Welcome to the Panel on

Emerging Hardware Technologies and Related Dependability and Security Challenges

Panellists

Jacob A. Abraham, Univ. of Texas, Austin, TX, USA

Helena Handschuh, Spansion EMEA, Levallios-Perret, France

Takashi Nanya, University of Tokyo, Japan

Alex Orailoglu, University of California, San Diego, CA, USA

Moderator:

Johan Karlsson, Chalmers Univ. of Technology, Göteborg, Sweden

What we heard so far …

Dependability threats and challenges

- Process variations
- Single event upsets (particle radiation, cross-talk, ..)
- Intermittent faults (gate-oxide break-down, …)
- Electromagnetic interference
- Aging faults (NBTI)
- Test, diagnosis and repair in CMOS and future technologies
- Error detection techniques for the nano regime

…. and haven’t heard

- Failure modes of new nano-devices.
  - Do we need new fault/error/failure models?
- How to avoid/tolerate design faults in chips with billions of components?
- Security issues
- What characterizes Nanocomputing:
  - Chips using new nano-devices (beyond CMOS) ?
  - Chips that combine CMOS with new nano-devices?
  - Chips with more than 10 Billion components?
  - Chips with more components than there are humans on Earth?

Questions to the panellists

- Which are the most important dependability and security threats imposed by nanocomputing?
- How would you rank the severity of the these threats in terms of the research and engineering effort required in order to mitigated them?
- Will the abundance of components (transistors and other nano-devices) provided by new hardware technologies allow us to deal with these threats using pure hardware solutions?
- How will nanocomputing affect the way we build reliable and secure software?