CALCE
CENTER FOR ADVANCED
LIFE CYCLE ENGINEERING

SMTA

AI Enhanced Physical Inspection for Counterfeit Microelectronics

Charles G. Woychik and Navid Asadizanjani*
NHanced Semiconductors, Inc.
Batavia, IL 60510
cwoychik@nhanced-semi.com
***Department of Electrical and Computer Engineering**
University of Florida,
nasadi@ece.ufl.edu

Genesis for Developing Secure Si-Interposers

PSM – Ushering PCB Security Through System-level MEMS Integration (N00014241205 6)

PM Meeting – 19th May 2025

UF | UNIVERSITY of FLORIDA

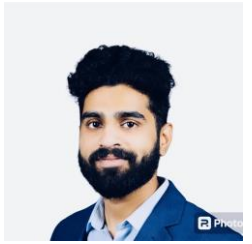
ASU

PSM Team

Program Managers ONR:
Dr. Ryan Craven
Dr. Daniel Koller

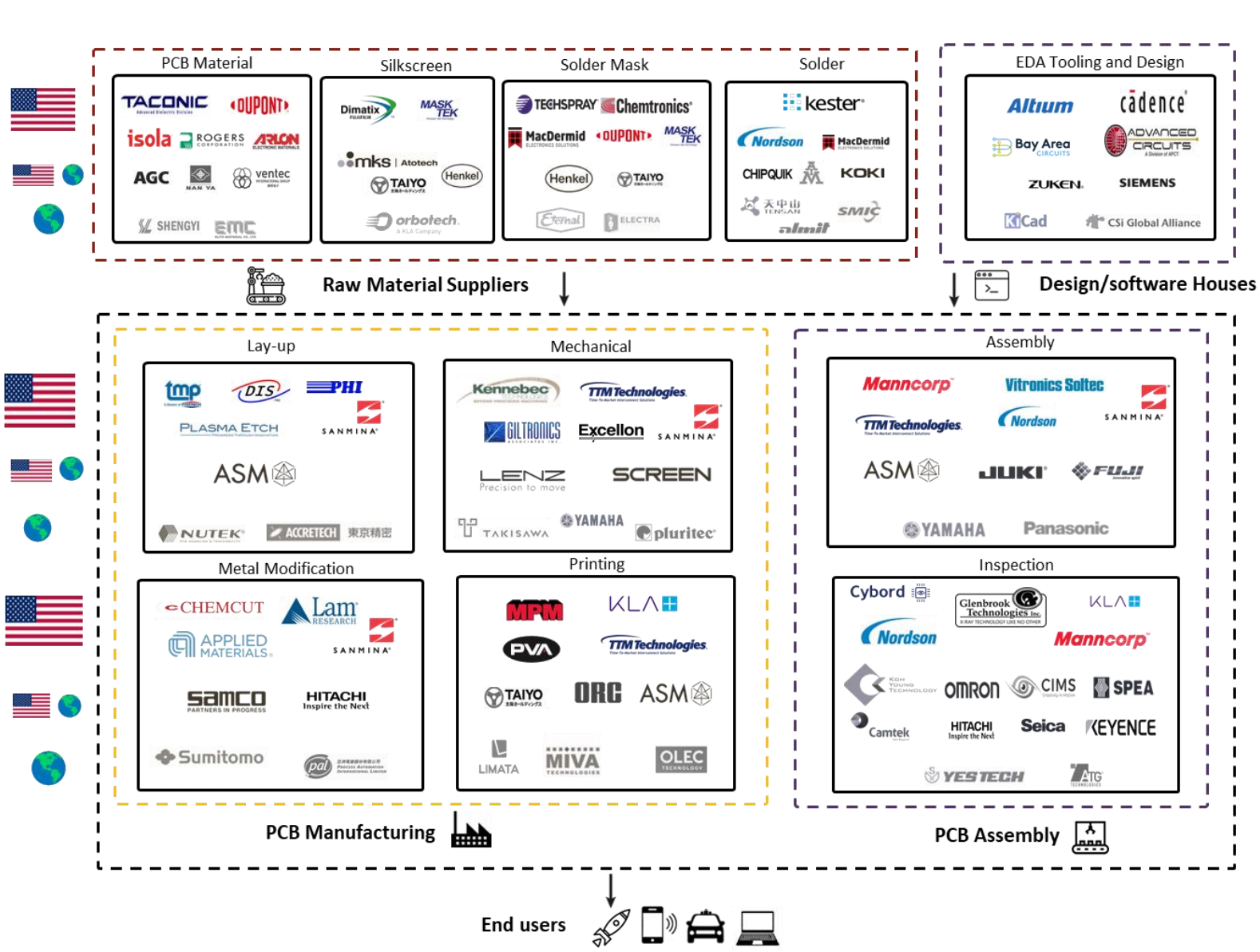
Task Leaders:
Dr. Navid Asadi (University of Florida)
Dr. Josh Hihath (Arizona State University)

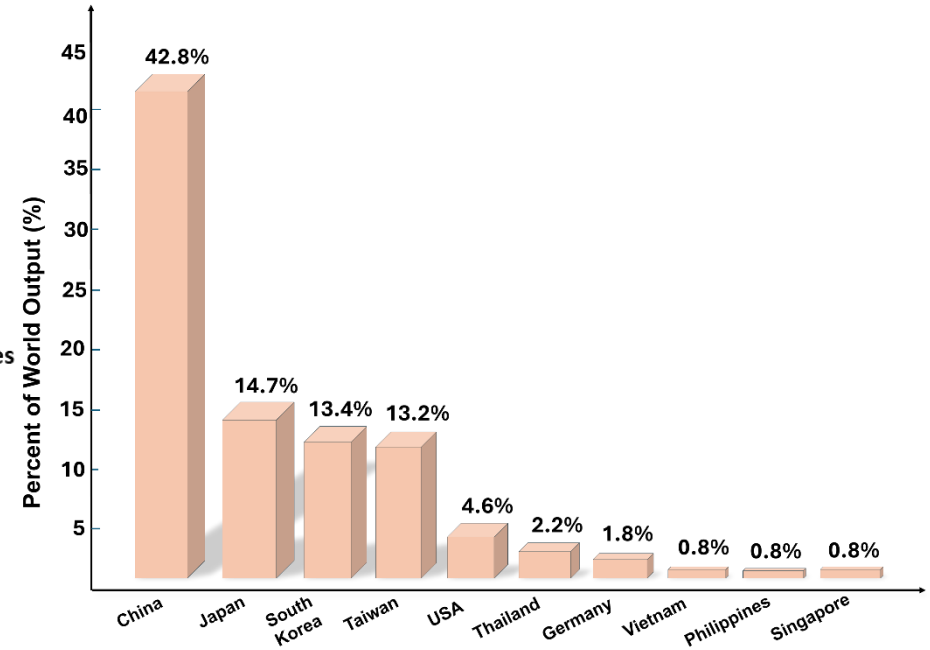

Students:
Himanandhan Reddy K (Univ. of Florida ECE, Ph.D.)
Pavanbabu (John) Arjunamahanthi (Univ. of Florida ECE, Ph.D.)
Shafkat Khan (Univ. of Florida ECE, Ph.D.)
Liam Hayes(Arizona State University ECE, Ph.D.)
Kyoungdu Kim(Arizona State University ECE, Ph.D.)
Bo Liu(Arizona State University ECE, Post doc)




BACKGROUND

PCB Ecosystem and Market





- ✓ **Supply Chain**: Covers raw materials, PCB manufacturing, design, and assembly.
- ✓ **Key Players**: Includes DuPont, ASM, KLA, Nordson, etc.
- ✓ **Market Share**: Bar chart shows country wise production distribution.

Global Landscape

North America is in a Weak Position for AP/HI

Reference: Yole 2023

Scenarios – Real Time Attacks

Your Air Force

An F-16 pilot died when his ejection seat failed. Was it counterfeit?

By Rachel S. Cohen

Sep 13, 2022

David Schmitz, then a staff sergeant, poses in 2014 at at Joint Base Lewis-McChord, Wash. (Jacob Jimenez/Air Force)

Defense One

China's Copycat Jet Raises Questions About F-35

New technical specs about China's new J-31 fighter, a plane designed to rival the American-made F-35 Joint Strike Fighter, popped up on a Chinese blog last...

IEEE Spectrum

Invasion of the Hardware Snatchers: Cloned Electronics Pollute the Market

Fake hardware could open the door to malicious malware and critical failures.

Hackaday

IPhone 6S NVMe Chip Tapped Using A Flexible PCB

Psst! Hey kid! Want to reverse-engineer some iPhones? Well, did you know that modern iPhones use PCIe, and specifically, NVMe for their...

The Aviationist

Iran unveils reverse-engineered version of captured U.S. RQ-170 stealth drone

Iran unveiled an RQ-170 drone allegedly manufactured by reverse-engineering of US Sentinel drone captured in December 2011.

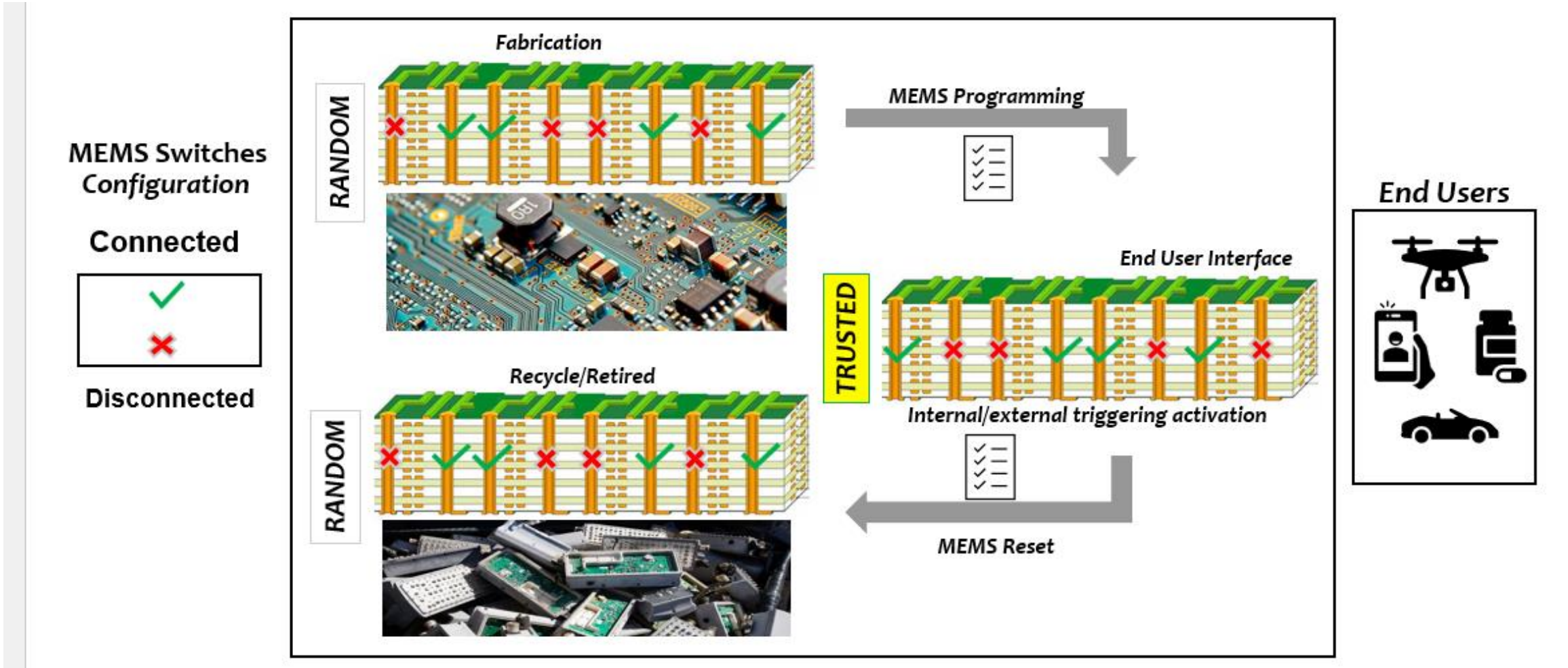
Hackaday

Reverse Engineering A PCB

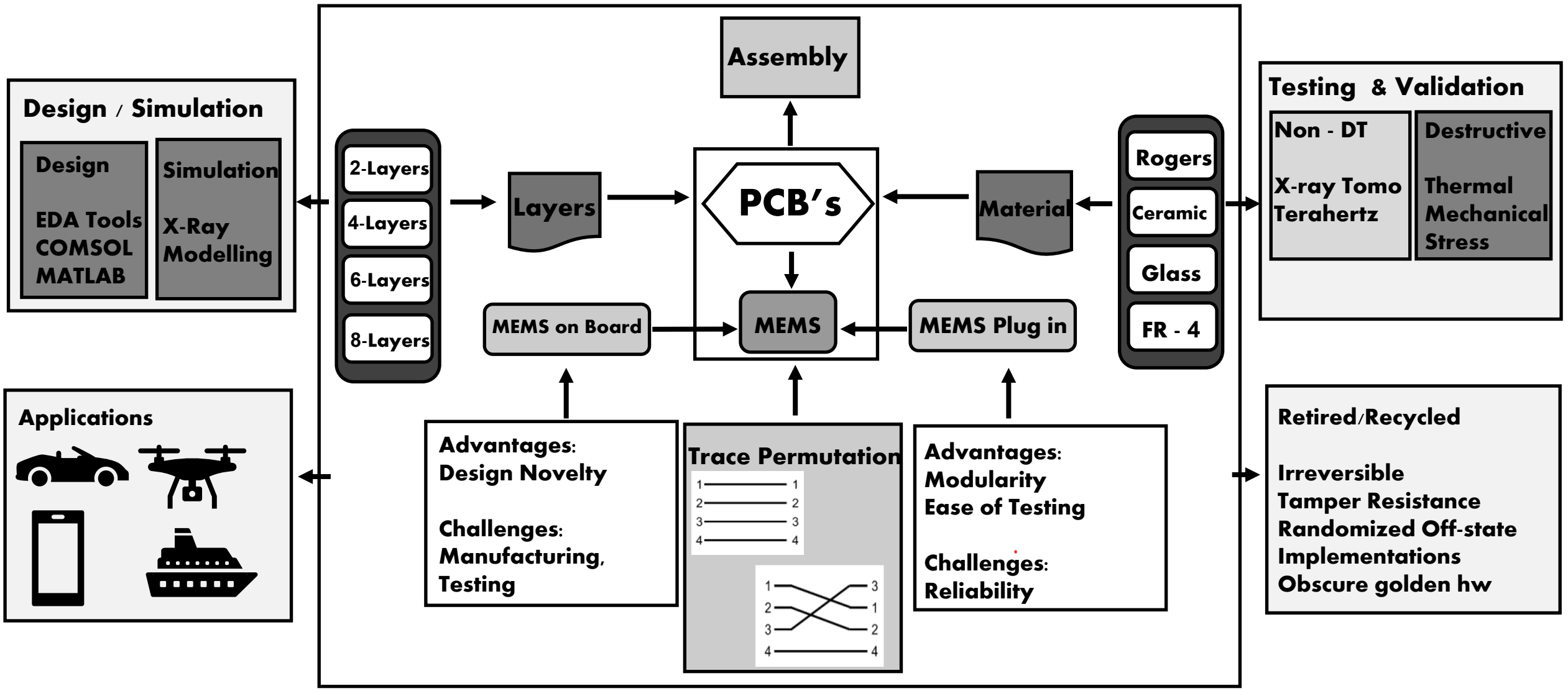
Occasionally when a device breaks, the defect is obvious. Whether it is a blown fuse or a defective capacitor, generally the easy to see...

RESEARCH APPROACH

PSM Strategy

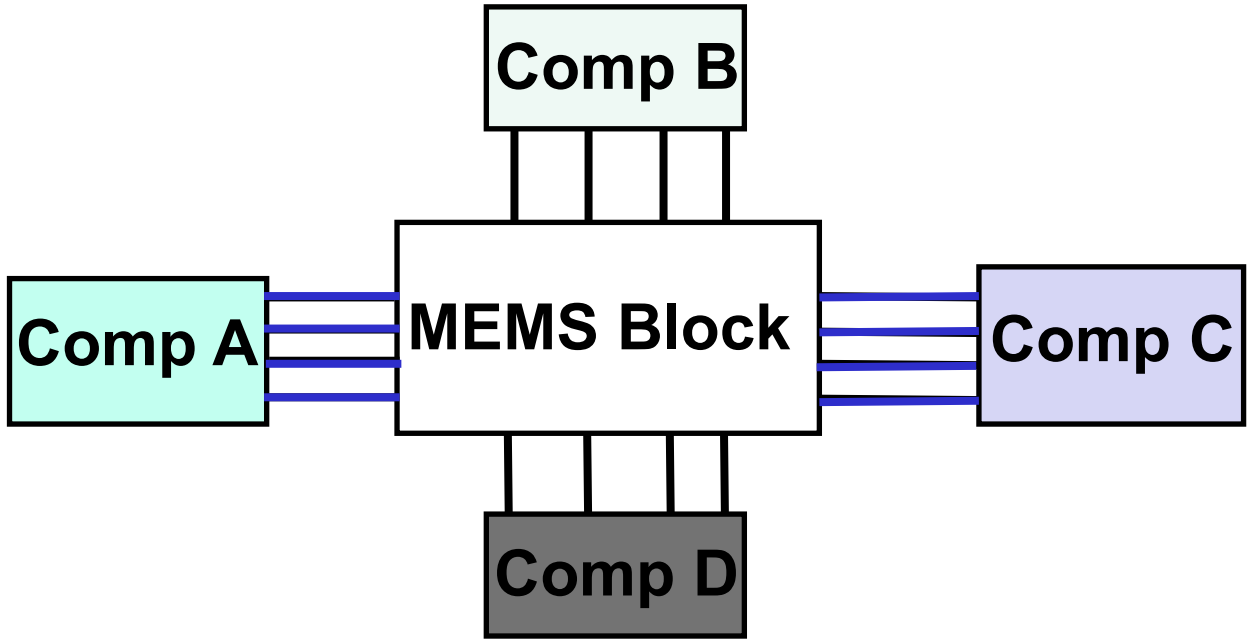


Solution Overview



Entropy Analysis – Case 1

Case 1: All 4 Traces Go to Only One Other Component at a Time



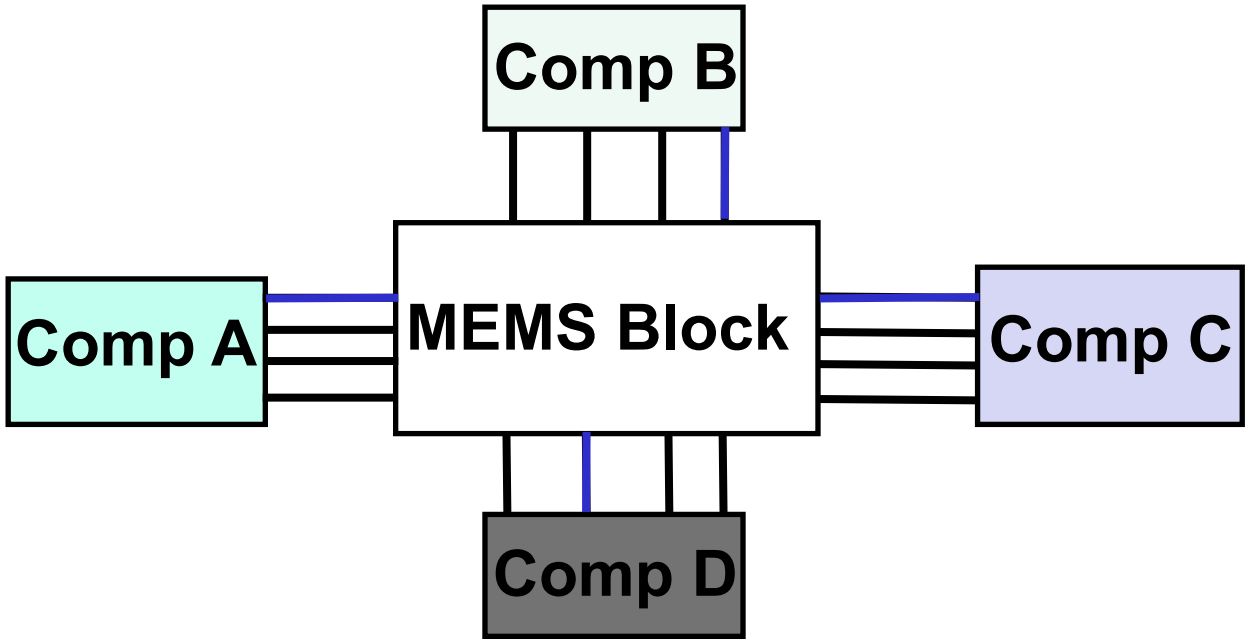
Case 1:

- Each component (e.g., Comp A) sends **all 4 traces** to just one of the remaining components (B, C, D).
- **3 destination choices** for each component.
- **4 traces** can be permuted in **4! = 24** ways.
- So, **total permutations per component** = 3 × 24 = **72**.

For each of the 4 components independently $72^4 = \boxed{26,873,856 \text{ total permutations}}$

Entropy Analysis – Case 2

Case 2: Traces Can Be Split Across Multiple Components



Case 2:

- Each of the 4 traces can be routed independently to any of the 3 other components.
- **Routing combinations per component** = $3^4 = 81$
- For each combination, **trace-to-pad permutations** ≈ 24 (assumes typical distribution like 2 to B, 1 to C, 1 to D).
- So, **total permutations per component** = 81 × 24 = **1,944**.

For each of the 4 components independently

$$1944^4 \approx \boxed{1.427 \times 10^{13} \text{ total permutations}}$$

Key Communication Unit

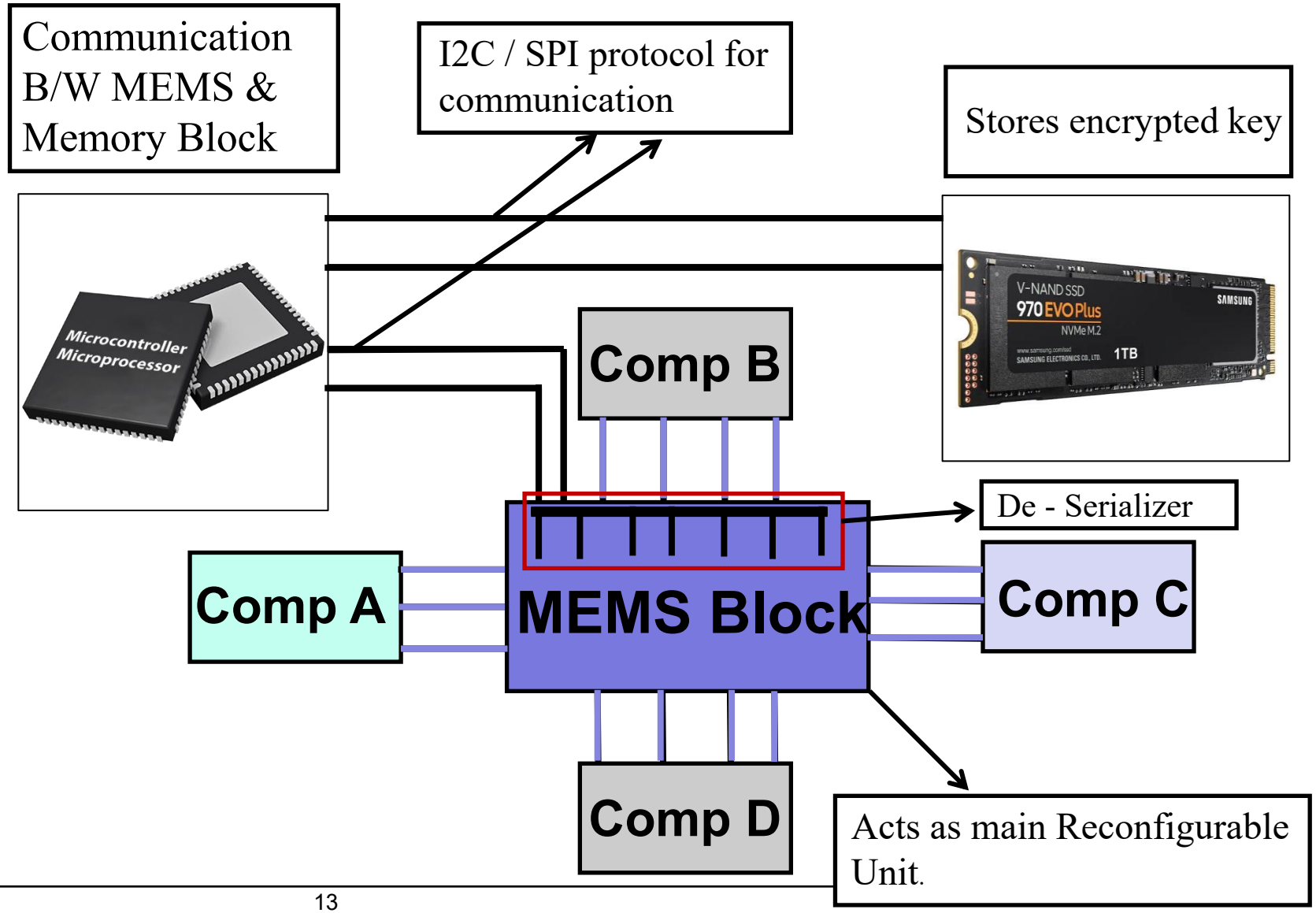
Step by Step Process

- **Power-Up**:
- Processor initializes and verifies the NVM integrity through digital certificate saved.

- **Key Retrieval**:
- The processor retrieves and decrypts the key securely.

- **Key Validation**:
- The MEMS block authenticates the key and configures accordingly.

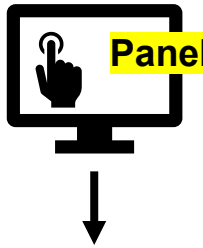
- **Configuration**:
- MEMS block establishes secure communication pathways between components.



MEMS-Enabled PCB Security (MEPS) – Workflow

Pre – Obfuscated Netlist → MEPS TOOL → Post – Obfuscated Netlist

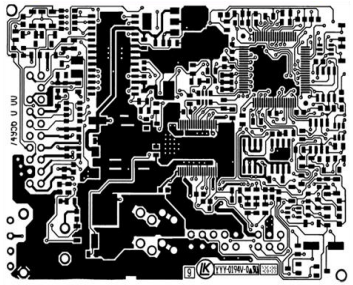
Constraints



User Inputs

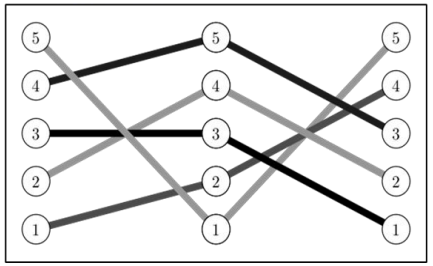
- Pre-Obfuscated Netlist
- Priority Components
- No of MEMS Plug In
- Size of MEMS Plug Ins

Parsed Netlist

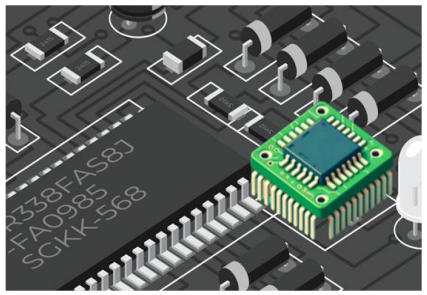


Identify Target Regions

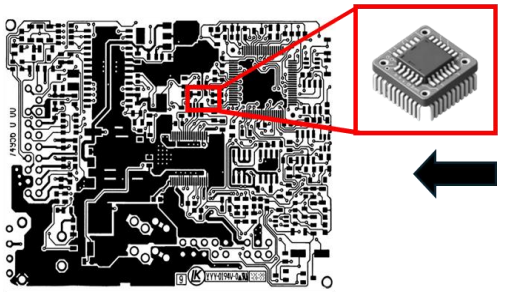
Assign Placement Scores



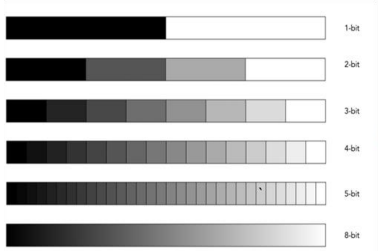
Finalize Placement



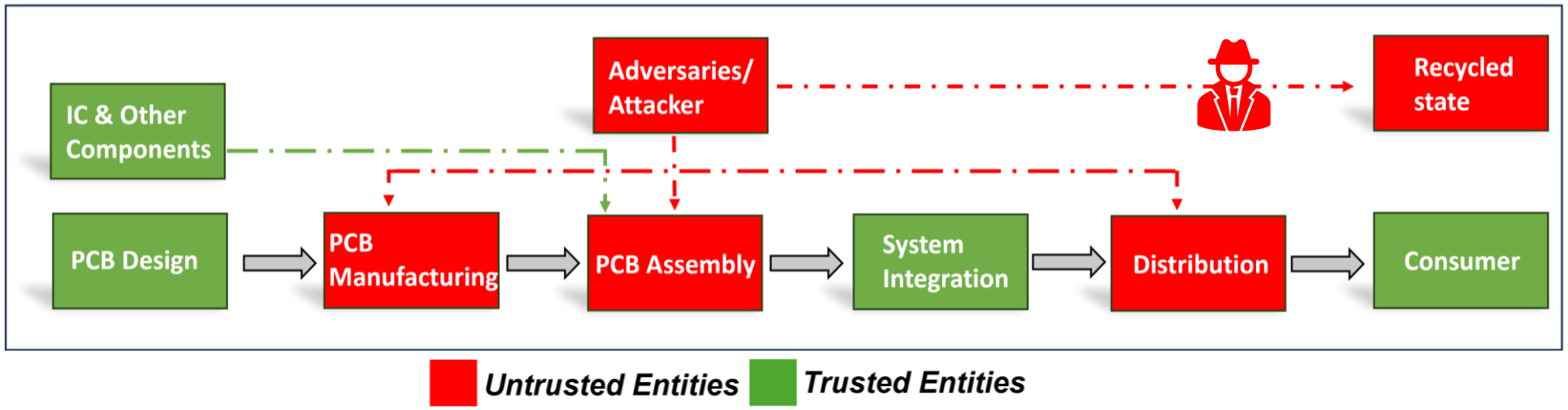
Modified Netlist



Configuration Bits

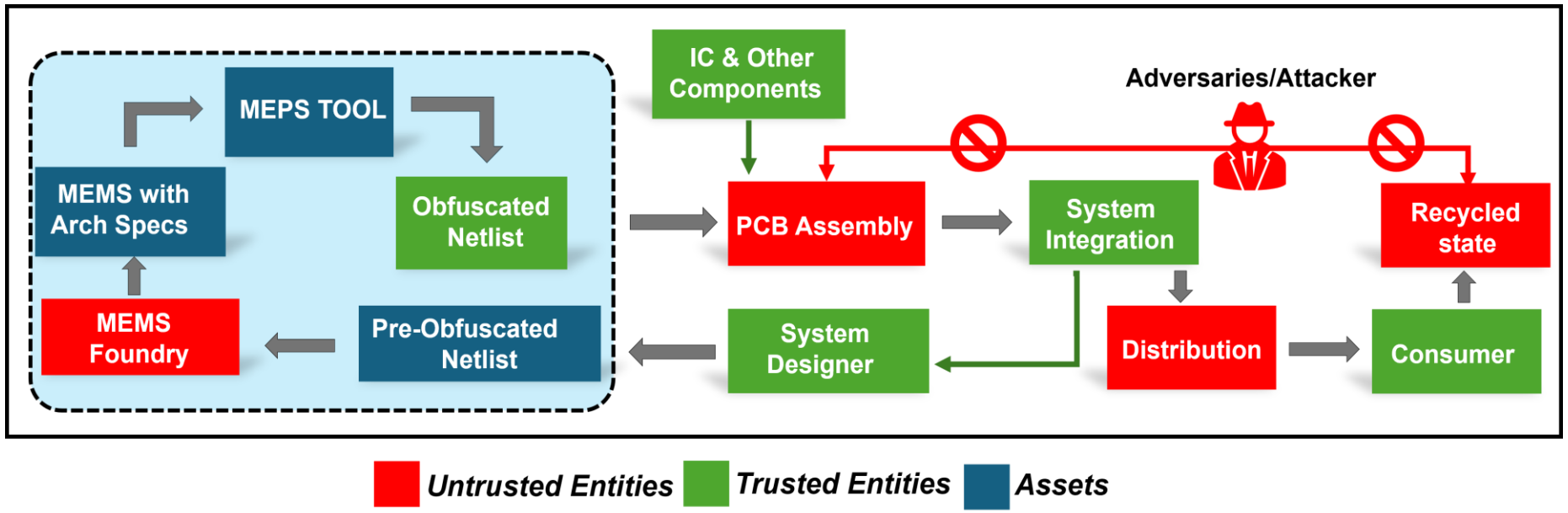


Supply Chain Before and After



Without MEPS

- Higher risk of tampering and counterfeiting.
- Predictable interconnects enable reverse engineering.
- Vulnerable end-of-life security.



With MEPS

- Unique MEMS arrays prevent replication.
- Reduced supply chain attack risks.
- Strong protection against reverse engineering.

MEMS Cantilever Beam Characteristics

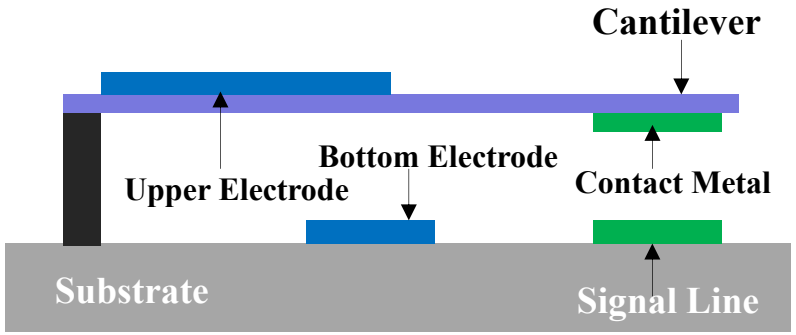


Table 1. Young's modulus and Poisson ratio for several materials

Material	Young's modulus (E) [GPa]	Poisson ratio (ν)
Polysilicon	141	0.27
Aluminum	70	0.33
Gold	79	0.44

for $L = 260$ μm, $w = 50$ μm, $h = 1$ μm and $d_o = 1$ μm

Beam Material	Density (kg/m³)	First natural frequency (kHz)
Polysilicon	2330	18.590
Aluminum	2700	258.03
Gold	19300	4.834

Component	Vibrational frequency
Submarine	10 – 200 Hz
Commercial aircraft	10 – 100 Hz
Military aircraft	10 – 2000 Hz
Medical devices (MRI)	20 – 100Hz

$$\frac{d^2y}{dx^2} = \frac{M}{EI}, \Rightarrow$$ Deflection of Cantilever beam

Higher deflection

Undesirable properties:

- Increased contact resistance
- Material fatigues
- Stiction
- Electrical failures

Natural frequency — **Higher the gap** — Operating environment frequency ⇒ Better performance

PSM proposed MEMS switch contains Aluminum, hence the optimal choice

Testing Methodologies

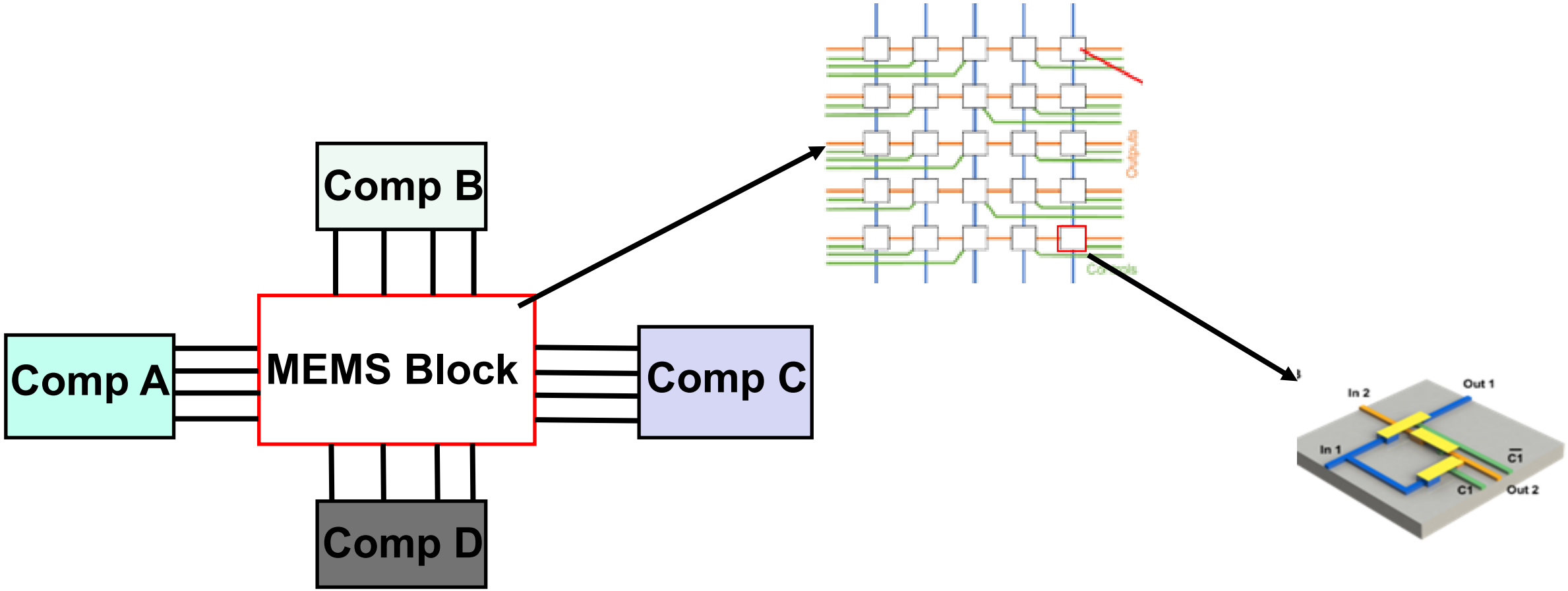
Tests	Details	Standards
Physical Inspection	Physical Inspection and Visual Check	ISO 9001:2015 – Quality management – Requirements. KGD
Electrical Characterization	Contact Resistance, Electrical Performance and Switching Performance Tests	MLF - PRF - 123 – Performance Specification Electronic Components, General Specification for, IEC 60512 – Connectors for Electronic Equipment Tests and Measurements, IEEE 1452 – Standard for a Smart Transducer Interface and Sensors and Actuators
Mechanical Characterization	Reliability and Durability Tests	IEC 60749 – Semiconductor Devices – Mechanical and Climatic Test Methods
	Temperature and Environmental Tests	MIL-STD-810 – Test Method Standard for Environmental Engineering Considerations and Laboratory Tests
	Vibration and Shock Resistance	IEC 60068-2 – Environmental Testing – Part 2: Tests, Test B: Dry Heat

Additional Testing Plans

Tests	Standards
Hermeticity and Packaging Tests	ASTM E2512 – Standard Test Method for Determination of Noise Equivalent Power (NEP) and Noise Equivalent Concentration (NEC) of a Photoacoustic Spectrometer
Calibration and Standardization	ISO/IEC 17025 – General Requirements for the Competence of Testing and Calibration Laboratories
Failure Modes and Reliability Tests	JEDEC, JESD22 – Series of standards for testing semiconductors devices, including mechanical and Environmental tests.

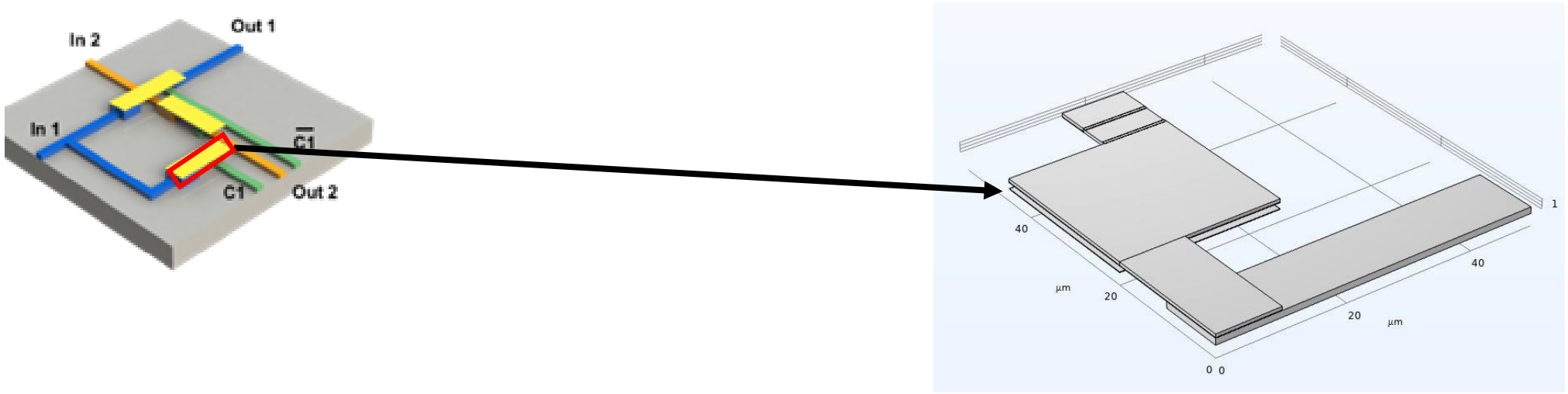
ASU Goals

- Design and Fabrication of MEMS block is critical to system level design
- Within each MEMS block, switching cells are present
- MEMS cantilever switches are the critical devices within each cell



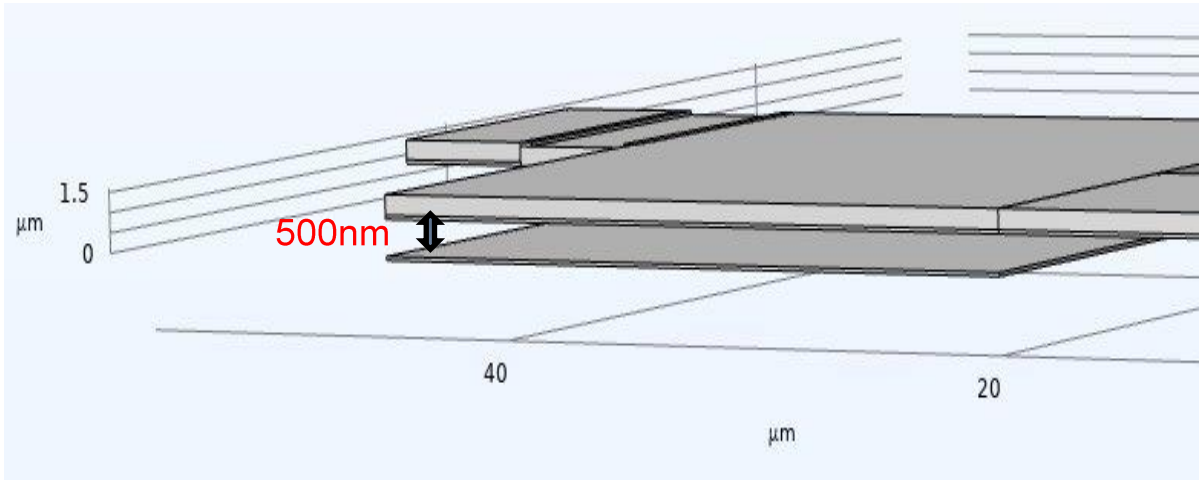
ASU Goals

- Initial design work – proof of concept for working switch structures
- Then, implementation into obfuscation cells and blocks may be initiated



Why MEMS?

- ❑No leakage current to detect at DC, difficult to detect at AC – Improves security by mitigating successful probing efforts
- ❑Sub-Micron Air Gap with high aspect ratio to cantilever height – makes optical and electron imaging difficult
- ❑Large dielectric features relative to metallic features – Further increases electron imaging difficulty
- ❑Commonly Fabricated – Much industry support from companies like HRL, ADI, TI...etc.



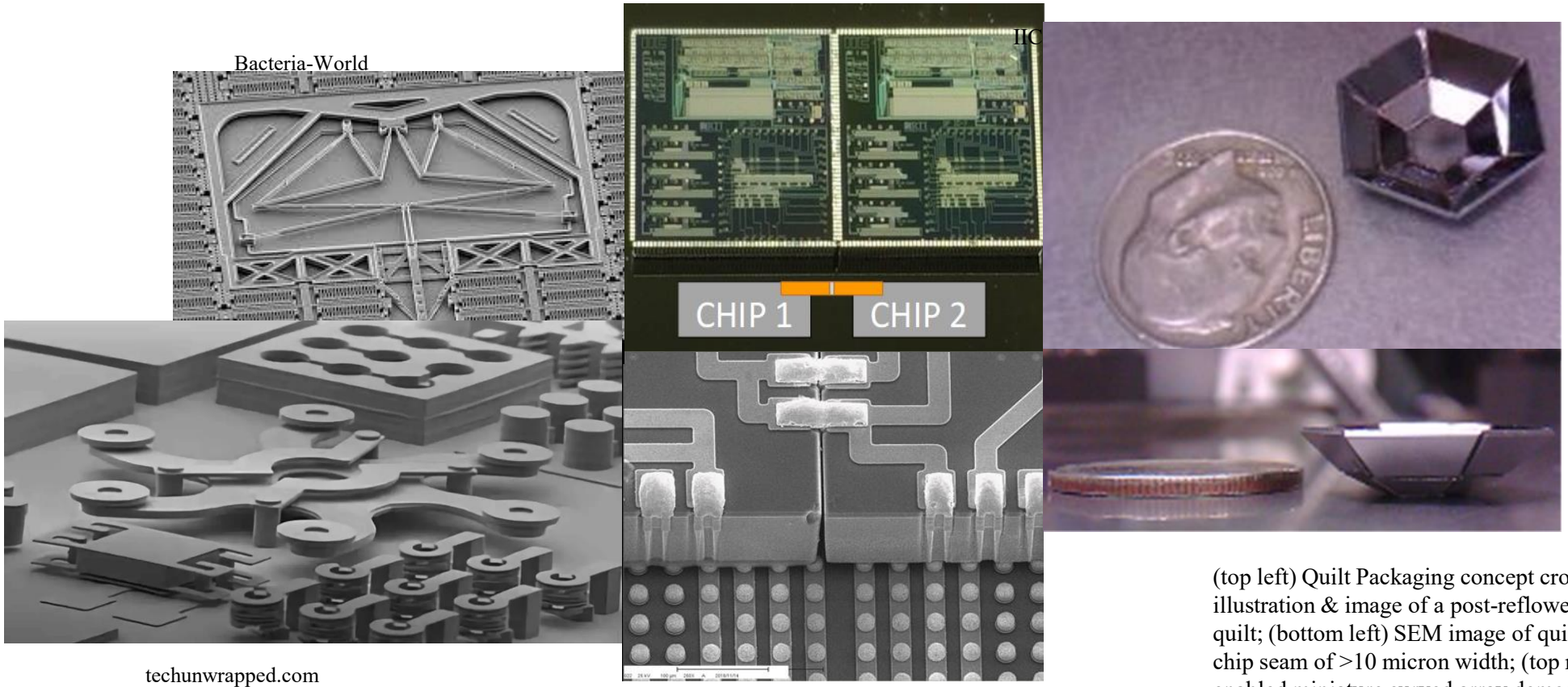
ANALOG DEVICES
HEAD OF WHAT'S POSSIBLE™

NHanced SEMICONDUCTORS

HRL LABORATORIES

NHanced Semi: Micro-Connections and 3D Structures

MEMS + Precision Electronics

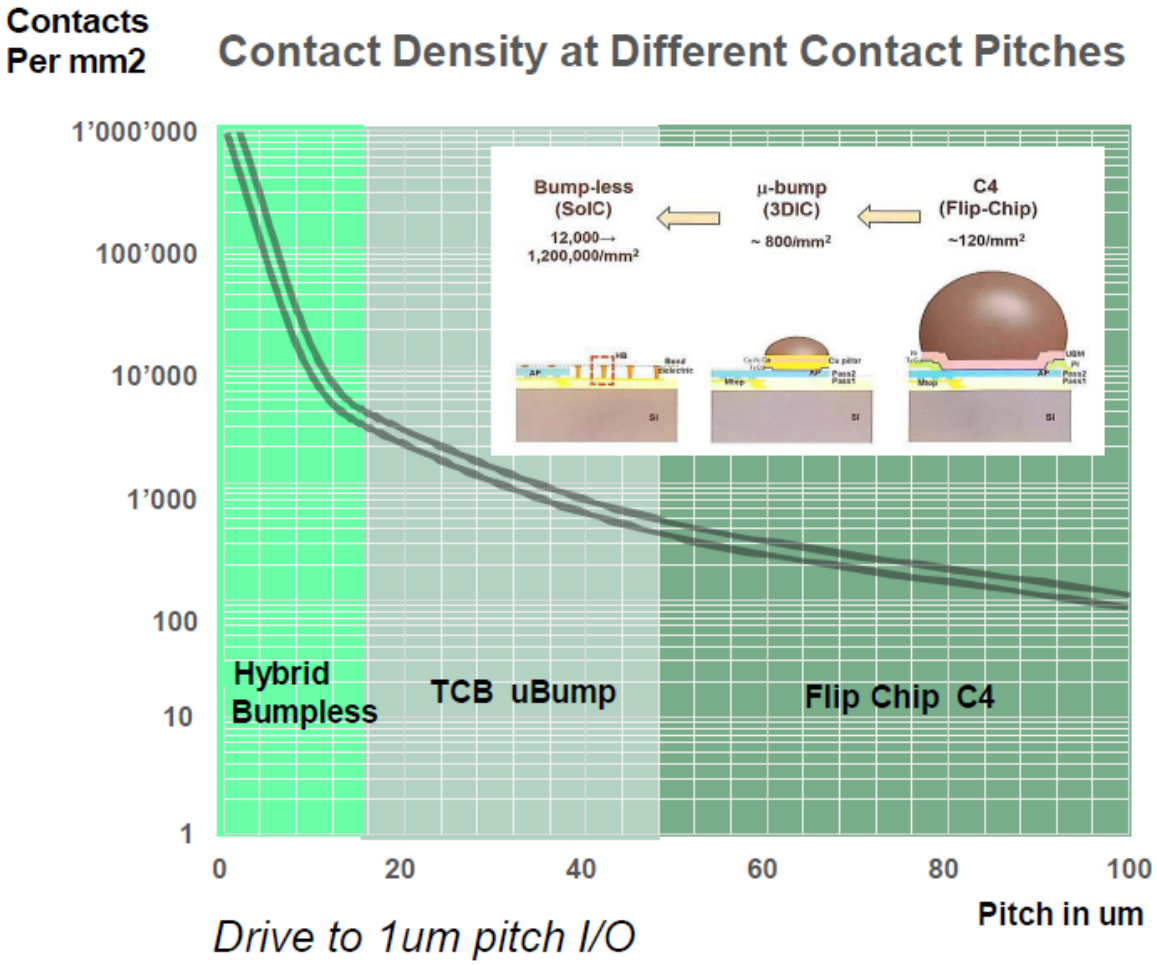


techunwrapped.com

(top left) Quilt Packaging concept cross-section illustration & image of a post-reflowed QP CMOS quilt; (bottom left) SEM image of quilted chip-to-chip seam of >10 micron width; (top right) QP-enabled miniature curved array demonstration article; (bottom right) profile view of QP-enabled miniature curved array.

NHanced SEMICONDUCTORS

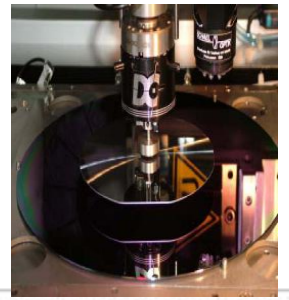
Hybrid Bonding Innovation

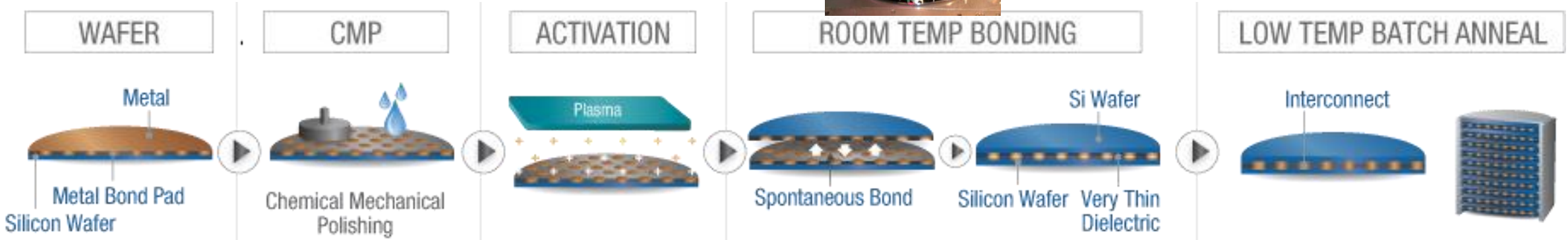


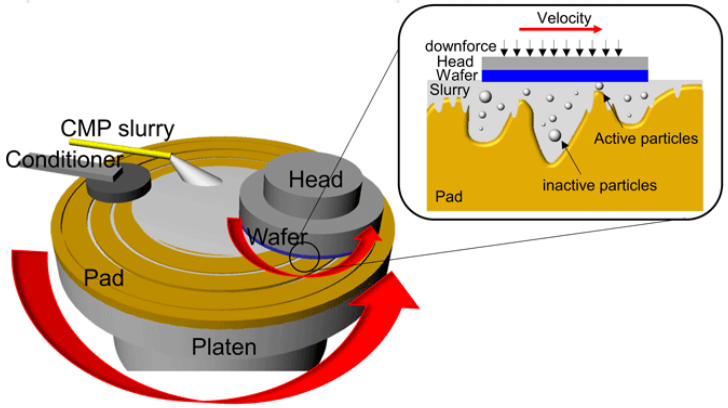
Tom Strothman, BESI

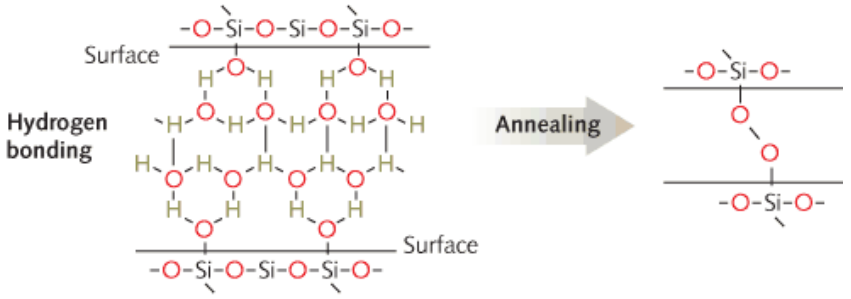
Intel

DBI®: Low Temperature Hybrid Bonding Process



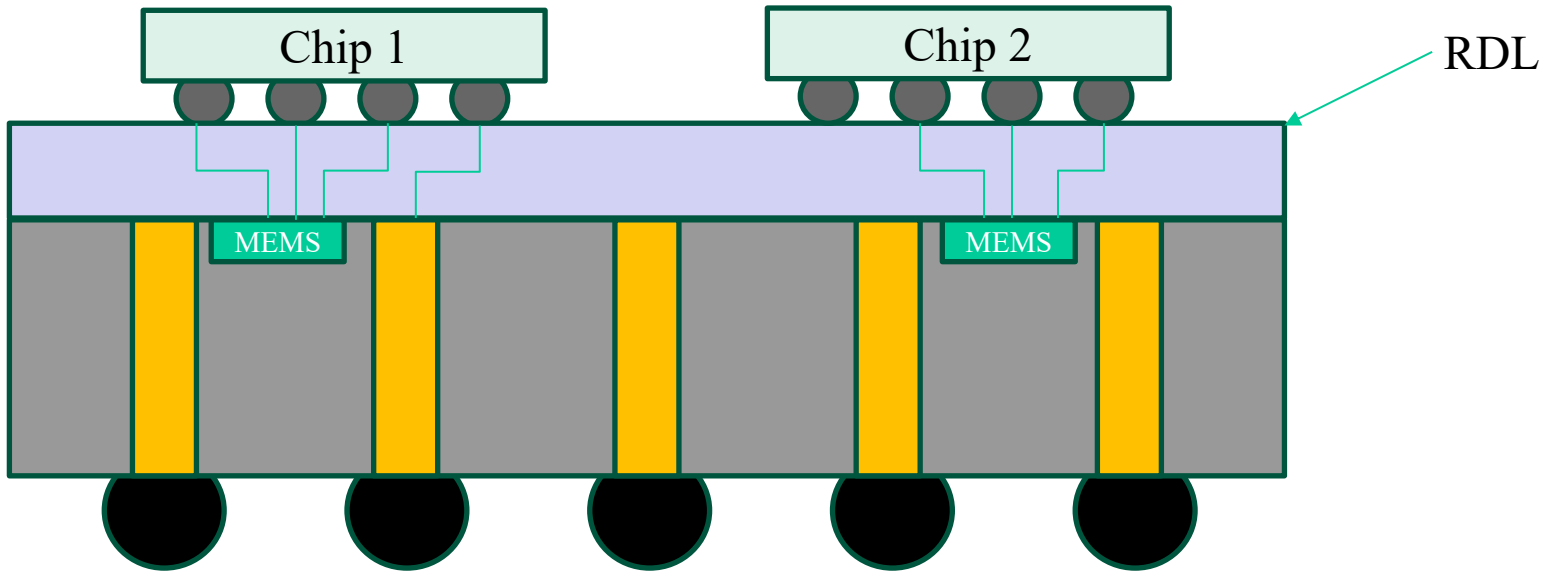




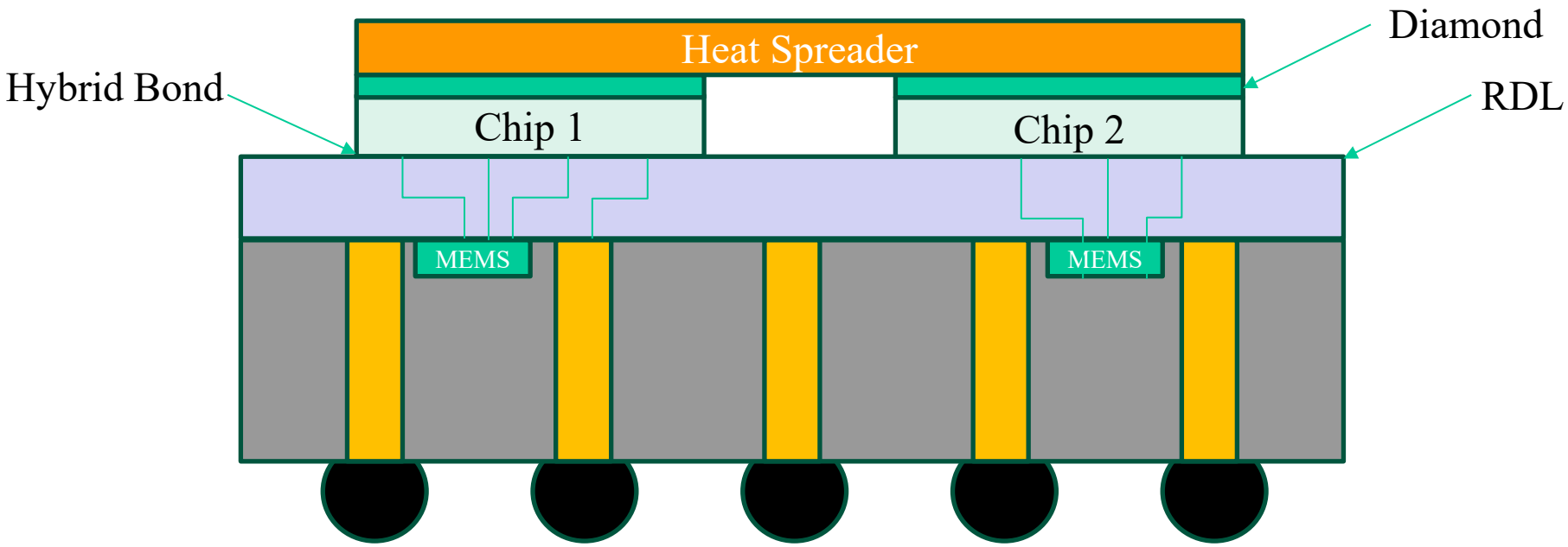


Jihoon Seo / Materials Research Society

Integrate a MEMS Device into a Si-Interposer



High Performance Package Using Si-Interposer



Testing Capabilities at SCAN Lab

Orion Nanofab
PHEMOS
Skyscan nanoCT
FERA3
LYRA3
Terahertz
Allied Sample Preparation
Optical Microscope
Acoustic

Virtual Walk: https://my.matterport.com/show/?m=YVWh646Zp5L
Lab Dataset: https://physicaldb.ece.ufl.edu/

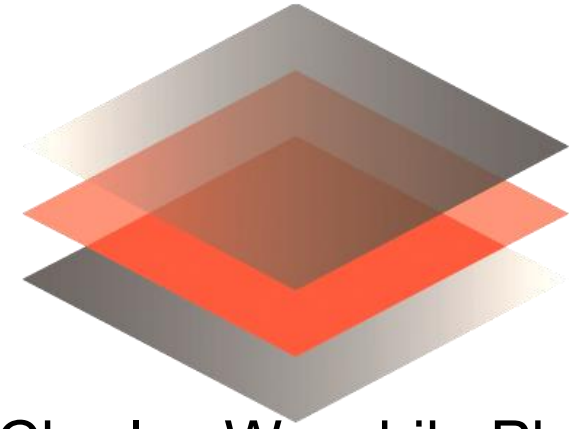
Summary

- A new focus on next generation of SECURED PACKAGES
  - Advanced Packaging
    - Unique MEMS arrays prevent replication.
    - Reduced supply chain attack risks.
    - Strong protection against reverse engineering.
  - Future is heterogenous integration using hybrid bonding
  - Interconnect focused – all BE0L additive processing
    - Better ROI
    - Lower development costs
    - Lower CAPEX
  - Leveraging existing foundries
    - Split Fab
  - More Than Moore Technologies
    - IP Centric
    - IP driven value – not cost of capital

Split Rock Lens – StackExchange

System Level Moore's Law

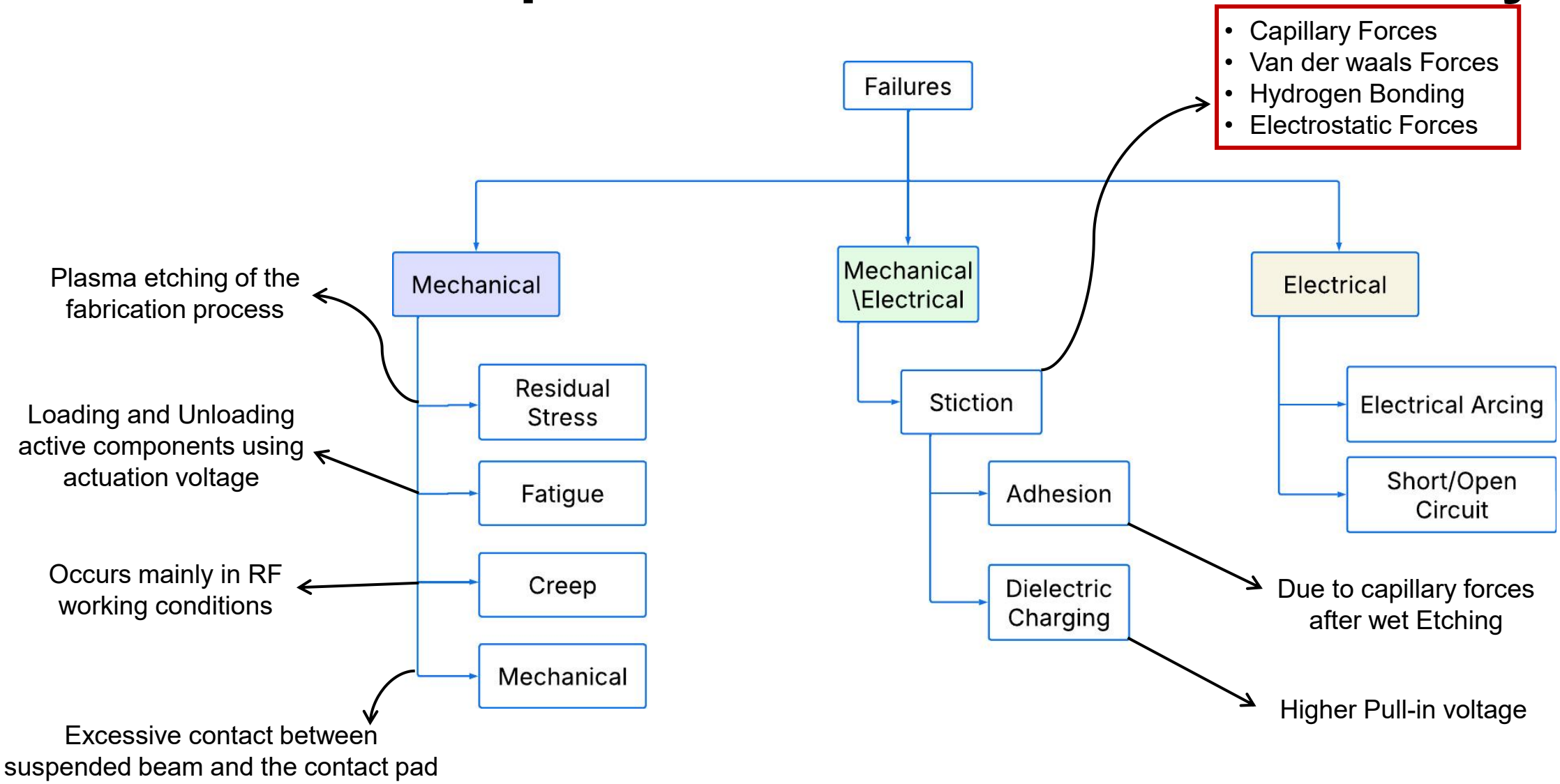
Thank You



Charles Woychik, Ph.D.
VP Business Development
NHanced Semiconductors, Inc.
cwoychik@nhanced-semi.com

Backup

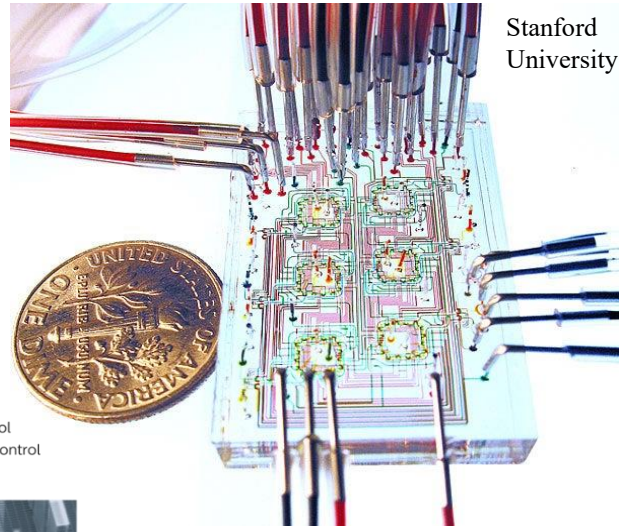
Failure Map of MEMS Switch for Reliability



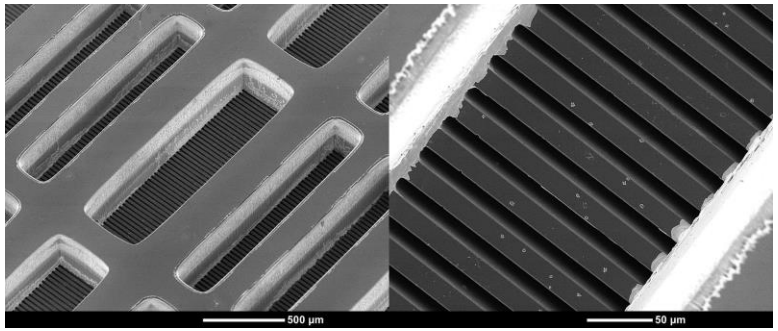
AP Services: Microfluidics and Cooling

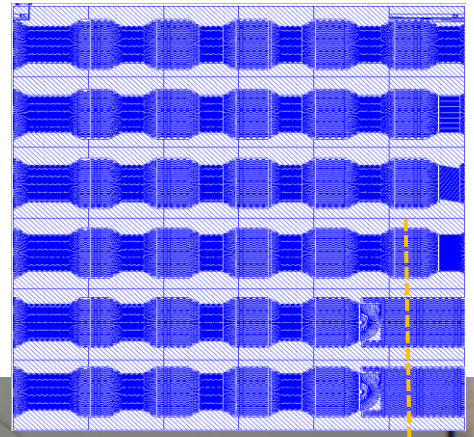
Chip Scale Cooling
For Ultra-Dense Electronics

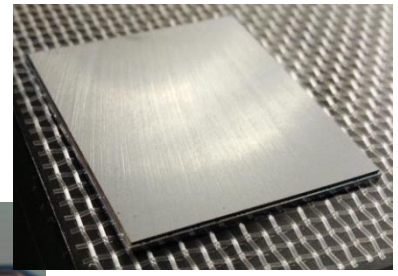
Biology + Electronics

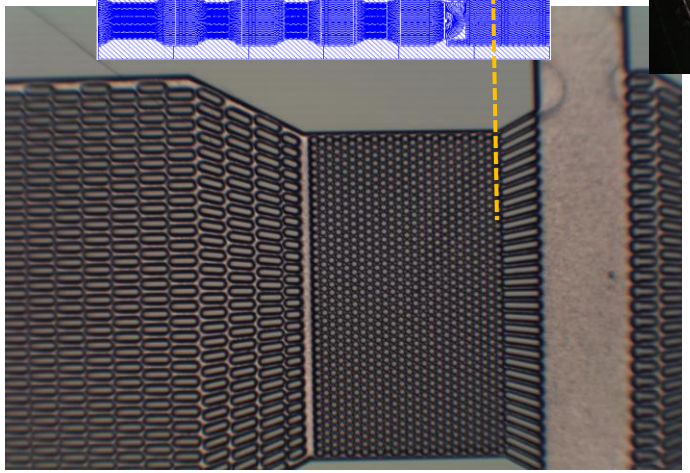


Purdue



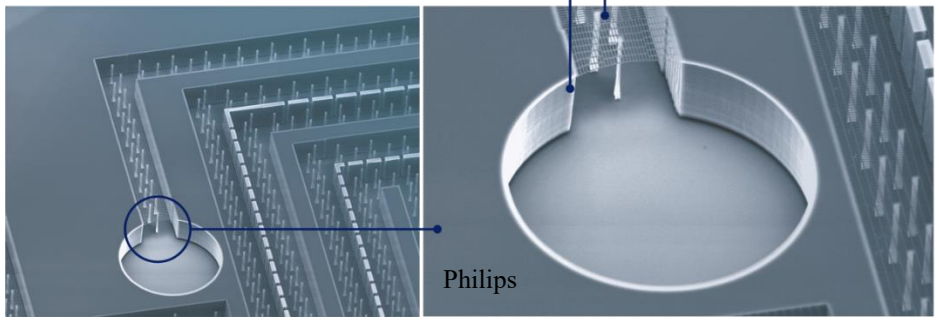






Our state-of-the-art tool set enables us to create microfluidic structures with accurate control:

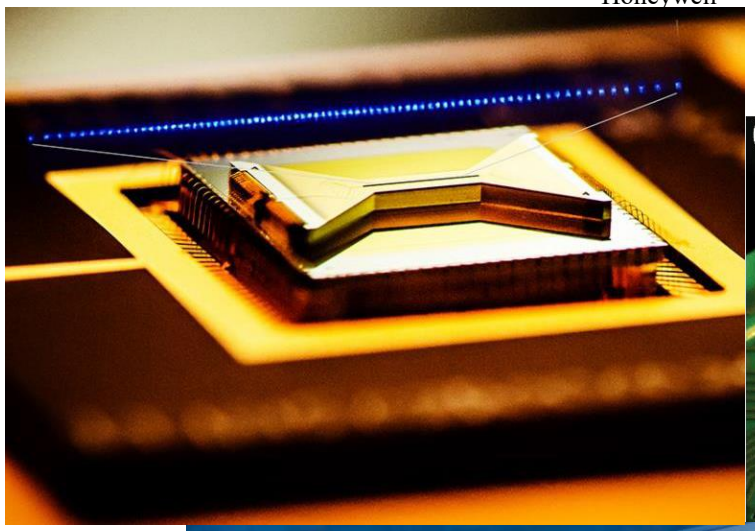
- <5 degree slope control
- Sub-µm feature size control
- µm range feature size



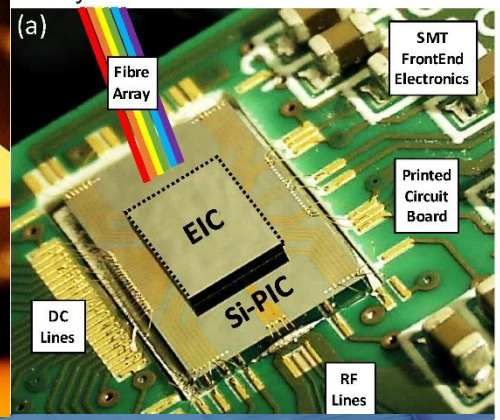
AP Market Drivers: Photonics & Quantum

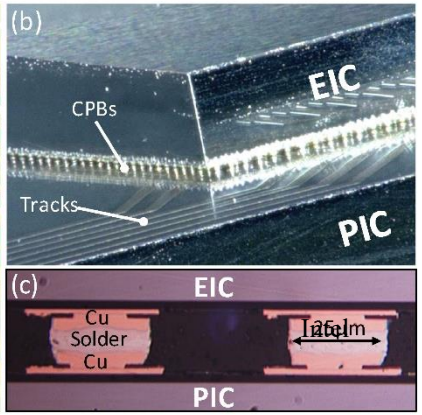
- I/O
  - Tb/s, <<100fJ/b
    - SiP 500ff I/O Load
    - 2.5D 25ff I/O Load
    - 3D 3ff I/O Load
- Processing
  - “Quantum Leaps”

Honeywell

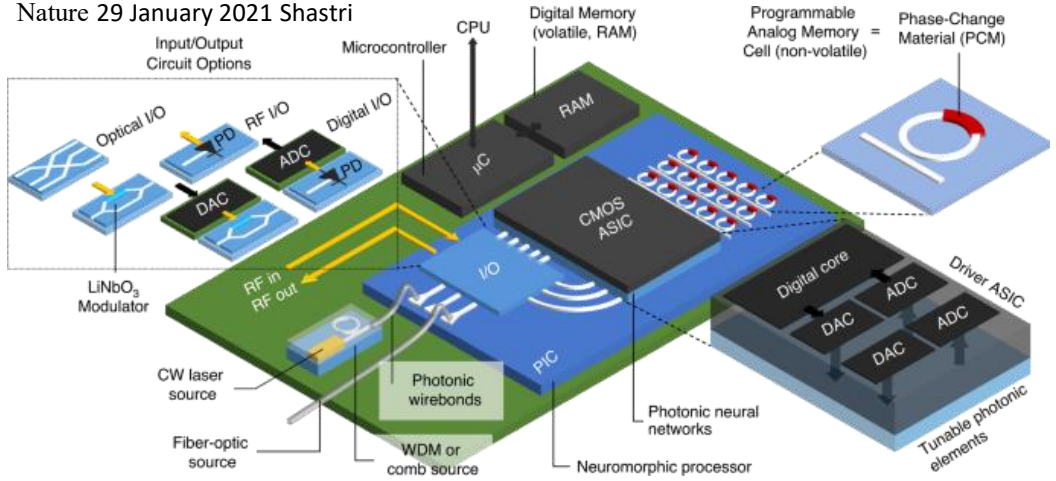


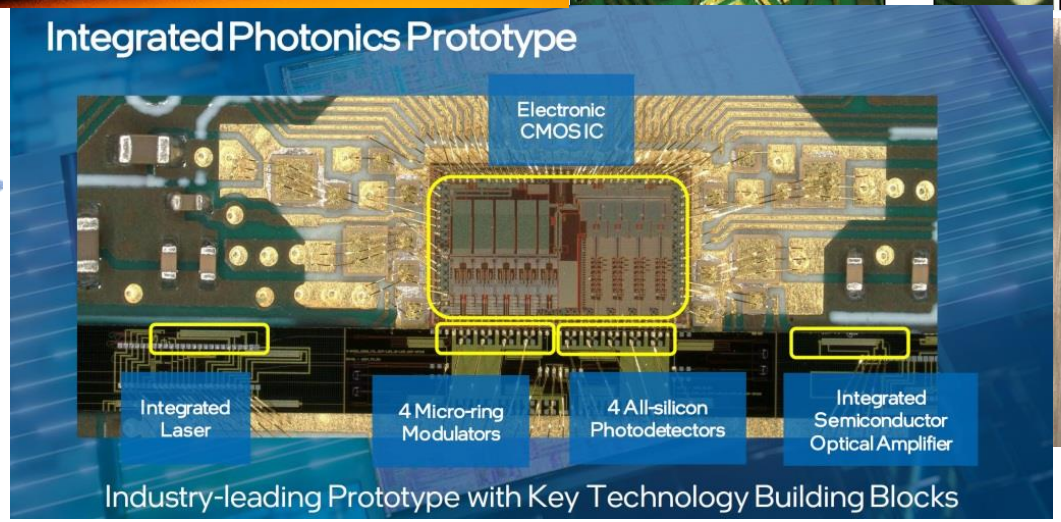
Tyndall National Institute Carroll et al

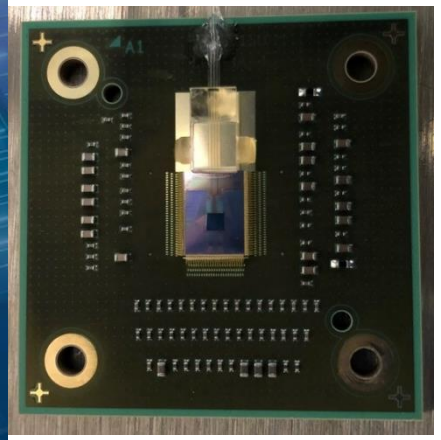




Nature 29 January 2021 Shastri



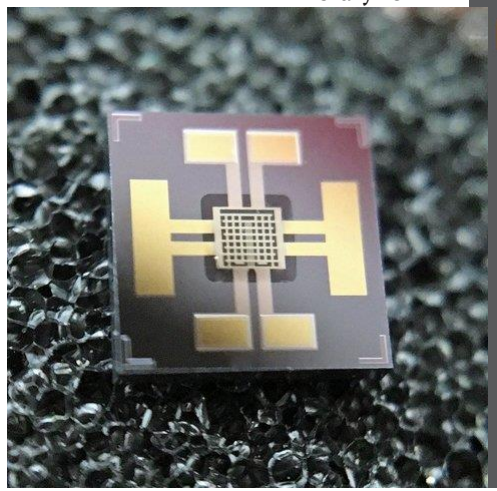


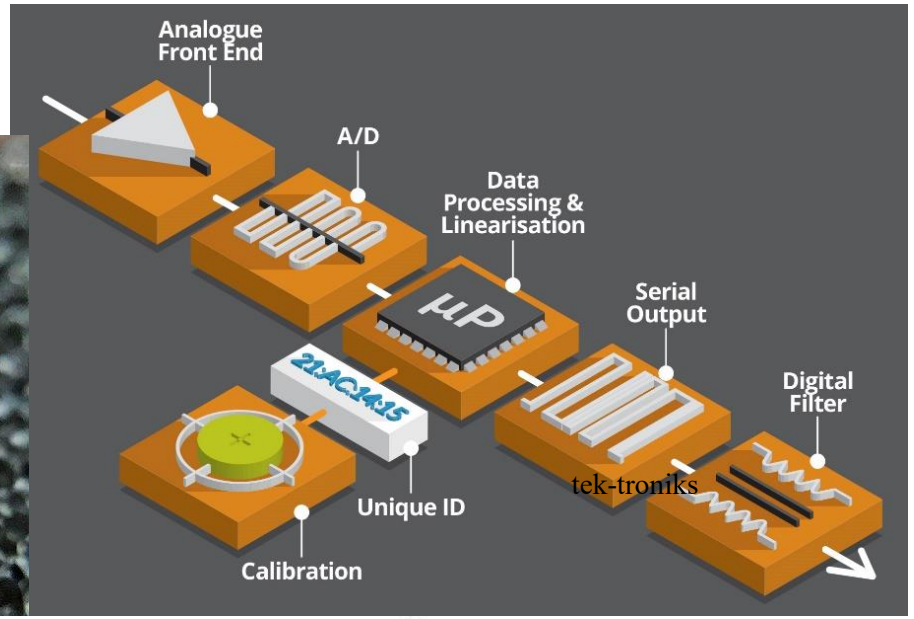


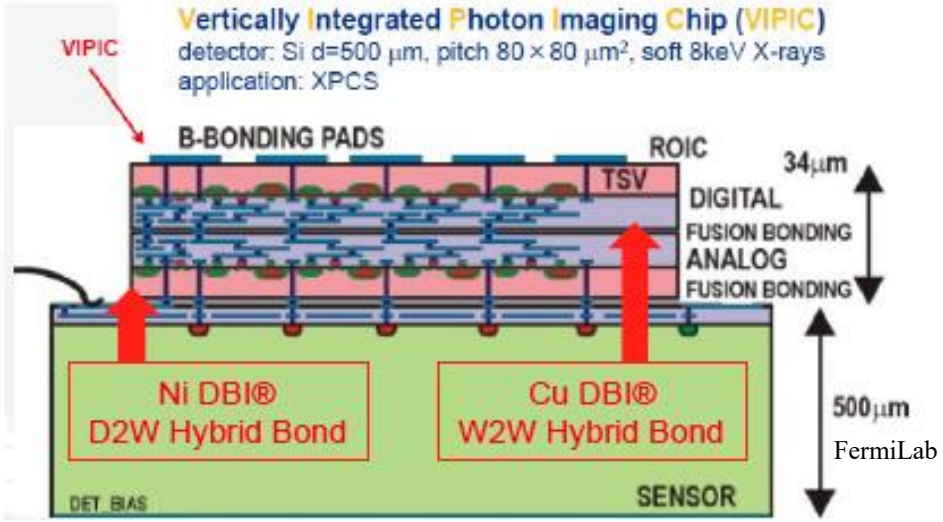
AP Market Drivers: Intelligent Sensors and Edge Compute

- Communication is limited
  - Data movement costs power
  - Data movement costs time
  - Data movement costs money
  - You can't aways "phone-home"

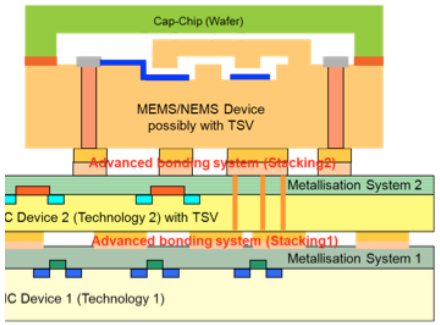
Micralyne







FermiLab



3DinCites