

Design Security in SRAM-based FPGAs

Jason Moore
Xilinx

ABSTRACT

In the past, the level of security surrounding programmable logic devices was not considered important due to the low-level “glue-logic” type functions that the PLD performed. However, as the complexity of programmable logic continues to increase, and as the devices approach “system-on-a-chip” levels of integration, the security of the functions within the device can be critical.

Design Security has a broad definition. At one end of the spectrum is commercial companies trying to protect their IP and their business well being. At the other end of the spectrum are government applications that require certification and physical separation of redundant functions. This paper will discuss design security features, such as the ability to encrypt the configuration bitstream, the string of 1s and 0s that define the operation of the device, which can be employed to address a wide range of security requirements.