

# Integrated Circuit Security in Military and Commercial Systems

John McCollum

Actel Corporation, 955 East Arques Ave., Sunnyvale CA

In recent years commercial users of FPGA's have become interested security to minimize the ease of copying their designs by competitors. In the military arena the two Gulf Wars and the Afghanistan conflict demonstrated the value of smart weapons in the modern military. It also demonstrated that such weapons often fall into enemy hands as in the case of the cruise missiles shot down by Iraq, the loss of the F117A in Serbia, as well as the landing of a Reconnaissance P3 in China. The electronics in these systems are probably being copied as we speak. The enemy could use the information he gleans from reverse engineering these systems to generate counter measures as well. Iraq most recently purchased and used GPS jammers from Russia in an attempt to defeat JDAMS. It would thus be useful if it were difficult to copy modern weapons systems as well.

## Security levels I ,II, III

Reverse engineering someone's integrated circuit can be rated as three different levels of attack as proposed by an article in the IBM Systems Journal.

**Level I:** A somewhat knowledgeable individual with cheap tools. These people are usually interested in end user products such as phone cards, debit cards and set top boxes.

**Level II:** A highly knowledgeable individual (often someone with inside knowledge) with access to expensive lab equipment, probably a commercial enterprise which might be a game copier.

**Level III:** A government backed lab with unlimited resources such as the NSA.

This paper will present examples of how parts have been reverse engineered and relate those examples to the above levels. Additionally the commonly available FPGA's will be examined as to how they fit into these groups and methods that could be used to attack them. From this presentation a designer will be able to determine what type of device best suits his security needs.