IC Design for Secure & Reliable Computing Systems

NSF Integrated Circuits Research, Education, and Workforce Development Workshop

Daniel Limbrick

Automated Design for Emerging Processing Technologies (ADEPT) Laboratory

Department of Electrical and Computer Engineering
North Carolina Agricultural and Technical State University

Thursday, October 14, 2021

Outline

Outline

NC A&T Overview

- Land-grant doctoral research university that opened in 1891
- One of the Historically Black Colleges and Universities (HBCUs)
- Student Population $\approx$ 13,000 (UG: 11,500; G: 1,500)
- Located in Greensboro, NC, (60 miles from Research Triangle Park)

Largest HBCU in the nation

#1 producer of black engineers in the nation

- **Population**
  - Faculty $\approx$ 20
  - Students $\approx$ 300 undergraduate; 50 graduate
- **Degrees**
  - B.S. in Computer Engineering, Electrical Engineering
  - M.S. in Electrical Engineering
  - Ph. D. in Electrical Engineering (1 of 4 HBCUs in country)

Courses Related to IC Design

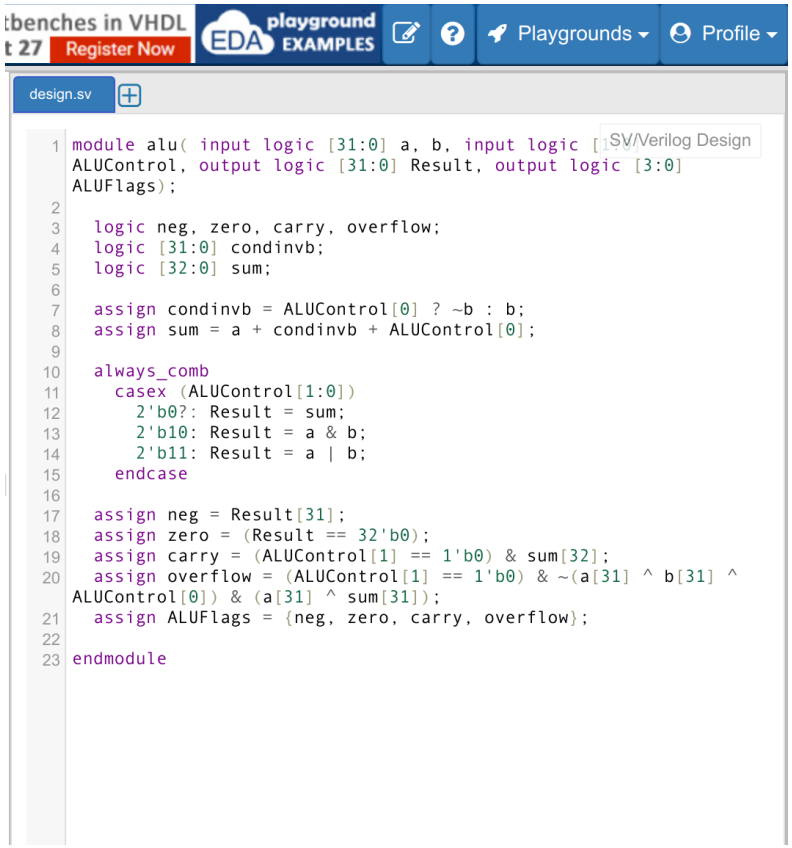
- **Undergraduate**
  - Digital Logic Design
  - Digital Systems Design
  - Advanced Digital Systems Design
  - VLSI Design
  - Senior Design
- **Graduate**
  - Advanced Digital Systems Design
  - VLSI Design
  - Fault Tolerant Digital Systems Design
  - Mixed-Signal VLSI Design
  - Advanced VLSI Design
  - Electronic Design Automation
  - Digital Systems Verification

Senior Design

- **Teams of four undergraduate students**
- **Two semester sequence**
- **Semester I**
  - Learn the design process as applied to electrical and computer systems
  - Learn technical design tools
  - Learn professional skills
- **Semester II**
  - Implement design
  - Test system blocks
  - Interface and test prototypes
  - Demonstrate teamwork, technical writing, communications, and project management
- **Example: Designing Pi HATs**

Course Tools

- EDAPlayground
- Cadence Digital IC tools (local server access)
- Mentor Graphics QuestaSim (local server access)
- Open-source tools through VM



Outline

ADEPT Research Lab

Automated Design for Emerging Processing Technologies

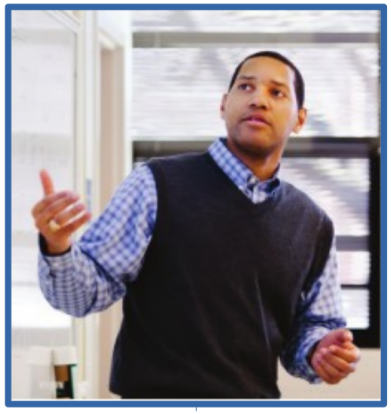
1. **Reliable ICs**
   - Fault Simulation
   - Fault Mitigation
2. **Secure ICs**
   - Secure Microkernels
   - Side-channel Attacks
3. **Emerging ICs**
   - Monolithic 3D ICs
   - Quantum Computing

Director

Dr. Daniel Limbrick
Associate Professor
August 2013-Present

Education

Postdoc - Georgia Tech
PHD, MS - Vanderbilt
BS - Texas A&M



Students

Ahmed Yiwere
PhD Student
(Expected May 2022)

Janani Aravind
PhD Student
(Expected May 2023)

Yohannes Bekele
PhD Student
(Expected May 2023)

Judith Hernandez-Campillo
MS Student
(Expected May 2023)

Dawood Rauf
MS Student
(Expected May 2023)

UG

Undergraduate Researchers
$\approx$ 4 per year

HS

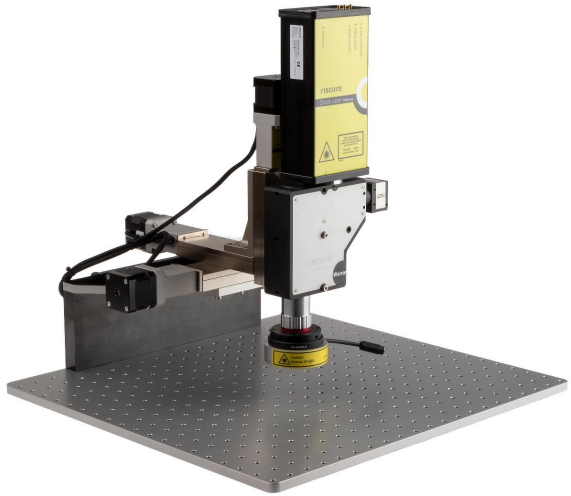
High School Researchers
$\approx$ 4 per year

ADEPT Research Approach

- **Design and fabricate secure/reliable microelectronics**
- **Use single-board computers as evaluation boards**
  - Arduino as sensor edge-computing node
  - Raspberry Pi as general-purpose computing platform
  - NVIDIA Jetson as AI computing platform
- **Run application benchmarks**
  - e.g., EEMBC AutoBench, MATLAB Autonomous Vehicle Toolbox, CARLA, data from AutoDrive Challenge
- **Demonstrate reliability mechanisms**
  - GDB-based fault injection
  - Laser fault injection
- **Demonstrate security attacks**
  - Rowhammer
  - Laser fault injection
  - Relate to critical systems
    - Space, automotive, military

ADEPT Research Equipment

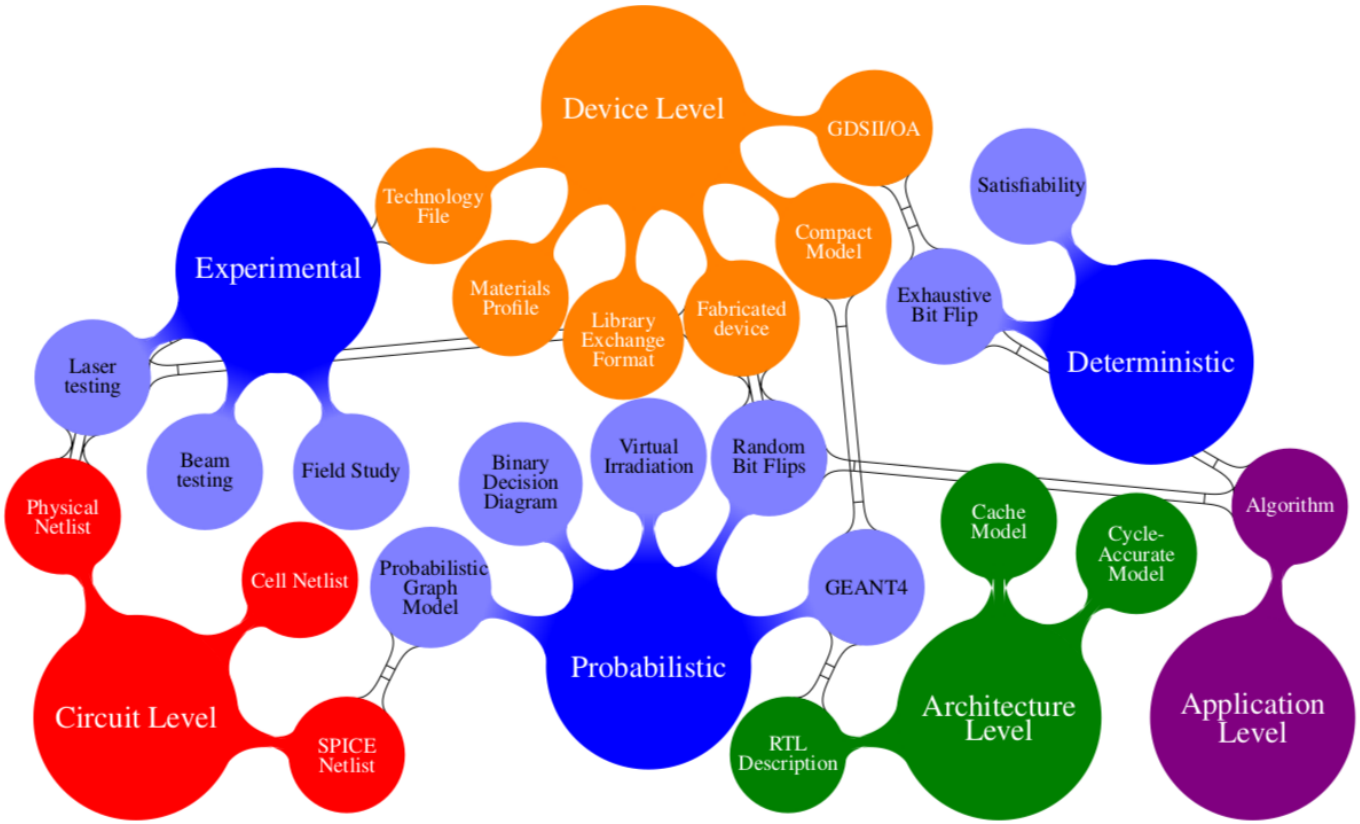
- **Servers**
  - Dell PowerEdge R720 (3)
  - NVIDIA Quadro RTX 6000 GPUs
- **Laser Fault-injection Station (funded; purchase pending)**
- **Single-board computing platforms and testbeds**
- **Agilent 16804A 136-channel logic analyzer**
- **FPGA Development Boards**



Outline

Cross-layer Fault Simulation

- Viewing the system in terms of “hardware” and “software” is a coarse-grained analysis
- Understanding the linkages among the quadrants is critical for development of a reliable system

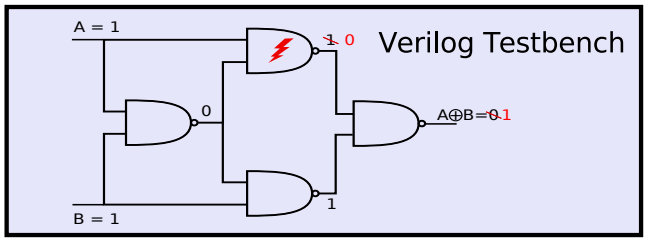


Simulating Soft Errors

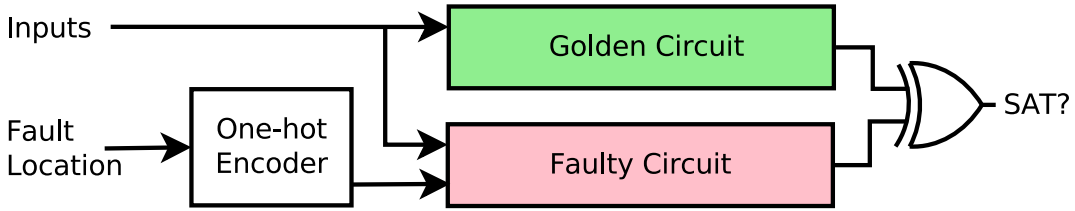
Deterministic

- Exhaustive vs. Satisfiability Solver

Exhaustive



SAT Solver

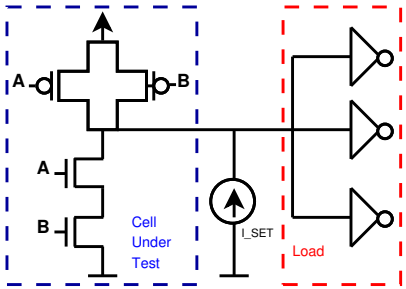


SAT Solver approach is more scalable and 15 times faster!

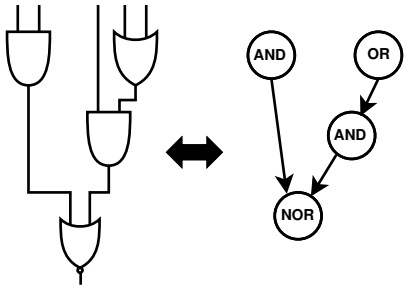
Probabilistic

- Probability of Failure (POF) = $P_{generation} \times P_{propagation} \times P_{latching}$

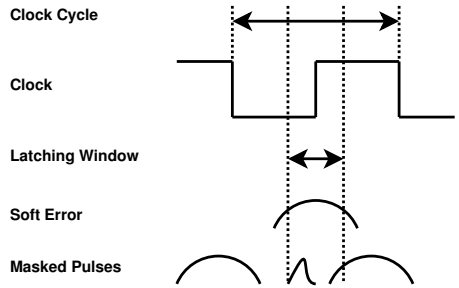
SPICE Modeling



Bayesian Statistics



Latch-window analysis



Device-level reliability metrics included in high-level analysis

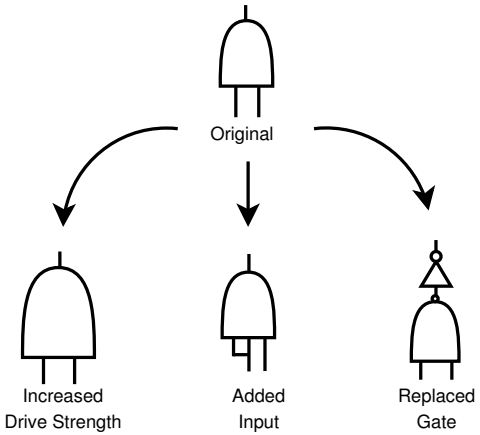
Requirements for Analyzing Physical Impact

- **Inputs**
  - Synthesized gate-level netlist
  - GDSII Layout
- **Outputs**
  - Location of gates that are vulnerable to SETs and/or SEMTs
  - Location of flip-flops that are vulnerable to SEUs
  - Input vectors that allow for each gate to be vulnerable
- **Tools**
  - Icarus Verilog
  - Yosys Open SYnthesis Suite (YOSYS)
  - PicoSAT
  - AIGER

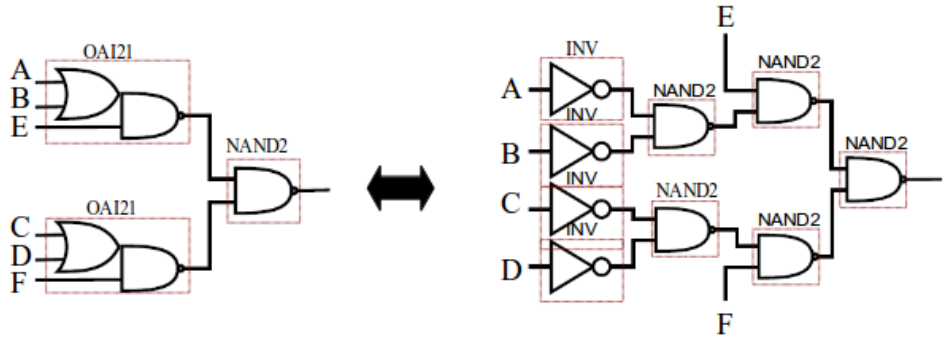
Fault Mitigation: RHBD/RHBC

- **Reliability-Aware Synthesis and Physical Design**
  - Leverages design constraints (e.g., area, delay, power)
  - Uses available standard cells (i.e., without redesigning the cell)

Cell Replacement

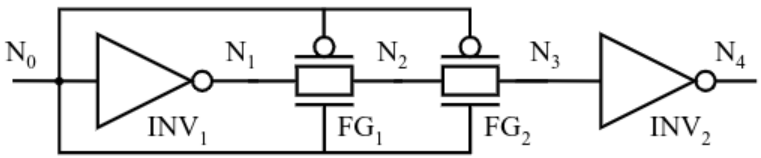


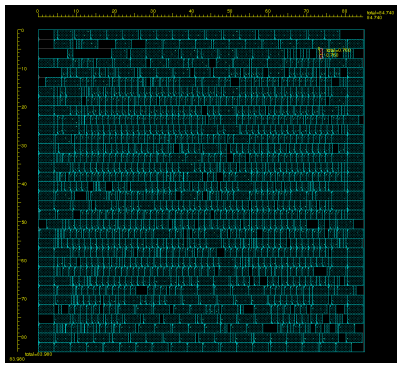
Subcircuit Replacement



Reliability improved by 20% with less than 1% power overhead!

- **Zero-penalty Improvement?**

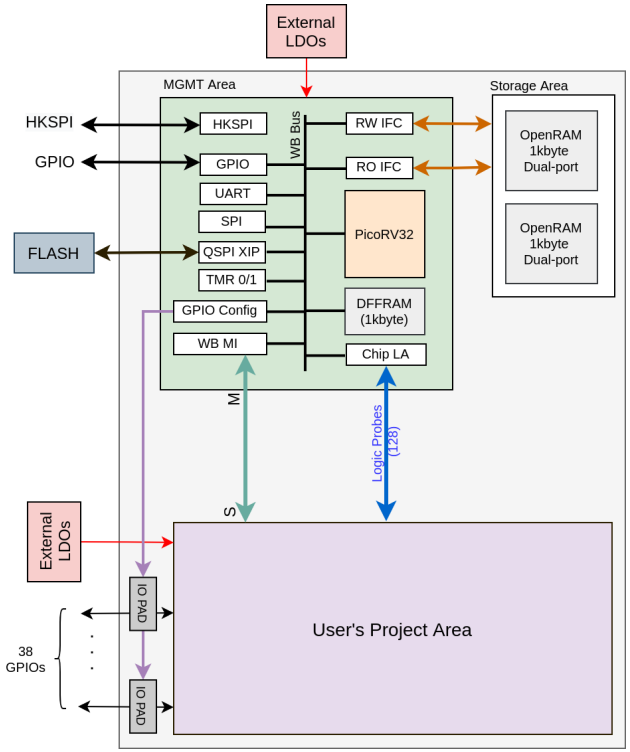




Outline

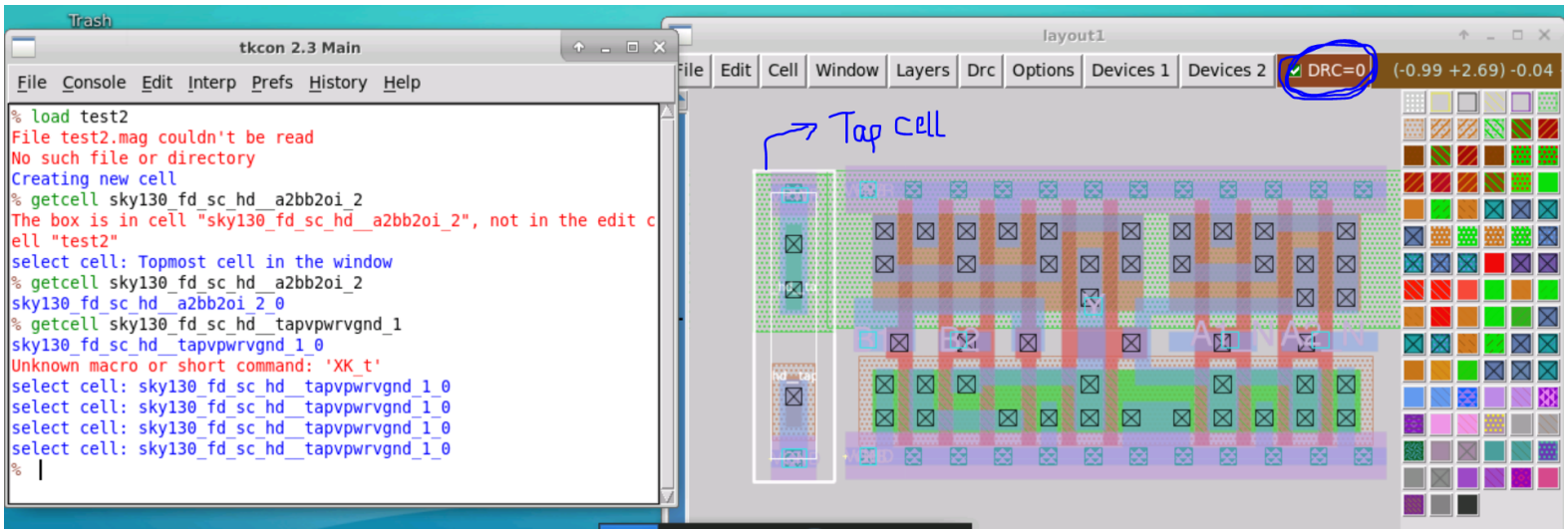
Radiation-Hardened-By-Construction Microprocessor

- **Sponsor: Office of Naval Research**
- **Project Period: July 1, 2021 to June 30, 2024**
- **Research Goals**
  - Design reliability-aware CMOS IC designs
  - Fabricate designs and verify performance
  - Inject faults via laser to validate reliability improvement
- **Google/Skywater/Efabless Open MPW Shuttle Program**
- **Skywater 130-nm CMOS**
- **Laser testing at Naval Research Laboratory and in-house**



Reliability-Aware DRC

- Create design rules that detect vulnerabilities (e.g., latch-up, charge sharing)
- Google/Skywater/Efabless Open MPW Shuttle Program
- Skywater 130-nm CMOS
- Trained student with “Physical Verification Using SKY130” workshop by Tim Edwards



Outline

Needs

- **Standardized open-source development and prototype boards**
  - Caravel harness?
- **Applications that connect to latest research trends (e.g., AI, Cybersecurity)**
  - No new VLSI or IC Design Faculty!
  - Administrators outside of area don't understand
- **Textbook integration**
  - Maximize class time (biggest pipeline stage)
  - Can then leverage educational and research resources
  - Shout out to Erik Brunvand!
- **Post-silicon run**
  - We built it! Now what?
- **Hardware competitions**
  - Adds a consistent target and more support
  - Shout out to IEEE SSCS International Student Circuit Contest

Questions