Nanoscale Technologies: Prospect or Hazard to Dependable and Secure Computing?

Jean Arlat

[jean.arlat@laas.fr]

Third IEEE/SBC/SMCC Latin-American Symp. on Dependable Computing
Morelia, Mexico — September 26-28, 2007

Context and Rationale

- Much less attention paid on hardware-related issues within FTCS/DSN, at the turn of the century…
- These issues are becoming an increasing concern wrt to Dependable and Secure Computing, but main players/actors are no longer within DSN…
- It appears essential to explicitly recognize such an important trend and provide a related forum within DSN
- Workshop on Dependable and Secure Nanocomputing at DSN'07 organized together with Ravi Iyer and Michael Nicolaïdis
- Well-attended and the feedback received was very much encouraging!

Overview

- Where do we Stand?
- Manufacturing Faults
- Transient Faults in Operation
- Hardware Vulnerabilities and Security Threats
- A Proposal for Resilient Processor Architectures
  —> Piotr Zajac, Jacques Collet, Yves Crouzet (LAAS-CNRS)
- Concluding Remarks

About The Moore Law...

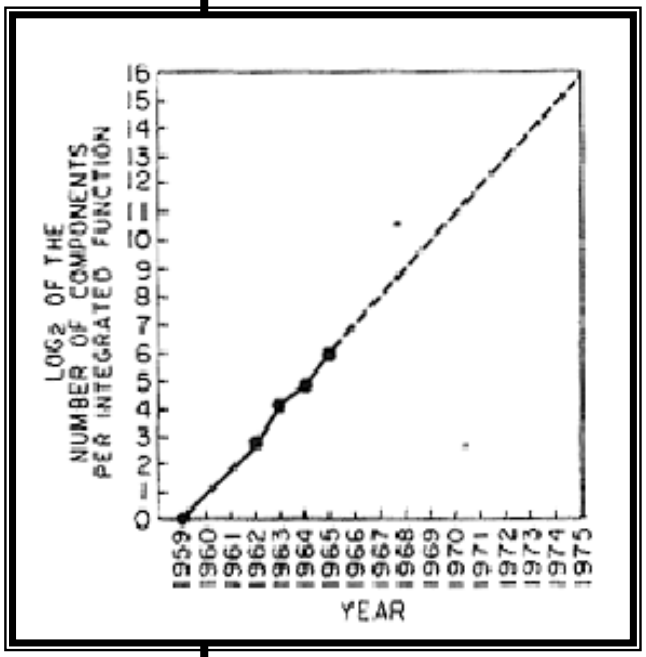
Cramming more components onto integrated circuits

Electronics, Volume 38, Number 8, April 19, 1965

With unit cost falling as the number of components per circuit rises, by 1975 economics may dictate squeezing as many as 65,000 components on a single silicon chip

By Gordon E. Moore

Director, Research and Development Laboratories, Fairchild Semiconductor division of Fairchild Camera and Instrument Corp.

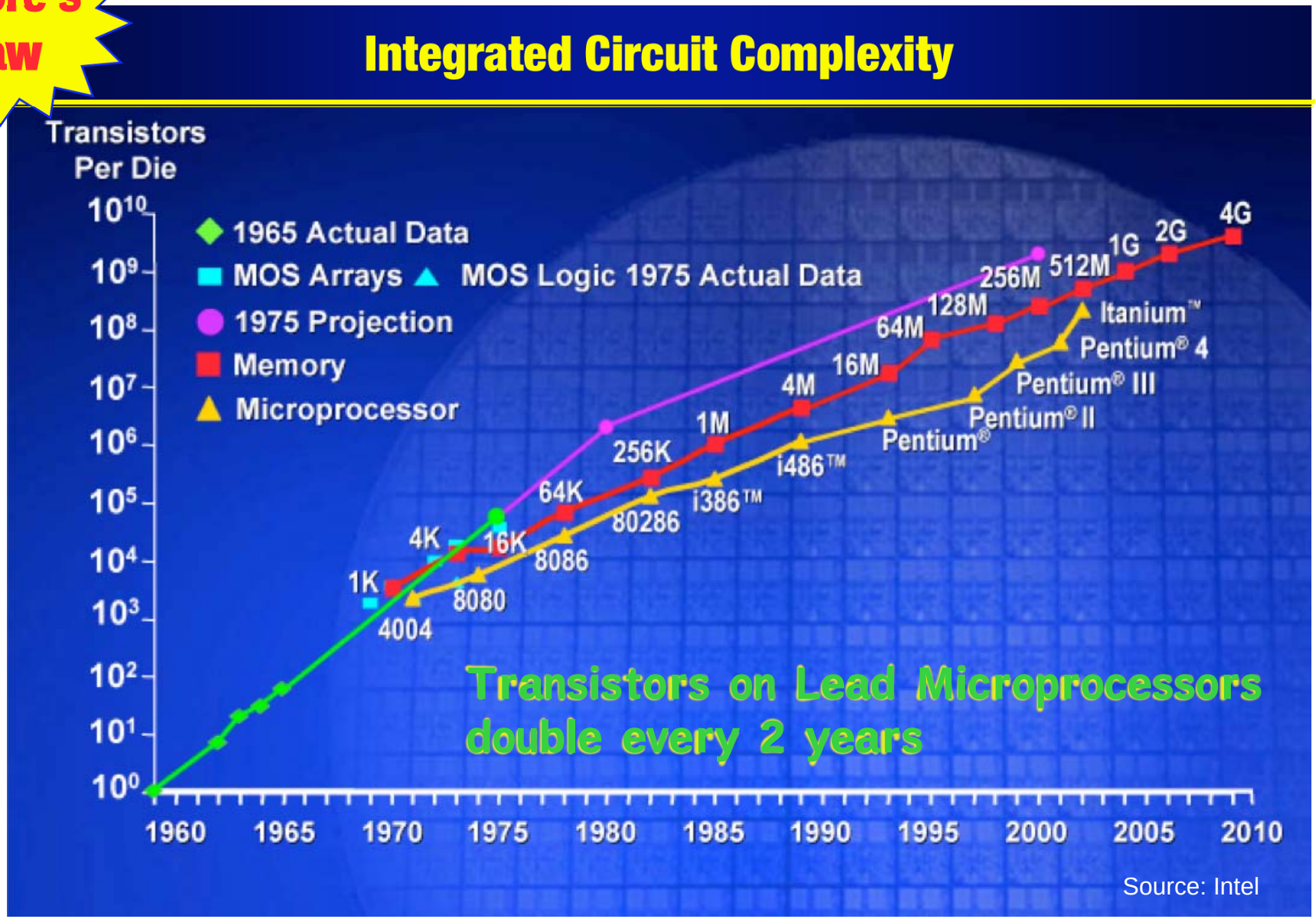


The future of integrated electronics is the future of electronics itself. The advantages of integration will bring about a proliferation of electronics, pushing this science into many new areas.

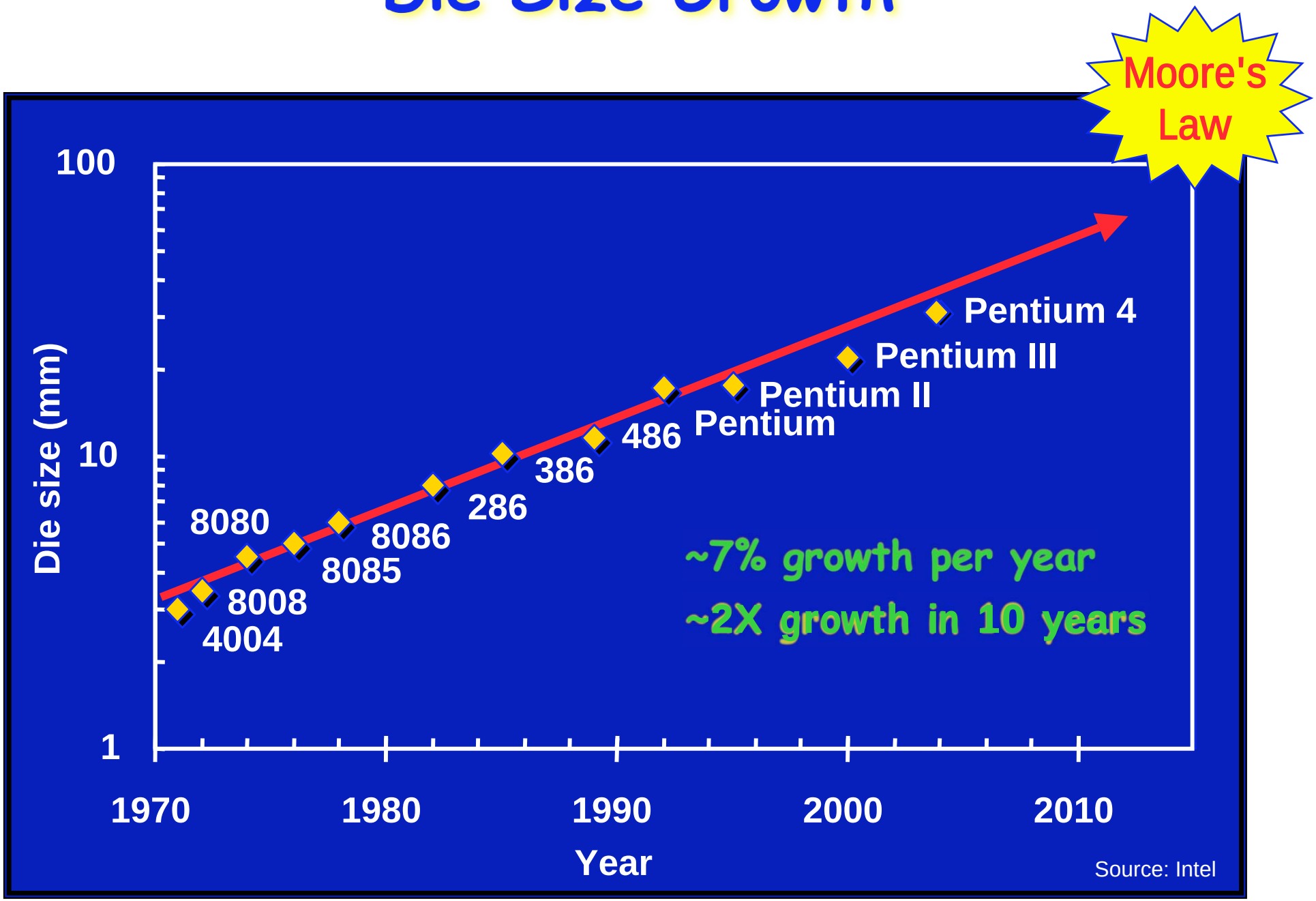
machine instead of being concentrated in a central
addition, the improved reliability made po
circuits will allow the construction of lar
Machines similar to those in existence

Trend in Transistor Size

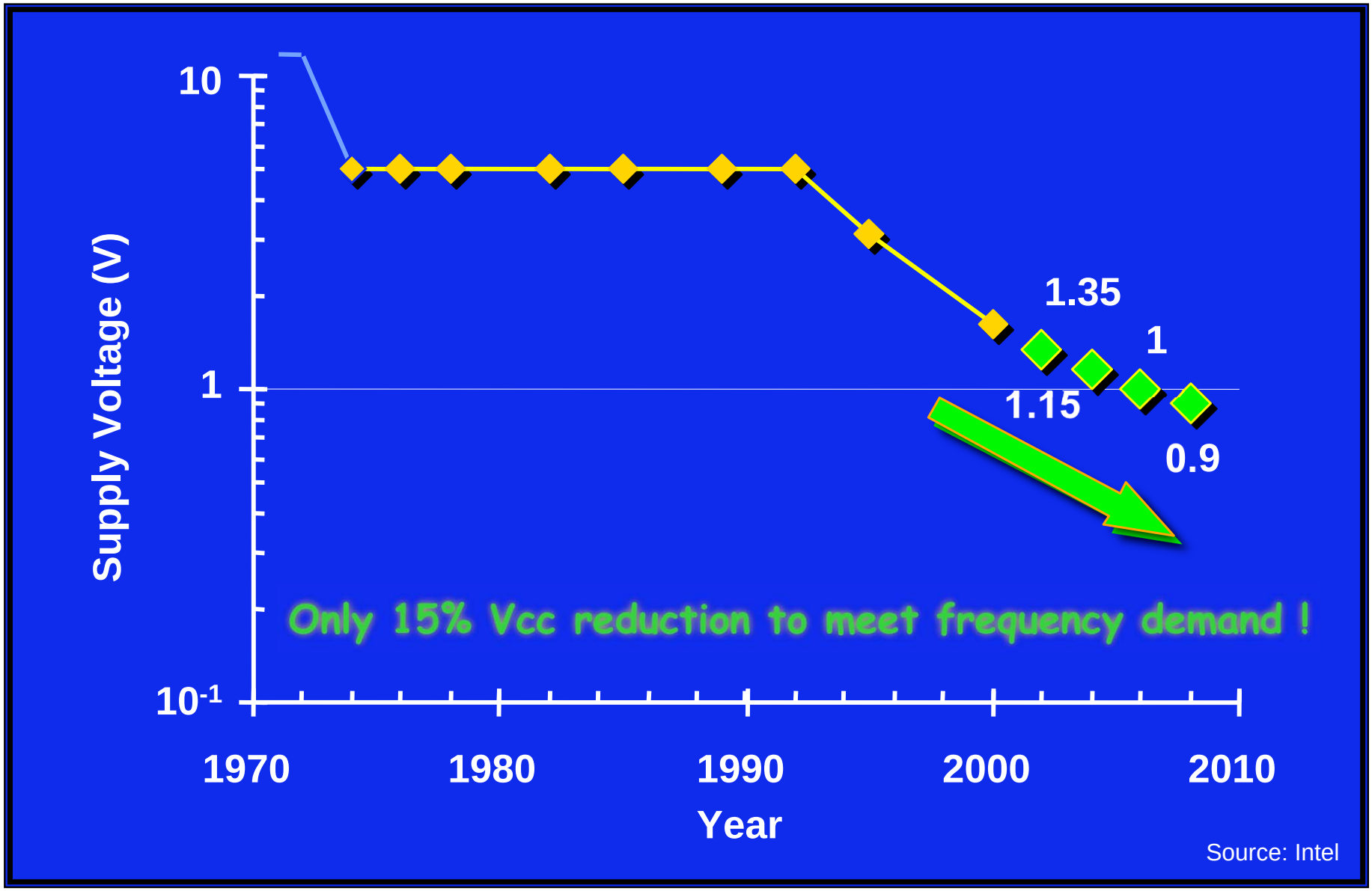
Moore's Law



Die Size Growth

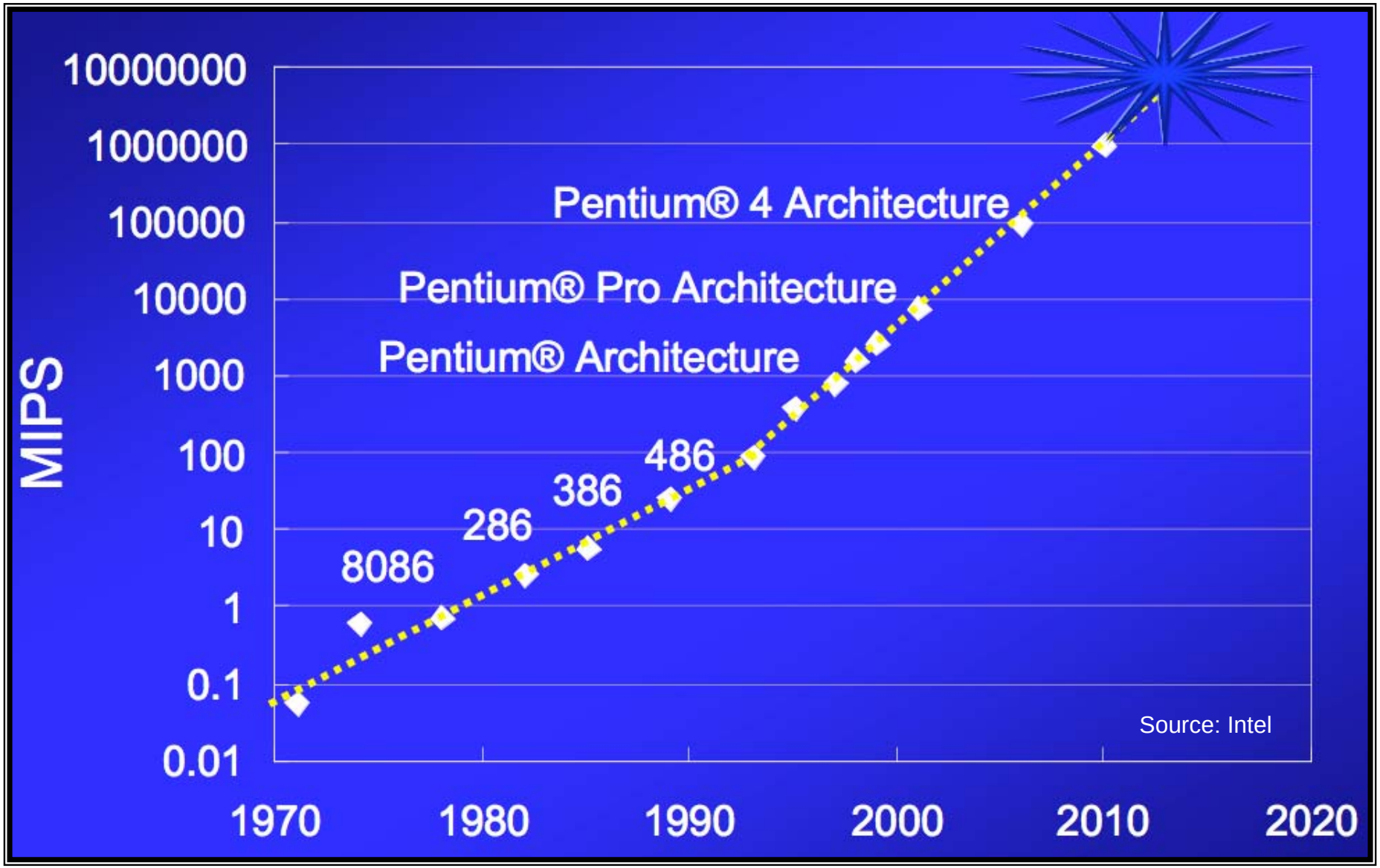


Power Supply



Trend in Microprocessor Performance

Goal: 10 TIPS by 2015 **How to get there ?**



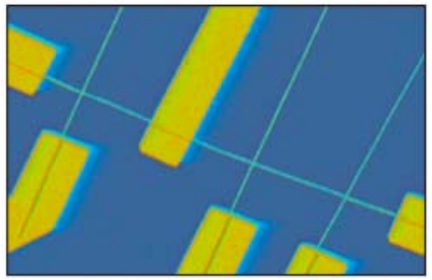
A Two-way Track…

- "More Moore": The Evolutionary Path… (top-down)
  Keep decreasing elementary device (silicon transistor) size
  —> Increasing Effect of Variations: Dopants, Threshold, Temperature, Delay, Low Signal Strength, etc.

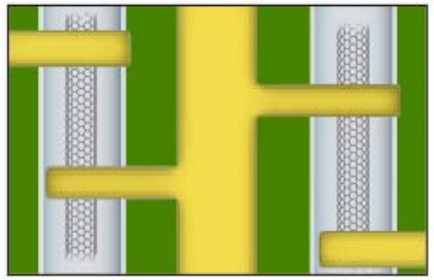
- "Beyond Moore": The Revolutionary Path… (bottom-up)
  Self-assembly of elementary devices in molecular electronics
  —> Many Major Open Issues: Signal amplification, Selective Control of Transistors, Cascading, Scalability, etc.

Nanoscale devices are inherently unreliable … and unpredictable!

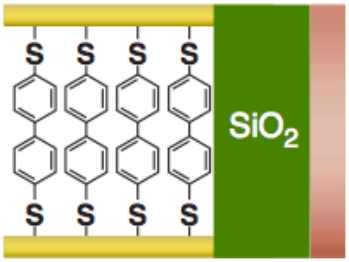
Molecular-scale Electronics (Examples)*



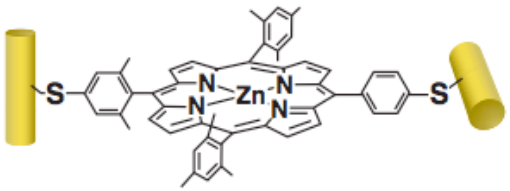
Nanowires: Diodes and transistors based on semiconductor nanowires assembled with microfluidics form AND, OR, NOR, and XOR circuits and logic functions (e.g., half adder).



Carbon NanoTubes: CNT Transistors connected by gold interconnects implement logic circuits such as: NOT or NOR circuits, static RAM cell,...



Organic molecules: Self-assembled monolayers of polyphenylene molecules form FETs that are are combined to create a NOT circuit



Biomolecules: (e.g., porphyrin molecules) store digital information as electrical charges, like dynamic RAM cells

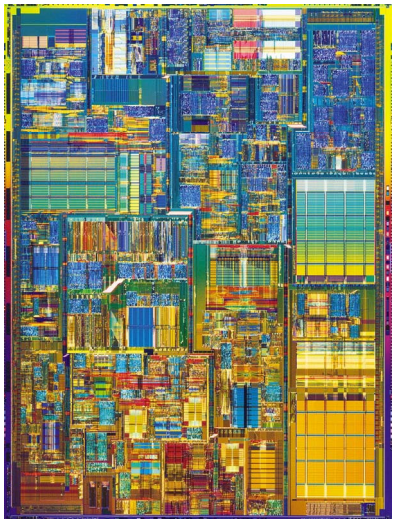
* From: G. Y. Tseng, J. C.Ellenbogen, "Towards Nanocomputers", *Science*, 294, 9 Nov. 2001, pp.1293-94

See also: T. Munakata (Ed.) "Beyond Silicon : New Computing Paradigms", *Communications of the ACM*, 50 (9), 2007, pp. 30-72

How did we get where we are today?

- **Technology improvements:**
  - Transistor size ↘; Power supply ↘; Clock frequency ↗; MIPS ↗; …
- **Architectural enhancements:**
  - RISC Scalar Architecture, Pipelining & On-die caching (Intel386,AIMPowerPC …)
  - RISC Super Scalar architecture ("multi-pipelining" and several ALUs/FPUs) and Branching prediction (Intel Pentium, AIM PowerPC970,…)
  - "Out-of-order" instruction processing — a form of data flow operation (Intel Pentium Pro, Power PC, etc.)
  - Extended pipelining stages (up to 20) introduction of execution trace cache and hyper-threading (Intel Pentium 4)

Evolution of Die Architectures and Sizes

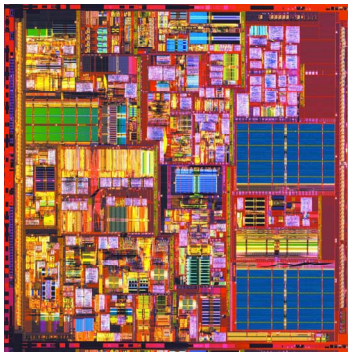


Core P4 “Willamette”

Technology: 180 nm

Size: 15.7mm x 13.8mm

2000-2001

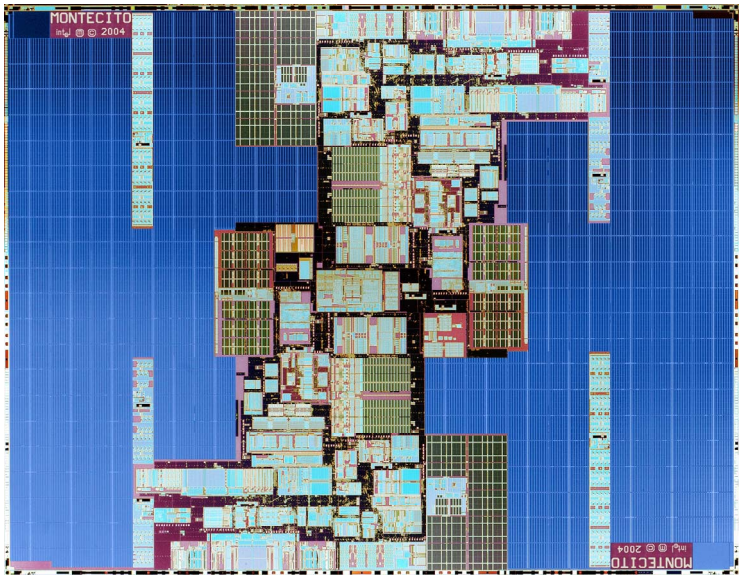


Core P4 ”Northwood”

Technology: 130 nm

Size: 11.27mm x 11.27mm

2002

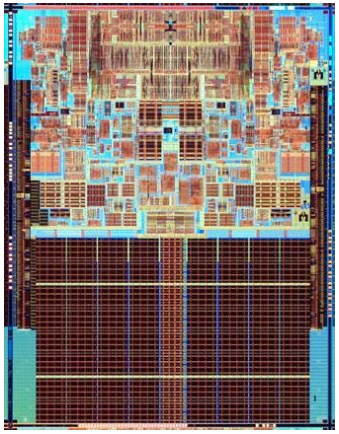


Dual Core Itanium “Montecito”

Technology: 90 nm

Size: 21.5mm x 27.72mm

July 2006



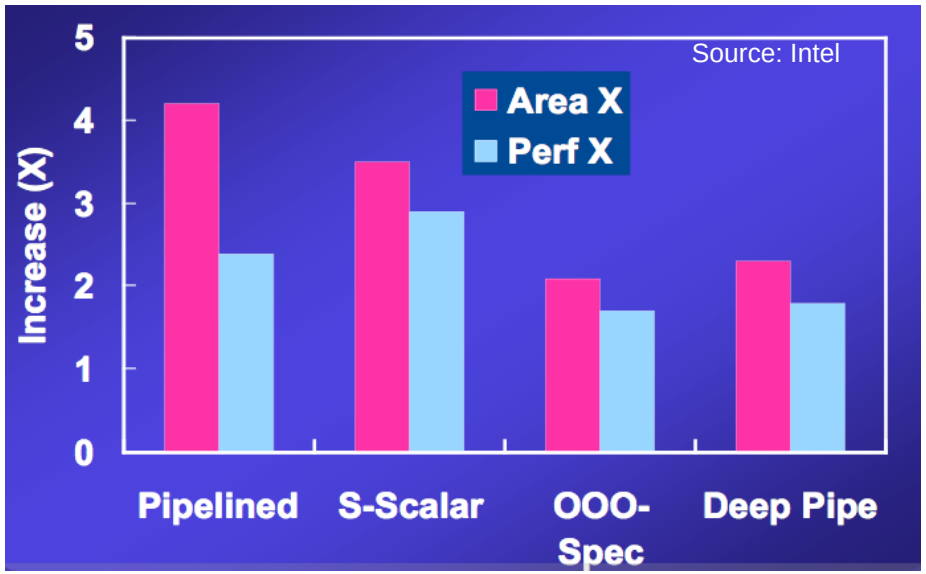
Core 2 Duo “Conroe”

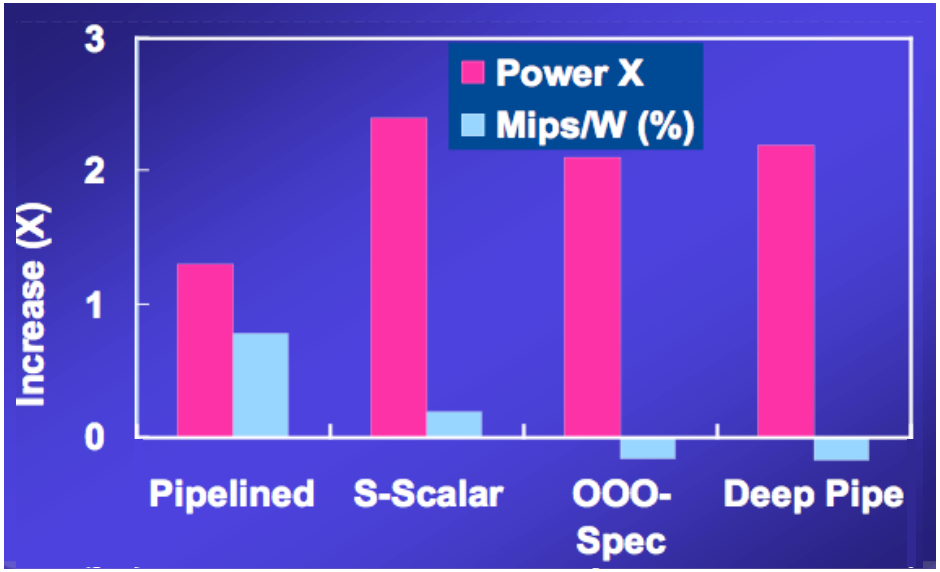
Technology: 65 nm

Size ≈ 13mm x 11mm

July 2006

What About Area & Power Efficiency?

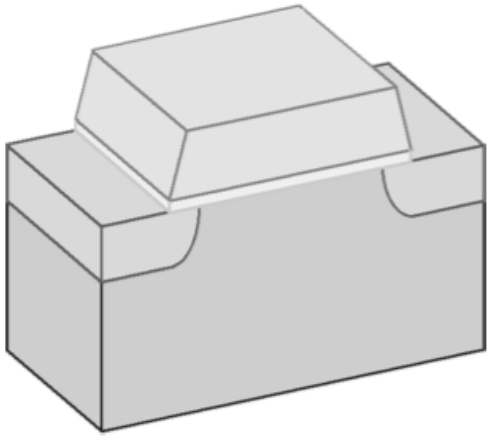




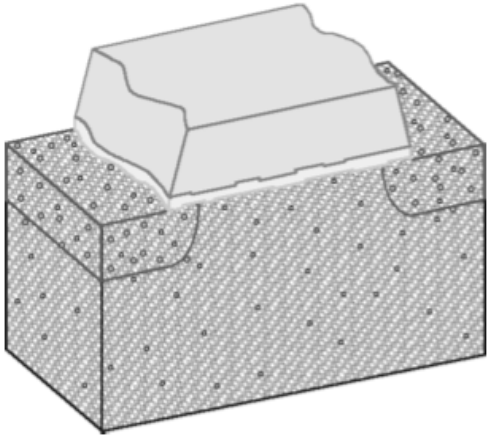
Computation Power / # Transistors & Frequency ↘ !!

Example	ARM2	Pentium P4
$\frac{\#\,Instructions/s}{\#\,Tors \times Clockfreq}$	$\frac{4\times10^{6}}{(3\times10^{4})\times(8\times10^{6})} \approx 1.3\times10^{-4}$	$\frac{10^{10}}{(10^{8})\times(2\times10^{9})} \approx 5\times10^{-8}$

Towards an "Atomistic" Device Concept

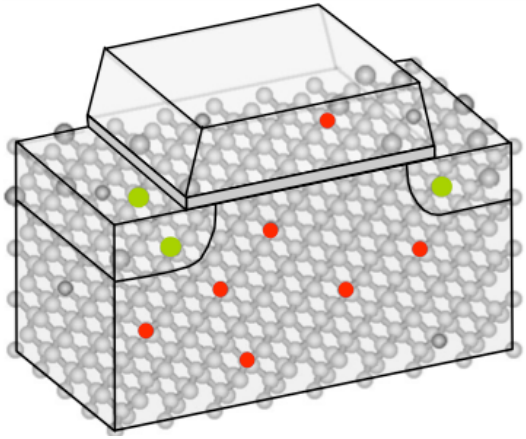


Today's MOSFET
Assumption:
Continuous ionised dopant charge and smooth boundaries and interfaces



Sketch of 20-nm MOSFET
Expected Mass Prod. ≤ 2010
< 50 Si Atoms in Channel

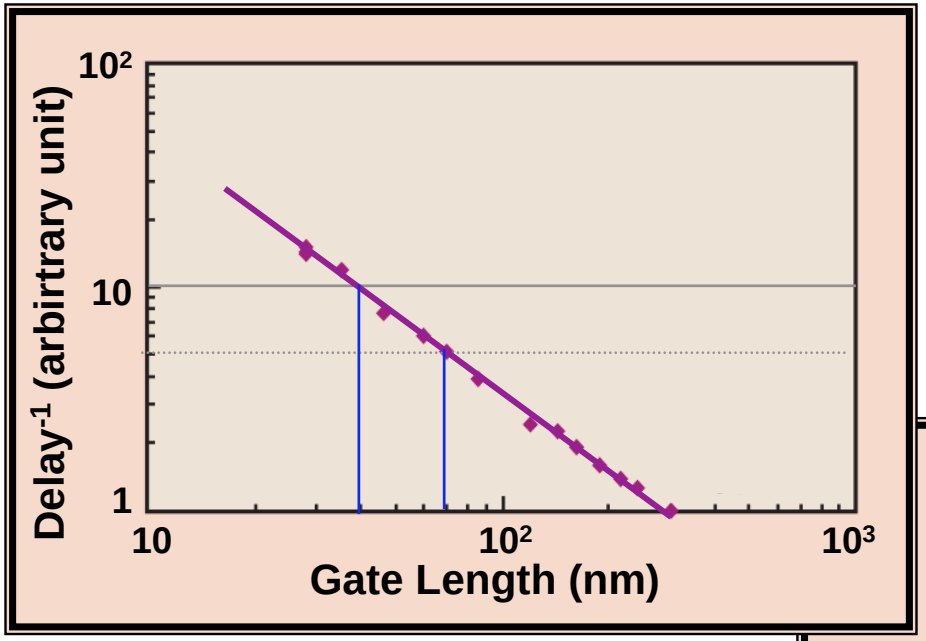
Random discrete dopants, atomic scale interface roughness, and line edge roughness introduce significant intrinsic parameter fluctuations



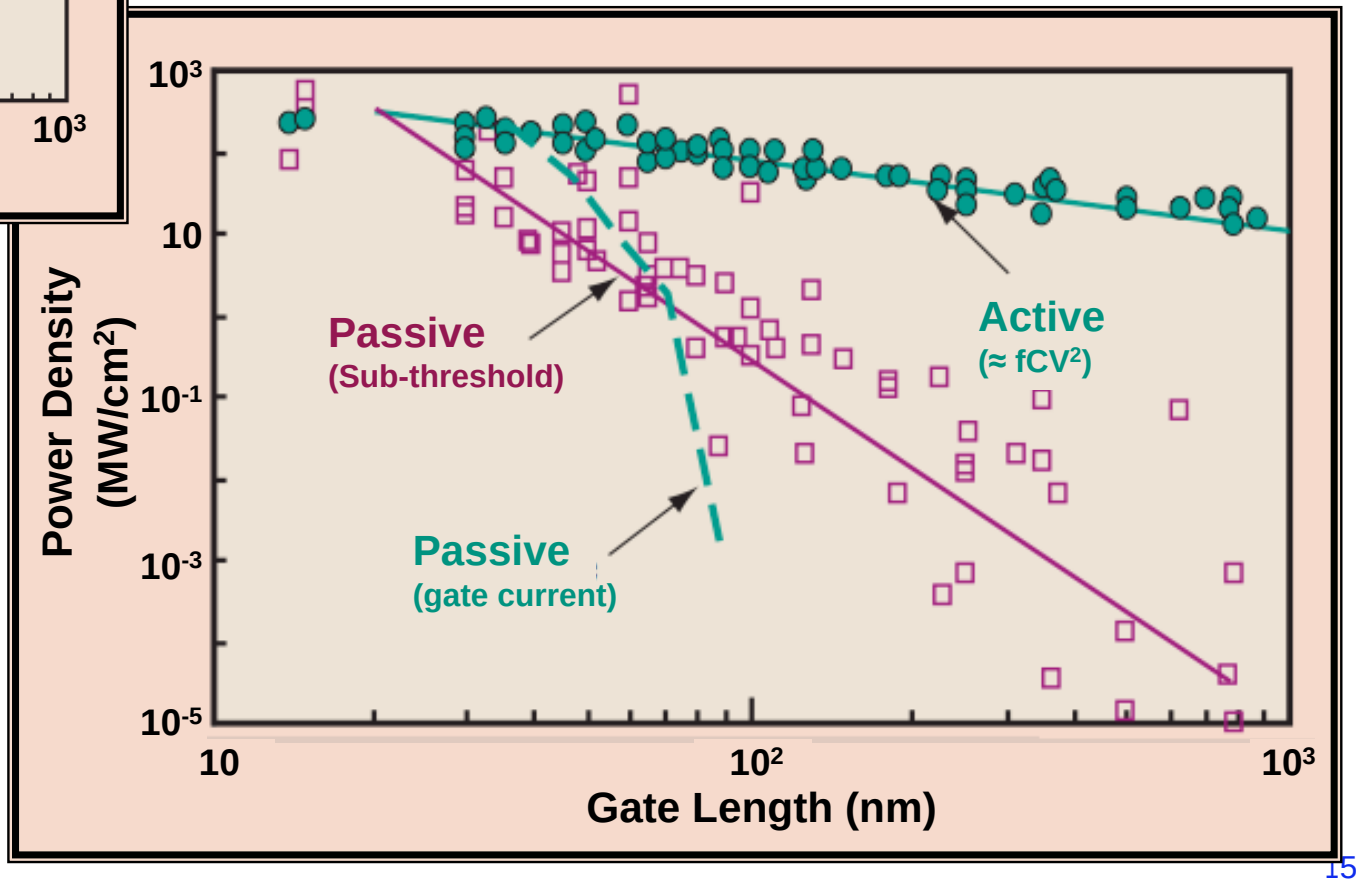
Sketch of 4-nm MOSFET
Expected Mass Prod. ≈ 2020
< 10 Si Atoms in Channel
Device becomes smaller than biologically important molecules such as ionic channels

Asenov *et al.*, "Simulation of Intrinsic Parameter Fluctuations in Decananometer and Nanometer-Scale MOSFETs", IEEE Trans. Electron Devices, 50 (9), pp.1837-1852, Sept. 2003.

Improved performance, but…

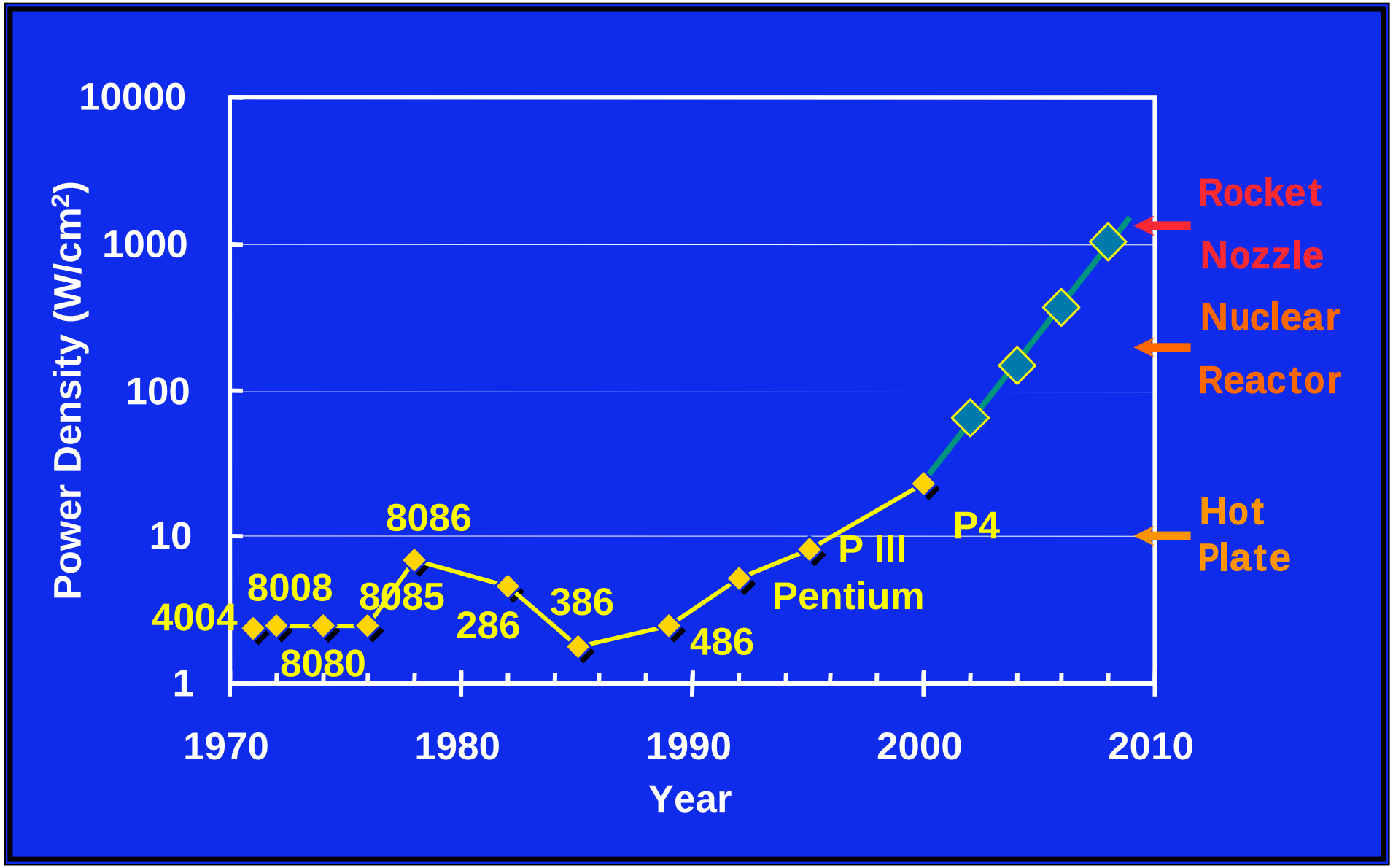


… Power is an issue!



Haensch *et al*., "Silicon CMOS devices beyond scaling", *IBM J. Res. & Dev. 50 (4/5)*, pp.339-361, July-Sept 2006

Power is Definitely a Real Concern



Top-Down Approach: Where do We Stand?

- Power dissipation ↗
- Process variations ↗
- Manufacturing (lithography, testing) costs ↗
- Yield ↘
- Prob. defects get undetected ↗

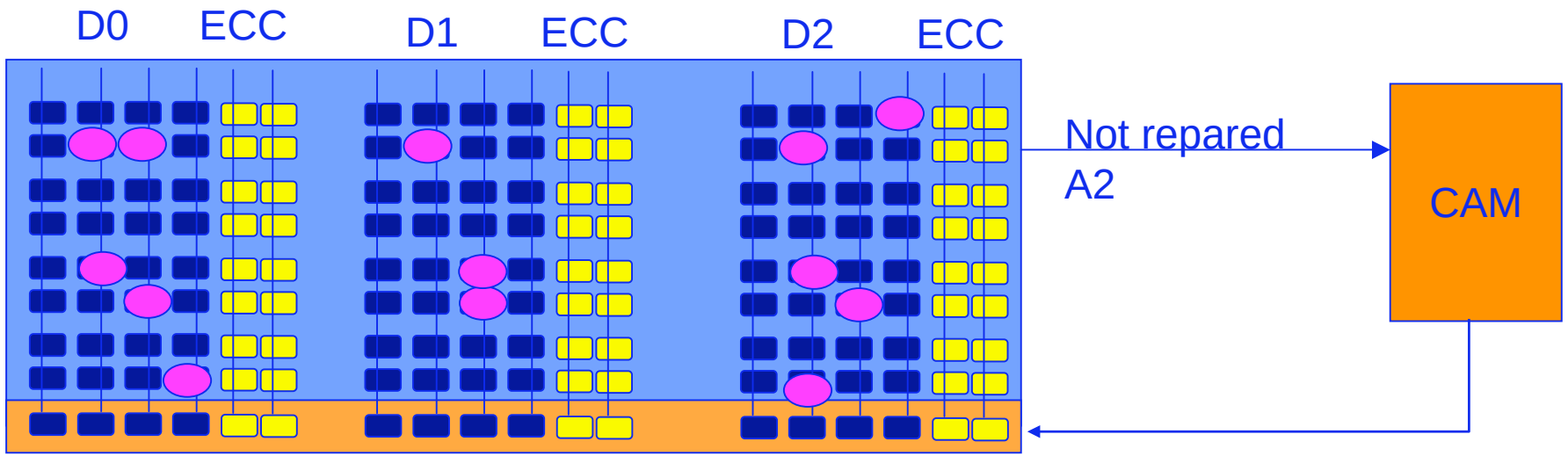
- Soft Error Rate ↗
- FIT ↗
- Vulnerability to attacks ↗

A New Set of Paradigms are Emerging

- Move away from the Basic “Frequency & Size” Rationales
- From “100% Correct” to “Less than Perfect” Circuits
- Resilience Achieved via Application of Redundancy Techniques wrt to Manufacturing Defects and Transient Faults
- Static and On-line Degradable-Reconfigurable Circuits (Memory)
- From “X-Scalar” to “Vectorial” Multi-Core Processor Architectures

Coping with Manufacturing Defects
Memory Devices

- **Yield Achieved via Static Configuration at Manufacturing Stage**
- **Advanced techniques combine ECC and line reconfiguration**



L. Anghel, M. Nicolaidis, N. Achouri, " Built In Self Repair Techniques for Based on ECC Codes to Cope with Memories Affected by High Defect Densities », IEEE VLSI Test Symposium 2004, Napa Valley, USA, April 2004.

SRAM-based FPGA Technology and Automotive Applications◊

- **Basic Assumptions**
  - Location: Denver, CO, USA ≈ 5,000 feet
  - Technology: 22μm SRAM-based FPGA 1M-gates
  - Prediction (SpaceRad 4.5): 1.05 x 10-4 upsets(*) / day

- **Let us consider a fleet of 500,000 vehicles, each featuring an airbag control system using this technology**

  —> Continuous operation ≈ 52.5 upsets / day

  Thus, an upset every 27.4 minutes!

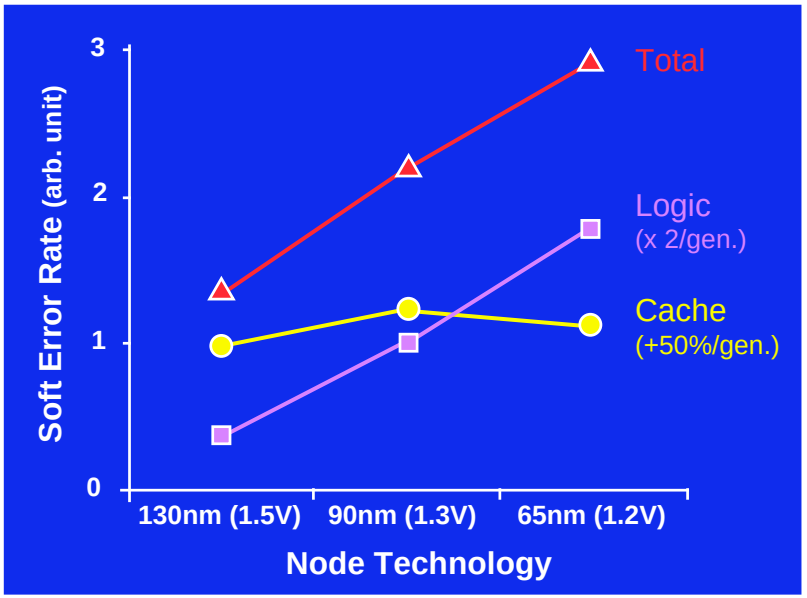
  —> Assuming 1 h use per day ≈ 2 upsets / day

(*) These are firm errors that will persist until the SRAM FPGA is reloaded (normally by power cycling or forcing reconfiguration)

◊ Martin Mason, Actel Corporation — *Automotive DesignLine Newsletter*, May 31, 2006

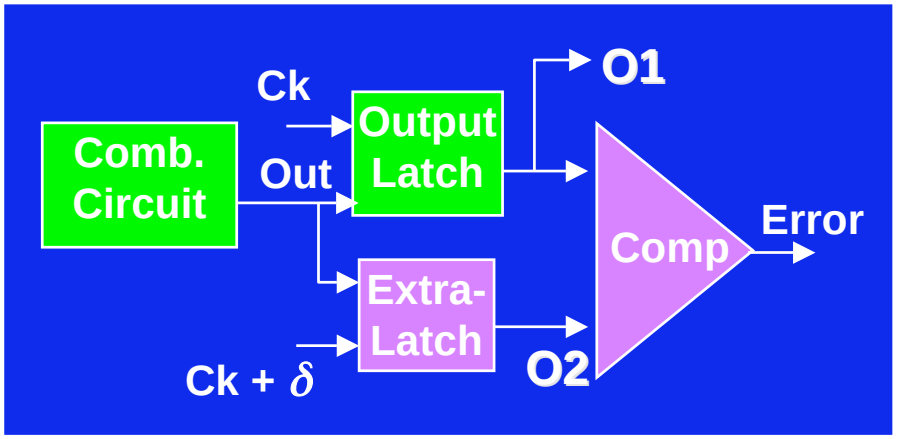
Coping with Transient and Delay Faults

- **Transient:**
  - Voltage/Current Variations, Crosstalk,
  - Particle induced fauls: Latches [SEUs] + Comb. Logic [SETs]) E.g., non-protected processor ——————>
- **Delay:**
  - Negative Bias Temperature Instability —> Impact on V_T

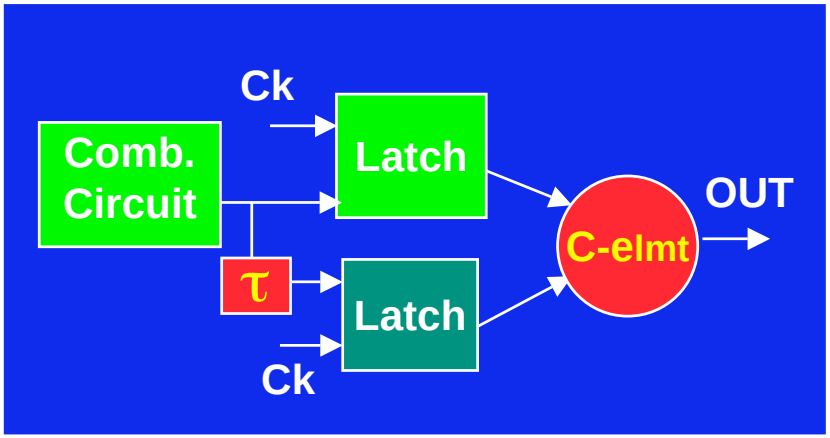


- **Errors induced by particles (SET & SEU) and delay faults**

Detection



Tolerance



a	b	c
0	0	1
1	1	0
0	1	z*
1	0	z*

z Previous stored value

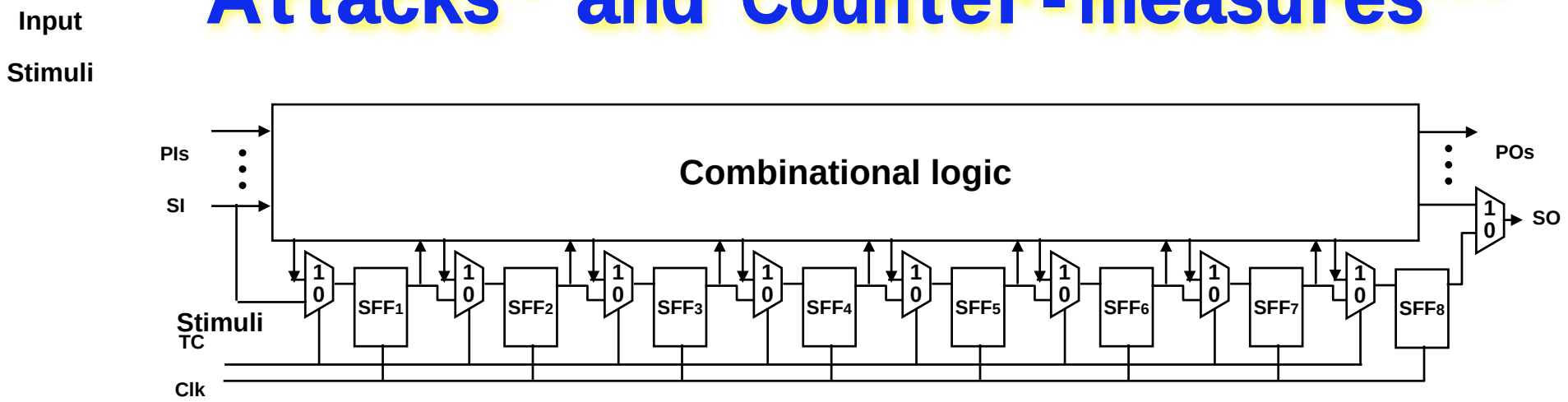
L. Angel *et al.,* DATE 2000. Application (ESA Leon RISC 32b processor) — Transfer to iROC in 2001
Optimizations/Extensions wrt to Tolerance of Delay Faults by ARM (Razor Scheme — 2004), and Intel (NBTI — 2006) — also Scan Chain Protection — 2004)

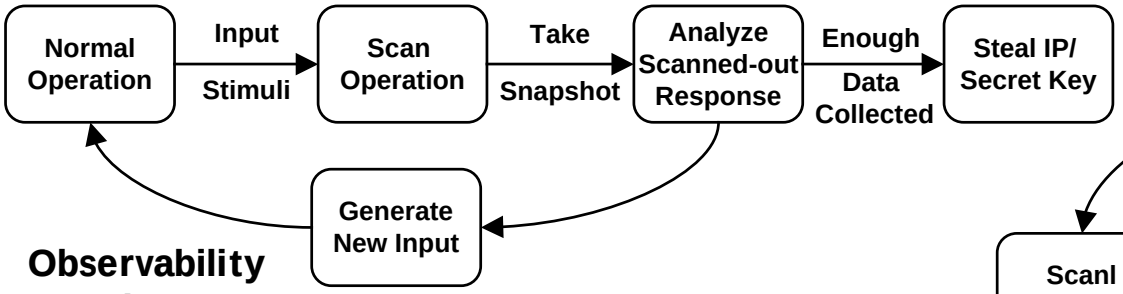
Coping with Hardware Vulnerabilities

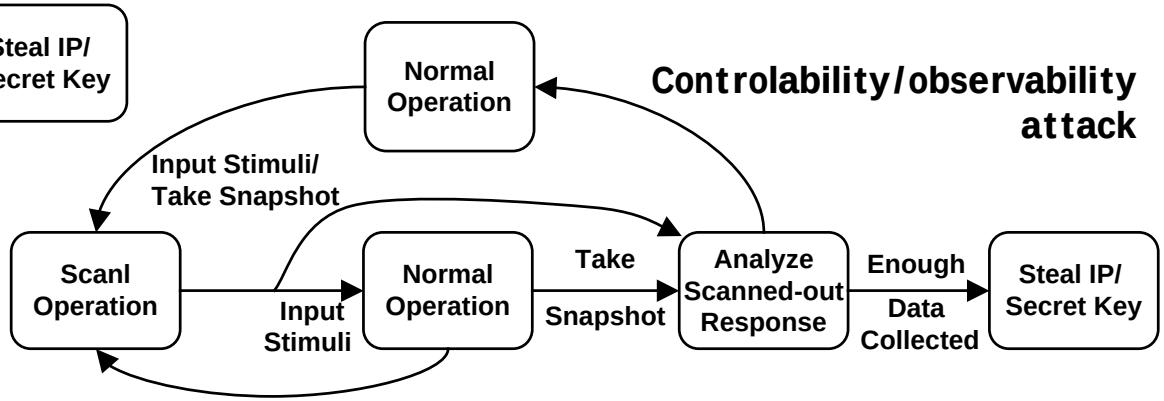
- **Target**
  - Cryptochips (Data Encryption Standard, Advanced Encryption Standard, Diversified AE)
  - On-chip Intellectual Property
- **Side Channel Attacks** (Information leakage)
  power consumption, timing information, electromagnetic radiation, radio-frequency analysis (contactless, RFID)
- **Differential Fault Analysis**
  Out-of-range environmental conditions or even fault injection
- **Good news**: "As technology shrinks, attacks get more difficult"*
- **Scan-based Testing**
  Enhance Controlability and Observability -- A Built-in Trojan Horse?

* Helena Handschuh, Spansion EMEA, WDSN'07

Examples of Scan-Chain-based Attacks* and Counter-measures**





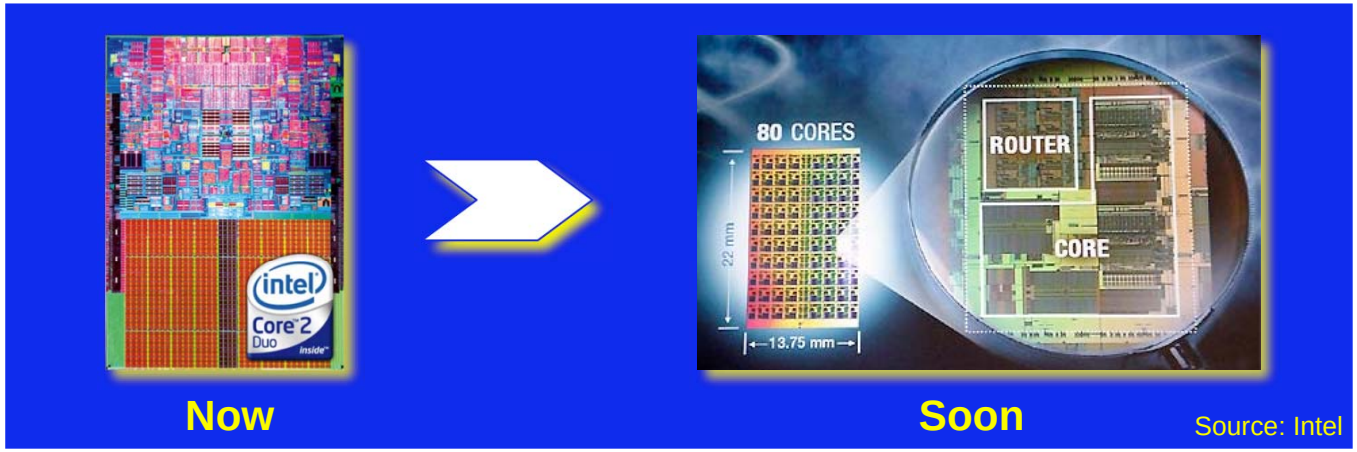


- **Posssible approaches**
  - **Using BIST (Buil-IN Self Test) for critical parts of the IC**
  - **Using an additional sigtnature**
  - **Scrambing the way the Scan Chain is used (e.g., via a LFSR)**

* J. Lee, M. Tehranipoor, C. Patel, J. Plusquellic, "Securing Designs Against Scan-Based Side-Channel Attacks", IEEE TDSC (to appear in 2007)

** D. Hély, F. Bancel, M.-L. Flottes, B. Rouzeyre, "Secure Scan Techniques: A Comparison", IEEE IOLTS'06, pp.119-124, 2006

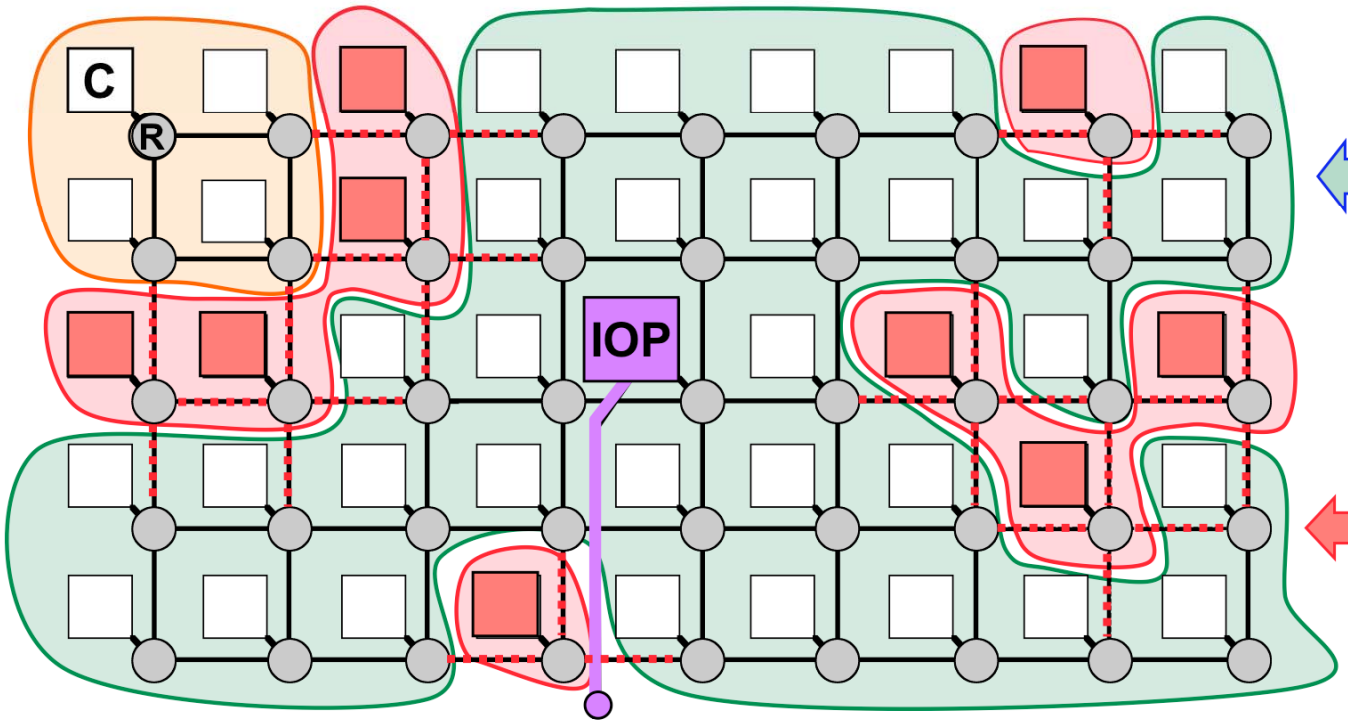
From Multi-Cores Architectures To Multi-Multi-Cores Architectures



- **Multi-Core: ↗ performance while coping with power dissipation issues (very high clock frequency)**
- **Still, ↘ transitor size for including many of such cores —> significant % of defective cores (more than 10%)**
- **Current context:**
  - **Chips are sorted according to frequency**
  - **Single core processor = “Downgraded” dual core circuits …**
- **How to go further: on-line reconfiguration to cope wih faults?**

Example Target Architecture

(5x9-node Network — Connectivity: 4)



Disconnected Zone

Single Connected Zone

Mutual Diagnosis v Bad Cores Isolated

P. Zając, J. H. Collet, J. Arlat, Y. Crouzet, "Resilience through Self-Configuration in Future Massively Defective Nanochips", Supplemental Volume DSN2007, Edinburgh, Scotland, UK, pp.266-271, 2007

C Core Processor

R Router

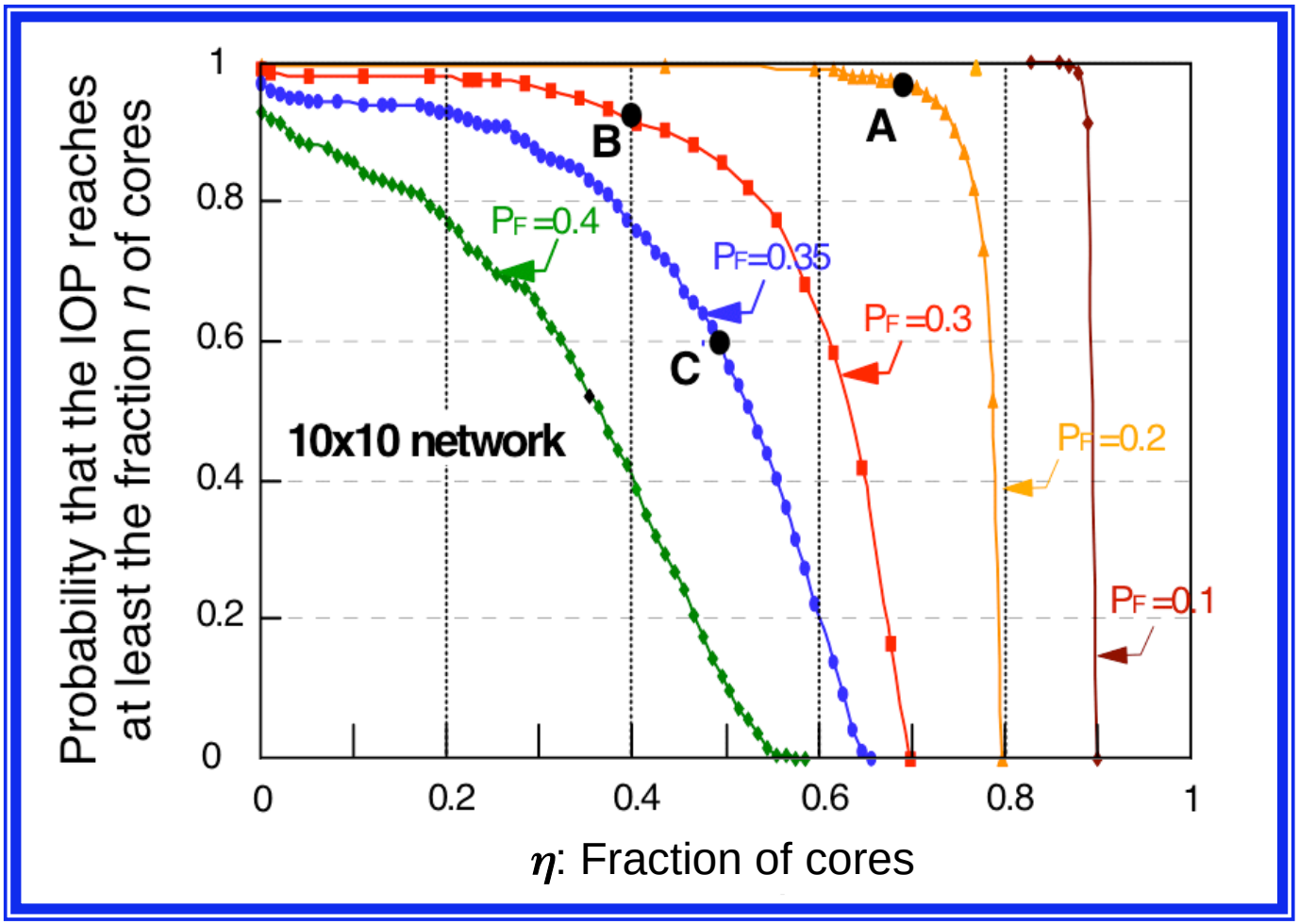
IOP I/O Port

Failed Core Processor

Inhibited Inter-router link

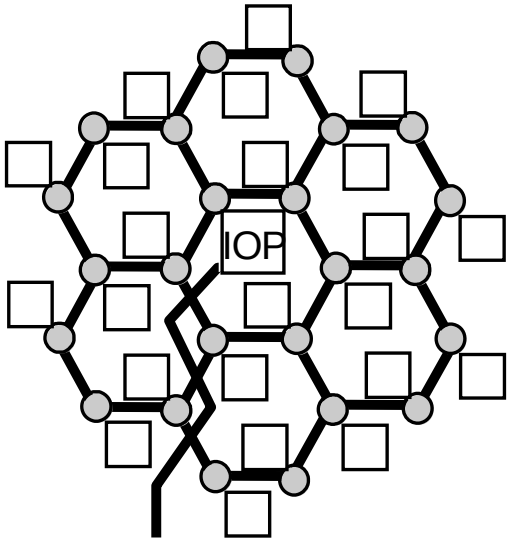
- ***Contract Net Protocol*** (CNP)
  - **Step 1: The IOP broadcasts a Request Message across the Single Connected Zone (flooding, possibly inside a propagation radius). Each core adds the route to each forwarded message.**
  - **Step 2: Each core sends an Acknowlegement Message to the IOP, which follows the RM route in the opposite direction.**
  - **Step 3: The IOP stores the discovered routes in a special buffer (Valid Route Buffer).**

Example of Results

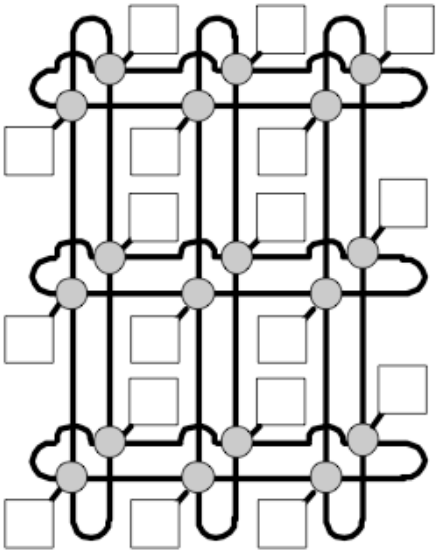


Point A (X_A = 0.68 and Y_A = 0.96) : the probability is approximately Y_A = 0.96 that the IOP reaches at least η = 68% of all cores when the core probability of failure P_F = 0.2.

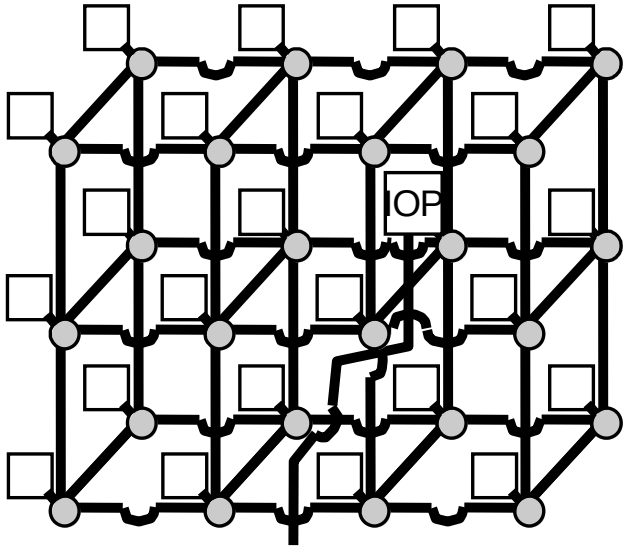
Other Possible Architectures



Hexagonal Net
(C=3, 24 nodes)



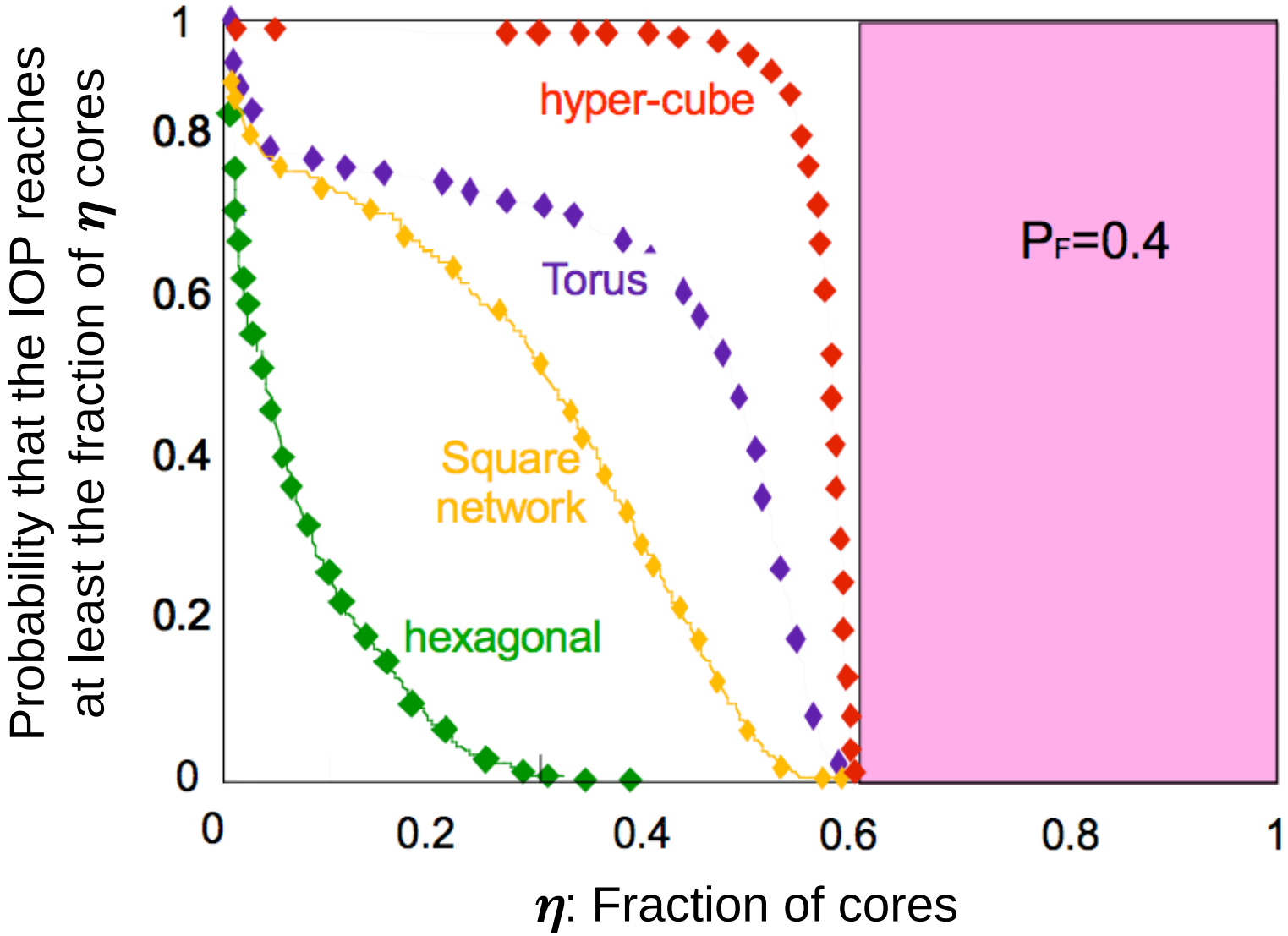
Torus
(C=4, 28 nodes)



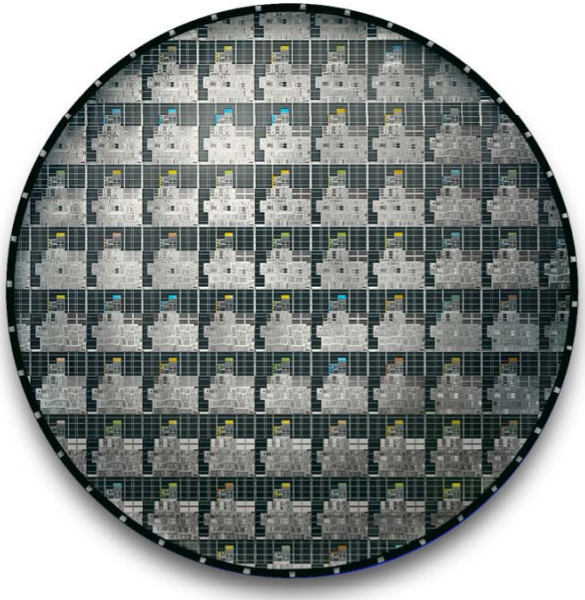
Hypercube
(C=5, 24 nodes)

Piotr Zając, Jacques Henri Collet, "Production Yield and Self-Configuration in the Future Massively Defective Nanochips", *22nd IEEE Int. Symp. on Defect and Fault Tolerance in VLSI Systems*, Roma, Italy, Sept 26-28, 2007

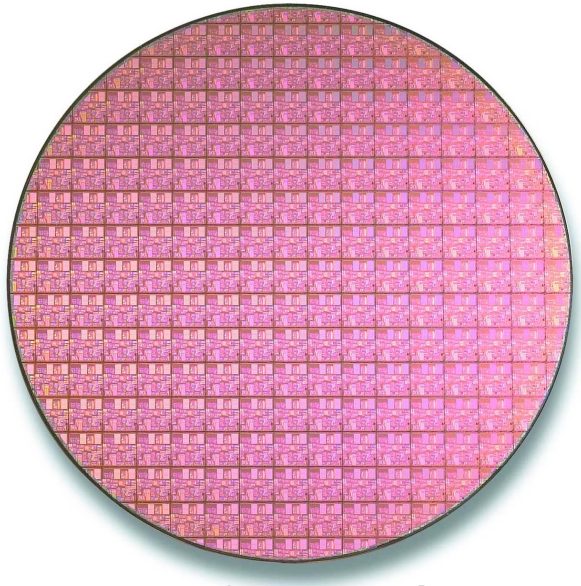
Impact of connectivity
(≈ 450-node Networks)



Concluding Remarks



300 mm Wafer — Itanium 2
0.18 μm — 21.6 mm x 19.5 mm



300 mm Wafer — Pentium 4
0.13 μm — 11.27 mm x 11.27 mm

- **The problems at stake are very challenging!**
- **Massively defective ICs including high % of "crummy" components are to be expected**
- **A "novel" perspective is thus emerging…**
- **Back to the seminal ideas by: Moore** (another one)**, Shannon* and von Neuman****
- **Old recipes — and much more— are back !**
- **A very good opportunity for our community**
- **Keep our fingers crossed that SW technology catches up …**

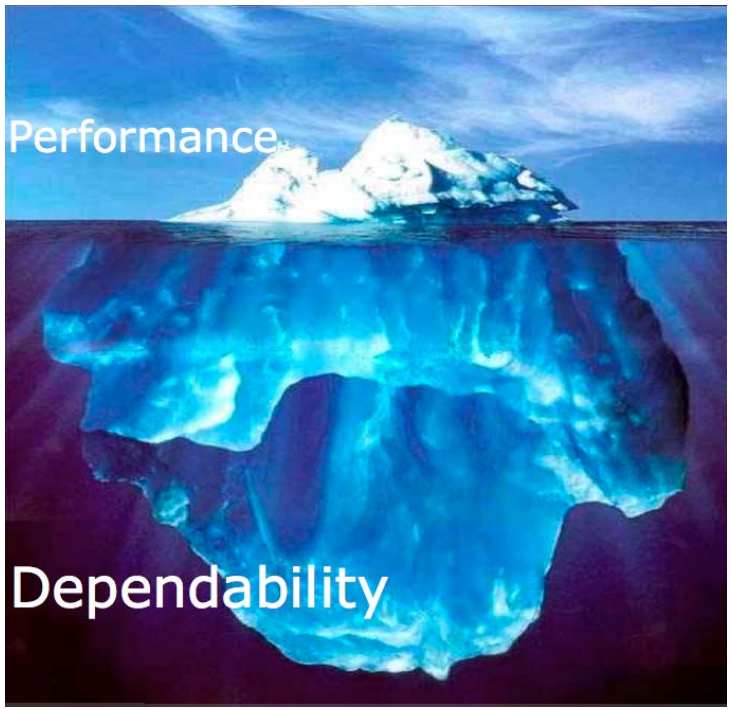
* E.F. Moore, C.E. Shanon, Reliable Circuits Using Less Reliable Relays, *J. Franlin Institute*, pp. 181-208, 281-297, 1956

** J. Von Neumann, Probabilistic Logics and the Synthesis of Reliable Organisms from Unreliable Components, *Automata Studies*, C.E. Shannon, J. McCarthy, Eds., pp. 43-98, 1955

Acknowledgement

- Ravishankar K. Iyer (UIUC) and Michael Nicolaïdis (TIMA)

- Contributors to the Workshop on Dependable and Secure Nanocomputing at DSN07, especially:
  - Janak H. Patel (UIUC),
  - Johan Karlsson (Chalmers U.)
  - Jacob Abraham (UT Austin),
  - Helena Handschuh (Spansion)
  - Takashi Nanya (U. Tokyo),
  - Alex Orailoglu (UCSD)
  - Sudhakar M. Reddy (U. Iowa)
  - Lorena Anghel (TIMA)
  - Cristian Constantinescu (AMD) —>



- Piotr Zajac, Jacques Collet and Yves Crouzet at LAAS-CNRS

- Work supported in part by IST NoE ReSIST (contract: 026764)