# LEVERAGING THE COMMERCIAL SECTOR AND PROVIDING DIFFERENTIATION THROUGH FUNCTIONAL DISAGGREGATION

Dr. Daniel S. Green, DARPA/MTO Program Manager

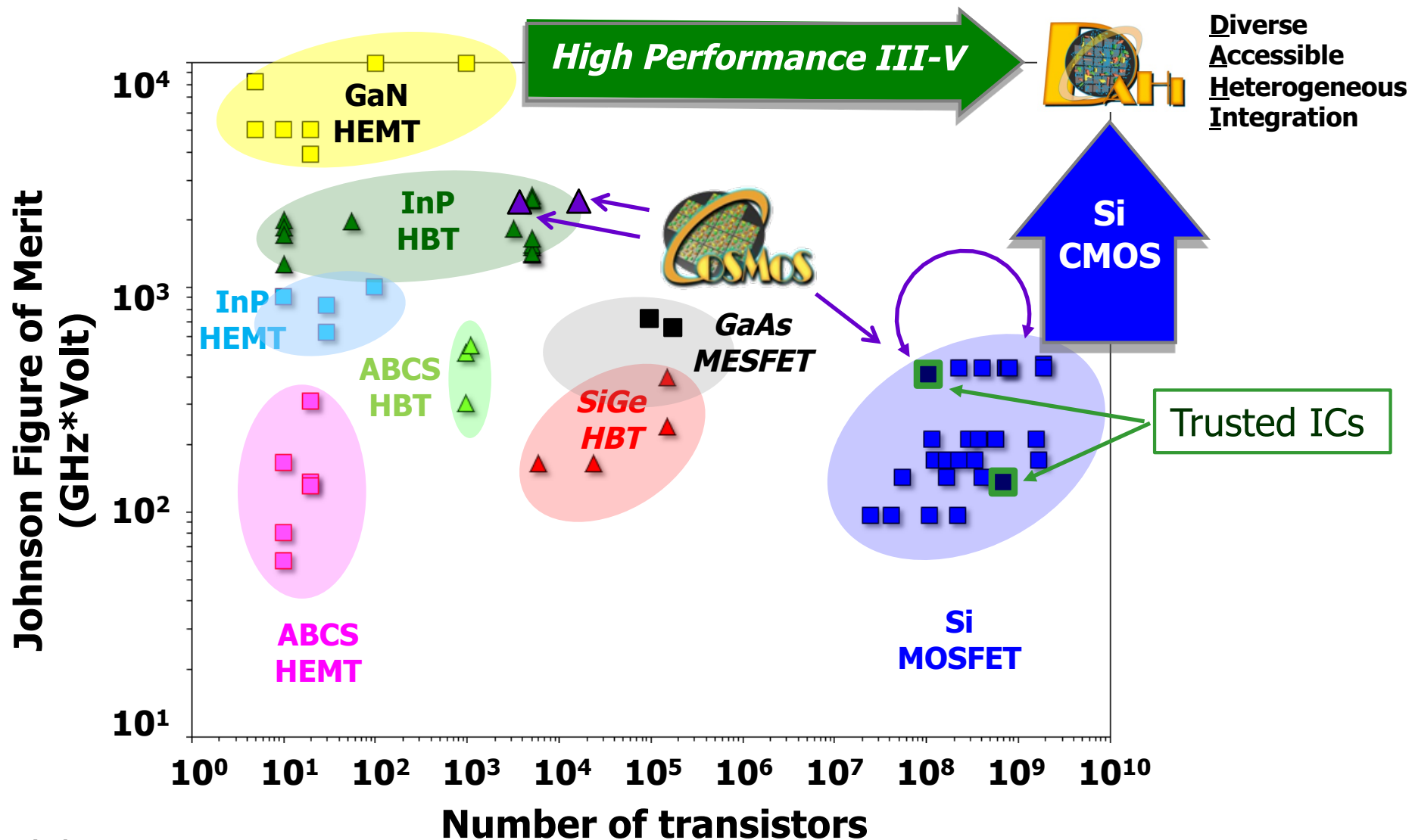NDIA Trusted Microelectronics Workshop

August 17, 2016

# The DARPA solution is to provide a menu of hardware security options that can be selectively applied based on need

|  | | Protection | Program | Microelectronics Security Threats | | | | |
|---|---|---|---|---|---|---|---|---|
|  | | | | Loss of information | Fraudulent products | Loss of access | Malicious insertion | Quality and reliability |
| High Government Intervention | | Government-proprietary | Other | ● | | | | |
| | | Fine Disaggregation and Transience | TIC (IARPA) | ● | ● | ● | ● | |
| | | | VAPR | ● | | | | |
| | | Functional Disaggregation | SPADE | ● | | | ● | ● |
| | | | DAHI | ● | | ● | ● | |
| | | | CHIPS | ● | | ● | ● | ● |
| High Commercial Sponsorship | | Obscuration and Marking | CRAFT | | | ● | | ● |
| | | | eFuses | ● | | | ● | |
| | | | SHIELD | ● | ● | | | |
| | | Verification and Validation | IRIS | | ● | | ● | ● |
| | | | TRUST | | ● | | ● | |

**DAHI and CHIPS can help protect against the malicious introduction of unknown functionalities into ASIC products.**

# Heterogeneous integration:
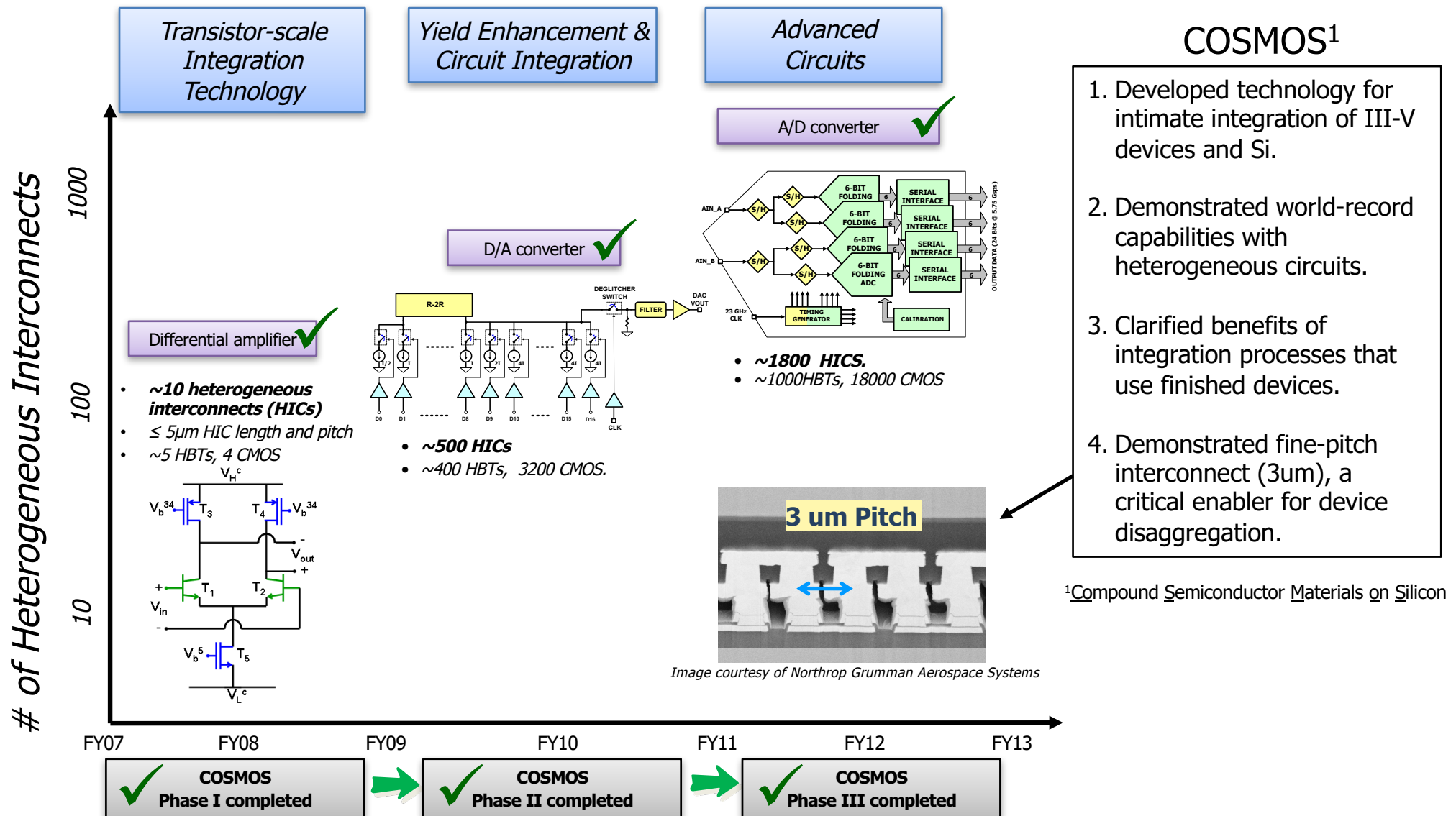## Broadens the device material options



**Johnson Figure of Merit (GHz*Volt)** vs **Number of transistors**

High Performance III-V

GaN HEMT

InP HBT

InP HEMT

ABCS HBT

SiGe HBT

GaAs MESFET

ABCS HEMT

Si MOSFET

Si CMOS

COSMOS

Diverse Accessible Heterogeneous Integration

Trusted ICs

**Terminology:**
InP = indium phosphide, GaN = gallium nitride, SiGe = silicon germanium, ABCS = antimonide-based compound semiconductor
HBT = heterojunction bipolar transistor, HEMT = high electron mobility transistor, CMOS = complementary metal oxide semiconductor
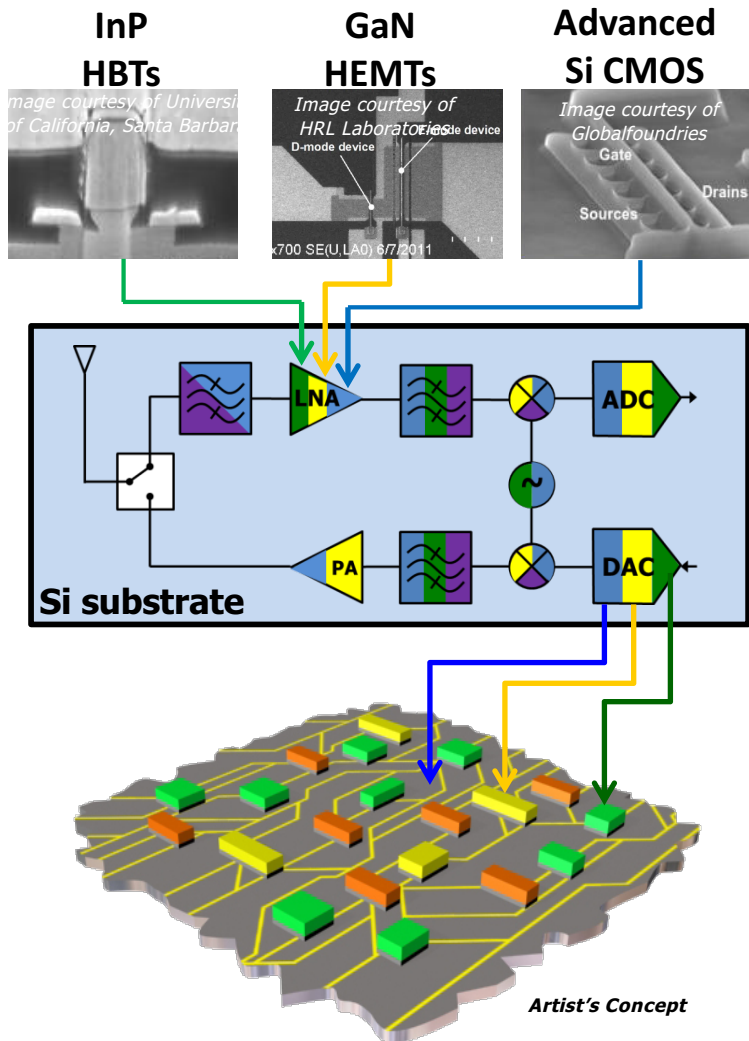COSMOS = Compound Semiconductor Materials on Silicon

# COSMOS program showed the promise of heterogeneous integration

**# of Heterogeneous Interconnects** (y-axis: 10, 100, 1000)

Transistor-scale Integration Technology

Yield Enhancement & Circuit Integration

Advanced Circuits

A/D converter ✔

D/A converter ✔

Differential amplifier ✔

- **~10 heterogeneous interconnects (HICs)**
- ≤ 5μm HIC length and pitch
- ~5 HBTs, 4 CMOS

- **~500 HICs**
- ~400 HBTs, 3200 CMOS.

- **~1800 HICS.**
- ~1000HBTs, 18000 CMOS

**3 um Pitch**

*Image courtesy of Northrop Grumman Aerospace Systems*

## COSMOS[1]

1. Developed technology for intimate integration of III-V devices and Si.

2. Demonstrated world-record capabilities with heterogeneous circuits.

3. Clarified benefits of integration processes that use finished devices.

4. Demonstrated fine-pitch interconnect (3um), a critical enabler for device disaggregation.

[1]Compound Semiconductor Materials on Silicon

(x-axis: FY07, FY08, FY09, FY10, FY11, FY12, FY13)

✔ COSMOS Phase I completed → ✔ COSMOS Phase II completed → ✔ COSMOS Phase III completed

**COSMOS:** Demonstrated benefits of integration of **completed** devices

# Diverse Accessible Heterogeneous Integration (DAHI) foundry for heterogeneous integration

**InP HBTs**

Image courtesy of University of California, Santa Barbara

**GaN HEMTs**

Image courtesy of HRL Laboratories
D-mode device    E-mode device
x700 SE(U,LA0) 6/7/2011

**Advanced Si CMOS**

Image courtesy of Globalfoundries
Gate
Drains
Sources

**Si substrate**

LNA — ADC
PA — DAC

**Heterogeneous technology integration in accessible foundry**



65 nm IBM CMOS Wafer

InP HBT Chiplets

GaN HEMT Chiplets
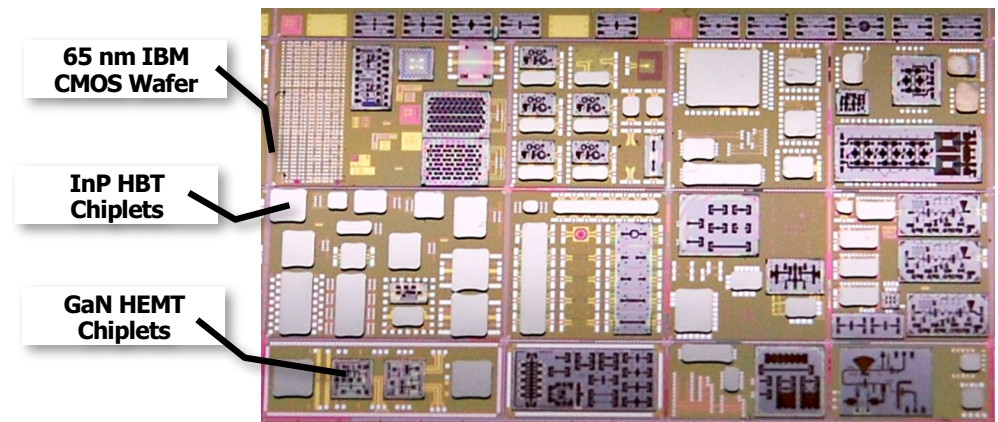
*(first three-technology integration demonstrated in Jan 2015)*
*Image courtesy of Northrop Grumman Aerospace Systems*

*Artist's Concept*

Heterogeneous Integration of a diverse array of devices on a common Si CMOS platform

*Goal:* To establish a versatile platform of heterogeneous integration that enables pervasive impact on DoD systems

# DAHI MPW0 CMOS + InP HBT + GaN HEMT demonstration



**65 nm IBM CMOS Wafer**

**InP HBT Chiplets**

**GaN HEMT Chiplets**

Team 1 · Yield TV · Team 4 · Team 7 · Team 1 · Team 5 · Team 8 · Calibration · Team 2 · Team 3 · Team 6 · Team 9
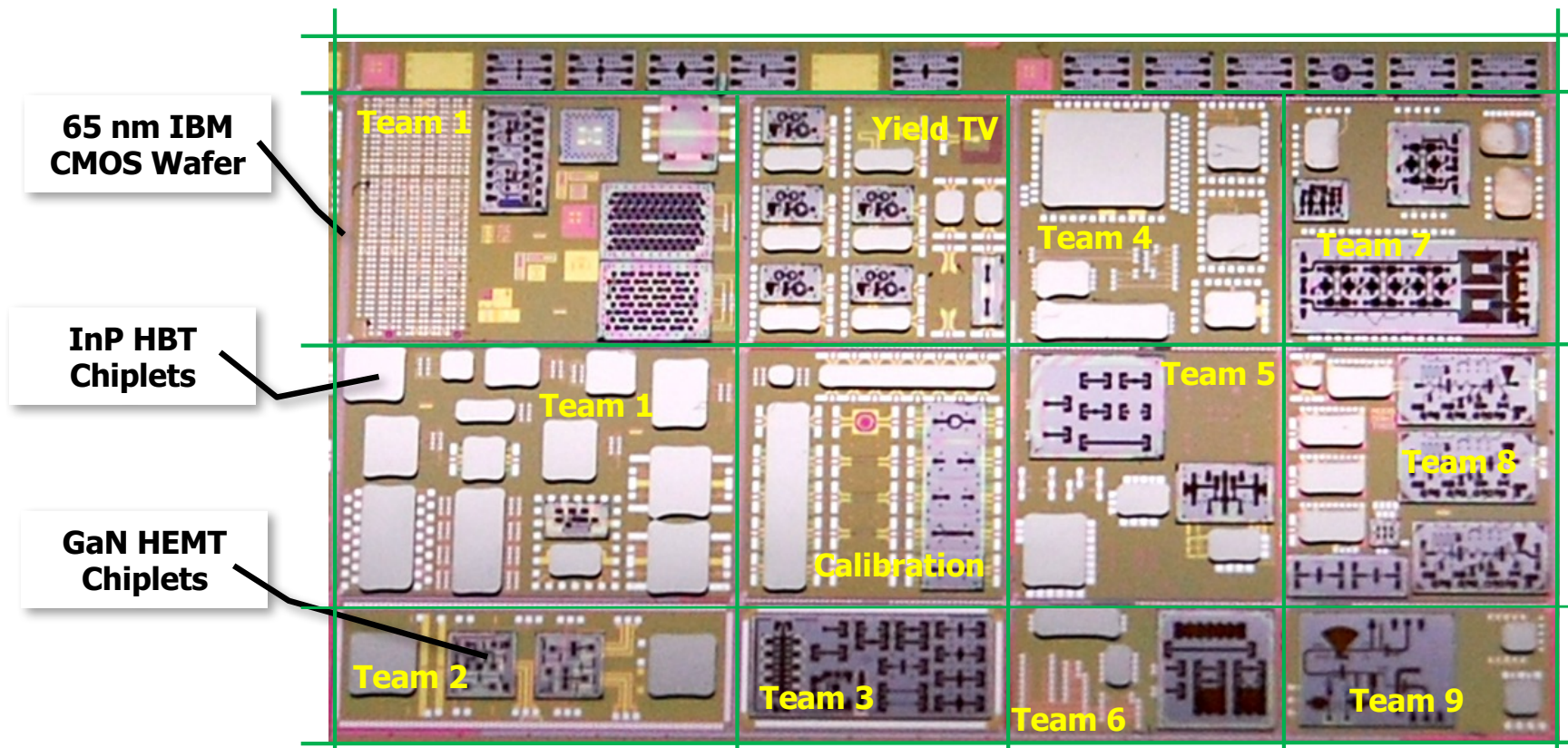
*(3 technology integration demonstrated in Jan 2015)*
*Image courtesy of Northrop Grumman Aerospace Systems*

## Successful integration of high performance III-V technologies with CMOS

**GlobalFoundries**
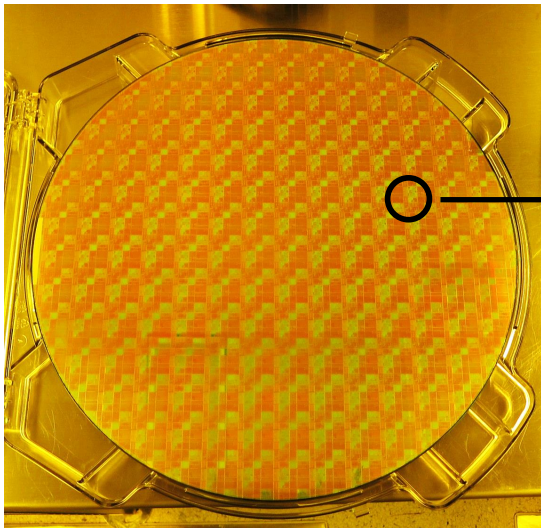
**Northrop Grumman**



300mm diameter Si CMOS wafer (45nm node)
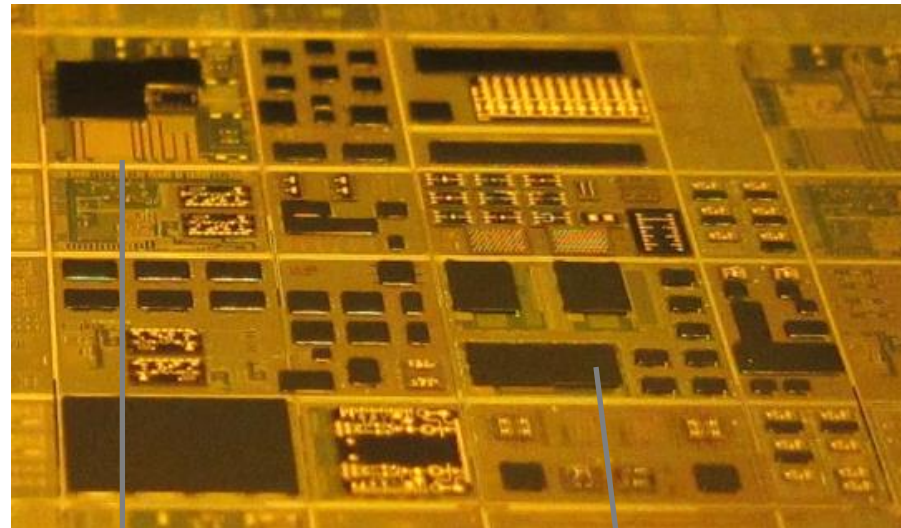
DAHI integration (Dec 2015): Si (45nm), InP (TF5 HBT), GaN (GaN20 HEMT)

**Northrop Grumman**

**BAE Systems**

**Teledyne**



99.94% HIC yield
98% HBT post-integration
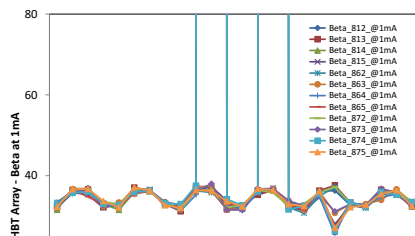
High foundry integration yields; test vehicles fully functional

$f_{OUT}$ 2.9 GHz

Output Spectrum

(noise floor ~ -75 dBm)
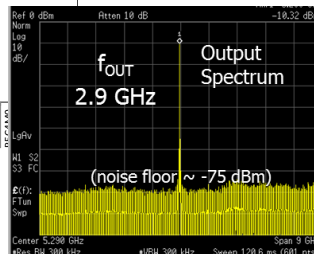
DAC with very low digital noise (-70dBc)
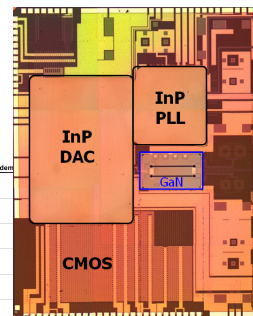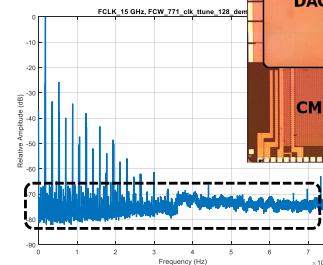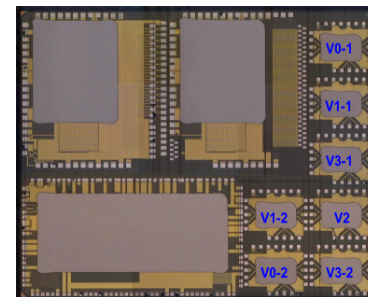
Successful testing identified optimal S/H circuit for ADC (>65dB SFDR @ 2GHz)

# Integration approach - disaggregation

**IBM**

MPW0: **65nm**
MPW1: **45nm**
MPW2: **45nm**

Standard CMOS fabrication → HIC Interface deposition → **CMOS wafer with HICs ready for integration**

**NGAS**

Standard GaN20 fabrication → Thinning / backside via etching → Backside metal deposition → Integration →

**HRL**

Standard T-3 fabrication → Thinning / backside via etching → Backside metal deposition → Integration →

**CMOS wafer with integrated GaN chiplets**

**NGAS**

Standard TF4/TF5 InP HBT fabrication → Thinning → Singulation and integration →

**CMOS wafer with integrated InP and GaN chiplets**

Nuvotronics

High-Q Passives standard process → Mechanical Integration

- Obfuscation - Disaggregation of circuit into multiple chiplets conceals total circuit design/performance – circuit design is compartmentalized by technology
- Anti-tamper - Tampering with individual chiplets complicated by lack of knowledge of overall circuit
- Minimizes semiconductor process change

Too much of a good thing is wonderful…

1. Silicon Carbide Interposer
   a. Better thermal conductivity
   b. Better thermal expansion mismatch
   c. Design/process studies underway
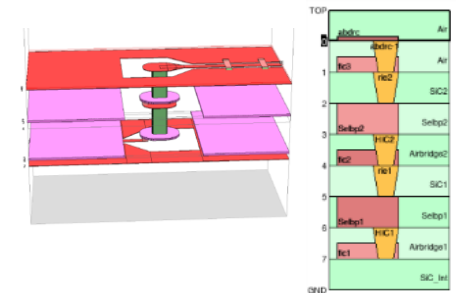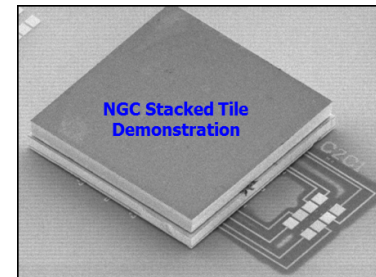   d. Pathfinder lots in process
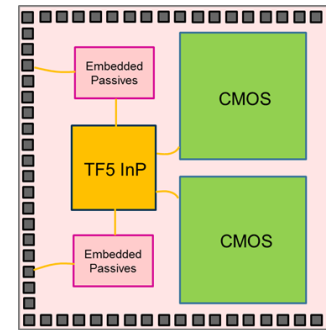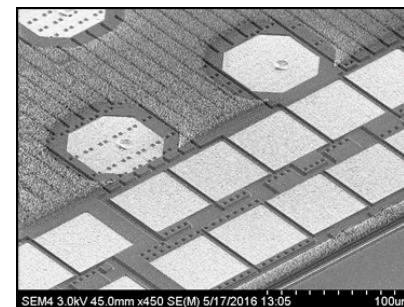


BAE SiC Interposer #5
11.5 x 11.5 mm
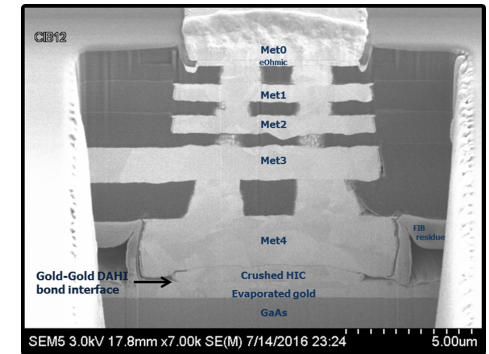


2. Chiplet Stacking
   a. Process demonstrations, design rule development underway
   b. RF transition modeling in process



3. COTS CMOS Tile Processing
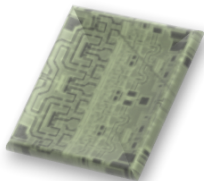   a. Developing handling tools and preparation processes



*Images courtesy of Northrop Grumman*
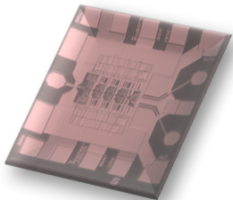
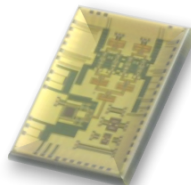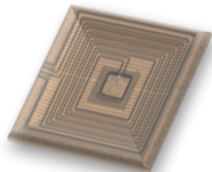**Chiplet process modules designed with IP re-use in mind**

GaN

VLSI Si

InP

SiGe

Passives

GaAs, MEMS, etc.

- Develop a pre-defined "common" interposer (SiC/Si/Glass) platform
- Populate common platform with library of chiplets of IP/circuit blocks
- Different complex configurations can be formed rapidly with reusable IP blocks/chiplets

Minimized NRE for rapid system prototyping

Design 1

Design 2

*Image courtesy of Northrop Grumman*

**3 um Pitch**

Example interconnect
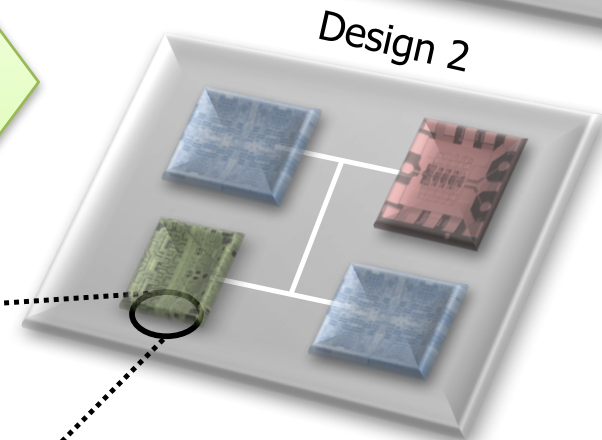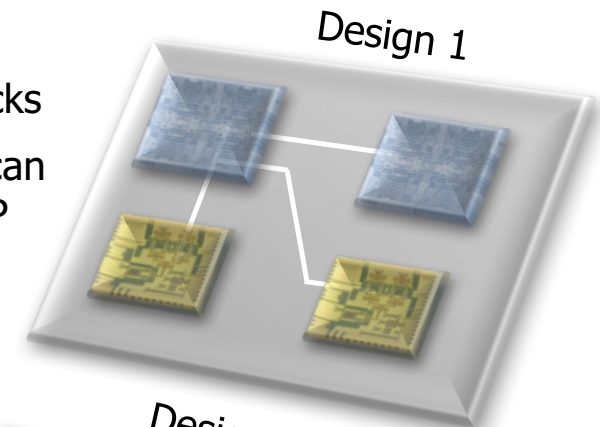
**DAHI-enabled integration technology plus IP re-use ecosystem to speed the design cycle and reduce the access cost**
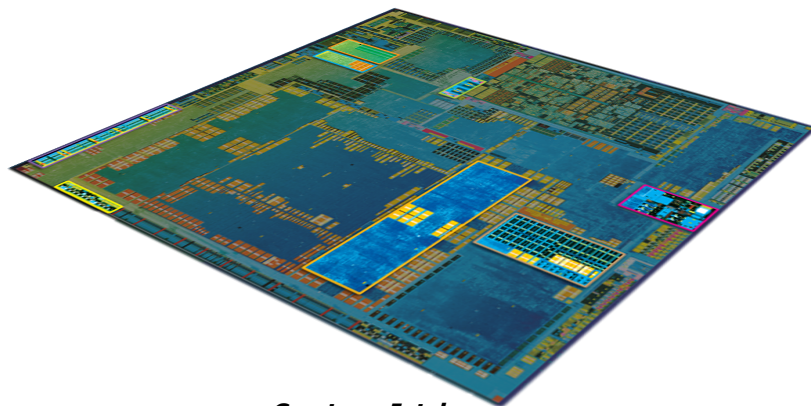
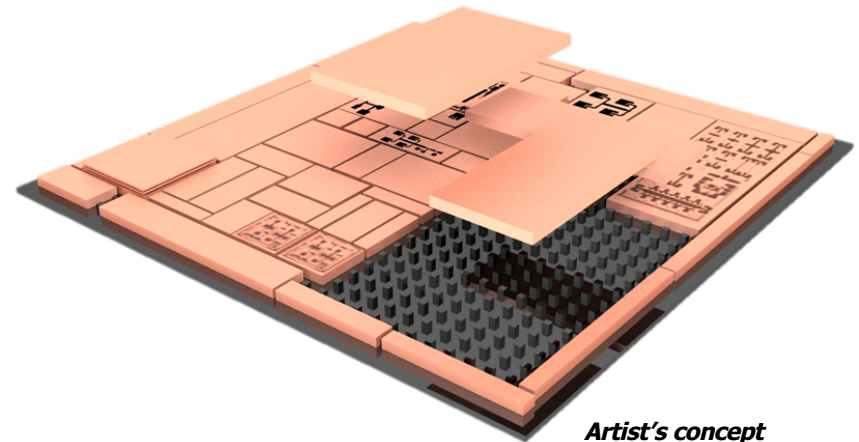*Common Heterogeneous integration and IP reuse Strategies program*

CHIPS will develop the **design tools and integration standards** required to demonstrate **modular electronic systems** that can leverage **the best of DoD and commercial** designs and technology.

### Today – Monolithic

### Tomorrow – Modular



*Courtesy: Intel*



*Artist's concept*

# What will CHIPS do?

Custom chiplets          Commercial chiplets

**COMM**          **RADAR EW**          **SIGINT**

*Artist's concept*
*Video not included here*

| | Adaptive filter | | SerDes | | SerDes |
|---|---|---|---|---|---|
| | Beam forming | | Beam forming | | Adaptive filter |
| | QR Decomp. | | QR Decomp. | | QR Decomp. |
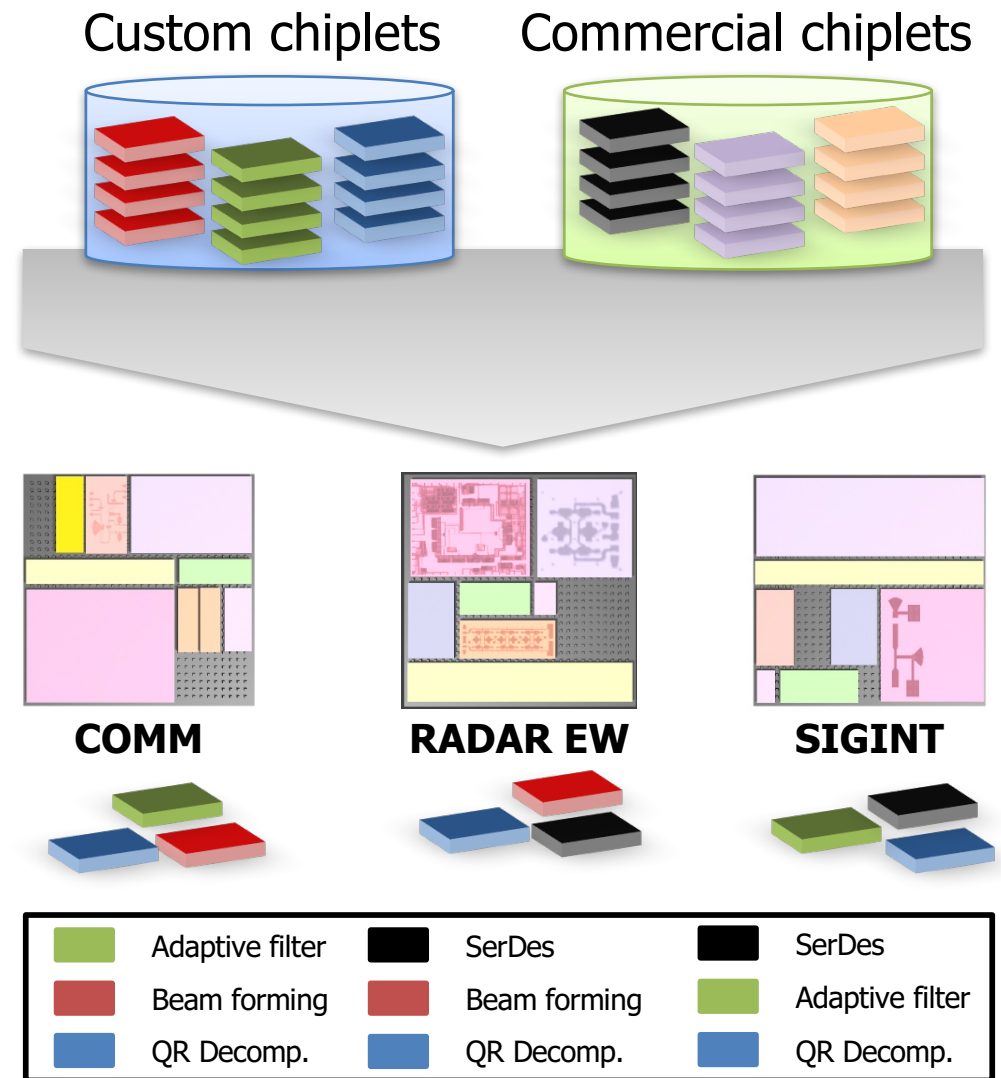
## CHIPS enables rapid integration of functional blocks at the chiplet level

# CHIPS impact on DoD electronics

Courtesy: Aitech

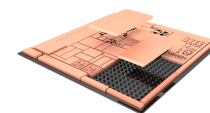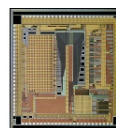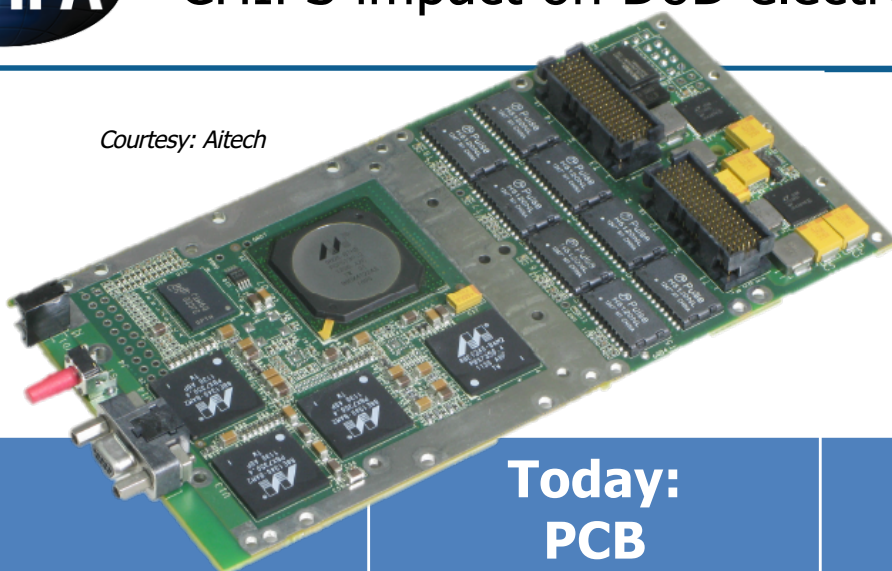| | Today: PCB | Today: Monolithic | Tomorrow: CHIPS |
|---|---|---|---|
| Cost (NRE) | $0.1's M | $5-10 M | ~$2 M |
| Schedule | 2 months | 21 months | 7 months |
| Modularity | Board-level | No | Die-level |
| IP Availability | COTS universe (packaged ICs) | Process node and vendor constrained | COTS and DoD pre-verified chiplets |
| Performance | Low | High | High |
| Heterogeneous Integration | Yes, within COTS universe | No | Yes |

**CHIPS is projected to reduce IC design to one-third cost and time**

# CHIPS metrics (preliminary)

### Design Level

| Parameter | Value |
|---|---|
| IP reuse (%) | > 50% public[1] IP blocks |
| Modular design (%) | > 80% reused[2] IP |
| Access to IP | > 3 sources[3] of IP |
| Heterogeneous integration | > 3 technologies[4] |

### Digital Interfaces

| Parameter | Value |
|---|---|
| Data rate (scalable)[5] | 10 Gbps |
| Energy efficiency[6] | < 5 pJ/bit |
| Latency[6] | ? 5 nsec |

### Analog Interfaces

| Parameter | Value |
|---|---|
| Insertion loss (across full bandwidth) | < 1 dB |
| Bandwidth | ? 50 GHz |

---

[1] Public IP is defined as IP blocks available through commercial vendors or available to DoD community.
[2] Reuse is defined as existing or previously designed IP that is re-implemented into the current system.
[3] For RFI purposes, any business unit would be considered a single source of IP.
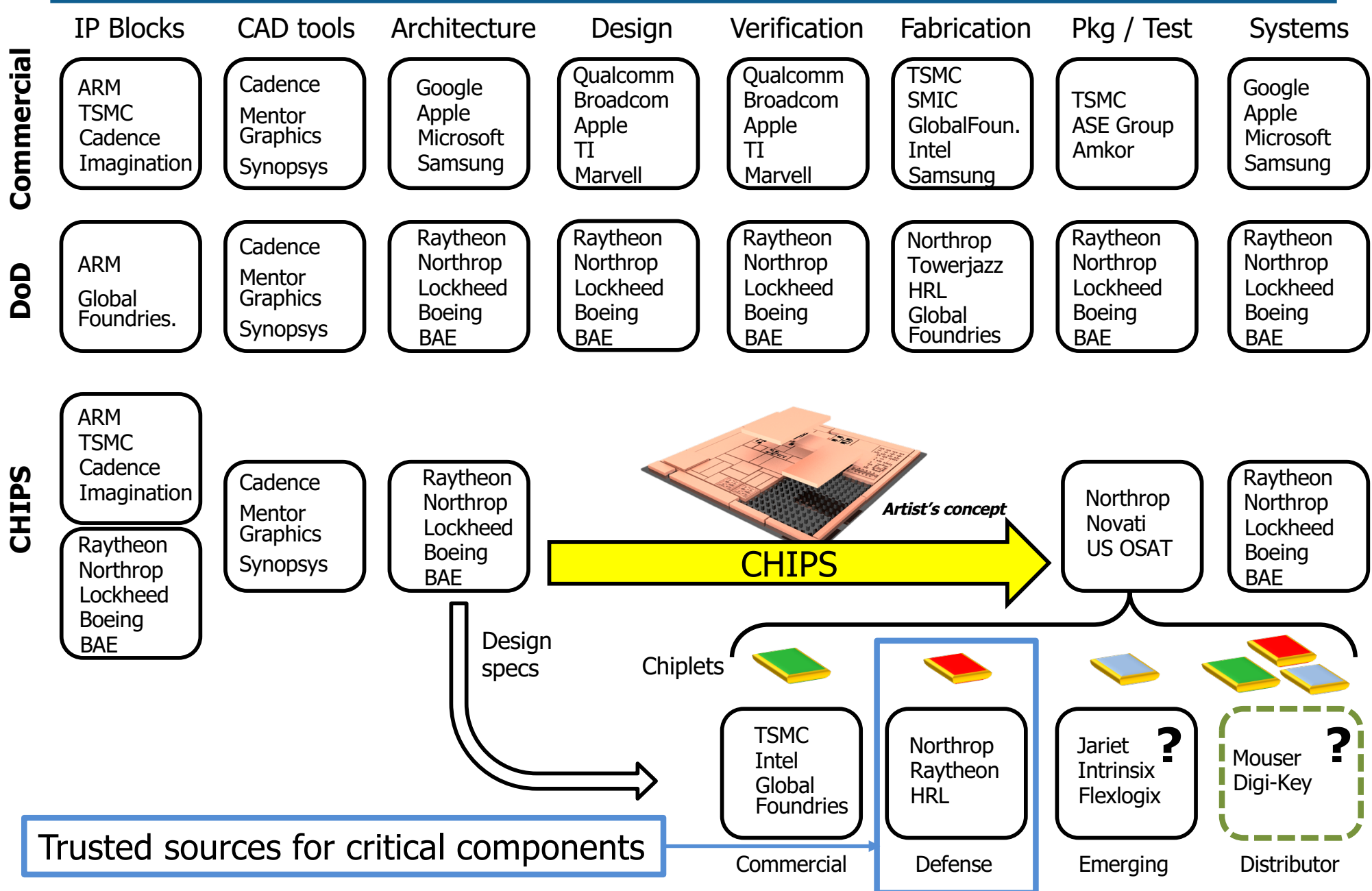[4] Various Silicon process nodes, RF passive, or compound semiconductor devices.
[5] Minimum bus/lane data rate, capable of scaling to higher data rates.
[6] Performance relating to transferring data between chiplets.
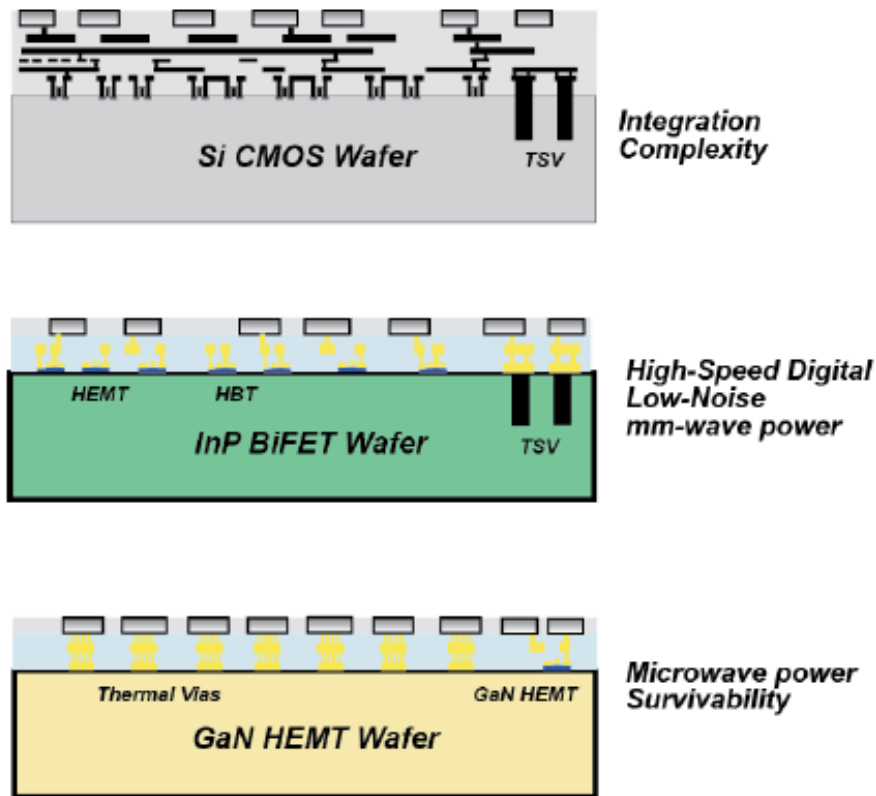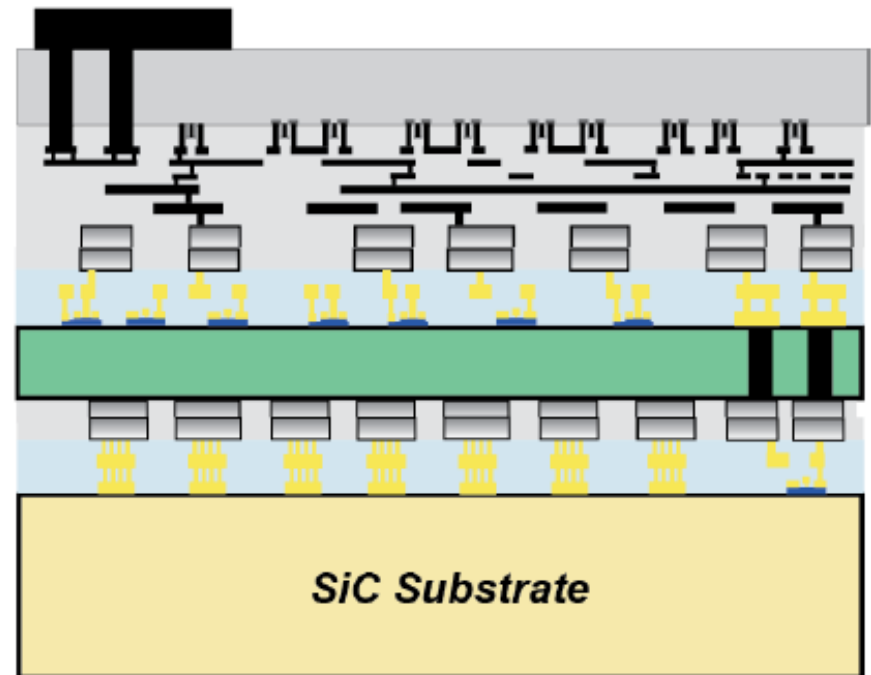
# CHIPS end state vs. conventional supply chain

| | IP Blocks | CAD tools | Architecture | Design | Verification | Fabrication | Pkg / Test | Systems |
|---|---|---|---|---|---|---|---|---|
| **Commercial** | ARM<br>TSMC<br>Cadence<br>Imagination | Cadence<br>Mentor Graphics<br>Synopsys | Google<br>Apple<br>Microsoft<br>Samsung | Qualcomm<br>Broadcom<br>Apple<br>TI<br>Marvell | Qualcomm<br>Broadcom<br>Apple<br>TI<br>Marvell | TSMC<br>SMIC<br>GlobalFoun.<br>Intel<br>Samsung | TSMC<br>ASE Group<br>Amkor | Google<br>Apple<br>Microsoft<br>Samsung |
| **DoD** | ARM<br>Global Foundries. | Cadence<br>Mentor Graphics<br>Synopsys | Raytheon<br>Northrop<br>Lockheed<br>Boeing<br>BAE | Raytheon<br>Northrop<br>Lockheed<br>Boeing<br>BAE | Raytheon<br>Northrop<br>Lockheed<br>Boeing<br>BAE | Northrop<br>Towerjazz<br>HRL<br>Global Foundries | Raytheon<br>Northrop<br>Lockheed<br>Boeing<br>BAE | Raytheon<br>Northrop<br>Lockheed<br>Boeing<br>BAE |

**CHIPS**

ARM<br>TSMC<br>Cadence<br>Imagination

Raytheon<br>Northrop<br>Lockheed<br>Boeing<br>BAE

Cadence<br>Mentor Graphics<br>Synopsys

Raytheon<br>Northrop<br>Lockheed<br>Boeing<br>BAE

*Artist's concept*

→ **CHIPS** →

Northrop<br>Novati<br>US OSAT

Raytheon<br>Northrop<br>Lockheed<br>Boeing<br>BAE

Design specs

Chiplets

TSMC<br>Intel<br>Global Foundries — Commercial

Northrop<br>Raytheon<br>HRL — Defense

Jariet<br>Intrinsix<br>Flexlogix **?** — Emerging

Mouser<br>Digi-Key **?** — Distributor

**Trusted sources for critical components**

# But there's more to DAHI than just the foundry…

CS-STACK TECHNOLOGY

Images courtesy of
Teledyne

Comparison to chiplet-based approach:

- ~10x reduced pitch → more interconnects per unit area (<2μm pitch, >$10^8$/cm$^2$ densities have been realized)
- Requires similar area sizes for GaN, InP, and CMOS
- Technology is significantly less mature than chiplet-based approach

# DAHI alternate flow:
## Wafer bonding of InP and Si CMOS (Teledyne/Tezzaron)
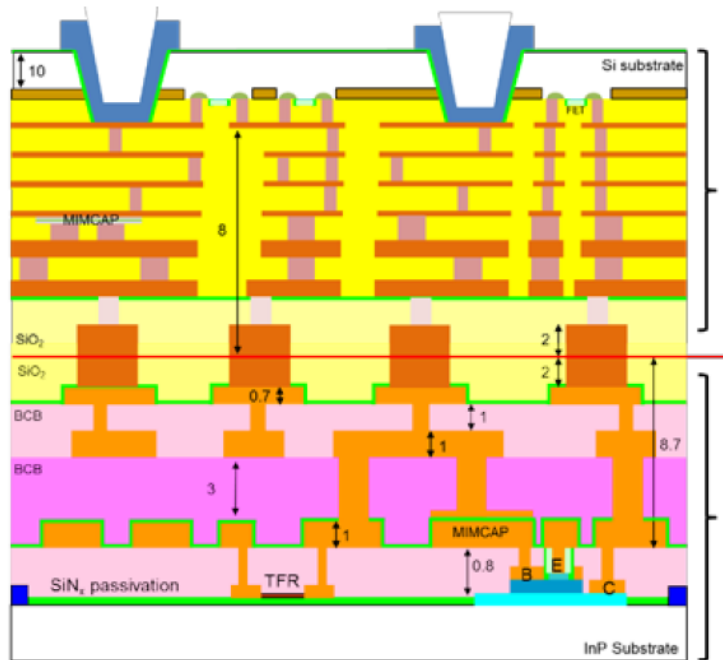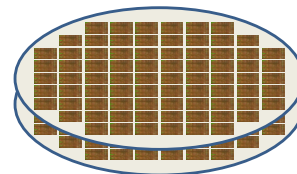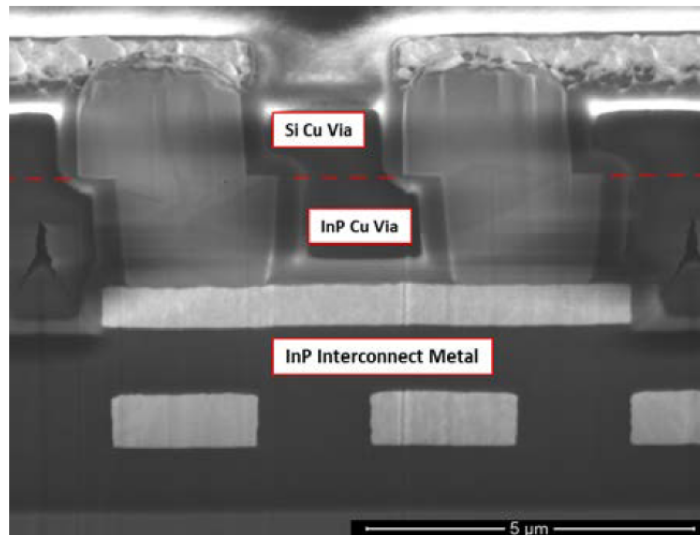


130 nm
Si CMOS
wafer

Cu/SiO₂
wafer
bond
interface

250 nm
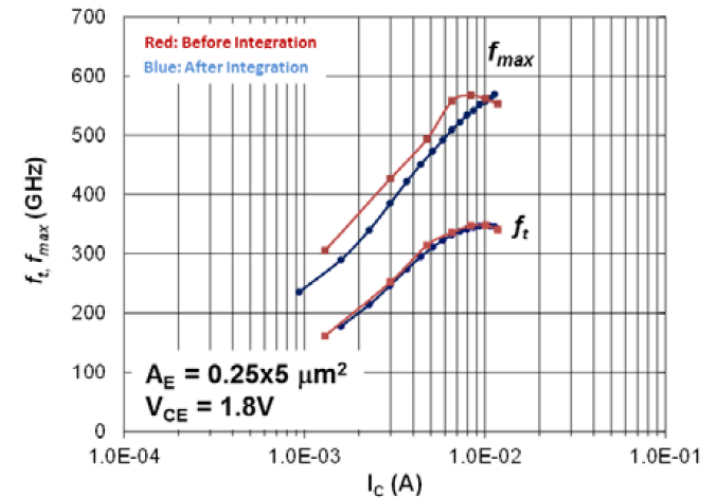InP HBT
wafer

Units in microns



wafer bonding



Fig. 5. Extrapolated $f_t$ and $f_{max}$ of 0.25x4μm² HBT before and after integration ($V_{CE} = 1.8V$)
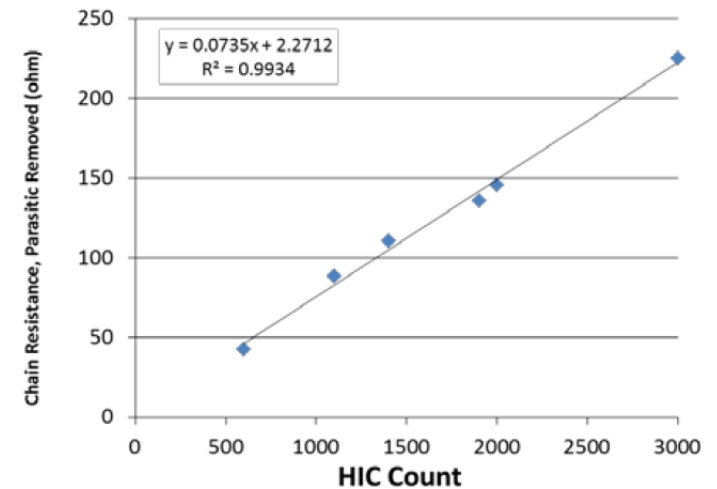


Fig. 6. Heterogeneous interconnection via chain resistance versus chain length.
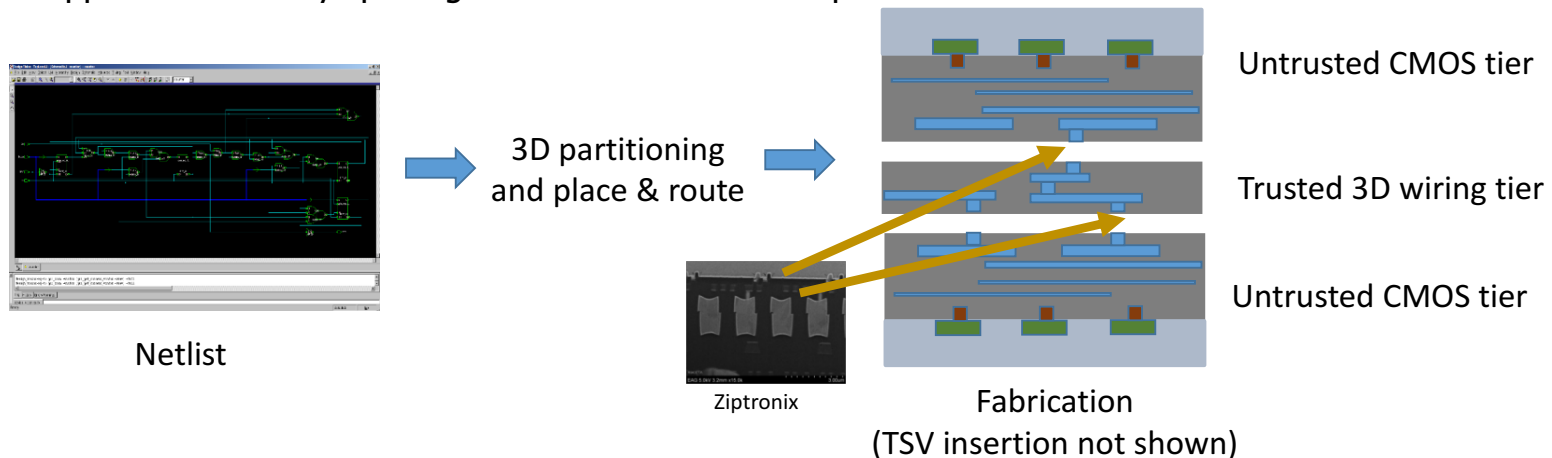
*Images courtesy of Teledyne*

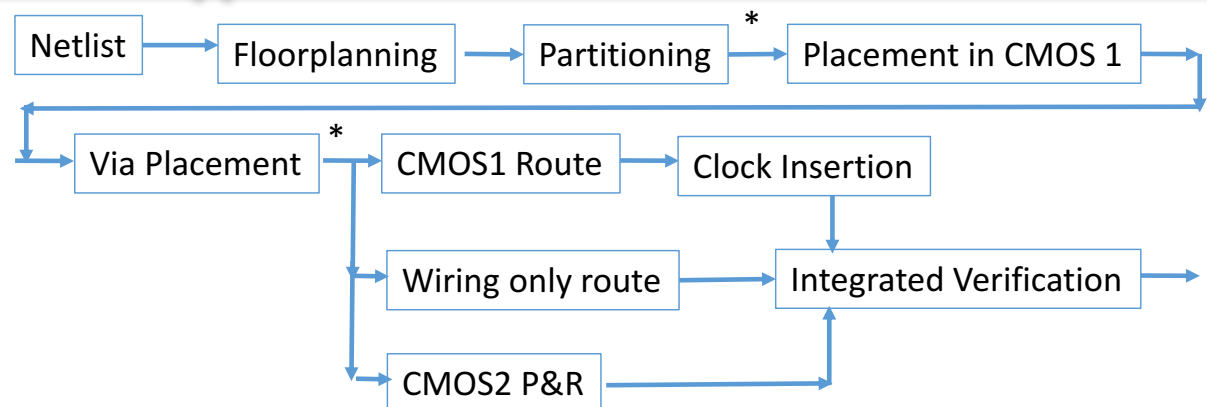# Concept: trusted fabrication through 3D ICs

## Problem Statement

- Can a trusted design be produced by integrating two untrusted CMOS chips and a trusted wiring only tier using established 3DIC fabrication techniques?
- TIC program approached this by splitting BEOL from FEOL but exposed difficulties



Netlist

3D partitioning and place & route

Ziptronix

Untrusted CMOS tier

Trusted 3D wiring tier

Untrusted CMOS tier

Fabrication
(TSV insertion not shown)

## Approach

- Put together basic CAD flow
- Run designs through this flow
- Investigate metrics against technology node, 3D integration pitch, and complexity of wiring only tier

*Images courtesy of NC State University*



Netlist → Floorplanning → Partitioning → *Placement in CMOS 1 → Via Placement → *CMOS1 Route → Clock Insertion → Integrated Verification; Wiring only route → Integrated Verification; CMOS2 P&R → Integrated Verification

## Exploring trust through combination of untrusted processes

Artist's concept

## Access and trust through disaggregation

www.darpa.mil