Workshop on Achieving and Assessing Safety with Computing Systems:

State of The Art and Challenges

Introduction

Lorenzo Strigini

52nd Meeting of the IFIP WG 10.4 on Dependable Computing and Fault Tolerance
Edinburgh, United Kingdom, June 28 - July 2, 2007
workshop organised by Robin Bloomfield, Zbigniew Kalbarczyk, Lorenzo Strigini

Which topics belong to “safety”?

- just the same problems that all engineering and computing deal with
- but taken very, very seriously
  - be *really* sure (enough) of safety properties before operation
  - don’t want to learn only after accidents
  - but must *really* learn from errors and surprises
  - must consider *whole* system (where exactly does it end?)
  - must achieve high confidence in the rarity of *quite* rare events

What's new in safety?

- safety is an old concern in computing
- important historical motivation for our area of work

- yet challenges grow:
  - more numerous, more critical systems
  - larger, more interconnected critical systems
  - demand for more rigorous safety justification
  - more dynamic markets, more off-the-shelf components

The programme

A sampler of problems and techniques in demanding applications, grouped around two general topics:

- *Friday*:
  Safety in large scale complex systems
- *Sunday*:
  Reasoning about safety:
  experience, evidence, arguments, certification

- each day ends with a panel discussion session
  - reactions and reflections on the day's talks and the broader picture
  - the day's speakers, plus a few invited to make brief initial statements, adding more viewpoints and concerns