5th IEEE Workshop On AI Hardware: Test, Reliability And Security (AI-TREATS)

Tallinn, Estonia, May 29-30, 2025

Program

Thursday, May 29, 2025	
16:30 – 16:45	**Opening Session** Annachiara Ruospo (Politecnico di Torino, IT) Theofilos Spyrou (Delft University of Technology, NL)
16:45 – 17:25	**Session 1: AI security and privacy** **Session Chair:** Theofilos Spyrou, Delft University of Technology, NL **R-CONV++: Uncovering Privacy Vulnerabilities through Analytical Gradient Inversion Attacks** Tamer Ahmed Eltaras[1], Qutaibah Malluhi[2], Alessandro Savino[1], Stefano Di Carlo[1] and Adnan Qayyum[3] [1] Politecnico di Torino, Italy [2] Qatar University, Qatar [3] Information Technology University, Pakistan **Input-Triggered Hardware Trojan Attack on Spiking Neural Networks** Spyridon Raptis[1], Paul Kling[1], Ioannis Kaskampas[1], Ihsen Alouani[2] and Haralampos-G. Stratigopoulos[1] [1] Sorbonne Université, CNRS, LIP6, France [2] CSIT, Queen's University Belfast, UK
17:30 – 18:30	**Anniversary Panel** **"AI-TREATS 5th anniversary panel: Lessons learned after nearly one decade of research"** **Moderator:** Alberto Bosio (Ecole Centrale De Lyon, France) **Panelists:** ● Elena-Ioana Vatajelu (TIMA - INPG, France) ● Haralampos Stratigopoulos (Sorbonne Université, CNRS, LIP6, FR) ● Maksim Jenihhin (TalTech - Tallinn University of Technology, Estonia) ● Said Hamdioui (Delft University of Technology, The Netherlands)

18:30 – 19:30	**Welcome Reception**
Friday, May 30, 2025	
09:00 – 10:00	**Keynote** **"Is AI Becoming a Good Driver? Reliability Issues in Artificial Neural Networks and Potential Solutions for Autonomous Vehicles"** **Session Chair:** Annachiara Ruospo, Politecnico di Torino (IT) **Speaker:** Paolo Rech (University of Trento, Italy) **Abstract:** Driverless cars are the new trend in the automotive market and, to burst deep space exploration, NASA and ESA are willing to add self-driving capabilities to their rovers. Ingenuity, landed in Mars in 2021, is the first autonomous vehicle to move outside of the Earth. To be implemented, a self-driving system needs to analyze a huge amount of images and signals in real time. This is achieved thanks to Convolutional Neural Networks (CNNs) executed on Graphics Processing Units (GPUs), dedicated accelerators implemented in Field Programmable Gate Arrays (FPGAs) or in Application Specific Integrated Circuits (ASICs), such as the Google's Tensor Processing Unit (TPU), or even in emerging architectures such as Processing In Memory (PIM) or Neuromorphic devices. In the talk, after a brief description of radiation effects at physical level, we will investigate the reliability of modern and emerging computing architectures executing neural networks, we will show if and why a neutron-induced corruption can modify the autonomous vehicles behaviors, and discuss the implications of these corruptions for the adoption of self-driving vehicles in large scale. The evaluation, to be accurate and precise, is based on the combination of beam experiments and fault injection at different levels of abstractions (RTL, microarchitectural, and software). This combination allows us to have a realistic evaluation of the error rate, distinguish between tolerable errors and critical errors, and to design efficient and effective hardening solutions for neural networks. Exploiting the potential of machine learning and taking full advantage of the computing resources in modern accelerators it is possible to significantly improve the neural network reliability with nearly-zero overhead. **Bio:** Paolo Rech received his master and Ph.D. degrees from Padova University, Padova, Italy, in 2006 and 2009, respectively. He was then a Post Doc at LIRMM in Montpellier, France. Since 2022 Paolo is an associate professor at Università di Trento, in Italy and since 2012 he is an associate professor at UFRGS in Brazil. He is the 2019 Rosen Scholar Fellow at the Los Alamos National Laboratory, he received the 2024 Italy-Canada innovation award, the 2020 impact in society award from the Rutherford Appleton Laboratory, UK and the Marie Curie Fellowship at Politecnico di Torino, in

	Italy. His main research interests include the evaluation and mitigation of radiation-induced effects in autonomous vehicles for automotive applications and space exploration, in large-scale HPC centers, and quantum computers.
10:00 - 10:30	**Coffee Break**
10:30 – 11:30	**Session 2: AI Accelerators and Design of SNNs** **Session Chair:** Ihsen Alouani, CSIT, Queen's University Belfast, UK **IR Drop-Resilient Memristor-Based Artificial Intelligence Accelerator Design** Emmanouil Arapidis[1], Theofilos Spyrou[1], Said Hamdioui[1] and Anteneh Gebregiorgis[1] [1] Delft University of Technology, The Netherlands **EAR – Endurance-Aware Retraining for Efficient DNN Inference on FeFET-Based Accelerators** Changhao Wang[1], Nicolò Bellarmino[1], Nima Kolahimahmoudi[1], Hanzhi Xun[2], Danyang Chen[3], Sicong Yuan[2], Xiuyan Li[3], Lin Wang[3], Giovanni Squillero[1], Mottaqiallah Taouil[2], Moritz Fieback[2], Said Hamdioui[2], Alberto Bosio[4] and Riccardo Cantoro[1] [1] Politecnico di Torino, Italy [2] Delft University of Technology, The Netherlands [3] Shanghai Jiao Tong University, China [4] Ecole Centrale de Lyon, France **Design and Variability Analysis of Spiking Neural Networks with Spintronic Synapses** Salah Daddinounou[1] and Elena Ioana Vatajelu[1] [1] TIMA - INPG, France
11:30 – 12:00	**Invited Talk** **Session Chair:** Nicolò Bellarmino, Politecnico di Torino (IT) **Speaker:** Leticia Maria Bolzani Pohls (Group Leader "Neuromorphic Hardware", IHP, Germany) **Title:** Reliability Assessment: Challenges when Adopting Emerging Technology-Based NNs

12:00 – 13:30	**Lunch Break**
13:30 – 15:10 (20 minutes each)	**Session 3: Reliability Assessment and Enhancement** **Session Chair:** Mahdi Taheri, Tallinn University of Technology, Estonia **Benchmark Suite for Resilience Assessment of Deep Learning Models** Alberto Bosio[1], Cristiana Bolchini[2], Luca Cassano[2], Antonio Miele[2], Salvatore Pappalardo[1], Dario Passarello[2], Annachiara Ruospo[3], Ernesto Sanchez[3], Matteo Sonza Reorda[3] and Vittorio Turco[3] [1] Ecole Centrale de Lyon, France [2] Politecnico di Milano, Italy [3] Politecnico di Torino, Italy **Metrics for Fault Detection in Image Segmentation DNNs** Vittorio Turco[1], Lorenzo Fezza[1], Annachiara Ruospo[1], Ernesto Sanchez[1] and Matteo Sonza Reorda[1] [1] Politecnico di Torino, Italy **Observations and Challenges on the Vulnerability Assessment of Dynamic Early-Exit Neural Networks** Georgios Konstantinidis[1], Maria Michael[1] and Theocharis Theocharides[1] [1] University of Cyprus/KIOS Research and Innovation Centre of Excellence, Cyprus **DEAR-CNN: Data-Efficient Assessment of Resiliency in Convolutional Neural Networks** Nicolò Bellarmino[1], Alberto Bosio[2], Riccardo Cantoro[1], Annachiara Ruospo[1] and Ernesto Sanchez[1] [1] Politecnico di Torino, Italy [2] Ecole Centrale de Lyon, France **Open-Source Tools for Reliability Assessment and Enhancement of Deep Neural Networks** Mohammad Hasan Ahmadilivani[1], Seyed Hamidreza Mousavi[1], Jaan Raik[1], Masoud Daneshtalab[1], Maksim Jenihhin[1]

	[1] Tallinn University of Technology, Estonia
15:10 – 15:15	**Closing Session**
15:15 – 15:30	**Coffee Break**