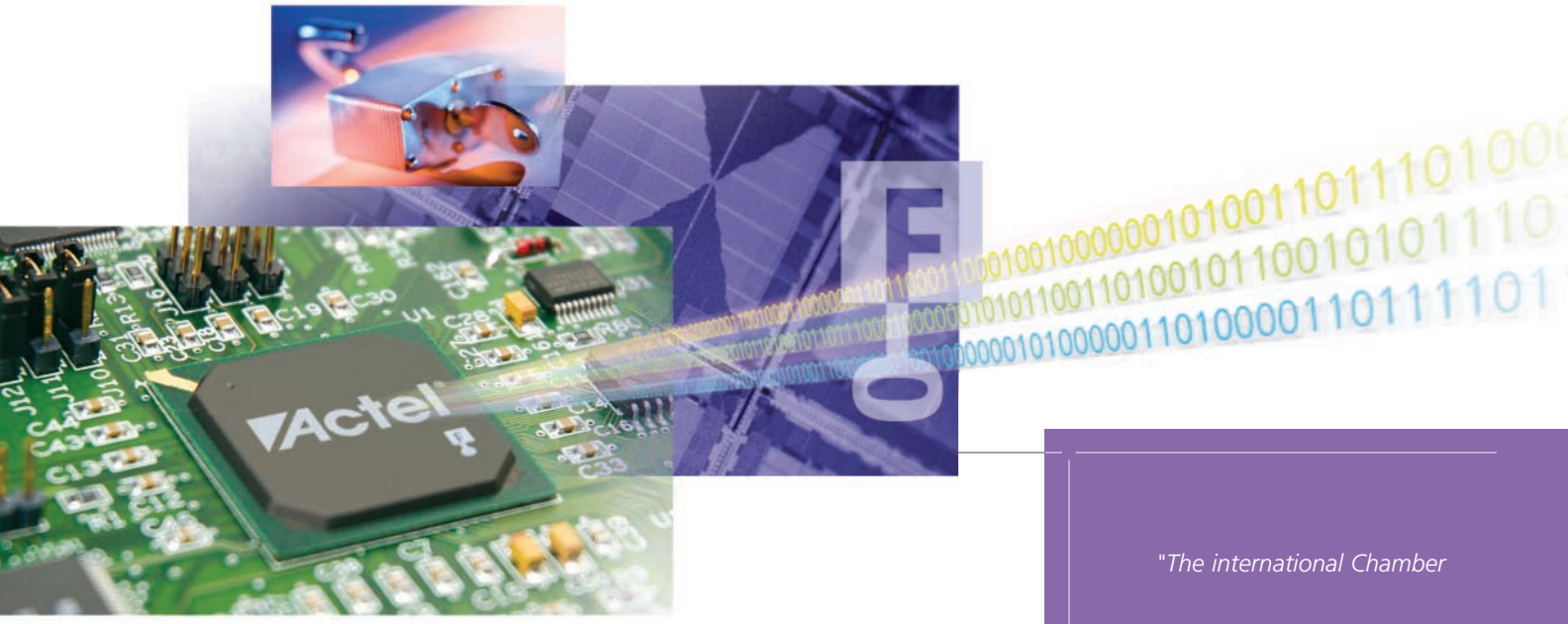
The Importance of Design Security

PROTECTING YOUR INVESTMENT



Inadequate design security is emerging as one of the single largest threats to the intellectual-property-based economies of the modern world. Consequences of inadequate design security can include lost revenue due to counterfeit products and increased liability due to product tampering. Inadequate security is caused by the failure of companies to implement basic security policies and utilize currently available technology. One simple way to improve overall design security is to select nonvolatile, secure FPGAs with FuseLock™ and FlashLock™ technology from Actel.

"The international Chamber of Commerce estimates that seven percent of the world trade is in counterfeit goods and that the counterfeit market is worth $350 billion."

— The International Anti-Counterfeiting Coalition

Product tampering and reverse engineering are virtually impossible with Flash and antifuse-based FPGAs.

Intellectual Property Theft

Intellectual property (IP) theft can take many forms, from the theft of trade secrets to the practice of overbuilding. IP theft through reverse engineering of a product or design is well documented, and such theft can cost a company millions in lost sales and profits when the pirated IP is used to produce competing products. More serious, the IP pirate can use the stolen design to build counterfeit products virtually identical to the original in all aspects, with warranty, support, and product liabilities shifting back to the company victimized in the first place.

As companies have moved manufacturing offshore, the risk of overbuilding has increased dramatically. Overbuilding is a practice done by unscrupulous subcontractors, who build more product than is ordered and sell the unauthorized surplus on the open market. This practice not only costs an OEM lost revenue for the units sold, but can also cause a significant erosion in overall profit margins.

SRAM FPGAs present a unique opportunity for IP pirates. Through a process referred to as cloning, a pirate can copy a board design, capture the configuration bitstream of the SRAM FPGA, and then build an exact copy of the system without having to understand any of the details about the logic contained in the FPGA.

The Myth of Patent Protection

Many companies mistakenly believe that patenting a design is an effective protection against design theft. While a patent certainly discourages reputable companies from even attempting to reverse engineer a product, it does little to discourage design piracy. IP pirates have little regard for the law or courts, and in fact, usually operate in countries with weak or nonexistent IP protection. Even if the pirate can be prosecuted in a country that respects IP rights, such a proceeding can be both lengthy and costly. Assuming that the pirating entity can be identified, it may not have enough assets to even warrant such an action. Winning a $10 million judgment against a bankrupt enterprise is little more than a moral victory. Patents represent only a marginal means of financial remedy, years after the fact, and not an effective design protection methodology. Using patent protection in addition to physical design protection is a good way to provide additional product security and especially brand protection.

Product Tampering

Although many companies may be aware of the threat from IP piracy, there are other far-reaching consequences when design security is insufficient. With the advent of programmable silicon products in the electronics marketplace, after-market tampering is becoming a growing area of concern. Such tampering could lead to either regulatory or product liability on the part of the manufacturer, and could possibly impact public safety. Implementing effective design security is a means of mitigating if not eliminating this risk.

Product reconfigurability extends beyond firmware to include the hardware itself, specifically programmable logic. Unfortunately, this flexibility does present a new problem: users can now override an OEM's factory settings, potentially causing the product to react in dangerous or harmful ways. In our litigious society, if a consumer is then injured, it could result in a product liability lawsuit.

This type of product tampering has other implications. For example, modified engine settings on a vehicle to gain more horsepower could result in shortened engine life and open the car manufacturer to warranty liabilities. This tampering could also go undetected, as the consumer could restore the factory settings prior to filing a claim. Malicious hackers could also modify the functionality of other key service and infrastructure equipment, potentially endangering the lives of users.

Implementing Design Security

There are two paths to implementing design security: alternate design techniques and the selection of a secure base technology. The first of these two paths, choosing alternate design techniques, is a way to prevent simple attempts at product tampering. By migrating processor-based designs to state-machine logic implemented in programmable logic, designers can not only retain product programmability and flexibility, but also reduce the system's susceptibility to tampering via firmware stored in Flash memory.

The second path to design security is the selection of a secure base technology. Actel Flash-based FPGAs offer the flexibility and reprogrammability of SRAM-based FPGAs without the inherent security risks of a downloaded bitstream. Being singe-chip, nonvolatile devices, Flash-based FPGAs do not require a programming bitstream at every power-cycle. Once programmed, Flash-based FPGAs retain their configuration until reprogrammed.

The configuration of Actel Flash FPGAs, with FlashLock technology, is protected by an on-chip security key between 79 and 263 bits. FlashLock even offers customers the option of permanently locking the device, rendering all device read back impossible.

Some Flash FPGAs offer the option of an encrypted configuration bitstream using a 128-bit AES cipher. This encrypted bitstream is then deciphered by an on-chip engine, providing the industry's highest level of security for upgradeable systems.

For even higher levels of security, Actel offers antifuse-based FPGAs with FuseLock. Since no bitstream is ever downloaded to the device, antifuse FPGAs cannot be cloned. Configuration is achieved via a programming routine run on specialized Actel hardware.

Both technologies, Flash and antifuse, make reverse engineering and product tampering virtually impossible. Moreover, as programming can be accomplished in a secure environment, access to the programming files can be controlled, thereby preventing overbuilding by unethical subcontractors.

SRAM FPGAs are especially vulnerable to IP theft and product tampering. Since a program bitstream must be read into the device at start-up, it is a simple matter to intercept this bitstream and clone the design or modify it to change the functionality of a product.

FuseLock and FlashLock offer the only secure manufacturing solutions in the industry.

Conclusion

Poor design security can expose companies not only to the theft of intellectual property and the resulting loss of revenue, but also to brand defamation, liability, and risk of product tampering. Designers can combat these risks by implementing alternate design techniques. More effectively, designers can eliminate and reduce risks by starting with a secure base technology. Of all the technologies available, only two—Flash and antifuse—form the basis for secure FPGAs. Actel is the only supplier offering both Flash and antifuse FPGAs, making Actel the leading supplier of secure programmable logic.

For more information on design security refer to the Actel Security Resource Center at **http://www.actel.com/products/rescenter/security/index.html**.

Organizations concerned with security can now access detailed information and links about security, security countermeasures, affected systems, and solutions to defeat unfriendly attacks.

For more information regarding **Design Security**, please contact your local **Actel** sales representative.

Actel®
www.actel.com

Actel Corporation
2061 Stierlin Court
Mountain View, CA
94043-4655 USA
Phone 650.318.4200
Fax 650.318.4600

Actel Europe Ltd.
Dunlop House, Riverside Way
Camberley, Surrey GU15 3YL
United Kingdom
Phone +44 (0) 1276 401 450
Fax +44 (0) 1276 401 490

Actel Japan
www.jp.actel.com
EXOS Ebisu Building 4F
1-24-14 Ebisu Shibuya-ku
Tokyo 150, Japan
Phone +81.03.3445.7671
Fax +81.03.3445.7668

Actel Hong Kong
www.actel.com.cn
Suite 2114, Two Pacific Place
88 Queensway, Admiralty
Hong Kong
Phone +852 2185 6460
Fax +852 2185 6488