www.advance-ict.eu

Advanced Design and Verification Environment for Cyber-physical System Engineering

Newsletter 2, December 2013

INTRODUCTION

Welcome to the second instalment of the ADVANCE newsletter. In the period since the last newsletter there have been a lot of developments within the ADVANCE project and a great deal of progression. Our first article will cover the first major change, which sees Selex ES (a Finmeccanica company) formally join the Consortium after previously providing industrial support to Critical Software Technologies on their Smart Grid case study. Fernando Mejia (ALSTOM) give an update on the Railway Interlocking case study. John Colley (University of Southampton) gives a brief on the Functional Mockup Interface Standard and why the ADVANCE consortium has chosen to adopt it.

Aside from the two main articles we will have our usual round up of progress with regard to all the other activities in the project including tool development, details of events the Consortium has supported with presentations on ADVANCE and what 2014 brings for the project.

SELEX ES JOINS ADVANCE

The ADVANCE Consortium is pleased to announce that Selex ES (a Finmeccanica company, based out of Basildon in the UK) has formally joined the project as a Consortium member, with specific interest in the Smart Grid case study.

During the first year of the ADVANCE project, WP2 leaders Critical Software Technologies had been liaising with Selex ES, in

both the UK and in Italy, as an industrial partner. Selex ES had been providing active requirements and issues for investigation, using the ADVANCE toolset and techniques, from their Gridkey product (http://www.gridkey.co.uk/). However, following the completion of that phase of work for Gridkey, a new challenge was required for the ADVANCE project's smart grid case study.

The timing, you might say, was apt. Selex ES/Gridkey had just embarked on a new project for Electricity North West to develop Low Voltage Integrated Automation (LoVIA). LoVIA will develop and then trial a new integrated solution and novel application of automated voltage control of low voltage (LV) distribution networks. The project will integrate existing and new distribution system equipment such as LV substation monitoring, including at the mid and end points of LV feeders, on-load tap change distribution transformers and distribution substation controllers to provide for co-ordinated automatic voltage control of LV networks.

As well as providing a single, secure communications point for the back-haul of remote monitoring data, replacing existing mutiple communication points, this integrated control solution will faciliate the regulation and control of LV network voltages based upon both local and remote-end real-time voltage measurements thus facilitating improved management of network voltage profiles and facilitating the coordinated control of multiple voltage regulating devices.

The LoVIA project fits perfectly within the framework of WP2 and will provide ample opportunity for the ADVANCE toolset to be used to enhance its development and answer a number of challenges that the project sets. Given the increased involvement of Selex ES in the ADVANCE project it seemed a natural step to invite them to become Consortium members and lend their wealth of experience in the Smart Grid domain to the further advancement of the project. We welcome Selex ES to the Consortium and look forward to continuing the strong working relationship that has been developed.

Luke Walsh, Critical Software Technologies

RAILWAY INTERLOCKING CASE STUDY

Interlocking is the component of the signalling system that sets and locks the routes for trains on request of the traffic operator and that commands the lights of the wayside signals according to the state of the routes. Using the ADVANCE methods and tools, ALSTOM Transport is developing a new component, called an Interlocking Dynamic Controller (IXL-DC), which dynamically checks the safety of the configurations computed by the interlocking at run-time.

ADVANCE has developed a proof strategy for the Event-B model of the Interlocking Dynamic Controller using the Theory Plug-in and other techniques developed for Model Construction and Proof in ADVANCE. This activity consisted of creating and proving, firstly, a very abstract and reduced Event-B model of the IXL-DC and then several refinements of that initial Event-B model that introduce progressively the relevant concepts. The last refinement is complete Event-B model of the IXL-DC. The purpose of this strategy is to analyse separately the concepts involved in the IXL-DC and to control the number and the complexity of the proof obligations generated by the Event-B model reducing thus the effort to proof the model. The Event-B model of the IXL-DC was tested using factory tests from an actual railway signalling system, enabled by the Simulation and Test Methods developed by ADVANCE.

Fernando Mejia, Alstom

ADVANCE ADOPTS THE FUNCTIONAL MOCKUP INTERFACE (FMI) STANDARD FOR MULTI-SIMULATION

"Functional Mock-up Interface (FMI) is a tool independent standard to support both model exchange and co-simulation of dynamic models using a combination of xml-files and compiled C-code. The first version, FMI 1.0, was published in 2010. The FMI development was initiated by Daimler AG with the goal to improve the exchange of simulation models between suppliers and OEMs. As of today, development of the standard continues through the participation of 16 companies and research institutes. FMI is supported by over 35 tools and is used by automotive and non-automotive organizations throughout Europe, Asia and North America."

https://www.fmi-standard.org

The ADVANCE multi-simulation framework now provides support for the import and multi-simulation of discrete and continuous components which comply with the FMI standard. This new facility allows for the seamless transition from formal, proof-based specification modelling to simulation and coverage-based verification of components whose implementation has been refined formally from the specification. For instance, a formal, Event-B model of a digital controller can be validated and verified using a continuous model of the environment in which it will operate before the actual implementation of the controller is available, resulting in the earlier detection of errors. Model-based tests developed at this stage can then be run on the controller implementation to measure the test coverage. Adopting the FMI standard means that ADVANCE users have access to a range of high quality tools and libraries, that can be integrated cleanly into the ADVANCE multi-simulation flow.

John Colley, University of Southampton

RODIN TOOL DEVELOPMENTS

The ADVANCE Project is building on the Rodin open source toolset for Event-B:

www.event-b.org

As well as maintaining the core Rodin platform, ADVANCE is developing new tool features as Rodin plug-ins relevant to engineering of cyberphysical systems. We highlight some of the tool developments.

Rodin platform maintenance: The maintenance of the Rodin platform and the associated plug-ins has been carried out as usual, giving top priorities to the requests from the case studies. Version 2.8 of the Rodin platform was released in June 2013. This included bug fixes and improvements to the Event-B prover.

Automated Proof and Model Checking: Version 1.1 of the SMT solver plug-in was released in October 2013, with excellent feedback from several users who have reported a significant improvement of proof automation. The constraint solving capabilities of ProB have been continuously improved along with scalability improvements. A new versions of the ProB disprover plug-in has been released which includes proof capability (when the sequent to prove involves only finite sets).

Language Extension: A new version of the Theory plug-in have been developed fixing some bugs found by the WP1 and WP2 case study, increasing the range of features and improving the overall usability of theories. The ProB model checker now supports animation and model checking of datatypes and operators defined in theories.

Model simulation with ProB: New visualization techniques have been integrated and developed within ProB 2.0: various reduced state space views, formula visualisations, as well as time-value diagrams. The scalability of ProB was a major effort. Low-level B models, in particular hardware models, can now be translated to TLA+ and be model checked by TLC. The results are fed back to ProB and replayed in the simulator. For low-level models this provides an order of magnitude performance improvement. The constraint solving kernel has been dramatically improved, guided by case studies and requirements of workpackages WP1 and WP2. One notable feature of the improved ProB kernel is its ability to automatically detect expansions of infinite sets, whereupon the relevant set comprehensions are kept symbolic.

Model-based testing: The model-based testing algorithm of ProB has been generalized and the constraint solver has been improved for the test case generation task. In particular, random enumeration has been added to the ProB kernel. The performance of the test-case generation algorithm has been improved (factor of 8 for one case study). A model testing view for ProB 2.0 has been developed.

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

LINKING SAFETY ANALYSIS WITH FORMAL MODELS

To meet the objective of integrating Safety Analysis into the ADVANCE method and toolset, we have adopted the Safety Analysis method proposed by Leveson, System-Theoretic Process Analysis (STPA), and use the requirements traceability capabilities of the ProR. The Functional Requirements are developed using the System Phenomena while the Safety Requirements are derived from the Controlled Phenomena. The Safety Constraints, derived systematically from the Safety Requirements, can then be represented formally in the Event-B model as invariants and guards. We configured ProR to capture the requirements phenomena and then linked the controlled phenomena to the safety analysis. We also linked the Event-B model invariants and guards to the safety requirements. In this way we were able to leverage the traceability facilities already provided by ProR.

Using Event-B refinement and proof, a controller can be developed for a safety-critical system which incorporates an STPA process model of the system to control the good behaviour of the system, detect faults in the system and mitigate hazards that arise from these faults. Event-B refinement ensures that the design decisions are clearly and formally represented and Event-B proof has been used to ensure that the safety constraints, represented as invariants, are preserved and the hazards correctly mitigated.

John Colley, University of Southampton

ACTIVITIES & EVENTS

The prevailing period has been a busy one for the Consortium, with a number of conferences and workshops attended and many papers presented. All the details can be found in our news and events section on the project website: http://www.advance-ict.eu/. With a particular highlight being the Dagstuhl Workshop on Integration of Tools for Rigorous Software Construction and Analysis which was part co-organised by Michael Leuschel of Heinrich Heine Universität Düsseldorf and saw members of the ADVANCE project from the University of Southampton, Systerel and Alstom Transport present on the on-going developments.

Two key plenary meetings were held in May and November 2013. These provided a great opportunity for the Consortium to meet and discuss the on-going project and the advancements being made. As well as allowing for greater collaboration and discussion on key topic areas. The November meeting also gave an opportunity for Selex ES to provide details to the whole Consortium of the LoVIA project.

Looking forward to next year, we are happy to announce that we will be holding two workshops in Autumn 2014 for interested parties from both Industry and Academia, dates and details to be announced. These workshops will look to engage with the full spectrum of institutions which could benefit from the utilisation of the ADVANCE toolset, and present to them the details of the Consortium's findings and developments.

Luke Walsh, Critical Software Technologies

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