Supply Chain Security Workshop

April 28 & 29, 2021

MEPTEC
THE NEXT GENERATION

www.meptec.org

Hardware Trojans and Counterfeit Microelectronics: Detection and Diagnosis

Michael H. Azarian, Ph.D.
Center for Advanced Life Cycle Engineering (CALCE)
University of Maryland
College Park, MD 20742 USA

April 28-29, 2021
MEPTEC Supply Chain Security 2021

Outline

- Nature of Threat: Tampered Devices, Clones, Hardware Trojans
- Challenges for Detection and Diagnosis
- Standards-Based Detection Methods: SAE AS6171
- Second Order Effect/Side Channel Methods
- CALCE Deep Learning-Based Method
- Future Directions

Counterfeit Part Types

- Counterfeit Electrical, Electronic, or Electromechanical (EEE) parts may be reclaimed from e-waste, product overruns, modified authentic parts, or copies.
- **Tampered:** modified for sabotage or malfunction
- Note: Tampered parts are not addressed in the current release of SAE AS6171, but will be included in future releases

Recycled
Remarked
Overproduced
Out-of-spec/Defective
Forged Documentation
Cloned
Tampered

As described in SAE AS6171[1]

[1]SAE AS6171, "Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts," 2016.

Tampered Parts

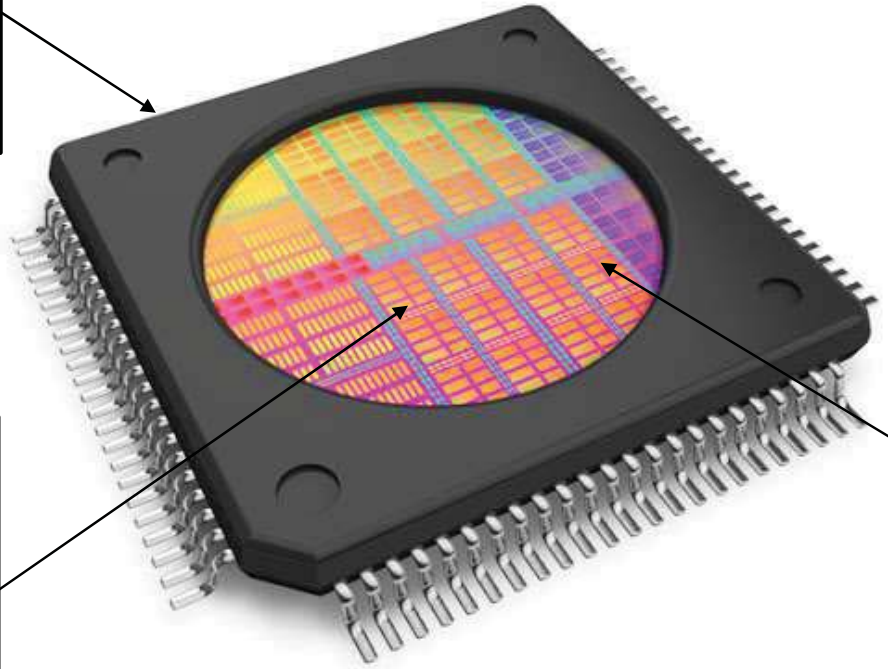
- Tampered parts are a category of counterfeit part which has been deliberately altered to perform a surreptitious function or to deviate from its expected performance.
  - Include *Hardware Trojans*
  - May be in the form of a Clone or an otherwise authentic part
- The behavioral change may be programmed to occur upon some internal or external trigger condition, after a fixed time or amount of usage, or based upon the condition of the part.
- Possible effects:
  - Change of functionality, potentially allowing targeted sabotage or defeat of security measures
  - Accelerated aging or failure, or
  - Unauthorized signal transmission or information leakage.

Hardware Trojans: Challenges and Threats

- Vulnerabilities can be introduced at various stages of development (e.g., register-transfer level (RTL), netlist, layout);
  - can be as subtle as modified dopant levels or thinned interconnects
- Can be introduced anywhere within supply chain:
  - 3rd party IP provider, system-on-chip integrator, foundry, distribution
- Must be able to pass all the usual manufacturing tests
  - Typical functional testing, fault testing, and superficial structural analysis often not sufficient
- Cloned devices require substantial resources to be effective
  - e.g., Nation-state engaged in cyber-warfare

Hardware Attacks

Cloned packaging could disguise a questionable chip as a legitimate one.

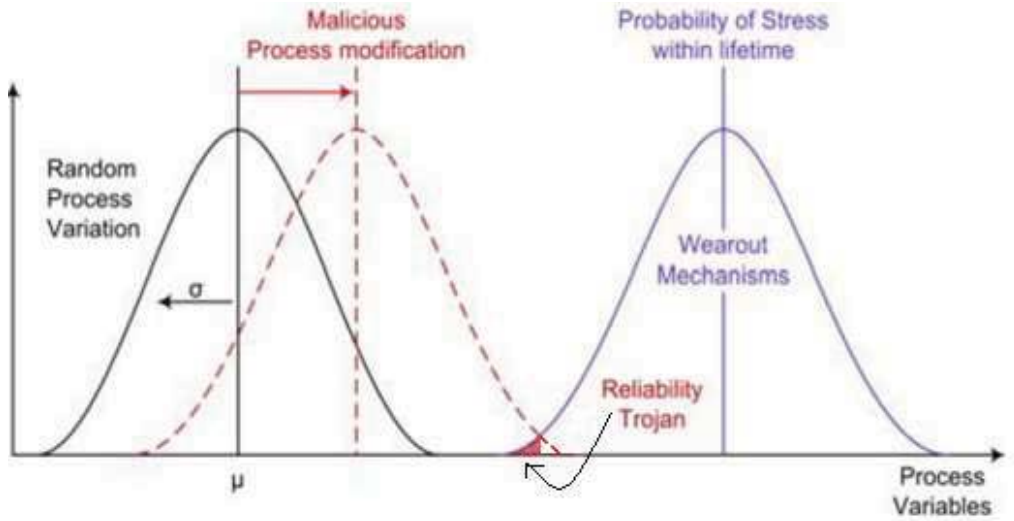


Adding extra transistors during design or fabrication could serve as a kill switch or trapdoor

During the layout process, new circuit traces and wiring can be added to the circuit. They can be used to create an additional output.

Process Reliability Trojans

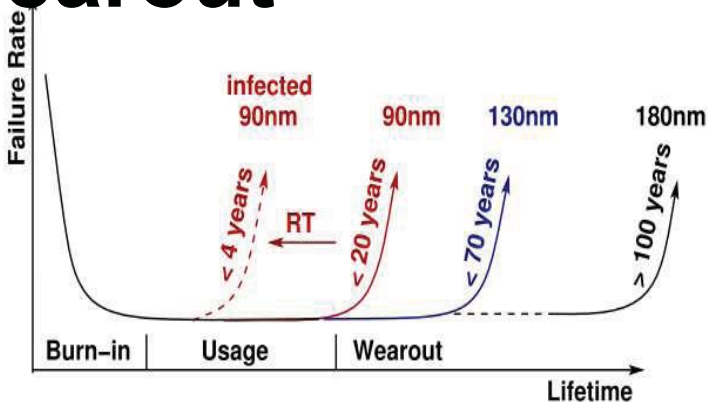
- Circuit manufacturers optimize their processes to ensure that wearout mechanisms occur beyond the useful lifetime of a device.
- Process reliability trojans (PRTs) are a type of hardware trojan that can be inserted by modifying process fabrication parameters like gate oxide thickness, purity and quality, nitrogen concentration near Si/SiO2 interface, etc.
- PRTs are extremely difficult to detect as they have no trigger and their only payload is accelerated aging.
- PRTs will raise the probability of the devices having a reduced lifetime by accelerating aging mechanisms.[1]



[1]Y. Shiyanovskii, F. Wolff, A. Rajendran, C. Papachristou, D. Weyer and W. Clay, "Process Reliability Based Trojans through NBTI and HCI Effects."

PRTs: Early Wearout

Even without knowledge of the circuit design, a subtle but malicious change to a process parameter can result in components with higher probability of failure.[1]



Mechanism	Lifetime Model	Failures	Parameters
Negative bias temperature instability (NBTI)	$\Delta Vth = \mathrm{A}\exp(\beta V_g)\exp\left(-\frac{E}{kT}\right)t^n$ ΔVth: Threshold voltage shift E: Activation energy, Vg: Gate voltage n: measured stress time exponent (0.15- 0.25) β: Measured gate sensitivity A: Function of process technology	• Switching time delay • Non-responsive device	• Nitrogen concentration near Si/SiO2 interface, • Gate dimensions • Gate oxide thickness
Hot Carrier Injection (HCI)	$\mathrm{t} = \mathrm{A}.\mathrm{e}\left(-\frac{E}{kT}\right).\left(\frac{I_{sub}}{W}\right)^{-n}$ I_{sub}: Substrate current W: Width of the CMOS device		• Drain doping levels • Channel lengths • Gate oxide thickness • Purity and quality of gate oxide

[1]Y. Shiyanovskii, F. Wolff, A. Rajendran, C. Papachristou, D. Weyer and W. Clay, "Exploiting Semiconductor Properties for Hardware Trojans"

Zero-Trust Architecture: A Model for the Future

- Push to transition from trusted foundries towards operation and development in zero-trust environments.
- Zero-Trust Architecture aims for information and network security that prevents data breaches by removing the notion of trust.[1]
- Instead of giving users complete access to the network, a zero-trust approach compartmentalizes data on a need-to-know basis that requires additional levels of authentication, such as onetime access codes for a user to access more sensitive data.
- To address hardware security, the Zero-Trust framework needs to be extended and modified to prevent infected hardware (e.g., tampered devices) from making it into field usage.

[1] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST, 2019, doi: https://doi.org/10.6028/NIST.SP.800-207-draft.

Two Approaches to Counterfeit Detection

- With access to an exemplar (golden, or known authentic part)
  - Direct comparison of layout, materials, functionality, 2nd order effects
- In the absence of an exemplar; strategies include:
  - Comparison to known IP (e.g., design, layout, materials, functional specifications) of device or netlist recovered through design recovery (reverse engineering)
  - Consistency within a lot
  - Existence of vulnerabilities, including side channels, especially in a side channel-resistant device

SAE AS6171 – Test Methods Standard

Test Methods Standard; General Requirements, Suspect/Counterfeit Electrical, Electronic, and Electromechanical Parts

Purpose	• Standardizes practices to detect Suspect/Counterfeit (SC) Electrical, Electronic, and Electromechanical (EEE) parts and to ensure consistency of test techniques and requirements across the supply chain. • *AS6171 is a workmanship standard*
Target Audience	• Independent Test Laboratories • Distributors & OEMs (with in-house testing capability) • OEMs, Integrators, and End-Users flowing down test requirements
Uses	• Test Methods for counterfeit detection (separate slash sheets: AS6171/1 – 11) • Serves as basis for accreditation of test laboratories for counterfeit testing • Requirements apply exclusively to test laboratories • Implements a risk-based approach to counterfeit part detection, and is unique among standards in doing this.
Status	• **Published by SAE (October 2016), with recent updates to some documents** • **Ongoing development of new and revised test methods.**

Standardization of a Risk-Based Methodology for Counterfeit Part Detection

- **DFARS[1] calls for risk-based policies and procedures**
- **DoD Instruction 4140.67[2] explains risk-based testing:**

  "anti-counterfeiting measures are required to **balance the risk** represented by counterfeit goods **against the impact to readiness and cost** of the measures."

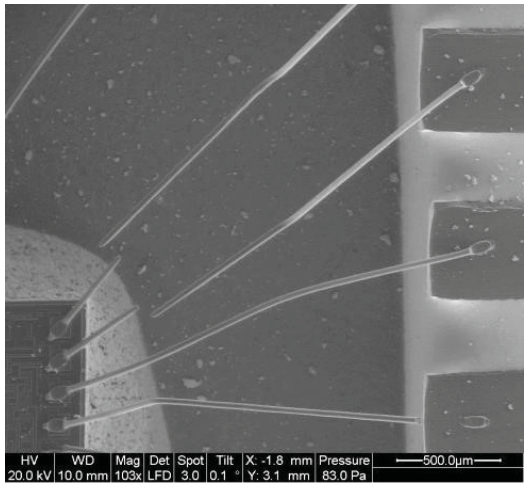
- **SAE G-19A Test Laboratory Standards Development Committee:**

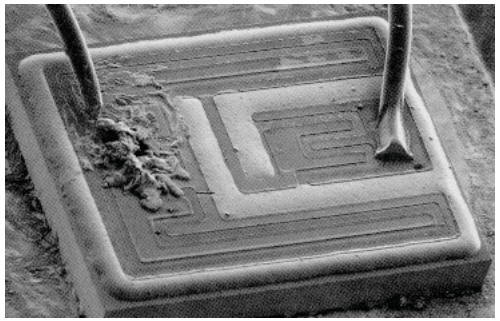
  Chartered in 2010 by SAE's Aerospace Council to **standardize risk based practices to detect suspect counterfeit components** and to ensure consistency across the supply-chain for test techniques and requirements

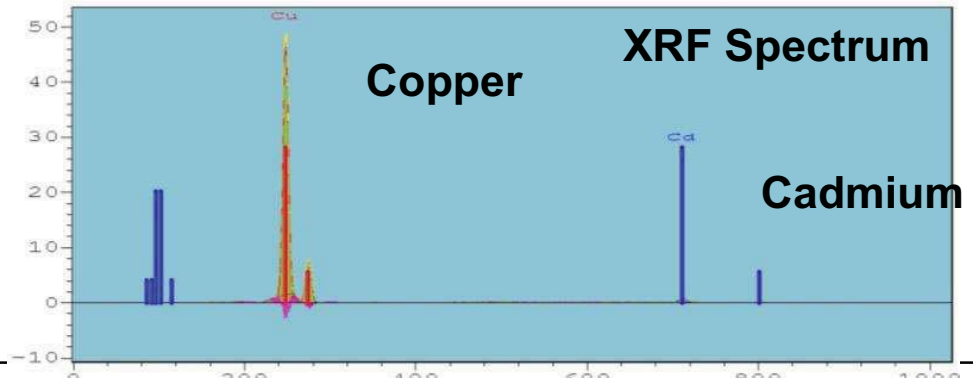
[1] Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.246-7007, Contractor Counterfeit Electronic Part Detection and Avoidance System (issued August 30, 2016).
[2] DoD Instruction 4140.67, "DoD Counterfeit Prevention Policy," Enclosure 2, section 8d, Apr. 26, 2013.

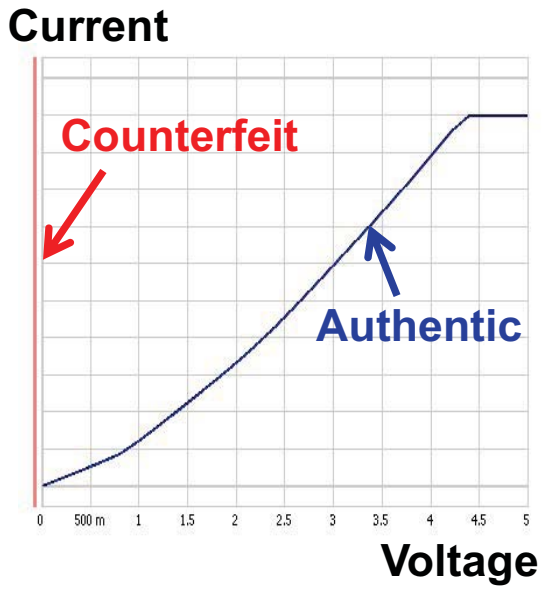
Counterfeit Defects

- **Counterfeit Defects** are indicators of potential counterfeiting.
- They include such features as damaged terminations, ghost markings, missing or broken bond wires, incorrect materials, and out-of-specification electrical parameters.









Defects Taxonomy for Tampered Parts: Proposed in SAE G19A Committee

T1 Unintended Communication

T2 Unexpected or Altered Netlist

T3 Exploitable Test Feature

T4 Unexpected Test Sequence Outcome

T5 Die Level Hardware Modification

T6 Unexpected Software Function and/or Performance

T7 Unexpected Software Code

T8 Unexpected Firmware Operation

T9 Unexpected Security Vulnerability

T10 Unexpected Emission or Signature

Unexpected Emissions (T10)

Examples of emissions or signatures include but are not limited to:

1. Electromagnetic Radiation
2. Conducted Radio Waves Frequency
3. Magnetic Characteristics
4. Power Behavior
5. Thermal Profile

- These are the basis for side channel attacks, and for detection methods using side channels (“second order effects”)

Existing AS6171 Test Methods

First Line of Defense: evidence of tampering, plus reliability

- **AS6171/2: External Visual Inspection** (EVI) (incl. *remarking, resurfacing*)
- **AS6171/7: Electrical Test**: *Functional Tests*; *ambient or over temperature (incl. environmental, burn-in, seal*)

Non-destructive: structural and material composition

- **AS6171/5: Radiological Inspection** (RI)
- **AS6171/6: Acoustic Microscopy** (AM)
- **AS6171/3: X-Ray Fluorescence** (XRF)

Destructive: structural; further materials analysis; functional recovery

- **AS6171/4: Delid/Decapsulation Physical Analysis** (DDPA)
- **AS6171/11: Design Recovery** (DR): device layout and function

Materials Analysis: evidence of tampering, clones

- **AS6171/8: Raman Spectroscopy**
- **AS6171/9: Fourier Transform Infrared Spectroscopy** (FTIR)
- **AS6171/10: Thermogravimetric Analysis** (TGA)

Test Methods for Tampered Parts

- The SAE G-19A committee has a sub-group dedicated to development of test methods for tampered parts.
- Two methods that are currently under development include:
  - Netlist Assurance
  - Digital Content Assurance (proposed)
- Design Recovery (AS6171/11) is undergoing revision for improved applicability to this part type
- Existing AS6171 test methods
- Other methods for detection include those based on second order effects; e.g., involving emissions or power consumption

Netlist Assurance (AS6171/16 proposed)

- Examines hardware netlists recovered from physical components
- Assesses an implemented digital design netlist in a microcircuit for undesired device behavior
- Four approaches:
  - Information Flow Analysis using Static Property Checking
  - Boolean Functional Analysis for Finding Stealthy Circuits
  - Logic Equivalence Checking
  - Intelligent and Known Pattern Detection

Design Recovery (AS6171/11)

- A destructive process used to obtain design information directly from a microcircuit.
  - Does the recovered design information match the intended function or physical layout of a known “good” or “control” sample or the original design?
- Based on analysis of the physical layout of the circuit.
  - Examples of physical defects which are indicators of a possible counterfeit device for which design recovery is particularly well suited include: wrong die, missing and/or misaligned contact window, parasitic transistors, cracks and other imperfections in a die or passivation layer, electromigration, etc..
- Circuits with the same functional behavior may have different physical design and therefore may not be counterfeit
  - revised design, newer technology or different implementations of the same functional behavior from different manufacturers.

Second Order (Side Channel) Methods

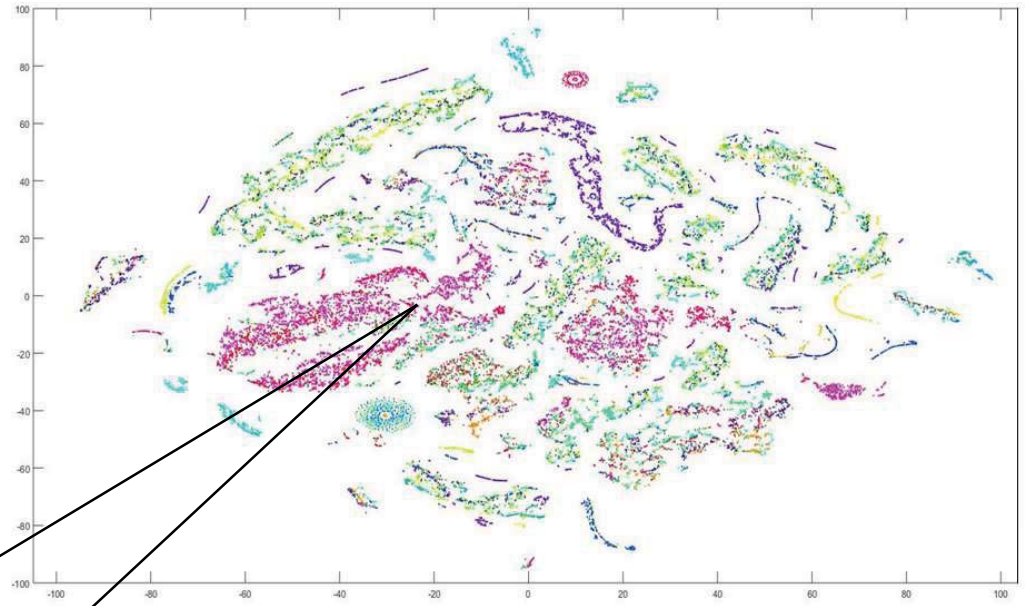
- Can be based on power consumption analysis
  - Can be static or dynamic
  - Simple or differential
  - May employ machine learning for anomaly detection or comparative analysis
  - Examples:
    - Barricade (Battelle)
    - Power Fingerprinting (PFP Cybersecurity)
    - Power spectrum analysis (Sandia National Labs)
    - SICADA (MIT-Lincoln Laboratories)
- Can also use electromagnetic radiation
  - e.g., ADEC (Nokomis)

PRT Detection and Diagnosis

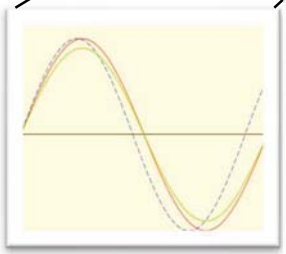
- Even advanced methods such as design recovery, netlist assurance, and side channel analysis are rarely effective against PRTs because
  - The extent of process variation required for accelerated aging can be subtle and hidden deep within the device
  - Process deviations may be due to incidental quality control issues, or due to malicious modifications to the fabrication process with the intent of doing harm during in-field operation.
  - Malicious modifications may produce circuits meeting their performance specifications, particularly since designers spend extraordinary effort to de-sensitize the circuit performance with respect to process variations.
- Real-time monitoring can be effective, but challenging: e.g. aging sensors, like ring oscillators (RO).[1]
  - RO can detect threshold voltage changes but different transistors in the circuit age at different rates, hence, multiple aging sensors will be needed to detect overall aging.
- CALCE has developed a deep learning-based approach for diagnosis of PRTs
  - Similar to concept of digital twin
  - Does not require extensive network of embedded sensors
  - Can be used for detection, diagnosis, and prognosis: Prognostics and Security Health Monitoring (PSHM)

[1]D. Sengupta and S. Sapatnekar, "Estimating Circuit Aging Due to BTI and HCI Using Ring-Oscillator-Based Sensors," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 36,

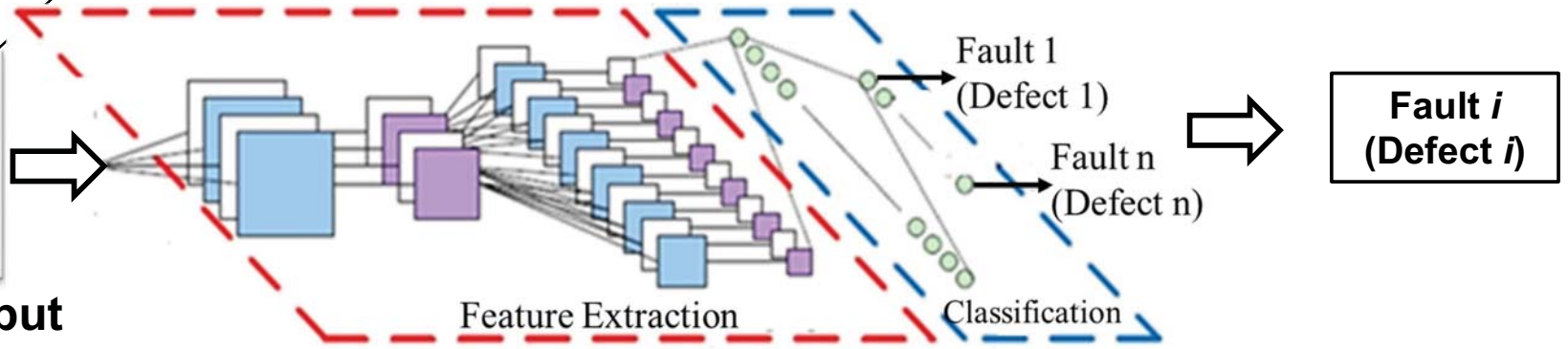
CALCE PSHM Method: Fault Diagnosis



Training Data 2D t-SNE representation



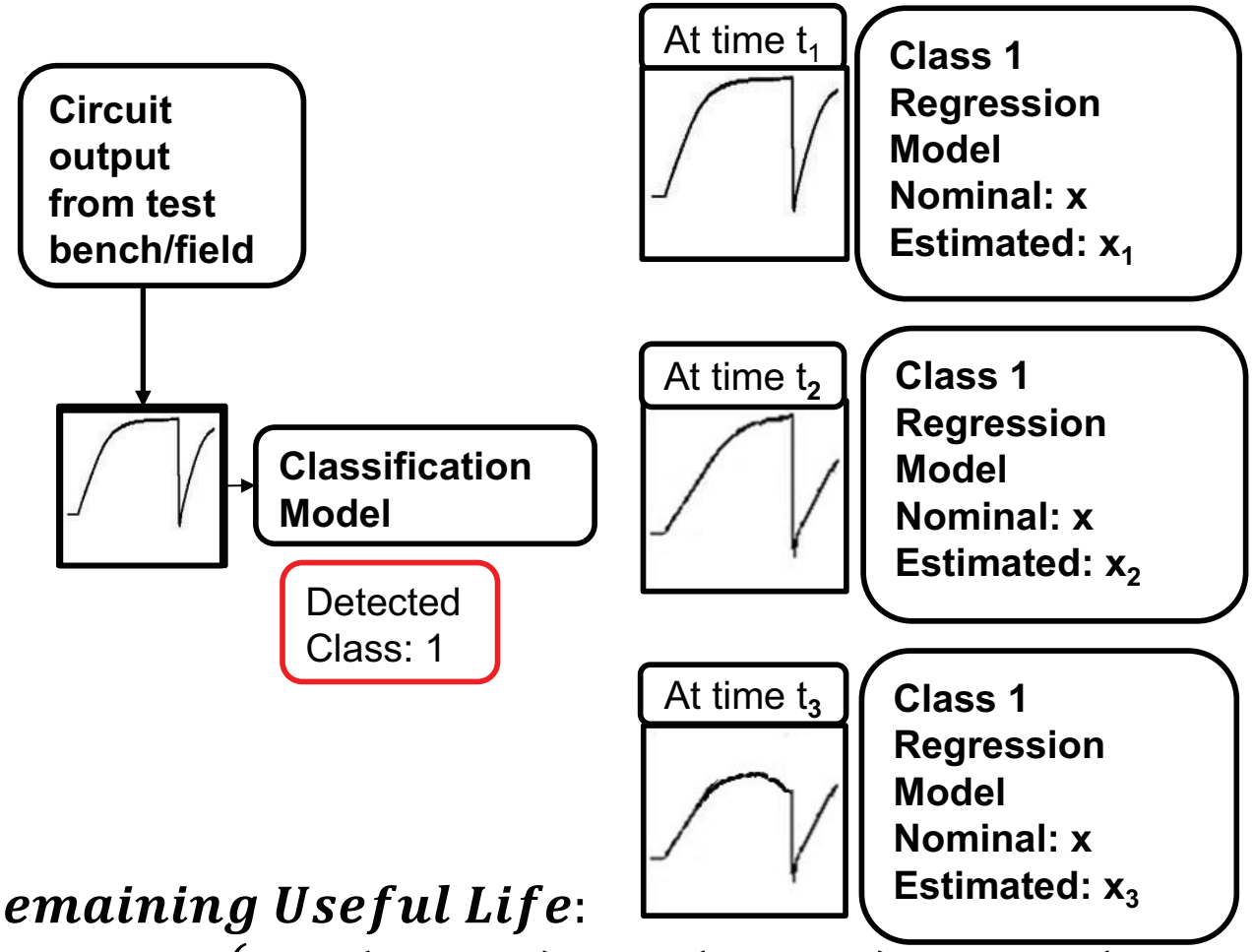
Circuit Output from Test Bench

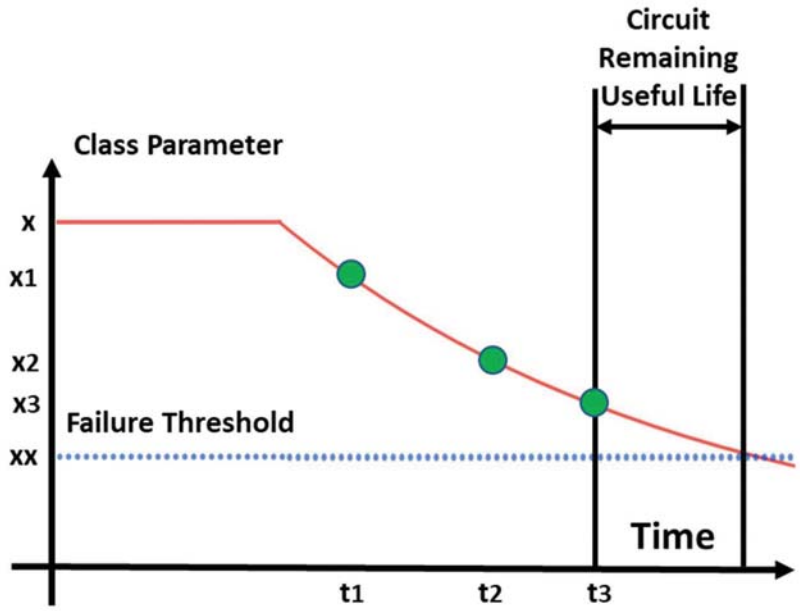


Classification Model

Fault *i*
(Defect *i*)

CALCE PSHM Method: Fault Prognosis





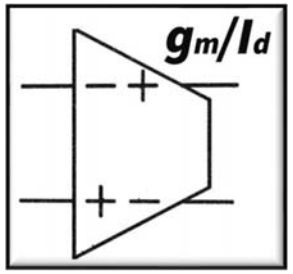
Remaining Useful Life:

$$RUL = \min\big(RUL(Class\ 1), RUL(Class\ 2), \ldots, RUL(Class\ N)\big)\ time\ units$$

Advantages of CALCE PSHM Approach

Design:

- Reduced simulation load, improved sensitivity (criticality) analysis
- Improved guidance for allocation of resources (test points)

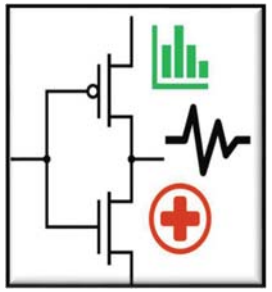


Testing:

- Complimentary to defect-oriented testing
- Increased test coverage, and reduced test escapes

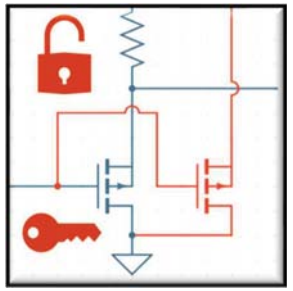
Economics:

- Increased market share in safety-critical applications
- Implementation of self-diagnostic and self-prognostic capabilities with minimal investment



Usage:

- Real-time diagnosis and prognosis



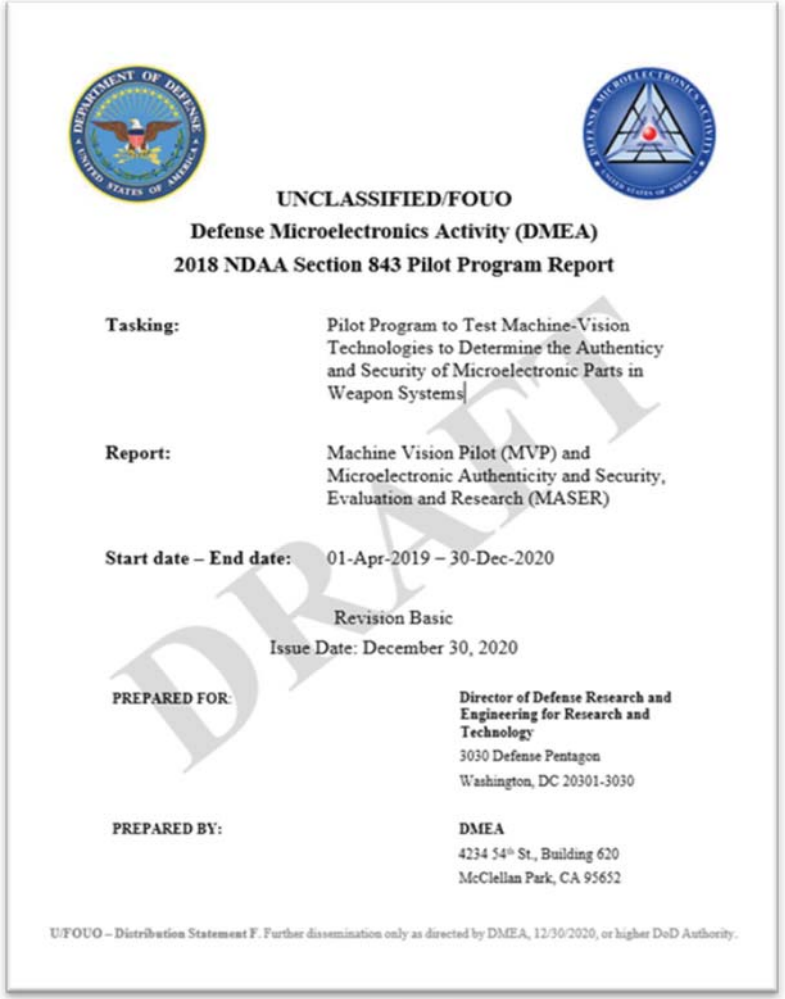
Security:

- Detection and discrimination between natural aging and maliciously induced aging
- Reduced reliance on trusted foundries.

Future Directions and Needs

- Further development and increased adoption of standards-based test methods by government and industry
  - e.g., second order effects, advanced methods for detection of tampered devices
- Collection of objective data on effectiveness of tests
  - e.g., CALCE-DMEA Study
- Diagnostic and prognostic tools for supply chain assurance and real-time threat detection (e.g., CALCE PSHM Method)

CALCE Pilot Program for DoD



UNCLASSIFIED/FOUO

Defense Microelectronics Activity (DMEA)

2018 NDAA Section 843 Pilot Program Report

Tasking: Pilot Program to Test Machine-Vision Technologies to Determine the Authenticy and Security of Microelectronic Parts in Weapon Systems

Report: Machine Vision Pilot (MVP) and Microelectronic Authenticity and Security, Evaluation and Research (MASER)

Start date – End date: 01-Apr-2019 – 30-Dec-2020

Revision Basic

Issue Date: December 30, 2020

PREPARED FOR: Director of Defense Research and Engineering for Research and Technology
3030 Defense Pentagon
Washington, DC 20301-3030

PREPARED BY: DMEA
4234 54th St., Building 620
McClellan Park, CA 95652

U/FOUO – Distribution Statement F. Further dissemination only as directed by DMEA, 12/30/2020, or higher DoD Authority.

DRAFT

- CALCE performed a 21 month study in 2019-20 for the Defense Microelectronics Activity (DMEA), funded under Section 843 of the 2019 National Defense Authorization Act (NDAA).
  - Review of emerging counterfeit detection systems and technologies, and comparison with SAE AS6171 standards-based testing, with a blind study of effectiveness with real counterfeits, including clones.
  - Review of existing legislation, standards, requirements, and policies (led by University of Maryland Carey School of Law)
- CALCE worked with ten technology organizations and SMT Corporation to assess the maturity of their technologies and their ability to detect counterfeit parts.
- The study provided a set of long and short term recommendations to the US DoD regarding technology adoption and procurement policies.

CALCE-DMEA Study

- The study focused on both conventional counterfeits and cloned parts.
- The blind study compared conventional, side channel (SC), and machine vision (MV) methods, for detection and authentication.
  - There were methods in each category with >99% accuracy, although technology readiness was still lagging for SC and MV methods.

Acknowledgements

- The Center for Advanced Life Cycle Engineering (CALCE): faculty, students, and the organizations that support our research and consortium
- Defense Microelectronics Activity (DMEA)
- Members of the SAE G-19A committee

THANK YOU

Dr. Michael H. Azarian

Center for Advanced Life Cycle Engineering (CALCE)

University of Maryland

SAE G-19A Committee Chair

mazarian@umd.edu

http://www.calce.umd.edu

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

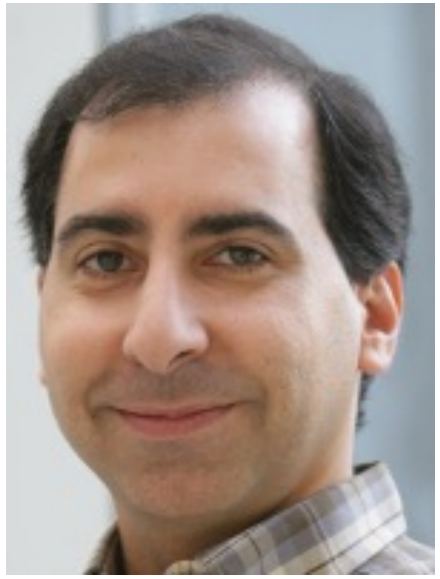
Supply Chain Challenges for Defense Systems

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

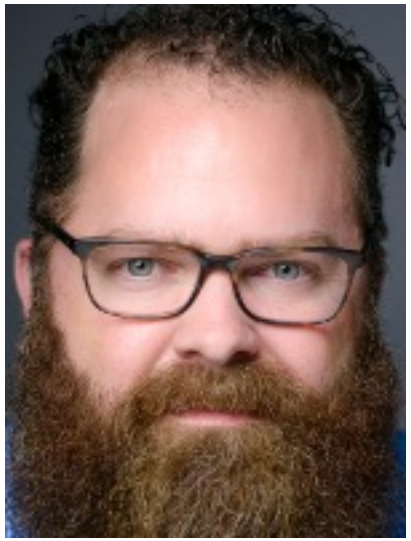


Michael Azarian
University of Maryland

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

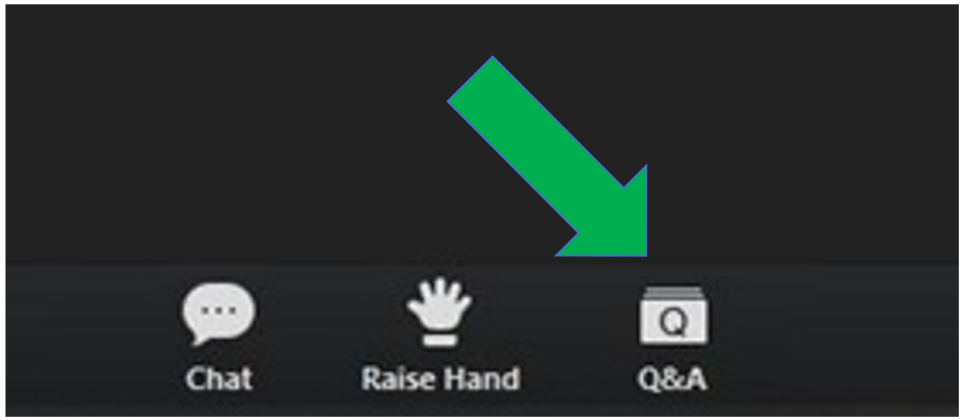
Reminders

Slides & Videos will be posted next week

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

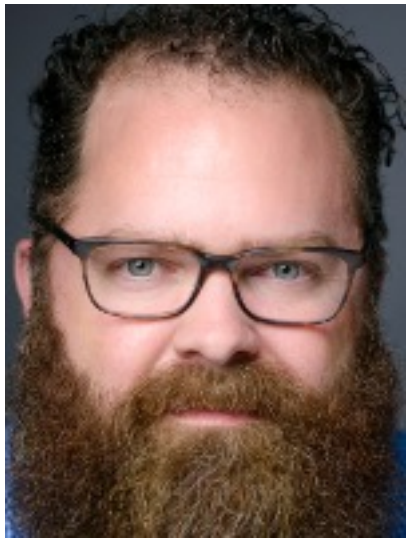
youtube.com/MEPTECpresents

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