# A Secure System and Method for Manufacturing Leading-Edge Semiconductors

**John Ellis**
**VP, Global Standards and Technology**
**SEMI**
**November 2, 2009**

## Problem Statement

In the past two decades, both the access and ability of the Department of Defense, Department of Energy and their associated agencies to access advanced technology for research, development, and production of advanced semiconductors at reasonable timeliness and costs has been greatly curtailed. Additionally, the drive towards cost reduction throughout the semiconductor industry has shifted significant manufacturing toward Asia, where the United States has clear political adversaries. Even allies in the Pacific Rim may shift alliances in the future as geopolitical and economic strength of various nations develop over time. The combination of these has led to a condition where the U.S. is more and more dependent on foreign manufacturing from potentially unsecure sources. The irony of the situation is that the U.S. still leads the globe in the development of advanced semiconductor technology.

## Strategic Problem

Strategically, the current situation, if left uncorrected, will lead to an inability to not only produce advanced technology for the U.S. military, but potentially will erode our ability to develop secure and uniquely targeted solutions to key military problems. We are already seeing this situation potentially develop. The current Cray Research contract with DARPA to develop their next generation processor is one example. If, according to plans, the advanced process is produced at Taiwan Semiconductor Manufacturing Company (TSMC), there is at least some likelihood that a part of the design will be leaked out. The warming relationship between Taiwan and China, while potentially adding to the stability of the region, is also a potentially source of information. The attitudes of China and Taiwan towards protection of intellectual property are a serious issue for businesses, let alone governments.

With IBM as the main foundry providing advanced technology for the US Government, there are concerns about having a second source available for advanced ICs. The conflict between IBM and Cray, as competitors, although unique, partially led to the plan to use TSMC as a foundry. Potentially, with the entry of the GLOBALFOUNDRIES, as a spin-off of Advanced Micro Devices, a second source, leading edge, US-based foundry is in the works. However, the business environment is currently one that provides no guarantees that either of these leading edge companies' technologies will be available, in a secure manner, in the future.

In the recent press (EE Times, February 2, 2009), we see that with IBM's recent layoffs and losses in semiconductor, that there is speculation that IBM might even spin-off their

chip unit, possibly to Samsung Electronics. Even if it doesn't spin-off the business, there is a real possibility that IBM will have to delay investment in their fab. With regard to GLOBALFOUNDRIES, the investment from the government of Abu Dhabi certainly causes concern with regards to control of the company. Abu Dhabi's Advanced Technology Investment Company (ATIC) will control nearly sixty-six percent of GLOBALFOUNDRIES.

A clear path forward towards security of the semiconductor supply chain for DoD applications is not apparent. The current economic downturn could certainly exacerbate the issue as companies struggle to survive and are faced with global investments, partnerships, and mergers that will certainly not be based on the needs of the US Government. So, in this uncertain environment, what can be done to secure a protected source of advanced technology for DoD applications?

**Economic Problem**

The profits in the semiconductor industry have been driven through increased performance, cost reduction, and high volumes. While there is a high mix of products in the market, the most advanced technologies are being used in the production of memories and logic aimed at the consumer market. The need for advanced, costly equipment in driving down the path of "Moore's Law" has caused a virtual explosion in the capital required to build a leading edge fab. Fabs on the order of 60k wafer starts per month are typical with some fabs being built to handle up to 150k wafer starts per month (on 300mm wafers). The cost of these fabs easily can run over $5B US.

The high throughput and commensurate cost of the semiconductor processing equipment, with some tools able to process up to 150 wafers per hour (wph), has virtually eliminated the possibility of a cost-effective means to build a low-cost fab producing leading-edge technology. In fact, cost projections of lithography equipment (using Extreme Ultra-Violet Lithography) required to produce 16nm technology will be on the order of $75M US, with a projected tool throughput of 60 wph. If the next wafer size transition occurs, equivalent lithography tools for 450mm wafers will be on the order of $100M US. With the need for potentially only hundreds of the most advanced, yet secure chips by DoD and DOE, the cost per wafer and cost per chip are extraordinarily high. A recent study by International SEMATECH Manufacturing Initiative estimated that the processed cost for a single-wafer per day, 300mm wafer fab would be on the order of $250K US for each wafer. In addition, the lithography mask costs alone would run in the millions of dollars.

Clearly, the only clear alternative under this scenario is to partner with a leading edge foundry. However, even this would not minimize the mask (reticle) costs for lithography. As stated earlier, the leading-edge foundry options in the US may have a tenuous future. Another alternative may be to approach other leading-edge integrated device manufacturers, such as Intel or Texas Instruments. However, these options have their own set of issues, including, but not limited to: access to production facilities for custom parts, accessibility, security, and business priority.

**Technical Problem**

In some aspects, the technical and economic constraints go hand-in-hand. In order to continue along the cost reduction path set by "Moore's Law", greater investments in R&D have been required. Likewise, to justify these investments, high demand and growth have been required, which means a constant reduction in end-unit pricing to continue the pervasive use of semiconductors as they penetrate the end-markets. In fact, whereas the early adopters of higher cost, semiconductor devices were government, and as prices reduced, significant use by corporations; the cost point has become so low, that the major market for devices and systems is now the consumer market. In some market segments, namely DRAM and Flash memory, the pricing has dropped faster than the ability to reduce the cost of the chips, causing serious instability in the markets.

The technical issues, therefore, end up being issues primary driven by the economics. The lower cost solutions to low-volume, leading edge capability are somewhat juxtaposed to the needs of high-volume. For example, the drive to larger and larger wafer sizes, which have provided some measure of cost reduction (the exact amount being debatable), have forced semiconductor suppliers to discontinue continued technology development on the smaller wafer sizes. The commensurate increase in cost of the new equipment further drives the need for higher volumes and cost reduction. Therefore, the most advanced technologies are now only available on tools designed for high volume manufacturing.

As the markets have become more diversified into the various tastes of the end users – namely consumers – the industry has embarked on initiatives internally and industry-wide to try to create more agile, flexible manufacturing for lower volume products. These have had mixed success. For a true, small volume company, the current mode of reconciling these two different models has primarily been to give up the captive fab and move to the fabless / foundry model. The difficulty here is that the expense of the tools and the need for volume production still permeates this model, leading to a few, very large foundries with high overall volume dominating the market. In fact, TSMC now controls approximately 49% of the overall market, and has most of the leading edge foundry capacity.

For the majority of the fabless community, the foundry model works well. Companies such as Xilinx and Qualcomm have used this model to their advantage – creating access to advanced technology while minimizing their own capital expense and risk. However, for other users, such as government, where security is paramount, this model has inherent risks. As leading-edge foundry capability either completely migrates overseas and has survival risks on the horizon in the US, a need for solution is clear. Ideally, a technical and economic solution to this problem would be one that provided a low-volume, secure, and captive capability at low cost.

A final issue, which may or may not be obvious, is that the drive to deliver consumer-oriented products has forced some companies to push the limits of the state-of-the art to such an extent that the products themselves may not be suitable for other more robust

applications. For example, in discussions with Infineon who is an active supplier for the automotive and medical markets, end-users are not aware of the limitations of using less-expensive parts from lower-cost competitors. In the push to achieve lower cost as a selling point, many devices cannot handle the environmental and failure rate requirements needed for high consequence markets. Unfortunately, many leading edge foundries pushing for the lowest cost solutions in the cost-competitive consumer market may also put high consequence applications using similar parts or processing at risk as well.

**Disruptive technologies**

For those familiar with Clayton Christensen's work on disruptive technologies, you are no doubt aware of the conditions that make an industry segment ripe for a disruptive technology.

> "A disruptive innovation is a technologically simple innovation in the form of a product, service, or business model that takes root in a tier of the market that is unattractive to the established leaders in an industry. Very often this occurs at the low end of a market. One condition is that the existing technology has to be more than good enough for what customers in the least demanding part of the market need. Second, you've got to be able to profitably provide the product or service at a low price point, from a business model that isn't attractive to established companies.[1]"

Examples include steel mini-mills, online trading, and home copies, to name just a few. In our case, low volume, leading-edge semiconductor manufacturing, with the added constraints of security is unattractive for device manufacturers. There is little money to be made. Additionally, the price point for developing one's own (government) capability is so high that this option has been deemed untenable.

**Drivers**

In looking at the drivers that led us to the current situation, there are some key questions to ask in looking for a technical and economic solution:

- What are the contributors to the cost of the leading-edge tools?
  - Technology
  - High-volume design
  - Wafer size
- Besides the tool cost, what are the other major cost components of a device?
  - Design
  - Mask Sets
  - Packaging
- What are the biggest issues with regards to security in chips?

[1] Nancy J. Lyons, Interview with Clayton Christensen, Inc magazine, February 01, 2002

- Loss of Intellectual Property
- Use of design information to develop countermeasures
- Injection of Trojans into delivered product
- Low quality

In trying to develop a solution, there are a few areas to explore.

**Approach**

Based on the contributors to the cost and security issues, this white paper proposes an investigation into a low cost, low volume, and secure solution for government applications. The potential system would also have application for low-volume prototyping at small and large semiconductor manufacturers and universities.

A key driver behind the cost of the current toolsets for leading edge manufacturing has been the need for high-volume. This has been the push towards larger wafer sizes and higher throughput. Mask sets for leading edge lithography are also a key driver, particularly when amortized over a small lot of chips.

> "Some believe a leading-edge 65nm "mask-set" could run about $1 million. A leading-edge, 45nm "mask-set" is $2-to-$2.2 million in the initial stages. And some estimate a 32nm "mask-set" could start at $4 million, putting this technology out of reach for most chip makers.[2]"

So, it is reasonable to ask, "what if a system was truly targeted at slow-speed (low-volume)?" Could smaller wafers with lower-throughput technologies be used? As an extreme, what if only one, smaller-sized processed wafer per day was used as a requirement, delivering potentially only 50 or fewer die per wafer?

Many constraints imposed on the factory are primarily there to ensure high-performance and high-throughput. These requirements also drive designers to use only technologies that will accommodate very high volume applications, helping minimize overall cost of ownership. For example, the sheer speed and overall area at which planarization, doping, and anneal need to take place force use of technologies such as chemical mechanical planarization (CMP), ion implant, and rapid thermal annealing (RTA). Under slower processing conditions, other technologies and material handling could be considered which are lower in cost and less complicated. Likewise, the need and method for cleaning deposition chambers might likely be changed when going from processing hundreds of wafers per hour to processing one per day. It would be the intention of a study or a workshop to explore what alternative, lower cost technologies might be brought to bear on semiconductor processing under these conditions.

Likewise, with small wafer size and low volume processing, it certainly may be possible to envision a design where the wafer stays completely within the processing system – either through bringing the processing chamber and tool to the wafer, or moving the

[2] Mark LePedus, *Toppan rolls 32-nm masks, but can industry afford it?*, EETimes, June 13, 2008

wafer between smaller, compact chambers and tools. Any work would leverage off current DARPA programs. For example, DARPA's Nanowriter program would be targeted to one of the key economic drivers, namely mask costs.

**Standard processing**

Some of the cost of leading-edge manufacturing comes through the development of unique, proprietary process technologies designed to ensure the leading companies stay in the lead. However, we know that standardization of equipment, materials, and processes lead to lower-cost manufacturing. For developing leading-edge ASICs, many processes could be optimized to deliver very good performance, acceptable to the designer, at lower-cost. The intent of a study would be to determine a means to deliver more than adequate, leading-edge solutions rather than accommodate all possible solutions.

Likewise, in the area of packaging, using a standard package(s) for prototyping would be an advantage. By targeting standards assembly, packaging and testing, it may very well be that a system for developing complete prototypes could be used in-house without the design, die, or package ever leaving a secure venue.

**Benefits**

Some of the benefits of a small, low-volume production system, if feasible, are clear. A somewhat self-contained system, allowing secure development and small-lot manufacturing of specialized integrated circuits would be of significant value. It would be the intention of any study to determine the overall cost of ownership of such a proposed system and analyze the risks and benefits of all alternatives.

**Spillover Benefits**

Assuming a system is feasible and would make economic sense for various agencies within the DoD and DOE, it is envisioned that over time such a capability would continue to be improved to the extent that universities and industry would consider the use of such as system, not only for experimental and prototype devices, but potentially for production. Likewise, the ability of the government to fund novel concepts and experiments at universities, with on-site processing and delivery of devices, could significantly improve the hands-on education within the US.

***Update as of November, 2009***

The semiconductor industry does appear to be recovering from the disastrous downturn we've experience the past two years. However, the supplier community has yet to see the fruits of the recovery in any substantial way. It will likely be at least 2011 until chipmakers see revenue on the order of the peak in 2007.

Whereas in the Winter this year, there were concerns about IBM Microelectronics' ability to upgrade equipment to the next generation technology, IBM is now beginning to place orders for upgrading equipment to 32nm technology.

GLOBALFOUNDRIES is moving forward with its plans to build a new Fab in upstate New York. However, their major investor, ATIC, also purchased Chartered Semiconductor, a Singapore-held and located foundry, and is forcing a merger between the two. This bodes well for GLOBALFOUNDRIES as it provides them with an immediate global presence in the foundry business and nearly 150 new customers, however, it will have some implications for security of the supply chain with Chartered's six Fabs all located in Singapore.

The dynamic nature of the semiconductor business combined with the strategic importance it has for the U.S. Defense Department and U.S. National Security continue to underscore the difficult reality we are facing now which will only be exacerbated in the future in regards to access to a secure source of leading-edge manufacturing. Latest developments in the industry only emphasize the need to have a technology solution that independent of the business environment. Given that the need for high-throughput, high-capital-intensity capabilities is driven by high-volume consumer demands, it is a highly risky strategy to couple our strategic needs to this business and technology model. Developing a low-volume, leading-edge capability allows us to decouple business and technology needs, and focus on developing secure, leading-edge solutions.