KERRY BERNSTEIN

PROGRAM MANAGER

DARPA/MTO

THE ELECTRONICS RESURGENCE INITIATIVE

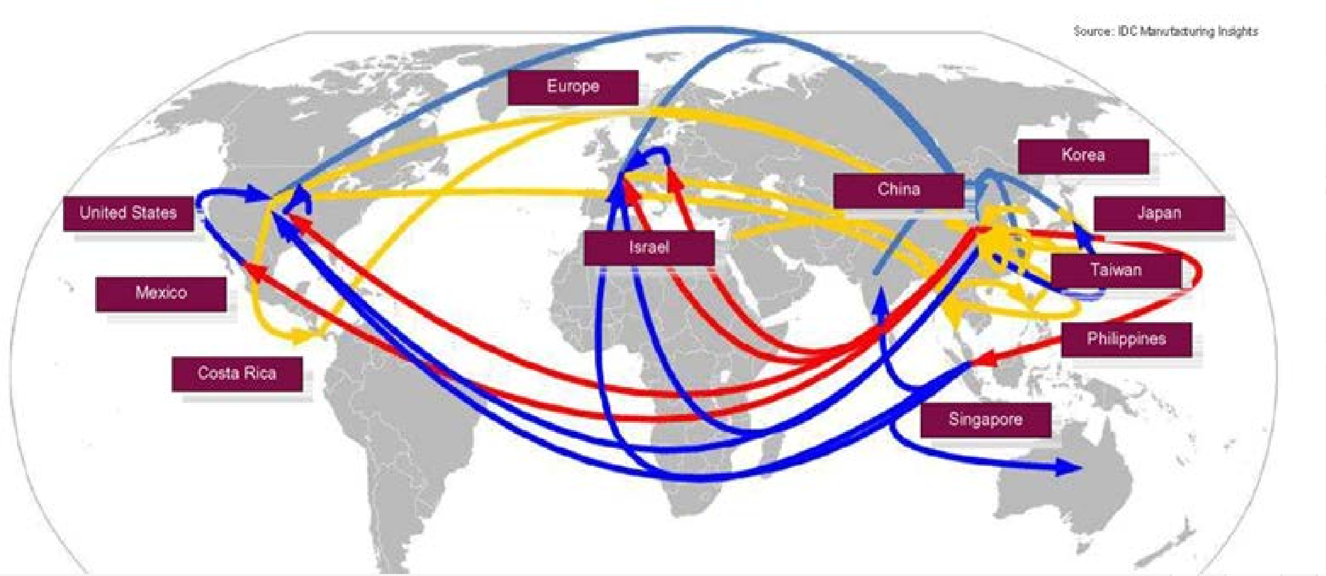
SHIELD SUPPLY CHAIN ASSURANCE TECHNOLOGY

KERRY BERNSTEIN, PROGRAM MANAGER, DARPA MTO

MICHAEL KANE, PRINCIPAL INVESTIGATOR, SRI INTERNATIONAL

CHRISTOPHER LANTMAN, SRI INTERNATIONAL

THE GLOBAL NATURE OF TODAY’S SUPPLY CHAINS MAKES CHAIN-OF-CUSTODY UNWORKABLE



Source: IDC Manufacturing Insights

Semiconductor Design

Semiconductor Manufacturing & Packaging

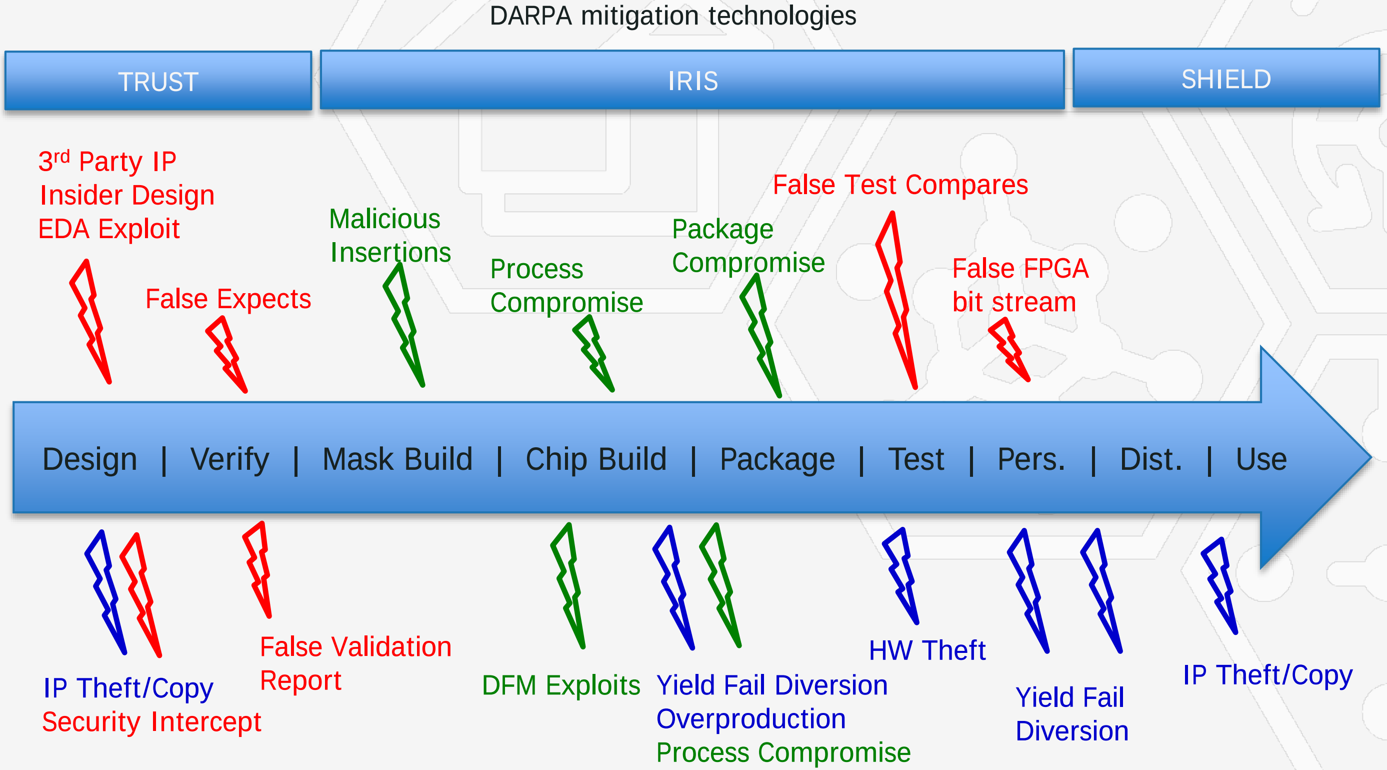
Printed Circuit Board Production

Printed Circuit Board Distribution

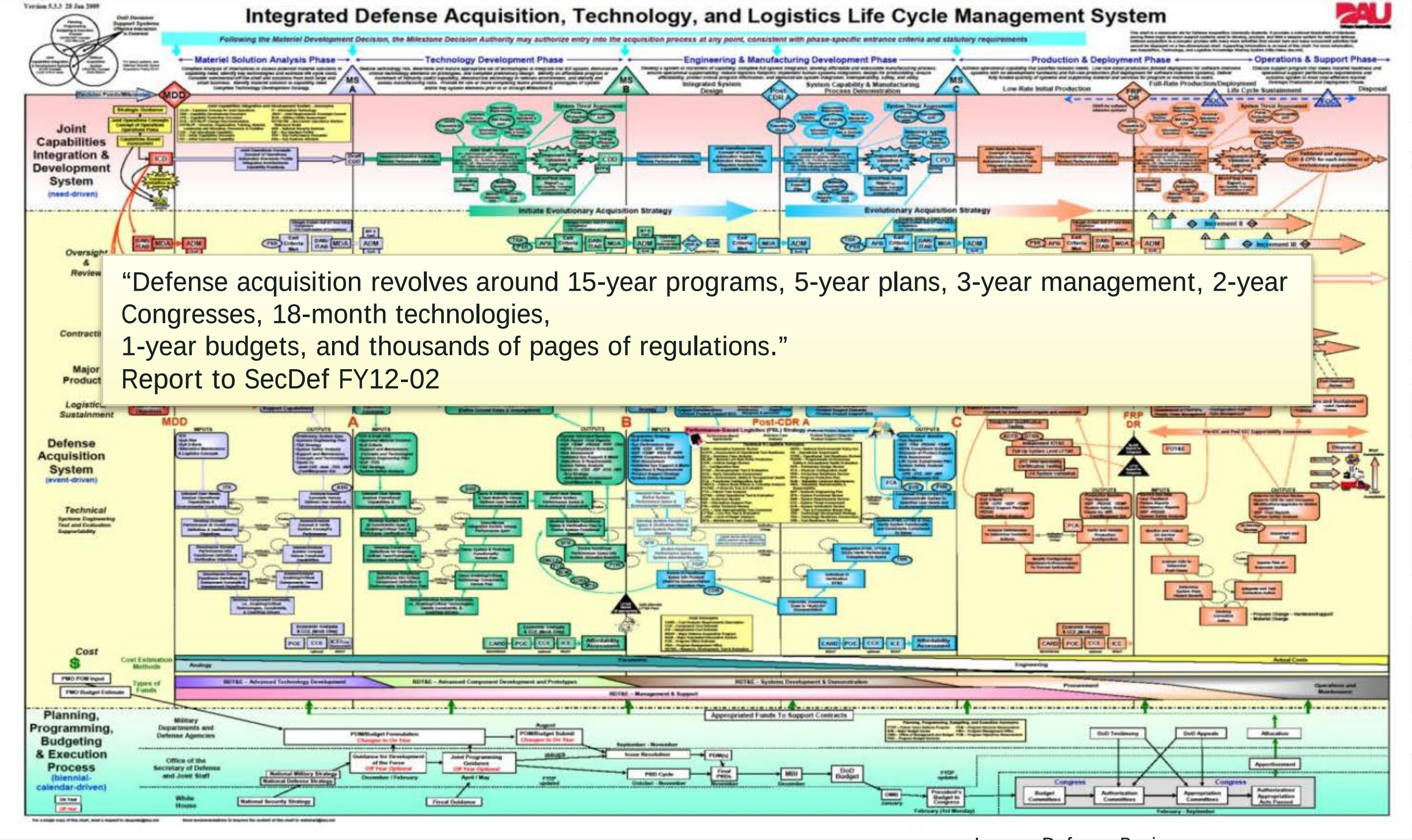
Source: IDC Manufacturing Insights & Booz Allen analysis

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

THREATS TO INTEGRATED CIRCUIT INTEGRITY



DOD ACQUISITION IS A MAN-MADE CHALLENGE


Version 5.3.3 28 Jun 2009
Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System
Following the Materiel Development Decision, the Milestone Decision Authority may authorize entry into the acquisition process at any point, consistent with phase-specific entrance criteria and statutory requirements
Materiel Solution Analysis Phase
Technology Development Phase
Engineering & Manufacturing Development Phase
Production & Deployment Phase
Operations & Support Phase
MDD
MS A
MS B
MS C
Post-CDR A
FRP DR
Integrated System Design
System Capability & Manufacturing Process Demonstration
Low-Rate Initial Production
Full-Rate Production/Deployment
Life Cycle Sustainment
Disposal
Joint Capabilities Integration & Development System
(need-driven)
ICD
CDD
CPD
Initiate Evolutionary Acquisition Strategy
Evolutionary Acquisition Strategy
Increment II
Increment III
Oversight & Review
Contracting
Major Products
Logistics/ Sustainment
Defense Acquisition System
(event-driven)
Technical
Cost
Cost Estimation Methods
Types of Funds
Planning, Programming, Budgeting & Execution Process
(biennial-calendar-driven)
DAU

“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

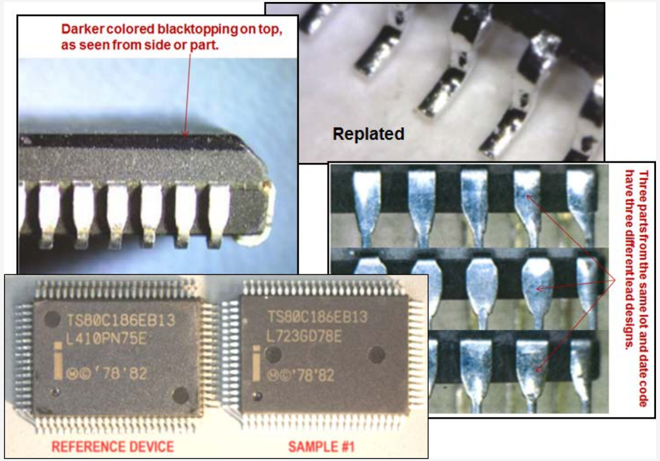
COUNTERFEITS VS CLONES

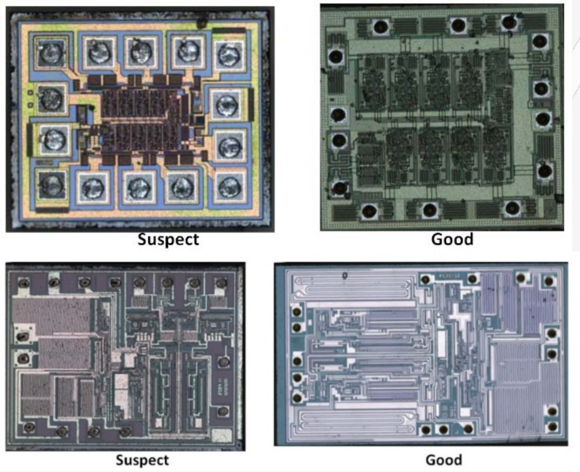
A counterfeit part is manufactured by the OEM and presented as new, but the performance and reliability of the part is questionable:

- 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

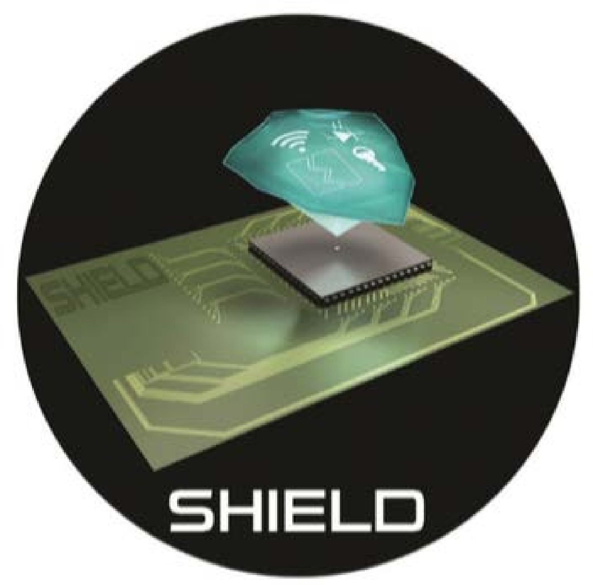

Darker colored blacktopping on top, as seen from side or part.
Replated
Three parts from the same lot and date code have three different lead designs.
TS80C186EB13
L410PN75E
'78'82
TS80C186EB13
L723GD78E
'78'82
REFERENCE DEVICE
SAMPLE #1



All images courtesy of NSWC Crane

SHIELD

TECHNICAL OVERVIEW



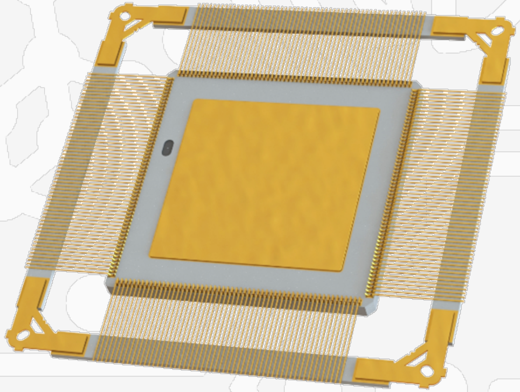
This work was funded by the Defense Advanced Research Projects Agency (DARPA) Microsystems Technology Office (MTO) under Contract No. HR0011-15-C-0010. The views, opinions and/or findings expressed are those of the authors and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government. Approved for Public Release, Distribution Unlimited.

SRI International®

SHIELD SECURES THE COMPONENT SUPPLY CHAIN

Electronic systems that are relied upon for national security depend on the performance and reliability of highly sophisticated electronic components. However, counterfeit electronics entering the DoD supply chain place our military personnel and our country at risk.

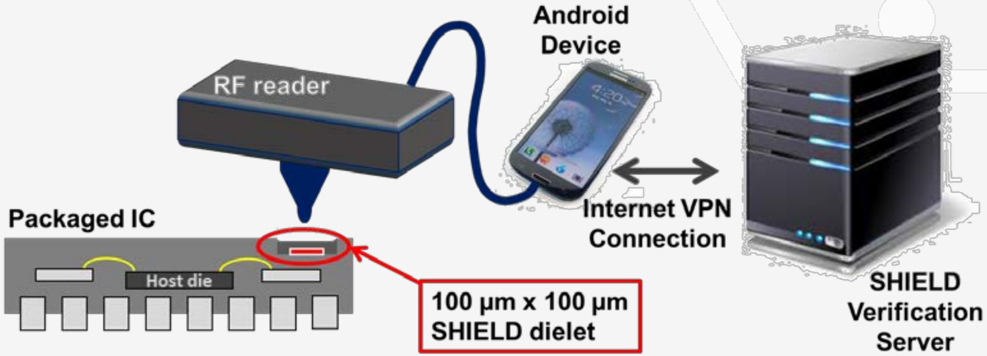
Under DARPA's SHIELD Program, SRI International has developed a novel end-to-end solution to secure the electronic component supply chain by using a low-cost identification chip embedded in microelectronic circuit packaging.



SHIELD OVERVIEW

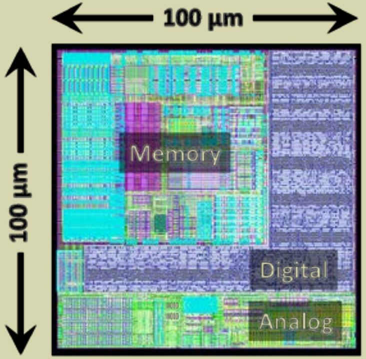
The SHIELD ID chip is called a “dielet” because it is only 100 µm square, smaller than a grain of fine sand. It can be authenticated wirelessly via an RF reader communicating securely over the internet with a remote SHIELD Verification Server.

The SHIELD dielet provides a hardware root-of-trust, guaranteeing the authenticity of the host IC by making counterfeiting very difficult and prohibitively expensive.

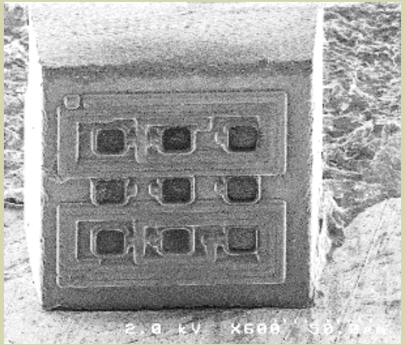


THE SHIELD DIELET

The dielet has a full Advanced Encryption Standard (AES) encryption engine with a unique 256-bit secret key programmed into nonvolatile memory at wafer probe and also enrolled with the server, enabling secure dielet authentication through a challenge-response protocol. It is fabricated in the TSMC 28 nm HPC CMOS process.



Layout of SHIELD dielet

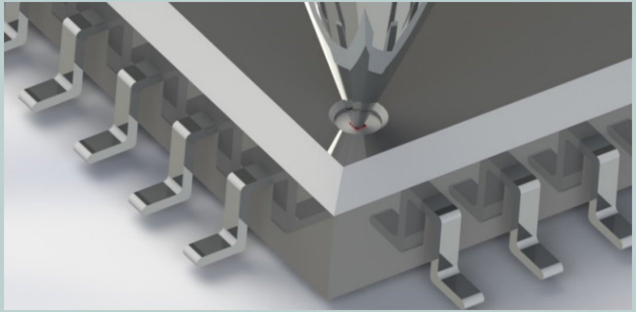


SEM image of dielet

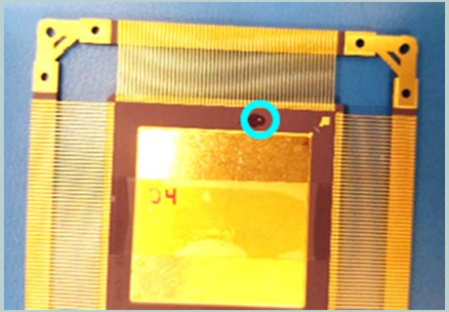
Dielet on nose
of Lincoln penny

A SHIELD ENABLED IC

Because it is only 100 µm square and 30 µm thick, a SHIELD dielet is easily embedded in a host IC package.



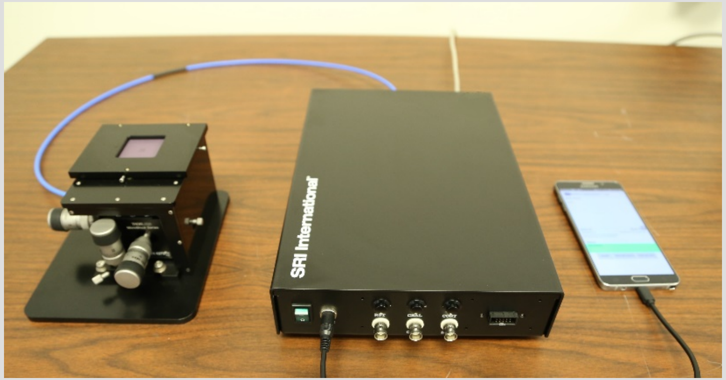
Dielet being placed into well in QFP package



SHIELD-enabled Xilinx FPGA in Kyocera 228-lead QFP package

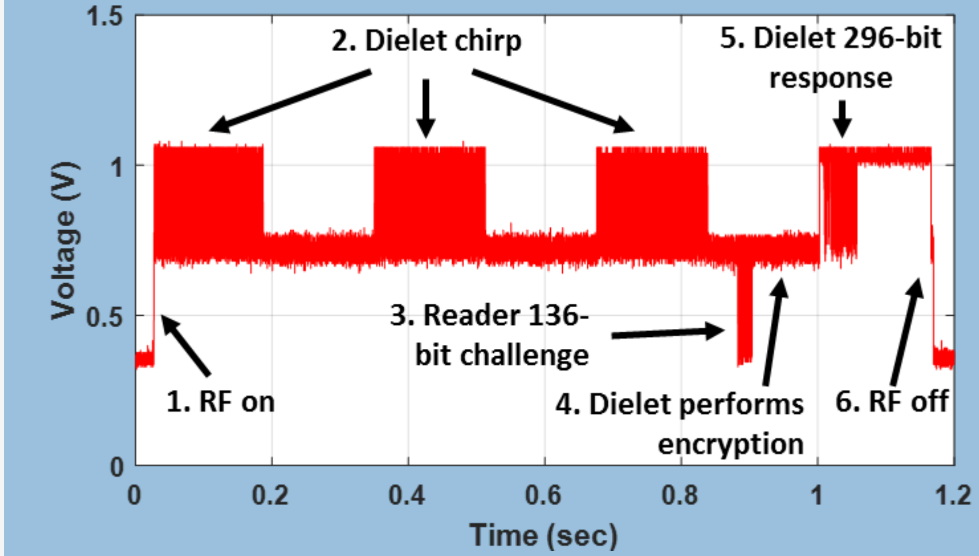
THE SHIELD READER

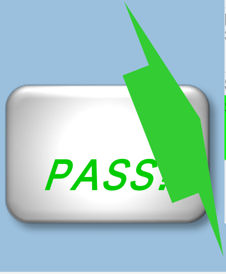
The SHIELD reader communicates wirelessly with the dielet. It is controlled by an Android handheld device such as a tablet or smartphone, which communicates over the internet via a secure VPN connection with the secure SHIELD server.

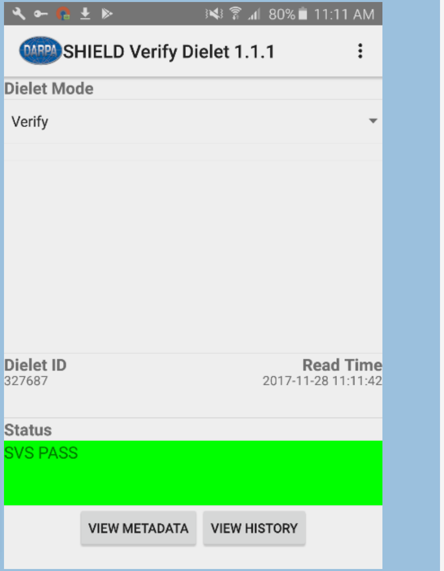


The SHIELD server is hosted on Amazon Web Services (AWS), where the dielet keys are stored securely using the AWS Key Management Service.

A SHIELD AUTHENTICATION TRANSACTION







SHIELD Verify Dielet 1.1.1

Dielet Mode

Verify

Dielet ID 327687

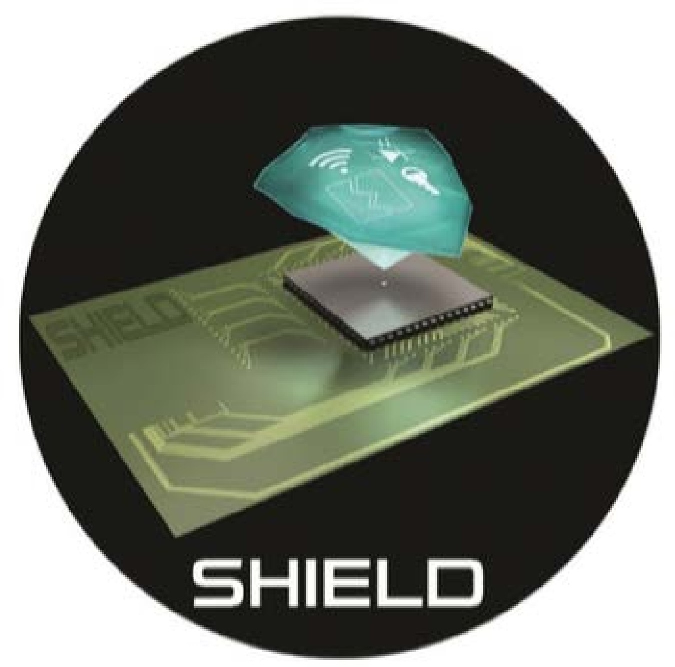
Read Time 2017-11-28 11:11:42

Status

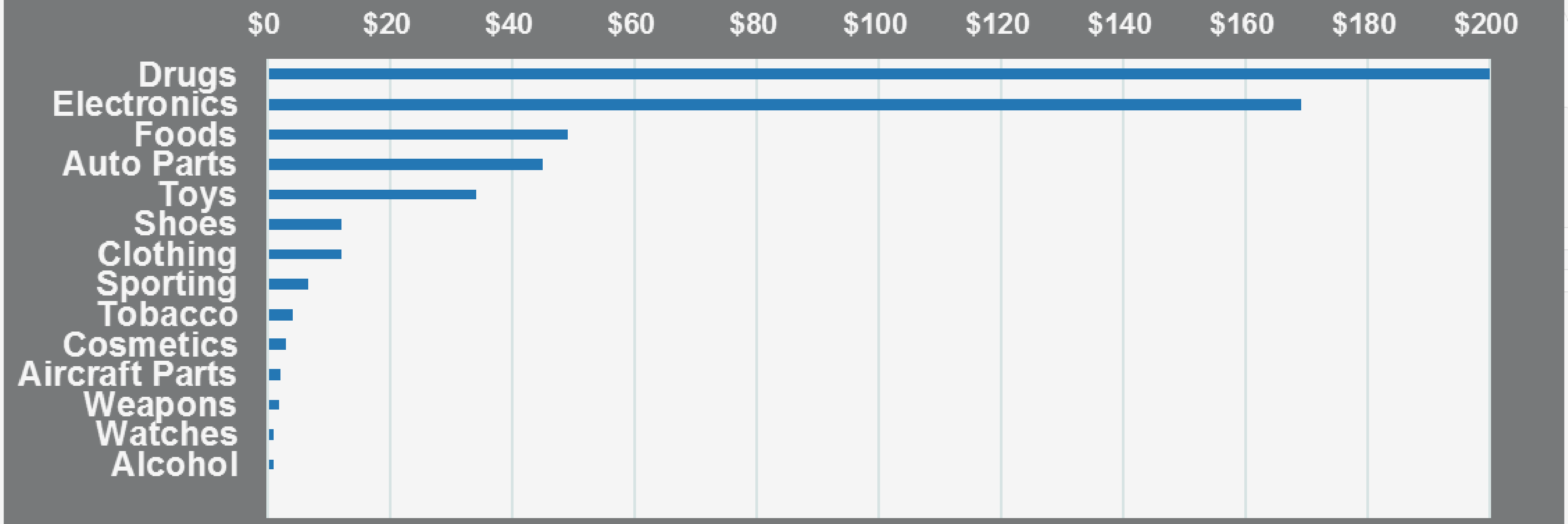
SVS PASS

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

MARKET ANALYSIS FOR ANTI-COUNTERFEITING SOLUTION



THE COST OF COUNTERFEITING IS ESTIMATED TO APPROACH A HALF TRILLION DOLLARS

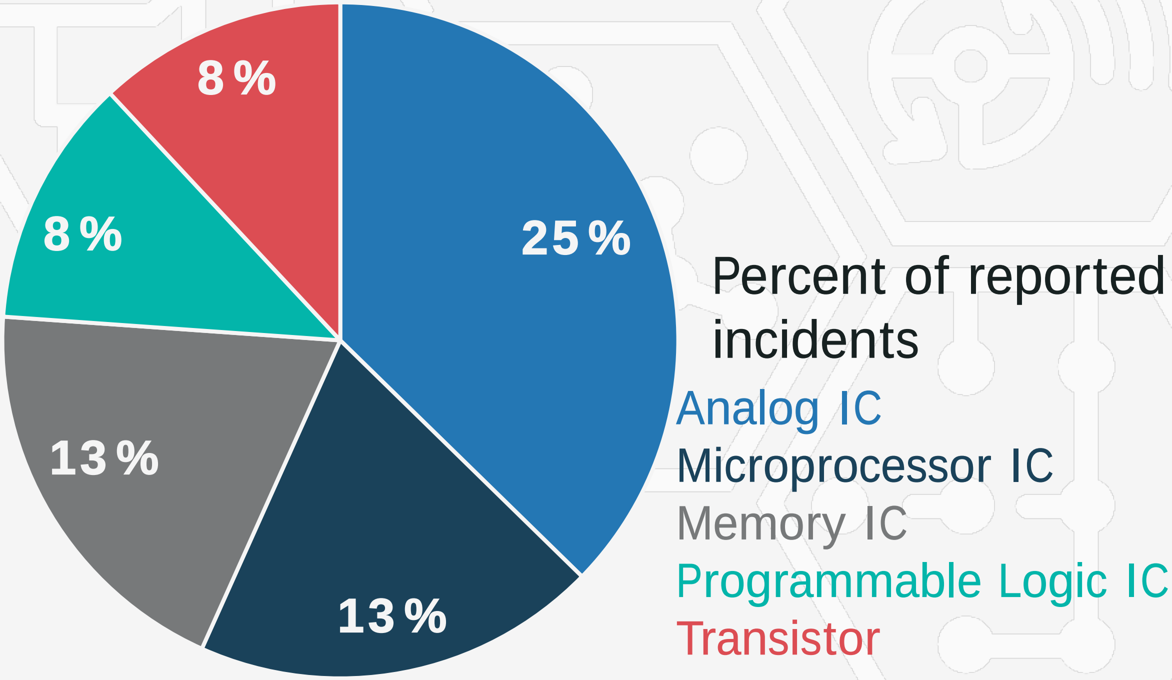


Global estimated counterfeiting revenue by industry in 2017 ($ Billion)

Sources: Havoscope (http://www.havocscope.com/counterfeit-goods-ranking/). Data used as a reference by the industry and multiple sources such as PwC, EY; NetNames, Counting the cost of counterfeiting, 2015; Frontier Economy - The Economic Impacts Of Counterfeiting And Piracy

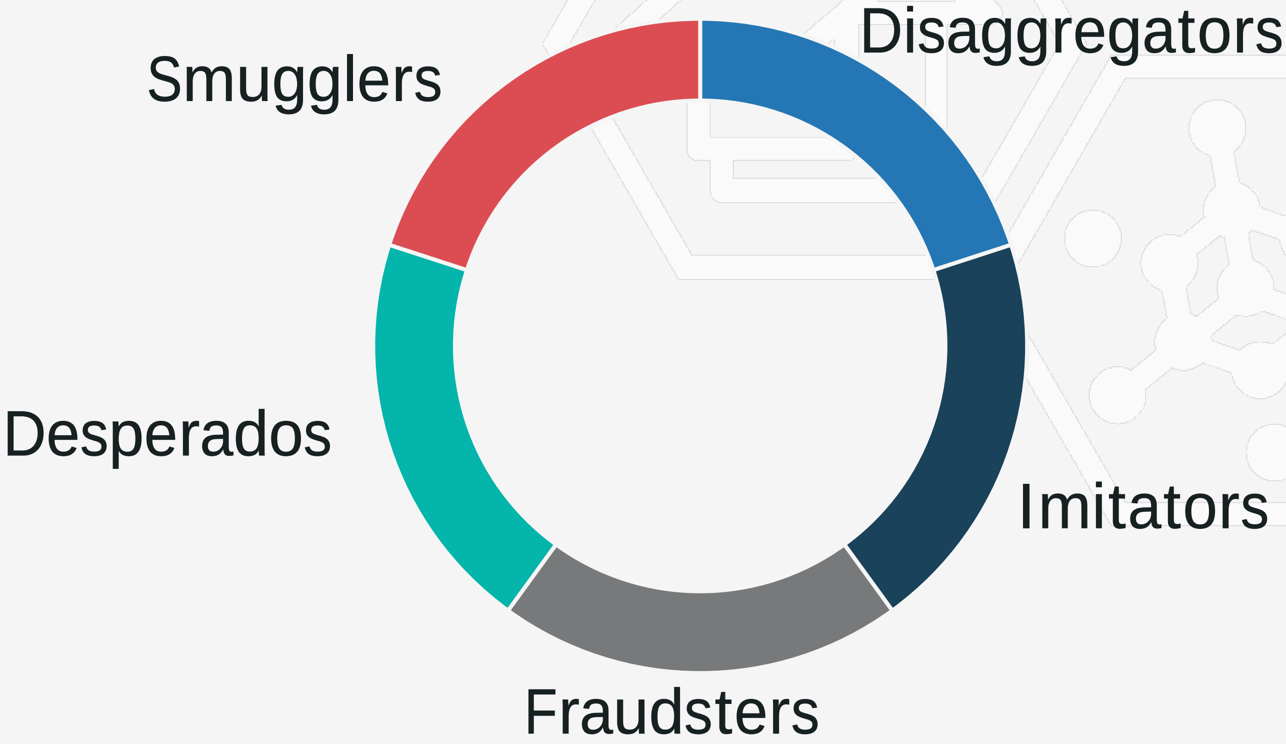
ELECTRONICS INDUSTRY IS HIT HARD BY COUNTERFEITING

US semiconductor manufacturers are losing $7.5Bn in annual revenue to counterfeiting


Percent of reported incidents

Sources: Anti-Counterfeiting of Integrated Circuits: RFID Tags as a Countermeasure, Sathya Kanth Vardhanapu, 2012; IHS Part Management, 2012; Counterfeited components, IHS, 2014

BRAND OWNERS ARE CONFRONTED BY FIVE COUNTERFEITER GROUPS



Many prominent terrorist organizations rely on illicit trade for financing up to 20% of terrorist attacks, an example of which is the 2015 Charlie Hebdo attack in Paris.

Sources: Business strategies in the counterfeit market , Journal of business research, 2011; Counterfeiting, piracy and smuggling: Growing threat to national security, EY, 2014

GRAY MARKET ACTIVITIES ARE A CHALLENGE

“Criminals remove microchips from old devices, recycle them and resell them to illegal device manufacturers. It is significant problem in Asia.”

(Senior Director Strategic Development, **Qualcomm**)

END-TO-END ANTI-COUNTERFEITING SOLUTIONS CAN ALSO GATHER SUPPLY CHAIN INFO

Spectrum of security services

Integrated System

Sell anti-counterfeiting tag with unique signatures, readers and encrypted data backbone.

Maintenance & Support

Remotely control reader, pick and place equipment, provide associated services (e.g., maintenance and repair).

Data Management

Create and validate product-specific data sets. Automatically report incidents.

Inactivate recalled products and clear associated data sets.

Brand protection

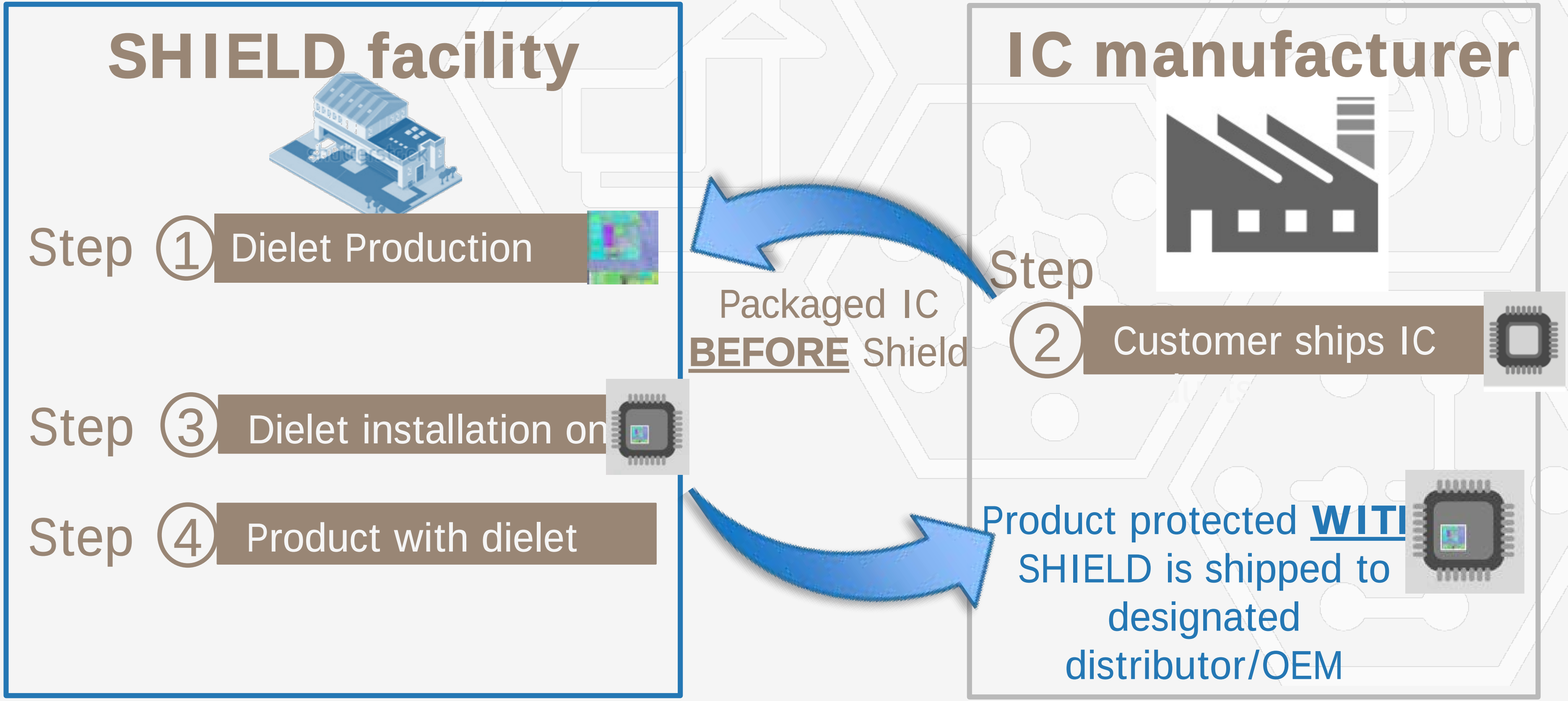
Monitor product and data streams along the supply chain.

Assist originators in prosecution of counterfeiting activities.

Value creation

Source: Webinar TAKING A FRESH LOOK AT COUNTERFEITING IN PHARMA & MEDICAL DEVICES: FROM ROOT CAUSES TO CURRENT SOLUTIONS, SICPA CLARIANT, 2017; Fighting counterfeit pharmaceuticals, PwC, 2017

SUPPLY MODEL OF SHIELD



SHIELD facility

Step ① Dielet Production

Step ③ Dielet installation on

Step ④ Product with dielet

Packaged IC **<u>BEFORE</u>** Shield

IC manufacturer

Step ② Customer ships IC

Product protected **<u>WITH</u>** SHIELD is shipped to designated distributor/OEM

SRI CONVERTS GOVERNMENT INVESTMENT TO SOCIETAL IMPACT

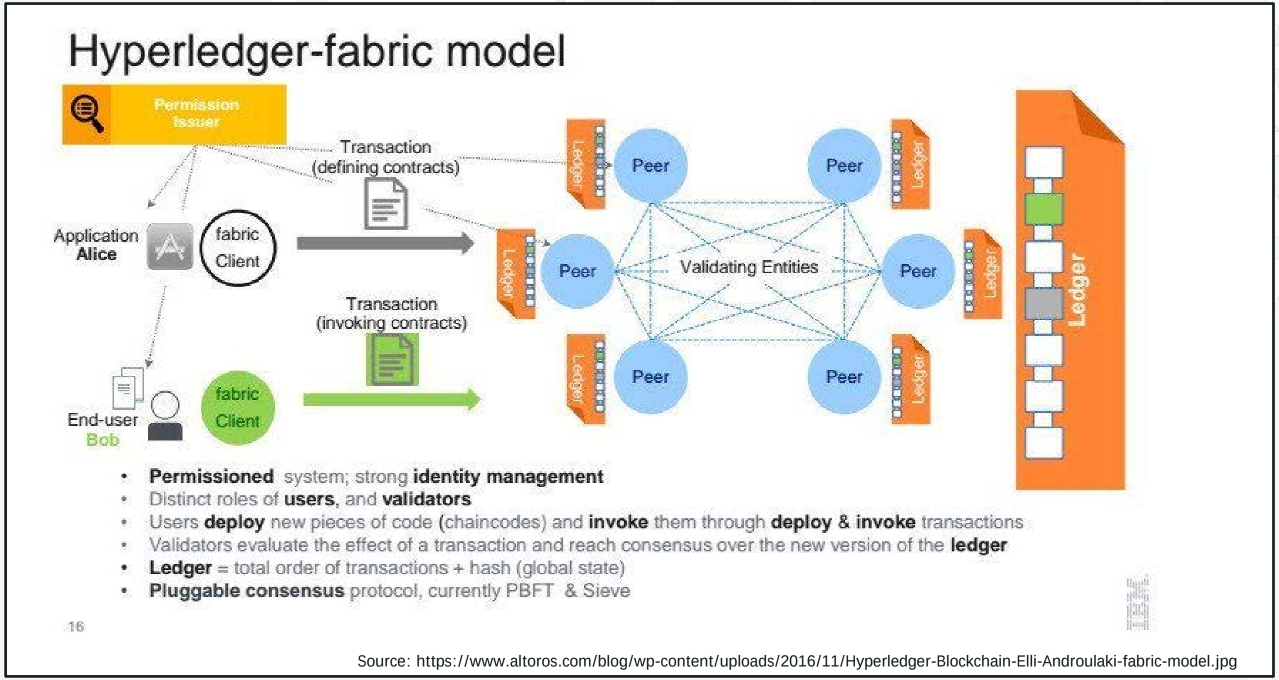
We look forward to partnering with you to bring SHIELD to the electronics industry.

CONTRACTS AND TRUST

https://evolllution.com/opinions/personalized-service-key-to-winning-training-contracts/

THE HYPERLEDGER PROJECT

IDENTIFY AND ADDRESS IMPORTANT FEATURES FOR A CROSS-INDUSTRY OPEN STANDARD FOR DISTRIBUTED LEDGERS



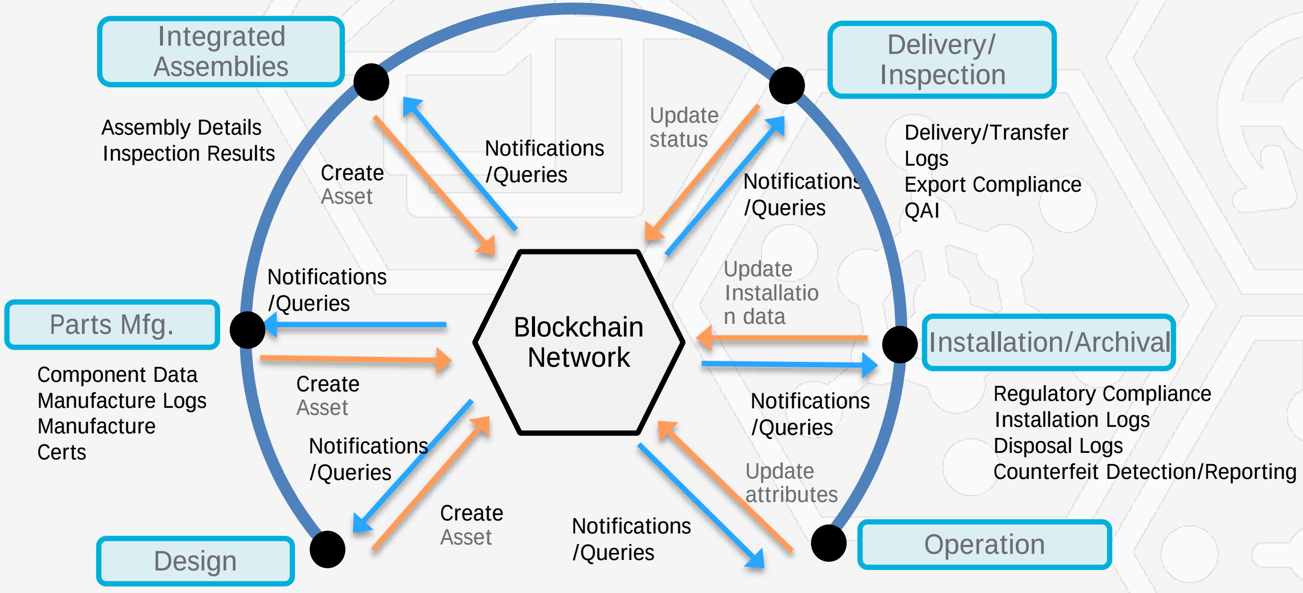
Hyperledger-fabric model

- **Permissioned** system; strong **identity management**
- Distinct roles of **users**, and **validators**
- Users **deploy** new pieces of code (chaincodes) and **invoke** them through **deploy** & **invoke** transactions
- Validators evaluate the effect of a transaction and reach consensus over the new version of the **ledger**
- **Ledger** = total order of transactions + hash (global state)
- **Pluggable consensus** protocol, currently PBFT & Sieve

16

Source: https://www.altoros.com/blog/wp-content/uploads/2016/11/Hyperledger-Blockchain-Elli-Androulaki-fabric-model.jpg

THE BLOCKCHAIN-PROTECTED SUPPLY CHAIN



Design Specs
Design Certifications

Operational Usage data

Potential Smart Contract Triggers at each stage

Image compliments of IBM Research

Distribution A, Approved for Unlimited Distribution

BLOCKCHAIN HW/SW BRIDGE / DRIVER SYSTEMS ARCHITECTURE

Chain of Trust in Blockchain/Hardware-Backed Supply Chains

Interaction/Reporting Layer

Visualiazation to track components and assemblies through various stages and time frames of a supply chain. Roles for various network participants.

Blockchain Layer

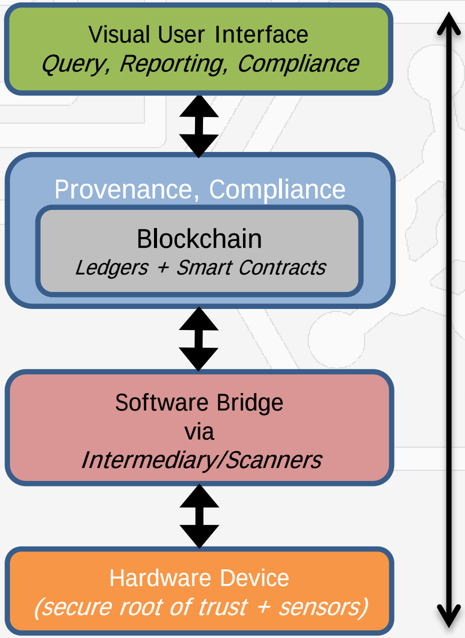
Immutable and certified recording of events observed on components at various stages of the supply chain in to the Blockchain Ledger.

Bridge Layer

Software Bridge on scanners to read data from components/assemblies with SHIELD hardware

Hardware Layer

Authentication, encryption, identity, data recording and reporting when sensed



End to End multi-party chain-of trust

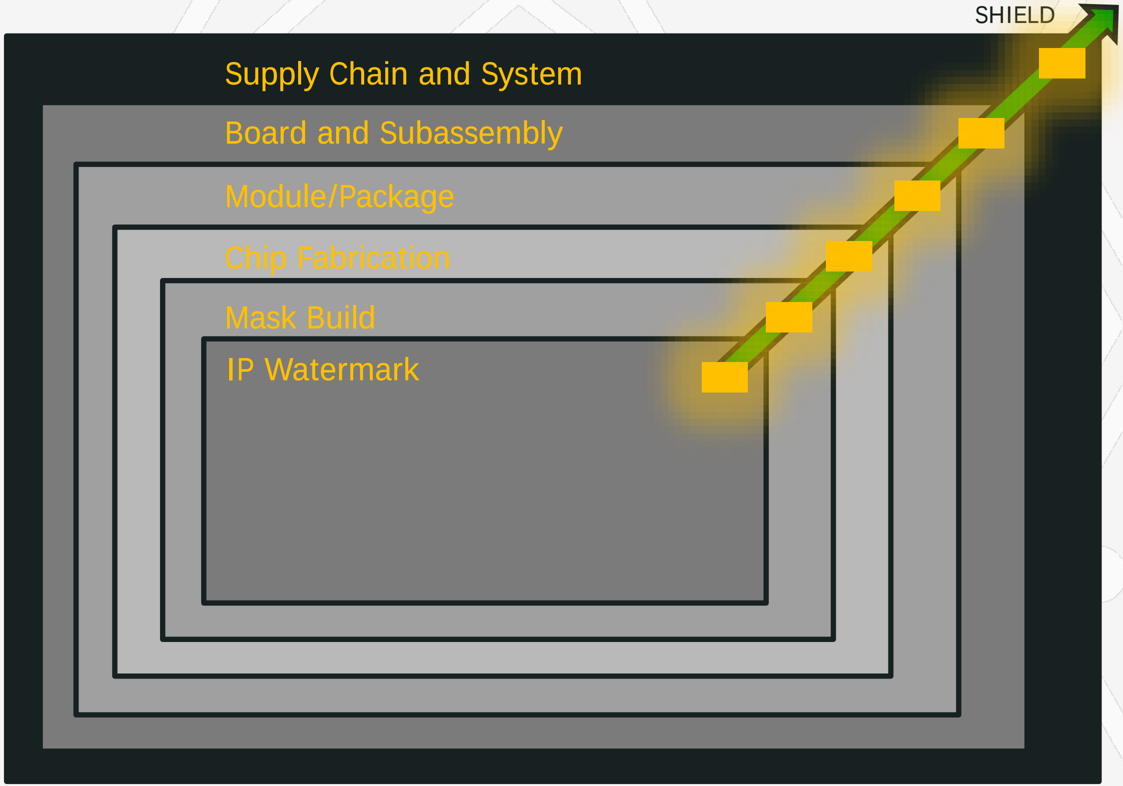
Protocols based on

- public/private keys
- encryption, signing
- HW identity

Source: IBM Research

Distribution A, Approved for Unlimited Distribution

HIERARCHICAL, AUDITABLE SHIELD/BLOCKCHAIN INTEGRITY



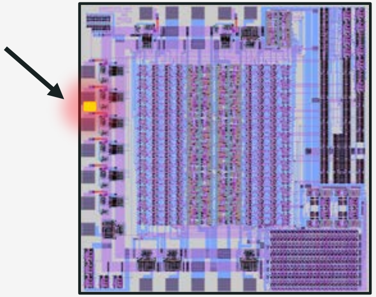
Distribution A, Approved for Unlimited Distribution

SHIELD-BASED MANUFACTURING CHAIN-OF-ASSURANCE

https://www.boldbusiness.com/communications/blockchain-pentagon-cybersecurity/

Watermark the base design

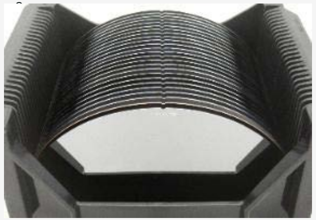
- SHIELD-supported Blockchain of on-chip AVP/RTPG ScanRing Outputs and LBIST/ABIST
- IBM Hyperledger / Smart Contracts



https://commons.wikimedia.org/wiki/File:Intel_80386_SX_die.JP

Include as IP in the chip

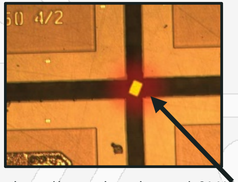
- To maintain chip provenance through the supply chain
- Make use of open space on chip to instantiate dielet IP
- May be used as a watermark throughout the design
- Example shown: discrete placement on unused I/O pad



http://www.h-square.com/Wafer_Aligners.html

Attach SHIELD to wafer

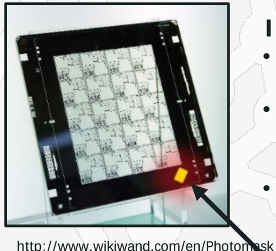
- SHIELD dielet is physically affixed to wafer blanks at supplier
- Track wafer authenticity through process gates in-line
- Interrogated at process gate transfer



https://www.photonics.com/a61419/For_Glass_and_Silicon_Wafer_Cutting_Shorter

Install in the wafer's dicing streets (kerf)

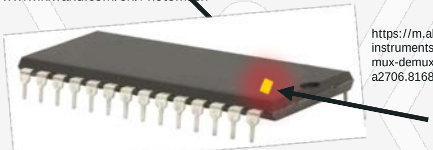
- To maintain design integrity during manufacturing.
- Dielet instantiated into kerf GDSII layout and diced out at singulation



http://www.wikiwand.com/en/Photomask

Install within the chip reticle

- To maintain integrity of the chip design during manufacturing.
- Dielet physically attached to reticle frame or glass and interrogated at transfer points
- Dielet instantiated as a site in the reticle



https://m.alibaba.com/guide/shop/texas-instruments-cd74hct4051e-ic-logic-analog-mux-demux-16dip_61468369.html?spm=a2706.8168337.0.0.boxicQ

Install within- or upon-chip packaging

- To provide component supply chain provenance
- custom package with recess for dielet, OR affixed to surface of chip with epoxy.

SHIELD IP can ensure trusted components from an untrusted fab

Microsystems Technology Office Microsystems Technology Office Microsystems Technology Office Microsystems Technology Office

ERI ELECTRONICS RESURGENCE INITIATIVE

SUMMIT

2018 | SAN FRANCISCO, CA | **JULY 23-25**

Distribution A, Approved for Unlimited Distribution