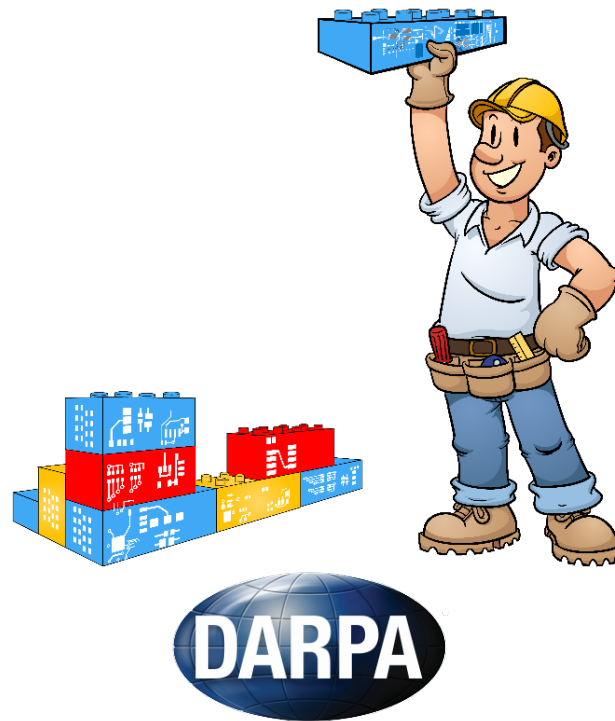


CIRCUIT REALIZATION AT FASTER TIMESCALES (CRAFT)

Dr. Linton Salmon, DARPA/MTO Program Manager



August 17, 2016



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

			Microelectronics Security Threats				
			Loss of information	Fraudulent products	Loss of access	Malicious insertion	Quality and reliability
High Government Intervention	Protection	Program					
	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		●		●	

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



CRAFT increases security

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.”

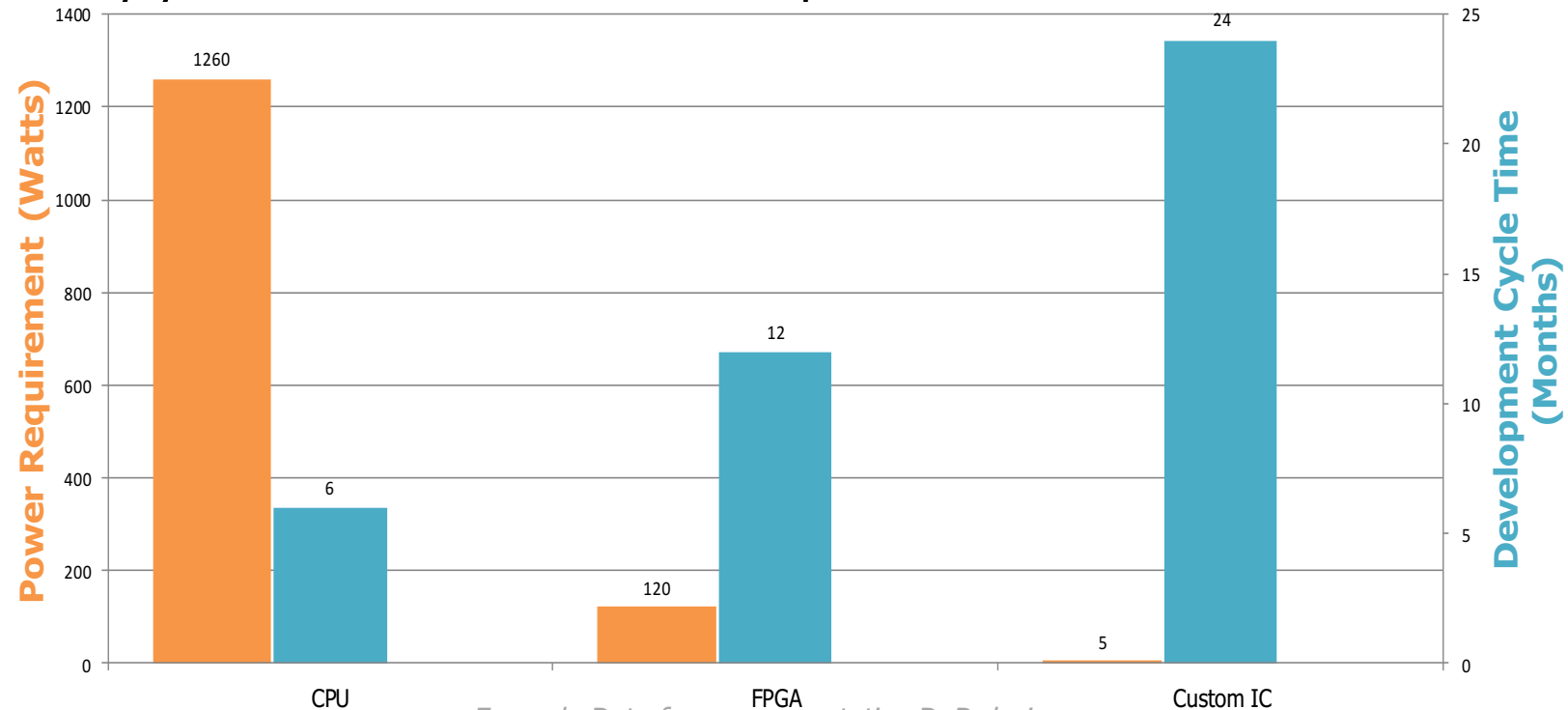
Faster designs in commercial, leading-edge CMOS are more secure because:

- 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.



Example Data from representative DoD design

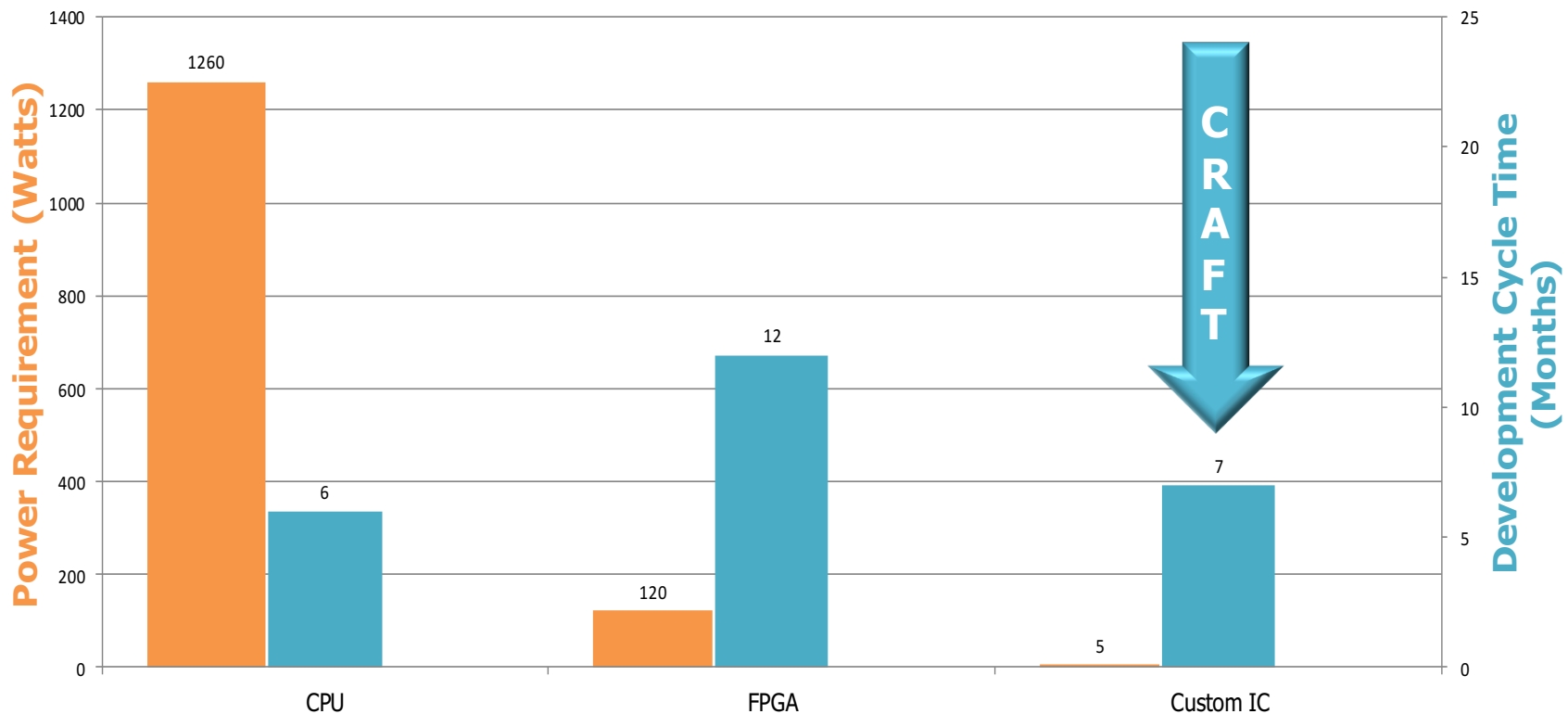
	Qty	Power Req.	Dev. Cycle Time	Current Character
General Purpose Central Processor (CPU)	28	1260W	~6 months	Low performance at power Flexible Quick to implement
Field Programmable Gate Array (FPGA)	4	120W	~12 months	Low performance at power Flexible Moderately quick to implement
Custom Integrated Circuit (Custom IC)	1	5W	~24 months	High performance at power Relatively inflexible Slow to implement



Performance versus development cycle times

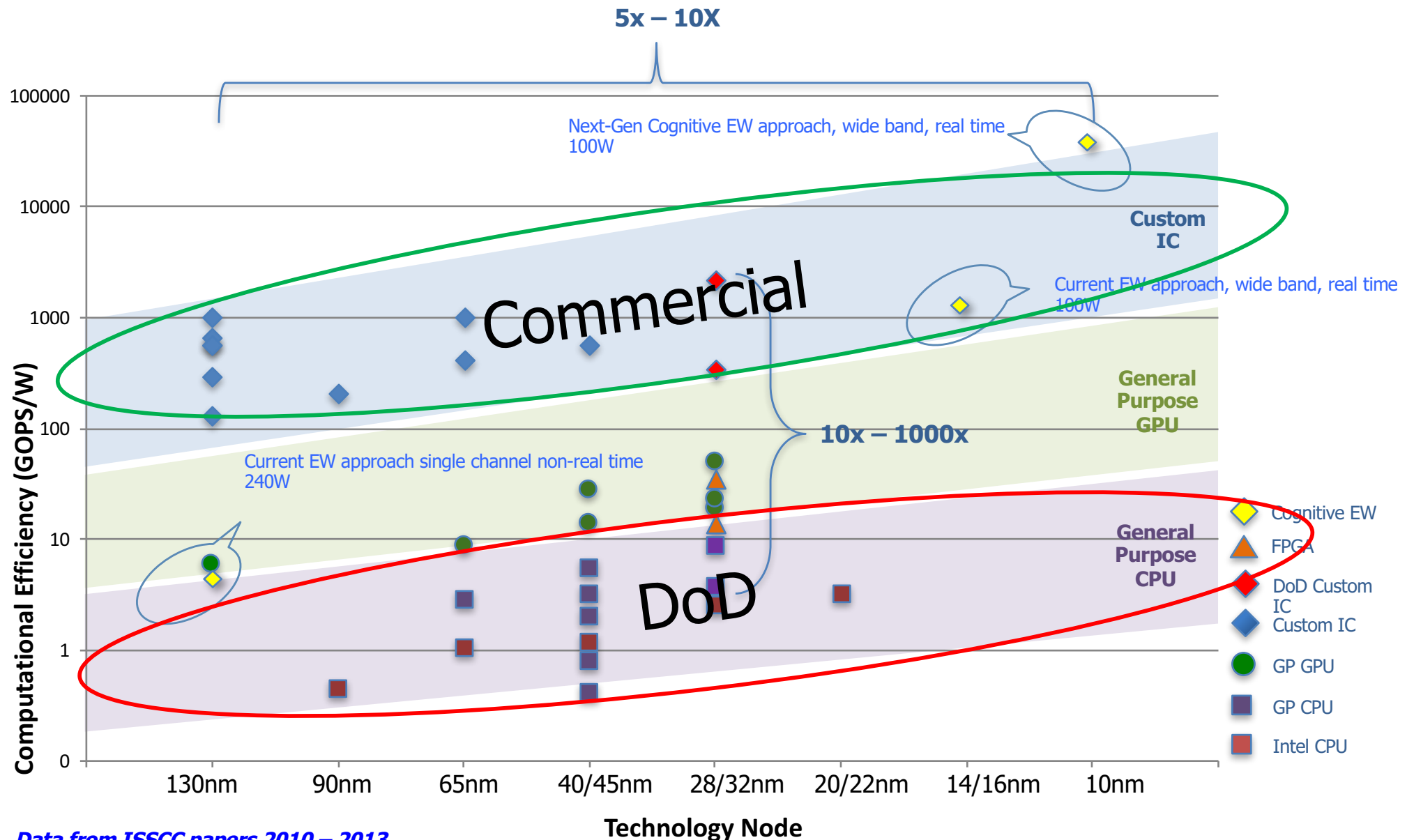
CRAFT Vision

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?



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

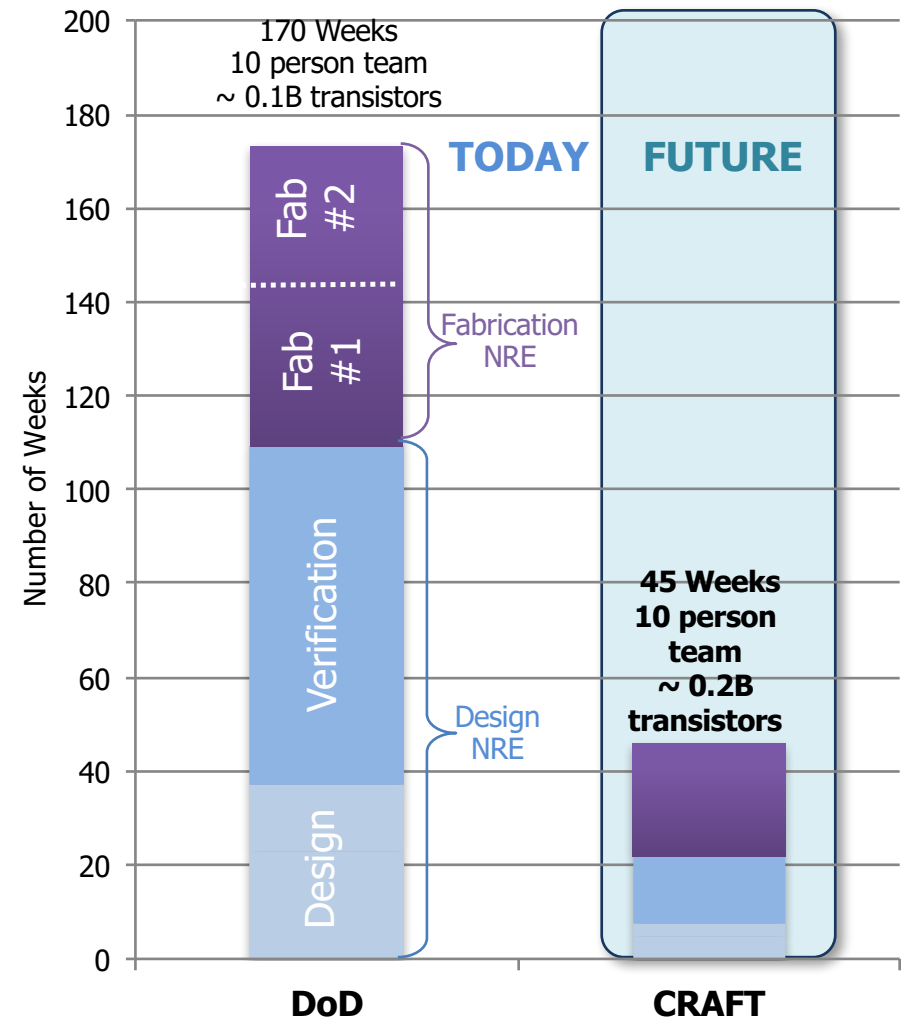
Existing DoD custom IC product cycle time can take as long as **2.5 years**.

- 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

14nm node example



Data from industry survey by DARPA consultants



Market differences

	Low Volume	Moderate Volume Commercial	High Volume Commercial
	<p>Pie chart showing cost breakdown for Low Volume: Design NRE (92%), Fab NRE (7%), and Production (1%).</p>	<p>Pie chart showing cost breakdown for Moderate Volume Commercial: Design NRE (69%), Fab NRE (22%), and Production (9%).</p>	<p>Pie chart showing cost breakdown for High Volume Commercial: Production (89%), Design NRE (9%), and Fab NRE (2%).</p>
Design Cost	Major contributor to total SoC cost	Major contributor to total SoC cost	Minor portion of total SoC cost
Fabrication Cost	Small contributor to total SoC cost	Significant contributor to total SoC cost	Major contributor to SoC cost
Volume	1k parts	1,000k parts	100,000k parts
Area	Not important	Relatively unimportant	Critical
Design Schedule/Risk	Critical	Critical	Critical
Performance at Power	Required	Required	Required



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

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

PORT/ MIGRATE

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

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"

REPOSITORY

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

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

* IP – Sub-circuits used for modern custom ICs

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



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

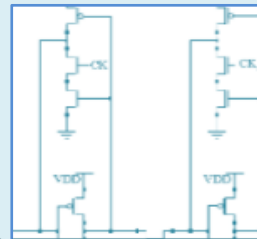
Raise Level of Abstraction

- Use existing EDA tools
- Higher level of hierarchy
- Use of generators/constructs

Object-Oriented Design (OOD) Flow

High-level object-oriented language -> Schematic

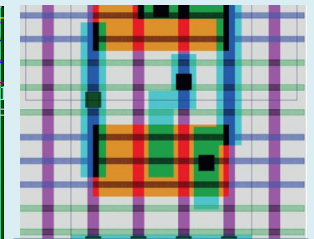
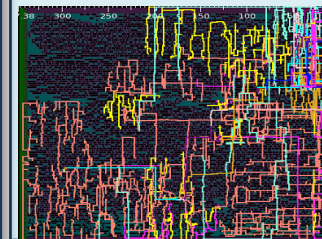
```
streampos begin,e  
ifstream myfile (  
begin = myfile.te  
myfile.seekg (0,  
end = myfile.tell  
myfile.close();
```



Place &
Route



Layout
Description



HL Code

OOD FLOW

SPICE

CELL/WIRE

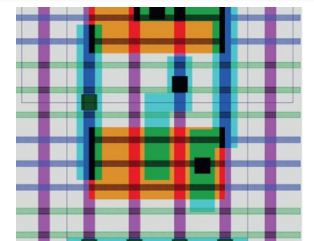
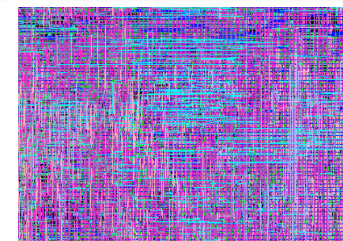
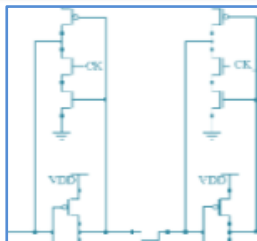
OASIS

Existing
ASIC
Flow

```
streampos begin,e  
ifstream myfile (  
begin = myfile.te  
myfile.seekg (0,  
end = myfile.tell  
myfile.close();
```

```
R4 -> MDR  
SP -> X, 4 -> Y  
add  
Z -> SP, MAR  
write, wait  
R0 -> X  
R5 -> MAR
```

```
FF : process (RST  
begin  
if rising_edge(C  
Q <= D;  
Q2 <= Q1;  
end if;  
if RST = '1' the  
Q <= '0';
```



HL Code

RTL

VHDL

SPICE

CELL/WIRE

OASIS

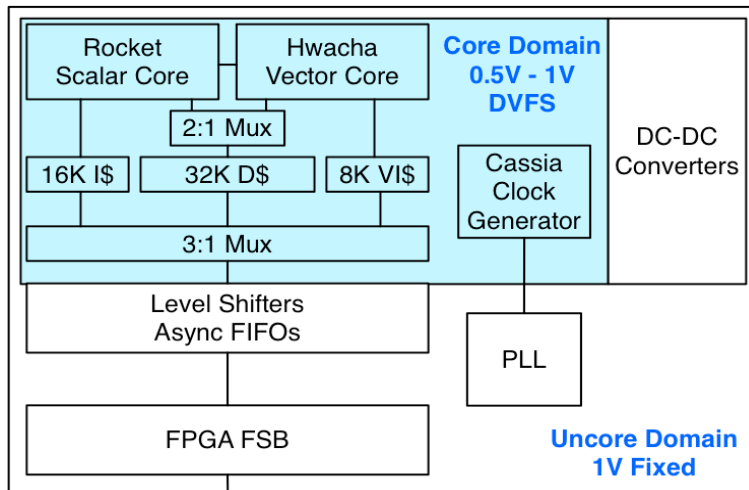
VERIFICATION

VERIFICATION



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

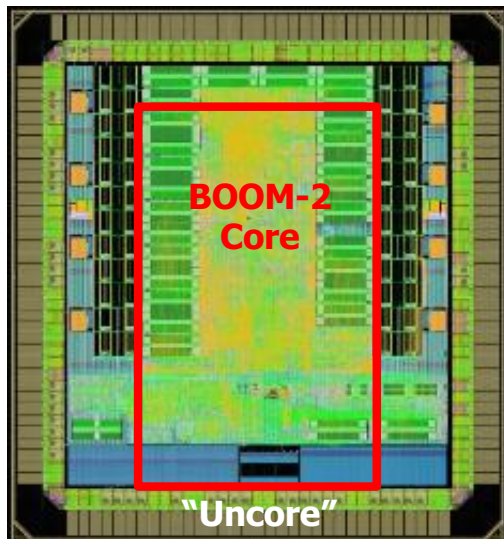


BOOM-2 RISC V Core

- 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"



Data from UC Berkeley RISC-V Center

BOOM-2 is a feasibility demonstration of an OOD flow on a small digital design in an academic environment.



Improving flexibility of DoD fabrication

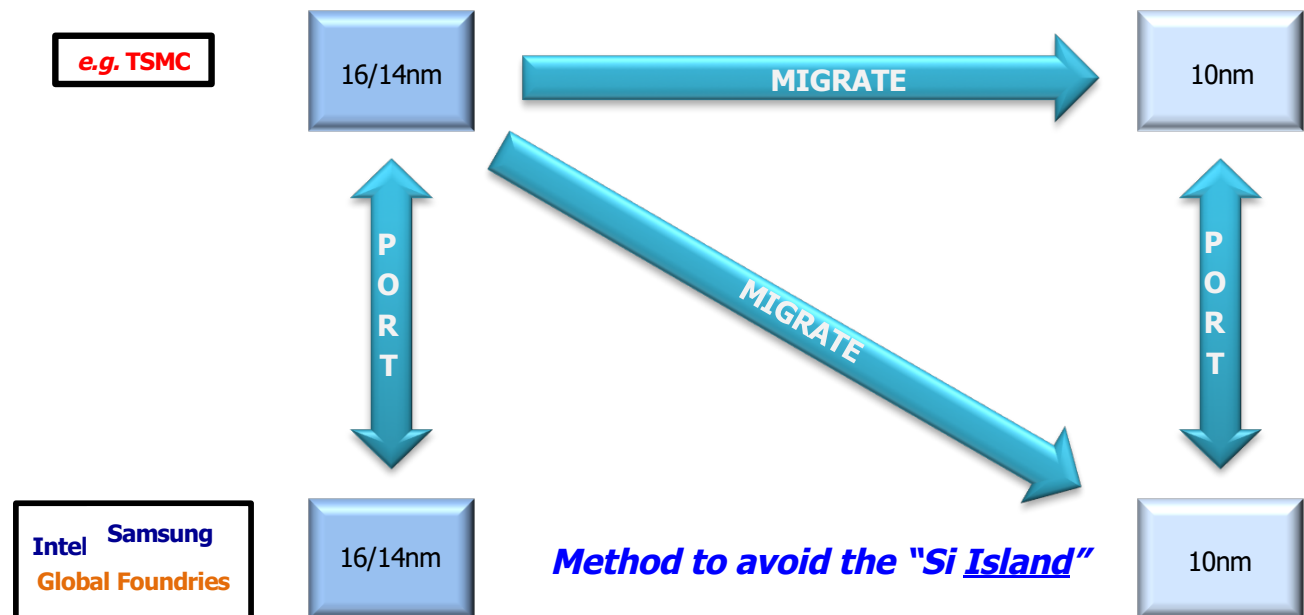
DESIGN

PORT/ MIGRATE

REPOSITORY

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

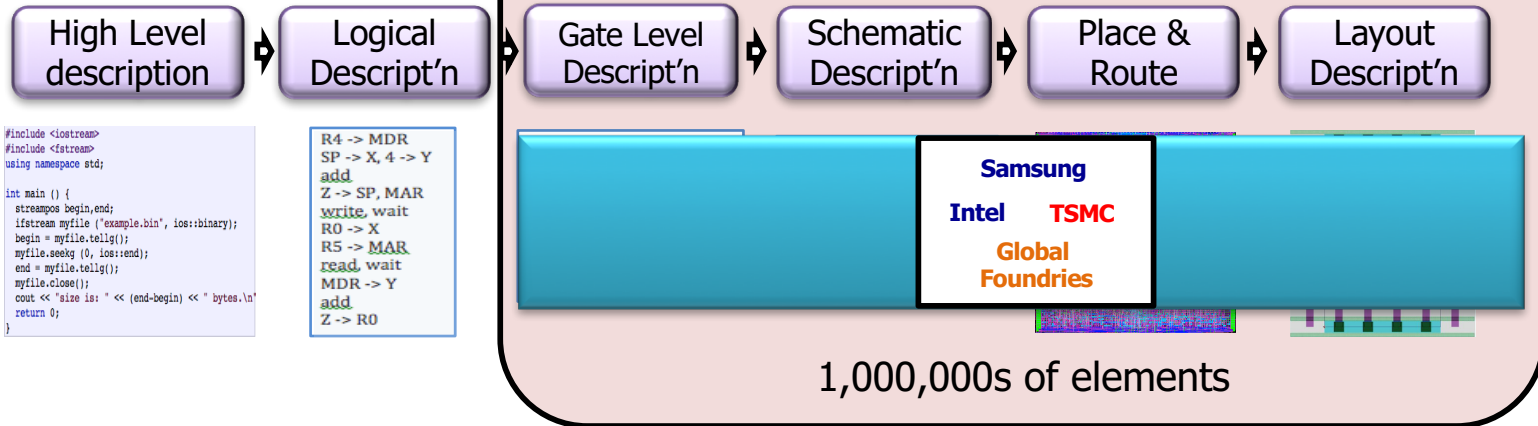


CRAFT aims to use new design flows to ensure multiple sources of supply and reduce node migration effort by 80%

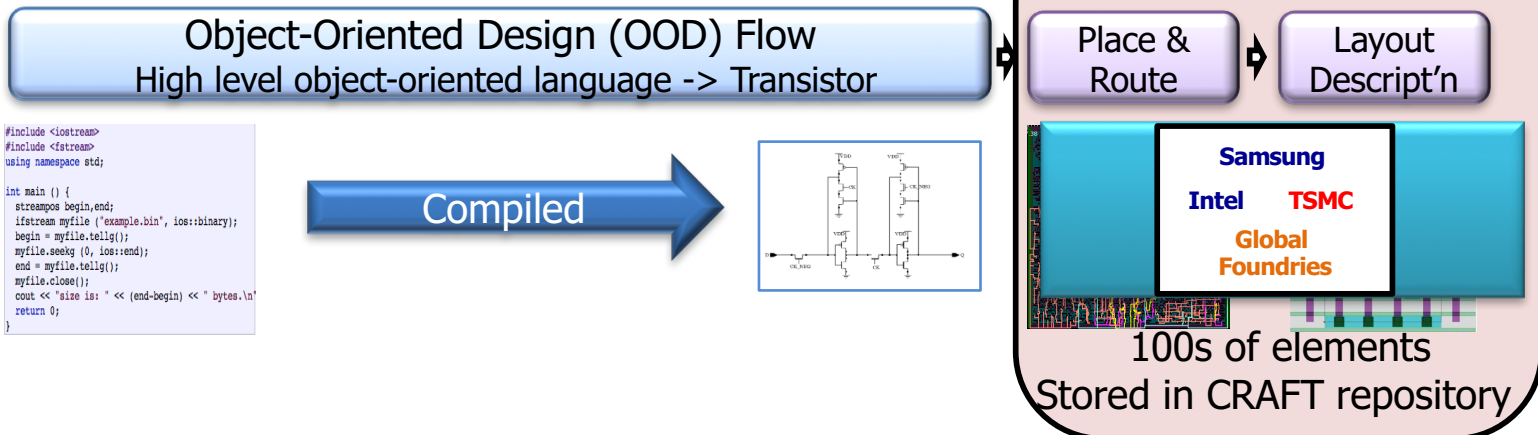


Facilitated port/migrate through use of the CRAFT OOD flow

Current ASIC Design Flow



New CRAFT Design Flow



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.



Repository

DESIGN

PORT/ MIGRATE

REPOSITORY

CRAFT aims to establish location for items required for DoD users of the OOD flow

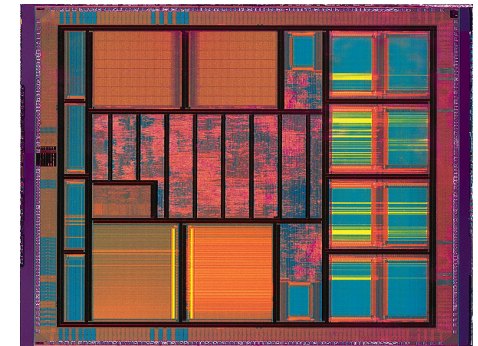
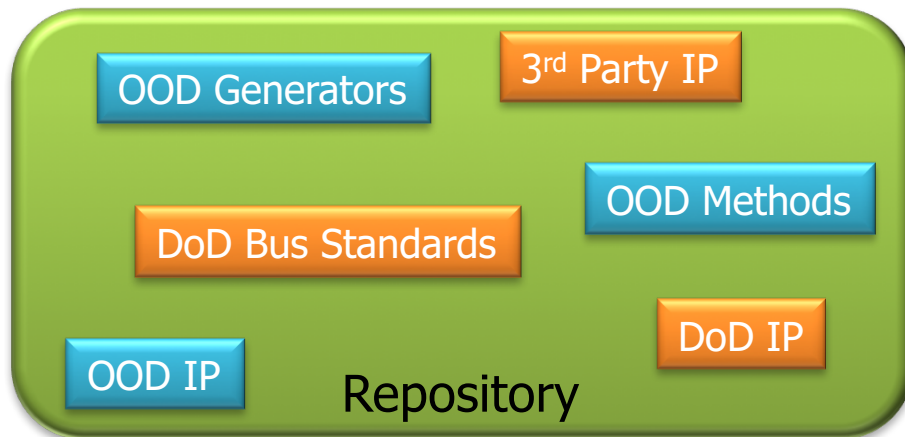


Image from Wikimedia Commons

OOD flow requirements

- OOD software, tools
- OOD components
 - Generators
 - Macros
 - OOD specific IP (eg. 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

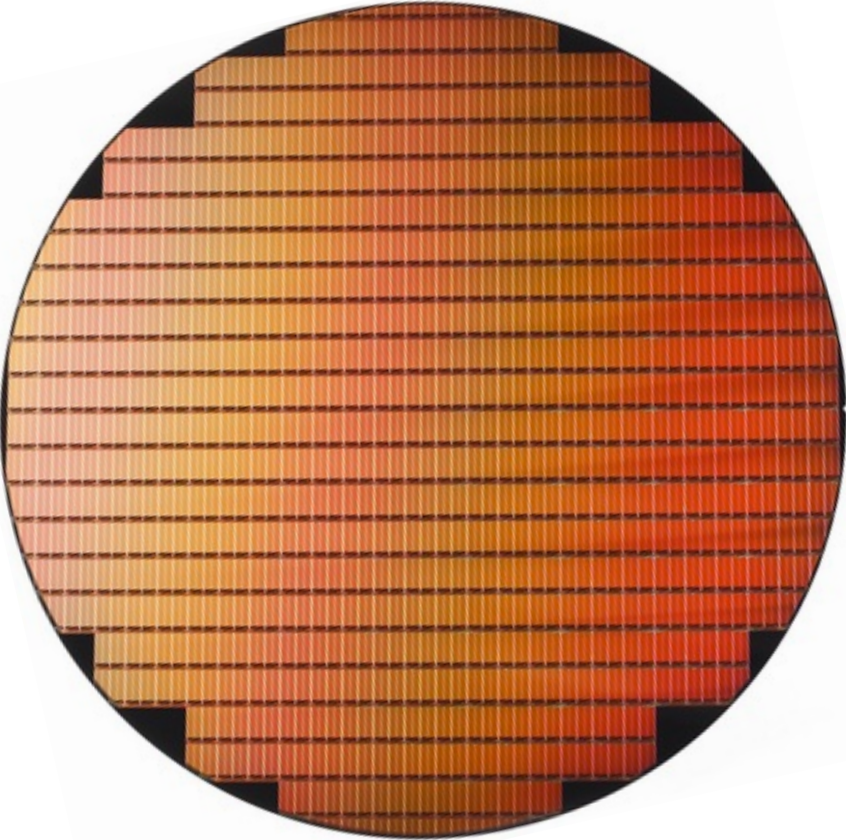
IP

- Foundry-provided IP (eg. SRAM bit cells, eFuse, ...)
- 3rd party IP (eg. logic library, memory compiler, ...)
- Government IP (eg. 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

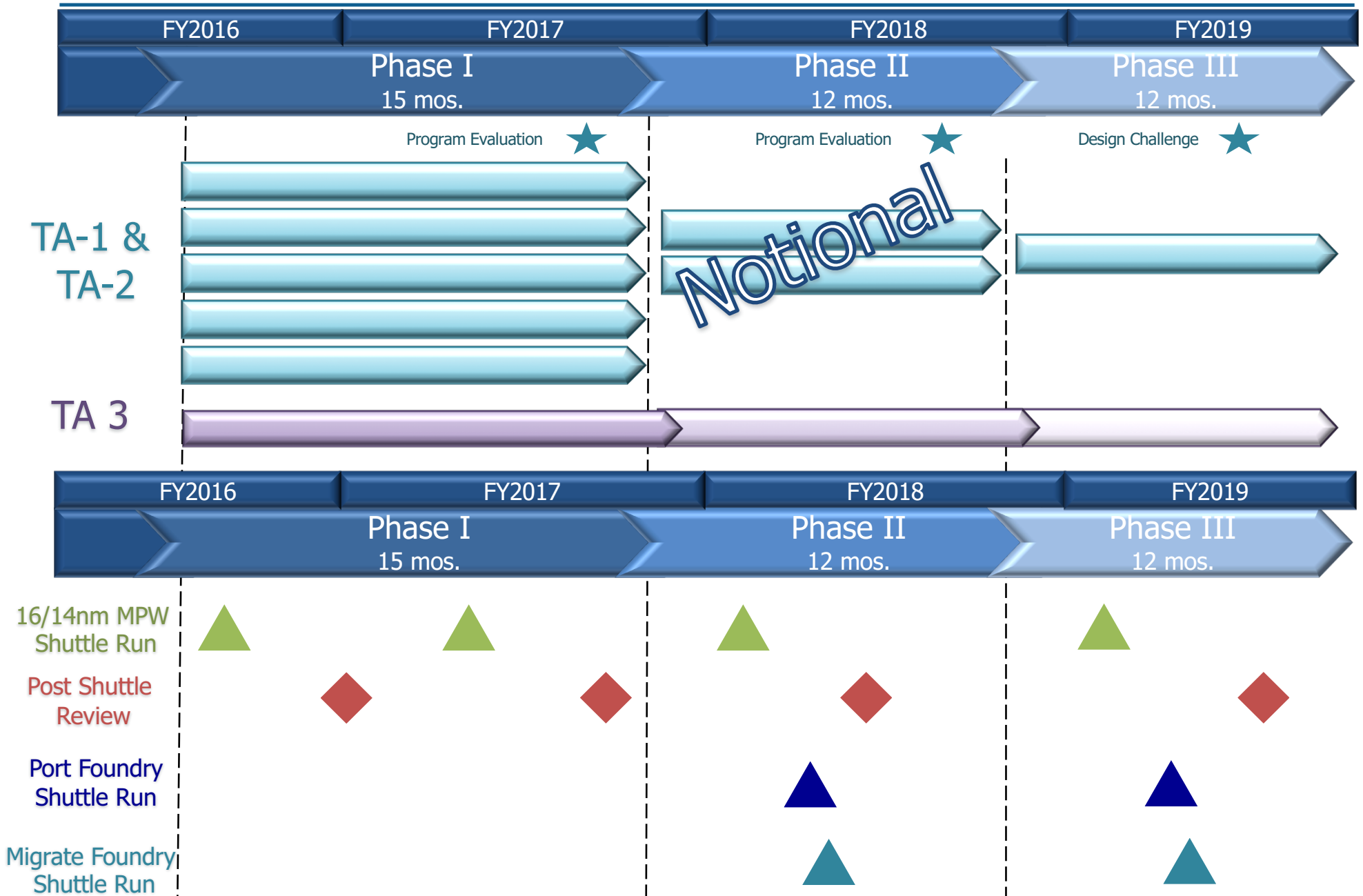


DARPA multi-project run (MPW) shuttle details

- **ALL runs available to ALL Defense Contractors**
 - Wafer diameter: 300mm
 - Single exposure area: 26mmX33mm
 - Exposures (shots)/wafer: ~80
 - Project area unit: 2.5mmX2.5mm
 - Projects/shot: ~100
- 
- A circular image of a 300mm wafer, showing a grid of exposure areas. The wafer is divided into a grid of small squares, each representing a project area. The colors of the squares vary from light orange to dark red, indicating different exposure levels or project areas.
- 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 (2.5mmX2.5mm)



CRAFT program plan





CRAFT performers

Prime	Prototype SoC	Anticipated Teams
UC-Berkeley	Multi-Application EW/Radar SoC	UC-Berkeley Northrop-Grumman Electronic Systems Cadence
Boeing	Multi-Application Reconfigurable DSP SoC	Boeing Stanford University UC-Los Angeles Totic Synopsys
Nvidia	Computer Vision Accelerator	Nvidia Harvard
Northrop-Grumman Aerospace Systems	High Performance Digital Receiver	Northrop-Grumman Aerospace Silicon Technologies Virginia Tech
UC-San Diego	Autonomous Vehicle Perception/ Decision SoC	UC-San Diego Cornell University of Michigan UC-Los Angeles
Carnegie-Mellon University	NA	Carnegie-Mellon University
USC/ISI	NA	USC/ISI Notre Dame University

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



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/mm² of die area
 - Die will be back within 6 months of design data delivery by users



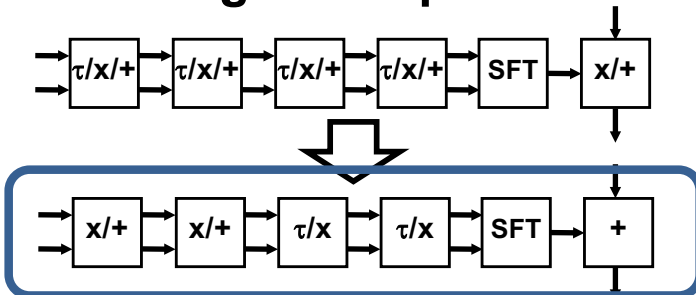
Securing designs in an open fabrication environment

- 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



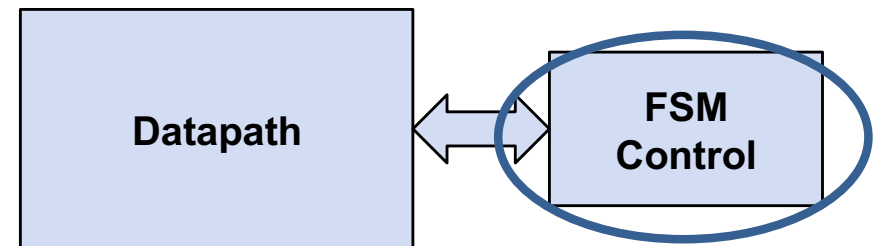
IC obscuration through personalization

Logic Datapath



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

Logic Datapath Control



- FSM can be obscured by using eFuses
- FSM obscuration obscures datapath use
- Control defined after personalization

Name of IP	Area Overhead	Power Overhead	Obfuscation Method
QR Decomposition (CLASS IC)	<1%	<1%	FSM
Eigen Value Decomposition (CLASS IC)	<1%	<1%	FSM
Communication Transmitter (CLASS IC)	<1%	<1%	FSM
Sparse Polynomial Equalizer (REDSOC IC)	<1%	<1%	Coefficient
Biquad Equalizer (REDSOC IC)	<1%	<1%	Coefficient
Nonlinear Equalizer (NLEQ IC)	<30%	<10%	Coefficient/Datapath
Sparse FFT (Sparse FFT IC)	<7%	<10%	FSM/Datapath

Source: MIT/Lincoln Laboratories



www.darpa.mil