Team 1: Future Needs & System Impact of Microelectronics Technologies

February 2nd 2017

Team Members

	Name	Organization
1	Charles Adams (Team Leader)	Northrop Grumman
2	Scott Anderson	Lockheed Martin
3	Eric Dauler	MIT Lincoln Laboratory
4	Antonio de la Serna	DRAPER
5	Michael Fritze	Potomac Institute for Policy Studies
6	Jim Gobes	Intrinsix
7	Craig Herndon	NSWC Crane
8	Grant Meyer	SRI International
9	Jeremy Muldavin	DASD(SE) Microelectronics Assurance
10	Dan Radack	IDA
11	Kirk Reynolds	Rockwell Collins
12	Ray Shanahan	ODASD(SE) Anti-Tamper & Hardware Assurance
13	Major Manny Trejo	DoD
14	Dean Brenner	Honeywell
15	Kenneth H. Heffner	Honeywell

Team 1: Approach

What are the future microelectronics capabilities needed by defense contractors to maintain our technical advantage? Are there ways to quantify the value of hardware component performance in the context of systems? Are there new hardware paradigms on the horizon that could be disruptive?

We have used the following as guidance for our discussions

1. **System Needs and System Capabilities: What are the future requirements for DoD Systems?**
2. **What are the emerging technologies enabling these capabilities at the component level?**
3. **How do we close the gap and enable the system capabilities ?**
4. **What are the trust and security issues for emerging technologies ?**

Future Requirements Drivers for Microelectronics (not in priority order)

1. **Access to Future Low Cost Components (3-D Packaging enabled, etc)**
   - Mike Fritze
2. **Future Component Availability (assured / counterfeit / DMS)**
   - Craig Herndon
3. **Improved Performance (higher level of integration, Flexibility),**
   - Scott Anderson
4. **Low Power Operation(RF Efficiency, low power processing)**
   - Jeremy Muldavin
5. **Security (CPI, Trust(Integrity), Cyber)**
   - Manny Trejo

Future System Needs Must Address All of These Requirements

Challenges with Future Microelectronics Requirements

- ***Challenges to Maintain technology superiority in dynamic new technical world***
  - Compromise risks of emerging technology
  - Access risks of emerging technology
  - *COTS risks (Everyone in the world has access to the same State of the Art COTS (drones, etc))*
  - Gaps / Shortfalls in State of the Art and Available Technologies
  - Increasing Complexity of Commercially Available Capability

These are common for all of the future system needs

Challenges and Mitigations: Low Cost Components

NDIA

Challenges to Maintain technology superiority in dynamic new technical world

- Complex Global Semiconductor Market w/ little USG influence
  - Technology advancements driving specialized commercial solutions and markets
  - Industry outpacing government development cycles
  - Migration / consolidation of industry outside of US
  - Moderate DoD Production Volume (~1% of total global demand)
  - IP protection and Traceability of sourcing is difficult
  - Material supply (location driven)
- Adversaries have Increased sophistication and capability
  - State sponsored entities driving change in this environment.
  - Protection/acquisition of IP is a major concern
- Government needs for Performance and Assurance are leading Industry
  - Lack of customization – diminishes technical superiority
  - Vulnerabilities – How do we ensure all components are void of risk
  - No model of the risk (supply chain, vulnerabilities)
  - Increased likelihood of DMS issues due to compressed technology cycles
  - Reliability – designed and rated for commercial operation
  - Currently heavy reliance on COTS for many systems

Low Cost Components Access Mitigations (Current)

- Global Foundries CFIUS Agreement (sole source)
- DMEA Trusted Suppliers / DLA Trusted Distributor
- Acquisition process requirements (ie 5200.44)

- Use of formal (internal) standards for trust
- Buy pre-internet components (naturally cyber resilient)

- DARPA, IARPA ,etc developing technologies for trust / assurance

Low Cost Components Mitigations (Future)

- Multiple trusted SOTA suppliers
  - Expand current list; Add categories
- Public private partnerships with Industry
  - US Industry and Allies; Split-fab
- Acquisition Reform
  - Clear trust requirements through entire supply chain
  - "Tiers of Trust" structure, Export control reform
- Advanced packaging approaches (3D/2.5D)
  - New route for custom "SOC" capabilities (CHIPPs)
  - Trust via obfuscation (SPADE, TIC)
- Trust through technology
  - Taggants (SHIELD), Portability & vetted IP reuse (CRAFT)
  - "Trust by design" & obfuscation

Challenges and Mitigations: Component Availability

Challenges to Maintain technology superiority in dynamic new technical world

- Complex Global Semiconductor Market w/ little USG influence
  - Technology advancements driving specialized commercial solutions and markets
  - Industry outpacing government development cycles
  - Migration / consolidation of industry outside of US
  - Moderate DoD Production Volume (~1% of total global demand)
  - IP protection and Traceability of sourcing is difficult
  - Material supply (location driven)
- Adversaries have Increased sophistication and capability
  - State sponsored entities driving change in this environment.
  - Protection/acquisition of IP is a major concern
- Government needs for Performance and Assurance are leading Industry
  - Lack of customization – diminishes technical superiority
  - Vulnerabilities – How do we ensure all components are void of risk
  - No model of the risk (supply chain, vulnerabilities)
  - Increased likelihood of DMS issues due to compressed technology cycles
  - Reliability – designed and rated for commercial operation
  - Currently heavy reliance on COTS for many systems

Component Availability Mitigations (Current)

- USG Contract with GFUS
- USG Trusted Suppliers / DLA Trusted Distributor
- DMSMS approaches:
  - USG legacy support (DMEA)
- Lifetime buys (when possible)

Component Availability Mitigations (Future)

- Public-private partnerships for SOTA access
  - US Industry & Allies, Split-Fab, etc
- Multiple trusted suppliers for key parts
- Trust approaches for COTs parts
- Updated acquisition policy for trust
  - Entire supply chain
  - Tiered structure
- Trusted systems from untrusted components (R&D)
- Better transition of USG R&D to US Industry
  - "Centers of Excellence"
  - Consortia

Challenges and Mitigations: Improved Performance

NDIA

Challenges to Maintain technology superiority in dynamic new technical world

- Complex Global Semiconductor Market w/ little USG influence
  - Technology advancements driving specialized commercial solutions and markets
  - Industry outpacing government development cycles
  - Migration / consolidation of industry outside of US
  - Moderate DoD Production Volume (~1% of total global demand)
  - IP protection and Traceability of sourcing is difficult
  - Material supply (location driven)
- Adversaries have Increased sophistication and capability
  - State sponsored entities driving change in this environment.
  - Protection/acquisition of IP is a major concern
- Government needs for Performance and Assurance are leading Industry
  - Lack of customization – diminishes technical superiority
  - Vulnerabilities – How do we ensure all components are void of risk
  - No model of the risk (supply chain, vulnerabilities)
  - Increased likelihood of DMS issues due to compressed technology cycles
  - Reliability – designed and rated for commercial operation
  - Currently heavy reliance on COTS for many systems

Improved Performance: Mitigations (Current)

- Trusted Supplier Networks
  - Access to advanced nodes for Silicon CMOS
  - Access to state-of-the-art (SOA) RF integrated circuits and compound devices
- COTs suppliers where applicable—economy of scale for leading edge components
- Development of new customized architectures/components
- Technology Investments:
  - NNMIs (Power America, AIM Photonics, Flex Hybrid), Title 3, ManTech, Service type investments, SRC—JUMP program
- Novel packaging and integration techniques
- DoD investments in assurance techniques for components and systems

Improved Performance: Opportunity (Future)

- Promote public private partnerships that support the gaps between commercial and USG in leading edge technologies
- DARPA/IARPA technology development approaches
- US leadership in design and trusted access to IP
- Continued USG investment in DoD technology performance needs that are not aligned with commercial market
- Additional focus on systems on integrated microelectronics—more than just the semiconductors
- Advances in PICs and heterogeneous packaging
- Investments for DoD applications in quantum, biological, AI, neuromorphic and other beyond CMOS technologies.

Challenges and Mitigations: Low Power Operation

NDIA

Challenges to Maintain technology superiority in dynamic new technical world

- Complex Global Semiconductor Market w/ little USG influence
  - Technology advancements driving specialized commercial solutions and markets
  - Industry outpacing government development cycles
  - Migration / consolidation of industry outside of US
  - Moderate DoD Production Volume (~1% of total global demand)
  - IP protection and Traceability of sourcing is difficult
  - Material supply (location driven)
- Adversaries have Increased sophistication and capability
  - State sponsored entities driving change in this environment.
  - Protection/acquisition of IP is a major concern
- Government needs for Performance and Assurance are leading Industry
  - Lack of customization – diminishes technical superiority
  - Vulnerabilities – How do we ensure all components are void of risk
  - No model of the risk (supply chain, vulnerabilities)
  - Increased likelihood of DMS issues due to compressed technology cycles
  - Reliability – designed and rated for commercial operation
  - Currently heavy reliance on COTS for many systems

Low Power Operation: Mitigations (Current)

- Commercial Efforts:
  - Lower-power digital processing available through custom software/firmware on existing GPUs, FPGAs and ASICs (trust is a risk for many parts)
  - Incorporation of non-volatile memories into systems
  - On-chip integration (SoC); existing hybrid/2.5D/3D packaging
  - Clock / power gating and dynamic voltage scaling available on some COTS parts & ASICs
- Government Efforts
  - GFUS advanced CMOS processes for trusted ASICs (lower-power digital and lower-power analog/digital co-designs)
  - Research into custom processes for low-power subthreshold CMOS

Low Power Operation: Opportunity (Future)

- Leverage Commercial Efforts:
  - Compiler-stage energy optimization (trust and availability of design tools + design IP should be protected)
  - Lower-power peripherals, interconnects and comm. (coordinate trusted suppliers / packaging / foundry access)
  - Technology platforms and design techniques for lower-power integration of analog components / design approaches
- Government Efforts:
  - Advanced packaging: heterogeneous integration, power sources for microsystems (need U.S. sources for low-volume)
  - U.S. leadership in flex technologies & beyond-CMOS technologies (develop with trust/assurance as a driver)

Challenges and Mitigations: Security

NDIA

Challenges to Maintain technology superiority in dynamic new technical world

- Complex Global Semiconductor Market w/ little USG influence
  - Technology advancements driving specialized commercial solutions and markets
  - Industry outpacing government development cycles
  - Migration / consolidation of industry outside of US
  - Moderate DoD Production Volume (~1% of total global demand)
  - IP protection and Traceability of sourcing is difficult
  - Material supply (location driven)
- Adversaries have Increased sophistication and capability
  - State sponsored entities driving change in this environment.
  - Protection/acquisition of IP is a major concern
- Government needs for Performance and Assurance are leading Industry
  - Lack of customization – diminishes technical superiority
  - Vulnerabilities – How do we ensure all components are void of risk
  - No model of the risk (supply chain, vulnerabilities)
  - Increased likelihood of DMS issues due to compressed technology cycles
  - Reliability – designed and rated for commercial operation
  - Currently heavy reliance on COTS for many systems

Security: Mitigations (Current)

- Planning/Integrating strategy into initial requirements phase as directed by DoDI 5200.44 & 4140.67
- Trusted Foundry & Trusted Suppliers
- Implementation of HW/security & trust initiatives (JFAC)
- Anonymous buys/Non-attributable 3rd party acquisitions
- Specialized qualification/counterfeit detection in supply chain
- Sensitive and disparate mitigation strategies beyond policy and regulations

Security: Opportunity (Future)

- Update acquisition strategy to consider impact on full lifecycle
- Promote trusted and trustable semiconductor capabilities for DHS critical infrastructure sectors – whole of government
- Enforce/expand Legislation to protect national interests
- Designate semiconductor capabilities as critical infrastructure
- Increase information sharing between government and industry
- Proactively broaden & better utilize Trusted Supplier Base
- Assess level of risk for major DoD subsystem components and determine specific level of trust required

Initial Collective Recommendations

- **Adapt Acquisition Policies**
  - Trust requirements/policies for whole of supply chain (not just fabrication)
    - Sustainment Awareness
  - Develop spectrum or “tiers” of trust levels/categories
    - Programs can choose what levels they need and can afford
- **Whole of USG approach**
  - Align major USG equities in secure Microelectronics (DoD, DOE, IC)
  - Demand aggregation & critical mass resources (funding)
- **Key areas for future trust capabilities**
  - Secure 3D/2.5D integration facilities
  - Access to SOTA US Industries
    - Public-Private partnerships, Split-fab
  - Trust R&D
    - Design for trust, verification/forensics, obfuscation, metrics, reconfigurability, etc
  - Robust/attractive environment for transitioning R&D results into US production
    - “Centers of Excellence”, NNMI centers, Consortia, etc

- **What are the other thoughts from the community?**