



Workshop on Dependable and Secure Nanocomputing

— Call for Contributions —

Thursday June 28, 2007 — Edinburgh International Conference Centre, UK

in conjunction with the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks — DSN-2007

Workshop Organizers

Jean Arlat, LAAS-CNRS, Toulouse, France
jean.arlat@laas.fr

Ravishankar K. Iyer, UIUC, Urbana-Champaign, USA
rkiyer@uiuc.edu

Michael Nicolaïdis, TIMA and iROC, Grenoble, France
michael.nicolaidis@imag.fr

Program Committee

Jacob A. Abraham, University of Texas, Austin, USA
Jacques Collet, LAAS-CNRS, Toulouse, France
Jiri Gaisler, Gaisler Research, Gothenburg, Sweden
Christian Landrault, LIRMM, Montpellier, France
Régis Leveugle, TIMA, Grenoble, France
Subhasish Mitra, Stanford University, CA, USA
Shubhendu S. Mukherjee, Intel, Hudson, MA, USA
Nithin M. Nakka, Motorola, Urbana-Champaign, IL, USA
Takashi Nanya, University of Tokyo, Japan
Rubin A. Parekhji, Texas Instruments, Bangalore, India
Michel Pignol, CNES, Toulouse, France
Jean-Jacques Quisquater, UCL, Louvain, Belgium
Pia Sanda, IBM, Poughkeepsie, NY, USA
Shiuhpyng W. Shieh, Nat. Chiao Tung Univ, Hsinchu, Taiwan
Matteo Sonza Reorda, Politecnico di Torino, Italy
Alex Yakovlev, University of Newcastle upon Tyne, UK
Vivian Zhu, Texas Instruments, Dallas, TX, USA

Important Dates

- Papers due: **March 16, 2007** 
- Acceptance notification: **April 13, 2007**
- Final version due: **May 4, 2007**

Further Information

For more information about DSN-2007 and the venue, please visit the conference web site at: www.dsn.org.

For workshop information, please send an email to the workshop organizers. See also: www.laas.fr/WDSN07.

Motivation

The evolution of nanocomputing technologies raises serious challenges both from the point of view of Dependability and Security. One classical issue to cope with is related to mitigating the impact of disturbances (e.g., the so called "soft errors") that are increasingly affecting the operation of computing systems. A wider issue is the impact of scaling, the inability to tightly control the manufacturing process to a degree possible before, as well as the impact of power, current and voltage fluctuations. These effects are expected to lead to not only a larger level of transients, but also a larger defect rate. Hence, the increasingly need to rely on fault tolerance techniques. Nevertheless, issues at stake go far beyond disturbances in operation. It is anticipated that general-purpose large-scale processor architectures will also suffer from low-fabrication yield resulting in a growing number of defective components at delivery. Indeed, the increased circuit sensitivity to small spot defects, the increasing sensitivity of long buses (Network on Chips) to cross talk, and in a larger extent the dramatic increase of statistical variation of process parameters in upcoming nanometric process nodes become the nightmare for yield and reliability engineers. Last but not least, one has to consider the risks faced by current integrated circuits, especially cryptographic devices, when exposed to malicious threats (including side channel attacks in smart devices and malevolent "fault injections" exploiting related vulnerabilities).

Scope and Objectives

The Workshop is aimed at characterizing these impairments and threats as well as distinguishing possible alternative design approaches and operation control paradigms that have to be enforced and/or favored in order to keep achieving dependable and secure computing. Three main goals were identified for the Workshop:

- a) Review the state-of-knowledge concerning the issues at stake in nanocomputing technologies: manufacturing faults, accidental operational faults, malicious attacks (trusted and intrusion tolerant devices).
- b) Identify existing solutions attached to various design options for mitigating faults and implementing secure and resilient computing devices and systems.
- c) Forecast the risks associated to emerging technologies and foster new trends for cooperative work, possibly combining various alternatives to help increase the pace of advances and solutions.

Participation, Submission and Information

The workshop is open to all researchers, designers and users involved with or having an interest in dependability and security of hardware technologies. We are interested in submissions from both industry and academia on all topics related to dependable and secure nanocomputing. Potential topics of interest include but are not limited to: emerging nanocomputing paradigms and models, failure modes and risk assessment,

yield and mitigation techniques in nanoscale technologies, on-line adaptive and reconfigurable nanoarchitectures, design techniques for developing resilient nanosystems, scalable verification and testing methodologies, network on chip and communication protocols, etc.

All prospective contributors should submit an extended abstract, work-in-progress report or position paper. Submitted papers must be original work with no substantial overlap with previously published papers or simultaneous submissions to a journal or conference with proceedings. The submissions should conform to the proceedings publication format (IEEE Conference style) and should range from two to six pages maximum (including all text, references, appendices, and figures). They should explain the contribution to the field and the novelty of the work, making clear the current status of the work. Each submission should start with a title, a short abstract, and names and contact information of the authors. Submissions must be made electronically (preferably, in PDF format) by sending an email to [dsn2007-nanocomputing\[at\]laas.fr](mailto:dsn2007-nanocomputing[at]laas.fr).

Submitted papers will be fully refereed by PC members. Accepted papers will be published in the supplement volume of the DSN 2007 proceedings. Authors of accepted papers must guarantee that their paper will be presented at the workshop.