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

DISTRIBUTION A. Approved for public release: distribution unlimited.
The DARPA solution is to provide a menu of hardware security options that can be selectively applied based on need.

<table>
<thead>
<tr>
<th>Protection</th>
<th>Program</th>
<th>Loss of information</th>
<th>Fraudulent products</th>
<th>Loss of access</th>
<th>Malicious insertion</th>
<th>Quality and reliability</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Government Intervention</td>
<td>Other</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fine Disaggregation and Transience</td>
<td>TIC (IARPA)</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VAPR</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SPADE</td>
<td>●</td>
<td></td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Functional Disaggregation</td>
<td>DAHI</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CHIPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Obscuration and Marking</td>
<td>CRAFT</td>
<td></td>
<td>●</td>
<td></td>
<td></td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>eFuses</td>
<td>●</td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SHIELD</td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verification and Validation</td>
<td>IRIS</td>
<td>●</td>
<td></td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>TRUST</td>
<td>●</td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
</tbody>
</table>

DAHI and CHIPS can help protect against the malicious introduction of unknown functionalities into ASIC products.
Heterogeneous integration: Broadens the device material options

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

Diverse Accessible Heterogeneous Integration

Si CMOS

Trusted ICs

High Performance III-V

Number of transistors

Johnson Figure of Merit (GHz*Volt)
COSMOS program showed the promise of heterogeneous integration

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

**Yield Enhancement & Circuit Integration**
- ~500 HICs
- ~400 HBTs, 3200 CMOS

**Advanced Circuits**
- A/D converter
- D/A converter

<table>
<thead>
<tr>
<th># of Heterogeneous Interconnects</th>
<th>FY07</th>
<th>FY08</th>
<th>FY09</th>
<th>FY10</th>
<th>FY11</th>
<th>FY12</th>
<th>FY13</th>
</tr>
</thead>
<tbody>
<tr>
<td>COSMOS Phase I completed</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COSMOS Phase II completed</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COSMOS Phase III completed</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

**COSMOS**
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.

*Image courtesy of Northrop Grumman Aerospace Systems*

1. Compound Semiconductor Materials on Silicon

**COSMOS:** Demonstrated benefits of integration of **completed** devices
Diverse Accessible Heterogeneous Integration (DAHI) foundry for heterogeneous integration

Heterogeneous technology integration in accessible foundry

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

65 nm IBM CMOS Wafer

InP HBT Chiplets

GaN HEMT Chiplets

Image courtesy of Northrop Grumman Aerospace Systems

(first three-technology integration demonstrated in Jan 2015)
DAHI MPW0 CMOS + InP HBT + GaN HEMT demonstration

Successful integration of high performance III-V technologies with CMOS

(3 technology integration demonstrated in Jan 2015)
Image courtesy of Northrop Grumman Aerospace Systems
DAHI MPW1: Excellent yield, successful initial tests

GlobalFoundries

300mm diameter Si CMOS wafer (45nm node)

Northrop Grumman

High foundry integration yields; test vehicles fully functional

99.94% HIC yield 98% HBT post-integration

Northrop Grumman

DAHI integration (Dec 2015): Si (45nm), InP (TF5 HBT), GaN (GaN20 HEMT)

BAE Systems

DAC with very low digital noise (-70dBc)

Teledyne

Successful testing identified optimal S/H circuit for ADC (>65dB SFDR @ 2GHz)
Integration approach - disaggregation

- 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

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
### Integration: Enabling IP and chiplet re-use

#### Chiplet process modules designed with IP re-use in mind

<table>
<thead>
<tr>
<th>GaN</th>
<th>VLSI Si</th>
</tr>
</thead>
<tbody>
<tr>
<td>InP</td>
<td>SiGe</td>
</tr>
<tr>
<td>Passives</td>
<td>GaAs, MEMS, etc.</td>
</tr>
</tbody>
</table>

- 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**

**Example interconnect**

**DAHI-enabled integration technology plus IP re-use ecosystem to speed the design cycle and reduce the access cost**

DISTRIBUTION A. Approved for public release: distribution unlimited.
What is CHIPS?

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?

CHIPS enables rapid integration of functional blocks at the chiplet level.
### CHIPS impact on DoD electronics

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

CHIPS is projected to reduce IC design to one-third cost **and** time
### CHIPS metrics (preliminary)

#### Design Level

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP reuse (%)</td>
<td>&gt; 50% public&lt;sup&gt;1&lt;/sup&gt; IP blocks</td>
</tr>
<tr>
<td>Modular design (%)</td>
<td>&gt; 80% reused&lt;sup&gt;2&lt;/sup&gt; IP</td>
</tr>
<tr>
<td>Access to IP</td>
<td>&gt; 3 sources&lt;sup&gt;3&lt;/sup&gt; of IP</td>
</tr>
<tr>
<td>Heterogeneous integration</td>
<td>&gt; 3 technologies&lt;sup&gt;4&lt;/sup&gt;</td>
</tr>
</tbody>
</table>

#### Digital Interfaces

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data rate (scalable)&lt;sup&gt;5&lt;/sup&gt;</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>Energy efficiency&lt;sup&gt;6&lt;/sup&gt;</td>
<td>&lt; 5 pJ/bit</td>
</tr>
<tr>
<td>Latency&lt;sup&gt;6&lt;/sup&gt;</td>
<td>? 5 nsec</td>
</tr>
</tbody>
</table>

#### Analog Interfaces

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insertion loss (across full bandwidth)</td>
<td>&lt; 1 dB</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>? 50 GHz</td>
</tr>
</tbody>
</table>

---

<sup>1</sup> Public IP is defined as IP blocks available through commercial vendors or available to DoD community.

<sup>2</sup> Reuse is defined as existing or previously designed IP that is re-implemented into the current system.

<sup>3</sup> For RFI purposes, any business unit would be considered a single source of IP.

<sup>4</sup> Various Silicon process nodes, RF passive, or compound semiconductor devices.

<sup>5</sup> Minimum bus/lane data rate, capable of scaling to higher data rates.

<sup>6</sup> Performance relating to transferring data between chiplets.
<table>
<thead>
<tr>
<th>Commercial IP Blocks</th>
<th>Commercial CAD tools</th>
<th>Architecture Designs</th>
<th>Design Verification</th>
<th>Fabrication</th>
<th>Pkg / Test</th>
<th>Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARM TSMC Cadence Imagination</td>
<td>Mentor Graphics Synopsys</td>
<td>Google Apple Broadcom Apple TI Marvell</td>
<td>Qualcomm Broadcom Apple TI Marvell</td>
<td>TSMC SMIC GlobalFoundries</td>
<td>TSMC ASE Group Amkor</td>
<td>Google Apple Microsoft Samsung</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DoD IP Blocks</th>
<th>DoD CAD tools</th>
<th>Architecture Designs</th>
<th>Design Verification</th>
<th>Fabrication</th>
<th>Pkg / Test</th>
<th>Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARM Global Foundries</td>
<td>Mentor Graphics Synopsys</td>
<td>Raytheon Northrop Lockheed Boeing BAE</td>
<td>Raytheon Northrop Lockheed Boeing BAE</td>
<td>Northrop TowerJazz HRL Global Foundries</td>
<td>Raytheon Northrop Lockheed Boeing BAE</td>
<td>Raytheon Northrop Lockheed Boeing BAE</td>
</tr>
</tbody>
</table>

**CHIPS**

**Design specs**

**Chiplets**

- **Commercial**
  - TSMC Intel Global Foundries
- **Defense**
  - Northrop Raytheon HRL
- **Emerging**
  - Jariet Intrinsix Flexlogix
- **Distributor**
  - Mouser Digi-Key

**Trusted sources for critical components**
But there’s more to DAHI than just the foundry...
DAHI alternate flow: wafer-scale bonding

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

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

**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**
Future of heterogeneous integration

Access and trust through disaggregation