www.advance-ict.eu

Advanced Design and Verification Environment for Cyber-physical System Engineering

Newsletter 3, June 2014

INTRODUCTION

Welcome to the third edition of the ADVANCE newsletter. In the last newsletter we introduced the developments planned for 2014. Now we are able to present the progress outputs of the first six months of that effort.

We decided at an early stage to adopt the Safety Analysis method proposed by Leveson, System--Theoretic Process Analysis (STPA) and to integrate it into the ADVANCE formal development flow. We have now applied STPA successfully to both of the ADVANCE industrial case studies. Jose Reis of Critical Software Technologies describes how beneficial it was to introduce STPA at an early stage of the Smart Grid development. Fernando Mejia (ALSTOM) gives an update on the Railway Interlocking case study and the value of using a refinement based approach to modelling, simulation and verification coupled with STPA-based safety analysis.

The Functional Mockup Interface (FMI) standard for simulation and model interchange, which we described in the last newsletter, is now implemented in the ADVANCE framework and supported by a new component diagram view which enables formal model development to be integrated seamlessly with simulation-based testing. We have already conducted FMI simulations of the Smart Grid Tap Controller within a detailed, continuous model of a grid with encouraging results. John Colley (University of Southampton) explains how the introduction of the capability to measure MC/DC coverage in the ADVANCE framework will enable coverage-directed testing to begin much earlier in the design flow.

To get a more comprehensive view of how the ADVANCE methods and tools have already been used successfully within existing, industrial development flows, then please attend one of our autumn industry days that we are holding in the UK and Germany.

AUTUMN INDUSTRY DAYS SHOWCASE ADVANCES IN CYBER PHYSICAL SYSTEM DEVELOPMENT AND VERIFICATION

The ADVANCE project will hold two ***Industry Days*** in the autumn. The first will be held in **Southampton** on **Wednesday 24th September 2014** and the second in **Dusseldorf** on **Thursday 23rd October 2014**. The aim of the industry days is 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.

The morning session begins with an overview of the ADVANCE processes and tools, followed by a presentation on the use of ADVANCE in the Smart Grid domain, highlighting the use of formal proof, requirements traceability and the application of FMI-based multi-simulation for testing and coverage. An external industrial, early adopter of the ADVANCE technology will then present their experiences with the methods and tools and the demonstrable benefits of incorporating ADVANCE into their existing processes.

In the afternoon, the focus will be on the use of ADVANCE in the railway interlocking domain, where the emphasis will be on requirements and hazard analysis, model visualisation and proof, followed by an open session when there will be opportunity for tool demonstrations and discussion. Throughout the day, the emphasis will be on demonstrating the business benefits that the ADVANCE approach can bring to existing cyber-physical system design and verification flows.

If you are interested in attending either workshop, please visit the ADVANCE website: www.advance-ict.eu

ADVANCE INTRODUCES MC/DC COVERAGE-DIRECTED MODEL TESTING

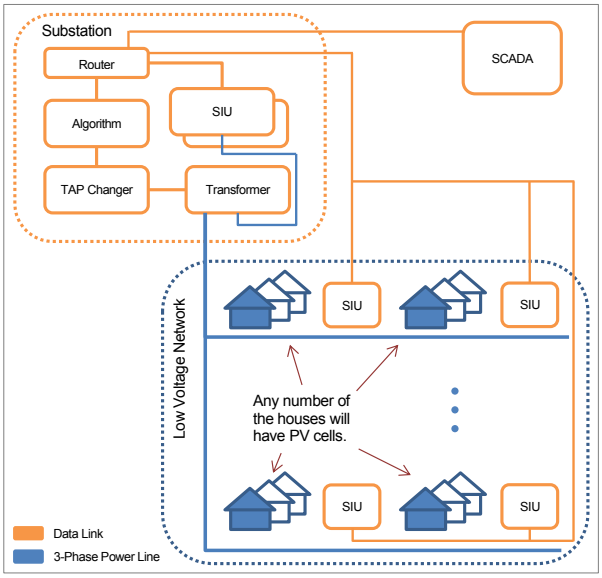
MC/DC coverage is a fundamental requirement for safety-critical system sign-off and DO178/254 certification, but up to now it has only been possible to apply it when the implementation is complete. There is a significant benefit in being able to apply MC/DC coverage criteria earlier in the design and development process, and with the introduction of the new ADVANCE MC/DC coverage facility for Model Testing, designers can now assess how well the tests they are developing will cover the implementation even before the implementation is available. The MC/DC facility builds on the coverage metrics that are already available for the Rodin platform. As a first step, the test developer can ensure that all model transitions are exercised by the tests. Once this has been accomplished, the MC/DC metric can be applied to each transition and the tests enhanced to ensure full coverage. For the model developer, applying this coverage-directed technique at each model refinement step will help in discovering errors much earlier in the development process. As the model is refined from the abstract, specification level to the concrete implementation level, a set of regression tests can be created at each refinement level, which is able to achieve full coverage and can provide increased confidence that the model meets its specification.

ADVANCE SAFETY ANALYSIS WITH EVENT-B AND STPA

"The fact that STPA provided a strong starting point for the models demonstrates the important role that safety analysis plays in the ADVANCE framework."
Jose Reis, Principal Consultant Engineer, Critical Software

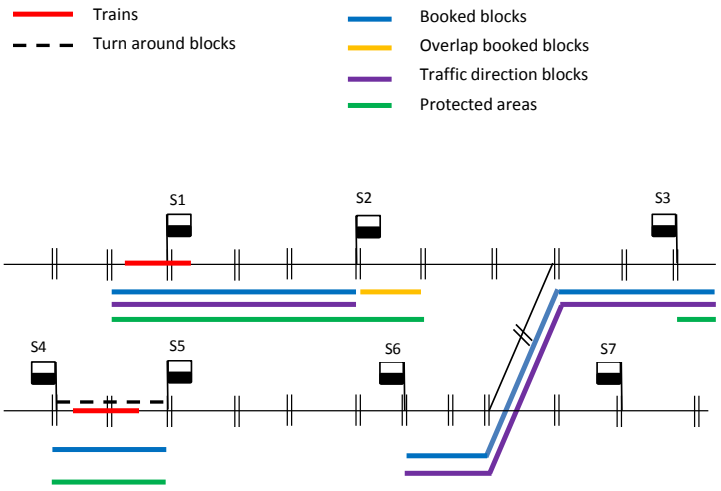
It is an important goal of the ADVANCE project not only to develop tools to support Cyber-physical system development and verification but also to put in place the methods and processes within which the tools can be most productively deployed. At an early stage of the project, System Theoretic Process Analysis (STPA), developed by Prof. Nancy Leveson, was identified as an approach to Safety Analysis which is ideally suited to complex Cyber-Physical System development and fits very well with the formal methods and tools developed under ADVANCE. Initially, the application of STPA within the Rodin formal development environment was

explored and validated in a series of small case studies and the results propagated within the ADVANCE consortium. Now, the STPA process is being applied to the two ADVANCE industrial case studies in the railway signaling and Smart Grid domains with encouraging results.



Safety analysis begins with a system-level Event-B model, where the system-level safety constraints are represented as Event-B invariants. Formal, Event-B refinement and decomposition are used to separate the discrete and continuous components and enable co-simulation. The discrete part is then further refined to define the model of the voltage controller and a behavioural model of the sensors and communications, which models communication failures in an abstract, non- deterministic manner. In the Smart Grid case study, STPA safety analysis has been completed and a hazard mitigation strategy identified. This led to safety properties being clearly identified at a very early stage of the design process.

RAILWAY INTERLOCKING CASE STUDY DEVELOPMENTS



Considerable advances have been made in Railway Interlocking case study. We have demonstrated the feasibility of a refinement-based approach to modelling, simulation and verification of a complex interlocking system. We have identified both strengths and weaknesses of the existing Rodin tools for Event-B and found that considerable improvements have been made to the tools over the last period. Our experiences with the development of a refinement strategy approach will provide important guidance for other systems engineers in the future, both within Alstom and externally. We have also developed a thorough understanding of where and how the ADVANCE methods and tools will contribute to enhancing the Alstom safety development process using STPA. Since the Alstom process is derived from processes defined by European standards, we believe many of these insights will be applicable to safety development in other domains.

RODIN USER AND DEVELOPER WORKSHOP, JUNE 2+3, TOULOUSE

ADVANCE members organised the 5th Rodin User and Developer workshop in Toulouse. The workshop had over 60 participants from academia and industry, including participants from Japan, USA and Australia. There was a presentation on WP1 (Railway case study) from Alstom and Systerel and a presentation on WP2 (Smart grid case study) from Critical Software Technologies. Teams from Düsseldorf and Southampton presented various results from WP3, WP4 and WP5 including the Theory plug-in, new model-checking features in ProB, the latest visualization features in BMotion Studio as well as the latest developments in multi-simulation, UML-B and code generation. Michael Butler and Asieh Salehi (Southampton) and Jean-Raymond Abrial (Systerel) provided participants with a tutorial on the latest version of the Rodin Theory plug-in. Matthias Güdemann from the European openETCS project gave a presentation on how openECTS successfully used Rodin, UML-B

and ProR to construct a traceable, verified safety analysis of the Radio Communications subsystem of the European Train Control System (ETCS) Specification.

ADVANCE PRESENTATIONS AT ABZ2014 CONFERENCE, JUNE 4-6, TOULOUSE

Member of the consortium presented papers describing ADVANCE results at the 4th International ABZ Conference in Toulouse. Notable was a keynote presentation from Laurent Voisin describing the rationale and history of the design of the Rodin platform for Event-B, the basis of the ADVANCE toolset, from its inception 10 years ago to today. The Düsseldorf presented the latest version of ProB and BMotion Studio while the Southampton team presented the latest results on multi-simulation and on code generation.

CONTACT

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

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

Or visit our website:

www.advance-ict.eu