



## PROJECT PROFILE

# Developing a model-based approach

### Supporting mission-critical embedded systems



Copyright Airbus - Image Graphique © I3M

**Several industries are currently facing the issue of developing mission-critical embedded computer-based systems with increasing complexity, dependability and economic pressures such as cost and time to market. Model-driven development/engineering (MDD/MDE) addresses those issues. Today, sectors such as aerospace, automotive and communications are rather segmented and are prone to study and promote dedicated solutions, whereas cross-fertilisation would be more beneficial. SPICES will implement an integrated MDD/MDE methodology for designing, verifying and implementing avionics mission-critical real-time embedded (RT/E) systems.**

Mission-critical RT/E systems are characterised by designs that cannot be achieved without taking into account and assessing overall resource use at the very early stages. Indeed, it is not possible to wait until a first implementation has been completed to discover that the design is not suitable to meet the system requirements.

In addition, the more complex the system, the more difficult it is to assess on paper that it is properly

designed and will meet all its functional and non-functional requirements such as real-time behaviour and safety constraints. Consequently, software architects and designers of mission-critical RT/E systems need early validation techniques coupled with a formal, non-ambiguous and sufficiently informative description of the future system – in other words, a consistent model. Moreover, they need to be able to ensure that the code that will actually run on the targeted hardware is consistent with the validated models.

Finally, the specialisation of software engineers and the project management issues call for a clear separation of roles between software architects, applications developers and target-level integration experts.

**Focusing on aerospace industry**  
SPICES aims at developing an MDD/MDE-compliant tool suite for the design, verification and development of mission-critical RT/E systems dedicated to the aerospace industry. The tool suite will be based on the architecture analysis and design language (AADL), formal methods, the lightweight common object request broker architecture (CORBA) component model (CCM) and the SystemC system description language, and will target both general-purpose processors and reconfigurable hardware. SPICES modelling, verification and code-generation tools will be integrated in the open-source Eclipse platform.

The main challenges of the project are:

- Extension of AADL for expressing functional and non-functional requirements;

## SPICES (ITEA 05015)

### Partners

- AIRBUS France
- Axlog Ingénierie
- BARCO Avionics
- CEA-List
- CETIC
- FéRIA
- K.U Leuven
- Israel Aircraft Industries
- LESTER
- SQS
- TCP
- THALES Avionics
- THALES Communications
- Universidad de Cantabria
- Verimag

### Countries involved

- Belgium
- France
- Israel

### Project start

July 2006

### Project end

June 2009

### Contact

#### Project Leader:

Anne-Marie Fouilliant  
THALES, France

#### Email:

anne-marie.fouilliant@fr.thalesgroup.com



## PROJECT PROFILE

- Application of formal validation techniques to extended-AADL models; and
- Development of a runtime support for dynamic enforcement of the non-functional policies necessary to meet the formally-verified non-functional requirements.

### Tackling major issues

The project challenges strongly reinforce, integrate and consolidate three major issues:

1. System-based approach to determine the best optimisation of the various constraints and implementation solutions;
2. Modelling-based engineering; and
3. Software component execution support.

The first expected result is a set of open-source Eclipse plug-ins validated with market leader representative applications and embedded platforms. And the second expected result is the provision of proper CCM-based execution support to the aerospace industry that can be plugged into the Eclipse-based AADL tool suite as a suitable model-driven architecture (MDA) platform.

### Meeting strong demands

Work in SPICES corresponds to a very strong demand in the avionics sector and space applications because of the expansion of software-intensive embedded

system components, the increase of the functional complexity and performance needs. Economic constraints make modelling of the software/hardware (SW/HW) platform absolutely necessary. These issues lead more and more to use of automated processes, with automatic generation of code, tests, analyses, validation, etc.

The automotive industry has also shown interest in the same approaches, as illustrated by European research projects such as ITEA EAST-EEA embedded electronic architecture and the automotive open system architecture (AUTOSAR) initiative. Although requirements are slightly different in terms of very large series, even higher competition and cost reductions, carmakers face the same needs for improved system development methods and automated processes.

Key actions will include:

- AADL extension;
- Adaptation of formal verification methods to extended-AADL models;
- Tailoring of a lightweight CCM framework to the avionics environment, with partitioned operating system and reconfigurable hardware;
- Demonstration of project results in three market-relevant user case studies;
- Standardisation action regarding AADL and CCM.

### ITEA 2 Office

High Tech Campus 69 - 3  
5656 AG Eindhoven  
The Netherlands  
Tel : +31 88 003 6136  
Fax : +31 88 003 6130  
Email : itea2@itea2.org  
Web : www.itea2.org

ITEA - Information Technology for European Advancement - is an eight-year strategic pan-European programme for pre-competitive research and development in embedded and distributed software. Our work has major impact on government, academia and business.

ITEA was established in 1999 as a EUREKA strategic cluster programme. We support coordinated national funding submissions, providing the link between those who provide finance, technology and software engineering. We issue annual Calls for Projects, evaluate projects, and help bring research partners together. We are a prominent player in European software development with some 10,000 person-years of R&D invested in the programme so far.

ITEA-labelled projects build crucial middleware and prepare standards, laying the foundations for the next generation of products, systems, appliances and services. Our projects are industry-driven initiatives, involving complementary R&D from at least two companies in two countries. Our programme is open to partners from large industrial companies, small and medium-sized enterprises (SMEs) as well as public research institutes and universities.



© Airbus S.A.S.

