

# ASSERT

## Automated proof-based System and Software Engineering for Real-Time applications

**KEYWORDS:** Avionics systems, proof-based system engineering, software modelling, Architecture Description Language (AADL), embedded systems, system families, configurable middleware, code generation, formal languages.

### Introduction

European Embedded Systems industry has entered an age of fierce competition where the cost and delay for the development of embedded software becomes more and more a discriminating factor. Studies have shown that the software productivity gap will still increase in the next years. Key responses to such issues rely on:

- Reducing the cost of system design failures, by enforcing a proof based system component approach, where design solutions are proven "correct by construction".
- Reducing the cost of test and integration activities that are reported to be as high as half of the total development cost.

### Objectives

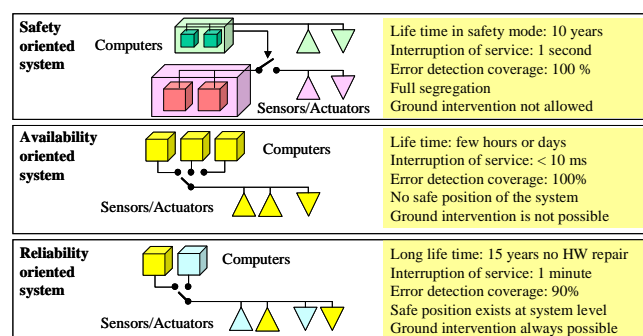
**ASSERT** applies to the computer-based system (CBS) engineering discipline as a whole, without distinction of application domains. It elaborates solutions over three major issues:

- ASSERT will identify system families supported by proven reference architectures and standardised building blocks.
- ASSERT will replace the classical engineering approach by a proof-based method encompassing the full system and software life-cycle and supported by a well-defined and automated process.
- ASSERT will prove the validity of its new concepts by demonstration on real industrial cases, an intensive education and training program and diffusion of the results within a network of industrial partners (A.NET).

### Expected Results

The results expected from ASSERT cover four complementary domains:

- A new System and Software Engineering Process, formalised, documented and integrated in the aerospace standards and possibly in other international standards.
- A set of tools implementing the System Engineering process, able to build the system model and to automate the requirement capture, modelling, verification and code generation covering the whole system life-cycle from early requirements to final implementation in code.
- The ASSERT System families able to instantiate Critical Real Time Embedded Systems from proven reference architectures and characterised properties. One family targeting high reliable systems will be fully developed and characterised down to hardware implementation. Other families oriented towards fault tolerant systems will be developed down to the AADL model.
- A set of standardised and customisable building blocks for transportation applications that will be available in open-source and stored in open repositories managed by space and aeronautic authorities.



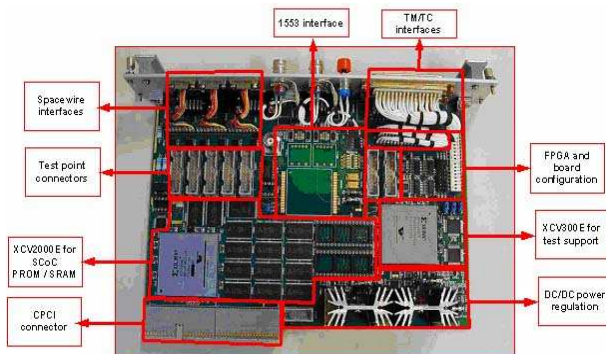
*Architecture principles of three main families that will be studied in ASSERT.*

## Partners and their role

ESA (European Space Agency) is the coordinator of the ASSERT project.

In order to ensure efficient scientific work, research and development activities and resources have been structured into five clusters and two pilot projects:

- **PBSE Cluster : Proof Based System Engineering and associated AADL extensions supported by an associated toolset development.** This cluster is led by INRIA and AXLOG Ingénierie with the active participation of ESA, VUT and CS.
- **DDHRT cluster: Dependability Distribution and Hard Real Time technologies with related AADL extensions definitions and developments.** DDHRT is led by CNRS-LAAS and ENST with the participation of DIT/UPM, VALIOSYS, INTECS, UPD and SCISys.
- **DVT cluster: Development and Verification Tools for software engineering.** This cluster is led by CNRS-VERIMAG, CS and ETH with the participation of ESTEREL Technologies, PROVER, INTECS, TERMA, VALIOSYS, UPD, AXLOG Ingénierie and ENST.
- **P&S cluster : Process & Standardisation,** led by SYNSPACE with the participation of ESA, ESI, Software, CS, EADS-ST, INRIA and AXLOG.
- **O&E cluster: Openness & Exploitation** is led by UPD and is in charge of implementing the dissemination policy of ASSERT results.
- **MA3S: Multi-domain Advanced Architecture for Automated Systems,** that covers the technical domains of launchers, Military Aircraft and Unmanned Aircrafts (UAV) and critical application in space. This Pilot project is led by EADS-ST with the participation of EADS-ST, EADS-CRC, BSSE, DASSAULT Aviation, MBDA France and EADS-ASTRIUM.
- **HRI: High Reliability Infrastructure.** It targets the space satellite domain with long lifetime without maintenance. This pilot project is led by ALCATEL SPACE and ALENIA Spazio with the participation of DUTCH SPACE.



An example of a computer node used by the Pilot Projects.

## ASSERT

### CONTRACT NUMBER

IST - 004033

### FULL NAME

Automated proof-based System and Software Engineering for Real-Time applications

### TYPE OF PROJECT

Integrated Project

### PROJECT PARTICIPANTS

ESA (European Space Agency), ALCATEL SPACE (France), ALENIA Spazio (Italy), EADS-ASTRIUM (France), AXLOG Ingénierie (France), BSSE (Germany), CS (France), DASSAULT Aviation (France), DIT/UPM (Spain), Dutch Space (The Netherlands), EADS CRC (Germany), MBDA France (France), EADS-ST (Germany and France), ENST (France), ESI (European Software Institute), Esterel Technologies (France), ETH (Switzerland), INRIA (France), INTECS (Italy), CNRS-LAAS (France), CNRS-VERIMAG (France), PROVER (Sweden), SCISys (United Kingdom), SoftWcare (Spain), SYNSPACE (Switzerland), Terma (Denmark), VALIOSYS (France), UPD (University of Padua, Italy), VUT (Austria)

### CONTACT PERSON

Dr. Eric Conquet  
TEC-EME  
European Space Agency  
Tel. +31 71 565 3244  
Fax. +31 71 565 5420  
[Eric.conquet@esa.int](mailto:Eric.conquet@esa.int)

### PROJECT WEBSITE

[www.mayeticvillage.com/assert](http://www.mayeticvillage.com/assert)

### BUDGET

Total cost: 15 M€  
Funding: 8.3 M€

### TIMETABLE

Starting date: 1. September 2004  
Duration: 36 months

This project is part of the portfolio of the  
**Embedded Systems Unit – C3**  
**Directorate General Information Society**

For more information please check:

[http://www.cordis.lu/ist/directorate\\_c/ems/](http://www.cordis.lu/ist/directorate_c/ems/)