A TECHNOLOGY-ENABLED NEW TRUST APPROACH

Dr. William Chappell
Director, DARPA Microsystems Technology Office (MTO)

NDIA Trusted Microelectronics Workshop

August 17, 2016

DISTRIBUTION A. Approved for public release: distribution unlimited.
DISTRIBUTION A. Approved for public release: distribution unlimited.
Develop processing architectures for next generation machine learning.

Move from fear to exploiting a new technology approach.

Expand our lead in the physical realm.
DoD faces unique security challenges in protecting its microelectronics against advanced nation-states.

**Fabrication & Assembly**

**Potential Attacks**
- Malicious insertion
- Fraudulent products
- Loss of CPI
- Poor quality
- Reliability failures
- Loss of access

**Overproduction & Test Fails**

**Counterfeiting**

**Hardware or IP theft**

**Cloning**

**Design Compromise**

**Reliability Compromise**

**Supply Chain Risk**

DISTRIBUTION A. Approved for public release: distribution unlimited.
Leading-edge microelectronics offer specific, military-relevant advantages to DoD

~5 - 10x performance gain from 130nm to 10nm

Computational Efficiency (GOPS/W) vs Technology Node

Data from ISSCC papers 2010 – 2013 and "Energy Efficient Computing on Embedded and Mobile Devices" on nVidia.com

DISTRIBUTION A. Approved for public release: distribution unlimited.
Example ASICs under development could deliver revolutionary capabilities to the warfighter

- **ACT**: Capture unprecedented volumes of RF data at 64Gs/sec for next-gen arrays
- **CLASIC**: Distinguish and classify RF signals for 180 hours on a cellphone battery
- **CLASS**: Disguise and dynamically vary signals for inexpensive LPI/LPD comms
- **DAHI**: 10x higher dynamic range arbitrary waveform generator for EW solutions
- **ReImagine**: Collect different data in a single camera frame with a reconfigurable ROIC
- **RF-FPGA**: A software-defined front end that works for 20GHz or below
- **SHIELD**: Verify the authenticity of components at every point in the supply chain
- **SPADE**: Build trusted circuits through 3D integration
- **UPSIDE**: Enable real-time machine learning for object recognition on UAV
Example ASICs under development could deliver revolutionary capabilities to the warfighter.

**ACT**
- Capture unprecedented volumes of RF data at 64Gs/sec for next-gen arrays
- Leverage the world’s best digital beamforming system

**SHIELD**
Verify the authenticity of components at every point in the supply chain

**CLASS**
Disguise and dynamically vary signals for inexpensive LPI/LPD comms

**CLASIC**
Distinguish and classify RF signals for 180 hours on a cellphone battery

**UPSIDE**
Enable real-time machine learning for object recognition on UAV

**DISTRIBUTION**
A. Approved for public release: distribution unlimited.
Example ASICs under development could deliver revolutionary capabilities to the warfighter

**ReImagine**
- Achieve full battlespace awareness with a single reconfigurable ROIC
- Simultaneously collect diverse data types from multiple regions of interest

14nm CMOS

**DISTRIBUTION A. Approved for public release: distribution unlimited.**
Example ASICs under development could deliver revolutionary capabilities to the warfighter

**Microscopic SHIELD dielet**

**SHIELD**
- Ensure the authenticity of genuine military electronic components
- Tag electronics at low cost with an encrypted 100µm x 100µm ASIC

**14nm CMOS**

**Example**
- **CLASS** Disguise and dynamically vary signals for inexpensive LPI/LPD communications
- **SHIELD** Verify the authenticity of components at every point in the supply chain
- **CLASIC** Distinguish and classify RF signals for 180 hours on a cellphone battery
- **UPSIDE** Enable real-time machine learning for object recognition on UAVs
- **DAHI** 10x higher dynamic range arbitrary waveform generator for EW solutions
- **ACT** Capture unprecedented volumes of RF data at 64Gs/sec for next-gen arrays
- **ReImagine** Collect different data in a single camera frame with a reconfigurable ROIC
- **RF-FPGA** A software-defined front end that works for 20GHz or below
- **SPADE** Build trusted circuits through 3D integration

**DISTRIBUTION A. Approved for public release: distribution unlimited.**
The semiconductor market sustains a large ecosystem, with many leading-edge firms operating within the United States. A few small players include:

- GLOBALFOUNDRIES
- Qorvo
- CREE
- Cypress
- ON Semiconductor
- TowerJazz

Govern't-owned Suppliers:

- Intel
- Samsung
- TSMC
- SK Hynix
- Micron
- Texas Instruments
- GLOBALFOUNDRIES
- Qualcomm
- ARM
- ...
DoD will have to collaborate with the multinational semiconductor firms with leading-edge capabilities

14-nm fabrication is only available through highly-consolidated, global multinational firms
Reliance on trusted suppliers can limit potential partners, yielding few options for trusted access to leading-edge CMOS

<table>
<thead>
<tr>
<th>Foundry Choices</th>
<th>Process node for leading-edge products</th>
<th>Design-to-chip turnaround time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commercial</td>
<td>Multiple global options</td>
<td>14nm – 10nm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9-10 months</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(400 engineers)</td>
</tr>
<tr>
<td>DoD</td>
<td>One strategic partner</td>
<td>65nm – 32nm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2-3 years</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(10 engineers)</td>
</tr>
</tbody>
</table>

Source: DMEA, as of Aug 2016
It is the right time for DoD to reflect on its strategy

**Today:** DoD relies on a single, sole-source supplier for leading-edge microelectronics

**Tomorrow:** Technology-driven security techniques can enable new DoD options for acquiring state-of-the-art, commercial microelectronics

---

**Sole-source Fabrication below 90nm**

**Trusted Design**

**Commercial Fabrication**

- GLOBALFOUNDRIES
- Samsung
- TSMC
- Intel

**Trusted DoD Electronics**
Selective application of countermeasures can demonstrate "trust through technology" for a representative device.

To ensure security and to leverage the globalized supply chain, DARPA and other agencies are developing a technology-enabled portfolio of protections.
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><strong>Government-proprietary</strong></td>
<td>Other</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Fine Disaggregation and Transience</strong></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><strong>Functional Disaggregation</strong></td>
<td>SPADE</td>
<td>●</td>
<td></td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></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><strong>Obscuration and Marking</strong></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><strong>Verification and Validation</strong></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>

- ● Primary Impact
- ● Secondary Impact

DISTRIBUTION A. Approved for public release: distribution unlimited.
We’ve adapted to the end of Dennard’s Law but are at an inflection point.

Post-Dennard, we lose the free exponential improvements in computing cost, speed, and power from improvements in fabrication technology.
Moore’s Law has allowed the military to increasingly depend on FPGAs

Global Military/Aeronautics Shipments

Source: Multiple industry market trackers & DMEA internal data from FPGA manufacturers

DISTRIBUTION A. Approved for public release: distribution unlimited.
The end of Moore’s Law is leveling the playing field, meaning now is the time to focus on ASIC access and specialization.

**Trust through technology**

Acquisition personnel can selectively apply protections based on a component’s criticality, the risks faced, and the need to access leading-edge technologies.