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></td>
<td>TIC (IARPA)</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fine Disaggregation and Transience</td>
<td>VAPR</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Functional Disaggregation</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>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>

CRAFT can help ensure multiple sources of supply for leading-edge ASICs, providing the flexibility to move between foundries when necessary.
CRAFT Vision

“To sharply reduce the barriers to DoD use of custom-integrated circuits built using leading-edge CMOS technology. Make design faster and access easier.”

Faster designs in commercial, leading-edge CMOS are more secure because:

- Decreased design effort enables more and faster updates
  - The time frame available to compromise an SoC is reduced
  - The time frame required to respond to a compromise is also reduced
- The inherent complexity and small feature size of FinFET designs make reverse engineering more difficult
  - Level of commercial reverse engineering difficulty would go from ~ 3 months of effort (90nm technology) to ~ 1 year of effort (FinFET technology)
- Use of commercial fabrication processes allows use of commercial security methods developed at great cost by the semiconductor industry
  - Massive amount of circuit verification
  - Independent, unbiased foundry services
  - Common libraries of secure IP
Performance versus development cycle times

Today you have to choose between performance and schedule/cost.

<table>
<thead>
<tr>
<th></th>
<th>Qty</th>
<th>Power Req.</th>
<th>Dev. Cycle Time</th>
<th>Current Character</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Purpose Central Processor (CPU)</td>
<td>28</td>
<td>1260W</td>
<td>~6 months</td>
<td>Low performance at power</td>
</tr>
<tr>
<td>Field Programmable Gate Array (FPGA)</td>
<td>4</td>
<td>120W</td>
<td>~12 months</td>
<td>Low performance at power</td>
</tr>
<tr>
<td>Custom Integrated Circuit (Custom IC)</td>
<td>1</td>
<td>5W</td>
<td>~24 months</td>
<td>High performance at power</td>
</tr>
</tbody>
</table>

Example Data from representative DoD design

DISTRIBUTION A. Approved for public release: distribution unlimited.
CRAFT Vision
To sharply reduce the barriers to DoD use of custom integrated circuits built using leading-edge CMOS technology while maintaining the high level of performance at power promised by this technology.
Why does DoD need custom ICs?

Current EW approach single channel non-real time 240W

Next-Gen Cognitive EW approach, wide band, real time 100W

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.
Current design flow takes so long that it is throttling DoD access to advanced technology

Existing DoD custom IC product cycle time can take as long as **2.5 years**.
- 60%: Design (most of which is verification)
- 40%: Fabrication (20%/fab spin)

Using “Object Oriented Design” and enhanced hierarchy, we want to achieve:
- Reduction in design time by 10X through a strong reduction in verification time and removal of minimum area constraint
- “First Time Right” design methods to eliminate the need for repeated fabrication runs.
- Reduction in fabrication time to 2X commercial

**Data from industry survey by DARPA consultants**

DISTRIBUTION A. Approved for public release: distribution unlimited.
## Market differences

<table>
<thead>
<tr>
<th></th>
<th>Low Volume</th>
<th>Moderate Volume Commercial</th>
<th>High Volume Commercial</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Design Cost</strong></td>
<td>Major contributor to total SoC cost</td>
<td>Major contributor to total SoC cost</td>
<td>Minor portion of total SoC cost</td>
</tr>
<tr>
<td><strong>Fabrication Cost</strong></td>
<td>Small contributor to total SoC cost</td>
<td>Significant contributor to total SoC cost</td>
<td>Major contributor to SoC cost</td>
</tr>
<tr>
<td><strong>Volume</strong></td>
<td>1k parts</td>
<td>1,000k parts</td>
<td>100,000k parts</td>
</tr>
<tr>
<td><strong>Area</strong></td>
<td>Not important</td>
<td>Relatively unimportant</td>
<td>Critical</td>
</tr>
<tr>
<td><strong>Design Schedule/Risk</strong></td>
<td>Critical</td>
<td>Critical</td>
<td>Critical</td>
</tr>
<tr>
<td><strong>Performance at Power</strong></td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
</tbody>
</table>

- **Design NRE**: 92% (Low), 69% (Moderate), 9% (High)
- **Production**: 1% (Low), 9% (Moderate), 89% (High)

*DISTRIBUTION A. Approved for public release: distribution unlimited.*
High-Level Description of CRAFT
CRAFT: Enabling use of the best commercial technology

CRAFT aims to provide solutions to the three major obstacles restricting custom IC design and fabrication for DoD systems.

**DESIGN**
- Design requires 18-24 months of effort
- Design verification takes far too much effort
- Fab cycles are too long and too uncertain
- Access to leading-edge CMOS is difficult

**PORT/MIGRATE**
- Designers are limited to one foundry
- Migration of designs from one node to another is difficult and expensive

**REPOSITORY**
- Severe lack of IP reusability for DoD designs
- Current audit model for custom IC design/hardware security is broken

*CRAFT aims to create new design flows that will reduce custom IC design cycle time by **10x** and increase design robustness through object-oriented design techniques*

*CRAFT aims to use new design flows to ensure multiple sources of supply and reduce node migration effort by 80% to keep DoD out of “the Silicon Island”*

*CRAFT aims to establish a data location and methodology to ensure 50% IP* reuse by DoD performers*

*CRAFT’s goal is to enable more efficient custom IC design/fabrication to enable HIGH performance electronic solutions **FASTER** and with more **FLEXIBILITY***

*IP – Sub-circuits used for modern custom ICs*
We need a new custom IC design flow

**New Software Tool**
- Use of modern software engineering methods
- Automated representation translation
- Automated verification
- Reduces effort required to port design to a 2nd source foundry
- Distributed through a government IP repository

**Object-Oriented Design (OOD) Flow**
High-level object-oriented language -> Schematic

**Raise Level of Abstraction**
- Use existing EDA tools
- Higher level of hierarchy
- Use of generators/constructs

**Existing ASIC Flow**

**New Software Tool**

**Object-Oriented Design (OOD) Flow**
High-level object-oriented language -> Schematic

**Raise Level of Abstraction**
- Use existing EDA tools
- Higher level of hierarchy
- Use of generators/constructs

**New Software Tool**

**Object-Oriented Design (OOD) Flow**
High-level object-oriented language -> Schematic

**Raise Level of Abstraction**
- Use existing EDA tools
- Higher level of hierarchy
- Use of generators/constructs

**New Software Tool**

**Object-Oriented Design (OOD) Flow**
High-level object-oriented language -> Schematic

**Raise Level of Abstraction**
- Use existing EDA tools
- Higher level of hierarchy
- Use of generators/constructs

**New Software Tool**

**Object-Oriented Design (OOD) Flow**
High-level object-oriented language -> Schematic

**Raise Level of Abstraction**
- Use existing EDA tools
- Higher level of hierarchy
- Use of generators/constructs

**New Software Tool**

**Object-Oriented Design (OOD) Flow**
High-level object-oriented language -> Schematic

**Raise Level of Abstraction**
- Use existing EDA tools
- Higher level of hierarchy
- Use of generators/constructs

**New Software Tool**

**Object-Oriented Design (OOD) Flow**
High-level object-oriented language -> Schematic

**Raise Level of Abstraction**
- Use existing EDA tools
- Higher level of hierarchy
- Use of generators/constructs

**New Software Tool**

**Object-Oriented Design (OOD) Flow**
High-level object-oriented language -> Schematic

**Raise Level of Abstraction**
- Use existing EDA tools
- Higher level of hierarchy
- Use of generators/constructs

**New Software Tool**

**Object-Oriented Design (OOD) Flow**
High-level object-oriented language -> Schematic

**Raise Level of Abstraction**
- Use existing EDA tools
- Higher level of hierarchy
- Use of generators/constructs

**New Software Tool**

**Object-Oriented Design (OOD) Flow**
High-level object-oriented language -> Schematic

**Raise Level of Abstraction**
- Use existing EDA tools
- Higher level of hierarchy
- Use of generators/constructs

**New Software Tool**

**Object-Oriented Design (OOD) Flow**
High-level object-oriented language -> Schematic

**Raise Level of Abstraction**
- Use existing EDA tools
- Higher level of hierarchy
- Use of generators/constructs

**New Software Tool**

**Object-Oriented Design (OOD) Flow**
High-level object-oriented language -> Schematic

**Raise Level of Abstraction**
- Use existing EDA tools
- Higher level of hierarchy
- Use of generators/constructs
Feasibility demonstration for CRAFT design goals: BOOM-2 RISC V Core designed using CHISEL

CHISEL is an Object Oriented Design demonstration flow/tool developed at UC-Berkeley

**BOOM-2 RISC V Core**

- Designed using CHISEL flow/tools
  - 6 graduate students ("2-pizza size team")
  - 6 months to design
- ~ 25M transistors and chip area of 1.0mm²
- 40nm technology
- 1.5 GHz clock rate
- Completed in November 2014

**CHISEL Specifics**

- CHISEL written in Scala programming language
- Parameterized generators used
- ~9,000 New “Lines of Code in CHISEL
- ~ 11,500 reused “Lines of Code” from previous projects
  - ~5,000 “Lines of Code” for processor
  - ~2,000 “Lines of Code” for floating point core
  - ~4,500 “Lines of Code” for “uncore”

**BOOM-2 is a feasibility demonstration of an OOD flow on a small digital design in an academic environment.**
CRAFT aims to enable facilitated transfer of designs to multiple companies and process flows.

- Build on the CRAFT-developed Object-Oriented Design flow to develop a port/migrate flow that reduces effort by 80%
- Fabricate and analyze CRAFT macros/generators at 16nm/14nm and 10nm at other foundries to facilitate migration
- Port prototypical designs to an alternate 16nm/14nm foundry, and migrate prototypical designs to a 10nm foundry

**Method to avoid the “Si Island”**

*CRAFT aims to use new design flows to ensure multiple sources of supply and reduce node migration effort by 80%*
Facilitated port/migrate through use of the CRAFT OOD flow

**Current ASIC Design Flow**
- High Level description
- Logical Descript’n
- Gate Level Descript’n
- Schematic Descript’n
- Place & Route
- Layout Descript’n

**New CRAFT Design Flow**
- Object-Oriented Design (OOD) Flow
  - High level object-oriented language -> Transistor

**CRAFT aims to sharply reduce the amount of “foundry-unique” work required for a design.**
**Design foundation will be developed at a 2nd source foundry as part of CRAFT.**
**The OOD Flow will be reused to reduce the effort to port designs.**
CRAFT aims to establish location for items required for DoD users of the OOD flow.

OOD flow requirements
- OOD software, tools
- OOD components
  - Generators
  - Macros
  - OOD specific IP (e.g. RISC-V processor, Vreg, ...)
- OOD examples and best practices
- Foundry-provided design rules and technology files

Data and models
- Foundry-provided reliability
- Extended reliability (government limits)
- Device and circuit radiation response
- IP
  - Foundry-provided IP (e.g. SRAM bit cells, eFuse, ...)
  - 3rd party IP (e.g. logic library, memory compiler, ...)
  - Government IP (e.g. rad hard library, A/D, ...)

CRAFT aims to establish a data location and distribution protocol to ensure efficiency through reuse of OOD flow components and methodology.

DISTRIBUTION A. Approved for public release: distribution unlimited.
DARPA multi-project run (MPW) shuttle details

- **ALL runs available to ALL Defense Contractors**
  - Wafer diameter: 300mm
  - Single exposure area: 26mm\(\times\)33mm
  - Exposures (shots)/wafer: ~80
  - Project area unit: 2.5mm\(\times\)2.5mm
  - Projects/shot: ~100

- A single FinFET process flow (TSMC 16FFC)
  - Bulk FinFET transistors with dual gate oxide
  - BEOL stack: 9 levels of Cu wiring
  - Standard passive components (no deep trench capacitor)
  - Standard eFuse blocks
  - HD and HP SRAM bit cell

- **Schedule**
  - PDK available: January, 2016
  - Training: May-June 2016
  - Firm shuttle commitment from users required: June, 2016
  - Design submission (GDS-In): July, 2016
  - Follow on runs 4/2017, 1/2018, 1/2019
  - Die back to users: (GDS-In + 6 months)

- **Aggregator/interface/training organization**
  - All questions for the foundry will go through MOSIS
  - All GDS will be sent to MOSIS

- User cost planned to be ~ $50K/project (2.5mm\(\times\)2.5mm)
### CRAFT performers

<table>
<thead>
<tr>
<th>Prime</th>
<th>Prototype SoC</th>
<th>Anticipated Teams</th>
</tr>
</thead>
<tbody>
<tr>
<td>UC-Berkeley</td>
<td>Multi-Application EW/Radar SoC</td>
<td>UC-Berkeley, Northrop-Grumman Electronic Systems, Cadence</td>
</tr>
<tr>
<td>Boeing</td>
<td>Multi-Application Reconfigurable DSP SoC</td>
<td>Boeing, Stanford University, UC-Los Angeles, Totic, Synopsys</td>
</tr>
<tr>
<td>Nvidia</td>
<td>Computer Vision Accelerator</td>
<td>Nvidia, Harvard</td>
</tr>
<tr>
<td>UC-San Diego</td>
<td>Autonomous Vehicle Perception/Decision SoC</td>
<td>UC-San Diego, Cornell University of Michigan, UC-Los Angeles</td>
</tr>
<tr>
<td>Carnegie-Mellon University</td>
<td>NA</td>
<td>Carnegie-Mellon University</td>
</tr>
<tr>
<td>USC/ISI</td>
<td>NA</td>
<td>USC/ISI, Notre Dame University</td>
</tr>
</tbody>
</table>

- Mixture of different types of entities across the industry
  - Commercial and defense companies
  - Small and large companies
  - Universities as prime contractors and sub contractors

DISTRIBUTION A. Approved for public release: distribution unlimited.
How does the industry obtain access to CRAFT results?

- CRAFT-developed software tools and design flows
  - Software tools and flows will be available through the funded repository
  - We will seek DoD example SoCs to implement using the flow in phases II and III

- Commonly needed commercial design IP
  - CRAFT DoD advisory board will recommend commonly needed commercial design IP
  - The CRAFT program will work broad agreement terms for the commercial IP

- Commonly needed commercial design software
  - The CRAFT design flow will lead to a set of commonly needed commercial design software
  - The CRAFT program will work broad agreement terms for this software

- CRAFT-dedicated, 16nm, multi-project runs that will occur every 9 months
  - All DoD contractors are welcome to place structures and circuits on these runs
  - Cost will be ~ $10K/mm^2 of die area
  - Die will be back within 6 months of design data delivery by users
Securing designs in an open fabrication environment

• Obscure circuit design intent by adding entropy to the released design data
  • Goal is to render the design data given to the foundry/mask shop unusable
  • Goal is to render the eventual design intent non-discernible by a thief or attacker

• Obscurity is then removed through post-wafer fabrication processes
  • Electronically activated fuses (efuse or anti-fuse), OR
    • Personalized at test or during system deployment
  • Embedded Non-Volatile Memory (NVM or Flash), OR
    • Personalized at test or during system activation
  • Other techniques TBD

• Advantages
  • Removes the risk of design data or die loss during mask and wafer fabrication
  • DoD-dedicated test equipment is inexpensive (~$100K) and relatively easy to implement while DoD-dedicated wafer fab is very expensive (~$10B) and exceptionally hard to implement

• Disadvantages
  • Requires an additional step in the IC design process to obscure the design
  • Does not protect the integrity of the original design data
  • Does not protect the integrity of the supply chain after final personalization
    • This will be addressed by the SHIELD program
IC obscuration through personalization

- Datapaths can be generalized to remove specificity of use
- Datapath specialization enabled by eFuses
- Data path defined after personalization

<table>
<thead>
<tr>
<th>Name of IP</th>
<th>Area Overhead</th>
<th>Power Overhead</th>
<th>Obfuscation Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>QR Decomposition (CLASS IC)</td>
<td>&lt;1%</td>
<td>&lt;1%</td>
<td>FSM</td>
</tr>
<tr>
<td>Eigen Value Decomposition (CLASS IC)</td>
<td>&lt;1%</td>
<td>&lt;1%</td>
<td>FSM</td>
</tr>
<tr>
<td>Communication Transmitter (CLASS IC)</td>
<td>&lt;1%</td>
<td>&lt;1%</td>
<td>FSM</td>
</tr>
<tr>
<td>Sparse Polynomial Equalizer (REDSOC IC)</td>
<td>&lt;1%</td>
<td>&lt;1%</td>
<td>Coefficient</td>
</tr>
<tr>
<td>Biquad Equalizer (REDSOC IC)</td>
<td>&lt;1%</td>
<td>&lt;1%</td>
<td>Coefficient</td>
</tr>
<tr>
<td>Nonlinear Equalizer (NLEQ IC)</td>
<td>&lt;30%</td>
<td>&lt;10%</td>
<td>Coefficient/Datapath</td>
</tr>
<tr>
<td>Sparse FFT (Sparse FFT IC)</td>
<td>&lt;7%</td>
<td>&lt;10%</td>
<td>FSM/Datapath</td>
</tr>
</tbody>
</table>

Source: MIT/Lincoln Laboratories