SANDIA REPORT

SAND2011-8415

Unclassified Unlimited Release

Printed December 2011

Moore's Law And The Impact On Trusted And Radiation-Hardened Microelectronics

Kwok Kee (K K) Ma

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Approved for public release; further dissemination unlimited.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: <http://www.osti.gov/bridge>

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: [http://www.ntis.gov/help/ordermethods.asp?loc=7-4-](http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online)

[0#online](#)

Moore's Law And The Impact On Trusted And Radiation-Hardened Microelectronics

Kwok Kee (K K) Ma
Advanced Microelectronics and Radiation Effects
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-1073

Abstract

In 1965 Gordon Moore wrote an article claiming that integrated circuit density would scale exponentially. His prediction has remained valid for more than four decades. Integrated circuits have changed all aspects of everyday life. They are also the “heart and soul” of modern systems for defense, national infrastructure, and intelligence applications.

The United States government needs an assured and trusted microelectronics supply for military systems. However, migration of microelectronics design and manufacturing from the United States to other countries in recent years has placed the supply of trusted microelectronics in jeopardy.

Prevailing wisdom dictates that it is necessary to use microelectronics fabricated in a state-of-the-art technology for highest performance and military system superiority. Close examination of silicon microelectronics technology evolution and Moore's Law reveals that this prevailing wisdom is not necessary true. This presents the US government the possibility of a totally new approach to acquire trusted microelectronics.

Acknowledgment

The author would like to thank Paul Dodd, Fred Sexton and David Myers for their review and suggestions of this work.

Table Of Contents

<i>Abstract</i>	3
<i>Acknowledgment</i>	4
<i>Table Of Contents</i>	5
<i>Executive Summary</i>	7
<i>Evolution Of Silicon Microelectronics Technology</i>	9
Flat-lining of Moore’s Law	9
Longevity of the 90-nm technology node	13
Sweet-spot 0.35- μ m technology node	15
Technology nodes for military systems	16
<i>Trusted Microelectronics</i>	17
“DoD needs a focused, tailored (trusted microelectronics) acquisition plan.”	17
Current US approach to acquire trusted microelectronics	17
Practical approach for the US to acquire trusted microelectronics	20
Feasibility of a government-controlled Trusted Microelectronics Program	21
<i>Rad-Hard Microelectronics</i>	25
Value proposition of radiation hardening methodologies	25
Trusted rad-hard microelectronics as an extension to the Trusted Microelectronics Program.....	27
<i>Future of Military Microelectronics</i>	29

Executive Summary

The invention of the transistor at Bell Labs led to the development of the first silicon integrated circuit by Fairchild in 1961. Since then, microelectronic circuits have changed all aspects of everyday life. They are also the “heart and soul” of modern systems for defense, national infrastructure, and intelligence applications. Trusted microelectronics, that is, microelectronic components that will perform as expected, free from compromises, denials, exploitation, or other adversary-intended results, are essential to the reliable operation of military systems. However, migration of microelectronics design and manufacturing from the United States to other countries has placed the supply of trusted microelectronics in jeopardy. The lack of trusted microelectronics has resulted in complex microelectronic devices with unknown pedigrees being designed into military defense systems. The consequence of using untrustworthy microelectronic components in a critical military system is grave. Unfortunately, there is very little the US can do to reverse the trend of microelectronics industry migration, which is driven by global economics. The US government’s approach to acquire trusted microelectronics has become ineffective in the current microelectronics industry environment, and the shortage of trusted microelectronics has reached a critical stage. It is, therefore, imperative that the US re-examine trusted microelectronics supply chain policy and make necessary changes in the immediate future.

The US government has adopted a policy of relying on commercial microelectronics companies as the primary source for military microelectronics. This policy was successful in the past because the US had been the driver of microelectronics industry, and there were many onshore, US-owned silicon foundries to supply military microelectronics. Furthermore, trustworthiness was not a prominent issue until a couple of decades ago. In recent years, the number of onshore foundries has diminished rapidly. Today, only five US-owned companies are capable of fabricating state-of-the-art microelectronics, IBM, Intel, Texas Instruments, Micron, and Freescale. Only one of the five companies, IBM, is accredited as trusted foundry that allows government-access to its state-of-the-art process to develop low-volume, custom military microelectronics. Policymakers recognize that it is possible that the US may lose access to state-of-the-art foundries in the near future. However, they continue the current military microelectronics supply chain policy because no viable alternative has been suggested.

Prevailing wisdom dictates that it is necessary to use microelectronics fabricated in a state-of-the-art technology, driven by Moore’s Law, for highest performance. The premise is that the US government needs continuous access to state-of-the-art foundries in order to maintain US military system superiority. Close examination of the evolution of silicon microelectronics technology and Moore’s Law reveals that this prevailing wisdom is not necessarily true. It is possible to fabricate highest performance microelectronics using only 90-nm technology. In fact, a foundry with 90-nm and 0.35- μm capabilities could fabricate the full spectrum of microelectronics that is needed for military systems. This presents the possibility of a totally new trusted microelectronics supply chain policy, a government-controlled Trusted Microelectronics Program. Such a program is feasible, both technically and economically. It would consist of a foundry (or foundries) with 90-nm and 0.35- μm fabrication capabilities, a silicon technology research

and development team, and a robust microelectronics component design and development effort, in which current microelectronic contractors could play a major role. The aspect of government-controlled is important. A government-controlled microelectronics supply chain not only could assure trusted military microelectronics supply, it also could provide microelectronic products with tailored capabilities dedicated for military applications. Commercial state-of-the-art microelectronics has become a global commodity; every country, including those that are unfriendly to the United States, has easy access to it. As critical microelectronics infrastructure moves overseas, these countries are in a position to adopt a government-controlled microelectronics supply chain policy, and thus deny the US access to certain critical microelectronics components. Therefore, trusted microelectronic components specially designed for military application is necessary for the US to maintain future military technology leadership. As such, the Trusted Microelectronics Program requires a long-term commitment dedicated for military microelectronics. The program should be managed by a government-controlled organization, such as a Federally Funded Research and Development Center (FFRDC).

Rad-hard microelectronics is essential for some military systems. Because of the high-consequence nature of certain systems, trust and reliability of rad-hard microelectronics are paramount. Assuring supply of trusted rad-hard microelectronics can be accomplished by extending the Trusted Microelectronics Program to cover rad-hard components. Currently, there is a significant technical gap between available rad-hard microelectronic components and state-of-the-art microelectronics. By extending the Trusted Microelectronics Program to cover rad-hard components, there is an added benefit of enabling the rad-hard technology to catch up with state-of-the-art products.

Evolution Of Silicon Microelectronics Technology

Flat-lining of Moore's Law

Gordon Moore published his famous paper, "Cramming more components onto integrated circuits," which predicted the exponential growth of the number of silicon transistors in an integrated circuit in 1965. Moore's prediction quickly took on the moniker "Moore's Law" and has held true for over four decades. One of the reasons for its success is that it provided a roadmap for all aspects of the semiconductor industry to plan for the necessary infrastructure and technology developments required to scale to future generations. This ultimately became instantiated in the annual ITRS roadmap. Silicon transistor feature size has shrunk from 25 micrometers in the early 1960s to 32 nanometers today. Research on transistor feature size scaling is ongoing for 22 nanometers and below. Integrated circuit density has grown from 2300 transistors in Intel's 4004 processor (1971) to over a billion transistors in state-of-the-art processors today. However, Moore's Law has been showing signs of flat-lining in recent years.

Concurrent with scaling, the cost of developing a complex integrated circuit using state-of-the-art silicon technology has been escalating exponentially. The original Moore's Law assumed the cost of transistors continues to decrease from expected advancements in batch fabrication. This is no longer true today. Even though the cost per transistor has been decreasing, the rate of decrease has been declining and is unable to keep up with the exponential growth of transistor density.

Figure 1 shows the escalating cost of developing a System-on-a-Chip (SoC) integrated circuit as technology scales. The costs of developing different type integrated circuits may vary from SoC, but they follow the similar trend. As a result, devices available in sub-100-nm technologies typically are massively produced commodity products such as microprocessors, memories, FPGAs, etc, where very high development and infrastructure costs can be amortized effectively. Very few systems, other than those high-volume applications such as personal computers, cell phones, and game consoles can justify the costs of ultra-deep-submicron custom integrated circuit development as feature sizes shrink below 90-nm. Integrated circuit development cost is a filter for using silicon technology, and that filter has become more and more restrictive as technology scales.

Figure 1 – SoC development cost have soared from \$20 million at 90nm to nearly \$100 million at 32nm. [source: International Business Strategies (IBS)]

Transistor reliability margin has been decreasing as feature sizes shrink. The original Moore's Law assumed fabrication advancements will enable acceptable yield with adequate reliability. Over the years, a number of studies on reliability vs. technology scaling have been done. The overall results show that reliability concerns such as wear-out mechanisms of time dependent dielectric breakdown, hot carrier injection, negative bias temperature instability, electromigration, stress-induced voiding, etc., are exacerbated as a result of scaling. As technology scales, constant failure rate increases and wear-out failure occurs earlier. Many products using technologies below 90 nanometers are not suitable for high-reliability operation in harsh environments.

Figure 2 – Product Failure Rate Trend As Technology Scales.
Mark White, Yuan Chen, "Scaled CMOS Technology Reliability User Guide." [source: JPL Publication 08-14 3/08]

Figure 2 is a summary of product failure rate trend as technology scales. In anticipating the less-than-100% transistor functionality and reliability when feature sizes shrink below 22-nm, the microelectronics research community has recently been investigating redundant designs, fault tolerant methodologies, and self reconfiguration and repair architectures.

Computing speed peaked in 2002 at 3.8 GHz and has gradually decreased since then. One of the byproducts of transistor scaling was the speed-up of transistor operation. This had become a corollary to Moore's Law. As late as 2000 when Intel's Pentium 4 processor came out, the International Technology Roadmap for Semiconductors (ITRS) was predicting that microprocessor speed would continue to increase smoothly to 30 GHz or so. Unfortunately, the prediction was inaccurate because it did not model the wiring delays of complex circuits and the power requirement to drive long signal lines. In other words, signal delay from connections and power consumption, rather than transistors, started to dominate integrated circuit operating speed as circuit complexity (transistor density) increased.

Figure 3 shows the history of Intel processor clock frequency. Since 2006 – 2007, processor frequencies have stabilized around 3.0 GHz. Designers have discovered that they can no longer use the inherent

Figure 3 – Intel Processor Clock Speed
[source: Intel]

transistor speedup from scaling to “brute force” computer performance improvement. Instead, today’s microprocessors are designed to operate at lower clock frequency with more efficient processor architectures. Mark Bohr, Senior Fellow at Intel has stated, “Achieving very high operating frequencies is no longer the prime target for new microprocessors. Instead, the goal has shifted to delivering higher performance combined with lower power. Power efficiency is the main scaling goal for chips used both in small hand held devices and in large data centers.”

Transistor supply voltage scaling to reduce integrated circuit power consumption had to stop at around 1.0V, the minimum voltage level that can be maintained without severely impacting transistor performance. The original Moore’s Law assumed power consumption of a transistor would decrease with smaller feature sizes, thus newer generations of integrated circuits would maintain a constant power density. Unfortunately, the decreasing rate of transistor power consumption has been unable to keep up with the exponential growth of transistor density. At 0.35 micrometer, the semiconductor industry made a decision to lower the power supply voltage from 5.0 V to 3.3 V to achieve an acceptable power density level. Reducing transistor power supply voltage is an effective approach to reduce power consumption of integrated circuits because power consumption is directly proportional to the square of power supply voltage. Since then, the power supply voltage has been lowered in each technology generation to compensate for increasing power consumption by transistors. However, as power supply voltages approach 1.0V, at which 90-nm technologies operate, performance of the transistors becomes severely impacted.

Figure 4 shows the supply voltage scaling prediction by ITRS. As late as 2002, ITRS was predicting that supply voltage would scale aggressively from 1.2V in 2001 to 0.4V in 2016. In reality, the supply voltage scaling was nowhere close to the 2002 prediction. It only reduced by 0.2V, from 1.2V in 2001 to 1.0V in 2010. The semiconductor industry was unable to

continue aggressive transistor supply voltage reduction below 90 nanometers and had to investigate alternative materials to improve transistor performance and to reduce power consumption. This has led to the development of hafnium-based high-k dielectrics and metal gates for transistors built in 45-nm technologies, as well as low-k dielectrics to isolate metal wiring layers. Additional material changes are being investigated for technology nodes below 22 nanometers. One possibility is to replace silicon with other materials with higher intrinsic mobility such as III-V compound semiconductors, carbon nanotubes, graphene, semiconductor nanowires, etc. It is interesting to note that the semiconductor industry’s current efforts on transistor scaling are primarily focused on

material research and configuration development, such as multi-gate, to improve transistor performance, while there is minimal research effort to improve signal connection efficiency. Today's state-of-the-art integrated circuits have 9 to 11 copper layers to handle the complexity of signal and power routing. It takes a significant amount of power and time delay to send a signal from one end of the die to the other end. The situation is only going to get worse as transistor density grows. Even if the semiconductor industry could eventually develop an ideal transistor with minimum power consumption and no static leakage current, the complexity of signal connections would dominate integrated circuit power consumption and operating speed. Effectively, signal connection complexity is limiting the number of transistors that can be used in a large circuit.

Chip-stacking technology is advancing rapidly. Chip-stacking is a viable alternative to increase transistor density through the third dimension instead of the two-dimensional transistor scaling. Today's packaging industry is routinely stacking 4 to 8 die in a package. More than 32-die stacks have been demonstrated by Vertical Circuits, Inc., a startup company in California. They claim their wafer-level approach to integrated circuit die stacking, the Micropede™, can be made from as few as 2 or as many as 1024 die. IBM announced in March 2010 that they are collaborating with two Swiss partners, École Polytechnique Fédérale de Lausanne (EPFL) and Swiss Federal Institute of Technology Zurich (ETH), to develop chip cooling techniques to support 3D chip architecture. The microelectronics industry is making significant progress to extend Moore's Law through 3D chip stacking instead of transistor scaling.

How long will Moore's Law continue? How long will Moore's Law continue is a question of economic drivers instead of technology capability. Many people in the past had predicted that Moore's Law would end soon because of technical difficulties in material and processing to continue transistor scaling. For decades they were wrong. Moore's Law continues to hold true today. It is an interesting exercise to examine the drivers for the continuation of Moore's Law's in the current environment. As discussed earlier, future transistor scaling would not advance computing speed because latency of complex signal connections is dominating computing system clock frequency. Future transistor scaling would not improve integrated circuit reliability; rather it would decrease integrated circuit reliability margins. Future transistor scaling would not reduce power consumption because signal transmission power of a complex circuit is overshadowing transistor power. Future transistor scaling would not increase circuit design complexity because connection complexity is limiting the number of transistors that can be used in a large circuit. Finally, future transistor scaling would further increase foundry capitalization and fabrication costs.

What then is driving Moore's Law? The answer is that foundry infrastructure cost can be amortized to reduce unit cost if the production quantity is large enough. Since the foundry and fabrication costs are escalating, production quantity must increase proportionally in order for the cost/profit tradeoff to be favorable. That implies new technology nodes are more and more optimized and dedicated to a small number of ultra-high-volume "killer" products. Stating this differently, economics, which has been the

“real” driver of Moore’s Law for over four decades, continues to exist today. However, the number of products to which this economic driver applies is diminishing.

In the past, the computer industry had a free ride on the wake of Moore’s Law. Whenever a new generation of silicon technology appeared, computer performance would essentially double automatically and the cost of a new computer would be reduced. As a result, computer performance exploded, along with consumer demand. The computing industry’s free ride ended when silicon technology shrank below 90 nanometers in the early years of 2000. Today’s advancements in computer performance mostly rely on design innovations such as multi-core processors, more efficient pipeline architectures, larger cache memories, higher data/memory bandwidth, etc. At this time, it appears material and processing technology advancements will support transistor scaling for at least several generations into the future, well below 22 nanometers. However, maintaining the growth of computer performance by design innovation is getting harder and harder for each generation, as evidenced by the slowdown of advancement in computer performance in the last decade. Will this affect future consumer demands, and thus the continued production quantity growth of “killer” products? Only time will tell. It is almost certain that when Moore’s Law comes to an end in the future, it will be the result of a diminishing economic driver rather than the lack of technical innovation.

Longevity of the 90-nm technology node

There are many indications that 90-nm technology is a major technology node that will be around for many years in the semiconductor industry.

90-nm technology is the first technology node with low-k dielectric material and full implementation of copper-stack connections, giving integrated circuits a significant boost in speed and power performance by improving connection efficiency. In the late 1990s, the microelectronics industry started to realize that interconnect delays within a complex circuit were limiting integrated circuit operating speed. Some 130-nm technologies introduced copper interconnects and low-k dielectric materials between metal layers to improve signal connection efficiency. Implementing copper-stack connections with low-k dielectrics was a major event in the silicon technology advancement roadmap. The material changes were not fully perfected and implemented until 90-nm technologies. There was a significant speed increase in the 130-nm and 90-nm technology nodes, and computing system operating frequency peaked in 2002 at 3.8 GHz. Since then, very little has been done by the semiconductor industry to improve on-chip signal connection efficiency. Therefore, 90-nm technology is the first technology node with the most efficient signal connection technology existing today.

90-nm technology is the last technology node in which aggressive transistor supply voltage scaling was employed by the semiconductor industry to reduce integrated circuit power consumption. A typical 90-nm transistor operates around 1.0V to 1.2V power supply voltage. From a power dissipation density vs. performance perspective, 90-nm technology is one of the more power-efficient technology nodes. By reducing the threshold voltage for turning transistors on, further reduction of transistor power supply

voltage below 1.0 V would have significantly increased transistor's off-state leakage current to an unacceptable level. Below 90 nanometers, the inability to further scale transistor supply and threshold voltages and fundamental physical limitations on the subthreshold slope lead to an over-constrained system that cannot offer both high performance and low power dissipation simultaneously.

The 90-nm technology is optimized in many performance aspects and its transistor-level performance is equivalent to or better than technologies with smaller feature sizes. This assertion is contrary to the prevailing wisdom that smaller transistors are better for an integrated circuit. Therefore the statement requires close examination to put it in context.

As transistor density continued to grow, there were several unintended consequences on the *design* of integrated circuits. First, signal interconnection delays in complex logic circuits started to dominate the integrated circuit performance. Second, it is extremely difficult and time consuming to accurately design and simulate a complex logic circuit because the circuit performance is highly dependent on a custom physical layout of ultra-small transistors and connections. A further side effect of this dependence of circuit performance on technology layout parameters is that designs are no longer easily transportable between different technologies. Third, the continued increase in power density due to transistor leakage is approaching a practical limit on the number of transistors that can be integrated into a circuit, even though transistor density is increasing as technology scales. In summary, the design complexity of an integrated circuit cannot keep up with the exponential increase of the transistor density from technology scaling. To mitigate these limitations, circuit designers started to use structured architectures and power-efficient circuits. The structured design approach keeps the logic complexity of individual designs at a manageable level while taking advantage of increased transistor density. The structured design approach also enables shorter connection wire lengths and minimizes long-wire global signals, which is the primary factor of limited circuit speed and increase power consumption. As a matter of fact, complexity of a single logic design exceeding 500K gate-equivalent is rare. All very-high-density integrated circuits are composed of step-and-repeat of smaller circuits. To mitigate excessive power consumption issues, designers also started to use power efficient circuits. A power efficient circuit typically is a large circuit with many transistors, but only a small portion of the circuit is actively consuming dynamic power. For example, in an asynchronous logic circuit, only a small portion of the circuit is actively switching and processing information changes. Another example is memories. Memories require many transistors to store information, but only a very small portion of the memory, i.e., a byte or a word, is being accessed at one time, actively consuming dynamic power.

A close study of microprocessor evolution in the last decade illustrates the changes to more structure and power efficient design approaches. In the past, logic complexity of state-of-the-art microprocessors tracked the density and advancement in silicon technology scaling. In fact, the number of transistors used in a microprocessor is often used as a matrix to illustrate Moore's Law for many years.

Figure 5 is one of many such illustrations from Intel. The Pentium 4 introduced in November 2000 represents the epitome of processor complexity. It achieved a very high clock speed of 3.8 GHz by using deep pipelines of up to 29 stages. However, the advantage of the Pentium 4 complex architecture in benchmark evaluations was not clear. Even at 3.8 GHz, the operating clock speed was far below Intel's expectation of 10 GHz as a result of the frequency ceiling due to transistor power leakage. Since then, advanced processor development has focused on multiple cores, increasing memory bandwidth, increasing the cache size, using shorter and more efficient instruction pipelines, along with lower clock speed. Processors developed after Pentium 4 put greater emphasis on energy efficiency and performance per clock, resulting in a less complex processor core.

Figure 5: Moore's Law illustrated by density of Intel Processors [source: Intel]

It is interesting to note that Moore's Law continues to hold true today only from a transistor density perspective. Other corollaries of the Moore's Law such as reliability, power consumption, operating speed and cost, have already flat-lined many years ago. The purpose of continued transistor scaling is to reduce production cost by increasing the number of products in a production run. The latest sub-90-nm silicon technology foundries are optimized for a few ultra-high-volume commodity products such as microprocessors, graphic accelerators, memories, and SRAM-based FPGAs. These products are specifically developed for consumer-oriented applications such as personal computers, mobile phones, gaming consoles, workstations for communication and data processing, etc. Stated differently, using the latest technology nodes to fabricate low-volume, high-reliability integrated circuits for military systems is, in general, not practical, and perhaps not advisable from performance and reliability points of view. With die-stacking technology maturing, one can envision that high-transistor-density products may be realized through three-dimensional expansion of the die instead of the shrinking of the feature sizes on a die. Looking ahead, the benefits of future generations of higher-density-transistor technology are diminishing. All these considerations are pointing to the conclusion that the 90-nm technology will be around a long time to support the needs of general microelectronic applications. The Chinese government has been purchasing 90-nm equipment from major US foundries when they were shutting down several years ago. This situation was mostly viewed as a "second-tier" country's attempt to catch up on technology. No noticeable assessments have been made to examine whether this was in the national interest of the US or not.

Sweet-spot 0.35- μ m technology node

0.35 micrometer is a very important feature size in the evolution of silicon technology. The 0.35- μ m node introduced in mid-1990 is a mature technology. With today's escalating costs, development and fabrication of 0.35- μ m integrated circuits are relatively

inexpensive. Capable of more than 10,000 logic gates per millimeter square silicon area, 0.35- μm technology is adequate to meet the requirements of medium and lower density integrated circuits, which account for a significant portion of microelectronic components in a system. These are some of the nice characteristics of the 0.35- μm technology, but they are not the reason why 0.35- μm technology is an important node in the evolution of silicon technology. What makes it particularly important is that 0.35- μm technology is the first major technology node using reduced power supply voltage. Prior to the 0.35- μm technology node, silicon integrated circuits were dominated by 5.0-V power supply devices. Reducing power supply voltage to 3.3 V enables lower power consumption of the integrated circuits. Therefore, 0.35- μm transistors are highly optimized from performance, transistor density, and power consumption perspectives. More importantly, the 3.3-V supply is not too low for precision analog signal applications. At 0.18- μm or smaller feature sizes, power supply voltages are drastically reduced to 2.0V, 1.8V, 1.6V, etc., thus degrading signal-to-noise ratio of analog signals. Most analog technology experts would agree that the 0.35- μm technology node is a sweet spot for analog circuits with highest transistor density and adequate signal-to-noise margin for precision analog signals. In addition to analog and mixed-signal functions, the 0.35- μm technology can be modified to handle high voltage signals, such as 10-12 V or higher. This is important for interface and power circuits, another class of integrated circuits in a system. The importance of the 0.35- μm technology node cannot be overemphasized for full system implementation.

Technology nodes for military systems

The study of the evolution of silicon microelectronics technology shows that Moore's Law continues to hold true today, but only from a transistor density perspective. The driver of continued transistor scaling is economics: reduced production cost of ultra-high-volume "killer" microelectronic products, of which the number is diminishing. Since 2000s, advancements in computing performance are mainly the result of innovations in integrated circuit design and architecture, not from transistor scaling. Looking ahead, the benefits of future generations of higher-density-transistor technology are diminishing. Therefore, this study concludes that using the latest technology nodes to fabricate low-volume, high-reliability integrated circuits for military systems is not practical, and perhaps not advisable from performance and reliability points of view. Finally, this study suggests that 90-nm and 0.35- μm technologies are two optimized technology nodes that can support fabrication of state-of-the-art military microelectronics components for the foreseeable future.

Trusted Microelectronics

“DoD needs a focused, tailored (trusted microelectronics) acquisition plan.” (DSB HPMS Report, 2005)

Microelectronics circuits are the “heart and soul” of modern systems for defense, national infrastructure, and intelligence applications. Trusted microelectronics, that is, microelectronic components that will perform as expected, free from compromises, denials, exploitation, or other adversary-intended results, are essential to the reliable operation of military systems. Migration of critical microelectronics design and manufacturing from the US to other countries started in the late 1980s and has accelerated in recent years. Driven by global economics, it is impossible to reverse the migration trend. The potential for untrustworthy integrated circuits to make their way into US defense systems is real, and the concern continues to heighten as time passes. Dr. William Howard, Chairman of the Defense Science Board Task Force on High Performance Microchip Supply stated succinctly, “DoD needs a focused, tailored acquisition plan, driven by a long-term vision of its semiconductor needs, to establish the basis, policy and operating guidelines for DoD-enabled access to trusted foundry services by the defense department, its contractors and others.”

Current US approach to acquire trusted microelectronics

Despite heightened awareness of the need and significant investment, the United States currently does not have an adequate trusted microelectronics program to supply trustworthy devices for defense systems. The Trusted Access Programs Office (TAPO) Trusted Foundry program, one of the most visible and well-funded microelectronics trusted supplier development initiatives, was established by the government in 2003. After eight years of the program, a close examination of the results leads to the conclusion that its impact on the supply of trusted microelectronics is marginal. The security requirements to be accredited as a “Trusted Foundry” are relatively minimal. As examples, only a few “key personnel” who has foundry product access are required to have security clearances. The requirements for a trusted foundry security plan can be easily satisfied by minor modifications to existing foundry procedures. The only “hard” requirement for trust accreditation is that a trusted foundry must be ISO9000 certified, which is a quality rather than security certification. Essentially, the TAPO trusted foundry accreditation is set up in such a way that any onshore microelectronics foundry could qualify with minimum effort. The reason is obvious, very little can be done to significantly enhance product trustworthiness without major impact to commercial foundry operation. As a result, trusted foundry accreditation has only incremental and limited improvement on product trustworthiness. The reality is that Trusted Access Program has far more to do with “Access” than “Trust.” It is designed to give programs access to an on-shore high-performance foundry once the government-owned trusted foundry was shut down at Fort Meade. The report by the Defense Science Board (DSB) Task Force on High Performance Microchip Supply in February 2005 stated, “...(Trusted Foundry Strategy) addresses near-term needs. It has no overall vision of its future microelectronics components needs and how to deal with them.” In 2005, DARPA initiated the Trust Program. DARPA’s approach is to develop technical methodologies to assure trustworthy microelectronic components. This program has sponsored some

significant trust validation solutions such as Physical Unclonable Function (PUF). However, after five years of effort, DARPA's Trust Program has failed to meet its original stated objective, that is, "to assure trustworthy microelectronic components regardless of the source of manufacturing." The program goal exceeded the available technology. DARPA has recently decided to terminate the Trust Program and initiate a new Integrity and Reliability of Integrated Circuits (IRIS) program. The objective of the IRIS program is to develop technologies that can derive the functionality of an IC to determine unambiguously if malicious modifications have been made to that IC. No doubt the IRIS program will develop innovative methodologies to derive IC functionality. Whether they will unambiguously determine the presence of malicious modifications of an IC remains to be seen. One thing is sure, DARPA's IRIS program, like its predecessor Trust Program, is an advanced technology research effort with little near-term impact to current trusted military microelectronics crisis.

The US government's current approach to assure trusted military microelectronics supply may be categorized into four approaches.

1. Federally-funded foundries. The main problems of this approach are the high cost necessary to avoid technology obsolescence and the narrowly focused mission for each foundry. Recently, operations at Fort Meade and Space and Naval Warfare Systems Command (SPAWAR) were shut down due to lack of funding for technology upgrades. Other federally-funded foundries are successful only in their narrowly focused missions. MIT Lincoln Laboratory is a research laboratory with minimum production capability. The Defense MicroElectronics Activity (DMEA) is established to support older technology nodes. The MESA Microfabrication Facilities at Sandia National Laboratories are dedicated to develop strategic radiation-hardened microelectronics technology and to fabricate trusted components for the nuclear weapon stockpile and supporting functions. None of the federally-funded foundries has the current capability to step up and produce the required variety and volume of parts as the nation's trusted military microelectronics supplier.
2. Rely on commercial foundries to develop microelectronic products suitable for military systems. The problem of this approach is that the product volume of military microelectronics is so small that no commercial foundry can justify their return on the investment required to maintain operations at a production level. BAE Systems and Honeywell SSEC are the two remaining commercial foundries dedicated to military systems. These two foundries have been searching, without success for two decades, for a sustainable and profitable business model to supply microelectronic devices for military applications. Their struggling survival is sustained only by continued government subsidies, which are highly unpredictable and depend on the whim of the Congress.
3. Gain access to major commercial foundries for military microelectronics fabrication. This approach resulted in the establishment of TAPO's trusted foundry using IBM. There are many pitfalls in this approach. For example, IBM has no incentive to modify their commercial fabrication process to accommodate special requirements for military microelectronics needs, including meeting the ruggedized requirement for environmental survivability. IBM is only a "quasi"

trusted facility for the reasons stated earlier. The likelihood of any major commercial foundry such as IBM changing its foundry's infrastructure to ensure "real" trust is nil in the absence of exorbitant government subsidies.

4. Military microelectronics acquisition policy and guidance. DoD has developed many acquisition policies and guidance since the early 1990s. Examples are Essential Program Information, Technologies, and/or Systems (SPITS) in 1994, Trusted Suppliers of ASICs in 2004, Critical Program Information (CPI) in 2005, Supply Chain Risk Management in 2008, Engineering for System Assurance Handbook in 2008, IC Industry Survey, System Assurance Handbook, Counterfeit Survey.... All these policies and guidance took a similar approach by analyzing and managing the risk of untrustworthy ICs. However, none of them address the fundamental issue, that is, that the supply source for trusted microelectronics is unstable and diminishing and will completely disappear soon. The epitome of the ineffectiveness of policy approaches can be illustrated when Congress, in October 2008, required DoD to develop policies for assuring trust in ICs within 180 days.

While the US government is struggling with the trusted microelectronics supply chain issue, the overseas migration of critical microelectronics infrastructure continues. Today, only five US-owned companies have state-of-the-art fabrication capability: IBM, Intel, Texas Instruments, Freescale, and Micron. According to Office of Technology Evaluation (OTE) of Department of Commerce, two of the five companies, Freescale and Micron, are in high financial risk category. Of the five companies, only one, IBM, is willing to allow the US government to have access to its state-of-the-art technologies to develop and produce low-volume, customer military microelectronic components. EE Times examined IBM's semiconductor capital expenditure plan and reported on November 24, 2010, "IBM appears set to gradually back away from semiconductor manufacturing and to rely for its leading-edge silicon on Samsung and GlobalFoundries as foundry suppliers." These facts clearly point to the instability of today's trusted microelectronics supply chain.

The lack of trusted microelectronics results in complex microelectronic devices with unknown pedigrees being designed into critical military defense systems. This is because the trusted microelectronics issue is complex and there isn't any simple, low-cost solution. The adoption and mandate of using commercial off-the-shelf (COTS) components by the military to save system development costs since early 2000 further exacerbates the situation. Since the early 1990s, the US government has recognized the importance of trusted microelectronics for military applications. Yet 20 years later, the government has still failed to secure the supply of trusted microelectronics. The reason is simple. The US government has been relying on the commercial sector as the sole source of microelectronics supply, and this source is moving overseas. In May 2008, IEEE Spectrum ran a feature article "The Hunt for the Kill Switch" by Sally Adee. The article gave a good overview of the danger of using untrustworthy components in military systems. It is not a question of whether or not one of the US military systems will be compromised, but rather a question of when we will discover major compromises have occurred. When that happens, the issue of trusted microelectronics for military systems will be addressed by the government with a new sense of urgency.

Practical approach for the US to acquire trusted microelectronics

*The trustworthiness of a device is directly proportional to the level of control of that device throughout its life cycle. One may consider “trustworthiness” and “vulnerability” as two faces of the same coin. Everyone would agree that it is impossible to build a house that is invulnerable to thieves. It is the continuing vigilant awareness and monitoring that make a home safe. The same thinking should apply to trusted microelectronics – but it doesn’t. Policymakers continue to hope (wish) for a process or procedure to acquire inexpensive, trusted microelectronic devices that are manufactured in an uncontrolled, untrustworthy, and in some cases, explicitly adversary-controlled environment. In the executive summary of the Defense Science Board (DSB) Task Force report on High Performance Microchip Supply, it is clearly emphasized, “Trust cannot be added to integrated circuits after fabrication; electrical testing and reverse engineering cannot be relied upon to detect undesired alterations in military integrated circuits.” Indeed, the lack of results from DARPA’s Trust Program further confirms the DSB report’s statement and what most experts already know, that is, today’s state-of-the-art integrated circuits are too complex to exhaustively verify every component to be free from undesired alterations. From a national security perspective, all commercial microelectronics foundries are operating in an unsecure environment. These foundries’ security procedures are focused upon protecting trade secrets at best. *The reality is that the government cannot rely on any commercial foundries, overseas or domestic, to supply trusted microelectronics.* The only trusted microelectronic devices are those that are designed, fabricated, packaged and tested in a controlled and trusted environment.*

This leads to the only logical conclusion, a government-controlled Trusted Microelectronics Program is necessary to assure a trustworthy microelectronics supply for future high-value military systems. A government-controlled Trusted Microelectronics Program would include the elements of microelectronics design, fabrication, packaging, and test.

1. A 90-nm foundry capability is necessary to support the development and production of high-throughput digital microelectronic components. The most economical approach to establish such a capability is through acquisition of a 90-nm foundry being decommissioned by the semiconductor industry.
2. A larger feature-size 0.35- μ m foundry capability is necessary to support the development and production of mixed-signal, high-voltage, and other microelectronics components. A military system needs high-density, high-performance digital microelectronic components; it also needs many larger feature-size microelectronic devices. There are federally-funded foundries in the US that currently have larger feature-size capability, including Sandia’s MESA Microfabrication Facilities.
3. Establish an appropriately sized foundry technology research and development team and maintain a robust microelectronic component design and development effort. Current military microelectronic contractors could play a major role in this infrastructure.

Feasibility of a government-controlled Trusted Microelectronics Program

The government-controlled Trusted Microelectronics Program consists of different elements, including microelectronics design, fabrication, packaging, and test. The questions are whether such an approach is feasible to meet the diverse need of military system critical microelectronics, and how much such a program would cost.

The government has been relying on the commercial microelectronic industry to supply military microelectronics. This led to the current trusted supplier crisis when the US microelectronic industry started to migrate overseas in the late 1980s. The situation has reached a critical stage because there are very few microelectronic companies left in the US. However, the US government has not changed its microelectronics supply chain policy. This is because of the prevailing wisdom that state-of-the-art microelectronic systems rely on state-of-the-art foundry products. As pointed out earlier in the study of silicon microelectronics technology evolution, this prevailing wisdom is no longer true. Since the 2000s, advancements of integrated circuit performance have primarily resulted from design and architecture innovations. Furthermore, the study showed that the 90-nm and 0.35- μm technology nodes are two well-suited to answer the needs of low-volume, high-reliability applications such as military systems. This suggests a new paradigm for military microelectronics supply. That is, *a 90-nm foundry and a 0.35- μm foundry could support the development and production of state-of-the-art military microelectronic components for the foreseeable future.*

The essence of a successful trusted military supplier solution relies on the supplier's ability to provide a portfolio of trusted microelectronic products that are as good as, or very close to, state-of-the-art commercial parts. There are a large number of microelectronic products available on the market. However, close examination of a complete microelectronic system would reveal that there is only handful of classes of microelectronic components: microprocessors, microcontrollers, FPGAs, memories, interface devices, A/D and D/A converters, power supplies, etc. Within each microelectronic class, typically there are several components that are most used by military systems. The total number of trusted microelectronic products that need to be developed for military systems is large, but it is not an insurmountable number. Component development would be an ongoing effort, and the infrastructure of existing military microelectronics contractors would play an important role. In addition, the government could license the design of existing commercial products, a practice that has long been used by the government to develop radiation-hardened microelectronics. The commercial designs would be validated for their trustworthiness and converted to the government-controlled foundry. The cost of such an approach would be significantly less than developing totally new microelectronics products.

Integrated circuit performance will continue to grow, but not at the frenetic pace we faced during the last four decades of the Moore's Law era. More significantly, performance improvement of new integrated circuits will rely less on density growth and more on architectural innovations and advances in packaging and communication. The current circuit design trend toward simpler, more efficient structured architectures will ease the design burden and increase design reusability. As an example, in the past, a

microprocessor would have become obsolete within a few years, replaced by a newer microprocessor with higher performance and more features whenever a new technology node was introduced. Nowadays, microprocessors utilize highly efficient, less complicated processor cores, and the focus of improvement is on architecture, such as multi-core, added memories, or enhanced memory bandwidth. One can envision a pre-designed microelectronics product portfolio that includes optimized processor cores for different structures. Therefore, the design obsolescence issue will be greatly reduced, enabling the government to develop a comprehensive product portfolio for meeting different system requirements.

Financially, the cost of a government-controlled Trusted Microelectronics Program is well contained. From a foundry infrastructure cost perspective, the flat-lining of Moore's Law leads to a more stable microelectronics technology environment. Foundries will start to consolidate and gravitate towards application needs. The life cycle of technology nodes will be extended, along with processing equipment support. All of these will lead to lower foundry equipment and infrastructure costs in the future. The facts that 90-nm technology is a highly optimized technology node and that we can rely on chip-stacking technology to achieve high transistor density have a profound impact on lowering the foundry infrastructure cost. It will no longer be necessary to chase Moore's Law by having a new foundry facility every few years in order to fabricate devices with state-of-the-art performance. From a product development infrastructure cost perspective, the fact that today's complex designs have structured architectures implies that it is possible to develop a design portfolio with limited number of design building blocks, and future design iterations and improvements can be accomplished on a shorter schedule and at lower cost. The US government currently spends \$3.0B to \$6.0B every year for the procurement of military microelectronics. With proper management, the Trusted Microelectronics Program could operate at a similar yearly budget level to supply military microelectronics needs. This vision will take several years to realize, but it is achievable.

A government-controlled microelectronics supply chain not only could assure trusted military microelectronics supply, it also could provide microelectronic products with unique capabilities dedicated for military applications. Commercial state-of-the-art microelectronics has become a global commodity; every country, including those that are unfriendly to the United States, has easy access to it. As critical microelectronics infrastructure moves overseas, these countries are in a position to adopt a government-controlled microelectronics supply chain policy (there are indications that some of them have already begun to do so), and thus deny the US access to certain critical microelectronics components. Therefore, trusted microelectronic components specially designed for military application is necessary for the US to maintain future military technology leadership. As such, the Trusted Microelectronics Program is an ongoing research, development, and production effort with a long-term commitment. *The most efficient approach to manage such a program is by an organization such as Federally Funded Research and Development Center (FFRDC).* There are many FFRDCs today, including the national laboratories. Some of them are qualified and suitable candidates for such a mission. While the linewidth of semiconductor manufacturing technology may

saturate, innovation in design, architecture, packaging and integration cannot be stopped. In addition, as research continues to pursue “Beyond Moore’s Law” options, the Trusted Microelectronics Program must move in step to evaluate the viabilities and vulnerabilities of alternative technologies to prevent new vulnerabilities from arising in performance, control, or operations.

Rad-Hard Microelectronics

Rad-hard microelectronics is essential for systems that operate in radiation environments. Examples are satellites and nuclear weapon systems. Even for systems that are not operating in hostile radiation environments, radiation effects have become a concern. The latest high-density integrated circuits, with very small transistor feature sizes, have become increasingly sensitive to cosmic rays present in the earth's atmosphere. This affects the reliable operation of complex systems in terrestrial or high-altitude applications.

Because of the high-consequence nature of some military systems, trust and reliability of rad-hard microelectronics are paramount. Assuring the supply of trusted rad-hard microelectronics is more difficult than typical trusted microelectronics. This is because special design and fabrication techniques are necessary to radiation hardening microelectronics devices. There are technical challenges and infrastructure investments required to harden state-of-the-art microelectronics. Unfortunately, rad-hard microelectronics, while critical to some military systems, constitutes only a small portion of the low-volume military microelectronics market. Commercial interest in rad-hard microelectronics technology research and product development is essentially nonexistent without government subsidy.

Value proposition of radiation hardening methodologies

Radiation hardened technology has been trailing further and further behind state-of-the-art silicon technology in recent years. Since the beginning of rad-hard technology development, rad-hard silicon foundries claimed to keep up with Moore's Law, with rad-hard components available one or two generations behind state-of-the-art commercial products. These rad-hard foundries have specially-developed and dedicated process lines to fabricate rad-hard devices. This radiation hardening methodology is called rad-hard-by-process (RHBP). As transistor feature sizes continued to shrink, the cost of developing new RHBP technology nodes became more and more expensive, and are prohibitively so today. As a result, there is no RHBP technology available now that is one or two generations behind state-of-the-art 22-nm commercial technologies. The last "true" RHBP technology node is 0.15- μm technology from Honeywell SSEC and BAE Systems. Today, the primary radiation hardening methodology for technology nodes below 0.15 micrometer is rad-hard-by-design (RHBD). The RHBD approach, as the name implies, does not require modification of foundry processes, thus no dedicated foundry process line is necessary. RHBD is essentially a collection of radiation-hardening design techniques. Each technique is able to mitigate a certain aspect of radiation effects. These techniques typically depend on specific technology node and the target application, and carry certain performance, power, and density penalties. As a result, most RHBD components are typically "quasi" radiation-hardened (rad-tolerant), depending on how many radiation hardening techniques are applied.

With high-density microelectronic components below 0.15 micrometer available only in non-rad-hard or rad-tolerant versions, designers of high-performance rad-hard systems have changed their design philosophy and approach. Driven by the need to continue to

improve system performance and to keep the development cost and schedule at reasonable level, rad-hard system designers have no choice but to use non-rad-hard or rad-tolerant parts when high-density components are needed. To overcome potential errors or failure of these components in radiation environments, system designers have to develop more robust and fault-tolerant systems to mitigate radiation effects. Some examples are double or triple redundancy, error detection and correction, periodic data scrubbing, functional reconfiguration, system reset, etc. Fortunately, most computing systems that require high-density, state-of-the-art components for high performance, such as imaging, sensor data reduction and processing, encryption, etc., can tolerate some degree of data noise and errors. These systems typically have the flexibility to use system architecture approaches to mitigate errors from radiation effects. However, the penalty for using non-rad-hard or rad-tolerant components is high, to the extent that system performance may be compromised. Obviously, rad-hard system designers would prefer to use rad-hard components if they exist, and if the cost-performance-schedule tradeoff allows.

The value proposition of current rad-hard-by-process (RHBP) methodology is limited to providing high-rel, rad-hard components of larger feature-size technologies. While high-performance data processing systems may tolerate some degree of data errors and distortions, systems that perform command and control functions usually cannot afford to have occasional errors. Therefore, “quasi” rad-hard components that may generate occasional errors are not suitable. Fortunately, most command and control functions, such as those in arming and firing of a weapon system, have relatively simple circuits. These systems could be implemented using components with larger feature-size technologies. This is the area where current RHBP technologies provide value. Another area that RHBP can provide value is mixed-signal, analog, and discrete power components. These components, by their technical nature, require larger feature-size technologies. To fully illustrate that the value proposition of RHBP is limited to larger-size technology nodes, consider the following anecdote. In the year 2000, Honeywell SSEC and BAE Systems successfully secured \$300M Title III funding from the government (\$150M for each company) to recapitalize and update their rad-hard processing line from the 0.25-0.35 μm to the 0.18- μm node. The name of the project was “One-Gen,” that is, keeping the radiation hardened technology one generation behind state-of-the-art technology. After working on this project three or four years, Honeywell and BAE Systems decided (or were directed?) to abandon the 0.18- μm node and moved the development effort to the 0.15- μm node. The reason given was that 0.18 μm technology in 2004 or 2005, the time when the development would have been completed, would be too far behind state-of-the-art technology. Honeywell and BAE Systems worked on 0.15- μm technology for another two or three years before rad-hard products became available. By that time, no one was mentioning “One-Gen” any more. The whole exercise illustrates how difficult it is to radiation harden a technology node as feature sizes become smaller. But that is not the point of this story. The point is that, after 0.15- μm RHBP capability was established, Honeywell and BAE Systems’ market share did not expand significantly relative to other RHBD vendors who provide rad-tolerant products. In other words, rad-hard system designers are opting for rad-tolerant or non-rad-hard state-of-the-art devices over 0.15- μm rad-hard components for high-

performance applications. The inability of RHBP foundries to keep up with state-of-the-art technologies limits their value of contribution to high-performance rad-hard systems. In fact, it should be noted that Honeywell and BAE Systems continue to maintain their older 0.8- μm , 0.5- μm and 0.35- μm rad-hard technologies.

The value proposition of current rad-hard-by-design (RHBD) methodology is limited by the penalties it incurs in performance, power and density. Unfortunately, there is no convenient, non-invasive way to harden a state-of-the-art commercial technology. The RHBD approach does not require a dedicated rad-hard process line in the foundry; however, it imposes a high cost in terms of circuit density and performance. Furthermore, RHBD devices typically depend on specific technology nodes and the target application, and therefore are not transportable between foundry technologies. Thus “rad-tolerant” devices are proliferating, in which only selected aspects of radiation effects were hardened, driven by perceived needs of specific systems. Currently there isn’t a comprehensive RHBD methodology portfolio that can cost-effectively keep up with transistor scaling. As silicon technology advances and feature sizes shrink, single-event effects (SEE) become dominant. The penalties of RHBD in terms of effectiveness, transistor speed, power dissipation and integrated circuit density, are increasing correspondingly. There are indications that when transistors are scaled below certain feature sizes, the performance degradation of some RHBD techniques is so severe that they are no longer a viable approach for radiation hardening. In other words, the effectiveness of current RHBD methodology is diminishing as transistor continues to scale.

In summary, current advancement in radiation hardening, both RHBP and RHBD, is lacking far behind state-of-the-art technology. There isn’t any cost effective and efficient radiation hardening approach that can keep up with transistor scaling. This situation could be stabilized if 90-nm becomes technology node of the future for military systems.

Trusted rad-hard microelectronics as an extension to the Trusted Microelectronics Program

The situation that rad-hard technology is trailing far behind state-of-the-art silicon technology can be traced to some fundamental issues: commercial industry has even less interest in the rad-hard microelectronics market than the broader military electronics market, and the rad-hard microelectronics community has not been able to keep up with the latest commercial foundry processes because of their associated costs. Furthermore, radiation hardening of sub-100-nm microelectronics presents a tremendous technical challenge and requires significant investment and long-term commitment. Since rad-hard microelectronics are essential to certain high-value military systems, government sponsorship is necessary to provide a focused effort. Therefore it is logical to extend the government-controlled Trusted Microelectronics Program to include Trusted Rad-hard Microelectronics. There are many advantages of such arrangement:

1. Foundry access. The rad-hard microelectronics community would regain direct foundry access without the concern of continuing escalation of foundry infrastructure cost.

2. Defined goal. With the 90-nm technology node being maintained for military applications for the foreseeable future, resources of rad-hard microelectronics development, either by process or by design, can be focused. The notion of “One-Gen” is no longer applicable.
3. Broadened scope. Development of microelectronic devices that can survive in extreme radiation environments is important to certain special government systems. Examples of these extreme radiation environments are high dose rate during a nuclear weapon blast, or high total dose accumulated during deep-space mission. In a market driven industry, those topics would have been ignored. Within the government-controlled Trusted Microelectronics Program, adequate resources could be justified to address these important issues.

With trusted rad-hard microelectronics as an extension to the Trusted Microelectronics Program, one can envision achieving an assured trusted rad-hard microelectronics supply chain in the future.

Future of Military Microelectronics

Security expert Richard A. Clarke in his book *Cyber War* (May 2010) defines “cyberwarfare” as “actions by a nation-state to penetrate another nation’s computer or networks for the purposes of causing damage or disruption.” William J. Lynn, U.S. Deputy Secretary of Defense, states that “as a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain in warfare...” In May 2010 the Pentagon set up its new U.S. Cyber Command (USCYBERCOM), headed by General Keith B. Alexander, director of the National Security Agency (NSA).

At the center of cyberwarfare are computers and networks that consist of “software,” a collection of computer program and data that tell a computer what to do, and “hardware,” the microelectronics that execute software. Defense against attack and hacking on software is difficult because of the dynamics and complexity of software operations. However, efforts are ongoing and progress is being made. On the other hand, defense against attack on hardware, that is, acquiring trusted high-performance microelectronics, has largely been at a standstill. The core issue is that more and more high-performance microelectronic devices are designed and manufactured overseas in an uncontrolled, untrustworthy, and in some cases, explicitly adversary-controlled environment. This trend continues to accelerate, driven by the world economy, and cannot be reversed.

For two decades, the US was unable to establish an effective policy to secure trusted microelectronics for military applications. This is because prevailing wisdom dictates that it is necessary to use microelectronics fabricated in a state-of-the-art technology for highest performance. The premise is that the US government needs continuous access to state-of-the-art foundries in order to maintain US military system superiority. Study revealed that this prevailing wisdom is not necessarily true. It is possible to fabricate highest performance military microelectronics using only 90-nm technology. In fact, a foundry with 90-nm and 0.35- μm capabilities could fabricate the full spectrum of microelectronics that is needed for military systems.

This paper proposes a new trusted microelectronics supply chain policy through a government-controlled Trusted Microelectronics Program. It would consist of a foundry with 90-nm and 0.35- μm fabrication capabilities, a silicon technology research and development team, and a robust microelectronics component design and development effort, in which current microelectronic contractors could play a major role. The study showed that this approach is technically and economically favorable compared to chasing Moore’s Law on feature-sizes, thus eliminates the need to further investment in later technologies for the foreseeable future. Trusted microelectronic devices specially designed for military application is necessary for the US to maintain future military technology leadership. As such, we recommend that the US Government make a long-term commitment dedicated for military microelectronics. To quote the Defense Science Board (DSB) High Performance Microchip Supply (HPMC) report, “Addressing this (trusted microelectronics supplier) problem is a uniquely governmental function.”

Distribution

1	MS0352	Dahlon Chu, 05330
1	MS0359	Ann Campbell, 01950
1	MS0457	Carolyn Hart, 02000
1	MS0509	Mike Knoll, 05300
1	MS0620	Fred Sexton, 05622
1	MS0868	Thomas Zipperian, 02700
1	MS1069	Marion Scott, 02300
5	MS1072	K. K. Ma, 01752
1	MS1072	Rita Gonzales, 01750
1	MS1077	David Sandison, 01740
1	MS1079	Gilbert Herrera, 01700
1	MS1083	Paul Dodd, 01752
1	MS1205	Jim Gosler, 00002
1	MS1319	Erik Debenedictis
1	MS0899	RIM-Reports Management, 9532 (electronic copy)