Our Annapurna

Kerry Bernstein, Program Manager
Microsystem Technology Office

Indianapolis, IN

2 August, 2017

Annapurna I (8091m) Northeast Face *Himalaya, Nepal*

http://www.intrepidtravel.com/us/nepal/annapurna-sanctuary-102173

10th highest Peak in the world, first 8000m peak climbed.
First Ascent 03 June 1950 by Maurice Herzog, Louis Lachenal

Our Annapurna

https://www.amazon.com/Annapurna-Conquest-Highest-Mountain-Climbed/dp/B00110CLBO/ref=sr_1_3?ie=UTF8&qid=1499616124&sr=8-3&keywords=annapurna+herzog

“There are other Annapurnas in the lives of men.”

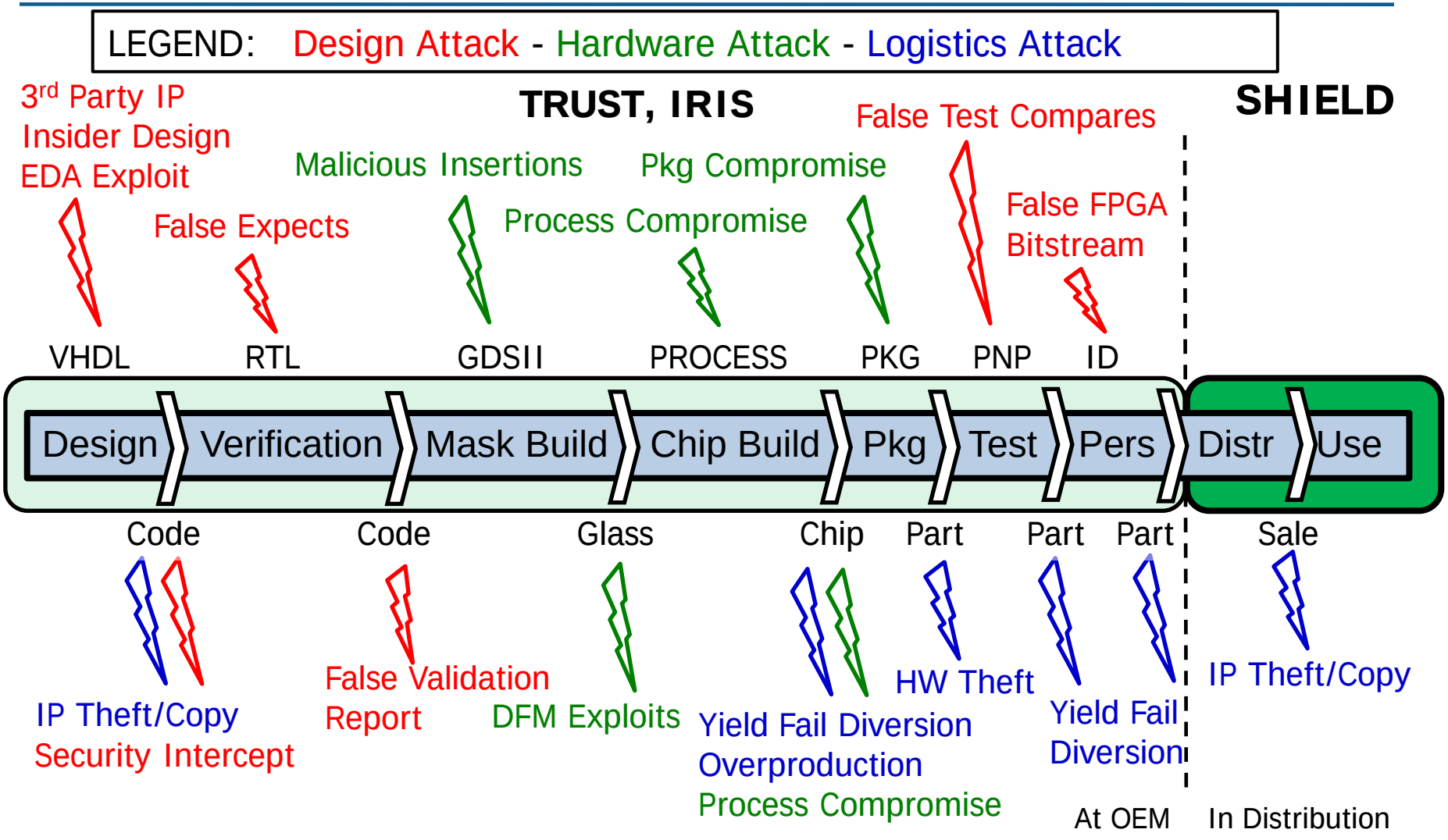
Maurice Herzog

From “Annapurna” 1952

What is *our* Annapurna?

The Nature of the Threat

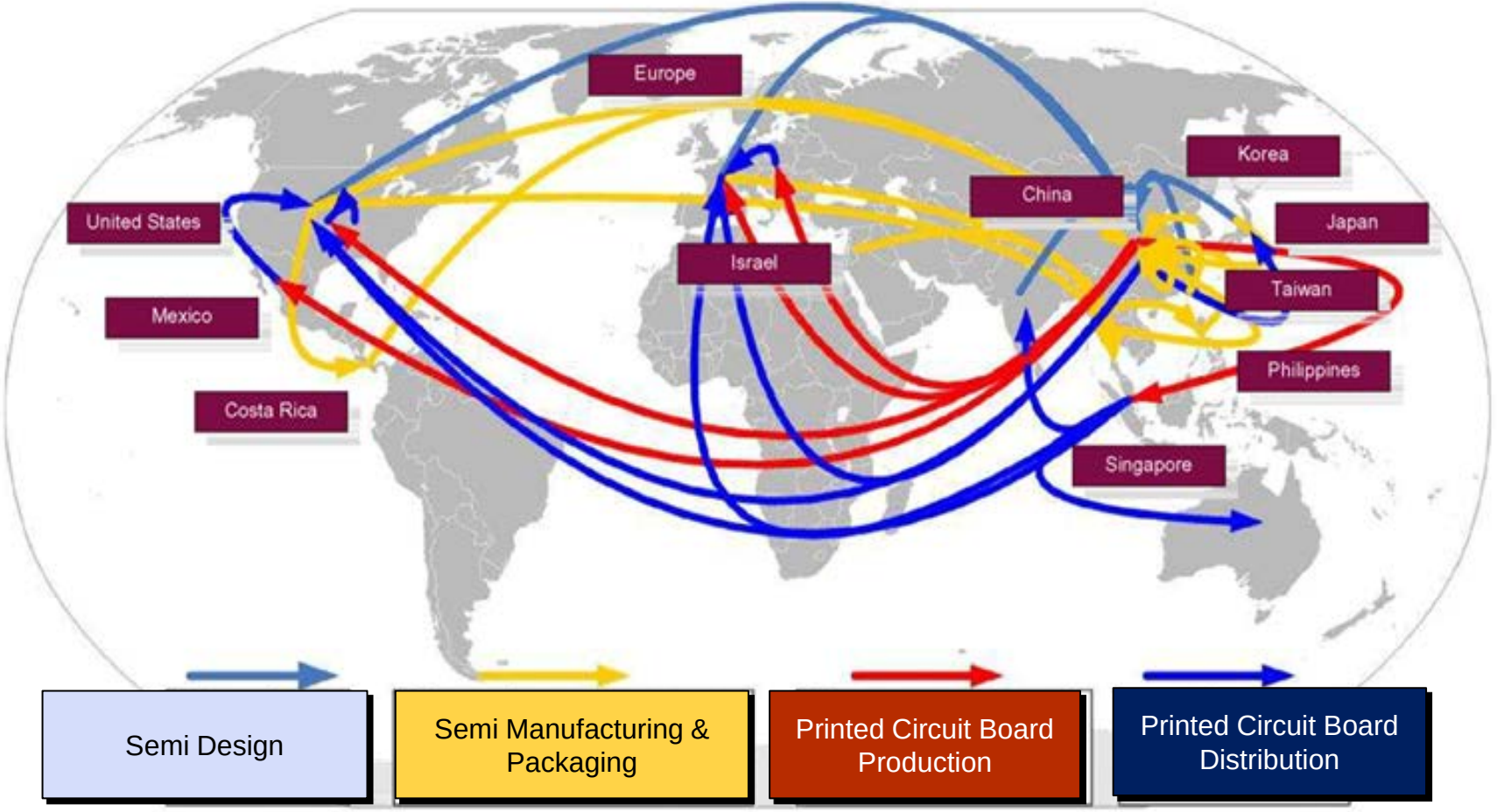
Hardware-specific Exploits



Exacerbating the Effect

The Global Nature of Today's Supply Chains

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

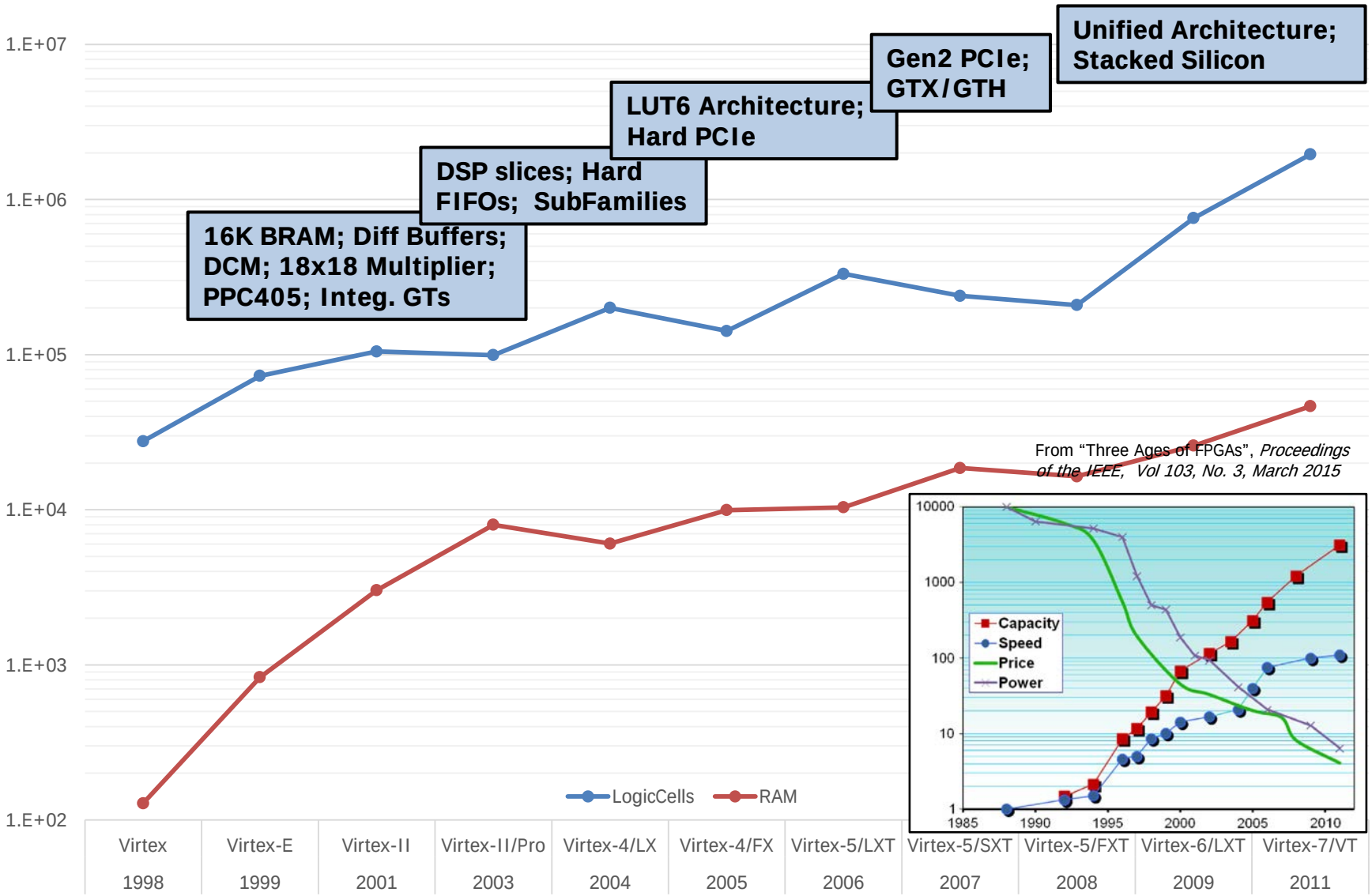


Source: IDC Manufacturing Insights & Booz Allen analysis

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

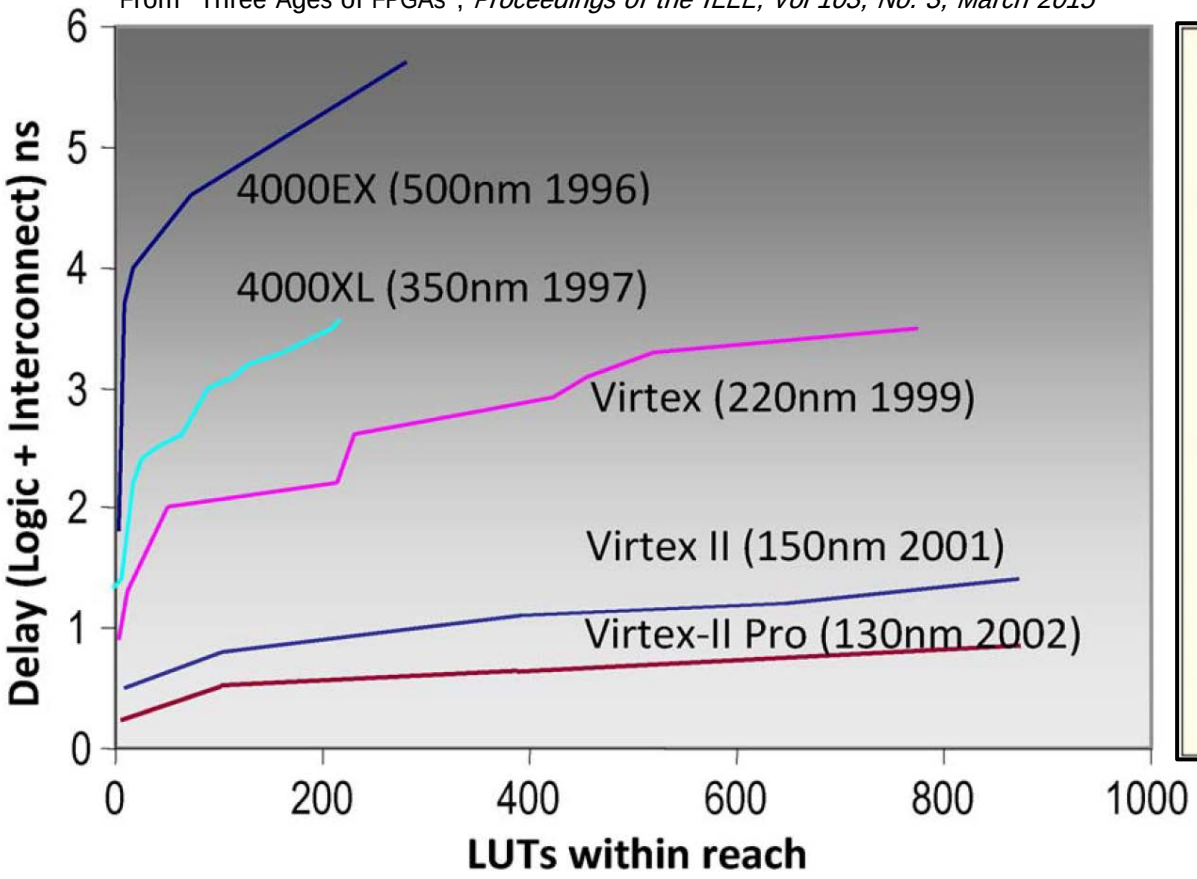
FPGA Evolution of Complexity *

* Data from https://forums.Xilinx.com/t5/Silicon-Devices-Others-Archived/Statistics-to-support-FPGAs-vs-multicore-CPUs-for-scientific/td-p/11995; KB/SM private communications



Complexity and FPGA "Effective" Span of Control

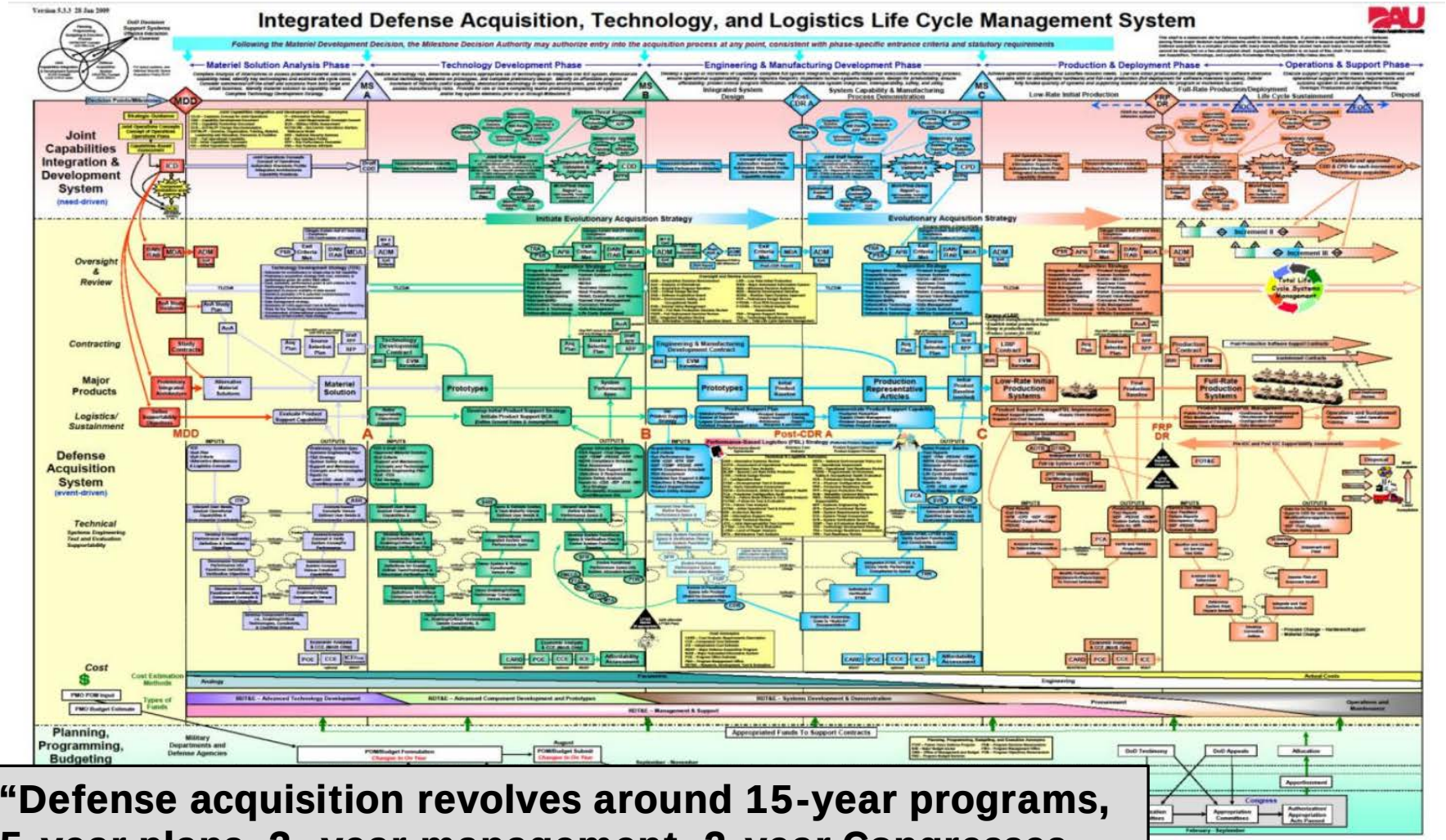
From "Three Ages of FPGAs", *Proceedings of the IEEE, Vol 103, No. 3, March 2015*



Gates, Registers and Routing	XC2000
Three-State Bus	XC3000
Dedicated Arithmetic	XC4000
Memory	XC4000
RAM Blocks	FLEX
Dynamic Reconfiguration	CAL/XC6200
Universal I/O	Virtex
LVDS I/O	Virtex
Programmable Clock	Virtex
Microprocessor	Excalibur
Source-Synchronous Transceiver	Virtex-II
Bitstream Encryption	Virtex-II
Transceiver	Virtex-II Pro
Multiplier	Virtex-4
Ethernet MAC / PCI Express	Virtex-4
System Monitor	Virtex-6
Analog to Digital Converter	Virtex-7
Floating Point Arithmetic	Stratix-10

Successive BEOL "Span of Control" improvements enabled greater on-chip Logical Effort, and increasingly complex IP

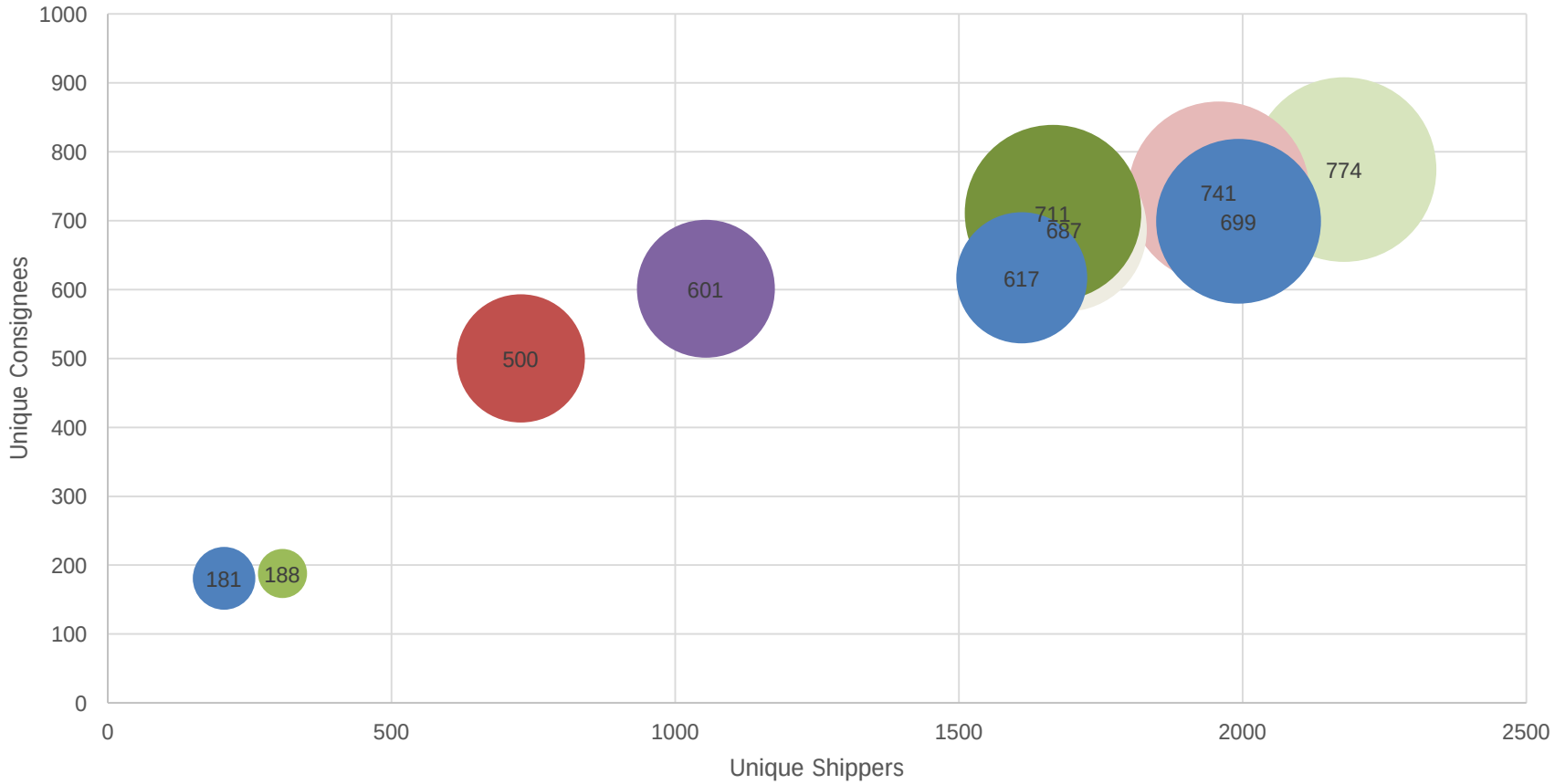
DoD Acquisition Is a Man-made Challenge



"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 compliments of Defense Business Board

CBP Data for Specific Shipments *

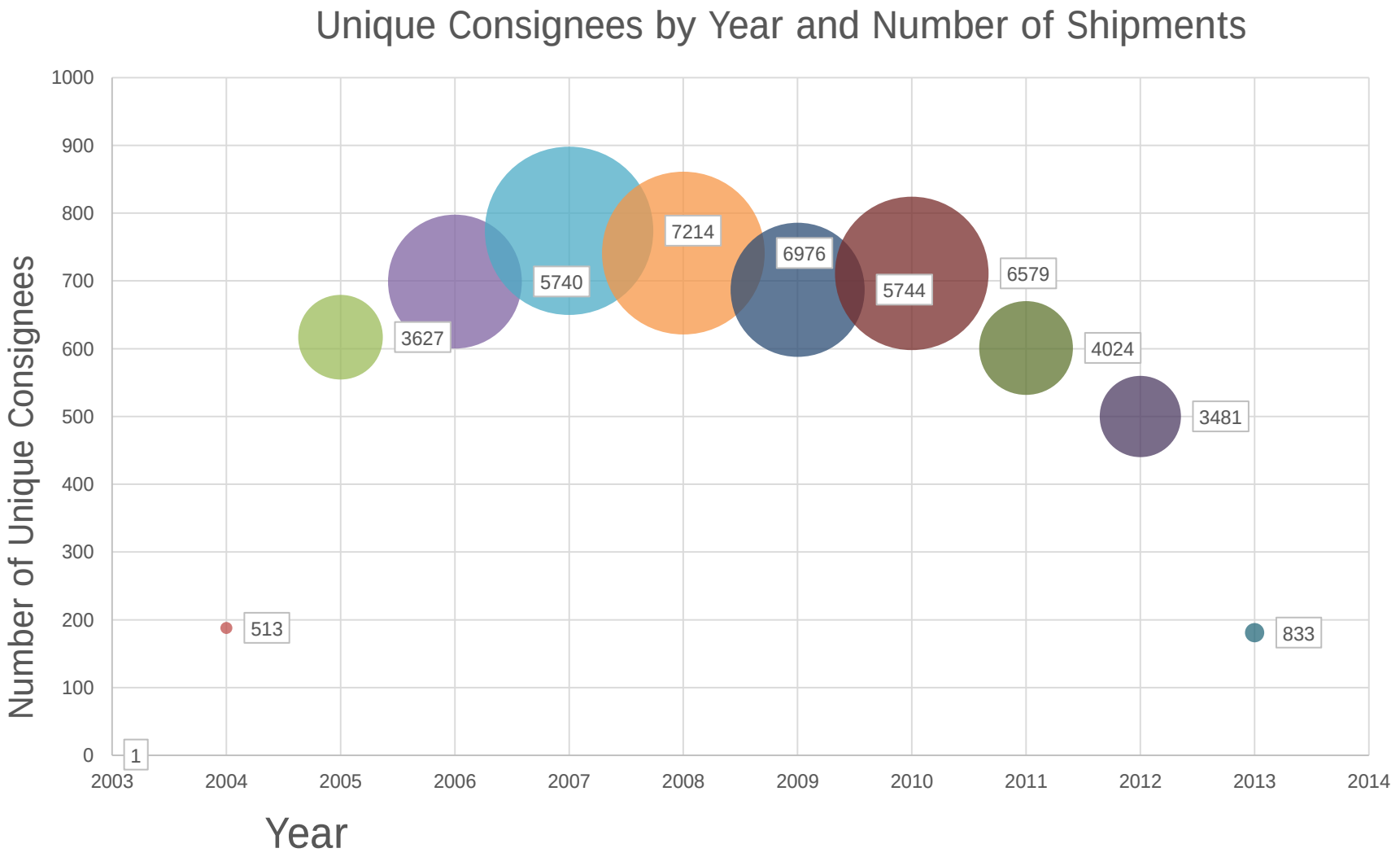


Top 90th percentile of Chinese, Hong Kong Counterfeit Exporters to US 1999-2013 Operations, data being updated to YE2016

** Data courtesy of Adam Hauch, DSS*
Compilation by Kyle Bunch, Arnett Brown, Kerry Bernstein

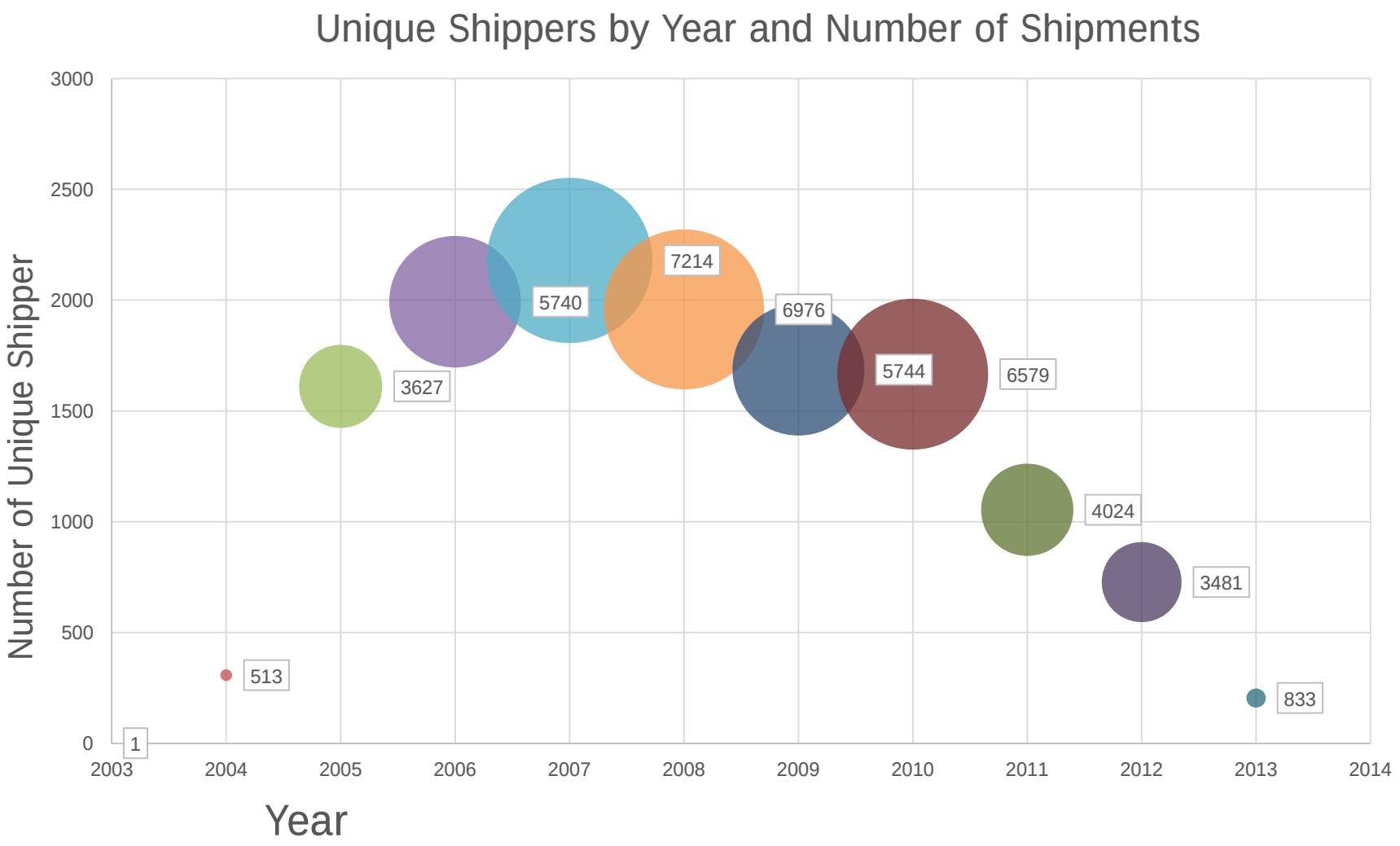
The Current US Impact

CBP Data for Specific Shipments *



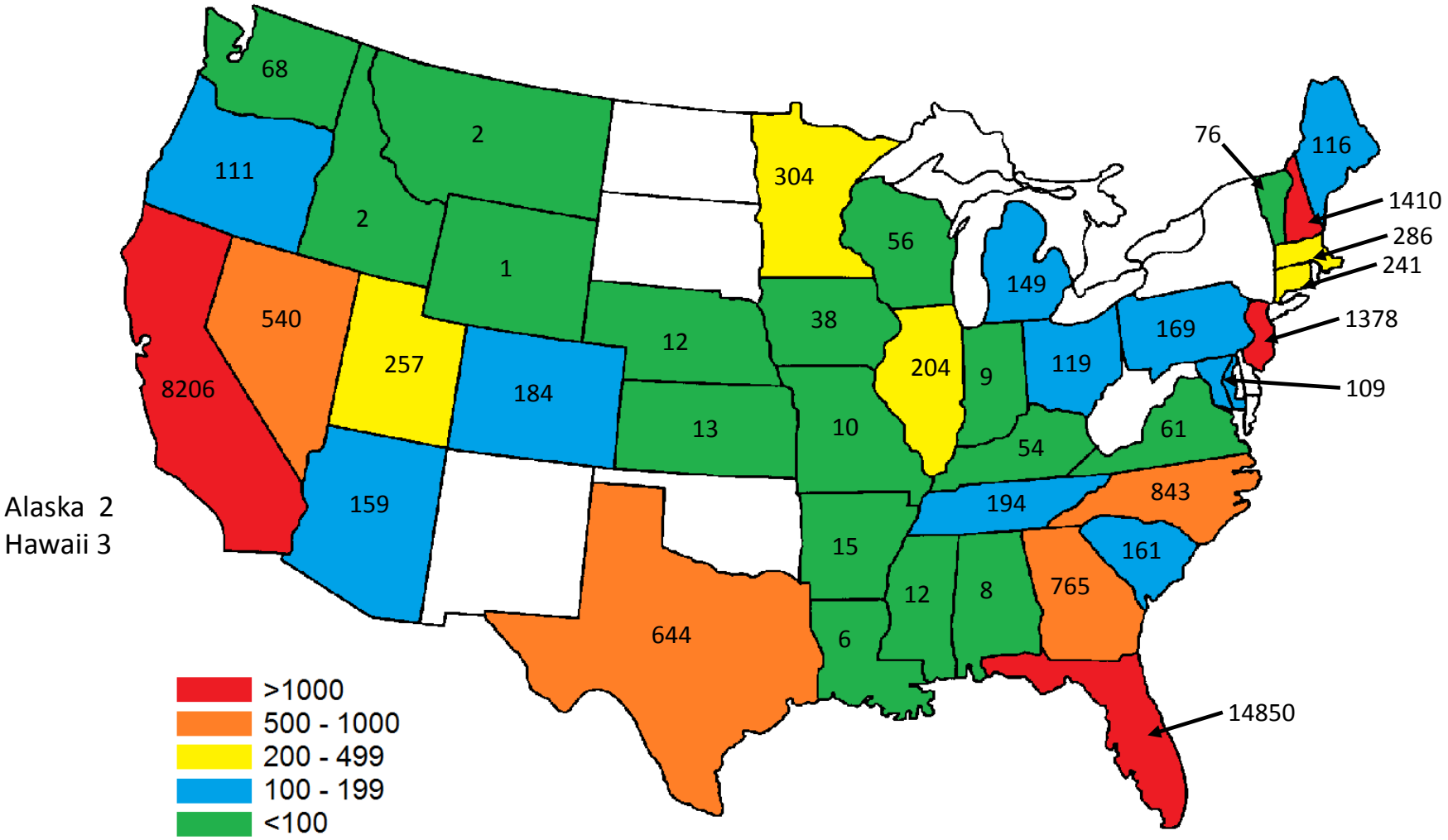
* *Data courtesy of Adam Hauch, DSS*
Compilation by Kyle Bunch, Arnett Brown, Kerry Bernstein

CBP Data for Specific Shipments *



* *Data courtesy of Adam Hauch, DSS*
Compilation by Kyle Bunch, Arnett Brown, Kerry Bernstein

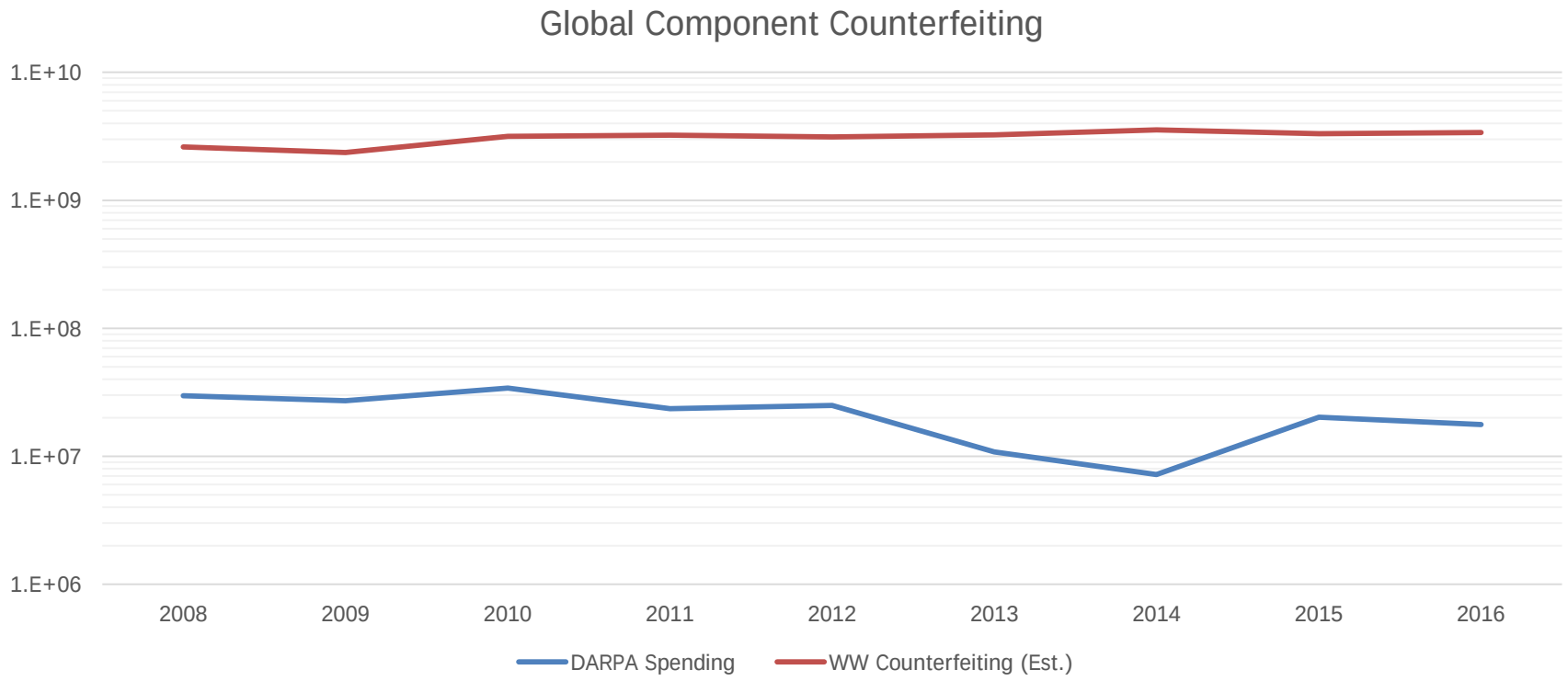
Counterfeit Destinations by State 2003-2013



* *Data courtesy of Adam Hauch, DSS*
Compilation by Kyle Bunch, Arnett Brown, Kerry Bernstein

The Science and The Data

Trends *



Effective use of limited funding is essential to address a threat 100X bigger and comprising 1% of global S/C Market.

* From "Qualification and Testing Process to Implement Anti-Counterfeiting Technologies into IC Packages" Nathalie Kae-Nune / Stephanie Pesseguier. STMicroelectronics, *DATE13 Conference 3/28/13*. Data compiled by S. Fazzari.

What It *Currently* Takes to Design a Chip

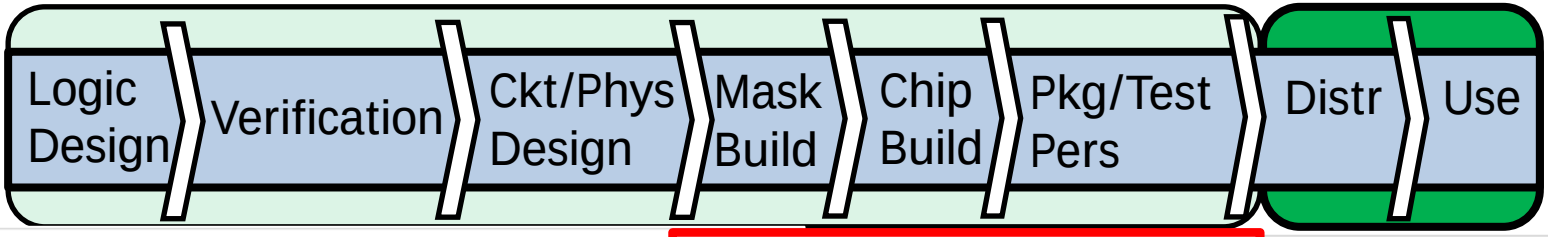
- 150 Logic Designers
- 150 Design Validation Engineers
- 50 Circuit Designers
- 25-40 Physical Designers**
- 20 Performance Verification Engineers
- 20-40 CAD/EDA Programmers**
- 10 Architects
- 10 Design Leads
- 10 Product Engineers
- 10 Design-for-Test Engineers
- 10 Timing Engineers
- 5 Technologists
- 5 Power Engineers

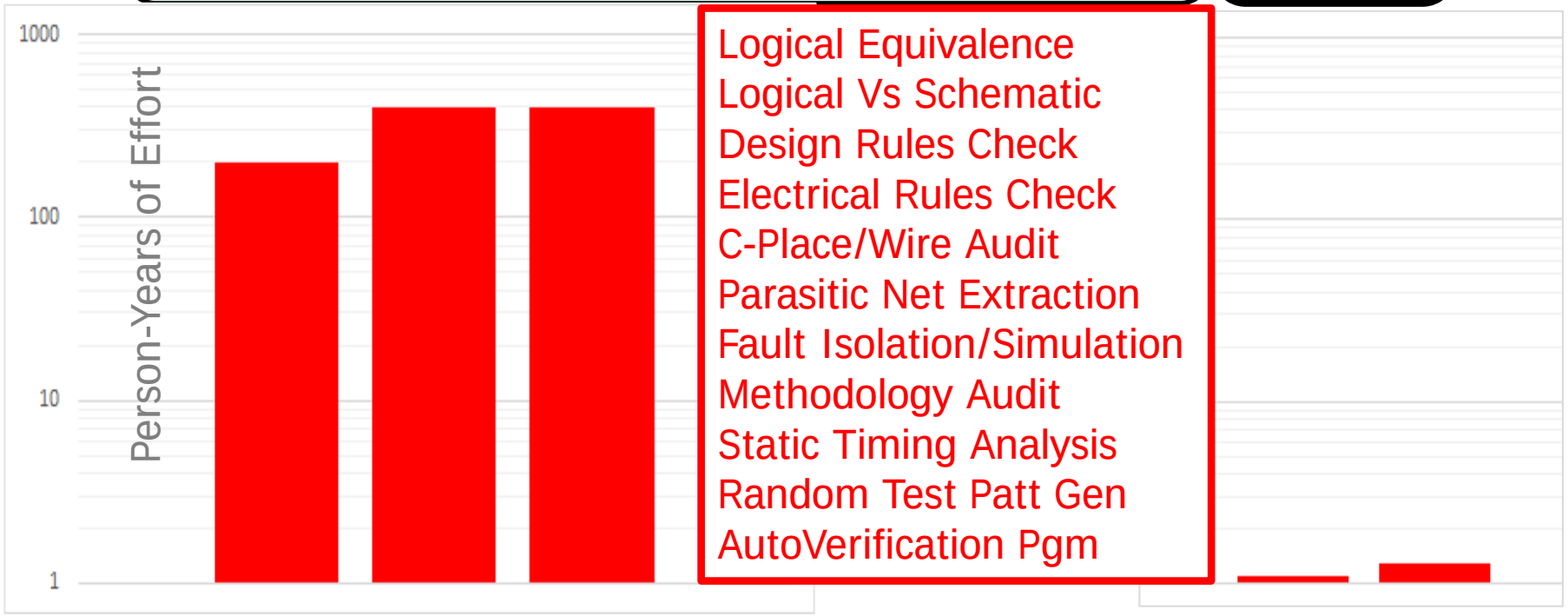
Industry technical prowess is an on-shore national treasure which is critical to delivering first-time-right, reliable high-performance product.

* Numbers from an actual product, assuming *experienced* engineers

** Count varies during design

Relative Cost of Compromising a µProcessor





Logical Equivalence
Logical Vs Schematic
Design Rules Check
Electrical Rules Check
C-Place/Wire Audit
Parasitic Net Extraction
Fault Isolation/Simulation
Methodology Audit
Static Timing Analysis
Random Test Patt Gen
AutoVerification Pgm

1000 PY required for design of a high performance processor *

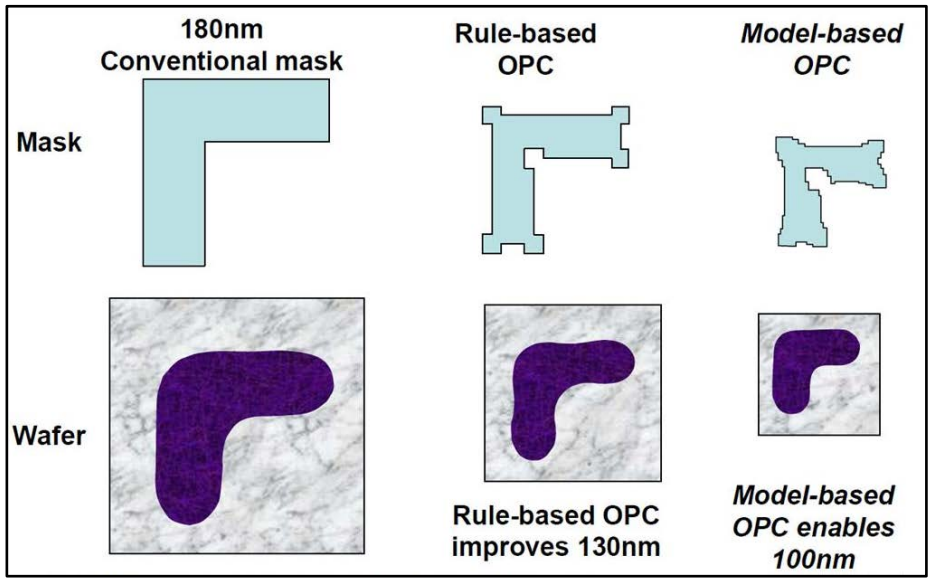
* Source: R. Wisnieff, J. Burns, IBM Research

Where would ***you*** attack a component?

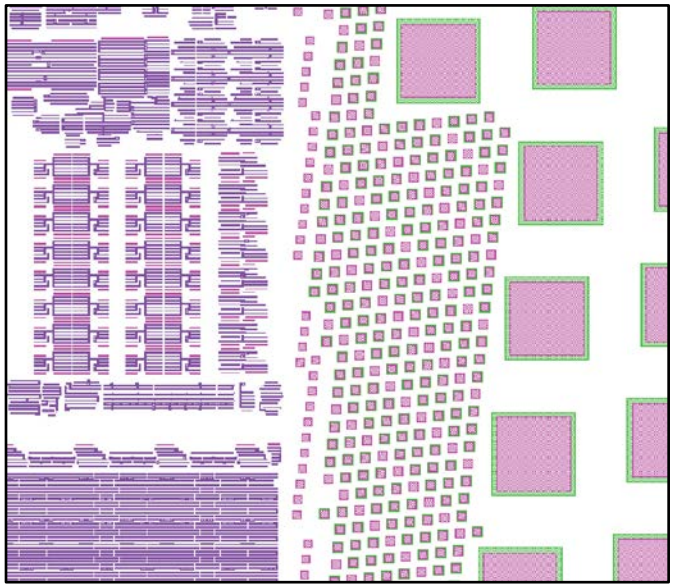
Est. t < 1.2 PY to engineer recent supply chain exploit

Source: EE Times

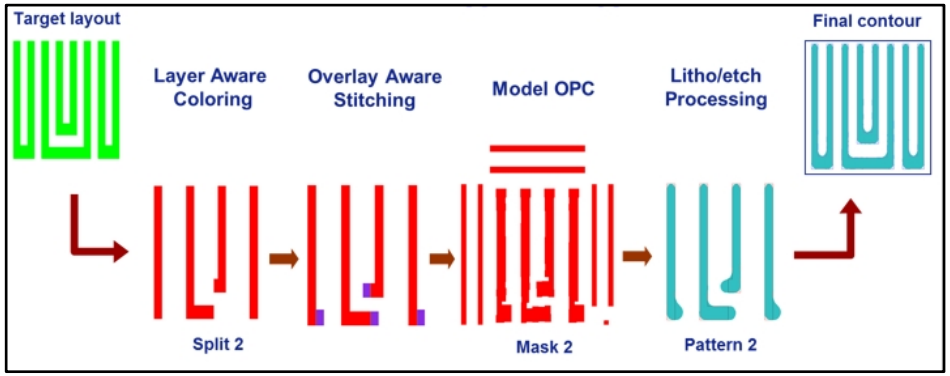
Mask Image Post-processing



https://nanohub.org/app/site/resources/2016/06/24507/slides/020.01.jpg



http://semiengineering.com/wp-content/uploads/2014/11/Fig2_Fill_65nm_20nm_MG.jpg



http://semimd.com/wp-content/uploads/2015/01/MP-F5.jpg

RET, OPC, DFM, DFY, Cheesing/Fill are closely-held, proprietary fab algorithms. GDSII sent to the fab is NOT what gets fabricated.

Required Characteristics for a useful PUF

The bar is pretty high !

- Inexpensive to fabricate - uses standard process
- Authentication can be performed in the field for free
- Has zero impact on the host reliability, lifetime, power, failure rate, yield, etc
- Can be interrogated at any time, any place, with no special equipment or training
- Doesn’t require immediate connectivity to check
- Entropy, Hamming Distances must be superior to the existing art
- Requires zero error correction coding, margin, or tolerance
- Provides trustworthy results within 2 seconds of interrogation
- Must be unspoofable and side-channel secure
- Must NEVER explicitly disclose or transmit its key or identity
- Must remain more reliable than host, and stable over time
- Must sense and report attempted compromises
- Must self-destruct upon any attempt to compromise
- Must be exquisitely difficult to reverse engineer
- Exhibits a unique identity in each instantiation.
- Tracks host’s physical and TCPIP location, movement through supply chain.

Check Your Equipment!
Features of Effective **Logic Obfuscation**

http://www.af.mil/News/Article-Display/Article/109833/team-of-airmen-to-attempt-mount-everest-climb/

First American Military Team on Mt. Everest

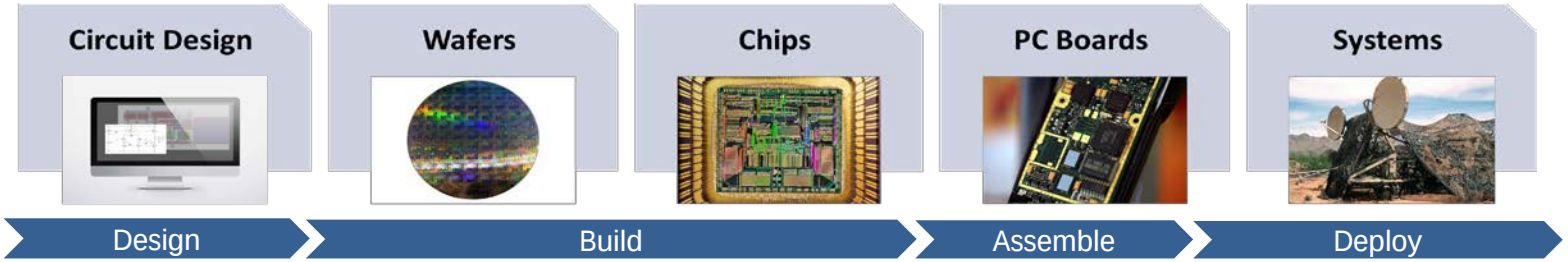
1. Hides in Physics packages exquisitely resilient to Reverse Engineering
2. Does not provide a pointer to where the personalization is stored
3. Massively asymmetric, excessively high number of potential state machines
4. Reliable / Stable / persistent. Does not reveal itself temporally
5. Logically complete; can express arbitrary logic, doesn't constrain minterm selection
6. Allows 100% test pattern coverage, fault isolation possible for shorts, opens
7. Personality doesn't need to be expressed to fab; personalized post-manufacture

We depend on proven gear to keep the warfighter safe

Potential Solutions

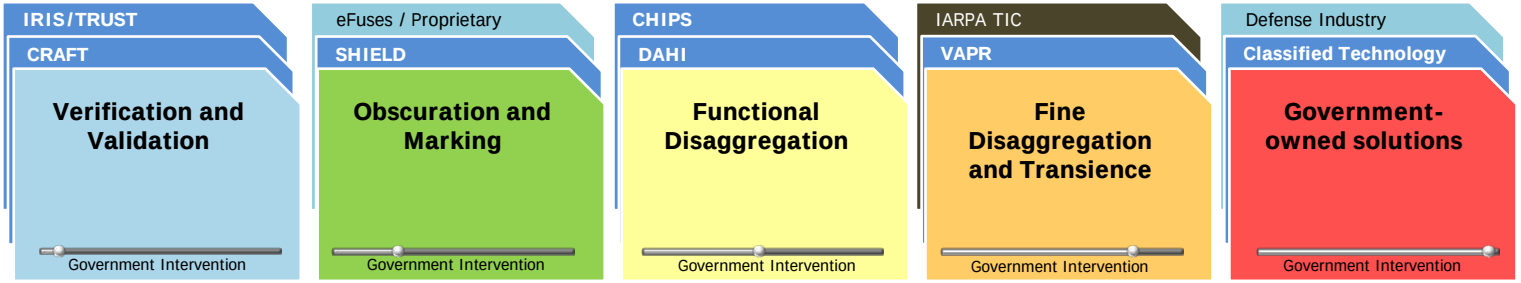
Goal: Provide (DoD) with secure, trustworthy, leading-edge microelectronics to enable critical capabilities

How does DoD acquire leading-edge microelectronics?



DoD's microelectronics supply chain relies on an evolving global enterprise of facilities and expertise to design, build, assemble, and deploy critical systems.

How can DoD ensure security while fully leveraging a globalized supply chain?



DARPA and other agencies are developing a technology-enabled portfolio of protections.

Closing Observations

1. **Its all about practicing good science.**
2. Threats to hardware security arise because of bigger problems. Addressing them requires multiple solutions.
3. Technology asymmetry will always win – It's why this threat currently exists. Let's move this asymmetry to our side.
4. We need to quit pursuing solutions to academic, hypothetical, low probability exploits. Pay attention to actual cost of entry.
5. Let US Industry do what it does best - design, build, and protect. Leverage checking methodology we already have first.
6. We will be successful by working together, not separately.

www.darpa.mil

Distribution A: Approved for Unlimited Distribution