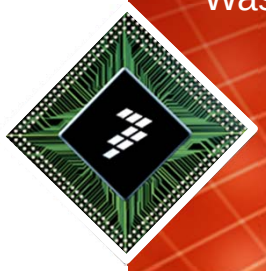
Semiconductor Manufacture and Potential Vulnerabilities

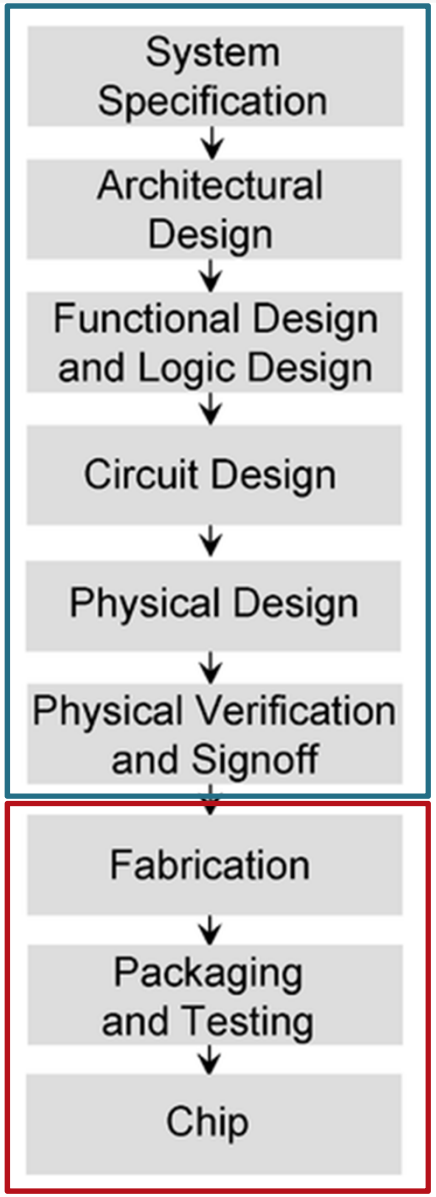
Kevin Kemp
Freescale Semiconductor

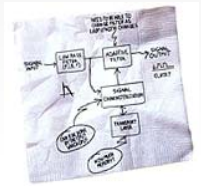
Software Assurance and Trustworthy Semiconductor Workshop
January 15 - 16, 2013
Washington DC



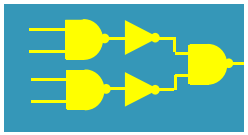
Freescale, the Freescale logo, AltiVec, C-5, CodeTEST, CodeWarrior, ColdFire, C-Ware, the Energy Efficient Solutions logo, mobileGT, PowerQUICC, QorIQ, StarCore and Symphony are trademarks of Freescale Semiconductor, Inc., Reg. U.S. Pat. & Tm. Off. Airfast, BeeKit, BeeStack, ColdFire+, CoreNet, Flexis, Kinetis, MagniV, MXC, Platform in a Package, Processor Expert, QorIQ Qonverge, Qorivva, QUICC Engine, Ready Play, SafeAssure, SMARTMOS, TurboLink, VortiQa and Xtrinsic are trademarks of Freescale Semiconductor, Inc. All other product or service names are the property of their respective owners. © 2011 Freescale Semiconductor, Inc.

Integrated Circuit Design and Manufacturing Flow

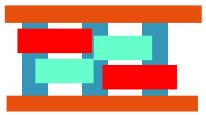




The first step is to define the functional specification and architecture of a chip to meet the needs of a particular application or market (e.g. computer processor, cellular transceiver, memory chip, microcontroller…)



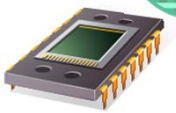
This step converts the specification into a register transfer level (RTL) description. The RTL describes the exact behavior of the digital circuits on the chip, as well as the inputs and outputs.



The chip design is assembled from the RTL using a library of available logic gates. This involves figuring out which gates to use, where to place them, and how to wire them together.

Many checks happen throughout the design process, and there is a detailed set of checks before the design is sent to the wafer fab.

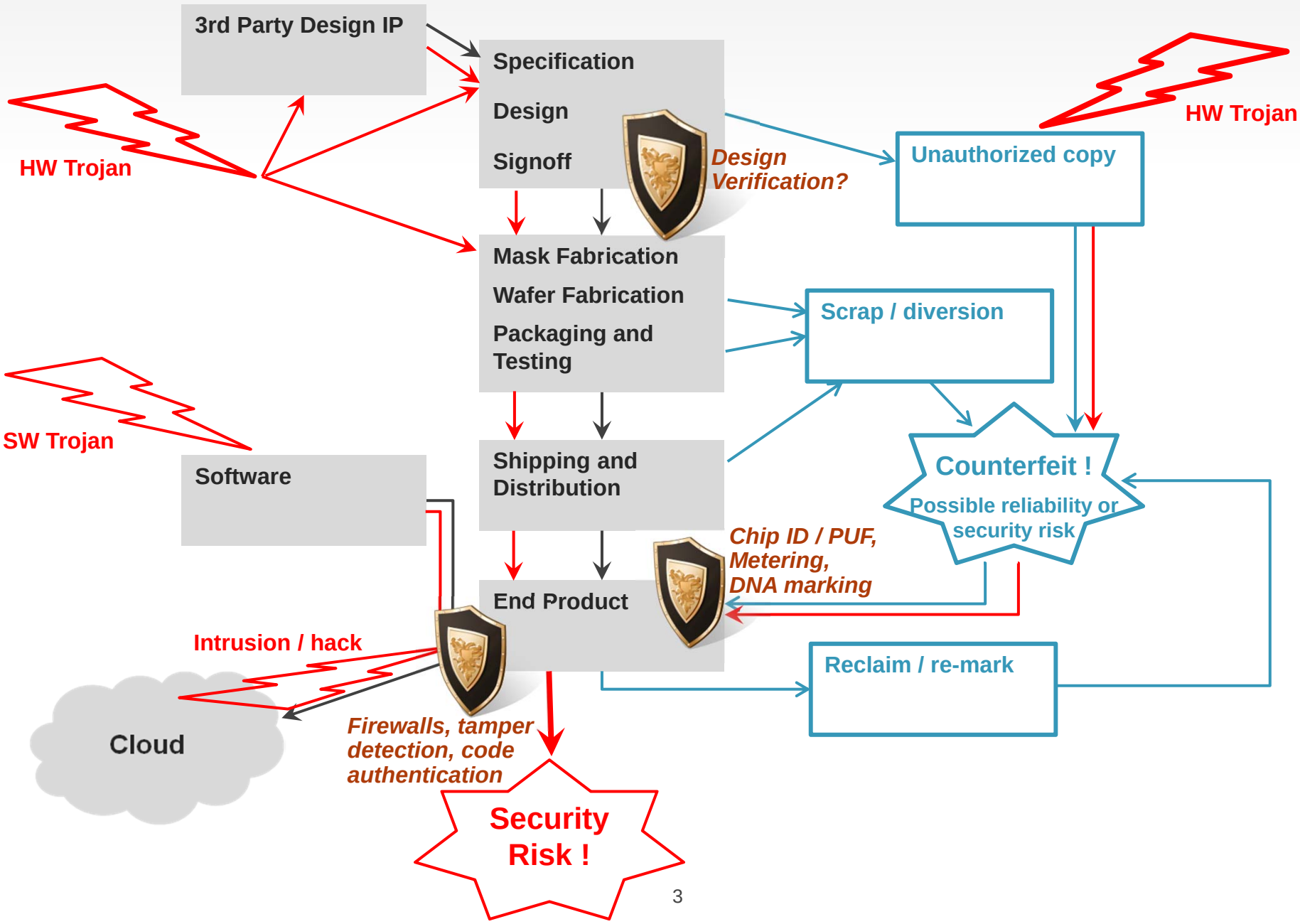
The physical design is etched into silicon wafers using a photolithography process to form the actual transistors and wiring.



Wafers are diced into chips and assembled in packages to be attached to a circuit board in the end product.

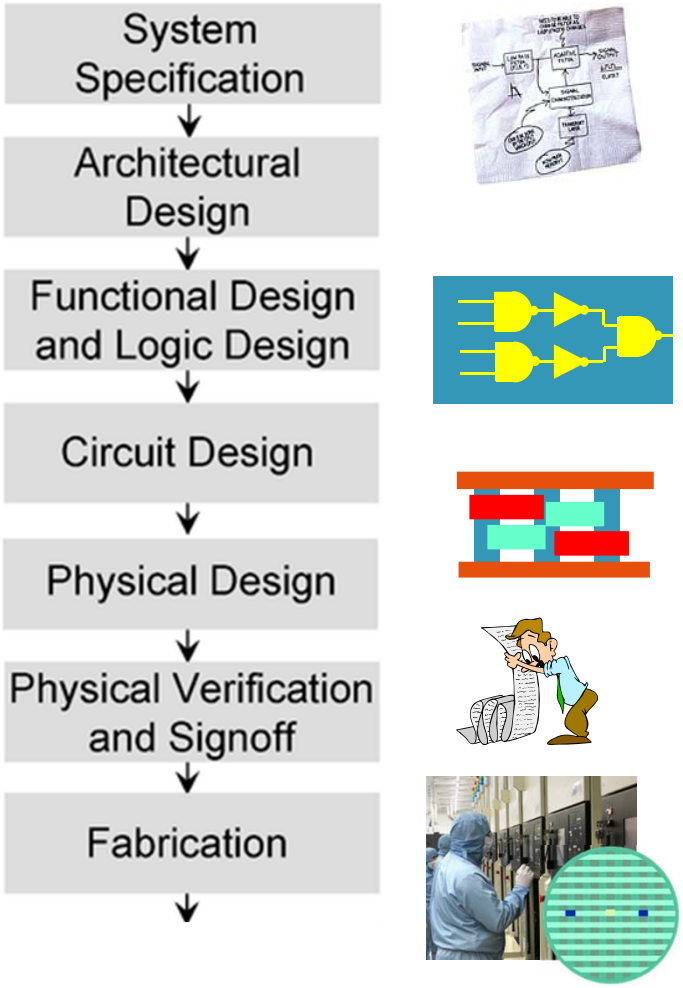
http://en.wikipedia.org/wiki/File:Integrated_circuit_design.png

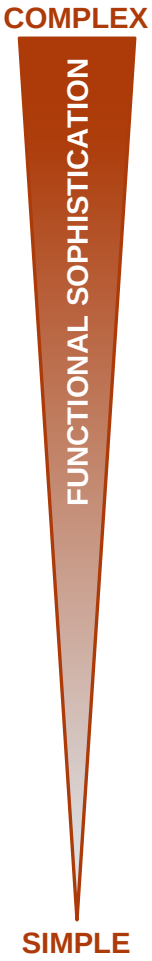
A Secure IC Design and Manufacturing Flow?



Hardware Trojans in IC Design Flow

Examples: Back doors, Time bombs, Side-channel communication paths…



HW Trojan Insertion

- Incorporate malicious behavior in specification / architecture
- Add logic triggers, counters, etc. to RTL
- Manipulate layout to add gates and wires
- Modify GDS data prior to mask fabrication
- Induce defects to reduce reliability or disable security features