Supply Chain Hardware Integrity for Electronics Defense (SHIELD)

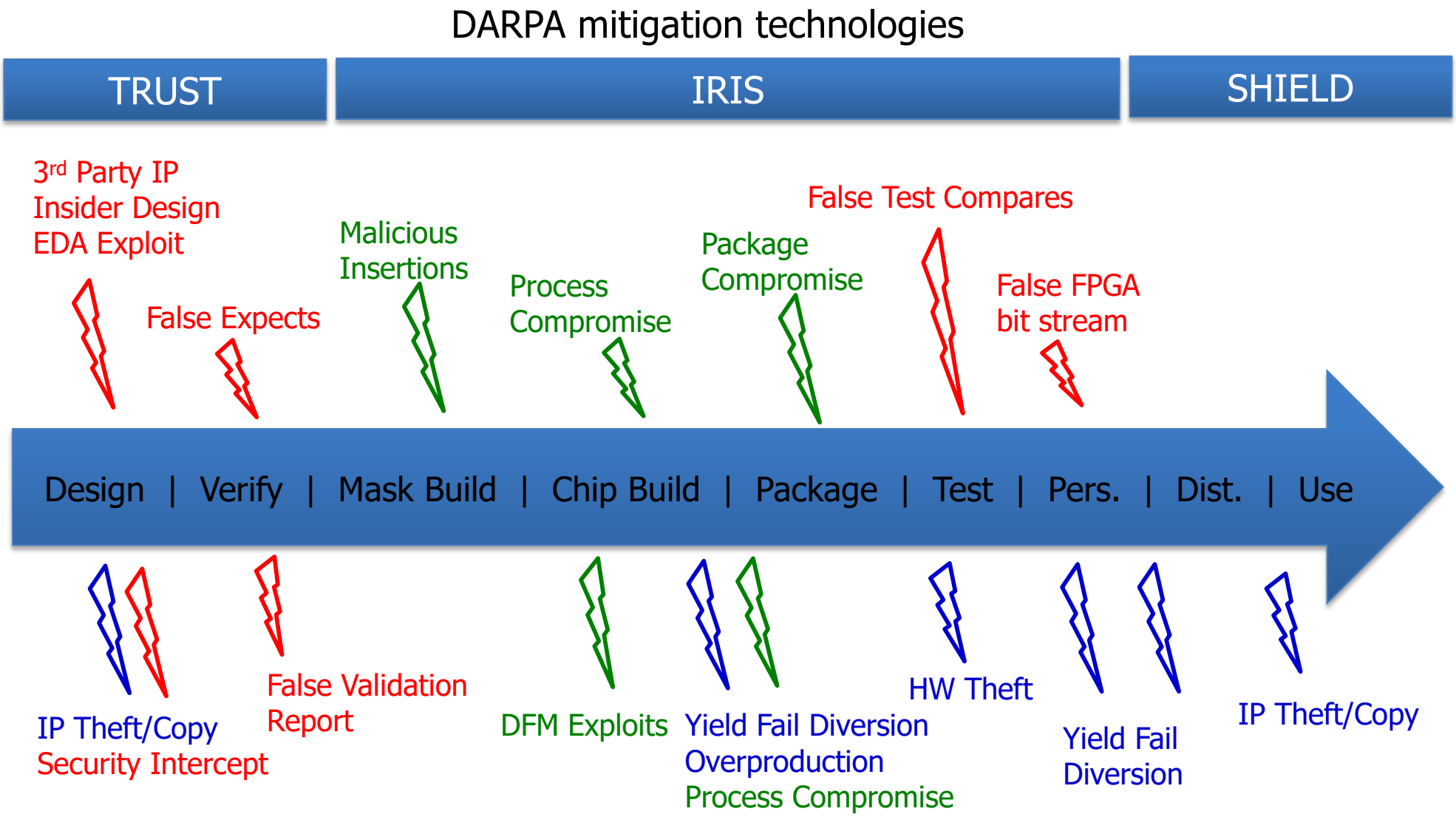
Serge Leef
Program Manager, Microsystems Technology Office
Defense Advanced Research Projects Agency

Software and Supply Chain Assurance Winter Forum 2018

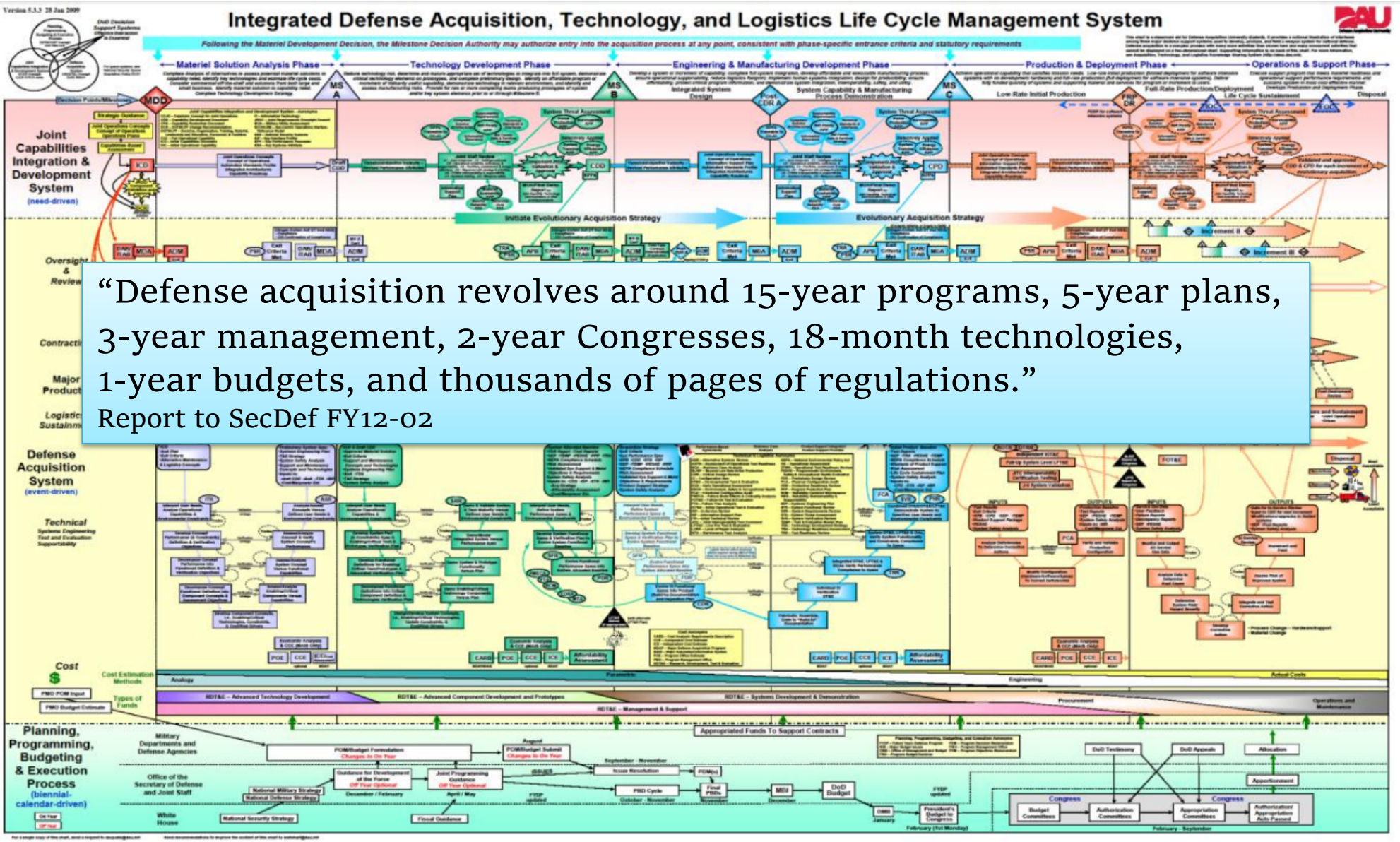
18 December 2018

Threats to Integrated Circuit Integrity

Threats to integrated circuit integrity



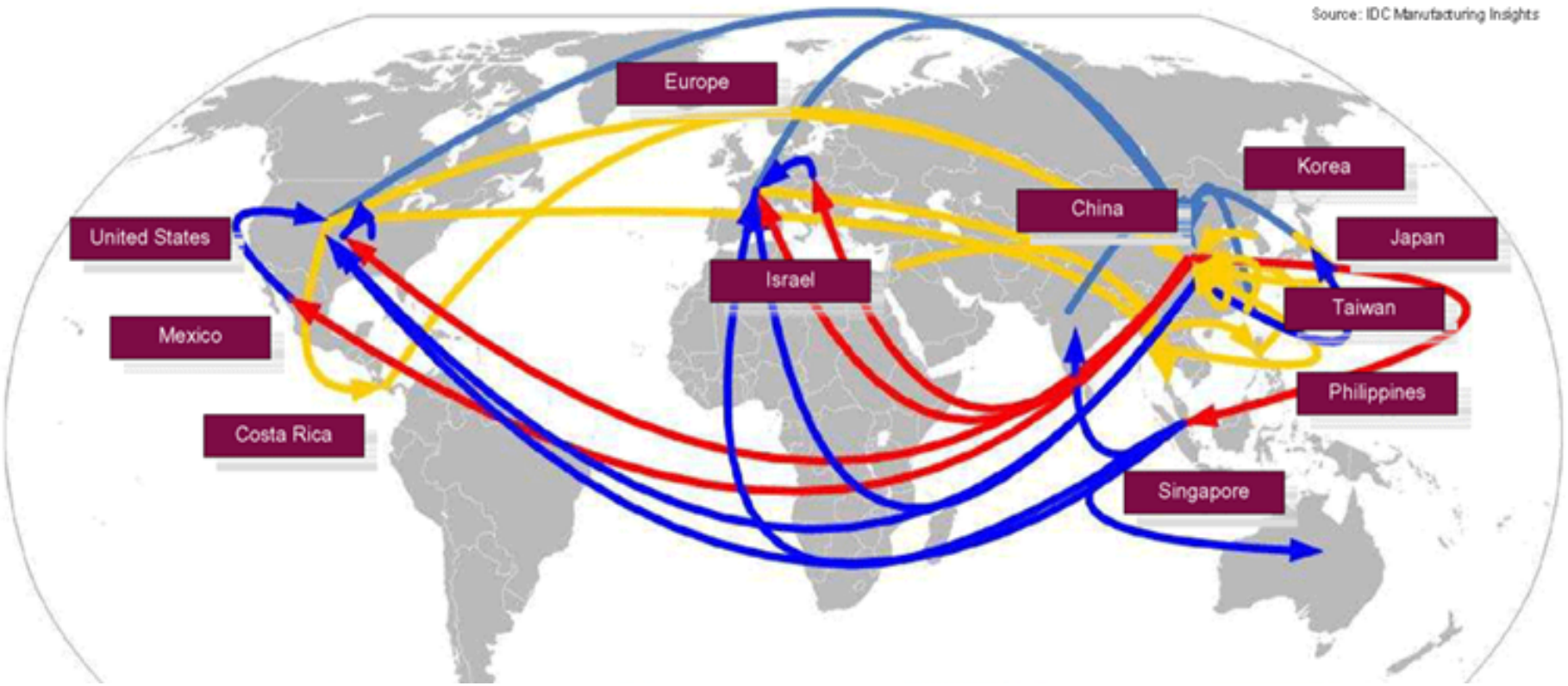
DoD Acquisition Is a Man-made Challenge



"Defense acquisition revolves around 15-year programs, 5-year plans, 3-year management, 2-year Congresses, 18-month technologies, 1-year budgets, and thousands of pages of regulations."
Report to SecDef FY12-02

Image: Defense Business Board

The Global Nature of Today's Supply Chains makes chain-of-custody unworkable



Semiconductor Design

Semiconductor Manufacturing & Packaging

Printed Circuit Board Production

Printed Circuit Board Distribution

Source: IDC Manufacturing Insights & Booz Allen analysis

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

US Electronic Waste is a Contributing Factor

Received in Developing Country

Shipping from/to U.S.

Resold

Removed from boards and sorted

Refurbished and remarked

Repackaged

All images courtesy of SMT Corporation

Effects on quality and reliability

Uncontrolled heating during part removal can cause die cracks or delamination, leading to immediate or latent failures.

Image courtesy of Basel Action Network

Mishandling or sanding of parts can cause latent Electrostatic Discharge (ESD) failures.

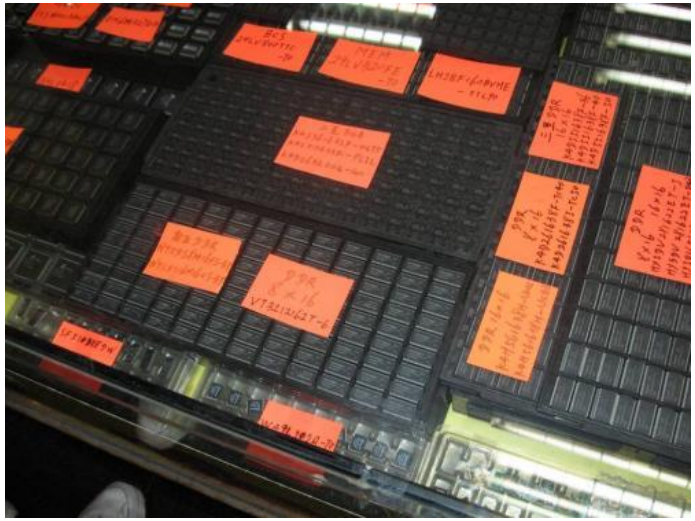


Image courtesy of SMT Corporation

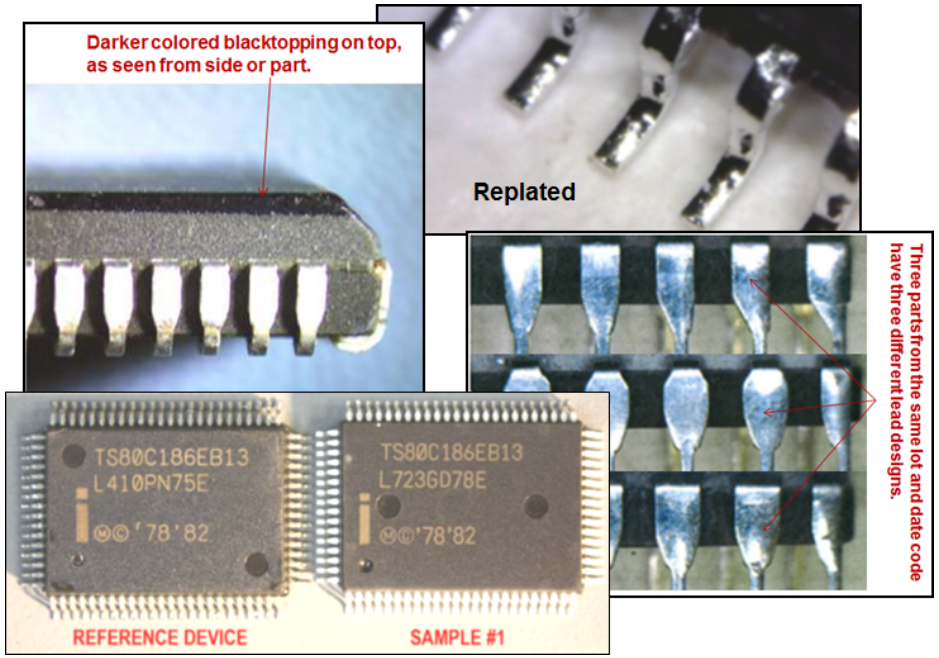
Counterfeits vs Clones

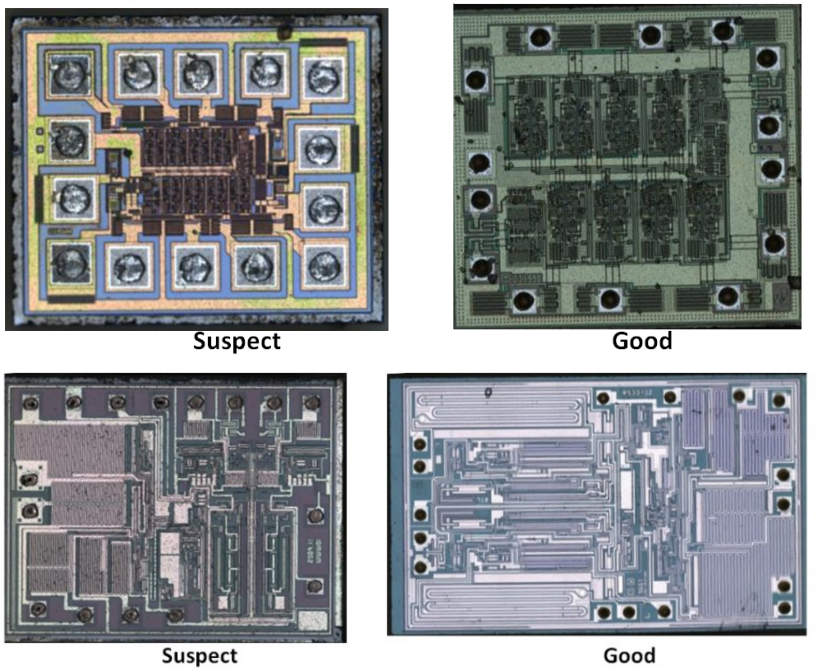
A counterfeit part is manufactured by the OEM and presented as new, but the performance and reliability of the part is questionable:

- Used components recycled/remarked
- OEM test failures
- Unlicensed fab overproduction

A cloned part is not manufactured by the OEM but may be designed to mimic the performance of the authentic part:

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



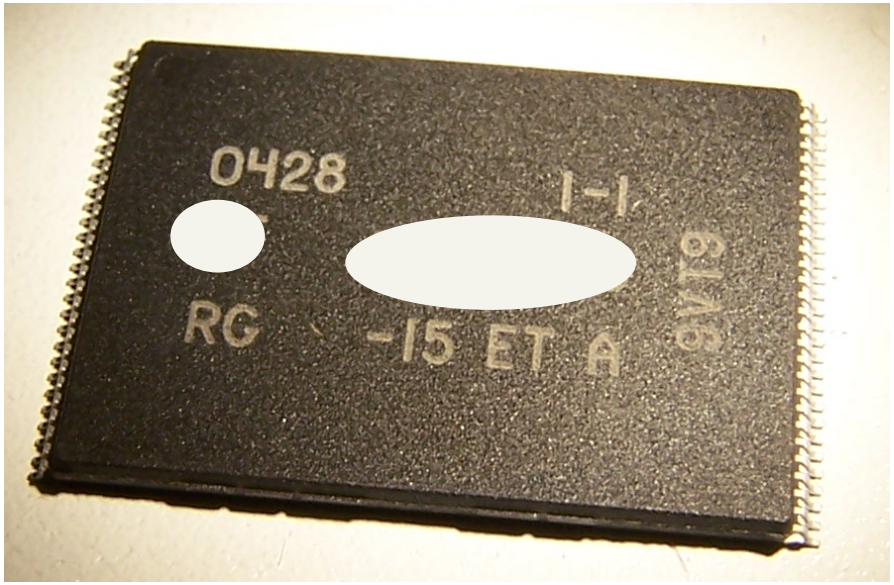


All images courtesy of NSWC Crane

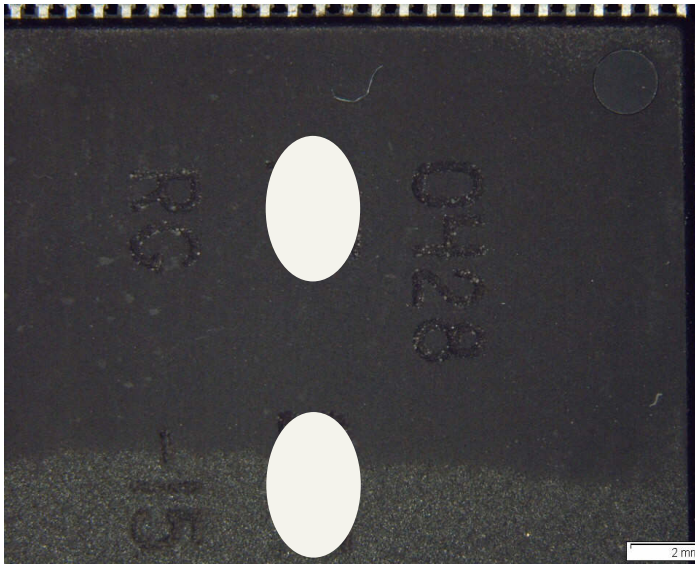
Counterfeits, Clones, Trojans

Things are Not Always as They Appear!

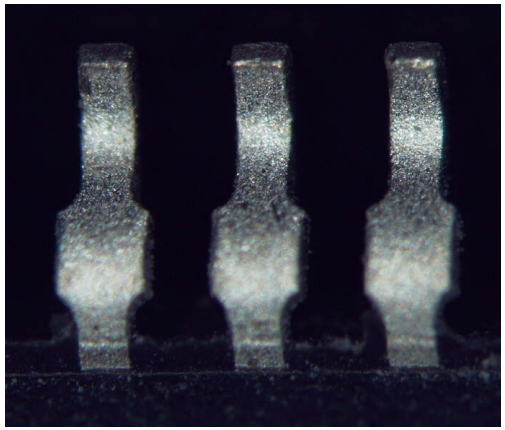
This part looks pretty good, right????



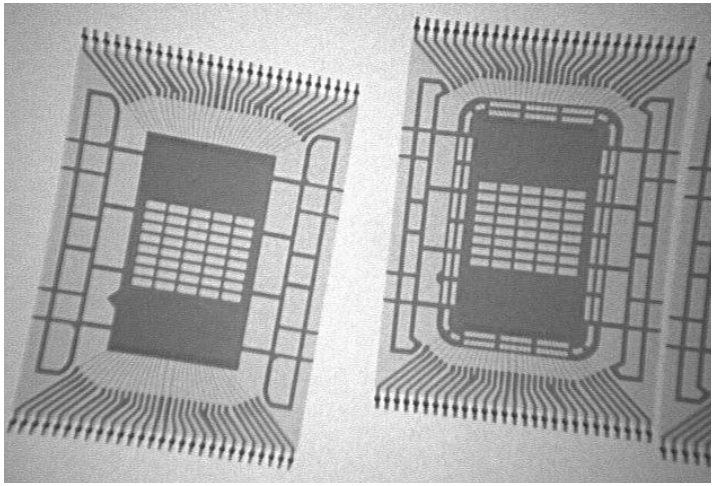
Source:
Images NSWC Crane



Blacktopped – After Dynasolve Soak

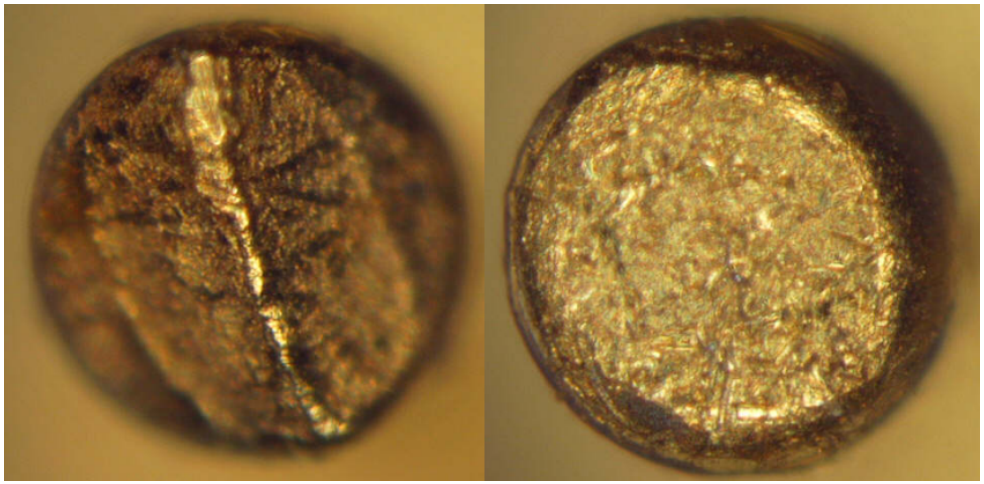


Re-Plated Leads

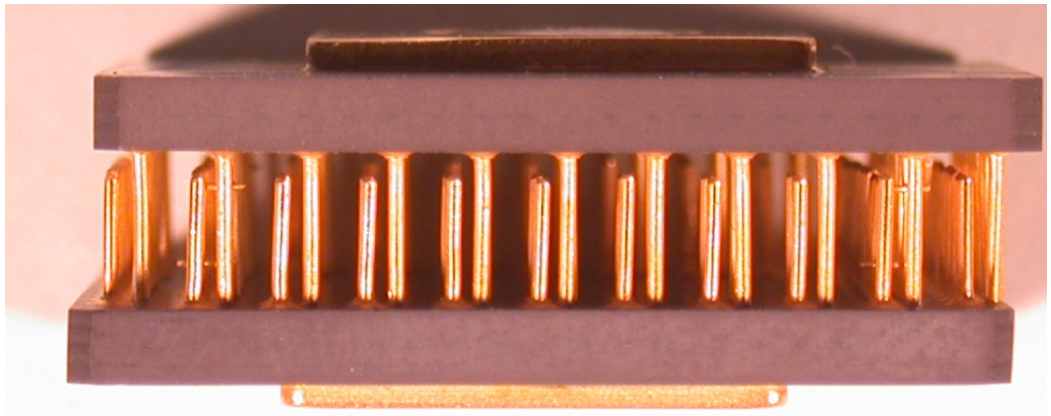


Different Lead Frames in Same Lot

Physical and Optical Inspection is Time Consuming, Labor Intensive, Thus Expensive!



Trimmed (wedge) vs. Untrimmed (flat) Leads



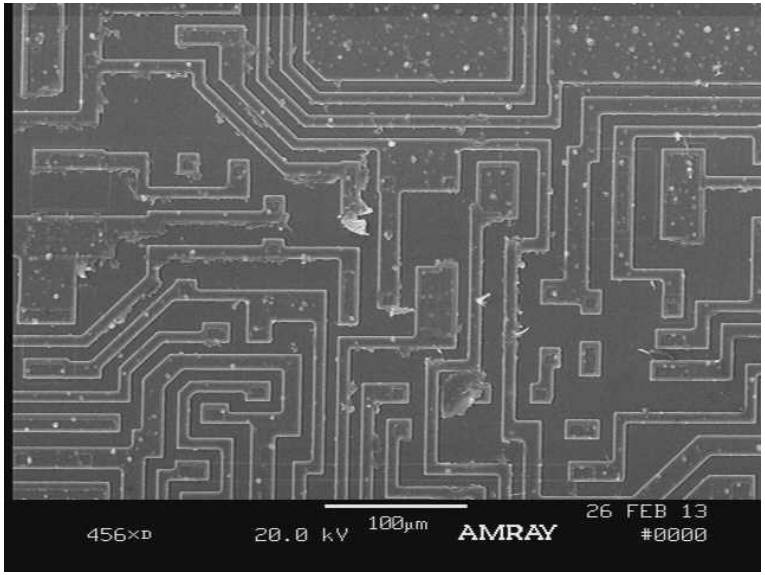
One Part has Trimmed Leads (Shorter than Legitimate Part)

Scratched Window from Sanding and Corroded Metal

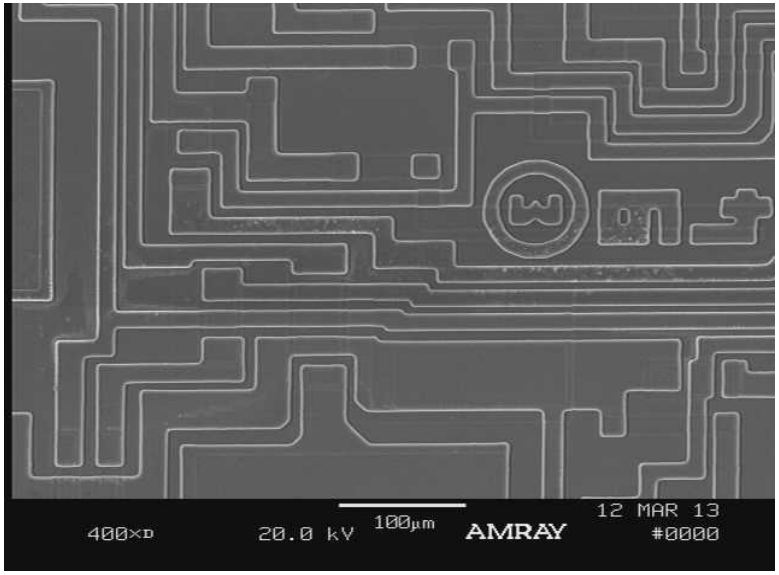
Source: Images NSWC Crane

Poor Quality Integrated Circuits

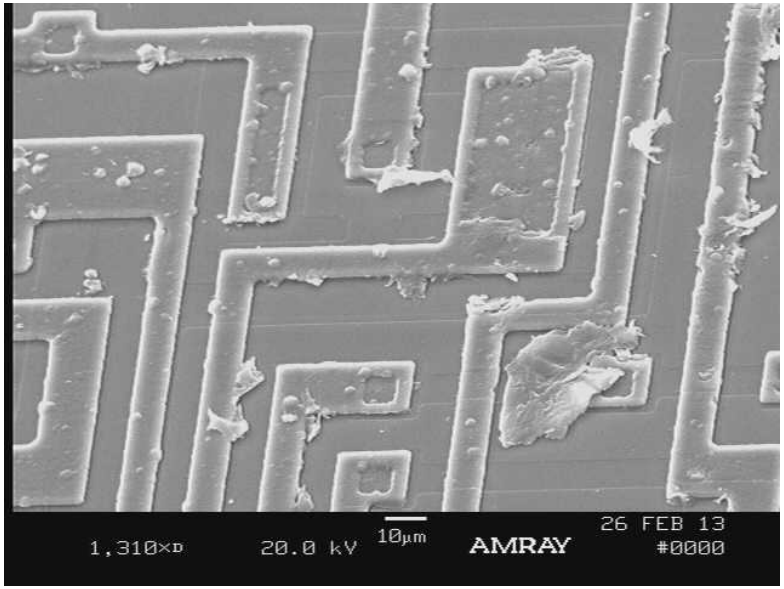
Low quality manufacturing process

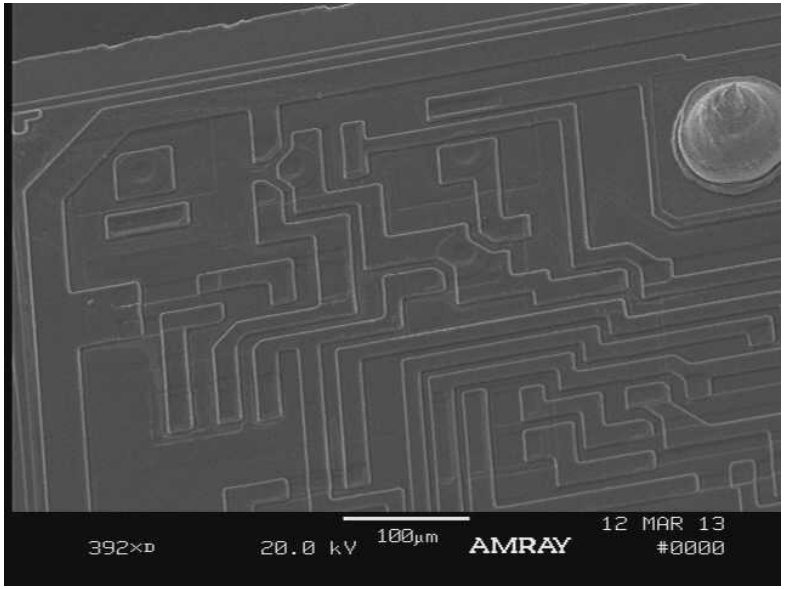


Example of Poor Quality



Good Part





Source:
Images NSWC
Crane

Open Source Hardware Trojan Research

Stealthy Dopant-Level Hardware Trojans[1]

Abstract. "…..In this paper we propose an extremely stealthy approach for implementing hardware Trojans below the gate level, and we evaluate their impact on the security of the target device. Instead of adding additional circuitry to the target design, we insert our hardware Trojans by changing the dopant polarity of existing transistors. Since the modified circuit appears legitimate on all wiring layers (including all metal and polysilicon), **our family of Trojans is resistant to most detection techniques**, including fine-grain optical inspection and checking against "golden chips"……."

[1]Source: Georg T. Becker[1], Francesco Regazzoni[2], Christof Paar[1,3], and Wayne P. Burleson[1]
[1]University of Massachusetts Amherst, USA
[2]TU Delft, The Netherlands and ALaRI - University of Lugano, Switzerland
[3]Horst Görtz Institut for IT-Security, Ruhr-Universitt Bochum, Germany

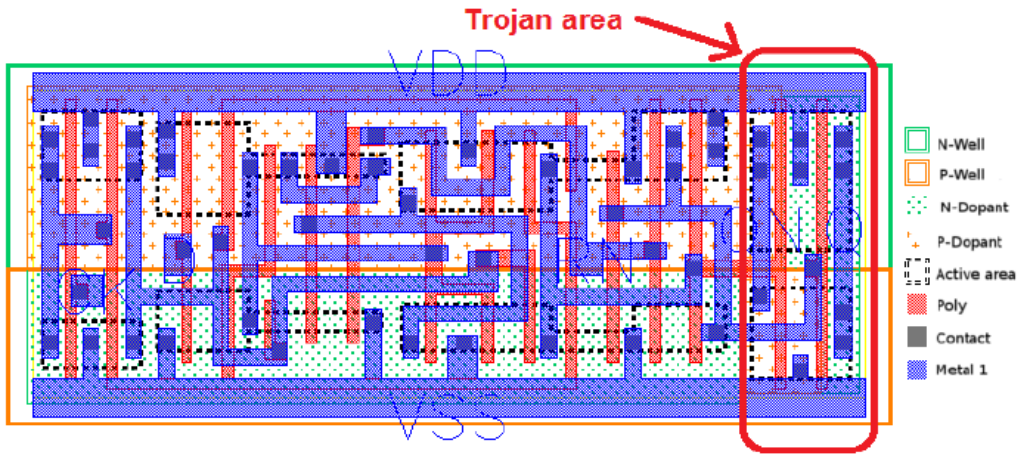
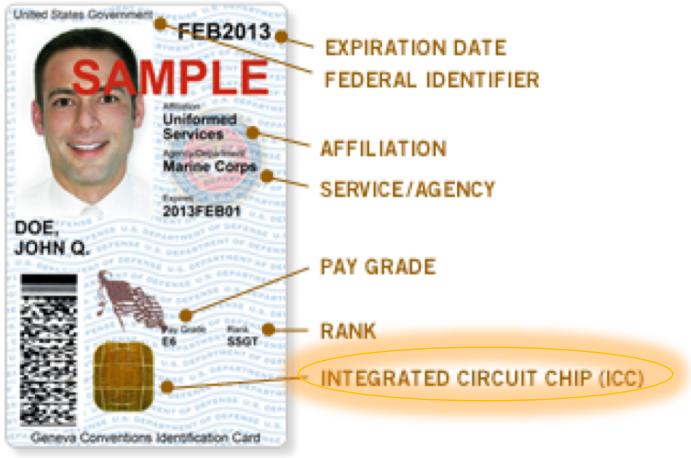


Fig. 2. Layout of the Trojan DFFR_X1 gate. The gate is only modified in the highlighted area by changing the dopant mask. The resulting Trojan gate has an output of $Q = V_{DD}$ and $QN = GND$.

SHIELD Overview

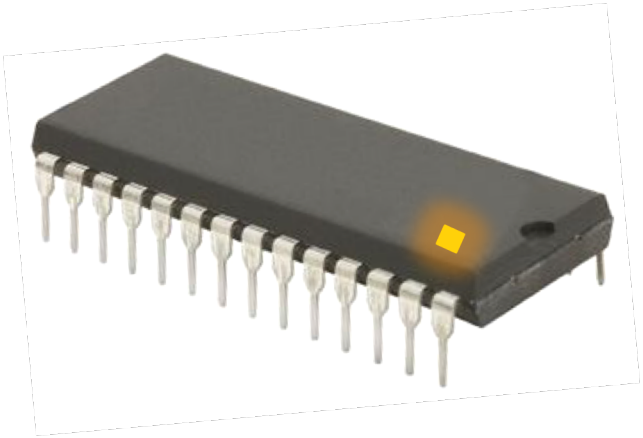
A Hardware Root of Trust for Integrated Circuits

Apply RFID chip concept…



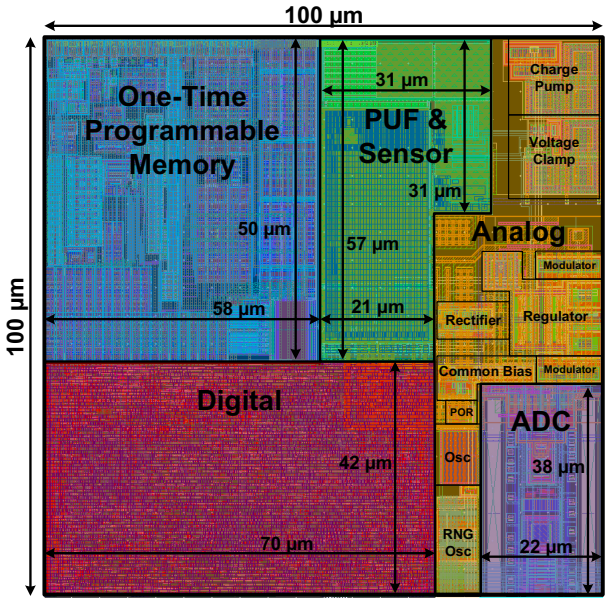
Common Access Card
- PIN (known only to card holder)
- ID Certificates

…to integrated circuit integrity



SHIELD Dielet
- Onboard encryption engine with secret key
- Serial ID

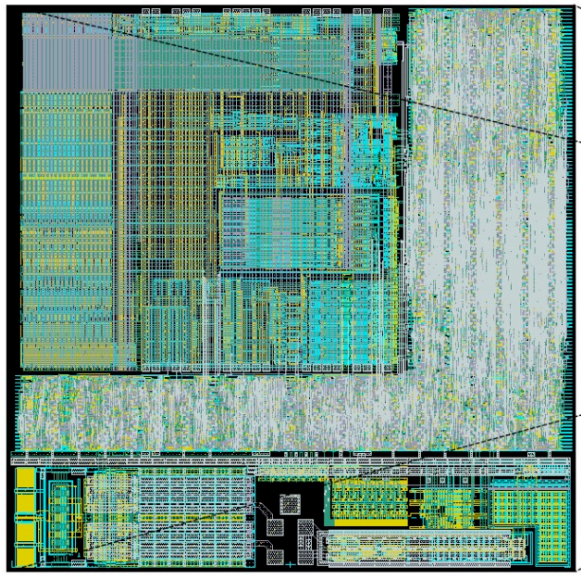
SHIELD – The DARPA Supply Chain Solution



Dielet floorplan (Northrop Grumman)
14nm CMOS

Key SHIELD Specifications

- Unique Key Storage
- Full 256-bit AES encryption engine
- Unpowered, passive intrusion sensors
- RF power and communication
- Transfer fragility
- 100µm x 100µm
- 50 µW Total Power
- Operating temp < 120°C
- Cost < $0.01 per dielet



Prototype dielet layout (SRI)
28nm CMOS

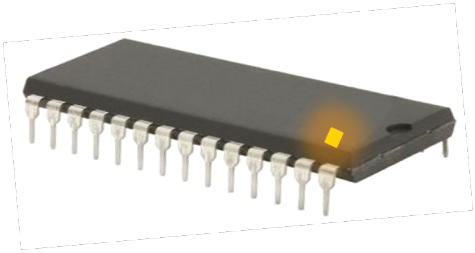
Asymmetric Security

- Non-resettable, "always on" intrusion sensors on dielet
- On-board encryption symmetric key that cannot be "coaxed" from dielet
- ID and Key are unique to the individual host IC (not just the part number)
- Interrogation history (date, time, location) stored on secure server
- Built-in fragility structures kill dielet if removal from host is attempted

SHIELD makes counterfeiting too expensive and too hard to do.

SHIELD Key Components

Dielet



Programmed on-reticle after manufacture

Installed on or within host IC package

- Embedded within package
- Custom package
- Epoxy to surface

No impact to host IC performance or reliability

Reader

Transmits at 5.8GHz to power dielet; 3.6GHz for data transfer

USB connection to smartphone, tablet or computer

Can be configured for high-volume interrogation (transaction time < 1 sec)

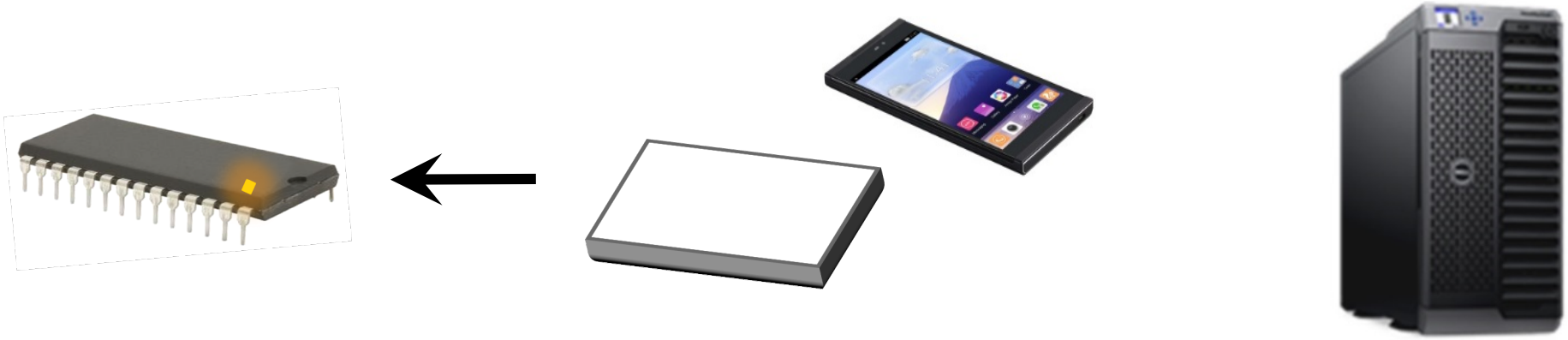
Remote Server

Communicates with reader via Internet connection; performers using Amazon and Microsoft web services

Maintains a record for each IC

- Manufacture date
- Part/package information
- Interrogation history

SHIELD Concept of Operation



1. Interrogate dielet on host IC

SHIELD Concept of Operation

2. Unique ID returned by host IC; reader sends ID to server

FAIL if no response from host IC

SHIELD Concept of Operation

3. Server sends unencrypted challenge to reader; reader forwards challenge to host IC

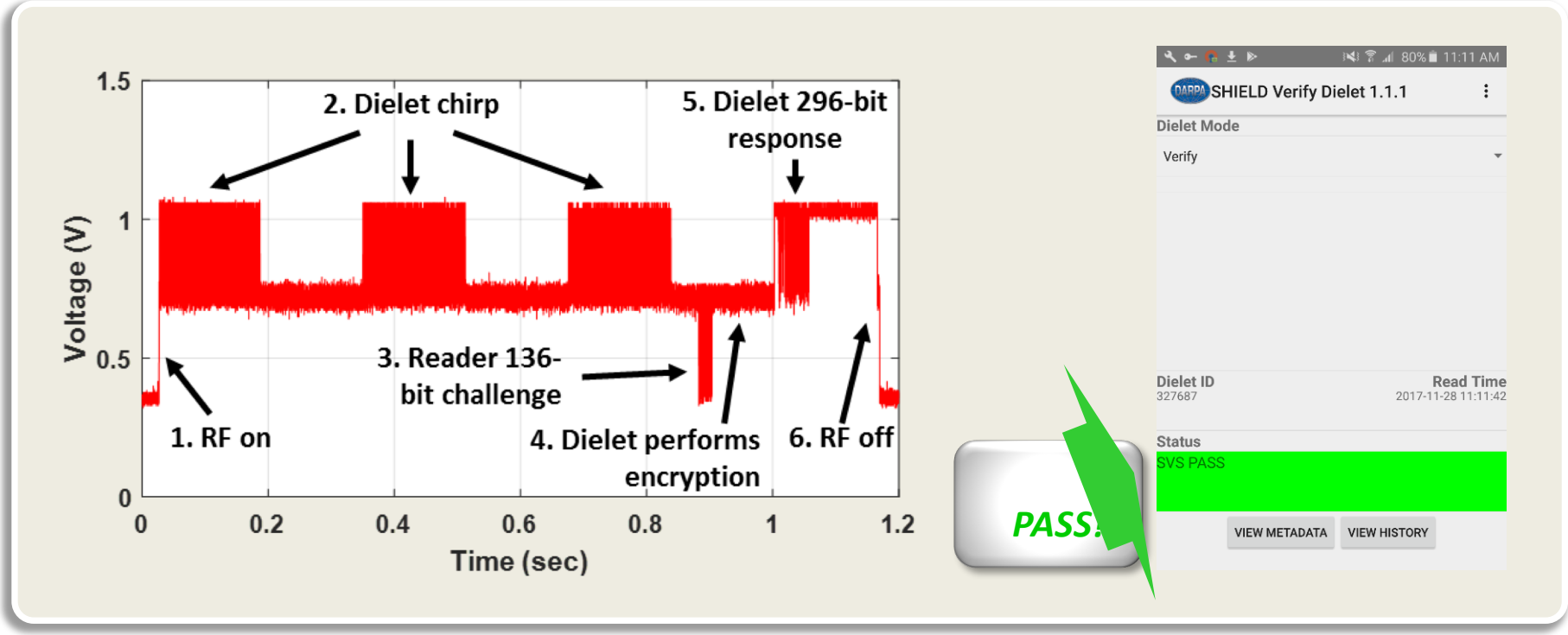
FAIL on discrepancy between server record and user visual ID
(example: user is testing microcontroller, but server reports ID belongs to an FPGA)

SHIELD Concept of Operation

4. Host IC sends encrypted response and sensor status; reader forwards to server

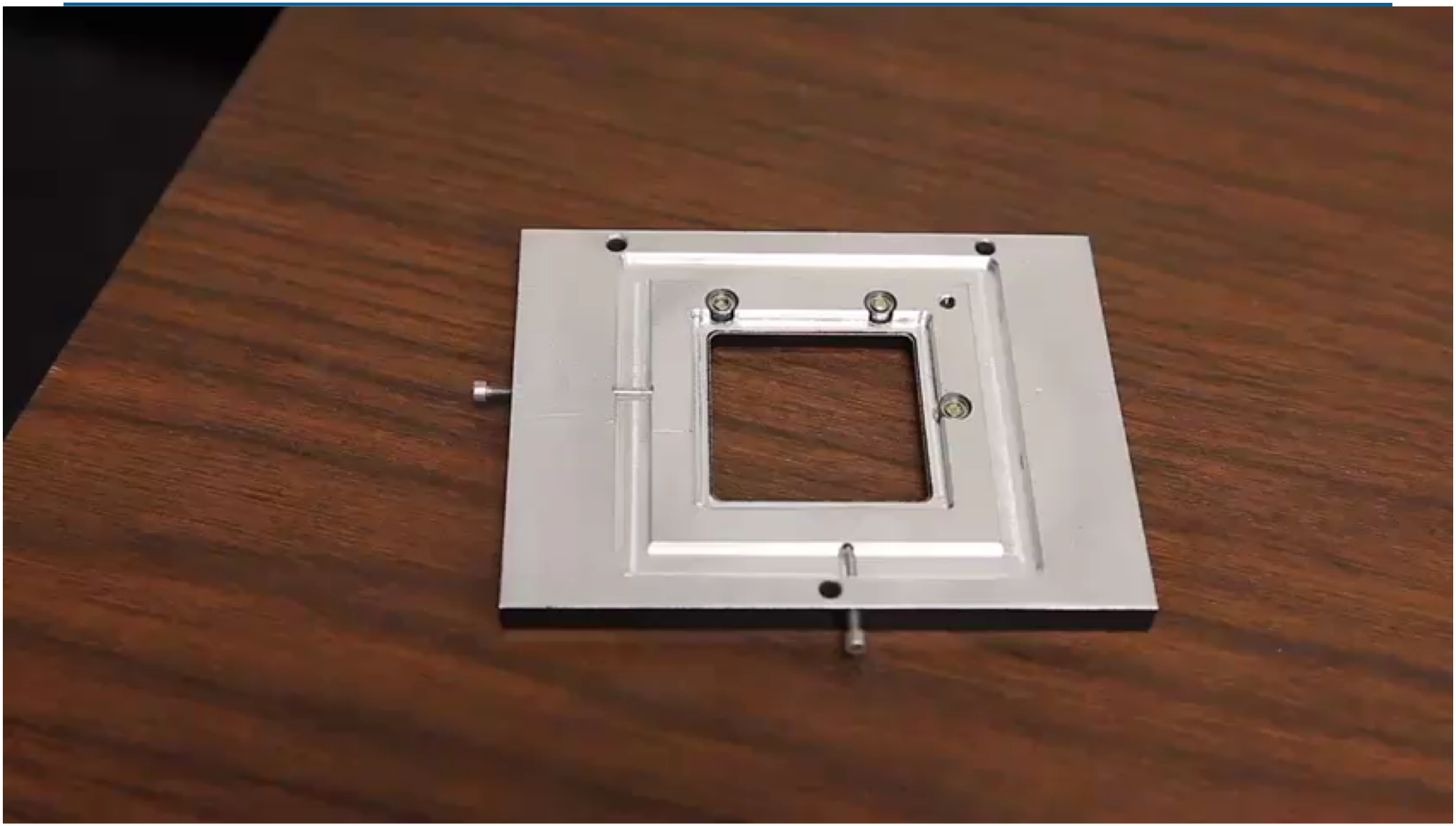
PASS if challenge/response match
FAIL if challenge/response do not match

A SHIELD Authentication Transaction



A complete SHIELD authentication transaction, including internet latency, takes only 1-2 seconds.

SRI International SHIELD Demo with Reader



SHIELD Program Structure and Performers

SHIELD Program Structure

- Program start: January 2015
- Performers:
  - Northrop Grumman (full SHIELD design)
  - SRI International (full SHIELD design)
  - Draper (sensors, fragility)
  - University of California, Berkeley (dielet power/communication, fragility)
  - University of Illinois/Carnegie Mellon University (dielet power/communication)
- Four year program in three phases
  - Phase 1: Technology Development (1.5 years)
  - Phase 2: Hardware Design (1.5 years)
  - Phase 3: Demonstrate the CONOP (1 year)

A Root-of-Trust Prohibitively Difficult to Exploit With Key Protection, Attack Resistant AES, and Smallest OTP

NORTHROP GRUMMAN

Advancing a Proven AT Tech Base Assessed to Defeat Advanced Threats

- ***Physically Unclonable Function (PUF)*** – Random process variation used to create dielet-derived portion of encryption key.

Sandia National Laboratories

- ***Tamper Detection Sensor*** – Sensor detects potential counterfeiting by capturing temperature excursions.

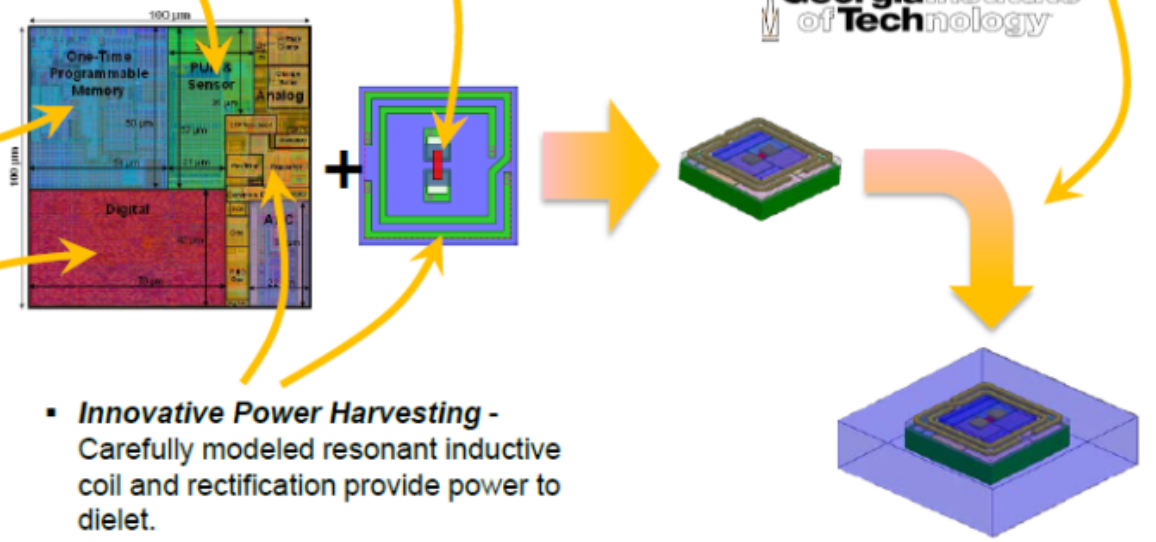
Sandia National Laboratories

- ***Innovative Encapsulation*** – Lamination process facilitates compatibility with existing surface mount infrastructure.

Georgia Institute of Technology

- ***14nm Gate-Oxide Rupture One-Time Programmable (OTP) Memory*** – Small and difficult to exploit, OTP contains 64-bit SN and 256-bit key split.

Kilopass



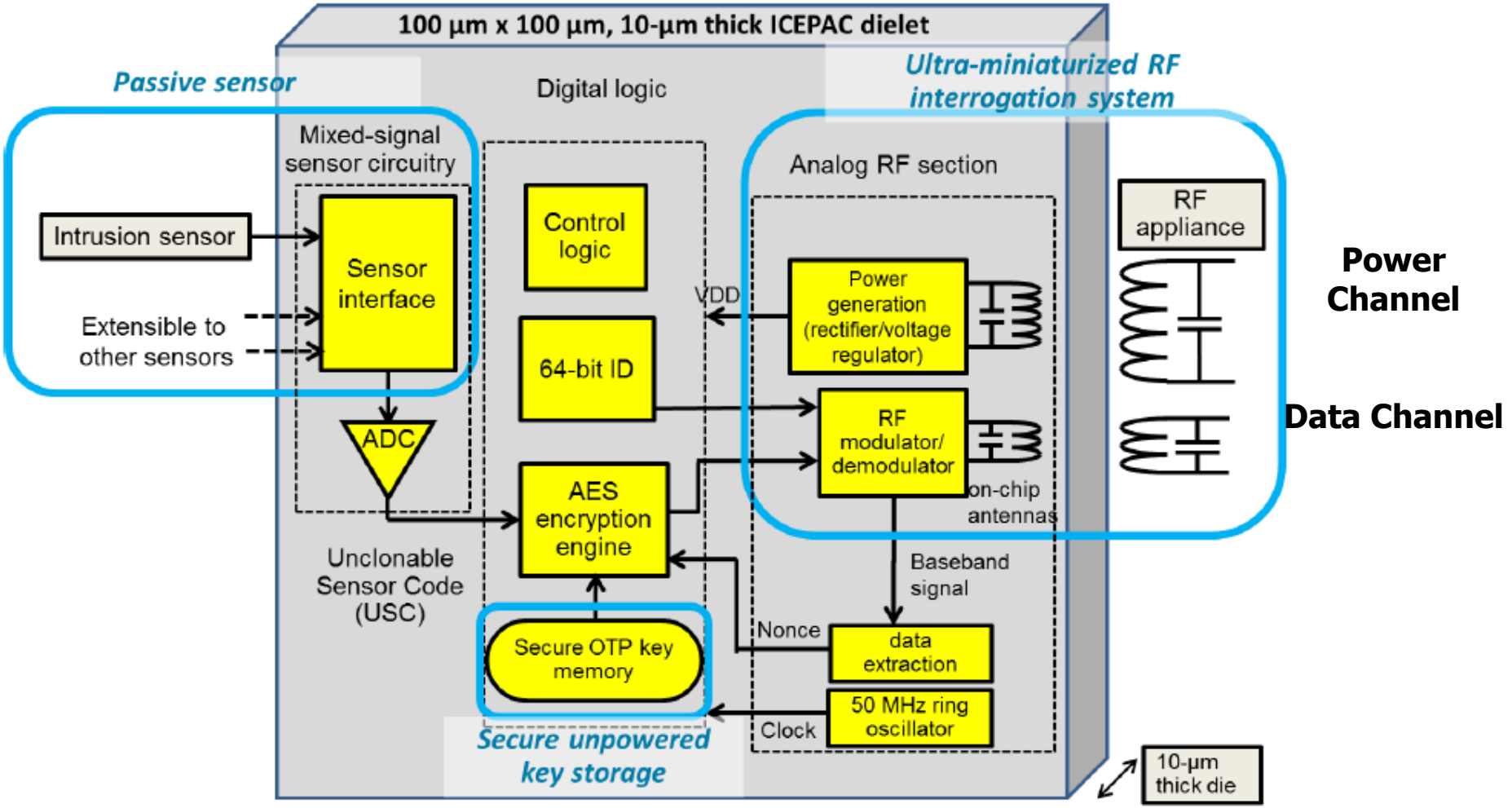
- ***Attack Resistant Cryptography*** - AES engine and jointly randomized split keys creates a strong Root-of-Trust.

NORTHROP GRUMMAN

- ***Innovative Power Harvesting*** - Carefully modeled resonant inductive coil and rectification provide power to dielet.

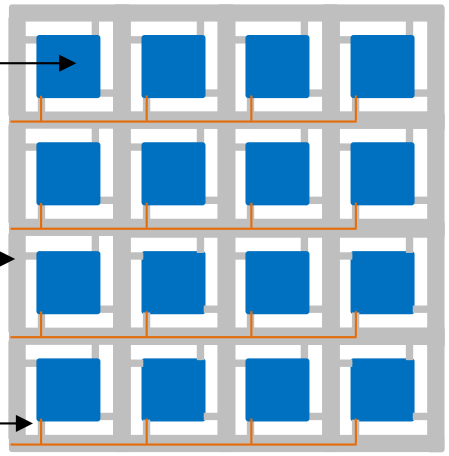
NORTHROP GRUMMAN

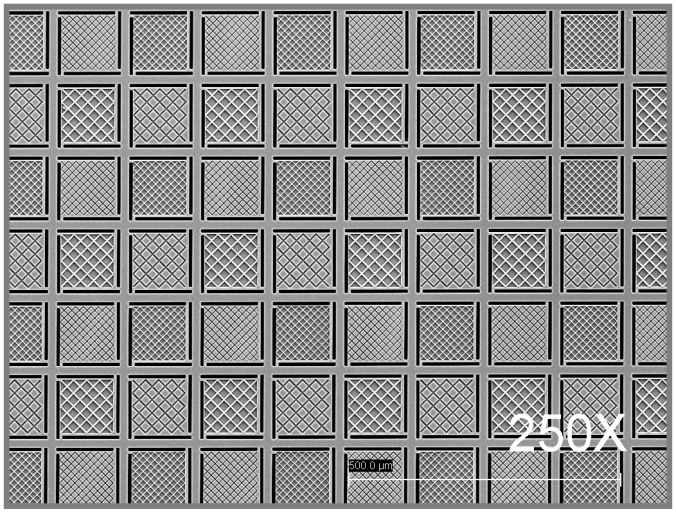
SHIELD Dielet Block Diagram



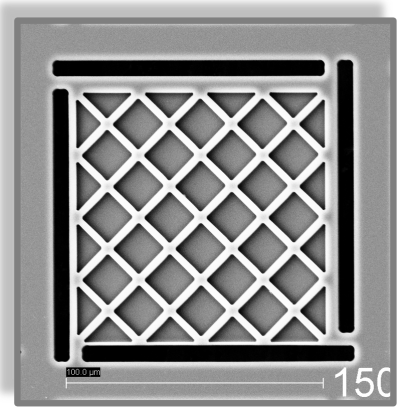
Draper Fragility Summary

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

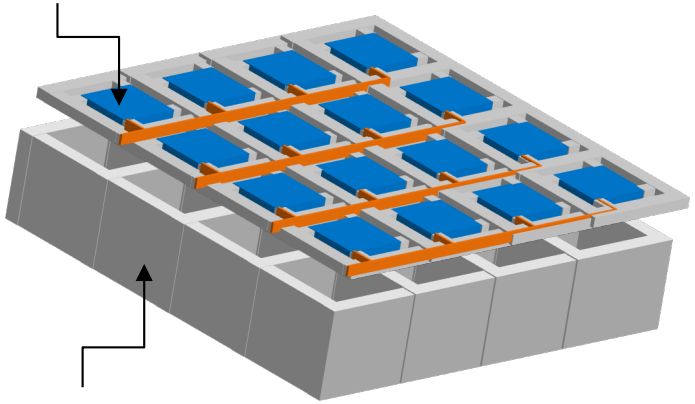




Top View (1,500x)



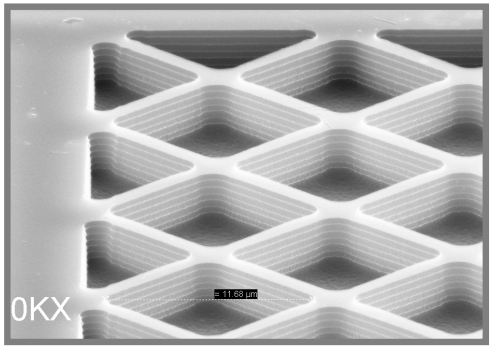
Released dielets anchored to a silicon frame



Carrier wafer with etched cavities under individual dielets

Key Features

- CMOS compatible architecture with high-yield backend processing
- Higher die count (lower cost) compared to dicing processes
- Strategically placed microstructures to aid in fragmentation



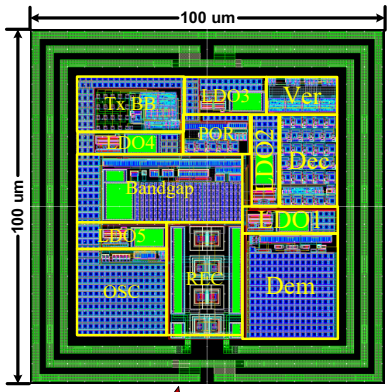
Perspective View (10,000x)

G. Perlin, et al.

65nm CMOS SHIELD "Technology Vehicle"

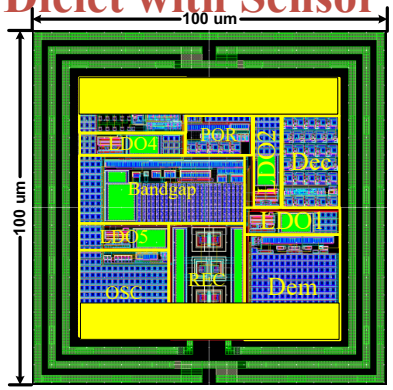
2016/5 Tapeout

Standalone Dielet



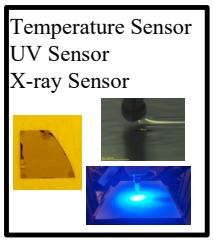
2016/12 Tapeout

Dielet with Sensor



Sensor

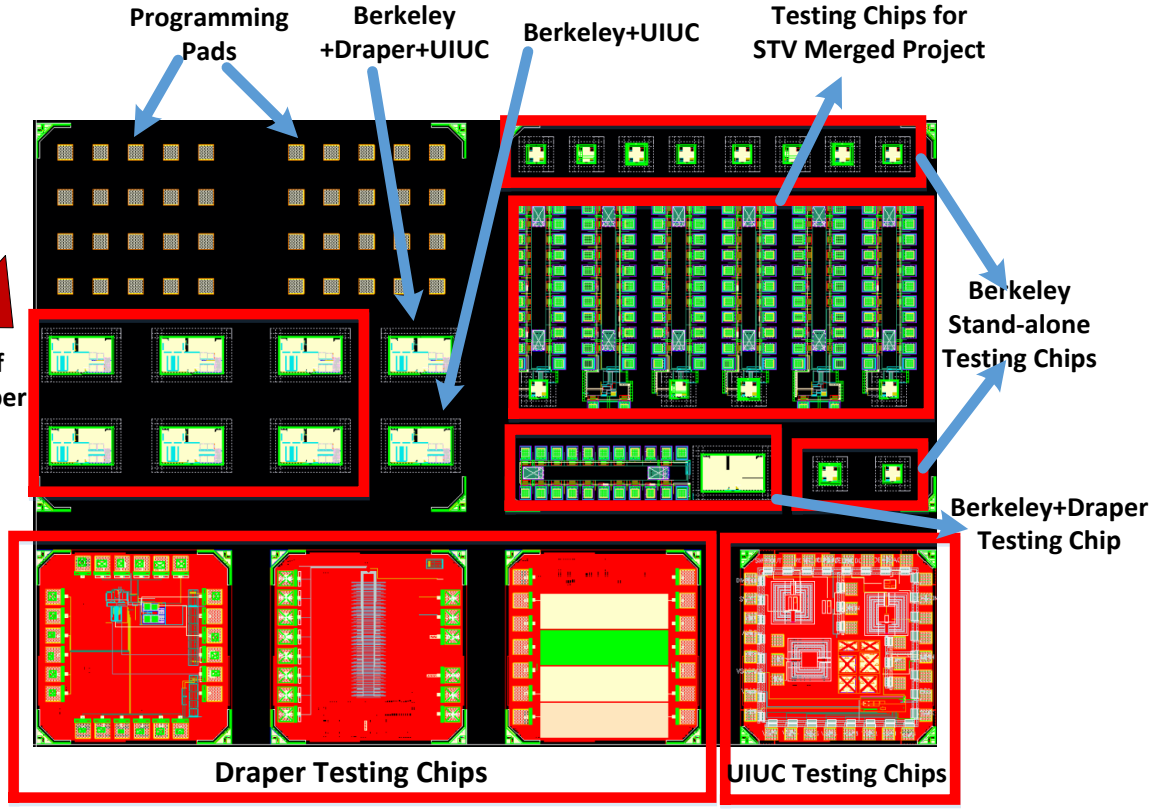
Temperature Sensor
UV Sensor
X-ray Sensor



2017/3 Tapeout

STV Merged Project

6 Versions of Berkeley+Draper



www.darpa.mil