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

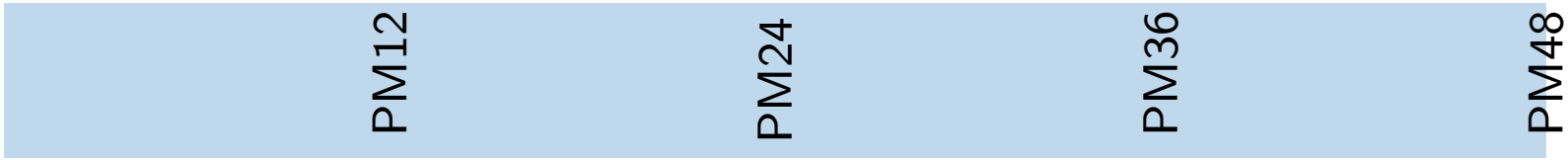
September 15, 2010

http://www.hats-project.eu

Project Status

PM12	PM24	PM36	PM48

Project Status

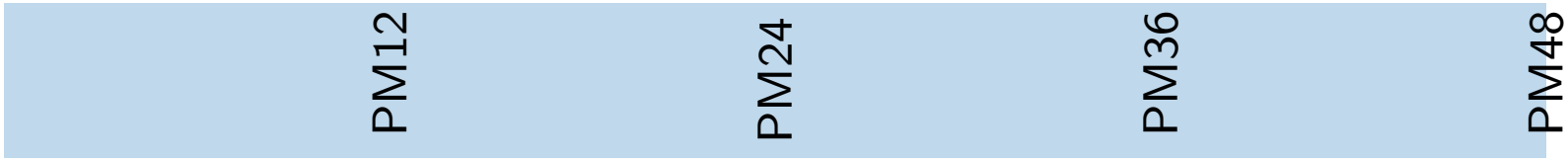


Elapsed Time

Project Status

	PM12	PM24	PM36	PM48
Elapsed Time				
Received Funding			5,27 M€	

Project Status

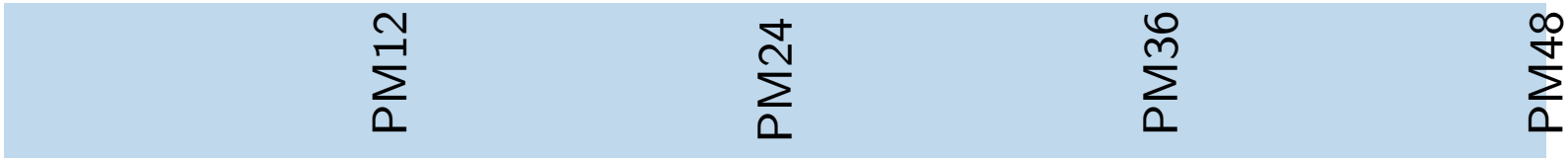


Elapsed Time

Received Funding 5,27 M€

Spent Resources (estimation based on first 12 PM)

Project Status



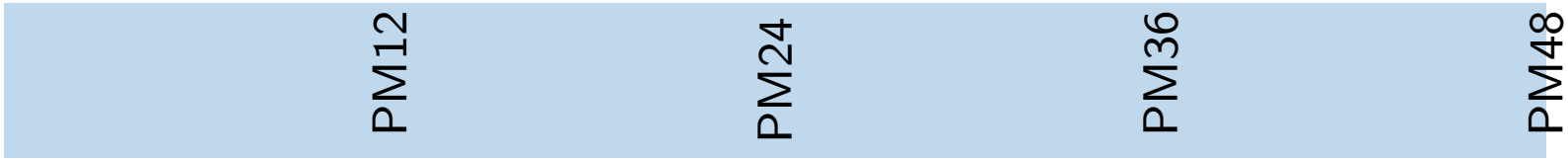
Elapsed Time

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



Elapsed Time

Received Funding

5,27 M€

0,37 M€

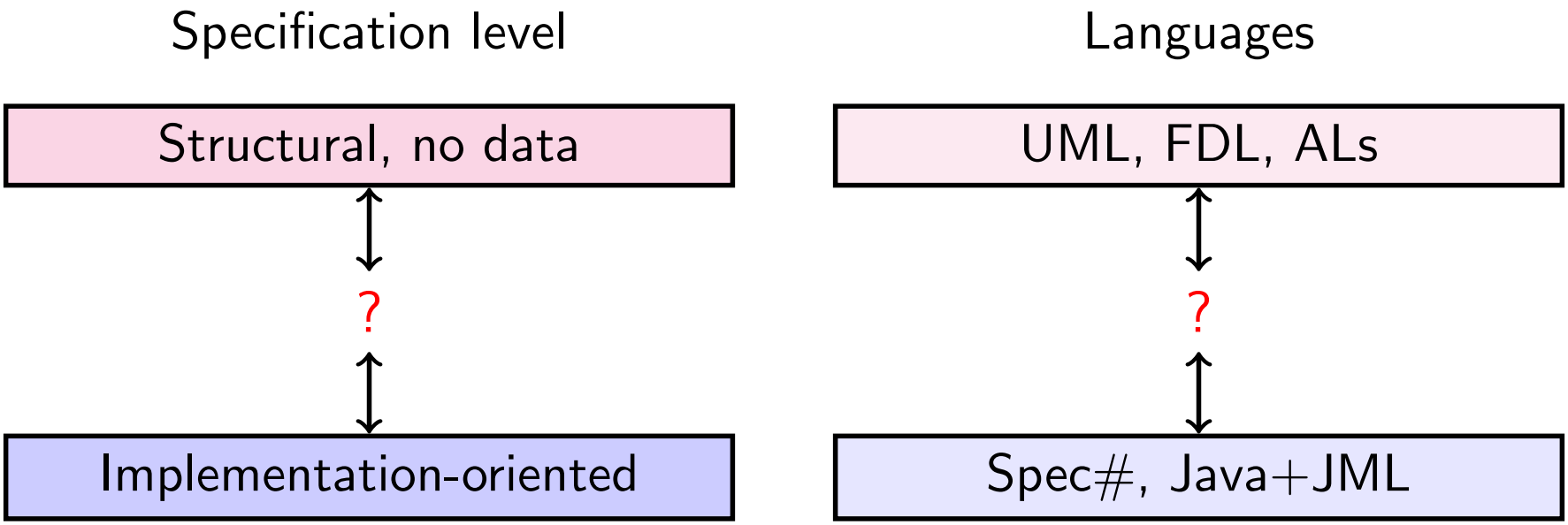
Spent Resources

(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

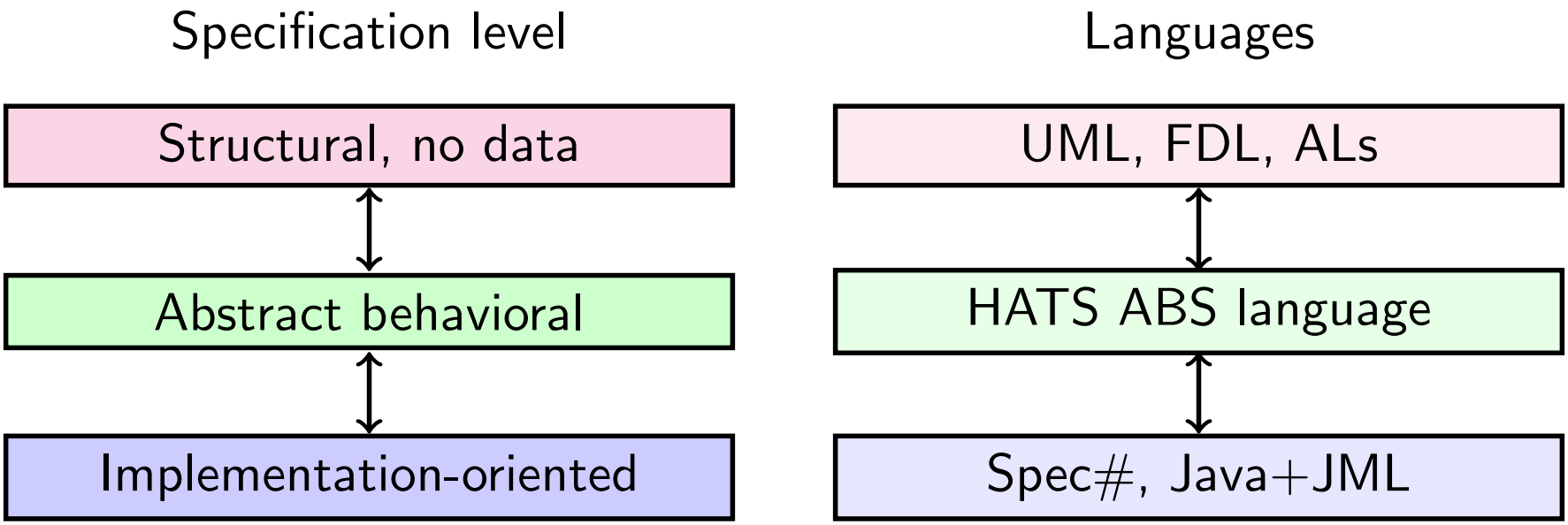
Mind the Gap!

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



Mind the Gap!

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



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, continous 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

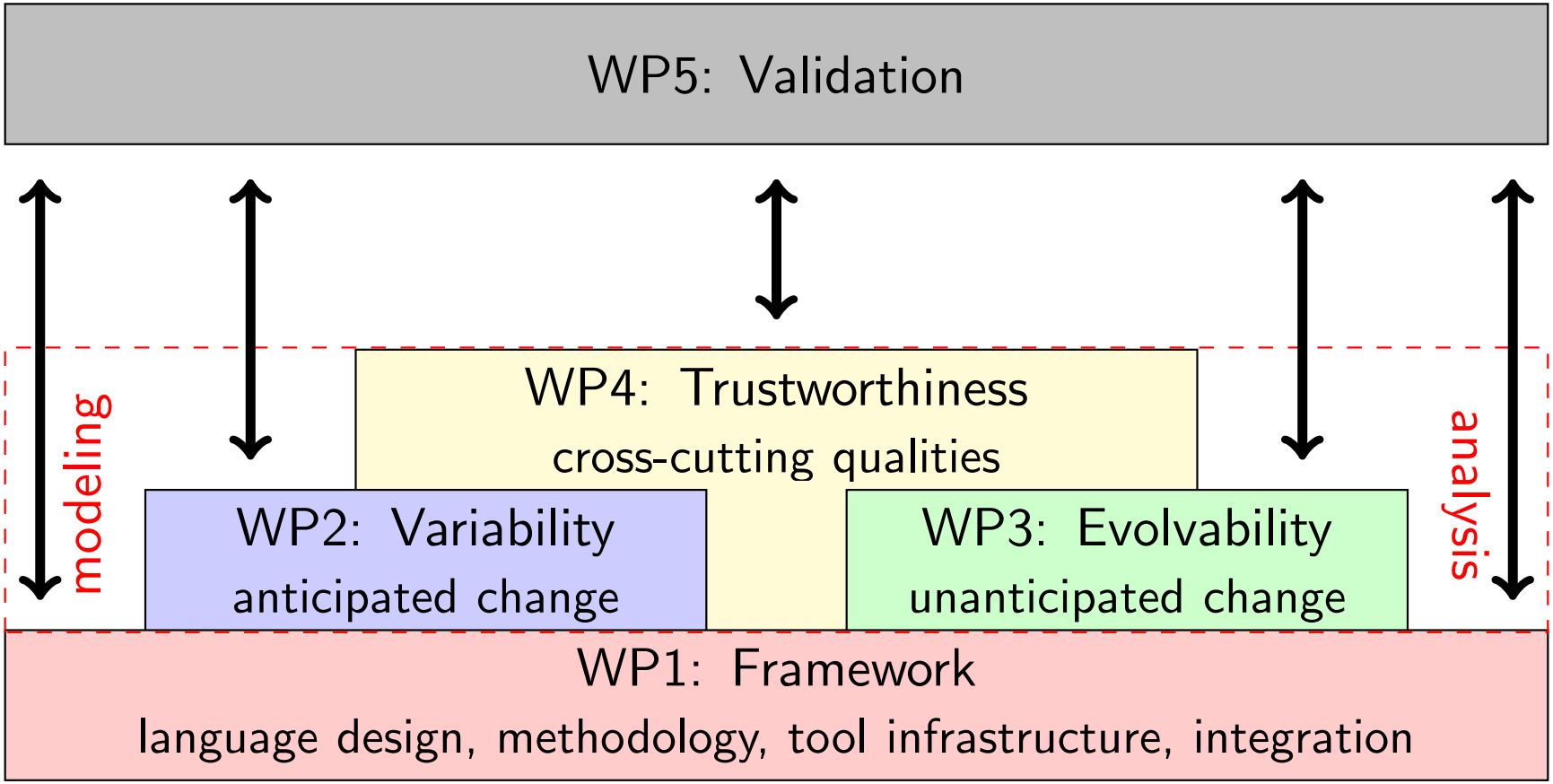
Formalization of SWPL-based development as main application

- 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



PM 18: Research Objectives and Main Results

Core ABS Language	Syntax, type system, operational semantics
HATS Tool Suite	Parser, editor (Eclipse, Emacs), type checker, simulator (Maude), Java code generation
HATS Methodology	SWPL process for ABS and HATS tool suite
Feature Modeling	(Generalized) Δ-modeling, influenced by traits, feature modeling language μTVL
Scalable Verification	Incremental verification techniques: composition, Δ-slicing of proofs, partial evaluation
Modeling Evolvability	Investigated dimensions/forms of evolution
Resource Guarantee	Extension of cost analysis framework COSTA
Requirements	Requirements analysis from 3 detailed case studies
Evaluation	3 case studies modelled with Core ABS, Milestone 1

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`

WP1: Framework (UKL)

1.2 KUL, PM 9–24 Feature Modeling, Platform Models, Configuration

WP2: Variability (UIO)

2.1 UIO, PM 6–30 A configurable deployment architecture

2.2 CWI, PM 1–24 Feature Integration

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

2.4 BOL, PM 12–36 Types for Variability

2.5 CTH, PM 6–24 Verification of General Behavioral Properties

Active/Upcoming Work Tasks Cont'd

WP3: Evolvability (KTH)

3.1 UKL, PM 1–24 Evolvable Systems: Modeling and Specification

3.2 NR, PM 18–36 Model Mining

3.4 KTH, PM 6–24 Evolvability at Bytecode Level

WP4: Trustworthiness (UPM)

4.1 UPM, PM 12–36 Security

4.2 UPM, PM 1–24 Resource Guarantees

WP5: Validation (FRH)

5.2 FRH, PM 6–18 Evaluation of Core Framework

5.3 CWI, PM 18–36 Evaluation of Modeling

WP6: Dissemination (FRG)

Dissemination (FRG), Exploitation (FRG), Training (BOL), CA (CTH)

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

Past Deliverables

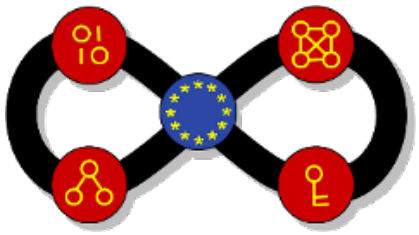
Del. No.	Deliverable name	WP No.	Lead Beneficiary	PMs	Type	Dissemination level	Deliv. date PM
6.1	Web site and project presentation	6	FRG	2	O	PU	2
7.2.a	Bi-Annual Management Report	7	CTH	4	R	PU	6, 12, 18
5.1	Requirements Elicitation	5	FRG	17	R	PU	6
7.3	Project Quality Plan	7	CTH	1	R	PU	11
6.4	Dissemination Plan	6	FRG	1	R	PU	11
1.1.a,b	Report on the Core ABS Language & Methodology	1	UIO	47	R	PU	12
2.2.a	First report on Feature selection and integration	2	CWI	22	R	PU	12
3.1.a	First report on Evolvable Systems	3	UKL	22	R	PU	12
7.1	Annual Activity Report	7	CTH	9	R	PU	12
7.2.b	Annual Financial Report	7	CTH	4	R	PU	12
5.2	Evaluation of Core Framework	5	FRH	17	R	PU	18

Upcoming Deliverables (Including IoC Effort)

Del. No.	Deliverable name	WP No.	Lead Bene-ficiary	PMs	Type	Dissemi-nation level	Deliv. date PM
4.2	Resource Guarantees	4	UPM	25	R	PU	24
1.2	Full ABS Modeling Framework	1	KUL	32	R	PU	24
2.2.b	Final report on Feature se-lection and integration	2	CWI	21	R	PU	24
2.5	Verification of Behavioral Properties	2	CTH	45	R	PU	24
3.1.b	Final report on Evolvable Systems	3	UKL	21	R	PU	24
3.4	Evolvability at Bytecode Level	3	KTH	19	R	PU	24
6.2	Exploitation strategy	6	FRG	15	R	PU	24

Careful planning & sufficient deadlines essential

Coordination Action EternalS (Task 6.4)



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

Coordination Action EternalS: Task Forces

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

`http://cordis.europa.eu/fp7/ict/programme/fet/flagship/`

- Two flagships frpm 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

Meetings in the Last 12 Months Cont'd

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

Specification Language, Logic & Calculus, 19–20 August 2010 Gothenburg

- 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 Δs in ABS, 25–26 August 2010 Oslo

- 9 participants from UIO, KUL, CTH, CWI
- Representation of Δ-Modeling in Full 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

Enlargement of HATS with IoC (presentation 15:15 today)

Tarmo Uustalu (IoC), Peeter Laud (Tartu), Keiko Nakata (IoC)

- 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 amendmend, 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