www.advance-ict.eu

Advanced Design and Verification Environment for Cyber-physical System Engineering

Newsletter 4, December 2014

INTRODUCTION

Welcome to the fourth and final edition of the ADVANCE newsletter. The vision of the ADVANCE project was to develop an integrated toolset that combined formal verification for deep analysis of system models with simulation for extensive validation of models based on realistic scenarios. This enables early stage analysis of cyber-physical systems, detecting specification and design errors early in the development process, prior to developing software-based control and integrating it with physical systems (or indeed prior to building the physical systems themselves). In this newsletter we report on how this vision has been realised with stories on the two major ADVANCE case studies on smart grids and railway interlocking. We also report on the very successful ADVANCE Industry Days, summarise the main tooling contributions of ADVANCE and conclude with plans for further exploitation of the ADVANCE results.

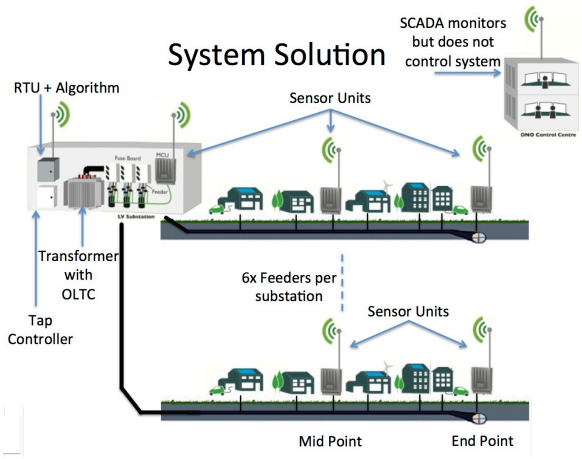
John Colley, *University of Southampton*

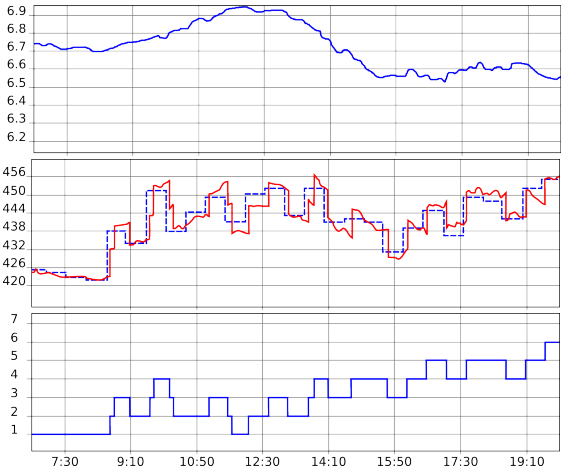
ADVANCE IN SMART GRIDS

Traditionally in electricity grids, energy flows from large generation stations down through the network to local consumption points. New localised electricity generation mechanisms (e.g., solar panels and wind turbines) and new consumption patterns (e.g., electric vehicles and heat pumps) introduce more complex patterns of energy flow through electricity grids. A major challenge facing electricity distribution operators is managing the new energy flows effectively. Addressing this challenge, Critical Software and Selex ES have completed a case study on applying ADVANCE methods and tools to automated voltage control on a smart grid. The case study was linked to a pilot project with a UK network operator and involved the use of an automated voltage

controller at a low voltage substation. The voltage controller is managed by a control algorithm that monitors voltage levels at multiple points on the low voltage network.

Critical Software and Selex ES used a combination of STPA-based safety analysis and formal modelling in Event-B to identify and analyse the system requirements on the voltage control. Through the use of ADVANCE formal verification technology, they were able to identify a number of issues around boundary cases and subtle behavior that were previously unknown. Verification was performed using a combination of automated theorem proving and model checking (ProB). ***Formal verification led to identification of improvements to the specification of the control algorithm with the advantage that these modifications were performed early in the development cycle, prior to implementation and testing.***





In order to validate the behaviour of the Event-B model of the voltage control against realistic environmental conditions, the ADVANCE multi-simulation framework was used. This allowed the Event-B controller model to be co-simulated using ProB together with a continuous model of the environment. The environment model was written in Modelica and was based on publically available models of energy generation and consumption. The graphs shown here illustrate the results of a co-simulation over a 12 hour period, with the transformer 'tap' position being controlled by the Event-B model (lower graph), and the medium voltage (top graph) and output voltage (middle graph) being generated by the Modelica model. ***The co-simulation demonstrated that the Event-B controller model behaved as expected for realistic environmental scenarios***.

BMotion Studio is a plug-in that enables the development of a graphical visualisation of states of the models in a way that is meaningful for the domain. This was used to produce a visualisation of a low voltage network that represents the topology of the network and the voltage levels at different points in the network. In the visualisation, the green lines represent transmission lines where the voltage is at a safe level while the yellow lines represent cases where the voltage is close to the boundary of the safe level. ***This visualisation was essential in comprehending the results of the simulation and in demonstrating the validity of the simulation to domain experts***.

As well as representing the simulation outputs visually using the ADVANCE tools, the formal model was also represented graphically using the UML-B state machine feature. This allows model to be represented as graphical state machines that are automatically translated to textual Event-B models to which formal

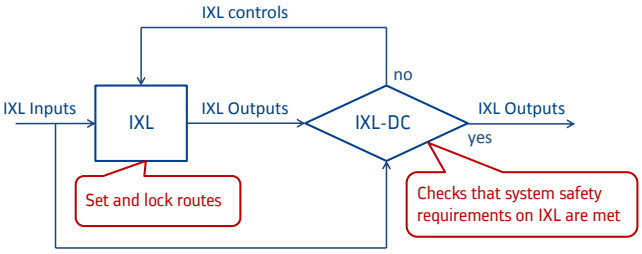
verification and co-simulation can be applied. It was felt that graphical representation of state machines makes it easier for domain experts to understand and develop formal models, thus easing the path to adoption.

The smart grid case study has demonstrated that the ADVANCE toolset does provide an engineering value in terms of avoidance of design errors early in the design cycle through modelling, verification and simulation. The ability to perform formal verification, simulation and visualization of results, along with support for formal graphical notations, all within the single ADVANCE toolset, was found to be very complementary. In the future, it is anticipated that 10,000s to 100,000s of automation devices will be deployed on low voltage distribution networks in the UK. The impact of any faulty operation of these new controls could result in poor service provision to customers, and might result in unsafe conditions. The cost of modification to correct errors in deployed systems could be high and therefore there is potential for a cost benefit to ensuring that systems deployed are "right first time". Selex ES and Critical Software will continue looking at opportunities to apply the ADVANCE toolset to follow on work on future smart grid projects for UK energy providers.

Jose Reis, Brett Bicknell, Karim Kanso, *Critical Software Technologies*
Neil Rampton, *Selex ES*

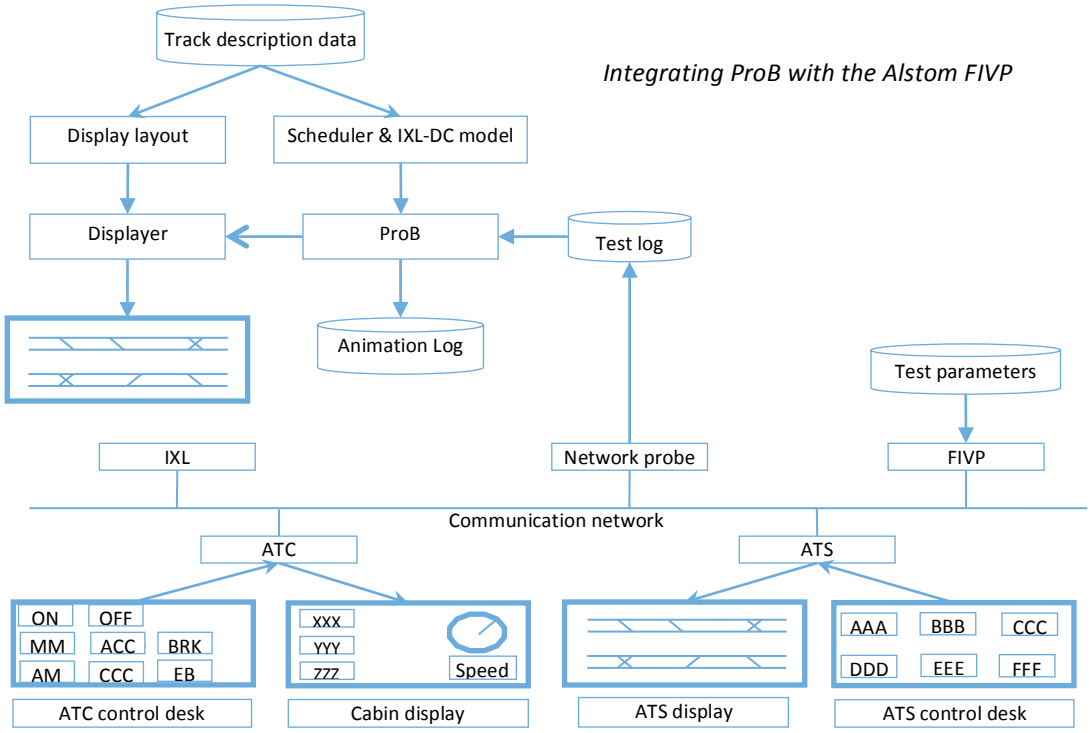
ADVANCE IN RAILWAY INTERLOCKING

Alstom have applied the ADVANCE methods and tools to a railway interlocking (IXL) Dynamic Controller (DC). The purpose of the IXL-DC is to check the safety of decisions made by the IXL on route setting and locking during operation. The advantage of separating the setting from the checking is that the IXL-DC can be superimposed on top of existing interlocking systems while still providing a provably safe interlocking system.



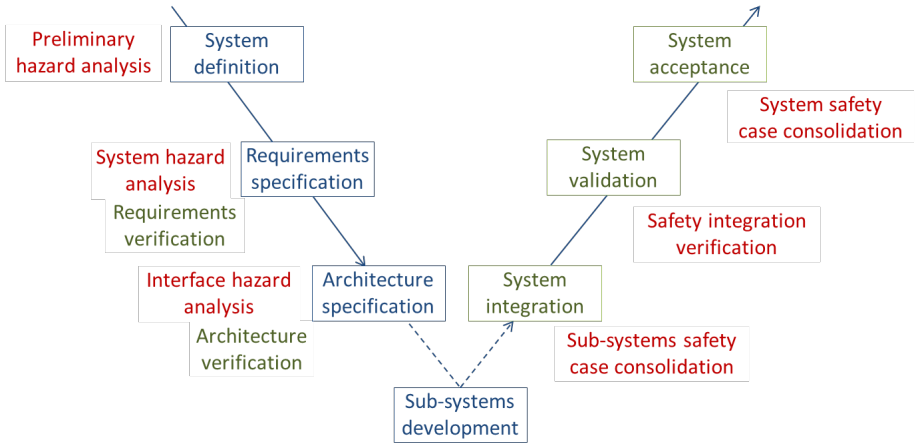
Following the ADVANCE process flow, hazard analysis using STPA was applied to identify the system-level safety properties. The STPA analysis focused on analysis of the control actions of the IXL, identifying how these might lead to hazards and thus what system level safety properties are required to prevent hazardous control actions. The system-level safety properties were formalized in Event-B and formal verification was used to provide proof that the system model complies with the safety requirements. The advantage of using Event-B for modelling and proof is that the IXL-DC model is made of a generic part proved once and for all and a specific part verified formally for each rail project. Using deductive proof means that the verification technique for the generic model is independent of the complexity and the implementation technology of the IXL. Extensive use was made of the Theory plug-in supported by the ADVANCE toolset. This allowed for the development of a set of domain theories relating to interlocking that helped to achieve greater reuse in modelling concepts and in proof rules.

The IXL-DC model was specified, created and validated following an integrated system development process. The Event-B model of the IXL-DC was tested in realistic conditions using the automated animation features that integrated the ProB model-checking and animation engine with Alstom's existing factory integration and validation platform (FIVP). This platform allows the testing of signalling systems in conditions close to real operating conditions, notably with the description of the specific operation lines and with continuous models of actual trains operated on these lines. A test log contains all the dated messages exchanged by the components of the signalling system during the test in the order they were sent, and represents, in some cases, several hours of operation during which most of the operation situations occur. Thus, a test log contains all the information needed by the IXL-DC and reproduces faithfully the environment of the IXL-DC.



Integrating ProB with the Alstom FIVP

Based on the case study experience, Alstom have developed a strategy for integrating ADVANCE methods and tools into Alstom's system development process in a way that contributes to the certification of Alstom's systems. The Alstom process complies with the requirements defined in CENELEC standards EN50126 and EN50129, and involves design, validation and verification, and safety activities. Those points in the Alstom development process where ADVANCE methods and tools could contribute to certification according to the CENELEC standards were identified. The safety activities and the activities of creation, validation and verification of Event-B models within the system development life cycle were identified and the evidence that these activities must provide was defined. ***The fact that the evidence is based on formal models and formal verification should strengthen the confidence of assessors and certifiers in the effectiveness of the actions taken to eliminate or mitigate the hazards. Also by basing certification on a pre-proved generic model, we are in a position to reuse certification effort across multiple projects.***



Taken separately, proof and simulation are powerful and useful techniques. But they are complementary and put together, as in ADVANCE technology, their power and usefulness is multiplied. Testing models in realistic conditions, as we did it in this case study, allows validation of their suitability; and proving suitable models allows exhaustive verification of their correctness. Thus ADVANCE provides the means to develop "by construction" valid and correct models. ***Compared to current practice this is a major technological breakthrough that will undoubtedly improve quality of systems and generate considerable savings as it is widely known that the most difficult and expensive errors to disclose and correct are system-level errors.*** Alstom will continue to use the 'Classical' B Method for software development, supplementing this with

ADVANCE technology for *system* level verification and validation. ADVANCE technology and Classical-B together provide an almost continuous and consistent formal development process, from system-level specification to software-level implementation.

Fernando Mejia, *Alstom*

ADVANCE INDUSTRY DAYS

The ADVANCE project held two industry days in the autumn: Southampton on Wednesday 24th September 2014 and Dusseldorf on Thursday 23rd October 2014. The aim of the industry days was to promote the results of the ADVANCE project through the industrial case studies, highlighting the ADVANCE process and its integration with existing processes and the role of the tools in supporting the process. Two external industrial, early adopters of the ADVANCE technology (AWE, Thales) also presented their experiences with the methods and tools and the benefits of incorporating ADVANCE into their existing processes. Both days were a great success with a range of industrial participants from Belgium, France, Germany, UK and USA.

Industry Day Programme:

- Overview of ADVANCE Process and Tools (University of Southampton)
- ADVANCE in Smart Grids (Selex ES, Critical Software): formal proof, requirements traceability and the application of FMI-based multi-simulation for testing and coverage
- ADVANCE in Railway Interlocking (Alstom, Systerel, University of Düsseldorf): requirements and hazard analysis, model visualisation and proof
- View from External industrial adopters:
    - AWE: Experience of Applying Rodin in an Industrial Environment
    - Thales: Formal Modelling of Railway Interlocking Using Event-B and the Rodin Tool-chain
- Tool demonstrations
- Discussion session

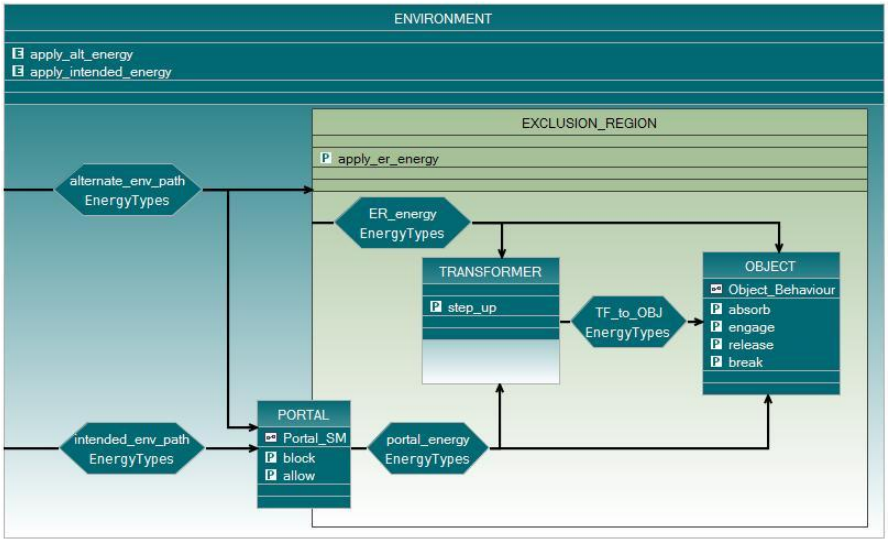
The slides are available on the ADVANCE website: http://www.advance-ict.eu/industry_days. The use of ADVANCE in smart grids and railway has already been covered above. We look in a little detail at the use by the external adopters and also summarise the main points of the discussion session.

AWE Experience of ADVANCE tools

A group in AWE (UK) has been using Formal Methods (in various forms) for over a decade. Their application of formal methods encompasses analysis of existing electrical/software systems, analysis of Safety Themes, and most recently, in applying mathematical rigour to the design of electrical systems. For this purpose, together with the University of Southampton, AWE developed a customisation of Event-B and UML-B called CODA. CODA provides a graphical interface and methodology to develop, analyse, and formally verify the interactions

between, and the behaviour of, the components of systems comprising both software and digital electronic hardware. CODA guides the designer to embrace modelling of the entire system. Extensive use is made of ADVANCE technology including ProB, UML-B and the SMT prover plug-in.

A recent application of the CODA methodology and tools, including tools supported by ADVANCE, analysed a slice of a system's functional behaviour. The formal modelling and verification forced resolution of ambiguities in the informal system definition, highlighted a disconnect between the requirements levels and ensured the problem was completely understood prior to implementation. Use of the SMT prover plug-in led to a very high degree of automation in the formal verification. Animation of the models using ProB helped to improve the confidence of the domain experts in the models. Overall the AWE team believe that the addition of mathematical rigour through CODA and related ADVANCE technology enhances their current engineering practice and is demonstrating benefits in an incremental manner.

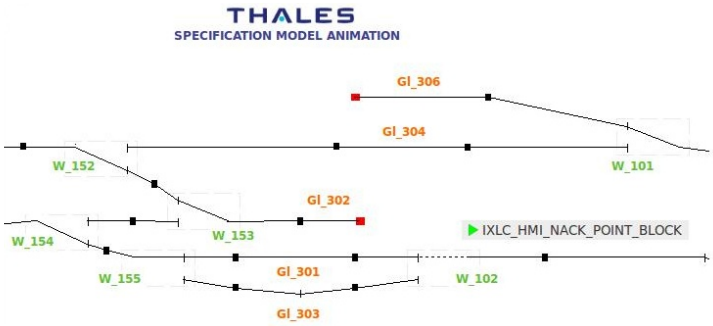


Thales Experience of ADVANCE tools

A group from Thales Transport has used Event-B and Rodin on an internal railway interlocking project. They made strong use of the UML-B feature supported in ADVANCE as engineers were already familiar with UML and this eased the adoption path. A particular emphasis was placed on producing a generic interlocking model that could be instantiated by specific rules about route locking since these rules can vary between rail operators. Supported by the Theory plug-in of Rodin, variability points in the model were represented by different definitions of mathematical operators visible within the model. Thales developed a feature model to represent the points of variability and selection of specific features is represented by selection of the relevant theory definitions. Generic safety properties are included in the generic model, and the Rodin provers are used to verify that instantiated models satisfy the generic properties. For example, here is a formalization of the property that a railway point should not move while it is blocked for a route:

```
IXLC_POINT
  ◦ safety_invariant_1: ∀ point · point ∈ POINT ∧ POINT_Block(point)=TRUE
                        ⇒ POINT_Moving(point)=FALSE not theorem ›Safety Invariant: a point that is blocked can not be moving
```

Thales made strong use of the ProB feature of Rodin to validate the Event-B models through animation. Visualisations of the ProB animation were developed to enable customers to provide early feedback on the validity of the models instantiated for their needs. The combination of proof and visual animation is allowing for detection of inconsistencies in product configurations early in the development process and this is viewed by the Thales team as being highly beneficial in terms of saving test and fix effort later. Thales have also explored the use of ProB to generate



functional tests from instantiated models and the use of code generation features to generate functional code. While these were viewed as promising, it was felt that further development is required to make them industrially usable.

Industry Day Discussion Outcomes

During the discussion sessions we asked the participants to address two questions:

1. ***What are the engineering challenges within your organization where ADVANCE technologies could help?***
2. ***What are the barriers to adoption of ADVANCE technology in your organization?***

For the first question, some participants identified the need for safety assurance methods for autonomous systems, such as UAVs, that are outside direct human control but where current methods are viewed as inadequate. It was felt that this might represent an opportunity for ADVANCE, especially because of the integration of simulation and verification supported by the ADVANCE tools. In networked systems-of-systems, where safety is intertwined with security, it was felt that the support for abstract modelling and analysis provided by ADVANCE could address a real need for having more rigour in system-level analysis. Many industrial designs start at very detailed levels, making meaningful analysis difficult. For certification of safety critical functions, traceability between high level safety requirements down to detailed designs is time consuming to construct and maintain; it was felt that the ADVANCE approach of linking requirements to high level models and refining high level models to detailed design models could make it easier to construct and maintain the consistency of the required traceability. More systematic and repeatable process for constructing safety cases was identified as a strong need. For cyber security, it is important to be able to understand unexpected behaviour as well as expected behaviour and the challenge of using ADVANCE tools for this purpose was posed. Participants who work on complex many-core processor architecture design said that the ability to explore alternative design choices for component interaction at the earliest possible design stages could lead to better designs. Many participants identified the need to achieve better reuse of designs and it was felt that the support provided by the ADVANCE approach for refinement, decomposition and theory definition might support this reuse at higher levels.

For the second question, the barriers to adoption, a key challenge identified by the participants is the need to find convincing ways of conveying the value to management of using tools such as ADVANCE in terms of both quality and cost. Undertaking more analysis at early stages of development would represent a significant change from existing practices and the value added by the extra effort upfront would need to be demonstrated early on. Another issue identified is that many organisations have adopted commercial tools for requirements management (such as DOORS) and simulation (such as Simulink) and ways of linking these to the ADVANCE tools would be essential. A range of competing modelling tools are available and it was felt that a clearer understanding of the benefits of ADVANCE tools over existing tools is required. It was felt that any tools would need to be robust and easy to use in order to be adopted and the ability to customize them for specific purposes would also be beneficial. Some organisations prefer to use domain specific tools rather than general purpose modelling tools and the ability to adapt ADVANCE tools to be domain specific would be important for these organisations. Some participants felt that a graphical representation for models (such as UML-B) was essential for their organisations while others felt this was less important. The need to train existing staff and the difficulty of recruiting staff with the appropriate skills was identified as a further barrier. An interesting discussion was also held around the issue of open source versus closed commercial tools and advantages (e.g., openness, low cost) and disadvantages (e.g., lack of vendor liability, lack of support) of open source were aired.

Michael Butler, *University of Southampton*

ADVANCE CONTRIBUTIONS TO THE RODIN TOOLSET

The ADVANCE tools referred to above are all part of the Rodin toolset for Event-B. Rodin is an open source Eclipse-based toolset that has been under development for a number of years prior to the start of ADVANCE. In ADVANCE we have made several significant contributions to the Rodin toolset. The core Rodin platform has been transitioned from Rodin 2.x to Rodin 3.x. This transition enabled strengthening of the API used by plug-in

developers to enable stronger enforcement of language rules thus preventing the construction of syntactic inconsistencies by plug-ins. Other major features developed by ADVANCE or greatly enhanced in terms of usability and performance are as follows:

- ProB: major performance and scalability improvements, new more flexible API
- Multi-simulation: support for integration of multiple simulation tools over FMI
- Theory plug-in: support for libraries of domain specific operators and proof rules
- Provers: SMT plug-in improves automated proof capabilities considerably
- BMotion Studio: much greater graphical flexibility through support for SVG
- ProR: support for traceability to safety analysis
- iUML-B: flexible integration with Event-B and richer state machine notation

The toolset is freely available and information on installation and use may be found here:

http://www.advance-ict.eu/tools

Michael Butler, *University of Southampton*
Michael Leuschel, *University of Düsseldorf*
Laurent Voisin, *Systerel*

SUSTAINING THE RODIN TOOLSET

The ADVANCE partners remain committed to continuing the maintenance and further development of the results of the project. The industrial partners have developed exploitation plans involving further use of the Rodin toolset on internal and client projects. The external adopters (AWE and Thales) are also planning to continue exploiting the toolset. We are in discussions with a number of other potential industrial adopters, some of whom became interested as a result of participation in the ADVANCE Industry Days. Systerel, University of Düsseldorf and University of Southampton will continue to offer professional services to support industrial organisations in adopting Rodin technology including training, support, tool customisation and new feature developments. Düsseldorf will provide services through their spin-off, FormalMind, while Southampton will provide services through their consultancy company, ECS Partners. Systerel, Düsseldorf and Southampton will continue to coordinate over the maintenance and evolution of the key features (e.g., core platform, ProB, Theory, SMT, UML-B, multi-simulation, composition). The ADVANCE partners would welcome collaboration with new partners seeking to explore the technologies.

Michael Butler, *University of Southampton*
Michael Leuschel, *University of Düsseldorf*
Laurent Voisin, *Systerel*

CONTACT

If you have any queries about the ADVANCE Project, please feel free to contact us:

Coordinator: John Colley (J.L.Colley@ecs.soton.ac.uk)

Or visit our website: www.advance-ict.eu