5th IEEE Workshop on AI Hardware: Test, Reliability, and Security

Tallinn, Estonia, May 29-30, 2025

Co-located with the 30th IEEE European Test Symposium 2025

The Workshop will take place in conjunction with the ***30th IEEE European Test Symposium 2025 https://ets2025.taltech.ee/***

Call for Contributions

Artificial Intelligence (AI) is today a rapidly evolving science that envisions the creation of intelligent systems capable of delivering numerous economic and social benefits. For its several qualities, AI can provide competitive advantages to companies and, in general, to the society. Recent advances in AI, in particular deep learning, have led to numerous applications, including computer vision, speech recognition, natural language processing, robotics, etc. This widespread use has raised several concerns about its deployment in safety-critical systems. As a matter of fact, AI will be the core enabling technology for autonomous vehicles. Simultaneously, there is intense activity in designing dedicated hardware specifically tailored for AI applications. On one hand, AI hardware accelerators are demanded to support the tremendous processing power, unprecedented speed, and memory costs that deep neural networks require to realize their full potential. On the other hand, there is a large incentive for moving the AI algorithms execution from the cloud into the edge devices, i.e. Internet-of-Things (IoT) devices, in particular for meeting data confidentiality and network bandwidth requirements and eliminating the communication latency. Edge devices are expected to include local AI processing, yet this is challenging as an edge device is a resource-constrained environment.

The aim of this Workshop is to focus particularly on the following emerging problems pertaining to AI hardware:

- **Testing**: fault modelling, fault simulation, test generation, post-manufacturing testing, design-for-test, built-in self-test, on-line testing, fault diagnosis.
- **Reliability**: reliability analysis, design-for-reliability, fault-tolerance, self-repair, functional safety.
- **Hardware security and trust**: IP/IC piracy, hardware Trojans, side-channel attacks, fault injection attacks.

Call for Submissions:

Perspective speakers are invited to submit an abstract, an extended abstract of up to 2 pages or a complete 6-page paper using the submission system:

https://easychair.org/conferences?conf=aitreats2025

An informal digest of abstracts and papers will be distributed to the attendees. We seek talks on novel scientific works or preliminary results, as well as perspective talks.

Key dates:

Submission of abstracts and papers: **February 28th, 2025**
Notification of acceptance: **March 28th, 2025**

Further Information:

Annachiara Ruospo
Program Chair
Politecnico di Torino, Italy
annachiara.ruospo@polito.it

Theofilos Spyrou
Program Chair
Delft University of Technology, The Netherlands
t.spyrou@tudelft.nl