Advanced Design and Verification Environment for Cyber-physical System Engineering

FP7 Information and Communication Technologies (ICT) Programme

Small or Medium-scale Focused Research Project (STREP) Proposal

Challenge 3: Alternative Paths to Components and Systems

Strategic Objective IST-2011.3.3 New Paradigms for Embedded Systems, Monitoring and Control towards Complex Systems Engineering

Coordinator:	John Colley
Coordinator organisation:	Southampton University
Coordinator email:	j.l.colley@ecs.soton.ac.uk
Coordinator fax:	+44 (0)23 8059 3045
Date of preparation:	June 15, 2011
Version:	5.0 (Abridged September 9, 2011)

List of participants:

Participant no. *	Participant organisation name	Part. short name	Country
1 (coordinator)	University of Southampton	SOUTHAMPTON	UK
2	Alstom Transport Information Solutions	AT	France
3	Systerel	SYSTEREL	France
4	University of Düsseldorf	UDUS	Germany
5	Critical Software Technologies Ltd	CSWT	UK

Summary of the ADVANCE Proposal

ADVANCE Goals: The overall objective of the ADVANCE project is the development of a *unified* tool-based framework for automated formal verification and simulation-based validation of cyber-physical systems. Unification will be achieved through the use of a common formal modelling language supported by methods and tools for simulation and formal verification. An integrated tool environment will provide support for construction, verification and simulation of models. The delivered methods and tools will overcome significant deficiencies in current practices in cyber-physical systems engineering that make verification and validation hugely costly and time consuming. The unified methods and tools framework will reduce the bottleneck in verification and validation of cyber-physical systems engineering.

ADVANCE Structure: The ADVANCE consortium consists of five strong and complementary partners representing a combination of leading European industrial players in systems engineering along with academic partners with internationally leading expertise in formal verification and simulation tools. Systerel together with the Universities of Düsseldorf and Southampton will lead the development of novel methods and tools while Alstom Transport Information Solutions and Critical Software Technologies Ltd will apply the resulting methods and tools to the engineering of intelligent transport and energy systems. We have identified an exciting opportunity to tackle several dimensions of the design space in a unified way by exploiting recent advances in technology for high-level formal modelling. In particular, we will build on an existing formal modelling language – Event-B – and its associated tools environment – Rodin – with strong support for formal verification; Rodin will be further strengthened and augmented with novel approaches to multi-simulation and testing. Building on Event-B and Rodin will allow us to make considerable progress within the period of the ADVANCE project.

ADVANCE Impact: Current engineering practices mean that designing cyber-physical systems to high assurance levels is hugely costly. It is widely recognised in industry and government that development costs will become prohibitive for future systems unless there are significant improvements in the methods and tools used for systems engineering. Significant advances in methods and tools to support validation and verification are required to address this potential bottleneck. The ADVANCE project will deliver methods and tools for formal modelling, verification and validation that will address this gap in existing engineering practice. The major impact of the ADVANCE methods and tools will be to reduce the cost associated with formal modelling and verification while increasing the benefits obtained. This will provide a competitive edge to European systems engineering companies allowing them to further strengthen the leading position of Europe in development of high quality embedded systems. The ADVANCE project is unique in addressing both simulation and formal verification within a single framework. Existing industrial users of Event-B and Rodin external to ADVANCE will serve as a strong basis for external dissemination and exploitation of the ADVANCE results.

Table of Contents

B.1 Scientific and technical concepts and work plan

B.1.1 Concept and objectives

In this section, the motivation for the ADVANCE Project is introduced. The conceptual framework for ADVANCE is outlined which in turn leads to a definition of the ADVANCE scientific and technological goals and to the definition of the measurable outcomes of ADVANCE. Section B.1.1 concludes by outlining the strong fit between the ADVANCE goals and the goals of Objective IST-2011.3.3 *New Paradigms for Embedded Systems, Monitoring and Control towards Complex Systems Engineering*[1].

B.1.1.1 Motivation for ADVANCE

Cyber-physical systems are integrations of computing and physical mechanisms engineered to provide physical services including transportation, energy distribution, manufacturing, medical care and management of critical infrastructure. Embedded monitoring and control represent well-established forms of cyber-physical systems. Increased use of networked and intelligent computing – in areas such as automated train systems, smart grid management, vehicle swarms, environmental monitoring and air-traffic management – means that the complexity of cyber-physical systems is growing dramatically.

As highlighted by a recent US Government report[2], the complexity inherent in cyber-physical systems place huge demands on the methods and tools required to engineer such systems. Cyber-physical systems are typically safety-critical which means that they need to be engineered to high assurance levels and strong evidence of assurance is required for certification. Current engineering practices mean that designing systems to high assurance levels is hugely costly; it is clear that development costs will become prohibitive for future systems unless there are significant improvements in the methods and tools used for cyber-physical systems engineering[2].

Cyber–physical systems are systems-of-systems consisting of integrations of communication, electronic, mechanical, power and software systems. The designers of cyber-physical systems need to deal with multiple design constraints including functional and safety goals for integrations of truly heterogeneous components, timing constraints, networking constraints, and dynamic and uncertain environmental constraints. Modelling in a variety of forms plays a central role in tackling these design dimensions. Software verification relies on models such as test sets and formal models against which to verify designs and implementation. Testing is the most common verification technique but formal verification tools (model-checking and automated theorem proving) also play a role and that role is increasing especially for critical applications. Simulation models of planned physical systems play a vital role in identifying and validating requirements and constraints on embedded software in early stages of development. Safety validation relies on models for analysing hazards and providing safety cases.

Although engineering methods exist for tackling individual dimensions of the design space – environment simulation, software validation, software verification, hardware verification, safety analysis, etc – it is currently very difficult to combine these within a single design environment. This is caused by a lack of uniformity in modelling methods and adds greatly to engineering costs. Construction of different kinds of models for different purposes is expensive in itself while ensuring consistency between different kinds of models adds to the costs. Indeed software is itself a form of model and its construction and verification against test sets and formal models is a major development cost.

Besides the lack of uniformity, a further problem both with ***validation*** (ensuring that the system specifications are appropriate) and ***verification*** (ensuring the implemented system satisfies its specifications) is that they tend to be performed quite late in the development lifecycle. The consequence of this is that the inevitable design problems, once identified, are expensive to fix. It also means that it is difficult to exploit commonalities in design, verification, safety assurance and optimisation across variants of product families since the analysis tends to be very solution-specific. Improved design support for product families is essential for achieving productivity improvements.

B.1.1.2 The ADVANCE Concept

The essential concept of the ADVANCE proposal is the key role played by ***modelling*** in cyber-physical systems engineering. Modelling should be used at all stages of the development process from requirements analysis to system acceptance testing. Modelling is *not* performed after the fact to verify implementations; it is used from the earliest stages of development to help engineers ***construct*** and ***organise*** the requirements, functionality and architecture of complex systems in ***coherent*** and ***tractable*** ways. Cyber-physical systems engineering involves technical coordination between large teams, including coordination between different engineering disciplines such as software, electronic, electrical and mechanical engineering; modelling serves as the ***technical***

coordination mechanism between teams and disciplines. Modelling serves as the core basis for final ***acceptance*** of systems as being fit for purpose.
The experience of this consortium is that most benefit is achieved from taking a ***formal modelling*** approach supported by strong ***formal verification*** tools. Formal modelling and verification lead to deeper understanding and higher consistency of specification and design than informal or semi-formal methods. In order to manage the complexity inherent in cyber-physical systems, our experience is that ***composition***, ***decomposition*** and ***refinement*** of formal models are key methods for structuring the formal modelling effort since they support separation of concerns and layered reasoning. A refinement approach means that models and compositions of models represent different ***abstraction levels*** of system design; consistency between abstraction levels is ensured by formal verification. Models and relationships between models will evolve as design progresses and understanding deepens. Many model refinements follow systematic patterns and ***model transformation tools*** can be used to automate the application of these patterns. Powerful ***automated proof tools*** are essential to make formal verification as automated as possible. Rather than having a single proof tool, it is more effective to provide a framework for combining a range of automated proof tools in a seamless way. In this way we can exploit externally developed verification tools as well as our own verification tools.
While formal verification is the method used to ensure consistency within and between models, ***simulation*** helps engineers ensure that models are ***accurate*** representations of desired functionality and of physical system components. Computer-based simulation allows experts to make judgements about the accuracy of models; the more comprehensive the simulation, the more confidence can be placed in the judgement. Different simulation tools are better suited to simulating different parts of cyber-physical systems such as environments, host platforms, controllers, physical plant and communications. As with a proof framework, rather than having a single simulation tool, it is more effective to have a multi-simulation framework for combining separate simulation tools in a seamless way.
While formal proof can be used to verify that the software parts of a cyber-physical system correctly implement a formal model, it is not feasible to use proof to verify a complete cyber-physical system. Comprehensive ***testing*** continues to play an essential role in system verification. The same formal models that are used in design can also be used to construct test cases for system verification. ***Model-based testing*** is a technique for systematic generation of test cases from formal models that can increase the confidence of the testing over ad hoc manual construction of test cases. Model-based testing ***tools*** automate the generation of tests.
Conventionally, ***correctness-by-construction*** refers to the use of formal models and refinement in the development of ***software***. ADVANCE will go beyond this, supporting the construction of cyber-physical ***systems*** and augmenting formal modelling and verification with simulation and testing.

B.1.1.3 Scientific and Technological Objectives of ADVANCE

The ADVANCE Project aims to achieve a unified approach to the treatment of validation and verification through the development of a common modelling approach along with an associated set of generation, verification and prediction tools. A common modelling framework will remove the need for unnecessary duplication of modelling effort and will allow design trade-offs for different dimensions to be explored and analysed in ways that are consistent with each other. The common modelling framework needs to be rich enough and rigorous enough to enable analysis and verification to be performed, as much as possible, at early stages of the design lifecycle on high-level models. The framework also needs to be rich enough to support a rigorous flow from high-level models to concrete implementations consisting of compositions of heterogeneous – hardware, software and physical – components. While the flow will require the application of engineering judgement at various stages, it should provide as much automation as possible for more systematic tasks.
The complementary expertise and technological base of the ADVANCE industrial and academic partners will be combined to achieve the following scientific and technological objectives:

1. Deliver methods and tools for construction, refinement, composition and proof of formal models

2. Deliver methods and tools for multi-simulation and testing based on formal models

3. Deliver the ADVANCE tools in open-source form integrated within a uniform framework with extensible architecture

4. Valid the methods and tools through application to cyber-physical case studies by industry partners in the transportation and energy sectors

5. Integrate the design methods and tools in system development flows including requirements and safety analysis

Fortunately we do not need to start from scratch in order to achieve our objectives. We will use the Event-B[3] formal modelling language as the basis for the common modelling language and we will build on the existing open-source Rodin[4] toolset for Event-B. Rodin is a powerful and extensible open-source Eclipse[5] toolset whose development has been supported by the FP6 RODIN Project and the FP7 DEPLOY Project[6]. Industrial experience to date with the Event-B modelling formalism demonstrates that it provides a solid basis for our endeavour. Event-B provides a rich formal modelling language together with a verifiable notion of refinement for relating models at different abstraction levels. Event-B has been used successfully to model cyber-physical systems including automotive control, industrial plant and rail control. The core Rodin platform supports mechanical analysis of Event-B models including proof obligation generation and automated and semi-automated proof. Rodin has facilities for extending the mathematical theories of the Event-B language and proof mechanisms. The open architecture of Rodin has allowed a number of plug-in tools to be developed including plug-ins for model-checking, animation, model composition and code generation.

Although the existing Rodin methods and tools go some way towards addressing our objectives, they do not go far enough. We have identified significant gaps in the methods and tools that need to be addressed by the ADVANCE project if we are to achieve our objectives. Rodin already provides a framework for integration of a range of proof tools; however this has not been exploited to its full potential. Although there is some support for model simulation in Rodin, it lacks the framework and power for the large scale multi-simulation that we envisage. Event-B provides a general-purpose mathematical language for specification and reasoning; however, this needs to be enriched further with language constructs and mathematical theories that are better suited to modelling of cyber-physical systems. Overcoming all of these current limitations in the Rodin toolset requires research and development of further methods and tooling by ADVANCE.

As outline in the previous two paragraphs, the Rodin toolset provides a strong baseline for achieving the ADVANCE objectives. Rodin is an open source Eclipse toolset with extensible architecture. It supports mechanical analysis of Event-B models including proof obligation generation and automated and semi-automated proof. Event-B is a general purpose language but enrichment in terms of new modelling patterns and new mathematical theories are required in order to apply Event-B in a cost effective way to new domains such as cyber-physical systems. The ProB plug-in for Rodin supports small scale simulation and test case generation but this is currently some way below the level required for ADVANCE. We now outline the new developments on top of the existing Rodin toolset that need to be delivered by ADVANCE in order to achieve each of the Objectives 1, 2 and 3:

- Achieving Objective 1: We will develop new modelling and composition patterns and new mathematical theories in Event-B that are suited to cyber-physical system development such as those systems in the validation case studies of the ADVANCE industrial partners. The Rodin tools will be extended to support analysis of these new patterns and theories.
- Achieving Objective 2: We will develop a tools framework on top of Rodin to support large scale multi-simulation of Event-B models that integrates different simulation tools. We will considerably extend the existing model-based testing and simulation capabilities of Rodin in terms of scalability and language coverage, including coverage of patterns and theories developed for Objective 2.
- Achieving Objective 3: All tools extensions in ADVANCE will follow the existing Rodin conventions that ensure further extensibility of tool capabilities and these new extensions will be made available in open source form.

The Rodin toolset was originally developed as part of the FP6 RODIN Project and the by the DEPLOY FP7 Project. DEPLOY finishes in January 2012, just a few months into the ADVANCE Project. As outlined above, the Rodin toolset being delivered by DEPLOY will form a very strong basis for tool developments in ADVANCE. Three of the ADVANCE partners, SYSTEREL, UDUS and SOUTHAMPTON, form the core team of tool developers of Rodin within DEPLOY and are in a very strong position to make the further tool developments required to achieve the objectives of ADVANCE. Since the Rodin toolset is open source and managed on sourceforge.org, there are no IP impediments to ADVANCE building on Rodin tools.

A further advantage of basing our developments on Rodin is that it already has a strong and growing user base. Rodin has users and developers in industry and academia who actively follow advances in the technology and they will provide a strong basis for dissemination of results on which we can build. Current industrial users of Rodin include DEPLOY partners such as Bosch, Clearsy, Siemens, Space Systems Finland and SAP as well as other companies such as AeS (Brazil), AWE (UK), General Motors (India) and XMOS (UK). These users demonstrate that Rodin is an industrial-scale toolset and will provide a strong vehicle for exploitation of the ADVANCE outcomes.

B.1.1.4 Measurable Outcomes from ADVANCE

The research and development in ADVANCE will provide the following measureable outcomes:

A. Extensions to the Rodin methods and tools providing richer language constructs and mathematical theories for modelling and reasoning about cyber-physical systems, including model refinement and composition. We will deliver new modelling and composition patterns and new mathematical theories in Event-B that are suited to cyber-physical systems. We will deliver extensions to the Rodin toolset to support verification with these patterns and theories.

B. Extensions to the Rodin methods and tools providing a framework for large-scale multi-simulation of assemblies of models and external simulations along with more powerful model simulation and simulator generation facilities. We will deliver a tools framework on top of Rodin to support large-scale multi-simulation of Event-B models that integrates different simulation tools in order that systems of the scale and complexity developed by the industrial partners can be simulated with high degrees of coverage.

C. Extensions to the Rodin methods and tools providing support for model-based testing including test case generation and instrumentation for comprehensive testing of developed software and systems. We will considerably extend the existing model-based testing capabilities of Rodin in terms of scalability and language coverage so that system implementations of the scale and complexity developed by the industrial partners can be tested.

D. Validation of the ADVANCE methods and tools based on application to two industrial case studies. The case studies will deliver collections of models, implementations, verification results and simulation results that will lead to new understandings of how ADVANCE methods and tools can be further improved and how they can be applied in industrial settings.

E. Guidelines for integration of ADVANCE methods and tools in the development flows. The case study results will be used to deliver guidelines for applying ADVANCE methods and tools in effective ways that add value to the design flow and can be integrated with existing development processes. This will include guidelines for linking formal modelling with requirements analysis and safety analysis and guidelines on effective ways to combine proof and simulation in design flows.

The following table shows how the ADVANCE Objectives listed in B.1.1.3 are addressed by the above measurable outcomes:

	Outcome A	**Outcome B**	**Outcome C**	**Outcome D**	**Outcome E**
Objective 1	X				
Objective 2		X	X		
Objective 3	X	X	X		
Objective 4				X	
Objective 5					X

All tools delivered by ADVANCE will be open source and will be integrated with the Rodin toolset (see Objective 3, B.1.1.3)

The following table provides indicators outlining how ADVANCE will impact European industry:

Efficiency and productivity in software development	The provision of a System-of-Systems development framework that will allow European industry to build on and further exploit the formal engineering methods that have already been developed in a range of European industrial sectors will help to improve productivity at the competitive edge of European industry.
Open and standard platforms and interfaces	ADVANCE is based on an existing, open development platform for formal engineering methods, Eclipse and Rodin.

B.1.1.5 Relevance to the FP7 ICT Workprogramme

The Objective ICT2011.3.3 for the FP7 ICT Workprogramme highlights the growing need to move towards a new way of engineering complex, distributed and co-operating systems so that they will meet their performance and energy-efficiency targets with high reliability and resilience. The overall aim of the ADVANCE project is to make major advances in "System-of-Systems" engineering methods through the development of a unified framework for formal verification and multi-simulation that exploits and builds upon the advances made in recent FP7 research on formal engineering methods.

These formal engineering methods, as for example developed in the DEPLOY FP7 project, introduce a *correct-by-construction* design and verification approach to the traditional engineering process and have been successfully applied to the development of components and sub-systems. ADVANCE addresses the challenge of designing, verifying and validating a "System-of-Systems", comprising a heterogeneous collection of independently-developed components and sub-systems, by complementing the *correct-by-construction* approach with a simulation-based method that enables the components and sub-systems to be composed in a secure manner to facilitate "System-of-Systems" development. The ADVANCE formal modelling framework will provide an approach to system verification and validation that is driven by proof, simulation and testing in a coherent and complementary way. Verification by proof will be driven by advances in automated proof and model-checking. Large-scale simulation will serve to validate the accuracy of formal models, especially models of physical sub-systems. Test-driven verification will enable the creation of comprehensive but compact test suites from formal models through the provision of *coverage measurements* which show how well the tests cover the system functionality.

As systems evolve and components and sub-systems are enhanced or replaced, the test suites provide the reference that ensures that the system still meets its requirements. As the system requirements evolve, the test suites too evolve and ensure that the modified systems meet their new goals.

Two case studies, one addressing the area of safety-critical transportation systems and the other the embryonic field of energy-aware electricity distribution will be developed by our industrial partners to shape and verify the methods and tools of the ADVANCE framework. Both case studies will follow existing or emerging European and international standards in their respective areas.

B.1.2 Progress beyond the state-of-the-art

This section describes the ways in which ADVANCE will make progress beyond the state-of-the-art. It covers three main areas: industrial practice, scientific knowledge, and engineering tools.

B.1.2.1 Progress beyond state of the art in industrial practice

ADVANCE will make significant progress in several areas beyond what is currently state-of-the-art in industrial engineering practice:

- Verification can consume more than 70% of the overall system development time and cost. To address this issue, ADVANCE will deliver a *design for verification* method for “System-of-Systems” engineering development that will facilitate component, sub-system and system verification throughout the development work-flow. In particular, verification costs reach a peak when the final system must be tested in the field. The ADVANCE method will focus particularly on design for *early* verification to facilitate the verification of individual system components within the system in the early stages of development and therefore minimise verification costs later in the engineering work-flow. Components and sub-systems will be developed using a formal, *correct-by-construction* approach augmented by traditional simulation-based verification techniques. From these formal component and sub-system descriptions, simulation models will be derived automatically to facilitate both system simulation and verification.
- Formal engineering methods enable greater mastery of complexity than do traditional engineering processes. It is the central role played by mechanically-analysed formal models throughout the system development that enables mastery of complexity. As well as leading to big improvements in system dependability, greater mastery of complexity also leads to greater productivity by reducing the expensive test-debug-rework cycle and by facilitating increased reuse of hardware and software. ADVANCE will enhance significantly the impact that formal engineering methods can have on modern industrial methods and work-flows by increasing the scope for effective deployment beyond that which is currently possible and broadening the applicability of *the correct by construction* approach.
- Up until now, formal engineering methods have been applied to the development of components and sub-systems. Exploiting these formal methods to support “System-of-Systems” engineering poses major new engineering challenges. ADVANCE will develop a framework within which a collection of independently-developed, heterogeneous components and sub-systems can be composed in a secure manner to enable

"System-of-System" design and development. Where feasible, the components and sub-system models will be developed using the formal, correct-by-construction approach supported by ADVANCE. This will not, however, preclude the use of models developed using other formal or simulation-based approaches. Provided that a host simulation environment is available for such models, then they too can be included in the ADVANCE framework to enable "System-of-Systems" verification.
- ADVANCE will develop novel validation and verification techniques to ensure that the interactions between the components and sub-systems can be comprehensively explored and tested so that this exploration can be used to assure the customer that the system delivers the expected functionality and that the testing results in a measure of how well the design has been *covered* by the tests.

The industrial deployment partners have identified specific advances in the state of the art in industrial engineering practice for their sectors that they see ADVANCE delivering:

- **Dynamic Trusted Railway Interlocking (Alstom Transport** Information Solutions**):** AT will model and verify formally a novel approach to controlling the interlocking between points and signals, based on state-of-the-art "Computer-based Interlocking" techniques and compliant with the CENELEC (European Committee for Electro-technical Standardization) and ERTMS (European Rail Traffic Management System) standards. AT will use ADVANCE to develop a proved model, automatically generate a simulation model and then use the ADVANCE simulation framework to verify that the planned system will satisfy its requirements prior to actual implementation. AT will also use the ADVANCE framework to develop the test suite that will be used to verify and sign-off the final embedded system implementation.
- **Smart Energy Grids (Critical Software Technologies Ltd):** A Smart Grid uses two-way communication between the electricity supplier and the consumer electrical installation and appliances to match effectively the consumers' electricity demand to the available supply by, for example, utilising off-peak electricity usage whenever possible. CSWT will use the ADVANCE "System-of-Systems" approach to model and verify formally the trusted, secure and reliable data interchange that will be required between supplier and consumer. CSWT will look to comply with the standards for Smart Grid Interoperability developed by the U.S. National Institute of Standards and Technology (NIST). CSWT has working relationships with a number of Smart Grid owners who take significant interest in the issues presented in the case study; these relationships will be exploited in order to acquire real-world information to support the case study.

B.1.2.2 Progress beyond state of the art in scientific knowledge

ADVANCE will move beyond the state-of-the-art in scientific knowledge in the following areas:

- Formal modelling and analysis techniques are scientifically quite mature. However the degree to which they scale up is not so well understood nor is there a proper understanding of the right deployment strategies to ensure effectiveness of use. ADVANCE will build on the experiences of the DEPLOY project to increase our understanding of how well formal methods scale and will increase our understanding of what further research is required to improve this scaling. ADVANCE will develop and expand the underlying automated proof and model checking technology of RODIN, extend the EVENT-B language where necessary to improve expressiveness and improve support for managing model complexity through composition and de-composition techniques.
- Formal modelling and analysis techniques have not been applied to large "System-of-Systems" engineering projects. ADVANCE will address this challenge by investigating how verification techniques such as simulation and model-checking can be combined with formal verification methods so that the specific strengths of each technique can be leveraged successfully when applied to systems of heterogeneous components and sub-systems.
- As well as providing the facility to develop directed tests, ADVANCE will develop techniques for generating tests automatically. The rate at which manual tests can feasibly be developed imposes a severe bottleneck on the design and verification process. Augmenting directed testing with automated random testing improves the rate at which tests can be created and can help to identify corner cases which escaped directed testing but can result in very large, poorly-targeted test suites; re-running such large test suites for every engineering change made to the design can itself become a major bottleneck. In addition, applying the test suite to the completed system may be restricted by both time and cost constraints. It is therefore important that generated tests suites are as small and well-directed as possible. *Constrained random testing* is widely used in modern System-on-Chip verification methodologies because it enables tests to be specified at a high level of abstraction and results in compact and efficient test suites. In ADVANCE, formal

techniques based on Event-B will be developed to model the system environment and enable constrained random testing.

- Measuring the outcome of a "System-of-Systems" verification process is necessary to facilitate design sign-off. To have confidence that the system is ready to be deployed it is necessary to establish, objectively, how well the verification has *covered* the design. ADVANCE will investigate and develop the coverage techniques and measurements that will be needed to support the work-flow. Coverage results can also be used to direct the test generation towards areas of the system not covered by the test suite.

B.1.2.3 Progress beyond state of the art in engineering tools

ADVANCE will make several advances beyond the state-of-the-art in engineering tools:

- Many formal engineering tools exist and are being used to some extent in industrial development. Semi-automated proof systems such as PVS, HOL, Isabelle, ACL2, Coq are general-purpose theorem provers that have been applied to analysis of systems[7]. The application of such general-purpose provers requires the development of a modelling approach and along with a potentially long list of formal properties to be proved. In ADVANCE, we will support a discrete event system modelling style based on Event-B that supports modelling at multiple levels of abstraction. The property to be proved will be a refinement between abstraction levels. This means that engineers can focus on modelling and proof and not be concerned with determining a large list of formal properties to be proved. The existing RODIN platform for EVENT-B model development will be enhanced to improve usability and capacity to support larger-scale developments. The responsiveness of the RODIN user interface and editors will be improved. The existing automated proof tools will be further developed to increase the proportion of proofs that are amenable to automatic discharge. Performance improvements to RODIN's model checking tools will greatly increase the proportion of the search space that can feasibly be covered. The Composition/Decomposition plug-in will be extended to facilitate re-use and group working on large projects. A library of *formal design patterns* will be developed to assist in the development of specifications for commonly occurring problems.
- Fully automated first-order provers such as SPASS, Simplify, Vampire and Waldmeister have become very powerful in recent years[8]. The mathematical language that they support is a lot less rich than Event-B but we will investigate links with these provers for those cases where they can be used. This will be facilitated using the TPTP interchange language for first-order provers.
- A range of model-checking tools[9] [10] are used for system analysis. Examples include Spin, SAL, SMV, UPPAAL and Alloy. These powerful tools provide modelling languages and property specification languages. Apart from Alloy, these model checkers support modelling styles that are close to implementation so they are not as well suited to early stages as Event-B. Alloy has a relational language similar to the set theory of Event-B. For all these tools, the focus is on proving properties at a single level of abstraction. In contrast in ADVANCE we will use a refinement approach allowing us to link very abstract levels to detailed implementation levels. Also we will support a combination of theorem proving and model checking for verification.
- Several program verification systems for mainstream programming languages are available that use automated verification technology. For example, Spark for Ada programs, JML for Java and Spec# use automated provers for program verification[11] [12]. Blast and Slam use model checking techniques for verification of C programs[13] [14]. PolySpace uses abstract interpretation for verification of C/C++ and Ada programs. These technologies focus on verification of implementations and thus they can only be used once an implementation has been constructed. In ADVANCE we will provide formal modelling support for earlier stages of specification and design.
- Several formal modelling tools provide automated code generation facilities. Atelier-B supports generation of Ada and C programs from low level B models. Scade supports generation of C programs from the Scade modelling language and uses the Prover automated proof system for verification. Perfect Developer supports generation of object oriented programs in a proprietary language from specifications. The KeY system supports the generation of Java programs from UML/OCL specifications. These systems are focused on the construction of software components so they are best used at later stages of development. ADVANCE will extend the state of the art in formal methods tools by providing a tool suite that covers a much broader range of the development process, both earlier, through support for system-level analysis, and later, through support for linking models to implementations and components and through support for system evolution.
- Many tool developers focus on the technical capabilities of their tools, neglecting tool usability and not maximising the productivity and effectiveness of tool usage. ADVANCE will develop and exploit a range of techniques for ensuring high levels of usability and productivity in tool usage including exploitation of high degrees of automated analysis, good user interface design guided by usage patterns, higher levels of user friendliness through complementing mathematical notation with appropriate graphical notation and though support for graphical animation of models.

- Existing industrial-strength formal methods tools are closed and difficult to extend or integrate with other tools. This is a major impediment to their take up by industrial organisations that have extant, sound, engineering processes. ADVANCE will extend that state of the art here by providing an open-source tooling platform with an open architecture that is extensible and therefore amenable to integration with other tools. The tools platform will support an open approach to proof, allowing the use of off-the-shelf and purpose-built automatic provers. The open architecture of the tools platform will also allow the integration of tools for semi-formal modelling languages such as UML. The toolset will be of a professional standard with professional levels of support.
- ADVANCE will implement a simulation framework, extending the RODIN platform, within which independently-developed, heterogeneous components and sub-systems can be composed in a secure manner to enable "System-of-System" design and development. The great difficulty faced in assembling compatible models of the components and sub-systems which are at the appropriate level of abstraction to enable effective and efficient system verification presents a major barrier to the adoption of "System-of-Systems" engineering methods. In ADVANCE, the models of the components and sub-systems, developed using formal techniques, are imported directly into the simulation framework using two, complementary techniques. In the first, a simulation model is generated automatically from the formal model using techniques that build upon the code-generation methods developed in the FP7 DEPLOY project. This technique will be used when the component model is mature and less-prone to frequent changes and will have the advantage of fast and efficient simulation. In the second, the model will be executed by its own host simulator and the ADVANCE multi-simulation framework will manage the communication of data between multiple simulation hosts, enabling simulation and verification of the whole system. This second technique will allow model development in other languages and environments is to be leveraged without the need to translate the models to the host ADVANCE format. The ProB formal model animator and model checker, also developed in the FP7 DEPLOY project, will be extended and its performance improved so that it too can be integrated within the ADVANCE multi-simulation framework. This will facilitate early system integration while the model is still being developed and allow interactive de-bugging.
- ADVANCE will extend and augment the test generation tool already proved in Rodin to facilitate constrained random testing. Hardware Verification Languages and tool environments such as Specman, VERA and SystemVerilog provide constraint-based random testing capabilities at a high level of abstraction and have been deployed successfully in the field of chip verification over the last decade.
- Measuring the coverage achieved by testing is an essential component of any constrained random testing methodology. ProB already provides the facility to measure coverage of Nodes and operations of Event-B models. ADVANCE will bring these coverage measurement facilities to the wider simulation framework. The simulation model generation capability provided by ADVANCE will allow the option of collecting coverage measurements during simulation and test.

B.1.3 Scientific and technological methodology and associated work plan

B.1.3.1 Overall strategy and general description

ADVANCE offers a balanced interplay between industrial deployment, scientific research and tool development, where companies in two sectors join their forces with three technology providers to meet the project goals. In what follows, we first briefly describe those aspects of the ADVANCE partners which are important for describing the overall deployment strategy of ADVANCE and the work plan. Thereafter the structure of the work plan will be presented followed up by the detailed descriptions of the work packages.

The Industrial Sectors and Partners

The industrial sectors, railway transportation (AT) and smart grid (CSWT) comprise two important European base industries of today. AT is a leading company in the rail signalling industry. Its mission is to supply rail operators with complete solutions that allow them to operate high-density mainline or urban networks in complete safety while informing passengers and optimising resources in real-time. The solutions meet network requirements and regulations at local, national and international levels. They are based on open architectures, tailored to local standards and offer the customers the possibility of a progressive, modular approach. CSWT provides solutions for mission and business critical information systems. Its customers are drawn from several markets including energy, the public sector, industry, aerospace and defence. CSWT designs, develops, tests, validates and assures software for mission and business critical information systems across Defence, Aerospace and Energy. AT have over 15 years of experience of formal methods for control software development with the B Method while CSWT have started trialling Event-B over the last 12 months. These partners will be supported by the technology providers in their application of the ADVANCE methods and tools. AT and CSWT will also contribute to the development of the ADVANCE methods and provide requirements definitions for ADVANCE tools.

Expertise of the Technology Providers

The two academic partners are world leaders in formal methods research. Three of the senior researchers (Abrial, Butler, Leuschel) are world-leading research scientists in formal methods. Through a subcontract, SYSTEREL brings to the consortium the outstanding experience of Jean-Raymond Abrial, the originator of B and Event-B. Butler and Leuschel play leading roles in the development of the Rodin toolset and lead strong research teams at SOUTHAMPTON and UDUS respectively. Voisin (SYSTEREL) is the main architect of the Rodin platform; he leads a strong team which has a twofold expertise in both applying formal methods and developing tools supporting formal methods. SYSTEREL has gained long-standing experience in applying formal methods in industry, more specifically B for software development and Event-B for systems analysis and design. SYSTEREL has also been in charge of the maintenance and coordination of development of the Rodin platform and associated tools since 2007. Hence, Europe is in a unique position when it comes to developing the ADVANCE methods and tools. Three of the partners (UDUS, SOUTHAMPTON, SYSTEREL) are at the core of the IST FP7 project DEPLOY where formal engineering methods, resilience approaches and a supporting tool platform were developed together with a range of industrial and academic partners. This combination of expertise is vital for building truly coherent and robust methods and tools. The academic partners have considerable experience in developing and applying a wide range of formal approaches like B[15] and Event-B[16], and model checking[17]. In ADVANCE the partners will build on this work.

Structure of the Work Plan

The work plan is divided into the following seven workpackages:

WP	*Title*	*Icon used in the proposal*
WP1	Dynamic Trusted Railway Interlocking Case Study	
WP2	Smart Energy Grids Case study	
WP3	Methods and Tools for Model Construction and Proof	
WP4	Methods and Tools for Simulation and Testing	
WP5	Process Integration: integrating methods and tools into development processes to maximum effect	
WP6	External Dissemination and Exploitation	
WP7	Management	

The following table shows how the ADVANCE Objectives listed in B.1.1.3 are addressed by these workpackages:

	WP1	**WP2**	**WP3**	**WP4**	**WP5**	**WP6**	**WP7**
Objective 1			X			X	X
Objective 2				X		X	X
Objective 3			X	X		X	X
Objective 4	X	X			X	X	X
Objective 5	X	X			X	X	X

A Road Map to the Work Plan

Let us first give a road map to the work plan. As we will see, the workpackages are divided up in four main groups:

- the two industrial deployment workpackages WP1 and WP2 ,
- the two methodology and tool workpackages WP3 and WP4,
- the process integration workpackage WP5,
- the external dissemination and exploitation workpackage WP6, and
- the management workpackage WP7.

In what follows, these five groups are briefly described in turn. In section B.1.3.2 we describe the timing structure of the workpackages. ADVANCE will run for two and a half years, M1 to M30.

Industrial Case Study Workpackages WP1 and WP2.

The industrial deployment workpackages (WP1, WP2) will involve the application of the ADVANCE methods and tools to cyber-physical systems. Both workpackages will follow a similar pattern of work consisting of four major tasks leading to four major milestones (Task X.1 to X.4 where X is 1 or 2):

- Task TX.1 Definition of Requirements
  - Definition of system requirements of the case study and
  - Identification of requirements on methods and tools – 3 months
- Task TX.2 Proof of Concept
  - Take a cut-down definition of the case study through the entire ADVANCE work-flow – 9 months
- Task TX.3 Full Case Study
  - Apply the method developed in Task TX.2 to the full case study – 15 months
- Task TX.4 Reflection
  - Enhance the ADVANCE method in the light of the experiences of Task TX.3 – 3 months

WP1 Case study - Dynamic Trusted Railway Interlocking: Interlocking is the component of the signalling system that sets and locks the routes for trains on request of the traffic operator and that commands the lights of the wayside signals according to the state of the routes. Clearly interlocking is a safety critical component since wrongly set routes may cause train collisions. Regardless of the verification technique used, it is difficult to demonstrate formally that all the configurations that an interlocking can command are safe. If formalisms based on mathematical proof, like Event-B, are used, it is difficult to link system safety properties, such as, “two incompatible routes should never be set at the same time”, with the actual actions of pre-existing interlocking which are defined at a very local level, such as, “the starting signal of a route is open if the points and traffic directions of the route are correctly positioned and locked”. Alternatively, if formalisms based on model checking, like state charts or Petri nets, are used, it is difficult to check all the possible configurations as they can be very numerous even for not too complex networks.
To overcome these difficulties AT intends to develop with the ADVANCE methods and tools a new component, called an Interlocking Dynamic Controller (IDC), which dynamically checks the safety of the configurations computed by the interlocking at run-time. IDC will be independent of the internal state of the interlocking and from the technology used to implement it, either automata or Boolean logic. Thus, it will be possible to adapt it to any existing interlocking system avoiding major re-engineering of existing interlocking systems. WP1 will identify and formalise the safety properties at the signalling system level; it will then identify those that should be allocated to the interlocking and will refine these ones until they are expressed in terms of the interlocking outputs. Then it will specify formally the actions that will check dynamically that these properties are satisfied. Mathematical proof will be essential to deal with the desired level of complexity and generality. To complement formal proof, the resulting models will be analysed by means of simulation and test cases and a prototype will be generated from the models in order to achieve comprehensive validation against existing interlocking systems.

WP2 Case study - Smart Electricity Grids: In the coming years, it is predicted that Europe will experience a reduction in energy generation capacity to a point where peak demand may exceed capacity. The challenges this poses together with the growing emphasis on energy efficiency and green power present significant difficulties to grid operators who cannot afford a mass reconfiguration of national and transnational grids. As grid operators worry about infrastructure, levels of service and billing, home owners and businesses are

becoming more aware of the financial savings possible through adopting energy efficiency schemes. An increasing number of appliances can be seen to support advanced energy saving options that can help to make them financially attractive in the long-term. Until recently, energy efficiency has been about individual devices making local savings without taking into account demand on the grid and the price of electricity. An intelligent, automated Smart Grid with a Smart Home system has the potential to solve all the issues mentioned and provide a win-win situation for all parties. Grid operators can allow the grid to manage demand & control automatically and receive up-to-date billing and service information. Consumers can be assured that their devices are operating in the most efficient manner (e.g. by using the cheapest rates possible).
Smart Grids are a system of systems, involving digital communications between grid management software systems and smart appliances at consumers' homes, layered on top of existing electricity grids. In WP2 we will model and verify the distributed monitoring and control together with communication between consumer devices, electricity suppliers and grid operators. Of particular concern is verification of the robustness and security of the communication infrastructure. Simulation and test case generation will be used to validate the formal models against existing grid architectures and components.

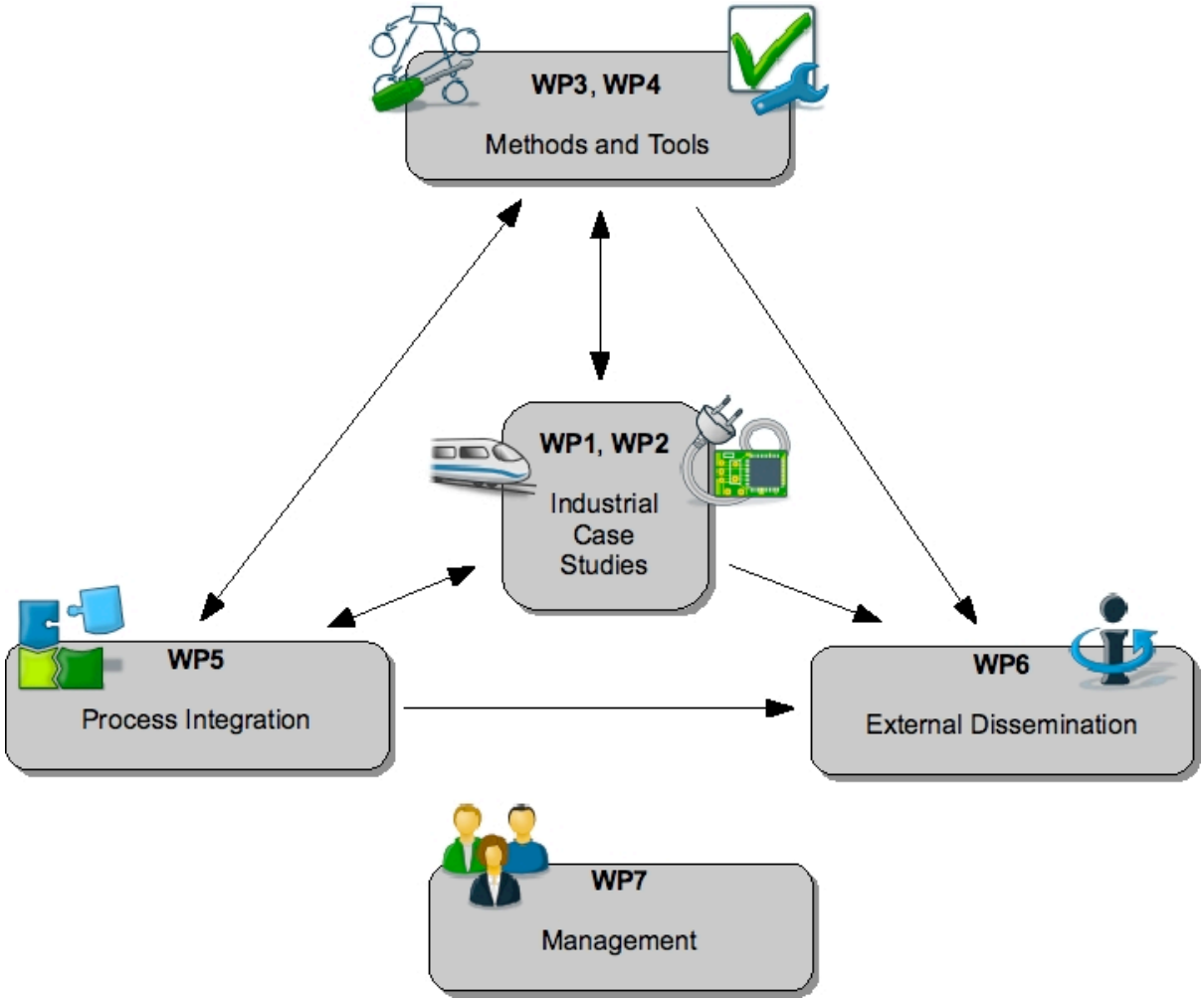

Diagram 1.1: Architectural view of ADVANCE

Methods and Tool Workpackages WP3 and WP4.

In addition to the case study workpackages there will be two research and development workpackages. The first, WP3 Methods and Tools for Model Construction and Proof, will focus on developing further the Rodin

platform to improve its usability for industrial applications, for instance in the areas of automated proof, plug-in management and user interface. A further role of this workpackage will be to provide expert formal proof support for the industrial partners. We will exploit off-the-shelf automated provers including first-order provers and SMT. WP3 will support extensions of the Event-B language required for cyber-physical systems and will considerably strengthen the composition and decomposition support for Event-B in Rodin.

The second, WP4 Methods and Tools for Simulation and Testing, will be responsible for developing the multi-simulation framework. This framework will allow for multi-simulation of assemblies of Event-B models together with external simulators through a clearly designed architecture within the Rodin environment. WP4 will improve the capacity of ProB to manage large industrial designs and extend it to support constrained random testing. This workpackage will also raise the level of abstraction at which code generation can be done above the state-of-the-art.

Process Integration Workpackage WP5.

It is important that the range of methods and tools developed by ADVANCE fit well together into a rigorous design flow and also fit well with overall design processes. We will develop design flows that combine simulation and formal verification unified by a common modelling language and toolset – Event-B and Rodin. These flows will provide guidelines on how the ADVANCE methods and tools may be combined in effective ways that add value to the design process. The flows will define steps to be taken in applying the methods and tools and provide guidelines on good practice to be followed as well as bad practice that is best avoided. Requirements analysis is a critical phase of any design process so we will develop methods the tools for linking requirements analysis with formal modelling. We will build on existing work that links structured requirements analysis with refinement-based formal approaches[18,19]. Safety analysis is of particular importance for cyber-physical system development and so we will develop methods and tools for linking hazard analysis methods (fault trees, event trees, HAZOP, FMEA, etc) with formal modelling. High-level safety analysis plays an important part in understanding hazards prior to formal modelling while, later in the flow, formal system models can be used as a basis for detailed safety analysis and certification. We will build on existing work that links safety analysis and certification with formal modelling[20,21]

We have deliberately not put methods and tools into separate workpackages. Our experience from previous endeavours is that because methods and tools are so closely intertwined, their separation is somewhat artificial and cumbersome. We have chosen instead to separate the methods and tools work along thematic lines – verification, simulation and integration.

Dissemination and Exploitation Workpackage WP6.

The results of the ADVANCE project (methods, tools, guidelines, case study material) will be disseminated to a broad industrial and academic community using electronic forum, through the establishment of an industrial interest group and through targeted dissemination workshops. We will build a community of industrial parties interested in tracking ADVANCE methods and tools. Several companies already use or have explored Rodin and they will provide a strong basis for the ADVANCE Industrial Interest Group (e.g., Bosch, GM, AeS Brazil, Siemens, SAP, Space Systems Finland, AWE, ClearSy, XMOS, NEC, ARM). We will also provide a repository of training resources and research results which will be linked with the existing Event-B repository[3]. This training material will be delivered in Masters courses at SOUTHAMPTON and UDUS. We will collaborate with other relevant ICT projects in order to cross fertilise ADVANCE R&D through joint workshops and through participation in standardisation efforts.

Management Workpackage WP7.

This work package involves project management and coordination activities, to be performed by the consortium lead (SOUTHAMPTON) between the European Commission and the consortium partners. It also includes the definition of a set of rules and project guidelines for the successful execution of the ADVANCE project, regular communicating of the project results to the consortium partners as well as the appointed project officer, and the organisation of an ADVANCE Executive Project Board.

Interactions between Workpackages

The focus of the Methodology and Tools workpackages, WP3 and WP4, and the Process Integration workpackage, WP5, is to provide for the needs of the industrial case studies, WP1 and WP2, and to deliver the

capabilities needed for real industrial deployment. Diagram 1.1 above shows the two-way dependencies between these workpackages.

B.1.3.2 Timing of work packages and their components

In this section we provide time lines for the workpackages and a description of the timing of the main deliverables.

The overall timing structure of ADVANCE

The time lines for the two industrial case study workpackages are shown in Diagram 1.2. and follow the same format. Each begins with a definition phase, followed by a *proof of concept* phase where a cut-down version of the case study is taken through the entire proposed method. At the end of this phase, the method is amended to take into account the experiences of the proof of concept work. This updated method is then applied to the full case study implementation. The final phase reflects on the experiences of the full case study phase and the method is again enhanced in the light of these experiences.

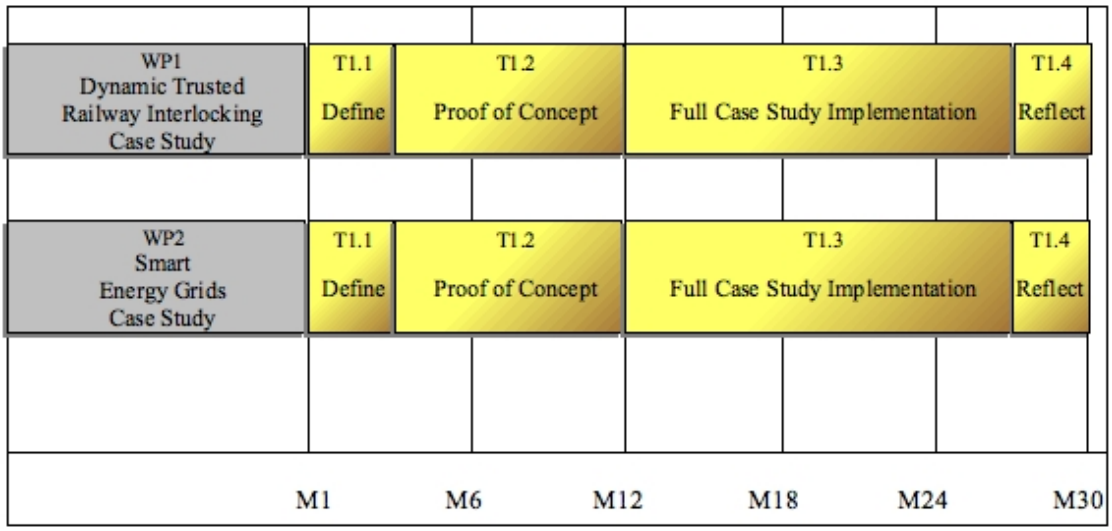

Diagram 1.2: Time diagram of WP1 and WP2

Diagram 1.3 shows the complete project Gantt Chart.

M12 will represent a significant point for review and refocus of the further work. As well as guiding the full implementation phase of the case studies, the experiences of the proof of concept phases will guide the further methods and tools work in WP3-WP5, clarifying needs on methods and tools and helping to prioritise. However there will be strong interaction between the case study workpackages and the methods and tools workpackages throughout the duration of the project through joint participation of the partners.

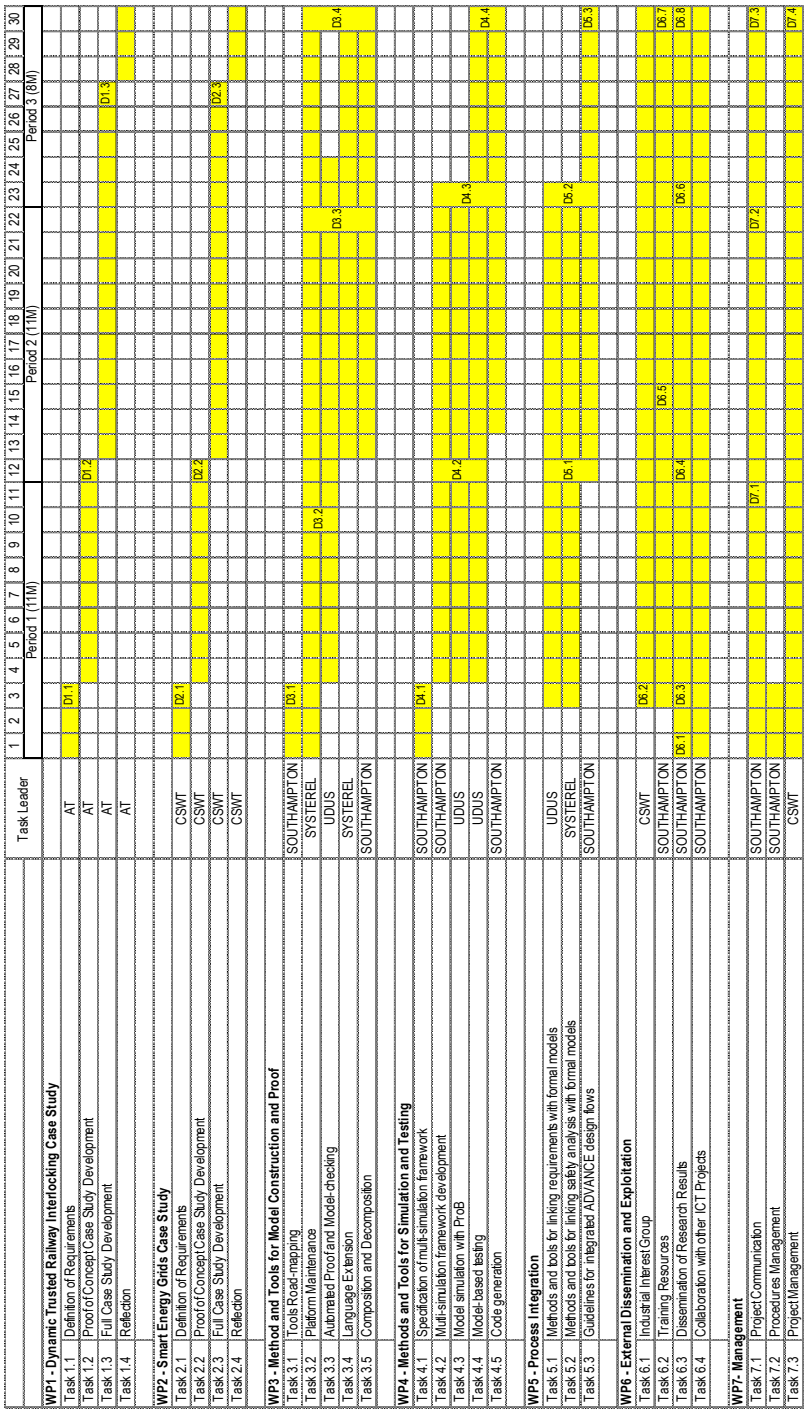

Diagram 1.3: Advance Project Gantt Chart

The timing structure of the deliverables

The industrial partners each deliver a Case Study Definition at M3. Also at this time, the on-line repository and electronic dissemination mechanisms will be in place and the specification of the multi-simulation framework completed.

M12 sees reports on the Proof of Concept phases for both Case Studies. M12 is when the first report of the Process Integration workpackage WP5. The first release of the ADVANCE training material will be available at M15.

The full reports for each Case Study will be produced at M27 and the final release of the ADVANCE training material at M30.

B.2 Implementation

B.2.1 Management Structure and Procedures

Project management

Southampton will be the Co-ordinating Participant and will undertake the tasks set out in Article II.2 of the EC-GA.

The Co-ordinator of ADVANCE will be John Colley (Southampton). Colley has participated in the management of several EU projects as well as other multi-industry and collaborative projects. As Co-ordinator he will chair project meetings, and will be responsible for the review, preparation and quality control of all deliverables and reports, and for monitoring project progress and compliance by the participants. The University of Southampton, which has a dedicated EU Finance Office, has extensive experience of FP7 projects, and is currently Co-ordinator for several FP7 Projects.

The Scientific Director, Michael Butler (Southampton). will ensure that the scientific and technological development of ADVANCE is properly coordinated between Workpackages 1 to 6, and will support the Co-ordinator on technical matters. Butler is an internationally leading scientist with extensive experience of management of EU and industry research projects.

Southampton's EU Finance Office will support the Co-ordinator on financial matters and undertake financial management of ADVANCE in accordance with EC-GA. It will deal with all financial transfers, monitor project budgets and administer any central funds.

Routine day to day management activities in ADVANCE will be delegated by the Co-ordinator to the Project Manager, Luke Walsh (Critical) who has experience in managing multi-industry and collaborative projects. The Project Manager will assist the Co-ordinator in collation of all non-technical documents such as Cost Statements, effort tables and annual management reports for the EU Project Officer and for the Project Board. The Project manager will also support the Co-ordinator in arranging and running project technical and management meetings. The Co-ordinator will retain overall responsibility for all aspects of management of ADVANCE.

A number of dedicated e-mail lists will be set up covering all workpackages, the Project Board and an "all hands" list. There will also be a list for interested parties external to the project which will be used as a dissemination tool.

The structure proposed for the management of ADVANCE is influenced by previous experience of partners on FP7 projects and by the best practise of the project members. It is designed to be as straightforward a structure as this project allows. The layers of management and organisation are shown below, in diagram 2.1.1.

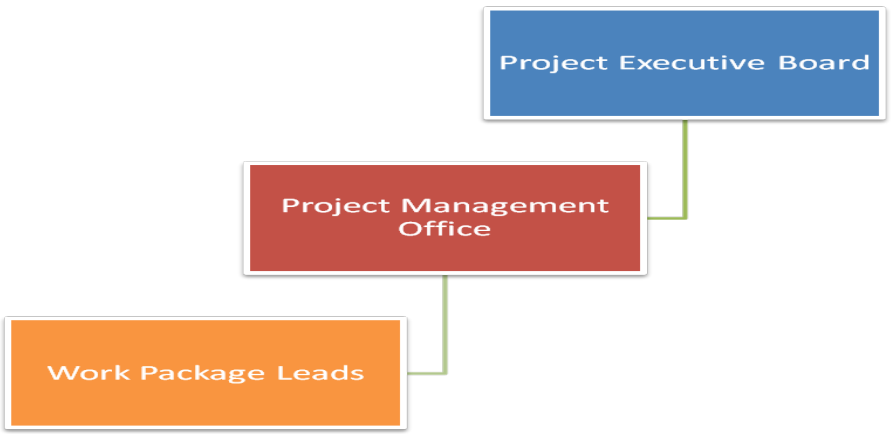

Diagram 2.1.1 Layers of Management

Project Executive Board

The project board will meet every six months and will be chaired by John Colley (SOUTHAMPTON). There will be no additional cost incurred in facilitating these project board meetings as they will be scheduled to take place on the same day as regular project meetings.

Membership of the Project Board has been set to ensure coverage across partners, workpackages and disciplines. Its members are: John Colley (SOUTHAMPTON), Michael Butler (SOUTHAMPTON), Jose Reis (CSWT), Fernando Mejia (AT), Michael Leuschel (UDUS) and Laurent Voisin (SYSTEREL). Others with skills and experience deemed necessary by the Board will be brought in as appropriate.

The Board will be responsible for the overall management of ADVANCE at a strategic level. The Board will be responsible for ensuring that the Project Management Office carries out its work to a high standard.

Furthermore, the Project Board will manage any calls for new partners deemed necessary and will act as selection committee. It will monitor and review any ethical considerations and will decide on press release and publication strategies. It will have overall responsibility for the knowledge management policies within ADVANCE and will deal with the resolution of any conflicts referred by WP Managers.

WP Leaders

Leaders of WPs will be highly experienced scientists in their own right and will provide information and documentation to Project Board within project deadline. WP leaders will be expected to produce reports to the PMO at least twice per year. The workpackage leaders will be as follows:

- WP1: Fernando Mejia (AT)
- WP2: Jose Reis (CSWT)
- WP3: Laurent Voisin (SYSTEREL)
- WP4: Michael Leuschel (UDUS)
- WP5: John Colley (SOUTHAMPTON)
- WP6: Alex Hill (CSWT)
- WP7: John Colley (SOUTHAMPTON)

All WP leaders are experienced project managers.

Consortium Agreement

Production of a suitable Consortium Agreement will be led by SOUTHAMPTON, and will be agreed by all partners, to be signed prior to the commencement of ADVANCE. This will cover in detail financial, and IP issues as well as conflict resolution procedures. This document will lay out project treatment of foreground and background IP however, within the project there will be an IP and Risk committee to monitor these issues and ensure that they are identified early and dealt with effectively.

IP and risk committee

This committee will be led by the project manager and will be made up of the Project Board.

Potential IP and risks will be identified through the work package leaders who will identify all potential IP and/or risk issues in their six month and annual reports and will alert the board to such issues The IP and Risk committee will then screen all publications, press releases and other forms of dissemination material for information that could compromise the IP-protection process, evaluate all such IP and decide whether there are realistic chances of obtaining protection. The committee will be able to sanction withholding data that could potentially compromise IP-protection for a defined period of time (up to 12 months). We anticipate that the main IP will be around the Industrial case studies since ADVANCE tools will be delivered in open source form.

The PMO takes a proactive approach to risk management with the key being early identification of potential risks, allowing time for appropriate plans for dealing with such issues to be produced. The “early warning” procedure for risk will follow a similar pattern to IP with regular contact between the PMO and technical managers at all levels. Examples of potential risks already identified include:

Potential Risk	Action Plan
A sudden unplanned withdrawal of a key partner delivering a critical component of the project	The Consortium Agreement will outline the exit procedure to be followed by any partner wishing (or obliged) to withdraw from the project.
A shortage of resources to complete a key activity on the critical path to a major project deliverable	Regular reporting by work package leaders to the Project Management Office will ensure that possible delays caused by shortage of resource are identified early and

	thus minimised. We also expect WP leaders to be involved proactively in work packages in order to anticipate risks and aid smooth transition to an agreed solution. Procedures will also be in place for situations where such issues cannot be dealt with at WP level and are therefore taken to the Project Board
A key issue or disagreement arising between members which creates a significant delay, impacting on project progress	There will be regular communication at all project levels both on a formal and informal basis. Such interactions should minimise misunderstandings and lengthy disagreements. Pro-active coordination and integration across the different work streams should minimise disagreements. Again escalation procedures will be in place for any issues not settled at WP level
Delays or inadequacies in funding in order to perform a critical WP or activity as scheduled	The Project Management Office will carry out extensive financial planning for ADVANCE, taking account of EC regulations and procedures. Such planning will attempt to ensure that partners, especially SMEs who are more vulnerable to cash flow problems are not inconvenienced unduly by the financial regime
An Industrial partner is forced, by market changes, to change policy towards ADVANCE	Any such issues will be identified and dealt with at this time. The project board will adapt the workplan for the remaining period.
IP or technical limitations of the Rodin platform will impede exploitation of the ADVANCE outcomes.	Since Rodin is open source there are no IP limitations on exploitation. The current industrial user base of Rodin is testament to its technical strength. The outcomes of ADVANCE will strengthen the technical capabilities considerably further. The industrial case studies of WP1 and WP2, along with external industrial users of Rodin and ADVANCE, will act as further drivers of technical strength of the tools.

The Consortium agreement, production of which will be led by SOUTHAMPTON, prior to the commencement of the project will be a key document in risk management since it will set out standards of conduct for all partners together with remedies for failure to meet such standards. This will give an agreed framework for the management of ADVANCE

Assessment and quality control

There will be two further levels of project monitoring:

- Assessment of the fulfilment of the project results with respect to its industrial deployment objectives. This self-monitoring task is essential in order to mitigate risks, in particular, those related to satisfying real industrial needs. The assessment will address the case study phases of definition, proof of concept, full development and reflection. The assessment will also allow the management to ensure that the methods and tools meet the industrial needs and react according to its risk management strategy. It will also help identifying uncovered challenges to address in the latter part of the project.

- All deliverables will be subjected to internal quality reviews. The draft deliverable will be made available for this review three weeks before deadline. Reviewers, who will be appointed by the Project Board and will be from the workpackage producing the document, will then have 2 weeks to carry out their task. They will provide a short written report to the authors and the Project Board. The authors will then take account of this review during preparation of the final; version. The final deliverable is passed to, and signed off by the Project Board before onward transmission to EU by the due date.

B.2.2 Beneficiaries

B.2.2.1 Critical Software Technologies Ltd (CSWT)

Critical Software provides solutions for mission and business critical information systems. Its customers are drawn from several markets including energy, the public sector, industry, aerospace and defence. Founded in 1998, the company today employs over 450 people at its various national and international sites with its headquarters and main technical centre in Coimbra, Portugal and auxiliary engineering facilities in Lisbon and Porto. The company is dynamic and outward looking with approximately 65% of the company's turnover resulting from contracts outside of Portugal. This is also evident in the company's workforce with over ten different nationalities being represented. In 2004 Critical established its second subsidiary, CSWT, in Southampton, UK.

CSWT designs, develops, tests, validates and assures software for mission and business critical information systems across Defence, Aerospace and Energy. CSWT delivers timely and cost effective quality and innovation. CSWT has a track record of on-time, on-budget and on-quality projects successfully implementing new technologies and products worldwide.

CSWT has already participated in several EU RTD projects in FP5, FP6 and FP7. It has managed, as prime contractor, several research and critical technology European Space Agency (ESA) projects involving embedded systems, such as RTEMS and xLuna. CSWT operates a management system based on the parent company's CMMI Level 5 and is ISO9001:2000 Tick-IT accredited.

The focus on Software Quality has driven a continuous improvement of CSWT's Development Process. The company's strong Quality foundations have enabled it to become a supplier to renowned customers in the most demanding industries. CSWT ensures outstanding software quality levels and project success by employing strict project management practices, coordination and control structures, and software engineering processes based on internationally recognized standards such as CMMI, ISO 9001:2000 Tick-IT, ISO 15504(SPICE), NATO AQAP 2110 and 150, ESA ECSS and EN9100.

Senior Staff Members

Mr. José Reis is a Senior Consultant Engineer at CSWT. He holds a Computer Science degree - 5 years duration – from Instituto Superior Técnico Lisbon. He plays a key role in the development of
Model Driven Engineering and Formal Methods within CSWT. He has been leading the team working on DEPLOY FP7 R&D project, ensuring that the Event-B Language and Tool RODIN is successfully experimented on an avionics sub-system. Mr Reis has been working with UK Prime Contractors, such as BAE Submarines, in the development of a Design Environment where Model Driven Engineering concepts/technologies apply. He has got experience with DO-178B and ECSS-E40 standards acquired in the verification and validation of avionics on-board software. Mr Reis has five years experience in Requirements Analysis and Solutions Architecture. He has developed significant customer facing and project management skills through the collaboration with various customers such as ESA, EADS Astrium, AgustaWestland, GE aviation. Mr Reis plays a key role in the development of CSWT's Quality Management System and has an interest in the definition and improvement of processes and methodologies. Prior to his current responsibilities, he worked as a solutions architect in European Ground Segment Technology Harmonisation Phase I and II, and worked on the development of a L1 data processor prototype for SMOS mission.
Alexander Hill graduated from the University of Southampton in BEng Digital Systems Engineering and has pursued a career balancing embedded software and hardware within the aerospace/defence industry. Alexander has a strong professional background in testing of embedded systems having worked on several testing projects for major defence and mobile-handset manufacturers. In addition to Engineering duties, Alexander has undertaken the role of Business Development for CSWT for the UK Energy Industry where his Engineering background helps to give him intimate knowledge of some of the problems faced in this technology driven sector.

Luke Walsh has

B.2.2.2 Alstom Transport Information Solutions (AT)

Alstom Transport Information Solutions (AT), with 4700 employees worldwide, is a leading company of the rail signalling industry. Its mission is to supply rail operators with complete solutions that allow them to operate high-density mainline or urban networks in complete safety while informing passengers and optimising resources in real-time. The solutions meet network requirements and regulations at local, national and international levels. They are based on open architectures, tailored to local standards and offer the customers the possibility of a progressive, modular approach.
AT's solutions are built essentially on three main systems that communicate through a data transmission network: a train supervision system that assists the operator to manage traffic and regulation of trains, a train

control system that assists and protects driving of trains and an interlocking system that sets and locks safe routes for trains. The two later systems involve safety-critical parts.
Mainline rail networks of Belgium, France, Italy, Morocco, Netherlands, Switzerland, United Kingdom, United States of America and Vietnam operate, or will operate soon, with AT's mainline solutions.
Urban rail networks in Brazil, Canada, Chile, China, Egypt, Hong-Kong, India, Italy, Mexico, Panama, Singapore, Spain, South Korea and Switzerland operate, or will operate soon, with AT's urban solutions.
Main tasks. AT leads WP1 on Dynamic Trusted Railway Interlocking Case Study. Its main tasks will be:

- to identify the requirements on methods, tools and on the case study itself in order to define the criteria that shall be used to evaluate the experiment;
- to define the method and the roadmap of the case study;
- to develop the case study according to the method and roadmap;
- to evaluate the case study according to the criteria of evaluation;
- to provide feedback on, and propose improvements of, the methods and tools developed by the other partners of the project.

Experience. AT has been designing and developing railway signalling systems for the last 30 years. It has thus acquired considerable expertise on train operation and protection systems and in the organisation of their development, test and commissioning. AT has constituted specific teams devoted to design, verification, validation, integration and assessment of safety-critical, systems, software and hardware. It has also developed the skills in the relevant fields: system engineering, networks and protocols, distributed and redundant architectures, information based system design, human-machine interfaces, control/command modelling and simulation, formal design of safety critical software, fail safe design of safety critical hardware, hazard trees analyses, failure mode effects analysis, international standards, etc.
Particularly relevant for this project is the AT expertise in formal methods. Indeed, AT is one of the earlier promoters of the B method, it contributed to its definition and it is the origin of AtelierB, the tool environment that supports the industrial application of the method. Furthermore, AT has been using the B method for the last 25 years for the design and implementation of the safety-critical software of trackside equipments and mainline and urban train protection systems.
In recent periods AT has been experiencing the B method and the ProB tool for system specification and analysis. It has created B models of parts of train protection and interlocking systems and has animated them with the ProB tool. Its purpose is to evaluate the worthiness and scalability of system model animation. The first conclusions are that it is worth and possible to animate significant system models.
All this put together makes that AT is able and willing to contribute to the definition and development of methods and tools for the formal design, validation and implementation of complex industrial systems.
Senior Staff Members.
Fernando Mejia led the B formal activities of AT for 15 years. As such, he designed AtelierB and developed some of its original tools (type-checker, proof obligation generator, prover); he conducted the design of B to Ada translators and the formal design and implementation of the safety-critical software of several trackside equipments and train protection systems. These activities lead him to contribute to the definition of the B method. Presently he conducts a project relating safety analyses and formal methods and experiments the B method for system specification and analysis.

B.2.2.3 Systerel (SYSTEREL)

SYSTEREL is a SME whose main activities are development, validation and evaluation of real-time and safety-critical systems. SYSTEREL main achievements thus concern:

- on-board systems with hard real time or safety requirements,
- safety related tools (data preparation, system maintenance, ...),
- formal specification of complex industrial systems,
- evaluation of the Reliability / Availability / Maintainability / Safety level of dependable systems.

Today's SYSTEREL activity is focusing on

- rail-bound transportation, particularly on track-side signalling systems and embedded calculators for either trains or automatic subways,
- avionics, by upgrading or validating critical systems such as inertial navigation or flight control systems
- defence, especially in the field of nuclear submarine propulsion regarding control and instrumentation,
- energy, for example by designing stimulator systems to help the validation of control/command and supervision of nuclear power plants,

- information-processing systems with safety and/or security requirements (fire-walling or secure transmission systems).

SYSTEREL also provides consulting in those areas, but 90% of its activity is made of fixed price projects.

Main tasks. SYSTEREL leads WP3 on Methods and Tools for Model Construction and Verification.

Within this workpackage, SYSTEREL will carry out the maintenance of the Rodin platform, together with the development of new plug-ins and features. SYSTEREL will also participate to the elicitation of modelling patterns to capitalize on its past experience of modelling in Event-B. Finally, SYSTEREL is heavily involved in the railway case study of WP1, where it will bring its expertise of interlocking systems. SYSTEREL will also participate to WP5 Process Integration, bringing in its double expertise in formal modelling and safety analysis. SYSTEREL also has the unique opportunity to bring Jean-Raymond Abrial into the consortium through a consultancy sub-contract. Mr Abrial is the originator of the Event-B notation and the Rodin platform. Being also the co-inventor of the Z notation and the B method, Mr Abrial has 20+ years experience of industrial application of formal methods. He will provide his expert methodological advice to the case studies and for eliciting recommended usage patterns of refinement, composition / decomposition and of the Rodin platform. His contributions to the project will be essential in helping the consortium to achieve the full goals of ADVANCE and it would be impossible to find the required expertise elsewhere.

Jean-Raymond Abrial retired a few years ago and thus could not enter the project on a full-time basis. He, however, has the opportunity to provide some consultancy (around 30 days per year) using the French status of "auto-entrepreneur". The ADVANCE consortium considers that a consultancy sub-contract of 80 days with Mr Abrial will be money very well spent and is the only way to allow the whole consortium to benefit from Mr Abrial's unique expertise.

Experience. SYSTEREL has been heavily involved for the past 10 years in the development of safety-critical systems. As such, the company has gained considerable experience in the application of formal methods to industrial projects, mainly in the railway industry (ALSTOM, ANSALDO transport, AREVA-TA, SIEMENS, THALES, 3S, RATP, SNCF). The projects developed using the B method range from *beacon speed control* software to trackside *automatic train control* software, and include the *beacon encoder*. All this software has been formally developed and achieved SIL4[1] certification.

In more recent years, SYSTEREL has also performed system modelling in Event-B for several industrial customers. The system models concerned were an *interlocking* railway system, the coordination between two zone controllers of a CBTC system, and the interaction of a zone controller with interlocking, wayside and on-board equipments. This practical experience allowed SYSTEREL to develop some expertise in the application of formal engineering methods in a real industrial context. But, it also showed that the technology was not mature yet, and that further research was needed to enhance their applicability to large-scale systems and systems-of-systems.

SYSTEREL has also been in charge of the maintenance of the Rodin platform since 2007. SYSTEREL has therefore developed extensive knowledge of the internals of the platform and is thus fully amenable to improve it within the ADVANCE project.

Senior Staff Members

Laurent Voisin has led the initial development of the Rodin platform (then at ETH Zurich). Most notably, he has defined the architecture of the platform and the fundamental principles governing its specification and design. He also took an active part in the development of the platform core. Since then, he has been the technical reference for the development and maintenance of the Rodin platform.

Christophe Métayer has expert skills in system modelling with Event-B, and has lead the development of several industrial-strength event-B models. He has also actively participated in the development of the Rodin platform and the animator plugin (then at ClearSy) and has expert knowledge of the Rodin platform internals.

Mathieu Clabaut has a solid experience in applying formal methods in an industrial context (including Event-B modelling). This experience also gave him good knowledge of various development processes used in industry as well as an insight of different railway systems.

Jean-Raymond Abrial is now retired, but provides some consultancy on a part-time basis. Previously, he had a long carrier as an independent consultant with strong connections to both the academic and industrial worlds. He has extensive experience in formal methods from both theoretical and practical point of views. He is the main inventor of Z and later B. He has also pioneered formal method tools, in particular, building widely used tools for these methods. He has been active in many projects dealing with the application of formal methods in

[1] *safety integrity level 4*, the highest level defined by the EN50128 standard.

industry. In ETH Zurich (his last position), he was the head of the team that defined the Event-B notation and the associated tools, namely the Rodin platform.

B.2.2.4 University of Düsseldorf (UDUS)

The Department of Computer Science of the University of Düsseldorf is a relatively new department, whose distinguishing aspect is the tight link with other scientific disciplines (in particular Biology and Medicine). The contribution to this proposed project will be made by the STUPS group, which has internationally leading expertise in formal methods and programming languages. In the area of programming languages, STUPS has expertise in partial evaluation, just-in-time compilation, abstract interpretation, and dynamic programming languages such as Python. In the area of formal methods, STUPS has considerable experience of animation, model checking and test-case generation, in particular for B, Z and CSP. STUPS has significant collaborative work with industry, in particular Siemens, ClearSy, Praxis Critical Systems, Bosch and AWE. The STUPS group has hosted the iFM'2009 conference as well as the AVoCS'2010 workshop. In addition to the projects listed below, the department of computer science was also involved in the XtreemOS FP6 Integrated Project.

Main tasks. UDUS will lead WP4, Methods and Tools for Simulation and Validation, and be responsible for extending the existing animation, model checking and model-based testing tools towards full industrial strength, in particular, by adding new features that are required for a successful industrial deployment. UDUS will be involved in scaling the current animation tools to full industrial models, developing new symbolic BDD/SAT methods for model checking, extending automated refinement checking and model-based testing for Event-B.

Experience. UDUS has developed and is maintaining the ProB toolset. The group has an extensive experience of using (constraint) logic programming, notably for implementing, analyzing, optimizing and verifying other programming languages. In addition, UDUS has extensive expertise in model checking, automatic refinement checking and model-based testing.

Senior Staff Members

Professor Michael Leuschel is head of the STUPS group. He has developed the ProB toolset for the validation of B specifications. Outside of formal methods, his main research areas are automatic program analysis and optimization (notably partial evaluation and abstract interpretation). He was awarded the IBM International Chair 1999 on Modelling and Optimization. He was the program chair of LOPSTR'02, PEPM'03, FMCO'09 and iFM'09, the symposium chair of PPDP'07, and is a member of the PEPM and LOPSTR steering committees and of the editorial board of the Journal of Theory and Practice of Logic Programming. He has published over 120 papers and developed several tools, such as the ECCE and LOGEN partial evaluation systems. He has been involved in several EU projects (Deploy, ASAP, PyPy, RODIN, POST) and the Eureka Eurostars project PyJIT.

Dr Stefan Hallerstede has extensive experience in refinement-based based formal methods. While working in industry was responsible for the development of a corresponding approach to hardware verification and supporting tools for code generation, in particular, of VHDL and SystemC. He worked with Jean-Raymond Abrial on the Event-B modelling method and co-developed a suitable formal verification tool, called Rodin. He has a PhD in Computer Science from the University of Southampton.

The following members of the STUPS group contributed to DEPLOY and will complete their PhD in 2011. *Daniel Plagge* has developed Z extension of ProB. *Marc Fontaine* is working on the combination of CSP and B, notably making ProB fully CSP-M compliant within an industry funded project. *Jens Bendisposto* has developed the Eclipse version of ProB and has adapted it to handle Event-B specifications within RODIN.

B.2.2.5 University of Southampton (SOUTHAMPTON)

During 2009/10 the University of Southampton was ranked 10th out of all UK Universities for research income received from the European Commission. The University is one of only 3 HE's in the UK to be awarded a *Financial Certificate of Methodology* from the European Commission. The School of Electronics and Computer Science at Southampton has internationally leading research across all areas of the ICT portfolio of research areas. Its research has achieved the top 5* rating in the last two Research Assessment Exercises, and in 2003 it was awarded the prestigious `best 5*' rating by HEFCE. The research proposed for this project will be carried out in the Dependable Systems and Software Engineering Research Group (DSSE), one of nine research groups in the school. The overall objective of the DSSE Group is to conduct research which leads to increases in the dependability of software based systems through the provision of architectures, construction methods, validation tools and the general advancement of software science. DSSE is very actively involved in the

application and development of the Rodin toolset for the Event-B formal methods (www.event-b.org). The DSSE group enjoys active collaboration with industrial partners such as Siemens, Bosch, Critical Software, SAP, NASA, RailSafe and Space Systems Finland mainly through EU-funded projects. The DSSE group consists of approximately 50 researchers.

Main tasks. In ADVANCE SOUTHAMPTON will lead WP5, Process Integration, and WP7, Management, and make a number of interrelated contributions. In the industrial deployment workpackages it will support the industrial partners in applying tools and methods through a mixture of training and expert advice and support. SOUTHAMPTON has considerable experience of teaching formal methods to undergraduates and postgraduates and also has considerable experience of supporting industrialists in the application of formal methods and tools. SOUTHAMPTON has experience of repository hosting (eg event-b.org, deploy-eprints.ecs.soton.ac.uk) and of workshop organisation (eg the Rodin workshop). SOUTHAMPTON has a lot of experience of combining methods and of developing methodological approaches which it will bring on-board for the WP5.

SOUTHAMPTON has contributed to the design of the Rodin platform and has developed Rodin plugin tools for model checking B (ProB) and for linking UML and B (UML-B). It will contribute to the development of tool support for the management of design patterns, decomposition of models and mathematical extensions of the language. SOUTHAMPTON will also contribute to the development of the multi-simulation framework and to the code generation work.

Senior Staff Members

Michael Butler is a Professor of Computer Science at SOUTHAMPTON where he leads the DSSE Group. He is internationally recognised as leading in refinement-based formal methods. He holds a PhD (Computation) from the University of Oxford. His research work encompasses applications, tools and methodology for formal methods, especially refinement based method such as B and Event-B. He has made key methodological contributions to the Event-B formal method, especially around model composition and decomposition. He plays a leading role in the development of several tools for B and Event-B especially the Rodin toolset. Butler has a strong track record of collaboration with industry (Siemens, Bosch, Critical Software, SAP, NASA, RailSafe and Space Systems Finland). Butler serves on the PC of many international conferences. He is PC Chair of FM2011, the leading international conference on formal methods. He is a Fellow of the British Computer Society, is Vice-chair of IFIP WG 2.3 Programming Methodology and is on the editorial boards of the Formal Aspects of Computing and Critical Computer-Based Systems journals.

John Colley has 20 years industrial experience in the Electronic Design Automation field, both developing and managing the development of software tools for hardware verification, spanning Verilog and VHDL simulation, code and state machine coverage and model checking. He was also responsible for the development of co-simulation interfaces to support third party logic and analog simulators, C models and hardware emulators. He has a PhD in Computer Science from the University of Southampton.

Colin Snook was heavily involved in the development and application of the UML-B tool in the MATISSE, PUSSEE, RODIN and DEPLOY projects. He received a PhD in Computer Science from the University of Southampton in 2002 and has published many papers on UML-B and U2B. Before his PhD he worked for ATEC developing safety critical control software.

Dr Bernd Fischer is Senior Lecturer in the DSSE Group. His expertise is in the development of high-assurance code generation methods. He is experienced in the application and development of automated reasoning tools such as first-order and higher-order theorem provers and software model checkers, and has also worked with semi-formal methods such as safety cases. Before joining SOUTHAMPTON in 2006, he has spent 8 years at the NASA Ames Research Center, where he developed the certifiable program generation approach, and has ongoing collaborations with NASA. Fischer has published more than 50 papers in the area of formal approaches to software engineering. He was PC Chair of the conference on Generative Programming and Component Engineering (GPCE'09) and is member of the IFIP WG2.11 on Program Generation.

B.2.3 Consortium as a whole

B.2.3.1 Consortium partners

Europe is in a unique position to conduct a project such as ADVANCE due to its traditional leading role in formal methods and tool development and due to considerable level of acceptance and understanding of formal methods in industry. The main criteria for selecting the ADVANCE partners was in choosing complementary

organisations with the excellent track records capable of working together to achieve the ambitious objectives of the project by delivering novel results through a tight inter-partner cooperation. It is our belief that we have built a consortium that will create added value by consolidating efforts of various partners.

The consortium has been built with great care and is based on a delicate balance between three kinds of partners:

- Industrial partners
- Academic partners
- Project Service Providers

The reasons for this organisation are carefully explained below.

Industrial Partners

Successful deployment of advanced engineering methods in industry, which is the ultimate goal of ADVANCE, can only be achieved if it can be demonstrated that industrial business units will eventually use this approach in the development of actual products. Therefore the industrial side of the consortium consists of two companies who have long recognised the benefits of formal methods and who are prepared to take the necessary steps to implement them.

Critical Software Technologies Ltd (CSWT) designs, develops, tests, validates and assures software for mission and business critical information systems across the Defence, Aerospace and Energy domains and has already participated in several EU RTD projects in FP5, FP6 and FP7.

Alstom Transport Information Solutions (AT), 4700 employees worldwide, is a leading company of the rail signalling industry. Its mission is to supply rail operators with complete solutions that allow them to operate high-density mainline or urban networks in complete safety while informing passengers and optimising resources in real-time. The solutions meet network requirements and regulations at local, national and international levels.

Academic Partners

These are the four roles the academic partners play in ADVANCE:

- The academic partners will assist the industrial partners in use of formal and simulation-based methods that emerge during the ADVANCE project. This role will consist of spending time with the industrial partners so that they will be able to acquire an adequate level of understanding of formal and simulation-based methods in the ADVANCE context as well as experience in using the tools which they will need for their case studies.
- The academic partners will learn from the difficulties encountered by the industrial partners in incorporating these methods in their development processes and will also learn about any difficult technical problems encountered by the industrial partners, with a view to providing research effort into solutions
- The academic partners will have an important role in conducting active research in the field of formal and simulation-based methods. Too often research in this field has concentrated on theoretical problems that are removed from the real problems encountered by industry. Here, thanks to experience gained from the DEPLOY project, the academic partners will be confronted by real problems, whose solutions will be of direct help to the industrial partners.
- The academic partners will also be very active in the development of tools in close contact with the practical tool developers (see below). Here too, the academic partners will develop new technologies by liaising with the industrial partners and thus finding out the kinds of difficulties they encounter in their practical usage of the methods.

There are two academic partners.

- SOUTHAMPTON has a very strong formal method group, which has devoted itself to the application of formal methods to industrial case studies and to the development of practical tools: within the framework of the FP7 project DEPLOY. Southampton has developed a powerful Eclipse-based tool linking UML to Event-B and has expertise in simulation, co-simulation and coverage technologies.
- UDUS also has a very strong formal method group, which has its roots in Southampton: they have already been very active in developing tools for model checking, coverage and animation with the Event-B method.

Both academic partners have traditionally strong links with industry and have been successfully working on industrial applications of formal methods and tools with the major international companies. The academic staff of ADVANCE includes researchers who laid the foundation of the modern formal methods and tools, as well as their successful industrial applications.

Project Service Providers

In a project such as ADVANCE, where the ultimate goal is the transfer of the formal methods technologies to various industries, it is of utmost importance to have a very strong open tool basis, which can be used and customized by the various participants.

For this goal to become a reality, it is extremely important to continue to develop and extend the tool kernel and plugins, which will be used throughout the project.

- SYSTEREL has a very strong expertise in the Rodin tool platform developed for Event-B. More precisely, the project leader of the Rodin platform, which was developed at ETHZ (Laurent Voisin), is now working with SYSTEREL together with a number of other engineers, who have a wide expertise in using B in real industrial projects. Through a subcontract, SYSTEREL brings to the consortium the outstanding experience of Jean-Raymond Abrial, the originator of B and Event-B. This company will not work in isolation: they will have substantial contact with the academic partners involved in the development of plugins. Moreover, their expertise in B and the tools will make them also one of the major contributors to training of the industrial partners.

B.2.3.2 Complementarity between partners

- The pure industrial participants provide and develop methods which broaden the scope for the application of formal engineering methods to their business domains
- The academic partners work with the industrial participants to learn from, and develop solutions to, the difficulties they encounter
- The technology provider delivers mature tools to the two previous categories of partners

This combination of cross-fertilizing roles will allow the project as a whole to cover a wide range of research and engineering challenges identified by this project.

The geographical distribution of the partners (France, Germany, UK) will engage a considerable part of the EC market. Moreover, CSWT's parent company in Portugal have a keen interest in formal methods and will track the results of ADVANCE carefully.

B.2.3.3 Industrial involvement in exploitation

The tool exploitation will be carried out by SYSTEREL. The overall project dissemination will be conducted by all partners, including the industrial ones.

Each industrial partner will plan at the beginning of the project how they intend to disseminate the results of ADVANCE, both internally towards their business units and externally towards their clients.

B.2.3.4 SMEs

ADVANCE includes one SME, SYSTEREL. Formal methods, especially B and Event-B, represents a core part of their business.

B.2.3.5 Subcontracting

Jean-Raymond Abrial, the originator of Event-B and the Rodin platform has now retired. He is however providing consultancy on a part-time basis (less than 30 days per year). This situation does not allow him to enter the ADVANCE project on a full-partner basis. SYSTEREL, having a collaboration framework defined with him, has the possibility to bring the outstanding expertise of Jean-Raymond Abrial through subcontracting.

B.2.3.6 Summary

The table below shows the main contribution of each partner to ADVANCE and the expertise it brings to the project.

Table 1:

Partner/role	*Contribution to ADVANCE*	*Expertise*
CSWT (industrial partner)	• Smart Energy Grids Case Study • Project Management	• expertise in providing solutions for mission and business critical information systems • develops, tests, validates and assures software for mission and business critical information systems across Defence, Aerospace and Energy

		• has already participated in several EU RTD projects in FP5, FP6 and FP7
AT (industrial partner)	• Dynamic Trusted Railway Interlocking Case Study	• provides solutions to meet rail network requirements and regulations at local, national and international levels • a leading company of the rail signalling industry for the last 30 years • expertise with the B method and the ProB tool for system specification and analysis
UDUS (academic partner)	• scalable techniques and tools for animating and model checking industrial specifications • tool development (animation, model checking, constrained random testing, coverage) • expert support, in particular for WP1 and WP2, as well as training • implementation of new domain specific specification formalisms	• expertise in formal methods, particularly model checking and animation (ProB) • tool building expertise and related expertise in (constraint) logic programming, static analysis, Java, and Eclipse development • expertise in (domain specific) language implementation and optimisation • experience with several FP5-6-7 projects
SYSTEREL (service provider)	• further develop and strengthen the RODIN platform • develop plugins needed for industrial deployment • manage the integration of plugins developed by ADVANCE partners • training and expert support to industrial partners • tool exploitation during and after the ADVANCE project	• more than 10 years of experience in the development of safety-critical systems • strong experience in formal development to achieve SIL4 certification • expert knowledge of the RODIN platform architecture • considerable experience in managing and realizing industrial size projects • experience in tooling supporting the development process of SIL4 systems
SOUTHAMPTON (co-ordinator,academic partner)	• training and support for application of formal methods and tools in industrial deployment • research in methods for reuse, evolution and dependability • research and development of tools for model construction and analysis especially (UML-like front end, model checking, linking verification tools) • dissemination including publication, participation in and organisation of workshops, development of training material	• experience of application of formal methods with industrial collaborators • considerable experience of participation in EU projects involving formal methods • development of methods for use of formal refinement in distributed systems • development of Rodin tools for formal modelling (UML-B), decomposition, theory extension, code generation • many years experience of delivering training in formal methods

B.3 Impact

B.3.1 Strategic impact

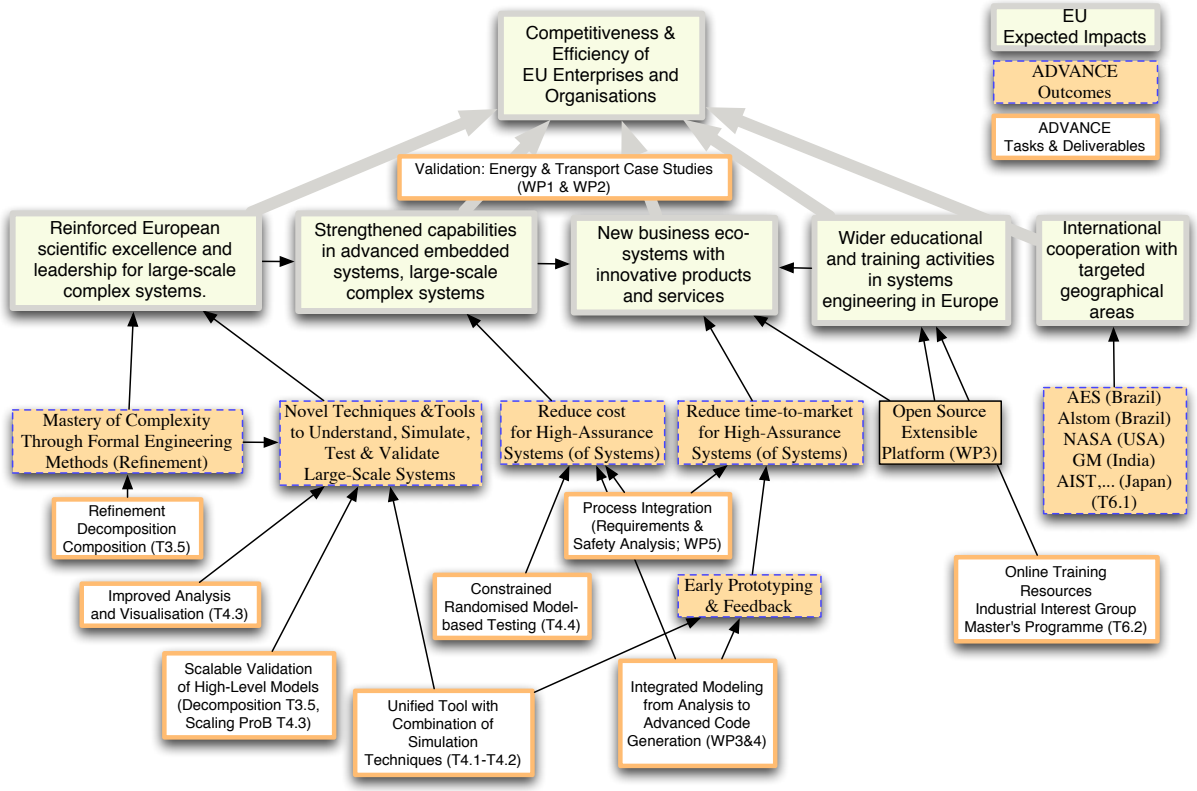

Figure 3.1: Key impacts of ADVANCE along with important outcomes required to achieve these impacts

B.3.1.1 Contribution towards the expected impacts

The primary impact of this proposal will be the ability to model and validate high-assurance cyber-physical systems, reducing the development cost and increasing the benefits of formal modelling.

More precisely, the ADVANCE project will achieve the following five expected impacts from the ICT workprogramme[2]:

1) Reinforced European scientific excellence and technological leadership in the design and operation of large-scale complex systems.

ADVANCE will enable the mastering of the complexity arising in large-scale complex systems through **formal engineering methods** in general and **refinement** in particular. The **scalability** in formal engineering tools will be improved and new ADVANCE technology will enable humans to better understand and design large-scale systems through **novel validation** / **verification** / **testing** techniques and tools.

2) Improved industrial competitiveness through strengthened capabilities in advanced embedded systems, in monitoring, control and optimisation of large-scale complex systems, in areas like energy, transport, and production, and in engineering of SoS.

Obviously, Impact 1, and all ADVANCE activities working towards it, will also work towards achieving impact 2. In addition, ADVANCE will achieve increased competitiveness by reducing the cost to develop **large-scale systems**, in particular high-assurance cyber-physical systems. The project will pay particular attention to the

[2] From **Objective ICT-2011.3.3**. They in turn aim at improving the competitiveness and efficiency of EU enterprises and organisations.

needs of the **transport** and **energy** sectors. The cost of using formal engineering methods will be decreased, while the benefits further increased in the form of an integrated tool environment with support for multi-simulation and testing.

3) New business eco-systems providing innovative products and services based on SoS.

Achieving impact 2 obviously also contributes towards achieving impact 3. In addition, ADVANCE will reduce the **time** to **market** for developing complex systems, in particular high-assurance systems. In particular, the formal models can be analysed and simulated very early in the development life cycle. The **open source platform** will enable external companies to apply the techniques and extend the tools for their needs, notably to incorporate domain specific requirements and new simulation tools. The use of the well-supported and open Eclipse platform as the foundation will ensure a broad audience. The transport and energy workpackages 1 & 2 of ADVANCE are novel applications of cyber-physical systems, and our workprogramme will ensure impact 3) can be achieved. Parts of those workpackages will measure to what extent the impacts 2 and 3 have been achieved.

The experience of CSWT and AT reveals that aerospace, energy, railway and other markets demand for more complex systems developed in short timescales and with reduced budgets. The problem becomes even more critical in civil markets open to companies based in India, China, where rates offered, put European companies under extreme pressure making them less competitive. In parallel with this major systems integrator companies/institutions such as EADS, BAE, ESA overspend large amounts of money due to problems with requirements specifications, lack of a common integration framework easily adaptable to various domains. The work developed in ADVANCE will provide the framework that System Integrators require to manage efficiently the integration of various sub-systems. ADVANCE outcomes as detailed in the previous paragraphs provide innovative products and services which will be fundamental to address market trends, increase the competiveness of European companies in the global market and reinforce the technological leadership of Europe.

4) Wider educational and training activities in systems and control engineering in Europe at all levels.

The new knowledge, techniques and tools will be made available to European companies in the form of online training resources, building on top of the open source platform. An **industrial interest group** will ensure the industrial training requirements are met, and can provide new companies with assistance. In addition, modules in the Master's programme at the Universities of Southampton and Düsseldorf will ensure training of the next generation of students.

5) International co-operation with targeted geographical areas creating mutual benefits which will further European interests on focused technical topics.

We are having close ties with the following companies: AES and Alstom from Brazil, NASA from the USA, General Motors from India and the National Institute of Advanced Industrial Science and Technology (AIST) in Japan.

These companies and institutes have a keen interest in using Event-B and we are already collaborating with them on industrial applications of Event-B. We will communicate with these companies using our industrial interest group (Task T6.1). In addition to increasing the dissemination of our project's results, we will ensure that the ADVANCE methods and tools will be useful to a wider range of industrial applications by incorporating the feedback from these partners. AIST in particular is leading a three year project to increase the uptake for formal engineering methods in Japan. This is a unique opportunity for ADVANCE to disseminate European research results and to establish tight links with companies using Event-B in Japan.

B.3.1.2 Important steps needed to bring about these impacts

Our workprogramme describes the important steps that are needed to achieve our impact. Figure 3.1 highlights the most important steps from the ADVANCE workprogramme and their relationship to the impacts. The industrial work packages WP1 and WP2 will validate the relevance and impact of ADVANCE. The initial steps of these work packages are of particular importance, because this is where the collaboration between the industrial and academic partner is started. While AT is already very experienced in applying the B formal method and already using ProB on realistic models, the academic partners must make a real effort to instruct CSWT and also understand issues incorporating Event-B within their development process.

Some advances in the formal engineering tools are essential to ensure that they can be applied productively to large scale models of systems of systems (WP3 & WP4), while advances in methodology are require to ensure the integration into existing design flows (WP5). The steps laid out in work package WP6 will instigate the synergies between academia and industry, and will maximise the impact of the contributions of ADVANCE.

B.3.1.3 Why this contribution requires a European approach

A European approach is imperative for ADVANCE. Indeed, the project builds upon Europe's lead in formal engineering methods, which is spread among various industrial partners and academic institutions around Europe . More concretely, ADVANCE builds on the Rodin platform, which was developed during the previous EU projects FP6 RODIN and FP7 DEPLOY. The required expertise for extending the Rodin platform for integrated modelling of large-scale cyber-physical systems is distributed among three EU countries: France (SYSTEREL) for the core platform and provers, UK (SOUTHAMPTON) for code generation, decomposition and refinement, and Germany (UDUS) for animation, model checking. The company SYSTEREL will ensure that the tool will be of a professional standard, while the academic partners will carry out the research to achieve the required unification and scalability of the techniques and the tool. The other industrial partners cover two different industrial sectors and will ensure the practical applicability and eventual wider impact of the project.

B.3.1.4 Accounts of other national and international activities

As already mentioned, our project builds upon the results of the FP7 DEPLOY project and FP6 RODIN project.

At the national level, the DFG (Germany) funded project GEPAVAS will deliver parallel and directed model checking for Event-B, which will further strengthen the novel validation techniques for large-scale systems to be developed in ADVANCE.

Ensuring software quality is a widespread concern among IT companies in Europe: more and more resources have to be devoted solely to quality assurance and testing. Hence, many EU projects try to improve the situation by developing novel techniques for model-based testing in a wide variety of settings and using a wide variety of approaches. Below is a list of those projects with a short summary of the project goals. We are already in contact with these projects, for example in form of a FP7 Collaborative Working Group which is led by Prof. Leuschel and Prof. Butler, as well as activities related to the FMCO symposium, which Prof. Leuschel and Dr. Hallerstede have organized in 2009. One distinguishing aspect or our project is the use of refinement to structure complexity and use of Event-B as semantic foundation to allow integrated modelling from early design on to code-generation. Still, we plan to collaborate with these projects and reuse results as much as possible.

PREDATOR (http://www.predator-project.eu). PREDATOR is an FP7 project (FP7-216008) which aims to improve the predictability of resource-constrained embedded systems by introducing resource-aware abstraction early in the design process. Current design methods focus on functional requirements and resource constraint violations are only detected later during validation, imposing severe re-work costs. The PREDATOR approach will enable generic, reliable architectural platforms to be developed with predicable behaviour. The uncertainty of real-time system behaviour and the penalties associated with this uncertainty will be reduced. The approach proposed by PREDATOR is entirely complementary to the refinement-based, correct-by-construction approach of ADVANCE and could be used in conjunction with ADVANCE simulation. There is therefore potential for collaboration with this project.

ProTest (http://www.protest-project.eu/). ProTest is a European Commission-funded project that is focused specifically on improving the reliability of service-oriented networks in the telecom sector. Based on the industry-standard telecoms language Erlang and its associated support library, the Open Telecom Platform (OTP), the project aims to develop a property specification language for service-oriented systems that can be used with Erlang/OTP to support property-driven testing. The project will also develop techniques for extracting properties automatically from test data. This approach contrasts with the approach proposed by ADVANCE where the property to be proved will be the validity of the refinement between abstraction levels and the properties used in system simulation will be derived from the formal model rather than the tests. Erlang, however, is a language which has natural synergies with Event-B and we will look to use the results from this project.

HATS (http://www.cse.chalmers.se/research/hats/). HATS, Highly Adaptable and Trustworthy Software using Formal Models, is an FP7 Integrated Project (FP7-231620) aims to bridge the gap between formal, architectural specification and software implementation by developing the Abstract Behavioural Specification (ABS)

language, a concurrent object-oriented modelling language that features functional data-types. ABS has been designed to provide a formal underpinning to the established, but informal, software product family-based (SWPF) development. ABS targets specifically behavioural specification, whereas the Event-B refinement method addresses all levels of specification from architectural to implementation. Behavioural specification case study results from this project will, however, be pertinent to ADVANCE.

Quasimodo (http://www.quasimodo.aau.dk/). Quasimodo is an FP7 project (FP-214755) which proposes the use of timed, hybrid and probabilistic automata to address the need to manage quantative constraints in the model-driven development of real-time systems. Quasimodo will allow the specification and analysis of stochastic elements as well as real time constraints, support the deployment of the design onto the target platform with efficient code generation and enable model-driven testing. As with the PREDATOR approach, the Quasimodo approach could be used in conjunction with ADVANCE simulation and there is potential for collaboration with this project.

MODELPLEX (http://www.modelplex.org/). The MODELPLEX FP6 project has developed an infrastructure for Model-Driven Engineering for the development and subsequent management of complex systems within a variety of industrial domains. Some of the goals are very similar to our own goals, and the ADVANCE project will profit from the MODELPLEX published results.

MADES (http://mades-project.ning.com/). The MADES FP7 project (FP-248864) will develop a model-driven approach for the development of embedded systems. The proposed approach relies heavily on model-to-model transformations, (e.g., translating to Alloy for validation). MADES will develop a dedicated language, based on the OMG standard, MARTE, which will support the full development process from design to implementation. ADVANCE will follow closely the emerging industry standards of which MARTE is a significant development.

MULTIFORM (http://www.multiform.bci.tu-dortmund.de/). MULTIFORM is an FP7 project (FP-224249) that is focused specifically on the integration and inter-operation of tools for complex control system development that use differing formalisms. Results from this project will be of value with respect to the wider deployment of the ADVANCE approach.

MOGENTES (https://www.mogentes.eu). MOGENTES, Model-based Generation of Tests for Dependable Embedded Systems, is an FP7 project (FP-216679) that aims to enhance significantly both the functional and constraint-related verification of dependable embedded systems. In particular it will address the requirements of the IEC61508, ISO WD 26262 and AUTOSAR standards for system stress and overload tests as well as functional safety tests. In addition to employing formal methods, MOGENTES will also develop fault injection techniques which are complementary to the ADVANCE simulation approach. There is therefore potential for collaboration with this project.

In the railway sector, INESS (http://www.iness.eu) is developing a European framework for rail industry. The aim of INESS is to develop specifications for a new generation of railway signalling systems to be used throughout Europe. This is relevant for WP1. SOUTHAMPTON is participating in one workpackage of the INESS project. This workpackage is using rigorous methods to validate and verify a UML model of a railway interlocking system. SOUTHAMPTON's contribution is to translate the UML model into UML-B and to use the Rodin tools to verify the model against given safety properties.

Another interesting project is Contrail (http://contrail-project.eu/), which is developing a complete Cloud platform. In previous work of the project partners, Event-B was used to formalize and validate data sharing agreements

Another related international activity is centred around the TOPCASED platform (http://www.topcased.org/). The platform promotes formal methods and model-driven engineering and is dedicated to critical embedded systems. Currently, it focuses on UML, OCL and SysML, while we focus on Event-B and refinement along with integrated formal modelling from analysis to advanced code generation. We will be closely following the development of the TOPCASED platform.

DESTECS (Design Support and Tooling for Embedded Control Software) is a consortium, funded under Call 4 of FP7 (contract number INFSO-ICT-*248134)*, that is working specifically on simulation methods and tools for the development of *fault-tolerant* embedded systems. DESTECS will develop a co-simulation environment

within which faults can be injected systematically to measure the fault tolerance of a system. We see potential for collaboration as we can offer the formal verification that they lack.

The *Artemis* industrial association and the *NESSI* initiative, while much broader in scope, are concerned with improved software development as well as with dependability of systems, software and services. Tony Hoare and Jay Misra, the internationally renowned computer scientists, are leading the development of an international Grand Challenge in Verified Software. This challenge involves applying theories and tools for software verification to large scale experiments in system verification through a coordinated international effort. ADVANCE will make a significant contribution to this challenge both thorough its industrial deployments and through its methods and tools.

B.3.1.5 Assumptions and external factors that may determine whether the impact will be achieved

It is crucial that the modelling environment suits the industrial users concrete needs and can be integrated into existing development chains. Work package WP5 on process integration was set up exactly to ensure the latter. Concerning the suitability, one industrial partner (AT) is already using B and Event-B to a considerable extent; its experience in the setting of the ADVANCE workprogramme will minimise the risk that our formal foundation is unsuitable in practice.

The achievement of the full impact will also depend on the effective eventual usage of the advanced engineering methods in the concerned industries. It will clearly also depend on strategic decisions made by these industries.

Such decisions, however, are outside the control of ADVANCE, as they depend on economic as well as political factors, but, ADVANCE's tight link with the two industrial users and its industrial dissemination activities, backed up by the experience gained in the DEPLOY project, will increase the possibility of such an outcome.

B.3.2 Measures for Dissemination and Exploitation

Michael Butler from SOUTHAMPTON, the leader of the WP6 External Dissemination and Exploitation workpackage will be responsible for coordinating all exploitation and dissemination activities, in close collaboration with the industry partners. Each ADVANCE partner will be responsible for defining its contribution to the dissemination and exploitation plan. The management of intellectual property will be the responsibility of the IP and risk committee, as outlined in B.2.1.

B.3.2.1 Dissemination of project results

Results will be disseminated in both industry and academic communities, the stress being put on industrial deployment. The industrial dissemination requires particular attention in order to convince a sufficient number of companies to use the tooling and its related methodology. That way, further exploitation will be facilitated at the end of the project. A key issue which we have recognised from the outset is the need to integrate our new tools with those in use in the industrial partners' existing development process.

An industrial interest group (IIG) will be established which will receive information about progress and results, and will be invited to workshops organised by the ADVANCE project. This will build on the existing group of industrial users of the Event-B language and Rodin toolset (e.g., Bosch, Siemens, SAP, Space Systems Finland, ClearSy, XMOS, NEC, ARM, GM, AeS Brazil, AWE).

ADVANCE will maintain an on-line repository of research results and use social networking media such as Facebook, Twitter and LinkedIn for dissemination.

Tool dissemination.

Hands-on sessions will be organised at the IIG dissemination workshops held at Month 16 and Month 28. These sessions will provide the opportunity to educate engineers and to allow them to use the tools in the context of their own application domains. They will also enable the ADVANCE developers to get feedback on how the tools and supporting documentation could be improved. Every major release will be announced publicly and presented in detail in the workshops.

ICT Project Dissemination.

ADVANCE will engage with collaboration activities organised by the ICT Objective "*New paradigms for embedded systems, monitoring and control towards complex systems engineering*" and participate in scientific workshops related to ICT Programme such as FMCO (Formal Methods for Components and Objects). The ADVANCE team will also participate actively in standardisation efforts in the rail and energy grid domains.

Outside Europe Dissemination.

Rodin is already being used in universities and industrial companies in North America, South America and Australia through the efforts of the DEPLOY projects. These users will be kept informed of the new tool developments and ADVANCE will look to expand the usage of Rodin outside Europe.

Education

The academic partners already use Rodin in undergraduate and postgraduate teaching. Training resources will be made available on-line and training material will be developed for use in the Masters programmes in both Southampton and Dusseldorf.

Transmission of information between the partners

The ADVANCE repository will be a combination of a public wiki and an eprints repository and will be managed by SOUTHAMPTON, who already manage the event-b.org and deploy-eprints repositories.

Sector-Specific Dissemination by the industrial partners

- AT will disseminate the results of the railway case study to the formal methods community, the railway industry and the standardization bodies. This will be achieved by presenting papers in dedicated conferences, and by participating in standardization committees.
- CSWT will be working closely with a number of Smart Grid owners during the WP2 development , will share the AVANCE results with these stakeholders and participate in the emerging standardisation efforts in this new domain.

Dissemination by the project service provider

SYSTEREL in their daily business already promote the use of Event-B for system modelling. The outcomes of ADVANCE will then naturally be integrated into this dissemination process. More precisely, in the scope of their business, SYSTEREL will provide educational sessions largely based on the ADVANCE outcomes, and also bring the existence and the benefits of such outcomes to the attention of their industrial customers.

Publications by the academic partners

The academic partners have very strong records in publishing their research results in leading international conference and journals. The DEPLOY project has resulted in more than a hundred research publications to date. We will continue this practice in ADVANCE, aiming to publish several papers each year targeted at a range of software engineering and formal methods conferences and journals.

Partners in ADVANCE will look to publish results into the appropriate community where possible. To this end, conference attendance is a must. Events we will look to target include:

International Conference on Formal Engineering Methods, International Conference on Dependable Systems and Networks, International Conference on Software Engineering, International Conference of Computer Safety, Reliability and Security, International Conference on Integrated Formal Methods, International Conference on Formal Techniques for Networked and Distributed Systems, International Symposium on Object-oriented Real-time Distributed Computing, International Computer Software and Application Conference, Computer Aided Verification, International Conference on Formal Methods and Software Engineering, International Automated Software Engineering Conference, International Symposium on Formal Methods, International Conference of B and Z Users, International UML Conference.

We will publish results in scientific journals such as the following:

ACM Transactions on Software Engineering and Methodology, Automated Software Engineering Journal, Formal Aspects of Computing, Formal Methods in System Design, IEEE Transactions on Software Engineering, International Journal on Software Tools for Technology Transfer, Journal of Automated Reasoning, Real-time Systems, Science of Computer Programming, Software-Practice Experience, Software and System Modelling, Software Testing Verification & Reliability

B.3.2.2 Exploitation of project results

The most easily exploitable results of the ADVANCE project are threefold:

- Tools, including the Rodin platform and the plug-ins developed during the lifetime of the project.
- Support documentation: user manuals, tutorials, examples, and methodological guides.
- Insight gained by industrial partners in applying formal methods to the case studies.

The participation of the industrial partners will bring them expertise in the application of formal methods, which will turn into a commercial advantage on their competitors. Moreover, the application of formal methods is well known to provide deep understanding of a problem domain, and thus will reinforce the proficiency of the industrial partners in their respective domain.

Tool exploitation

The Rodin platform is and will be open source, allowing anyone to use it, thanks to the provided support documentation. However, to ensure continued industrial usability, SYSTEREL will also provide on-going support of the platform on a paid basis. This service will be performed in tight coordination with the Rodin platform coordination structure, which is entering into force this year. SYSTEREL is already providing training for the Rodin platform and the use of Event-B modelling, and will continue beyond the end of the ADVANCE project. Finally, thanks to the achievements of the ADVANCE project, SYSTEREL will improve its service offer around the application of formal engineering methods.

The openness of the Rodin platform will also allow it to be used by the academic partner as a framework for further research around formal methods and new tools supporting them, beyond the ADVANCE project.

Standardization activities

Where appropriate the industrial partners will use the results of the successful case studies to contribute to their respective normative frameworks (such as IEC 61508 and EN 50128 for the transportation sector). As there is only one reference implementation of event-B, namely the Rodin platform, there is no plan yet to initiate standardization work around the Event-B language.

B.3.2.3 Management of intellectual property

Management of knowledge and intellectual properties will be dealt with by way of a Consortium Agreement. This document will be developed, signed and in force during the contract negotiation period. The process will be driven by experts at the Coordinating Institution (CSWT) and the negotiation of this agreement will make use of appropriate expertise throughout the Consortium.

The tools developed in WP4 will be released as an open source. The licensing policy chosen is EPL (Eclipse Public Licence).

B.4 Ethical issues

ETHICAL ISSUES TABLE

	YES	PAGE
Informed Consent		
• Does the proposal involve children?		
• Does the proposal involve patients or persons not able to give their consent?		
• Does the proposal involve healthy adult volunteers?		
• Does the proposal involve Human Genetic Material?		
• Does the proposal involve Human biological samples?		
• Does the proposal involve Human data collection?		
Research on Human embryo/foetus		
• Does the proposal involve Human Embryos?		
• Does the proposal involve Human Foetal Tissue/ Cells?		
• Does the proposal involve Human Embryonic Stem Cells?		
Privacy		
• Does the proposal involve processing of genetic information or personal data (eg. Health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction)		
• Does the proposal involve tracking the location or observation of people?		
Research on Animals		
• Does the proposal involve research on animals?		
• Are those animals transgenic small laboratory animals?		
• Are those animals transgenic farm animals?		
• Are those animals cloned farm animals?		
• Are those animals non-human primates?		
Research Involving Developing Countries		
• Use of local resources (genetic, animal, plant etc)		
• Benefit to local community (capacity building i.e. access to healthcare, education etc)		
Dual Use		
• Research having directly military application		
• Research having the potential for terrorist abuse		
ICT Implants		
• Does the proposal involve clinical trials of ICT implants?		
I CONFIRM THAT NONE OF THE ABOVE ISSUES APPLY TO MY PROPOSAL	√	

References

[1] European Commission. *Framework 7 ICT Workprogramme 2011/12*.

[2] President's Council of Advisors on Science and Technology. *Leadership Under Challenge: Information Technology R&D in a Competitive World: An Assessment of the Federal Networking and Information Technology R&D Program*, 2007. http://www.nitrd.gov/Pcast/reports/PCAST-NIT-FINAL.pdf

[3] Event-B and Rodin website http://www.event-b.org/

[4] J. R.Abrial, M. Butler, S. Hallerstede, T. S.Hoang, F. Mehta, L. Voisin. *Rodin: An Open Toolset for Modelling and Reasoning in Event-B*. Intl J on Sw Tools for Tech Transfer (STTT), Vol 12, Num 6, 2010.

[5] Eclipse website: http://www.eclipse.org/

[6] DEPLOY Project Website: http://www.deploy-project.eu/

[7] Cooper, D. 1985. Overview of Theorem Proving. *SIGSOFT Softw. Eng. Notes* 10, 4 (Aug. 1985), 53-54.

[8] A. Voronkov. First-Order Theorem Provers: the Next Generation. Extended Abstract. citeseer.ist.psu.edu/656327.html.

[9] D. Jackson. *Software Abstractions: Logic, Language, and Analysis*. MIT Press, 2006.

[10] G. J. Holzmann. The Model Checker Spin, *IEEE Trans. on Software Engineering*, Vol. 23, No. 5, May 1997.

[11] L. Burdy, Y. Cheon, D. Cok, M. Ernst, J. Kiniry, G. T. Leavens, K. Rustan M. Leino, and E. Poll. An overview of JML tools and applications. *International Journal on Software Tools for Technology Transfer*, 7(3):212-232, June 2005.

[12] M. Barnett, K. Rustan M. Leino, and W. Schulte. The Spec# programming system: An overview. In *CASSIS 2004*, LNCS vol. 3362, Springer, 2004

[13] T. Ball, S. K. Rajamani. The SLAM Project: Debugging System Software via Static Analysis, *POPL 2002*, January 2002.

[14] D. Beyer, T. A. Henzinger, R. Jhala, and R. Majumdar. The Software Model Checker Blast: Applications to Software Engineering. *Int. Journal on Software Tools for Technology Transfer*, 2007.

[15] J.-R. Abrial. *The B-Book*. Cambridge University Press, UK, 1996

[16] J.-R. Abrial, *Modeling in Event-B*, *System and Software Engineering*, Cambridge University Press 2010

[17] M. Leuschel, M. Butler, *ProB: An Automated Analysis Toolset for the B Method*. International Journal on Software Tools for Technology Transfer, 10 (2). pp. 185-203, 2008.

[18] S. Yeganefard, M. Butler, and A. Rezazadeh. *Evaluation of a Guideline by Formal Modelling of Cruise Control System in Event-B*. In: Proceedings of the Second NASA Formal Methods Symposium (NFM 2010), Washington DC. 2010.

[19] M. Jastram, S. Hallerstede, M. Leuschel, A.G. Russo. *An Approach of Requirements Tracing in Formal Refinement*. In: VSTTE'10 Verified Software: Theories, Tools and Experiments, Edinburgh 2010.

[20] E. Troubitsyna. *Integrating Safety Analysis into Formal Specification of Dependable Systems*. In Proc. of Intl IEEE Workshop on Fault-Tolerant Parallel and Distributed Systems. IEEE Comp. Society, 2003.

[21] D. Brown, H. Delseny, K. Hayhurst, V. Wiels. *Guidance for Using Formal Methods in a Certification Context*. ERTS 2010, Toulouse May 2010.