RAPID AUTHENTICATION THROUGH VERIFICATION, VALIDATION, AND MARKING

Mr. Kerry Bernstein, DARPA/MTO Program Manager

NDIA Trusted Microelectronics Workshop

August 17, 2016

The DARPA solution is to provide a menu of hardware security options that can be selectively applied based on need

High Government Intervention

↕

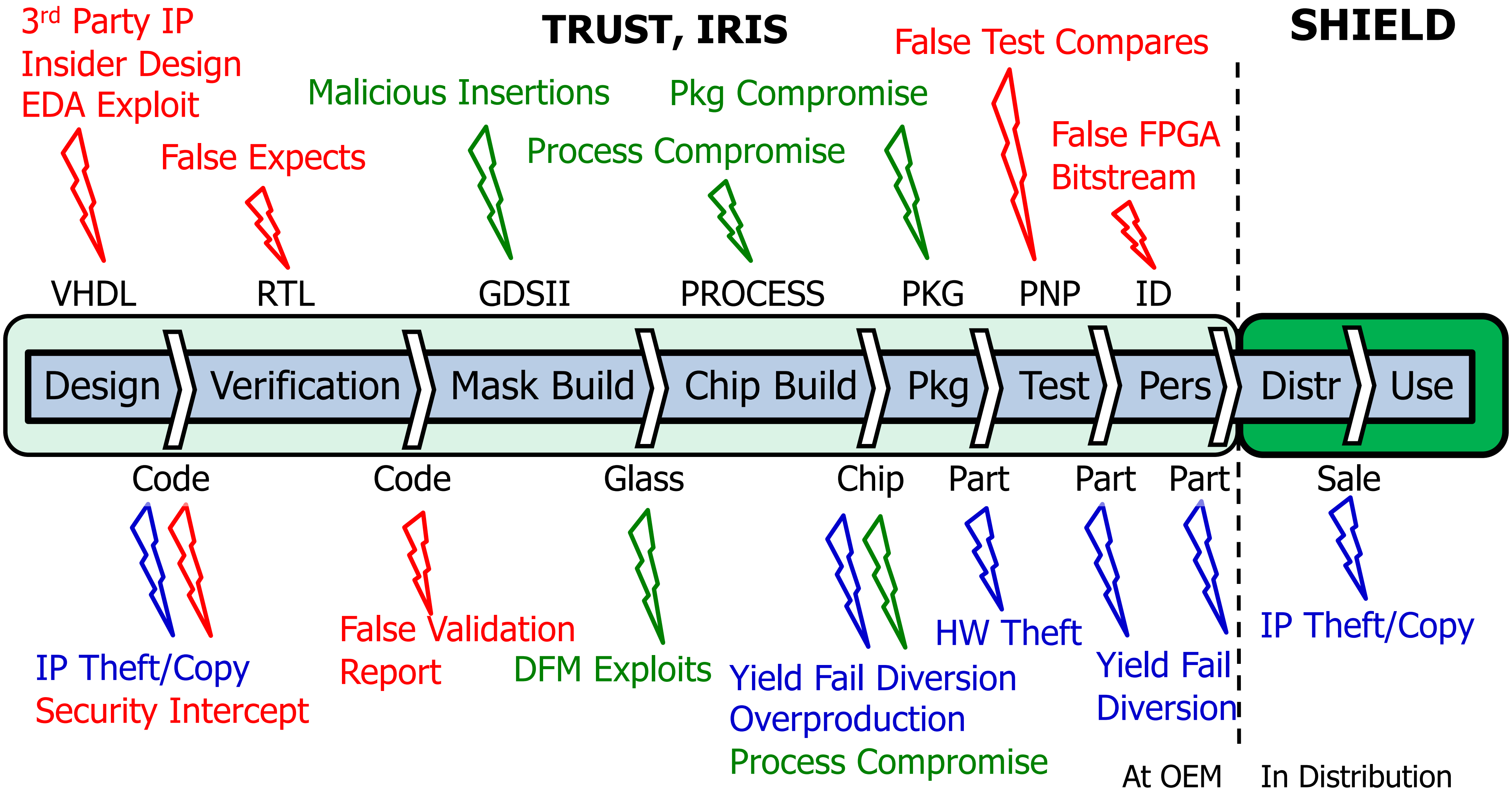
High Commercial Sponsorship

		Microelectronics Security Threats				
Protection	*Program*	Loss of information	Fraudulent products	Loss of access	Malicious insertion	Quality and reliability
Government-proprietary	Other	●				
Fine Disaggregation and Transience	TIC (IARPA)	●	●	○	○	
	VAPR	●				
Functional Disaggregation	SPADE	●			●	●
	DAHI	●		○	●	
	CHIPS	○		○	●	●
Obscuration and Marking	CRAFT			●		●
	eFuses	●			●	
	SHIELD	○	●			
Verification and Validation	IRIS		●		●	●
	TRUST		○		●	

SHIELD, IRIS, and TRUST can help protect against the introduction of fraudulent products and ensure that genuine microelectronics perform only as expected.

Hardware-specific exploits, mitigations

LEGEND: Design Attack - Hardware Attack - Logistics Attack



3rd Party IP
Insider Design
EDA Exploit

False Expects

Malicious Insertions

TRUST, IRIS

Process Compromise

Pkg Compromise

False Test Compares

False FPGA
Bitstream

SHIELD

VHDL RTL GDSII PROCESS PKG PNP ID

Design Verification Mask Build Chip Build Pkg Test Pers Distr Use

Code Code Glass Chip Part Part Part Sale

IP Theft/Copy
Security Intercept

False Validation
Report

DFM Exploits

Yield Fail Diversion
Overproduction
Process Compromise

HW Theft

Yield Fail
Diversion

IP Theft/Copy

At OEM

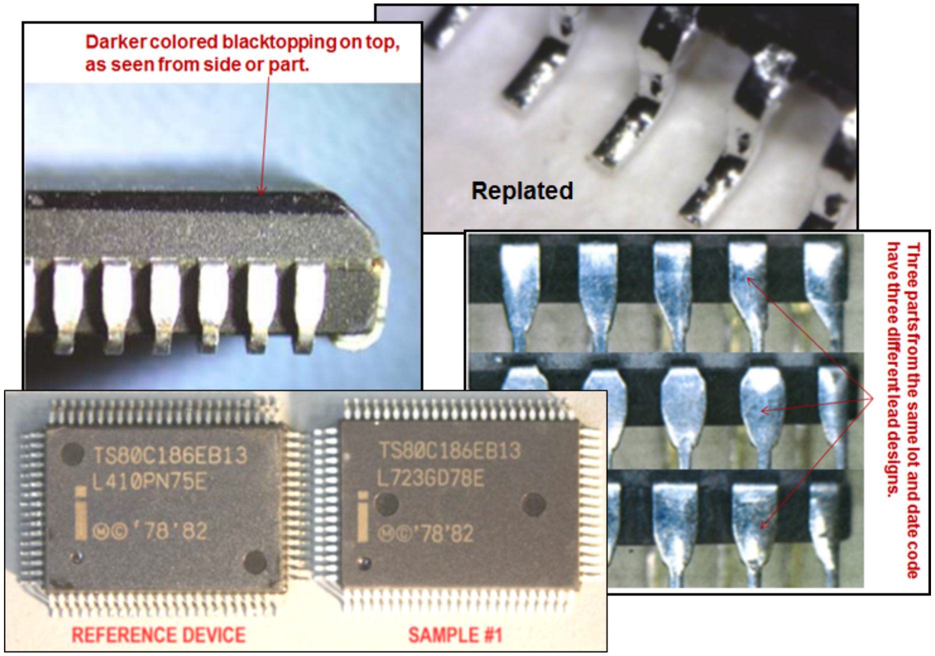
In Distribution

Counterfeits vs clones

Counterfeits

Still the original part from OEM:

- Recycled used components
- OEM's fab test failures sold on black market
- Unlicensed fab overproduction

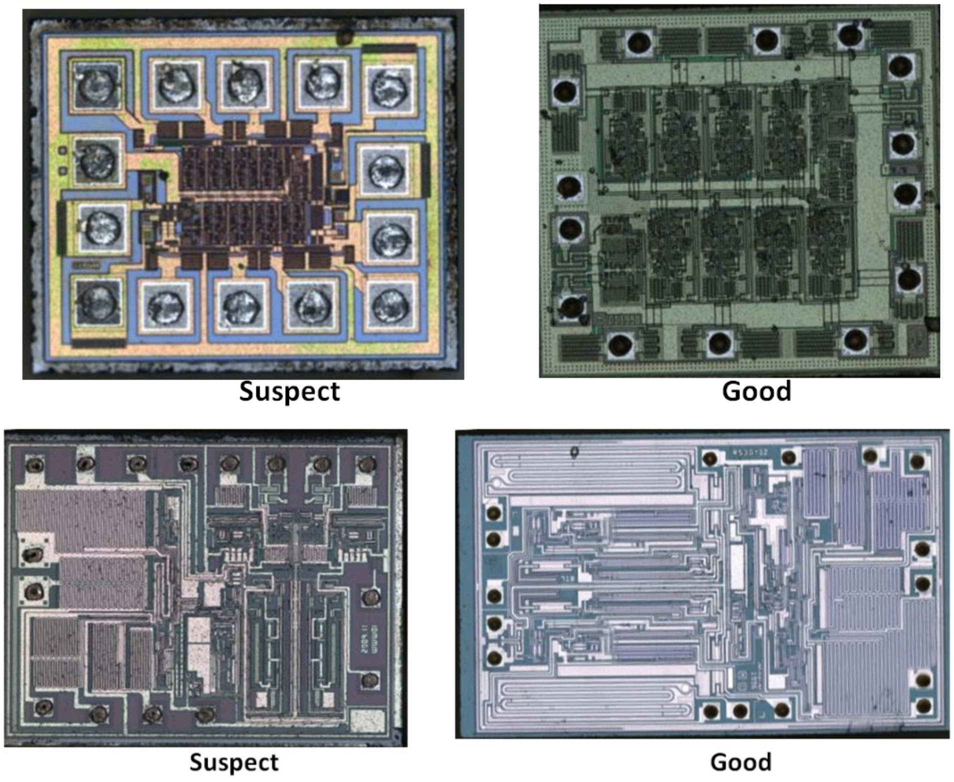

Darker colored blacktopping on top, as seen from side or part.
Replated
Three parts from the same lot and date code have three different lead designs.
TS80C186EB13
L410PN75E
©'78'82
TS80C186EB13
L723GD78E
©'78'82
REFERENCE DEVICE
SAMPLE #1

All images courtesy of NSWC CRANE

Clones

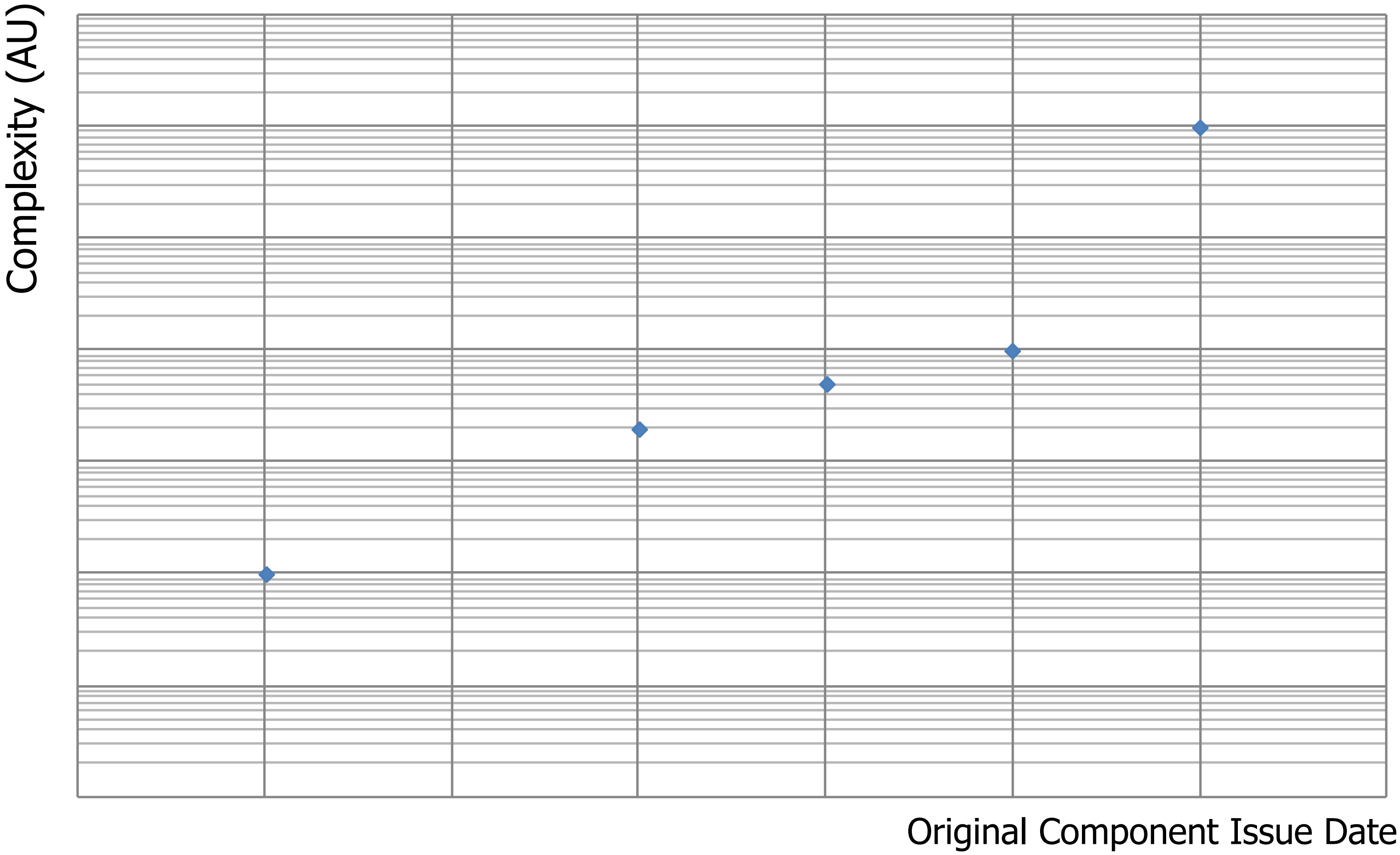
A completely different part:

- Copies fabbed in foreign plant
- New design of reverse-engineered components using stolen IP, potentially with altered function



Trend in reverse engineered + cloned component growth

Exemplary high-level clone discoveries collected over past 3 years*



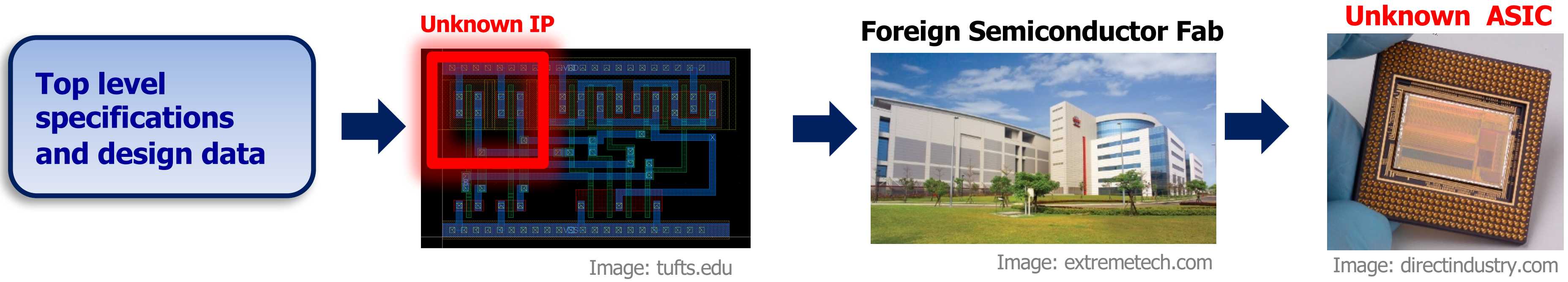
Counterfeiter skills for reverse engineering complex components are growing, and tracking Moore’s Law

* Developed with B. Hamilton, NSWC Crane

TRUST in Integrated Circuits

Integrated circuits must function as designed – no more, no less

ASIC (Application-Specific Integrated Circuit) vulnerabilities



Top level specifications and design data

Unknown IP

Image: tufts.edu

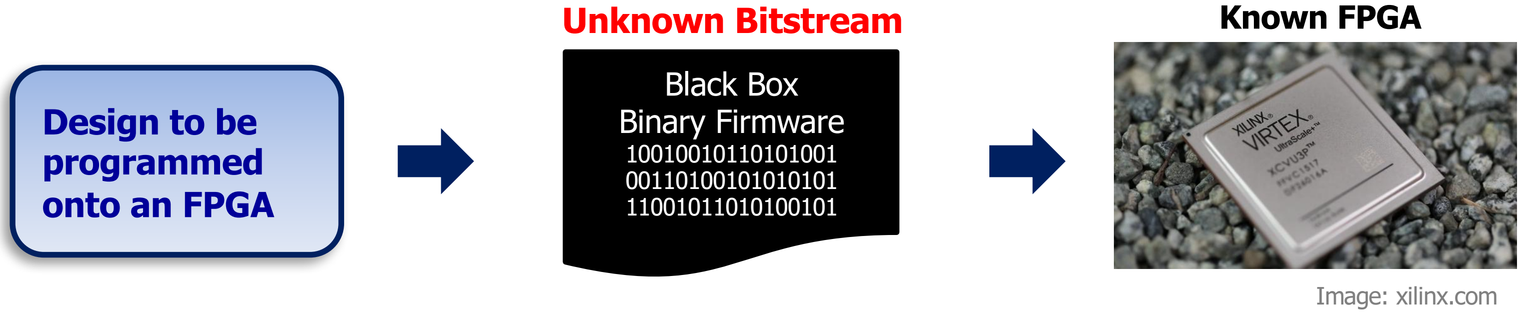
Foreign Semiconductor Fab

Image: extremetech.com

Unknown ASIC

Image: directindustry.com

FPGA (Field Programmable Gate Array) vulnerabilities



Design to be programmed onto an FPGA

Unknown Bitstream

Black Box
Binary Firmware
100100101101010001
001101001010101010
110010110101001010

Known FPGA

Image: xilinx.com

The TRUST program addressed these vulnerabilities in four thrusts:

1. Trust in fabrication for ASICs
2. Trust in design for ASICs
3. Trust in FPGAs
4. Trust in third-party intellectual property (IP)

Integrity and Reliability of Integrated circuitS (IRIS)

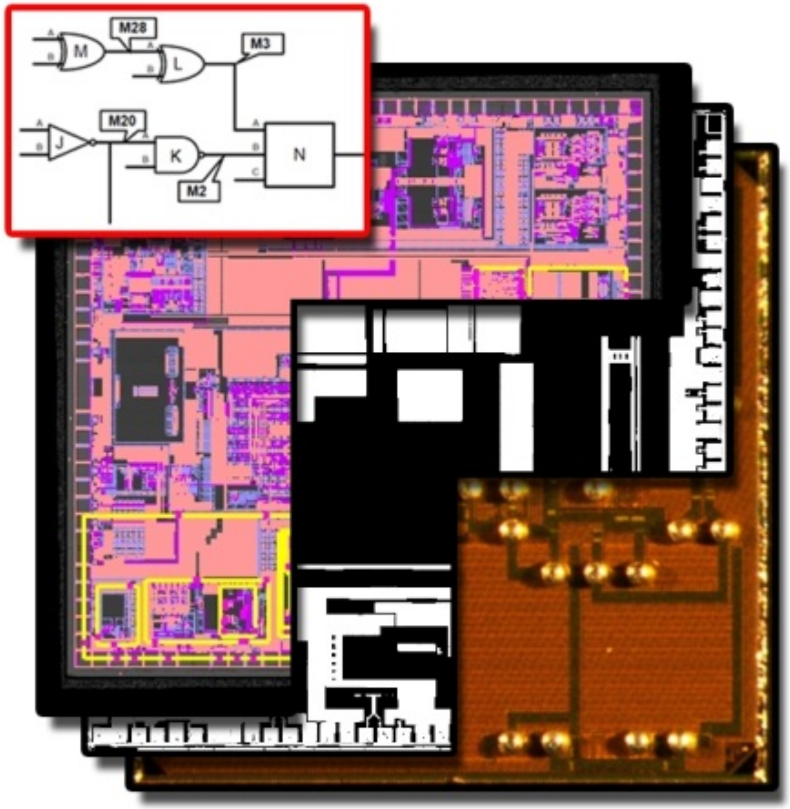
IC functionality extraction and reliability estimation

Objectives

- 100% functionality derivation given a limited data sheet and an IC, FPGA or 3rd party IP
- MTTF analysis of an IC given limited sample size
- Forensics to identify IC anomalies and determine impact on reliability

Capabilities developed

- Non-destructive imaging for feature resolution
- Algorithms for pattern recognition and netlist extraction
- Data analytics for functional derivation
- Advanced modeling and simulation techniques for reliability analysis



Artist's rendering of images provided by
Air Force Research Laboratory

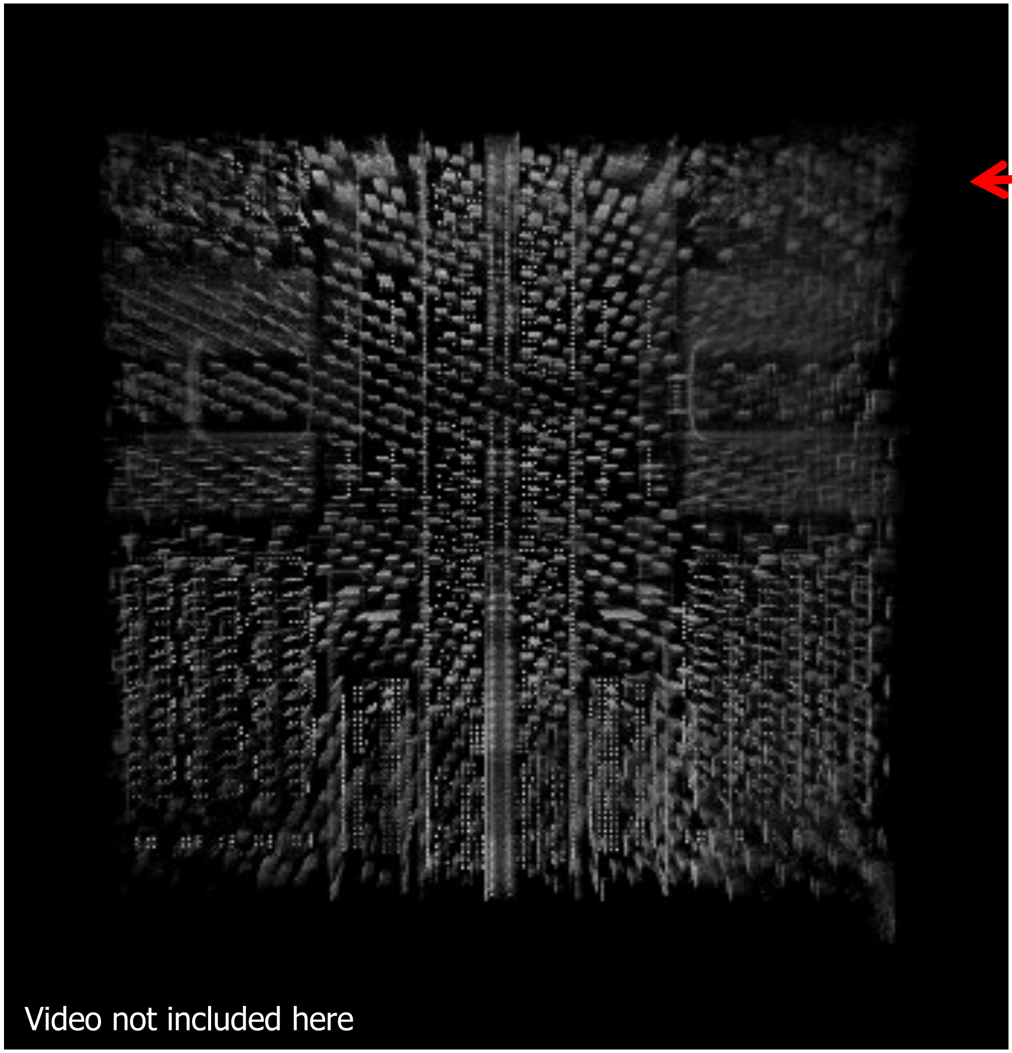
Virtual Laboratory

- Designed, developed and debugged test articles for performer analysis
- Evaluated performer techniques for scientific soundness, and results against program metrics

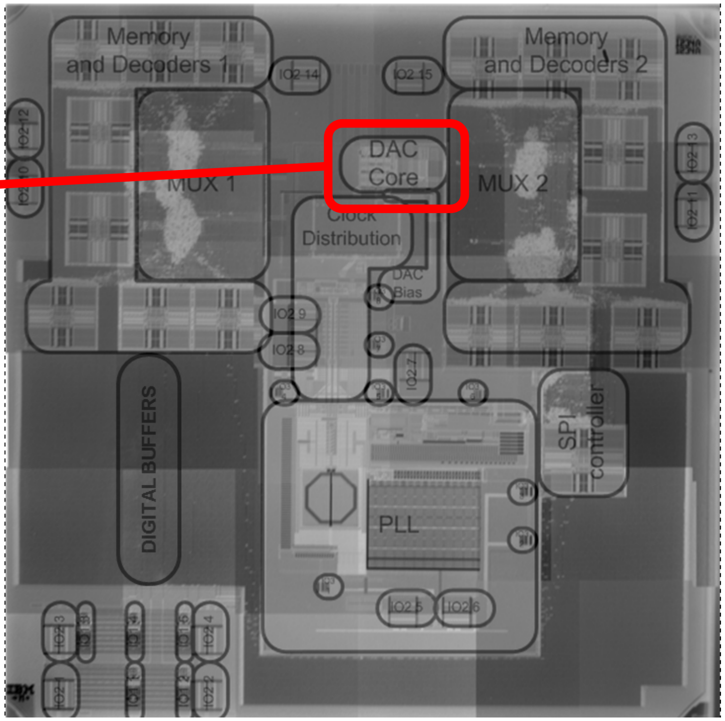
Performers

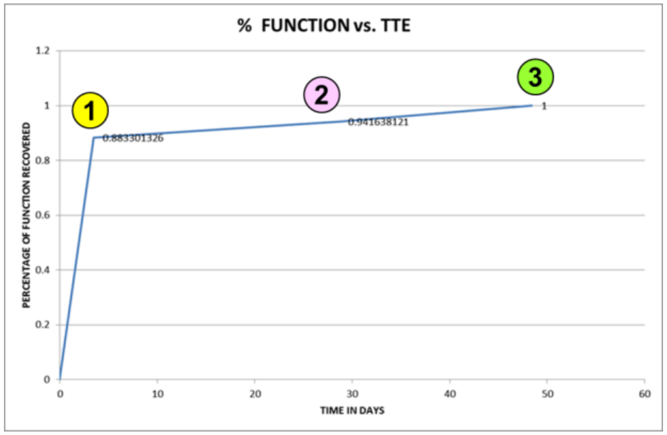
BAE Systems
SRI International
USC Information Sciences Institute
Raytheon
Luna (MacAulay Brown)
Orora
R3 Logic
Case Western Reserve Univ.
Georgia Tech
University of Michigan
Boeing
IBM
University of Arkansas

3D reconstruction of DAC – Non-destructive



Video not included here

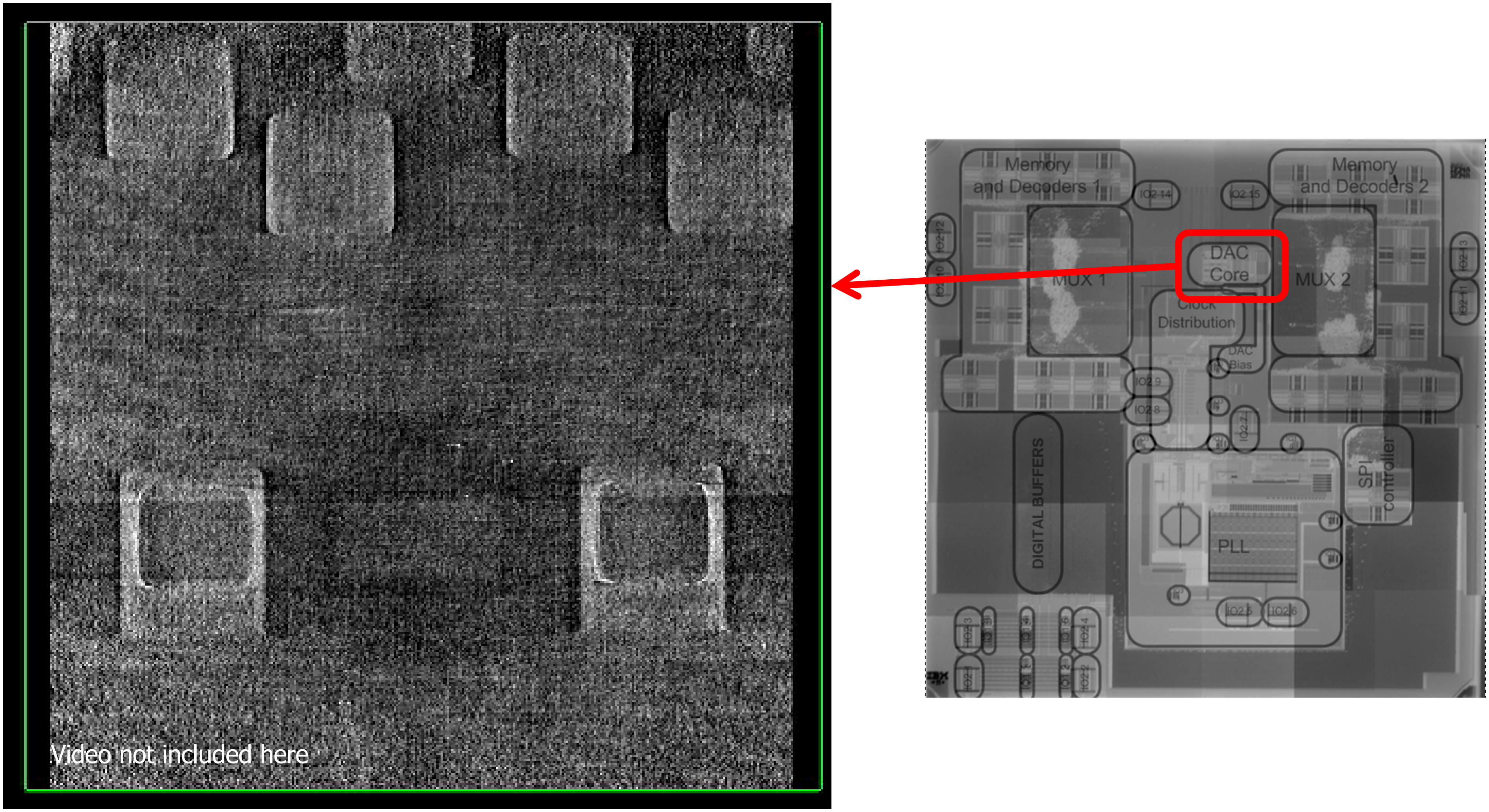




All images courtesy of SRI International

ENABLES 3D VISUALIZATION AND SPATIAL ANALYSIS

Layer extraction on DAC


Video not included here

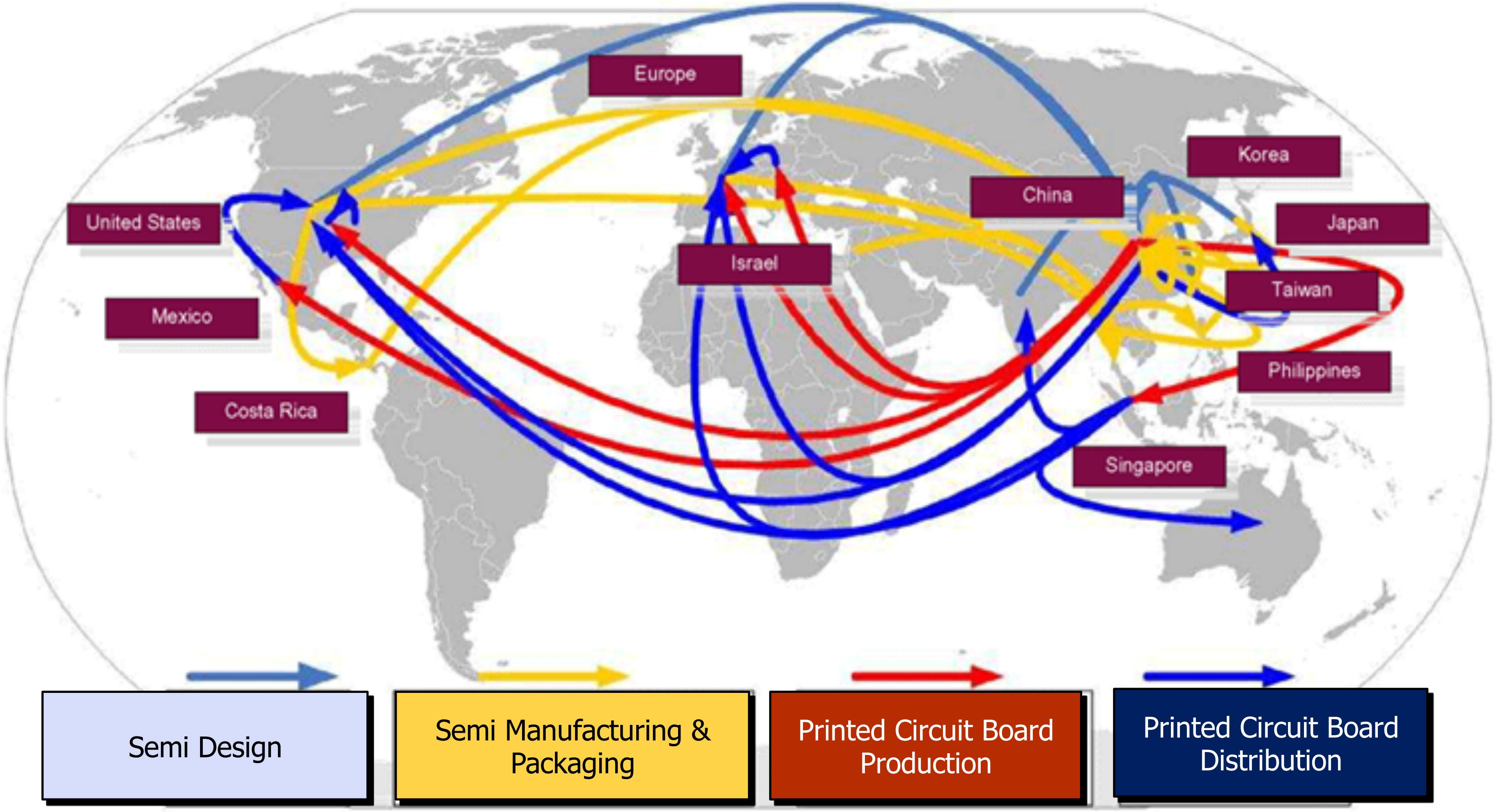
All images courtesy of SRI International

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

DISTRIBUTION A. Approved for public release: distribution unlimited.

The global nature of today's supply chains

Global nature of supply chain makes chain-of-custody unworkable



Semi Design

Semi Manufacturing & Packaging

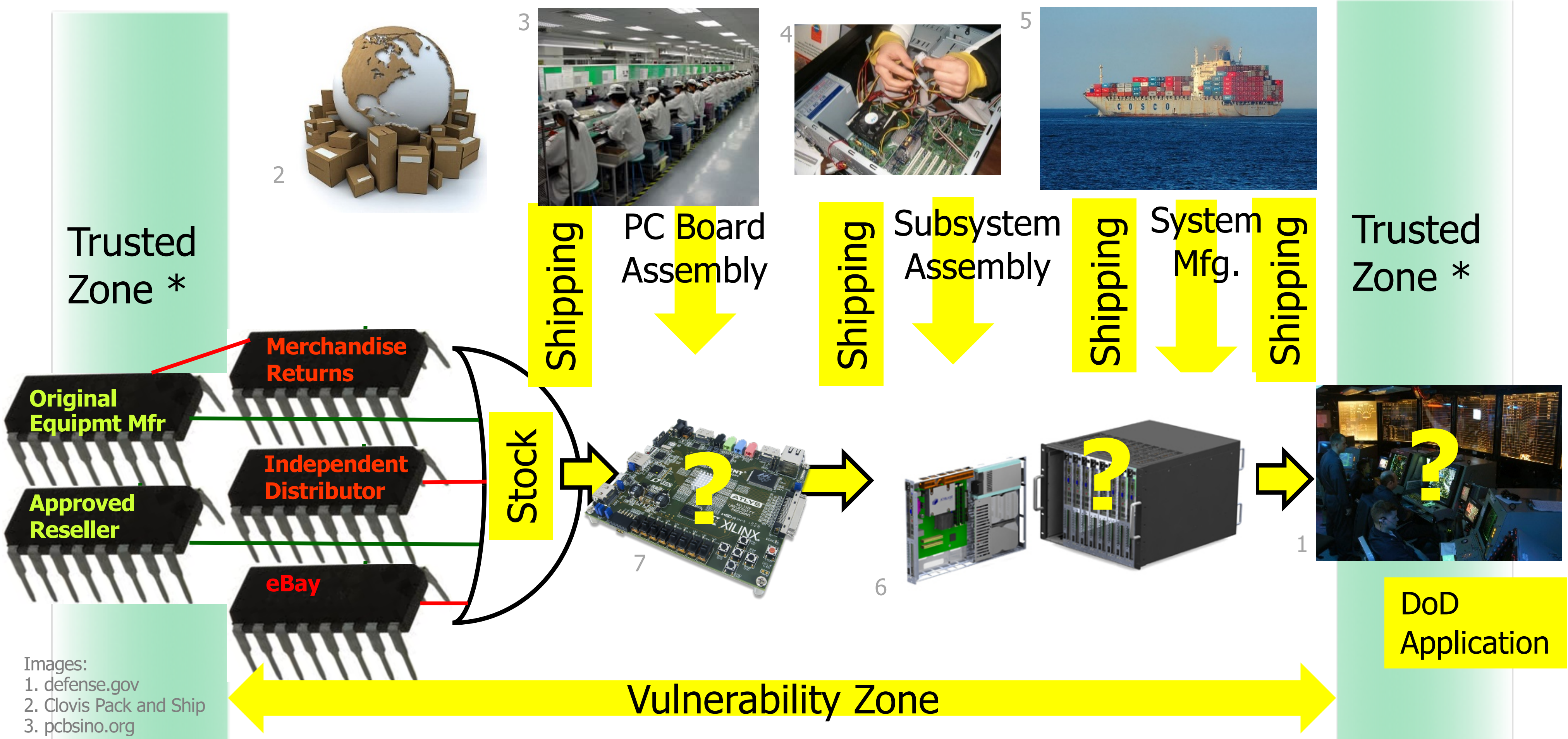
Printed Circuit Board Production

Printed Circuit Board Distribution

Source: IDC Manufacturing Insights & Booz Allen analysis

Lifecycle shown for a single Joint Strike Fighter component, which changes hands 15 times before final installation

Current untrusted logistical supply chain



Trusted Zone *

Original Equipmt Mfr

Approved Reseller

Merchandise Returns

Independent Distributor

eBay

Stock

Shipping

PC Board Assembly

Shipping

Subsystem Assembly

Shipping

System Mfg.

Shipping

Trusted Zone *

DoD Application

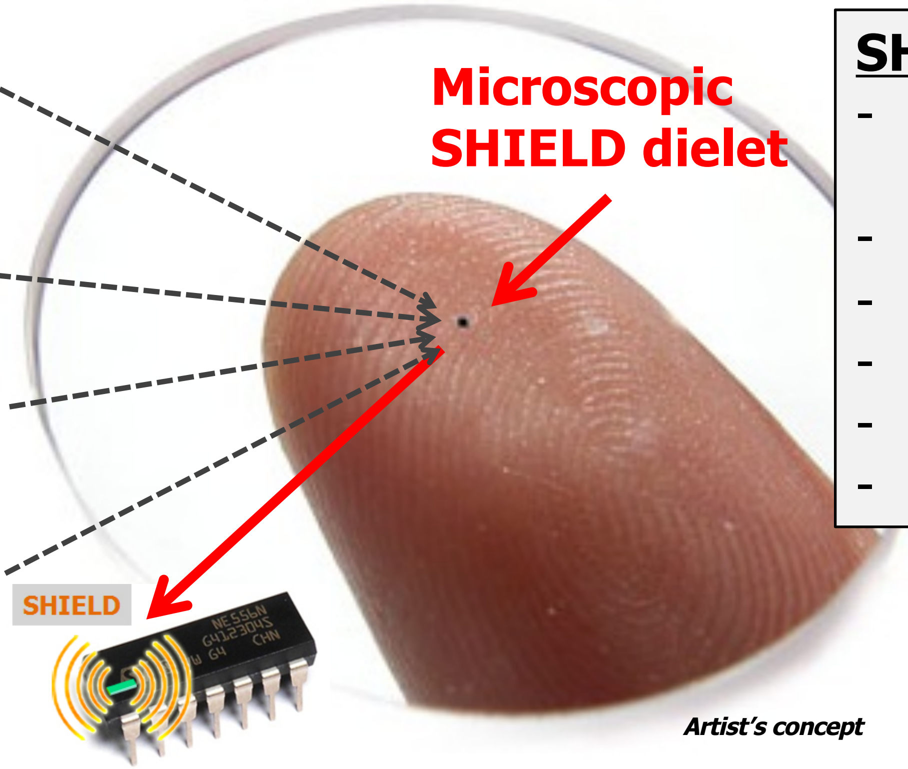
Vulnerability Zone

Images:
1. defense.gov
2. Clovis Pack and Ship
3. pcbsino.org
4. brighthub.com
5. Wikimedia commons
User: Fletcher6
6. texasmicro.com
7. digilent.com

For all but simplest exploits, DoD has little system component assurance of authenticity

***Assume parts have OEM integrity before leaving first Trusted Zone**

SHIELD: DARPA's supply chain solution



Hardware Root-of-Trust
Fragile Key Storage

Full Encryption Engine

Unpowered
Passive Sensors

Inductive Powering
and Communication

Microscopic SHIELD dielet

Artist's concept

<u>SHIELD Target Spec</u>

- **100μm x 100μm (0.01 mm² Area)**
- **100K Devices**
- **100 MHz Clock Rate**
- **50 μW Total Power**
- **T ≤ 120°C**
- **<1¢ per dielet**

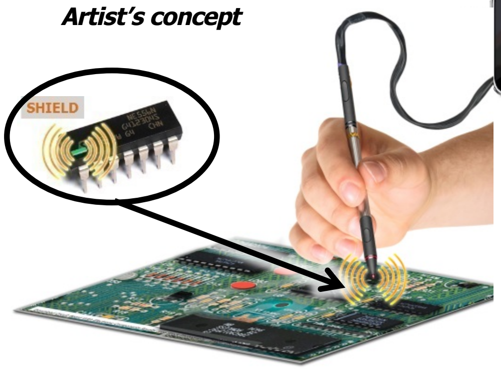
DARPA SHIELD will develop the ability to provide nearly 100% assurance against certain known threat modes quickly, on demand, at any step of the supply chain, at extremely low cost.

SHIELD makes counterfeiting too expensive and too hard to do.

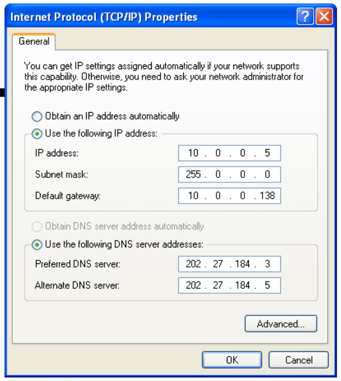
Image courtesy of Hitachi:
http://www.hitachi.com/New/cnews/030902.html

Example SHIELD CONOP

Artist's concept



TCPIP Address (VPN)



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 0 . 0 . 5

Subnet mask: 255 . 0 . 0 . 0

Default gateway: 10 . 0 . 0 . 138

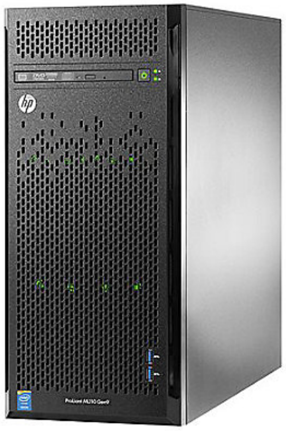
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

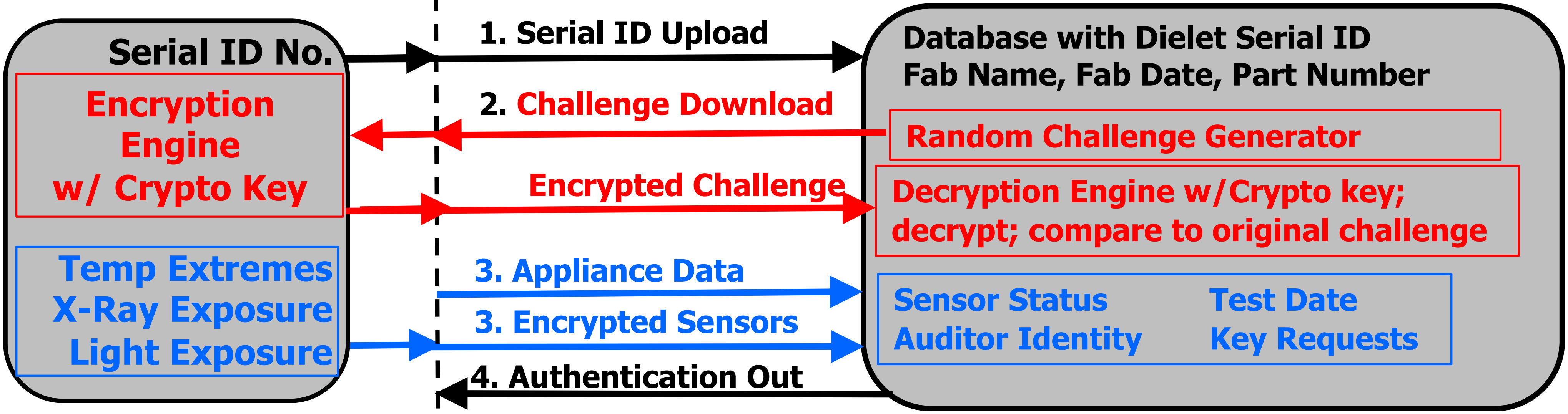
Preferred DNS server: 202 . 27 . 184 . 3

Alternate DNS server: 202 . 27 . 184 . 5

Image: cdw.com



Dielet **Smartphone** **Server**



Serial ID No.

Encryption Engine w/ Crypto Key

Temp Extremes
X-Ray Exposure
Light Exposure

1. Serial ID Upload

2. Challenge Download

Encrypted Challenge

3. Appliance Data

3. Encrypted Sensors

4. Authentication Out

Database with Dielet Serial ID
Fab Name, Fab Date, Part Number

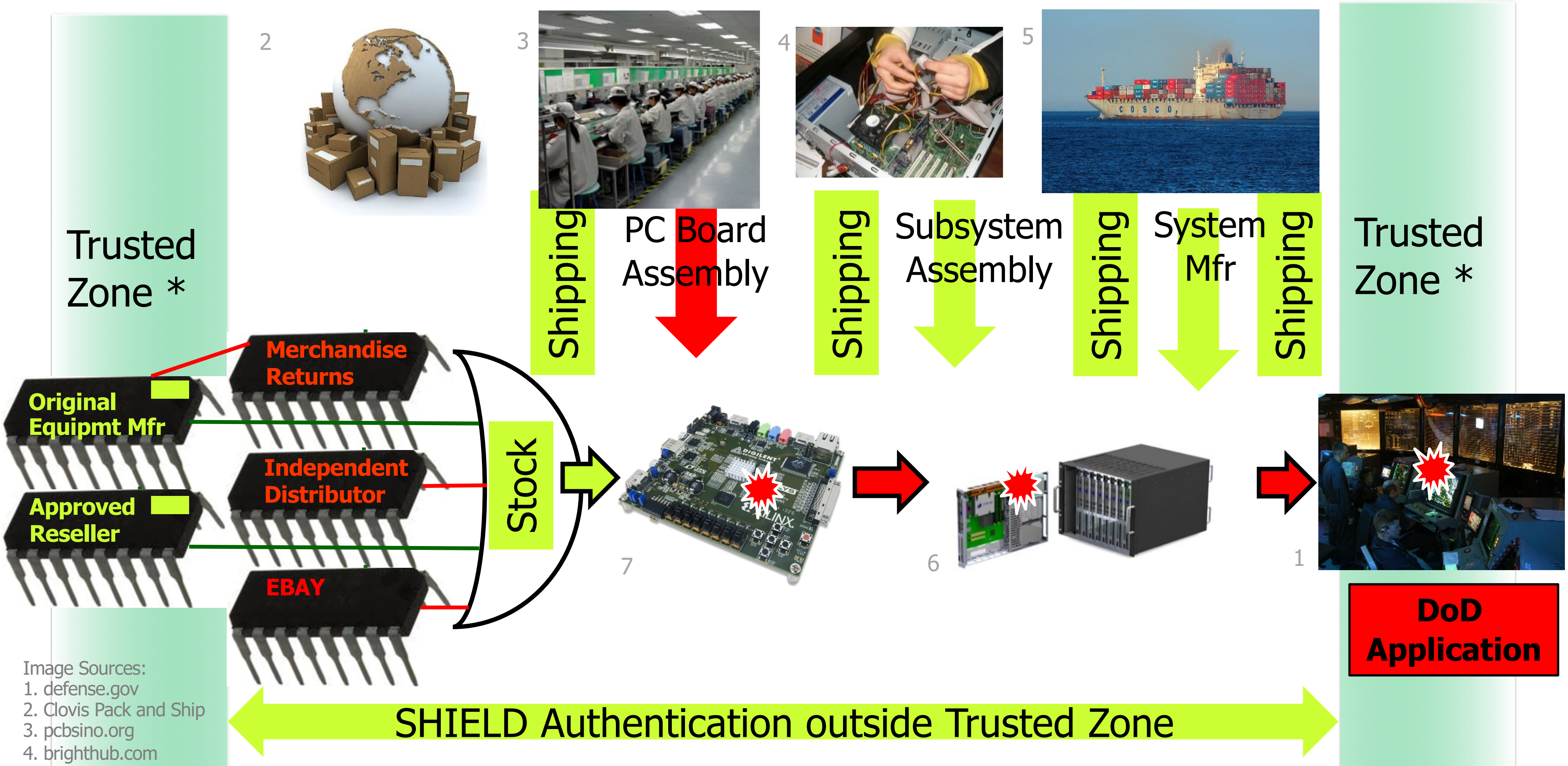
Random Challenge Generator

Decryption Engine w/Crypto key; decrypt; compare to original challenge

Sensor Status	**Test Date**
Auditor Identity	**Key Requests**

DISTRIBUTION A. Approved for public release: distribution unlimited.

Revisiting the supply chain – now with SHIELD implementation



Trusted Zone *

2

3

4

5

Shipping

PC Board Assembly

Shipping

Subsystem Assembly

Shipping

System Mfr

Shipping

Trusted Zone *

Original Equipmt Mfr

Approved Reseller

Merchandise Returns

Independent Distributor

EBAY

Stock

7

6

1

DoD Application

SHIELD Authentication outside Trusted Zone

Image Sources:
1. defense.gov
2. Clovis Pack and Ship
3. pcbsino.org
4. brighthub.com
5. Wikimedia commons
User: Fletcher6
6. texasmicro.com
7. digilent.com

Component compromises are now visible at any point along the supply chain

*** Assume parts have OEM integrity before leaving first Trusted Zone**

DISTRIBUTION A. Approved for public release: distribution unlimited.

What makes SHIELD “DARPA-worthy?”

At 100µm by 100µm by 10µm thick, the SHIELD dielet is on track to be the smallest integrated circuit ever developed

- Whole new technologies for building the “science of SMALL”
- Remote chip communication and powering using microscopic antennae
- Design of passive sensors that cannot be reset or inadvertently triggered

SHIELD dielet surrogate (SRI International)

Picking and Placing
A 100 µm x 100 µm x 10 µm
Silicon Dielet

DARPA SHIELD

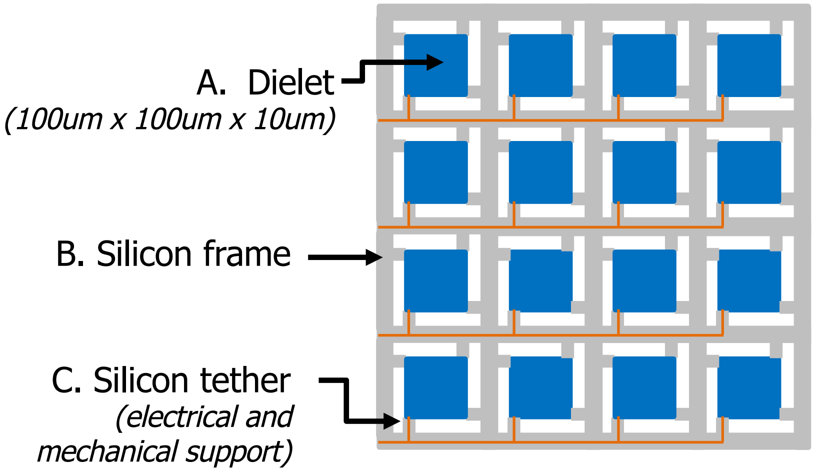
SRI International
July 28, 2015

Video not included here

Microscopic Sort and Pick (SRI International)

Example technology - Draper fragility

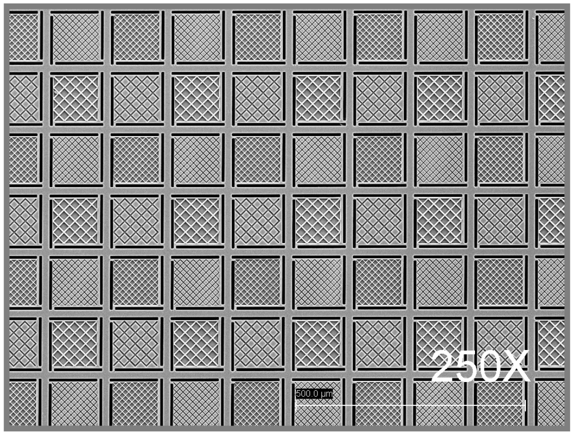
Goal: design and develop a high-yield, low cost architecture for the fabrication, testing, and packaging of ultra-thin (<10µm) dielets with engineered fragility



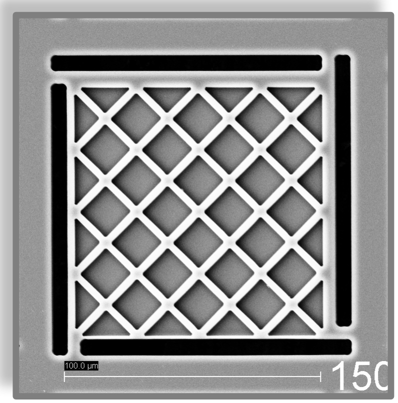
A. Dielet *(100um x 100um x 10um)*

B. Silicon frame

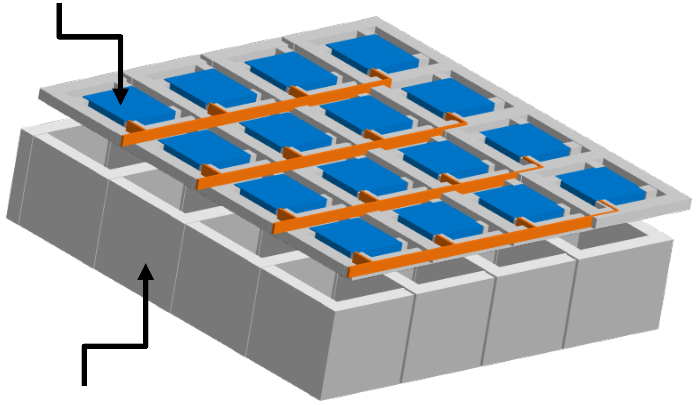
C. Silicon tether *(electrical and mechanical support)*



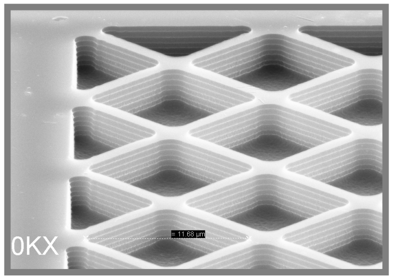
Top View (1,500x)



Released dielets anchored to a silicon frame



Carrier wafer with etched cavities under individual dielets



Perspective View (10,000x)

Video not included here

G. Perlin, et al.

Images courtesy of Draper Laboratories

Fab-of-Origin (ClearMark, Chromologic, IC Forensics)

- Fab-of-Origin looks for fab-signatures to identify origin of a component
- Idiosyncrasies associated with fab-specific tooling, recipe, sequence
- Needed to trace DoD, non-DoD clones and counterfeits to originating foundry (Smart Grid, Cyber Systems, Communications, etc…)

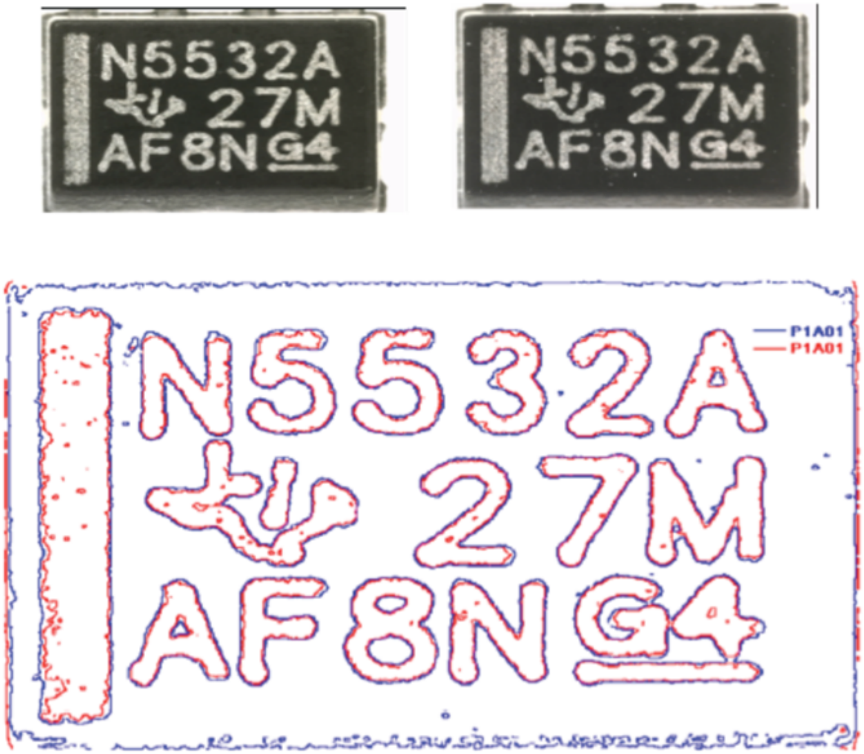
MTO SBIR SB133-03: Fab of Origin

http://mediad.publicbroadcasting.net/p/innovationtrail/files/201301/IMG_0362.JPG

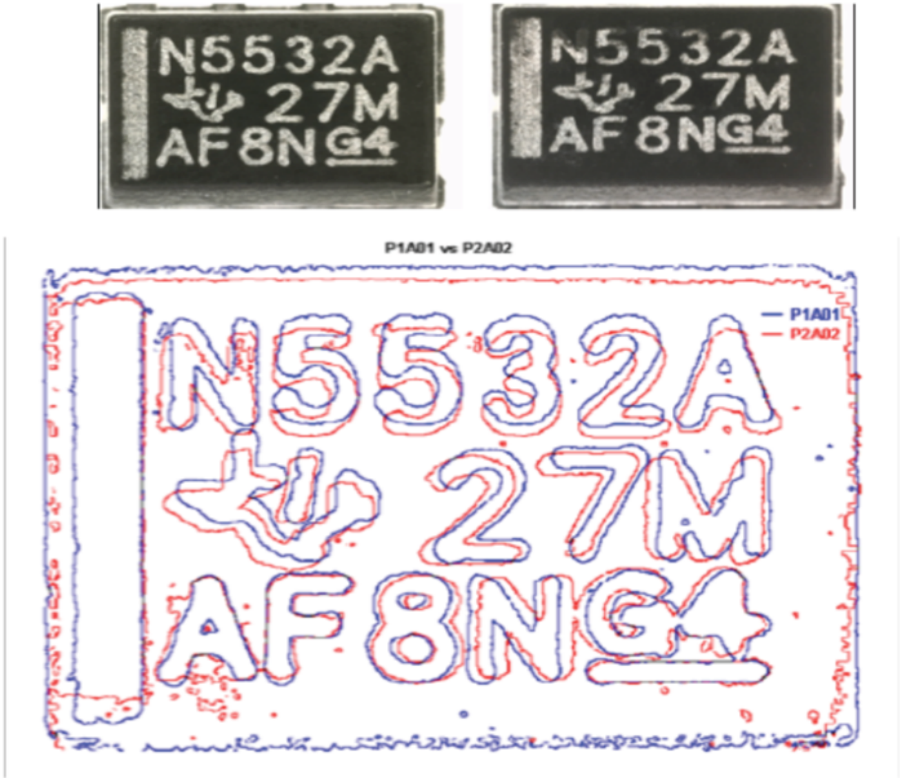
http://www.turbosquid.com/3d-models/c4d-factory-smoke/229722

Once SHIELD determines a chip to be a counterfeit, Fab-of-Origin will provide the insight needed to identify where it was made.

Thinking “outside the box”
Determining Fab-of-Origin



Two parts, marked by the same laser tool



Two parts, marked by different laser tools in the same facility

Images compliments of Clearmark, Inc.

What characterizes the circuit layout of an ASIC?

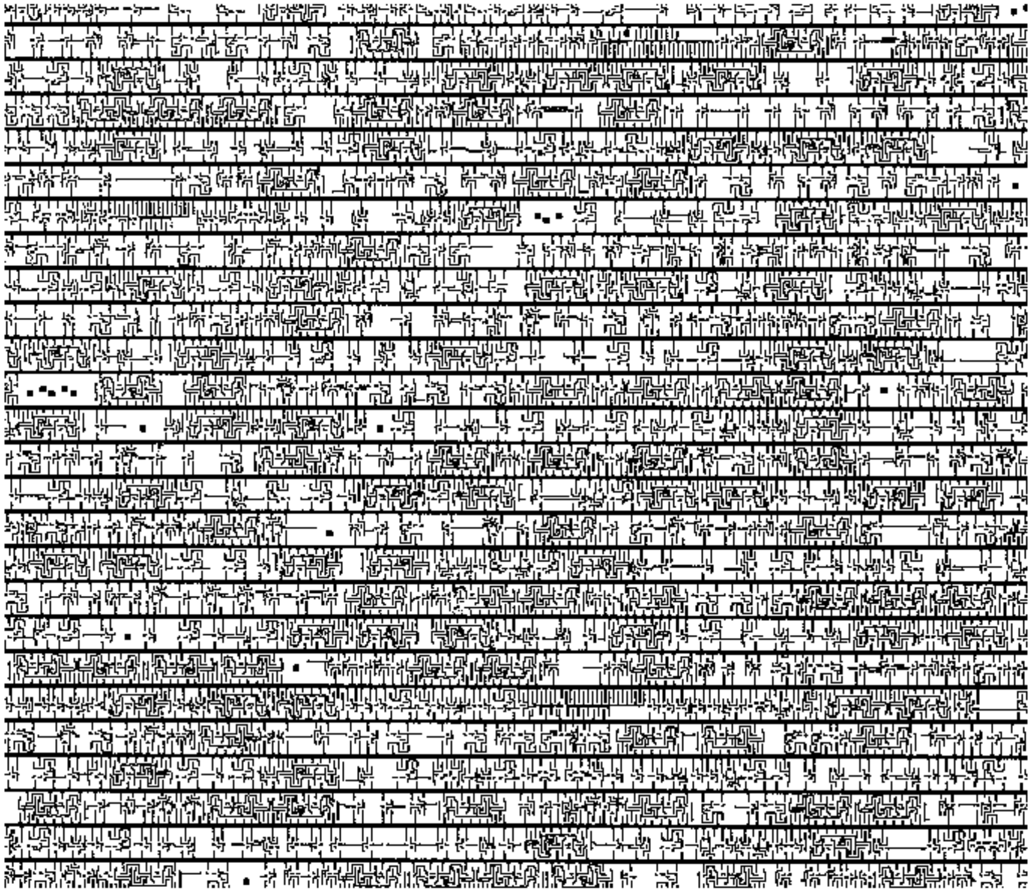


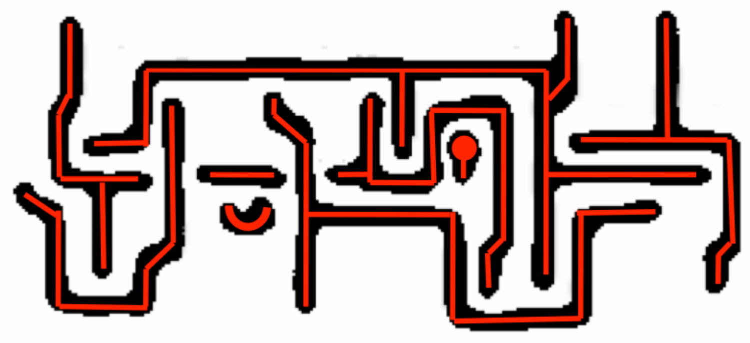
Image courtesy of Air Force Research Laboratory

Medium is (M1) metallization patterns in SEM image tiles

Image courtesy of Clearmark Systems

Basis patterns are *unknown* cell designs from the standard library for the foundry

Image courtesy of Clearmark Systems



The layout information is contained in the line drawing of the patterns

www.darpa.mil