Panel on “Evidence and Arguments…”

Bev Littlewood

Centre for Software Reliability, City University, London

b.littlewood@csr.city.ac.uk

Just a few thoughts…

- After-the-fact reliability/safety achievements are very impressive in general, *but variable*
- But *before-deployment* assessment still very difficult
- Safety case/arguments:

(assumptions, evidence) -> (safety claim, confidence)

  - Note the role of confidence: often forgotten. There is inherent uncertainty in the process of constructing arguments

- Why is it difficult? Why *uncertainty* in arguments?
  - Assumptions - there is always doubt about their truth
    - E.g., spec. correctness, oracle correctness, independence issues, etc
  - Evidence
    - E.g., strength/weakness, disparate in nature, poor empirical support (e.g. process -> product), engineering judgment, independence issues again!
  - “->”
    - Combining all this is *hard* because it’s so disparate
    - Subtle interactions (e.g. between different assumption doubts: *not* independent)
    - *Reasoning* is a fallible process
  - Confidence
    - Need a calculus - probability? Yes, because of need to assess *risk*. BBNs?