Security vs. Test Quality:  
Fully Embedded Test Approaches Are the Key to Having Both

Stephen Pateras  
LogicVision  
pateras@logicvision.com

There is a growing acceptance in the industry that with 0.13um processes and beyond, at-speed structural testing is the only viable methodology for achieving acceptable quality levels with acceptable yields. Fully embedded at-speed structural test approaches have been growing in use over the past several years. For embedded memories, fully embedded test approaches are now widespread in use. For random logic testing, three approaches are currently in use. The full scan ATPG methodology provides a fully external test approach. The more recent ATPG compression based methodologies represent a hybrid approach consisting of some internal IP as well as reduced external scan test data. Finally the logic BIST methodology represents a fully embedded test approach requiring no external test data.

There is growing evidence that fully embedded test approaches for logic can provide increased product quality (lower DPM levels) while maintaining or lowering manufacturing test costs over existing external or even hybrid approaches. In addition to these benefits, embedded test has the unique advantage of being fully portable and reusable. Most designs today are designed hierarchically, with cores often being designed by different teams or even acquired from 3rd party providers. With an embedded test approach, a block or core can be made fully self-testable, with a standard interface (e.g. IEEE P1500) for accessing the embedded test capabilities. This not only provides test cost savings when the core is reused either within the design or across different designs, but also provides two distinct security benefits. The first of these benefits is IP protection. Because the core does not need to be processed for test insertion, it is possible to deliver the core as a black box. In additional since all test pattern data and results are generated and analyzed on chip, there is no need to provide any stimulus or expect test data along with the core. This is turn removes any possibility of using this data to reverse engineer the core design.

The other security issue is access to sensitive data stored inside the device once it is active in the field. Any external access to embedded memories or internal functional registers represents such a security risk. With embedded testing approaches, external access to either memories or internal functional registers is not typically required for go/no go production testing. External access is only provided to the embedded test IP for initialization and failure result extraction. Although the failure result extraction process may result in the need to provide some access to internal functional registers, this access can be made dependent on embedded test IP access instructions. These instructions are typically (or can be made to be) 32 to 64 bits long and therefore provide a secure entry point.

In summary, security is simply another factor which can best be addressed by fully embedding test and diagnostic capabilities within the silicon.