Formal Methods for SOA and Internet of the Future

Michael Leuschel
University of Düsseldorf

Michael Butler, Univ. of Southampton
Thierry Lecomte, ClearSy
Formal methods: a history

1960 Hoare's Elliot Brothers Algol 60 compiler
1959 Backus-Naur Form FM for languages
1949 Alan Turing paper on programming
1947-48 Von Neumann and Goldstine propose six-step programming process, starting with conceptualising the problem mathematically
1970 Clear in US
1973 IBM's VDM by Cliff Jones
1979 STC formal design methods symposium at Cambridge
1978 Hoare's CSP
1980 Formal semantics of Ada
1983 Spark for Ada
1985 Raise Esprit
1996 Formal definition of B; VDM ISO standard
2002 Z ISO standard
NATS pioneers biggest ATC advance since radar

A set of computer-based predictive tools developed by NATS will trigger the biggest change in Air Traffic Control since the introduction of radar.

iFACTS – Interim Future Area Control Tools Support – will further improve safety and provide Controllers with a set of advanced support tools, which will enable them to increase the amount of traffic they can comfortably handle. In trials, the system has delivered significant capacity increases.

NATS, the UK’s leading air traffic services provider, has pioneered research and development of advanced air traffic control tools for several years from its simulator and research centre at Hurn. The iFACTS project will deliver a subset of these tools onto the system at the company’s main en-route Control Centre at Swanwick in Hampshire.

“This is one of the most exciting developments in the aviation industry in decades and we’re now very close indeed to introducing it,” said Paul Barron, NATS’ Chief Executive.

As well as giving us the tools to increase capacity at the rate our customers tell
Praxis appointed to work on the biggest change in air traffic control systems since the introduction of radar

Praxis, a leading specialist in critical systems engineering has been appointed by National Air Traffic Services (NATS) to work on a £10 million Air Traffic Control (ATC) partnering contract. Praxis will write the specification and develop the software for a new ATC System called iFACTS which will trigger the biggest change in ATC since the introduction of radar.
Example: Canarsie 2006

- New York Line L
- Mixed-Mode of Operation 24/7
- 273,000 Lines of B
  - 110,000 Lines automatically generated
- 82,500 Proof Obligations

Source Siemens, [B07]
• 17,88 MIO EUR 4-Year Project

• Started February 2008

• Deployment of Formal Methods (Event-B) in Industry

www.deploy-project.eu
Key Ingredients

- Open Platform based on Eclipse
- scalable tools & methodologies
- Real Deployment in Industry
- Existing FM Users (Siemens, Systerel, ClearSy)
- New Areas (Bosch, SAP, SSF, ...)
- Training & Measurement
DEPLOY Goals

• Understand and justify the role of formal engineering methods in building dependable systems
• Address the barriers to deploying formal engineering methods in industry
• Achieve deployment of formal engineering methods
• Scale and professionalise Rodin technology
  – Rodin: Eclipse-based toolset (RODIN FP6)
Industrial deployment partners

The industrial deployment will be in major sectors

• Bosch: automotive
• Siemens: rail transportation
• Space Systems Finland: space systems
• SAP: business information
Technology providers

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

• **Training** of the engineers involved in the deployment
• Close **integration** of methods into company development processes
• Devoting significant resources to early development phases
• Define and collect of the **metrics** for evaluation of productivity and dependability
• Ensuring **resilience** and **security** by application of the appropriate development patterns
• Provision of **expert support** in deployment of advanced engineering technologies and in analysis of results
Activities to date

• Training of industrial engineers
• Commence work on pilot projects
  – Siemens: Trainguard system
  – Bosch: cruise control
  – SAP: B2B service engineering
  – SSF: BepiColombo (Mercury) instrument SW
• Roadmap for Rodin Toolset
• Identification of research challenges:
  – requirements traceability, reuse,
  – dependability, security

22 Sept 08
Rodin Open Tool Platform

• Extension of Eclipse IDE (Java based)
• Supports Event-B formal method
• Rodin Eclipse Builder manages:
  – Consistency/refinement PO generator
  – Proof manager
  – Propagation of changes
• Plug-ins:
  – UML-B, ProB, AnimB, Brama, …
Working Group

- Formal Methods for
- Service-Oriented Architectures &
- Internet of the Future

- (but we are open to other applications of formal methods !)
Purpose

• Why are some projects using FM and others not?

• Identify
  • Positive & Negative experiences
  • Opportunities & Obstacles
  • Added value

• Role of FM in Internet of the Future
Other WG FM Participants

- COMPAS: Compliance-driven Models, Languages, and Architectures for Services
- ProTEST: methods and tools to support property-based development of systems
- GRID4ALL
- GREDIA
- SmartLM
- XtreemOS, GridTrust, SIMS, Alive, Irmos
Objective 1: Workshop

- 16th of February 2009 in Düsseldorf
- Co-located with Integrated Formal Methods conference iFM 2009
Other Objectives

• Springer Book
  • Lead: John Derrick, ProTest
• Project Proposal for Call 5?
• Further details to be discussed at Workshop
Wiki

Interested?

- Michael Leuschel
  leuschel@cs.uni-duesseldorf.de

www.deploy-project.eu