HATS:
Highly Adaptable & Trustworthy Software
Using Formal Models
Report from the Coordinator

Reiner Hähnle
Chalmers University of Technology, Gothenburg, Sweden

Second Annual HATS Project Meeting
Kaiserslautern 6–8 September 2010

September 15, 2010

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

<table>
<thead>
<tr>
<th>PM12</th>
<th>PM24</th>
<th>PM36</th>
<th>PM48</th>
</tr>
</thead>
</table>

- **ElapsedTime**
- **Received Funding**
  - 5.27 M€
  - 0.37 M€
- **Spent Resources** (estimation based on first 12 PM)
- Project started 1 March 2009, all participants are active as planned
- Ca. 70 people involved in HATS (according to hats-all), 39 here
- Funding for 2nd period received 13 Jul 2010, 23% of EC contribution
- Transferred to all participants 16 Aug 2010
- Extension with IoC Tallinn 75PM from 1 May 2010

---

R. Hähnle

HATS Report from the Coordinator
### Project Status

<table>
<thead>
<tr>
<th>PM12</th>
<th>PM24</th>
<th>PM36</th>
<th>PM48</th>
</tr>
</thead>
</table>

#### Elapsed Time

- Project started 1 March 2009, all participants are active as planned
- Ca. 70 people involved in HATS (according to hats-all), 39 here
- Funding for 2nd period received 13 Jul 2010, 23% of EC contribution
- Transferred to all participants 16 Aug 2010
- Extension with IoC Tallinn 75PM from 1 May 2010

---

R. Hähnle
HATS Report from the Coordinator
My project report

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), 39 here

Funding for 2nd period received 13 Jul 2010, 23% of EC contribution

Transferred to all participants 16 Aug 2010

Extension with IoC Tallinn 75PM from 1 May 2010

R. Hähnle
HATS Report from the Coordinator
# Project Status

<table>
<thead>
<tr>
<th>PM12</th>
<th>PM24</th>
<th>PM36</th>
<th>PM48</th>
</tr>
</thead>
</table>

## Elapsed Time

## Received Funding

| 5.27 M€ |

## Spent Resources

(ESTIMATION BASED ON FIRST 12 PM)
Project Status

PM12  PM24  PM36  PM48

Elapsed Time

Received Funding  5,27 M€

Spent Resources (estimation based on first 12 PM)

- Project started 1 March 2009, all participants are active as planned
- Ca. 70 people involved in HATS (according to hats-all), 39 here
- Funding for 2nd period received 13 Jul 2010, 23% of EC contribution
- Transferred to all participants 16 Aug 2010
## Project Status

### Project Started 1 March 2009, all participants are active as planned
- Ca. 70 people involved in HATS (according to hats-all), 39 here
- Funding for 2nd period received 13 Jul 2010, 23% of EC contribution
- Transferred to all participants 16 Aug 2010
- Extension with IoC Tallinn 75PM from 1 May 2010

### Elapsed Time

<table>
<thead>
<tr>
<th>PM12</th>
<th>PM24</th>
<th>PM36</th>
<th>PM48</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Received Funding
- 5,27 M€
- 0,37 M€

### Spent Resources
(estimation based on first 12 PM)
How to rigorously model behavior of large, distributed OO systems?

**Specification level**

- Structural, no data

**Languages**

- UML, FDL, ALs
- Spec#, Java+JML

?
How to rigorously model behavior of large, distributed OO systems?

- Specification level
  - Structural, no data
  - Abstract behavioral
  - Implementation-oriented

- Languages
  - UML, FDL, ALs
  - HATS ABS language
  - Spec#, Java+JML
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:
   - “Hard” feature consistency, data integrity, security, property verification, code generation, . . .
   - “Soft” visualization, test case generation, specification mining, type checking, . . .

   Develop analyses hand in hand with ABS to ensure feasibility

3. Methodological and technological framework integrating HATS tool architecture and ABS language
Mitigating Technological Risks

Lack of Relevance

Counter measures:

▶ Apply to empirically successful method to develop reusable software: Software product lines (SWPL)
▶ Thorough requirements analysis, continuous evaluation

Feasibility: Analysis methods don’t scale up

Counter measures:

▶ Develop analysis methods hand in hand with ABS

Stuck on the Ground

Counter measures:

▶ Develop core ABS first, layered language design
▶ Provide basic tools (compiler, simulator, editor) early
The Main Innovations of HATS

A formal, executable, abstract, behavioral modeling language

- **State-of-art** on specification of concurrent, compositional software
- **Interdisciplinary**: combines advances in verification, concurrency, specification, programming languages communities
- **Adaptability** drives the design

Formalization of SWPL-based development as main application

- **Leveraging** formal methods tools to SWPL
- Adaptation of a SWPL development methodology to HATS

Analyses techniques/tools developed in tandem with ABS

- Several new **incremental** approaches
- **Complete** ("hard") and **incomplete** ("soft") technologies
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
<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core ABS Language</td>
<td>Syntax, type system, operational semantics</td>
</tr>
<tr>
<td>HATS Tool Suite</td>
<td>Parser, editor (Eclipse, Emacs), type checker, simulator (Maude), Java code generation</td>
</tr>
<tr>
<td>HATS Methodology</td>
<td>SWPL process for ABS and HATS tool suite</td>
</tr>
<tr>
<td>Feature Modeling</td>
<td>(Generalized) $\Delta$-modeling, influenced by traits, feature modeling language $\mu$TVL</td>
</tr>
<tr>
<td>Scalable Verification</td>
<td>Incremental verification techniques: composition, $\Delta$-slicing of proofs, partial evaluation</td>
</tr>
<tr>
<td>Modeling Evolvability</td>
<td>Investigated dimensions/forms of evolution</td>
</tr>
<tr>
<td>Resource Guarantee</td>
<td>Extension of cost analysis framework COSTA</td>
</tr>
<tr>
<td>Requirements</td>
<td>Requirements analysis from 3 detailed case studies</td>
</tr>
<tr>
<td>Evaluation</td>
<td>3 case studies modelled with Core ABS, Milestone 1</td>
</tr>
</tbody>
</table>
First Annual Project Review

Reviewers

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

15–16 March 2010 in Brussels, EC premisses

- Present: 7 WP leaders + Per Waborg + Richard Bubel
- Preparation meeting 14 March 2010
- Reviewers had read the deliverables in detail
- Want all site/task leaders present next time
- Emphasize formal quality of review artifacts
- Asked to improve alignment with ABS platform, specifically: type systems (BOL), model checking (KTH), resources (UPM)
First Annual Project Review: Recommendations

1. Relate and integrate all HATS artefacts, techniques and methods within the HATS development methodology
2. Clarify the role of formal methods in your approach wrt SWPL
3. Clarify relation between ABS, modelling languages (UML), and programming languages
4. Relate bytecode inlining to ABS and feature modelling language
5. Relate resource analysis framework to SWPL
6. Clarify what kind of properties are meant to be verified
7. Improve deliverables, present tool demos, create review templates
8. Make tools, case studies, tutorials, manuals available

All (revised) deliverables in first reporting period (PM1–12) accepted!
Active/Upcoming Work Tasks

PM 18–24: most active project phase, 12 active technical tasks

See also HATS Website Work Packages|Organization Schema
Active/Upcoming Work Tasks

PM 18–24: most active project phase, 12 active technical tasks

See also HATS Website Work Packages Organization Schema

<table>
<thead>
<tr>
<th>WP1: Framework (UKL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2 KUL, PM 9–24 Feature Modeling, Platform Models, Configuration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WP2: Variability (UIO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1 UIO, PM 6–30 A configurable deployment architecture</td>
</tr>
<tr>
<td>2.2 CWI, PM 1–24 Feature Integration</td>
</tr>
<tr>
<td>2.3 CTH, PM 18–36 Testing, debugging, and visualization</td>
</tr>
<tr>
<td>2.4 BOL, PM 12–36 Types for Variability</td>
</tr>
<tr>
<td>2.5 CTH, PM 6–24 Verification of General Behavioral Properties</td>
</tr>
<tr>
<td>WP3: Evolvability (KTH)</td>
</tr>
<tr>
<td>------------------------</td>
</tr>
<tr>
<td>3.1 UKL, PM 1–24 Evolvable Systems: Modeling and Specification</td>
</tr>
<tr>
<td>3.2 NR, PM 18–36 Model Mining</td>
</tr>
<tr>
<td>3.4 KTH, PM 6–24 Evolvability at Bytecode Level</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WP4: Trustworthiness (UPM)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1 UPM, PM 12–36 Security</td>
<td></td>
</tr>
<tr>
<td>4.2 UPM, PM 1–24 Resource Guarantees</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>WP6: Dissemination (FRG)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Dissemination (FRG), Exploitation (FRG), Training (BOL), CA (CTH)</td>
<td></td>
</tr>
</tbody>
</table>
Dissemination Efforts

(Discussed in more detail by Ralf tomorrow 16:30)

Highlights of last 12 months

▶ Categories “News”, “Publications”, “Deliverables” at Website
▶ General presentations of the Project by RH:
  • FP7 FET Theme ICT-2007.8.6 “Forever Yours” Cluster Meeting, March 2010, Brussels, Belgium
  • 4th International Symposium On Leveraging Applications of Formal Methods, Verification and Validation (ISoLA), October 2010, Amirandes, Heraclion, Crete
▶ HATS Track at FMCO 2009 during FMweek, Eindhoven Nov 2009:
  • RH: HATS project overview and scalable verification
  • Arnd Poetzsch-Heffter: Modular specification and verification in HATS
  • Martin Steffen: Design of an abstract behavioral specification language
▶ Workshop ”Formal Methods in Software Product Line Engineering” (FMSPLE) at the Software Product Line Conference (SPLC), September 2010, Jeju Island, South Corea
<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>6.1</td>
<td>Web site and project presentation</td>
<td>6</td>
<td>FRG</td>
<td>2</td>
<td>O</td>
<td>PU</td>
<td>2</td>
</tr>
<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</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>1.1.a,b</td>
<td>Report on the Core ABS Language &amp; Methodology</td>
<td>1</td>
<td>UIO</td>
<td>47</td>
<td>R</td>
<td>PU</td>
<td>12</td>
</tr>
<tr>
<td>2.2.a</td>
<td>First report on Feature selection and integration</td>
<td>2</td>
<td>CWI</td>
<td>22</td>
<td>R</td>
<td>PU</td>
<td>12</td>
</tr>
<tr>
<td>3.1.a</td>
<td>First report on Evolvable Systems</td>
<td>3</td>
<td>UKL</td>
<td>22</td>
<td>R</td>
<td>PU</td>
<td>12</td>
</tr>
<tr>
<td>7.1</td>
<td>Annual Activity Report</td>
<td>7</td>
<td>CTH</td>
<td>9</td>
<td>R</td>
<td>PU</td>
<td>12</td>
</tr>
<tr>
<td>7.2.b</td>
<td>Annual Financial Report</td>
<td>7</td>
<td>CTH</td>
<td>4</td>
<td>R</td>
<td>PU</td>
<td>12</td>
</tr>
<tr>
<td>5.2</td>
<td>Evaluation of Core Framework</td>
<td>5</td>
<td>FRH</td>
<td>17</td>
<td>R</td>
<td>PU</td>
<td>18</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>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>

Careful planning & sufficient deadlines essential
Trustworthy Eternal Systems via Evolving Software, Data, and Knowledge

- Website: https://www.eternals.eu/
- Project Partners:
  - Univ Trento, CTH, INRIA, KUL (IP coordinators)
  - Queen Mary Univ (Ebroul Izquierdo), Waterford Inst. (Jim Clarke)
- Budget: 550 kEUR for 36 months
- Start date: 1 March 2010
- Goals/instruments (only COORD, no RTD)
  - Task Forces (survey state-of-art, set agenda)
  - Workshops, Training Courses
  - Community Building
  - Road maps, white papers, input to future calls
EternalS Relies mainly on Task Forces

- Structure the participants of EternalS in manageable units
- Topical organization around themes that concern all partners
- Provide platform for actual work, structuring meetings, etc.

EternalS Task Forces (structure closely related to HATS agenda!)

Work Package 1 Task Force Management, Leader: Reiner Hähnle

TF1 Diversity awareness and management (Leader: Ina Schaefer)
- investigate mechanisms that model/handle diversity in IT-systems
- from HATS: Dave Clarke, Reiner Hähnle, Ina Schaefer

TF2 Time awareness and management (Leader: Michael Hafner)
- dynamic and adaptive systems with focus on security
- from HATS: Martin Steffen

TF3 Self-adaptation & evolution by learning (Leader: Richard Johansson)
- learning/control techniques for autonomous evolution of systems
- from HATS: you??
FET Flagship Initiative

Very Large-Scale FET ICT Research Programmes


- Two flagships from 2013 onwards for 10 years
- 1,000,000,000 € (yes, 10^9!) each
- From Spring 2011: six 1-year CAs with 1.5M€ for preparation
- Core in ICT, but multidisciplinary

The Social Computer: Internet-Scale Human problem solving

http://socialcomputer.eu/

- Consortium coordinated by Fausto Giunchiglia (LivingKnowledge)
- Closely related to EternalS CA its IPs
- Several HATS members involved (talk to me if interested):
  Reiner Hähnle (WP leader CA), Mads Dam, Dilian Gurov, Davide Sangiorgi
- Workshop in Brussels 1 October 2010
Meetings in the Last 12 Months

WT 1.2+2.2 Joint Meeting, 28–29 October 2009 Leuven

▶ 7 participants from CTH, FRH, CWI, KUL, FRG
▶ Feature Modeling
▶ Requirements analysis

WT 1.1, HATS Methodology, 26–28 January 2010 Oslo

▶ 10 participants from CTH, FRH, FRG, UKL, UIO, NR
▶ Agree on HATS methodology
▶ Planning D1.1b

WT 1.1, Methodology & Feature Integration, 1 Feb 2010 Amsterdam

▶ 4 participants from FRH, CWI
▶ Positioning of Δ-modelling in the HATS methodology

Please complete/correct this info & add agenda/minutes on website
### WT 4.2+5.2 Requirements Analysis & Evaluation, 28 April 2010 Madrid
- 5 participants from FRH, UPM
- Requirements analysis and Evaluation of Task 4.2 (Resources)

### WT 5.2 Evaluation, 10 May 2010 Amsterdam
- 10 participants from FRH, UIO, KUL, CWI, FRG, UKL, CTH, KTH
- Defining roadmap for evaluation of core ABS

### WT 1.2 Feature Modeling, 11 May 2010 Amsterdam
- 10 participants from UIO, KUL, CWI, UKL, CTH, IoC, KTH
- Theory of Feature Models, Δ-Modeling

### WT 2.5 Behavioral Verification, 11 May 2010 Amsterdam
- 10 participants from UIO, KUL, CWI, UKL, CTH, IoC, KTH
- Specification and Verification of Concurrent ABS Programs
Meetings in the Last 12 Months Cont’d

WP 3 Meeting, 12 May 2010 Amsterdam
- 10 participants from NR, UIO, KUL, UKL, CTH, IoC, KTH, BOL
- Planning of WT 3.1, 3.3, 3.4, 3.5

- 9 participants from UIO, UKL, CTH, CWI, KTH
- Coordinating specification approach for ABS
- Coordination among WT 1.2, 2.3, 2.5, 2.6, 4.3

Integration of $\Delta$s in ABS, 25–26 August 2010 Oslo
- 9 participants from UIO, KUL, CTH, CWI
- Representation of $\Delta$-Modeling in Full ABS
### 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
<table>
<thead>
<tr>
<th>Changes in the Consortium</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enlargement of HATS with IoC (presentation 15:15 today)</strong></td>
</tr>
<tr>
<td>Tarmo Uustalu (IoC), Peeter Laud (Tartu), Keiko Nakata (IoC)</td>
</tr>
</tbody>
</table>
| ▶ The perfect bureaucratic storm:  
  unprecedented, software not intended for enlargement, change of PO, holidays in Sweden, then Estonia, then Belgium, ... |
| ▶ Still not everything finalized, but will dated back 1 May 2010 |
| ▶ CA consists of simple amendment, no modifications |
| **Univ Genova as 3rd party to BOL** |
| ▶ Replaced with local expertise in BOL, objectives & budget unchanged |
| ▶ Formal amendment to GA necessary (accepted by EC 14 Dec 2009) |
| **FRH being bought by another company** |
| **SME status to change in final project year** |
| **FRG changes site leader** |
| Karina Villela takes over from Ralf Carbon |
Relation with the Commission

Change of Project Officer
- 23 June 2010: PO changed from Rüdiger Martin to Wide Hogenhout
- Experienced PO who was also responsible for Mobius

Date and Place for Review of Second Project Phase (PM13–24)
- Takes place in Brussels at EC premisses
- Preparation meeting on Wednesday 23 March, 2011
- Review meeting on 24–25 March, 2011 (until Friday noon)
- All site leaders and leaders of active WTs must be present
Summary: Main Results and Achievements

- Passed first project review
- All deliverables of first period approved
- Core ABS finished, extensive case studies modelled
- Achieved first Milestone (D5.2)
- First version of tool suite available and usable
- Work started/on track in all active Work Tasks
- Many dedicated WT meetings, good participation
- All participants highly motivated
- Solid publication record
- Successful application for enlargement with IoC from 1 May 2010
- SAB and EUP participate in AM, 2 of 3 SAB members present
- Strong presence in EternalS CA
- Participation in FET Flagship proposal