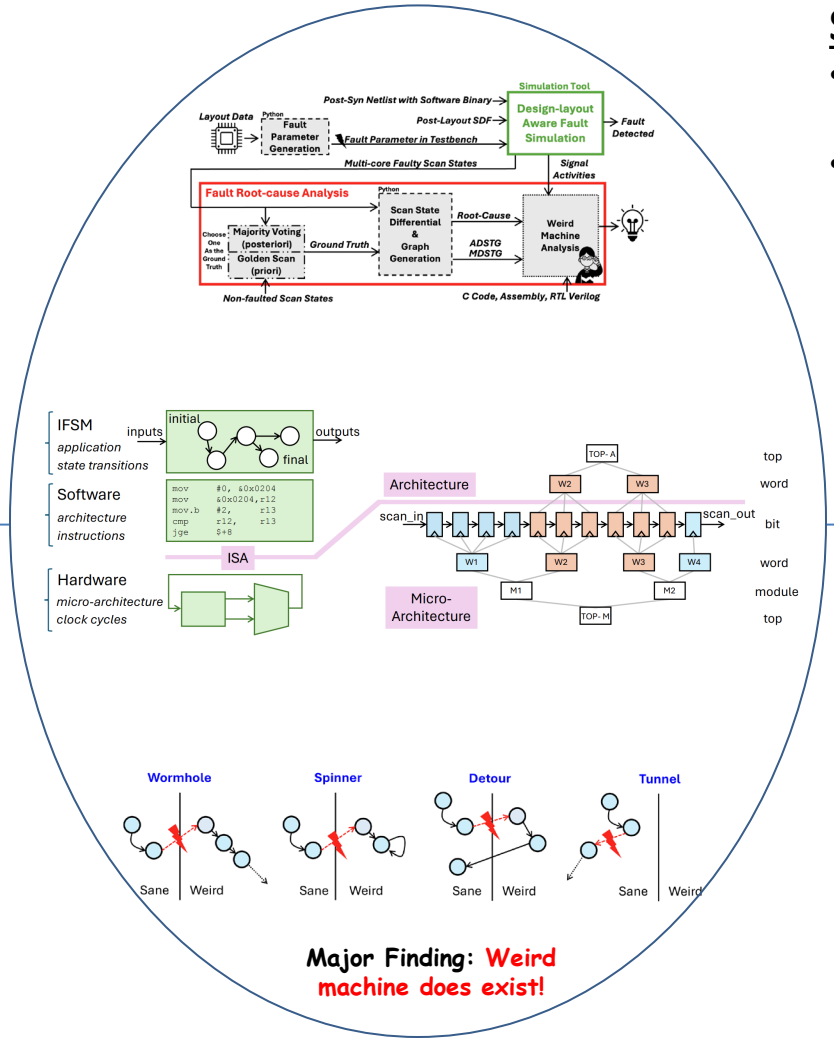
# FMitF: Track I: A Principled Approach to Modeling and Analysis of Hardware Fault Attacks on Embedded Software

## Challenge:

- The impact of HW faults on SW is poorly understood
- An improved fault model is needed to apply rigorous formal methods to program verification and repair
- Need a tighter link between HW design and SW verification, and a better understanding of HW threads to SW

## Solution:

- Study empirically impact of HW faults on ISA using HW simulation
- Use symbolic methods to quantitatively verify programs while considering fault attacks




## Scientific Impact:

- Realization in ASIC (180nm)
  *With 6 identical MSP430 cores*
- Publication:
  *[CHES 2024] Fault Detective: Explainable to a Fault, from the Design Layout to the Software*
  *[POPL 2025] An Incremental Algorithm for Algebraic Program Analysis*

## Broader Impact and Broader Participation:

- Enable novel chip design and better countermeasure
- Improve reliability and security of software
- Courses on secure chip design (WPI) and software verification (USC)
- Trained PhD students
- Keynote talk on career at SPLASH 2024 Doctoral Symposium


NSF 2220345: University of Southern California, Chao Wang, wang626@usc.edu
NSF 2219810: Worcester Polytechnic Institute, Patrick Schaumont, pschaumont@wpi.edu