The National Academies of
SCIENCES · ENGINEERING · MEDICINE

AIR FORCE STUDIES BOARD

Optimizing the Air Force Acquisition Strategy of Secure and Reliable Electronic Components

The Workshop Tasking

- Define the current technological and policy challenges with maintaining a reliable and secure source of microelectronic components
- Review the current state of acquisition processes within the Air Force for acquiring reliable and secure microelectronic components
- Explore options for possible business models within the national security complex that would be relevant for the Air Force acquisition community

In accordance with established workshop practice, the committee did not provide consensus recommendations

Workshop Committee

- ROBERT H. LATIFF, RLatiff Associates, *Chair*
- MICHAEL ETTENBERG, Dolce Technologies
- CRAIG L. KEAST, MIT Lincoln Laboratory
- RANDAL W. LARSON, MITRE Corporation
- TERRY P. LEWIS, Raytheon Company
- CELIA MERZBACHER, Semiconductor Research Corporation
- BERNARD S. MEYERSON, IBM
- PAUL D. NIELSEN, Software Engineering Institute
- STARNES E. WALKER, University of Delaware

Staff

- Joan Fuller, Air Force Studies Board Director
- Carter W. Ford, Responsible Staff Officer
- Marguerite E. Schneider, Administrative Coordinator
- Dionna C. Ali, Research Assistant

Workshop Presentations

SAF/AQR (Dr. Walker)	ASD (SE) (Ms. Baldwin)
NIST (Mr. Boyen, Ms. Paulsen)	DARPA MTO (Dr. Bernstein)
AFSPC/SMC (Mr. Davis)	DMEA (Mr. Marrujo)
IDA (Dr. Cohen)	NSWC (Mr. Hamilton)
AFOSI (Mr. Lyden)	MITRE (Dr. Goldman)
Aerospace (Dr. Yarborough)	NDIA SSE (Ms. Dunlap)
DOE/NSC (Mr. Devenport)	IBM (Dr. Meyerson
IARPA (Dr. McCants)	

The Electronics Landscape

- Continued and accelerating globalization of microelectronics industry presents national security program designers with challenge of how to ensure components operate as designed

- Contributing to a growing inability to either understand or assure system security and reliability:
  - off-shoring of parts manufacture
  - decreased DoD influence on the industry due to a small comparative demand
  - diminished U.S. expertise

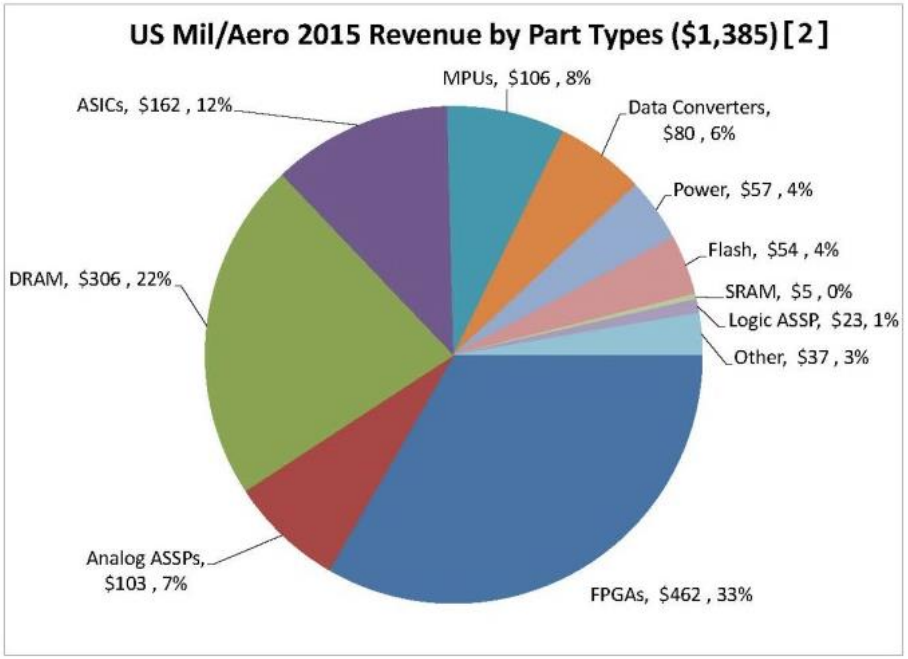
Microelectronics in DoD Systems

DOD Buys ~ 5B in microelectronics [1]

- 3.6-$4.1B in COTS
- ~$1-1.5B in Mil/Aero

Important Risk Segments

- ASICs (12%)
- FPGAs (33%)
- Analog+Logic ASSPs (8%)
- Data Converters (6%)
- Military Specific DSPs and Processors (8%)
- Memories (26%)



Sources: [1] IDA Assessment and [2] dataBeans 2014, All data projected for 2015

Application Specific Standard Product (ASSP) - an integrated circuit (IC) dedicated to a specific application market and sold to more than one user. A type of IC with embedded programmable logic, combining digital, mixed-signal and analog products. When sold to a single user, such ICs are ASICs (Gartner)

SOURCE: Dr. Brian Cohen, IDA, presentation to the workshop.

Supply Chain Risks

DoD Program Protection focuses on risks posed by malicious actors

SOURCE: Ms. Kristen Baldwin, ASD (SE), presentation to the workshop.

Key Workshop Themes

- DODI 5200.44
- Program Protection Policies
- Emerging Counterfeiting Capabilities
- Acquisition System Implementation
- Physical Limits of Current Technology
- Trusted Foundry Model
- New Fabrication Methods

Key Theme 1: DoDI 5200.44

- DoDI 5200.44 has impacted DoD's approach to Supply Chain Risk Management (SCRM)
  - enforcing an updated approach to program protection planning;
  - expanding the mission of DMEA;
  - requiring ASICs to be supplied by a trusted foundry;
  - enabling AFOSI to investigate domestic companies and U.S. persons for supply chain threats;
  - requiring testing to evaluate the trustworthiness of hardware and software components; and
  - requiring more rigor in the prevention and detection of counterfeits.

Key Theme 2: Program Protection Policies

- Program protection imposed by “top down” policy requires “bottom up” implementation in order for the intent of integrating trust to be realized.
  - through verifiable confidence in the integrity of the hardware, firmware, and software components
- Acquisition reality is that if a fool-proof trusted component was provided, it is unclear who would be required to use it.
  - and by what evidence could it be accepted if not documented by these policies and processes?
- Government program offices are making performance demands, security demands, and reliability demands that the industrial base is increasingly unable to guarantee.
- Problem is exacerbated by diminishing government support for expensive and unique test facilities and inconsistent requirements from the system designers.
- Industry is looking to the government for leadership and guidance and, in its absence, is having to make tough, sometimes non-optimum, choices.

Key Theme 3: Emerging Counterfeiting Capabilities

- Clones and mimics are more advanced types of counterfeit capability and an emerging concern as they are harder to detect.

- Current visual inspection and common testing methods will not reveal the lack of performance expected of the authentic component.

AFOSI notes the Air Force is the largest consumer of old and obsolete technologies

Upwards of 50 percent of Air Force sustainment parts originate in the grey market

Field Programmable gate Arrays (FPGA) are a particular concern

Key Theme 4: Acquisition System Implementation of DoDI 5200.44

- Current acquisition system status quo is lacking in implementation of DoDI 5200.44, which was to provide program protection for threats emanating from the supply chain and vulnerabilities in design.

- Training, guidance, and security evaluation criteria need to be included in solicitations with metrics. Enforcement is needed at the program level.

Supply Chain Risk Management Requirements (SCRM) must be made part of Requests for Proposal (RFP)

Key Theme 5: Physical Limits of Current Technology

- Current technology is at the end of an era as physical limits of microelectronics have been reached (i.e., traditional scaling based Moore's Law is coming to an end).

- Although this is a problem for current foundries, this may be an opportunity to prepare for the next era where trust is a requirement for next-generation components.

Key Theme 6: Trusted Foundry Model

- Trusted foundry model is a solution to a bygone era
- New approach to assure access to trusted microelectronics may be required.
- Solution is not a dedicated government-run foundry
  - DoD requires many different types of electronic parts and a single foundry cannot support all these different needs (as noted above).
- DARPA approach of figuring out how to build "trusted" integrated circuits in an untrusted supply chain
- Proposed DoD strategy of seeking to extend the existing contract with Global Foundries to buy time, while making investments in test, evaluation, and validation capabilities and in alternative approaches to the trusted foundry model (e.g., DARPA's approach)

Key Theme 7: New Fabrication Methods to Replace Trusted Foundry Model

- One common vision to secure trusted components is to develop fabrication methods that ensure the microelectronics can be protected from alteration, controlled, and verified.
- As evidenced by the presentations from DARPA, IARPA, and industry, multiple new architectures and technologies exist that may provide solutions.
- Split manufacturing is an alternative business model to the current approach by DoD.
- Split manufacturing involves doing the initial processing steps (front end of line, or FEOL) at one foundry and finishing the fabrication at another foundry (back end of line, or BEOL).
- A higher degree of security can be obtained by doing the split earlier in the process of manufacture.

Questions?

POC: Carter Ford (cford@nas.edu)