ReSIST Second Open Workshop Resilience in computing systems and infrastructures: a research agenda

Roma, Italy, 18 October 2007

Assessability

Industry's view

Jean-Paul Blanquart
Astrium Satellites, Toulouse, France

EADS astrium

Assessability, gaps and resilience

- An assessability gap is simply a gap:
  - A technology that would be accessible but couldn't be assessed is, in practice, not accessible from industry's viewpoint
- What does resilience assessment means?
  - Resilience has to do with
    - Changes, not necessarily foreseen, clearly identified in advance
    - Robustness
  - Assessment (industry) has to do with
    - Evidence of compliance with respect to some specification, requirements
    - But.. Difference kinds of evidence (technical, informed expert judgement, formally or contractually agreed, …)

Representativeness, significance

- Modelling resilience, and modelling systems in terms of resilience (GA1), a clear and important challenge
- Modelling complex systems (GA6, 12, 16, 17): if a system is inherently complex, its model is inherently… wrong?
- Faultloads and workloads for resilience assessment (GA5)
- Evolution metrics (GA7)… we do love metrics but again we must know what they represent, and what they are used for
- On-line assessment (GA9): a priori a little bit late but finally, very important: evolution must be controlled

Data

- Scenario-based assessment (GA2)
  - Also of (potential) interest for design (the “design from crash” paradigm)
  - How to assess the significance of the scenarios, their applicability to our system, the “coverage”?
  - How to abstract them into sufficient generic patterns?
  - How to still address appropriately the scenarios that no longer occur… because we knew how to prevent them?
- Speaking of data… how to assess the data part of some software, or to assess software taking into account its data… especially changing data, i.e., (basic) means for evolvability?

Quantitative assessment, dependability case (GA3, 4)

- Quantitative assessment… easier acceptance for security than for software reliability?
- Isn't there some "Heisenberg effect" when trying to measure the characteristics of security attacks?
- Mixing quantitative and qualitative or deterministic claims and arguments into a consistent convincing dependability case
- Dependability case: a framework to formalise and clarify the notion of software criticality?
- Not only final assessment. Important as support to design

Resilience overestimation

- Observed dependability in a stable situation is certainly a bad estimator of resilience though in absence of a good one, the confusion is quite easy.
- Co-evolution of threats and means (GA7)… a nice idea. Note that, as in biology, we shouldn't imagine necessarily some progress. Many systems evolve towards decreased dependability, badly controlled, because of the difficulty to evaluate the available dependability margins
- Responsibility failures (GA18): not knowing who is in charge is not the only issue. In many cases people don't even perceive the need for change in roles and responsibilities, especially in case of overestimated resilience