

# ASSERT

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

*Eric Conquet*

*ESA/ESTEC*

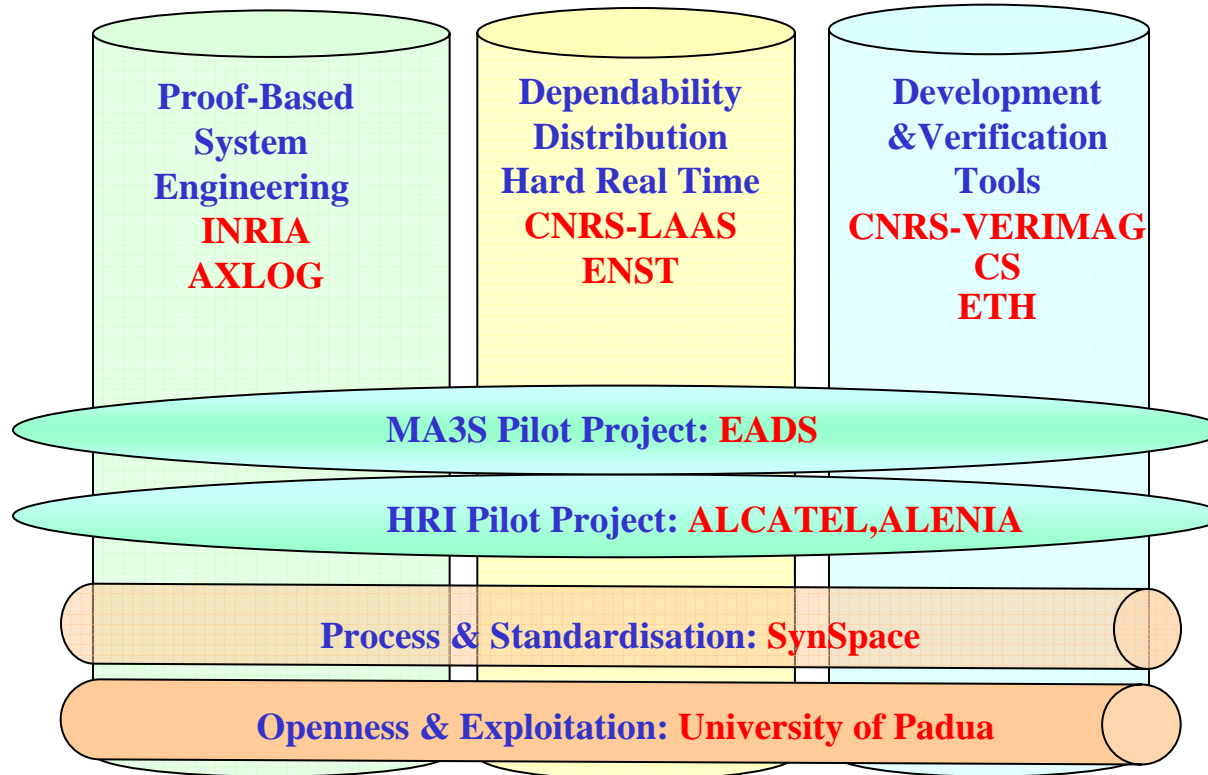
*TEC-EME, Software Engineering and Standardization*

*Noordwijk, The Netherlands*

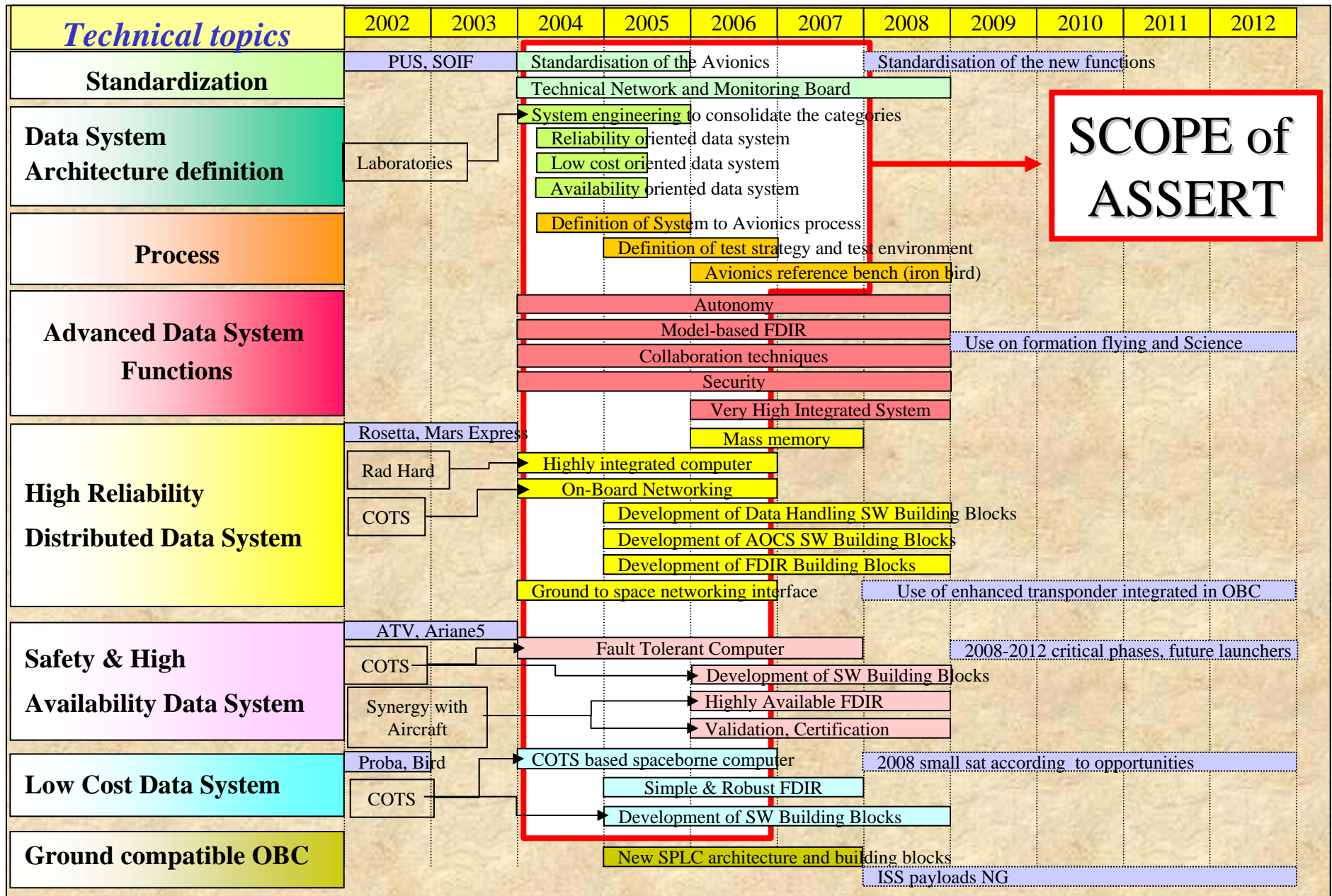
- **Related strategic objective: Embedded Systems**
- **Type of instrument: Integrated Project**
- **Number of partners: 29**
- **Project cost: 15 M€**
- **Amount of EC funding: 8.3 M€**
  - *Roughly 50% of the project cost (the rest is funded by the partners)*
- **Total duration of the project: 3 Years.**
- **Expected starting date: 1<sup>st</sup> September 2004.**

- **ESA is the coordinator of ASSERT.**
- **Consortium with major space and aircraft companies**
  - *Could have been bigger but limitation due to funding and manageability,*
  - *Could have been enlarged to include other industrial domains.*
- **Network of space companies within ASSERT**
  - *Will have a privileged access to some ASSERT results*
- **Synergy with other industrial domain**
  - *Sharing strategic view*
  - *Sharing methods and tools*
  - *Exchanging experience*
  - *Develop common products and technologies*

ASSERT is structured into scientific clusters and Outcomes are assessed through two Pilot Projects.



- **ASSERT implements the harmonisation**
- **Establish solid connection with EC.**
- **Primes will have to enhance their practice on system design (system=data processing system)**
- **SME's will be able to invest on tools and building blocks**
- **Research lab's will implement the ESTEC ambitious technical strategy.**
- **All companies and lab's are connected through a network: ANET**
- **Dissemination to industry, university, projects**
- **Connection with external partners: Airbus, Peugeot (PSA), AADL committee.**



**SCOPE of ASSERT**

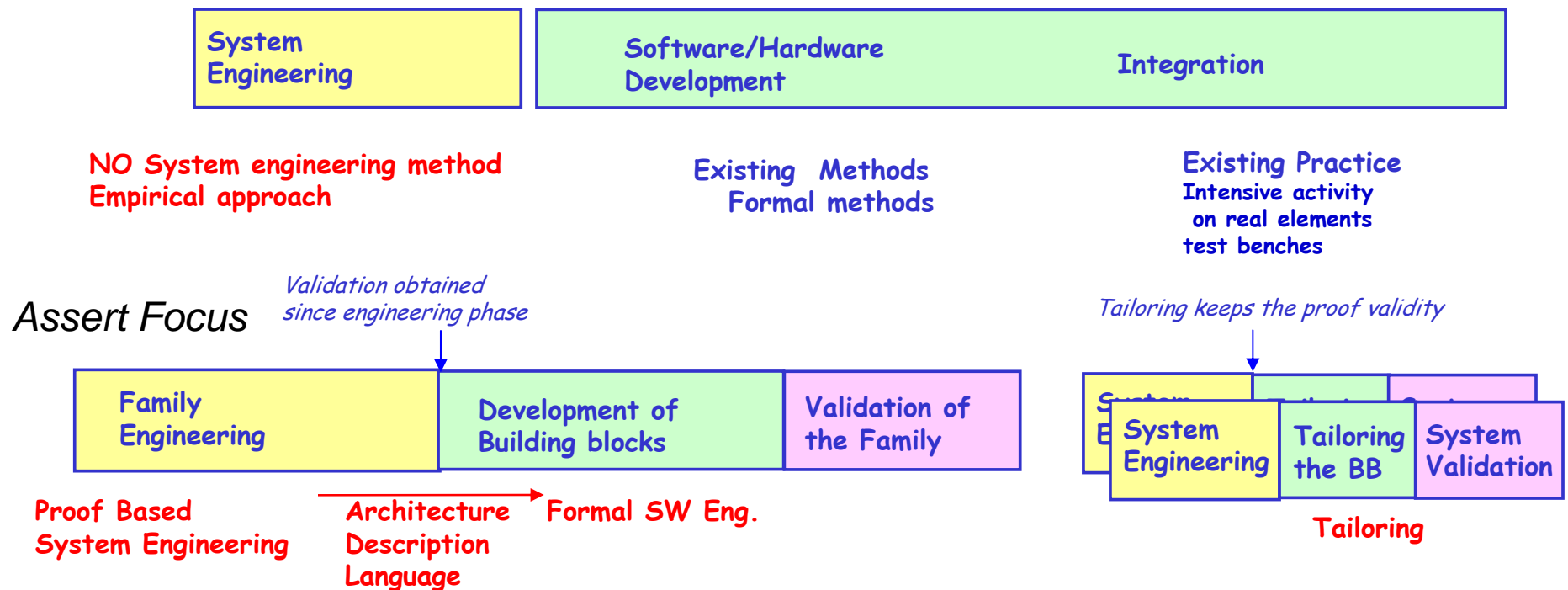
1. **Technical University Vienna**
2. **ETH -Swiss Federal Institute of Technology**
3. **SynSpace**
4. **BSSE**
5. **EADS Corporate Research Center**
6. **EADS-Space Transportation (D)**
7. **Terma A/S**
8. **European Software Institute**
9. **SoftwCare**
10. **ALCATEL-Space**
11. **ASTRIUM (EADS) SAS**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



# Technical overview

- **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.*

## Embedded Systems (EMS) Life Cycle Activities.... and Problems



### Methodological Features

- ▶ Mastering the complexity once
- ▶ Proving the basics of the family once
- ▶ Full coverage of EMS development cycle
- ▶ Multi-domains and Dissemination are essential

### Benefits

- ▶ production of a new system from family
- ▶ schedule and cost efficient
- ▶ full confidence in proofs at family level
- ▶ Proofs are kept for each instance

## Major technical breakthrough brought by PBSE (1/2)

- **A mature System definition must be based on sound basis.**
  - *Mathematics for Aeronautic, Space, bridges, steel.*
  - *There is no such strong support for computer based systems.*
- **Computer systems are based on hidden mathematics for scheduling, resource, error, communication management.**
  - *We have to enforce this view in order to prove the system behaviour and properties.*
- **Having this basis defined will allow to industrialise the domain.**
  - *Building a bridge means applying already proved rules.*
  - *Building a computer based system will mean applying the family and the PBSE tailoring rules.*

- **Start with requirement capture: what are the desired properties and constraints,**
- **Create the specification,**
- **Look for an existing solution, or create a new one,**
- **Prove that the solution fulfills the requirements and give the Feasibility Conditions (conditions under which the proof is valid)**
- **If the solution is implemented correctly, it works by design.**

## Major technical breakthrough brought by PBSE (2/2)

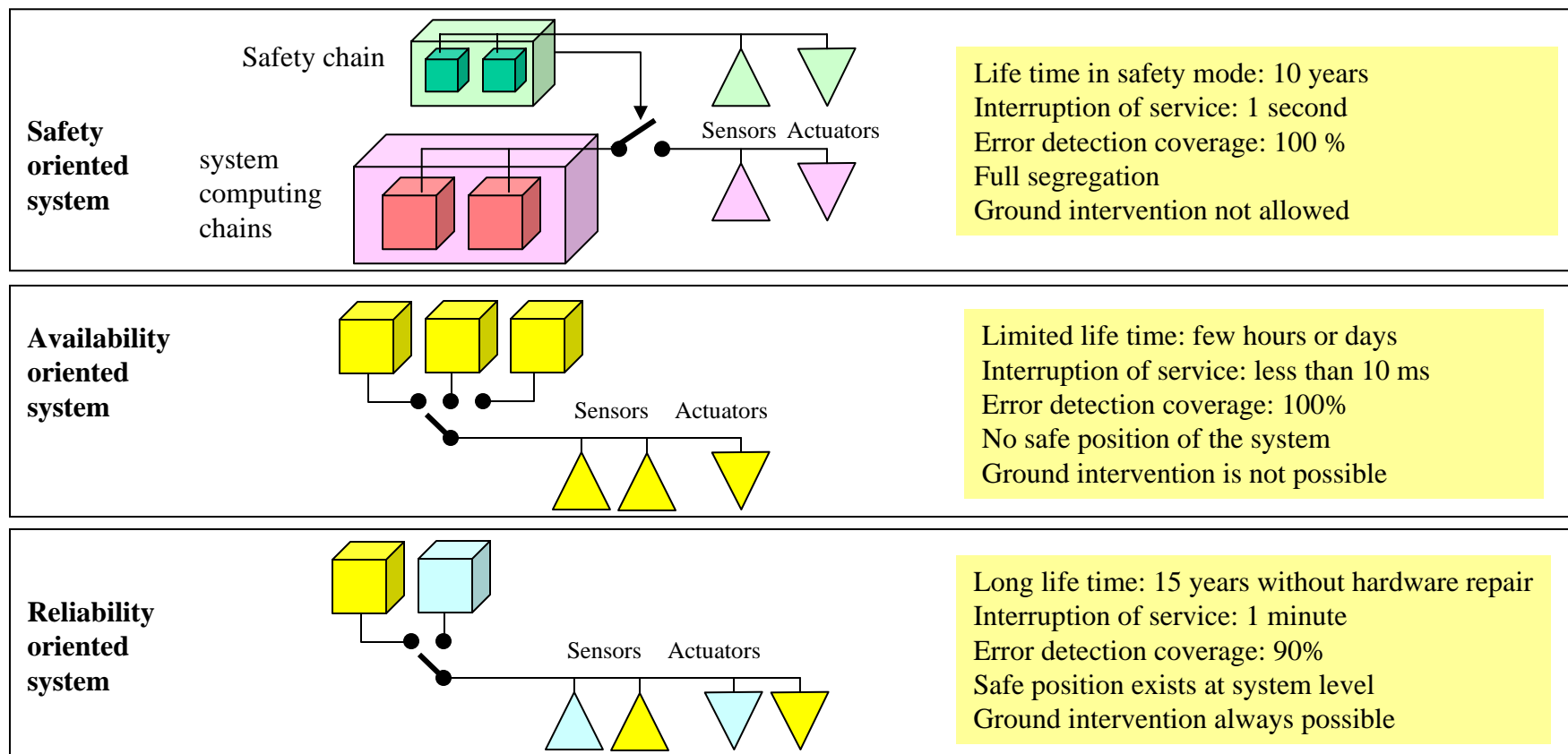
- **PBSE system design is the assembly of already proven solutions (algorithms). The assembly being demonstrated as composable and then proven.**
  - *Incremental development is then allowed as properties and interface are well defined.*
- **Flexibility in the design cycle is provided through the tailoring of the adopted solutions.**
  - *The FC proves that within these conditions the system is tailorable while keeping the proof valid.*
- **Whenever the FC does not fulfil the system needs, it is not too late to partly rerun the requirement capture.**
  - *It will allow early stopping of badly designed system before going to manufacturing.*

# **Proof-Based System Engineering?**

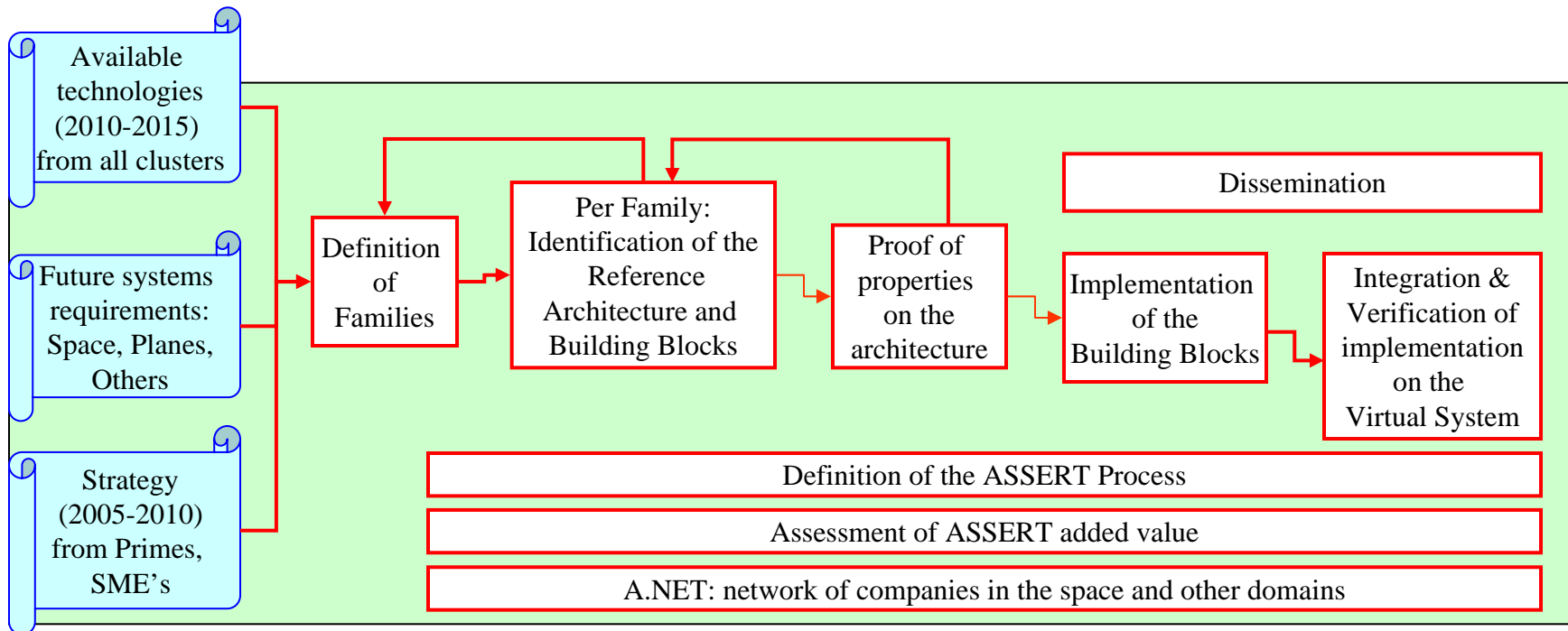
## **An example on the PHIDIAS project (DGAC-Thomson Airsys-INRIA)**

- **Example of PBSE helpful in “early stopping”**
- **New ATC/ATM**
- **According to theoretical results: impossibility result →  
No solution**
- **Savings? Avoid embark in endless design,  
implementation, testing phases (can’t work).**
- **Quantification? Total contract = 100 MFF**

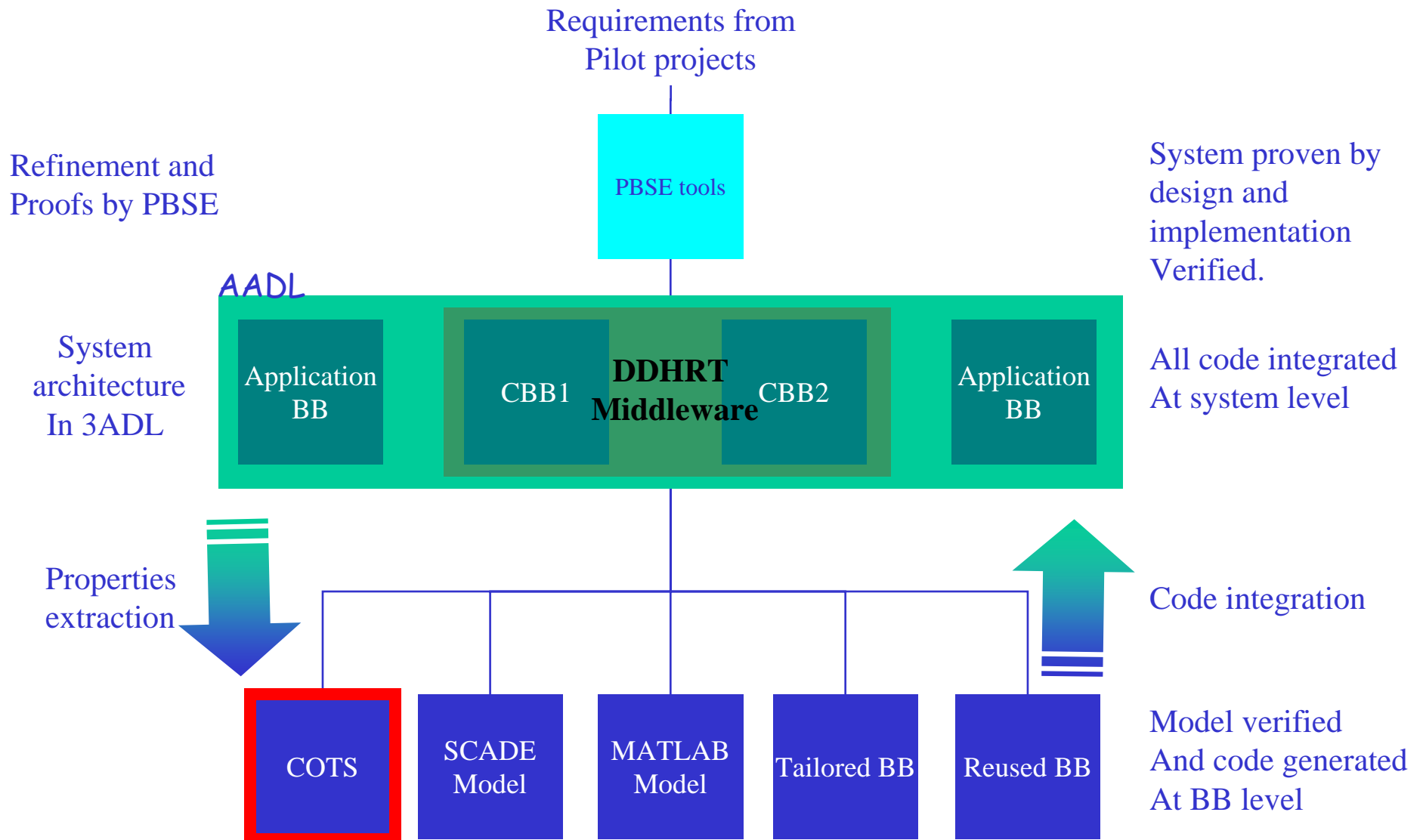
- Harmonisation shows that for what concern data systems: Earth Observation, Science and other systems can share the same platform.
- Design of new systems must no more be done according to market segments but according to their properties: dependability, reliability, ...



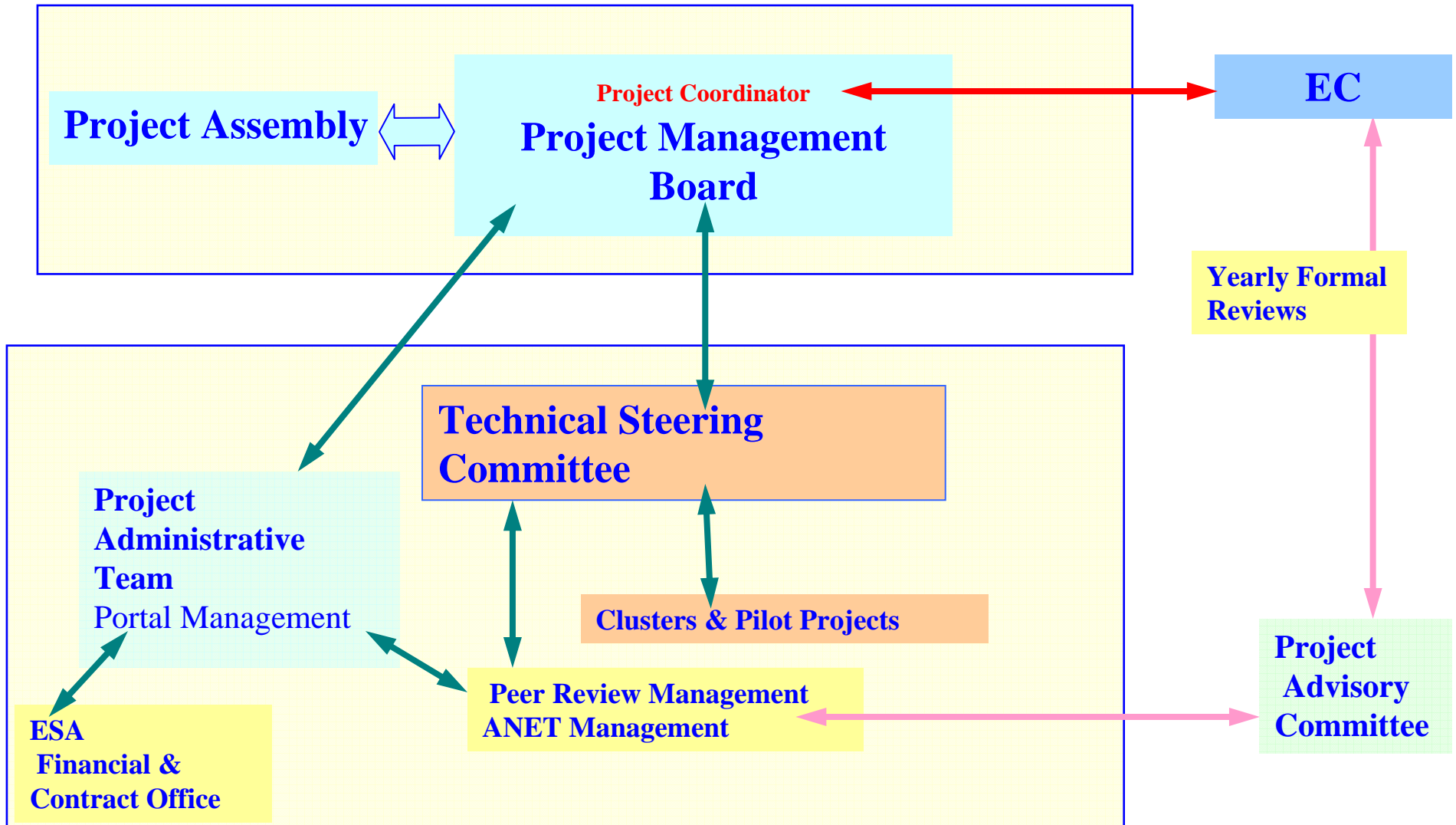
- **ASSERT will develop** methods, process, and tools **for continuous** proof-based approach **from early system specification down to final implementation for avionic systems.**
- **ASSERT will** develop and prove architectures of system families **so that instantiation of these families within a project can be done within 2 years time (instead of 4) with operational costs of the system divided by 5 to 10.**
- **ASSERT outcomes:**
  - A system design process based on the use of system families,
  - Architectures and building blocks (Hardware and Software components),
  - supporting tools for the data processing function of critical Embedded Systems requiring fault tolerance, safety and hard real-time.



## Needs for tool support in ASSERT



# Assert Management Structure



- **Interests from the ASSERT point of view:**
  - *AADL is one of the major stones of the ASSERT strategy,*
  - *Many ASSERT partners have expressed interest to work on or around AADL (language extensions, tool support, additional analysis).*
  - *ASSERT strategy is clearly linked to the use of common standards.*
- **Interest from the Committee perspective.**
  - *ASSERT will be a source of proposals for extending/improving AADL,*
  - *ASSERT will give the Committee the access to different case studies,*
  - *ASSERT is an entry point to a large consortium.*
  - *ASSERT will prototype tool support for AADL modelling, analysis, code generation, connection with other formalisms/tools.*
  - *ASSERT has access to a significant budget and manpower.*

# **How to implement the ASSERT/AADL Committee link?**

- **Participation of ASSERT partners to the meetings:**
  - *Does not necessarily mean that all ASSERT partners have to be members of the committee!*
- **Organization of common international events:**
  - *May include tutorials and presentation of case studies.*
- **Participation of Committee members to the ASSERT advisory committee:**
  - *Experts can be appointed by the EC to be part of formal annual reviews of project results.*
- **Common lobbying actions on both side of the atlantic:**
  - *To get funding from the EC (opportunities to come)*
  - *To get funding from US institutions (NSF, ...)*
- **Other ideas?**