Security Top Ten

Ten Steps a Company Should Take to Guard Their Intellectual Property

The majority of successful attacks on embedded systems and programmable semiconductor components can be traced to the exploitation of a small number of security flaws. Identifying these points of vulnerability and correcting the security flaws is critical to prevent the compromise of an entire system. Often these vulnerabilities are well known, and attackers only focus on the best means for accessing proprietary data, as most organizations do little to address the problem. IP theft loves complacency. The embedded system security community is meeting this problem head on by identifying the most critical design security problems. This consensus list represents an example of cooperation between designers and suppliers from security conscious organizations.

Secured by Actel

Steps Designers Can Take to Guard Their Intellectual Property

1 Don't be complacent. Utilize the most secure programmable logic technology available to minimize potential attacks at the physical level. Of all commercially available technologies, volatile SRAM-based FPGA technologies are the least secure. 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 by a competitor 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.

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 regarding the protection of intellectual property, please contact your local Actel sales representative or go to http://www.actel.com/products/security/

Actel
www.actel.com

Actel Corporation
955 East Arques Avenue
Sunnyvale, CA USA 94086
Telephone 408.739.1010
Facsimile 408.739.1540

Actel Europe Ltd.
Maxfli Court, Riverside Way
Camberley, Surrey GU15 3YL
United Kingdom
Telephone +44 0 1276.401450
Facsimile +44 0 1276.401490

Actel Japan
EXOS Ebisu Building 4F
1-24-14 Ebisu Shibuya-ku
Tokyo 150, Japan
Telephone +81 0 3.3445.7671
Facsimile +81 0 3.3445.7668