The U.S. semiconductor landscape

The U.S. military must have access to microelectronics capabilities equivalent to and exceeding those of U.S. adversaries

The U.S. semiconductor industry has notable advantages:

- For approximately two decades, U.S.-headquartered firms have accounted for half of global semiconductor sales.\(^1\)
- The United States has a majority of the global market for integrated circuit design and fabrication, which represents over 80% of the global semiconductor market.\(^1\)
- The top integrated device manufacturer, top three fabless companies, top three Electronic Design Automation companies, and two of the top three equipment manufacturers by revenue are U.S. headquartered.\(^1\)

To confidently maximize these advantages, the U.S. government must be able to verify the confidentiality, integrity, and availability of products in its semiconductor supply chain.

\(^1\) 2017 PCAST report “Ensuring Long-Term U.S. Leadership in Semiconductors”

DARPA is developing technologies to mitigate risks inherent to semiconductor production and to safely leverage more of the available onshore and allied capabilities.
Leading-edge (≤65nm) microelectronics offer specific, military-relevant advantages to the Department of Defense (DoD).

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

10x-1000x improvement from CPUs to GPUs & ASICs

Data from ISSCC papers 2010 - 2013 and "Energy Efficient Computing on Embedded and Mobile Devices" on nVidia.com
Leading-edge ASICs under development in MTO programs could deliver revolutionary capabilities to the warfighter

**Example ASIC***

- **ACT**: Capture unprecedented volumes of RF data at 64Gs/sec for next-gen arrays
- **CLASS C**: 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
- **Relimagine**: 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 UAVs

*ASICs from MTO programs

ASIC – application specific integrated circuit
RF – radio frequency
LPI/LPD – low probability of intercept/detection
ROIC – readout IC

DISTRIBUTION A. Approved for public release: distribution unlimited.
Leading-edge ASICs under development in MTO programs 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

32nm SOI vs. 14nm FinFet

**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

**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
• Leverage the world’s best digital beamforming system

32nm SOI vs. 14nm FinFet

**SPADE**
Build trusted circuits through 3D integration

**RF-FPGA**
A software-defined front end that works for 20GHz or below

**ReImagine**
Collect different data in a single camera frame with a reconfigurable ROIC

**Image Source** – Northrop Grumman

---

**DISTRIBUTION A. Approved for public release: distribution unlimited.**

ASIC – application specific integrated circuit
ACT – Arrays at Commercial Timescales
SOI – Silicon on Insulator
Leading-edge ASICs under development in MTO programs could deliver revolutionary capabilities to the warfighter.

- **CLASS Disguise and dynamically vary signals for inexpensive LPI/LPD comms**
- **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 UAV**
- **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
• Achieve full battlespace awareness with a single reconfigurable ROIC
• Simultaneously collect diverse data types from multiple regions of interest

14nm CMOS

SOA digital ROIC pixel layout using 65 nm CMOS

25 µm

14 nm CMOS pixel with computation

~6 µm

~10 µm

Images courtesy: MIT Lincoln Laboratory

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

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

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

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

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

**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

---

**Microscopic SHIELD dielet**

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

**14nm CMOS**

---

**SHIELD** - Supply Chain Hardware Integrity for Electronics Defense

ASIC - application specific integrated circuit
The United States hosts three of the five most advanced leading-edge fabrication facilities onshore.

14-nm fabrication is only available through highly-consolidated, global multinational firms.
However, DoD faces unique security challenges in protecting its microelectronics.

**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.
DARPA aims to ensure that DoD can safely access the multiple semiconductor capabilities available to the commercial sector.

**Today:** DoD leverages one strategic partner for leading-edge microelectronics.

- Trusted Design
- Sole-source Fabrication below 90nm
  - Portions of GLOBALFOUNDRIES
- Trusted DoD Electronics

**Commercial Fabrication**
- Full access to GLOBALFOUNDRIES
- Samsung
- TSMC
- Intel

**Added:**
- A new menu of protections
- Trusted circuit analysis tools

**Tomorrow:** Technology-driven security techniques enable additional options for acquiring state-of-the-art, commercial microelectronics, based on each DoD program’s need.

DISTRIBUTION A. Approved for public release: distribution unlimited.
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 a menu of hardware security options that can be selectively applied to tackle known security threats.

<table>
<thead>
<tr>
<th>Protection</th>
<th>Program</th>
<th>Microelectronics Security Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>CPI Theft</td>
</tr>
<tr>
<td>Strategic Foundry</td>
<td></td>
<td>●</td>
</tr>
<tr>
<td>Partnerships</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Government-proprietary</td>
<td>Other</td>
<td>●</td>
</tr>
<tr>
<td>Fine Disaggregation</td>
<td><strong>TIC (IARPA):</strong> Disaggregate ASICs into non-functional parts</td>
<td>●</td>
</tr>
<tr>
<td>Transience</td>
<td><strong>VAPR:</strong> Shatter lost, misplaced, or end-of-life ASICs on command</td>
<td>●</td>
</tr>
<tr>
<td>Blended Partnerships</td>
<td><strong>SPADE:</strong> Use secure parts to monitor commercial components packaged together into a single ASIC</td>
<td>●</td>
</tr>
<tr>
<td>Functional Disaggregation</td>
<td><strong>DAHI:</strong> Disaggregate ASICs into functional subcomponents</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td><strong>CHIPS:</strong> Establish a library of pre-verified, modular ASIC design IP</td>
<td>□</td>
</tr>
<tr>
<td>Commercial Manufacturing</td>
<td><strong>CRAFT:</strong> Apply modularity to reduce ASIC design effort and allow portability across foundries</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td><strong>eFuses:</strong> Obscure ASIC functionality until after manufacture</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td><strong>SHIELD:</strong> Authenticate ASICs at any point in the supply chain</td>
<td>□</td>
</tr>
<tr>
<td>Obscuration and Marking</td>
<td><strong>IRIS:</strong> Derive an ASICs functionality and reliability</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td><strong>TRUST:</strong> Reverse engineer ASICs and compare to design</td>
<td>□</td>
</tr>
</tbody>
</table>

**TIC** - Trusted Integrated Chips  
**VAPR** - Vanishing Programmable Resources  
**DAHI** - Diverse Accessible Heterogeneous Integration  
**CHIPS** - Common Heterogeneous Integration & IP Reuse Strategies  
**CRAFT** - Circuit Realization at Faster Timescales  
**SHIELD** - Supply Chain Hardware Integrity for Electronics Defense  
**IRIS** - Integrity and Reliability of Integrated Circuits  
**TRUST** - Trusted Integrated Circuits
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**

- **Verification and Validation**
- **Obscuration and Marking**
- **Functional Disaggregation**
- **Fine Disaggregation and Transience**
- **Government-proprietary Techniques**

- **Advanced Verification**
- **Design Obscuration**
- **Functional Disaggregation**
- **Gov't-specific features**
- **Certified Trusted Assembly**

---

14nm commercially-sourced part
High performance
Generic components

90nm trusted part
Program-specific features
Domestic industry base

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