Keynote Talk (VERDI)

# On Improving the Robustness of Convolutional Neural Networks Using In-Parameter Zero-Space Error Correction Codes

**Juan Carlos Ruiz**

## Abstract

Convolutional neural networks (CNNs) are currently of great interest in critical domains demanding image classification to support advanced safety-oriented features, such as those deployed in autonomous driving or medical image analysis. Providing high degrees of accuracy in object recognition comes with a high computational cost that requires the support of specific hardware accelerators.

These accelerators are rarely designed to protect CNN parameters during the inference process, which may lead to object misclassification provoking unsafe situations. On the one hand, the multiplicity of bits that can be potentially flipped by single event upsets increases with larger technology scales. On the other hand, as CNNs interconnect to other systems, they become further exposed to malicious faults (attacks) that may crush their inference process by simply flipping a small number of vulnerable parameter bits.

In this talk, we will see how to exploit the assessment information provided by fault injection experiments to increase the robustness of a CNN against the occurrence of multiple bitflips by using error correction codes (ECCs). The approach will be exemplified using a floating point-based CNN that is prototyped on a programmable logic device. Then, we will study how the approach can be deployed without retraining the considered CNN, using well-known and proven ECCs and at an in-memory and zero-space cost.

## Short Biography

Juan Carlos Ruiz is a permanent professor at UPV (Universitat Politècnica de València, Spain). He is member of the Fault-Tolerant Systems Research Group (GSTF) of ITACA, a UPV research institute. He is also member of the Department of Computer Engineering (DISCA) of the UPV. He teaches computer engineering and mobile cybersecurity in the UPV Bachelor degree on Computer Science. He is the Academic Director of the UPV Master Program on Computer Engineering and Networking, where he also provides lectures on dependable computing. His research is mainly focused, although not limited to, the verification of safety-critical embedded systems through fault injection. He is the currently the leader of the Spanish research project DEFADAS, whose aim is to provide means to assess and improve the robustness of FPGA-based convolutional neural networks. He regularly contributes as Program Committee, Organization Committee or Conference Chair to the most important conferences on dependable and secure computing systems, such as the IFIP/IEEE Dependable Systems and Networks Conference. He is author of more than 80 peer-refereed publications. Since 2024, he chairs the steering committee of the European Dependable Computing Conference.

## Acknowledgements

Grant PID2020-120271RB-I00 funded by MCIN/AEI/10.13039/501100011033