

ASSERT proposal for a FP6 project

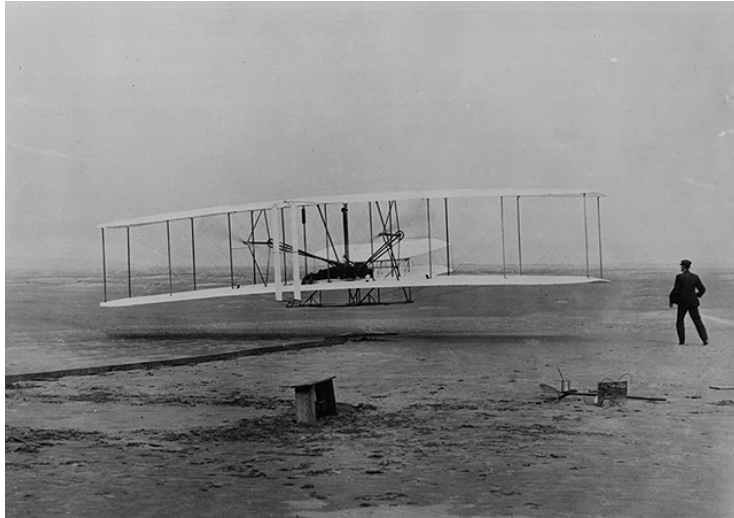
*Automated **S**ystem and **S**oftware **E**ngineering
for **R**eal-**T**ime applications*

Eric Conquet

ESA/ESTEC - TOS-EME

AADL Comittee Meeting – Nashville

October 2003



In 1903, an empiric approach to build a flyable and controllable aircraft.

In 2003, a scientific approach to build a reliable and safe aircraft.



And in system and software engineering?

Rationale for ASSERT.

- An ESA “SW crisis” document reported in 2002 a number of issues at SW level for space applications:
 - *Cost and schedule overruns.*
 - *SW issues not really understood at system level.*
 - *SW crisis is probably also a System crisis.*
- How can we develop more complex systems with the current approach?

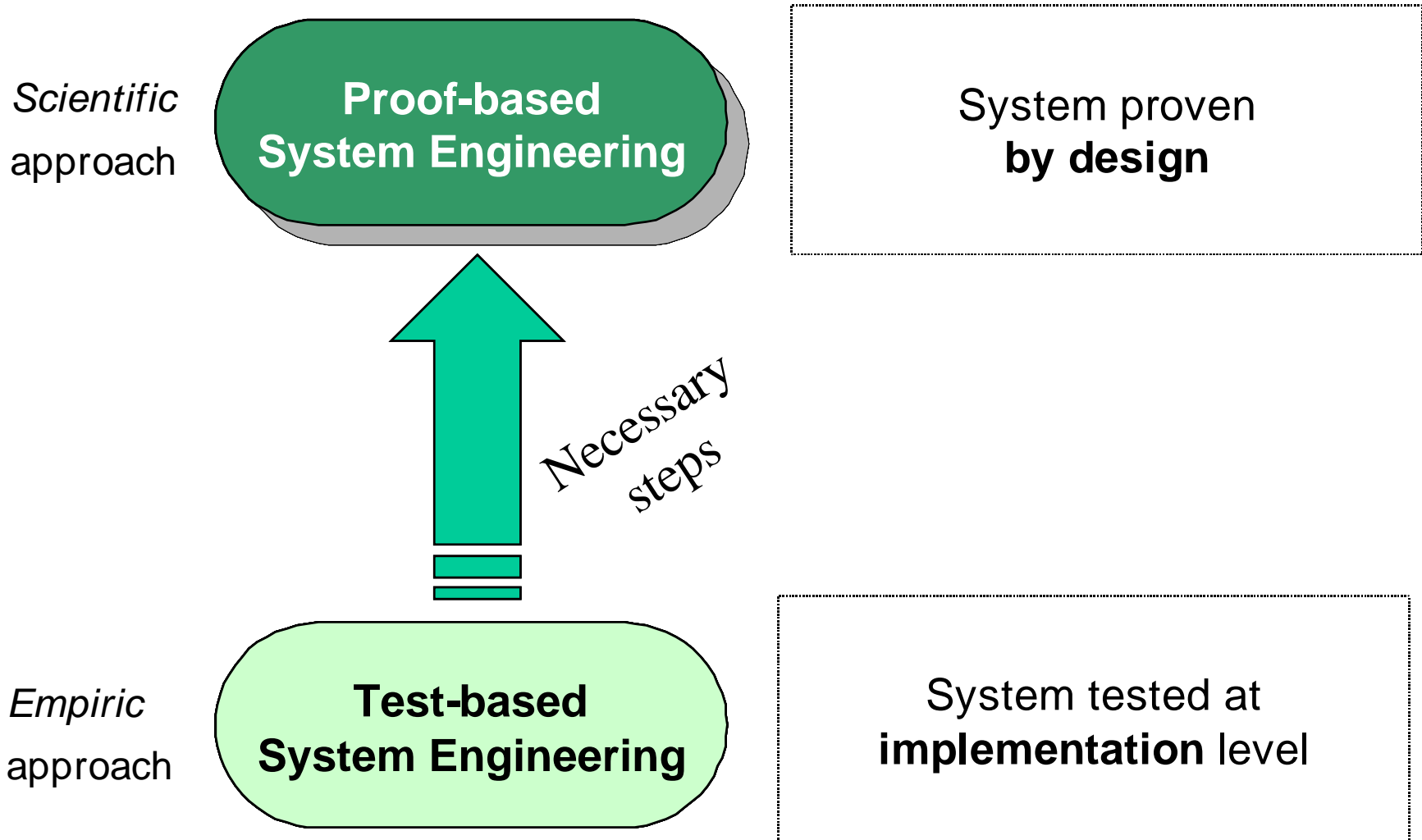
System and SW Engineering Today.

- Mostly an empiric approach:
 - *System and SW design are build from team experience and quality is unknown until the test phase.*
 - *Paper specification: How to verify properties and completeness?*
 - *Poor traceability: How to be sure that design is complete and consistent?*
 - *Manual coding and testing: How to reduce cost?*
- Poor reuse of best practices: How to benefit from already proven mechanisms?

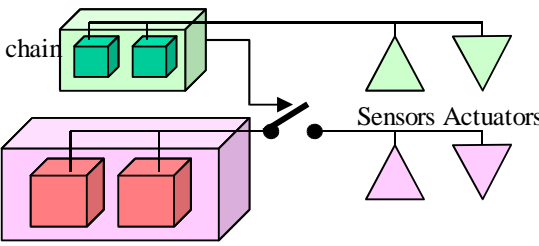
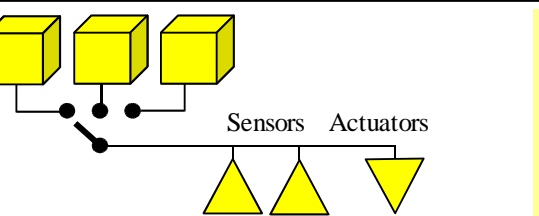
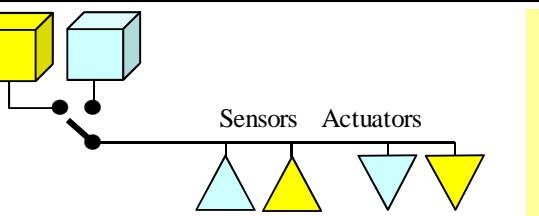
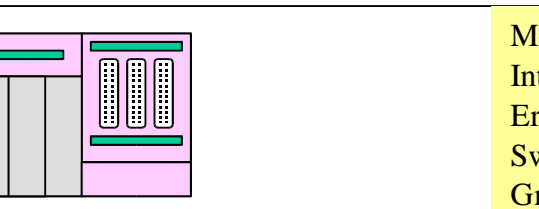
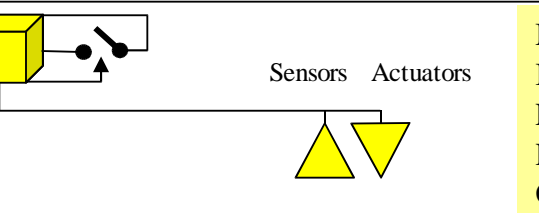
What can be changed?

- From an empiric to a **scientific** approach in system and SW engineering: by introducing proof obligations at ALL steps (PBSE approach).
- From specific to **generic** solutions: define system families to build common architectures for cross-domains problems.
- From paper to **model**: use the AADL language to support all system design and verification activities.
- From individual to **team**: disseminate those best practices through an education and training program.

ASSERT: a pragmatic path to achieve an ambitious vision.



From system families to generic architectures.

<p>Safety oriented system</p> <p>system Computing chains</p>		<p>Life time in safety mode: 10 years Interruption of service: 1 second Error detection coverage: 100 % Full segregation Ground intervention not allowed</p>
<p>Availability oriented system</p>		<p>Limited life time: few hours or days Interruption of service: 10 ms Error detection coverage: 100% No survival mode at system level Ground intervention is not possible</p>
<p>Reliability oriented system</p>		<p>Long life time: 15 years in orbit Interruption of service: 1 minute Error detection coverage: 90% Survival mode at system level Ground intervention always possible</p>
<p>Ground technology oriented system</p>		<p>Medium life time: 3 years Interruption of service allowed Error detection coverage: 90% Switch payload to safe state when error Ground intervention always required</p>
<p>Cost oriented system</p>		<p>Medium life time: 3 years Interruption of service allowed Error detection coverage: 80% Robust survival mode at system level Ground intervention always required</p>

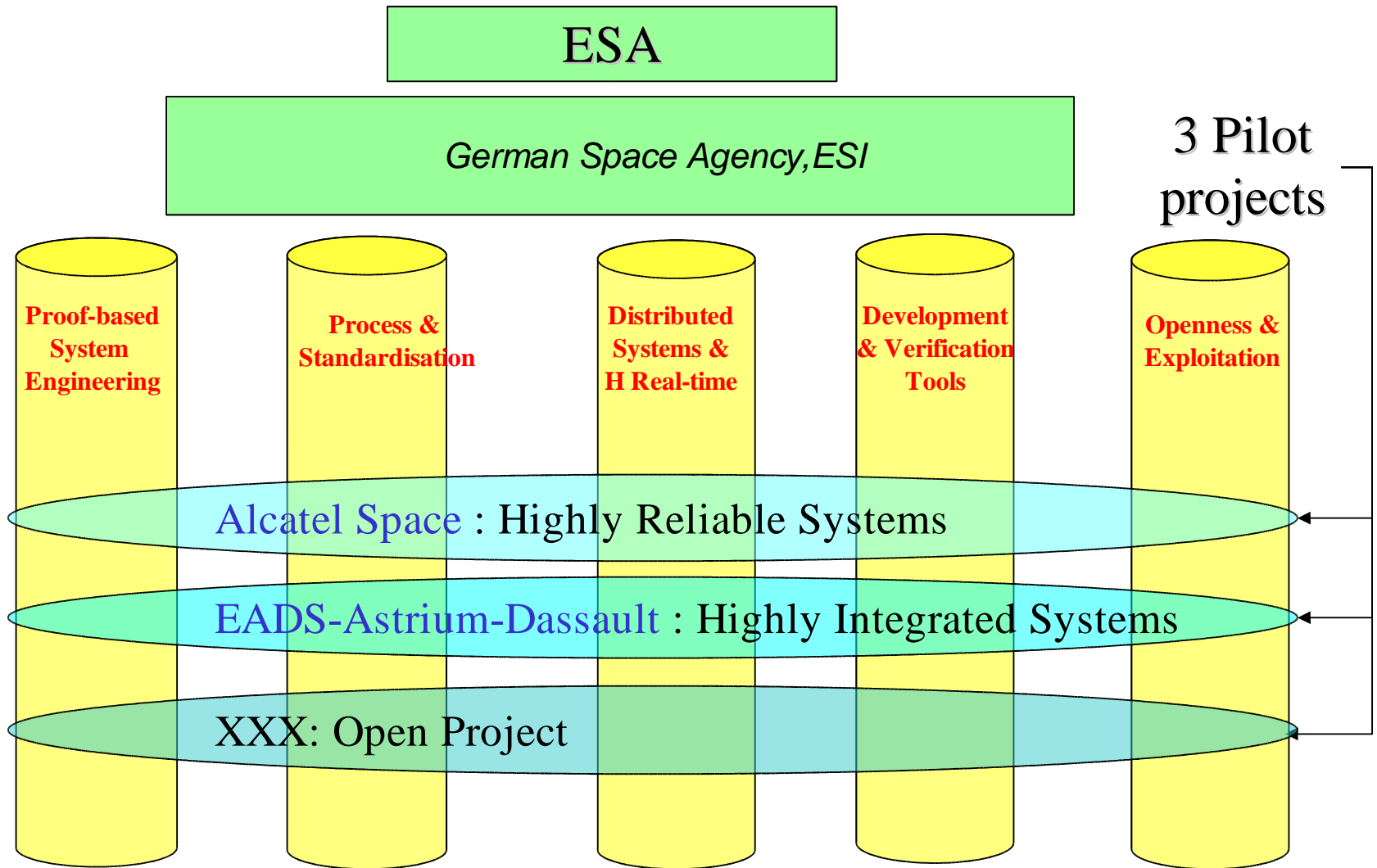
The ASSERT project at a glance.

- Coordinated by ESA (Eric Conquet & Philippe David)
- 32 partners
- 10 countries
- Overall budget: 20.6 Meuros
- Requested EC funding: 11.6 M Euros
- Total effort: ~2000 man months (166 man years)
- Expected Kick Off: June 2004.
- Duration: 3years (2004-2007)

ASSERT and AADL

- AADL to support the requirements capture phase (identify required properties)
- AADL to capture system families reference architectures
- AADL to define architecture building blocks (system design patterns)
- AADL to build complete system architectures by composing Building Blocks (proof of composition rules)
- AADL to automatically generate the complete system.
- AADL to smooth the transition from system to SW (integration of SW components modelled with formal languages)

ASSERT: 2 dimension organization



5 Clusters: Academic, SME's, tool provider

Companies involved in ASSERT

- Agencies:
ESA, German Space Agency, ESI.
- System Primes:
Astrium-space(F+D), Alcatel(F), EADS-ST(F&D), EADS CRC(D), Alenia(I)
- Space companies:
CS- France, Dutchspace(NL), Terma(DK), Scisys(UK), Intecs(I)
- Aircraft companies:
Dassault(F), EADS-MBDA(F+D).
- Academic:
VERIMAG(F), Padoua University(I), LAAS(F), ENST-Paris(F), Technical University of Madrid (E), INRIA(F), ARCS(A), University of Valencia(E), University of Vienna(A), University of Zurich(CH).
- Quality, Process:
SYNSPACE(CH).
- Tool provider:
Esterel-Technologies(F), TNI-Valiosys(F), Axlog(F), BSSE(D)

Cooperation between ASSERT and the AADL committee

- Extensions to AADL: PBSE support, distribution, dependability,...
- AADL tool support
- Transitions from system engineering to SW engineering.
- Applications of AADL to industrial cases.
- Definition of a SE process using AADL.
- Education and training program.