Information Society Technologies

RODIN
Rigorous Open Development Environment for Complex Systems

Specific Targeted Research Project , EU IST FP6

Brian Randell (on behalf of Sascha Romanovsky)
University of Newcastle upon Tyne, UK

Participants

University of Newcastle upon Tyne, UK (Coordinator) - Sascha Romanovsky

Aabo Akademi University, Turku, Finland - Kaisa Sere

ClearSy System Engineering, France - Thierry Lecomte

Nokia Corporation, Finland - Colin Willcock

Praxis Critical Systems Ltd, UK - Adrian Hilton

VT Engine Controls Ltd, UK - John Brightman

Swiss Federal Institute of Technology, Zurich, Switzerland - Jean-Raymond Abrial

University of Southampton, UK - Michael Butler

***Start**: September 1, 2004*
***End**: August 31, 2007*
***Total cost:** 4,397,850.00 Euros*
***EC contribution:** 3,171,000.00 Euros*

***Web site:** rodin.cs.ncl.ac.uk*

Industrial Interest Group

Adelard, UK
Alstom Transportation, France
AWE Aldermaston, UK
DGA, France
Escher Technologies, UK
Gemplus, France
IBM UK
I.C.C.C. Group, Czech Republic
QinetiQ, UK
RATP, France
STMicroelectronics, France
VTT, Finland

Objectives

The overall objective is the creation of a methodology and supporting open tool platform for the cost-effective rigorous development of dependable complex software systems and services

Main Advances aimed for in:

- Formal Design Methods

- Fault Tolerance

- Design Abstractions

- Tool platform

Formal Design Methods.

Mastering complexity requires design techniques that support clear thinking and rigorous validation and verification. **Formal design** methods do so.

Fault Tolerance.

Coping with complexity also requires architectures that are tolerant of faults and unpredictable changes in environment. This is addressed by **fault tolerance** design techniques.

Dependability consideration should start from the early stages of system development.

The aim is to deal with faults in the system environment, faults of the individual components, and component mismatches, as well as errors affecting several interacting components.

Design Abstractions.

We will tackle complex architectures: our systems approach will support the construction of appropriate **abstractions** and provide techniques for their structured refinement and decomposition.

Tool platform.

Tool support for construction, manipulation and analysis of models is crucial and we will concentrate on a comprehensive **tool platform** which is openly available and openly extendable and has the potential to set a European standard for industrial formal method tools.

Workpackages:

WP1. Research drivers (case studies)

WP2. Methodology

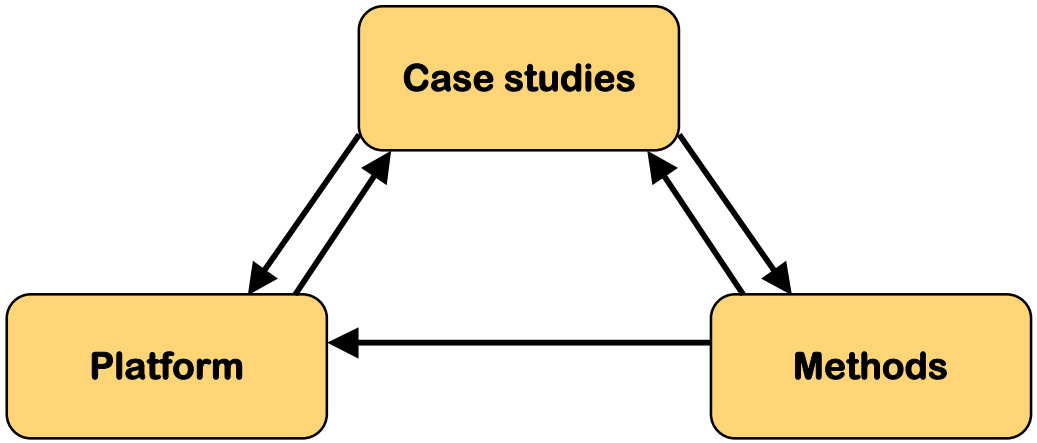
WP3. Open tool kernel

WP4. Modelling and verification plug-ins

WP5. Dissemination and exploitation

WP6. Project management

WP7. Project review and assessment



WP1. Research drivers

The methods and platform will be validated and assessed through industrial case studies:

Case study 1: Formal Approaches to Protocol Engineering (Nokia)

Case study 2: Engine Failure Management System (VT Engine Controls)

Case study 3: Formal Techniques within an MDA Context (Nokia)

Case study 4: CDIS Air Traffic Control Display System (Praxis)

Case study 5: Ambient Campus (U. of Newcastle)

WP2. Methodology

To produce the RODIN methodology for rigorous development of complex systems.

To make advances in the basic research areas related to formal system modelling and mapping of models, software reuse, and formal reasoning about system fault tolerance, reconfiguration, mobility and adaptivity.

This includes development of templates for fault tolerant design methods (exception handling, atomic actions, compensation), as well as for reconfigurability, adaptivity and mobility.

WP3. Open tool kernel

To develop a set of *basic kernel tools* implemented on a certain *platform container* that can be extended by the *plug-ins* being developed in WP4.

Openness of the platform is the prime aim.

Generality of the platform.

Based on the use of *Eclipse*.

WP4. Modelling and verification plug-ins

To develop a range of tools to support the application of the RODIN methodology being developed in WP2.

1. **Linking UML and B**
2. **Petri net-based model checking**
3. **Constraint-based model checking and animation**
4. **Model-based testing**
5. **Code Generation**

Novel Aspects

- pursuit of a systems approach
- combination of formal methods with fault tolerance techniques
- development of formal method support for component reuse and composition
- provision of an open and extensible tools platform for formal development

Expected Project Results

A collection of reusable development templates (models, architectures, proofs, components, etc.) produced by the case studies

A set of guidelines on a systems approach to the rigorous development of complex systems, including design abstractions for fault tolerance and guidelines on model mapping, architectural design and model decomposition

An open tool kernel supporting extensibility of the underlying formalism and integration of tool plug-ins

A collection of plug-in tools for model construction, model simulation, model checking, verification, testing and code generation

RODIN Presentations to date

I. Johnson, C. Snook, A. Edmunds & M. Butler
Rigorous development of reusable, domain-specific components, for complex applications.
CSDUML'04 - 3rd International Workshop on Critical Systems Development with UML, October 2004, Lisbon

C. Schröter, V. Khomenko.
Parallel LTL-X Model Checking of High-Level Petri Nets Based on Unfoldings.
Proc. CAV'2004, Alur, R. and Peled, D.A. (Eds.). Springer-Verlag, Lecture Notes in Computer Science 3114. 2004. pp. 109-121.

Relevant Prior Publications

J.-R. Abrial. *The B-Book: Assigning programs to meanings*. Cambridge University Press,.1996.

A. Avizienis, J.-C. Laprie, C. Landwehr, B. Randell. Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Trans. on Dependable and Secure Computing*. 1, 1, 2004.

M. J. Butler. Stepwise Refinement of Communicating Systems. *Science of Computer Programming*, 27, 1996.

M.C. Gaudel, V. Issarny, C. Jones, H. Kopetz, E. Marsden, N. Moffat, M. Paulitsch, D. Powell, B. Randell, A. Romanovsky, R.J. Stroud, F. Taiani. *Final Version of DSoS Conceptual Model (CSDA1).* CS-TR: 782, School of Computing Science, University of Newcastle, July 2003.

C. Jones, A formal basis for some dependability notions. In *Proceedings of the 10th Anniversary Colloquium of UNU/IIST Formal Methods at the Crossroads: From Panacea to Foundational Support,* Lisbon, Portugal, 2002 Aichernig, B.K. and Maibaum, T. (Eds.) LNCS 2757. 2003.

C. Jones. *Systematic Software Development using VDM*. 1990.

M. Leuschel, M. Butler. ProB: A Model-Checker for B. *Proc. FM 2003: 12th Intl. FME Symposium*. Pisa, September, LNCS 2805, 2003.

A. Romanovsky, C. Dony, J.L. Knudsen, A. Tripathi (Eds.). Advances in Exception Handling Techniques, *LNCS-2022*, 2001.

K. Sere, E. Troubitsyna. Safety Analysis in Formal Specification. In J. Wing, J. Woodcock, J. Davies (Eds.), *FM'99 - Formal Methods. Proc. of World Congress on Formal Methods in the Development of Computing Systems*, Toulouse, France, LNCS 1709, 1999.

Since September 2004

Kick-off meeting:

October 4-6, 2004. Newcastle upon Tyne

Work to date:

- Defining the evaluation criteria and traceable requirements documents for the case studies

- Making final decisions on RODIN platform architecture

- Finalising Event B language