Abstraction, Refinement and Decomposition for Systems Engineering

Michael Butler
University of Southampton, United Kingdom

These lectures will address the key role played by formal modelling and verification in systems engineering. Modelling may be used at all stages of the development process from requirements analysis to system acceptance testing. Formal modelling and verification lead to deeper understanding and higher consistency of specification and design than informal or semi-formal methods. In order to manage system complexity, abstraction, refinement and decomposition of formal models are key methods for structuring the formal modelling effort since they support separation of concerns and layered reasoning. A refinement approach means that models and compositions of models represent different abstraction levels of system design; consistency between abstraction levels is ensured by formal verification.

The lectures will use the Event-B formal modelling language and the associated Rodin toolset for Event-B. Event-B is a state-based formal method for system-level modelling and analysis. The key features of Event-B are the use of set theory as a modelling notation, the use of refinement to represent systems at different abstraction levels and the use of mathematical proof to verify the consistency between refinement levels. The Rodin Platform is an Eclipse-based IDE for Event-B that provides effective support for refinement and mathematical proof. The platform is open source, contributes to the Eclipse framework and is further extendable with plugins.

The lectures will be structured as follows:

- System abstraction and model refinement
- Role of proof and tools in Event-B modelling
- Structuring refinement
- Decomposing models
- Implementing models

Relevant case studies will be used to exemplify the techniques.

References

[1] J.-R. Abrial. *Modeling in Event-B: System and Software Engineering*. Cambridge University Press; 2012.

[2] J.-R. Abrial, M. Butler, S. Hallerstede, T.S. Hoang, F. Mehta, L. Voisin. *Rodin: An Open Toolset for Modelling and Reasoning in Event-B*. International Journal on Software Tools for Technology Transfer (STTT); Vol. 12(6); pp. 447-466; 2010. `http://eprints.soton.ac.uk/271058/`

[3] M. Butler. *Decomposition Structures for Event-B*. In: Integrated Formal Methods iFM2009; LNCS 5423; Springer; 2009. `http://eprints.soton.ac.uk/266965/`

[4] M. Butler, D. Yadav. *An Incremental Development of the Mondex System in Event-B*. Formal Aspects of Computing; Vol. 20(1); pp. 61-77; 2008. `http://eprints.soton.ac.uk/263346/`

[5] A. Edmunds, A. Rezazadeh, M. Butler. *Formal Modelling for Ada Implementations: Tasking Event-B*. In: Ada-Europe 2012: 17th International Conference on Reliable Software Technologies, Stockholm, SE; pp. 11-15; 2012. *http://eprints.soton.ac.uk/335400/*