J Electron Test (2016) 32:241–242
DOI 10.1007/s10836-016-5596-y

Editorial

Vishwani D. Agrawal[1]

Received: 8 May 2016 / Accepted: 8 May 2016 / Published online: 14 May 2016
© Springer Science+Business Media New York 2016

Nine papers and four *Letters* constitute this issue. The topics discussed are boundary scan, automatic test equipment (ATE), fault tolerance, security, and RF measurements. The papers appearing as first, third, fifth and sixth are derived from the *Sixteenth IEEE Latin American Test Symposium* (LATS), Puerto Vallarta, Mexico, March 25–27, 2015.

The first paper gives the design of reconfigurable scan hardware for board test. Here, the boundary scan implemented on FPGA provides test time reduction. Authors are Aleksejev and Devadze of Tallinn University of Technology, Tallinn, Estonia, and Jutman and Shibin of Testonica Lab OÜ, Tallinn, Estonia.

Next, a paper on automatic test equipment (ATE) examines effects of power supply fluctuation on the test result. When the ATE supply waveform differs from that of the normal functional supply a faulty device can pass the test or a good device can fail. The authors propose a dynamic power integrity control technique to match the ATE power supply with that in user's environment. The paper is contributed by Ishida and Kusaka from Advantest Corporation, Gunma, Japan, Nakura and Asada of University of Tokyo, Tokyo, Japan, and Komatsu of Tokyo Denki University, Tokyo, Japan.

Fault tolerance and reliability is the theme for the next four papers. First, a paper proposes a method to compensate for the effect of negative bias temperature instability (NBTI) on the critical path delay. Carefully derived stimuli help selected pMOS transistors recover from deterioration caused by NBTI. This paper is authored by Jenihhin, Tihhomirov, Kostin, Raik and Ubar from Tallinn University, Tallinn, Estonia, Squillero, Gaudesi, Reorda from Politecnico di Torino, Torino, Italy, and Copetti, Vargas, Poehls and Medeiros from Catholic University – PUCRS, Porto Alegre, Brazil.

The second paper in the fault tolerance group introduces the concept of statistical vulnerability window (SVW) to analyze the observable effects of single event transients. Contributors are Raji form Shiraz University, Shiraz, Iran and Ghavami from Shahid Bahonar University of Kerman, Kerman, Iran.

Continuing with the theme of fault tolerance, the next paper uses three-dimensional analysis of FinFET devices in a static memory cell. The result allows determination of the fin height with a proper tradeoff between soft error robustness and noise stability. Authors of this paper are Villacorta from Polytechnic University of Aguascalientes, Aguascalientes, Mexico, Segura from University of Balearic Islands, Mallorca, Spain, and Champac from National Institute for Astrophysics, Optics and Electronics (INAOE), Tonantzintla, Puebla, Mexico.

The final paper in the fault tolerance group is authored by Copetti, Medeiros, Poehls and Vargas from Catholic University – PUCRS, Porto Alegre, Brazil. They place an on-chip circuit that monitors the NBTI-related aging effects and then varies the supply voltage for compensation, thus extending the lifetime of the chip.

Next, three papers discuss hardware security. The first of these is authored by Zamanzadeh and Jahanian from Shahid Beheshti University G.C., Tehran, Iran. The paper gives a method to detect any unwanted attempt at changing the function implemented on an FPGA. A security plug-in tool automatically inserts a "security path" in the FPGA to detect and obfuscate such attempts.

✉ Vishwani D. Agrawal
vagrawal@eng.auburn.edu

[1] Department of ECE, Auburn University, 200 Broun Hall, Auburn, AL 36849, USA

A hardware security attack refers to either a theft of data being processed, or some maliciously induced faulty or harmful operation. When an attacker uses nonfunctional or physical information about the hardware we refer to it as side channel attack (SCA). The paper, contributed by Saeedi, Hossain and Kong from Macquarie University, Sydney, Australia, employs machine learning techniques to analyze the side channel information.

Machine learning is also used in the next paper to facilitate reverse engineering for detecting Trojan hardware in a circuit. The authors are Nasr and Abdulmageed from Al-Azhar University, Cairo, Egypt.

There has been a growing interest in hardware Trojans from electronics community. Readers not familiar with the subject may refer to the Editorial and two lead articles that appeared in *JETTA*, volume 30, number 1, February 2014.

Lately, we have seen an increase in the submission of manuscripts in the *JETTA Letters* category. These are brief (six pages or shorter) communications that convey useful ideas, analyses or results. They have a rapid review cycle and are examined by the editorial board for quick decisions. We have four *Letters* appearing in this issue.

In the first *Letter*, Streitwieser from ams AG, Unterpremstaetten, Austria presents an adaptive ATE procedure to reduce the test time with estimated small defect level.

The second *Letter*, contributed by Jothin of KGiSL Institute of Technology, Coimbatore, India and Vasanthanayaki of Government College of Technology, Coimbatore, India, presents an adder design in which performance is enhanced by allowing errors that are cosidered tolerable for the targeted application.

The third *Letter* gives analysis and design of a 65 nm CMOS SRAM cell with increased tolerance for single event upset (SEU). Authors are Q. Chen from Xi'an Microelectronics Technology Institute, Xi'an, Shaanxi, China, Wang, L. Chen, Zhao, Liu, M. Chen and X. Li from University of Saskatchewan, Saskatoon, SK, Canada, and L. Li from Dalhousie University, Halifax, NS, Canada.

The fourth *Letter* is contributed by Zhu, Mo, Xu, Shang, Wang, Huang and Yu from Zhejiang University, Hangzhou, China. They give a design for a built-in capacitance-to-frequency converter for on-chip capacitance measurement with high accuracy.