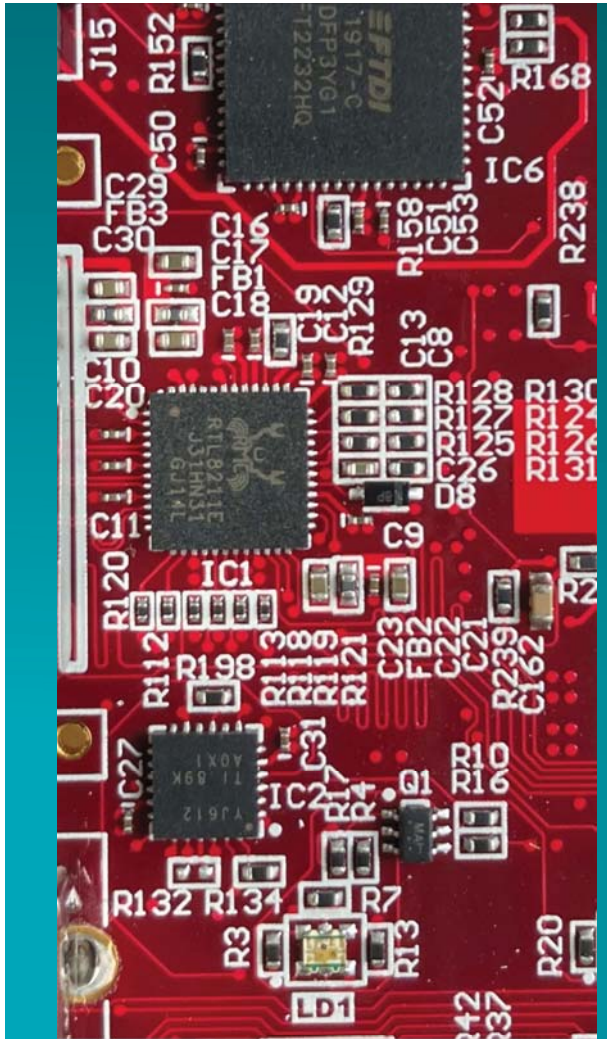
Supply Chain Security Workshop

April 28 & 29, 2021

MEPTEC
THE NEXT GENERATION

www.meptec.org

Booz | Allen | Hamilton



A PERSPECTIVE ON THE DOD SUPPLY CHAIN

Saverio Fazzari *fazzari_saverio@bah.com*
Doug Palmer *palmer_doug@bah.com*

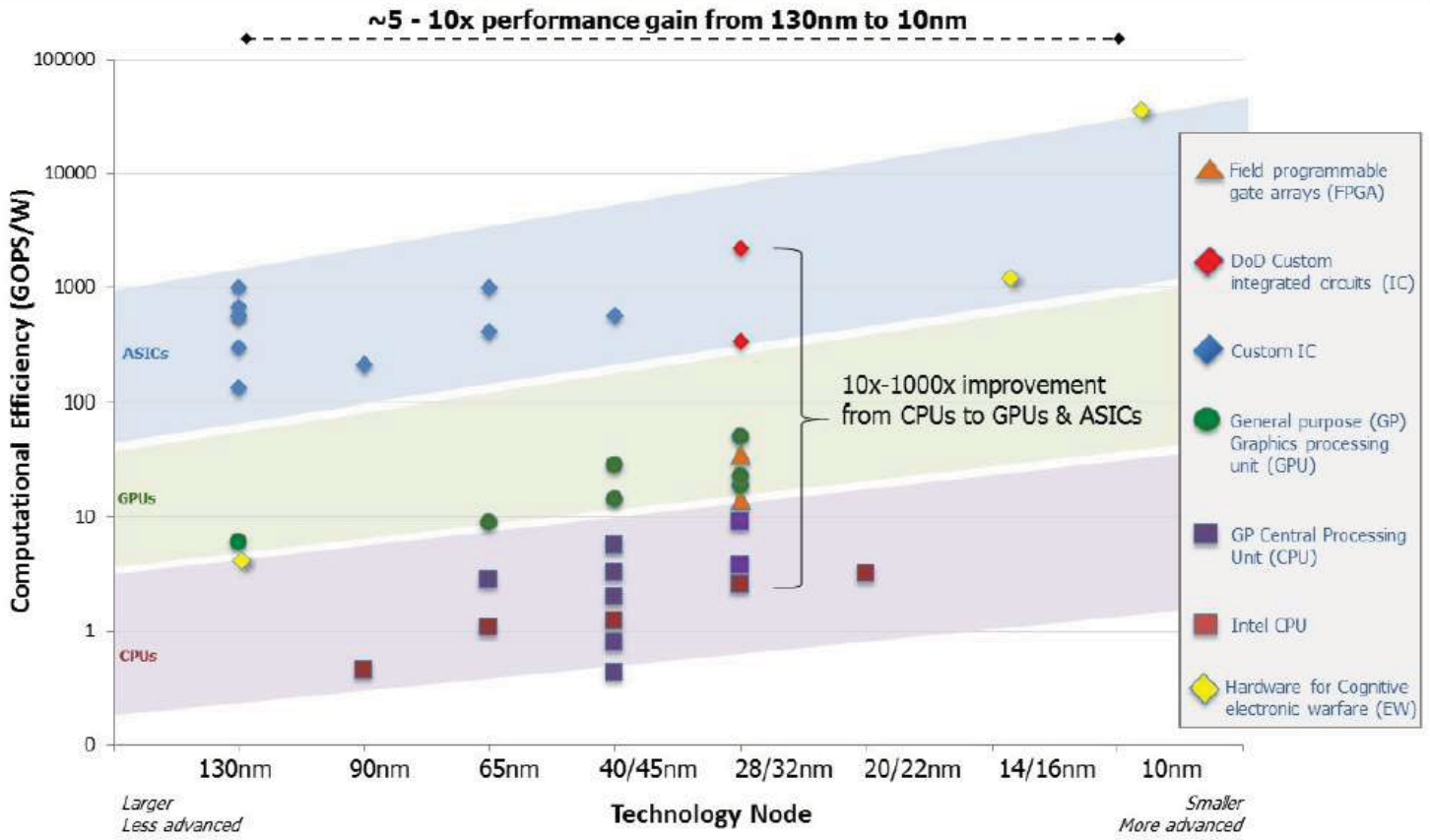
APRIL 2021

CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER

OVERVIEW

- Introduce the challenge problem for supply chain issues in DoD
- Past history in this space
- Current approaches
- Tools that Booz Allen uses.

THERE IS A SHIFT UNDERWAY AS PROGRAMS ADVANCE FROM TODAY'S PROCESSES TOWARDS ADVANCED NODES



DOD INITIATIVES

- **DoD has a focus on upgrading microelectronics used by Defense systems/platforms**
  - Platform requirements will require next generation hardware to meet needs
  - Both Government and Commercial off the shelf (GOTS/COTS) parts are being built
  - Vast Majority of $1.5 Billion DOD ICs are COTS such as Intel processors and FPGAs

Current technology requirements

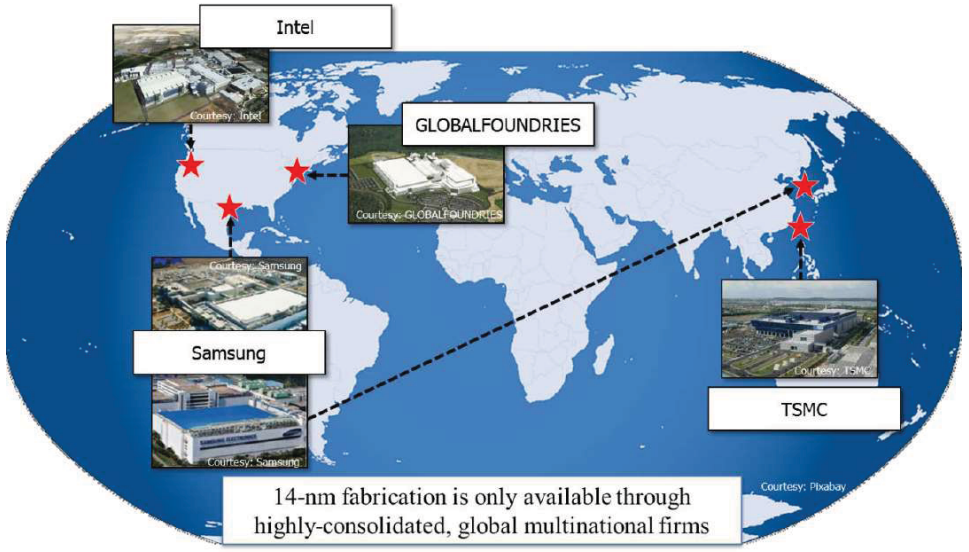
Digital COTS - Global Foundries (production node is 45nm)

Analog GOTS – Global Foundries (production node is 130 nm)

RF GOTS – Qorvo

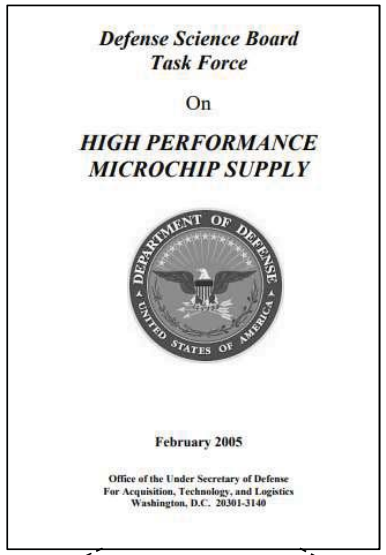
Rad Hard – Honeywell(150nm)

GOTS are built due to Size, Weight, Area, Power, Cost, Environment and Security (SWAPCES) reasons



ADVANCED MICROELECTRONICS PLAY AN INTEGRAL ROLE IN U.S. MILITARY TECHNICAL ADVANTAGE, AND ARE A SIGNIFICANT DOD BUDGET EXPENDITURE

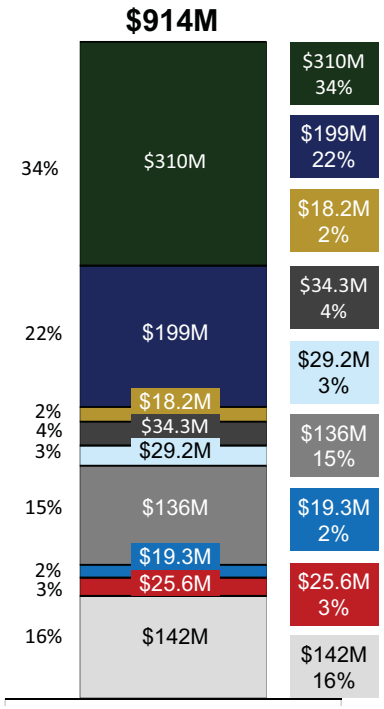
DoD Reliance Upon Microelectronics



"The microelectronics industry [is the] supplier of hardware capability that underlies much of America's modern military leadership technology"

Amount Spent by DoD on Semiconductor Components[1]

– Year 2015 –

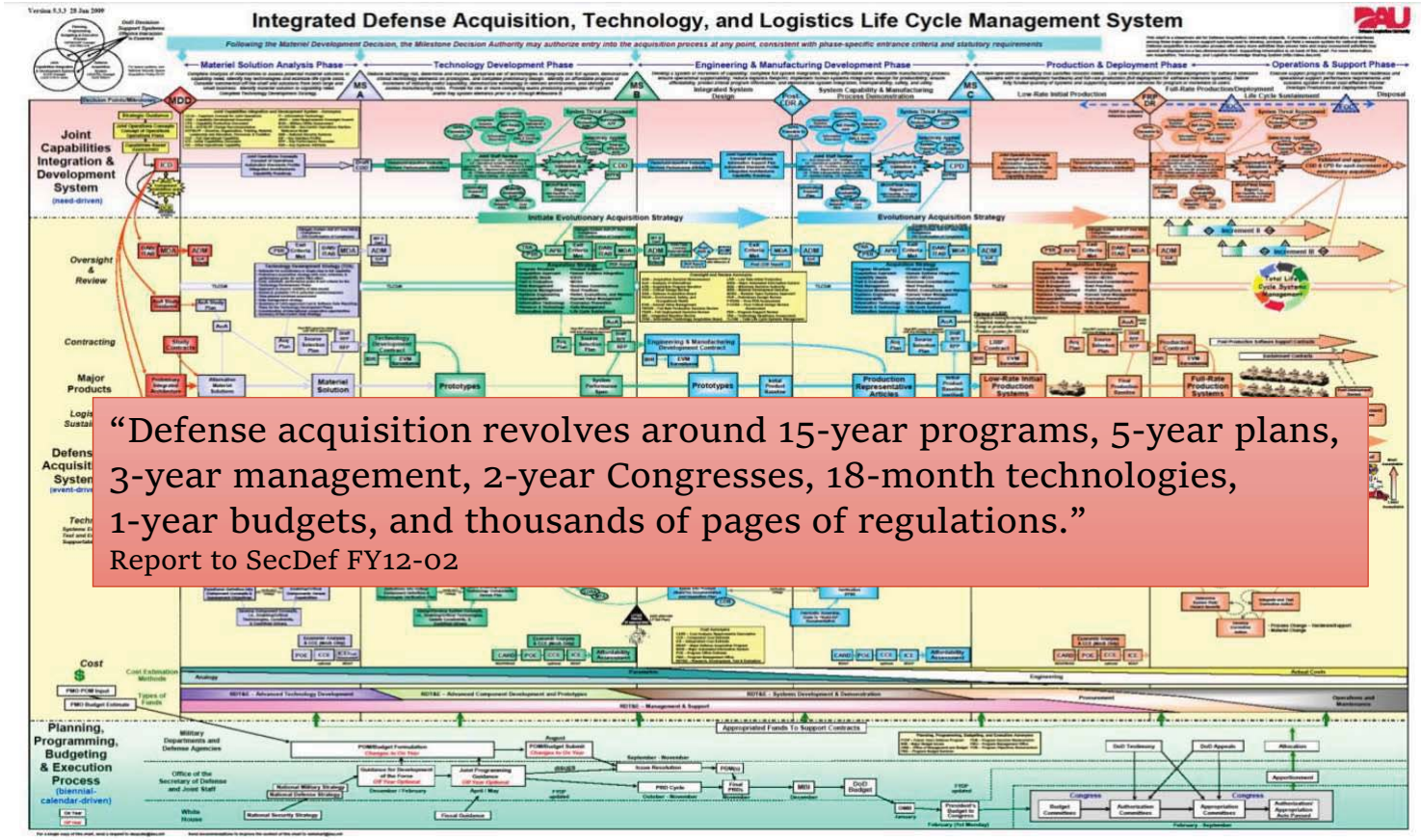


Semiconductor Types

Type	Description
Logic	▸ From simple logic gates and flip-flops to field-programmable gate arrays (FPGAs)
Memory	▸ ICs used for storage and general processing – NOR Flash, NAND Flash, DRAM, SRAM, EEPROM
DSP	▸ Digital Signal Processor (DSP) – MPU's optimized for processing communications signals
MCU	▸ Micro-controller Unit (MCU) – contains processor core, memory, and input/output ports
MPU	▸ Micro-processing Unit (MPU) – primarily Intel core processors
Analog	▸ Single-purpose analog and mixed-signal integrated circuits used for sound, voice, video transmission
Sensors	▸ Accelerometers, yaw rate sensors, gyroscopes ▸ Temp. sensors, pressure sensors, MEMs
Optoelectronics	▸ LEDs, photo transistors, photo diodes, photo-light emitters and detectors, opto-couplers
Discretes	▸ Single circuit elements – diodes, bipolar transistors, RF transistors, power transistors

Note: 1) Amount spent by DoD is amount of parts purchased by Defense Supply Center, Columbus (DSCC); Projections are based on 2015 Databeans report forecast
Source: Databeans 2011 Mil/Aero Semiconductor report and Booz Allen analysis

DOD ACQUISITION IS A MAN-MADE CHALLENGE

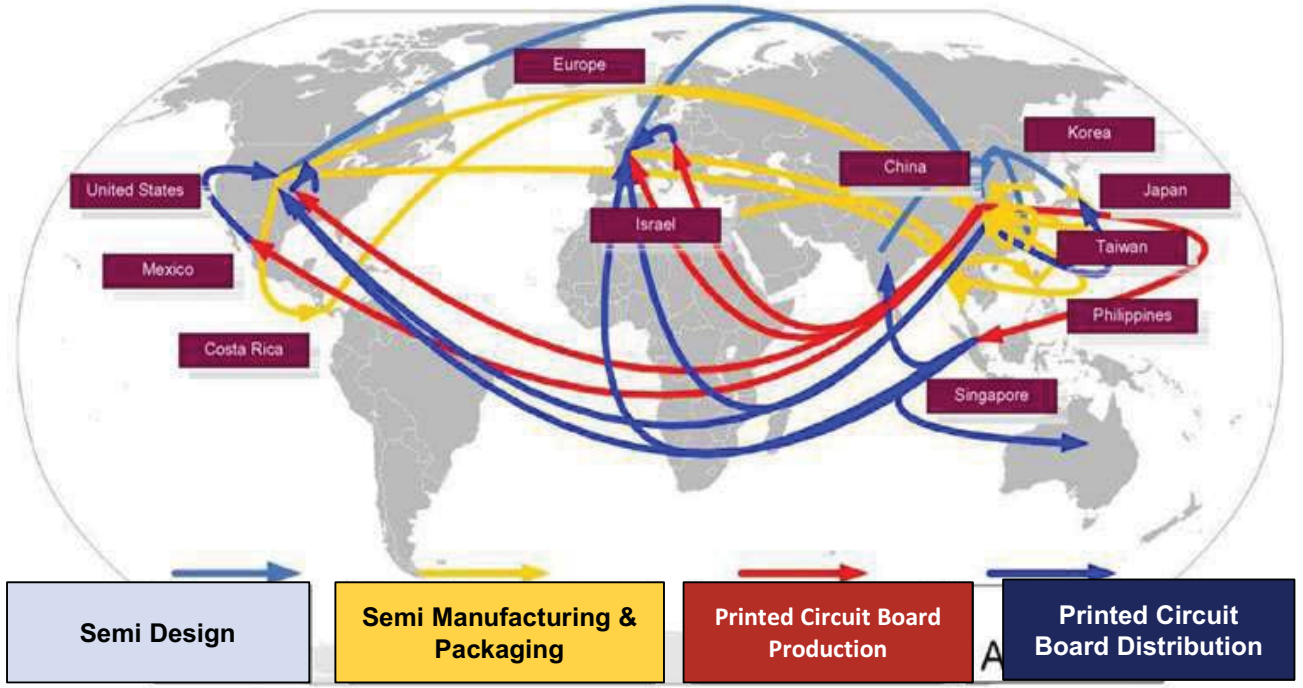


"Defense acquisition revolves around 15-year programs, 5-year plans, 3-year management, 2-year Congresses, 18-month technologies, 1-year budgets, and thousands of pages of regulations."
Report to SecDef FY12-02

Image: Defense Business Board

THIS IS A GLOBAL PROBLEM

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

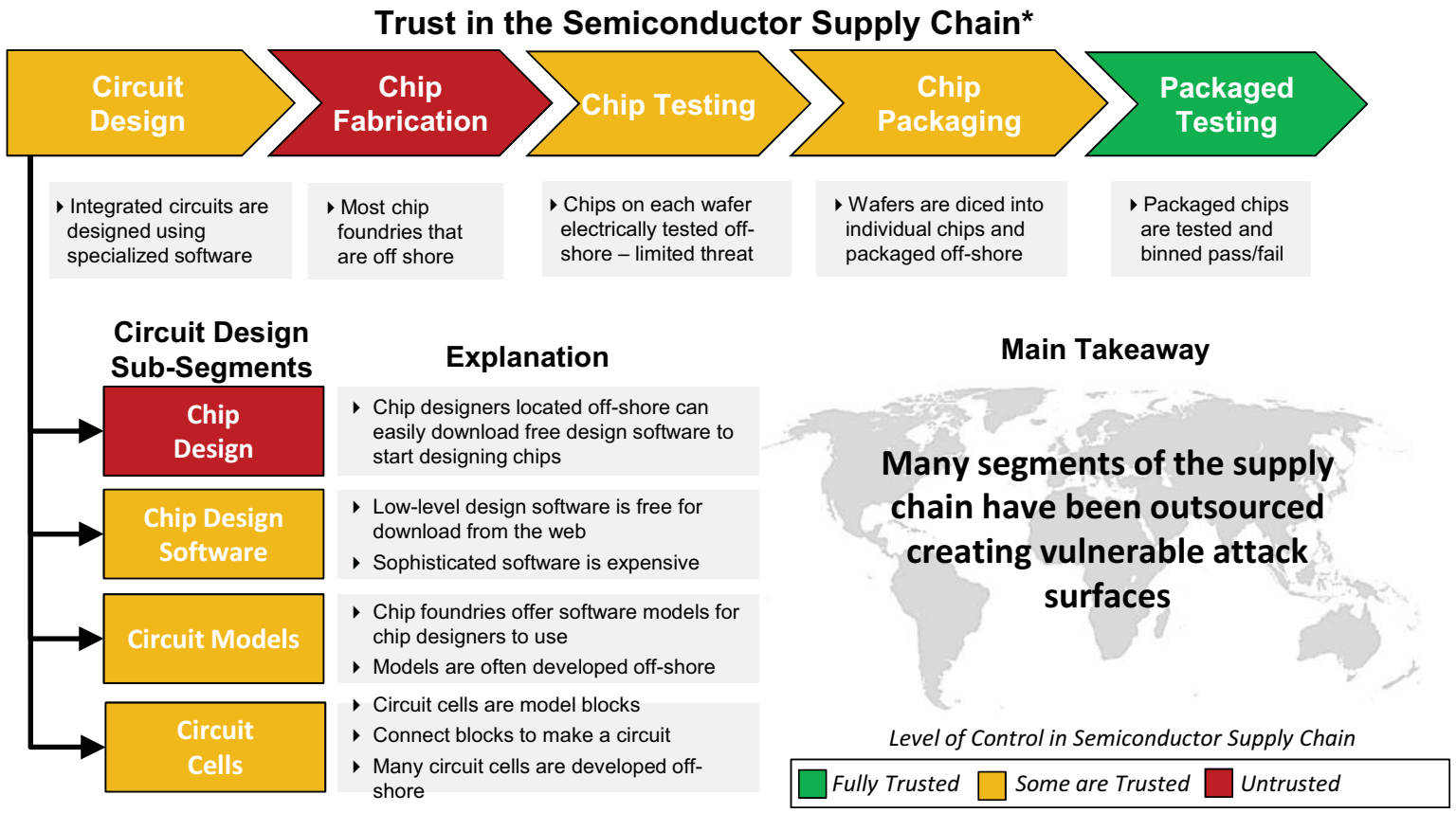


Source: IDC Manufacturing Insights & Booz Allen analysis

Lifecycle shown for a single component
– Component changes hands 15 times before final install

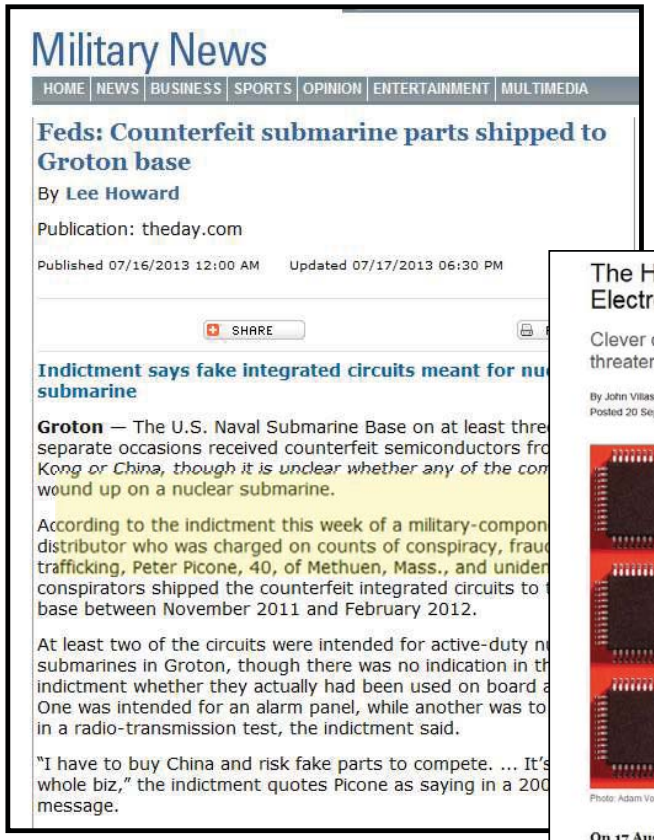
Image: Defense Business Board

OUTSOURCING AND SEGMENTATION HAVE REDUCED THE COSTS OF COTS PARTS, BUT CREATED SECURITY AND TRUST ISSUES



*Source: * S. Leef, Mentor Graphics, Design for Security Conference, March 2014*

SUPPLY CHAIN HAS BEEN A PROBLEM FOR A WHILE



Military News

HOME | NEWS | BUSINESS | SPORTS | OPINION | ENTERTAINMENT | MULTIMEDIA

Feds: Counterfeit submarine parts shipped to Groton base

By Lee Howard

Publication: theday.com

Published 07/16/2013 12:00 AM Updated 07/17/2013 06:30 PM

SHARE

Indictment says fake integrated circuits meant for nu submarine

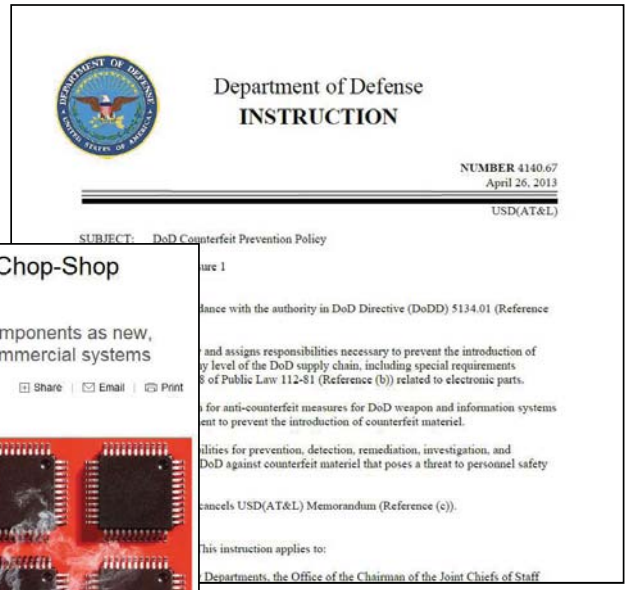
Groton — The U.S. Naval Submarine Base on at least thre separate occasions received counterfeit semiconductors fr Kong or China, though it is unclear whether any of the con wound up on a nuclear submarine.

According to the indictment this week of a military-compon distributor who was charged on counts of conspiracy, frau trafficking, Peter Picone, 40, of Methuen, Mass., and unide conspirators shipped the counterfeit integrated circuits to base between November 2011 and February 2012.

At least two of the circuits were intended for active-duty n submarines in Groton, though there was no indication in t indictment whether they actually had been used on board One was intended for an alarm panel, while another was to in a radio-transmission test, the indictment said.

"I have to buy China and risk fake parts to compete. ... It' whole biz," the indictment quotes Picone as saying in a 20 message.

Distributor indicted for supplying counterfeits to Grumman Electric Boat, July 2013



Department of Defense

INSTRUCTION

NUMBER 4140.67
April 26, 2013
USD(AT&L)

SUBJECT: DoD Counterfeit Prevention Policy

ure 1

dance with the authority in DoD Directive (DoDD) 5134.01 (Reference

and assigns responsibilities necessary to prevent the introduction of
y level of the DoD supply chain, including special requirements
8 of Public Law 112-81 (Reference (b)) related to electronic parts.

for anti-counterfeit measures for DoD weapon and information systems
ent to prevent the introduction of counterfeit materiel.

ilities for prevention, detection, remediation, investigation, and
DoD against counterfeit materiel that poses a threat to personnel safety

ancels USD(AT&L) Memorandum (Reference (c)).

his instruction applies to:

Departments, the Office of the Chairman of the Joint Chiefs of Staff

Dept. of Defense Instruction
NUMBER 4140.67, 26 April 2013

The Hidden Dangers of Chop-Shop Electronics

Clever counterfeiters sell old components as new, threatening both military and commercial systems

By John Villasenor & Mohammad Tehranipoor
Posted 20 Sep 2013 | 4:03 GMT

Share | Email | Print

Photo: Adam Voorhes

On 17 August 2011, Boeing warned the U.S. Navy that an ice-detection module in the P-8A Poseidon, a new reconnaissance aircraft, contained a "reworked part that should not have been put on the airplane originally and should be replaced immediately." In a message marked "Priority: Critical," the company blamed the part, a Xilinx field-programmable gate array (FPGA), for

SPECTRUM Magazine
October, 2013, pp. 41-45

DOD SUPPLY CHAIN THREATS CONTINUE AND BROADEN IN SCOPE

Hardware Backdoors, Trojans


Daily Mail .com

Could a vulnerable computer chip allow hackers to down a Boeing 787? 'Back door' could allow cyber-criminals a way in

- Vulnerability 'hard wired' into chips in aircraft
- Could be impossible to eradicate
- 'Back door' in chips made by Actel

By ROB WAUGH
PUBLISHED: 13:59 EDT, 30 May 2012 | UPDATED: 13:59 EDT, 30 May 2012

A hidden 'back door' in a computer chip could allow cyber-criminals a way to override and control computer systems on Boeing 787s


The Register

Security

Intel ME controller chip has secret kill switch

Researchers find undocumented accommodation for government customers

By Thomas Claburn in San Francisco 29 Aug 2017 at 00:12 80 SHARE

https://www.theregister.co.uk/2017/08/29/intel_management_engine_can_be_disabled/

https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Counterfeit Electronics


Military.com BENEFITS NEWS VETERAN JOBS MILITARY LIFE VIDEOS

DEFENSETECH

Fake Parts are Everywhere

Well, after months of research, Senate Armed Services Committee investigators have discovered "a flood" counterfeit parts in everything from critical navigation software for newly modernized C-5 Galaxy cargo planes to "assemblies" destined for RQ-4 Global Hawk spy planes, submarines and even Stryker Mobile Gun Systems.

https://www.military.com/defensetech/2012/05/22/fake-parats-are-everywhere


SWFL companies accused of importing, selling counterfeit products

Two Southwest Florida companies are accused of importing then selling counterfeit electronic parts according to a lawsuit filed in federal court.

http://www.nbc-2.com/story/38568807/swfl-companies-accused-of-importing-selling-counterfeit-products


FOR IMMEDIATE RELEASE Tuesday, May 1, 2018

Orange County Electronics Distributor Charged with Selling Counterfeit Integrated Circuits with Military and Commercial Uses

LOS ANGELES – The owner of PRB Logics Corporation, an Orange County-based seller of electronic components, was arrested this morning on federal charges alleging he sold counterfeit integrated circuits, some of which could have been used in military applications.

Rogelio Vasquez is charged in a 30-count indictment that alleges he acquired old, used and/or discarded integrated circuits from Chinese suppliers that had been repainted and remarked with counterfeit logos. The devices were further remarked with altered date codes, lot codes or countries of origin to deceive customers and end users into thinking the integrated circuits were new, according to the indictment. Vasquez then sold the counterfeit electronics as new parts made by manufacturers such as Xilinx, Analog Devices and Intel.

https://www.justice.gov/usao-cdca/pr/orange-county-electronics-distributor-charged-selling-counterfeit-integrated-circuits

Hardware Hacking Research, Competitions

black hat DEFCON ZERO DAY INITIATIVE PWN2OWN

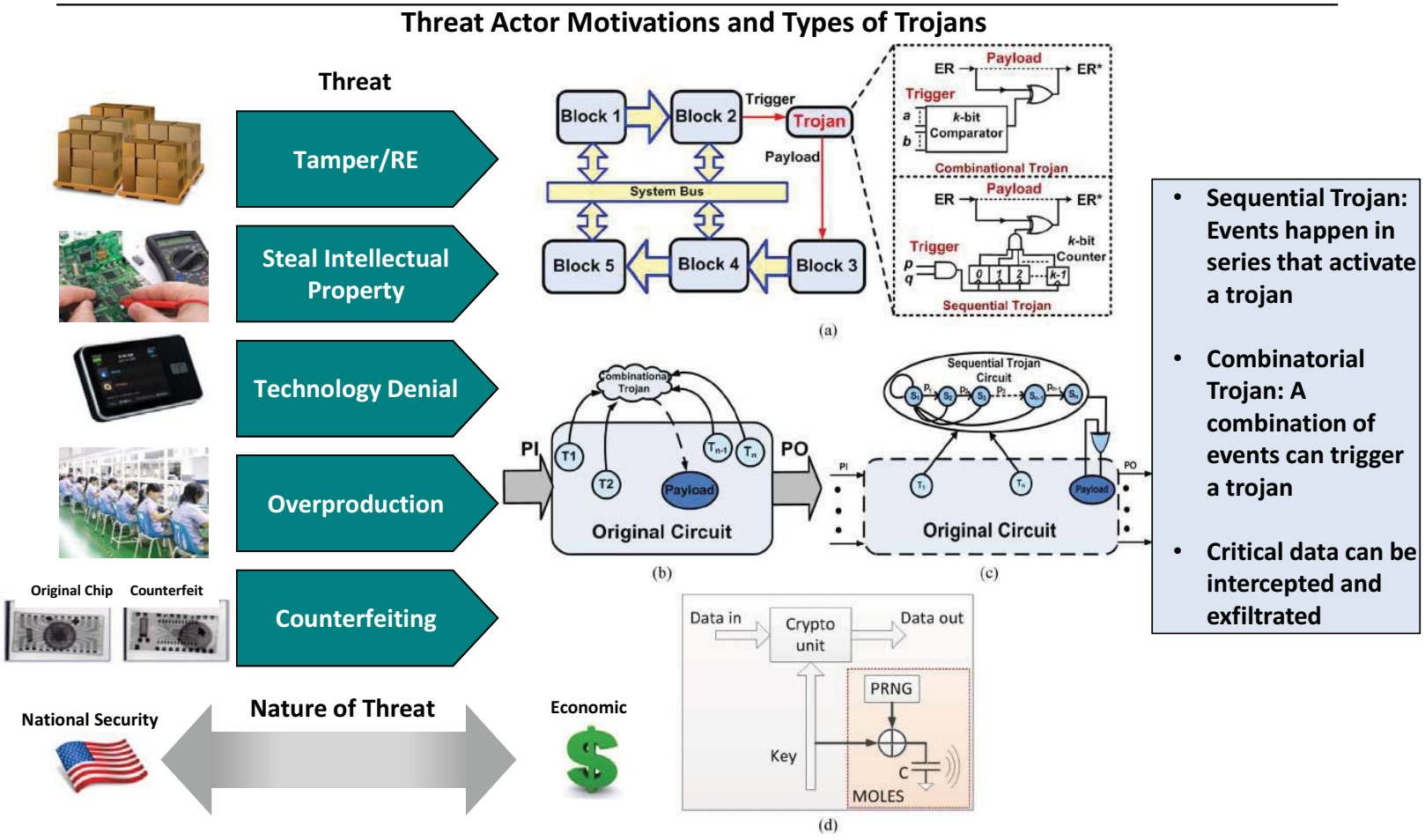
Hackaday.io HOST 2018 HACK THE PENTAGON

Hardware Vulnerabilities & Lists

SPECTRE MELTDOWN FORESHADOW

CAPEC CVE Common Vulnerabilities and Exposures NVD

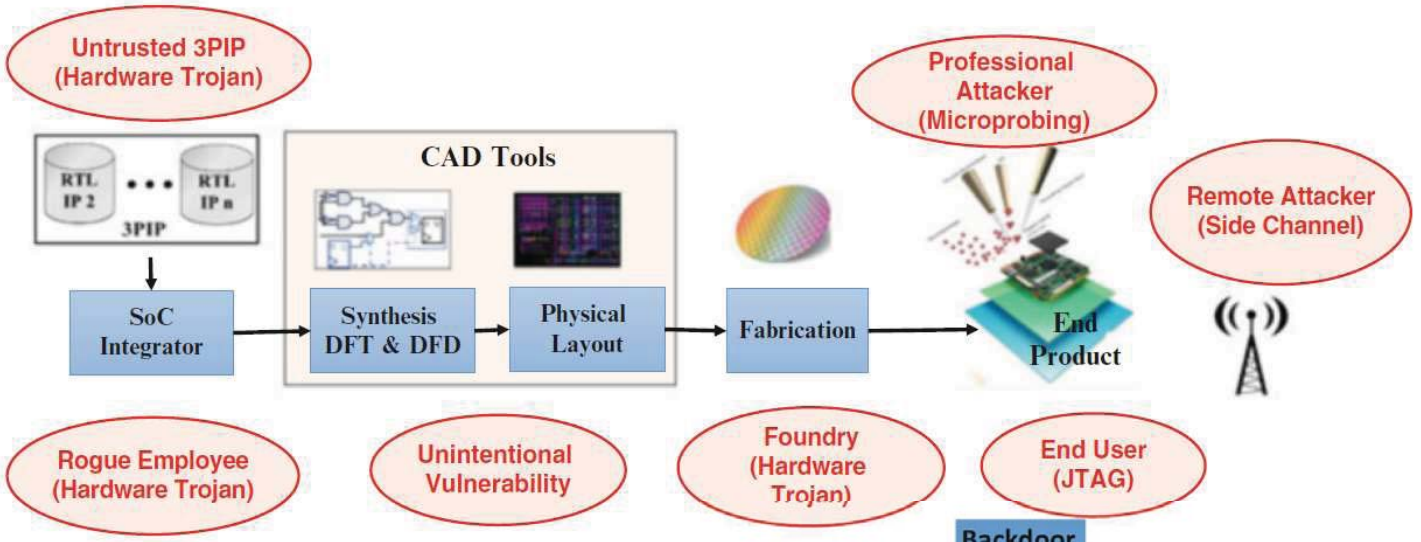
THREAT ACTORS ARE MOTIVATED BY A VARIETY OF REASONS, AND COMPONENTS CAN BE COMPROMISED BY MANY INADVERTENT AND MALICIOUS METHODS



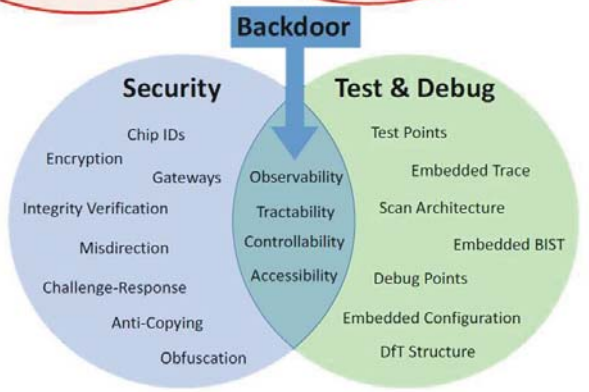
- **Sequential Trojan: Events happen in series that activate a trojan**
- **Combinatorial Trojan: A combination of events can trigger a trojan**
- **Critical data can be intercepted and exfiltrated**

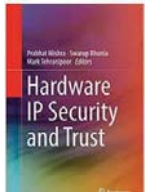
https://www.researchgate.net/figure/Hardware-Trojan-attacks-in-different-forms-a-combinational-and-sequential-Trojans_fig3_264124590

POTENTIAL ADVERSARIES IN DIFFERENT STAGES OF THE SOC DESIGN PROCESS



- Design errors
- CAD tool errors/artifacts
- Design for Test (DFT)
- Design for Debug (DFD)

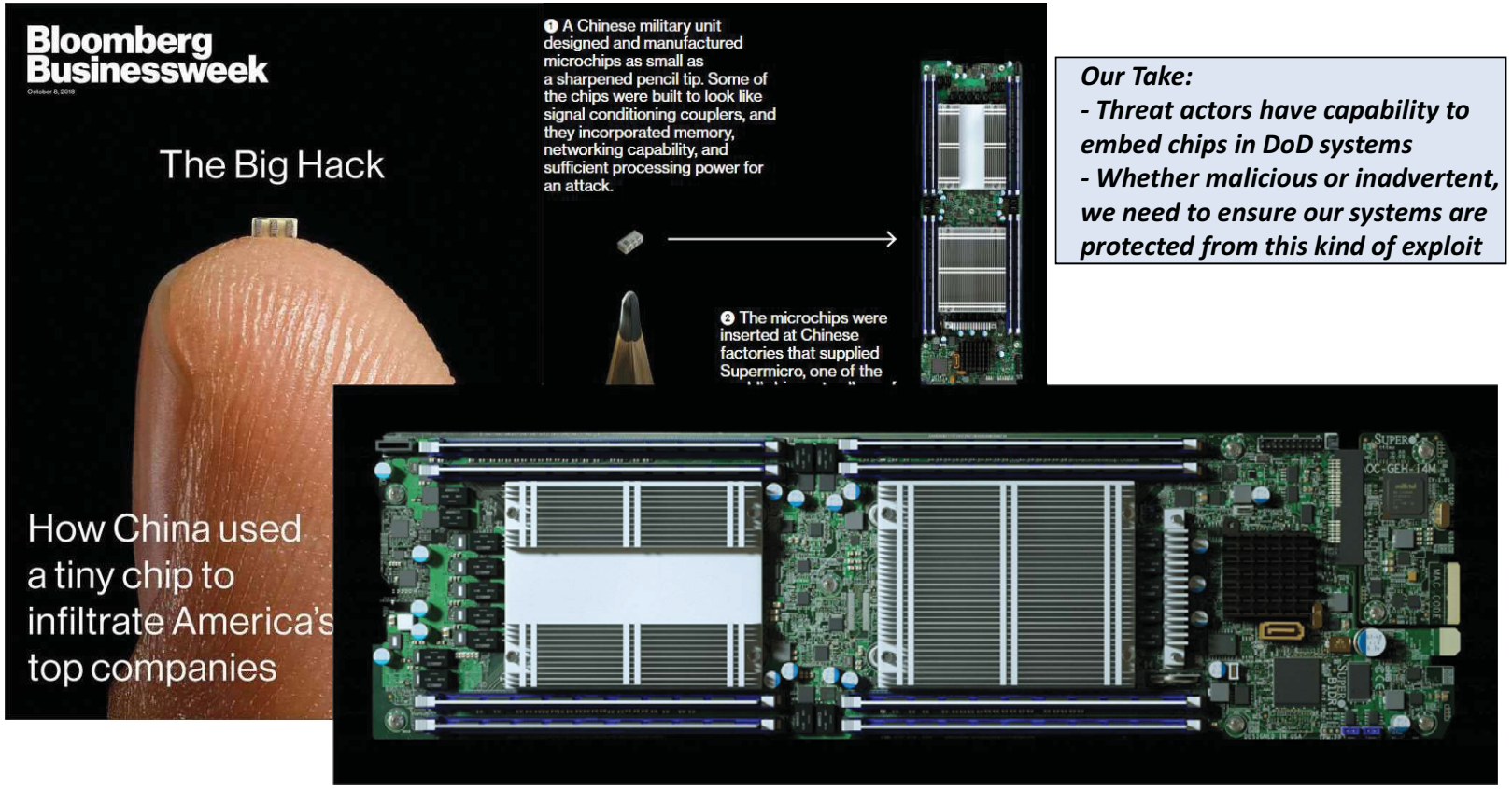




"Hardware IP Security and Trust" edited by Mishra, P., Bhunia, S., Tehranipoor
https://rd.springer.com/book/10.1007/978-3-319-49025-0

RECENT NEWS REPORTS ABOUT "THE BIG HACK" GIVES US FURTHER INSIGHT INTO THREAT ACTOR MOTIVATIONS AND METHODS

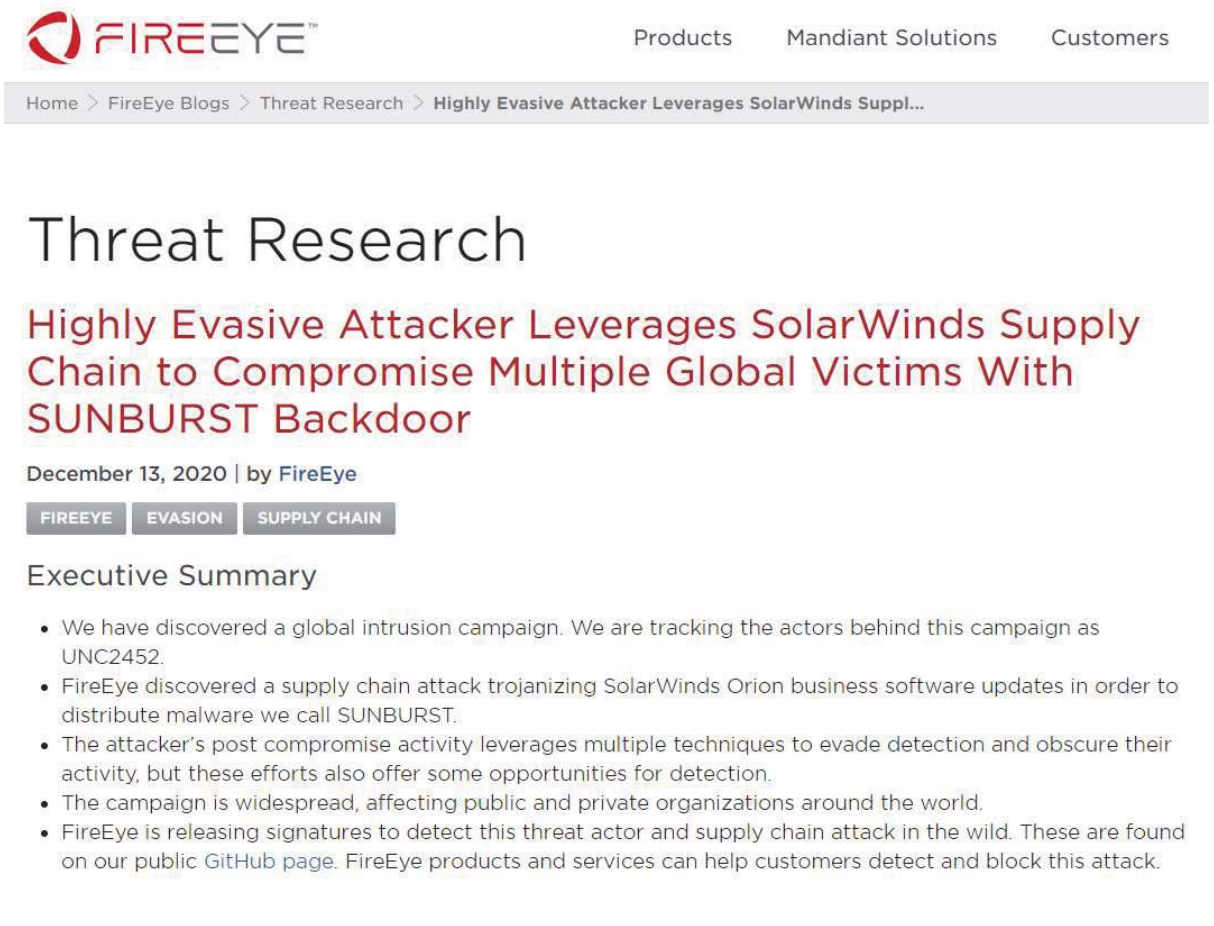
Threat Spotlight : "The Big Hack"



Our Take:
- Threat actors have capability to embed chips in DoD systems
- Whether malicious or inadvertent, we need to ensure our systems are protected from this kind of exploit

https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

RECENT SOLARWINDS SUPPLY CHAIN ATTACK COMPROMISED A MAINTENANCE SERVER TO DISTRIBUTE UNWANTED FUNCTIONALITY INTO A SOFTWARE SUITE



FIREEYE

Products Mandiant Solutions Customers

Home > FireEye Blogs > Threat Research > **Highly Evasive Attacker Leverages SolarWinds Suppl...**

Threat Research

Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor

December 13, 2020 | by FireEye

FIREEYE EVASION SUPPLY CHAIN

Executive Summary

- We have discovered a global intrusion campaign. We are tracking the actors behind this campaign as UNC2452.
- FireEye discovered a supply chain attack trojanizing SolarWinds Orion business software updates in order to distribute malware we call SUNBURST.
- The attacker's post compromise activity leverages multiple techniques to evade detection and obscure their activity, but these efforts also offer some opportunities for detection.
- The campaign is widespread, affecting public and private organizations around the world.
- FireEye is releasing signatures to detect this threat actor and supply chain attack in the wild. These are found on our public GitHub page. FireEye products and services can help customers detect and block this attack.

DOD IS RESPONDING WITH NEW POLICIES & INITIATIVES, INCLUDING ENHANCED SCRM PROCEDURES AND USE OF MICROELECTRONICS SMES IN ASSESSMENTS

DoD Policy Updates and New Initiatives

DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

MAR 1 3 2018

MEMORANDUM FOR SECRETARIES OF MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
CHIEF MANAGEMENT OFFICER
CHIEF, NATIONAL GUARD BUREAU
COMMANDERS OF THE COMBATANT COMMANDS
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF OPERATIONAL TEST AND EVALUATION
CHIEF INFORMATION OFFICER OF THE DEPARMENT DEFENSE
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE AFFAIRS
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS
DIRECTOR OF NET ASSESSMENT
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF DOD FIELD ACTIVITIES

SUBJECT: Enhanced Section 806 Procedures for Supply Chain Risk Management in Support of DoD Trusted Systems and Networks

Our adversaries continue to discover new methods to sabotage, disrupt, or otherwise degrade our systems and extract DoD information. It is critical that DoD components are extra vigilant in managing supply chain risk practices when procuring and integrating information and communications technology (ICT), whether as a product or as a service, into DoD national

Department of Defense
INSTRUCTION

NUMBER 5200.44
November 5, 2012
Incorporating Change 2, July 27, 2017
DoD CIO/USD(AT&L)

SUBJECT: Protection of Mission Critical Functions to Achieve Trusted Systems and Networks

References: See Enclosure 1

1. PURPOSE. This Instruction, in accordance with the authorities in DoD Directive (DoDD) 5134.01 (Reference (a)) and DoDD 5144.02 (Reference (b)):

a. Establishes policy and assigns responsibilities to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or critical components, as defined in this Instruction, by foreign intelligence, terrorists, or other hostile elements.

b. Implements the DoD's TSN strategy, described in the Report on Trusted Defense Systems (Reference (c)) as the Strategy for Systems Assurance and Trustworthiness, through Program Protection and cybersecurity implementation to provide uncompromised weapons and information systems. The TSN strategy integrates robust systems engineering, supply chain risk management (SCRM), security, counterintelligence, intelligence, cybersecurity, hardware and software assurance, and information systems security engineering disciplines to manage risks to system integrity and trust

Department of Defense
Assured Microelectronics Policy

Senate Report 113-85

JULY 2014

Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics

GlobalFoundries to help DMEA with chip fabrication for mission-critical military electronics

March 21, 2017
By John Keller
Editor

McCLELLAN, Calif. – U.S. military microelectronics experts are looking to GlobalFoundries U.S. 2 LLC in Hopewell Junction, N.Y., to continue providing foundry and electronic chip fabrication services for crucial U.S. military electronics systems.

Officials of the Defense Microelectronics Activity

Air Force to kick off trusted computing program to give military access to COTS microelectronics

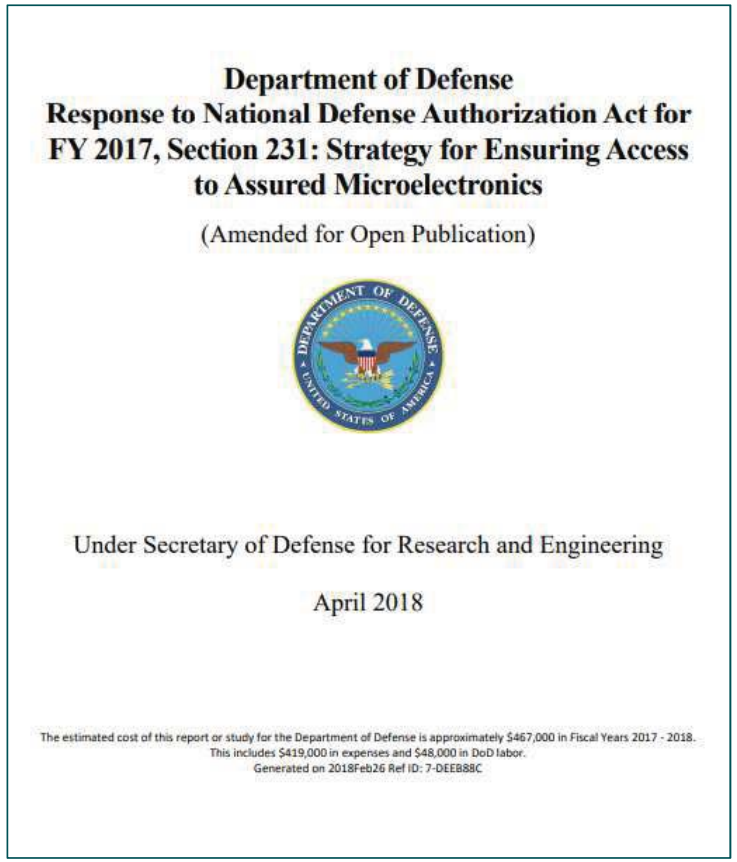
October 20, 2017
By John Keller
Editor

WRIGHT-PATTERSON AFB, Ohio – U.S. Air Force researchers are kicking off a program to develop new trusted computing microelectronics technologies to enable broader use of commercial off-the-shelf (COTS) electronic components in military systems.

Officials of the Air Force Research Laboratory have issued a presolicitation (FA8650-18-S-1201) for the

RECENT DOD NDAA LANGUAGE OUTLINES AN 8 ELEMENT STRATEGY FOR ENSURING ACCESS TO TRUSTED ELECTRONICS

Recent DoD Trusted Electronics Guidance



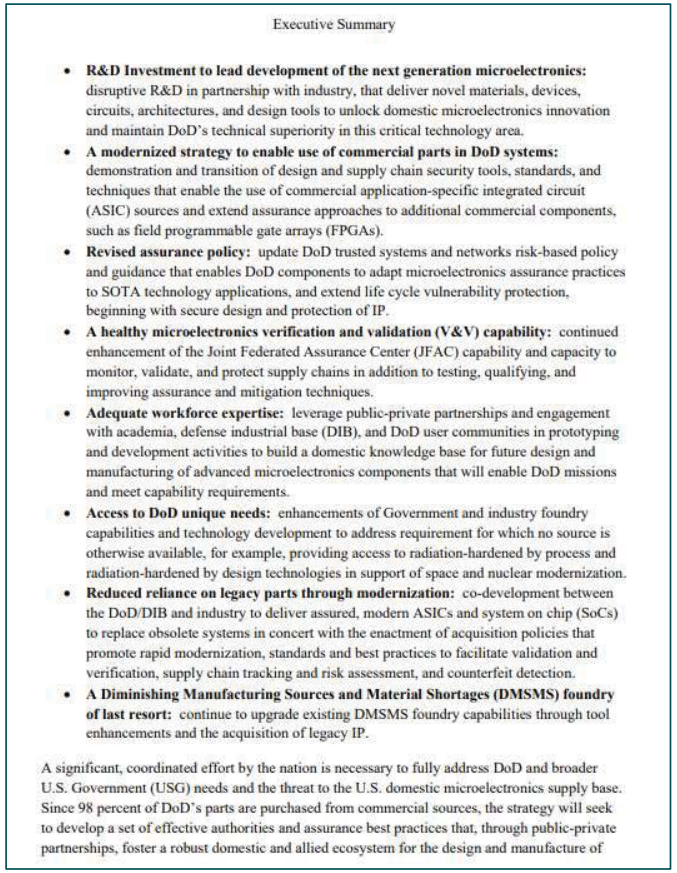
Department of Defense
Response to National Defense Authorization Act for FY 2017, Section 231: Strategy for Ensuring Access to Assured Microelectronics

(Amended for Open Publication)

Under Secretary of Defense for Research and Engineering

April 2018

The estimated cost of this report or study for the Department of Defense is approximately $467,000 in Fiscal Years 2017 - 2018.
This includes $419,000 in expenses and $48,000 in DoD labor.
Generated on 2018Feb26 Ref ID: 7-DEEB88C



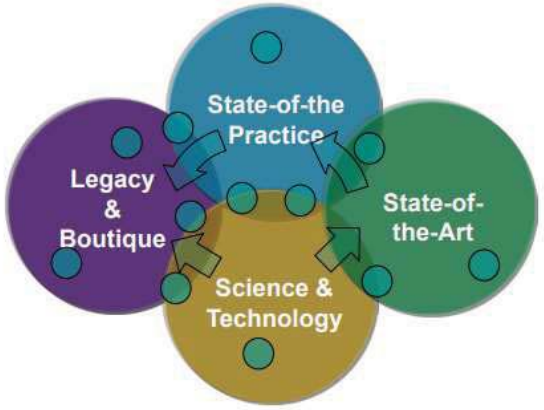
Executive Summary

- **R&D Investment to lead development of the next generation microelectronics:** disruptive R&D in partnership with industry, that deliver novel materials, devices, circuits, architectures, and design tools to unlock domestic microelectronics innovation and maintain DoD's technical superiority in this critical technology area.
- **A modernized strategy to enable use of commercial parts in DoD systems:** demonstration and transition of design and supply chain security tools, standards, and techniques that enable the use of commercial application-specific integrated circuit (ASIC) sources and extend assurance approaches to additional commercial components, such as field programmable gate arrays (FPGAs).
- **Revised assurance policy:** update DoD trusted systems and networks risk-based policy and guidance that enables DoD components to adapt microelectronics assurance practices to SOTA technology applications, and extend life cycle vulnerability protection, beginning with secure design and protection of IP.
- **A healthy microelectronics verification and validation (V&V) capability:** continued enhancement of the Joint Federated Assurance Center (JFAC) capability and capacity to monitor, validate, and protect supply chains in addition to testing, qualifying, and improving assurance and mitigation techniques.
- **Adequate workforce expertise:** leverage public-private partnerships and engagement with academia, defense industrial base (DIB), and DoD user communities in prototyping and development activities to build a domestic knowledge base for future design and manufacturing of advanced microelectronics components that will enable DoD missions and meet capability requirements.
- **Access to DoD unique needs:** enhancements of Government and industry foundry capabilities and technology development to address requirement for which no source is otherwise available, for example, providing access to radiation-hardened by process and radiation-hardened by design technologies in support of space and nuclear modernization.
- **Reduced reliance on legacy parts through modernization:** co-development between the DoD/DIB and industry to deliver assured, modern ASICs and system on chip (SoCs) to replace obsolete systems in concert with the enactment of acquisition policies that promote rapid modernization, standards and best practices to facilitate validation and verification, supply chain tracking and risk assessment, and counterfeit detection.
- **A Diminishing Manufacturing Sources and Material Shortages (DMSMS) foundry of last resort:** continue to upgrade existing DMSMS foundry capabilities through tool enhancements and the acquisition of legacy IP.

A significant, coordinated effort by the nation is necessary to fully address DoD and broader U.S. Government (USG) needs and the threat to the U.S. domestic microelectronics supply base. Since 98 percent of DoD's parts are purchased from commercial sources, the strategy will seek to develop a set of effective authorities and assurance best practices that, through public-private partnerships, foster a robust domestic and allied ecosystem for the design and manufacture of

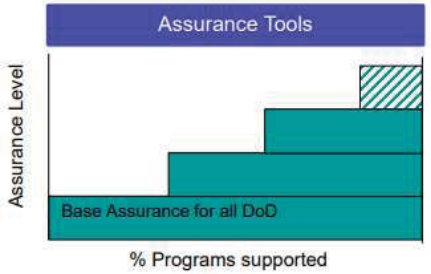
T&AM CHALLENGES INCLUDE AVAILABILITY, ACCESS, AND ASSURANCE OF ASIC, FPGA, AND COTS COMPONENTS

Trusted and Assured Microelectronics (T&AM) Domains and Technical Challenges

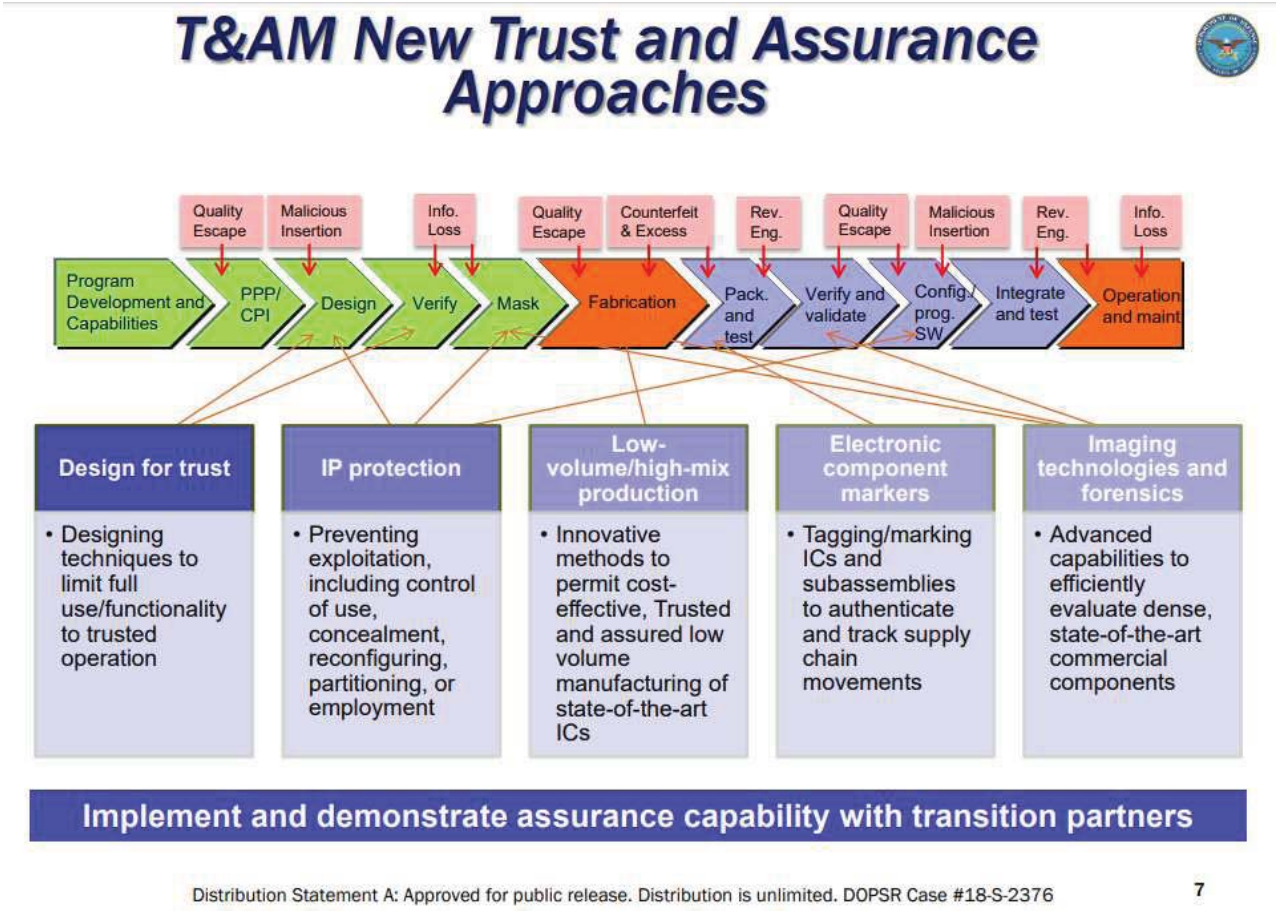


Availability	Access	Assurance
•Assured and expanded supply chain for specialized microelectronics for DoD systems •Increased assurance and expanded supply options for Legacy parts	•Lower barriers to safely access and develop advanced semiconductor-based systems to address new threats •Robust design & validation tool access	•Leverage an assured global supply and partners in U.S. semiconductor industry •Competitive advantage for new markets through enhanced assurance practices

ASIC	FPGA	COTS
•Dense Digital CMOS •RF & Mixed Signal •Compound Semiconductors	•Commercial SoC w/FGPA •Rad-hardened •Low-power	•Microcontrollers •Analog components •PcB assemblies



DOD IS DEVELOPING NEW TRUST AND ASSURANCE APPROACHES IN FIVE MAJOR AREAS



RECENTLY, KEY DOD STAKEHOLDERS ARE CONSIDERING THE IMPLICATIONS OF ZERO TRUST TO THE MICROELECTRONICS SUPPLY CHAIN

Dr. Lisa Porter – Former Deputy Under Secretary of Defense for Research and Engineering
https://www.youtube.com/watch?v=JMgLcEc_a-U

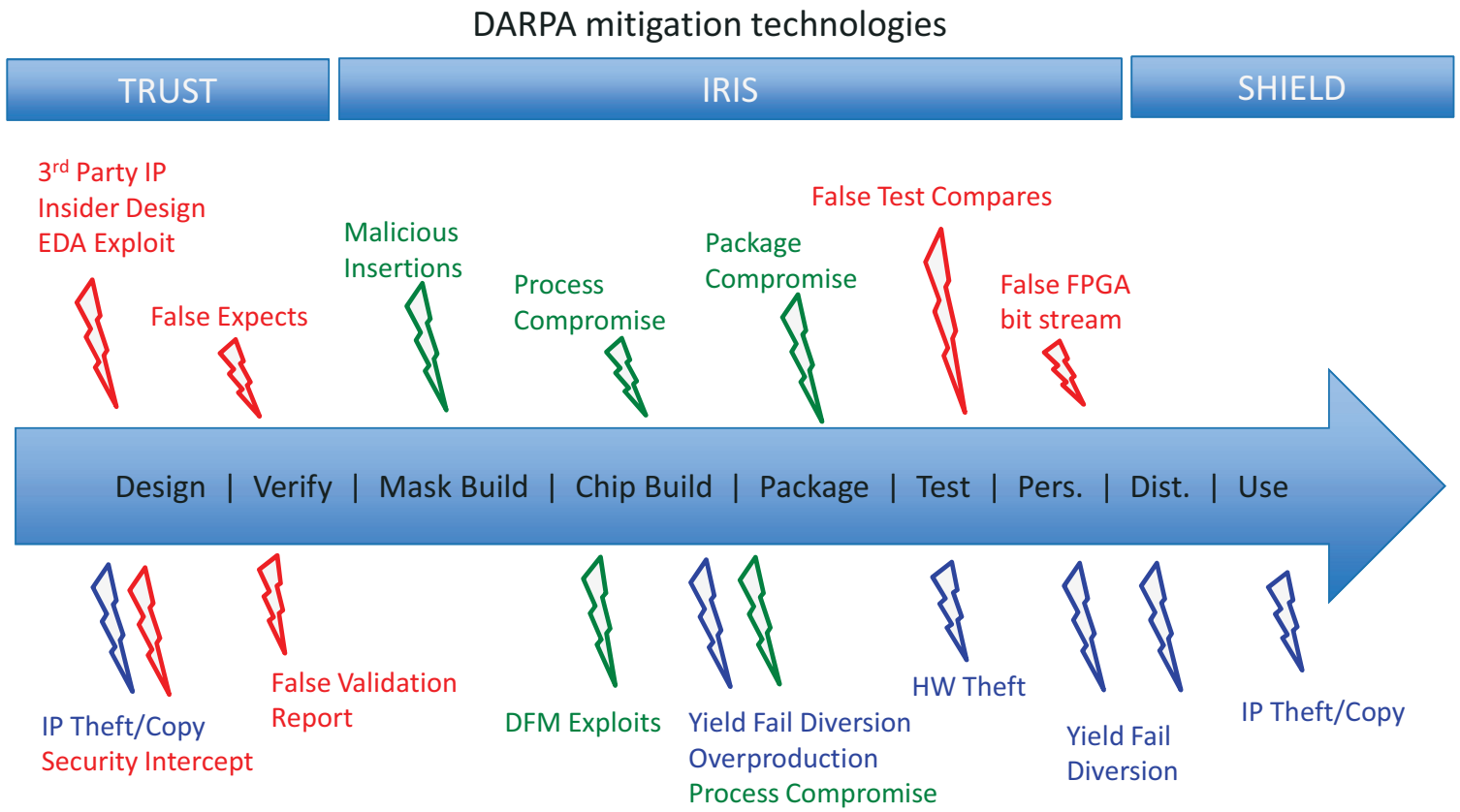
DoD Zero Trust Supply Chain Considerations

"When we consider all of the attack vectors […] throughout our supply chains […] we can fool ourselves into thinking that the best approach to this complex, globally intertwined world is to try to wall ourselves off, to create perfectly secure and isolated systems. Instead, **we must shift our thinking about trust and security**."

"A lot of work lies ahead of us to effectively adopt a holistic, "zero-trust" approach to security in microelectronics - **Data collection and analysis methods must be developed** and applied along the entire lifecycle, in a manner that does not introduce significant throughput impact or prohibitive cost"

"We must develop data-driven security techniques and protocols that are complimentary to advanced commercial design and manufacturing processes so that we can protect our designs and ensure that what we procure functions exactly as intended. **Data—not perimeters —must be the ultimate arbiter of the trust** that we assign to the electronics that we build."

THREATS TO INTEGRATED CIRCUIT INTEGRITY



Sources:https://eri-summit.darpa.mil/docs/20180725_1545_SHIELD.pdft

DID YOU KNOW? BOOZ ALLEN INVENTED THE TERMS SUPPLY CHAIN AND SUPPLY CHAIN MANAGEMENT IN 1980

- According to Supply Chain Digest, "In 1979/1980 a small team of consultants in the Operations Group of Booz Allen & Hamilton in Europe around Mr. **Keith Oliver**, Partner of Booz Allen Hamilton in London, coined the phrases of "Supply Chain" and "Supply Chain Management".
- The project was a Pan-European Supply Chain Strategy plus implementation for the company Landis & Gyr (today integrated into Siemens) in Zug, Switzerland.
- The project was performed in the years 1980 - 1981 and published in the German business magazine "Wirtschaftswoche" in 1982.

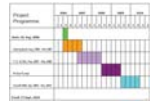
http://www.scdigest.com/assets/newsviews/10-12-16-1.php?cid=4027

CLIENTS FACE DECISIONS ON HOW BEST TO MITIGATE RISK : THE COSTS AND IMPACTS OF EACH MITIGATION SHOULD BE WEIGHED, AND NOT ALL ARE POSSIBLE FOR EACH PART

Drivers of Unreliable and Counterfeit Part Production

- **Old, Obsolete Designs** – as a part becomes obsolete, it disappears from stock, replaced by a another, better-designed part
- **Life Cycle** – not enough inventory to last a military product's entire 30-year lifespan
- **Procurement Process**
  - Purchased from an untrusted source to meet cost & schedule demands
  - Poor traceability / authentication
- **Suspicious Part Sales / Threat Actors** – profit motive and malicious intent can incentivize poor quality assurance and sales practices
- **Gov't Regulations** – Environmental regulations, such as lead-free requirements can drive parts reclamation
- **Quality Assurance** – inadequate test & inspection procedures

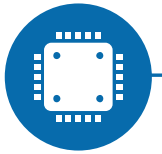
Example Mitigation Actions

Change Suppliers	Identify higher quality components from a different supplier 
Conduct Component Testing	Perform various levels of testing on components to capture issues 
Change Supplier Behaviors	Changing the way suppliers operate in order to enhance security or confidence in lower tiers 
Select Different Parts/Designs	Changing the design of the system to parts that are high assurance and available 
Accept and Monitor Risk	Some risks are acceptable based on the overall system criticality and can be accepted and monitored 

Supply Chain Risk Management approaches need to identify these sources of risk and link them back to the client's desired outcomes: Reliability, Performance, Trust, Security, and Value

WE HAVE CONSOLIDATED A SET OF CAPABILITIES TO SUPPORT MICROELECTRONICS TRUST, ASSURANCE, TECHNOLOGY PROTECTION, AND SCRM NEEDS

Booz Allen T&AM Cross-Market Capabilities



MICROELECTRONICS TRUST, ASSURANCE, AND SECURE DESIGN

- Assess the microelectronics technology and design for Trust, Integrity, and vulnerability to exploitation
- Analyze, simulate, emulate, and apply techniques to verify performance, identify weaknesses, and implement security features

TECHNOLOGY PROTECTION

- Research next generation techniques and approaches, quantify the potential for success and protection of critical program information
- Develop enabling technologies to meet next generation mission demands, create prototype demonstrations and assess performance

MICROELECTRONICS SUPPLY CHAIN RISK MANAGEMENT

- Understand the complex microelectronics supply chain and assess vulnerabilities of suppliers and the underlying technologies
- Characterize threat landscape, identify and quantify risks to systems, determine mitigation strategies, implement protection measures, monitor effectiveness

POCs

Doug Palmer	palmer_doug@bah.com
Saverio Fazzari	fazzari_saverio@bah.com

Thank you sponsors!

Amkor's Differentiators

Technology

Advanced Packaging Leadership
Engineering Services
Broad Portfolio

Quality

QualityFIRST Culture
Execution
Automation

Service

Design & Test Through Drop Ship
Manufacturing Footprint
Local Sales & Support

Global Companies Rate Advantest THE BEST ATE Company 2020

Advantest receives highest ratings from customers in annual VLSIresearch Customer Satisfaction Survey.

Advantest received an overall score of 9.5 out of 10, with highest ratings in categories of:

Technical Leadership – Partnership – Uptime – Commitment – Trust in Supplier – Quality of Results – Product Performance – Recommended Supplier

"Year-after-year the company has delivered on its promise of technological excellence and it remains clear that Advantest keeps their customers' successes central to their strategy. Congratulations on celebrating 32 years of recognition for outstanding customer satisfaction."

— **Risto Puhakka**, President VLSIresearch

Technical Program Committee (TPC)

Ivor Barber
Advanced Micro Devices

Jeff Demmin
Keysight Technologies

Ira Feldman
Feldman Engineering

MEPTEC
THE NEXT GENERATION

Virtual Event Schedule

Join us for two online sessions

Wednesday	April 28, 2021	8:00 - 11:00 am PDT
Thursday	April 29, 2021	8:00 - 11:00 am PDT

Your personal Zoom link is the same for both days.
Zoom will send you a reminder before the start of each session.

MEPTEC
THE NEXT GENERATION

Speakers April 28

Saverio Fazzari
Booz Allen Hamilton

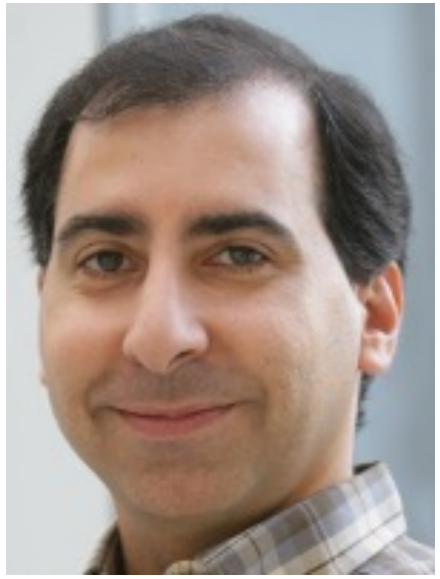
Supply Chain Challenges for Defense Systems

Sridhar Swamy & Akash Malhotra
Advanced Micro Devices

Securing Supply Chain

Nader Sehatbakhsh
University of California Los Angeles (UCLA)

Hardware and Supply Chain Security in the era of Advanced Heterogenous Integration

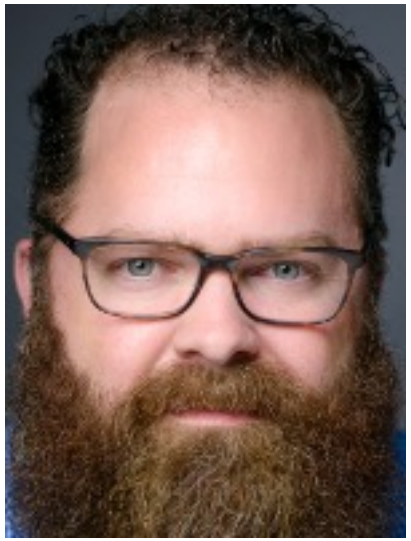


Michael Azarian
University of Maryland

Hardware Trojans and Counterfeit Microelectronics: Detection and Diagnosis

MEPTEC
THE NEXT GENERATION

Speakers April 29



Matthew Areno
Intel
Identifying Supply Chain Threats – An Honest Assessment

Ajay Sattu
Amkor Technology, Inc.
Automotive Semiconductor Unit Level Traceability

Navid Asadi
University of Florida
Physical Assurance and Inspection of Electronics

MEPTEC
THE NEXT GENERATION

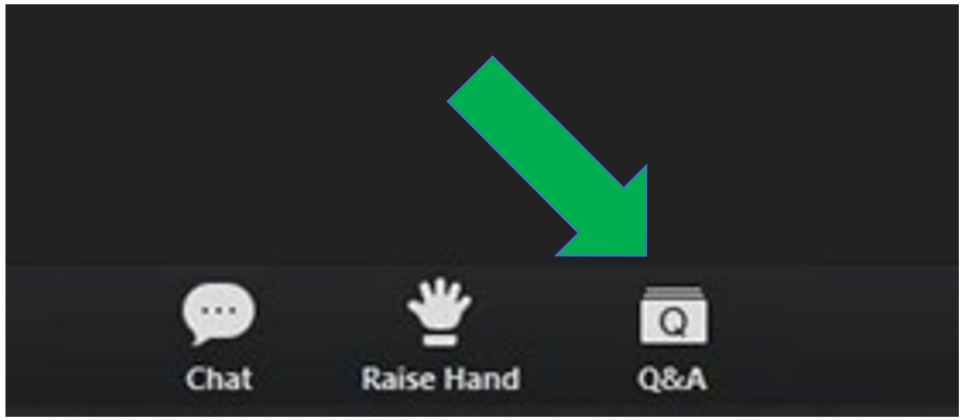
Reminders

Slides & Videos will be posted next week

http://events.meptec.org/supply-chain-security-2021 /

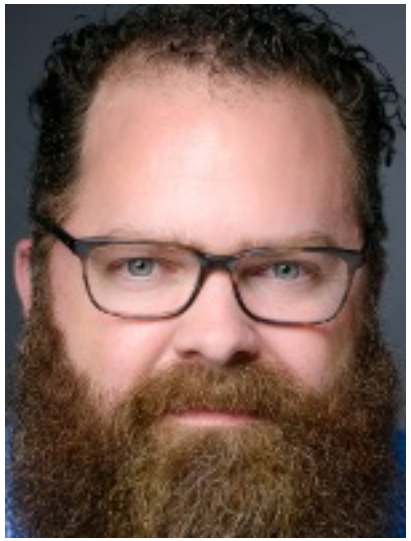
youtube.com/MEPTECpresents

Please use the Q&A window for your questions



MEPTEC
THE NEXT GENERATION

Speakers April 29



Matthew Areno
Intel
Identifying Supply Chain Threats – An Honest Assessment

Ajay Sattu
Amkor Technology, Inc.
Automotive Semiconductor Unit Level Traceability

Navid Asadi
University of Florida
Physical Assurance and Inspection of Electronics

MEPTEC
THE NEXT GENERATION

Virtual Event Schedule

Join us for two online sessions

Wednesday	April 28, 2021	8:00 - 11:00 am PDT
Thursday	April 29, 2021	8:00 - 11:00 am PDT

Your personal Zoom link is the same for both days.
Zoom will send you a reminder before the start of each session.

MEPTEC
THE NEXT GENERATION

Thank you sponsors!

Amkor's Differentiators

Technology

Advanced Packaging Leadership
Engineering Services
Broad Portfolio

Quality

QualityFIRST Culture
Execution
Automation

Service

Design & Test Through Drop Ship
Manufacturing Footprint
Local Sales & Support

Global Companies Rate Advantest THE BEST ATE Company 2020

Advantest receives highest ratings from customers in annual VLSIresearch Customer Satisfaction Survey.

Advantest received an overall score of 9.5 out of 10, with highest ratings in categories of:

Technical Leadership – Partnership – Uptime – Commitment – Trust in Supplier – Quality of Results – Product Performance – Recommended Supplier

"Year-after-year the company has delivered on its promise of technological excellence and it remains clear that Advantest keeps their customers' successes central to their strategy. Congratulations on celebrating 32 years of recognition for outstanding customer satisfaction."

— **Risto Puhakka**, President VLSIresearch

COPYRIGHT NOTICE

The content of this presentation is the work and opinion of the author(s) and is reproduced here as presented at the **Supply Chain Security Workshop** (April 28 & 29, 2021).

MEPTEC
THE NEXT GENERATION

www.meptec.org

COPYRIGHT NOTICE

www.meptec.org

MEPTEC
THE NEXT GENERATION