



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

**Dr. Eric Conquet**  
**ESA/ESTEC**  
**TEC-SWE, Software Engineering and Standardization**  
**Noordwijk, The Netherlands**

## ASSERT genesis

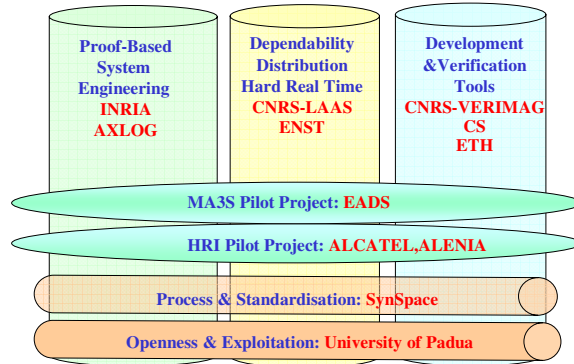
- Software crisis: origin is in fact a lack in system engineering.
- Current System design approach is exceedingly empirical.
- It is unable to cope with increasing systems complexity.
- Use of formal techniques at software level without any formal approach at system level is a nonsense.
- Requirements:
  - System Architecture must be proven by construction,
  - All new systems shall be built from a limited set of proven system families.
  - A continuous proof based approach (from system requirements down to final implementation) must be used, replacing the test effort
  - Industry has to be strongly involved in this new process definition and implementation in order to generate the expected ROI.

- A project partially funded by the European Commission under the IST priority of the FP6.
- Targeted area in the IST: Embedded Systems
- Type of instrument: Integrated Project
- Number of partners: 29
- Project cost: 15 M€
- Amount of EC funding: 8.3 M€
  - Roughly 50% of the project cost (the rest is funded by the partners)
- Total duration of the project: 3 Years.
- Started on the 1st September 2004.

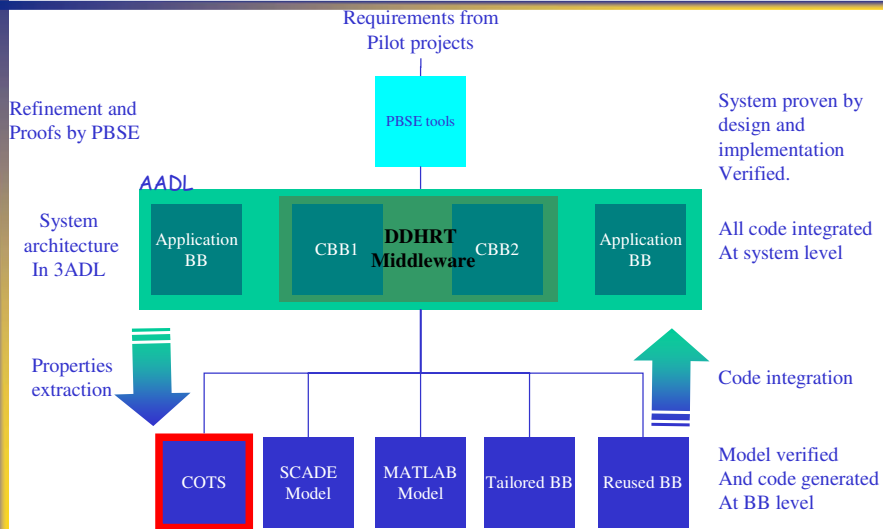
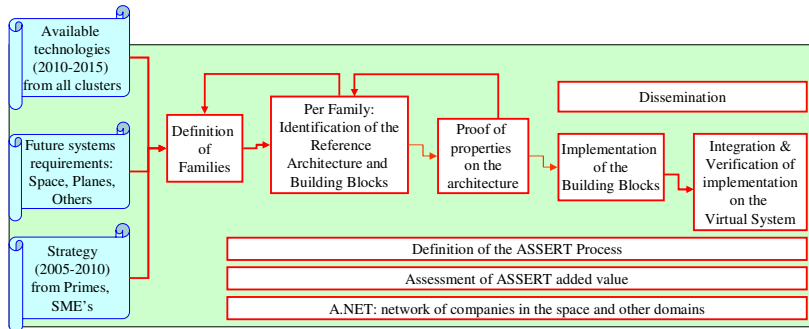
- System = computer systems (e.g. on board computers).
- System and Software engineering = to solve the SW crisis by bridging the System/SW gap
- Proof-based System and Software engineering = System and SW designs will be proven before implementation
- Real-time systems = systems with high dependability constraints (on which we depend!)

ASSERT aims at reconciling system and software engineering through a continuous proof-based approach applicable to real-time systems.

Coordination: ESA  
 Clusters: to bring the scientific and technical expertise  
 Pilot Projects: to assess the project outcomes.



1. **ESA - Coordinator**
2. Technical University Vienna
3. ETH -Swiss Federal Institute of Technology
4. SynSpace
5. BSSE
6. EADS Corporate Research Center
7. EADS-Space Transportation (D)
8. EADS-Space Transportation (F)
9. Terma A/S
10. European Software Institute
11. SoftwCare
12. ALCATEL-Space
13. ASTRIUM (EADS) SAS
14. Axlog Ingenierie
15. CS - Systèmes d'Information
16. DASSAULT Aviation
17. DIT/UPM university of Madrid
18. MBDA France
19. ENST- Ecole Nationale Superieure des Télécommunications
20. ESTEREL Technologies
21. INRIA - Institut National de Recherche en Informatique et Automatique
22. CNRS - LAAS&VERIMAG
23. TNI-Valiosys
24. ALENIA SPAZIO SpA
25. INTECS HRT
26. University of Padua
27. Dutch Space BV
28. PROVER
29. SciScys



## ASSERT after 1 year: weaknesses?

- Yes, some!
- Technical Integration is lagging:
  - Size and heterogeneity of the consortium do not help
  - The first year was used to open all technological boxes
- The project has been victim of the "wait for being better" syndrome.
  - A good idea could be replaced by a better one, one of these days!
  - The ambitious vision has pushed partners to propose new solutions, not always mature.
  - This syndrome has delayed the production of demonstrable results.
- Communication to the outside world has to be improved:
  - Make the project googable!
  - Attract people from the outside world to build the A.net.

## ASSERT after 1 year: major achievements

- The project has passed the first review without big damages,
- The PBSE requirement capture approach has finally convinced industrial partners:
  - A separation between functional and non-functional properties at system level was appreciated.
- A common understanding of the ASSERT process has emerged:
  - The work made by the Process and Standardisation cluster to capture the process is impressive
- The whole project has now a clear vision on how to reach its ambitious objectives.

- After the review, the project is working on the implementation plan for the next period.
- This period will be the time of:
  - Production of demonstrable results ("Put your hands on the real things!")
  - Communication and dissemination to real space projects,
  - Dissemination to other industrial domains through A.Net.
  - More links between ASSERT and other initiatives (TOPCASED, MODELWARE), or other international committees (AADL, OMG, SAE)
- Stay tuned and contact us!