DEPLOY Integrated Project

Deployment of advances engineering methods for high productivity and dependability in European industry

http://www.deploy-project.eu/

Alexander Romanovsky

Newcastle University, UK

November, 2008

Newcastle University
Åbo Akademi University
BOSCH
cetic Your connection to ICT research
CLEARSY SYSTEM ENGINEERING
ETH Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich
HEINRICH HEINE UNIVERSITÄT DÜSSELDORF
NOKIA
SAP
SIEMENS
UNIVERSITY OF Southampton
SPACE SYSTEMS FINLAND
Systerel

Information

- ICT FP7, call 1, Strategic Objective ICT-2007.1.2: Service and Software Architectures, Infrastructures and Engineering
- February 2008 - January 2012
- www.deploy-project.eu
- DEPLOY Interest Group
- FP6 STREP RODIN project (2004-2007) on creating a rigorous open development environment for complex systems rodin.cs.ncl.ac.uk
- www.event-b.org - an open-source extendable Eclipse development environment, called the *RODIN platform*

Challenges

- Increasing dependence of our society on critical systems
- Dealing with complexity of software-intensive systems
- Building highly dependable systems and assuring that they are correct, trustworthy and resilient
- Understanding and justifying the role of advanced formal engineering methods
- Industrial deployment of the existing advanced methods and supporting tools

Formal Methods

B

ation de la méthode B développée

CLEARSY
SYSTEM ENGINEERING

ALSTOM

SIEMENS

ATELIER B Projets ferroviaires
Avril 2007

DEPLOY Philosophy

- Mastering complexity through **rigorous stepwise development**
- Systems should be designed by **modellers and architects**
- Ensuring **dependability** through rigorous system development
- Use of **advanced engineering** methods supported by the tools
  - System level modelling at multiple levels of abstraction
  - Importance of proof
  - Strong incremental tool support
- Deploy a **professional scalable development** environment

DEPLOY Objectives

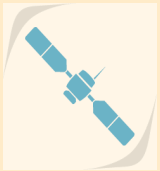
- The **overall aim** is to make major advances in engineering methods for dependable systems through the deployment of formal engineering methods
- DEPLOY aims to really help **European industry** and to support efficient development of real-scale systems
- Drivers
  - achieving and evaluating industrial **take-up** of the DEPLOY methods and tools
  - necessary **further research** on methods and tools
- Demonstrate improvements in system **dependability** and **productivity**
  - by reducing test-debug-rework and facilitating reuse

Industrial Deployment Partners

The industrial deployment will be in five sectors

- automotive
- rail transportation
- space systems
- business information
- pervasive telecoms





Technology Providers

- Newcastle University (Coordinator)
- Aabo Akademi University
- ETH Zurich
- Heinrich-Heine Universität Düsseldorf
- University of Southampton
- Systerel (FR)
- CETIC (BE)
- ClearSy (FR)

Method

- stepwise development based on model refinement, exemplified by Event B
- combined with the use of a number of other modelling techniques
  - UML
  - CSP
  - π-calculus
  - B

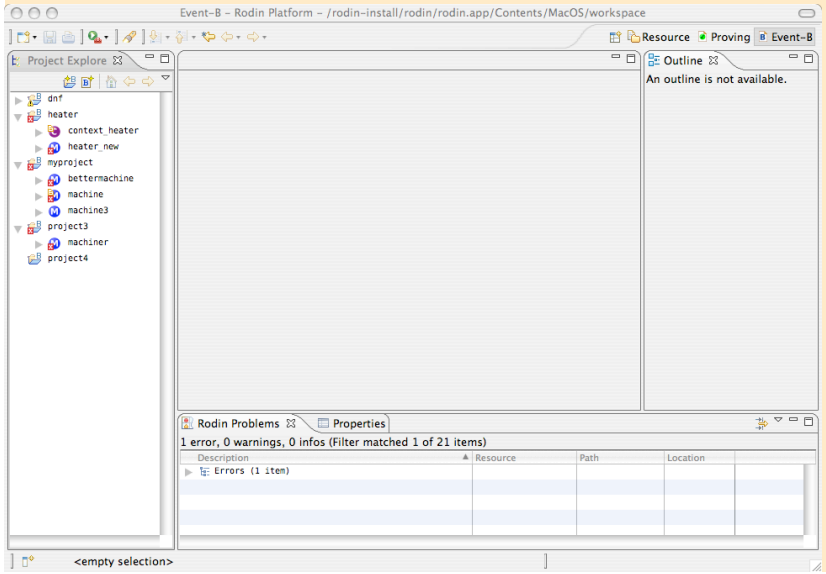
Achieving and demonstrating dependability

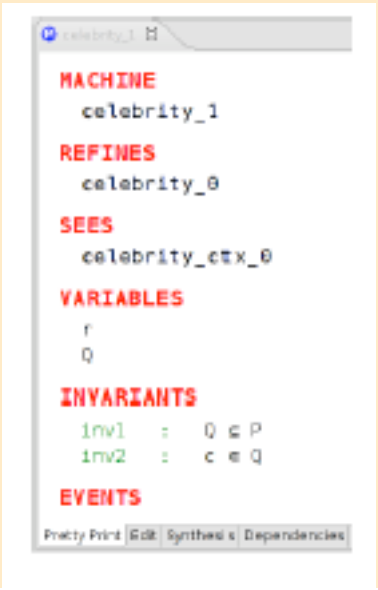
Design for resilience

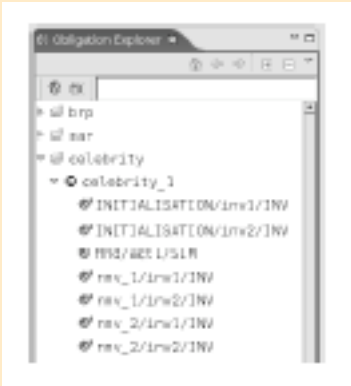
- 4 strands of work:
  - Specifying fault tolerance (deriving specification)
  - Resilience (methods and models)
  - Security (building correct secure systems)
  - Stochastic reasoning about reliability and safety

The RODIN platform

- Eclipse environment for Event B development
- Extandable with **plugins**: UML, animation, model-checking, π-calculus/mobily modelling, CSP, B, requirement tracing, pattern support, model testing, documentation, debugging, composition/decomposition, …
- Several provers (cross verification)
- Open source, openly available



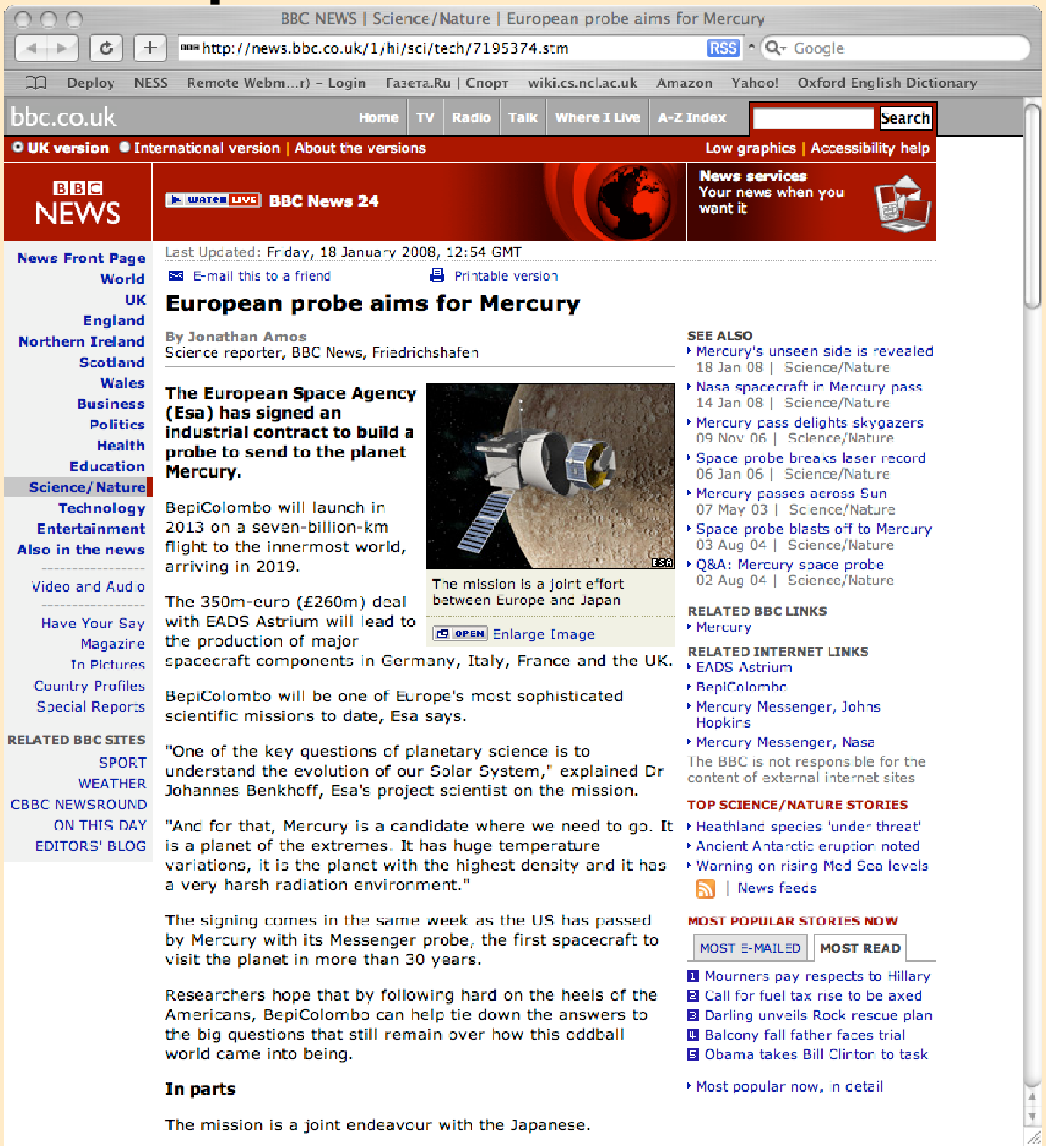




Expected Results

- ***Real industrial deployment***
- Each deployment partner will become ***self sufficient***
- DEPLOY will provide ***scientifically valuable artefacts***
- ***Thorough assessment*** of formal engineering methods
- ***Research advances*** in complex systems engineering methods
- ***A professional open development platform*** based on Eclipse
- ***Strategies*** for ***integration*** of formal methods and tools with existing ***sector-specific*** development processes
- An ***organisation*** which will be the home of the open platform
- A ***body*** made of industrial users and technology providers
- ***Training material and courses***

Expected Results



BBC NEWS | Science/Nature | European probe aims for Mercury

http://news.bbc.co.uk/1/hi/sci/tech/7195374.stm

bbc.co.uk | Home | TV | Radio | Talk | Where I Live | A-Z Index | Search

UK version | International version | About the versions | Low graphics | Accessibility help

BBC NEWS | WATCH LIVE BBC News 24 | News services Your news when you want it

News Front Page | World | UK | England | Northern Ireland | Scotland | Wales | Business | Politics | Health | Education | Science/Nature | Technology | Entertainment | Also in the news | Video and Audio | Have Your Say | Magazine | In Pictures | Country Profiles | Special Reports

RELATED BBC SITES: SPORT | WEATHER | CBBC NEWSROUND | ON THIS DAY | EDITORS' BLOG

Last Updated: Friday, 18 January 2008, 12:54 GMT

E-mail this to a friend | Printable version

European probe aims for Mercury

By Jonathan Amos
Science reporter, BBC News, Friedrichshafen

The European Space Agency (Esa) has signed an industrial contract to build a probe to send to the planet Mercury.

BepiColombo will launch in 2013 on a seven-billion-km flight to the innermost world, arriving in 2019.

The 350m-euro (£260m) deal with EADS Astrium will lead to the production of major spacecraft components in Germany, Italy, France and the UK.

The mission is a joint effort between Europe and Japan

OPEN Enlarge Image

BepiColombo will be one of Europe's most sophisticated scientific missions to date, Esa says.

"One of the key questions of planetary science is to understand the evolution of our Solar System," explained Dr Johannes Benkhoff, Esa's project scientist on the mission.

"And for that, Mercury is a candidate where we need to go. It is a planet of the extremes. It has huge temperature variations, it is the planet with the highest density and it has a very harsh radiation environment."

The signing comes in the same week as the US has passed by Mercury with its Messenger probe, the first spacecraft to visit the planet in more than 30 years.

Researchers hope that by following hard on the heels of the Americans, BepiColombo can help tie down the answers to the big questions that still remain over how this oddball world came into being.

In parts

The mission is a joint endeavour with the Japanese.

SEE ALSO
- Mercury's unseen side is revealed 18 Jan 08 | Science/Nature
- Nasa spacecraft in Mercury pass 14 Jan 08 | Science/Nature
- Mercury pass delights skygazers 09 Nov 06 | Science/Nature
- Space probe breaks laser record 06 Jan 06 | Science/Nature
- Mercury passes across Sun 07 May 03 | Science/Nature
- Space probe blasts off to Mercury 03 Aug 04 | Science/Nature
- Q&A: Mercury space probe 02 Aug 04 | Science/Nature

RELATED BBC LINKS
- Mercury

RELATED INTERNET LINKS
- EADS Astrium
- BepiColombo
- Mercury Messenger, Johns Hopkins
- Mercury Messenger, Nasa

The BBC is not responsible for the content of external internet sites

TOP SCIENCE/NATURE STORIES
- Heathland species 'under threat'
- Ancient Antarctic eruption noted
- Warning on rising Med Sea levels

News feeds

MOST POPULAR STORIES NOW

MOST E-MAILED | MOST READ

1. Mourners pay respects to Hillary
2. Call for fuel tax rise to be axed
3. Darling unveils Rock rescue plan
4. Balcony fall father faces trial
5. Obama takes Bill Clinton to task

Most popular now, in detail

Where we are now (month 10)

- A series of kickoff meetings (plenary, tools & methods, …)
- Block training course for the industrial engineers
- Kick-off meetings organised by the deployment industrial partners: research and tooling issues identified and coordination plans built
- Minipilots developed and analysed
- Ongoing work on the medium-scale pilots (focusing on reqs and early architectural design)
- First feedback to method and tool developers is received

Where we are now (month 10)

- Fault tolerance:
  - tracing fault tolerance requirements
  - developing a library of fault tolerance refinement patterns
  - modelling fault tolerance middleware
  - formal specification of the fault assumptions about the system environment
  - integration structuring mechanisms (e.g. scopes and roles) using stepwise refinement
- DEPLOY interest group is operational
- Event-B and Platform wiki is fully operational
- First dissemination evens have been organised: France, Turkey, Brazil