

Three SoC Application Segments Require Embedded OTP Memory

– Craig Rawlings, Director of Marketing, [Kilopass Technology Inc.](http://www.kilopass.com)

The use of high density one-time programmable (OTP) memory is now gaining considerable interest within the chip design community. The main reason for this renewed interest in OTP is the ability to tightly integrate high density permanent memory with digital logic in vanilla CMOS. The opportunity to tightly integrate OTP with SoC architectures sparks the system architect or designer's imagination in three strong value-added application segments. They are: Security, SoC Configurability, and Manufacturability-Usability.

As the semiconductor industry races for a non-volatile memory technology that is process scalable, high density, low power, and high performance, today's designers are forced to choose from available memory technologies based on specific application requirements. These requirements force trade-offs between such things as volatile versus non-volatile, high-performance versus low-power, etc. Unfortunately, these trade-offs become more severe when there is a standard logic CMOS chip requirement for non-volatile memory (NVM).

This is due to the fact that CMOS Logic NVM technologies are limited to one of three main types: fuse, antifuse, and floating gate. Of these three, the only NVM technology type that is process scalable and high density is the antifuse type (one-time programmable). Since the CMOS antifuse class of OTP memory uses only a single core transistor for the programming element within the bit cell, the memory array is very high density. Conversely, due to data retention issues associated with charge leakage, there is no high density multi-time programmable (MTP) technology that is process scalable on a standard logic CMOS process. At the same time, trade-offs for going to a Flash process include substantially higher wafer costs and degraded system performance.

This NVM backdrop highlights the historical limitations that have prevented new architectural SoC features that require tightly integrated permanent memory on chip. With the invention of the CMOS logic antifuse, designers and architects are now rapidly imagining new uses that bring substantial value to most, if not all, segments of the semiconductor industry. Of course, memory is a requirement for virtually all devices, but non-volatile memory fills specific system requirements that must maintain the state of the memory after power-off.

Security Application Requirements

Many new standards such as HDMI, WiMax, and BlueRay include well defined security schemes. Since software is much more easily modified in a system's volatile memory and, therefore, is inherently vulnerable, these new security standards include hardware security. As with any standard, there is a significant investment in hardware as well as the digital media that may

support it. With these new standards, if the security sub-system is compromised, the standard itself may well be compromised resulting in substantial economic damage.

This has led to the realization that in order to protect standards that include security, the security component to such standards must itself be protected. The weak link which is first attacked is the encryption key and/or ID used in a security scheme. By finding and understanding sensitive security data, the system's security may eventually be understood, bypassed, or otherwise compromised. While highly sophisticated encryption schemes are prevalent, until recently there has been no safe NVM repository in which to store security data such as keys. This has rapidly become the weak link in hardware security standards. Contrary to this weakness, the CMOS logic antifuse provides physical layer security for information stored in hardware (silicon).

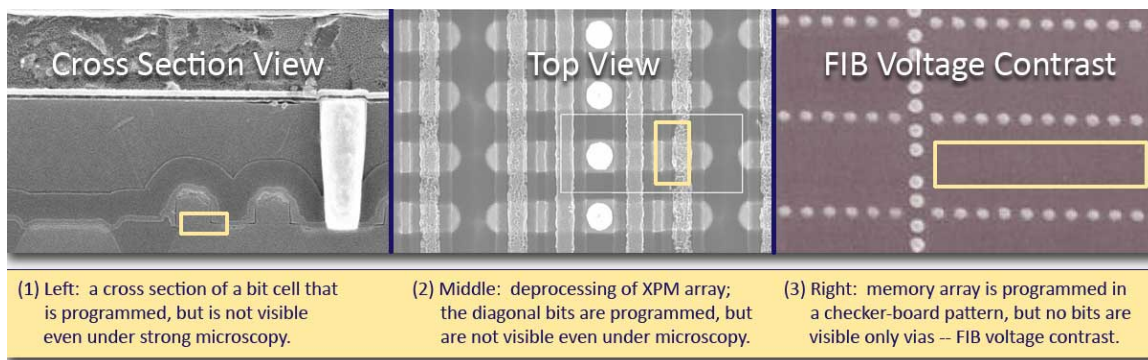


Figure 1. CMOS Logic Antifuse – Physical Layer Security

Credible evidence of the CMOS antifuse's ability to hide information in silicon is illustrated in the three photographs in Figure 1. Additionally, since the OTP memory is on-chip, additional system design measures may be taken to make the device tamper-proof, such as password protecting the OTP memory within the system chip. This newer memory technology provides unprecedented physical layer security needed to protect large investments in standards which heavily rely on data security. Furthermore, a company's investment in intellectual property may be further protected within the SoC.

SoC Configurability

It is a common expression amongst chip designers that, "silicon is unforgiving!" All of us in the business have been stung by the decidedly long design and manufacturing cycle times associated with producing a chip. This expression is further emphasized as the investment to develop a semiconductor device on a state of the art process escalates to tens of millions of dollars.

It is interesting to observe that as the non-recurring expenses (NRE) involved in producing a chip increase, the cost per gate of logic are continuing on their Moore's Law path downward. Thus, the value of being able to provide some level of SoC configurability brings with it the potential for large economic benefits as illustrated in Figure 2 below.

For system designers, SoC configurability may take on many different forms—too many to itemize here. The primary intention of adding configurability is to reduce the number of unique mask sets needed to support a more complex product line or range of similar products. Ultimately, a common platform architecture might be used to reduce R&D costs in a common product segment where features may be segmented or further differentiated in post production. The primary benefits are, of course, reduced engineering risk, time-to-market risk, and inventory risk without significantly increasing the unit cost.

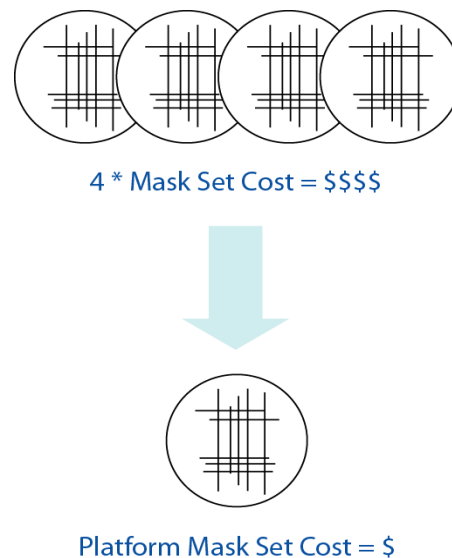


Figure 2. SoC Configurability Leads to Reduced R&D Costs

Common forms of SoC configurability may be achieved through the storage of boot code in a CMOS antifuse OTP memory module. This in-system programmable boot code may be used to pass configuration information to code stored in the less expensive masked ROM. Similarly, system configuration and/or firmware parameters may be stored in OTP, maximally leveraging the on-chip OTP memory. By these means, a common chip may be used to support international markets or multiple market segments with differing standards and requirements. Since the device is not configured until final test and shipment, inventory, obsolescence and other operational risks are minimized.

Manufacturability and Usability

With the possibility of storing system state information at any stage of manufacturing or the product life cycle, new possibilities exist for how chip makers think about hardware. A good example might be how we as people deal with getting older. Inevitably, we adapt. For instance, as our metabolisms slow down, we might (arguably) adapt by eating less. In essence, we are able to adapt with changes in our body to the degree that we have permanent memory. Similarly, the ability to adapt to system changes over a product's life cycle requires non-volatile memory. By tightly integrating OTP in the SoC, designers and architects may provide their customers with highly differentiated product advantages.

A list of several possible applications for enhancing manufacturability and product usability are as follows:

- Memory repair for increasing yield on larger memories
- Pixel repair for imaging applications to improve quality and yield
- ROM patch capability for field updating of firmware—correcting firmware errors in-system
- Digital trim and calibration of analog circuits in order to improve precision, performance, quality, and yield
- Triple module redundancy and other forms of self-healing applications in mission critical applications that require high availability
- System auto-calibration for sensors and imaging applications in order to assure consistent color and performance throughout the product's life cycle
- Intelligent customer product adaptation in order to automatically adapt a product feature to changing use preferences over time

Innovation and creativity will continue to expand additional applications in this segment as systems increase in complexity. The ability to permanently maintain state information within the SoC device itself will simplify SoC interfaces and usability accruing significant product advantages over competing technologies without this capability.

Summary

As the inventor of the CMOS logic antifuse for embedded non-volatile memory applications, it has been exciting to experience the various new types of use models for this more recent class of standard logic CMOS IP. This is made possible by continuing to invest in qualifying Kilopass' CMOS antifuse technology called XPM (X-tra Permanent Memory) at multiple foundries and on numerous process geometries and sub-nodes. Through this investment in qualifying down to 65nm this year, Kilopass customers, already in high volume production, continue to have assurances that this important technology will be reliable and will have negligible impact to yield. These results have been verified with over 15 million devices using XPM technology to date.

For more information about these exciting applications for on-chip OTP and more information regarding Kilopass' XPM memory technology, please visit us at www.kilopass.com or send us an email at klptinfo@kilopass.com.