


NDIA Trusted Microelectronics Joint Working Group

Team 4 New Methods to Instill Trust in Semiconductor Fabrication Preliminary Report

Presented by
Dr. Pat Hays, The Boeing Company
at NDIA's 8th
Trusted Microelectronics Workshop
February 2, 2017

A solid red diagonal bar is located in the bottom left corner of the slide, extending from the bottom edge towards the right.

Team Members

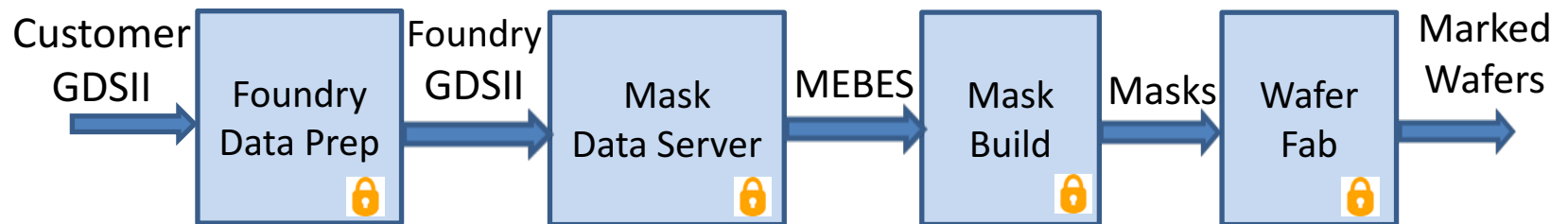


Name	Organization	Split Mask	Functional Disaggregation & Packaging	Equivalence Checking	Fab Options	New Design Approaches
John Robert Adams Elizabeth Klein-Lebbink Nick Sramek	The Aerospace Corporation		X		X	
Todd Bauer	Sandia	X (chair)				X
Greg Creech	GLC Consulting					X (chair)
Dave Davis	USAF SMC			X		
Brad Ferguson	Cypress					
Pat Hays	Boeing			X (chair)		
Robert Irie, Rob Ciccariello	MIBP					X
Sean Johnson	Intelesys			X		X
Scott Jordon	Jazz	X	X (chair)			
Steve McNeil	Xilinx			X		
Eric Miller	Boeing		X			X
John Monk	Northrop Grumman	X			X (chair)	
Mike Newman	Aeroflex (Cobham)		X		X	
Ken O'Neil, Paul Quintana	Microsemi			X		
Mark Porter	General Dynamics					
Dan Radack	IDA			X		X
Tim Scott	Novati		X		X	
John Weaver	Tectonic Labs					X
Ken Wetzel	SMI Inc.		X		X	
Ed Yarbrough, Gordy Braun, Ken Heffner	Honeywell				X	

New Methods to Instill Trust in Semiconductor Fabrication

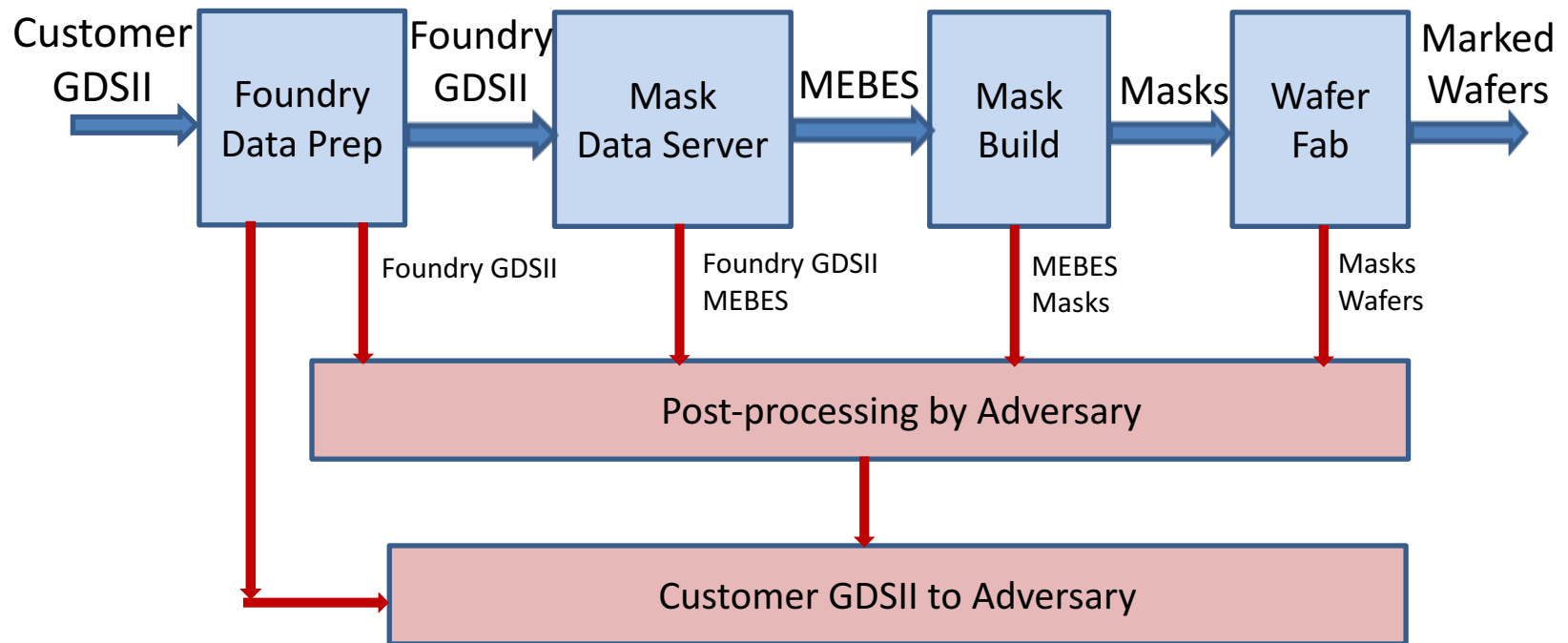
- **The Problem:** the Trusted Foundry Program Currently Does Not Support
 - Access to the most advanced process technologies
 - Access to off-shore foundries
- **The Hypothesis:** High-Tech Methods Can Instill Sufficient Trust to Enable Policy Changes That Will Solve the Above Problems *and* Further Improve Trust at Established Trusted Foundries
- **The Methodology:** Evaluate the Spectrum of Methods vs *Pragmatic* Criteria
- **The Deliverables:**
 - Present findings at GOMAC, March 20, 2017, Reno, NV
 - Recommendations Report, March 31, 2017

Semiconductor Fab – The Trusted Flow



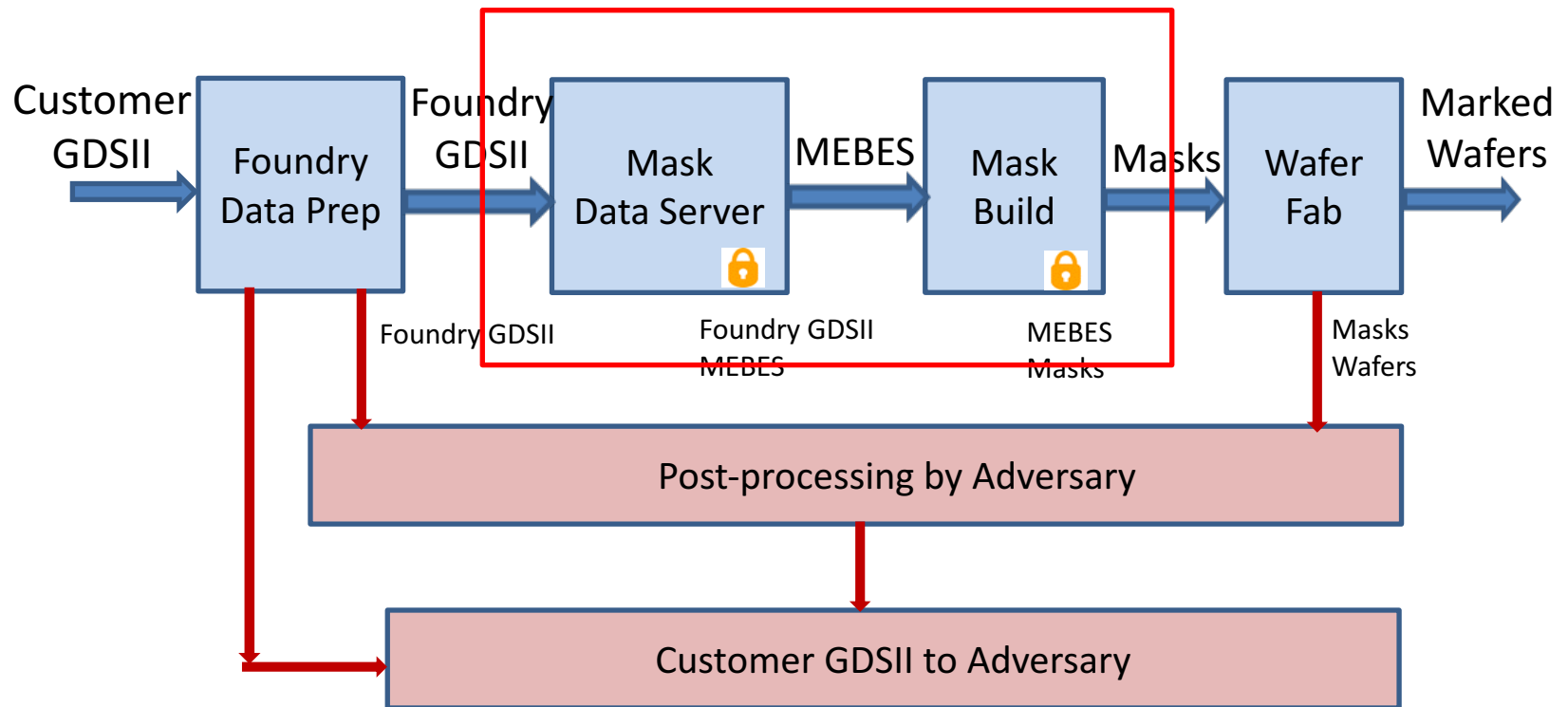
Trusted Facility

Semiconductor Fab – Vulnerabilities



The Customer Design Can be Lost At Every Stage of the Fab Process




Semiconductor Fab – Residual Vulnerabilities With Independent Trusted Mask Shop



Trusted Facility

A Couple Doors are Locked, Others are Still Open

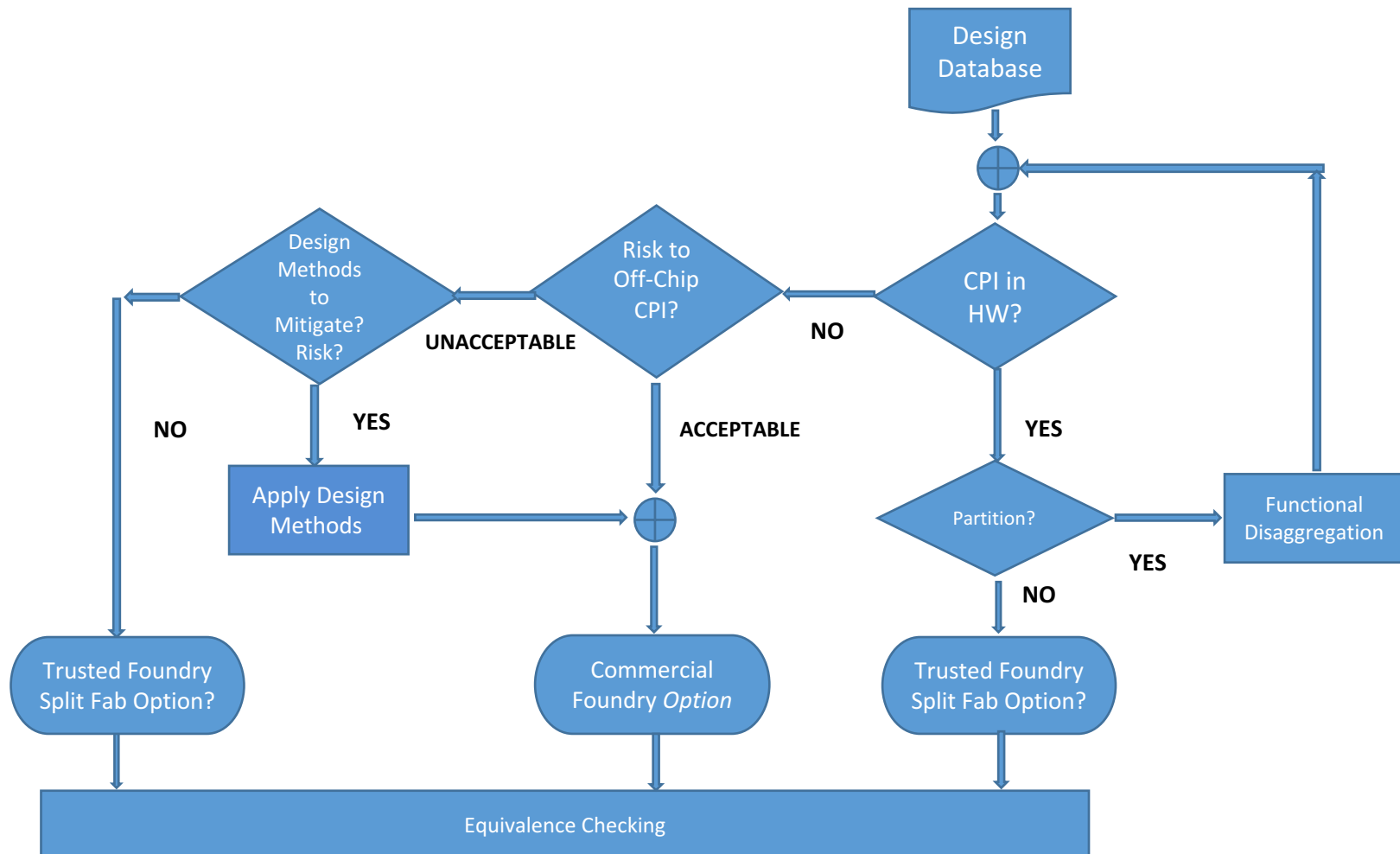
Reverse Engineering – Enabling DoD Losses

Crotale R440	Hainan Island Incident	Harpoon Missiles Sold to Pakistan
<ul style="list-style-type: none"> China developed the HQ-7 SAM system partly from reverse-engineering the Crotale in the early 1980s. Iran is believed to have developed their own variant, the Shahab Thaqeb in the early 2000s based upon the Chinese HQ-7 	<ul style="list-style-type: none"> U.S. Navy EP-3E ARIES II is forced to land after mid-air collision with a Chinese J-8II interceptor fighter. Accusations of components 'gone missing' 	<ul style="list-style-type: none"> U.S. accuses Pakistan of illegally modifying Harpoon anti-ship missiles Modification increased range and threatened India
		
<p>Counterfeiting</p> <p>Reverse engineering to enable theft of system design and/or software</p>	<p>Capability Losses</p> <p>Reverse engineering to learn capabilities, procedures, methods, equipment, intelligence and operational data</p>	<p>Malicious Tampering</p> <p>Reverse engineering to enable modification of system or software for unauthorized usage</p>

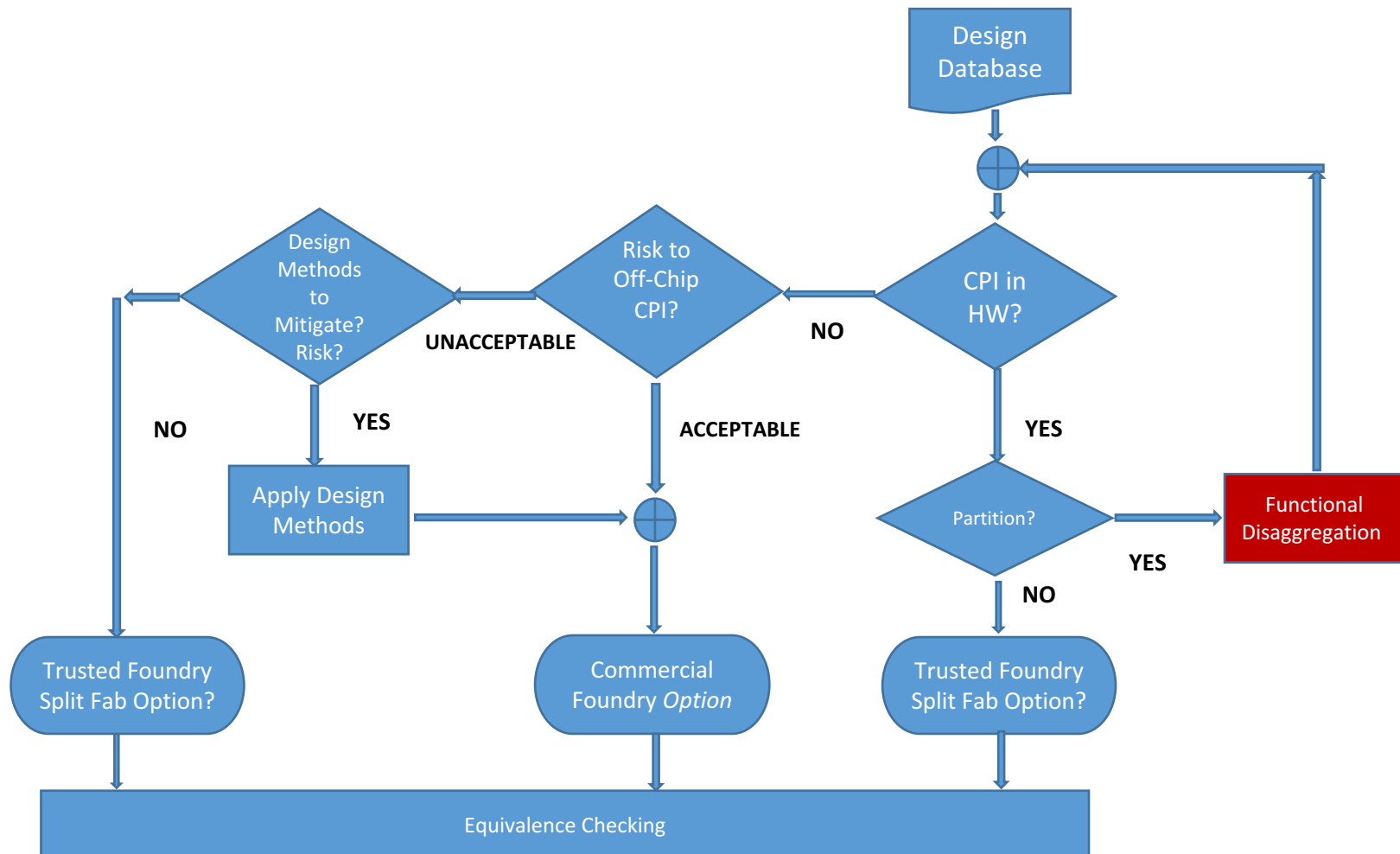
New Methods Evaluated by Team 4

- **Functional Disaggregation**
 - Partition into 2 or more dice, delimiting Trusted Foundry requirement
 - Subcommittee chair: Scott Jordan (Jazz)
- **New Design Methods**
 - Methods to prevent RE of design or RE of device functionality
 - Subcommittee chair: Gregg Creech (Ohio State University)
- **Split Fab**
 - FEOL layers and BEOL layers fab'd at different foundries
 - Subcommittee chair: Todd Bauer (Sandia)
- **Equivalence Checking**
 - Compare artifacts against customer intent
 - Subcommittee chair: Pat Hays (Boeing)

New Methods to Instill Trust – One Size Does Not Fit All



New Methods to Instill Trust – Functional Disaggregation (1/3)



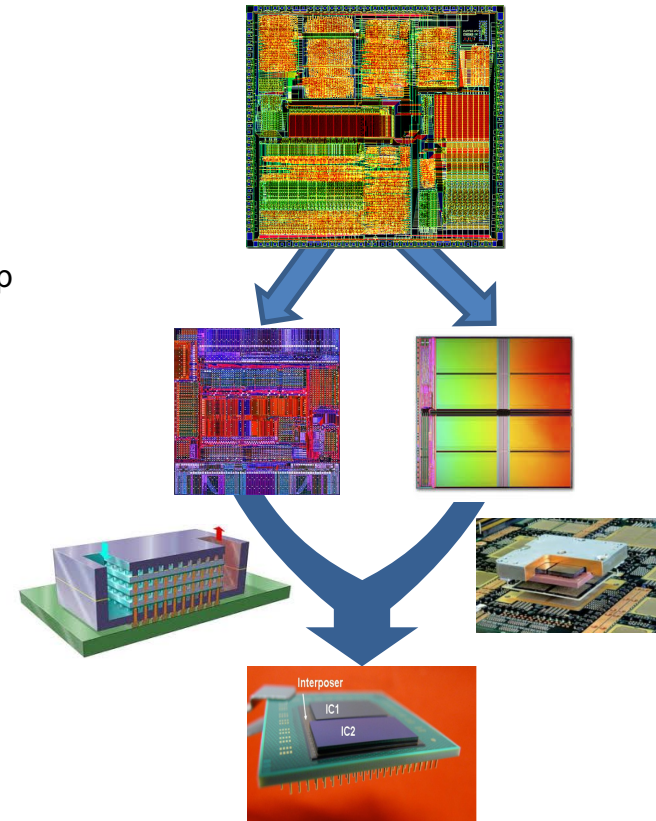
New Methods - Functional Disaggregation (FD) (2/3)

• Introduction

- An otherwise monolithic integrated circuit solution is partitioned between two or more separate elements
 - IC's within the same reticle
 - Multiple technologies and fabs
- Reassembled using connectivity fabrics such as: circuit-level, 2.5/3D integration, heterogeneous integration, advanced multichip modules, package stacking or board-level integration

• Potential Benefits

- Option A) Eliminate need for non-Trusted node
 - Achieve high level of integration without resorting to non-Trusted advanced nodes
- Option B) Partition into Trusted IC(s) and non-Trusted IC(s)
 - Most sensitive CPI is fab'd in Trusted node
 - Advanced PPA requirements in non-Trusted node
- Option C) Enable use of all non-Trusted nodes
 - Disaggregate circuit blocks to obfuscate functionality



New Methods - Functional Disaggregation (3/3)

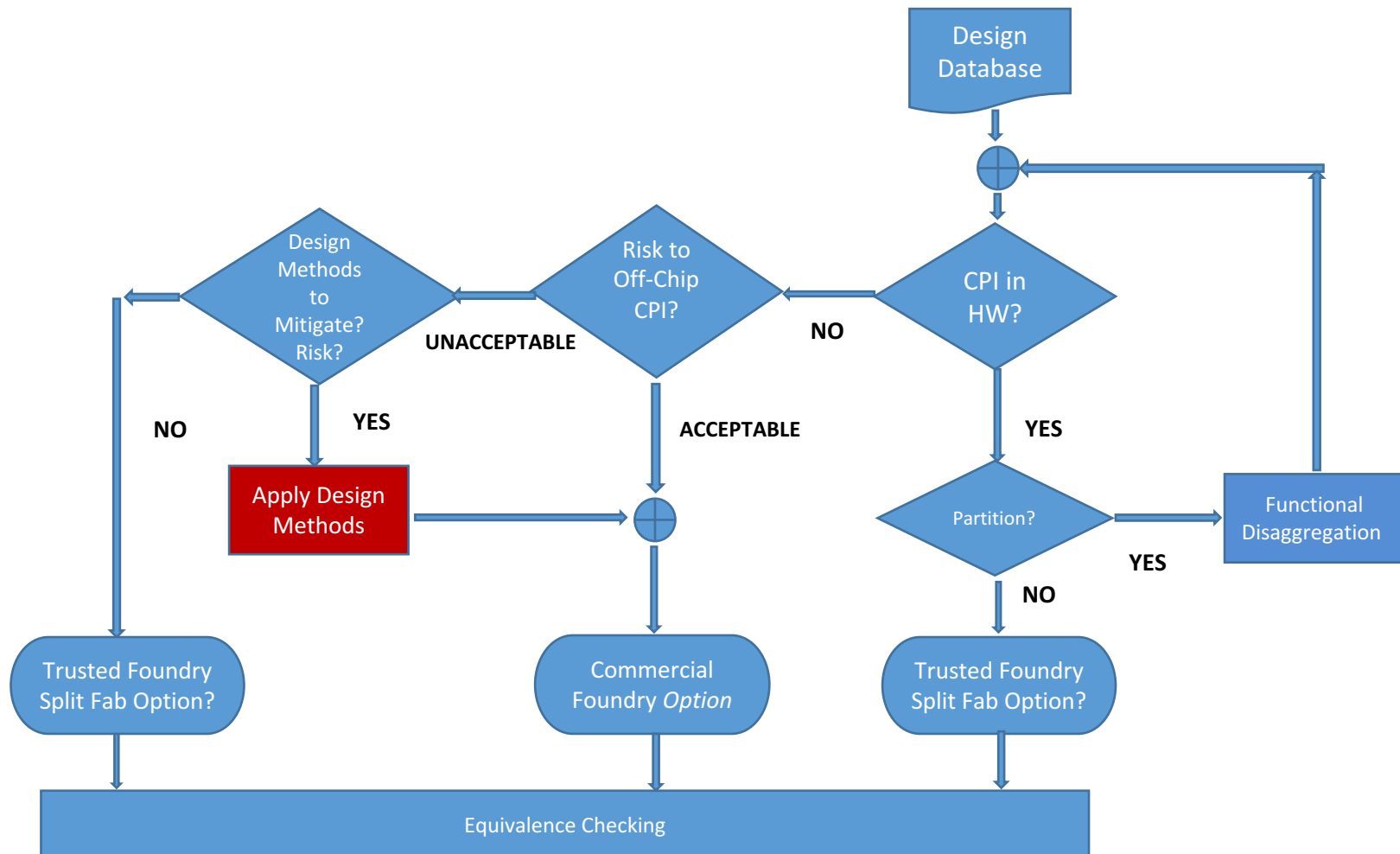
- **Challenges**

- Incremental IC and module development cost
- Interfaces may degrade performance and security
 - Exposes interfaces among dice which must be protected from passive and active monitoring attacks. Strategy: use cryptographically secure interfaces and/or sensors
- Option A – All ICs Trusted
 - Will not be feasible for the most advanced PPA requirements (i.e. designs requiring highest performance and/or lowest power and/or smallest area/footprint)
- Option B and C (additional challenges) – Some ICs non-Trusted
 - Non-Trusted IC is vulnerable to Trojans/malware. Strategy: wrap & monitor

- **Recommendation**

- Subject to the above challenges, FD is expected to have merit for many developments
- The DARPA MTO office is currently funding two programs (CHIPS and SPADE) that involve functional disaggregation. Track their findings
- Success will be design dependent. Need to develop guidelines for successful application and review

New Methods to Instill Trust – Design (1/3)



New Methods - Design (2/3)

- **Introduction**

- IC design techniques, which have emerged (or will soon emerge) from research. Several examples:
 - Circuit Obfuscation/Camouflage – modification of an IC design to hide or obscure the functional intent
 - Physical Unclonable Function (PUF) – a circuit which creates a deterministic, but process-dependent number; the number can be used as a root-of-trust in cryptographic key formation
 - Process Specific Function (PSF) – a circuit used to create a chip-unique signature in the EM spectrum

- **Potential Benefit**

- Obfuscation – penalize adversary by increasing RE time
- PUF – prevent adversary from learning the device operation even after the device RE has been successfully RE'd
- PSF – detection of malicious insertions



New Methods - Design (3/3)

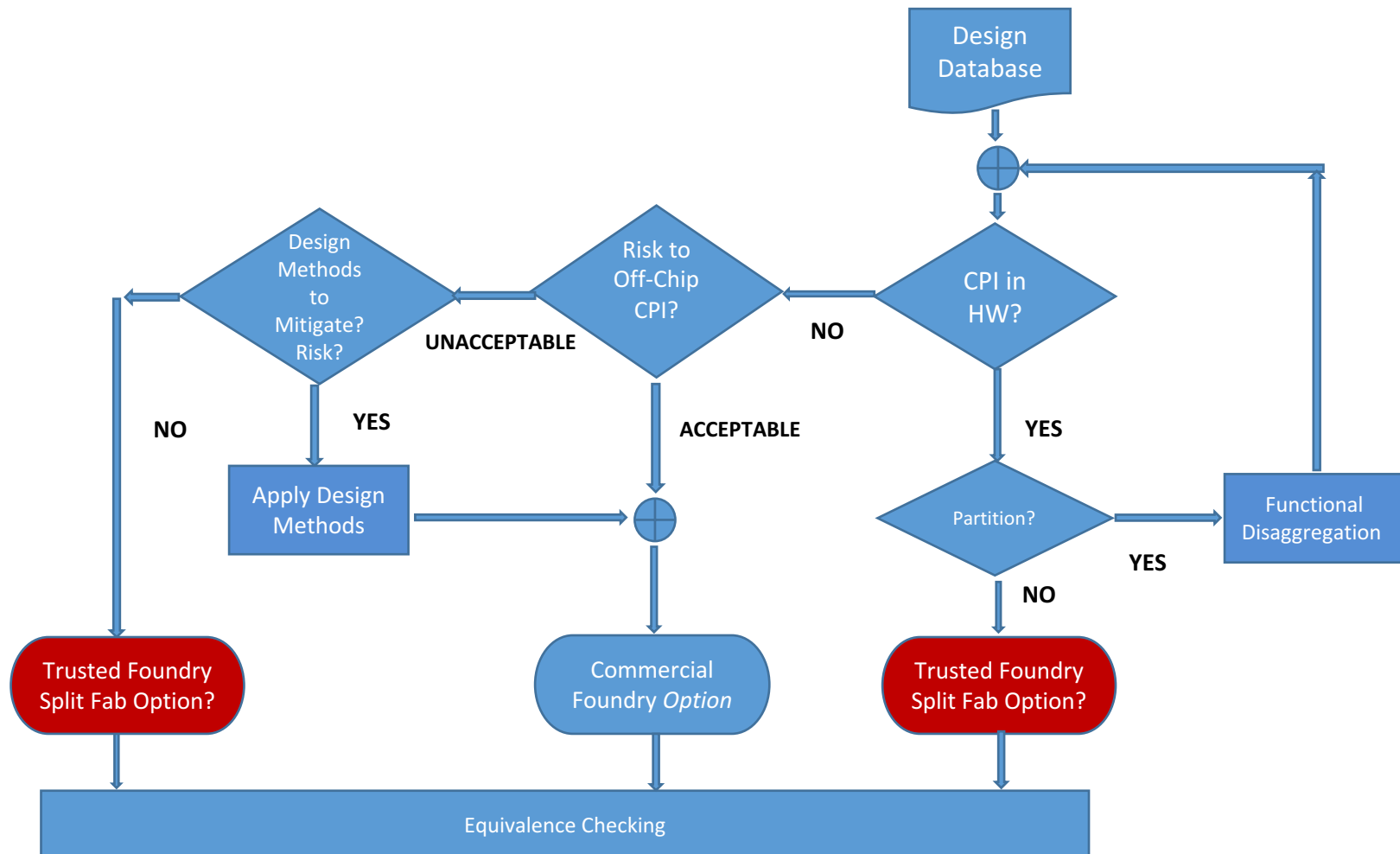
- **Challenges**

- Obfuscation – resists limited, but not advanced, RE attack
- PUF
 - The PUF number must achieve sufficient inter-chip randomness
 - The trick is to derive a stable PUF number from the process-dependent entropy source. The PUF number must be stable across temperature, voltage, noise, semiconductor ageing
 - Licensable PUFs (Intrinsic-ID, Verayo) have been applied in high volume. MicroSemi's SmartFusion2 and the latest Altera & Xilinx FPGAs integrate PUFs (Intrinsic-ID)
- PSF – not ready for prime time (Signal/noise ratio? Detection of *any* mod vs *some* mods?)

- **Recommendation**

- PUFs are practical now
- The Trust community is not sufficiently familiar with the benefits of PUFs to protect semiconductors. Recommend that guidelines and training be funded within the Trust community.

New Methods to Instill Trust – Split Fab (1/3)



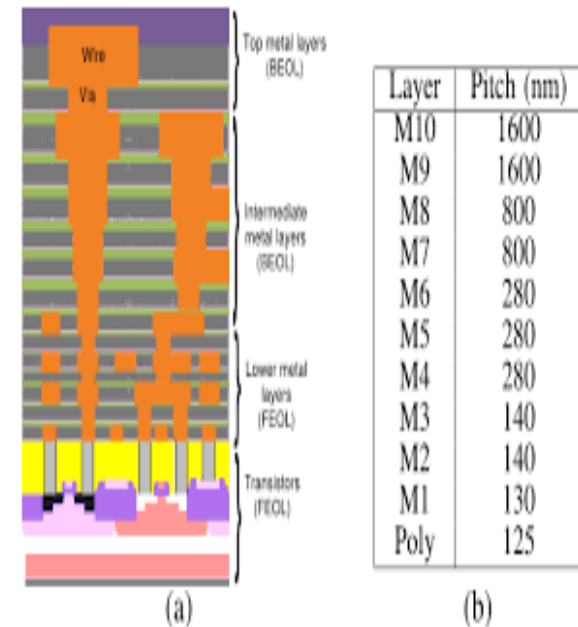
New Methods – Split Fab (2/3)

• Introduction

- Front End of Line (FEOL) processing and Back End of Line (BEOL) processing at two different fabs
- Currently the subject of the IARPA Trusted Integrated Chips (TIC) program

• Potential Benefit

- A) Both fabs are DMEA-certified Trusted Foundries
 - Can enable technical innovation. New combinations of processes, devices, materials
 - Examples: integration of Jazz SiGe FEOL with Novati's copper BEOL; introduction of aluminum nitride to build resonators, filters and transducers; RRAM integration
- B) The FEOL fab is not a Trusted Foundry
 - Open trusted access to advanced process nodes because the BEOL layers and design intent is not shared with the non-Trusted FEOL fab



New Methods – Split Fab (3/3)

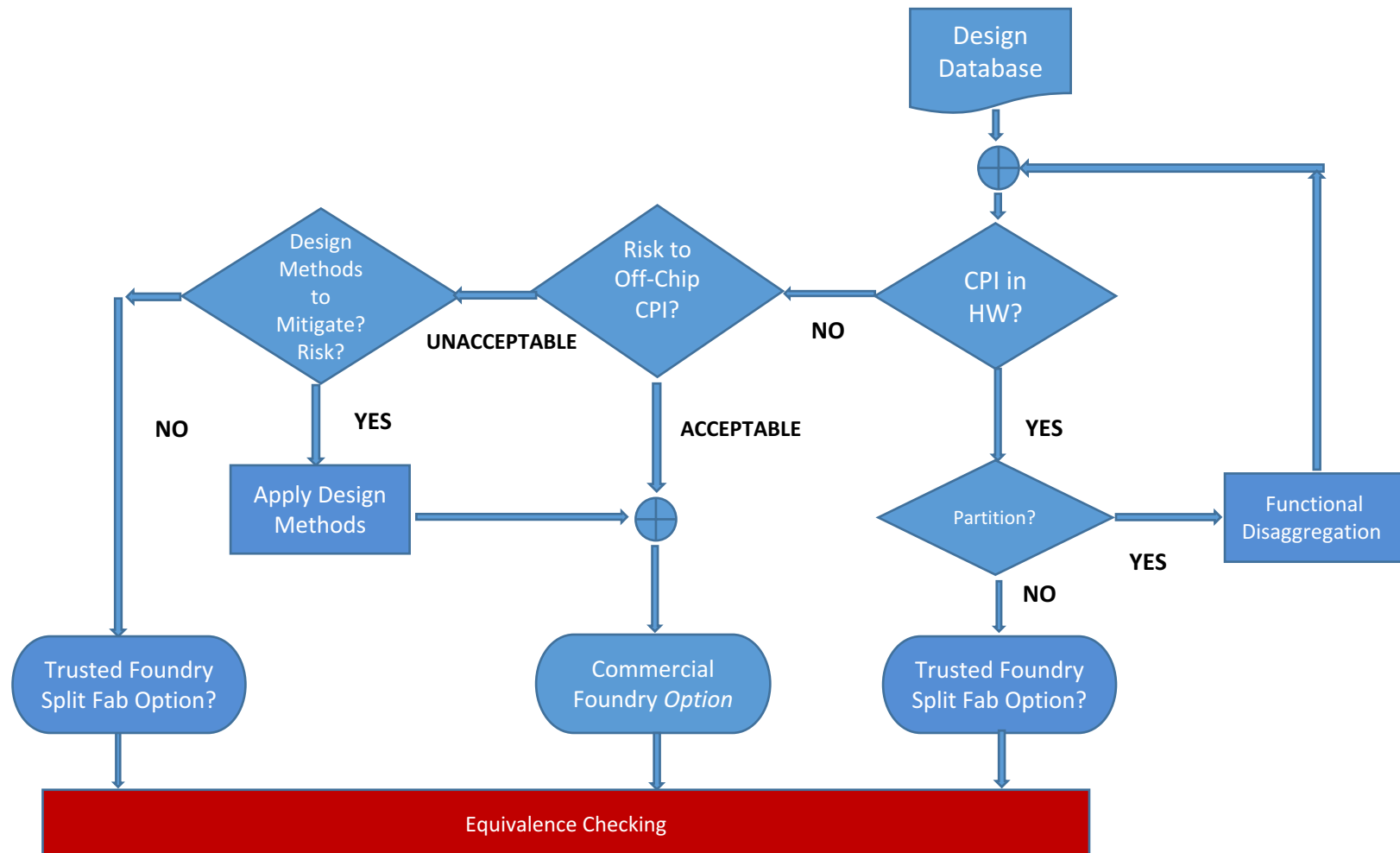
- **Challenges**

- Each FEOL/BEOL combination is, in effect, a new process node; creating both technical and business challenges
- Technical Challenges
 - Customers require production-qualified EDA flows, design kits and physical IP (SERDES, memories, cell libraries, etc) and reliability.
 - Lithography challenges – compatible mask alignment, registration, etc. (generally requires sharing process information)
 - Material compatibility – thermal stress, adhesion, etc.
 - Can a trailing edge BEOL be built on top of an advanced FEOL?
 - Can the above challenges be mitigated if the BEOL matches the FEOL fab's BEOL?
- Business Challenges
 - Financial investment, as required to overcome the above challenges
 - Legal agreements to enable sharing sensitive information between fabs

- **Recommendation**

- No visible near-term likelihood for Option B (advanced, non-Trusted FEOL; trailing, Trusted BEOL)
- Option A (both foundries, Trusted) may open specialized technical capabilities (not Trust-related) for trailing edge customers within the DMEA Trusted Foundry program

New Methods to Instill Trust – Equivalence Checking (1/3)



New Methods – Equivalence Checking (2/3)

- **Introduction**

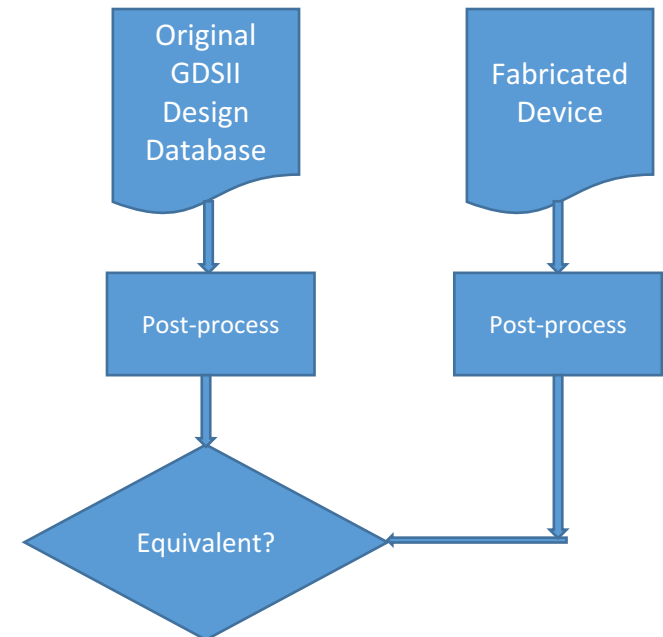
- The tapeout GDSII database is compared to the fabricated semiconductor device. The GDSII and/or device are post-processed to enable comparison.

- **Potential Benefit**

- Reduce risk of malicious insertion during fabrication

- **Equivalence Checking Techniques**

- Trojan detection techniques – research stage
 - Digital watermarking. (Straightforward for protection of SW, FPGA bitfiles, Soft IP)
 - Path delay analysis
 - Electromagnetic (EM) signatures
- Verification of correctness – research stage
- Defensive delaying – costly but workable



New Methods – Equivalence Checking (3/3)

- **Status & Challenges – Defensive Delaying**

- Top layers are delayed with CMP; lower layers with Ga+ FIB
- As each layer is exposed its SEM-imaged; key is image repair software
- At 14nm, typically ~5 samples are required, but netlists been reconstructed with a single sample
- As a defensive strategy, only reconstruction and compare of individual layers is required
- Cost estimate: ~\$200K for a 5mm x 5mm 14nm die
- Challenges:
 - Sampling strategy: per-wafer-lot? per-wafer?
 - Cost reduction
 - Trust in the delaying service

- **Recommendation**

- Application of defensive delaying in sensitive programs
- Continued development to reduce delaying cost and potentially enable per-chip equivalence checking

Recommendations - Preliminary

- New Methods have the potential *in some cases*, to instill a sufficient degree of trust in semiconductor fabs which are currently outside the DMEA Trusted Foundry program.
- Exploiting this potential will require investments, as recommended in this presentation, to ensure robustness of the most promising methods
- **One size does not fit all !**
 - DoDI 5200.44 should be modified to create “Trust Levels” which are defined by attack vulnerability, rather than by required implementation
 - Acceptability of an ASIC together with its foundry strategy vs the required Trust Level will be design-specific, dependent on how successfully the New Methods can be applied
 - The pragmatic approach to determining Acceptability is to establish a documentation and review process under DoDI 5200.44
- These recommendations will be further specified in the Team 4 final report