DARPA "TRUST in IC's" Effort

Dr. Dean Collins
Deputy Director, MTO
7 March 2007

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
07 MAR 2007	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
DARPA TRUST in ICsEffort	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **DARPA**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

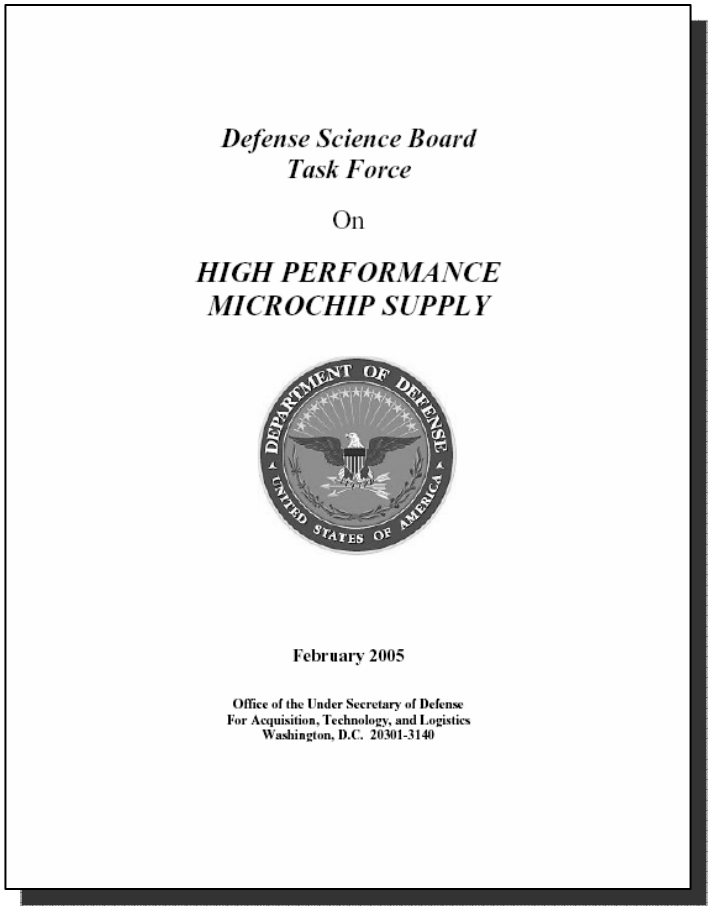
13. SUPPLEMENTARY NOTES
DARPA Microsystems Technology Symposium held in San Jose, California on March 5-7, 2007. Presentations, The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**14**	

High Performance Microchip Supply



http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf

- **For the DOD's strategy of information superiority to remain viable, the Department requires:**
  - **Trusted, Affordable, Timely Supply of Integrated Circuits (ICs)**
  - **A continued stream of exponential improvements in the processing capacity of microchips and new approaches to extracting military value from information.**
- **Technical Aspects of Trusted Circuits:**
  - **Design**
  - **IC Fabrication**
  - **IC Packaging**

Technical and Structural Vulnerabilities

- **A small number of special circuit IC components are essential for the nation's defense. Many have no commercial demand:**
  - **Radiation hardening, high power microwave, mm-wave and sensors.**
- **Global economic pressures are driving IC design and manufacturing to foreign soil and out of US control to ensure trust and availability:**
  - **Taiwan, PRC, Singapore, Korea and Japan**
  - **Cost for building 300mm wafer, 65nm chip fabrication plant is now approaching $3B.**
  - **In addition to trust, the country faces a potential "Reverse-ITAR" restriction environment for future supply**
- **Dedicated facilities (NSA, Sandia, Honeywell, etc.) cannot provide the performance, variety and volume of DOD needs.**
- **This creates significant future vulnerability for critical systems:**
  - **Trust cannot be added to circuits after fabrication**
  - **Reverse engineering cannot be relied upon to detect undesired IC alterations.**
- **"Trusted Foundry Program" provide interim measure for trusted high performance IC's – "take or pay" basis**

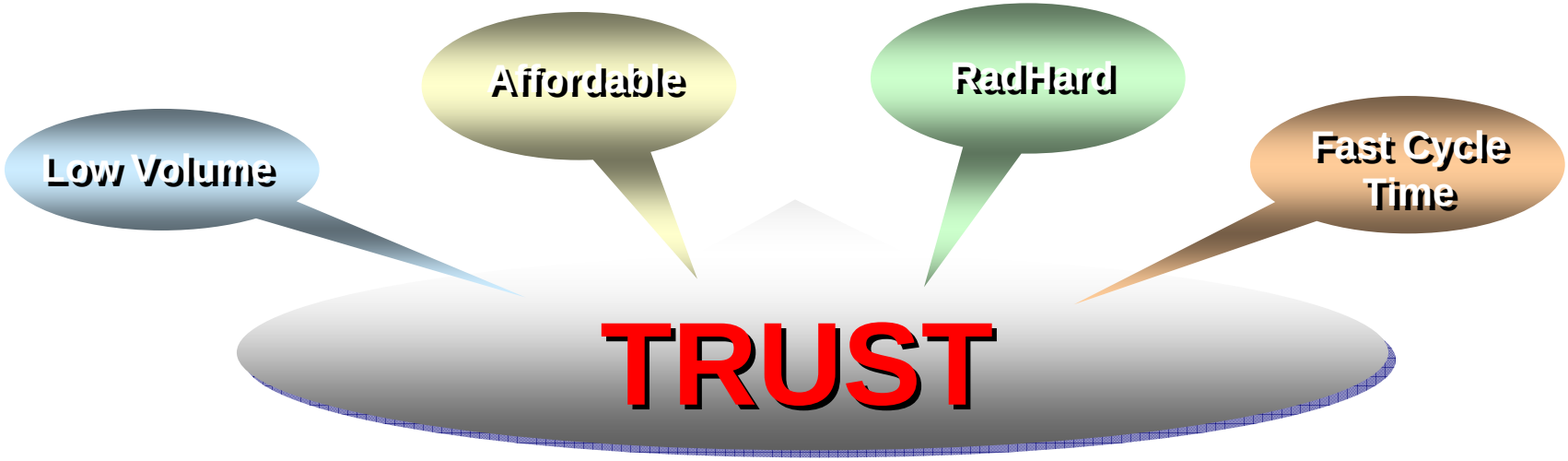
What is the Nature of the Adversary?

- **It is assumed that the adversary is a nation/state with modern semiconductor capability that has the:**
  - **Motivation**
  - **Opportunity**
  - **Talent**
  - **Manpower**
  - **Time / Patience**

  to do significant harm to the USA

"Overlap of TRUST with Other Issues"

- **Although TRUST is not synonymous with RadHard, affordable, low volume and fast cycle time, many customers for trusted parts also desire these other attributes**



Trustworthy computing (with software) cannot exist until we have trustworthy hardware to build it on

TRUST
Commercial Efforts

Automobiles (GM)

Smart Cards/Smart Keys (Samsung, Infineon)

Integrated Circuits – (INTEL)

Cell Phones – (Motorola)

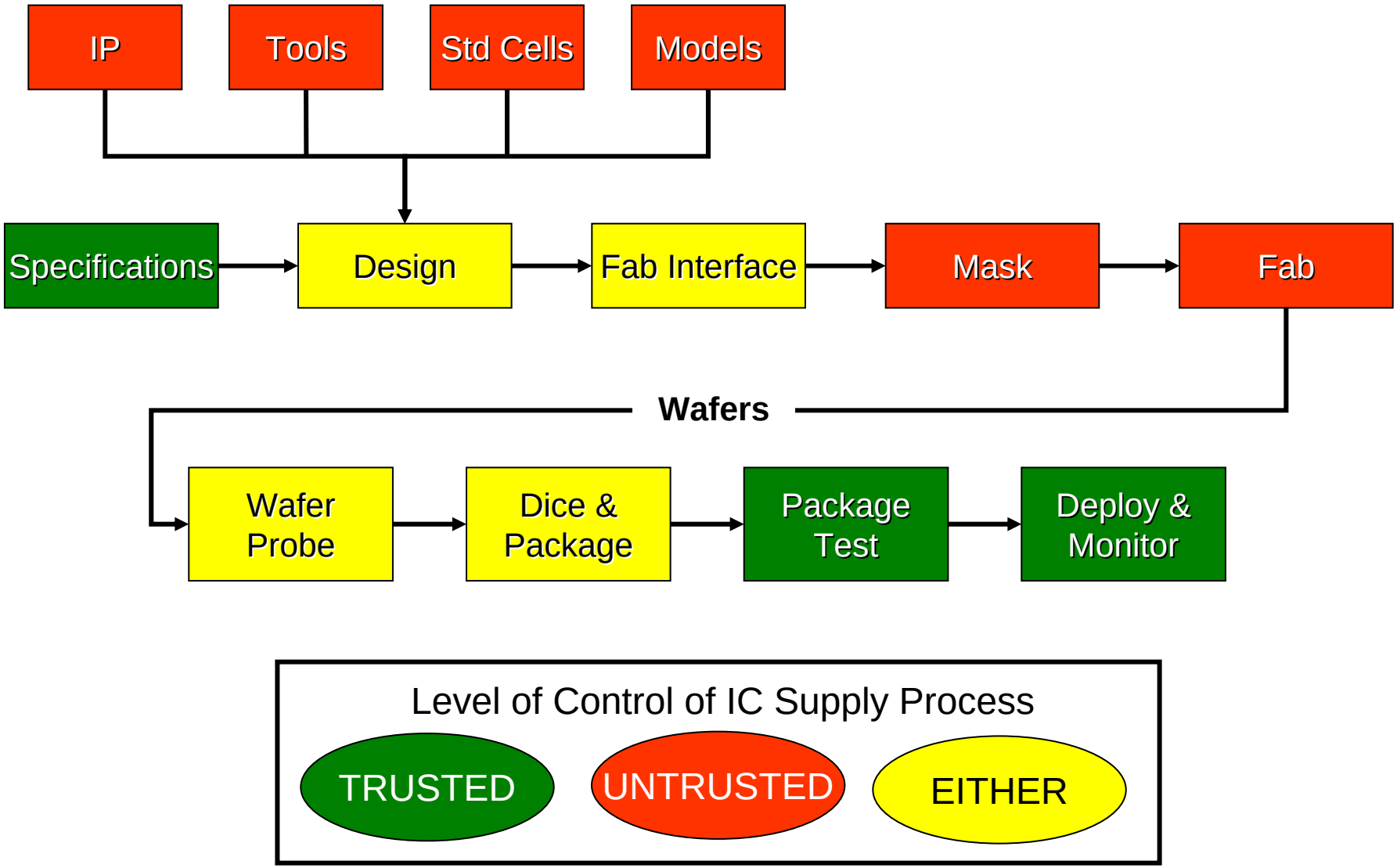
Set Top Boxes – (Motorola)

Secure Blue – (IBM)

Commercial Reverse Engineering – (Chipworks, Semiconductor Insights, CPU Tech)

The government can benefit from commercial practices

New Supply Chain Structure



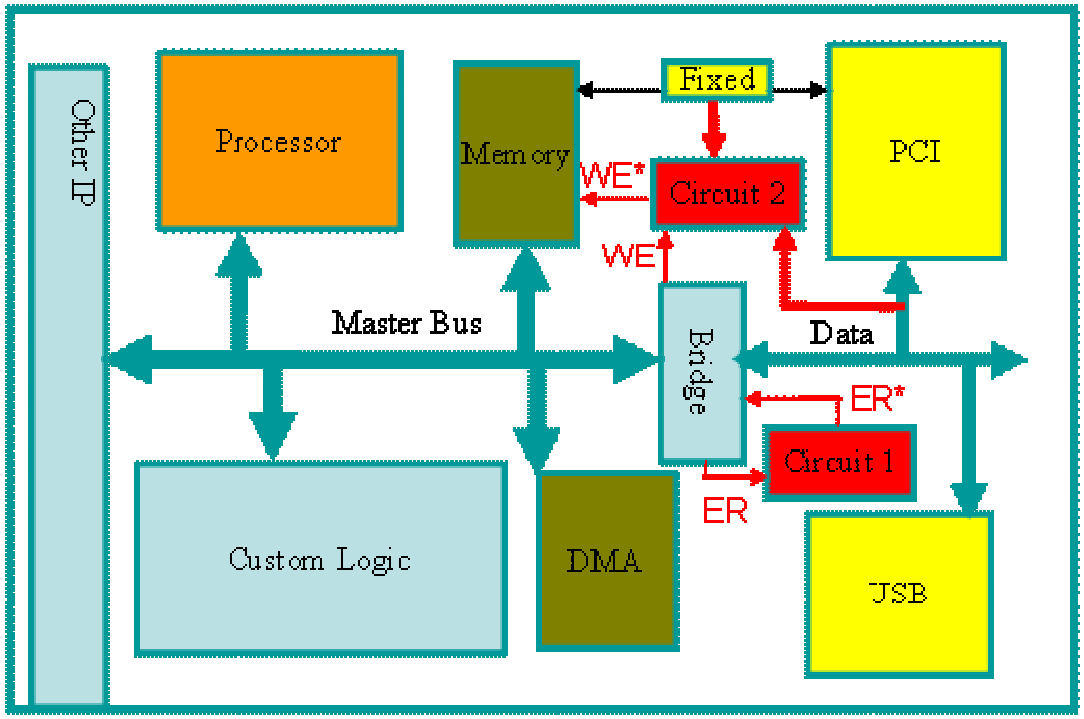
DARPA Hard Problems

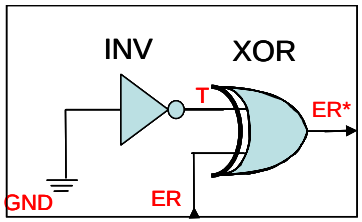
- How do you trust the design cycle to faithfully generate only the microelectronics desired?
- How do you trust microelectronics chips when they are manufactured in a non-trusted facility, such that they will faithfully perform only the function they are designed for?
- How do you trust that the testing on the microelectronic chips will faithfully determine that the chip will operate only as designed. (no more – no less)
- How do you know that the packaging of the chip does not introduce features into or misidentify the chip?
- How do you determine that the packaged chip has not been tampered with after installation, and how do you communicate the fact of tampering?

Areas of Interest

- **CASE1:** Given an IC corresponding to a known design, does the IC that is delivered do what it is supposed to do and nothing more? This is the case when the Fabrication facility is not trusted but the design process is. The problem is to determine whether the IC hardware received has been modified in order to determine that the fabrication can be trusted.
- **CASE2:** Given a specification and an IC design is the design true to the specification? In this case one assessing the trust of the design software and synthesis tools. The design itself must be validated.
- **CASE3:** Given a re-configurable IC, does the configurable data (bit stream) in the device accurately represent what was intended by the specification, design and VHDL synthesis?

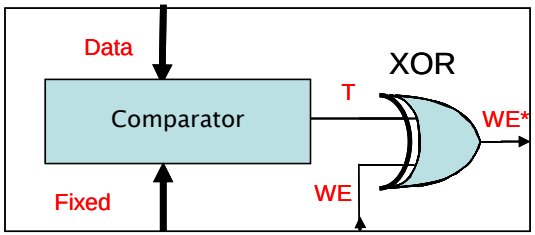
Standard IC with Extra Circuits Added





T	ER	ER*
1	0	1
1	1	0

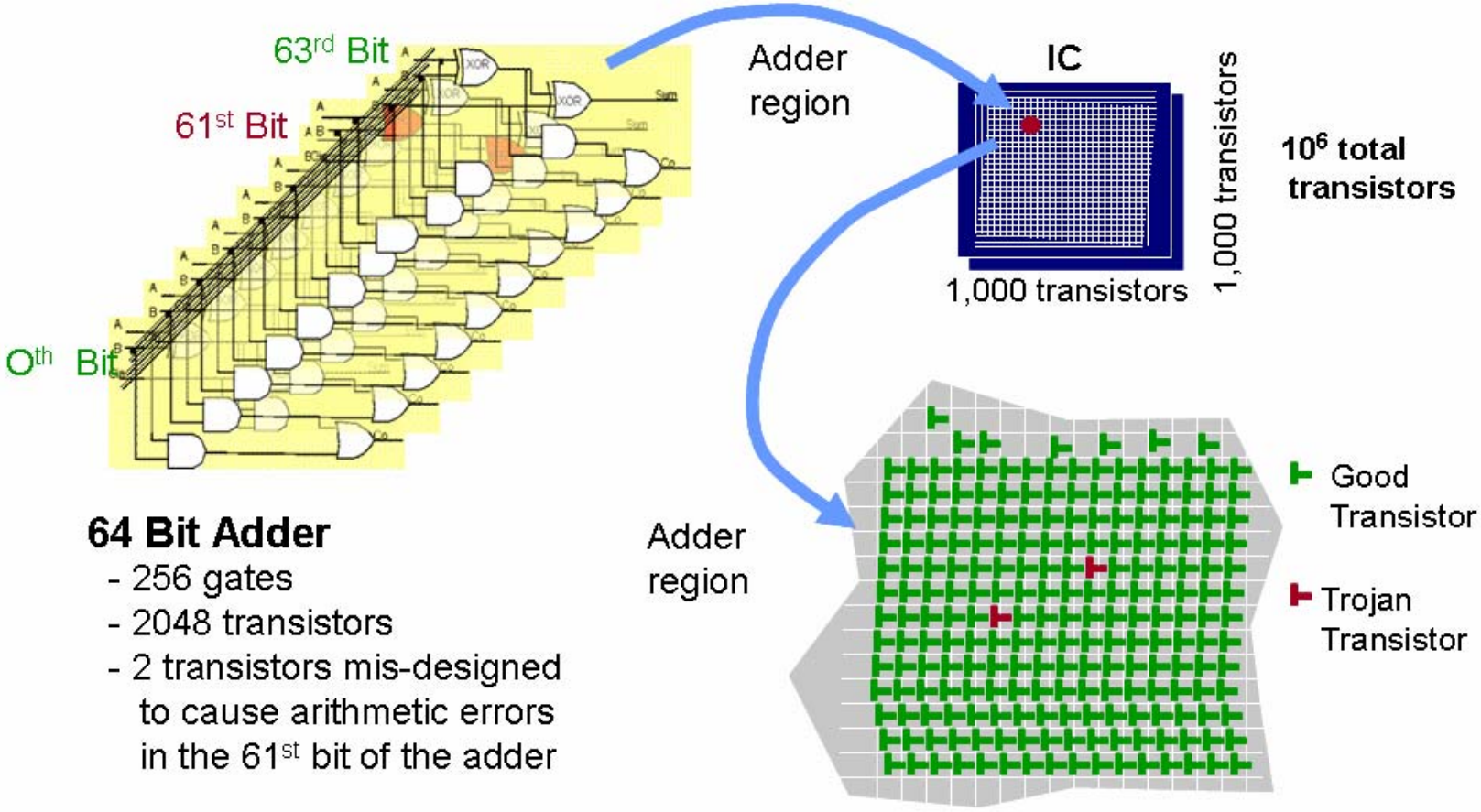
Example Circuit 1 – Trigger Always On



Data	Fixed	T	WE	WE*
232	234	0	0	0
233	234	0	1	1
234	234	1	0	1
235	234	0	0	0

Example Circuit 2 – Event Triggered Condition

Metrics Challenge



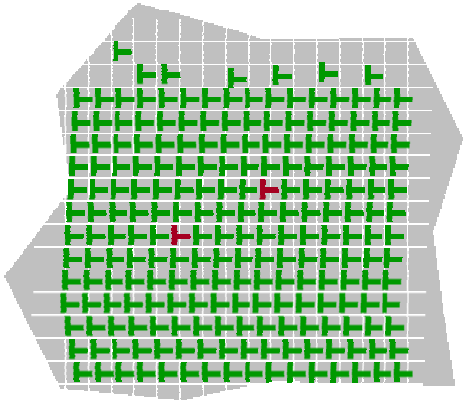
64 Bit Adder

- 256 gates
- 2048 transistors
- 2 transistors mis-designed to cause arithmetic errors in the 61st bit of the adder

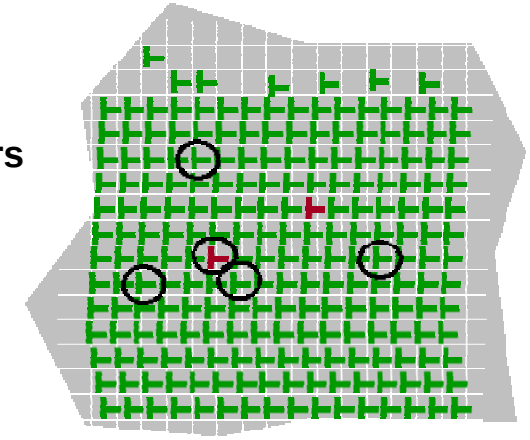
How Does One Quantify the Performance of Alternative Approaches to Detect Additions, Deletions, and Modifications to the Desired Design ?

P_D/P_{FA} Metrics Considerations

Example 1 – Tests Performed at the Transistor Level



Transistors called bad

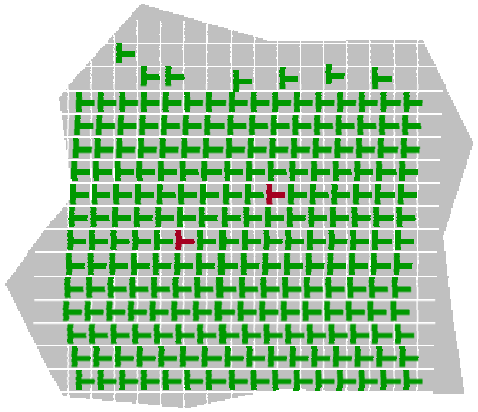


Test at Transistor Level – "rogue" transistors detected

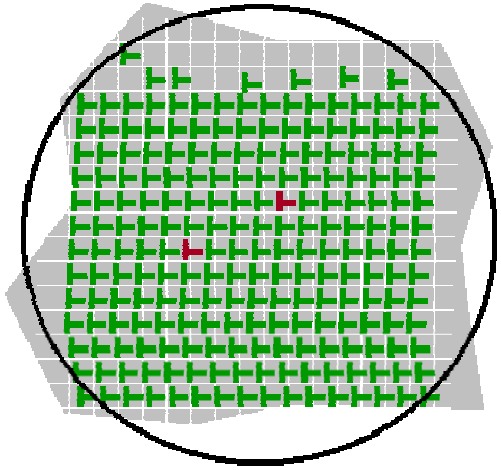
$P_D = 1/2 = 50.0\%$

$P_{FA} = 4/10^6 = 4*10^{-6}$

Example 2 – Tests Performed at the Functional Level



Adder called bad



Test at Functional Level - "2048 transistor adder does not function properly "

$P_D = 2/2 = 100.0\%$

$P_{FA} = (2048-2)/10^6 = 2.046*10^{-3}$

Key Technical Challenges

Key technical challenges for TRUST in ICs include:

- Destructive reverse engineering of an IC in a cost and time efficient manor.
- Determining if all the chips on a single wafer are identical.
- Determining the effectiveness of a non-destructive reverse engineering techniques.
- Sensitivity and effectiveness of software techniques to prevent and/or detect the insertion of malicious circuits during the design cycle.
- Determining the independence of various transistor Pd measurements.
- Relating transistor level Pd/Pfa metrics to IC level Pd/Pfa metrics.

Further Interests

Other areas of personal interest beyond TRUST in ICs:

- Device technologies that extend beyond Moore's Law.
- Device technologies which allow effective circuit level learning to take place.
- Devices based on entangled quantum effects such as matter waves, quantum computing and quantum key distribution
- Circuit functions which adapt to the environment.
- Complex Microsystems which marry advanced architectures to unique devices.
- Recruiting high quality Program Managers for MTO