System-Level Vulnerability and Mitigation

**Prof. Bruce Jacob, Hongxia Wang,
Samuel Rodriguez, Cagdas Dirik**

Electrical & Computer Engineering

AFOSR-MURI Final Review, July 2006

Overview

Primer: Circuits & Systems & How They Fail

- **Components of digital systems**
- **Internal & External vulnerabilities**

Quantifying External Vulnerability

- **DUT: Test chip fabricated in AMI’s 0.5µm process**
- **Comparison of vulnerability: DUT’s clock/data inputs**

Quantifying Internal Vulnerability

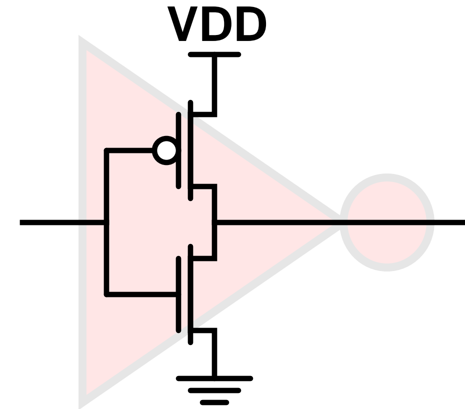
- **Predictive 45nm BSIM4 models integrated w/ Spectre**
- **Shmoo plots for Drowsy & DR-Gated-GND SRAM cells**

Mitigation

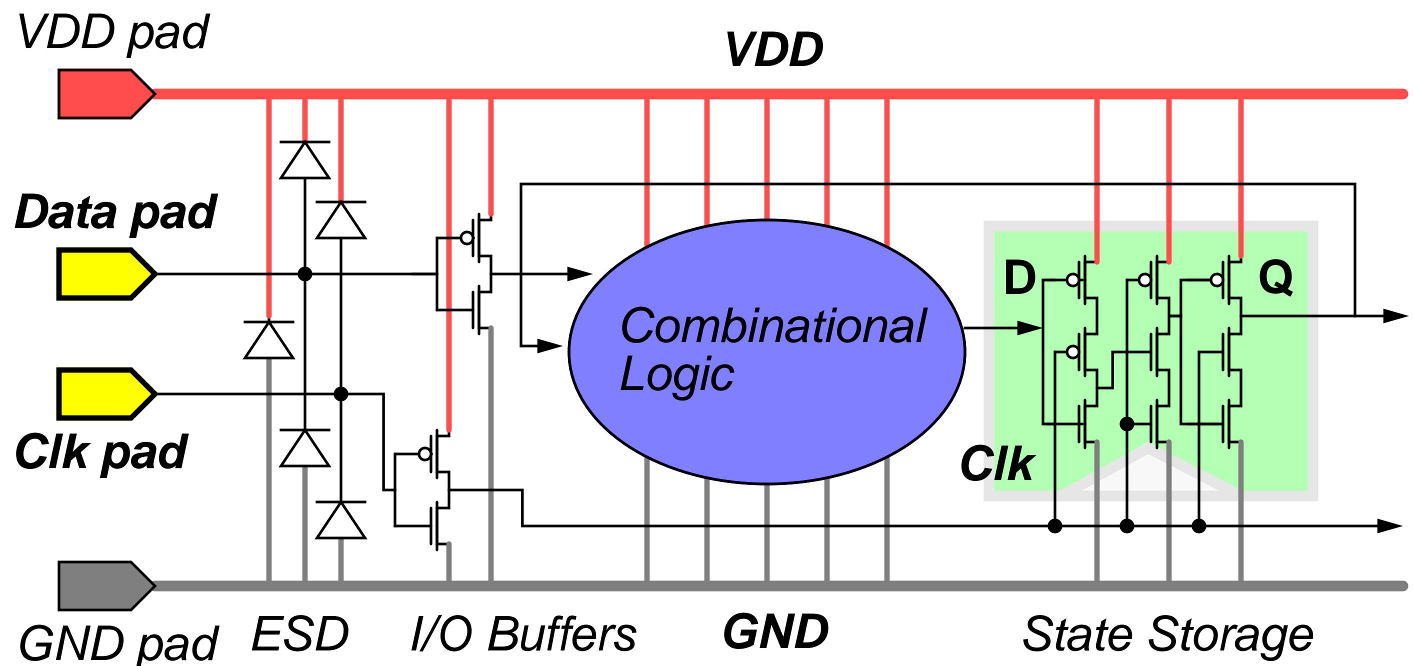
- **TERPS architecture & prototype chipset**
- **System verification**

Primer: Digital Systems

Simple Digital *Circuit:*

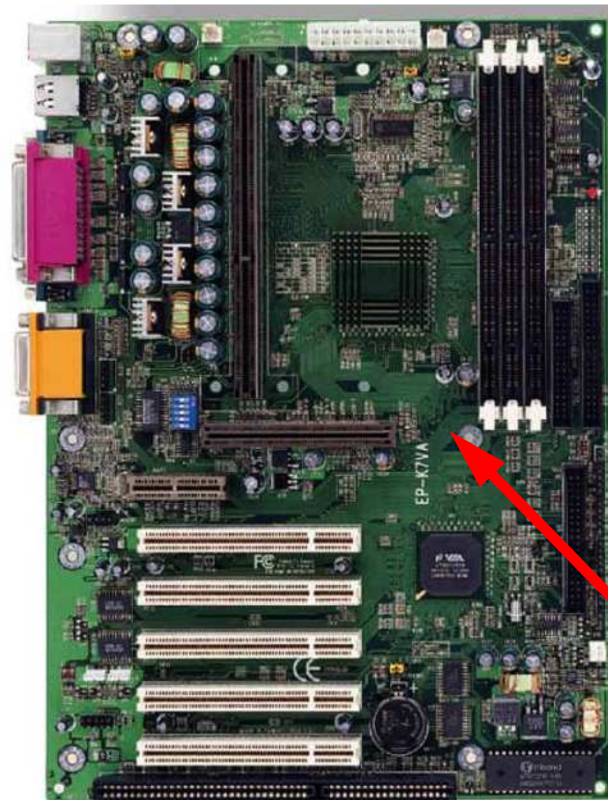


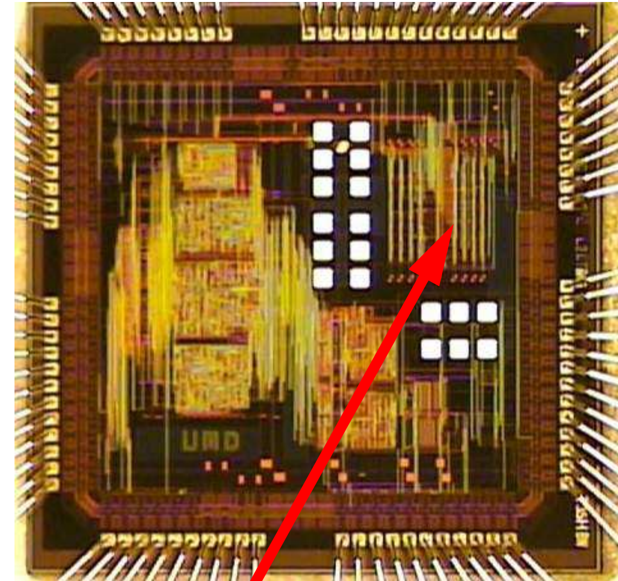
Simple Digital *System:*



Primer: Digital Systems

"External" vs. "Internal" Vulnerability



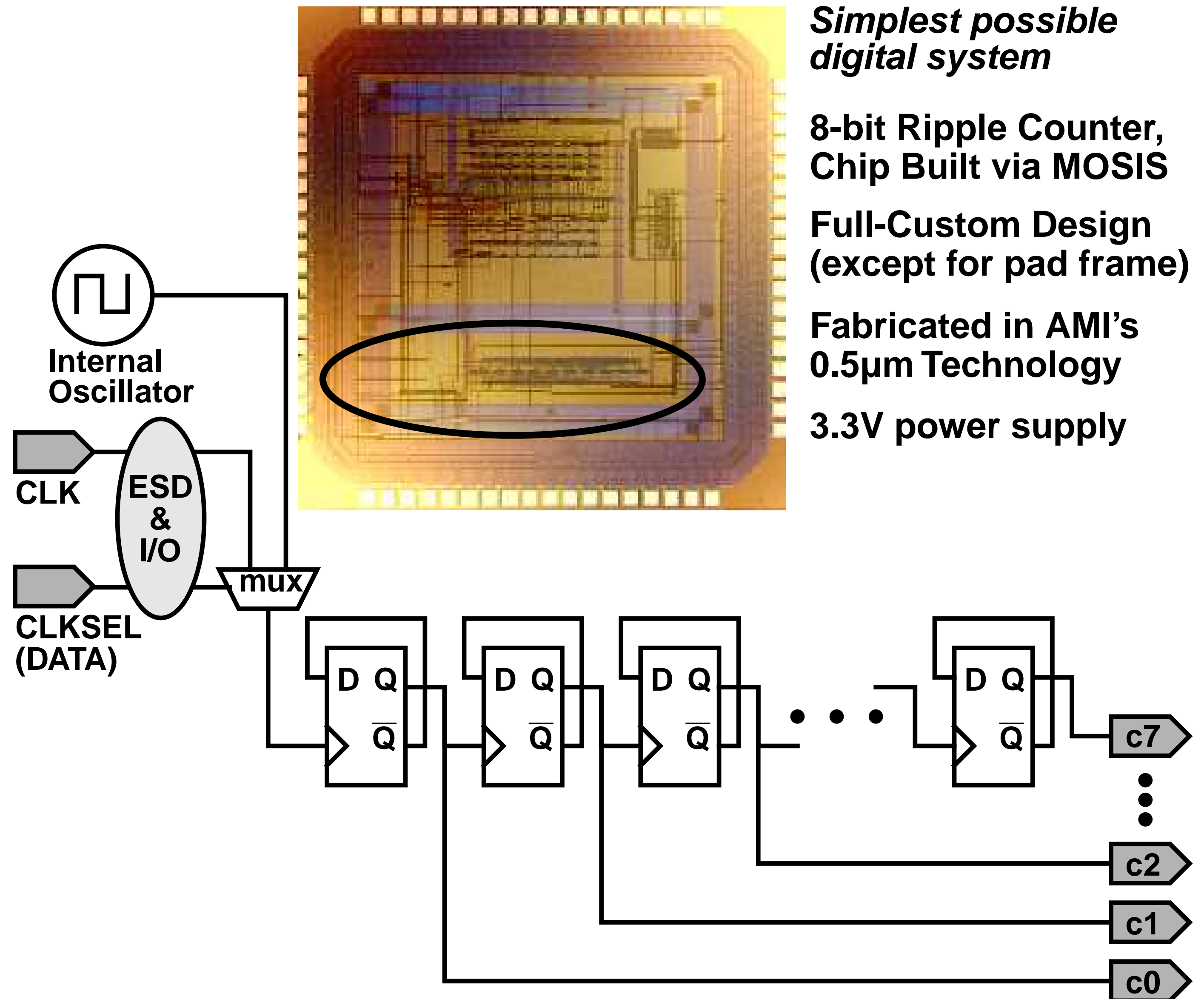


Internal: Intra-chip traces

External: Inter-chip traces

- **External Signals:** ***How easily can they sneak into chip?***
- **Internal Signals:** ***How easily can they upset state?***

External Vulnerability: DUT



Simplest possible digital system

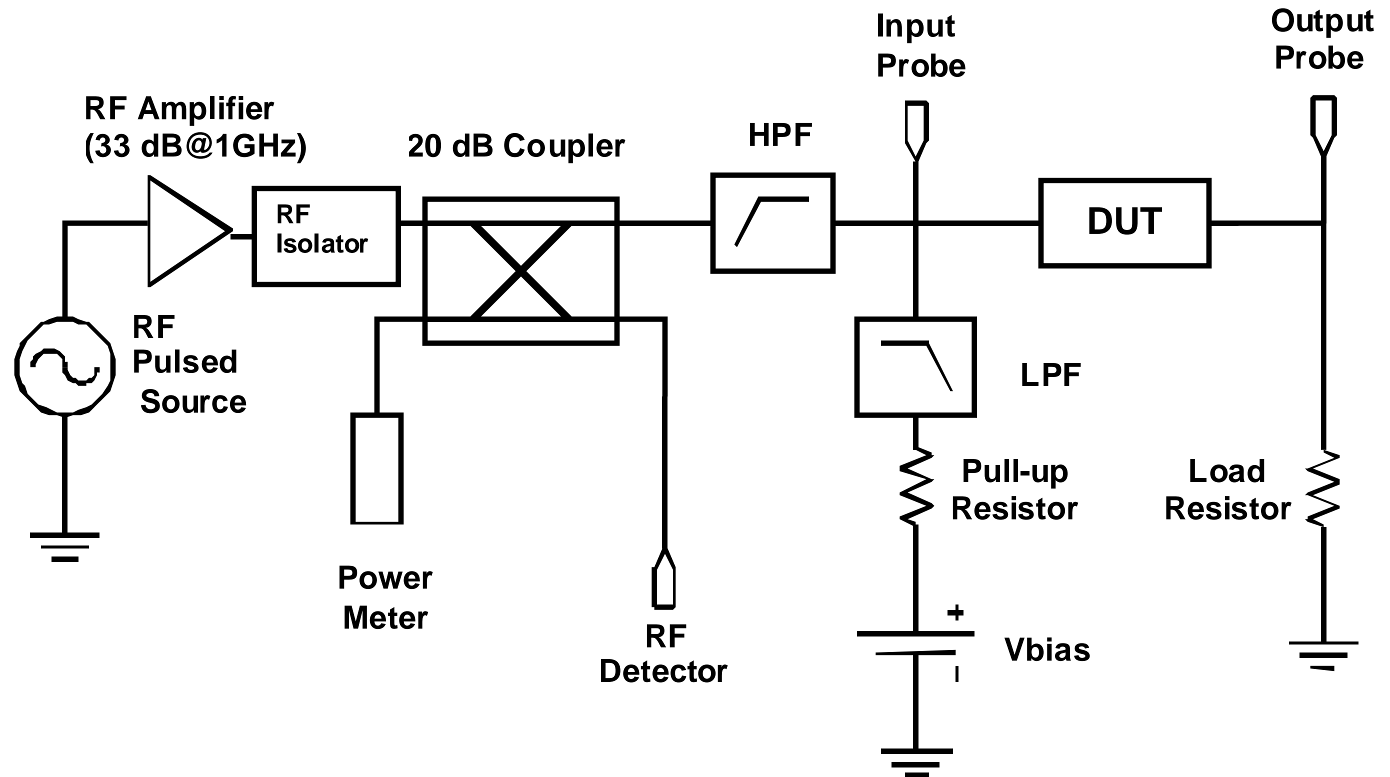
8-bit Ripple Counter, Chip Built via MOSIS

Full-Custom Design (except for pad frame)

Fabricated in AMI's 0.5µm Technology

3.3V power supply

Experimental Set-Up



Power Amp 33dB at 1GHz

Freq 800MHz – 4.2Ghz with 1.2W max power

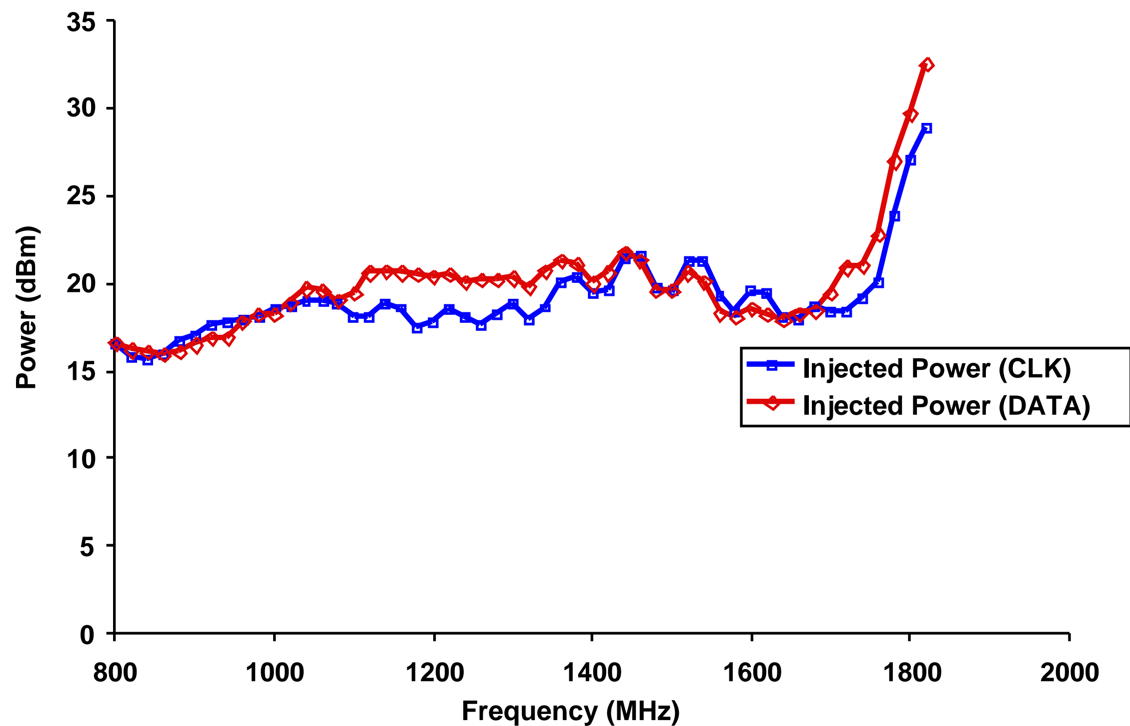
Test Board

CLK & CLKSEL

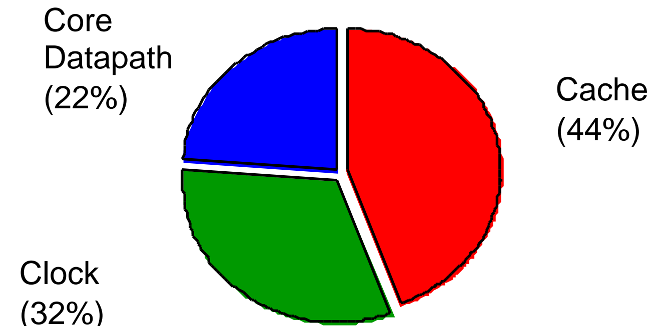
Counter Output

CLK vs. DATA Inputs

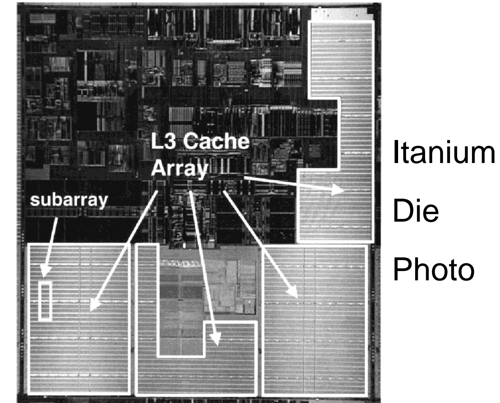
Power-v-Freq. required to cause incorrect behavior (state change in digital logic)



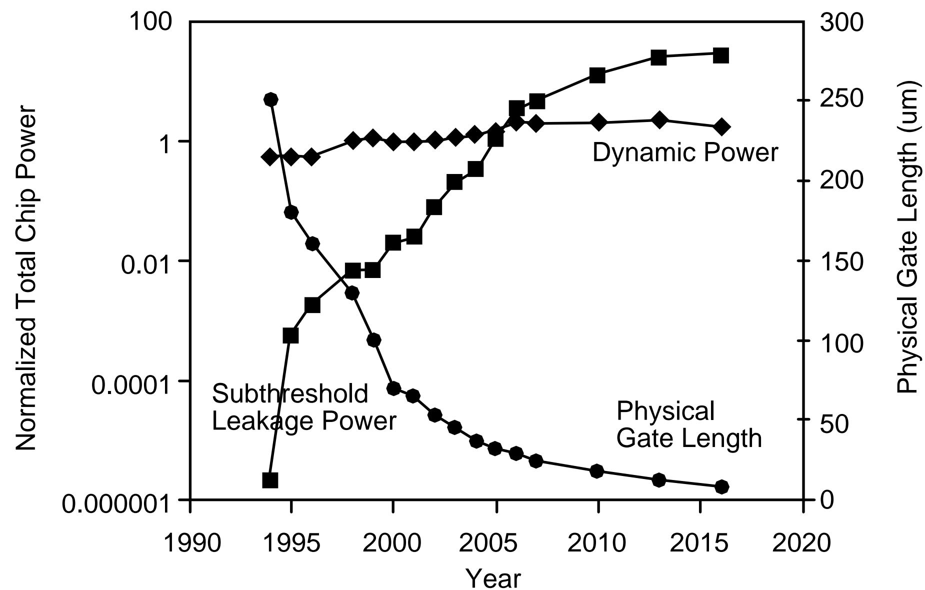
Internal Vulnerability: SRAM



Breakdown of power dissipation for a 200MHz 3.3V 0.35um processor with 32kB/32kB/1MB caches

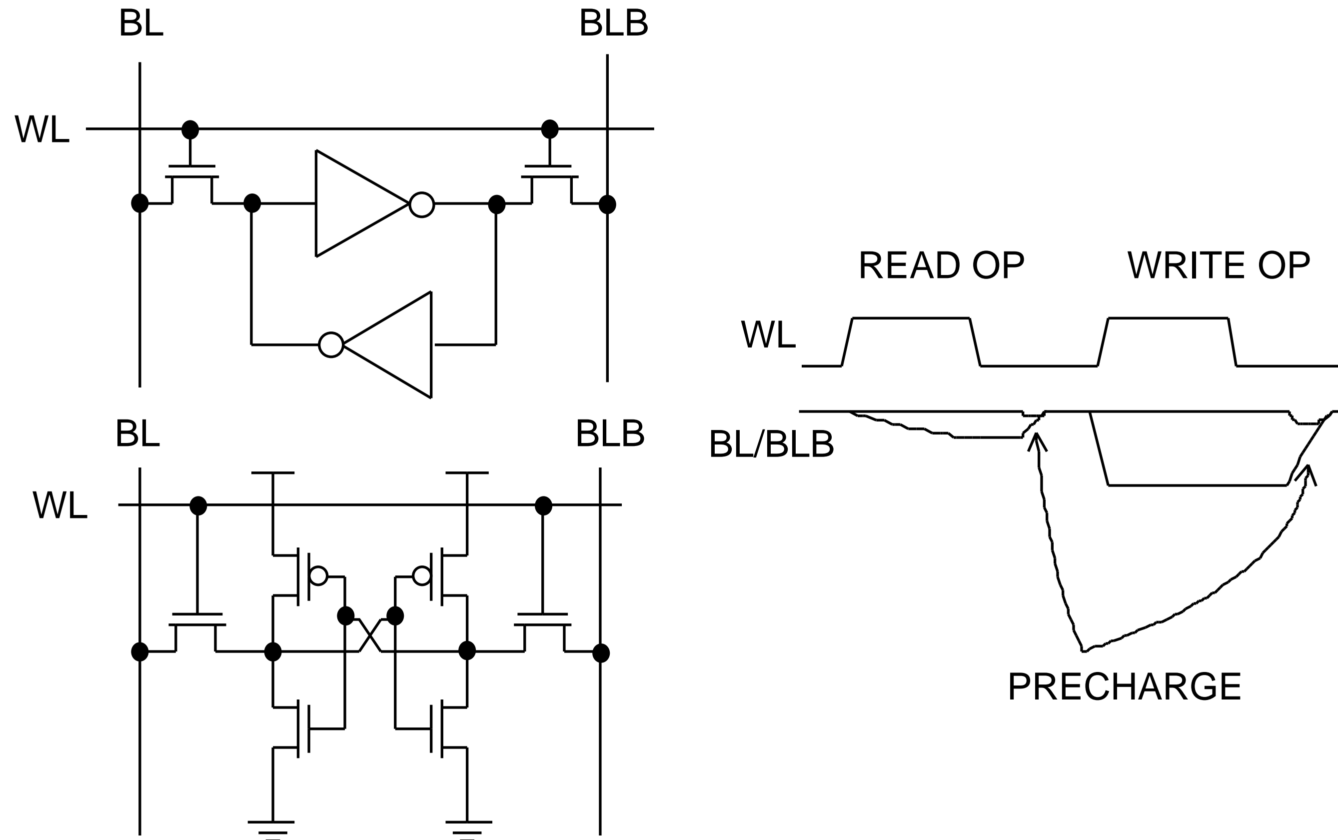


Fraction of die area and transistor count dedicated to caches is large and increasing



People care about reducing cache power, static & dynamic

SRAM Implementation

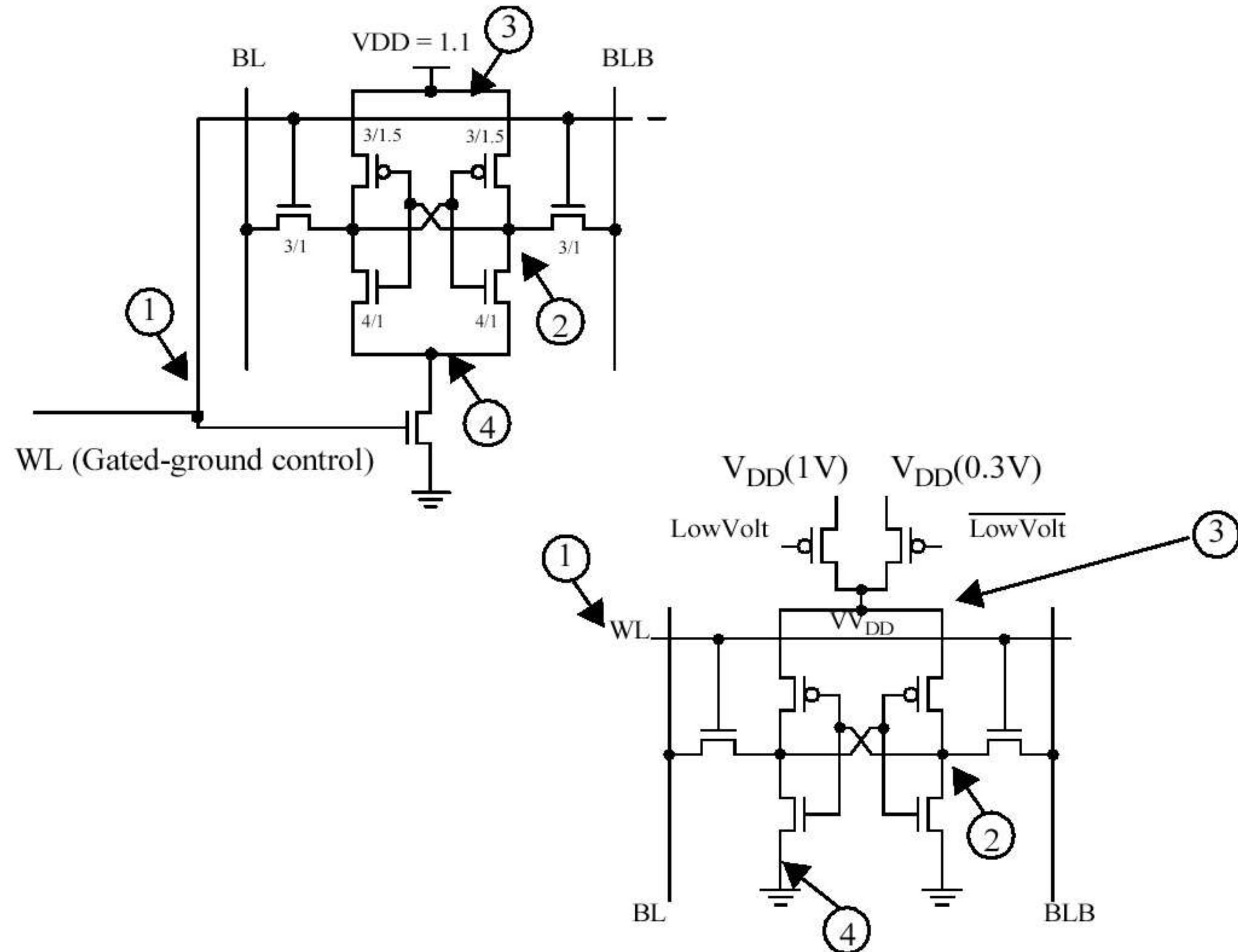


SRAM memory cell (top)

Full CMOS 6T implementation (bottom)

State of bitlines (right) *(note coupling)*

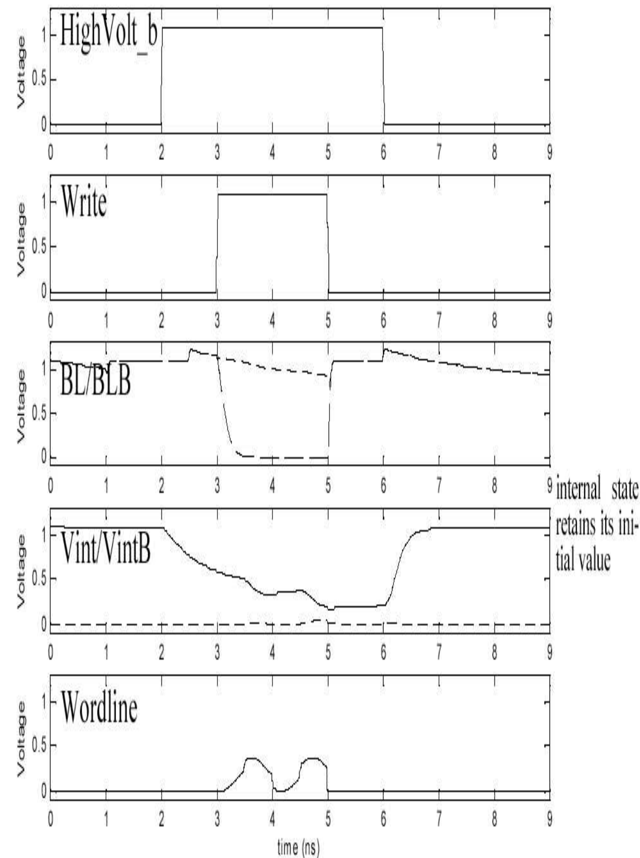
Experimental Set-Up

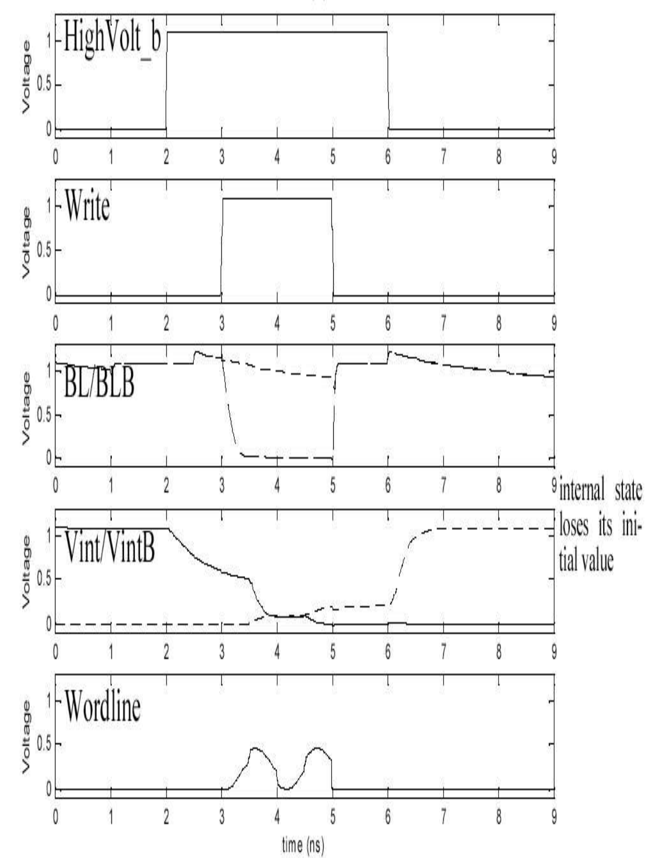


- **Data-Retentive Gated-Ground (top) and Drowsy Cache (bottom) circuits, with noise-injection sites shown**

SRAM Noise Immunity

SRAM cells with noise injected:





State is retained **State is lost**

SRAM Noise Immunity

Shmoo plots

Successful run
Failed run

Drowsy wordline

EMI amplitude
0.4V
0.3V
0.2V
0.1V
0.0V

0 25 69 113 156 200
Percentage of nominal coupling capacitance (%)

(a)

DRG wordline

EMI amplitude
0.4V
0.3V
0.2V
0.1V
0.0V

0 25 69 113 156 200
Percentage of nominal coupling capacitance (%)

(b)

Drowsy internal node

EMI amplitude
0.4V
0.3V
0.2V
0.1V
0.0V

0 25 69 113 156 200
Percentage of nominal coupling capacitance (%)

(c)

DRG internal node

EMI amplitude
0.4V
0.3V
0.2V
0.1V
0.0V

0 25 69 113 156 200
Percentage of nominal coupling capacitance (%)

(d)

SRAM Initial Results

Low-power SRAM circuits most susceptible to noise (EMI) through wordline coupling

Explained by strong differential noise that affects the internal state whenever the wordline has enough strength to turn on the access transistors.

For example, when the initial state of an idle or inactive memory cell is “1”, and a “0” is being written to a neighboring cell such that the bitline goes low (and the complementary bitline stays high), a voltage difference exists between the internal node and the bitline it is connected to (also true for the complementary side). The access transistors to idle memory cells are ideally turned off to isolate the internal nodes from the bitlines, but any noise present in the wordline will tend to induce currents through the access transistors that produces differential-mode noise across the cross-coupled inverter latch, potentially overwriting it and corrupting its stored state.

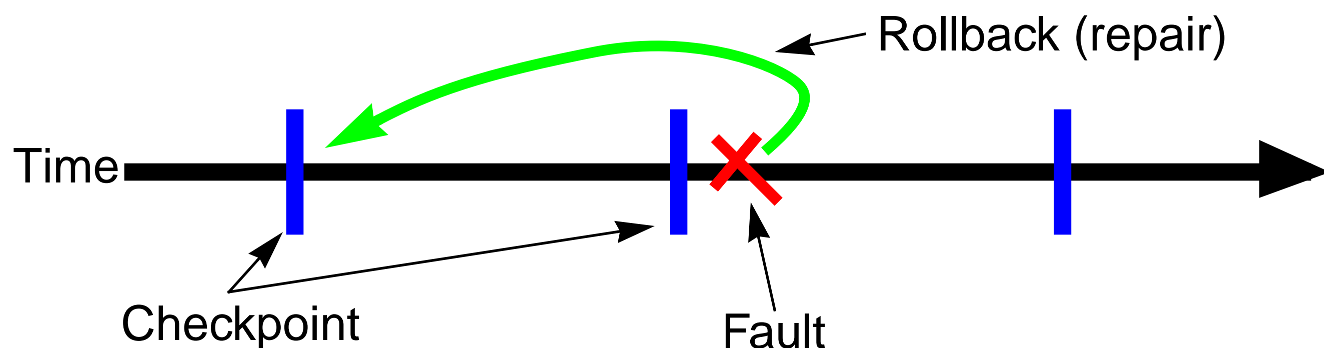
Because MOSFET switching characteristics change with temperature, future/present work investigates thermal effects

Mitigation: TERPS

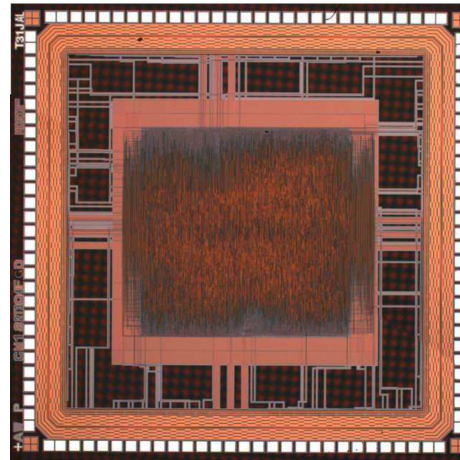
Problem: susceptibility to (intentional) EMI

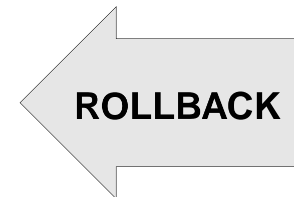
- **Vdd ↓ ⇒ circuit sensitivity ↑**
- **T_{clk} ↓ ⇒ circuit sensitivity ↑**
- **L_{eff} ↓ ⇒ circuit sensitivity ↑**
- **ECC not a solution for wordline coupling**
- **Clock coupling takes out whole chip**

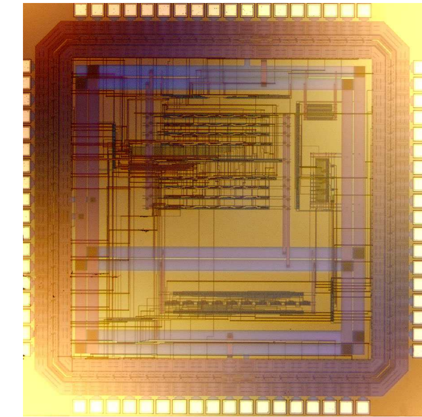
Solution: checkpoint/rollback



Prototype Chipset







RiSC CPU **Safe Storage**

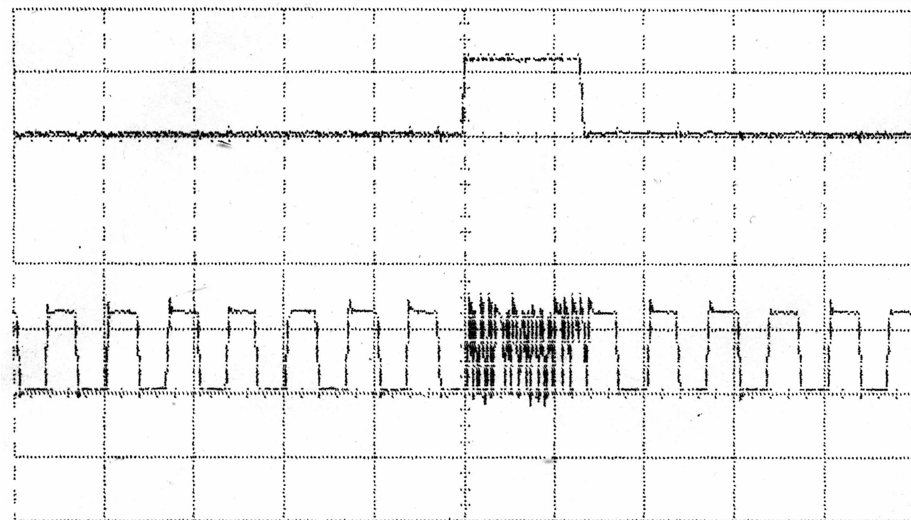
CPU state is periodically saved to safe storage (includes register file, program counter, pending memory requests, etc.)

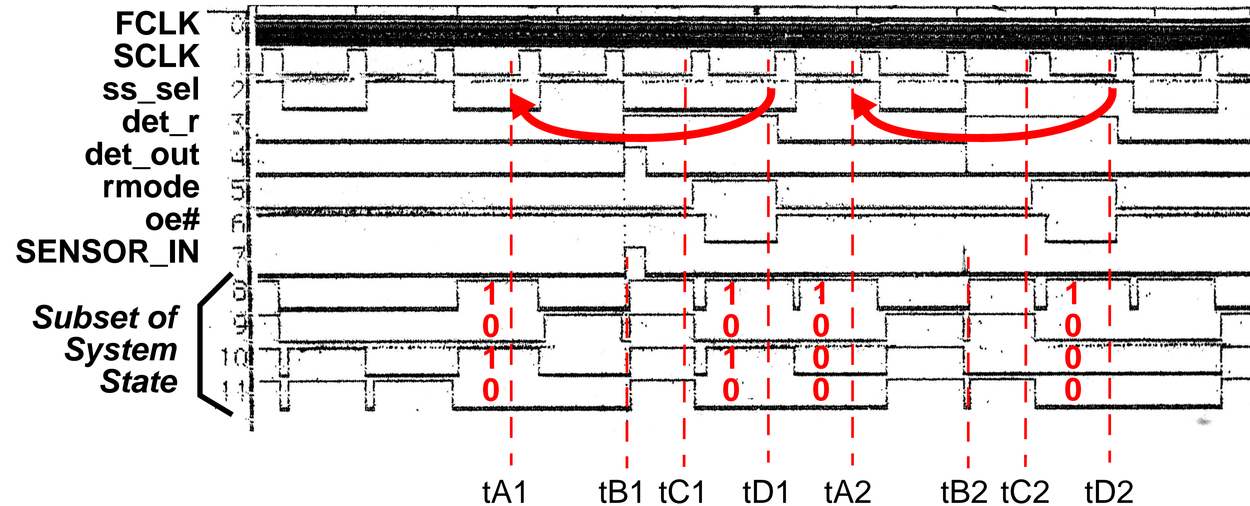
State is restored upon detection of high EMI levels

Efficient operation requires high inter-chip bandwidth (optical, 3D integration, etc.)

2D Test Board

Validation vs. Interference





Acknowledgments, etc.

INVALUABLE AID:

Todd Firestone and John Rodgers

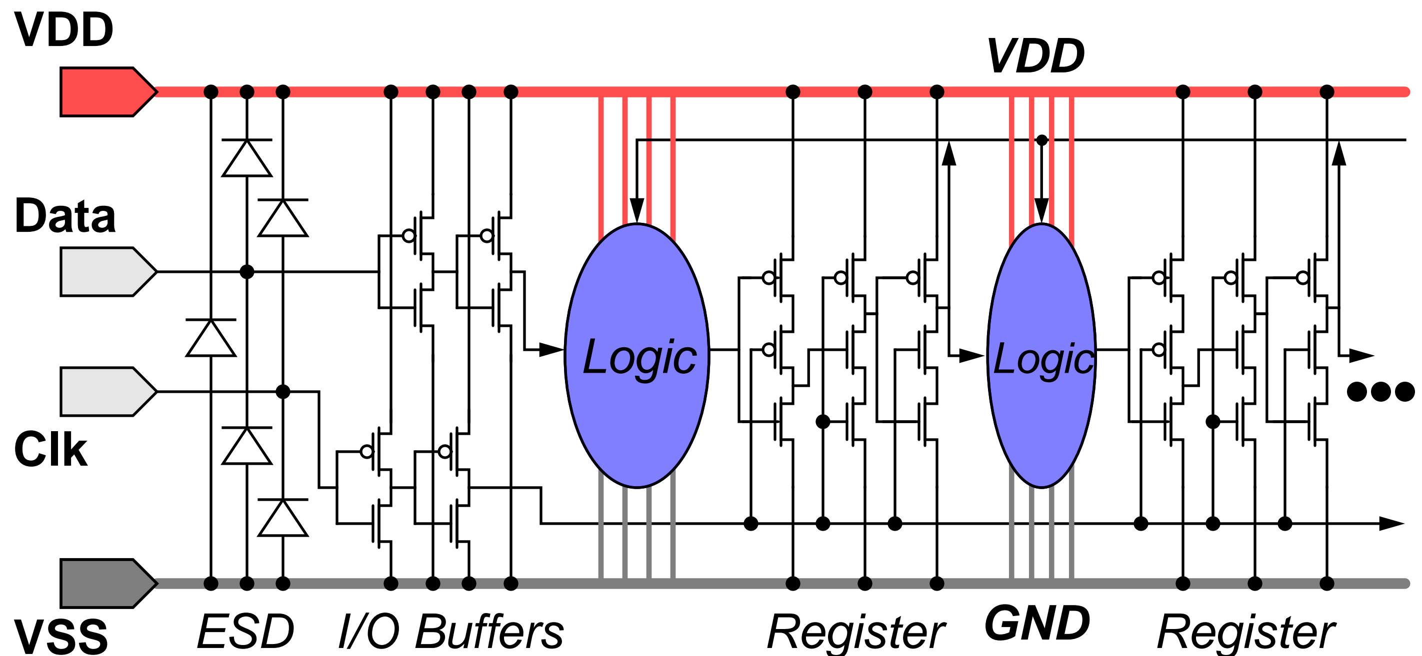
PUBLICATIONS:

- **“Energy/power breakdown of pipelined nanometer caches (90nm/65nm/45nm/32nm),” S. Rodriguez and B. Jacob, *ISLPED*. October 2006.**
- **“Electromagnetic interference and digital circuits: An initial study of clock networks.” H. Wang, S. Rodriguez, C. Dirik, and B. Jacob. *Electromagnetics*, vol. 26, no. 1, pp. 73-86. January 2006.**
- **“TERPS: The Embedded Reliable Processing System.” H. Wang, S. Rodriguez, C. Dirik, A. Gole, V. Chan, and B. Jacob. *ASP-DAC*. January 2005.**
- **“Radio frequency effects on the clock networks of digital circuits.” H. Wang, C. Dirik, S. Rodriguez, A. Gole and B. Jacob. *EMC*, pp. 93-96. August 2004.**

BACKUP SLIDES

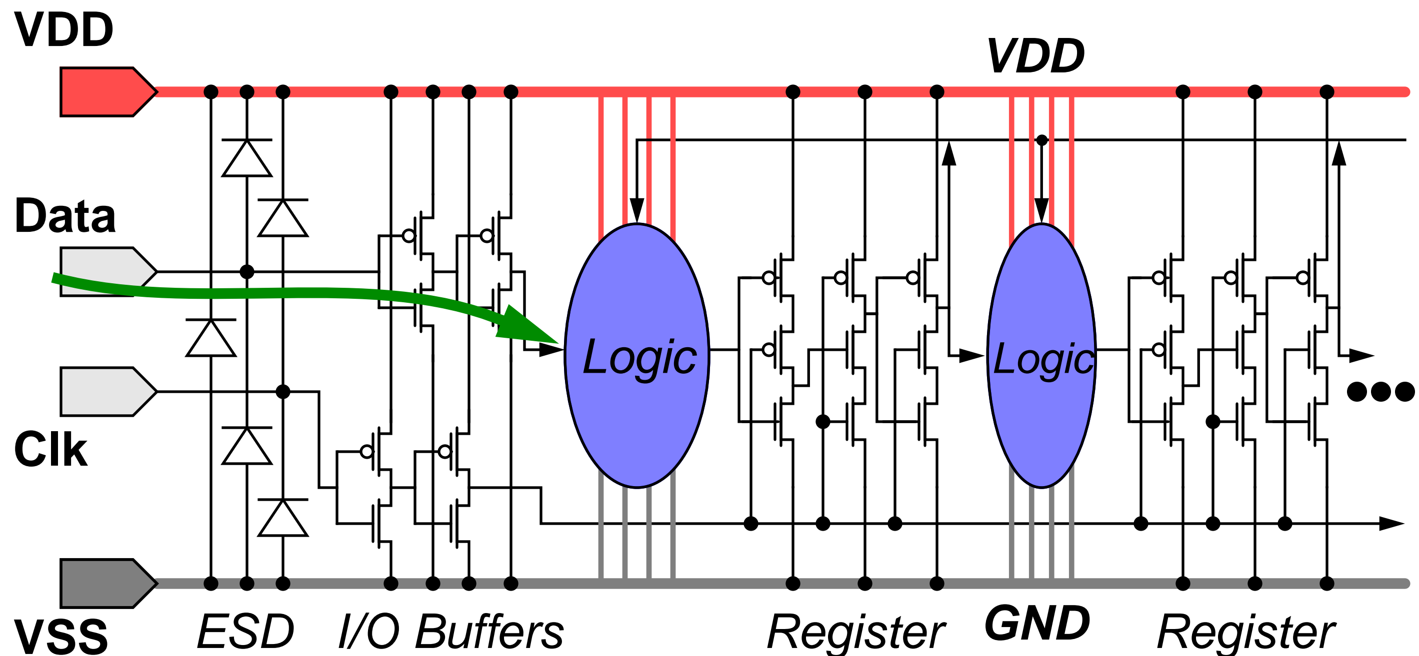
Primer: Digital Systems

How To Make This System Fail …



Primer: Digital Systems

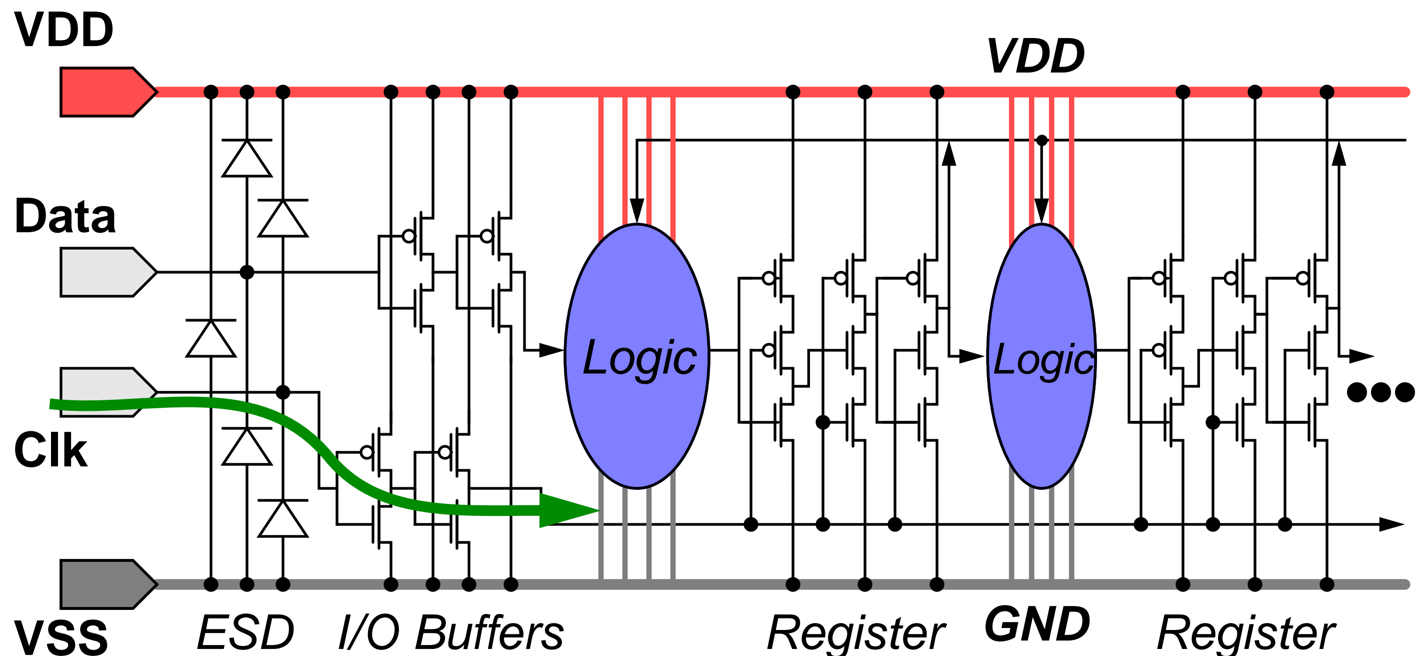
How To Make This System Fail … DATA



- **RF that makes it this far (past initial I/O buffers) has corrupted the system: only solution is to use higher level bus- or packet-encoding techniques**
- **Corrupted data can lead to incorrect results, software crash/reboot, transmission to remote nodes, etc.**

Primer: Digital Systems

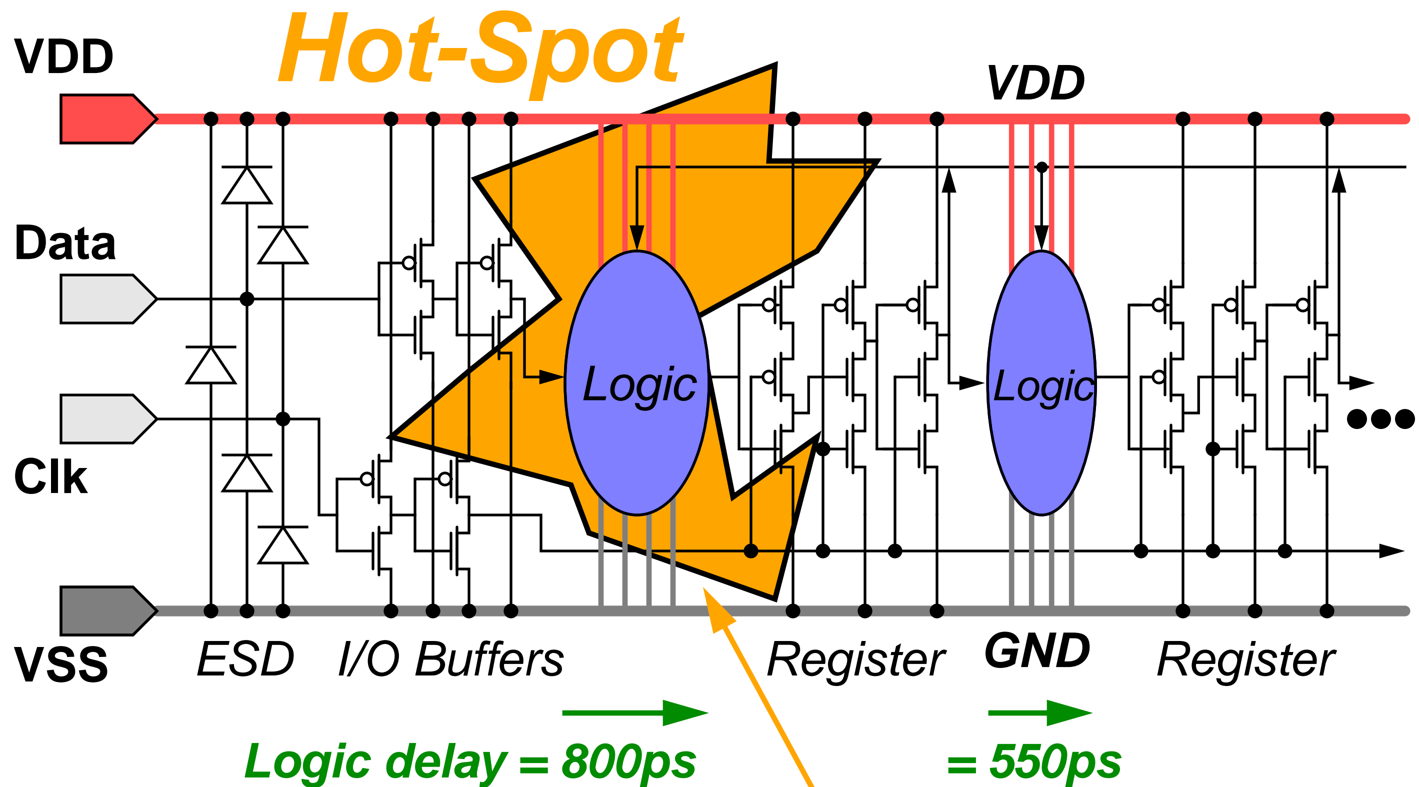
How To Make This System Fail … CLOCK



- RF that makes it this far (past initial I/O buffers) has corrupted the system: packet-encoding techniques that might detect data corruption are inapplicable
- Unwanted clock edges likely result in metastability, lead to incorrect results, most likely system crash

Primer: Digital Systems

How To Make This System Fail … CLOCK

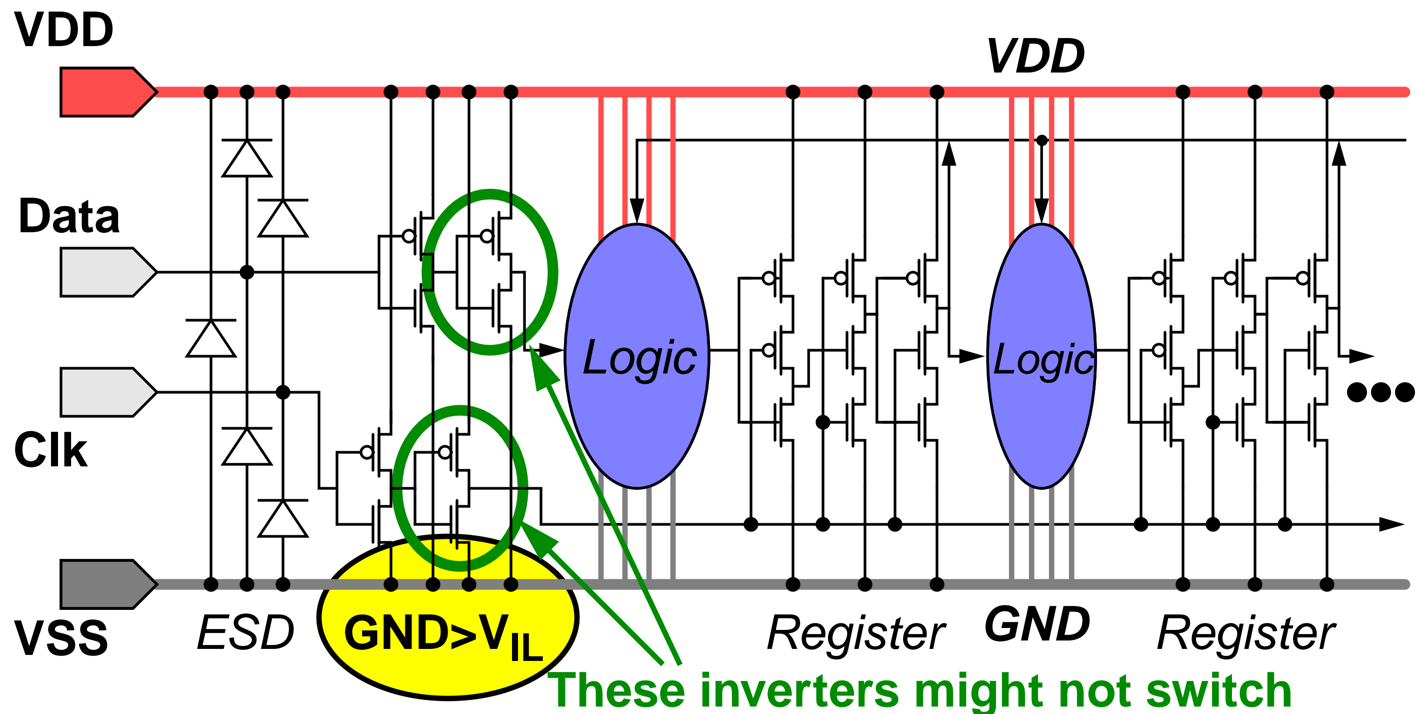


This portion of the system logic heats up, experiences more delay than other areas

- **Thermal gradients in synchronous systems disastrous (consider tight timing margins in GHz systems)**

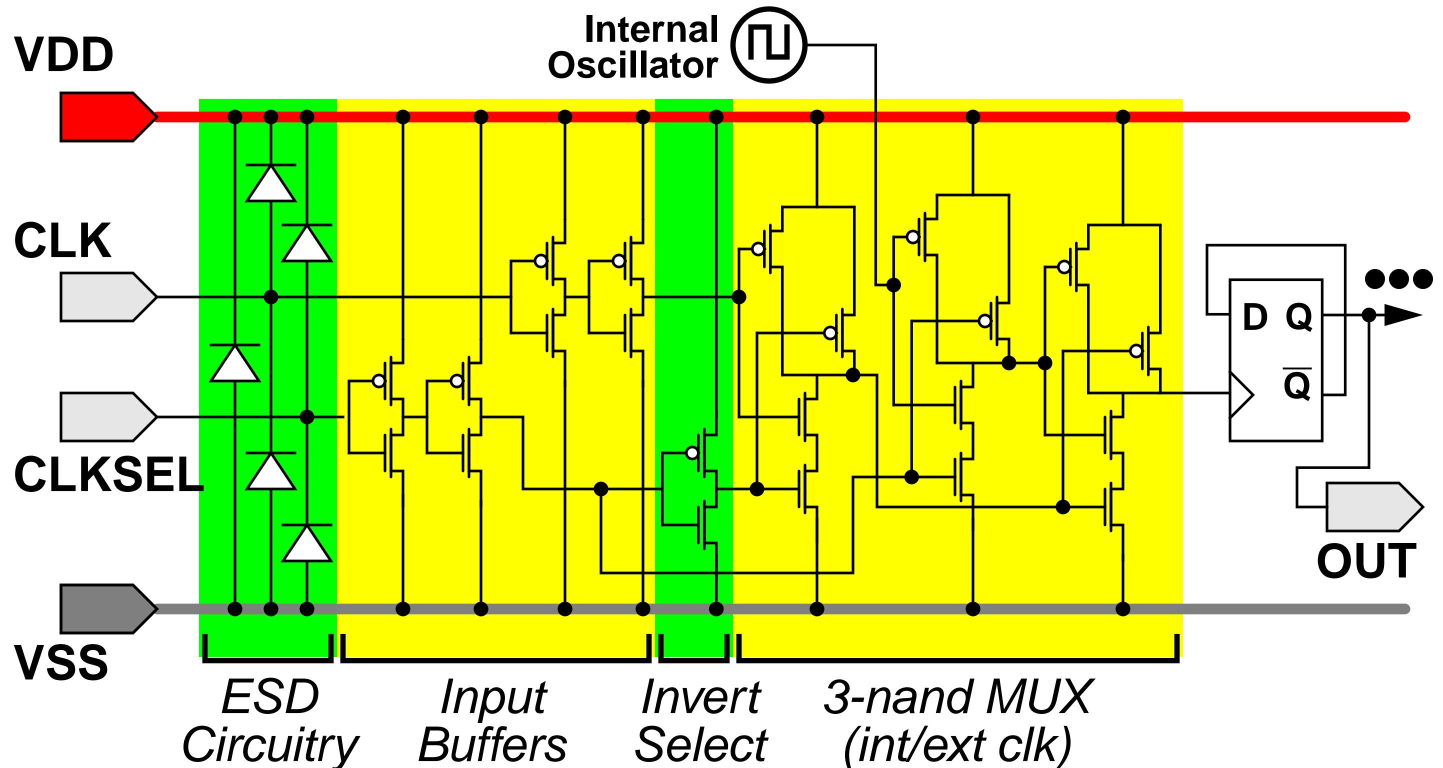
Primer: Digital Systems

How To Make This System Fail … VDD/VSS



- Localized (or global) ripples on groundplanes can cause logic to misbehave, inputs to be misinterpreted (e.g. suppose Data/Clk = 1, V > V_{IL} on gate of 2nd INV)
- Causes same effects as data/clock corruption

DUT Circuit Perspective

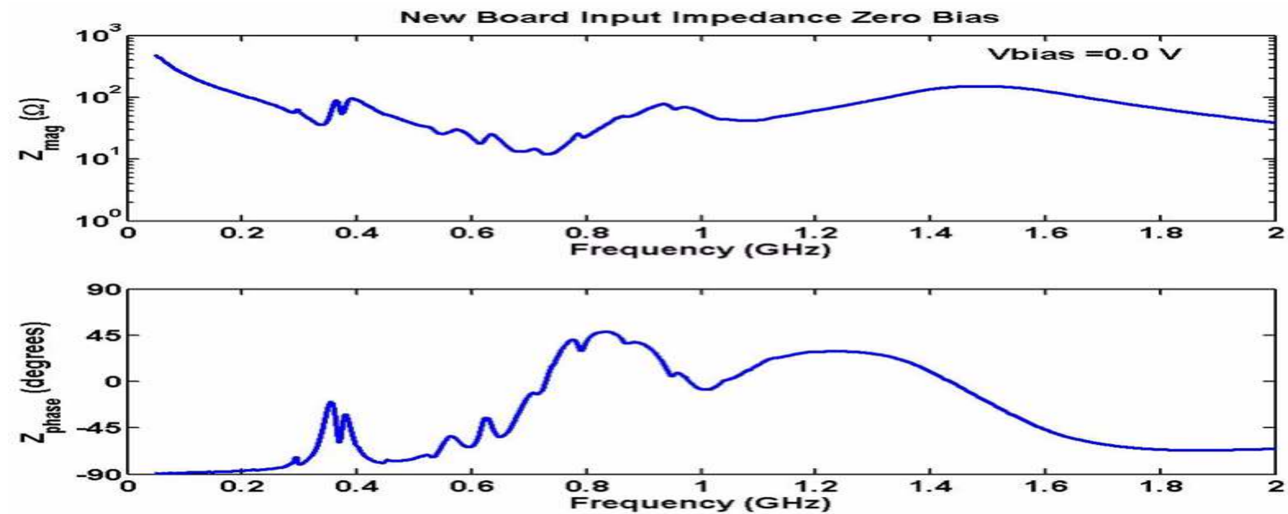


Points of Interest:

- **Digital system built from complementary gate designs (high input impedance, low output impedance).**
- **CLK only driving MUX, one DFF (*see previous slide*).**
- **=> CLK and CLKSEL see virtually identical loads.**

Input Impedance

CLK pin



CLKSEL (data) pin