D.6.8 - PLAN TO DISSEMINATE AND USE FOREGROUND KNOWLEDGE

ADVANCE

Grant Agreement:	*287563*
Date:	*30/11/2014*
Pages:	*30*
Status:	*Final*
Authors:	*Luke Walsh, Critical Software, Michael Butler, University of Southampton*
Reference:	*D6.8*
Issue:	*1*

Partners / Clients:

FP7 Framework Programme	***European Union***

Consortium Members:

University of Southampton	***Critical Software Technologies***	***Alstom Transport***	***Systerel***	***Heinrich Heine Universität***	***Selex ES***

Project ADVANCE
Grant Agreement 287563
“Advanced Design and Verification Environment for Cyber-physical System Engineering”

ADVANCE Deliverable D.6.8

Plan to Disseminate and Use Foreground Knowledge

Public Document

December 15, 2014

http://www.advance-ict.eu

Authors and Contributors

Name	Contact	Description
Luke Walsh	lwalsh@criticalsoftware.co.uk	Author
Michael Butler	mjb@ecs.soton.ac.uk	Author
John Colley	J.L.Colley@ecs.soton.ac.uk	Contributor
José Reis	jreis@criticalsoftware.co.uk	Contributor
Michael Leuschel	leuschel@cs.uni-duesseldorf.de	Contributor
Fernando Mejia	luis-fernando.mejia@transport.alstom.com	Contributor
Laurent Voisin	laurent.voisin@systerel.fr	Contributor
Neil Rampton	neil.rampton@selex-es.com	Contributor

TABLE OF CONTENTS

1. Introduction

1.1 Objective

This objective of this document is to detail the plans of each member of the ADVANCE consortium with regard to their future use of the methods and tools developed under the project. It provides plans for commercial and educational (where appropriate) exploitation and general dissemination. It also outlines existing exploitation of ADVANCE methods and tools by external industrial users and other funded research projects. Dissemination activities focused on industrial audiences undertaken by project partners during the final period are described.

1.2 Audience

This document will be delivered to the European Commission under the FP7 funded project ADVANCE. It is also intended for public consumption and will be made available through the ADVANCE project website: www.advance-ict.eu.

1.3 Document Structure

Section 1 (Introduction) introduces the document.

Section 2 (Documents) presents the list of applicable and reference documents.

Section 3 (Commercial Exploitation) provides details of the commercial exploitation plans of each partner.

Section 4 (Educational Exploitation) provides details of the educational exploitation plans of each academic partner.

Section 5 (External Exploitation) provides details of exploitation of ADVANCE methods and tools by external industrial users.

Section 6 (Dissemination) provides details of project dissemination activities.

2. Documents

This section presents the reference documents for this report.

2.1 Reference documents

Table 1 lists the reference documents for the report. A document is considered a reference if it is referred but not applicable to this document. Reference documents are mainly used to provide further reading.

Reference document	Document number	Issue
[RD-1] D6.3 ADVANCE Communication & Dissemination Plan	CSWT-EUADV-2011-DOC-00258	2
[RD-2] ADVANCE Description of Work	-	4

Table 1: Reference Documents

3. Commercial Exploitation by Partners

The ADVANCE consortium was formed of industry and academic members who all have an interest in the Rodin toolset and the development of their formal methods offering. The aim for all members involved in the project has not just been the further advancement of the toolset, but also how best to utilise the toolset in a commercial market. As such, each member has drawn up plans to move forward commercially with the toolset post project completion. Below are provided details of the commercial exploitation details of each member:

3.1 Alstom Transport

Alstom specifically designed the IXL-DC to meet the requirements of the Paris railway operator, RATP, regarding the full compliance of interlocking systems with system safety requirements. Alstom will then integrate the IXL-DC in its response to the tenders of RATP for the revamping of existing urban lines (4 and 11) and suburban lines (RER B) and for the construction of the new lines 15 to 18 of the “Grand Paris” project. These projects represent, as regarding the interlocking system market alone, 20 to 30 million euros. Thus, in the short term the RATP market is the main target of Alstom’s IXL-DC, but it is not the only one. If opportunities arise, Alstom will propose the IXL-DC to all railway operators that demand formal and exhaustive verification of interlocking systems, the New-York City Transport Authority for instance. In the medium term Alstom will integrate the IXL-DC in all its interlocking systems, urban and mainline, and propose it to all railway operators.

The IXL-DC concept gave ideas of new and more innovative systems. Interlocking systems are built from a set of interlocking rules, also called “principles”, specific to each country and even to each railway operator. For instance the Belgian, British, German and French interlocking principles are all different. Moreover, in France, the interlocking principles of RATP and SNCF (French mainlines railway operator) are different. This raises the “variability” problem of interlocking systems, i.e. modifying an interlocking system originally developed for a given operator for an operator with different interlocking principles leads to high costs of verification, validation and maintenance. IXL-DC is reused in a project whose aim is to generate complete interlocking systems independent of interlocking principles as it ensures compliance with safety requirements (more or less) independently of the interlocking principles. This project is funded by the Belgian Wallonia region.

Alstom will integrate ADVANCE technology in Alstom’s system development process and will draw concrete benefits from this integration as it did when it integrated Classical-B technology in its software development process. Alstom’s system development process involves the conventional phases enforced by the CENELEC EN50126 standard: system definition, requirements specification, architecture specification, subsystems development, system integration, system validation and system acceptance. ADVANCE technology shall be integrated in these phases as follows. First, the STAMP/STPA hazard analysis method will be used by the safety assurance team during the requirements specification and the architecture specification phases in order to identify respectively system and interface safety requirements. Second, the Event-B technology – creation, animation and proof of an Event-B model of the system – shall be used by the design team during the requirements specification and the architecture specification phases. This is analogous with Alstom’s software development process that enforces the development of a Classical-B model of safety-critical software during the software requirements and architecture specification phases. Third, the Event-B system model will be verified as regarding compliance of the model with functional and safety requirements, relevance and completeness of the animation tests and correctness of the proof by the verification team at the end of the requirements specification and the architecture specification phases. This is analogous with Alstom’s software development process that enforces the same sort of verification of the Classical-B model of safety-critical software at the end of the software requirements and architecture specification phases. Fourth, the system integration and validation phases will use the results of the formal development of the Event-B system model to avoid safety-related tests covered by the animation tests and the proof of the model. This is analogous with the Alstom's software development process that avoids integration and unit tests of software components automatically generated from proved Classical-B components. The system process integrating ADVANCE technology provides means to design correct systems by construction and thus reduces validation and non-quality costs. That is why Alstom expects significant savings from the introduction of ADVANCE technology.

Some of the tools developed or improved in ADVANCE will be used for activities not directly related with development of Event-B models. This is the case with ProB. Alstom will use this tool to check the compliance of actual instantiation system data to formal instantiation data rules. Alstom will also use ProB to discharge the proof obligations of Event-B and Classical-B models that can be discharged by examining, in reasonable time, all their possible instantiations.

To create the IXL-DC model Alstom created and proved a mathematical theory of graphs. And, for the proof of that theory and of the IXL-DC model, Alstom created about 150 proof rules dealing with standard mathematical operators relevant to graph representations of railway networks. The graph theory shall be reused in other models as graphs are extensively used in railway models. The proof rules will be integrated in Alstom’s proof rule data base and thus will be reused for the proof of other Event-B and Classical-B models. Reuse of these objects will save considerable efforts in the development of systems and software.

3.2 Critical Software Technologies Ltd.

Formal methods forms a key part of the business development strategy for CSWT. That strategy is looking to with current and new customers to enhance its formal methods offering and to utilise it in full lifecycle development programmes. Throughout the term of the ADVANCE project CSWT has been working on parallel projects to further develop the toolset (in conjunction with the University of Southampton) and to introduce the toolset to wider markets. Post project CSWT plans to continue this work through its business development strategy and implement the following plans.

- Continue collaboration with Selex ES and look at opportunities to apply the ADVANCE toolset to follow on work on the LOVIA project:
  - Presentations to the wider Selex ES group to investigate how the toolset can be further used.
  - Other activities will be pursued with Selex ES but these cannot be made public as they are commercially sensitive
- Get involved in follow-up R&D work to further develop the toolset
  - Explore opportunities through Innovate UK to develop the toolset further into a specific sector.
- Further expand the industrial interest group and use that forum to disseminate knowledge to a wider audience including Prime Contractors, Distribution Network Operators and Government Bodies.
- Provision of support to customer
  - Provide consultancy services to customers who intend to use the toolset but that may not have the relevant background for its use or may have issues with its open source nature.
- Seek involvement with a working group aimed at supporting the development of a software/systems/safety engineering standard applicable to markets such as Energy.
- Disseminate the work with Critical Software group with a view to integrate aspects of the ADVANCE toolset with the software engineering process.

- Exploit usage of ADVANCE toolset to other markets in particular the aerospace market. Aerospace is an important market for CSWT and the latest DO-178C certification standard for airborne software will provide new commercial opportunities for CSWT for exploitation of the ADVANCE toolset. We will include the use of ADVANCE in our commercial offerings around aerospace certification.

3.3 Heinrich-Heine University of Düsseldorf

Heinrich-Heine University of Düsseldorf has many links with industrial partners including Alstom, Thales and Clearsy, and is keen to exploit the fruits of its research. Formal Mind bridges the gap between science and industry and was founded as a spin-off from the Heinrich-Heine University of Düsseldorf in response to the successful exploitation of the ProB tool within the EU FP7 project DEPLOY. FormalMind provides support and customization for the various parts of the Advance tool chain, in particular those centring around the open-source products ProB and ProR (but not exclusively). The Advance project will help UDUS and FormalMind adapt its tools for other markets, hopefully reaching a much wider audience than with the current railway centred activities. In future we plan to turn the existing co-simulation tool chain developed during the ADVANCE project into a product with commercial potential in many industrial domains. Currently, UDUS is conducting a three year research project with Thales Germany, which also uses the Advance developments for modelling the Thales Radio Block Centre (RBC). UDUS is also using the ProB tool to model the legal requirements about study options in various faculties and generate student time tables and find and analyse course combinations which cannot be studied within the legally required duration.

3.4 Selex ES

Selex is keenly interested in methods and tools that will help us ensure that new electricity grid control mechanisms are effective and trustworthy. Because of the increased deployment of renewable micro-generation, such as domestic solar panels, the trend in the UK electricity grid is away from a top-down structure where generation happens at the top levels towards a structure where generation happens at all levels. This introduces the needs for more automated monitoring and control of voltage levels at multiple points in the grid.

WP2 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. In the future, we anticipate 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 impact in unsafe conditions. The cost of modification to correct errors in deployed systems could be high and therefore there is cost benefit to ensuring that systems deployed are "right first time". We will continue our collaboration with CSWT looking at opportunities to apply the ADVANCE toolset to follow on work on the LOVIA project and future smart grid projects for UK energy providers.

We have also disseminated the ADVANCE results within the wider Selex ES group to encourage greater uptake in other business areas. To this end an internal dissemination event was held in early Dec 2014 for the UK engineering management (including engineering managers across multiple sectors of the business, and functional engineering leads), to present the ADVANCE approach and toolset. The company develops and delivers a wide range of electronics products, systems and solutions across the defence, aerospace and homeland security domains.

There was a clear interest expressed by the Selex ES engineering management team in the ADVANCE process and the potential benefits for other market sectors within the business.

An action was taken to investigate whether a suitable project could be identified for a more full exploration and evaluation of the process and techniques, so that the benefits can better be evaluated, to consider whether the ADVANCE approach should be adopted as a standard engineering process for relevant parts of the product development portfolio.

3.5 Systerel

Systerel has presented the results of the ADVANCE project to its regular customers at every opportunity, reinforcing the perception of its expertise in the application of formal methods in Industry.

In the first half of 2014, Systerel has already started applying the ADVANCE method in a service contract for a new customer. The service consisted in developing a formal model of a hoist in a light aircraft and proving it safe. The results of this contract have been very well perceived by the customer who had no previous experience with formal methods.

Finally, Systerel has also taken advantage of the expertise that it has gained developing the Rodin platform and associated plug-ins by winning several service contracts with one of its regular customers developing other Eclipse-based tools.

After the end of the project, Systerel will continue to leverage the results of the ADVANCE project to gain more contracts in formal modelling and tool development. Systerel will continue proposing professional service around the Rodin platform (maintenance and new feature development).

3.6 University of Southampton

Since 2010, the University of Southampton has been engaged in commercial activity around Rodin and UML-B through a consultancy company called ECS Partners (www.ecs.soton.ac.uk/business/consultancy). ECS Partners is owned by the School of Electronics and Computer Science at Southampton and has a full-time business development manager. ECS Partners has commercial contracts with a number of UK and international companies involved in safety critical domains based on Rodin and UML-B. Our role is principally around supporting adoption of Event-B, UML-B and Rodin within the organisations in the form of training, method support, tool support and tool customisation. We find that UML-B, developed at Southampton, is particularly attractive for industrial organisations and we will develop the profile of UML-B further to ease the adoption route by industrial organisations.

Our exploitation plans for the ADVANCE results will be to provide adoption support services for companies through ECS Partners that incorporates results from ADVANCE, in particular, linking safety analysis and UML-B. The current level of business has been achieved without any explicit marketing. We plan to market our services more clearly to grow and sustain the level of business to support a team of 4-5 staff in the immediate future. To manage a potentially larger level of business we will also consider spinning out an adoption support service as a company that is separate to ECS Partners. The business model will continue to use the open source tools developed in ADVANCE. In some cases, we will develop bespoke Rodin plug-ins for customers (e.g., specialised modelling plug-ins, code generators) on a commercial basis.

4. Educational Exploitation

As there are two academic partners within the ADVANCE consortium it provides a great opportunity for the knowledge gained and tools used/developed during the project to be passed on in an education forum. As such the consortium is able to disseminate the techniques used to ensure future understanding and exploitation by undergraduates and postgraduates. Below are the details of the plans for each of the academic partners:

4.1 Heinrich-Heine University of Düsseldorf

The University of Düsseldorf teaches formal engineering in a variety of modules, mainly at the Masters level. Similarly to Southampton, Rodin, Event-B and ProB are major components of those courses. In addition, many Masters theses are carried out in this area. The ADVANCE project provides those students a strong industrial relevance for their studies and theses. There is also a growing demand for graduates familiar with formal engineering methods. The Advance project (and any further project) will enable us to incorporate new results into the programme and ensure that we can prepare the students for work in the areas of CPS and safety critical systems.

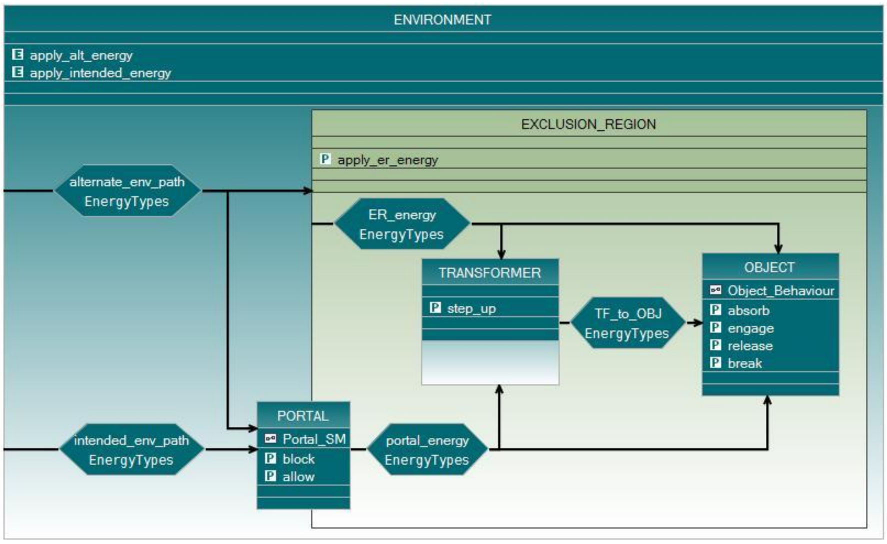
4.2 University of Southampton

The University of Southampton teaches courses at Bachelors and Masters level on formal design methods. Rodin, Event-B and UML-B are already major components of those courses. We also teach specialised short courses on Rodin and on multi simulation to PhD students. The curriculum for our Bachelors and Masters programmes is updated on a regular basis. This will give us the opportunity to incorporate new results coming from the ADVANCE project into our teaching programme. Using material that has strong industrial relevance is very attractive to our students and ADVANCE will provide a rich source of industrially-relevant training material.

5. External Exploitation

5.1 AWE

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 the entire system. Extensive use is made of ADVANCE technology including ProB, UML-B and the SMT prover plug-in.

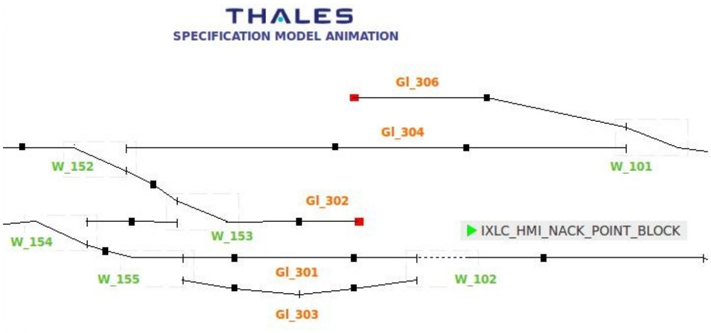


© British Crown Owned Copyright 2014/AWE

A recent application of the CODA methodology and tools, including tools support 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 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 practices and is demonstrating benefits in an incremental manner.

5.2 Thales

A group from Thales Transport have used Event-B and Rodin on an internal railway interlocking project. They made strong use of the UML-B feature support 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.

Thales made strong use of the ProB feature of Rodin to valid 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.

5.3 WITZ Corporation Japan

WITZ Corporation Japan (http://www.witz-inc.co.jp) and their subsidiary, Atelier, have used the B Method and Event-B on a number of projects. WITZ specializes in embedded software development for Japanese engineering organisations. Event-B was used by WITZ on two projects to date:

- Secure communications middleware
- Real-time control system

In both cases the modeling and formal verification using Rodin (ProB and Rodin provers) identified problems in the original specifications (security vulnerabilities and timing errors) and the use of the tool was viewed as ding considerable value to the WITZ engineering process.

5.4 Other Research Projects

Here we outline some other research projects that exploited ADVANCE methods and tools.

5.4.1 OpenETCS

OpenETCS is a European ITEA-2 Project in which Systerel brings its combined expertise in applying formal methods, railway signalling and dependability, to a consortium of 32 partners that are developing a formal model of the core of ETCS (European Train Control System) with the aim of helping different suppliers improve the interoperability of their respective solutions. In the OpenETCS project, Systerel have applied Event-B and Rodin to modelling and verification of part of the European Train Control System (ETCS) Specification.

5.4.2 HASTE

HASTE (2013-2014) is a project funded by the UK Defence Science Technology Laboratory (DSTL) looking at advance testing methods. The project was led by CSWT with Universities of Southampton and Leicester as partners. Southampton developed a demonstrator application of ADVANCE methods and tools on an aerospace related case study including the use of STPA for hazard analysis, and Event-B

5.4.3 PRiME

The PRiME Project, 2013-2018, is a large (£5.6M) multi-site UK project (funded by EPSRC) lead by Southampton on energy-efficient reliable many-core systems. ADVANCE methods and tools are being deployed in PRiME as part of the many-core runtime management workstream, including the use of Event-B modelling and verification, multi-simulation and code generation.

6. Dissemination

In this section we describe the main dissemination activities that ADVANCE partners undertook during the final period. The ADVANCE Industry Days were a key mechanism for dissemination of the final results and we also presented ADVANCE results at other events. A range of papers covering ADVANCE were published in relevant journals, conferences and workshops.

Post project all partners will continue with activities that will disseminate the knowledge of the ADVANCE project and its results. Several papers are currently under review and in preparation and partners will continue to prepare papers on the topics covered in the ADVANCE project. Also, ADVANCE partners will continue providing tutorials at various different workshops and seminars.

6.1 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 demonstrable 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, 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 and by the external adopters has already been covered above. We summarise here the main points of the discussion sessions.

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?***
3.

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 support by the ADVANCE tools. In networked systems-of-systems, where safety is intertwined with security, it was felt that the support for abstract modeling and analysis provided by ADVANCE could address a real need for having more rigour in system-level analysis. Many industrial design 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 earl 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 modeling 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 modeling tools and the ability to adapt ADVANCE tools to be more domain specific would be important for this 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) were aired.

6.2 ADVANCE Participation in Other Dissemination Events

November 2013

Michael Butler presented the ADVANCE methods and tools to the UK CDF (Crypto Developers Forum). This group consists of leading UK companies working in cybersecurity.

April 2014

Michael Butler and Colin Snook presented the ADVANCE methods and tools to the Thales UK Software Engineering Team. This group consists of the software engineering leads from the Thales UK business units of across the domains in which they operate (rail, defence, aerospace, cybersecurity).

Michael Butler gave an overview of ADVANCE at the UK Workshop on Cyber-Security of ICS and SCADA systems organised by the Research Institute for Trustworthy Industrial Control Systems, Airbus Group Innovations and the Airbus Centre of Excellence in SCADA Cyber Security & Forensics Research in Leicester.

June 2014

ADVANCE is contributing to the organisation of the 2014 Rodin User and Developer Workshop in Toulouse on 2+3 June. ADVANCE is contributing a tutorial session on the Theory Plug-in as well as several presentations covering on-going tool development work in ADVANCE.

July 2014

The University of Southampton had a showcase stand at the Farnborough Airshow, the major annual event for the UK aerospace industry. This included a presentation on ADVANCE methods and tools.

August 2014

Colin Snook, Vitaly Savicks and Jens Bendisposto gave an overview of ADVANCE and ran a project booth giving demos of Rodin, iUML-B, ProB2, BMotion Studio2 and Mixed-simulation as part of the European Project Space at the Simultech 2014 Confernce in Vienna.

October 2014

John Colley gave a tutorial on ADVANCE methods and tools at DVCon Europe (Design and Verification Conference and Exhibition) in Munich.

December 2014

Michael Butler presented ADVANCE methods and tools at a joint Lloyds Register / University of Southampton dissemination event. Lloyds Register is a leading certification authority across multiple domains and has recently moved a large part of its operation to the University of Southampton campus.

A poster on ADVANCE was presented at the GCHQ annual conference for the Academic Centres of Excellence in Cyber Security.

6.3 Website, Newsletters and Press Release

The ADVANCE public website was kept up to date with news, publications, training material and presentations from the ADVANCE Industry Days.

During the final period, ADVANCE produced two newsletters, one in June 2014 and the other in December 2014, highlighting key results (see appendix). As well as being placed on the ADVANCE website, the newsletters were distributed to the members of the ADVANCE Industry Interest Group (over 200 industrial contacts in Europe and internationally).

On behalf of the ADVANCE Consortium, the media relations team of Critical Software produced a final press release (see appendix) and targeted at industry and trade press. The following have published the press release.

All About Shipping

http://www.allaboutshipping.co.uk/2014/12/16/launch-of-advance-marks-new-phase-in-the-development-of-cyber-physical-systems/?utm_source=rss&utm_medium=rss&utm_campaign=launch-of-advance-marks-new-phase-in-the-development-of-cyber-physical-systems

Embedded Control Europe

http://www.embedded-control-europe.com/tools-software/4-tools-software/2442-advance-new-systems-engineering-framework

New Electronics

http://www.newelectronics.co.uk/electronics-news/engineering-framework-set-to-boost-system-development/66509/

Railway-technology

http://www.railway-technology.com/contractors/testing/critical-software/presslaunch-of-advance.html

Dataintellirail

http://dataintellirail.com/home.aspx

6.4 Publications in Period 3

6.4.1 Journal papers

1. Hallerstede, Stefan, Jastram, Michael, Ladenberger, Lukas (2014). A Method and Tool for Tracing Requirements into Specifications. Science of Computer Programming, 82: 2–21, March 2014.

2. Said, Mar Yah, Butler, Michael and Snook, Colin (2013). A Method of Refinement in UML-B. Software and Systems Modelling. December 2013.

3. David Déharbe, Pascal Fontaine, Yoann Guyot, Laurent Voisin (2014) Integrating SMT solvers in Rodin. Sci. Comput. Program. 94: 130-143.

4. Salehi Fathabadi, Asieh, Butler, Michael and Rezazadeh, Abdolbaghi (2014) Language and tool support of event refinement structures in Event-B. In, Formal Aspects of Computing (in press).

6.4.2 Book Chapter

5. Michael Leuschel, Jens Bendisposto, Ivaylo Dobrikov, Sebastian Krings, Daniel Plagge (2014) From Animation to Data Validation: The ProB Constraint Solver 10 Years On. In Jean-Louis Boulanger (ed.): Formal Methods Applied to Complex Systems: Implementation of the B Method, Wiley ISTE: 427-446, 2014.

6.4.3 Conference papers

6. Salehi Fathabadi, Asieh, Snook, Colin and Butler, Michael (2014) Applying an integrated modelling process to run-time management of many-core systems. In, 11th International Conference on Integrated Formal Methods (iFM), Bertinoro, IT, 09 - 11 Sep 2014.

7. Savicks, Vitaly, Butler, Michael and Colley, John (2014) Co-Simulating Event-B and Continuous Models via FMI. In, 2014 Summer Computer Simulation Conference.

8. Laurent Voisin, Jean-Raymond Abrial (2014) The Rodin Platform Has Turned Ten. In Proceedings ABZ'14, LNCS 8477, 2014.

9. Dominik Hansen, Michael Leuschel (2014) Translating B to TLA + for Validation with TLC. In Proceedings ABZ'14, LNCS 8477, 2014.

10. Michael Leuschel, David Schneider (2014) Towards B as a High-Level Constraint Modelling Language. In Proceedings ABZ'14, LNCS 8477, 2014.

11. Andy Edmunds (2014) Templates for Event-B Code Generation. In Proceedings ABZ'14, LNCS 8477, 2014.

12. Pereverzeva, Inna, Butler, Michael and Salehi Fathabadi, Asieh, Laibinis, Linas and Troubitsyna, Elena. (2014) Formal Derivation of Distributed MapReduce. In Proceedings ABZ'14, LNCS 8477, 2014.

13. Savicks, Vitaly, Butler, Michael and Colley, John (2014) Co-simulation Environment for Rodin: Landing Gear Case Study. In, In ABZ 2014: The Landing Gear Case Study, Springer Communications in Computer and Information Science, Vol. 433, 2014.

14. Dominik Hansen, Lukas Ladenberger, Harald Wiegard, Jens Bendisposto, Michael Leuschel (2014) Validation of the ABZ Landing Gear System using ProB. In ABZ 2014: The Landing Gear Case Study, Springer Communications in Computer and Information Science, Vol. 433, 2014.

6.4.4 Workshop papers

15. Minh-Thang Khuu, Laurent Voisin, Fernando Mejia (2014) Modeling a Safe Interlocking Using the Event-B Theory Plug-in. In 5th Rodin User and Developer Workshop.

16. Brett Bicknell, Karim Kanso, Jose Reis (2014) Smart Grids: Multi-Simulation, An Application. In 5th Rodin User and Developer Workshop.

17. Asieh Salehi, Colin Snook, Michael Butler (2014) Run-time Management of Many-core Systems using Rodin. In 5th Rodin User and Developer Workshop.

18. John Colley, Michael Butler (2014) From Untimed Specification to Cycle-Accurate Implementation - Cyber-Physical System Model Refinement with Event-B. In 5th Rodin User and Developer Workshop.

19. Michael Leuschel, Jens Bendisposto and Dominik Hansen (2014) Unlocking the Mysteries of a Formal Model of an Interlocking System. In 5th Rodin User and Developer Workshop.

20. Toby Wilkinson, Michael Butler, John Colley, Colin Snook (2014) Generating Tests for COTS Components with Event-B and STPA. In 5th Rodin User and Developer Workshop.

21. Colin Snook (2014) iUML-B Statemachines. In 5th Rodin User and Developer Workshop.

22. Daniel Plagge, Michael Leuschel (2014) A Practical Approach for Validation with Rodin Theories. In 5th Rodin User and Developer Workshop.

23. Savicks, Vitaly, Butler, Michael, Colley, John and Bendisposto, Jens (2014) Rodin Multi-Simulation Plug-in. In, 5th Rodin User and Developer Workshop.

24. Dominik Hansen, Jens Bendisposto, Michael Leuschel (2014) Integrating ProB into the TLA Toolbox. In TLA Workshop 2014.

25. Sebastian Krings, Jens Bendisposto, Michael Leuschel (2014) Turning Failure into Proof: Evaluating the ProB Disprover. In Proceedings of the 1st International Workshop about Sets and Tools, 2014.

26. Lukas Ladenberger, Ivaylo Dobrikov, Michael Leuschel (2014) An Approach for Creating Domain Specific Visualisations of CSP Models. In Human-Oriented Formal Methods (HOFM 2014), LNCS, 2014.

27. Bendisposto Jens, Krings Sebastian, Leuschel Michael (2014). Who watches the watchers: Validating the ProB Validation Tool. In Proceedings of the 1st Workshop on Formal-IDE, Electronic Proceedings in Theoretical Computer Science.

28. Witulski John, Leuschel Michael (2014). Checking Computations of Formal Method Tools - A Secondary Toolchain for ProB. In Proceedings of the 1st Workshop on Formal-IDE, Electronic Proceedings in Theoretical Computer Science.

6.4.5 Papers in preparation

29. Michael Butler, Richard Banach, Jean-Raymond Abril (2014). Modelling and Refining Hybrid Systems in Event-B and Rodin (under review).

30. University of Southampton, Systerel, Theory Extension in Rodin.

31. University of Southampton, Decomposition of Control Systems models in Event-B.

32. University of Southampton, Principles and Practice of Co-simulation for Event-B.

33. University of Southampton, Integrating Hazard Analysis and Event-B Formal Development for Control Systems.

34. University of Southampton, Integrating Event-B Code Generation and Co-simulation.

35. Dominik Hansen, Michael Leuschel (2014) Translating B to TLA + for Validation with TLC. Journal version of ABZ'14 paper.

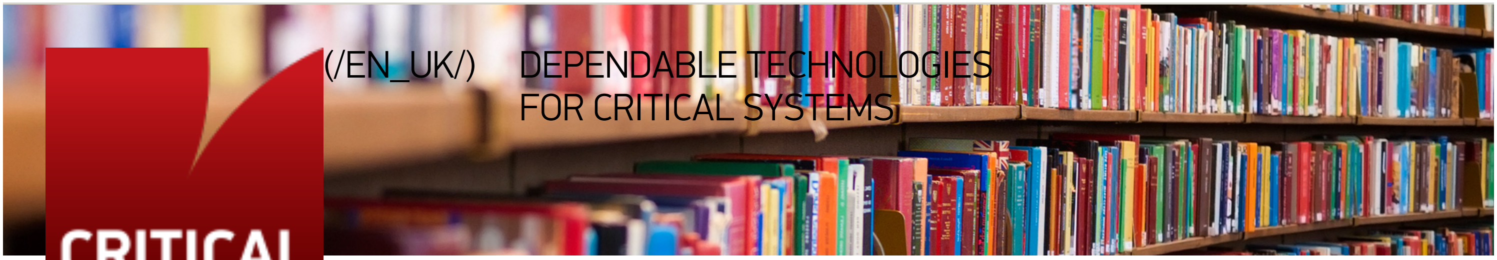
36. Dominik Hansen, Lukas Ladenberger, Harald Wiegard, Jens Bendisposto, Michael Leuschel (2014) Validation of the ABZ Landing Gear System using ProB. Journal version of ABZ’14 paper.

37. Sebastian Krings, Michael Leuschel. Inferring Physical Units in B Models. Journal version of SEFM’13 paper. Submitted.

38. David Schneider, Michael Leuschel, University of Düsseldorf, Using the ProB constraint solver for real-life university time-tabling (tentative title).

39. Michael Leuschel, Sebastian Krings, Solving Higher-Order Constraints over unbounded variables (tentative title).

40. Sebastian Krings, Michael Leuschel, SMT Solving Using the ProB Model Checker. Submitted.



HOMEPAGE (/EN_UK/HOMEPAGE) > MEDIA CENTRE (/EN_UK/MEDIA-CENTRE) > PRESS RELEASES (/EN_UK/MEDIA-CENTRE/PRESS-RELEASES)

MEDIA CENTRE

Press Releases (/en_UK/media-centre/press-releases)

News in Brief (/en_UK/media-centre/short-news)

Insights (/en_UK/media-centre/insights)

Brand Centre (/en_UK/media-centre/brand-centre)

< back (/en_UK/media-centre/press-releases)

LAUNCH OF ADVANCE MARKS NEW PHASE IN THE DEVELOPMENT OF CYBER-PHYSICAL SYSTEMS

December 12, 2014

The launch of a new systems engineering framework is set to revolutionise the design, verification and validation of complex cyber-physical systems.

The result of the EU-funded “ADVANCE” project, the framework provides an engineering process and a free-to-use toolset that addresses safety and correctness at the earliest possible development stage. The ADVANCE toolset has been launched as an upgrade to the existing open-source Rodin platform, extending the capabilities of Rodin with more powerful and innovative verification and simulation capabilities.

Current engineering practices mean that designing cyber-physical systems to high assurance levels is often prohibitively expensive.Three years in the making, the newly launched features will help engineers to reduce the costs of system development by providing accurate models that simulate system behaviour. This means that issues can be identified and design errors eliminated as early in the development lifecycle as possible. The toolset’s new formal verification features will also help engineers to more efficiently test critical systems in ensuring suitable safety-assurance levels.

The upgraded platform has already demonstrated its ability to improve the designs of “event-driven” systems, such as those controlling railway interlocking functions and low-voltage smart grids, and is capable of supporting the development of systems from a broad range of industries. At “Industry Days” held in Southampton and Düsseldorf, the platform’s capabilities were demonstrated by industrial users in the railway, smart energy and defence sectors.

Prof. Michael Butler, of the University of Southampton and Scientific Coordinator of the ADVANCE consortium, said: “It is widely recognised that development costs will become prohibitive for future systems unless significant improvements are made in the methods and tools used for systems engineering. The Rodin toolset is unique in addressing both simulation and formal verification within a single framework, in a cost-effective way.”

José Reis, Principal Consultant Engineer at Critical Software Technologies Ltd, added “Rodin’s new visualisations and simulations will be clear even to non-specialists, allowing engineers to efficiently understand the technical details and consequences of the system they are working on, more effectively fixing errors well in advance of any commitments to a final design.”

The new features are freely available as part of the Rodin open-source platform, which can be downloaded at www.event-b.org/install.html (http://www.event-b.org/install.html).

Following the success of the project, the ADVANCE consortium is now looking for further funding streams to continue to develop Rodin’s capabilities, which will enable the platform to handle even larger system-modelling capabilities while introducing further features. The consortium includes CRITICAL Software Technologies, Alstom Transport, Selex ES, Systerel, the University of Southampton and the University of Düsseldorf.

Further details of the ADVANCE project are available on the project website: www.advance-ict.eu (http://www.advance-ict.eu/).

< back (/en_UK/media-centre/press-releases)

Share: 0

Advance

www.advance-ict.eu

SEVENTH FRAMEWORK PROGRAMME

Advanced Design and Verification Environment for Cyber-physical System Engineering

Newsletter 4, December 2014

UNIVERSITY OF Southampton

ALSTOM

Selex ES
A Finmeccanica Company

systerel
Safe real-time solutions

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

CRITICAL
SOFTWARE

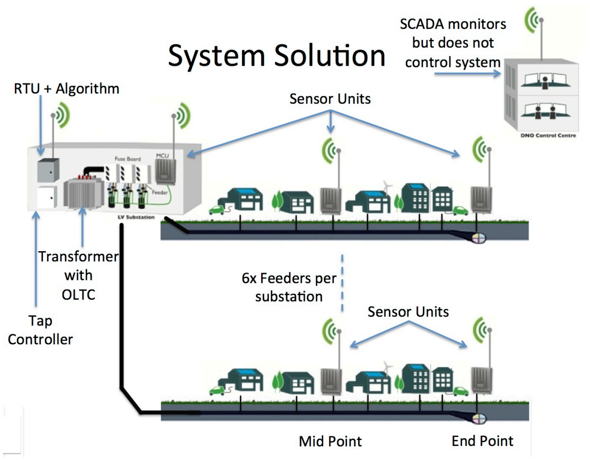
INTRODUCTION

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.

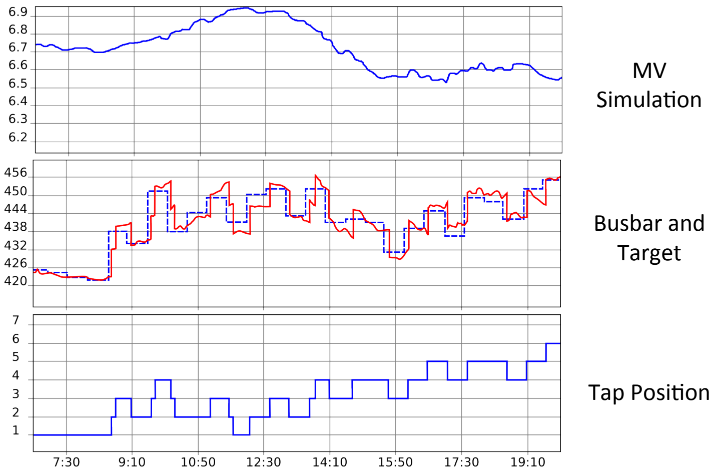
John Colley, *University of Southampton*

ADVANCE IN SMART GRIDS

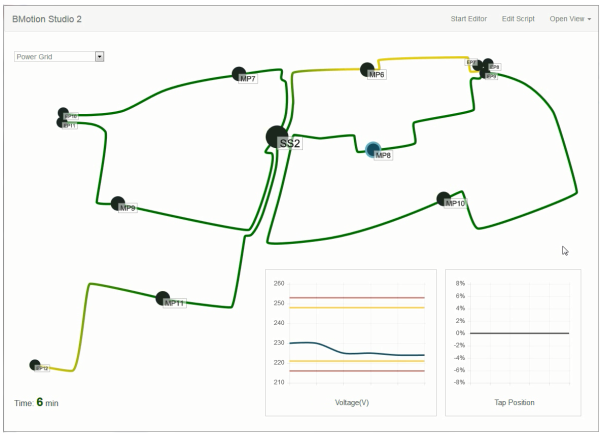
Traditionally in electricity grids, energy flows from large generation stations down through the network to local consumption points. New localised electricity generation mechanisms (e.g., solar panels and wind turbines) and new consumption patterns (e.g., electric vehicles and heat pumps) introduce 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***.

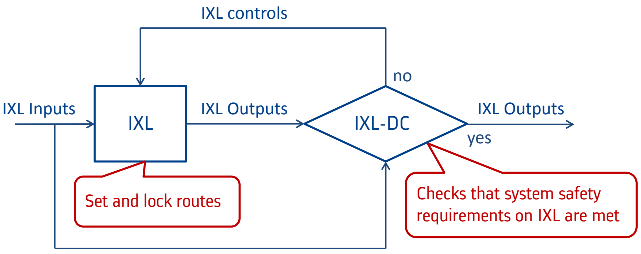
As well as representing the simulation outputs visually using the ADVANCE tools, the formal model was also represented graphically using the UML-B state machine feature. This allows model to be represented as graphical state machines that are automatically translated to textual Event-B models to which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

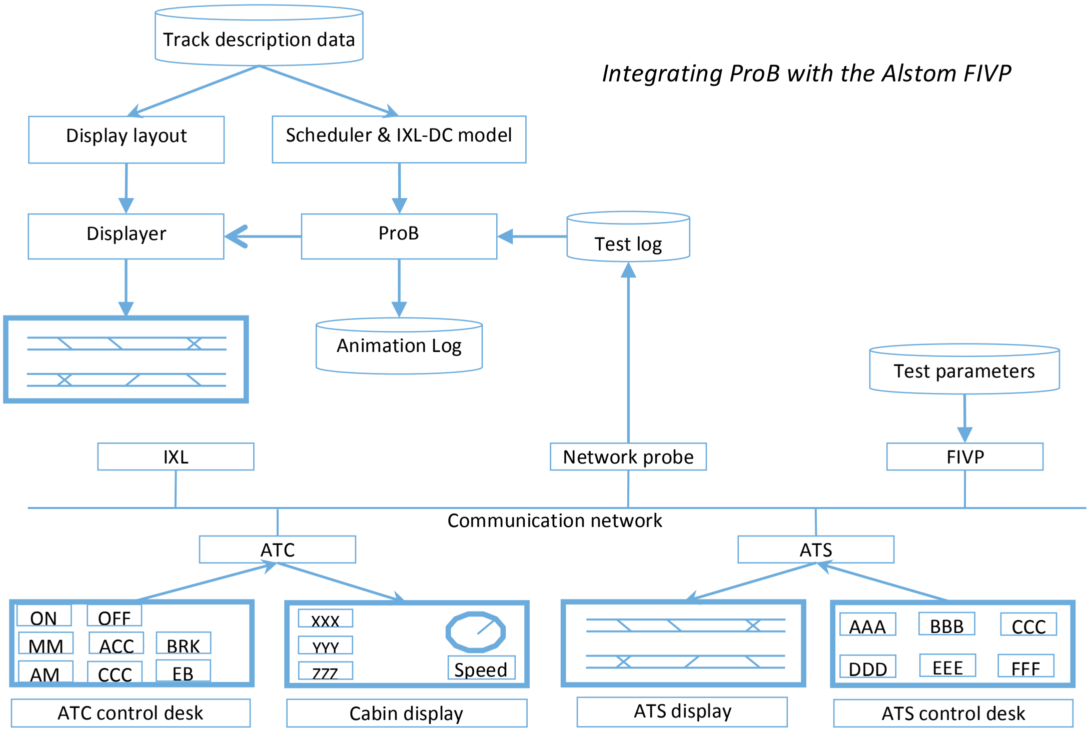
ADVANCE IN RAILWAY INTERLOCKING

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.



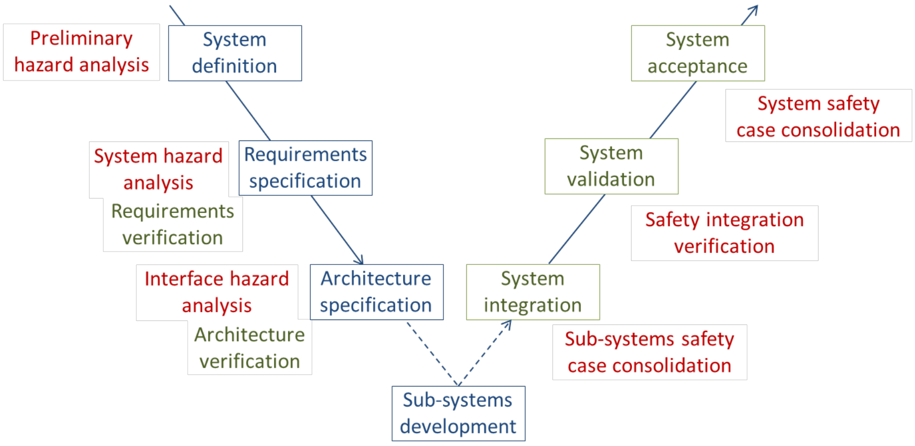
Following the ADVANCE process flow, hazard analysis using STPA was applied to identify the system-level safety properties. The STPA analysis focused on analysis of the control actions of the IXL, identifying how these might lead to hazards and thus what system level safety properties are required to 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.***


Preliminary hazard analysis
System definition
System hazard analysis
Requirements specification
Requirements verification
Interface hazard analysis
Architecture specification
Architecture verification
Sub-systems development
System integration
Sub-systems safety case consolidation
System validation
Safety integration verification
System acceptance
System safety case consolidation

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.

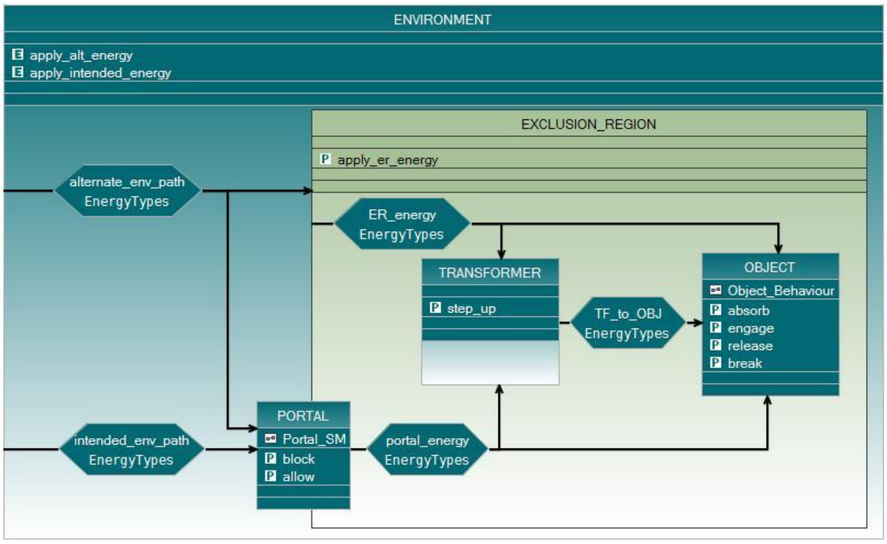
Industry Day Programme:

- 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.

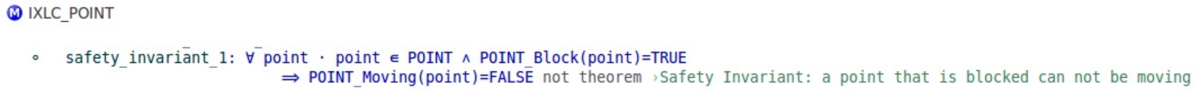


© British Crown Owned Copyright 2014/AWE

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

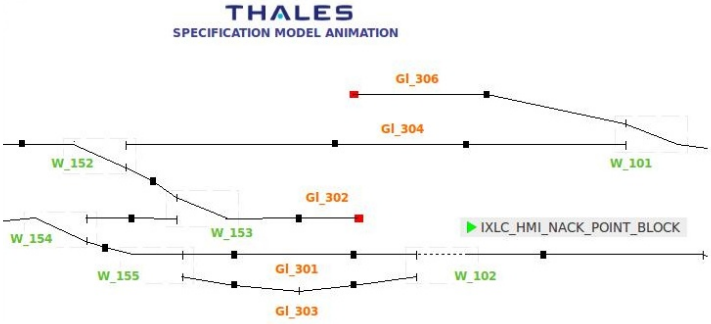
A group from Thales Transport has used Event-B and Rodin on an internal railway interlocking project. They made strong use of the UML-B feature supported in ADVANCE as engineers were already familiar with UML and this eased the adoption path. A particular emphasis was placed on producing a generic interlocking 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