Recent Advances in FPGA Design Security Reduce Insider Threats

G. Richard Newell
SoC Products Group, Microsemi Corporation

Abstract

Recent and announced advances in FPGA security architectures show the promise of reducing insider threats at several stages of the supply chain. These include threats from insiders at the device manufacturer, overbuilding devices or selling "floor sweepings" (failed parts); through distribution, where parts may be re-marked with more expensive model numbers and sold to unsuspecting systems houses; to the end-user's manufacturing plant where there may be insiders overbuilding at the system-level or installing malicious code in place of the user's own design.

From random bit generators to PUFs and elliptic curve cryptography, this talk will show how all the pieces fit together in a modern FPGA designed with enhanced security features to thwart the insider threat.