A Perspective on the Role of Open-Source IP In Government Electronic Systems

Linton G. Salmon
Program Manager
DARPA/MTO

RISC-V Workshop

November 29, 2017
The US Department of Defense (DoD) Needs Custom SoCs

Future
New Architecture
New Technology

Neuromorphic Processor
11 TOPS/W (SONIC)

Current DoD
Existing Architecture
Older Technology
**Most of the Cost for DoD Custom SoCs is in Design**

<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 Costs are Skyrocketing

Transistors, log scale

Cost ($M)

- Transistors per chip, '000
- Design Cost
- Total HW Cost
- Verification Cost

Technology Node: 180, 130, 65, 45, 32, 22, 14

Distribution Statement “A” (Approved for Public Release, Distribution Unlimited)
Snapdragon is a compilation of designs from many sources
- Foundation IP (logic library, SRAM compiler, IO circuits)
- Internal IP (connectivity, DSP, GPU)
- Licensed IP (ARM CPU)
- 3rd party IP (Image processor)
Root Cause of Design Cost Growth is Complexity Growth

2016 average:
- 175 IP blocks
- 80% reuse

Source: Research Corporation, 2014

Distribution Statement “A” (Approved for Public Release, Distribution Unlimited)
Is Open-Source IP the Answer?
Open-Source IP Provides Strong Benefits for DoD

- Open-source IP can sharply reduce the resources, time, and complexity required for DoD custom SoC design
- Open-source IP can be easily used to design for unique DoD applications
- Detailed information available with open-source IP can enable greater trust
- Open-source IP permits increased use of unique DoD security approaches

Source: Linton Salmon
The Challenge

- The Open-Source community needs to develop a complete infrastructure
- Open-source IP needs to be more robust than is currently the case
- The community needs to develop a model to fund infrastructure
- The support model must assure long term support and continued development of open-source IP
Open-source IP can sharply reduce the resources, time, and complexity required for DoD custom SoC design

- Open-source IP can enable SoC specialization for unique DoD applications
- Detailed information available with open-source IP can enable greater trust
- Open-source IP permits increased use of unique DoD security approaches

Source: Linton Salmon
• Unique differentiation doesn’t require development of the entire platform
• Most of the content in custom DoD SoCs is composed of standard modules
  • The secret sauce is critical, but a small part of current design efforts
  • Low-volume DoD SoCs cannot support the commercial IP cost burden
• Open-source IP can address both the cost and availability of standard IP
• Open-source IP macros are a critical first step, but integration IP is also needed
• Widely accepted standards are required for distributed development
• DoD has a very wide variety of needs and applications
  • Wide differentiation in needs (large systems to IoT-like applications)
  • High-performance and low-power are the common characteristics
  • Die volumes are always low
• Open-source IP can provide the blocks and the standard infrastructure
• Differentiation is then easy and relatively inexpensive
  • Much of the design is already ready and can be reused
  • Design can focus on the areas requiring specialization
• Unique implementations are critical and specialization is required for success
Trust and RISC-V

- Open-source IP enables greater scrutiny by the DoD to ensure trust
  - Assurance that the SoC will work is provided by robust IP
  - Assurance that the SoC will only do as specified is provided through inspection

- Design and chip can be inspected in complete detail because all of the IP data are available for inspection
  - Can inspect and lock the implementation at C++, RTL, and/or GDS
  - DoD can control the locked implementation

- DoD can own the entire chip

*Source: Wikimedia Images and UC-Berkeley*
• Hardware security requires the ability to modify the SoC, including 3\textsuperscript{rd} party IP
  • Security against tampering
  • Security against cyber-attack
• DoD generally requires more extensive security than commercial applications
  • More extensive security enabled by open-source IP
  • Security levels do not require agreement by an extensive commercial community
• Added security capabilities require a robust base and infrastructure
DARPA Interest in RISC-V

RISC-V is adaptable
  - ISA is open-source
  - Many implementations are open-source

RISC-V is an open standard
  - Makes transition across the DoD easier
  - Standardization enables extensions to the open-source

RISC-V processors can be built in a way that can be trusted
  - Since open-source, full visibility and inspection is possible
  - DoD can control the IP completely

RISC-V can be used to enable increased security
  - Security extensions can be easily added
  - Security extensions can be close held as the core IP is standardized

Source: www.riscv.org
The Challenge

- The Open-Source community needs to develop a complete infrastructure
- Open-source IP needs to be more robust than is currently the case
- The community needs to develop a model to fund infrastructure
- The support model must assure long term support and continued development of open-source IP

Source: Wikimedia Images
• Required characteristics
  • The entire infrastructure – most of it is not enough
  • Robust infrastructure – must always work
  • Infrastructure must be easy to use
• Common infrastructure could be a great strength of RISC-V
  • ISA
  • Common processor implementations
  • Interconnect and associated IP
  • EDA design tools
Needs: Robustness and Dependability

- DoD requires robustness and dependability of the open-source infrastructure
  - Verification complete
  - Clear documentation on how to use
  - Robustness validated through Si implementation and test
  - Not the role or a strength of universities
- Savings requires the ability to depend on the open-source IP
- Savings require the robustness of the IP across extended performance ranges
A successful open-source infrastructure requires a lot of work
  • Work to design the correct IP modules
  • Work to maintain, upgrade, and facilitate use of the infrastructure
  • One reason the current model is so expensive

This large amount of work must be compensated in someway
  • Money
  • Other types of value
  • Not the role of DARPA – we fund projects, not infrastructure

Much of the work is difficult, but not exciting
Needs: Improvements over Time

- Open-source IP effort requires continual maintenance and improvement
  - Moore’s law has driven the expectation of continual improvement
  - A static technology will no longer be used
- Must update regularly
  - Performance
  - Architecture
  - Fabrication technology
- DoD time scales are 10-25 years
DARPA Programs Driving Open-Source IP

- Power Efficiency Revolution for Embedded Computing (PERFECT)
  - PM – Andreas Olofsson

- Circuit Realization at Faster Timescales (CRAFT)
  - PM – Linton Salmon

- System Security Integrated Through Hardware and Firmware (SSITH)
  - PM – Linton Salmon

- Posh Open Source Hardware (POSH)
  - PM – Andreas Olofsson

- Intelligent Design of Electronic Assets (IDEA)
  - PM – Andreas Olofsson
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 Ghetto.”

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.
Today: Patch and Pray
*2800 vulnerability instances
2800 software patches

Future: SSITH
SSITH will protect against all 7 hardware classes

Legend
- Open Vulnerability
- Block Vulnerability
- Open to Attack
- Blocked Attack

Develop hardware design tools and IP to provide inherent security against hardware vulnerabilities that are exploited through software in DoD and commercial electronic systems.

*2015 MITRE-recorded hardware vulnerabilities (CVE)

Distribution Statement “A” (Approved for Public Release, Distribution Unlimited)
IDEA and POSH

**Intelligent Design of Electronic Assets (IDEA)**

**Posh Open Source Hardware (POSH)**
- An open source System on Chip (SoC) design and verification eco-system that enables cost effective design of ultra-complex SoCs.

The 1980’s DARPA MOSIS effort removed fab cost and fab access barriers and launched the fabless industry. The ERI Design effort will address today’s design complexity and cost barriers, creating the environment needed for the next wave of US semiconductor innovation.