ADVANCED DESIGN AND VERIFICATION ENVIRONMENT FOR CYBER-PHYSICAL SYSTEM ENGINEERING

ADVANCE

Key innovation

Cyber-physical systems are integrations of computing and physical mechanisms engineered to provide physical services including transportation, energy distribution, manufacturing, medical care and management of critical infrastructure. The essential concept of the ADVANCE project is the key role played by ***modelling*** in cyber-physical systems engineering. Modelling should be used at all stages of the development process from requirements analysis to system acceptance testing.
While formal proof can be used to verify that the software parts of a cyber-physical system correctly implement a formal model, it is not feasible to use proof to verify a complete cyber-physical system. Conventionally, ***correctness-by-construction*** refers to the use of formal models and refinement in the development of software. ADVANCE will go beyond this, supporting the construction of cyber-physical ***systems*** and augmenting formal modelling and verification with simulation and testing.

Technical approach

Although engineering methods exist for tackling individual dimensions of the design space – environment simulation, software validation, software verification, hardware verification, safety analysis, etc – it is currently very difficult to combine these within a single design environment. This is caused by a lack of uniformity in modelling methods and adds greatly to engineering costs. The experience of the ADVANCE consortium is that most benefit is achieved from taking a ***formal modelling*** approach supported by strong ***formal verification*** tools. Formal modelling and verification lead to deeper understanding and higher consistency of specification and design than informal or semi-formal methods. While formal verification is the method used to ensure consistency within and between models, ***simulation*** helps engineers ensure that models are ***accurate*** representations of desired functionality and of physical system components. Different simulation tools are better suited to simulating different parts of cyber-physical systems such as environments, host platforms, controllers, physical plant and communications. As with a proof framework, rather than having a single simulation tool, it is more effective to have a multi-simulation framework for combining separate simulation tools in a seamless way. ***Model-based testing*** is a technique for systematic generation of test cases from formal models that can increase the confidence of the testing over ad hoc manual construction of test cases. The rate at which manual tests can feasibly be developed imposes a severe bottleneck on the design and verification process. As well as providing the facility to develop directed tests, ADVANCE will develop techniques for generating tests automatically.

Demonstration and Use

The focus of ADVANCE is to develop and deliver Methodology and Tools that fit well together in a rigorous and Integrated Process that will be validated with two

Contract number

287563

Project coordinator

University of Southampton

Contact person

Dr John Colley

Electronics and Computer Science

University of Southampton

Highfield Campus

SO17 1BJ

Southampton, UK

Tel: +44 (0)23 8059 4506

Fax: +44 (0)23 8059 3045

j.l.colley@ecs.soton.ac.uk

Project website

www.advance-ict.eu

Community contribution to the project

2.55M Euro

Project start date

01 10 2011

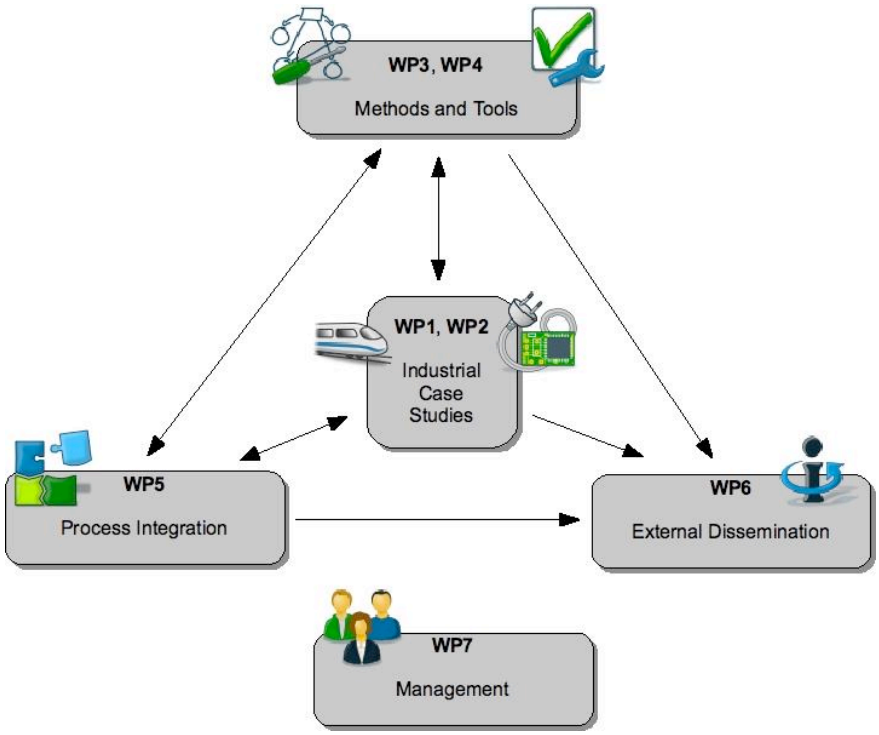
Duration

30 months

industrial case studies, Dynamic Trusted Railway Interlocking and Smart Energy Grids.

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. ALSTOM Transport is developing with the ADVANCE methods and tools a new component, called an Interlocking Dynamic Controller (IDC), which dynamically checks the safety of the configurations computed by the interlocking at run-time.

Until recently, energy efficiency has been about individual devices making local savings without taking into account demand on the grid and the price of electricity. Critical Software will model and verify the distributed monitoring and control of a smart energy grid together with communication between consumer devices, electricity suppliers and grid operators. In both case studies, simulation and test case generation will be used to complement formal proof.



Scientific, Economic and Societal Impact

ADVANCE will reinforce European scientific excellence and technological leadership in the design and operation of large-scale complex systems, improve 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. ADVANCE will achieve increased competitiveness by reducing the cost to develop high-assurance cyber-physical systems, supporting new business eco-systems that provide innovative products and services. 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.

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