Semiconductor Manufacturing & Design
COMMUNITY

Tech Industry security highlighted by the iPhone access controversy

-Blog by:
Cédric Mayor, Chief Technical Officer, Presto Engineering, Inc., Caen, France cedric.mayor@presto-eng.com

-The confrontation between Apple and the FBI over the FBI's request for assistance in hacking a known terrorist's iPhone brought the topic of security to the top of the agenda for the tech industry. Recent developments, including the FBI's withdrawal of its request and Apple's subsequent demand that the FBI now share information the security vulnerability that permitted a third party to hack the iPhone, have only emphasized the "moving target" nature of security. Whether manufacturing a car, a smartphone, or a smartcard, How to ensure that each die in an IoT SiP/McM (multichip module) device can be tested along a route of trust.

How to provide a seamless test manufacturing flow that efficiently and effectively detects manufacturing quality issues while injecting secrets from customers, without storing the secret information, needing to decrypt it, or leaving it open to reverse engineering.

How the injection of secrets/certificates impacts DFT and diagnosis of the chip. These sensitive operations require the insertion of secret keys, tokens, certificates and boot loaders into the device during wafer probe or at final test on the package level. The secret vectors must be dynamically allocated and are often reshuffled by the end-customers to disaggregate the supply chain. The test floor must include an encrypted server gateway, and the ability to selectively push the encrypted information into the right device on wafer, which is usually locked at the end of the wafer test and completely isolated when the wafer is sawn. Test and assembly is really the only opportunity to address confidentiality since the heterogeneous nature an IoT devices necessarily involves the sourcing of die from different vendors and requires validation of trust for each component. Test providers that can deliver a secure workflow will be critical contributors to the security of the IoT.

Overlooked Semiconductor Technology Plays a Key Role in Secure IoT

February 18th, 2016

Blog by:

Cédric Mayor, Chief Technical Officer, Presto Engineering, Inc., Caen, France

Over the past 40 years, the semiconductor industry has worked hard to miniaturize ICs, and has stayed very much in line with Moore’s eponymous prediction. In fact, the latest frenzy into the sub-20nm node and beyond has been primarily driven by smart phone applications, an industry that is constantly looking for new points of differentiation as the market rapidly matures and manufacturers are challenged to find new novel features to entice consumers with. The latest application processors for Apple and Qualcomm, which are running on 14nm and 16nm foundry nodes, are perfect examples. In this stampede to be at the leading edge, the industry has inadvertently deserted a many technology and capacity capabilities of the semiconductor manufacturing process.

The industry’s single-minded focus on advanced technology has left mature modular process nodes between 180nm and 90nm, on 8- or 12-inch wafer size, to be set to the side. Yet there is a wealth of process technologies and ready libraries in this process range for engineers to build perfectly marketable ICs, such as ASIC’s and SoCs, that optimize designs traditionally found in conventional PCB-based sub-assembly or module applications.

When you add the advancement of sensor technologies like MEMS, radiofrequency, optical circuits, all the ingredients are there to create some very interesting products for markets where size is just a little less preoccupying than it is in smart phones and tablets.

The up and coming IoT market, which is expected to double in size in the next four years, is the perfect match for these technologies. While combining sensors, analog to digital conversion, local processing, storage, secure element hardware, and communications in a single application is not new to the industry, rethinking of these IoT applications in industry, home, cities, health, and transportation with a view to taking advantage of semiconductor integration is new. And thanks to mature/mainstream semiconductor technologies, it is both possible and economically viable. Designing a chip on older fab nodes can often be accomplished within a $5 million US dollar budget!

With the advent of independent service suppliers at different stages of the semiconductor manufacturing process, fabless companies do not need to be a major players in the industry to make their own ICs. Market forecasters, like Gartner and McKinnsey, have predicted that the IoT will generate thousands of new applications for electronics and semiconductor consumption. I expect that this new demand will make its way into custom IC’s, because the required infrastructure is already there and using it is easier and less expensive to do than it was only a few years ago.

I see a paradigm shift on the horizon. Integrating and miniaturizing multifunction systems using older process technologies may be a bit less glamourous than the long running chase to minimize devices and process geometries, but it will be an important transition for the industry.