Event-B: from RODIN to DEPLOY

Jean-Raymond Abrial, David Basin, Thai Son Hoang, Matthias Schnalz
Chair of Information Security, Department of Computer Science, ETH Zürich, Switzerland

Event-B

Event-B is a formal method for developing discrete transition systems that are correct by construction. An important technique is refinement.

Applications:
- Embedded systems: mechanical press controller
- Concurrent systems: Simpson's 4-slot algorithm
- Sequential programs: traversing a linked list
- Distributed systems: leader election algorithms
- Parallel systems: digital circuits
- Large-scale systems in a possibly hostile environment: railway systems

Contributions

Our main contribution is the Event-B modeling method and the Rodin platform. Important properties:
- Event-B as a formal method for modeling transition systems via refinement
- The underlying logic is a restricted version of classical set theory.
- Systematic treatment of partiality
- Carefully designed notation leads to simple proofs.
- Event-B is applicable to various problem domains.
- The Rodin platform supports incremental development.
- The Rodin platform is free, open-source, and extensible.
- Various case studies have been developed using the Rodin platform.

Some Challenges

- Identify domain-specific challenges through case studies with SAP and Bosch.
- Define formal patterns to facilitate reuse of models and proofs.
- Reuse generic models by instantiation.
- Incorporate decomposition of models for compositional reasoning and reuse.
- How to reuse, instantiate, and extend logical theories in a practical way?
- Improve existing automatic theorem provers and integrate decision procedures.
- Incorporate probabilistic choices.
- Find methodologies for modeling security.

Past Collaborators

- Melanie Hallende (post-doc)
- Farhad Mehta (master student)
- Francois Terrier (PhD student)
- Laurent Veani (chief architect of the Rodin platform)

Selected Publications

7. After extending Event-B with probabilistic choice, it is still possible to prove convergence properties without referring to complicated probabilistic theory. S. Hallende and T. S. Hoang. Qualitative probabilistic modelling in Event-B. In iCFP, volume 4594 of LNCs, pages 291-312, 2007.

Best Paper Award