HATS:
Highly Adaptable & Trustworthy Software Using Formal Models

Report from the Coordinator

Reiner Hähnle

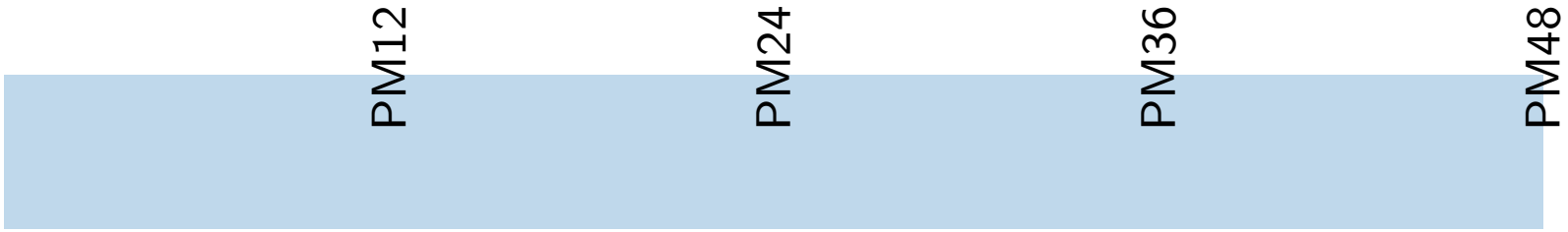
Technical University of Darmstadt, Germany

Third Annual HATS Project Meeting
Oslo 5–7 September 2011

September 2, 2011

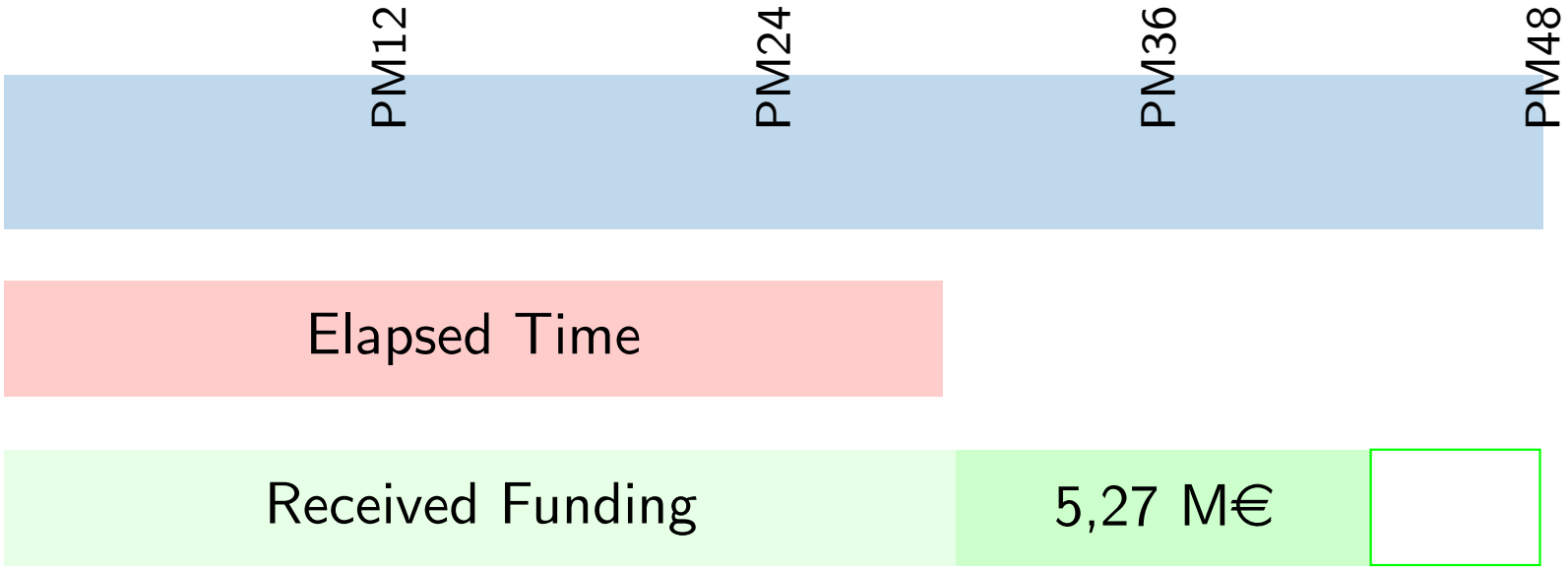
http://www.hats-project.eu

Project Status

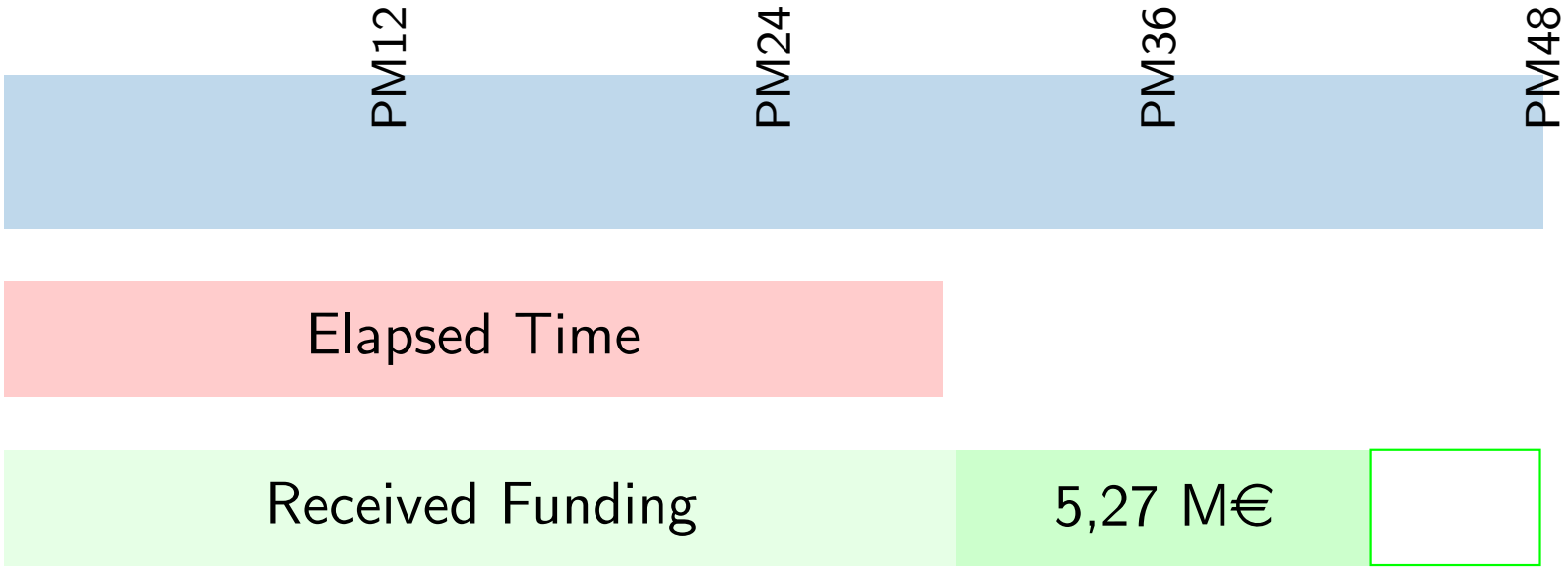


Project Status

Project Status

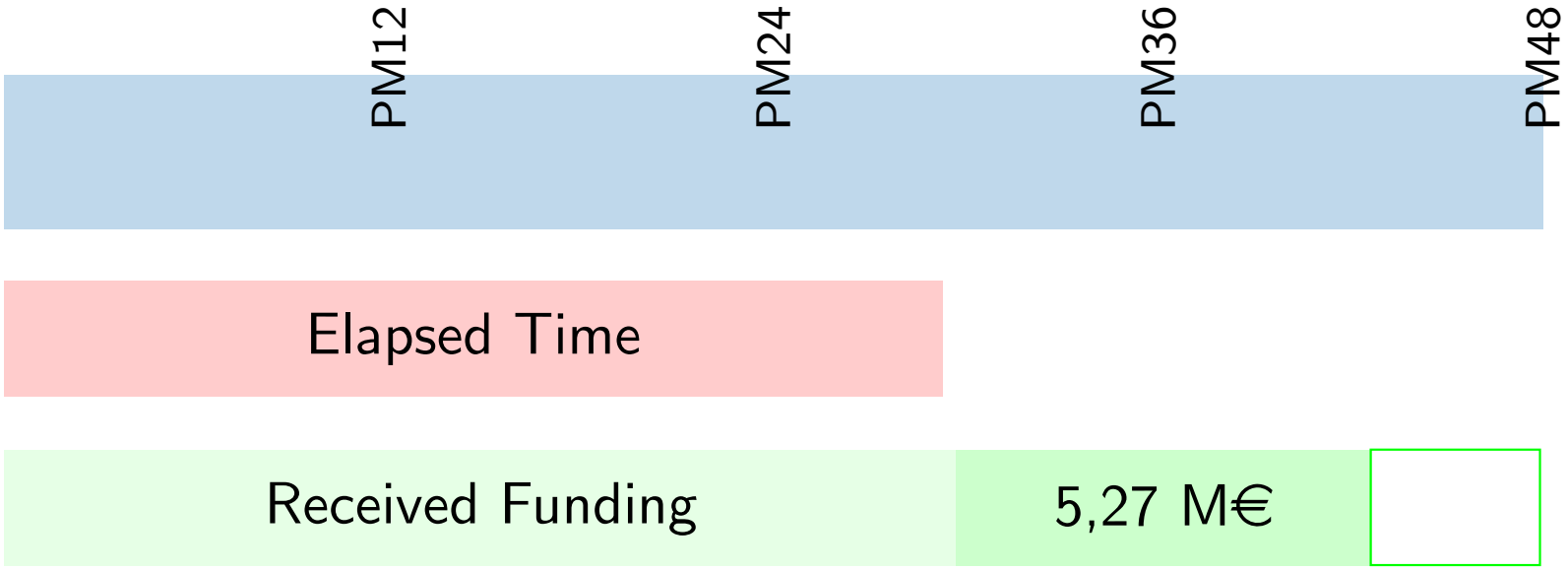


Project Status



(estimation based on first 24 PM)

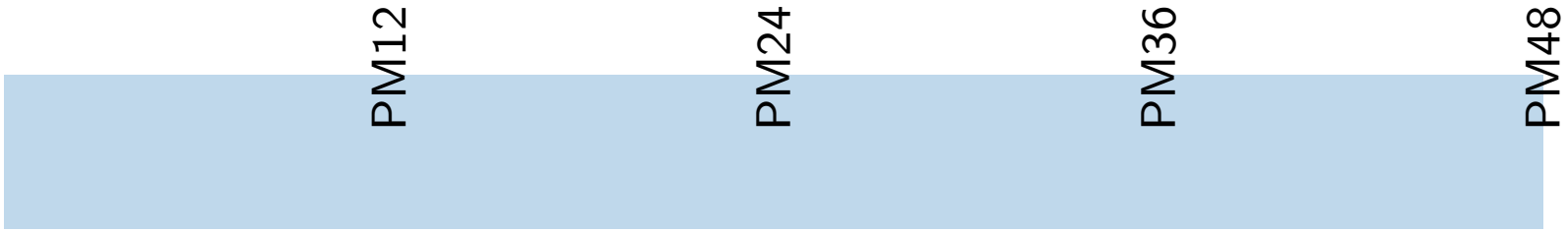
Project Status



(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€

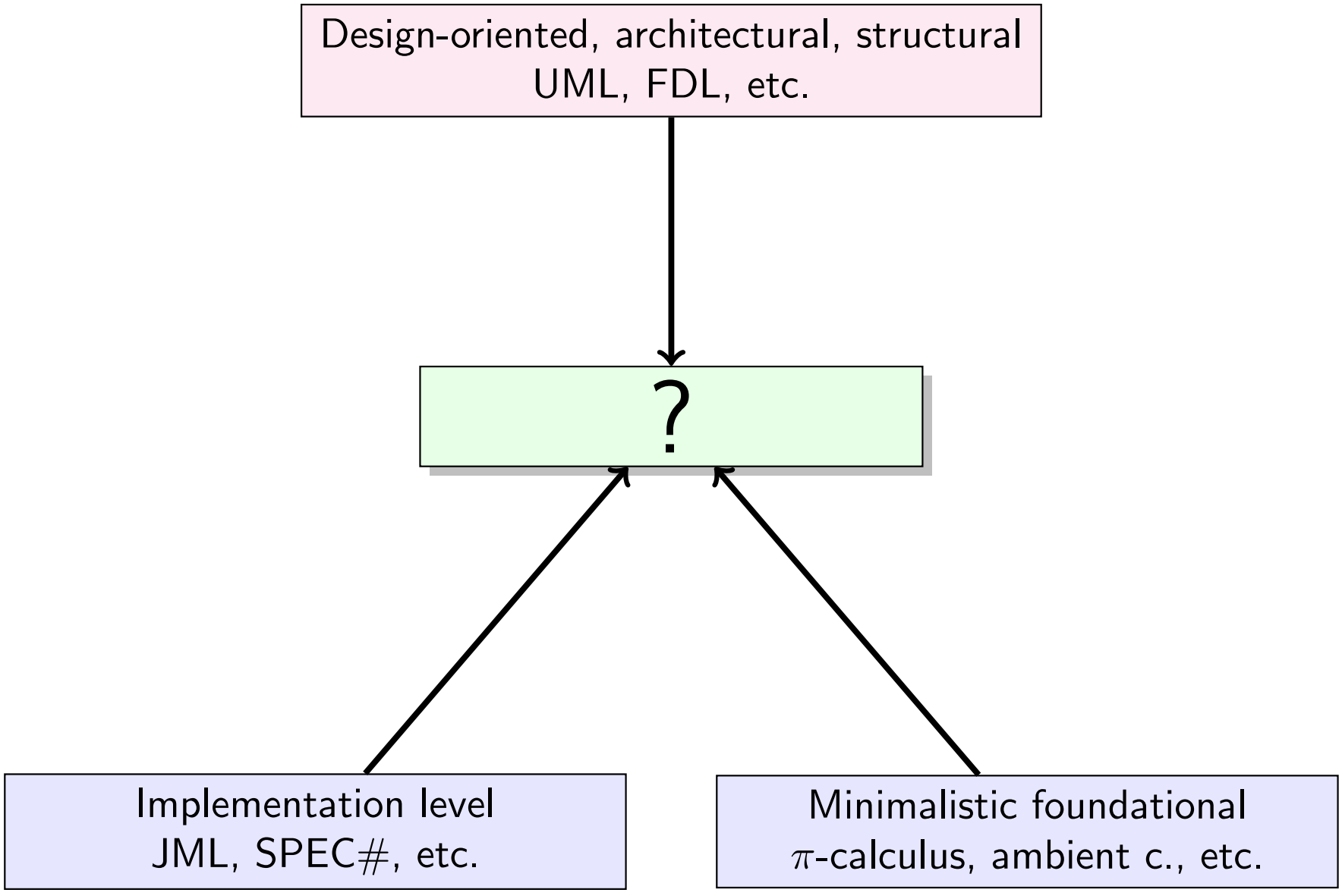
0,37 M€

Spent Resources

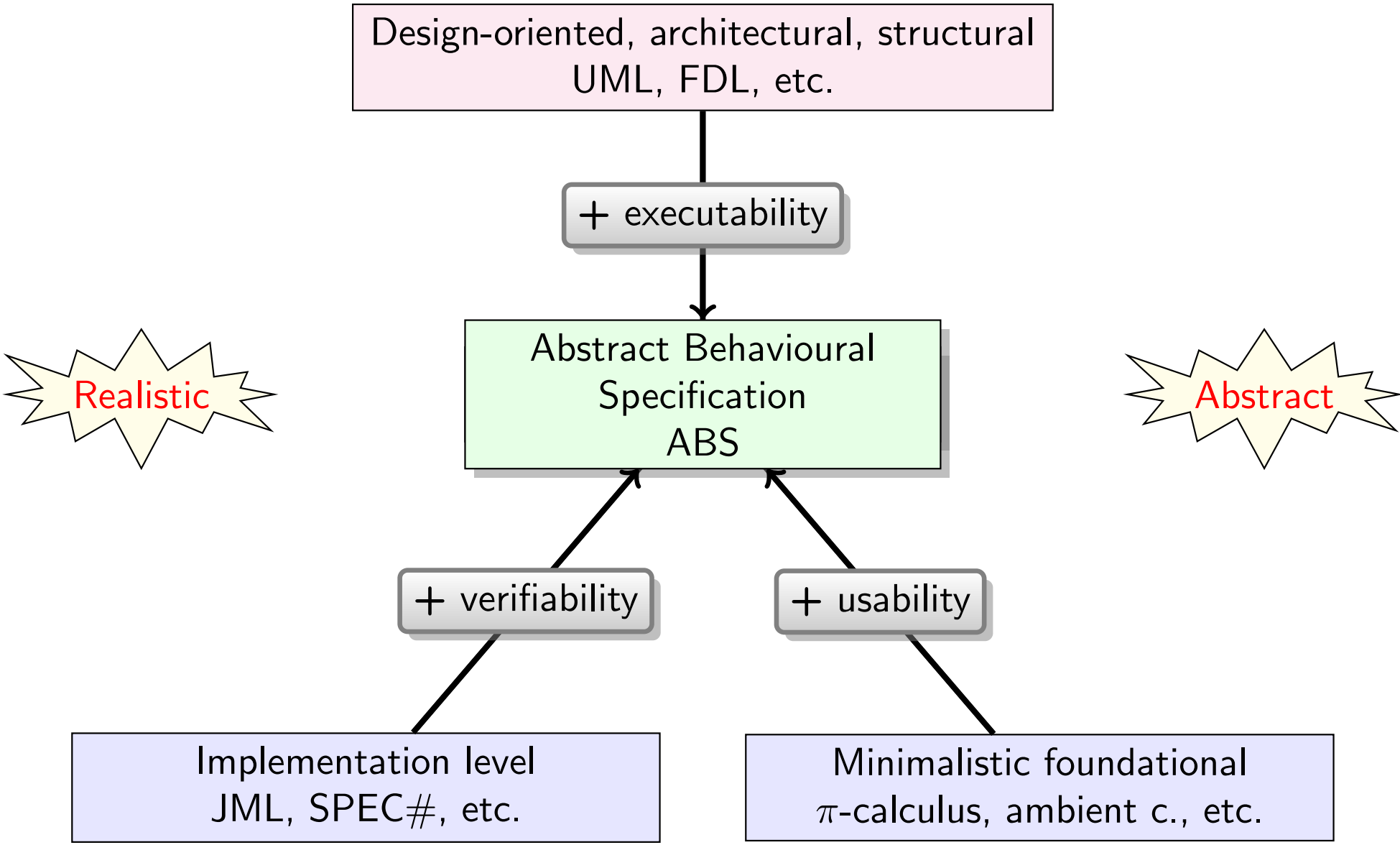
(estimation based on first 24 PM)

- 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

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
Realistic
Abstract Behavioural
Specification
ABS
Abstract
+ verifiability
+ usability
Implementation level
JML, SPEC#, etc.
Minimalistic foundational
π-calculus, ambient c., etc.

What We Deliver

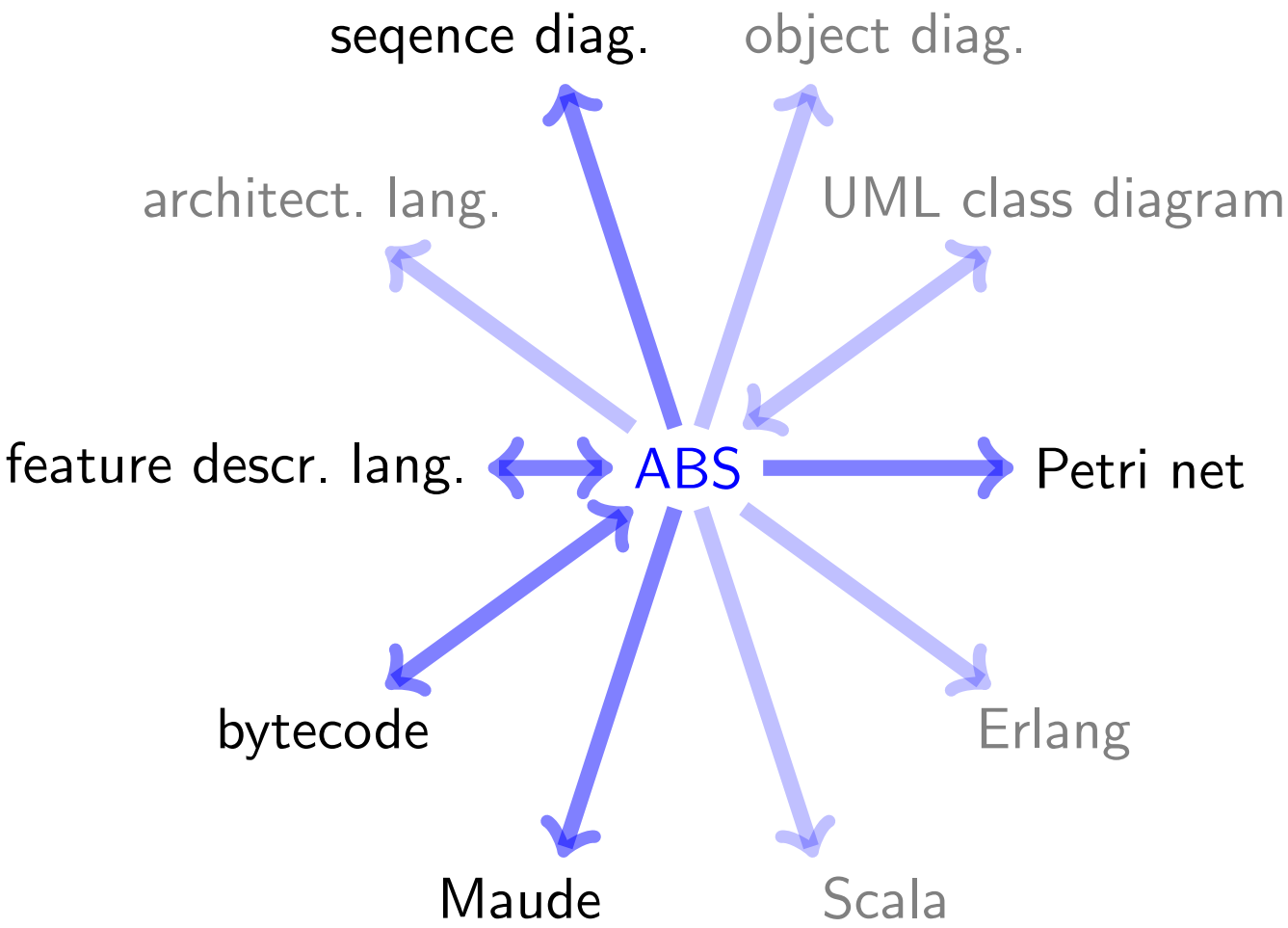
A tool-supported formal method for
building highly adaptable and trustworthy software

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

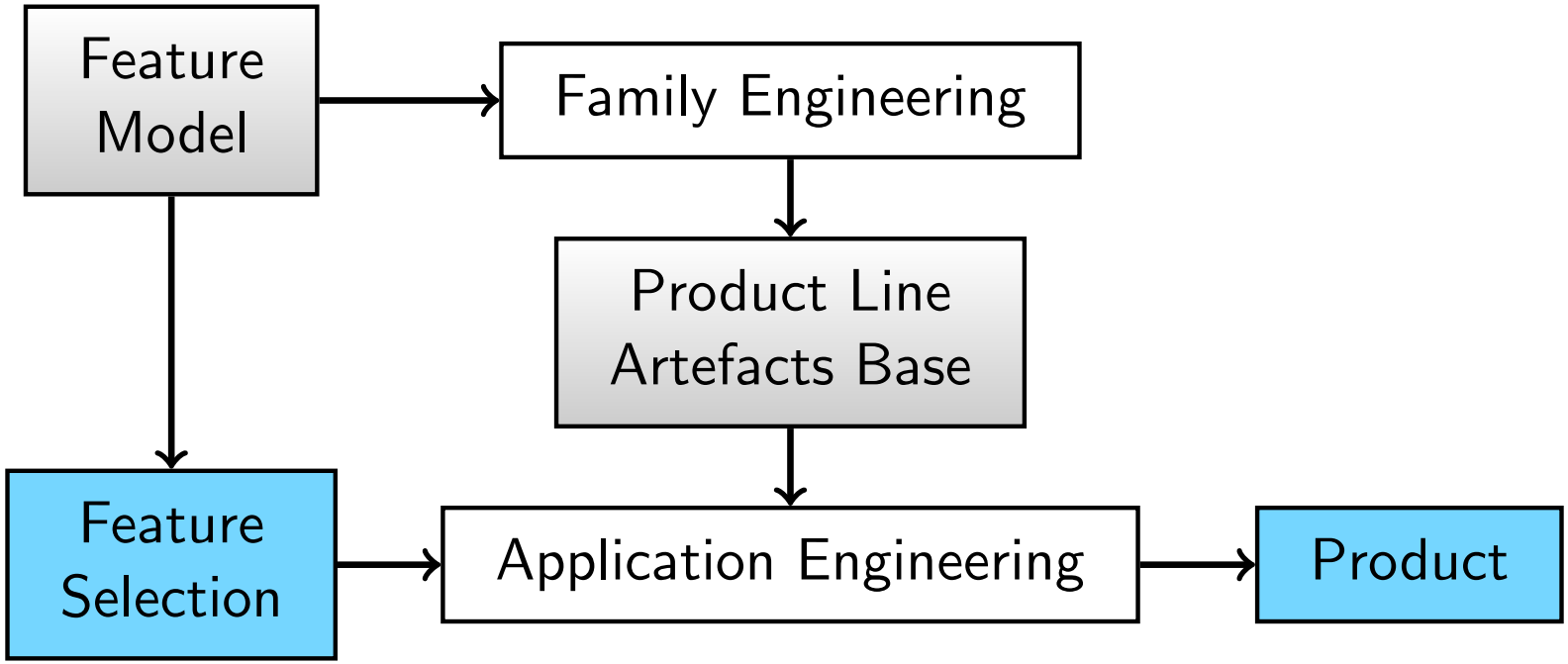
Vision: A Single-Source Technology for Highly Adaptive, Concurrent Software Systems



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

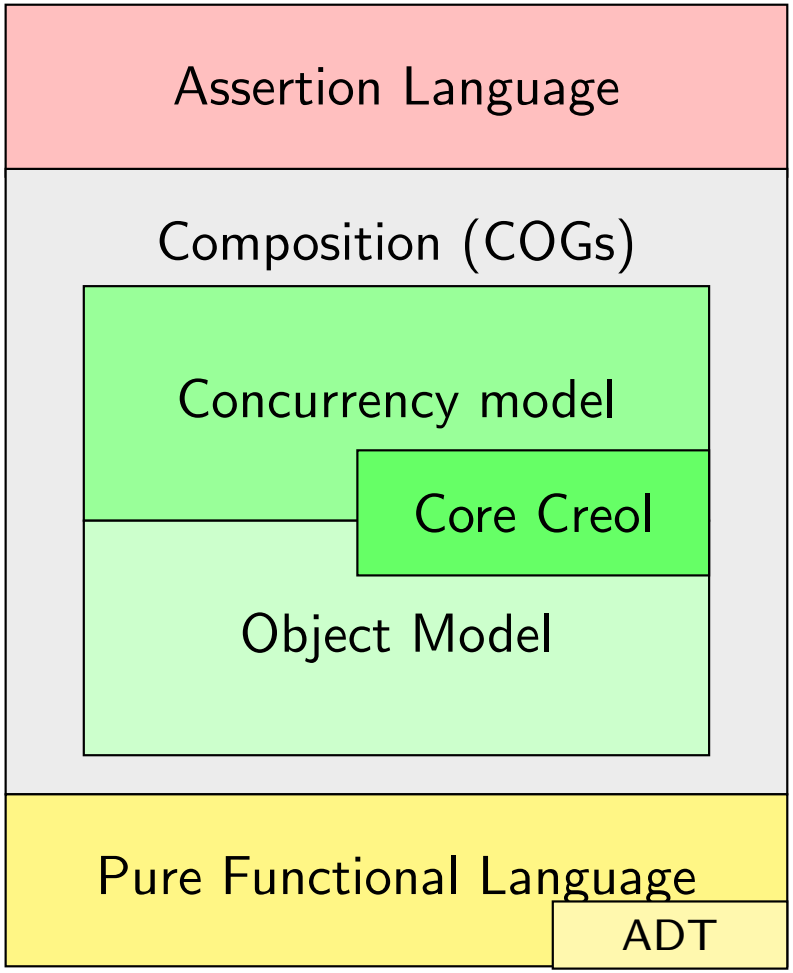
Develop analysis methods in tandem with ABS language

- Incrementality
  - Delta modeling, delta specification, delta verification
- Compositionality
  - Concurrency model
  - Proof systems

Important Project Principles (III)

Early evaluation

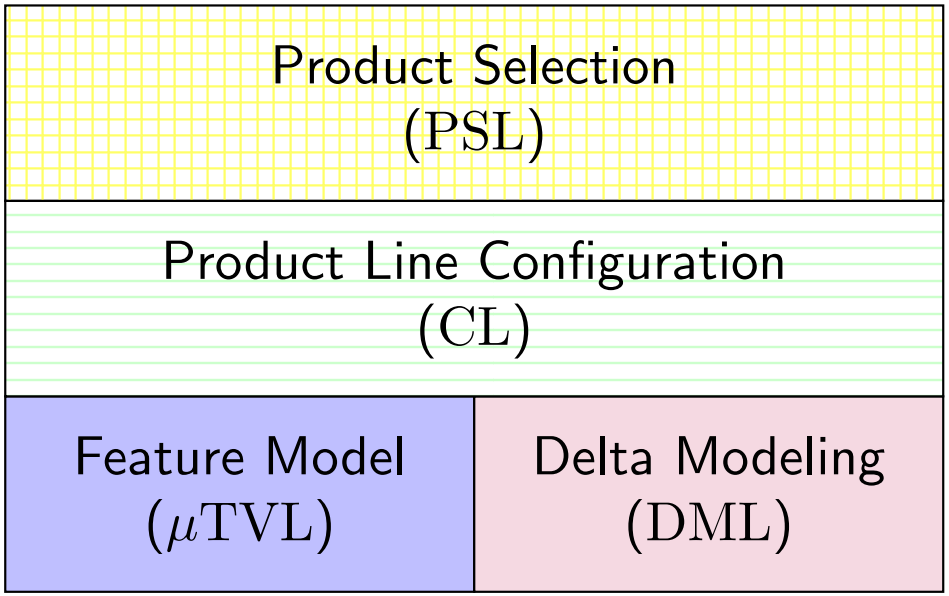
- Develop Core ABS first

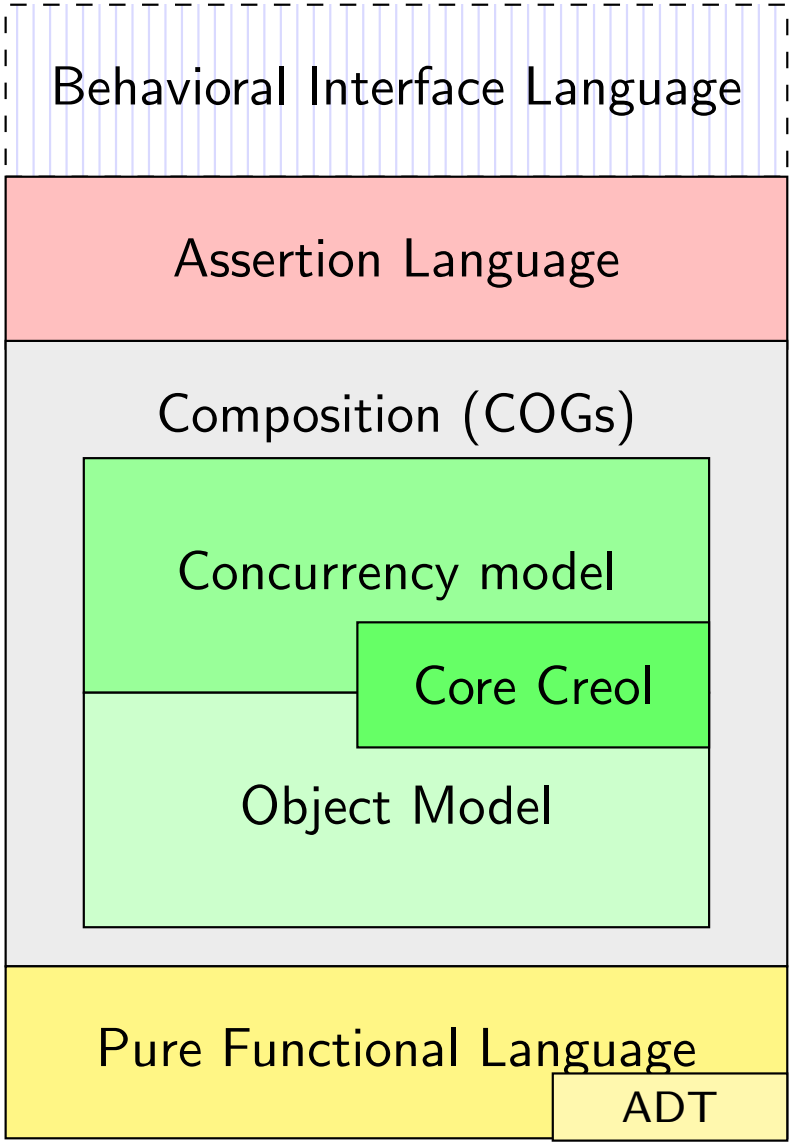


Important Project Principles (III)

Early evaluation

- Develop Core ABS first
- Layered language design

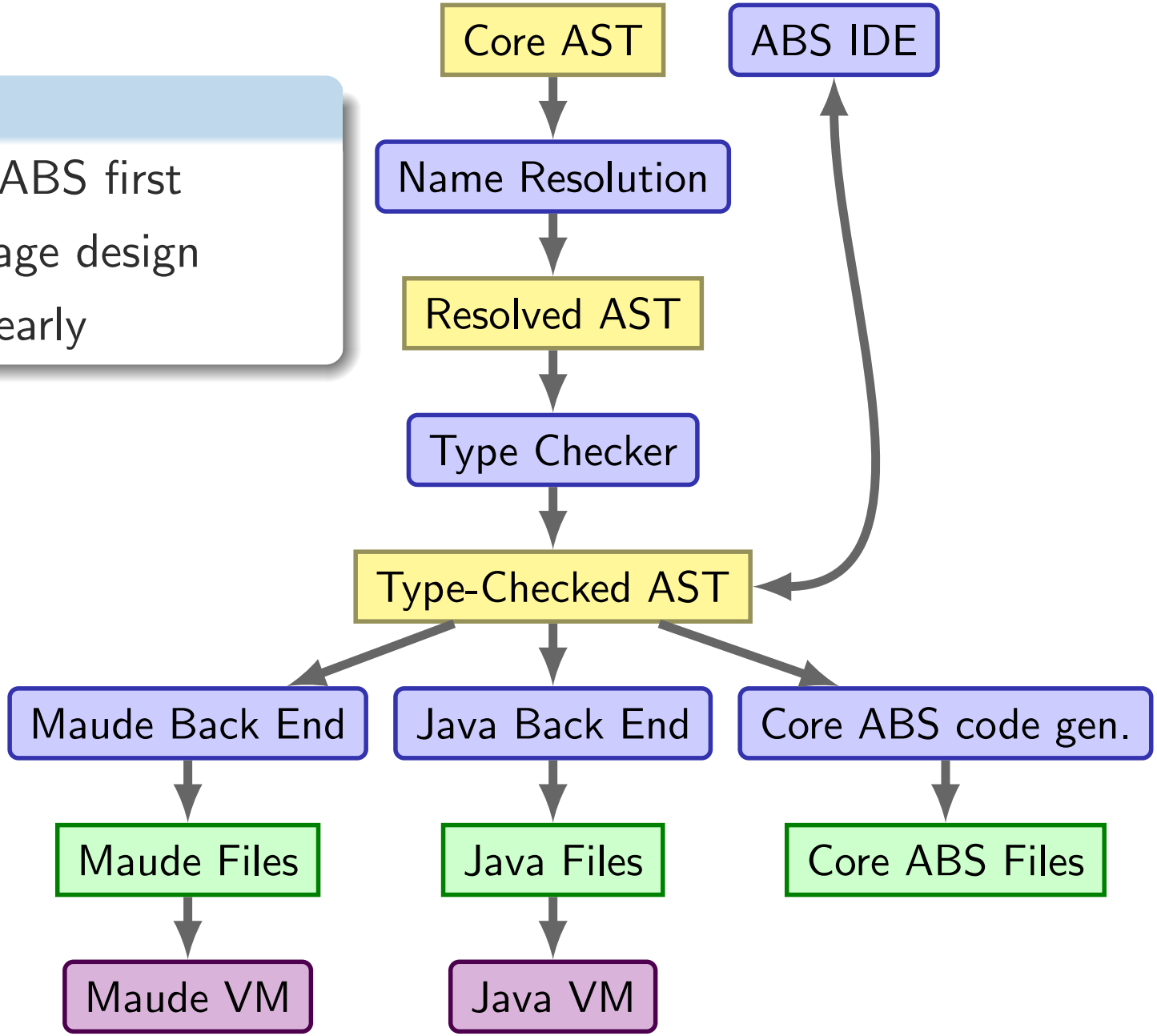




Important Project Principles (III)

Early evaluation

- Develop Core ABS first
- Layered language design
- Provide tools early



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

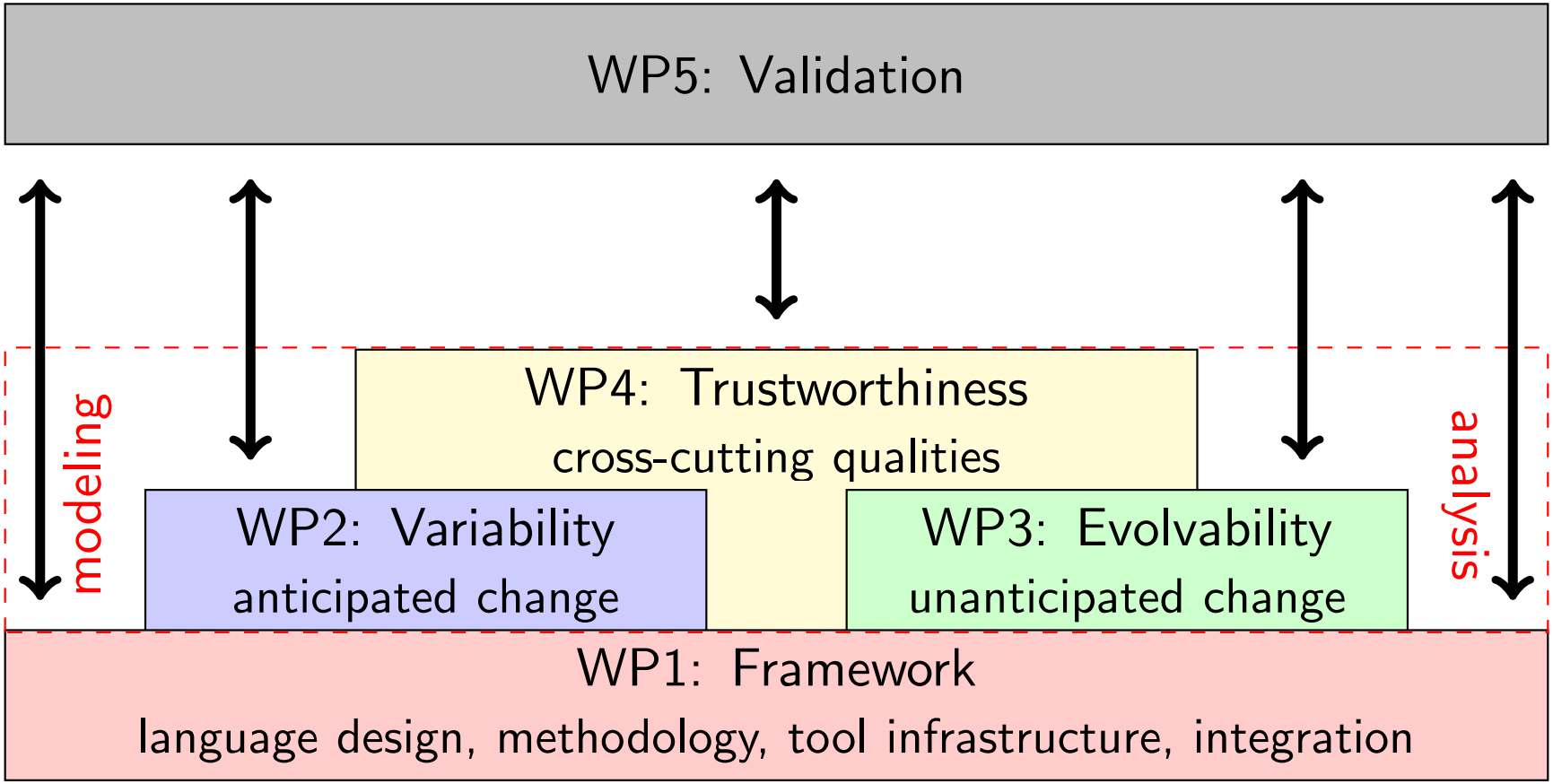
Scalable technologies developed in tandem with ABS

- 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



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:
- Preparation meeting 23rd March 2011
- Went very well (in particular, tool demo was convincing) ...

Second Annual Project Review: Recommendations (excerpt)

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. Need to ensure a continuous quality of the research in the areas where Ina Schaefer was leading the work.
8. Presentation improvements to deliverables/periodic report.

All deliverables in second reporting period (PM13–24) accepted w/o changes!

Active/Upcoming Work Tasks

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

Active/Upcoming Work Tasks Cont'd

WP3: Evolvability (KTH)

3.2 NR, PM 18–36 Model Mining

3.3 KUL, PM 24–42 Hybrid Analysis for Evolvability

3.5 KTH, PM 24–48 Autonomously Evolving Systems

WP4: Trustworthiness (UPM)

4.1 UPM, PM 12–36 Security

4.3 BOL, PM 24–28 Correctness

4.4 FRG, PM 30–42 Auto Configuration and Quality Variability

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 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

Past Deliverables

Del. No.	Deliverable name	WP No.	Lead Beneficiary	PMs	Type	Dissemination level	Deliv. date PM
7.2.a	Bi-Annual Management Report	7	CTH	4	R	PU	6, 12, 18, 24, 30
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
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 selection 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

Upcoming Deliverables (Including IoC Effort)

Del. No.	Deliverable name	WP No.	Lead Bene-ficiary	PMs	Type	Dissemi-nation level	Deliv. date PM
2.1	Configuration deployment	2	UIO	35	R	PU	24
2.3	Debugging, Visualisation , and test generation	2	CTH	36	R	PU	24
2.4	Types for variability	2	BOL	21	R	PU	24
3.2	Model Mining	3	NR	45	R	PU	24
4.1	Security	4	UPM	21	R	PU	24
5.3	Evaluation of Modeling	5	CWI	19	R	PU	24

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 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 4.3 Meeting on Abstract/Specification Languages, 11th July 2011, Bologna

- 12 participants from BOL, CTH, CWI, IoC, UKL
- Developing a specification language for ABS

WT 3.5 Autonomously Evolving Systems, 27 June 2011, Kaiserslautern

- 6 participants from UKL, KTH, FRG
- Kick-Off Meeting

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

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

Summary: Main Results and Achievements

- 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