HATS:
Highly Adaptable & Trustworthy Software Using Formal Models

— Report from the Coordinator —

Reiner Hähnle
Technical University of Darmstadt, Germany

Third Annual HATS Project Meeting
Oslo 5–7 September 2011

December 3, 2012

http://www.hats-project.eu
Project Status

PM12
PM24
PM36
PM48

Project started 1 March 2009, all participants are active as planned

Ca. 70 people involved in HATS (according to hats-all), 48 here

Funding for 3rd period received 30 Jun 2011, 27% of EC contribution

Transferred to all participants 10 Aug 2011

Extension with IoC Tallinn 75PM from 1 May 2010
Project Status

PM12 PM24 PM36 PM48

Elapsed Time

R. Hähnle
Project Status

PM12  PM24  PM36  PM48

Elapsed Time

Received Funding  5,27 M€

Project started 1 March 2009, all participants are active as planned
Ca. 70 people involved in HATS (according to hats-all), 48 here
Funding for 3rd period received 30 Jun 2011, 27% of EC contribution
Transferred to all participants 10 Aug 2011
Extension with IoC Tallinn 75PM from 1 May 2010
PM12  PM24  PM36  PM48

Elapsed Time

Received Funding  5,27 M€

Spent Resources  (estimation based on first 24 PM)
Project started 1 March 2009, all participants are active as planned
- Ca. 70 people involved in HATS (according to hats-all), 48 here
- Funding for 3rd period received 30 Jun 2011, 27% of EC contribution
- Transferred to all participants 10 Aug 2011
Project Status

Elapsed Time

Received Funding 5,27 M€

Spent Resources (estimation based on first 24 PM)

- Project started 1 March 2009, all participants are active as planned
- Ca. 70 people involved in HATS (according to hats-all), 48 here
- Funding for 3rd period received 30 Jun 2011, 27% of EC contribution
- Transferred to all participants 10 Aug 2011
- Extension with IoC Tallinn 75PM from 1 May 2010
Mind the Gap!

- Design-oriented, architectural, structural
  UML, FDL, etc.

- Implementation level
  JML, SPEC#, etc.

- Minimalistic foundational
  $\pi$-calculus, ambient c., etc.
Mind the Gap!

Design-oriented, architectural, structural
UML, FDL, etc.

+ executability

Abstract Behavioural Specification
ABS

+ verifiability
  Implementation level
  JML, SPEC#, etc.

+ usability
  Minimalistic foundational
  $\pi$-calculus, ambient c., etc.
What We Deliver

A tool-supported formal method for building highly adaptable and trustworthy software

Main ingredients

1. Executable, formal modeling language for adaptable software: Abstract Behavioral Specification (ABS) language
2. Tool suite for ABS/executable code analysis & development:
   Analytic functional/behavioral verification, resource analysis, feature consistency, RAC, types, TCG, visualization
   Generative code generation, model mining, monitor inlining, ...
3. Develop methods in tandem with ABS to ensure scalability
4. Methodological and technological framework integrating HATS tool architecture and ABS language
Vision: A Single-Source Technology for Highly Adaptive, Concurrent Software Systems

- Sequence diagram
- Object diagram
- Architectural language
- UML class diagram
- Feature description language
- Bytecode
- Maude
- Erlang
- Petri net
- Scala
Important Project Principles (I)

Ensuring relevance

- Thorough requirements analysis; continuous (industrial) evaluation
- Apply to empirically highly successful development method: Software product line engineering (PLE)
Important Project Principles (II)

Feasibility: ensure that analysis methods scale up

Develop analysis methods in tandem with ABS language

- Incrementality
  - Delta modeling, delta specification, delta verification

- Compositionality
  - Concurrency model
  - Proof systems
Early evaluation

- Developed Core ABS first
### Important Project Principles (III)

**Early evaluation**
- Developed Core ABS first
- Layered language design

<table>
<thead>
<tr>
<th>Product Selection (PSL)</th>
<th>Delta Modeling (DML)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature Model ($\mu$TVL)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Product Line Configuration (CL)</th>
<th>Behavioral Interface Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assertion Language</td>
<td>Core Creol</td>
</tr>
<tr>
<td>Composition (COGs)</td>
<td></td>
</tr>
<tr>
<td>Object Model</td>
<td>Pure Functional Language</td>
</tr>
<tr>
<td></td>
<td>ADT</td>
</tr>
</tbody>
</table>

R. Hähnle
HATS Report from the Coordinator 110905 7 / 25
Important Project Principles (III)

Early evaluation
- Developed Core ABS first
- Layered language design
- Provide tools early

Diagram:
- Core AST
  - Name Resolution
    - Resolved AST
      - Type Checker
        - Type-Checked AST
          - Maude Back End
            - Maude Files
              - Maude VM
          - Java Back End
            - Java Files
              - Java VM
          - Core ABS code gen.
            - Core ABS Files
              - Core ABS VM

R. Hähnle

HATS Report from the Coordinator
The Main Innovations of HATS

A formal, executable, abstract, behavioral modeling language

- Cutting-edge research on modeling of concurrent, OO systems
- Combines state-of-art in verification, concurrency, specification, and programming languages communities
- Adaptability drives the design

Scalable technologies developed in tandem with ABS

- Incremental, compositional
- Analytic as well as generative technologies

Formalization of PLE-based development as main application

- Leveraging formal methods tools to PLE
- Define FM-based development methodology for PLE
Work Organisation in HATS

WP5: Validation

WP4: Trustworthiness
cross-cutting qualities

WP2: Variability
anticipated change

WP3: Evolvability
unanticipated change

WP1: Framework
language design, methodology, tool infrastructure, integration

modeling

analysis
PM 30: Research Objectives and Main Results

Full ABS Framework  Feature and platform models, behavioral interfaces
  ▶ Micro Textual Variability Language
  ▶ Delta Modeling Language
  ▶ Product Line Configuration Language
  ▶ Product Selection Language

Core ABS Tool Suite  Parser, type checker, editors, simulator
  ▶ Fully integrated into Eclipse
  ▶ Java code generation

Milestone M2, Deliverable 1.2, Task 1.2

Feature Integration  Relation of feature and behavioral models
  ▶ Product composition by delta modeling

Milestone M2, Deliverable 2.2b, Task 2.2

Modeling Evolvability  Investigate dimensions/forms of evolution
  ▶ Architectural component model

Milestone M2, Deliverable 3.1b, Task 3.1
Further Second Year Objectives & Results

**Scalable Verification**
- Compositional/incremental verification
  - Compositional behavioral verification
  - Compositional program logic
  - Deadlock analysis

  Deliverable 2.5, Task 2.4, 2.5

**Bytecode Evolvability**
- Monitor inlining, code generation
  - Security monitors for concurrent ABS

  Deliverable 3.4, Task 3.4

**Resource Guarantees**
- Estimation/verification of resource bounds
  - Runtime estimates of concurrent ABS

  Deliverable 4.2, Task 4.2

**Evaluate Core ABS**
- Expressiveness, usability, methodology
  - Three case studies of which one industrial

  Milestone M1, Deliverable 5.2, Task 5.2, 5.3
Second Annual Project Review

Reviewers

- Patrick Heymans, University of Namur
- Marco Roveri, Fondazione Bruno Kessler
- Kaisa Sere, Åbo Academy
- Martin Wirsing, LMU Munich

24th-25th March 2011 in Brussels, EC premisses

- Present:
  Reiner, Einar, Arnd, Jan, Davide, Elvira, Richard, Gilles, Per, Dave, Peter, Bjarte, Dilian, Frank, Karina
- Preparation meeting 23rd March 2011
- Went very well (in particular, tool demo was convincing) …
1. ABS language occupies a very interesting “niche”: links to the more “classical” abstraction levels should be studied and understood
2. Continue the successful development of the HATS tool suite
3. Evaluate roles and relevance of verification properties for PLE: develop systematic approach for the use of verification properties
4. Clarify the advantages and drawbacks of delta programming
5. Continue to take integration between project partners seriously
6. Study the extension of the COSTA framework to adaptable systems
7. Improved quality of the project work appreciated
8. Presentation improvements to deliverables/periodic report

All deliverables in 2nd reporting period (PM13–24) accepted w/o changes!
Active/Upcoming Work Tasks

See also HATS Website “Work Plan|WP Timing & Deliverables”
See also HATS Website “Work Plan|WP Timing & Deliverables”

**WP1: Framework (UKL)**

1.3 CTH, PM 25–42 Analysis

1.4 IoC, PM 25–42 System Derivation and Code Generation

1.5 NR, PM 25–48 Integrated Tool Platform

**WP2: Variability (UIO)**

2.1 UIO, PM 6–35 A configurable deployment architecture

2.3 CTH, PM 18–36 Testing, debugging, and visualization

2.4 BOL, PM 12–36 Types for Variability

2.6 UKL, PM 24–42 Refinement and Abstraction
### Active/Upcoming Work Tasks Cont’d

#### WP3: Evolvability (KTH)

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Team</th>
<th>Duration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2</td>
<td>NR</td>
<td>18–36</td>
<td>Model Mining</td>
</tr>
<tr>
<td>3.3</td>
<td>KUL</td>
<td>24–42</td>
<td>Hybrid Analysis for Evolvability</td>
</tr>
<tr>
<td>3.5</td>
<td>KTH</td>
<td>24–48</td>
<td>Autonomously Evolving Systems</td>
</tr>
</tbody>
</table>

#### WP4: Trustworthiness (UPM)

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Team</th>
<th>Duration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>UPM</td>
<td>12–36</td>
<td>Security</td>
</tr>
<tr>
<td>4.3</td>
<td>BOL</td>
<td>24–48</td>
<td>Correctness</td>
</tr>
<tr>
<td>4.4</td>
<td>FRG</td>
<td>30–42</td>
<td>Auto Configuration and Quality Variability</td>
</tr>
</tbody>
</table>

#### WP5: Validation (FRH)

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Team</th>
<th>Duration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3</td>
<td>CWI</td>
<td>18–36</td>
<td>Evaluation of Modeling</td>
</tr>
</tbody>
</table>

#### WP6: Dissemination (FRG)

<table>
<thead>
<tr>
<th>Team</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FRG</td>
<td>Dissemination, Exploitation, Training, CA</td>
</tr>
<tr>
<td>BOL</td>
<td>Exploitation</td>
</tr>
<tr>
<td>CTH</td>
<td>CA</td>
</tr>
</tbody>
</table>

R. Hähnle

HATS Report from the Coordinator
Dissemination Efforts

(Discussed in more detail by Karina tomorrow)

Highlights of last 12 months

- Organization of FMSPLE 2010 at SPLC in South Korea
  - Involvement in FMSPLE 2011 at SPLC in Munich
- Organization of a special track at FMCO 2010 in Austria
- Article in IEEE Computer, February 2011
  - Formal Methods in Software Product Line Engineering
- Coordination Action EternalS
  - First deliverables have been produced
- HATS lecture at COST IC0701 Summer School
- HATS tutorial at ECOOP’11, Lancaster, UK
- Meeting with Ericsson, Gothenburg
## Past Deliverables

<table>
<thead>
<tr>
<th>Del. No.</th>
<th>Deliverable name</th>
<th>WP No.</th>
<th>Lead Beneficiary</th>
<th>PMs</th>
<th>Type</th>
<th>Dissemination level</th>
<th>Deliv. date PM</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.2.a</td>
<td>Bi-Annual Management Report</td>
<td>7</td>
<td>CTH</td>
<td>4</td>
<td>R</td>
<td>PU</td>
<td>6, 12, 18, 24, 30</td>
</tr>
<tr>
<td>5.1</td>
<td>Requirements Elicitation</td>
<td>5</td>
<td>FRG</td>
<td>17</td>
<td>R</td>
<td>PU</td>
<td>6</td>
</tr>
<tr>
<td>7.3</td>
<td>Project Quality Plan</td>
<td>7</td>
<td>CTH</td>
<td>1</td>
<td>R</td>
<td>PU</td>
<td>11</td>
</tr>
<tr>
<td>6.4</td>
<td>Dissemination Plan</td>
<td>6</td>
<td>FRG</td>
<td>1</td>
<td>R</td>
<td>PU</td>
<td>11</td>
</tr>
<tr>
<td>4.2</td>
<td>Resource Guarantees</td>
<td>4</td>
<td>UPM</td>
<td>25</td>
<td>R</td>
<td>PU</td>
<td>24</td>
</tr>
<tr>
<td>1.2</td>
<td>Full ABS Modeling Framework</td>
<td>1</td>
<td>KUL</td>
<td>32</td>
<td>R</td>
<td>PU</td>
<td>24</td>
</tr>
<tr>
<td>2.2.b</td>
<td>Final Report on Feature selection and integration</td>
<td>2</td>
<td>CWI</td>
<td>21</td>
<td>R</td>
<td>PU</td>
<td>24</td>
</tr>
<tr>
<td>2.5</td>
<td>Verification of Behavioral Properties</td>
<td>2</td>
<td>CTH</td>
<td>45</td>
<td>R</td>
<td>PU</td>
<td>24</td>
</tr>
<tr>
<td>3.1.b</td>
<td>Final Report on Evolvable Systems</td>
<td>3</td>
<td>UKL</td>
<td>21</td>
<td>R</td>
<td>PU</td>
<td>24</td>
</tr>
<tr>
<td>3.4</td>
<td>Evolvability at Bytecode Level</td>
<td>3</td>
<td>KTH</td>
<td>19</td>
<td>R</td>
<td>PU</td>
<td>24</td>
</tr>
<tr>
<td>6.2</td>
<td>Exploitation strategy</td>
<td>6</td>
<td>FRG</td>
<td>15</td>
<td>R</td>
<td>PU</td>
<td>24</td>
</tr>
</tbody>
</table>
## Upcoming Deliverables (Including IoC Effort)

<table>
<thead>
<tr>
<th>Del. No.</th>
<th>Deliverable name</th>
<th>WP No.</th>
<th>Lead Beneficiary</th>
<th>PMs</th>
<th>Type</th>
<th>Dissemination level</th>
<th>Deliv. date PM</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Configuration Deployment</td>
<td>2</td>
<td>UIO</td>
<td>35</td>
<td>R</td>
<td>PU</td>
<td>35</td>
</tr>
<tr>
<td>2.3</td>
<td>Debugging, Visualisation, and Test Generation</td>
<td>2</td>
<td>CTH</td>
<td>36</td>
<td>R</td>
<td>PU</td>
<td>36</td>
</tr>
<tr>
<td>2.4</td>
<td>Types for Variability</td>
<td>2</td>
<td>BOL</td>
<td>21</td>
<td>R</td>
<td>PU</td>
<td>36</td>
</tr>
<tr>
<td>3.2</td>
<td>Model Mining</td>
<td>3</td>
<td>NR</td>
<td>45</td>
<td>R</td>
<td>PU</td>
<td>36</td>
</tr>
<tr>
<td>4.1</td>
<td>Security</td>
<td>4</td>
<td>UPM</td>
<td>21</td>
<td>R</td>
<td>PU</td>
<td>36</td>
</tr>
<tr>
<td>5.3</td>
<td>Evaluation of Modeling</td>
<td>5</td>
<td>CWI</td>
<td>19</td>
<td>R</td>
<td>PU</td>
<td>36</td>
</tr>
</tbody>
</table>

Careful planning & sufficient deadlines essential
Meetings in the Last 12 Months

WT 3.2, Model mining, 28–29 October 2010, Oslo
  ▶ 6 participants from CTH, KTH, NR, UPM
  ▶ Kick-off meeting

WT 4.1, Security, 8–9 November 2010, Leuven
  ▶ 10 participants from CTH, IMDEA, KTH, NR, IoC, KUL
  ▶ Kick-off meeting

WT 2.3, Testing, debugging and visualization, 16-17 December 2010, Stockholm
  ▶ 9 participants from CTH, FRH, KTH, UPM
  ▶ ABSUnit, Test generation: Learning-based, etc., Visualization
Meetings in the Last 12 Months Cont’d

WT 2.1 and 2.4, 10-11 January 2011, Bologna
▶ 16 participants from BOL, CTH, FRH, UIO, IoC, UPM

WT 4.1 Security Workshop, 12 April, Oslo
▶ 3 participants from IoC, KTH, NR
▶ common platform for reasoning about security in multiagent systems using MCMAS to models ABS COGs

Cluster Meeting I, 5-6 May 2011, Leuven
▶ Kick-off metings: Task 4.3 and 3.3 & ABSUnit meeting

Cluster Meeting II, 18-20 May, 2011 Amsterdam
▶ Kick-off meetings: WT 1.3, 1.4, 1.5 and 2.6
Meetings in the Last 12 Months Cont’d

WT 3.5 Autonomously Evolving Systems, 27 June 2011, Kaiserslautern
- 6 participants from UKL, KTH, FRG
- Kick-Off Meeting

WT 4.3 Formal Specification of ABS, 11–13 July 2011, Bologna
- 12 participants from BOL, CTH, CWI, IoC, UKL
- Developing a specification language for ABS
Scientific Advisory Board (SAB) & End-User Panel (EUP)

Scientific Advisory Board (SAB)

The SAB helps the SC with follow-up of work package activities

- Sophia Drossopoulou, Imperial College London, UK
- Ugo Montanari, University of Pisa, Italy
- Frank van der Linden, Philips Electronics N.V., The Netherlands

End-User Panel (EUP), Confirmed members, to be extended!

Project-external companies interested in the HATS technology

- Gian Luca Cattani, MAPS SpA, Italy
- Dario Avallone, Engineering Ingegneria Informatica, Italy
- Thomas Santen, European Microsoft Innovation Center, Germany
- Andreas Roth, SAP AG, Walldorf, Germany
- James Hunt, aicas GmbH, Karlsruhe, Germany
- Marco Pistore, Fondazione Bruno Kessler, Trento, Italy
- Thomas Walter, DOCOMO Euro-Labs, Munich, Germany
Changes in the Consortium

Coordinator changes employer

From 1 Sep 2011:

▶ Reiner Hähnle moves to TU Darmstadt
  • Richard Bubel (from 1 Oct), Ran Ji (from 1 Nov) follow
  • Wolfgang Ahrendt stays at CTH (mainly involved in T4.3)

▶ Scientific coordination moves also to TUD

▶ TUD becomes new project node
  • Most of CTH’s remaining RTD budget moved to TUD

▶ Project coordination and financial coordination stays at CTH

▶ Amendment has been submitted, but not yet approved
Relation with the Commission

Change of Project Officer

Our new project officer is Roumen Borissov replacing Wide Hogenhout

Date and Place for Review of Third Project Phase (PM25–36)

- Takes place in Tallinn! (before ETAPS)
- Preparation meeting on Wednesday, 21 March 2012
- Review meeting on March 22–23, 2012 (until Friday noon)
- All site leaders and leaders of active WTs must be present
Passed second project review with encouraging feedback
All deliverables of second period approved w/o revision
Work started/on track in all active Work Tasks
Many dedicated WT meetings, good participation
All participants highly motivated
Solid publication record
Good dissemination events (IEEE Computer, ECOOP)
SAB and EUP participate in AMs, 2 of 3 SAB members present
Strong presence in EternalS CA