LOCA SERIES / Reading Club: Software-Only Semantic Diverse Redundancy for High-Integrity AI-Based Functionalities

Abstract

Dual (DMR) and Triple Modular Redundancy (TMR), often with some form of diversity, are used in safety-critical systems to realize those functionalities at the highest integrity level providing fault detection and/or tolerance capabilities. Redundant executions are intended to provide bit-level identical results and, upon any mismatch, an error is assumed and recovery actions taken as needed. In this work, we note that many emerging AI-based functionalities are intrinsically stochastic (e.g., camera-based object detection), and hence, their correctness must be judged semantically, with room for variations across correct outcomes (e.g., confidence must be above a given threshold). Building on this observation, we propose strategies to create DMR and TMR implementations of AI-based functionalities that bring not only fault tolerance against random hardware faults, but also against AI model inaccuracies. Those strategies, which can be realized with software-only means and ported to virtually any computing platform, build on input data modifications affecting the inference computations, but not the expected semantic output (e.g., introducing some limited random noise in the input data).

Short bio

Martí Caro received his B.S. degree in Informatics Engineering from the Universitat Politècnica de Catalunya (UPC) in 2020, and his M.S. degree in Innovation and Research in Informatics from UPC in 2022. He is currently pursuing a Ph.D. at the Department of Computer Architecture at UPC. In 2020, he joined the Computer Architecture and Operating Systems (CAOS) group at the Barcelona Supercomputing Center (BSC), where he is conducting research for his Ph.D. with a focus on making deep learning solutions more efficient and secure.

Speakers

Speaker: Martí Caro Roca. First stage researcher. Computer Sciences, BSC
Barcelona Supercomputing Center - Centro Nacional de Supercomputación