Dependability and Security Challenges in Emerging Technologies

Jacob A. Abraham

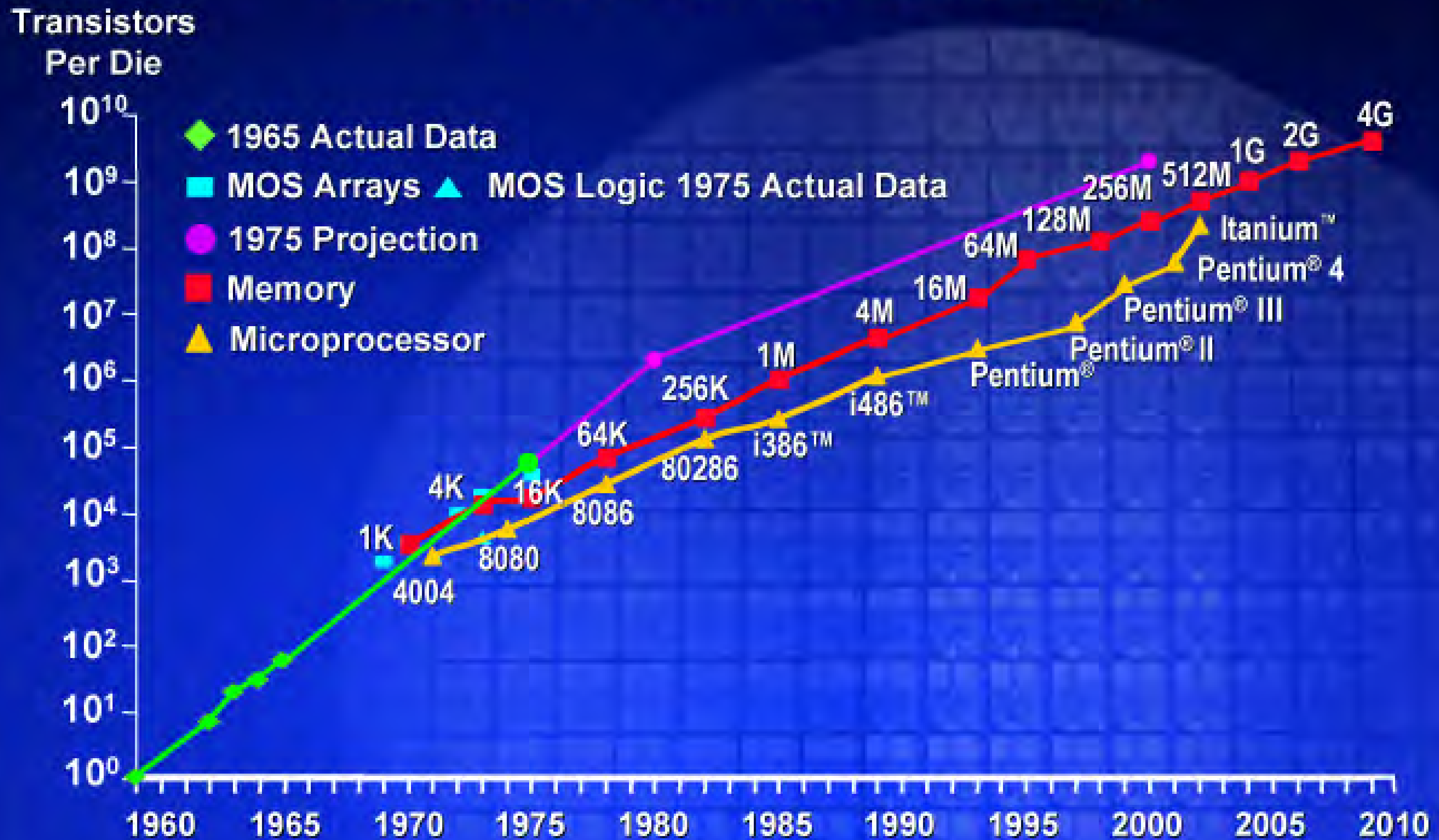
University of Texas at Austin

Workshop Panel

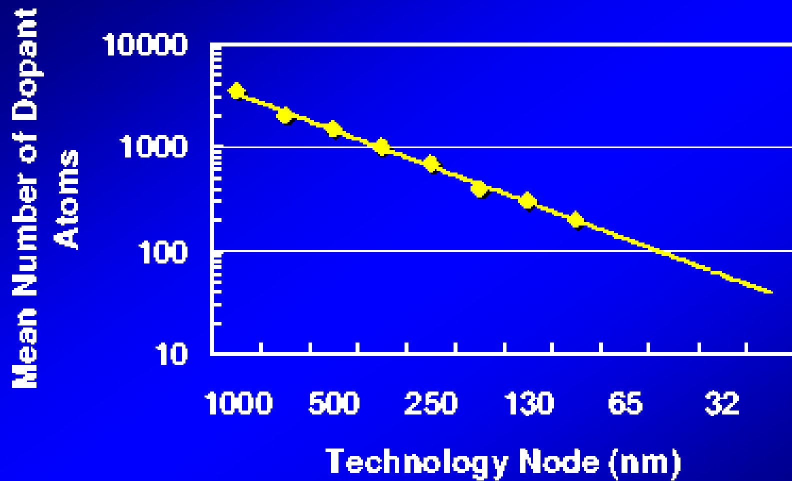
June 28, 2007

Nanoscale CMOS Trends

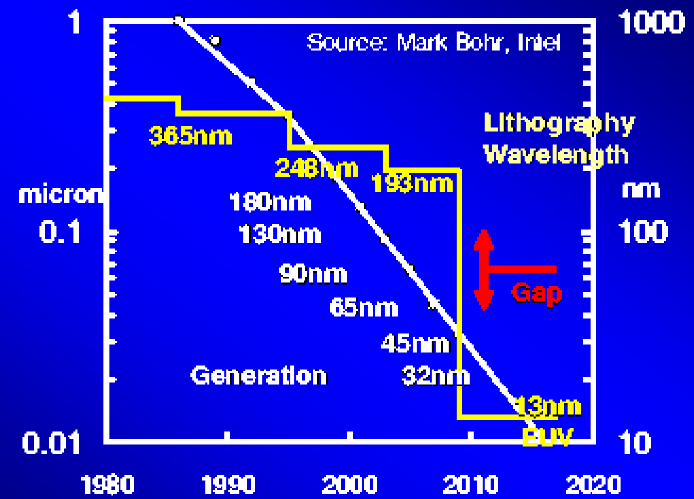
Moore's Law



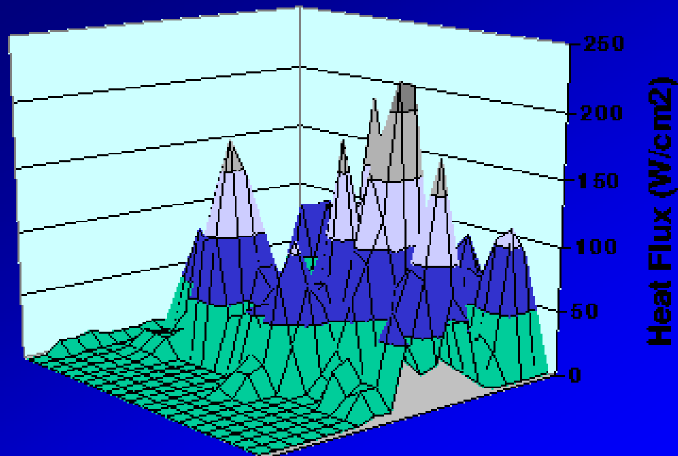
Process Variations



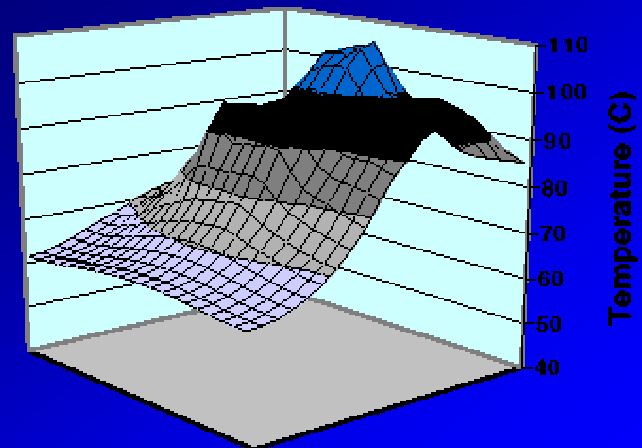
Random Dopant Fluctuations



Sub-wavelength Lithography



Heat Flux (W/cm²)—Vcc variation

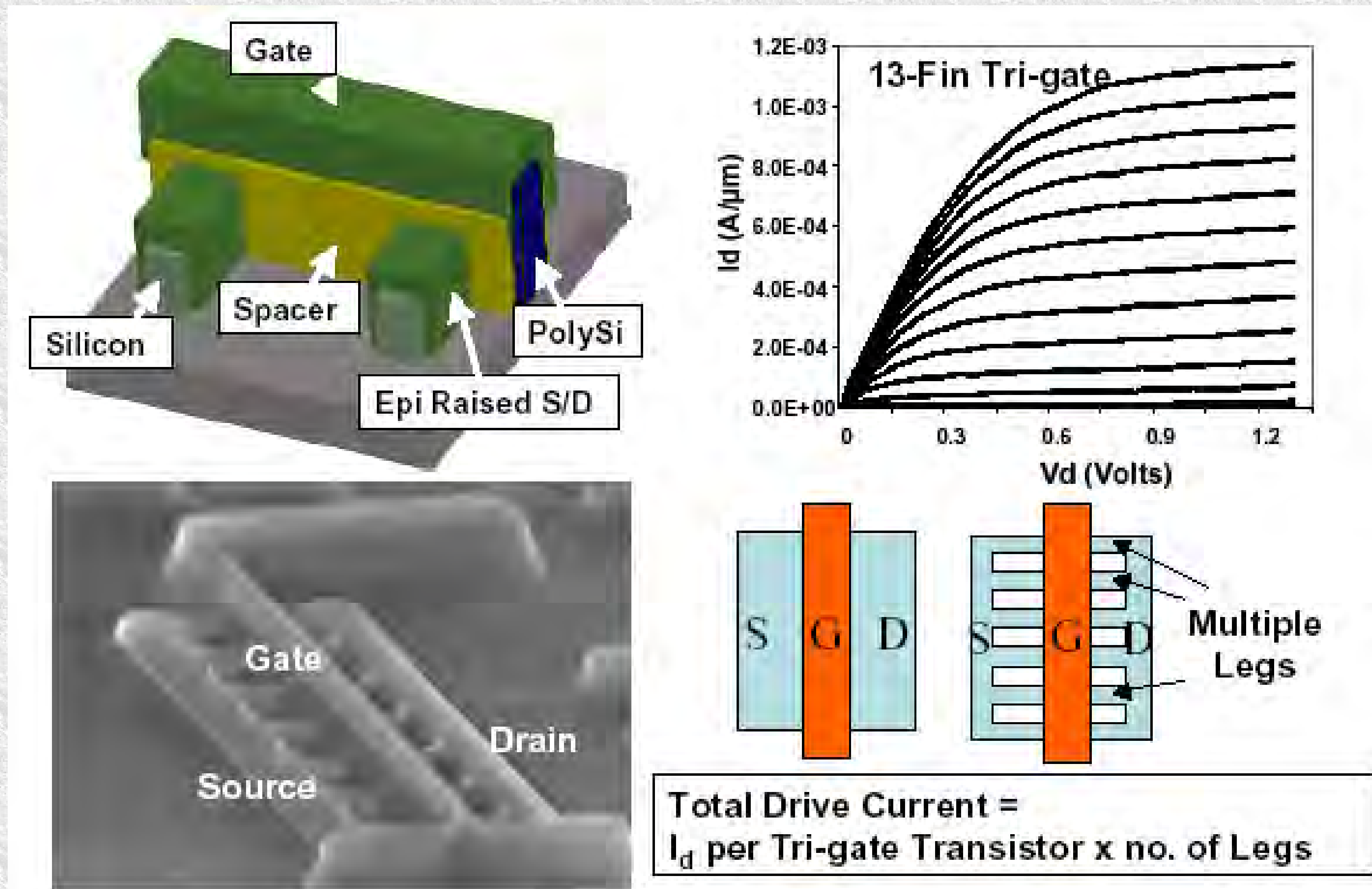


Temp Variation & Hot spots

Source: Intel

Nanoscale CMOS Example

Fin-FETs

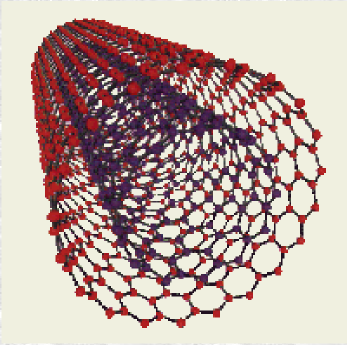


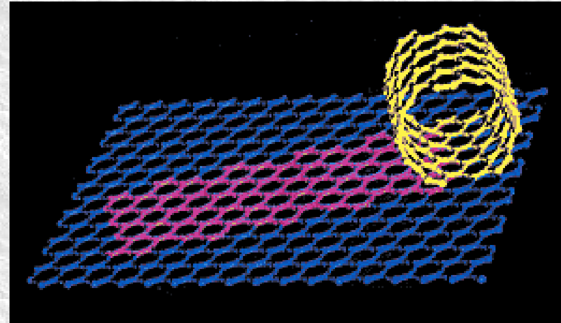
Effects on Circuits and Systems

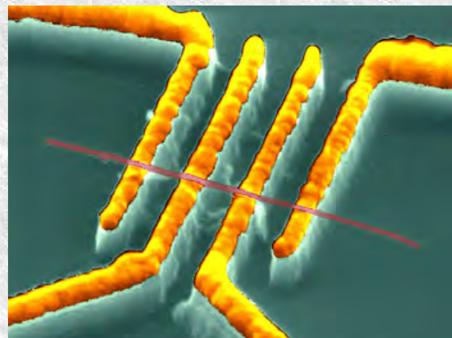
- Experiments on **chips today** show that running some chips at rated speeds produce errors
  - Correct operation when running at normal speeds
- Resistive opens (possible in copper interconnect) cause delay defects
- Crosstalk effects could also cause errors
- As technology scales down, **chips in the future** prone to erroneous operation due to:
  - **Process variations (soft errors)**
  - **Increasing defects (today's memories are an example)**

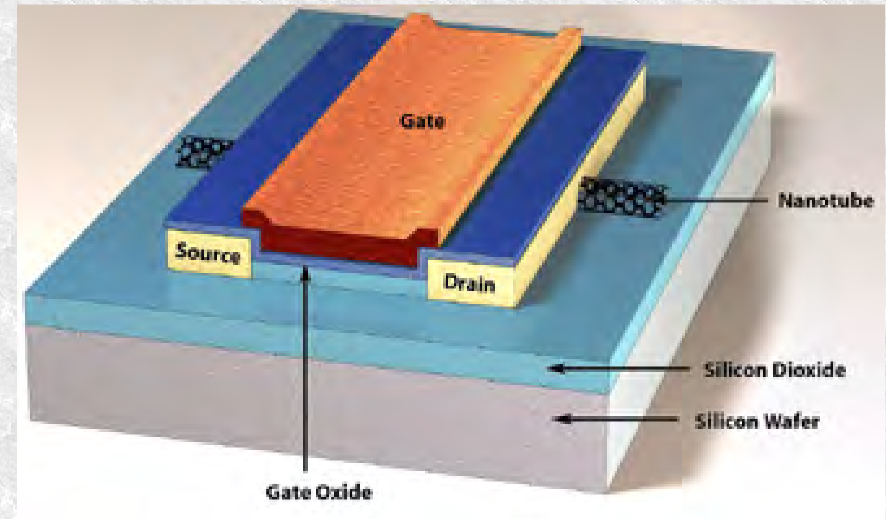
New Nano Systems

Carbon Nanotubes

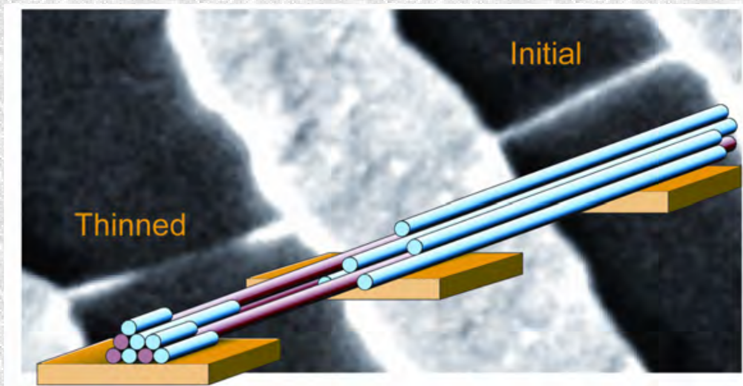


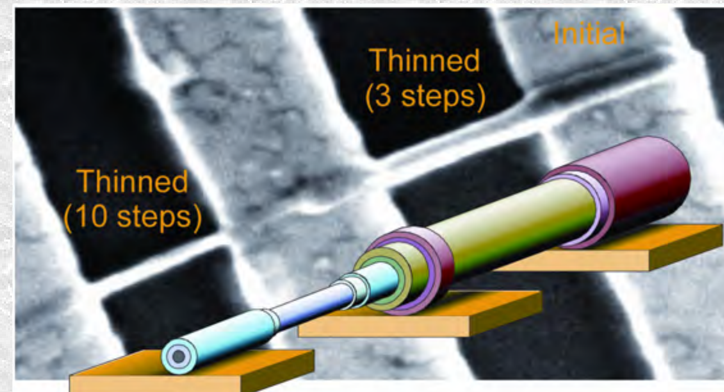






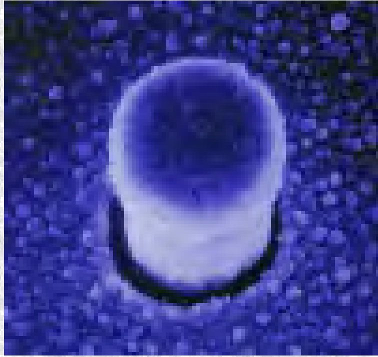
Courtesy: IBM

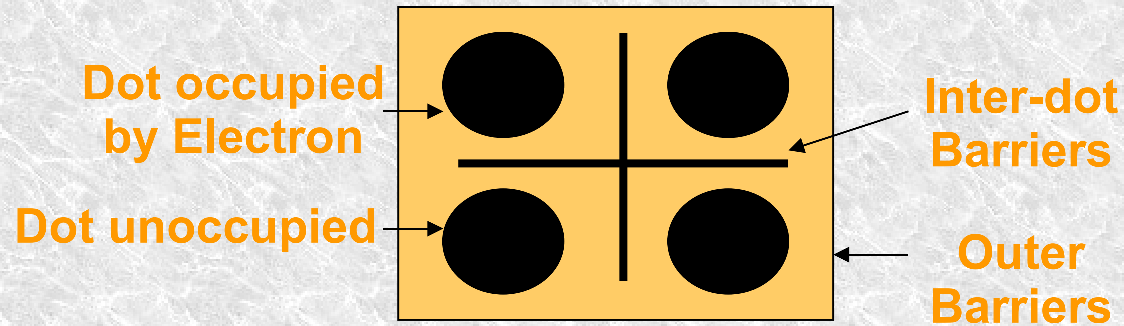




New Nano Systems

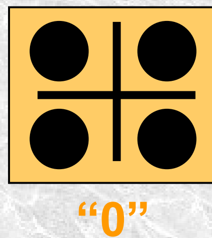
Quantum Devices



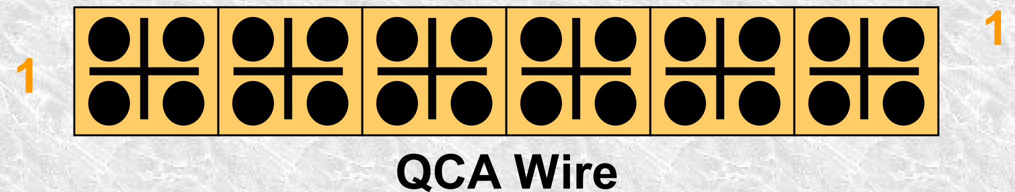


Quantum Cellular Automata

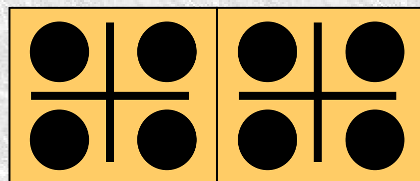
"1"



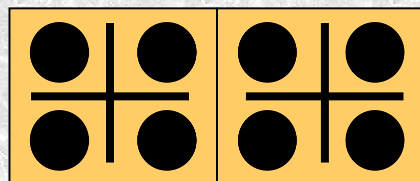
"0"



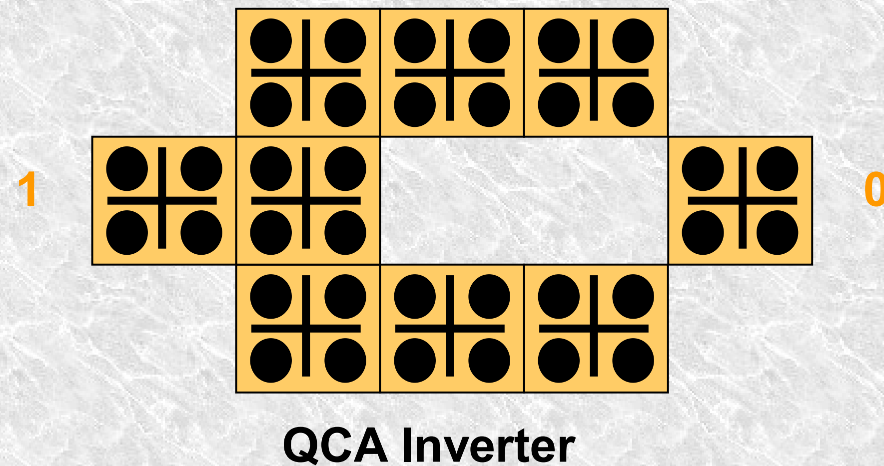
QCA Wire



Stable



Unstable



QCA Inverter

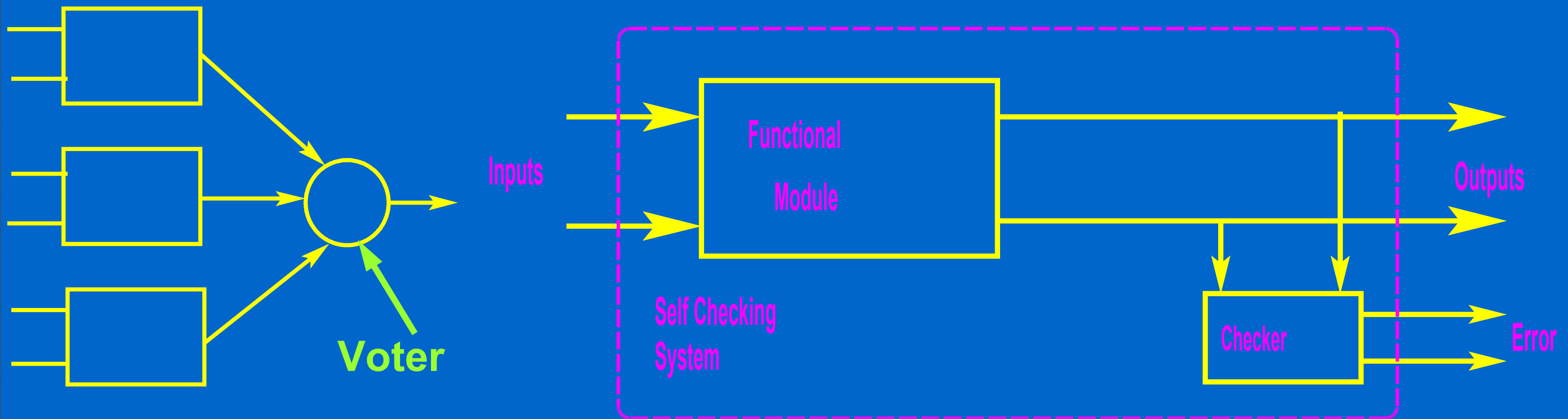
Dealing with Errors

- Redundancy
  - Hardware (duplication/retry, triplication)
  - Time (recomputation)
- **Basic ideas in dealing with errors are not new**
- Moore and Shannon, 1956:
  - "Reliable Circuits Using Less Reliable Relays"
- von Neumann, 1956:
  - "Probabilistic Logic and the Synthesis of Reliable Organisms from Unreliable Components"
- Self-checking circuits (1970s)
- Algorithm-based fault tolerance (1980s)
- Software-based checks (control flow checks, etc.) (1980s)

Redundancy at Different Levels

Switch (Circuit) level

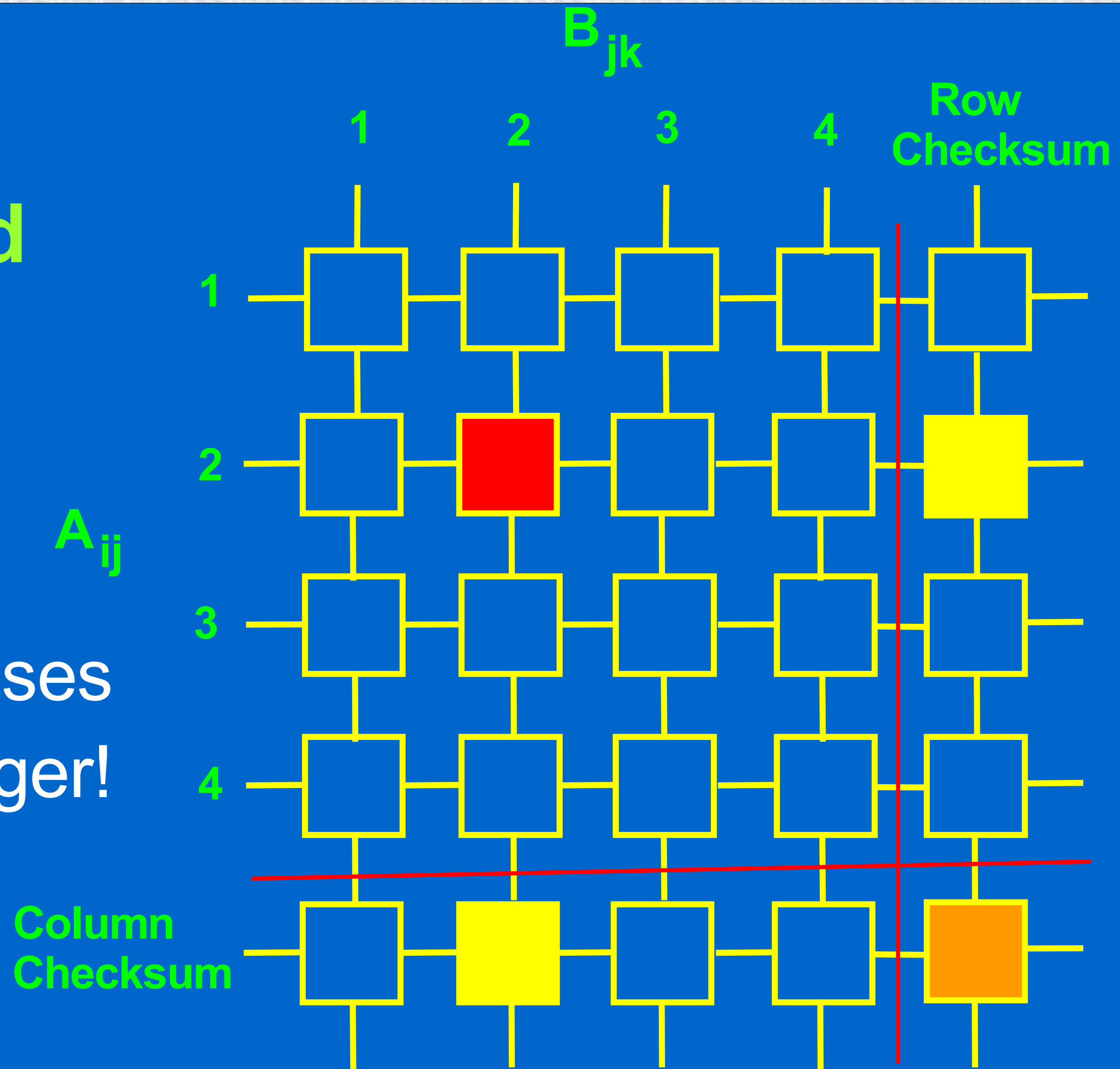
Module level



Protecting Computations at the System Level

Algorithm-Based Fault Tolerance

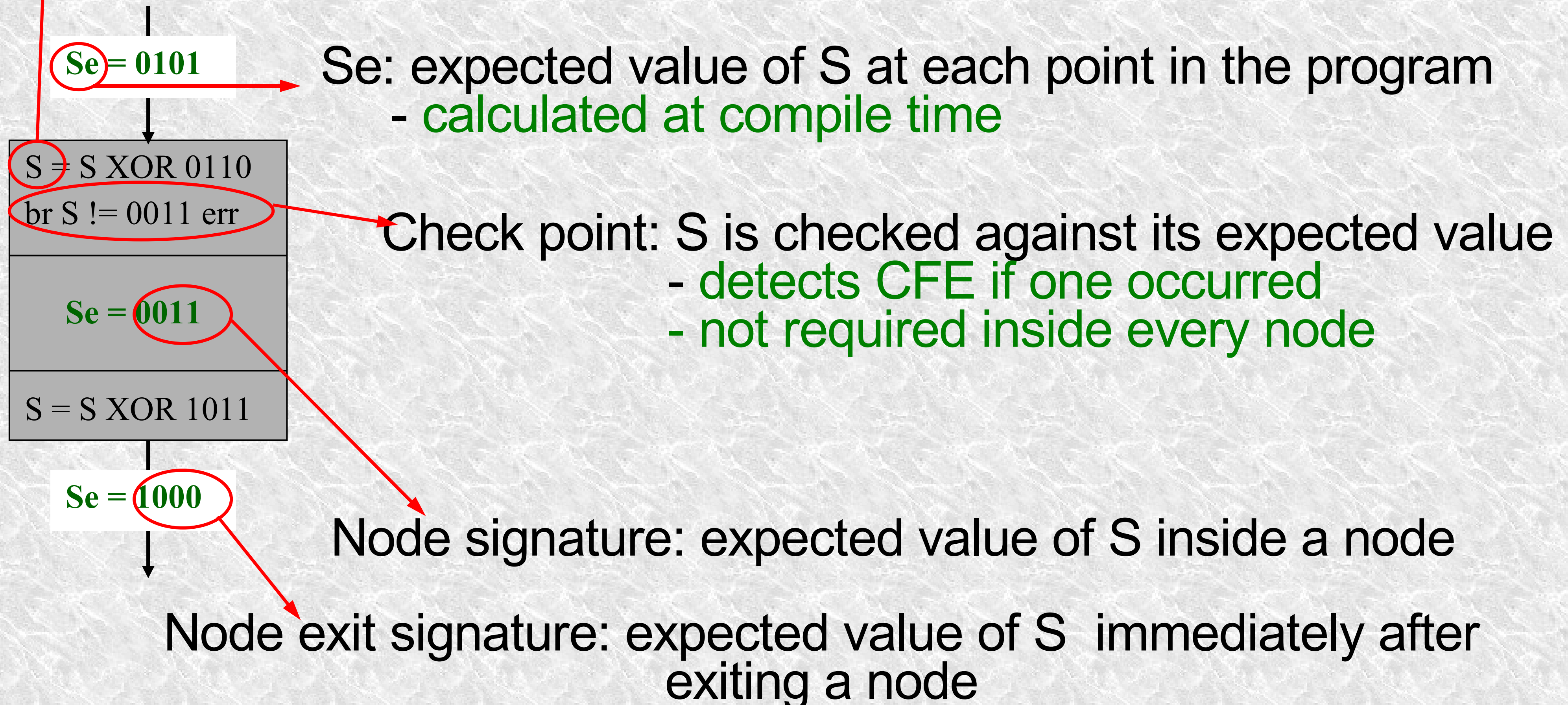
Overhead decreases as system gets larger!



CEDA: Control-flow Error Detection through Assertions (Integrated with GCC)

S: global runtime signature register

- updated at the beginning and end of each node
- each update either an XOR or an AND operation
- op. performed based on the program graph properties

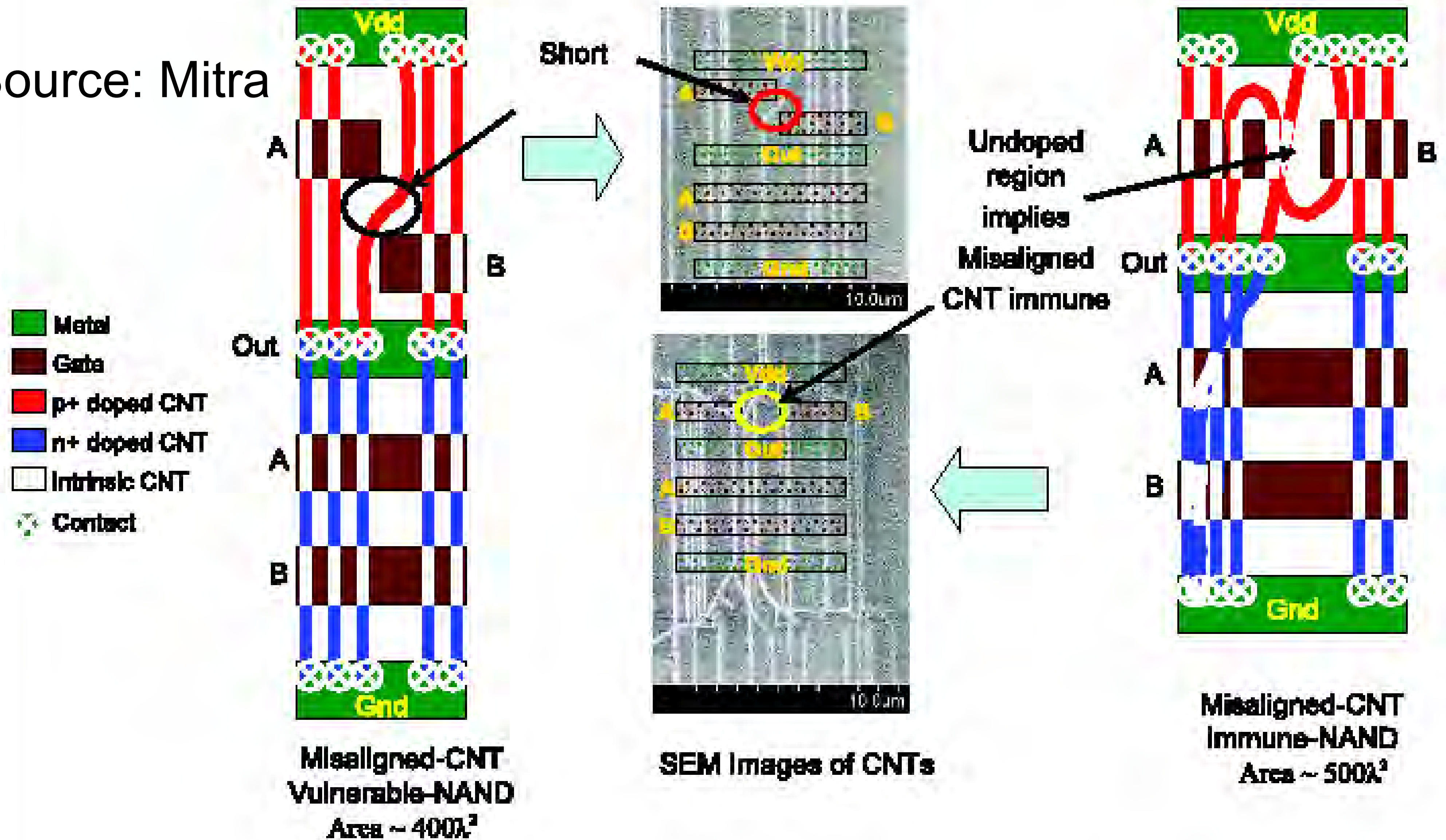


Dealing with Faults

- Increasing possibility of defects
- **Defect tolerance key for yield**
- **Want system to start in a good state**
  - Cannot produce cost-effective DRAMS without replacing faulty cells with spares
  - However, sparing cells is much more difficult for logic (very high cost for multiplexers, routing)

Defect Tolerance in Carbon Nanotube Circuits

Source: Mitra



Misaligned-CNT Vulnerable-NAND Area ~ $400\lambda^2$

SEM Images of CNTs

Misaligned-CNT Immune-NAND Area ~ $500\lambda^2$

What are some of the characteristics of future products?

Low-cost consumer products

High frequency, high resolution signals

System service (what matters is what customer sees)

Regulations

Market Size (B$)

1400
1200
1000
800
600
400
200
0

1991
'93
'95
'97
'99
2001
'03
'05
'07
'09
'11

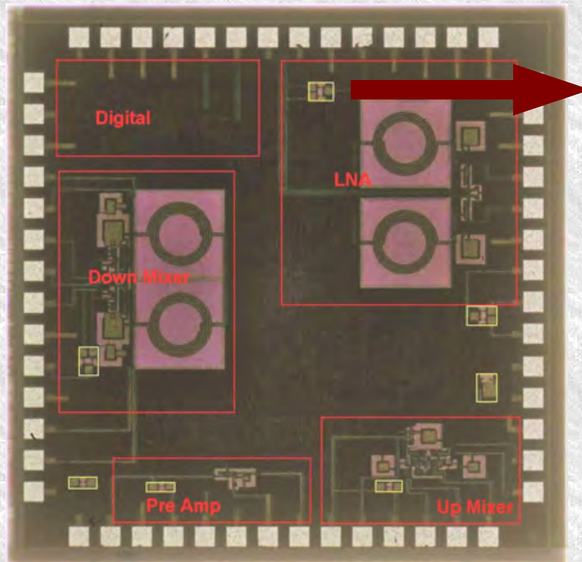
MS-SOC Contribution to the SoC Market Size

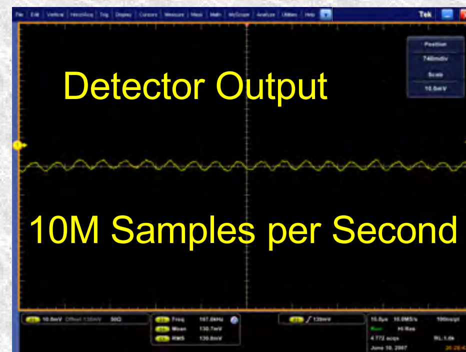
World Wide Semiconductor Market Size

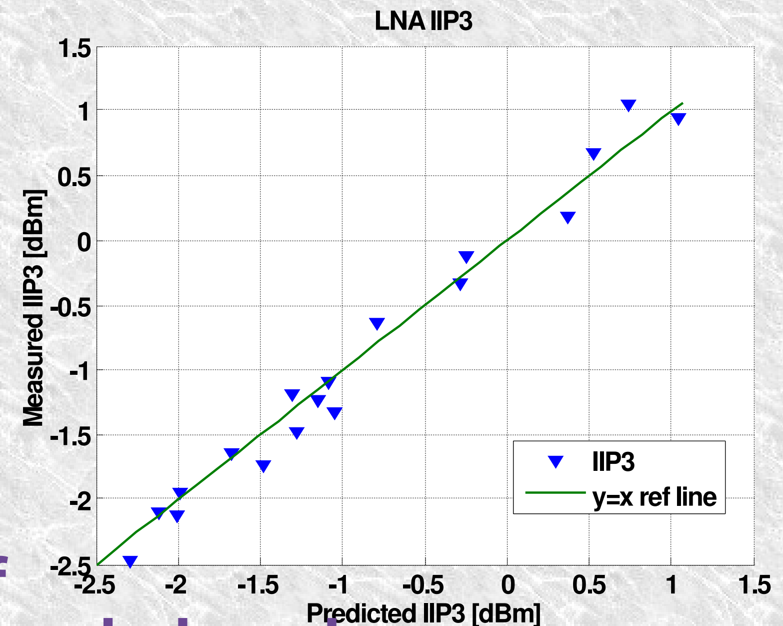
SoC Market Size

Objective of dependability

- **Guarantee that the system meets customer or regulatory specifications**
- Need not check **directly** for the specifications
  - This is becoming impossible to do with low cost
- Only solution for systems of the future is **indirect** checks from which the specifications can be inferred accurately







Third harmonic of 940 MHz RF system deduced from 10 MS/sec detector output

Conclusions

- Need to deal with soft errors (due to variations, etc.)
  - Detection and correction techniques
- Tolerate defects in manufacture
  - Lots of devices, but efficiently using them is key
- Level to apply solutions?
  - Usually higher levels are better
  - May find good solutions at low levels, too
- Can utilize many “old” techniques
- Need to look for “new” techniques