

Syndicated®

News, tips, and notes for improving the Quality of Results in FPGA and ASIC design

Design Security in FPGAs

by Jon Ewald, Director, Product Marketing, Actel, Corp.

With the increase in density, features, and performance, FPGAs have found their way into the heart of today's electronic systems. What was once the ASIC domain now belongs to the FPGAs. Most, if not all of the components in today's systems designs can be purchased as standard products. The FPGA is what differentiates the system and contains your company's valuable IP.

Choosing an FPGA with inherent design security can help to guarantee the integrity of your system and protect your valuable IP. Antifuse and Flash based FPGAs offer the best security against design theft. Since these technologies are non-volatile there is no configuration data stream that can be easily captured and copied.

The biggest concerns in design theft are cloning, reverse engineering, and over building. Cloning is when a design is copied without making any modifications. In the case of an SRAM FPGA, the configuration stream can easily be captured and cloned without understanding how the design works. Reverse engineering is when a design is copied and then modified to either improve upon it or to alter it to prevent legal action for copy write infringement.

Overbuilding is a less known issue but potentially one of the most severe. Unscrupulous contract manufacturers have been known to over build a production run and sell the overage on the open market cutting into your revenue. To prevent this you need to control the IP that is in the FPGA. By utilizing secure, non-volatile FPGAs you can direct ship these key components to the CM. With an SRAM based FPGA the boot PROM can easily be cloned and your product over built.

The following ten steps can help you to guard your intellectual property:

1. Don't be complacent. Where needed utilize the most secure programmable logic technology available to minimize potential attacks at the physical level. Nonvolatile FPGAs offer the most secure solution.
2. If your design uses dedicated inputs and outputs, make sure that you have guarded against simple I/O scan attacks. Such attacks attempt to reverse engineer a design by cycling through a large number of possible inputs and then monitoring the outputs to determine the internal logic functions.
3. Employ procedures to implement and track IP and programming changes to limit exposure of your designs in the manufacturing channel. Limit third party access to critical design information whenever possible.
4. Consider adding digital "watermarks"/"fingerprints" to your design. These are unique features or attributes of the design that can later be used to prove that a design claimed to be "independently" developed is really a copy.
5. If outsourcing production, take steps to ensure that additional units are not produced without your knowledge. Overbuilding is among the most common forms of design theft.
6. Use trusted silicon vendors such as Actel to implement the design. An Actel device programmed in a secure environment protects customers' proprietary IP.

"Design Security" continued from page 1

Steps management can take to guard its intellectual property:

7. Establish a security policy that defines corporate security goals, this is a critical first step. Make sure that all employees understand the need for security and the company's commitment to vigorously defend its intellectual property rights. Make security part of your corporate quality goals.
8. Take steps at the designer level to ensure designs do not leave with an employee but remain company property.
9. With the rise of broadband connectivity, more design work can now be done remotely. If employees are working remotely, ensure all design work is done using a secure centrally accessed server that also serves as a depository for any relevant EDA tools.
10. As a last resort, don't be afraid to use the legal system to pursue those who are infringing on your intellectual property.

For more information, visit the Actel Security Resource Center at <http://www.actel.com/products/security/index.html>. 

