Event-B: from RODIN to DEPLOY

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

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

Rodin deploy

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: reversing a linked list
- Distributed systems: leader election algorithms
- Parallel systems: digital circuits
- Large systems in a possibly hostile environment: railway systems

RODIN Project (09/2004–08/2007)

- European sixth framework programme
- Specific targeted research project
- Full title: rigorous open development environment for complex systems
- Partners: University of Newcastle, Abo Akademi, ClearSy, Nokia, Praxis, VTEC, ETH Zurich, University of Southampton
- Objectives: create a methodology and supporting open tool platform for the cost effective rigorous development of dependable complex software system and services.
- ETHZ's task: develop a core tool platform for Event-B.

DEPLOY Project (01/2008–12/2011)

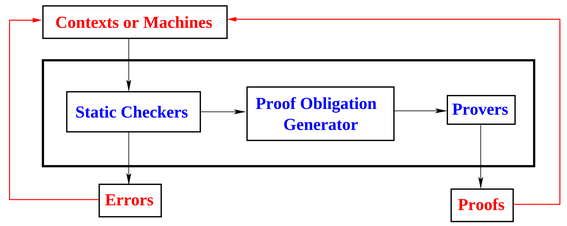
- European seventh framework programme
- Large scale integrated project
- Full title: industrial deployment of advanced system engineering methods for high productivity and dependability
- Industrial partners: Bosch, SAP, Siemens, Space Systems Finland
- Academic partners: University of Newcastle, Abo Akademi, CETIC, ClearSy, ETH Zurich, University of Düsseldorf, Systerel, University of Southampton
- Objectives: make major advances in engineering methods for dependable systems through the deployment of formal engineering methods.
- ETHZ's tasks:
  - Technology transfer to partners
  - Industrial case studies
  - Integration of decision procedure
  - Research on a methodology for security
  - Contribute to development and maintenance of tools.

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.

Development Process within the Rodin Platform



Example: Finding Maximum

Specification

maximum
begin
$m := max(ran(f))$
end

- Input $f \in 1 \mathinner{..} n \rightarrow \mathbb{N}$ is an array of numbers.
- Output m is the maximum of the numbers in f.

Refinement

maximum
refines *maximum*
when
$p = q$
then
$m := f(p)$
end

inc
when
$p < q$
$f(p) \leq f(q)$
then
$p := p + 1$
end

dec
when
$p < q$
$f(q) < f(p)$
then
$q := q - 1$
end

Invariants

invariants:
$p \in 1 \mathinner{..} n$
$q \in 1 \mathinner{..} n$
$p \leq q$
$max(ran(f)) \in f[p \mathinner{..} q]$

Simulation Proof Obligation

$\ldots$
$max(ran(f)) \in f[p \mathinner{..} q]$
$p = q$
$\vdash$
$max(ran(f)) = f(p)$

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 choice.
- Find methodologies for modeling security.

Past Collaborators

- Stefan Hallerstede (post-doc)
- Farhad Mehta (PhD student)
- Francois Terrier (master student)
- Laurent Voisin (chief architect of the Rodin platform)

Selected Publications

1. The Event-B book:
   J.-R. Abrial. *Modeling in Event-B: System and Software Design*. Cambridge University Press. To appear in early 2009.
2. Development of a semi-reactive system – topology discovery – in Event-B.
   T. S. Hoang, H. Kuruma, D. Basin and J.-R. Abrial. Developing Topology Discovery in Event-B. To appear in *iFM* 2009.
3. Systematic treatment of partiality: A model is well-defined only if a partial function is never evaluated outside of its domain.
   F. Mehta. A practical approach to partiality - a proof based approach. In *ICFEM*, volume 5256 of *LNCS*, pages 238–257, 2008.
4. About patterns:
   J.-R. Abrial and T. S. Hoang. Using design patterns in formal methods: An Event-B approach. In *ICTAC*, volume 5160 of *LNCS*, pages 1–2, 2008.
5. Refinement, decomposition, and instantiation in Event-B:
   J.-R. Abrial and S. Hallerstede. Refinement, decomposition, and instantiation of discrete models: Application to Event-B. *Fundamenta Informaticae*, 77(1-2):1–28, 2007.
6. How reactive (incremental) development is supported within Rodin:
   F. Mehta. Supporting proof in a reactive development environment. In *SEFM*, pages 103–112. IEEE Computer Society, 2007.
7. After extending Event-B with probabilistic choice, it is still possible to prove convergence properties without referring to complicated probabilistic theory.
   S. Hallerstede and T. S. Hoang. Qualitative probabilistic modelling in Event-B. In *iFM*, volume 4591 of *LNCS*, pages 293–312, 2007.
   Best Paper Award
8. The Event-B notation has been carefully designed to be simple, easily teachable and suitable for a modelling tool.
   S. Hallerstede. Justifications for the Event-B modelling notation. In *B*, volume 4355 of *LNCS*, pages 49–63, 2007.
9. An introduction to the Rodin platform:
   J.-R. Abrial, M. J. Butler, S. Hallerstede, and L. Voisin. An open extensible tool environment for Event-B. In *ICFEM*, volume 4260 of *LNCS*, pages 588–605, 2006.
10. An investigation of the interplay between probabilistic theory and Event-B:
    C. Morgan, T. S. Hoang, and J.-R. Abrial. The challenge of probabilistic Event-B. In *ZB*, volume 3455 of *LNCS*, pages 162–171, 2005.