

# **2025 IEEE 31st International Symposium on On-Line Testing and Robust System Design (IOLTS 2025)**

**Ischia, Italy  
7-9 July 2025**



**IEEE Catalog Number: CFP25OLT-POD  
ISBN: 979-8-3315-3335-9**

**Copyright © 2025 by the Institute of Electrical and Electronics Engineers, Inc.  
All Rights Reserved**

*Copyright and Reprint Permissions:* Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

***\*\*\* This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP25OLT-POD
ISBN (Print-On-Demand):	979-8-3315-3335-9
ISBN (Online):	979-8-3315-3334-2
ISSN:	1942-9398

**Additional Copies of This Publication Are Available From:**

Curran Associates, Inc  
57 Morehouse Lane  
Red Hook, NY 12571 USA  
Phone: (845) 758-0400  
Fax: (845) 758-2633  
E-mail: [curran@proceedings.com](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

## Table of Contents

### **A Digital SRAM Modeling for Cell-Aware Testing and Test Algorithms Evaluation...1**

*Dorian Ronga, Xhesila Xhafa (Lirmm), Eric Faehn (Stm), Patrick Girard (Lirmm), Thibault Vayssade (Univ. Montpellier, Cnrs, Lirmm), Arnaud Virazel (Lirmm)*

### **A Fuzzy Logic-Based System for Detecting Trustable Physical Unclonable Functions...6**

*Mohammad Reza Heidari Iman (Tima Lab), Sergio Vinagrero (Inl), Elena Ioana Vatajelu (Tima Laboratory), Giorgio Di Natale (Tima)*

### **A Runtime Efficient Graph-Based Cell-Aware Model Generation for Structural SRAM Testing...10**

*Gianmarco Mongelli, Xhesila Xhafa (Lirmm), Eric Faehn, Dylan Robins (St), Patrick Girard, Arnaud Virazel (Lirmm)*

### **AI-based Classification of Adversarial Attacks vs. Hardware Fault Corruptions in the Split Computing context...16**

*Giuseppe Esposito, Enrico Magliano, Nicola Scarano, Tamer Ahmed Eltaras, Juan Guerrero, Stefano Di Carlo (Politecnico Di Torino), Marco Levorato (University Of California Irvine), Luca Mannella, Josie Rodriguez Condia, Annachiara Ruospo, Alessandro Savino, Matteo Sonza Reorda (Politecnico Di Torino)*

### **Accurate Analysis of Silent Data Corruptions in Programmable AI Accelerator Microarchitectures...23**

*Odysseas Chatzopoulos (University Of Athens), Maria Trakosa (University Of Athens), Dimitris Gizopoulos (University Of Athens)*

### **Adaptive Testing of Compute-in-Memory Based CNNs Using Probabilistic Test Acceptance Limits...27**

*Anurup Saha (Georgia Tech), Kwondo Ma (Rebellions), Chandramouli Amarnath (Google), Moinuddin Qureshi, Abhijit Chatterjee (Georgia Institute Of Technology)*

### **Anomalous IoT Behavior Detection Based on SARIMA Reference Waveform...34**

*Ryusei Eda (Department Of Computer Science And Communications Engineering, Waseda University), Nozomu Togawa (Department Of Computer Science And Communications Engineering, Waseda University)*

### **Autoencoder-Based Detection of Physical-Layer Anomalies in Automotive CAN Networks...39**

*Antonio Battaglia (University Of Messina, Italy), Nicasio Canino (University Of Pisa, Italy), Pierpaolo Dini (University Of Pisa, Italy), Giovanni Lombardo (University Of Messina, Italy), Francesco Longo (University Of Messina, Italy), And Daniele Rossi (University Of Pisa, Italy)*

### **Bloom Filters for Soft Error Detection: Neutron and Fault Injection Validation...43**

*Elijah Cishugi (University Of Twente), Tijmen T. Smit (University Of Twente), Bruno Endres Forlin (University Of Twente), Cazzaniga Carlo (Rutherford Appleton Laboratory-Isis), Kuan-*

*Hsun Chen (University Of Twente), Marco Ottavi (University Of Twente, University Of Rome Tor Vergata)*

**Body Bias Injection on the FLASH Memory Accelerator of a 32-bit Microcontroller...50**

*Ziling Liao, Florent Bruguier, Philippe Maurine,*

**Building Resilient AI: Strengthening Data, Security, and Robustness in Neural Networks...57**

*Deepak Ravikumar (Purdue University), Jimmy Ian Gammell (Purdue University), Kaushik Roy (Purdue University)*

**CANDoSA: A Hardware Performance Counter-Based Intrusion Detection System for DoS Attacks on Automotive CAN bus...61**

*Franco Oberti (Dumarey), Stefano Di Carlo, Alessandro Savino (Politecnico Di Torino)*

**Comparative Analysis of TID Effects in a 65 nm FD-SOI Process under Gamma-Ray and Alpha-Ray Irradiation...66**

*Hikaru Nakamoto, Taiki Ozawa, Ryuichi Nakajima, Haruto Sugisaki, Keita Yoshida (Kyoto Institute Of Technology), Jun Furuta (Okayama Prefectural University), Kazutoshi Kobayashi (Kyoto Institute Of Technology)*

**Detecting Hardware Trojans in Microprocessors via Hardware Error Correction Code-based Modules...71**

*Alessandro Palumbo (Centralesupélec, Inria, Cnrs, Irisa, France), Ruben Salvador (Centralesupélec, Inria, Cnrs, Irisa, France)*

**Dose Effects and Mitigation in 28nm FD-SOI Advanced Interface Bus Chiplet Interconnect...78**

*Antoine Rouget (Stmicroelectronics/Cea-List/Uga), Fady Abouzeid (Stmicroelectronics), Adrian Evans (Cea-List), Victor Malherbe (Stmicroelectronics), Aleksandra Chumakova (Esrf), Philippe Roche (Stmicroelectronics), Fabien Clermidy (Cea-Leti)*

**Evaluating ECC for Cache Reliability Under Multi-Bit Upsets: A Design Space Exploration...83**

*Foteini Kotsimpou, George Papadimitriou, Dimitris Gizopoulos (University Of Athens)*

**Exploiting Reconfigurable Intelligent Surfaces to Achieve Multi-Receiver Physical Layer Security...91**

*Simone Marrocco (University Of Trento, Italy), Paolo Casari (University Of Trento, Italy), Michele Segata (University Of Trento, Italy)*

**Fault Diagnosis in ReCAM Arrays...95**

*Haneen G. Hezayyin (Karlsruhe Institute Of Technology), Mahta Mayahinia (Kit University), Mehdi Tahoori (Karlsruhe Institute Of Technology)*

**Fault Tolerance in Quantized and Pruned Convolutional Neural Networks...102**

*Wilfred Guillemé (Univ. Rennes, Inria, Irisa), Angeliki Kritikakou (Univ Rennes, Inria, Irisa), Youri Helen (Dga Mi), Cedric Killian (Université Jean Monnet Saint-Etienne), Daniel Chillet (University Of Rennes 1, Irisa/Inria)*

**GPD: Predictive control flow error detection leveraging data flow error detection methods...109**

*Raghunandana K, Yogesh Prasad R (Indian Space Research Organisation), Matteo Sonza Reorda (Politecnico Di Torino), Virendra Singh (Indian Institute Of Technology Bombay)*

**Human-Artificial Intelligent Threat Modelling in the Automotive Domain...114**

*Giampaolo Bella (University Of Catania, Italy), Gianpietro Castiglione (University Of Catania, Italy), Sergio Esposito (University Of Catania, Italy), Mirko Mangano (University Of Catania, Italy), Giacomo Pampallona (University Of Catania, Italy), Mario Raciti (Imt School For Advanced Studies, Italy), Salvatore Riccobene (University Of Catania, Italy), Daniele Santamaria (University Of Catania, Italy)*

**Improving Error Correction with Weak-Bit Information in Resistive Memories...118**

*Valentin Gherman (Cea List), Ishai Naveh (Weebit Nano Ltd), Bastien Giraud (Cea List), Antoine Hebert (Cea List), Gabriel Molas, Giuseppe Piccolboni, Zeev Freidin, Amir Regev, Matan Guttman, Ilan Sever (Weebit Nano Ltd)*

**Leveraging Image-based Transformations to Mitigate Adversarial Attacks in AI-based Safety-critical Systems...125**

*Martí Caro (Barcelona Supercomputing Center (Bsc-Cns)), Axel Brando (Barcelona Supercomputing Center (Bsc)), Jaume Abella (Barcelona Supercomputing Center (Bsc-Cns))*

**Leveraging Open-Source Bitstream Documentation for FPGA Soft-Error Robustness Analysis...130**

*Christian Fibich, Leonardo Lovric (University Of Applied Sciences Technikum Wien)*

**Lightweight Concurrent Out-of-Distribution Detection in Hyperdimensional Computing Hardware...137**

*Mahboobe Sadeghipourrudsari, Vincent Meyers (Karlsruher Institut Für Technologie (Kit)), Mehdi Tahoori (Karlsruhe Institute Of Technology)*

**Machine Learning-Based Parametric Fault Detection in Analog and Mixed-Signal Circuits...144**

*Jules Kouamo, Emmanuel Simeu (Tima Laboratory), Michele Portolan (Siemens)*

**NAPER: Fault Protection for Real-Time Resource-Constrained Deep Neural Networks...149**

*Rian Adam Rajagede, Muhammad Husni Santriaji (University Of Central Florida), Muhammad Arya Fikriansyah, Hilal Hudan Nuha (Telkom University), Yanjie Fu (Arizona State University), Yan Solihin (University Of Central Florida)*

**NAVIGator: Exploring the Voltage Limits of AMD NAVI GPUs for Energy Efficient Computing...157**

*Maria Trakosa, Odysseas Chatzopoulos, George Papadimitriou, Dimitris Gizopoulos (University Of Athens)*

**Neuromorphic Computing for Embodied Intelligence in Autonomous Systems: Current Trends, Challenges, and Future Directions...165**

*Alberto Marchisio And Muhammad Shafique*

**Next-Generation Quantum Neural Networks: Enhancing Efficiency, Security, and Privacy...169**

*Nouhaila Innan, Muhammad Kashif, Alberto Marchisio, Mohamed Bennai, Muhammad Shafique*

**On Post-Quantum Attribute-based Encryption for Automotive Over-the-Air Software Updates...173**

*Gianluca Dini, Salvatore Lombardi, Tommaso Antonini (University Of Pisa)*

**On the validity of SEE simulation for rad-hard analog ASICs...177**

*Valentin Gutierrez, Gildas Leger (Imse-Cnm), Antonio Gines (Imse-Cnm (Csic, Universidad De Sevilla)), Carlos Dominguez (Ommatidia Lidar), Eduardo Peralias (Instituto De Microelectronica De Sevilla (Imse-Cnm))*

**On-Line Test of Fully Integrated Voltage Regulators for High Performance Microprocessors of Autonomous Systems...182**

*Martin Eugenio Omana (University Of Bologna), Alex Menghi (Hera Group), Alessandro Stefani (Zivan Srl), Enrico Vicini (Micron Technology), Cecilia Metra (University Of Bologna), Giuseppe Froio (Marvell Technology), Stefano Petrucci (Intel Corp.)*

**PLL Over-Clocking Through Repeated Fault Injections...189**

*Louis Dubois (Lirmm - Anssi - Dga), Philippe Maurine (Lirmm)*

**Quantum AI: Harnessing the Power of Quantum Computing for Scalable and Adaptive Learning...196**

*Samuel Yen-Chi Chen*

**ReDiM: An Efficient Strategy for Read Disturb Mitigation in RRAM-Based Accelerators...200**

*Jianan Wen (Ihp Gmbh–Leibniz Institute For High Performance Microelectronics), Andrea Baroni (Ihp Gmbh–Leibniz Institute For High Performance Microelectronics), Alberto Mistrioni (Ihp Gmbh–Leibniz Institute For High Performance Microelectronics), Eduardo Perez (Ihp Gmbh–Leibniz Institute For High Performance Microelectronics), Cristian Zambelli (Università Degli Studi Di Ferrara), Christian Wenger (Ihp Gmbh–Leibniz Institute For High Performance Microelectronics), Milos Krstic (Ihp Gmbh–Leibniz Institute For High Performance Microelectronics), Leticia Maria Bolzani Pöhls (Ihp Gmbh–Leibniz Institute For High Performance Microelectronics)*

**Real-Time Fault Analysis in RISC-V Processors: A Case Study Using the Internal State Monitor...207**

*Roua Boulifa, Giorgio Di Natale (Tima), Paolo Maistri (Cnrs)*

**SHIELD: PSO-Based Hardware Trojan DetectIon for Efficient and Low-Cost Defense...214**

*Mostafa Hosseini (University Of Zanjan), Ali Azarpeyvand, Mahdi Taheri (Tallinn University Of Technology), Tara Ghasempouri (Tallinn University Of Technology), Maksim Jenihhin (Tallinn University Of Technology)*

**STDP-Trained Spiking Neural Network Reliability Assessment Through Fault Injections...218**

*Zalfa Jouni (Sorbonne Université, Cnrs, Lip6, Paris, France), Haralampos Stratigopoulos (Sorbonne Université, Cnrs, Lip6, Paris, France)*

**Secure and Flexible WebAssembly Deployment Infrastructure for Automotive Cyber-Physical Systems...226**

*Tancredi Orlando (University Of Messina, Italy), Michele Arena (University Of Messina, Italy) , Luca Dagati (University Of Messina, Italy) , Giovanni Merlino (University Of Messina And Cini, Italy) , Francesco Longo (University Of Messina And Cini, Italy)*

**Securing the Control of Digital Beamforming...230**

*Love Barany (Lund University), William Eriksson (Beammwave Ab), Joel Åhlund (Advenica Ab), Daniel Bakic (Beammwave Ab), Erik Larsson (Lund University), Joakim Axmon, Markus Törmänen (Beammwave Ab)*

**Side-Channel Attack Detection using gem5 and Machine Learning: A Case Study on Fault-based Attacks in RISC-V...237**

*Mahreen Khan (Telecom Paris, Institut Polytechnique De Paris), Maria Mushtaq (Telecom Paris, Institut Polytechnique De Paris), Renaud Pacalet (Telecom Paris, Institut Polytechnique De Paris), Ludovic Apvrille (Telecom Paris, Institut Polytechnique De Paris)*

**Side-Channel Extraction of Dataflow AI Accelerator Hardware Parameters...242**

*Guillaume Lomet (Inria), Ruben Salvador (Inria), Brice Colombier (Université Jean Monnet Saint-Etienne), Vincent Grosso (Laboratoire Hubert Curien), Olivier Sentieys (Inria), Cedric Killian (Université Jean Monnet Saint-Etienne)*

**TIMA-PUF: Time Measurement based Arbiter PUF...249**

*Azzadine Thajte (Tima), Laurent Fesquet (Tima Laboratory), Giorgio Di Natale (Tima)*

**Towards Semantic Coherence: Understanding Cybersecurity and Digital Sovereignty in the Automotive Landscape...256**

*Elisa Sorrentino (Institute Of Informatics And Telematics Cnr, Italy), Anna Federica Spagnuolo (Institute Of Informatics And Telematics Cnr, Italy), Alessio Portaro (Institute Of Informatics And Telematics Cnr, Italy), Maria Taverniti (Institute Of Informatics And Telematics Cnr, Italy), Elena Cardillo (Institute Of Informatics And Telematics Cnr, Italy)*

**When Silicon Fails Silently: Characterizing Hardware-Induced Corruption in LLM Training...261**

*Jeffrey Jian Ma, Hengzhi Pei, Leonard Lausen, George Karypis*