3rd Workshop on Dependable and Secure Nanocomputing

— Call for Contributions —

Monday June 29, 2009 — Estoril, Lisbon, Portugal

in conjunction with the 39th Annual IEEE/IFIP International Conference on Dependable Systems and Networks — DSN-2009

The Workshop is also linked to the 15th IEEE Int. Online Testing Symp. (IOLTS) that is taking place in Lisbon area on June 24-27, 2009

Workshop Organizers

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

Cristian Constantinescu, AMD, Fort Collins, CO, USA
cristian.constantinescu@amd.com

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

Johan Karlsson, Chalmers University, Göteborg, Sweden
johan@chalmers.se

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

Program Committee

Jacob A. Abraham, University of Texas, Austin, USA
Lorena Anghel, TIMA, Grenoble, France
Davide Appello, STMicroelectronics, Agrate Brianza, Italy
Vikas Chandra, ARM R&D, San Jose, CA, USA
Yves Crouzet, LAAS-CNRS, Toulouse, France
Giorgio Di Natale, LIRMM, Montpellier, France
Babak Falsafi, EPFL, Lausanne, Switzerland
Richard E. Harper, IBM Research, Yorktown Heights, NY, USA
Shubhendu S. Mukherjee, Intel, Hudson, MA, USA
Takashi Nanya, University of Tokyo, Japan
Jean-Jacques Quisquater, UCL, Louvain, Belgium
Juan Carlos Ruiz García, Univ. Politécnica de Valencia, Spain
Allan Silburt, Cisco Systems, Ottawa, ON, Canada
Arun Somani, Iowa State University, Ames, USA
Janusz Sosnowski, Warsaw University of Technology, Poland
Andreas Steininger, Vienna University of Technology, Austria
Alan Wood, Sun Microsystems, Santa Clara, CA, USA
Yervant Zorian, Virage Logic, Fremont, CA, USA

Important Dates

NEW!

- **Papers due: March 23, 2009**
- **Acceptance notification: April 20, 2009**
- **Final version due: May 11, 2009**

Further Information

About DSN-2009 and the venue: **www.dsn.org**

About the Workshop: **www.laas.fr/WDSN09** or contact the organizers at **dsn2009-nanocomputing[at]laas.fr**

Motivation and Theme

Unprecedented levels of information processing, novel architectural solutions and a new realm of applications promise to be reached thanks to the advances in semiconductor technologies for integrating extremely large numbers of transistors or processing elements into a chip. Towards this ends, two main tracks are being considered:

- **"More Moore"**: this track is pushing further the long standing Moore's Law-based trend in chip development that aims at reducing the dimensions of silicon microelectronics.
- **"Beyond Moore"**: this track features atomic assemblies of nanoscale technologies; these include nanowires, carbon nanotubes or organic molecules, etc., and extend also to quantum computing, optical computing and micro/nanofluidics.

Due to the differences in relative advances and current industrial concerns attached to each track, the Workshop will emphasize the top-down track for which such an evolution raises serious challenges both from the Dependability and Security viewpoints. Nevertheless, considerations attached to the emerging nanoscale technologies are also part of the scope of the Workshop.

In both cases, it is expected that circuits will be impaired by significant variations affecting process parameters and thus will become a nightmare to reliability engineers for reaching an acceptable manufacturing yield at viable cost. The dramatic reduction of digital devices is accompanied by a decrease in power supply and threshold levels which in turn results in lower noise immunity and greater sensitivity to particles. Moreover, additional instabilities may affect circuit parameters in operation, e.g., NBTI in CMOS devices.

Examples of vulnerabilities and malicious threats related to hardware chips are information leakages attached to side channels attacks or differential fault analysis based on applying environmental disturbances or even fault injection. Potential vulnerabilities are also related to the observability and controllability facilities provided by scan-based testing devices.

Scope and Objectives

The Workshop aims at addressing these impairments and threats as well as distinguishing novel design approaches and operation paradigms that are to be enforced and/or favored to keep achieving dependable and secure computing. Three main goals are identified for the Workshop:

- **Review** the state-of-knowledge about the main threats in nanocomputing technologies: manufacturing defects, accidental faults, malicious attacks.
- **Report** on existing solutions and **propose** new design options for mitigating faults and implementing secure and resilient computing devices and systems.
- **Forecast** the risks associated to emerging technologies and **foster** new trends for cooperative work at technological and system levels.

Topics of Interest, Submission and Information

The Workshop is open to researchers, designers and users involved with or interested in dependability and security of hardware technologies. Submissions from industry and/or academia on all topics related to dependable and secure nanocomputing are encouraged. 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 nano-scale technologies, on-line adaptive and reconfigurable nanoarchitectures, design techniques for developing resilient nanosystems, fault-tolerant architectures specific to nanoscale circuits, 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. Submissions 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 not exceed six pages (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 will be fully refereed by three PC members. Submissions must be made electronically (in PDF format), preferably via the Workshop Webpage (**www.laas.fr/WDSN09**).

Authors of accepted papers must guarantee that their paper will be presented at the Workshop. Accepted papers will be published in the supplement volume of the DSN 2009 proceedings.

About IOLTS and DSN: In 2009, IOLTS and DSN will be held back to back in geographically close sites in Lisbon area (IOLTS finishing two days before WDSN09). IOLTS and WDSN cover technically close, though complementary, domains. This provides a unique opportunity to interested participants attending both events to benefit from a comprehensive coverage of topics related to dependable and secure computing and critical applications, spanning technology level, gate-level and RTL level issues, analysis and assessment techniques as well as architectures encompassing also software and system levels. For more information about IOLTS, see: www-tima.imag.fr/conferences/iolts/iolts09

Update: March 3, 2009