

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, <i>TIMA</i>

Error Detection and Correction of Single Event Upset (SEU) Tolerant Latch''''''3

N. Julai, A. Yakovlev and A. Bystrov

SETTOFF : A Fault Tolerant Flip-Flop for Building Cost-efficient Reliable Systems''''''''''9

Y. Lin and M. Zwolinski

SEU Tolerant Robust Memory Cell Design''''''''35

Md. Shayan, V. Singh, A. D. Singh and M. Fujita

Soft-Errors Resilient Logic Optimization for Low Power''''''3;

S. Pandey and K. Brink

Session	Session 2 – Reconfigurable Logic
Moderator	I. Koren, <i>U Mass Amherst</i>

SEU-X: A SEU Un-eXcitability Prover for SRAM-FPGAs''''''47

C. Bernardeschi, L. Cassano and A. Domenici

Analyzing and Alleviating the Impact of Errors on an SRAM-Based FPGA Cluster''''''53

A. B. Dhia, L. Naviner and P. Matherat

Transparent Structural Online Test for Reconfigurable Systems''''59

Md. S. Abdelfattah, L. Bauer, C. Braun, M. E. Imhof, M. A. Kochte, H. Zhang, J. Henkel and H-J. Wunderlich

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

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

A Real-Case Application of a Synergetic Design-Flow-Oriented SER Analysis''''65

M. Vilchis, R. Venkatraman, E. Costenaro and D. Alexandrescu

Fault-Based Reliable Design-On-Upper-Bound of Electronic Systems for Terrestrial Radiation Including''''6;
Muons, Electrons, Protons and Low Energy Neutrons

E. Ibe, T. Toba, K. Shimbo and H. Taniguchi

Neutron Radiation Test of Graphic Processing Units''''77

P. Rech, C. Aguiar, R. Ferreira, C. Frost and L. Carro

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

The Influence of Clock-Gating on NBTI-Induced Delay Degradation''''83

J. Pachito, C. V. Martins, J. Semião, M. Santos, I. C. Teixeira and J. P. Teixeira

Relation Between HCI-Induced Performance Degradation and Applications ''''89
in a RISC Processor

C. Bertolini, O. Heron, N. Ventroux and F. Marc

Do More Camera Pixels Result in a Better Picture?''''95

G. H. Chapman, I. Koren and Z. Koren

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.

Session	Session 5 – Memories and 3D Integration
Moderator	S. Hamdioui, TU Delft

Low Power Embedded DRAM Caches using BCH Code Partitioning; 9;

P. Reviriego, A. Sánchez-Macian and J. A. Maestro

On the Functional Test of L2 Caches; 6

M. Riga, E. Sanchez and M. S. Reorda

Through-Silicon-Via Built-In Self-Repair for Aggressive 3D Integration; 3

M. Nicolaidis, V. Pasca and L. Anghel

Session	Special Session 3 – Variability and Bugs: How to find them?
Organizer	Puneet Gupta, UCLA
Moderator	J. Abella, BSC

Measuring and Monitoring Variability P IC

P. Gupta

Correlating Models and Silicon in the Presence of Variability P IC

V. Chandra

Effective Post-Silicon Validation P IC

S. Mitra

Session	Session 6 – Miscellaneous
Moderator	N. Mentens, KU Leuven

Test Access Mechanism for Chips with Spare Identical Cores; 9

O. Sinanoglu

RIIF - Reliability Information Interchange Format; 325

A. Evans, M. Nicolaidis, S-J. Wen, D. Alexandrescu and E. Costenaro

On Line Monitoring of RF Power Amplifiers with Embedded Temperature Sensors; 32;

J. Altet, D. Mateo and D. Gómez

Session	Special Session 4 – Panel: Reliability of Hard Real-time Systems in 32nm and Beyond: Who Will Solve the Challenges?
Organizer	Said Hamdioui, TU Delft

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
----------------	----------------------------

A Fault Attack Robust TRNG''''336

E. Böhl and M. Ihle

Architectural Vulnerability Aware Checkpoint Placement in a Multicore Processor''''33:

A. Lotfi, A. Bayat and S. Safari

Evaluation of Test Algorithms Stress Effect on SRAMs under Neutron Radiation''''343

G. Tsiligiannis, L. Dillo, A. Bosio, P. Girard, A. Todri, A. Virazel, A. D. Touboul, F. Wrobel and F. Saigné

Event-Driven On-Line Co-Simulation with Fault Diagnostic''''345

M. Baklashov

Fault Coverage of a Timing and Control Flow Checker for Hard Real-Time Systems''''349

J. Wolf, B. Fechner and T. Ungerer

Fault Missing Rate Analysis of the Arithmetic Residue Codes based Fault-Tolerant FIR Filter Design''''352

Z. Gao, W. Yang, X. Chen, M. Zhao and J. Wang

Functional Level Embedded Self Testing for Walsh Transform based Adaptive Hardware''''356

A. Burg and O. Keren

Gatewaying IEEE 1149.1 and IEEE 1149.7 Test Access Ports''''358

F. R. Fernandes, R. J. S. Machado, J. M. Ferreira and M. G. Gericota

Neutron-Induced Soft Error Rate Estimation for SRAM using PHITS''''35:

S. Yoshimoto, T. Amashita, M. Yoshimura, Y. Matsunaga, H. Yasuura, S. Izumi, H. Kawaguchi and M. Yoshimoto

Pilot Symbol Driven Monitoring of Electrical Degradation in RF Transmitter Systems using Model Anomaly''''364 Diagnosis

S. Deyati, A. Banerjee and A. Chatterjee

Reliable and Secure Memories based on Algebraic Manipulation Correction Codes''''368

Z. Wang and M. Karpovsky

Session	Session 8 – Secure Hardware
----------------	------------------------------------

Moderator	G. Di Natale, LIRMM
------------------	----------------------------

Cross-Level Protection of Circuits Against Faults and Malicious Attacks''''372

V. Tomashevich, S. Srinivasan, F. Foerg and I. Polian

Punctured Karpovsky-Taubin Binary Robust Error Detecting Codes for Cryptographic Devices''''378

Y. Neumeier and O. Keren

Stream Cipher Hash based Execution Monitoring (SCHEM) Framework for Intrusion Detection on ''''384 Embedded Processors

A. Chaudhari and J. Abraham

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

Algorithmic Techniques for Robust Applications''''38:

R. Kumar

Analysis of FinFET Technology on Memories''''38;

E. Amat, A. Asenov, R. Canal, B. Cheng, J-Ll. Cruz, Z. Jakšić, M. Miranda, A. Rubio and P. Zuber

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

An Efficient Probability Framework for Error Propagation and Correlation Estimation''''392

L. Chen and M. B. Tahoori

Logic Masking for SET Mitigation using Approximate Logic Circuits''''398

A. Sánchez-Clemente, L. Entrena, M. García-Valderas and C. López-Ongil

Towards Optimized Functional Evaluation of SEE-Induced Failures in Complex Designs''''3: 4

D. Alexandrescu and E. Costenaro

SEU Sensitivity of Robust Communication Protocols''''3: :

C. Lopez-Ongil, M. Portela-Garcia, M. Garcia-Valderas, A. Vaskova, L. Entrena,

J. Rivas-Ábalo, A. Martín-Ortega, J. Martínez-Oter, S. Rodríguez-Bustabad and I. Arruego