PBSE and AADL in ASSERT

Jean-François Tilman
Axlog ingénierie

Jean-François.Tilman@axlog.fr
Agenda

- Introduction
- The ASSERT project
- PBSE and TRDF
- AADL for this purpose
- Prospects
ASSERT
ASSERT objectives

- ASSERT = "Automated proof-based System and Software Engineering for Real-Time applications"
- "Software crisis": current empirical practices and increasing complexity.
- Purpose: improvement of the development process and quality of operational systems by:
  - following a PBSE method during the whole development cycle;
  - using an ADL to write specifications exchanged across lifecycle phases;
  - ensure the continuity with the SW development.
ASSERT clusters and leaders

PBSE (Inria, Axlog)

- Dependability Distribution
- Hard Real Time (LAAS, ENST)

Development Verification Tools (CS, Verimag, TNI, ETH)

Multi-domain Advanced Available Automated System pilot project (EADS-ST, Astrium, Dassault Aviation)

Highly Reliable Infrastructure pilot project (Alcatel, Alenia)

Open pilot project

Process & Standardisation (Synspace)

Openness & Exploitation (University of Padua)
PBSE and TRDF
The PBSE approach

- PBSE = "Proof-Based System Engineering"
- Aim: a system engineering method for computer-based systems aimed at eliminating faults in the early phases of lifecycles.
  => rigorous specifications & fulfillment of proof obligations.

<table>
<thead>
<tr>
<th>Phases</th>
<th>Contents/outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement capture (RC)</td>
<td>description of the application/user problem</td>
</tr>
<tr>
<td></td>
<td>specification of the computer-based system problem (CBR)</td>
</tr>
<tr>
<td>System design &amp; validation (SDV)</td>
<td>specification of a computer-based system solution (CBS)</td>
</tr>
<tr>
<td>Feasibility &amp; dimensioning (FD)</td>
<td>building block composability checking and tailoring</td>
</tr>
<tr>
<td>Integrated testing (IT)</td>
<td>generation of the complete suite of tests needed to check the implemented CBS with respect to worst-case (load &amp; failure) scenarios</td>
</tr>
</tbody>
</table>
The PBSE life-cycle

- Requirement capture
- System design & validation
- Feasibility & dimensioning
- CBS construction (implementation and/or assembly of reused building blocks)
- Integrated testing
- Fielding of CBS

non-ambiguous, consistent and complete description of the problem, of the solution (+ proofs (CBS solves CBR))
Building an architecture

- A building-block is any concept which can be used from the upper specification down to the final implementation.
- PBSE concern stops where starts implementation, but it stops with a "proven specification" of what must provide the terminal BB to be eligible to participate to a CBS.
TRDF

- TRDF = *Temps-Réel, Traitement Distribué, Tolérance aux Fautes* (Real-Time, Distributed Treatments, Fault Tolerance)
- TRDF is a PBSE method based on deterministic approaches/solutions.
- Developed at INRIA, and is today the only existing PBSE method, tried successfully in various domains.
- See [GLL1998] for more information.
Success stories of PBSE/TRDF

- P1 (1995-97): Modular avionics (air combat) for Dassault Aviation and French MoD => validation of the full TRDF method (from RC to CBS implementation).

- P2 (1996-97): For IPSN (French Atomic Energy Authority): how to tell whether COTS can be used in safety critical systems?

- P3 (1996-98): For French Ministry of Research and DA => PBSE solves problems that cannot be solved with (formal) SW engineering methods - which may explain the "SW crisis".

- P4 (1997): Analysis of the Ariane 5 flight 501 failure => Satellite launcher explosion has been caused by 1 fault in the RC phase – SW is not the "culprit" (contrary conclusions in the official IB report).

AADL for this purpose
AADL in ASSERT

- ASSERT needs an ADL to handle non-ambiguous, consistent and complete descriptions of applications/user problems.

- The most mature ADL in this domain is AADL; => Axlog has promoted AADL, which has been chosen as a base for the project.

- AADL has not been initially designed for this specific purpose. => the studies will reveal complements and extensions to support the needs of ASSERT.
AADL extensions

- Several kinds of extensions may be proposed for AADL:
  - PBSE extensions: to support the proof obligations at any level of the description;
  - DDHRT extension: the needs of the dependability and distribution cluster are probably closer with the current AADL (e.g., connectors).
- => collaboration with the AADL standardisation committee.
PBSE tools

- In ASSERT, several prototype tools will be developed to support the process. The aim is to have an expertise of AADL to demonstrate the feasibility of these tools:

  - RC tool: to support the requirement capture phase (questionnaires, dictionaries);
  - SDV tools: to support system design and validation (system design "assistants");
  - FD tool: Oracles to support feasibility and system dimensioning;
  - IT tool: Oracles to support (final) integrated testing.
ADeS

- ADeS is an example of a possible SDV tool.
- It has been developed during the AADL study led by Axlog for ESA.
- Its purpose is the simulation of the behaviour of an architecture described with AADL.
- The results of a simulation are not proofs, but they may help the designer in its work.
Prospects

- Two major goals of ASSERT are to check:
  - is it possible to build PBSE tools?
  - can such tools be used by the "average" engineer, in the course of a real project?

- Timescale: by mid-2006, prototypes of PBSE tools will be available and assessed.

- Rationale: the adoption of PBSE methods appears to be the best strategy to achieve the "faster, cheaper, better" goal.
References