Back to Hogwarts

Preventing and Creating Surprise in Hardware Cyber at DARPA MTO

Kerry Bernstein, Program Manager

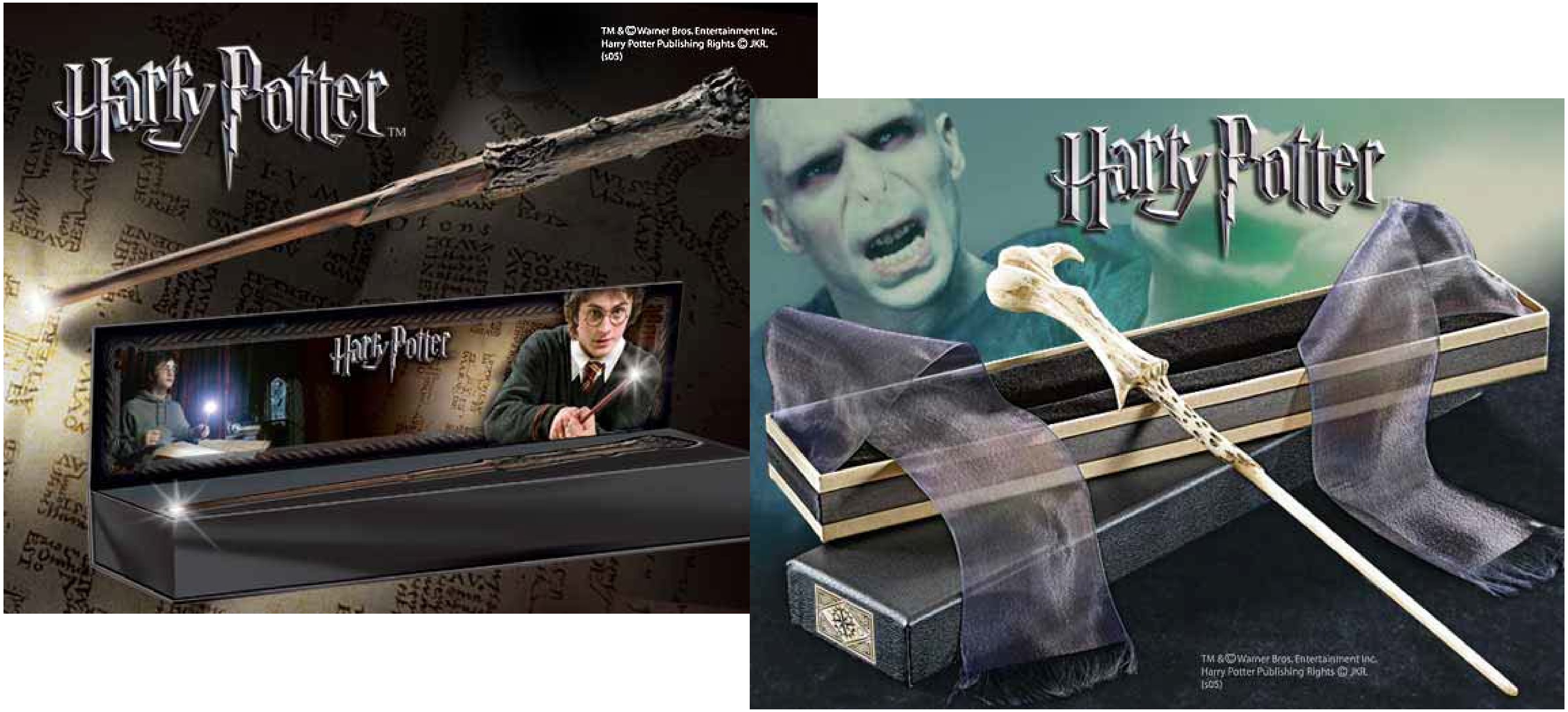
DARPA MTO

Briefing prepared for NEPP

12 June 2013

Approved for Public Release, Distribution Unlimited.
The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

Magic Wands

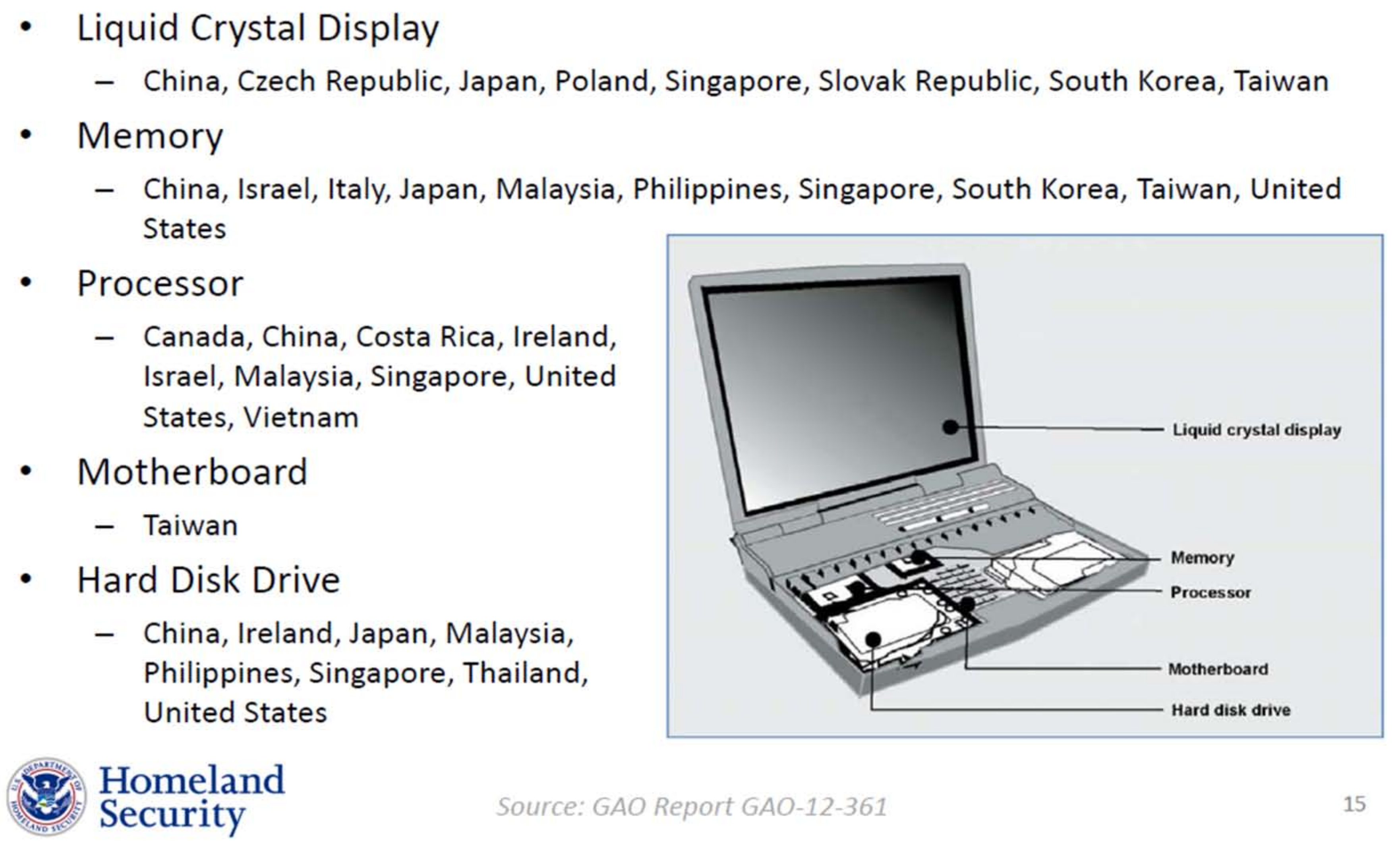

Harry Potter™
TM & © Warner Bros. Entertainment Inc.
Harry Potter Publishing Rights © JKR.
(s05)
Harry Potter
Harry Potter
TM & © Warner Bros. Entertainment Inc.
Harry Potter Publishing Rights © JKR.
(s05)

Harry Potter’s wand and Lord Voldemort’s wand are both made of Elder Wood.

Outline

- Motivation for Hardware Authentication
- Assessing Complexity For Security
- Program Overviews
- Emerging Issues in Hardware Cyber

Common Suppliers of Laptop Components

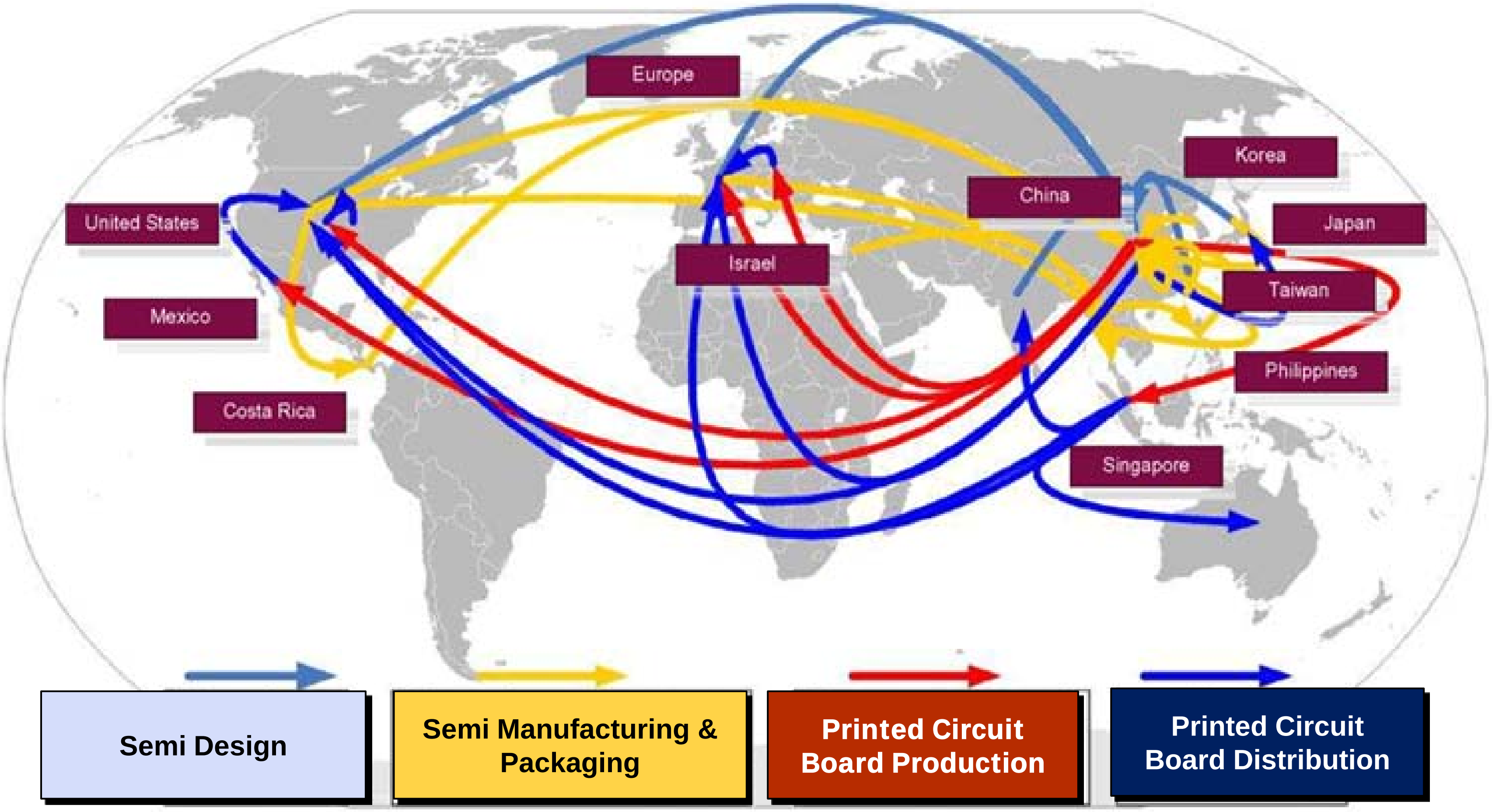


- Liquid Crystal Display
  - China, Czech Republic, Japan, Poland, Singapore, Slovak Republic, South Korea, Taiwan
- Memory
  - China, Israel, Italy, Japan, Malaysia, Philippines, Singapore, South Korea, Taiwan, United States
- Processor
  - Canada, China, Costa Rica, Ireland, Israel, Malaysia, Singapore, United States, Vietnam
- Motherboard
  - Taiwan
- Hard Disk Drive
  - China, Ireland, Japan, Malaysia, Philippines, Singapore, Thailand, United States

Source: GAO Report GAO-12-361

Electronics logistics is global

Semiconductor & Printed Circuit Board Supply Chain



Semi Design

Semi Manufacturing & Packaging

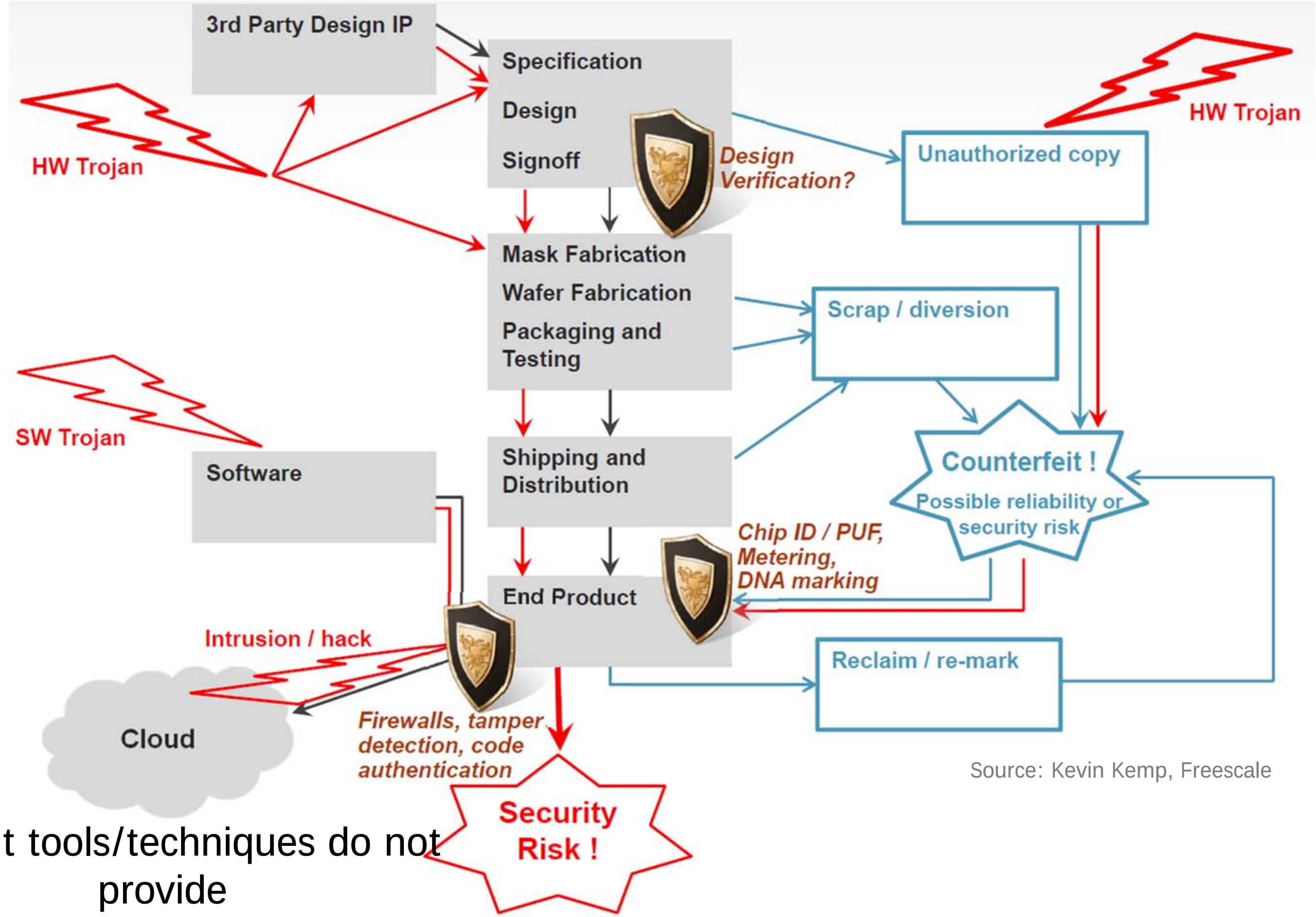
Printed Circuit Board Production

Printed Circuit Board Distribution

Source: IDC Manufacturing Insights & Booz Allen analysis

Distribution Statement A, Approved for Unlimited Distribution

Semiconductor Design & Manufacture Flow: Potential Points of Vulnerability



Source: Kevin Kemp, Freescale

Current tools/techniques do not provide
broad security assurance

Distribution Statement A, Approved for Unlimited Distribution

Exemplary Threat Taxonomy

Local / Network Malicious Code

- Trojan
- Virus/Worm

Local / Network Exploits (exploiting bugs)

- Data-directed attacks
- Buggy code/firmware

Physical Platform

- **Physical / Software side / covert channels**
- **Conducted and radiated emissions (TEMPEST)**
- **Malicious functionality insertions**
- **Materials / reliability integrity compromise**
- **Flaws in design / implementation**
- **Broken ciphers / cryptographic algorithms**
- **Counterfeit hardware, Supply Chain Interception**
- **Anti-Tamper Circumvention**

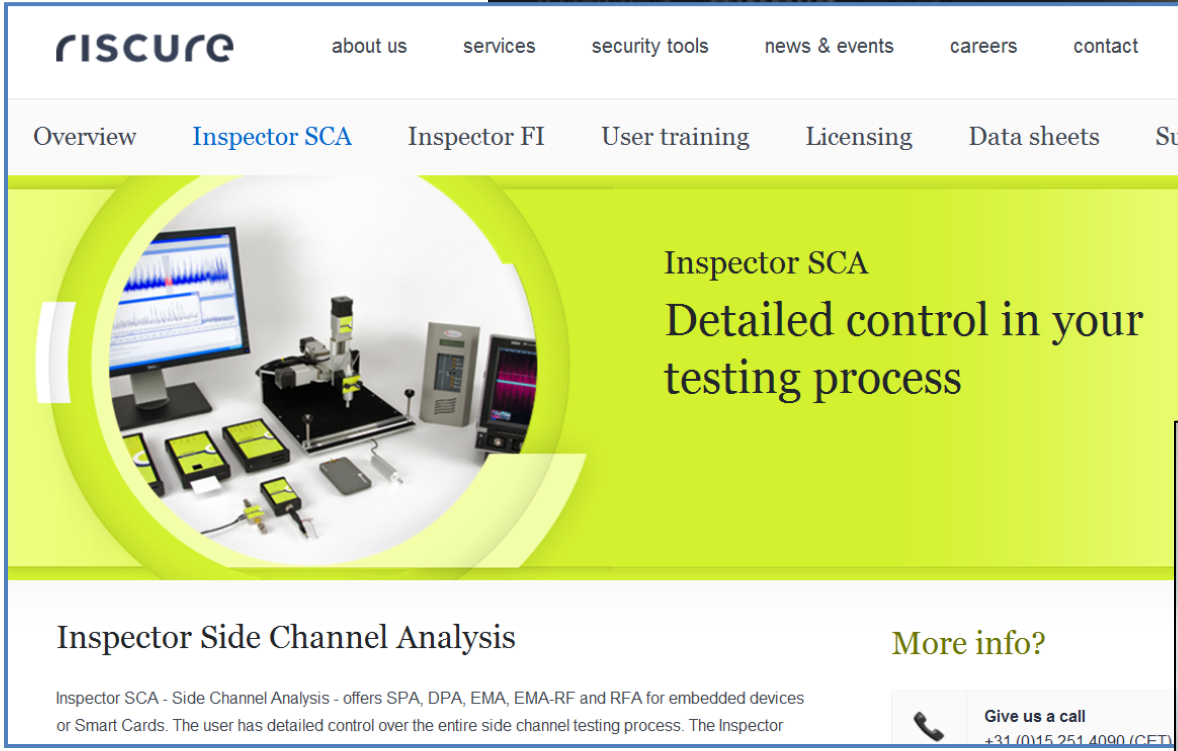
Operations

- Untrusted operator or end user
- Trusted end user/ operator with inadvertent action
- Process or operation failure
- Configuration errors

Threat Space: Side-Channel Attacks are Algorithmic

http://www.cellebrite.com/mobile-forensic-products/ufed-ultimate.html

Logical and Physical Extraction of Mobile Data



riscure

about us | services | security tools | news & events | careers | contact

Overview | Inspector SCA | Inspector FI | User training | Licensing | Data sheets | Support

Inspector SCA

Detailed control in your testing process

Inspector Side Channel Analysis

Inspector SCA - Side Channel Analysis - offers SPA, DPA, EMA, EMA-RF and RFA for embedded devices or Smart Cards. The user has detailed control over the entire side channel testing process. The Inspector

More info?

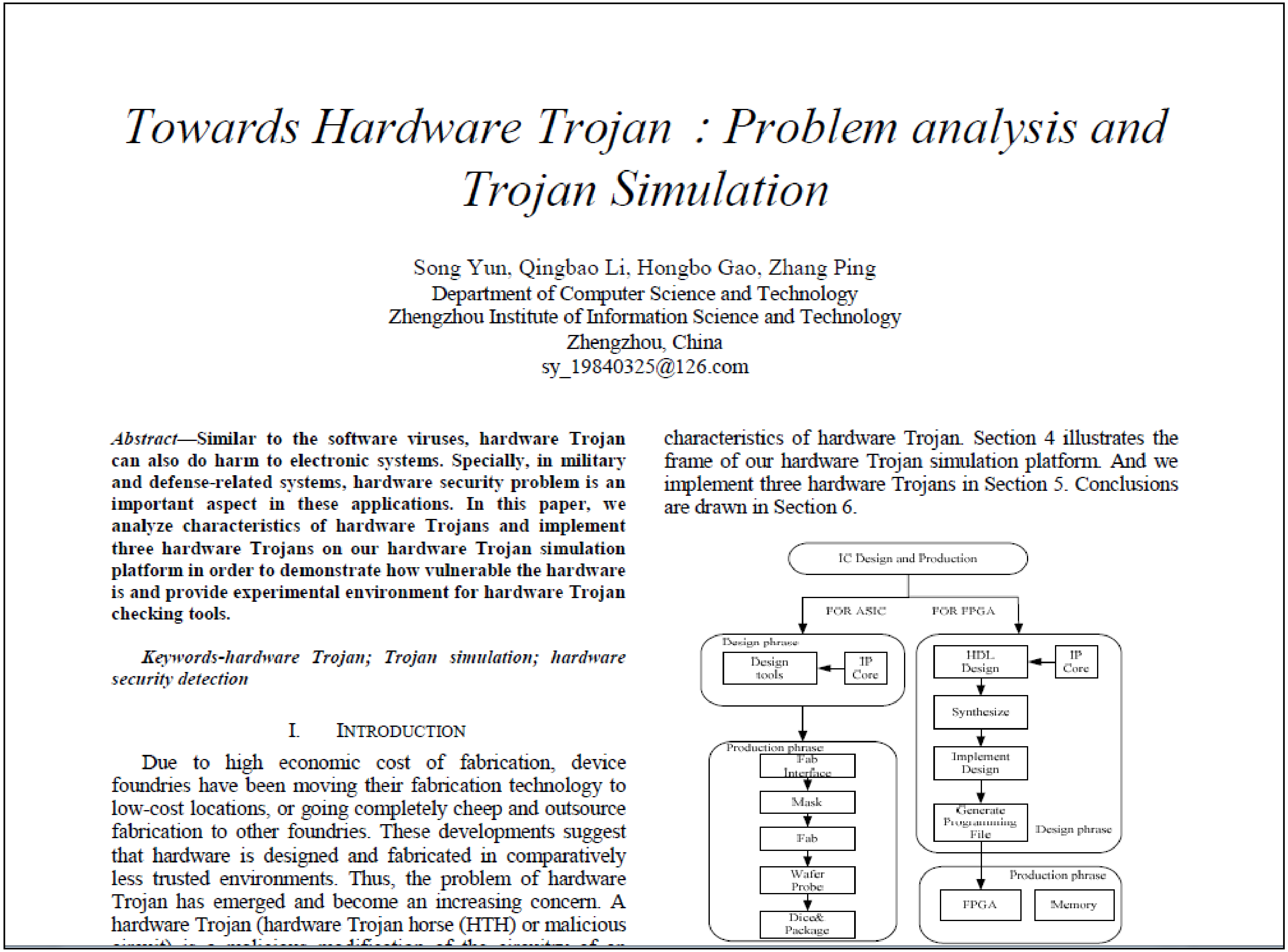
☎ Give us a call

+31 (0)15 251 4090 (CET)

http://www.riscure.com/tools/inspector/inspector-sca

http://pwnieexpress.com

A Syllabus for Hardware Intrusion



Towards Hardware Trojan : Problem analysis and Trojan Simulation

Song Yun, Qingbao Li, Hongbo Gao, Zhang Ping
Department of Computer Science and Technology
Zhengzhou Institute of Information Science and Technology
Zhengzhou, China
sy_19840325@126.com

***Abstract*—Similar to the software viruses, hardware Trojan can also do harm to electronic systems. Specially, in military and defense-related systems, hardware security problem is an important aspect in these applications. In this paper, we analyze characteristics of hardware Trojans and implement three hardware Trojans on our hardware Trojan simulation platform in order to demonstrate how vulnerable the hardware is and provide experimental environment for hardware Trojan checking tools.**

Keywords-hardware Trojan; Trojan simulation; hardware security detection

I. INTRODUCTION

Due to high economic cost of fabrication, device foundries have been moving their fabrication technology to low-cost locations, or going completely cheep and outsource fabrication to other foundries. These developments suggest that hardware is designed and fabricated in comparatively less trusted environments. Thus, the problem of hardware Trojan has emerged and become an increasing concern. A hardware Trojan (hardware Trojan horse (HTH) or malicious

characteristics of hardware Trojan. Section 4 illustrates the frame of our hardware Trojan simulation platform. And we implement three hardware Trojans in Section 5. Conclusions are drawn in Section 6.

A Few Preliminary Tech Observations

1. Cybersecurity is often thought of as a software or network problem. We know better.

2. VLSI Process is the convolution of 4 processes: Deposition, Removal, Patterning, Implanting. All 4 are vulnerable to intentional compromise. Its as true for FPGAs as it is for full custom.

3. We've provided the *illusion* of scaling for years now. The infusion of technology band-aids for this illusion supports yet more evil in all semiconductors – Customs, ASICs, as well as FPGAs.

4. Custom IP on board modern FPGAs are provided by 3rd party vendors, and are as vulnerable to exploit as custom ICs.

5. Design Complexity provides opportunity for intrusion. Custom processors, ASICs or FPGAs are all MOSFETS + Interconnects.

6. No coincidence that exploits may be commonly asserted with same processes, materials and design tools as those used in conventional process card and failure analysis.

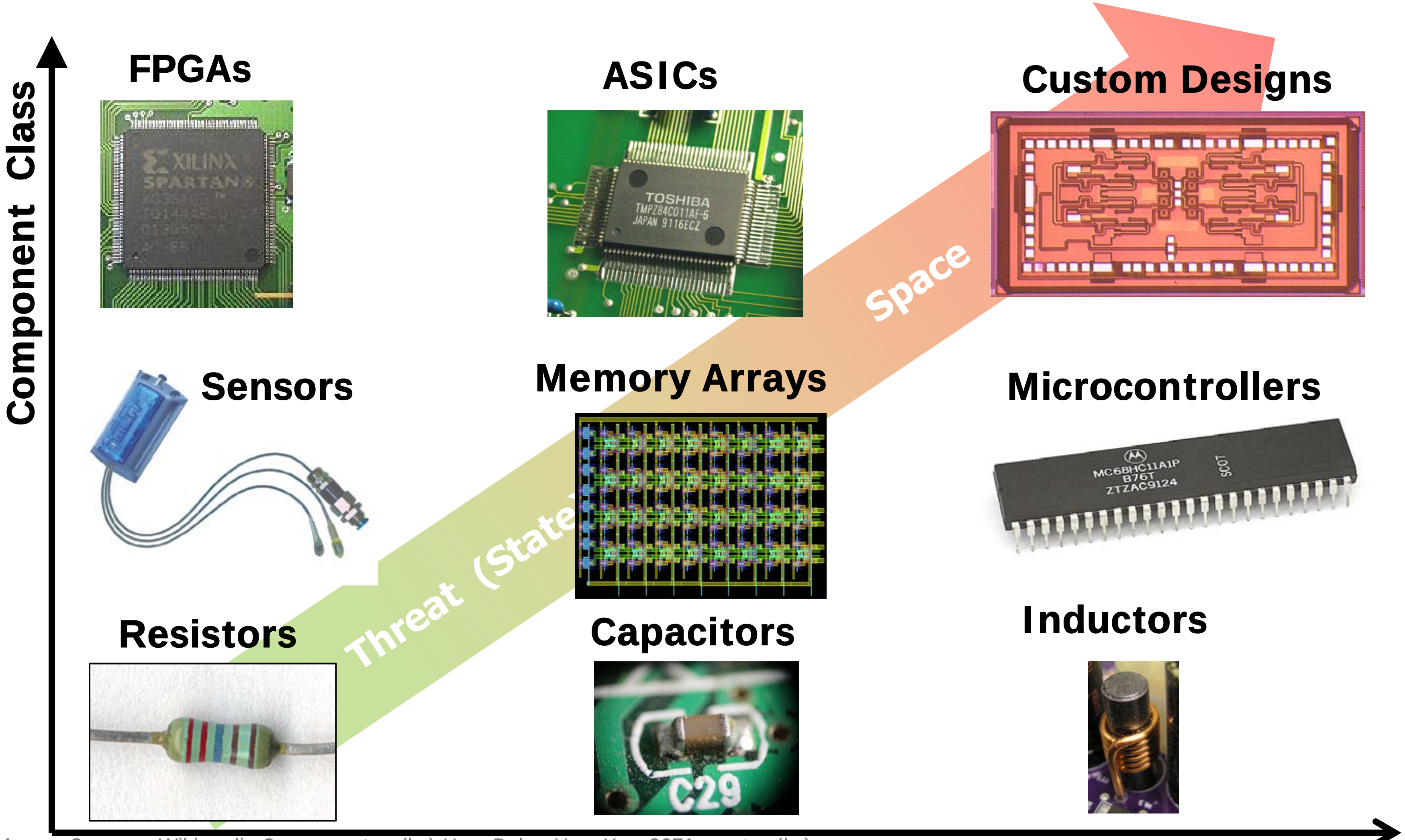
Distribution Statement A, Approved for Unlimited Distribution.

Outline

- Motivation for Hardware Authentication
- Assessing Complexity For Security
- Program Overviews
- Emerging Issues in Hardware Cyber

Distribution Statement A, Approved for Unlimited Distribution.

Varieties of Potentially Vulnerable Computing Components



Component Class

FPGAs

ASICs

Custom Designs

Sensors

Memory Arrays

Microcontrollers

Resistors

Capacitors

Inductors

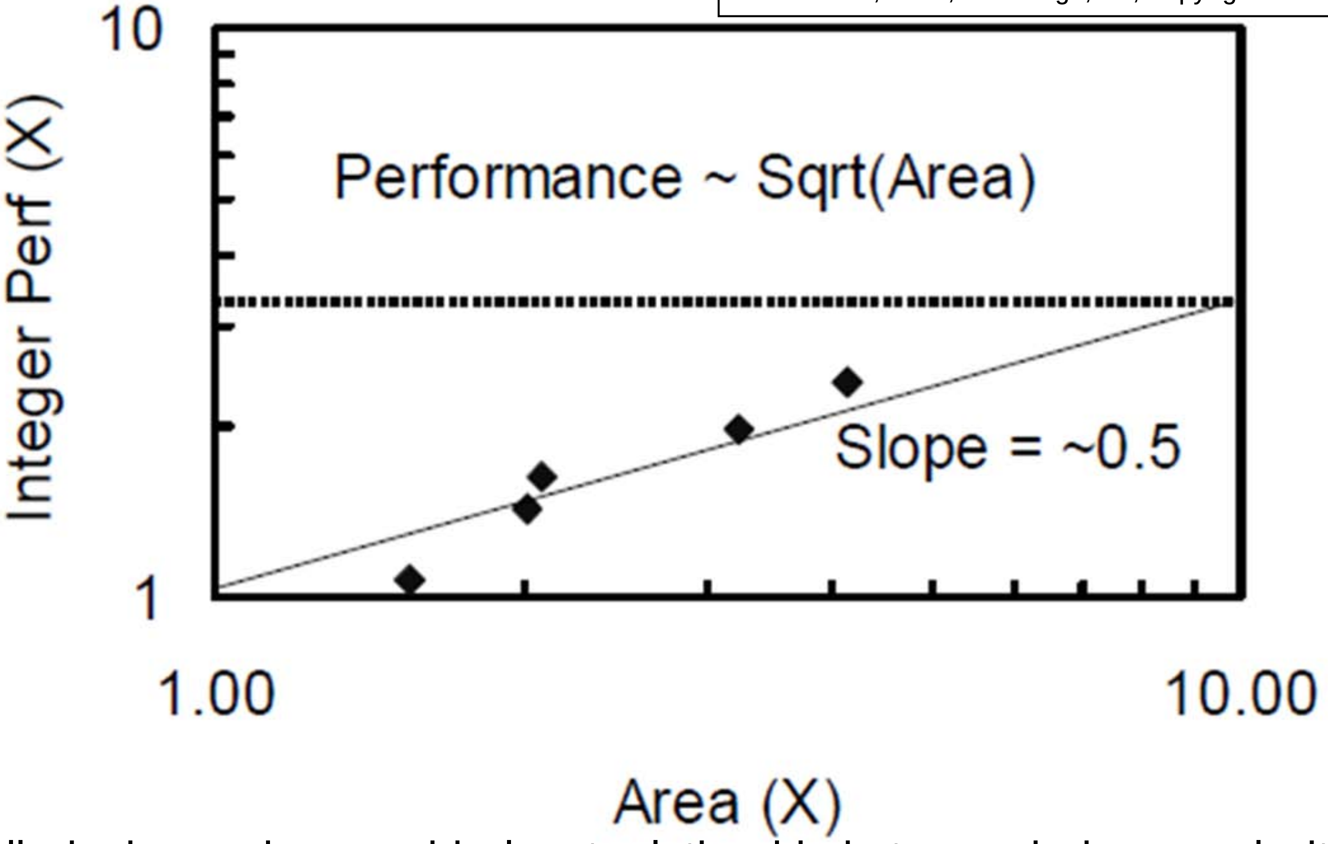
Threat (State) Space

Component Complexity

Image Sources: Wikimedia Commons top (l-r) User:Dake, User:Yaca2671, center (l-r) User:MSRDatenlogger, Konstantin Lanzet, bottom (l-r) User: Janke, Alex Khimich, Audrius Meskauskas

Pollack's Rule *

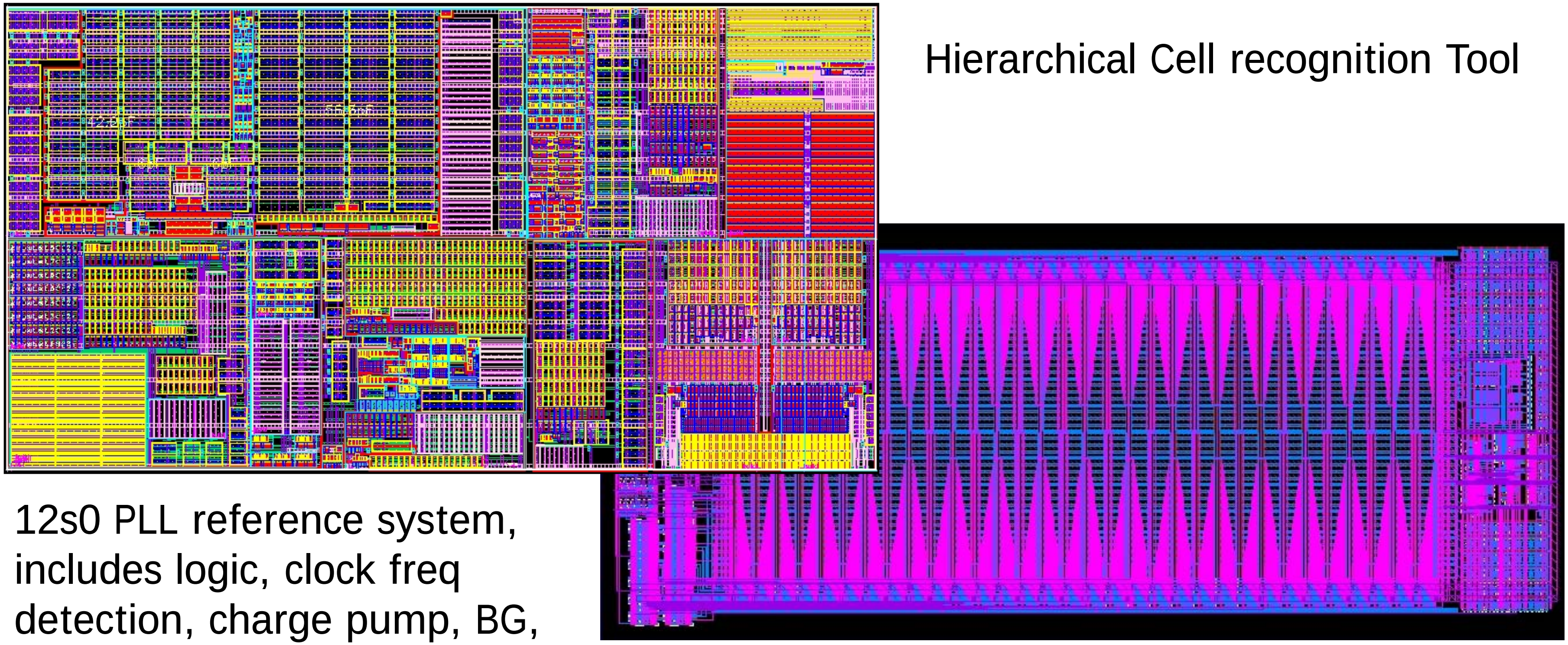
* From "**Thousand Core Chips—A Technology Perspective"** Shekhar Borkar *DAC 07*, June 4-8, 2007, San Diego, CA, Copyright 2007 ACM 1-58113-688-9/03/0006



- Pollack observed an empirical sqrt relationship between design complexity (i.e. *chip area*, or *number of devices*) and performance
- But Analytic treatment of complexity needs a more quantitative model

(BTW – **Pollack anticipated our need to go multicore**: improving thru-put as sqrt(C) was clearly a losing proposition for Uniprocessors !!!)

Layout-Based Analog Complexity Assessment

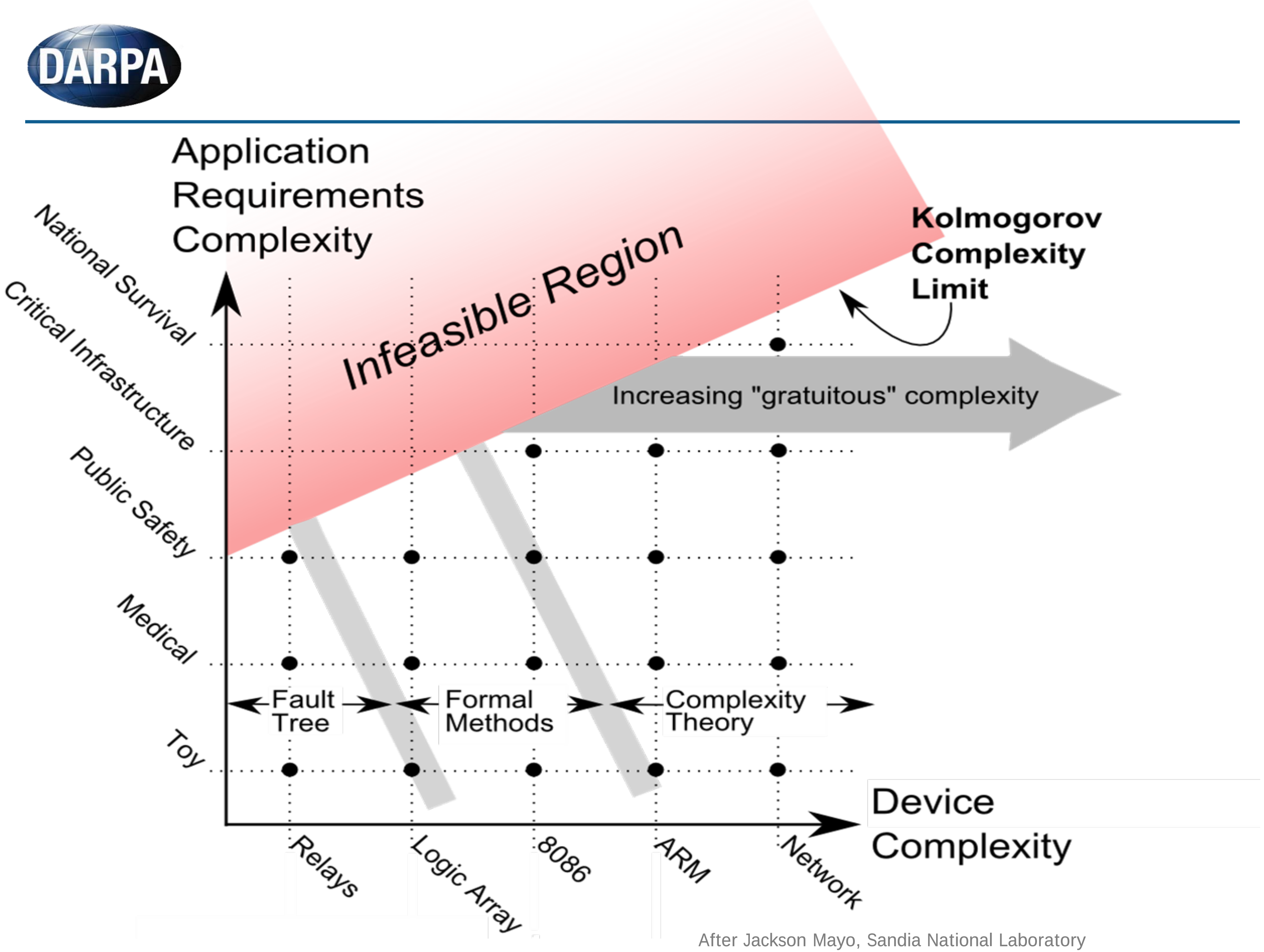


Hierarchical Cell recognition Tool

12s0 PLL reference system, includes logic, clock freq detection, charge pump, BG, current mirrors, dividers, V2I, multiple high current reg. stages, comparators. Approximately **1K FETs** and other components.**450 um x 240um (1.08E5 um^2)**.

DAC in 10LP. Approx 1K resistors, **1K FETS** in the main section, 100 FETs + caps on the right, logic on the left. **800um x 350um (2.80E5 um^2)**

Same component count, similar areas - different complexity

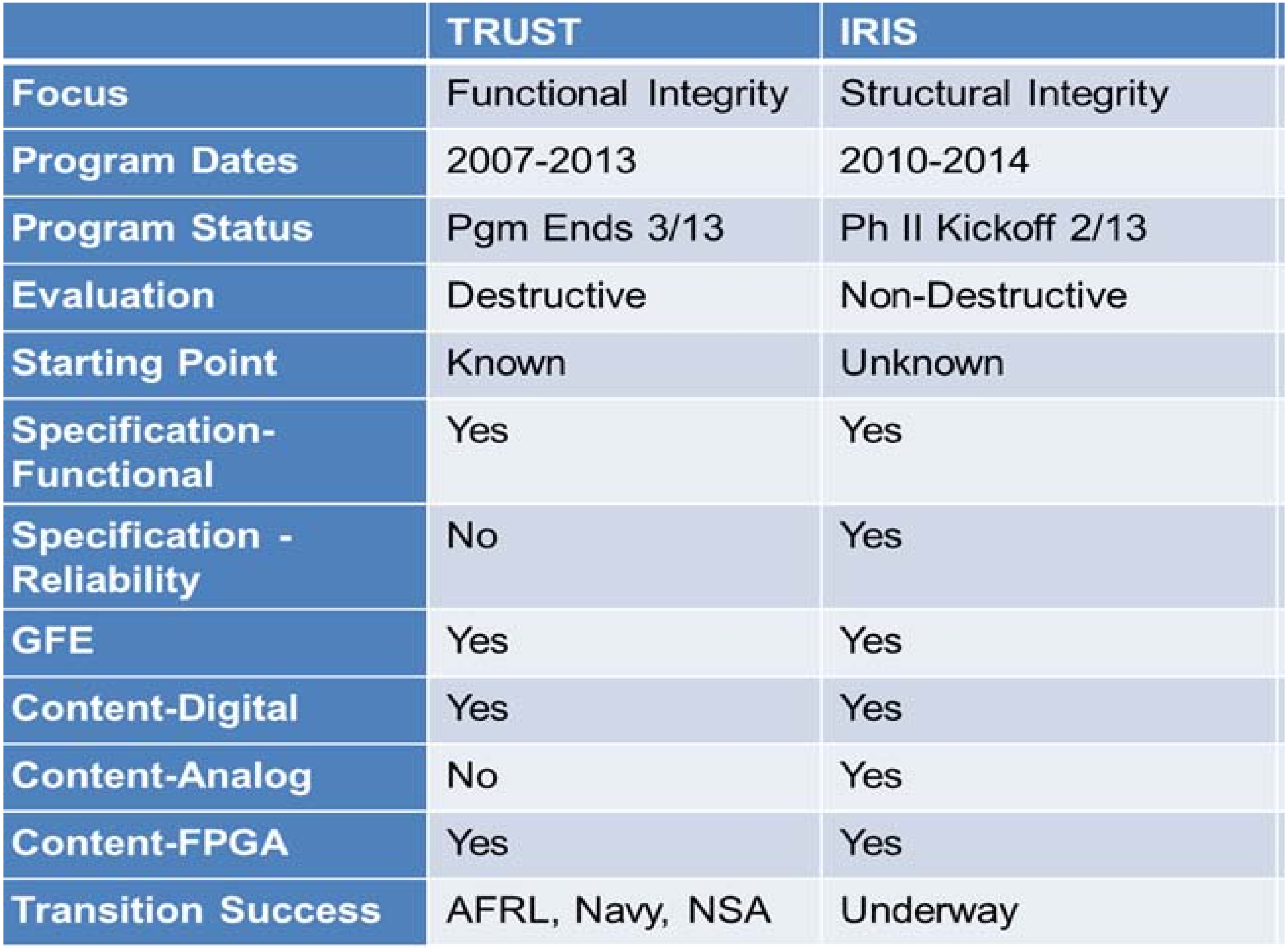


After Jackson Mayo, Sandia National Laboratory

Outline

1. Motivation for Hardware Authentication
2. First – Assessing Complexity For Security
3. Program Overview
4. Emerging Issues in Hardware Cyber

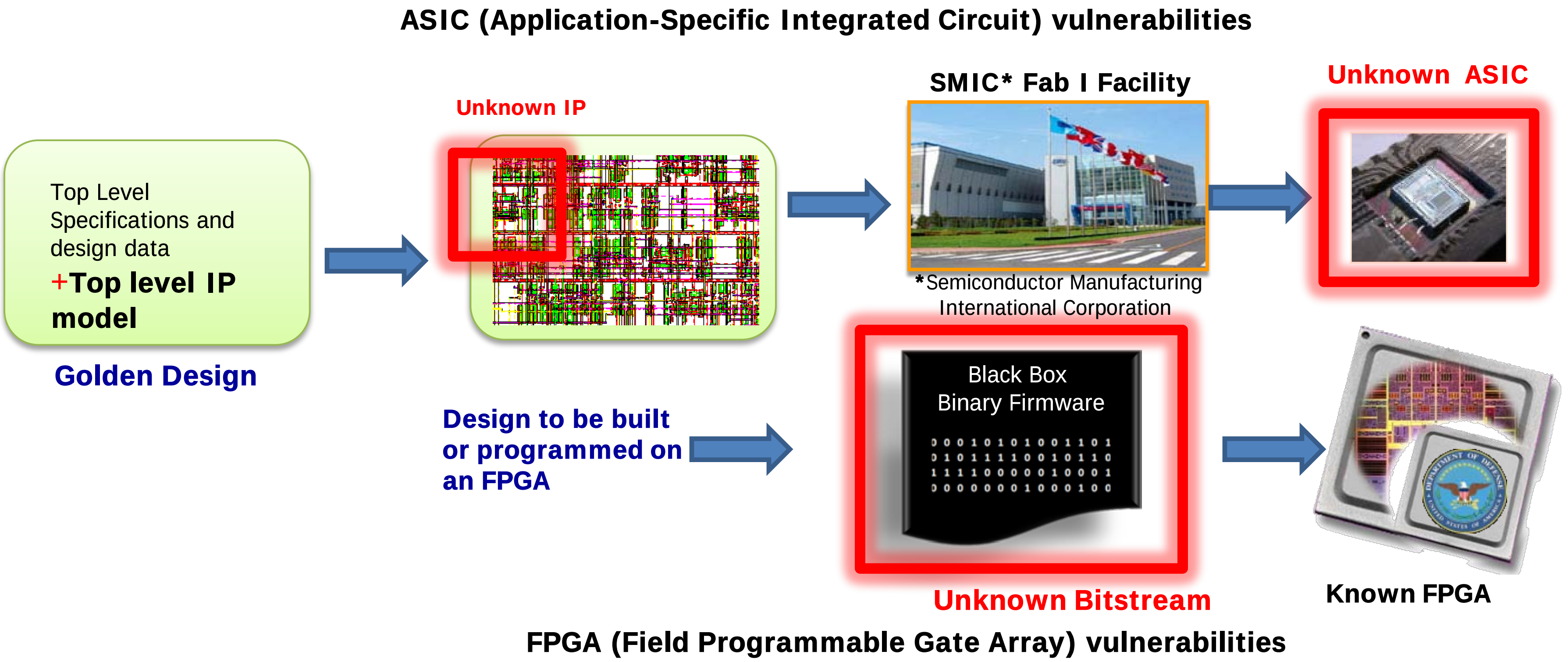
DARPA MTO Hardware Cyber Program Matrix



	TRUST	IRIS
Focus	Functional Integrity	Structural Integrity
Program Dates	2007-2013	2010-2014
Program Status	Pgm Ends 3/13	Ph II Kickoff 2/13
Evaluation	Destructive	Non-Destructive
Starting Point	Known	Unknown
Specification-Functional	Yes	Yes
Specification - Reliability	No	Yes
GFE	Yes	Yes
Content-Digital	Yes	Yes
Content-Analog	No	Yes
Content-FPGA	Yes	Yes
Transition Success	AFRL, Navy, NSA	Underway

* FPGAs dropped in IRIS Phase II to be treated entirely separately.

Vision: ICs Used in Weapons Systems Must Perform as Designed – No More, No Less



ASIC (Application-Specific Integrated Circuit) vulnerabilities

Top Level Specifications and design data

+Top level IP model

Golden Design

Unknown IP

SMIC* Fab I Facility

*Semiconductor Manufacturing International Corporation

Unknown ASIC

Design to be built or programmed on an FPGA

Black Box Binary Firmware

Unknown Bitstream

Known FPGA

FPGA (Field Programmable Gate Array) vulnerabilities

- No current solutions exist today that can analyze an advanced IC in less than 6 months – requires substantial capital investment
- The TRUST program addresses this critical and growing problem for the DOD in 4 thrusts
  - Trust in fabrication for ASICs
  - Trust in design for ASICs
  - Trust in FPGAs
  - Trust in third-party intellectual property (3PIP)
- DARPA has been working with transition partners throughout Phase III

Distribution Statement A, Approved for Unlimited Distribution.

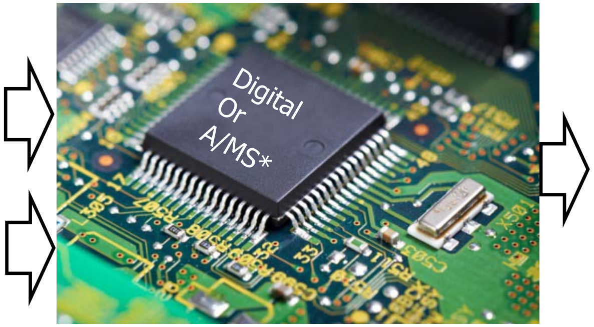
IRIS Program:
Integrity and Reliability of Integrated Circuits

Extract functionality and predict reliability of military ICs

COTS or GOTS Integrated Circuit
(unknown architecture, incomplete specifications)

Apply functionality and reliability analysis tools

Use non-destructive imaging techniques



*Analog/Mixed-Signal

Capability Objectives

- Derive 95% of the functionality of ICs utilized in military systems
- Verify the reliability of commercial ICs acquired for military systems

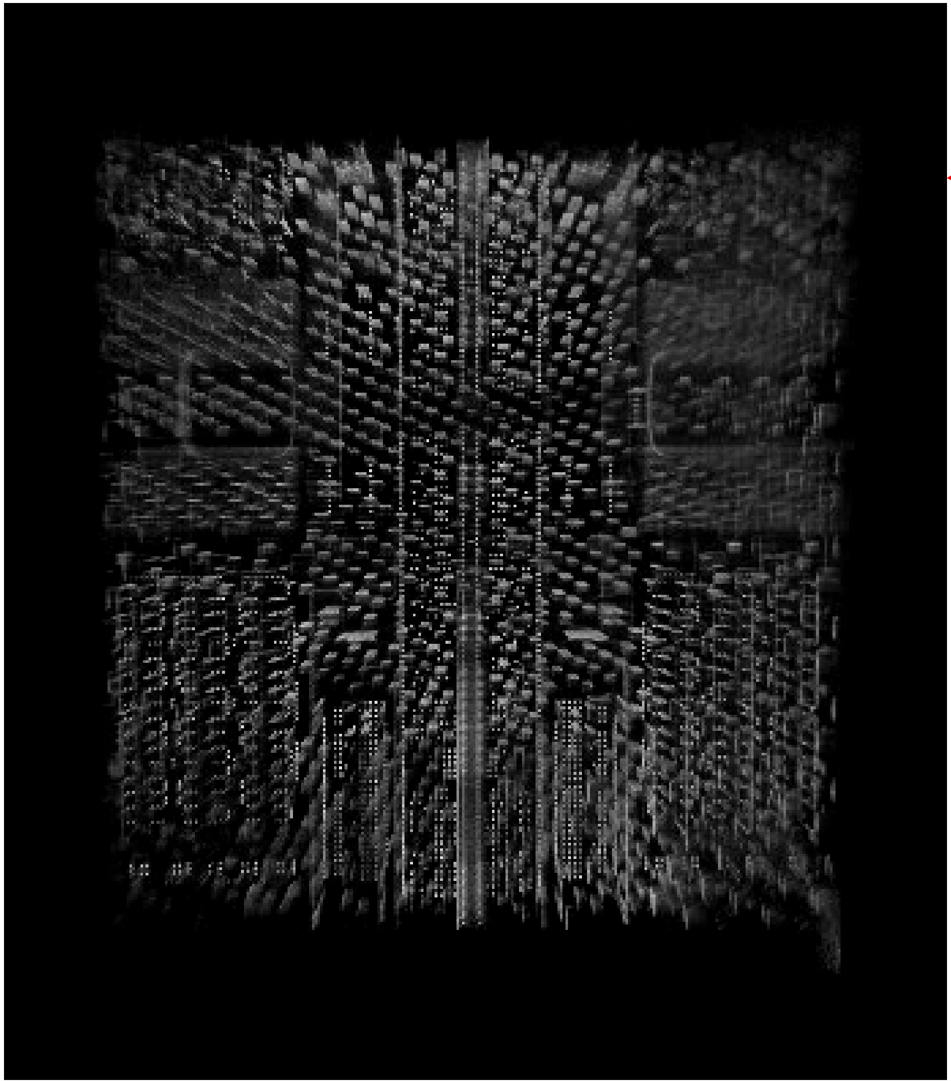
Goals

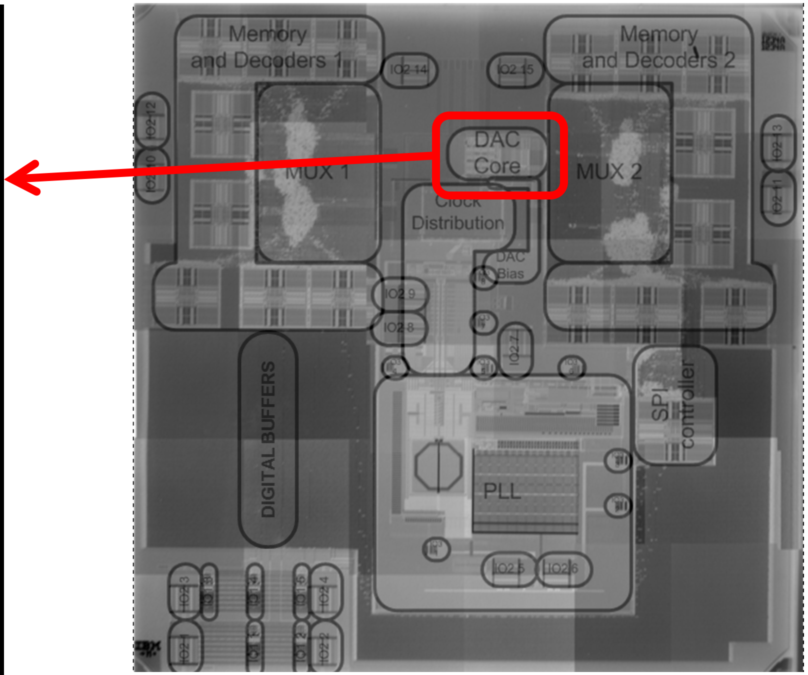
- Develop tools capable of determining the functionality of ICs in cases where the complete IC spec is not known or available
- Develop techniques for reliability testing using small sample sizes / reduced test time
- Validate these methodologies on current design topologies:
  - Digital and Analog/Mixed-Signal ASIC circuits
  - Field Programmable Gate Arrays (FPGA)
  - Third Party Intellectual Property Cores

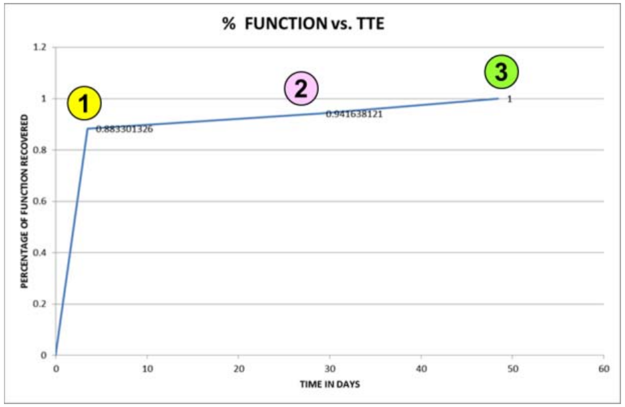
Reverse Engineering (RE) Observations

1. RE techniques scale *inversely* with technologies: As device count grows, analysis area shrinks
2. There's a *strong non-linear component* to scaling impact:
   a. Non-destructive reverse engineering ("far-field observation", w/ conventional optics, sensors) resolution already inadequate; incapable of supporting future scale
   b. Study at required scales (i.e < 10 nm) requires at least partial destructive RE.
      - Backside silicon removal
      - Front-side delayering
3. Frequency Scaling introduces additional obfuscation
4. New Materials (i.e. HfO2) require additional techniques
5. **Hierarchical assertion** to steer advanced RE tooling is *essential* going forward as device counts continue to climb

3D RECONSTRUCTION OF DAC - NON DESTRUCTIVE





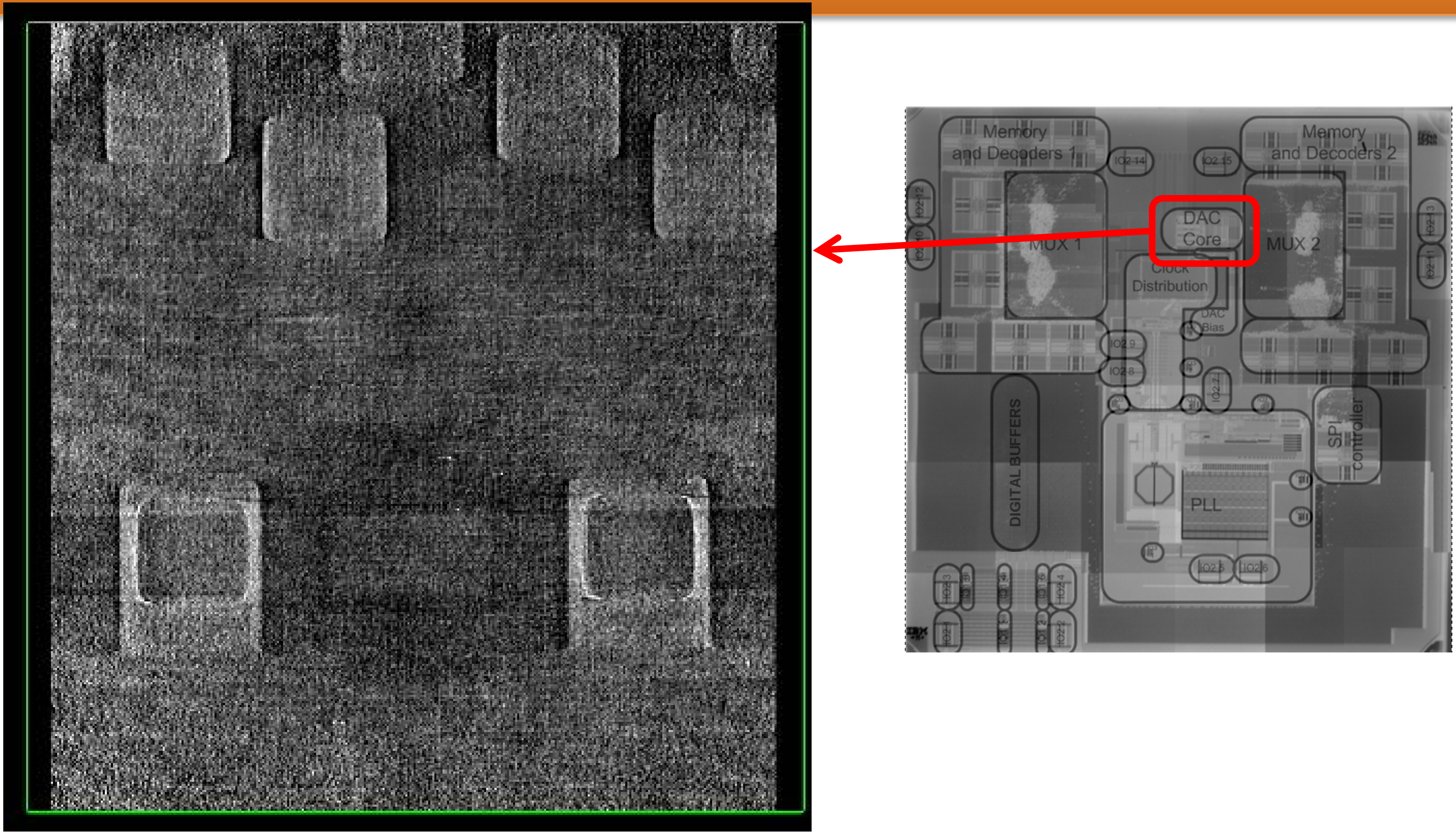


ENABLES 3D VISUALIZATION AND SPATIAL ANALYSIS

NON-DESTRUCTIVE SENSING

LAYER EXTRACTION ON DAC

HIGH RESOLUTION IN DEPTH ENABLES LAYER SEPARATION AND MEASUREMENT OF THICKNESS WITHOUT GRINDING



Distribution Statement A, Approved for Unlimited Distribution

Outline

- Motivation for Hardware Authentication
- Assessing Complexity For Security
- Program Overviews
- Emerging Issues in Hardware Cyber

Distribution Statement A, Approved for Unlimited Distribution

Advanced Future Supply Chain Risk Management

Chain of Custody and precision logistics are insufficient to track a global supply chain, and hierarchical program development

Advanced Supply Chain technologies will provide important new insights beyond simple authentication:

- Present location
- Age
- Fab, lot, wafer of origin
- Operating condition, current opcodes
- Emanating? TEMPESTed?

- Removed and Replaced?
- Chain of custody
- Temperature extremes seen
- AT Sensor activated?
- Autonomic or remotely invoked Self-destruct

Future SCRM Technologies include

- **PUFs**
- **Strained glass**
- **Botanical DNA**
- **RFID or Bluetooth Tags**

- **Ring Oscillators**
- **Memory Bias**
- **Isotope tags**
- **IDD**

Anticipating Change

Images.wikia.com/harrypotter/images/9/94Hogwarts_Grnad_Staircase_and_portraits_in_1966.JPG www.darpa.mil

Distribution Statement A, Approved for Unlimited Distribution