Open Forum

Trusted Integrated Circuit Strategy

Sydney Pope

***Abstract*—Microcircuits and related electronic devices are increasingly dominated by global commercial interests, making issues of trust (intellectual property theft and anti-tampering), product reliability, and assured sources of supply increasingly difficult to manage. The purpose of this paper is to present possible strategies to help address both defense and aerospace risks in this area.**

***Index Terms*—Anti-tampering, counterfeit, diminishing manufacturing, integrated circuit (IC), microcircuit, microelectronic, parts obsolescence, product assurance, semiconductor, trusted foundry.**

I. Introduction

THE product development strategies and supply-chain management practices of today do not adequately prevent electronic device tampering, counterfeiting, and reverse engineering. They do not assure that components, which are heavily dependant upon commercially derived technologies and designs, will conform to the performance demands inherent in aerospace and defense environments. Neither do they depend on them being maintainable throughout their service-life.

II. Globalization of Microcircuit Industry

Over the past 20 years, tremendous leaps forward have occurred in the globalization of economy. This has been brought about by rapid improvements in communications and information technology. Major advancements in electronics, especially microelectronics have provided the means by which developing nations can become members of the industrialized community.

The estimated effects of these economic factors can be seen in Fig. 1. The Semiconductor Industry Association estimates the total global sales for semiconductor devices in 2004 to be $214B and $227.5B for 2005 with a projection of close to $300B in 2009. In the recent past, the Asia/Pacific region has enjoyed a proportionally much larger share of this sales growth as well as manufacturing while the U.S. share remained flat and is projected to stay that way for the near future. The vast majority of semiconductor sales are for products such as personal computers and cell phones with markets for these consumer goods no longer restricted to just Japan, North America, and Western Europe.

A review of the Department of Defense (DoD) annual budget indicates that the U.S. military portion of microcircuits sales is approximately 1% of the world market and less than 9% of the U.S. market ($3.6B out of $40.7B).

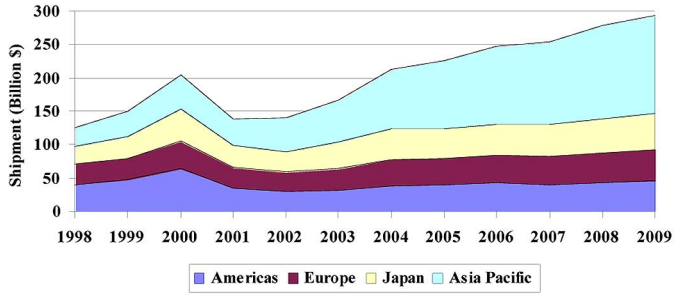

Fig. 1. Changes in the distribution of global semiconductor sale (data from Semiconductor Industry Association).

In the early days of the semiconductor industry, the military market was a large fraction of overall sales and helped to drive technology. Developments in leading edge technology are now driven by large commercial markets, no longer by the military/aerospace market. "While the military provided the original test bed for many computers and microelectronics, defense needs are not the driver for the newest technologies in these fields in most cases" [1].

With the growth of consumer markets, the DoD's ability to control and influence the electronics sector has diminished. The General Accounting Office's September 2006 Report on Offshoring of U.S. Semiconductor and Software Industries noted that the military held a key role in the initial development of the microelectronics industry. However, research and development expenditures (and influence) from the commercial sector over the past decade have grown significantly beyond federal expenditures [2].

Just as the electronics industry precipitated the rise of a global economy and the growth of global industry and consumerism, so have these market forces aided the expansion and migration of the industry away from industrialized nations like the United States and Japan. As shown in Percentages of World's Semiconductor Foundries, during the 1980s and 1990s, these two nations had the majority of microelectronic foundries. Today, they have less than 20% each of the world's microelectronic manufacturing facilities, while emerging industrialized nations in the Asian and Pacific Regions possess 45% of the world's foundries.

While markets, manufacturing costs, and industrial policies have affected the global semiconductor industry, the need for "trust" in these components is complicating matters for defense systems. An effective strategy for trusted integrated circuits (ICs) must comprehend the types and sources of components, as well as their deployment and lifecycle (see Fig. 2).

III. Trust and Counterfeiting

In his October 10, 2003, memorandum, then Deputy Secretary of Defense Paul Wolfowitz called for the development of a Defense Trusted Integrated Circuit Strategy (DTICS). He acknowledged the force multiplying advantage that leading edge electronic technology provides. He also recognized that potential adversaries could tamper with the microelectronic devices used in defense and aerospace systems in ways that are undetectable and steal intellectual property from designs and thereby defeat key defense systems. The strategy should therefore provide for safeguarding the most critical ICs used in sensitive weapons,

Manuscript received February 1, 2008. This work was recommended for publication by Associate Editor M. G. Pecht upon evaluation of the reviewers comments.

The author is with the Office of the Deputy Under Secretary of Defense for Industrial Policy, Department of Defense, Washington, DC 20301 USA.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCAPT.2008.918319

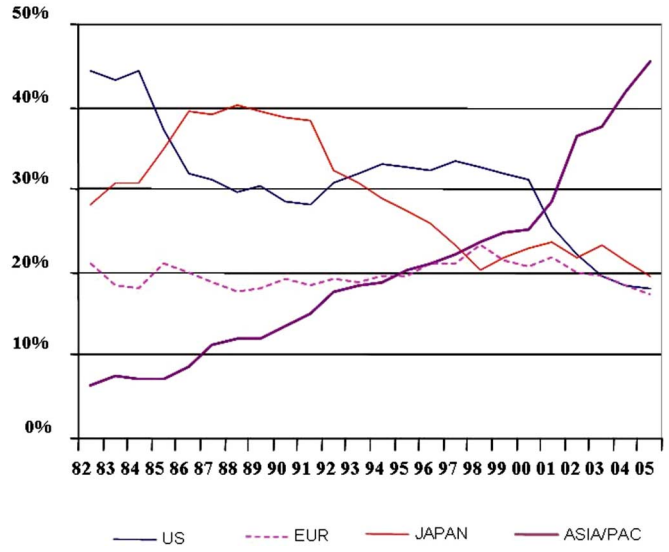

Fig. 2. Percentages of world's semiconductor foundries (data from Semiconductor Industry Association).

intelligence, and communication systems. In order to preserve unrestricted access to this technology, it should stimulate and support vigorous open markets and innovation.

Subsequently, a Defense Science Board (DSB) study entitled "High Performance Microchip Supply" was initiated. The resulting report, released in February 2005 recommended strategy to sustain a strong competitive microelectronics industrial base to address the risk of tampering. It recommended the development of a trusted environment for acquiring microelectronic devices, especially those used in classified applications.

A particular and immediate concern for the DSB was the establishment of a trusted environment for producing low volumes of application specific integrated circuits (ASICs). This environment is currently being provided under the Trusted Foundry Program. The DSB also recognized that commercial off-the-shelf (COTS) components used in sensitive military applications could also be compromised. The study noted that "Neither extensive electrical testing nor reverse engineering is capable of reliably detecting compromised electronic components" [3]. However, a combination of electrical testing and reverse engineering techniques could be developed to detect COTS semiconductors, such as field programmable gate arrays (FPGAs) that have been compromised [4]. Of course neither testing nor reverse engineering can identify whether intellectual property has been compromised.

Counterfeiting of electronic parts is a growing concern. "A counterfeit electronic component is one where material, performance, or characteristics are knowingly misrepresented by the vendor, supplier, distributor, or manufacturer" [5]. The objective of tampering is to engage in espionage or sabotage; whereas the motivation for counterfeiting is economic. The effect of either is the same; intentionally compromised devices may be impossible to detect and can jeopardize both mission and life. This is why both counterfeiting and trust are cited in the Trusted Foundry Program budget justification.

The most effective approach for avoiding counterfeit electronic components is to purchase product directly from the original component manufacturer, or from a distributor, reseller, or aftermarket supplier who is franchised or authorized by the original manufacturer. A substantial number of products required to produce and support defense electronics, however, are no longer available from the original component manufacturer or through its franchised or authorized suppliers. Independent distributors are often used to fill this gap. While various mitigation methods can reduce the risk of receiving counterfeit parts from independent distributors, there is no fail safe method. A suite of inspections and tests are necessary to detect counterfeits and eliminate infant mortality defects, and to establish high level of confidence in field performance and reliability. Acquisition traceability mechanisms and product assurance controls for product acquire from Independent Distributors must improve. Electronic part manufacturers need to be made partners in these efforts and efforts coordinated with government efforts [6]. The possibilities of building supply chain trust through the use of covert tagging techniques should also be investigated for critical items [7].

IV. Diminishing Manufacturing Sources

In August 2004, the Acting Undersecretary of Defense for Acquisition, Technology, and Logistics (USD AT&L), Michael Wynne, directed a parallel effort to DTICS called "Microelectronics Strategic Management." Its purpose was to define DoD microcircuit requirements (short and long term) and develop a technology roadmap to address Diminishing Manufacturing Sources and Material Shortages (DMSMS). DoD program manager guidance on DMSMS best practices is found in DoD SD-22 [15].

Defense and aerospace communities need to improve the way they track and manage DMSMS and electronic device obsolescence issues. An example of information sharing is the Government-Industry Data Exchange Program (GIDEP) Discontinued Parts Listing. This program has had limited success as it depends on voluntary submission of information. Greater use of it has been widely advocated.

A more disciplined approach for managing DMSMS issues under consideration by DoD is the collection, consolidation and tracking of indentured bills of material (BOM) information. A centralized and shared BOM database could help preserve military readiness by identifying preferred parts and communicating DMSMS issues across programs and throughout the supply chain. A decentralized approach advocated by industry is for DoD to rely more on them for performance based logistics support. They would retain configuration and maintenance responsibility of fielded systems and make maintenance and modification cost-trade decisions. There are benefits with both approaches and possibly a combination of the two may provide an optimal solution.

V. Product Quality and Reliability

Both the DoD and the aerospace industry are concerned about the diverging gap between our high reliability performance requirements and the high-volume, relatively short life-cycle needs of the private consumer electronics market. This is resulting in product assurance concerns that are becoming more difficult to address as microelectronic devices become more powerful, but less capable of accommodating extreme environmental and high reliability demands.

The defense and aerospace sector's ability to influence the microelectronics industry has diminished with the growth of other markets. Today, these two sectors comprise less than 2% of the world demand for microelectronic devices. "The aerospace industry depends on electronic components, but can no longer count on sources of stable designs that are specified for our specific applications. We must learn how to use components produced for other industries that are quite unlike ours" [8].

As microcircuit size decreases, greater attention is needed to control production processes. There is increased risk of gate leakage or electromigration (a form of short-circuiting), especially if there are inconsistencies in substrate material. Smaller feature sizes enable greater circuit density and more rapid switching speeds, but faster operation also generates increased amounts of heat. Excess heat will degrade life-cycle

performance if not controlled. Even though the semiconductor industry applies tools and methods to assure product quality and reliability for the consumer and industrial markets, this level of product assurance is insufficient for most if not all defense and aerospace applications.

Devices used in defense and aerospace applications are subject to environmental effects not commonly found in the consumer market such as the need for long term storage periods, and environmental factors such as shock, vibration, Initial Nuclear Radiation (INR), Electromagnetic Environmental Effects (E3) and wide temperature range. Atmospheric radiation effects are also a concern to the aerospace industry. Aircraft and especially spacecraft are vulnerable to cosmic ray and solar particle radiation total dose and single event upsets with future electronic systems being more vulnerable due their higher sensitivity [9].

VI. Trust Strategy Concept

DoD policy is that trust is a minimum requirement for defense systems [10]. DoD defines trust as 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, i.e., microelectronics. Furthermore, DoD defines trusted sources as those that:

1) provide an assured "chain of custody" for both classified and unclassified ICs;
2) ensure that there will not be any reasonable threats related to disruption in supply;
3) prevent intentional or unintentional modification or tampering of the ICs;
4) protect the ICs from unauthorized attempts at reverse engineering, exposure of functionality or evaluation of their possible vulnerability.

The DoD is in the process of developing a trusted ICs strategy and policy that is comprehensive, viable, cost-effective, realistic, and in the long term that ensures the supply of trusted ICs for defense applications. A comprehensive trust policy must include multilayered defense-in-depth as a practical strategy, involving people, technology, and operations. Anonymity in COTS ICs procurement is one of the defensive elements [11]. Other key defensive elements include:

- trusted suppliers;
- trusted products;
- design information hiding;
- anti-tamper technology;
- failure detection and forensics;
- damage mitigation;
- approved quality;
- chip signature authentication.

The DoD has established mission assurance and confidentiality designations as a way of measuring system level trust requirements for acquisition [12], [13]. For custom designed devices that need the highest level of trust, such as those used for secure communication, the Trusted Foundry Program is available to provide access to the needed manufacturing capabilities. Microcircuits can be designed, manufactured, and distributed in a trusted environment [14].

Under the Trusted Foundry Program, ASIC and military unique microcircuits are designed, manufactured, tested, packaged and handled in a strictly controlled environment like that used for classified programs. This level of control incurs additional cost and may not be appropriate to microcircuits that do not require the highest levels of trust. For many microcircuits used in defense and aerospace applications, a different approach for achieving lower levels of trust is being developed.

The vast majority of trust issues associated with microcircuits in general can be mitigated by protecting the anonymity of application. Contractors do not usually tell component manufactures and distributors where their products will end up being used except maybe when a supply problem occurs and after a system has been made and delivered. This is too late to do anything about obsolescence or diminishing sources. Addressing trust via anonymity of application increases the difficulty in managing obsolescence.

DoD Major Defense Acquisition Program plans should be vetted as part of the normal Defense Acquisition Board approval process. Standard government contract provisions would be applied to suppliers of systems, components, and devices to adopt acquisition practices that acquire products in a commingled manner that maximize market leverage and promote anonymity

This approach could also include a combination of acquisition practices that will promote trust in FPGAs. This technology can be very flexible in application and represents a majority of the COTS ICs used today. COTS FPGAs fabricated offshore could contain hidden features, which could be exploited, including malicious reprogramming during software download. It would be cost prohibitive to monitor and manage offshore semiconductor wafer fabrication. However, post production trust verification methods underdevelopment may provide a means for assuring trust for the next generation of critical systems. Trusted FPGAs and other commercially derived devices could be cost-effectively implemented through a combination of reverse engineering, development of invasive and noninvasive testing techniques, and development of anti-tamper packaging.[1]

VII. DMSMS Policy Concept

Trust through anonymity acquisition practices work against efforts to qualify components for aerospace and defense applications, promote DMSMS issues, and can limit opportunities to share BOM information. Anonymity is useful for hiding defense application of the ICs from the market, particularly when COTS products are used. A possible solution to this is to use trusted third parties to retain anonymity, while at the same time monitoring and addressing issues of obsolescence. For instance, third parties could use GIDEP as an alert service for communicating when components are about to become unavailable, which would also facilitate lifetime buyouts.

Suppliers of high priority systems, components, and devices should adopt and tailor commercially available standards for addressing DMSMS issues and assure process and product conformance. The government should encourage the cost-effective use of electronic component specifications and commercially available standards such as ANSI/GEIA EIA-STD-4899-A [16] and GEIA 0002-1 [17].

A shared goal of both industry and government should be the standardization of microelectronic products into interchangeable or substitutable families of devices to facilitate adaptation technology refresh in legacy systems when obsolescence becomes an issue. This would increase industry purchasing power and permit better management of product obsolescence and diminishing sources. Executive agents could be established through private distributors who will work in partnership with the aerospace industry and defense intelligence communities. They would provide a conduit for performing random independent qualification testing to validate product conformance and counter counterfeiting and intentional tampering by adversaries.

When a device used in a legacy system is no longer available and component refresh is not practical, reverse engineering may be the best and possibly only option. The availability of intellectual property can greatly simplify the reengineering process. Although it can prove costly, advancements in reverse engineering technology provide way to

[1]Proposals have been submitted by industry to DARPA to develop techniques for addressing the chip development process to ensure trust in COTS FPGAs for government product applications.

remanufacture obsolete devices even when intellectual property is not available.

VIII. Product Assurance Policy Concept

Government, system integration contractors, and original equipment manufactures would benefit from common language and methods for defining performance and reliability requirements, prioritizing criticality of end use, and assuring device conformity. Product verification criteria should be communicated through program acquisition strategy, systems engineering, and test and evaluation master planning documents, and electronic component management plans. System integration contractors, device manufacturers, and distributors should agree upon common test criteria for assuring devices operate within established performance criteria.

A way to establish and improve testing regimes would be to provide for critical techniques of recognized product trust and assurance verification. A business case could be developed that establishes executive agents responsible for maintaining access to trusted suppliers and supplies of standard commercial aerospace and defense microelectronic devices and other electronic devices at risk, such as power regulators and circuit cards.

Combining to the maximum extent practicable the standardization of common commercial aerospace and defense performance requirements can mutually enhance both anonymity and product assurance and the establishment of industry-recognized qualification testing regimes. Industry associations and the standardization community are in the best position to lead this effort, but the DoD must also participate and advocate as needed. An objective would be to leverage technologies that permit greater flexibility in their application, such as FPGA in order to minimize the number of unique or custom designs required by the aerospace and defense communities.

IX. Path Forward

The defense and aerospace community must be able to trust their electronic systems and assure their availability. For major system development programs and for any mission and flight safety critical microcircuits, ASIC or unique microcircuit devices should be identified and controls put in place to ensure that trust and counterfeiting risks are addressed. Where anti-tapering is of paramount concern, such as to protect classified or sensitive communications, customers may incur additional expense for imposing controls beyond industry practice. However, to the maximum extent practicable, standards mutually agreed upon by both government and industry should be developed that address trust for most mission critical defense, space, and flight safety applications.

Commercially developed and adopted systems employing COTS electronic components may be perfectly suitable for less critical applications such as ground support equipment, trainers and simulators, and automated information systems. Establishment of industry trust standards will help to ensure the appropriate use of commercially available devices, such as FPGAs as a cost-effective alternative to ASICs or other unique devices. Regardless of the device used for critical mission and flight safety applications, assured sources of supply and product assurance requirements should be verified according to both the customer's imposed special requirements and industry accepted practice.

Obsolescence and reliability issues resulting from advancements in microcircuit technology can be best mitigated through employment of systems engineering techniques to address potential risks up front. The defense and aerospace community should fully adopt evolutionary acquisition and spiral development strategies by upfront planning and funding for technology refresh and insertion of new technology in legacy and production programs.

The Office of the Deputy Undersecretary of Defense for Industrial Policy [ODUSD (IP)] is working with other elements of DoD to implement the strategy presented in this paper. Defense and aerospace acquisition practices should mutually support an approach that encompasses the emerging trends in both the commercial industry and the requirements of future defense and aerospace programs. ODUSD (IP) believes that GEIA, AIA and other industry association committees and forums provide the best environment to accomplish this.[2]

References

[1] *"Linkages: Manufacturing Trends in Electronic Interconnection Technology,"* Nat. Res. Council, 2005, pp. 31–34.

[2] U.S. Government Accountability Office, "Offshoring: U.S. Semiconductor and Software Industries Increasingly Produce in China and India," GAO-06–423, Sep. 2006, pp. 40–41.

[3] Department of Defense, "High Performance Microchip Supply," Defense Science Board Task Force Rep., Feb. 2005, pp. 4–26 [Online]. Available: http://www.acq.osd.mil/dsb/reports/2005–02–HPMS_Report_Final.pdf

[4] *Trust for Integrated Circuits*, DARPA BAA 06–40, Aug. 2006.

[5] M. Pecht and S. Tiku, "Bogus: Electronic manufacturing and consumers confront a rising tide of counterfeit electronics," *IEEE Spectrum*, vol. 43, no. 5, pp. 37–46, May 2006.

[6] K. Chatterjee and D. Das, "Semiconductor manufacturers' efforts to improve trust in the electronic part supply chain," *IEEE Trans. Compon. Packag. Technol.*, vol. 30, no. 3, pp. 547–549, Sep. 2007.

[7] K. Chatterjee, D. Das, and M. Pecht, "Solving the counterfeit electronics problem," in *Proc. Pan Pacific Microelectron. Symp. (SMTA)*, Jan. 30–Feb. 1 2007, pp. 294–300.

[8] L. Condra, "Combatting electronic component obsolesce by Using Common Processes for Defense and Commercial Aerospace Electronics," *Nat. Def. Ind. Assoc.*, pp. 1–12, Sep. 1999.

[9] C. Dyer and D. Rodgers, "Effects on spacecraft and aircraft electronics," in *Proc. Eur. Space Agency Workshop*, 1998, pp. 1–11 [Online]. Available: http://esa-spaceweather.net/spweather/workshops/proceedings_w1/SESSION1/dyer_effects.pdf,_1998

[10] E.D. Maynard, B. Cohen, C. Lau, and V. Sharma, "Defense trusted integrated circuits policy," in *Proc. GOMACTech'06*, San Diego, CA, 2006, [CD ROM].

[11] B. Cohen, J. Neumann, and V. Sharma, "Anonymity in COTS integrated circuit procurement," Inst. Def. Anal., IDA Doc. D-3167, Oct. 2005.

[12] Department of Defense, "Information assurance," DOD, Directive 8500.1.

[13] Department of Defense, "Defense acquisition system," DOD, Directive 5000.1.

[14] G. Carlson, "Trusted foundry: the path to advanced SiGe technology," in *Proc. IEEE Comp. Semicond. Integr. Circuit Symp. (CSIC'05)*, Oct./Nov. 2005, pp. 1–4.

[15] *"Diminishing Manufacturing Sources and Material Shortages (DMSMS) Guidebook"* Department of Defense, Nov. 2006 [Online]. Available: http://www.dmea.osd.mil/docs/sd22dmsms_Guidebook.pdf

[16] *Standard for preparing an electronic components management plan*, EIA-STD-4899–A, ANSI/GEIA, Dec. 2007.

[17] *Aerospace Qualified Electronic Component (AQEC) Requirements, Volume 1: Integrated Circuits and Semiconductors*, GEIA-STD-0002–1, Government Electronics and Information Technology Association, Dec. 2007.

[2]Paper reflects incorporation of OSD (AT&L), DMSMS Working Group, Institute of Defense Analysis, Aerospace Industry Association, Government Electronic Industry Association, and Semiconductor Industry Association comments received since first circulated February 2007 in draft as "Trusted Integrated Circuit Policy."

Sydney Pope received the B.Eng. degree from the University of Buffalo, Buffalo, NY, the M.S. degree in management from Salve Regina University, Newport RI, and the Diploma in international security and strategic studies from the U.S. Naval War College, Monterey, CA.

He joined the Office of the Deputy Under Secretary of Defense for Industrial Policy, Department of Defense, Washington, DC, in September 2005. He is the Department's Defense Priorities and Allocation System lead and is responsible for managing all aspects of the program. He is also lead analyst for the ground vehicle, soldier equipment, and electronics sectors. He is a technical and business expert in industrial capabilities and capacities and is responsible for establishing policies and brokering solutions that enable industry to meet DoD needs. Prior to his current assignment, he was with the Defense Contract Management Agency were he held numerous management and supervisory positions over 14 years including the Headquarters Director of Contract Technical Operations and as the Deputy Commander for the largest contract management field office in that Agency. Before 1991, he held assorted program management, contracting, and engineering assignments with the Air Force, Navy and Defense Logistics Agency. He entered federal service in 1977.

Mr. Pope is a Certified a Professional Contracts Manager.