ADVANCE

ADVANCED DESIGN AND VERIFICATION ENVIRONMENT FOR CYBER-PHYSICAL SYSTEM ENGINEERING

Contract Number : **287563**

Project Website : **www.advance-ict.eu**

Project Coordinator: **University of Southampton**

Contact Person: **Dr John Colley, *j.l.colley@ecs.soton.ac.uk***

Engineering challenge addressed by ADVANCE

Infrastructure systems, such as rail networks and electricity grids, that provide services to citizens and public bodies are increasingly engineered as ***Cyber-Physical Systems*** (CPS), that is, complex integrations of physical and software components with high degrees of automation and networked communication. While the increased integration of software and communication with physical systems allows for much greater flexibility and automation in control, it also increases the possibility that system design errors will compromise system operation and safety, leading to disruption of service and accidents. Future CPS will dramatically exceed the capabilities and complexity of current embedded systems in terms of richness of functionality and degrees of networking, resilience, performance and autonomy. Current design methods rely heavily on prototyping and testing to guarantee both functional and non-functional system characteristics. While these techniques are invaluable, they are very expensive, particularly as they tend to be applied late in the development cycle when errors are more costly to fix. Moreover, testing of networked systems is notoriously difficult, which makes the design of trustworthy CPS particularly challenging. Current engineering practices mean that designing systems to high assurance levels is hugely costly; it is recognised that development and assurance costs will become prohibitive for future systems unless there are significant improvements in the methods and tools used for CPS engineering.

Key innovations in ADVANCE

> ***The FP7 ADVANCE Project produced new system modelling, verification and simulation innovations that enable cost-effective assurance to be achieved in engineering of CPS. These innovations are delivered as an integrated tool suite and a supporting methodology.***

The core of the ADVANCE methodology is the use of the Event-B modelling language where verification is based on formal proof methods that are independent of the scale of system state space. While formal verification technology is a powerful way of ensuring that systems satisfy key properties including safety properties, it is not sufficient for validating system models against known and expected environmental operational scenarios. Enabling validation activities to take place early in the life cycle means that requirements can be analysed and corrected long before the expensive process of designing, building and testing a system. The ADVANCE Project considerably enhanced the Rodin toolset for modelling and verification in Event-B. Rodin is an open source development with an open architecture that enabled ADVANCE to contribute several major plug-ins to support the ADVANCE methodology.

Formal verification is becoming established in industrial hardware design and, to an extent, in software development. However the use of formal modelling and verification technology in developing and assuring ***systems*** (consisting of mechanical, communications, and software components) represents a step change in systems engineering. For the first time, the ADVANCE Project has demonstrated that it is feasible to apply formal modelling, verification and simulation to industrial scale systems. To enable this, ADVANCE made major improvements in the performance of the

automated verification, model-checking and simulation capabilities for Event-B. A key innovation of ADVANCE was a tool-supported method for developing domain specific theories that enable reuse for modelling and verification concepts within and between models. A rich and flexible visualisation framework allows domain-specific visualisations of model animation to be created that allow for easy validation by domain experts. ADVANCE also enhanced the state machine modelling capabilities of UML-B, a graphical version of Event-B, making formal modelling of CPS more accessible to engineers who may lack familiarity with the mathematical concepts of Event-B

The novel ADVANCE multi-simulation framework provides support for the import and multi-simulation of discrete and continuous components, which comply with the FMI standard for integration of simulation tools. This 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.

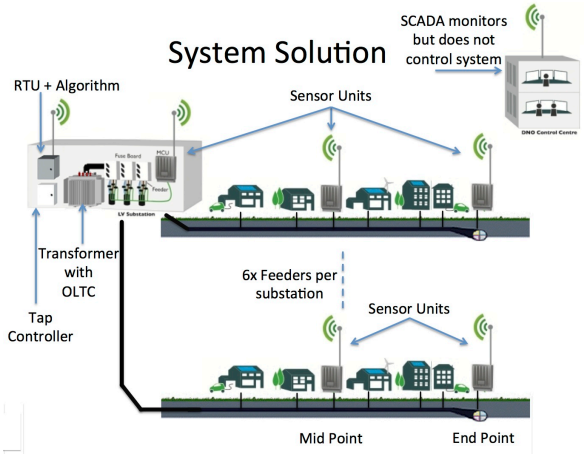
The engineering methodology developed by ADVANCE brings together requirements and safety analysis with formal modelling and simulation. The methodology incorporates the STPA safety analysis process for systematic identification of safety properties and hazard mitigation. This analysis is further strengthened through formal modelling of identified safety properties and verification of system behaviour and hazard mitigation against safety properties. The project developed guidelines explaining how the ADVANCE methods and tools can support existing safety certification standards in the railway domain (CENELEC EN50126, EN50129) and aerospace domain (DO-178C)

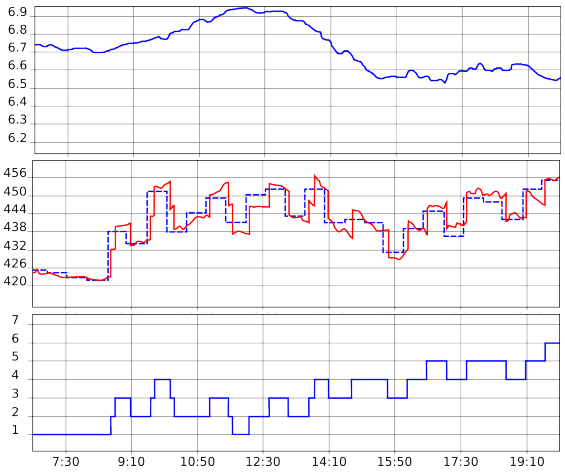
The ADVANCE project has realized its vision of developing an integrated toolset that combines formal verification for deep analysis of system models with simulation for extensive validation of models based on realistic scenarios. This enables early stage analysis of cyber-physical systems, detecting 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).

Demonstration and Use of 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.***





MV Simulation

Busbar and Target

Tap Position

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***.

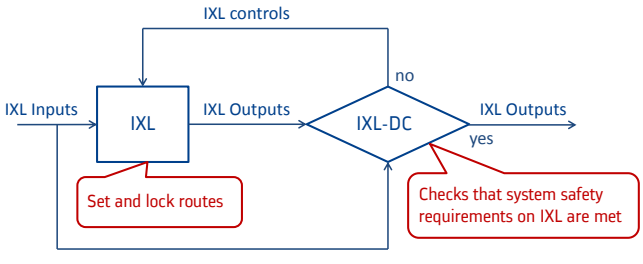
BMotion Studio is a plug-in that enables the development of a graphical visualisation of states of the models in a way that is meaningful for the domain. This was used to produce a visualisation of a low voltage network that represents the topology of the network and the voltage levels at different points 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.

Demonstration and Use of ADVANCE in Railway Interlocking

Alstom 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

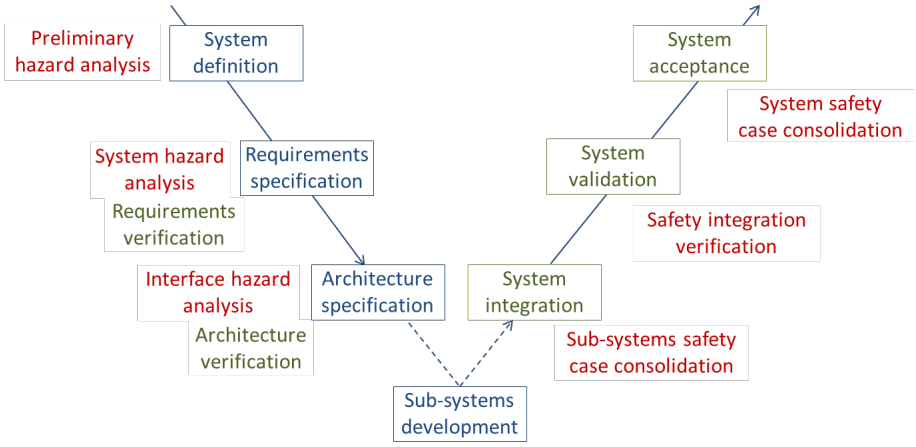


top of existing interlocking systems while still providing a provably safe interlocking system.

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.

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



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

Scientific, Economic and Societal Impact

ADVANCE reinforces European scientific excellence and technological leadership in the design and operation of large-scale complex systems, improves industrial competitiveness through strengthened capabilities in advanced embedded systems, in monitoring, control and optimisation of large-scale complex systems, in areas like energy, transport, and production, and in engineering of large-scale systems. In particular, the outcome of the ADVANCE Railway case study will be to improve safety in the railway domain for dynamic trusted railway interlocking, and the outcome of the Smart Grid case study will be to have an impact on the efficiency of energy distribution in the emerging smart grid market, in which Selex ES has already a market presence.

For the railway case study, an experienced safety and certification expert from the Alstom RAMS team has contributed to the identification of safety requirements in the formal model and to the assessment of the compliance of the ADVANCE process to certification requirements. For the smart grid case study, Selex ES have provided expert input into the formal modeling of Low Voltage Networks which will result in a smart grid solution which not only is energy efficient but can also avert transformer failure, thereby ensuring more reliable and cost-effective energy supply to meet future user demand.

In addition to supporting the development of applications in the railway and smart grid domains through its open, extensible platform, ADVANCE can achieve increased competitiveness by reducing the cost to develop high-assurance cyber-physical systems in general, supporting new business eco-systems that provide innovative products and services that can plug in to the ADVANCE development and verification environment. In particular, the development of tools and methods for requirements traceability and safety analysis within ADVANCE will have a positive impact on the development and certification of other safety-critical systems. ADVANCE will widen educational and training activities in systems and control engineering in Europe at all levels, and promote international co-operation with targeted geographical areas, creating mutual benefits which will further European interests.

The ADVANCE Partners

The ADVANCE consortium consists of six strong and complementary partners representing a combination of leading European industrial players in systems engineering along with academic partners with internationally leading expertise in formal verification and simulation tools. Systerel and the Universities of Düsseldorf and Southampton led the development of novel methods and tools while Alstom and Critical Software applied these to the engineering of intelligent transport and energy systems. Selex ES, as the end user of the energy system development, brings industrial and commercial experience to the exploitation of the methods and tools developed. All the partners have developed plans for future exploitation of the ADVANCE results. The technology provider partners (Systerel and the Universities of Düsseldorf and Southampton) have developed business models involving provision of commercial servces to support adoption and customization of the ADVANCE toolset. The industrial technology user partners (Alstom, Critical Software and Selex ES) have identified upcoming projects and business areas where the ADVANCE tools can be applied to achieve high degrees of assurance.

Project partners	Country
University of Southampton	UK
ALSTOM Transport	France
Systerel	France
University of Düsseldorf	Germany
Critical Software Technologies Ltd	UK
Selex ES Ltd	UK