The Quest for Secure and Reliable Electronic Components

Collaboration on Quality in the Space and Defense Industry (CQSDI)
Cape Canaveral, FL
March 2017.

Robert H. Latiff, Ph.D.
Maj Gen, USAF (Ret)
What, Me Worry?

MAD
What’s The Issue?

• Electronics are everywhere, they’re unbelievably complex, and getting more so
• We’re not entirely certain we can trust them
The Situation

• They’re Ubiquitous
  – Consumer electronics
  – Internet of Things, 5G
  – Autonomous Systems
    • Commercial- automotive
    • Defense
  – Artificial Intelligence
  – Our bodies: Cyber-physical devices
  – And of course, space systems
Implantable and Wearable Medical Devices

- **Bio-Medical**
  - EEG Electroencephalography
  - ECG Electrocardiogram
  - EMG Electromyography (muscular)
  - Blood pressure
  - Blood SpO2
  - Blood pH
  - Glucose sensor
  - Respiration
  - Temperature
  - Fall detection
  - Ocular/cochlear prosthesis
  - Digestive tract tracking
  - Digestive tract imaging

- **Sports performance**
  - Distance
  - Speed
  - Posture (Body Position)
  - Sports training aid

- **Cyber-human interfaces**

Images courtesy CSEM, Switzerland
The Electronics Landscape

• Continued and accelerating globalization of microelectronics industry challenges national security program designers
  – How to ensure components operate as designed – and no more

• 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
Pressures

• National security electronics industrial base is under pressure
  – Increasingly unable to meet program office performance, security, and reliability demands
  – At the mercy of the electronics manufacturers and suppliers
    • Diminished ability to supply the kind of high-quality, high-reliability systems needed
    • Significant resources are expended in quality assurance, as most suppliers are now off-shore.

• Diminishing government support for expensive and unique test facilities
  – Contractors concerned about the ability to adequately test parts for reliability over long lifetimes, and for radiation tolerance
  – Understanding of the failure mechanisms in accelerated life testing is lacking
  – Poor understanding of the implications of failure mechanisms at the chip level.

• Contractors concerned over inconsistency in the reliability evaluation criteria they receive from differing segments of the government.
  – Leads to greater expense and a need to either repeat work or do unnecessary testing

• Industry looks to the government for leadership and guidance and, in its absence, makes tough, sometimes non-optimum, choices
They’re More Complex

Early Production Logic/Foundry Roadmap beyond 2016

<table>
<thead>
<tr>
<th>Year</th>
<th>2012</th>
<th>2014</th>
<th>2016</th>
<th>2018</th>
<th>2020</th>
<th>2022</th>
<th>2024</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node (nm)</td>
<td>22</td>
<td>14</td>
<td>10</td>
<td>7</td>
<td>5</td>
<td>3.5</td>
<td>2.5</td>
</tr>
<tr>
<td>Interconnect CD (nm)</td>
<td>40</td>
<td>30</td>
<td>20</td>
<td>15</td>
<td>10</td>
<td>7.5</td>
<td>5</td>
</tr>
</tbody>
</table>

- **Wafer Scaling**: 300mm → 450mm
- **Transistor**: FinFET → SiGe → Nanowire → III-V or III-V Tunnel FET
- **Interconnect**: Dual Damascene → Single Damascene → Subtractive Copper/Alternatives
- **Embedded Memory**: SRAM/eDRAM → MRAM
- **Patterning**: Immersion Multi Patterning → Multi-Patterning → Self-Assembly → EUV
Technical Understanding Critical for Both

Detailed knowledge of chemistry and physics of operation and failure
One of the goals of the National High Reliability Electronics Virtual Center (HiREV)
The Situation

• They’re Ubiquitous
  – Consumer electronics
  – Internet of Things, 5G
  – Autonomous Systems
    • Commercial-automotive
    • Defense
  – Artificial Intelligence
  – Our bodies: Cyber-physical devices

• We can’t totally trust them
  – Off-shore manufacture
  – Counterfeit
## 2014F Top 20 Semiconductor Sales Leaders ($M)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>Intel</td>
<td>U.S.</td>
<td>48,321</td>
<td>51,368</td>
<td>6%</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>Samsung</td>
<td>South Korea</td>
<td>34,378</td>
<td>37,259</td>
<td>8%</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>TSMC*</td>
<td>Taiwan</td>
<td>19,935</td>
<td>25,088</td>
<td>26%</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>Qualcomm**</td>
<td>U.S.</td>
<td>17,211</td>
<td>19,100</td>
<td>11%</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>Micron + Elpida</td>
<td>U.S.</td>
<td>14,294</td>
<td>16,614</td>
<td>16%</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>SK Hynix</td>
<td>South Korea</td>
<td>12,970</td>
<td>15,838</td>
<td>22%</td>
</tr>
<tr>
<td>7</td>
<td>8</td>
<td>TI</td>
<td>U.S.</td>
<td>11,474</td>
<td>12,179</td>
<td>6%</td>
</tr>
<tr>
<td>8</td>
<td>7</td>
<td>Toshiba</td>
<td>Japan</td>
<td>11,958</td>
<td>11,216</td>
<td>-6%</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>Broadcom**</td>
<td>U.S.</td>
<td>8,219</td>
<td>8,360</td>
<td>2%</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>ST</td>
<td>Europe</td>
<td>8,014</td>
<td>7,374</td>
<td>-8%</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>Renesas</td>
<td>Japan</td>
<td>7,975</td>
<td>7,372</td>
<td>-8%</td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td>MediaTek + MStar**</td>
<td>Taiwan</td>
<td>5,723</td>
<td>7,142</td>
<td>25%</td>
</tr>
<tr>
<td>13</td>
<td>14</td>
<td>Infineon</td>
<td>Europe</td>
<td>5,260</td>
<td>6,151</td>
<td>17%</td>
</tr>
<tr>
<td>14</td>
<td>16</td>
<td>NXP</td>
<td>Europe</td>
<td>4,815</td>
<td>5,625</td>
<td>17%</td>
</tr>
<tr>
<td>15</td>
<td>13</td>
<td>AMD**</td>
<td>U.S.</td>
<td>5,299</td>
<td>5,512</td>
<td>4%</td>
</tr>
<tr>
<td>16</td>
<td>17</td>
<td>Sony</td>
<td>Japan</td>
<td>4,739</td>
<td>5,192</td>
<td>10%</td>
</tr>
<tr>
<td>17</td>
<td>15</td>
<td>Avago + LSI**</td>
<td>Singapore</td>
<td>4,979</td>
<td>5,087</td>
<td>2%</td>
</tr>
<tr>
<td>18</td>
<td>19</td>
<td>Freescale</td>
<td>U.S.</td>
<td>3,977</td>
<td>4,548</td>
<td>14%</td>
</tr>
<tr>
<td>19</td>
<td>20</td>
<td>UMC*</td>
<td>Taiwan</td>
<td>3,940</td>
<td>4,300</td>
<td>9%</td>
</tr>
<tr>
<td>20</td>
<td>21</td>
<td>Nvidia**</td>
<td>U.S.</td>
<td>3,898</td>
<td>4,237</td>
<td>9%</td>
</tr>
</tbody>
</table>

**Top 20 Suppliers:** 237,379 $M in 2013, 259,562 $M in 2014, 9% change

**Top 20 Suppliers Excluding Foundries:** 213,504 $M in 2013, 230,174 $M in 2014, 8% change

*Foundry, **Fabless

Source: IC Insights' Strategic Reviews Database
Counterfeits Increasingly Sophisticated

Notice difference in font, character spacing, and laser thickness/texture. The one on the left (legitimate) also has a small sticker on the right side. The syntax of line 3 is different. You can’t see very well in this picture, but the pin one indicator has radiused edges (smooth) and the counterfeit one does not, and the surface texture is different.

Overall, however, the counterfeit part is very convincing. Firmware tests confirm that it is, in fact, a much older version of indicated part, which had a different part number (13, not the indicated 13A). It also draws much more current (more than x2) indicating it is the older model.
Air Force Sponsored National Academies Workshop
16-18 March 2016
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, Program Officer
- Marguerite E. Schneider, Administrative Coordinator
- Dionna C. Ali, Research Assistant
Workshop Presentations

• SAF/AQR
• ASD/SE
• DARPA
• DMEA
• NSWC
• NIST
• AFSPC/SMC
• DOE/NCS

• IARPA
• AFOSI
• IDA
• NDIA
• AEROSPACE
• MITRE
• IBM
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
DOD: A Bit Player in a $300B Industry

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%)


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)
• **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 for the intent of integrating trust to be realize
    
    • through verifiable confidence in the integrity of the hardware, firmware, and software components
Quality Escape: Product defect/ inadequacy introduced either through mistake or negligence during design, production, and post-production handling resulting in the introduction of deficiencies, vulnerabilities, and degraded life-cycle performance.

Reliability Failure: Mission failure in the field due to environmental factors unique to military and aerospace environments such as particle strikes, device aging, hot-spots, electro-magnetic pulse, etc.

Fraudulent Product: Counterfeit and other than genuine and new devices from the legally authorized source including relabeled, recycled, cloned, defective, out-of-spec, etc.

Malicious Insertion: The intentional insertion of malicious hardware or software, or defect to enable physical attacks or cause mission failure; includes logical bombs, Trojan ‘kill switches’ and backdoors for unauthorized control and access to logic and data.

Reverse Engineering: Unauthorized extraction of sensitive intellectual property using reverse engineering, side channel scanning, runtime security analysis, embedded system security weakness, etc.

Information Losses: Stolen data provides potential adversaries extraordinary insight into US defense and industrial capabilities and allows them to save time and expense in developing similar capabilities.

DoD Program Protection focuses on risks posed by malicious actors.

FIGURE 1-2 Spectrum of supply chain risks. SOURCE: Kristen Baldwin, Acting Deputy Assistant Secretary of Defense for Systems Engineering and Principal Deputy Assistant Secretary of Defense for Systems Engineering, presentation to the workshop on March 16, 2016. Distribution Statement A – Approved for public release by DOPSR; SR#15S-1541 applies. Distribution is unlimited.
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.
FIGURE 2-2 Technological capabilities and approaches to detecting counterfeits. SOURCE: Brett Hamilton, Chief Engineer Trusted Microelectronics, JFAC Hardware Assurance Lead, Global Deterrence and Defense Department/Flight Systems Division, Naval Surface Warfare Center, presentation to the workshop on March 16, 2016.
Key Theme 4: Acquisition System Implementation of DoDI 5200.44

- Current acquisition system status quo is lacking in implementation of DoDI 5200.44

- 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
Observations

• Increasingly, FPGAs and GPUs as accelerative elements within systems, rather than replacement of long lead time and design intensive ASICs.

• Intel acquired Altera, a leading FPGA manufacturer, and is implementing monolithic chips containing close-coupled CPUs and FPGAs having shared memory.

• Systems on a chip with a dual functionality make possible real-time monitoring and validation of critical FPGA functions by an independently programmed yet close-coupled CPU.

• Functionally and architecturally diverse single chips may be far more robust in terms of security of function than can be achieved with a simple software-or hardware-based defense.

• Active real-time system assurance must also be explored as first or second lines of defense again malicious functionality implemented in a critical system during its manufacture
  – whether by direct monitoring
  – or via behavioral monitoring by a cognitive system exploring departures from a norm

Myerson, IBM
Key Theme 6: Trusted Foundry Model

- Trusted foundry model is a solution to a bygone era
  - Trusted Foundry Program helps to ensure that ASIC design and fabrication is performed by secure, domestic sources,
    - BUT, it is used for only about 2% of the 1.9B integrated circuits in defense systems
  - The trust program does little to address the supply chain risk management aspects of Field Programmable Gate Arrays (FPGA)
    - DOD is still reliant on the commercial supply chain.
  - New approach to assure access to trusted microelectronics may be required.
Key Theme 7: New Fabrication Methods to Replace Trusted Foundry Model

• Common vision to secure trusted components
  – Develop fabrication methods that ensure the microelectronics can be protected from alteration, controlled, and verified.

• Split Manufacturing is one option
  – An alternative business model to the current approach by DoD
  – Involves doing the initial processing steps (front end of line) at one foundry and finishing the fabrication at another foundry (back end of line).
  – A higher degree of security can be obtained by doing the split earlier in the process of manufacture
Discussion

• We may be chasing too much performance
• 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
• Must learn how to build “trusted” integrated circuits in an untrusted supply chain
• Good DoD strategy
  – seeking to buy time with the Global Foundries extension
  – while making investments in test, evaluation, and validation capabilities
  – and alternative approaches to the trusted foundry model
• Multiple new architectures and technologies exist that may provide solutions
What Now?

• The workshop only scratched the surface of the issues
  – identified areas needing more study
• Potential for AF Sponsored, Classified Consensus Study, with Recommendations
• DOD, IC, and DOE interest
Possible Study Tasks

– Identify Air Force requirements for secure and reliable microelectronic components and rank their criticality.

– Identify the current and forecasted threats to the supply chain.

– Provide scenarios concerning consequences and impact of compromised electronic components.

– Identify acceptable levels of trust required for Air Force capabilities requiring secure and reliable microelectronic components.

– Describe current Air Force acquisition policies and requirements for secure and reliable microelectronic components.

– Compare approaches used by other Services, intelligence community, and industry and address possible risk mitigation strategies.

– Highlight the technical and organizational challenges in prescribing either hardware, software or hybrid approach.