Editorial

Vishwani D. Agrawal

Received: 27 January 2014 / Accepted: 27 January 2014 / Published online: 5 February 2014
© Springer Science+Business Media New York 2014

The term “Trojan” is derived from the story of the wooden horse used by the ancient Greeks to trick defenders of Troy into taking concealed warriors into their city. The legendary 10-year war took place in the Bronze Age (13th or 12th century BC), beginning with the abduction of Helen from Sparta by prince Paris of Troy and ending in destruction of Troy.

The two lead articles in this issue tell a story of reappearance of Trojan threat in the 21st century AD. These are contributed by Guin and Tehranipoor of University of Connecticut, Storrs, Connecticut, USA and DiMase of Honeywell Inc., Morristown, New Jersey, USA. In the interest of promoting this area of growing importance, we are offering *free access* to the introductory article, “Counterfeit Integrated Circuits: Detection, Avoidance and the Challenges Ahead.” Thus, any reader can download the article from the website of *JETTA* free of cost at least for 2 years.

Due to globalization of the semiconductor design and fabrication processes, integrated circuits are increasingly vulnerable to malicious activities and alterations. These vulnerabilities raise serious concerns regarding possible threats to military systems, financial infrastructures, transportation security and medical devices. An adversary can introduce a Trojan designed to disable or destroy a system at some future time or the Trojan may leak confidential information and secret keys covertly to the adversary. Counterfeit electronic devices can be equally disastrous since they may not meet the original component specification.

Looking into today’s supply chain, there are numerous vulnerabilities in every step of the process that threaten the security of the electronics circuits and systems. Tampering

with the original RTL, netlist, or layout, or IP piracy are major issues during design process. An untrusted GDSII (Graphic Database System-II) developer, foundry, or assembly can tamper with the design, overproduce the ICs, or ship defective parts to the market. Similar vulnerabilities exist in system validations, distribution, and the end-of-life of the electronics systems. Each of these vulnerabilities poses unique challenges to test and reliability engineers.

Counterfeiting and piracy are longstanding problems growing in scope and magnitude. They are of great concern to government and industry. As the complexity of the electronic systems, along with the ICs used in them, increased significantly over the past few decades, they are assembled (fabricated) globally to reduce the production cost. For example, large foundries can offer lower prices to design houses, located in different countries. This globalization leads to an illicit market willing to undercut the competition with counterfeit parts. If these parts end up in critical applications like defense, aerospace, or medical systems, the results could be catastrophic. See the recent article by J. Villasenor and M. Tehranipoor, “Chop-Shop Electronics,” *IEEE Spectrum*, October 2013, pp. 40–45. No one knows exactly how big this market is because most of the counterfeit chips go undetected and some may simply be considered quality problem. Today’s test and detection mechanisms have major deficiencies.

This issue contains ten articles, nine papers and one *Letter*. The topics covered are security and trust (first two papers), verification, 3D-stacked IC, memory testing, MEMS testing, RF testing, and non-classical faults. The paper on MEMS testing is derived from the program of the *IEEE Latin-American Test Workshop* (LATW) of 2012 and three other papers, those appearing as second, fourth and seventh, are from the *IEEE North Atlantic Test Workshop* (NATW) of 2013. Guest Editor are Leticia Maria Bolzani Pohls for LATW and Tian Xia for NATW.

V. D. Agrawal (✉)
Department of ECE, Auburn University, 200 Broun Hall, Auburn,
AL 36849, USA
e-mail: vagrawal@eng.auburn.edu

The first article attempts, for the first time, to present various types of counterfeits, the defects associated with each type, and their detection methods. The article also presents the unique challenges to implementing these test methods and to their effectiveness in detecting different types of counterfeit ICs. It presents anti-counterfeit measures to prevent widespread counterfeiting, and describes the effectiveness and limitations of these techniques. This article should provide researchers in the academia and practitioners in industry a much better understanding of the magnitude of the problem, the shortcomings, and the challenges ahead in addressing this very difficult problem. *Readers can access this article free of cost.*

The second article elaborates on testing aspects of the security issues mentioned above.

In the third paper the authors, Favalli from University of Ferrara and Dalpasso from University of Padova in Italy, use Boolean satisfiability (SAT) to solve verification and test problems of switch-level circuits. Specific applications discussed are equivalence checking and test generation for bridging faults.

Next paper presents a method for improving the yield of wafer-to-wafer bonding in 3-D stacked devices. The authors, Zhang and Agrawal of Auburn University, Alabama, USA, propose using a sector symmetry in chip placement such that sectors can be cut and interchangeably used for stacking. Although the proposed physical design loses some chip sites, the loss is more than made up in the yield gain.

The authors of the next paper are Murali Krishna and Sailaja from the University College of Engineering at Kakinada, Andhra Pradesh, India. To reduce power dissipation in the address generator of memory BIST, a linear feedback shift register (LFSR) is split into two sections, each controlled by separate specially designed clocks. They estimate an amazing 90 % reduction in the power consumption of the address generator.

Next, an electrical test for accelerometer MEMS is implemented using a Wheatstone bridge set up in a paper by Rekik

from University of Sfax, Tunisia, and Azaïs, Mailly and Nouet from LIRMM, France.

RF power sensor is the topic of a paper by Feng and Onabajo of Northeastern University, Boston, Massachusetts, USA. The sensor measures temperature difference using a two-stage CMOS amplifier, whose low power version in 180 nm technology consumes 1.125 mW and provides a peak sensitivity of 185.7 mV/°C over an 8 °C dynamic range.

The next paper examines clock faults in a synchronous circuit. The fault model assumes a change in the duty cycle. The analysis shows that such faults can potentially result in short-path problems normally caused by the violation of the minimum path delay requirement. Authors are Rossi, Omaña, Cazeaux and Metra of University of Bologna, Italy and Mak from GlobalFoundries, Sunnyvale, California, USA.

Power supply noise is studied next. Authors, Kandiyala Rao, Robucci and Patel from University of Maryland Baltimore County in USA, describe a system of analysis that considers both IR and Ldi/dt effects. Circuit partitioning and a convolution-based analysis make the system significantly faster than a full-chip SPICE analysis. Effects of power supply noise on path delays are demonstrated.

Appearing at the end, a *JETTA Letter* is contributed by Ren and Chen of University of Saskatchewan, Canada, He, Shi and Guo of China Institute of Atomic Energy, Beijing, China, Wen and Wong of Cisco Systems, Inc., San Jose, California, USA, van Vonno of Intersil Inc., Milpitas, California, USA, and Bhuvu of Vanderbilt University, Nashville, Tennessee, USA. They discuss single-event transient (SET) measurements from heavy ion, proton, and pulsed laser experiments.

To begin 2014 and volume 30 of *JETTA*, we are adding Hans Manhaeve to the editorial board. His picture and biography appear in this issue. A list of reviewers who conducted reviews for *JETTA* in 2013 appears in this issue as well. We acknowledge their contribution to the journal and thank them for devoting their expertise and time to the service of the profession.