Observations: to common issues underlying the presentations today

Lorenzo Strigini

Balance between deterministic and probabilistic reasoning

"DO178C will weaken wording from *testing* to *verification* , to cover testing and/or formal verfication

- The real tension is between deterministic (formal or testing) evidence/reasoning and statistical evidence/reasoning

- [What is the exchange rate: how many test cases for one proof? *clearly simplistic question but ...]*
- you have to delimit by deterministic reasoning the areas where you need statistical reasoning
- **challenge:** have we good examples to propose?

socio-organisation issues: rituals vs philosophy

the prescriptive approach is broken ... but shall we fix it? It still helps.

- prescriptions reduce project/contract uncertainty for actors in a development/acceptance/licensing process
- hence attractive fallacy “I follow the prescribed process, therefore I achieve the target safety level”
- so... condemn the fallacy, destroy corporate incentive for many good practices, and ask instead for very complex reasoning that engineers are not prepared for?
- **challenge:** how to chart a non-safety-decreasing route from less desirable state to more desirable state?