Security is the key

Built in crypto functions help to combat the prevalence of counterfeit components.

By **G. Richard Newell**.

The counterfeiting of electronic components continues to rise alarmingly. IHS iSuppli reported that, in the first eight months of 2012, more than 100 incidents of counterfeiting were reported each month. In the past six years, more than 12million parts have been discovered to be fakes.

Counterfeiting is a major risk to everyone in the electronics supply chain, but the cost of dealing with an incident is not shared equally. The US military sector, for example, is now covered by the National Defense Authorization Act for Fiscal Year 2012. Section 818, which deals with the detection and avoidance of counterfeit electronic parts, places the burden of corrective action on the prime contractor to the Department of Defense. In other sectors, the burden rests with the end user. However, subcontractors and suppliers are still vulnerable to the reputational and business relationship risk of falling victim to forgery. The ability to prevent counterfeits from entering your supply chain is clearly critical.

Spotting fake components

Counterfeits are often difficult to spot; they could be parts from the approved supplier which failed production testing and were not destroyed properly or recycled then diverted by criminals into the supply chain. They could also be lower grade components relabelled or repackaged to resemble more expensive extended temperature or endurance devices.

One approach that can be used use to cut the risk of having counterfeit components make it to the pcb is to adopt good business processes in which all parts are only sourced from authorised distributors. Even so, there remains a risk that counterfeit components can still make it into the supply chain through approved channels if legitimate shipments are somehow switched with fakes unknown to the supplier.

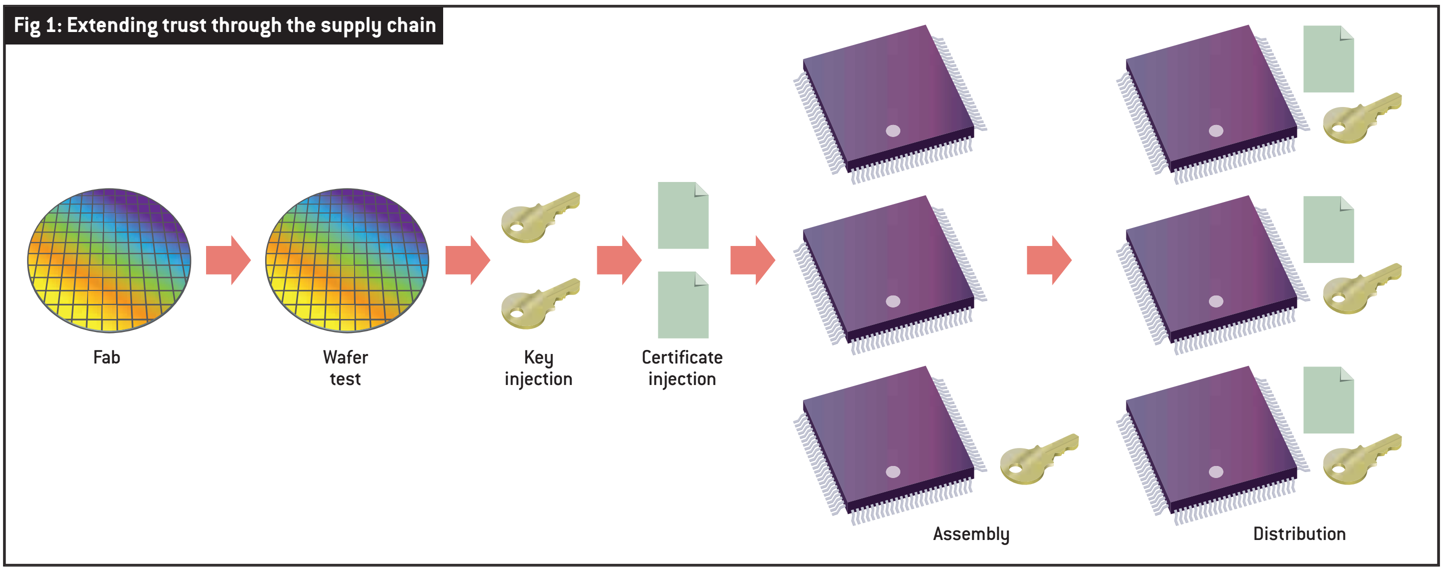
The risk of fake parts entering a high quality supply chain can be reduced dramatically using technical means that take advantage of key characteristics of the semiconductor supply chain. The design and fabrication of the source wafers by an original component manufacturer (OCM) is the most trusted part of the supply chain. The OCM has a high degree of control over device quality through to component level test. The key to counterfeit free components is to extend this trust into the entire supply chain so counterfeits cannot end up in an electronic system. By putting electronic tags and markers into the silicon itself, a device can provide evidence of its authenticity at any point.

Criminals will attempt to reverse engineer the markers used to distinguish fake components from genuine so they can make their devices appear to be authentic. The requirement is for a technical solution this is both tamper resistant and hard to spoof.

Some identification techniques are easier to forge than others. A simple marker, such as a device code accessed through a serial port, may only identify the device as a member of a broad class, not individually. A major problem with a class marker is that if the technique used to embed it within a device becomes available to counterfeiters, the identification technique becomes practically worthless. If individual devices are marked with a public identifier plus a unique private key, the counterfeiter has to determine how the markers are applied and used in order to determine whether a part is genuine or not. Simply reverse engineering and copying the public identifier from a genuine part to a series of fakes will not work, since the associated private keys are much harder to learn and clone.

Physically unclonable functions (PUFs) provide one way to tie a device to its mark of authenticity. Each IC is subtly different to its neighbours on wafer, even though all that make it through test will operate in the same manner.

Fig 1: Extending trust through the supply chain



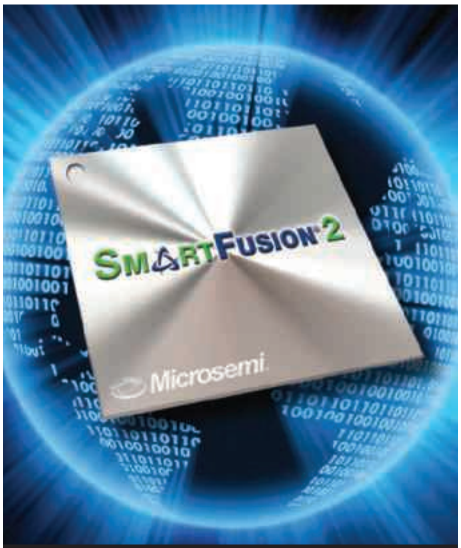
For example, internal srams have subtle biases such that, when they are first powered up, they contain a pattern of 1s and 0s that is essentially random from die to die, but which is consistent from power cycle to power cycle for that die. Repeatability can be as high as 80% under different test conditions. This pattern can be used as an unclonable device 'fingerprint' that, together with a digital certificate stored as part of the manufacturing and test process, guarantees authenticity.

There are a number of requirements for the digital certificate. The first is the presence of embedded non volatile memory to store the data and a communications interface to allow the data to be read. The device needs sufficient computational capability to implement cryptographic functions in real time such that the secret value certified is never exposed. The certification circuitry is used to answer challenges with responses consistent with a public key supplied by the manufacturer to allow testing for authenticity.

Hardware level security on top of these functions ensures criminals cannot probe the device. Microsemi's SmartFusion2 SoC fpgas implement all these functions, making them suitable for a strong technical anti counterfeiting solution.

With the necessary hardware in place, a secret key can be injected into the device at wafer test. This is followed by injection of a digital certificate bound to the secret key at the assembly and binning stage. This process provides a certificate that has been securely signed by the OCM and which supports all downstream anti counterfeiting measures. The certificate, which can be interrogated at any point, provides traceability for suppliers and end users, providing a way of guaranteeing a counterfeit free supply chain downstream.

The public data in the certificate can contain not just a unique device number, but also a model number with grading information and the assembly date code. Grading data can weed out valid parts remarked by forgers to resemble higher grade parts. The date code assists in identifying older devices that require additional screening to ensure they are new and have not been previously used.



SmartFusion2 SoC fpgas are suitable for use in a strong technical anticounterfeiting solution.

The production mechanism ensures only good devices receive a certificate, which prevents the representation of failed components as good ones. The hardware security module (HSM) at the fab logs each certificate securely, so the OCM knows exactly how many have been issued.

As part of a screening process, such as checking the delivered device against the order, SmartFusion2 devices can be authenticated in a number of ways. The certificate's integrity and signature can be checked using the Microsemi public key. The certificate can be checked for listing on a certificate revocation list and the device itself can be checked to ensure that it knows the correct unique private cryptographic key and is bound correctly to the certificate. This proves the certificate belongs to that particular device and is not a copy of a certificate belonging to another device.

By adopting a strong foundation of technologies for anti counterfeiting, devices such as SmartFusion2 provide the assurance of authenticity that is now needed in the forgery prone electronics supply chain – not just for the devices themselves, but also for the subsystems into which they are assembled.

Author profile:

G. Richard Newell is senior principal product architect with Microsemi's SoC products group.