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

September 2, 2011

http://www.hats-project.eu
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), XX 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

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), XX 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

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), XX 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

R. Hähnle
Project Status

Elapsed Time

Received Funding 5,27 M€

Spent Resources (estimation based on first 24 PM)
Project Status

- 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), XX 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

- **0,37 M€**

( 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), XX 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
π-calculus, ambient c., etc.

Realistic

Abstract

Abstract Behavioural Specification (ABS) provides + executability, + verifiability, and + usability.

Implementation level includes JML, SPEC#, etc., while Minimalistic foundational includes π-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, ...  

   Develop methods in tandem with ABS to ensure scalability

3. 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
- Feature description language
- UML class diagram
- Bytecode
- Maude
- Scala
- Erlang
- Petri net
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
Important Project Principles (III)

Early evaluation

- Develop Core ABS first

Diagram:
- Assertion Language
- Composition (COGs)
  - Concurrency model
  - Core Creol
- Object Model
- Pure Functional Language
  - ADT
Important Project Principles (III)

Early evaluation
- Develop Core ABS first
- Layered language design

---

Behavioral Interface Language

- Assertion Language
- Composition (COGs)
- Concurrency model
- Core Creol
- Object Model

Product Selection (PSL)
- Feature Model ($\mu$TVL)
- Delta Modeling (DML)

Product Line Configuration (CL)
- Pure Functional Language
  - ADT
Important Project Principles (III)

Early evaluation
- Develop 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
# 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
WP5: Validation

WP4: Trustworthiness
cross-cutting qualities

WP2: Variability
anticipated change

WP3: Evolvability
unanticipated change

WP1: Framework
language design, methodology, tool infrastructure, integration
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
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:
- Preparation meeting 23rd March 2011
- Went very well (in particular, tool demo was convincing) …
ABS language occupies a very interesting “niche”. Links to the more “classical” abstraction levels should be studied and understood.

Continue the successful development of the HATS tool suite.

Evaluate roles and relevance of verification properties for PLE. Develop systematic approach for the use of verification properties.

Clarify the advantages and drawbacks of Delta programming.

Continue to take integration between project partners seriously.

Study the extension of the COSTA framework to adaptable systems.

Improved quality of the project work appreciated. Need to ensure a continuous quality of the research in the areas where Ina Schaefer was leading the work.

Presentation improvements to deliverables/periodic report.

All deliverables in second reporting period (PM13–24) accepted w/o changes!
See also HATS Website Work Packages | Organization Schema
Active/Upcoming Work Tasks

See also HATS Website Work Packages|Organization Schema

**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
<table>
<thead>
<tr>
<th>WP3: Evolvability (KTH)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2 NR, PM 18–36 Model Mining</td>
</tr>
<tr>
<td>3.3 KUL, PM 24–42 Hybrid Analysis for Evolvability</td>
</tr>
<tr>
<td>3.5 KTH, PM 24–48 Autonomously Evolving Systems</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WP4: Trustworthiness (UPM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1 UPM, PM 12–36 Security</td>
</tr>
<tr>
<td>4.3 BOL, PM 24–28 Correctness</td>
</tr>
<tr>
<td>4.4 FRG, PM 30–42 Auto Configuration and Quality Variability</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WP5: Validation (FRH)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2 FRH, PM 6–18 Evaluation of Core Framework</td>
</tr>
<tr>
<td>5.3 CWI, PM 18–36 Evaluation of Modeling</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WP6: Dissemination (FRG)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dissemination (FRG), Exploitation (FRG), Training (BOL), CA (CTH)</td>
</tr>
<tr>
<td>R. Hähnle</td>
</tr>
<tr>
<td>HATS Report from the Coordinator</td>
</tr>
<tr>
<td>110905 15 / 25</td>
</tr>
</tbody>
</table>
Dissemination Efforts

(Discussed in more detail by Karina tomorrow)

Highlights of last 12 months

- Organization of FMSPLE 2010 at SPLC in South Korea
- 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
<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</th>
<th>PM</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.2.a</td>
<td>Bi-Annual Mgmt. Report</td>
<td>7</td>
<td>CTH</td>
<td>4</td>
<td>R</td>
<td>PU</td>
<td>6, 12, 18, 24, 30</td>
<td></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>
<td></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>
<td></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>
<td></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>
<td></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>
<td></td>
</tr>
<tr>
<td>2.2.b</td>
<td>Final report on Feature selection integration</td>
<td>2</td>
<td>CWI</td>
<td>21</td>
<td>R</td>
<td>PU</td>
<td>24</td>
<td></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>
<td></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>
<td></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>
<td></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>
<td></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>24</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>24</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>24</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>24</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>24</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>24</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, 08 November 2010, Leuven
- Participants from CTH, IMDEA, KTH, NR, IoC
- 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 meetings: 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

<table>
<thead>
<tr>
<th>Meeting Title</th>
<th>Date</th>
<th>Location</th>
<th>Participants</th>
<th>Agenda</th>
</tr>
</thead>
<tbody>
<tr>
<td>WT 4.3 Meeting on Abstract/Specification Languages</td>
<td>11th July 2011</td>
<td>Bologna</td>
<td>12 participants from BOL, CTH, CWI, IoC, UKL</td>
<td>Developing a specification language for ABS</td>
</tr>
<tr>
<td>WT 3.5 Autonomously Evolving Systems</td>
<td>27 June 2011</td>
<td>Kaiserslautern</td>
<td>6 participants from UKL, KTH, FRG</td>
<td>Kick-Off Meeting</td>
</tr>
<tr>
<td>Integration of $\Delta$s in ABS</td>
<td>25–26 August 2010</td>
<td>Oslo</td>
<td>9 participants from UIO, KUL, CTH, CWI</td>
<td>Representation of $\Delta$-Modeling in Full ABS</td>
</tr>
</tbody>
</table>
### 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 1st of September:

- Reiner Hähnle moves to TU Darmstadt.
- Scientific coordination moves also to TUD
- Project coordination and financial coordination stays at CTH.
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
- Review meeting on March, 2011 (until Friday noon)
- All site leaders and leaders of active WTs must be present
Passed second project review
All deliverables of second period approved
Work started/on track in all active Work Tasks
Many dedicated WT meetings, good participation
All participants highly motivated
Solid publication record
SAB and EUP participate in AM, 2 of 3 SAB members present
Strong presence in EternalS CA