Silent Data Corruption in Robot Operating Systems (ROS): A Case for End-to-End System-level Fault Analysis Using UAVs

Yu-Shun Hsiao¹, Zishen Wan², Tianyu Jia³, Radhika Ghosal¹, Abdulrahman Mahmoud¹, Arjit Raychowdhury², David Brooks¹, Gu-Yeon Wei¹, Vijay Janapa Reddi¹

¹Harvard University, MA  ²Georgia Institute of Technology, GA  ³Peking University, China
*Equal Contributions, listed in alphabetical order

SILENT DATA CORRUPTION IN AUTONOMOUS SYSTEMS

- **Motivation:** Silent Data Corruption (SDC) has shown a significant threat in computing, from server scale systems to emerging application areas. Safety and reliability of autonomous systems is critical.

- **Challenge:** No suitable fault analysis tool; Autonomous machines are complex cyber-physical systems.

- **This work:** What is SDC impact on end-to-end system-level autonomy metrics for autonomous aerial robots? How to enhance the resiliency of autonomous system against SDC with lightweight techniques?

FAULT ANALYSIS FRAMEWORK

- **Fault Injection**:
  - Hardware transient faults during compute, portable to any ROS-based systems.

- **Host Sim.**
  - AirSim Interface
  - Compaion Computer

- **Planning**
  - Motion Planner: Shortest Path + Smoothing...

- **Control**
  - Path Tracking/Command Issue

- **ROSFI**
  - Attach + Sync
  - Fault Injection: Continue

- **QoF Metrics**
  - Flight time
  - Success rate
  - Mission energy

- **Fault Detection and Mitigation**
  - **Fault Detection**:
    - Application-aware anomaly detection
  - **Fault Mitigation**:
    - Skip and re-compute
  - **Overhead Evaluation**:
    - compared with DMR and TMR, software-based anomaly detection leads to <0.3% overhead.

ACKNOWLEDGMENTS

This work was supported in part by C-BRIC and ADA, two of six centers in JUMP, a Semiconductor Research Corporation (SRC) program sponsored by DARPA.