HATS:
Highly Adaptable & Trustworthy Software Using Formal Models

— Report from the Coordinator —

Reiner Hähnle

Technical University of Darmstadt, Germany

Fourth Annual HATS Project Meeting
Valencia 4–6 September 2012

December 3, 2012

HATS
Highly Adaptable and Trustworthy Software using Formal Models

SEVENTH FRAMEWORK PROGRAMME

http://www.hats-project.eu

Project Status

- Project started 1 March 2009, all participants are active as planned
- $>$ 70 people involved in HATS (according to `hats-all`), 40 here
- Funding for 4th period received 1 Aug 2012
  - Only small amount, as remaining 15% withheld until Final Report ready (10% to be paid after final report, 5% contingency fund)
  - Hence, no transfer maid to participants at this time
- More details on finances by Per, after my presentation
- More details on dissemination by Karina, on Thursday

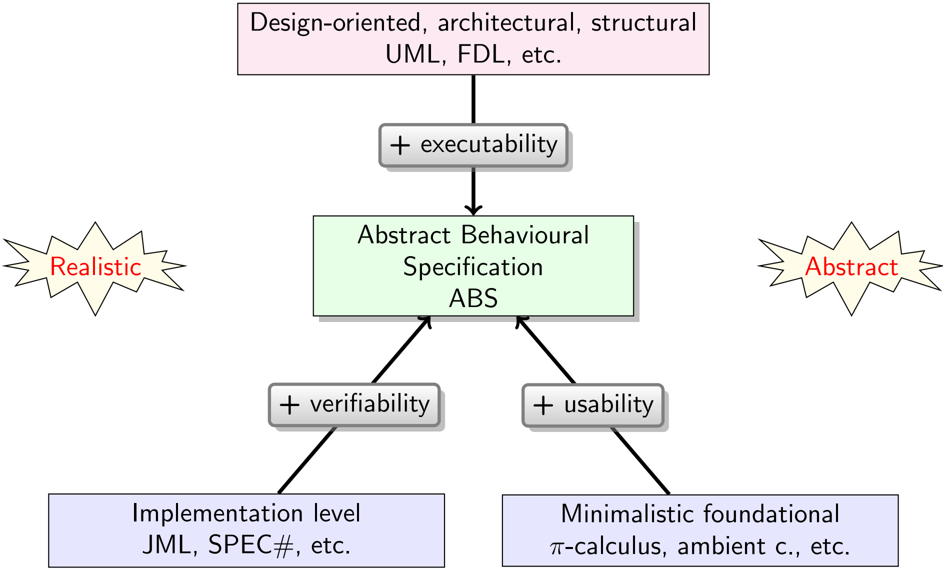
Mind the Gap!

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

Implementation level
JML, SPEC#, etc.

Minimalistic foundational
π-calculus, ambient c., etc.

Mind the Gap!


Design-oriented, architectural, structural
UML, FDL, etc.
+ executability
Abstract Behavioural Specification ABS
Realistic
Abstract
+ verifiability
+ usability
Implementation level
JML, SPEC#, etc.
Minimalistic foundational
π-calculus, ambient c., etc.

What We Deliver

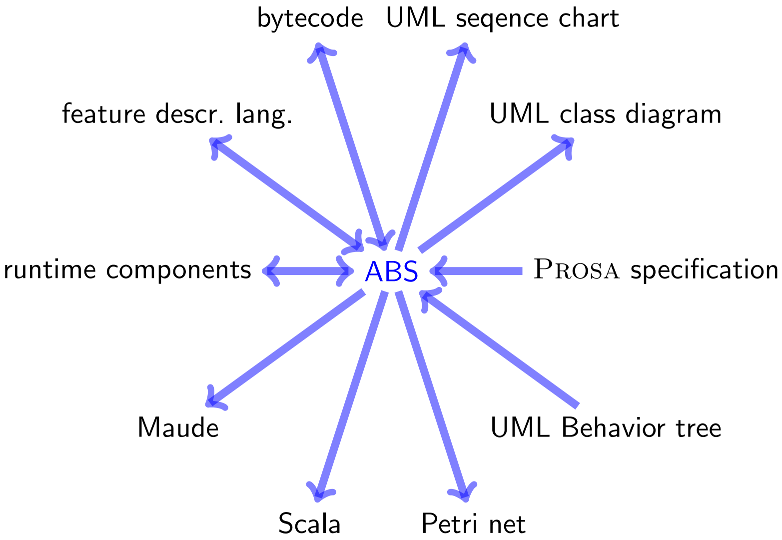
A tool-supported formal method for
building highly adaptable and trustworthy software

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~~ Reality: A Single-Source Technology for Highly Adaptive, Concurrent Software Systems



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

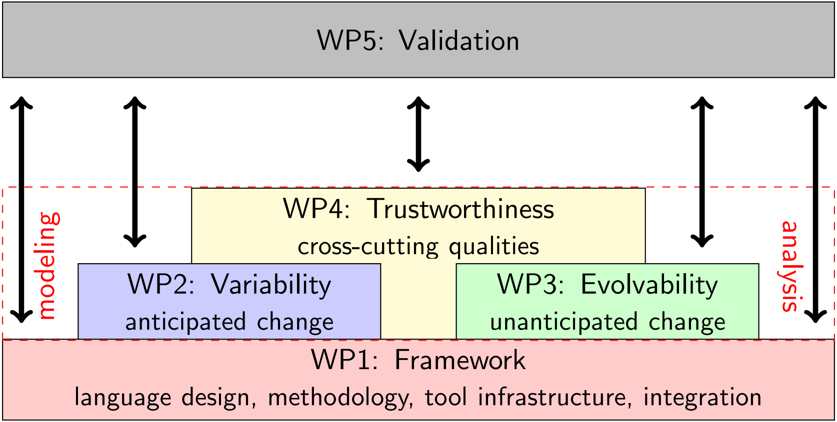
Scalable technologies developed in tandem with ABS

- 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



PM42: Research Objectives & Main Results — M3

Development Methods

- Delta modeling workflow based on abstract delta modeling (T5.3)
- End-to-end product derivation with correction, optimization (T1.4)

Analysis Methods in particular, at feature modeling level

- Near/far location type analysis (T1.3), deadlock analysis (T4.3)
- Type system for checking type-safety of delta models (T2.4)
- Glass box test case generator and ABSUnit framework (T2.3)
- Deductive, sound compilation from ABS to bytecode (T2.6)
- KeY-ABS formal verification (T4.3)

Generative Methods

- Model mining from code, traces, product descriptions (T3.2)
- Automatic construction of crypto protocol implementation (T4.1)
- Scala backend for ABS (T1.4)

Security Policies

- Information-flow type system for core ABS (T4.1)
- Logic-based and dynamic enforcement of security policies (T4.1)

PM42: Further Objectives & Main Results

Dynamic Aspects, Evolvability

- Deployment components to model low-level notions (T2.1)
  - Schedulers, load, bandwidth
  - Real-time ABS
- Abstract failure model and type system (T2.1, T2.4)
- ABS component model (T2.1, T3.3)
- ABS-NET: semantics for network-aware runtime ABS (T3.5)

Evaluation & Exploitation

- Fredhopper Access Server replication system (T5.3)
  - Modeled with Full ABS as basis for validation of M2
- Some models in S.P.L.O.T. feature model repository (T5.3)
- Finalized list of exploitable items (T6.2)

User Interface

- Workflow-driven user interface with extension guidelines (T1.3)

Third Annual Project Review

Project Officer

Roumen Borissov

Reviewers

- Patrick Heymans, University of Namur
- Marco Roveri, Fondazione Bruno Kessler
- Kaisa Sere, Åbo Academy (offline due to illness)
- Martin Wirsing, LMU Munich

22nd-23rd March 2012 in Tallinn, IoC premisses

- Present:
  Reiner, Einar, Arnd, Rudi, Davide, Mario, Elvira, Richard, Gilles, Wolfgang, Per, José, Peter, Bjarte, Mads, Frank, Taslim, Tarmo
- Preparation meeting 21st March 2012
- Went very well ("good to excellent" progress)

Third Annual Project Review: Main Recommendations

1. Validation: more objective and quantitative evaluation (WP5)
   - Quantitative comparison between FRH code and its ABS model
   - Discuss advantages using the HATS methodology wrt current practice
   - All the developed techniques and tools shall be applied to the considered case studies (otherwise, corrective actions or justification)
   - Table with considered/covered requirements for each case study
   - List of tools applied on each case study
2. Classification of verification properties, their role and relevance in PLE
3. A systematic approach for the use of verification properties
4. Better define the objectives and scope of Configuration (T4.4)
5. All functionalities and techniques integrated in tool chain
6. Increase number of joint journal publications, develop book summarizing the major results, propose tutorials at major conferences
7. Technology papers (as promised in the slides at review)
8. Excerpt of the feedback from SAB and EUP shall be provided

All deliverables in 3rd reporting period (PM15–36) accepted w/o changes!

Active/Upcoming Work Tasks

See also HATS Website "`Work Plan|WP Timing & Deliverables`"

WP1: Framework (UKL)

1.5 NR, PM 25–48 Integrated Tool Platform

WP2: Analysis (UIO), PM45: Analysis Final Report (TUD)

WP3: Evolvability (KTH)

3.3 KUL, PM 24–46 Hybrid Analysis for Evolvability
3.5 KTH, PM 24–48 Autonomously Evolving Systems

WP4: Trustworthiness (UPM)

4.3 BOL, PM 24–48 Correctness
4.4 FRG, PM 30–45 Auto Configuration and Quality Variability

WP5: Validation (FRH)

5.4 FRH, PM 30–48 Evaluation of Tools & Techniques

Final Deliverables

Del. no.	Deliverable name	WP no.	Lead beneficiary	Nature	Dissemination level	Delivery date	Comments
D1.5	Integrated tool platform	1	NR	report	public	48	early start
D2.7	Analysis final report	2	TUD	report	public	45	multiple tasks, shifted
D3.3	Hybrid analysis for evolvability	3	KUL	report	public	46	shifted
D3.6	Final Report	3	KTH	report	public	48	
D3.5	Autonomously evolving systems	3	KTH	report	public	48	
D4.3	Correctness	4	BOL	report	public	48	
D4.4	Auto configuration quality variability	4	FRG	report	public	45	part of M4 shifted
D5.4	Evaluation of tools & techniques	5	FRH	report	public	48	validates M3, M4
D6.3	Training Material	6	BOL	report	public	48	PhD school proceedings

Scientific Advisory Board (SAB) & End-User Panel (EUP)

Scientific Advisory Board (SAB)

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

- Ferrucio Damiani, University of Torino, Italy
- 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

Summary: Main Results and Achievements

- Passed second project review with very encouraging feedback
- All deliverables of third period approved w/o revision
- Work started/on track in all active Work Tasks
- Many dedicated WT meetings, good participation
- All participants highly motivated
- Very good publication record (FMCO track, ISoLA track)
- Good dissemination events (FMSPLE, Ericsson, SAP, Google)
- HATS Summer School in Bertinoro
- SAB and EUP participate in AMs, 2 of 3 SAB members present
- Continued strong presence in EternalS CA