Field Programmable Gate Array (FPGA) Assurance

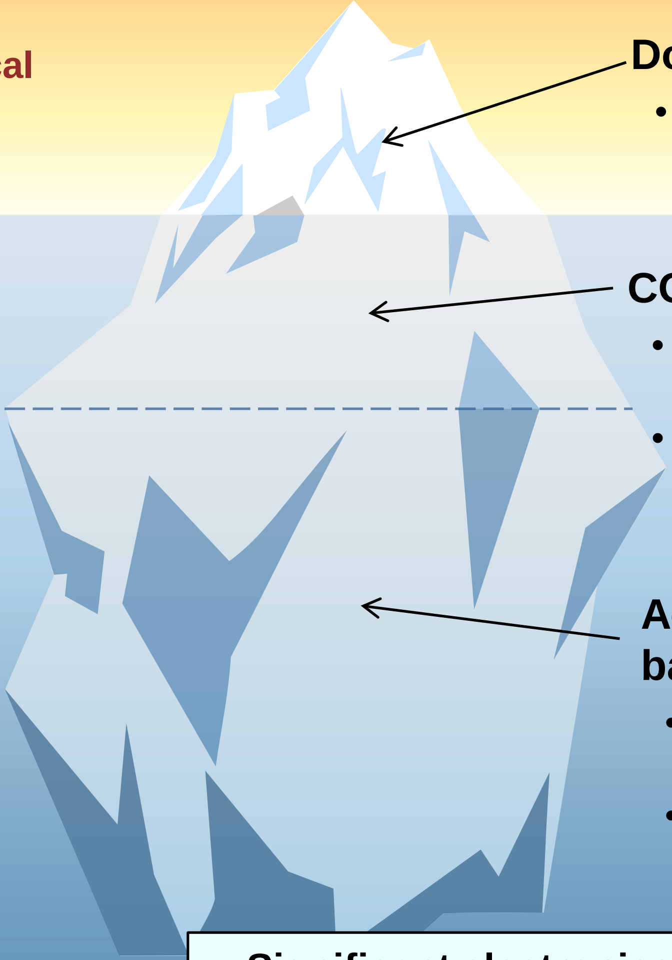
Raymond C. Shanahan
Deputy Director, Anti-Tamper/Hardware Assurance
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

20th Annual NDIA Systems Engineering Conference
Springfield, VA | October 26, 2017

Electronics as a Strategic Issue

Current Tactical Issue

Larger Strategic Issue



DoD Trusted Electronics Issue

- **Options for domestic trusted manufacture of custom DoD electronics are diminishing**

FY03-present: DoD Trusted Foundry Program

COTS Electronics Assurance (DoD & Beyond†)

- **Most COTS electronics used in DoD systems are fabricated overseas; significant risk from tamper**
- **Risks similar for the broader national security community, banking, critical infrastructure, etc.**

PB 2017: Trusted & Assured Micro-electronics

Access to Electronics / Electronics-based economic growth

- **Shift in electronics fabrication creates potential for overseas control**
- **End of Moore’s Law potential carries economic impacts**

PB 2018/ POM 19: Microelectronics Innovation for National Security and Economic Competitiveness

Significant electronics challenges represent a strategic level national issue

† Including the broader national security community, banking, critical infrastructure, commercial industry, etc.

Need for Assured FPGA Functionality

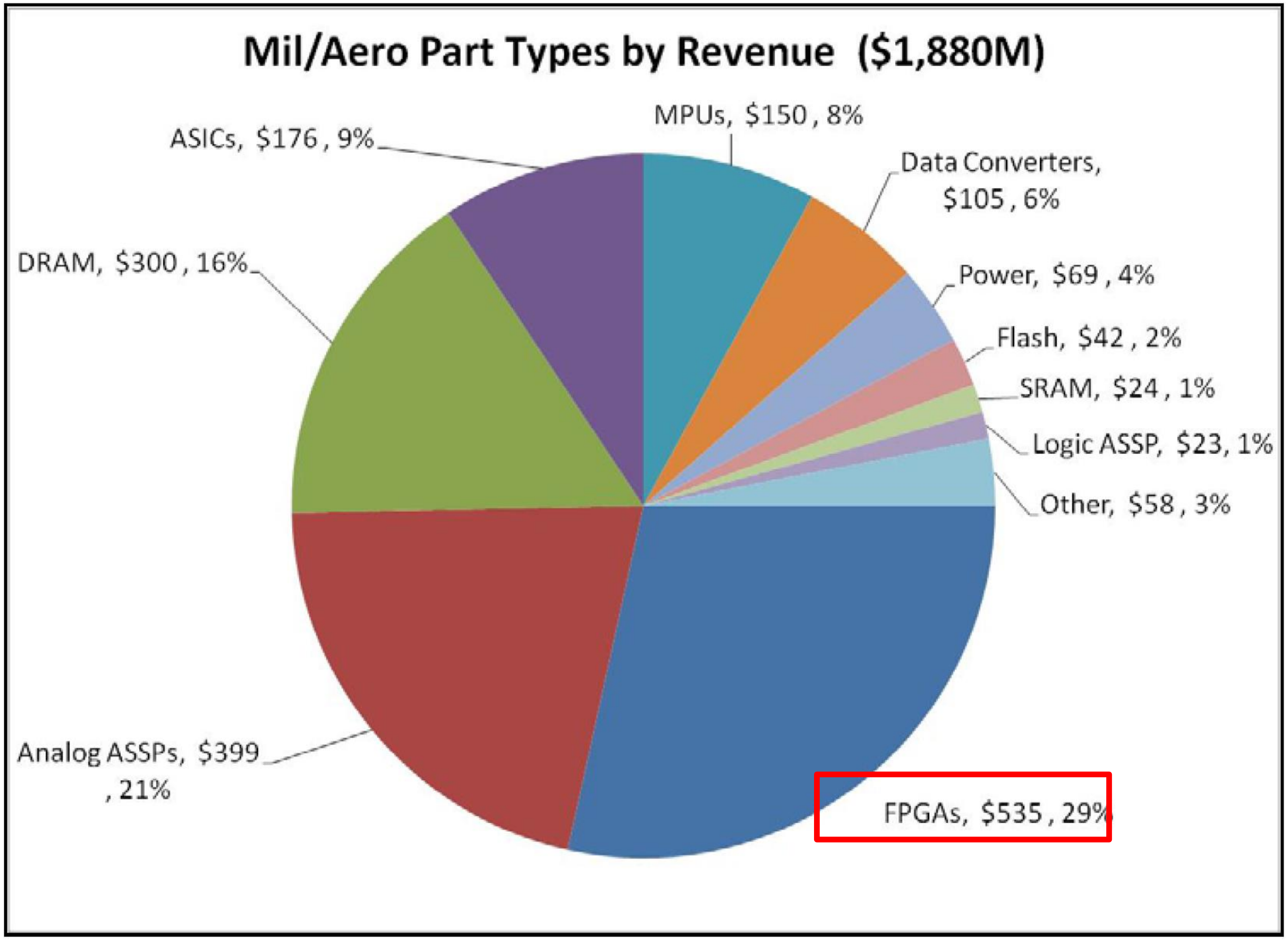
- **Commercial FPGAs are in widespread use across National Security Systems (NSSs) in embedded, special purpose applications**
  - Programmable nature of FPGAs and System on Chips (SOCs) make them vulnerable to cyber malware and malicious insertion
- **While Application-Specific Integrated Circuits (ASICs) have performance of ten to a thousand times that of FPGAs, FPGAs are seen as achieving custom hardware performance without the high manufacturing cost of custom ASICs**

FPGA applications:

- Communication systems
- UAVs
- Tactical robotics
- Radar systems
- Missile control
- Satellites
- Ships
- Vehicle control systems
- Other

Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-0031 applies. Distribution is unlimited.

FPGA Usage by Revenue in Military/Aerospace Sector



Source: IDA report, Examination of DoD's Use of Microelectronics in Weapon Systems, 2013

Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-0031 applies. Distribution is unlimited.

Policy Requirement for Trust vs. Assurance

- **There is no policy requirement in DoDI 5200.44 for a Trusted FPGA or other COTS product; only ASICs as follows:**
  - "In applicable systems, integrated-circuit-related products and services shall be procured from a trusted supplier using trusted processes accredited by the Defense Microelectronics Activity (DMEA) when they are custom-designed, custom-manufactured, or tailored for a specific DoD military end use (generally referred to as application-specific integrated circuits (ASIC))."
- **However, there are policy requirements for assurance in DoDI 5200.44, to include the following of particular relevance to FPGAs:**
  - "Mission critical functions and critical components within applicable systems shall be provided with assurance consistent with criticality of the system, and within their role within the system."
  - "Control the … security of software, firmware, hardware, and systems throughout their lifecycles, including components or subcomponents from secondary sources. Employ protections that manage risk in the supply chain for components or subcomponent products and services (e.g., integrated circuits, field-programmable gate arrays (FPGA), printed circuit boards) when they are identifiable (to the supplier) as having a DoD end-use."
  - "Detect the occurrence of, reduce the likelihood of, and mitigate the consequences of unknowingly using products containing counterfeit components or malicious functions in accordance with DoDI 4140.67"
  - "Detect vulnerabilities within custom and commodity hardware and software through rigorous test and evaluation capabilities, including developmental, acceptance, and operational testing"

Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-0031 applies. Distribution is unlimited.

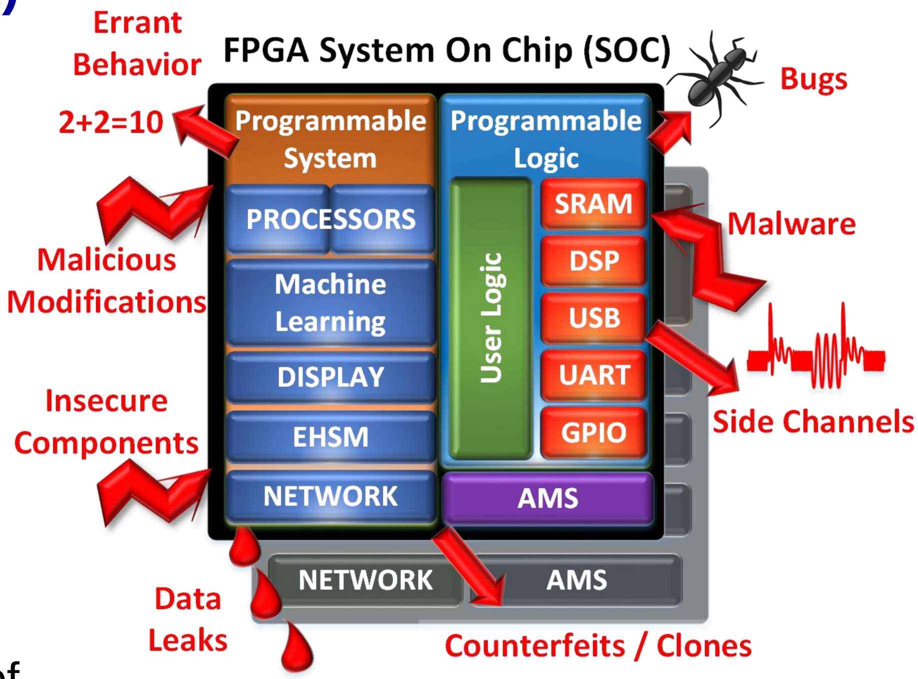
Definitions of Trust and Hardware Assurance

- **The NDAA FY2017 Sec. 231 trust definition below reflects DASD(SE)'s working definition of the term, "hardware assurance (HwA)"**
  - The other trust definition below is used by the DoD Trusted Foundry Program
- **Planned update of DoD Instruction (DoDI) 5200.44 needs to add, clarify, and harmonize the definition(s) of HwA and/or trust**
  - Needed to eliminate existing confusion in the community between what constitutes trust versus HwA; sometimes referred to as "big T" versus "little T" trust or assurance
  - These definitions do not compete with one another, but can be complementary if integrated and harmonized into an internally consistent definition or set of definitions within DoDI 5200.

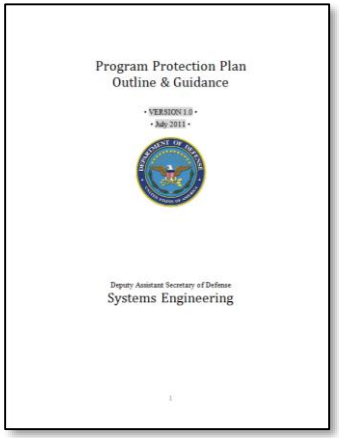
2004 AT&L Memorandum	NDAA FY2017 Sec. 231
trust: "the confidence in one's ability to secure national security systems by assessing the integrity of the people and processes used to design, generate, manufacture and distribute national security critical components"	**trust:** "with respect to microelectronics, to the ability of the Department of Defense to have confidence that the microelectronics function as intended and are free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during its lifecycle"

FPGA/SOC Assurance Risks

- **Commercial FPGA/SOC security, third party intellectual property (3PIP), and Electronic Design Automation (EDA) tools are largely unverified**
- **Industry unlikely to invest unless encouraged**
- **Some Military/Aerospace and specialty needs are not being met**
- **DoD uses FPGAs heavily in critical systems and many potential vulnerabilities exist**
  - Potential for compromise of IP confidentiality and/or integrity, or EDA tool integrity, from design through deployment
  - Inconsistencies and uncertainty/lack of clarity in methods, policy, and enforcement
  - Supply chain threat and vulnerability awareness is poor



Advancing Hardware Assurance



Program Protection Plan
Outline & Guidance

• VERSION 1.0 •
• July 2011 •

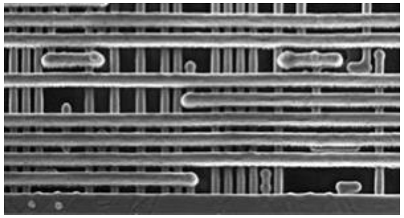
Deputy Assistant Secretary of Defense
Systems Engineering

1

Policy

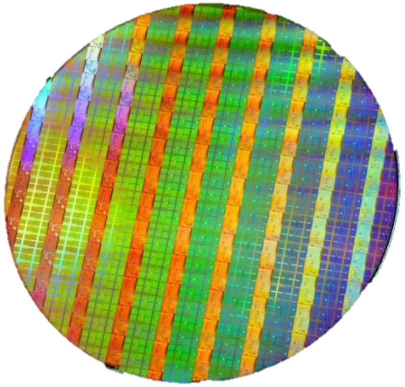
- DoD Instruction (DoDI) 5000.02
- Program Protection Plan (PPP)
- International Traffic in Arms Regulations (ITAR) update (in work)

```
private static boolean needsXmlnsAttributes() {
    try {
        StringWriter writer = new Str
        TransformerHandler probe                    sformerHandler();
        probe.setResult(new St
        probe.startDocument(
        probe.startPrefixMa
        probe.startElement                        utesImpl());
        probe.endElement("
        probe.endPrefixMap
        probe.endDocument(
        return writer.toSt
    } catch (Exception e)
        throw new Unsupporte                     ls");
    }
}
```



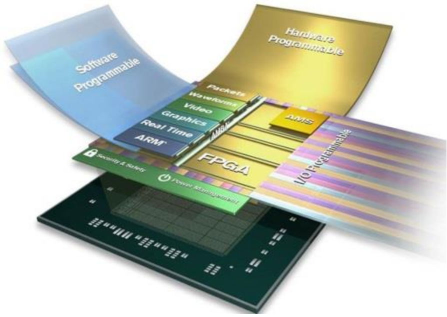
Joint Federated Assurance Center

- Software assurance Know-how & tools
- Hardware assurance Know how & tools
- Advanced V & V capabilities
- Firmware Assurance planning



Trusted & Assured Microelectronics

- Access to state-of-the-art foundries
- Trust and assurance methods and demonstration
- Industrial best practices for assurance
- Implement & Demo



COTS and FGPA

- Supply chain risk management
- FPGA Assurance Strategy
- Radiation hardened microelectronics initiative

Microelectronics Trust Verification Technologies

Design Verification

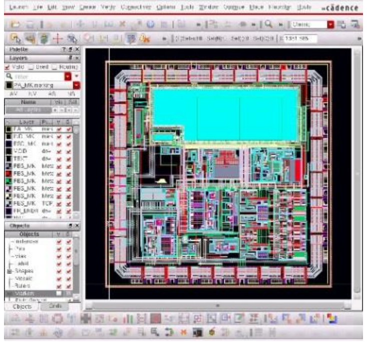
- Verification/assurance of designs, IP, netlists, bit-streams, firmware, etc.

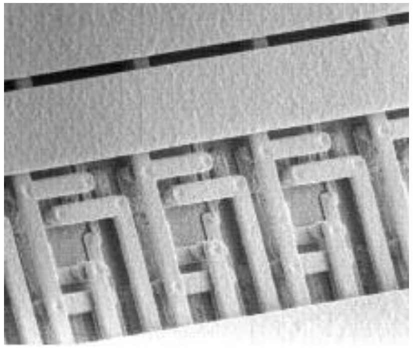
Physical Verification

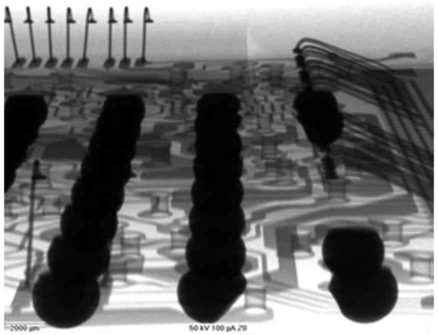
- Destructive analysis of ICs and Printed Circuit Boards

Functional Verification

- Non-destructive screening and verification of select ICs

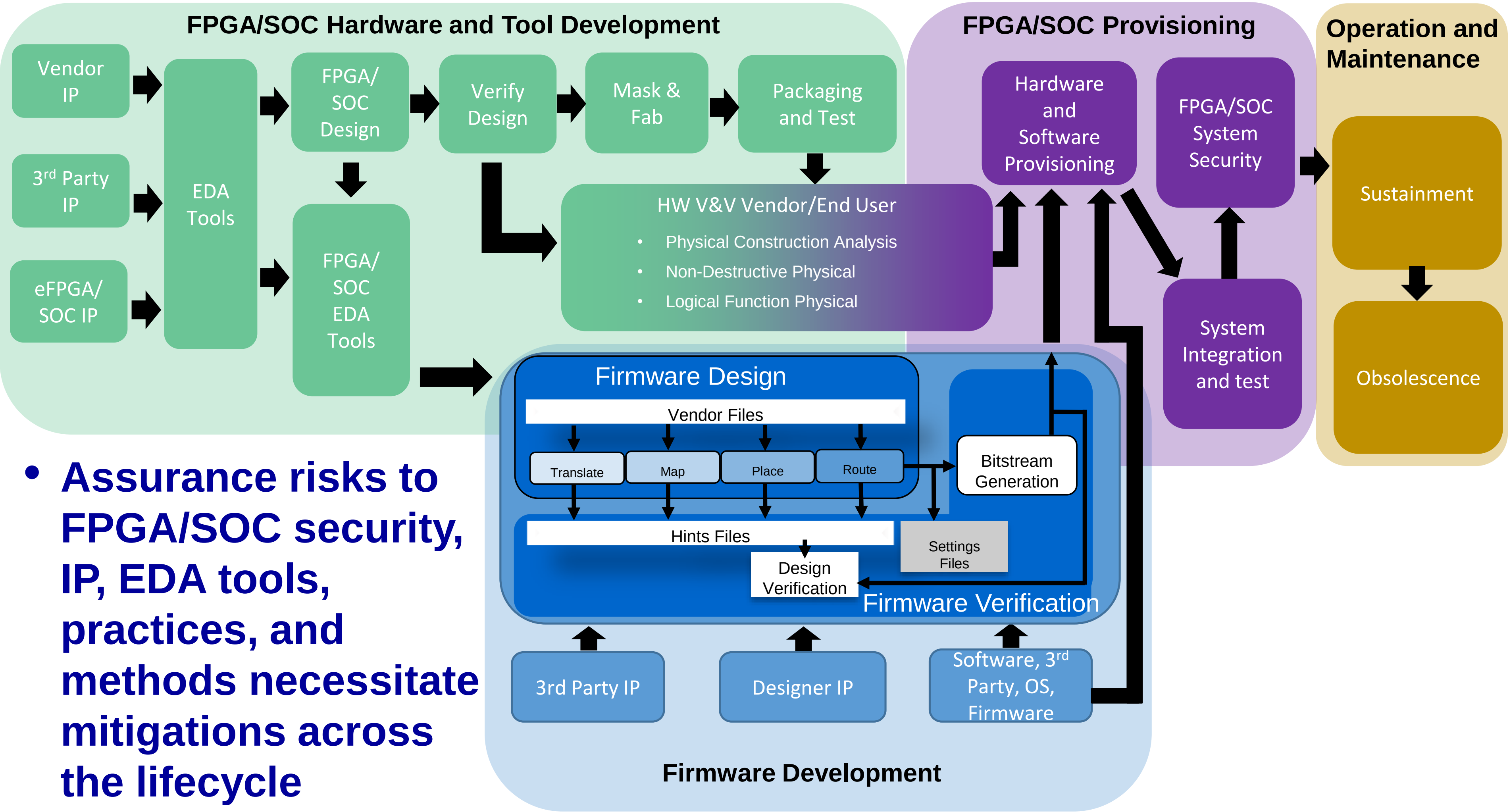






DoD, Intelligence Community, and DoE enhancing capability to meet future demand

FPGA/SOC Lifecycle Map

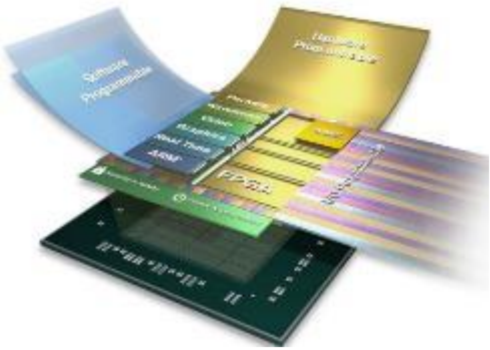


- **Assurance risks to FPGA/SOC security, IP, EDA tools, practices, and methods necessitate mitigations across the lifecycle**

Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-0031 applies. Distribution is unlimited.

FPGA Assurance Strategy Overview

- **DASD(SE) continues to refine the strategy to address FPGA assurance risks in coordination with the Joint Federated Assurance Center (JFAC) HwA Technical Working Group (TWG) and the Trusted and Assured Microelectronics (T&AM) program**
  - Leverage existing USG and industry efforts to the maximum extent possible
  - Promote community awareness of related USG efforts via a series of workshops and conference
  - As a community, continuing to identify and refine the portfolio of assurance efforts to focus on with the goal of synchronizing and eliminating stove-pipes and separate, single-point solutions when possible
  - Identify gaps and/or activities requiring investment and elevate relevant needs to the JFAC Steering Committee for prioritization and direction regarding resourcing
  - In particular, align with, and inform, the execution plan for the T&AM program



FPGA Assurance Strategy has multiple FPGA Assurance Focus Areas across the FPGA Lifecycle

		FPGA/SoC Hardware Development · FPGA/ Firmware Development · FPGA/SoC Provisioning · Operation & Maintenance
AVAILABILITY	DoD Specific Needs	Increase availability for DoD specific needs in Military/Aerospace, e.g., Strategic Radiation-Hardened (SRH) technologies, and other domestic manufacturing needs
	Leverage Related Efforts	Coordinate with other major efforts across the DoD, Intelligence Community (IC), the broader United States Government (USG), industry, and academia. For example: • Defense Production Act (DPA) Title III Trusted FPGA • Trust in FPGA Studies • Aerospace Terms of Reference (TOR) related to assured FPGA and ASIC development
ACCESS	Supply Chain Threat	Enhanced interaction with the IC to provide more specific threat information to enable enhanced threat assessment and vulnerability analysis
	Industry Engagement	Engage FPGA manufacturers, EDA, 3PIP, and other vendors to facilitate: • USG IV&V access to timely/detailed supply chain information, e,g., design, chain of custody, etc. • Design tool and 3PIP distribution and enterprise usage • Verification features in the design or that are enabled by the design tools • Commercial verified and validated security features, EDA tools, 3PIP or other supply chain tools
	Policy and Guidance (P&G) and Standards	Develop, contribute to, and/or adopt P&G and standards that promote best practices across DoD and other USG acquisition programs as well as industry to the extent possible • Facilitate use of commercially viable/supportable tools, IP, and best practices where possible
ASSURANCE	Independent Verification And Validation (IV&V)	Expand JFAC IV&V capability and capacity for physical, functional and design V&V to be offered to clear contractors and USG acquisition programs, leverage co-development, data access, design for assurance, and other best practices to enable better V&V
	New HwA Techniques and Tools	Develop and facilitate the transition of new HwA techniques and tools to verify and validate, protect the confidentiality and integrity of, and gain insight into the chain of custody of, IP, EDA tools, and the FPGAs/SOCs themselves

FPGA Activities and Investments

Overall

Inputs

- Established relationships and programs with FPGA and other vendors
- JFAC labs, FFRDCs, expertise
- Other USG partners and commercial suppliers
- Programs and COTS parts

Investments & Actions

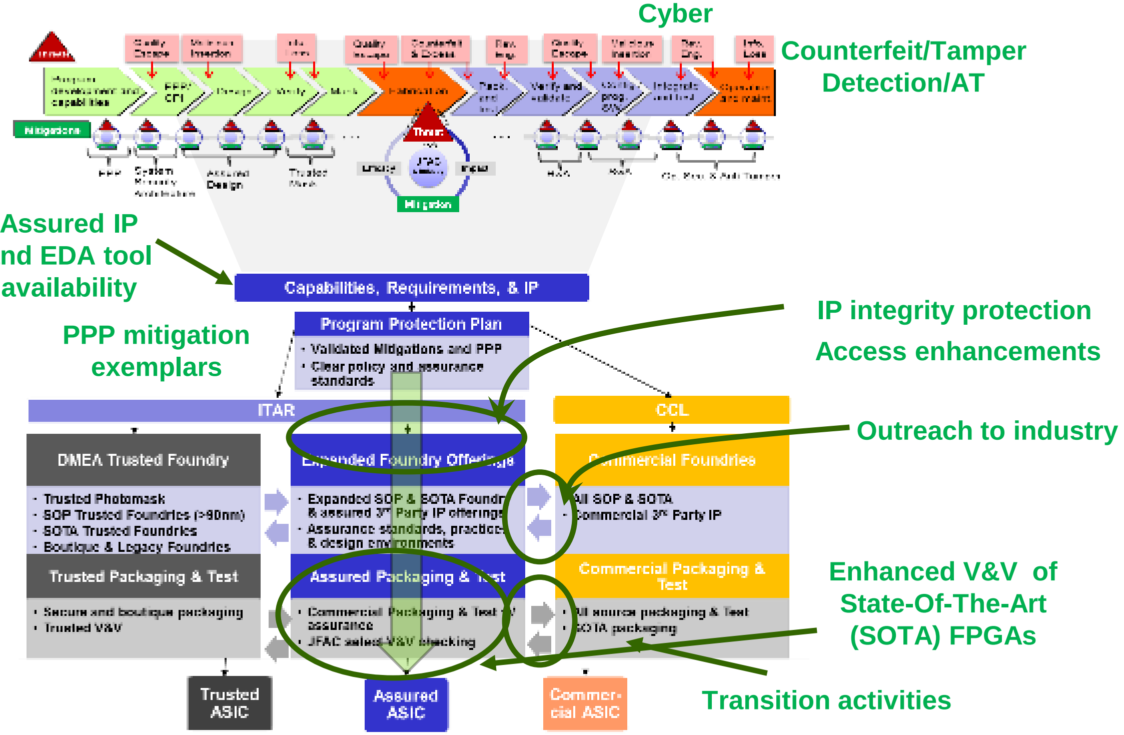
- EDA tool and 3PIP V&V development
- Physical V&V tool and capability development
- Security and assurance architecture development
- Radiation testing and validation

Outcomes

- USG and third party EDA and 3PIP V&V tools
- JFAC-assessed FPGA list, IV&V tools, vulnerability assessments
- Counterfeit and SCRM tools
- P&G, standards, and best practices, PPP
- SRH assessments

Investment Breakout

Availability	Access	Assurance
15.0%	18.9%	66.0%



Cyber

Counterfeit/Tamper Detection/AT

Assured IP and EDA tool availability

PPP mitigation exemplars

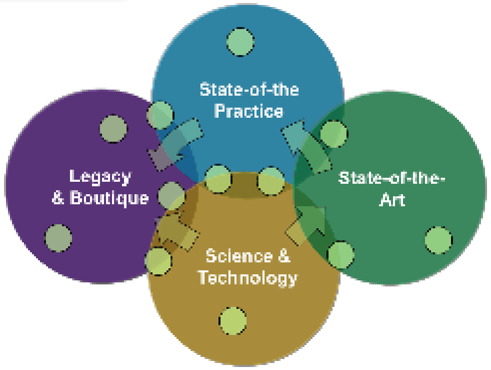
IP integrity protection

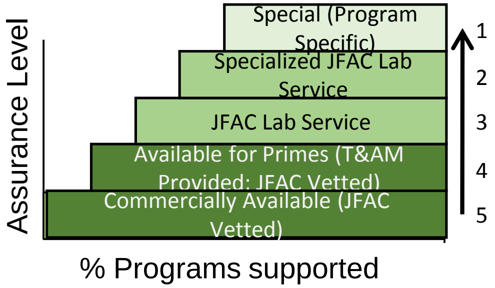
Access enhancements

Outreach to industry

Enhanced V&V of State-Of-The-Art (SOTA) FPGAs

Transition activities

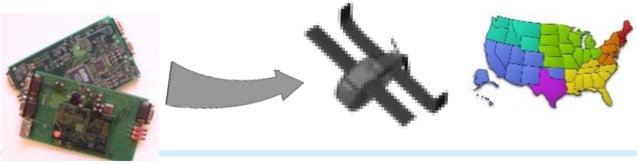
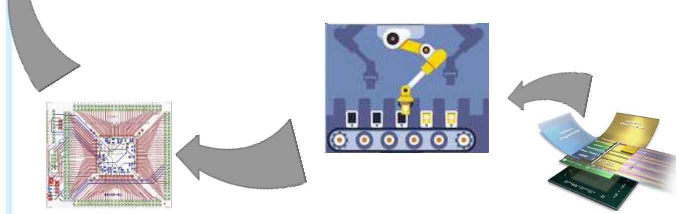
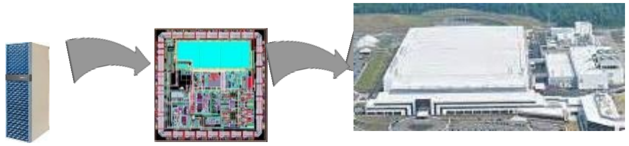




Special (Program Specific)
Specialized JFAC Lab Service
JFAC Lab Service
Available for Primes (T&AM Provided: JFAC Vetted)
Commercially Available (JFAC Vetted)
1
2
3
4
5
Assurance Level
% Programs supported

Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-0031 applies. Distribution is unlimited.

FPGA Strategy Outcomes

	Problem	Actions & Investments	Outcomes
Availability	• DoD influence is limited and national security needs not satisfactory for required production and volume	• Support domestic, manufacturing of SOTA FPGAs and industrial engagement for USG and strategic growth application areas, including radiation-hardening, high voltage, etc.	• Availability of assured SOTA FPGAs, tools, and IP for USG acquisition programs 
Access	• Potential for compromise to confidentiality and integrity through design access, COTS insertion, and deployment of commercial FPGA creates risk when USG accesses SOTA FPGA	• Evaluate and adopt best practices, and specialized tools and services to assure integrity and confidentiality of IP	• Enhanced USG access to assured SOTA FPGAs, IP, and EDA tools 
Assurance	• DoD uses FPGAs heavily in critical systems and many potential vulnerabilities exist	• Provide USG HwA community with access to, or knowledge of, assured USG IP, 3PIP, EDA tools, experts, secure computing, techniques, etc. for innovation 	• Assurance throughout the FPGA/ SOC lifecycle through secure design environments, best practices, V&V and supply chain tools, and specialized services 

Leverage Related Efforts

- **Trust in FPGA Studies**
- **JFAC HwA TWG efforts**
- **Defense Production Act (DPA) Title III Trusted FPGA Projects**
  - In FY17, DPA Title III Phase 1 worked with FPGA vendors to develop product strategies to allow USG to assure FPGAs
  - In FY18, Phase 2, planned start of implementation of those product strategies
- **Defense Microelectronics Activity (DMEA) Trusted FPGA Study**
  - Congressional Add to engage major vendors
- **Anti-Tamper Executive Agent-related technology development**
- **Printed Circuit Board and Interconnect Technology Executive Agent technology development**

Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-0031 applies. Distribution is unlimited.

Leverage Related Efforts (cont’d)

- **NSA/R2-sponsored FPGA Trust & Integrity Research**
  - Aerospace documenting this research. Final product in FY17
- **Mission Assurance Improvement Workshop (MAIW) and Aerospace Terms of Reference (TOR)**
  - FPGA assurance-related TORs for design, Trust Assurance, and SME training in development
  - Other FPGA and ASIC related TORs already completed
- **National Defense Industrial Association FPGA Assurance Workshops**
- **Intelligence Advanced Research Projects Activity Trusted Integrated Circuit (TIC) Phase 3**
  - FPGA developed using split fabrication
- **Defense Advanced Research Projects Agency programs**

Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-0031 applies. Distribution is unlimited.

The Way Ahead

- **Program engagement**
  - Foster early planning for HwA and SwA, design with security and assurance in mind
  - Implement expectations in plans and on contract
  - Support vulnerability analysis and mitigation needs
- **Community collaboration**
  - Achieve a networked capability to support DoD needs: shared practices, knowledgeable experts, and facilities to address malicious supply chain risk
- **Industry engagement**
  - Communicate strategy to tool developers and develop standards for common articulation of vulnerabilities and weaknesses, capabilities and countermeasures
  - Co-development of next generation COTS with DoD capabilities and assurance considered
- **Advocate for R&D**
  - HwA and SwA tools and practices
  - Strategy for trusted microelectronics, to include FPGAs/SOCs, that evolves with the commercial sector
- **People!**
  - Improve awareness, expertise to design and deliver trusted systems

Systems Engineering:
Critical to Defense Acquisition

Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering
http://www.acq.osd.mil/se

For Additional Information

Raymond C. Shanahan

Deputy Director, Anti-Tamper/ Hardware Assurance

ODASD, Systems Engineering

571-372-6558

raymond.c.shanahan.civ@mail.mil

E-mail – osd.pentagon.ousd-atl.mbx.fpga-assurance@mail.mil

JFAC Portal -- https://jfac.army.mil