Overview of Supply Chain Assurance

of Intelligent ICs

November 2013

Introduction

The counterfeiting of electronic devices has become a real problem in recent years. This fraudulent activity has affected high-value components where the highest profit can be made. Using intelligent ICs, it is possible to minimize or totally alleviate fraud that could arise in the supply chain. Microsemi has developed a cryptographic solution for the problem of supply chain assurance to ensure the highest levels of security and prevention of counterfeiting in IGLOO®2 FPGAs and SmartFusion®2 System-on-Chip (SoC) FPGAs. The mechanisms commonly used for counterfeiting high-value devices include the following:

- Upgrading components
  - Remarking less expensive device variants as more expensive ones
- Reclaiming and reselling used components as new devices
  - No guarantee of reliable operation after removal from a used system
- Over-building by foundry or test suppliers or rogue insiders
  - Possible fraudulent supply of parts that failed test

In military or other secure systems, the burden for counterfeit components was previously on the end user. The cost of replacing, redesigning, or rebuilding equipment to correct the deployment of a counterfeit device would rest on the individual service branch and its budget. With the increase of counterfeit components, the military, in the *National Defense Authorization Act (NDAA) for Fiscal Year 2012, Sec. 818* Detection and Avoidance of Counterfeit Electronic Parts, places the burden of corrective action on the DoD prime contractor.

Two Forms of Solutions to Counterfeiting

Suggested answers to the counterfeiting problem come in two forms:

- Process solutions: Buy only from authorized distributors
  - Reduce risk considerably by buying only from approved suppliers
  - What if the components stocked by an approved channel are counterfeit?
- Technical solutions: Positively identify legitimate devices
  - Requires strong tamper resistance and a ’hard-to-spoof’ technique
  - Only as good as production controls, such as chain-of-custody of ID technology)

Depending on the component being protected, different technical solutions for supply chain assurance are possible. Some identification techniques are easier to forge than others; some may only identify the device as a member of a broad class, not individually. In any case, the critical elements of the ID technology used must be controlled. If they become available to counterfeiters, the identification technique may become nearly worthless. The strongest known techniques can be applied by an intelligent IC that has at least some of the following characteristics:

- Embedded nonvolatile memory
- Sufficient computation power to implement cryptographic algorithms in real-time
- Digital communication interfaces for data interchange
- Built-in hardware-level security

IGLOO2 FPGAs and SmartFusion2 SoC FPGAs from Microsemi are ideal for the creation of a strong anti-counterfeit solution because they possess all the above features. The Microsemi solution has the following features:

- Cryptographic device certificate identifies legitimate devices individually
- Extremely strong, tamper-resistant, and 'hard-to-spoof'
- Protected by FIPS PUB 140-2 Level 3 cryptographic controls being installed in Microsemi facilities

The National Institute of Standards and Technology's FIPS PUB 140 standard specifies controls used to protect very high-value assets, up to and including state secrets. A device identification technology whose security rests on cryptography and these well-proven controls is very strong compared to any other process-based or technical identification technology.

Supply Chain Assurance

Any intelligent electronic component undergoes several stages in its supply chain:

- Design by the original component manufacturer (OCM)
- Wafer fabrication
- Wafer test
- Assembly and binning
- Distribution
- Utilization in an electronic system

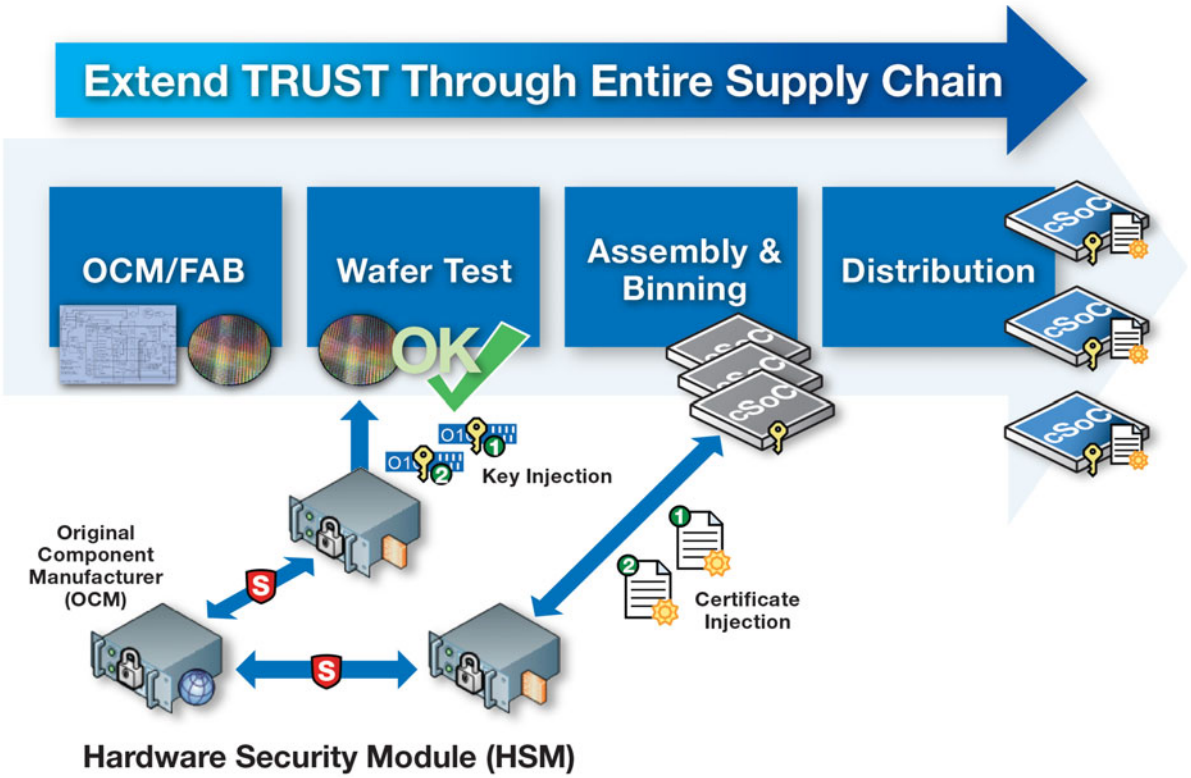

Figure 1: **Supply Chain Assurance**

The design and fabrication of the device by an OCM is the most trusted part of the process. However, wafer test, assembly and binning without strong anti-counterfeiting solutions are less so, and distribution channels, especially those not authorized by the OCM, are fraught with risk. The aim is to build on the trust available in the earlier stages and extend the trust in the first stages of this process further and further down the chain so that ultimately counterfeit devices cannot be injected into the supply chain and end up in an electronic system.

Hardware Security Module

By using external hardware it is possible to authenticate wafers, inject unique cryptographic keys and sign digital certificates that are specific to each individual device. A hardware security module (HSM) is a tamper resistant, tamper evident, security-hardened computer that is used to perform the wafer authentication, key injection, and certificate signing functions at a remote wafer test or assembly location. Although it is located within the potentially less secure remote location, the HSM can be used to securely store and manipulate private keys. If the HSM is tampered with, it will erase any sensitive data it contains—such as cryptographic keys—before it can be extracted. Fear of leaving evidence of tampering is a strong incentive to play by the rules for a contract manufacturer who does not want to lose business over trust issues.

The HSM initially verifies that the device and wafer being tested is the expected one using authentication features designed in at the lowest transistor and interconnect levels. Then and only then does it generate a secret key which is injected into the device. This key is unique to an individual device and prevents upgrading of such components by authenticating only components with the exact parameters specified in the traveler. Using public key methods, all communications between the HSM and the device can be validated and protected by encryption.

Digital Certificate

After a secret key has been injected into the device at the wafer test stage, a digital certificate is injected into the device at the assembly and binning stage. This certificate contains many fields, including the following:

- OCM identifier
- Device serial number
- Model number with grading information
- Assembly date code
- Data binding the certificate with the secret key previously injected

The HSM ensures only good devices receive a certificate, which prevents the representation of failed components as good ones. The HSM securely logs each certificate so the OCM knows exactly how many have been issued. The certificate is injected after test and binning so it contains authenticated device grading information. This facilitates user detection of devices tested to a lower speed or temperature grade than indicated by package-top markings, which could potentially be fraudulent (modified). The date code tells when a device was assembled and, similar to the grading information, can be compared to the part marking to detect fraud. This comparison may assist in electronically identifying older devices that require additional screening to ensure they are new and have not been previously used.

The certificate is signed by the OCM (Microsemi, in this case) using a secret key known only to the OCM, but the key to verify the certificate can be made public. Anyone with the right technology and the OCM's public key can read and verify the device certificate, thus proving with cryptographically high assurance levels that the data fields in the certificate have not been tampered with, and proving the certificate was signed by the OCM. The certificate can be interrogated on various occasions:

- Receipt of the component (incoming inspection)
- Product assembly, programming and test
- Receipt of final system-level product
- After deployment of the final product to the field

As part of a screening process, such as checking the delivered device against the order, IGLOO2 FPGAs and SmartFusion2 SoC FPGAs can be authenticated against the following:

- The certificate's integrity and signature, using the Microsemi public key
- The certificate can be checked for listing on a certificate revocation list (CRL)
- Verifying the device knows the device-unique secret key stored in the device and bound to the certificate
  - This proves that the certificate belongs to that particular device and is not a copy of a certificate belonging to another device.
- The device can also check that any data fed to it matches parameters in its certificate.

Certificate Revocation List

Any certificate can be invalidated by the OCM by adding it to the appropriate certificate revocation list for that device type. The CRL describes certificates which, for any reason, should not be trusted any longer. Following are examples of when the CRL would be updated:

- Inventory retest failure
- Production failure
- Field application obsolescence
- Theft of components
- Detection that a device has been tampered with

Physically Unclonable Function

To provide true device binding, an intrinsic physical property with a high degree of repeatability and individuality can be used. Such a behavior is known as a physically unclonable function (PUF). In an electronic circuit, any internal SRAM memories, when powered up but before being written to, will contain a random collection of 1s and 0s. These are largely due to the nano-scale individual manufacturing differences of each memory cell (plus some noise), and are replicable to a high degree from power-up to power-up (typically more than 80% repeatability over all test conditions). This unique pattern of 1s and 0s, specific to an individual device, can be used to identify that particular device, analogous to the way fingerprints can provide biometric identification of people. Cryptographically binding this "silicon biometric" with the digitally-signed device certificate provides the strongest, most tamper-resistant, and difficult to forge method known today for assuring the pedigree of intelligent devices.

Conclusion

During programming of IGLOO2 FPGAs and SmartFusion2 SoC FPGAs, the configuration bitstream is authenticated against the parameters certified by the device certificate and the unique device secret key. Using this technique provides the best assurance available that the device being programmed is free from supply chain counterfeiting issues:

- Upgrading of components
- Reclaiming and reselling used components as new devices
- Overbuilding by foundry or test suppliers or rogue insiders

The complete IGLOO2 FPGA and SmartFusion2 SoC FPGA anti-counterfeit solution provides the functions and production controls you need for a complete secure supply chain, from design and fabrication to user programming and deployment to field operation.

To Learn More:

Secure Life Cycle

1. Securing Your Embedded System Life Cycle
2. Securing Your Supply Chain Life Cycle

Protecting Your Design IP

1. Protect FPGAs from Power Analysis
2. How Easy is it to Secure Your Designs?
3. What is Design Security in a Mainstream SoC Chalk Talk

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo CA 92656 USA
Within the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996

55900148-1/11.13