Panel session

"Balancing cost and assurance in embedded systems development"

Jérôme Hugues, GET-ENST

MONTEREY'06

TELECOM PARIS
école nationale supérieure des télécommunications

A few statements ..

- Embedded systems are widely used
- .. Including for life-critical systems
- .. For which assurance is a necessity
- Some of you took an airplane to come, right ? ;)

- High-Assurance systems should be trusted
  - .. but this is has a cost to support DO-178B, ARINC653, etc
- How much ? How important ?

Statements I like

- "There are two ways of constructing a software design. One way is to make it so simple that there are obviously no deficiencies. And the other way is to make it so complicated that there are no obvious deficiencies." (Prof. C.A.R. Hoare)
- « As soon as we started programming, we found to our surprise that it wasn't as easy to get programs right as we had thought. Debugging had to be discovered. I can remember the exact instant when I realized that a large part of my life from then on was going to be spent in finding mistakes in my own programs. » (M. Wilkes)
- « Computer science is not a science » (Alice, my wife, working on Video & Signal processing)

- Sounds rather discouraging

TELECOM PARIS
école nationale supérieure des télécommunications

Increasing assurance ?

- It is the application of engineering rules
  - Coding restrictions, well-defined patterns, reviews ..
- Engineering is the art of applying well-known concepts to solve problems
  - And research the art of defining new (consistent) concepts
- It works fine when it comes to automotive, building, electronics
- Many software projects demonstrate high-assurance using dedicated process can in fact reduce cost
  - Ada, SPARK, synchronous languages (Scade)..

- Why is it different for s/w ? Why should it increase cost ?

What increases cost of s/w

- Hard to define methods, harder to have them respected
  - Goes against many (bad) habits, untold elements
- C/S is plagued by non-technical drivers
  - Fashion (Python, Eclipse, etc)
  - Poor contract writing (poor specification)
  - "Gurus"
  - Shortsighted managers
    - ✓ *Cost to develop vs cost to maintain*
  - Difficult to separate technology from supporting tools

TELECOM PARIS
école nationale supérieure des télécommunications

Assurance & cost

- Assurance is usually not gained by increasing cost, but by respecting a well-thought design process
- A project need
  - Personal rigor
  - Respect for guidelines, methods
  - And a good process and supporting tools
- Deviations from a (good) engineering process create inbalance
- Let us be engineers, software architects; not coders !