   Correct-by-construction SoC Design, Springer, 2013.
   [Chapter 3 from this book is available from the library as an e-resource - recommended reading].
6. E. M. Clarke, O. Grumberg and D. Peled, *Model Checking*, MIT Press, 2000.
   [Available in the library - recommended reading]
7. D. A. Peled, *Software Reliability Methods*, Springer Verlag, 2001.
8. C. Kern and M. R. Greenstreet, *Formal Verification in Hardware Design: A Survey*, ACM Transactions on Design Automation of Electronic Systems, Vol. 4, No. 2, April 1999.
   [recommended reading]

Further Information

Further information will be posted using Canvas.