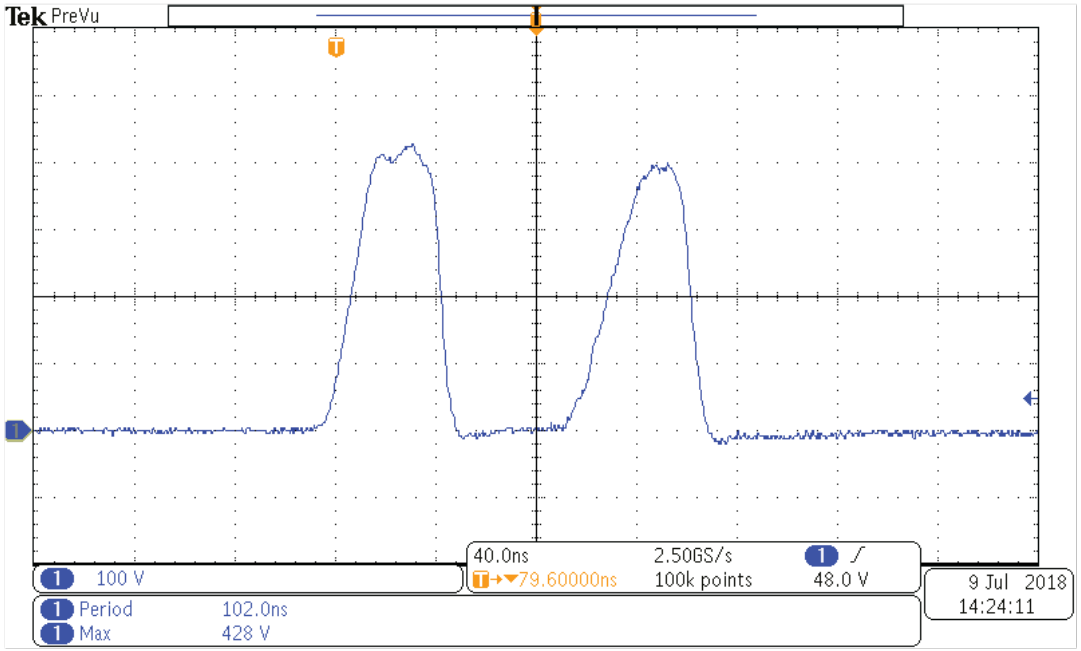
UF Nelms Institute for the Connected World
UNIVERSITY of FLORIDA

Cross Layer EM Fault Injection Assessment Framework

ORLANDO ARIAS
UNIVERSITY OF MASSACHUSETTS, LOWELL
EMAIL: ORLANDO_ARIAS@UML.EDU

What is EM Fault Injection?

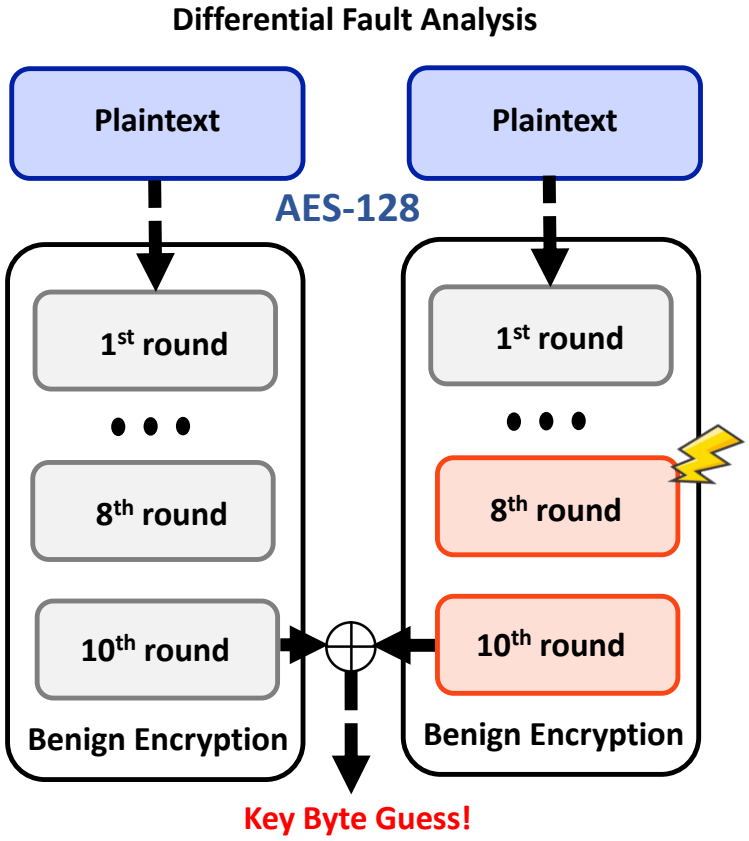


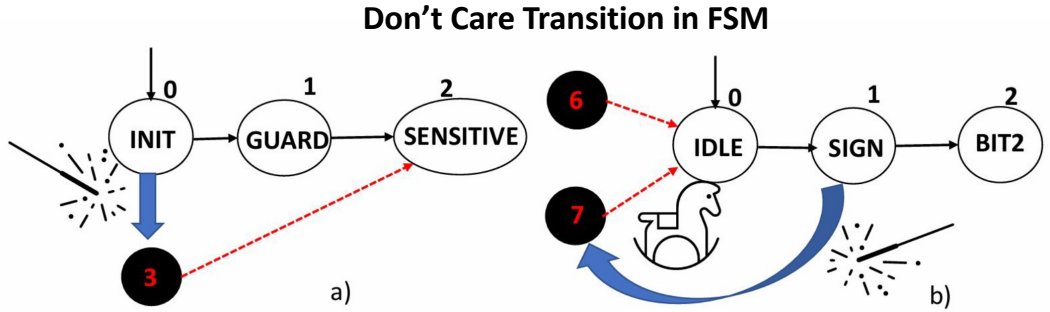
- Apply directly on digital circuits to cause bitflip
- Generate high frequency high magnitude EM pulse
- Usually Near-field

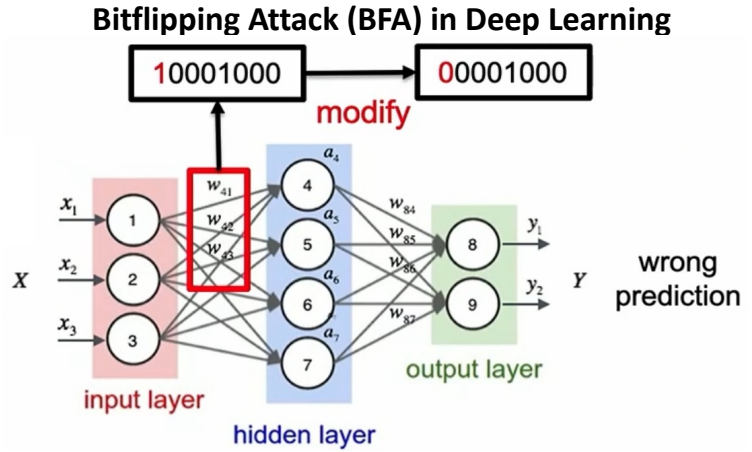
ChipSHOUTER Specs

Charge Voltage Range	150V to 500V
Charge Energy	625 mJ
Inserted Pulse Min Width (1mm tip)	15 nS (TYP)
Inserted Pulse Max Width (1mm tip)	80 nS (TYP)
Inserted Pulse Min Width (4mm tip)	24 nS (TYP)
Inserted Pulse Max Width (4mm tip)	480 nS (TYP)

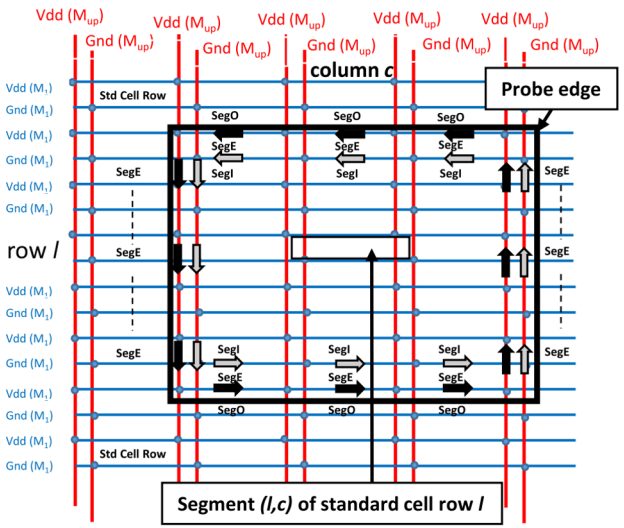
Consequences







EMFI Modeling (Dumont et al. TCAD)



Takeaway:

- EMFI causes undervolt in PDN segments close to probe edge
- Bitflipping in register is caused by undervolt in glue logics and clock tree

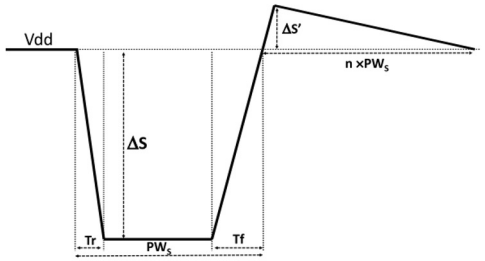


Fig. 13. Swing variation model.

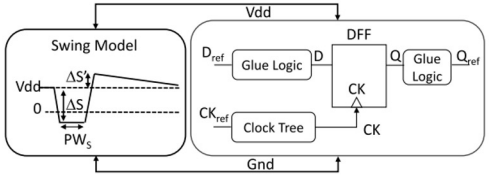
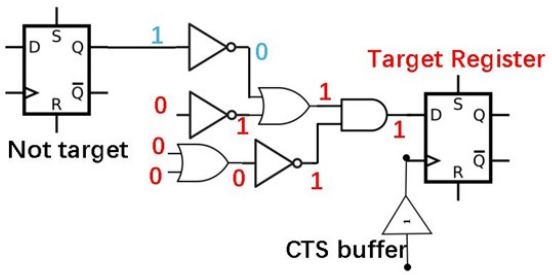


Fig. 14. Circuit considered during simulations.

Sampling Fault !

Two Cases of Sampling Fault

Case 1: Undervolt Event in Glue Logics



Any of the red 0/1 becoming 1/0 during EMFI will cause the D value to flip from 1 to 0.

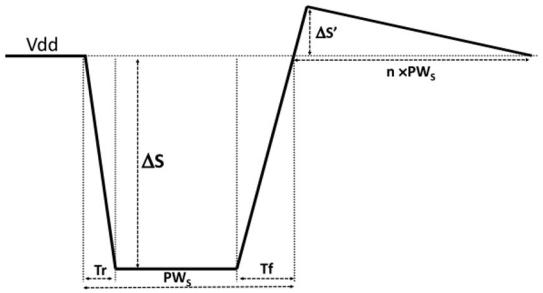
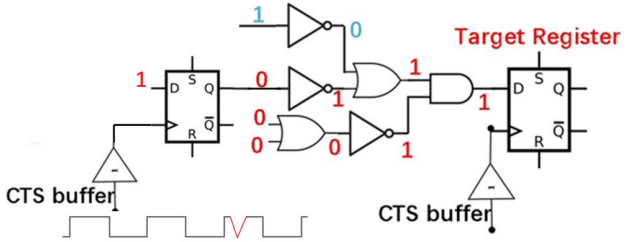


Fig. 13. Swing variation model.

Case 2: Undervolt Event in Clock Tree



Additional clock caused bitflip.

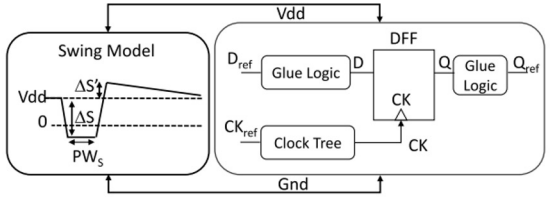
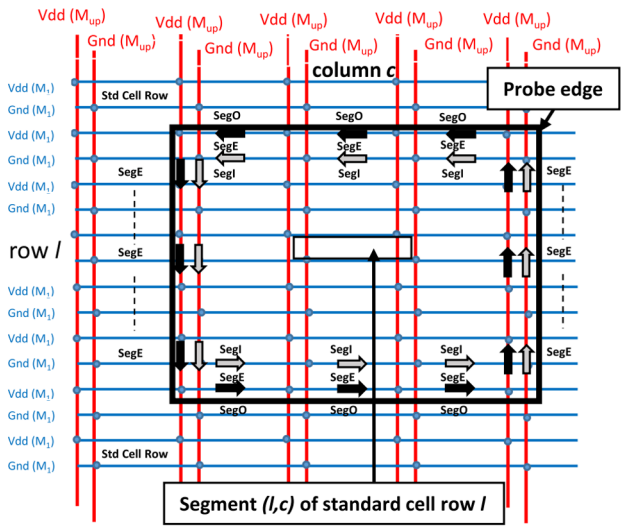


Fig. 14. Circuit considered during simulations.

EMFI Modeling (Dumont et al. TCAD)



Takeaway:

- EMFI causes undervolt in PDN segments close to probe edge
- Bitflipping in register is caused by undervolt in glue logics and clock tree

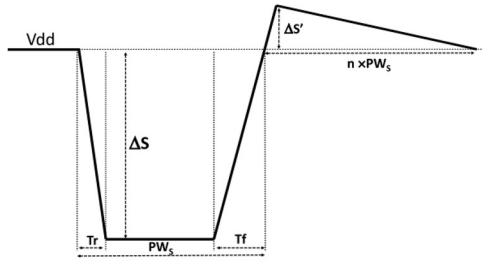


Fig. 13. Swing variation model.

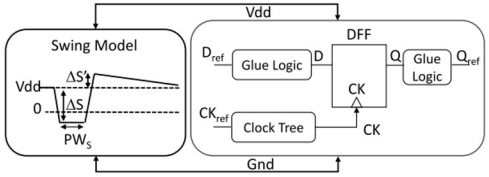
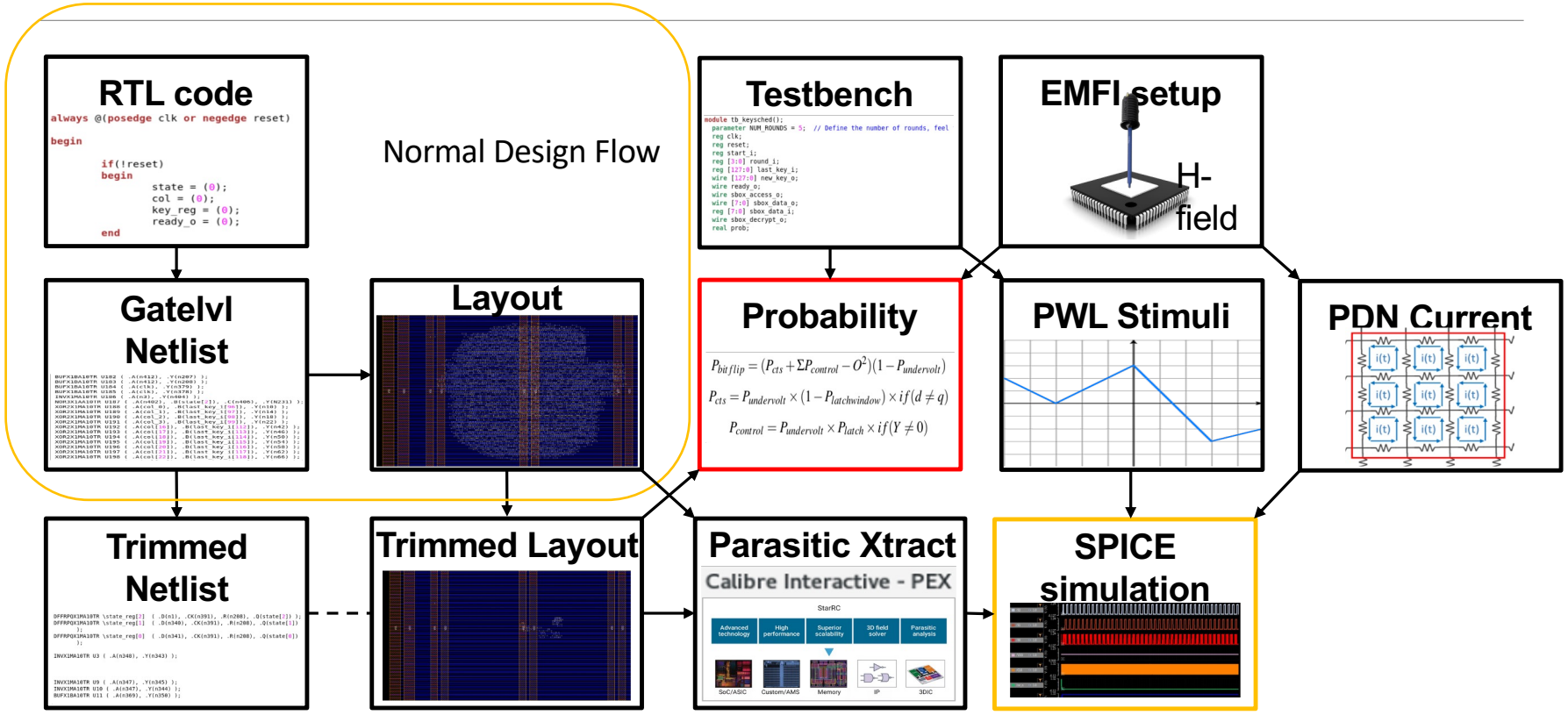


Fig. 14. Circuit considered during simulations.

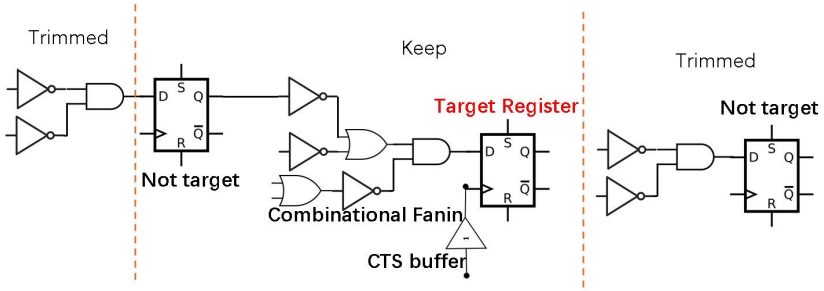
Limitations: Proof-of-concept work, systematically introduced the cause and reasoning of EMFI causing bitflip, but how to model EMFI in VLSI design

We need EDA tools for evaluating the actual bitflipping likelihood of registers for VLSI designs

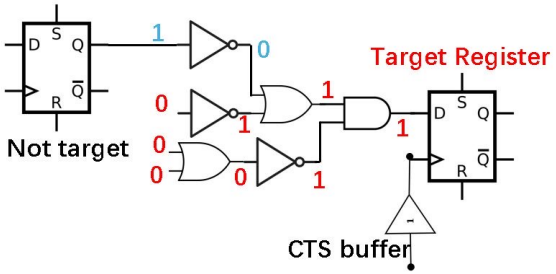
EMFI Assessment Framework (ISQED'25)



Bitflipping Probability Equations under EMFI



Trimming Strategy: Keep the glue logics and clock tree connected to the target register



Find internal control signals that flip the register

Eq1: Single register bitflipping probability

Sum $P_{bitflip} = (P_{cts} + \Sigma P_{control} - O^2)(1 - P_{undervolt})$

Case 2 $P_{cts} = P_{undervolt} \times (1 - P_{latchwindow}) \times if(d \neq q)$

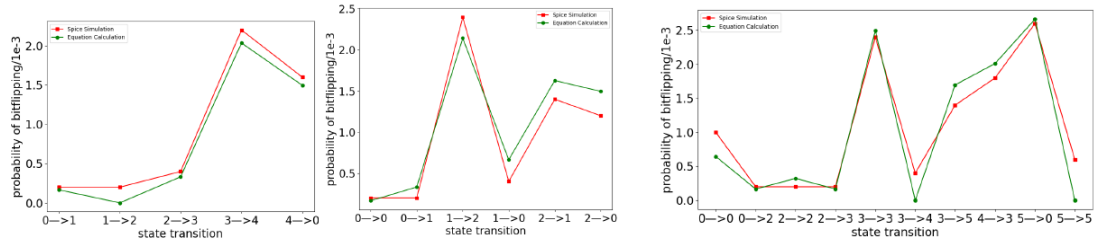
Case 1 $P_{control} = P_{undervolt} \times P_{latch} \times if(Y \neq 0)$

Eq2: Conditional bitflipping probability

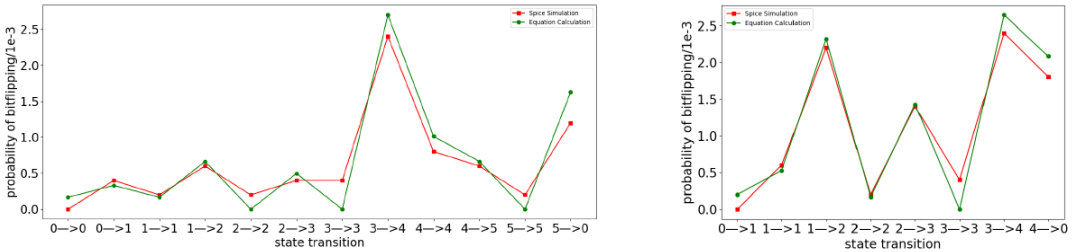
$$P(XY) = (P(X) - P(X_1))(P(Y) - P(Y_1)) + P(X_1)$$

$$P(Y|X) = \frac{(P(X) - P(X_1))(P(Y) - P(Y_1))}{P(X)} + \frac{P(X_1)}{P(X)}$$

Equation vs. Simulation



(a) Register state[2] of FSM in Sys-temC AES (b) Register STATE[1] of FSM in APB2SPI (c) Register state[2] of FSM in RS232 U-XMIT verilog



(d) Register pcmSq[2] of FSM in IMA ADPCM-ENC

(e) Register recvstate[2] of FSM in UART-1

Simulation Results:

- Post-layout Simulation on 5 benchmarks shows our proposed probability equation has an mean error lower than 10% of the mean value.

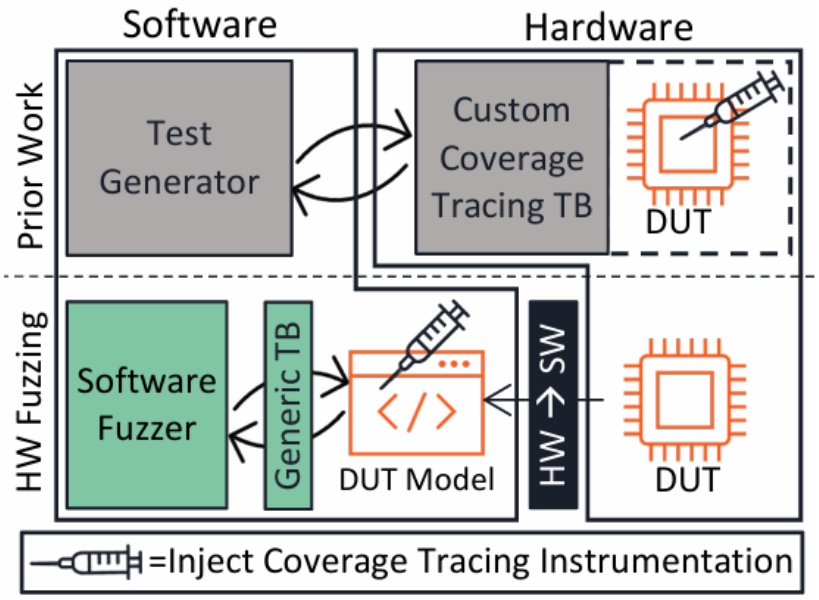
Discrepancy Cause:

- two or more control signal gates in different PDN segments are undervolted at the same time

Future Work

Combining EMFI Assessment Framework with Hardware Fuzzing:

- Our framework updates the Fuzzer with dynamic bitflipping probability of certain flip-flops
- The Fuzzer will try to maximize the bitflipping probability and uncover the most susceptible legit instructions / input for hardware systems
- Designers being aware of such vulnerabilities, adjusting the floorplan and patching the issue in advance
- Evaluations have been conducted on RISC-V SoC designs.



UF Nelms Institute for the Connected World
UNIVERSITY of FLORIDA

Questions?