2012 IEEE 18th International On-Line Testing Symposium

(IOLTS 2012)

Sitges, Spain
27 – 29 June 2012

IEEE Catalog Number: CFP12OLT-PRT
ISBN: 978-1-4673-2082-5

Technical Papers

Session	Session 1 – SEU Tolerance
Moderator	**R. Velazco**, *TIMA*

Session	Session 2 – Reconfigurable Logic
Moderator	**I. Koren**, *U Mass Amherst*

Session	Special Session 1 – Embedded Tutorial: Online Security Monitoring for ICs
Presenters	**Miron Abramovici**, *Tiger's Lair*

Abstract

Security for ICs has become a very important problem for devices used in critical infrastructure and military applications. Trojan horses and tampering attacks pose tremendous risks. Existing security techniques cannot guarantee pre-deployment Trojan detection, and tampering attacks also occur post-deployment. Therefore on-line security checking is necessary.

Our approach is based on distributed reconfigurable instrumentation where the instruments monitor the behavior of the IC to detect tampering attacks and to provide countermeasures when attacks are detected. The instruments are continuously reconfigured so they can be time-shared for many different security checks. Our approach is able to detect an attack such as Stuxnet (the most powerful malware ever written) and to prevent its destructive effects. The instruments are also periodically configured for self-testing to assure that the security hardware has not been tampered.

Session	Session 3 – Radiation Experiments and Analysis
Moderator	**O. Heron**, *CEA List*

Session	Session 4 – Circuit Degradation
Moderator	**J. Figueras**, *UPC*

Session	Special Session 2 – Panel: Cross Layer Reliability - Challenges and Standards Requirements
Organizers	**Michael Nicolaidis**, *TIMA* **Shi-Jie Wen**, *CISCO*
Panelists	**Magdy Abadir**, *Freescale* **Dan Alexandrescu**, *iRoC Technologies* **Adrian Evans**, *CISCO* **Eishi Ibe**, *Hitachi* **Gabriele Saucier**, *Design & Reuse* **Yervan Zorian**, *Synopsys*

Summary
In modern ICs, Design for Reliability is mandatory for a fast increasing number of application domains.Teams designing complex SoCs reuse IP cores coming from multiple sources. Similarly, teams designing complex electronics systems use chips coming from multiple providers. Evaluating the reliability of complex systems comprising numerous components is extremely difficult and implies component-reliability reuse (chip and IP core providers prequalify the reliability of their products and supply the related information to the users), and dedicated tools for evaluating the reliability of complex systems from the reliability of their components.

This panel brings together recognized experts in Design for Reliability to discuss: the challenges they face in modelling the reliability of complex systems; their vision of the tools and techniques that are required in order to solve these challenges; requirements for new standards (e.g. a language for cross layer reliability information interchange); and other related issues.

Summary

Hard real-time systems are characterized by their critical timing requirements in forms of deadlines. Failure to meet such deadlines results in a system failure. Examples of such systems include anti-lock brakes and aircraft control systems.As the technology continues scaling, several challenging roadblocks emerge; e.g., variability, transient faults, accelerated degradation and ageing (e.g. due to Negative Bias Temperature Instability), power induced problems, etc. Consequently, the design of real-time systems becomes extremely complicated. To guarantee the severe reliability and dependability requirements of such systems, designers have to address these issues at all design levels, from software to hardware and system integration.

The panel aims at gathering opinions from researchers working in various fields of system design and integration (from software to hardware) on how to address emerging questions about reliability and dependability of future hard real-time systems. E.g. do we need to address issues at hardware level (technology, circuit/IP, system), at software

level or through hardware/software co-design techniques? Do we need to revise the existing design methodologies and used models? Do we need to enhance existing fault tolerance schemes or do we really need breakthroughs?, etc.

Session	Session 7 – Posters

Session	Session 8 – Secure Hardware
Moderator	**G. Di Natale**, *LIRMM*

Session	Special Session 5 – Future Reliability Solutions: New Applications and New Devices
Organizer	**D. Gizopoulos**, *U Athens*
Moderator	**A. Chatterjee**, *Georgia Tech*

Session	Session 9 – Soft Errors Analysis and Tolerance
Date/Time	Friday, 29 June 2012 / 11:40 – 13:00
Moderator	**I. Levin**, *Tel Aviv U*