ECE 459/559
Secure & Trustworthy Computer Hardware Design

Introduction

Garrett S. Rose
Spring 2017

THE UNIVERSITY OF TENNESSEE KNOXVILLE

Goals

- Learn state-of-the-art security primitives and methods, including emerging technologies and security trends
- Integration of security as a design metric, *NOT* an afterthought
- Protecting intellectual property (IP) against piracy & tampering
- Understand attacks and how to provide countermeasures
- Understand vulnerabilities in design and fabrication processes
- Understand component design and supply chain vulnerabilities

Some Topics Covered

- Cryptographic cores
  - Vulnerabilities & processing overhead
- Attack vectors
  - Physical, Invasive vs. non-invasive
- Physically unclonable functions (PUF)
- True random number generators (TRNG)
- Anti-piracy
  - Watermarking, passive & active hardware metering
- FPGA Security
  - Trusted design in FPGAs
- Hardware Trojans – detection & prevention
- Counterfeit detection & avoidance

Motivation for Hardware Security

- HW security is becoming increasingly important

  "Hardware security sneaks into PCs,"
  – Robert Lemos, CNET News.com, 3/16/05

  "Microsoft reveals hardware security plans, concerns remain,"
  – Robert Lemos, SecurityFocus 04/26/05

  "Princeton Professor Finds No Hardware Security In E-Voting Machine,"
  – Antone Gonsalves, InformationWeek 02/16/07

  "Secure Chips for Gadgets Set to Soar,"
  – John P. Mello Jr. TechNewsWorld, 05/16/07

  "Army requires security hardware for all PCs,"
  – Cheryl Gerber, FCW.com, 7/31/2006

- www.trust-hub.org

Example: Time for Smart Cards

- By end of 2006, many European countries migrated to smart cards
  - Voting: In Sweden you can vote with your smart card which serves as a non-repudiation device
  - Telecommunications: Many cellular phones come with smart cards in Europe and will soon be shipping in the United States
  - Mass Transit: British Air relies on rail and air connections more than most airports
- In 2006, ~27M contactless cards were in circulation in the US, the number was estimated to top 100M in 2011
  - Example: DHS requires port workers to have smart ID cards
  - Entertainment: Most DSS (Digital Satellite Service) dishes in the US use smart cards

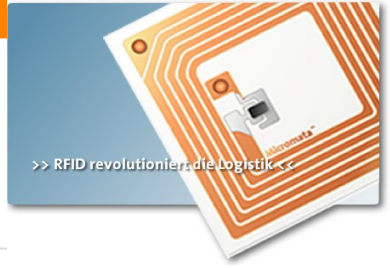
Smart Cards – Attacks

"Access Control: Smart Cards Under Attack - Literally,"
– Ken Warren, Security Magazine, 3/17/06

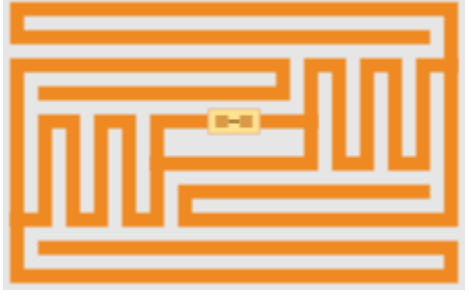
"Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks,"
– Saar Drimer and Steven J. Murdoch, USENIX SECURITY, 2007

"Vulnerability Is Discovered In Security for Smart Cards,"
– John Markoff, New York Times, 5/13/2002

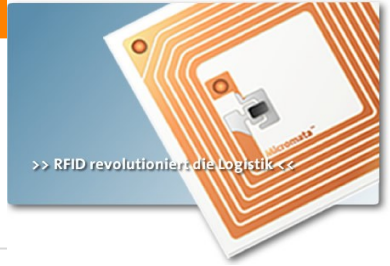
Example: RFIDs



- Radio-frequency identification (RFID) – the use of an object for the purpose of identification and tracking using radio signals
- Most RFID tags contain at least two parts:
  - Integrated circuit for storing and processing information, modulating and demodulating a RF signal, and other special functions
  - Antenna for receiving & transmitting the signal
- Some RFID tags are active (battery powered) and some are passive

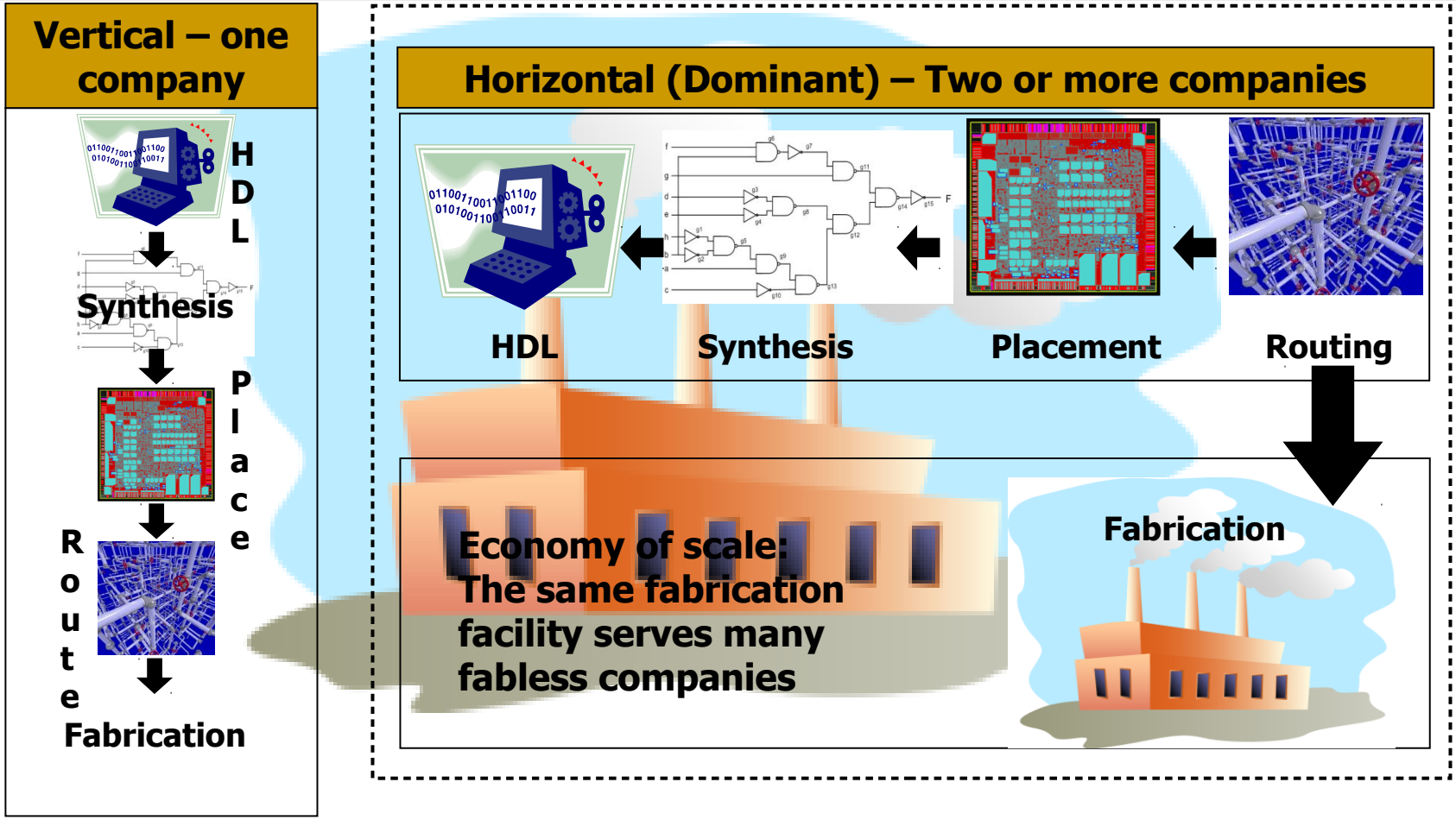


Example: RFIDs



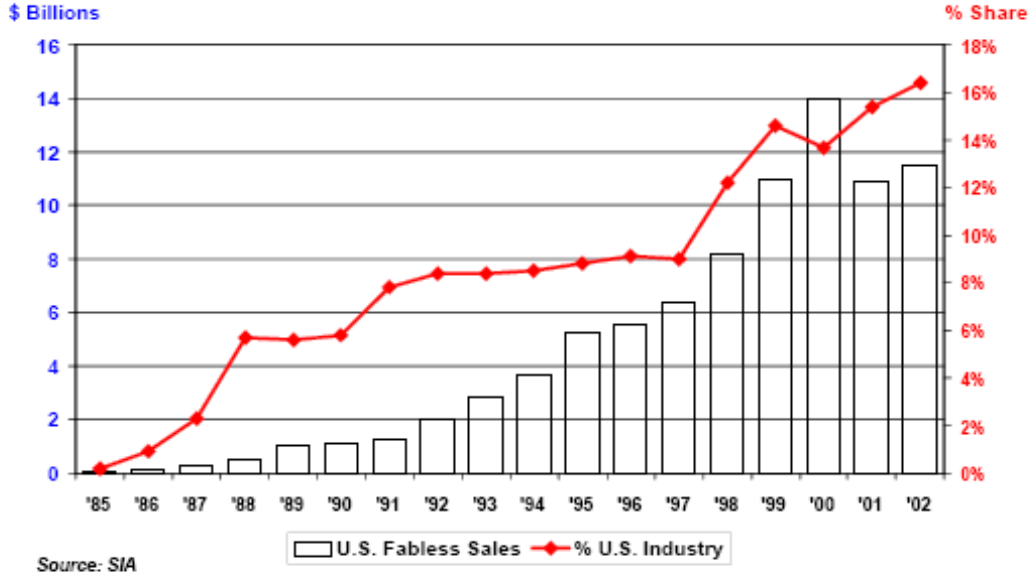
- Many applications in securing transactions:
  - Inventory Control Container / Pallet Tracking
  - ID Badges and Access Control
  - Fleet Maintenance Equipment / Personnel Tracking in Hospitals
  - Parking Lot Access and Control
  - Car Tracking in Rental Lots
  - Product Tracking through Manufacturing and Assembly
- Challenge: Can we create security mechanisms light enough to be suitable for RFIDs?

Semiconductor Industry
A Shift in the Business Model



Semiconductor Industry Business Model

The fabless/foundry business model has grown to 16% of the U.S. chip industry. The trend is strongest in the leading process technology portion of the industry

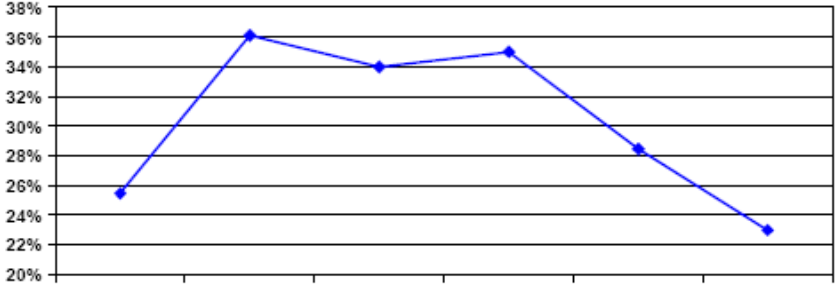


Source: SIA

Leading-Edge Technology

The cost of building a full-scale, 300 mm wafer 65 nm process fabrication plant is about $3bn; TSMC has spent more than $9bn!

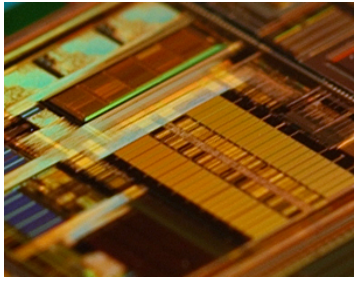
U.S. industry's share of capital expenditures falling and in leading edge semiconductor manufacturing capacity.



Leading Edge	< 0.4µ	< 0.3µ	< 0.3µ	< 0.2µ	< 0.2µ	< 0.16µ

Source: SICAS/SIA

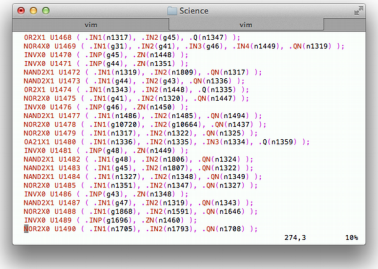
Hardware Threats



IP Vendor

System Integrator

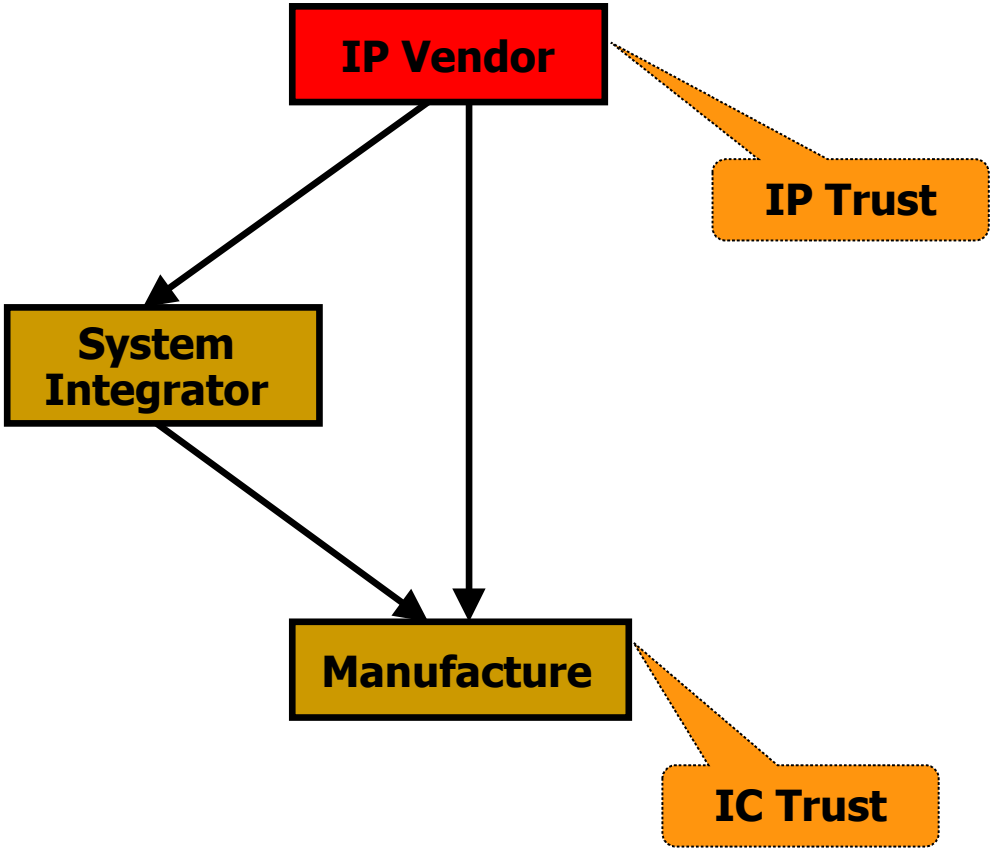
Manufacture



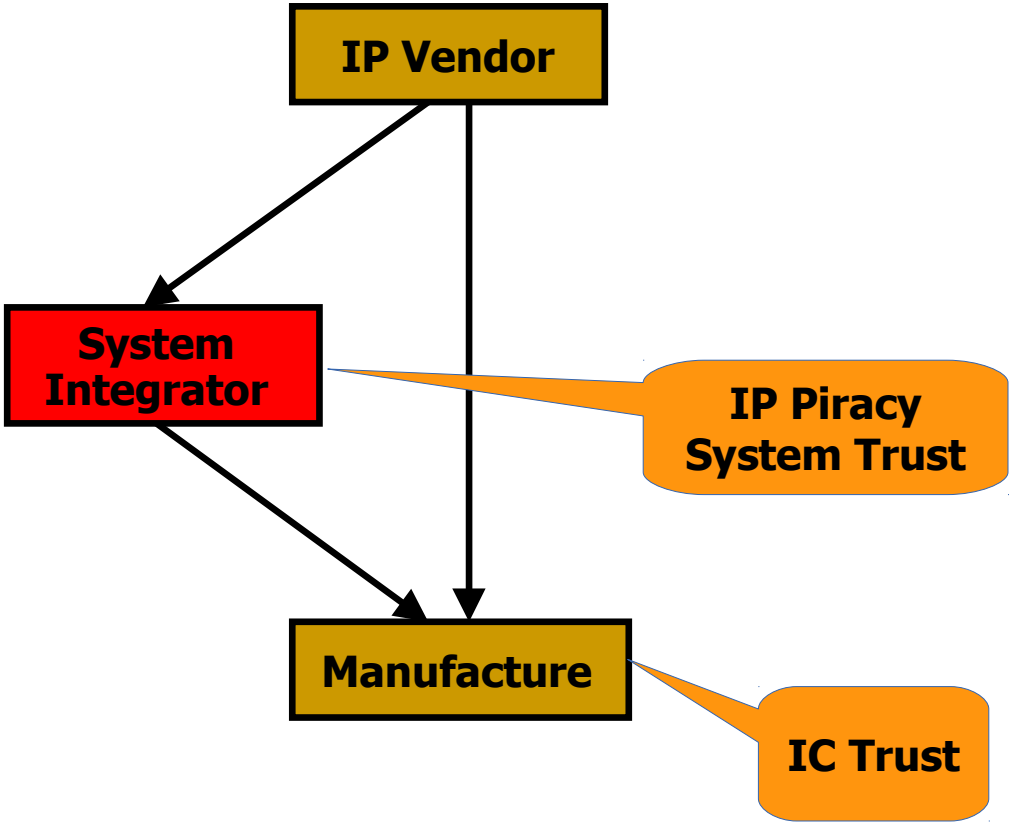
THE UNIVERSITY OF TENNESSEE KNOXVILLE

Any of these steps can be untrusted

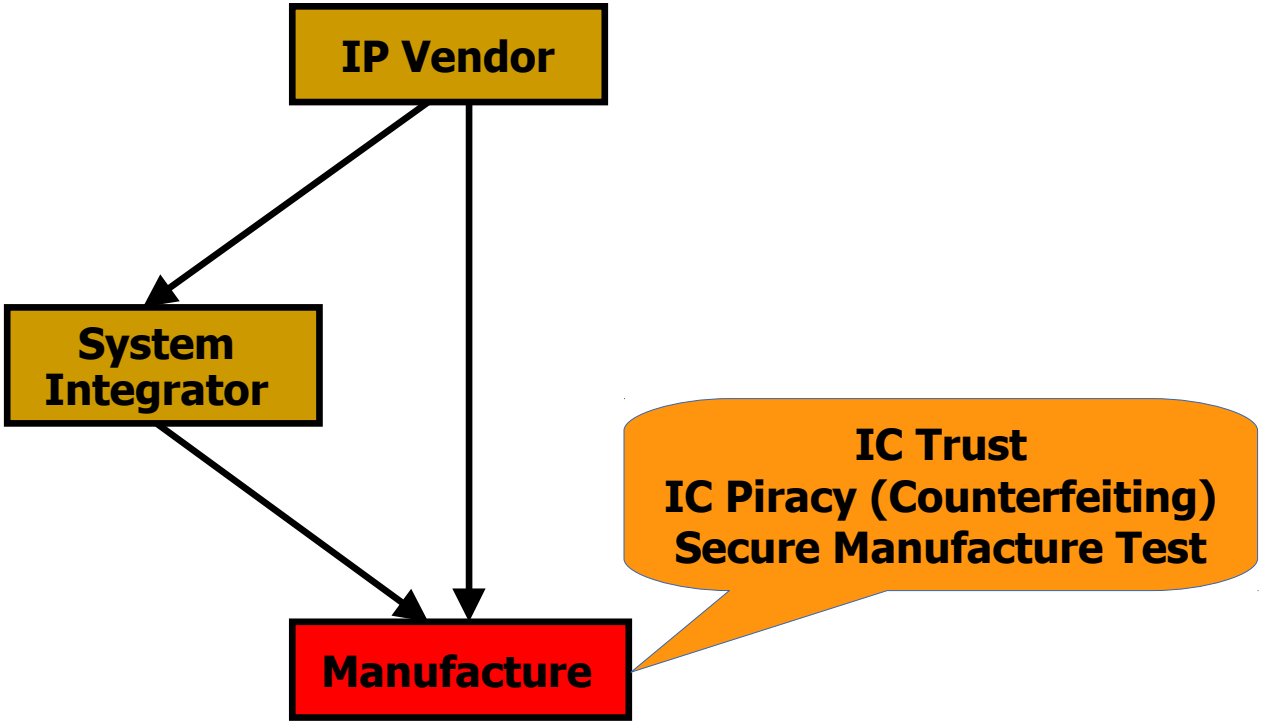
Hardware Threats



Hardware Threats

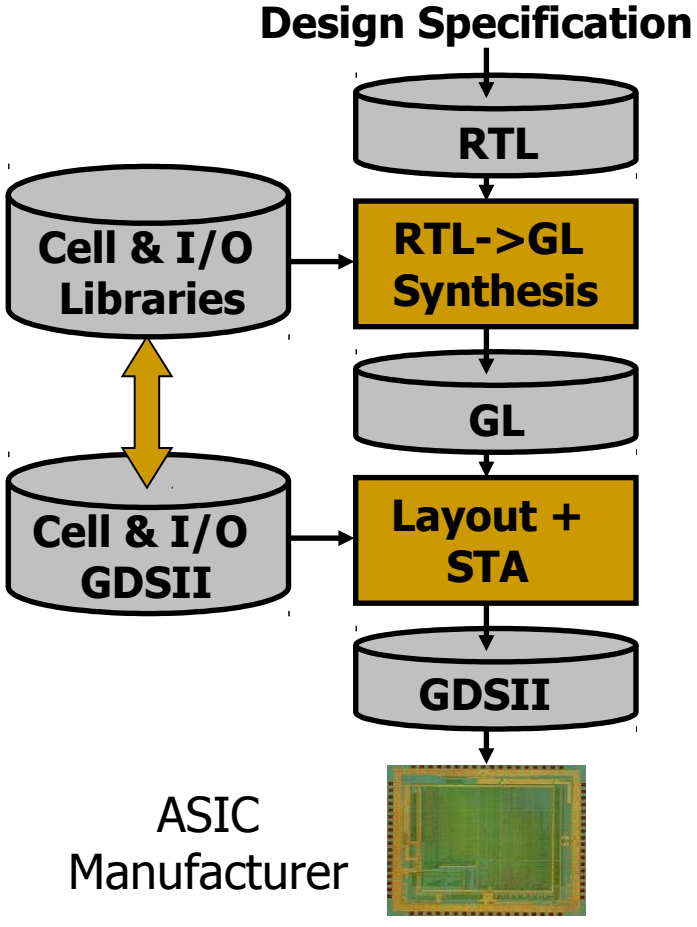


Hardware Threats



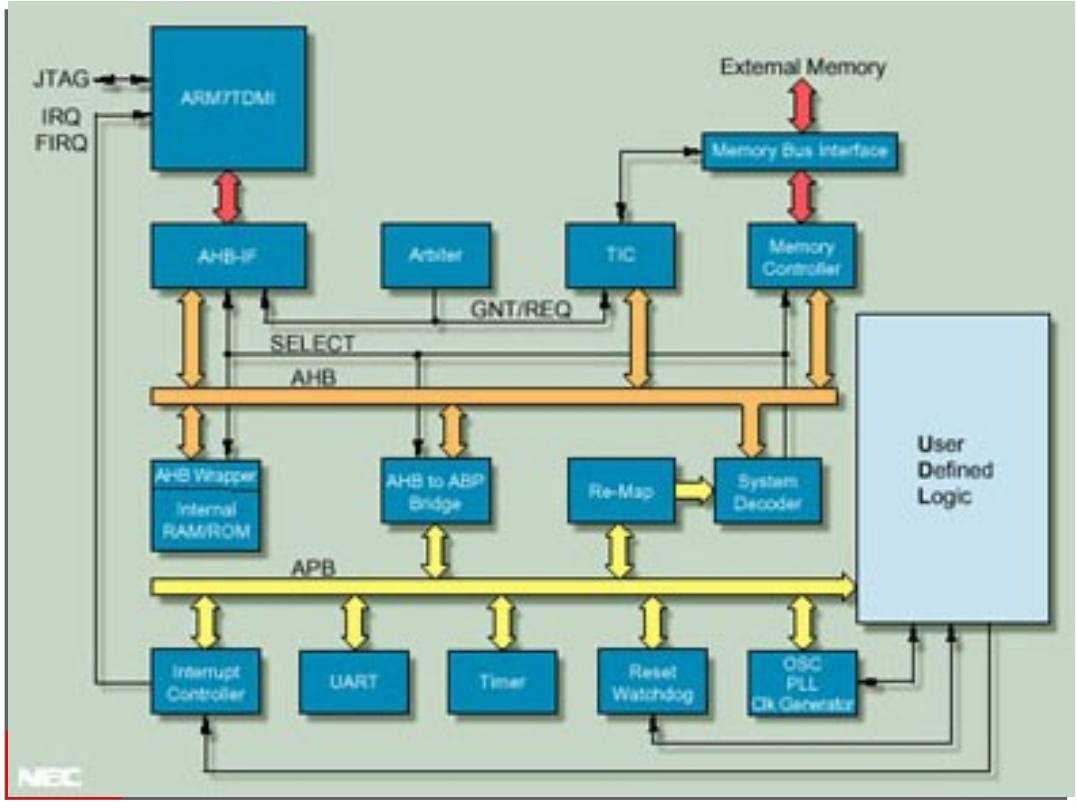
Untrusted

Design Flow – The Old Way

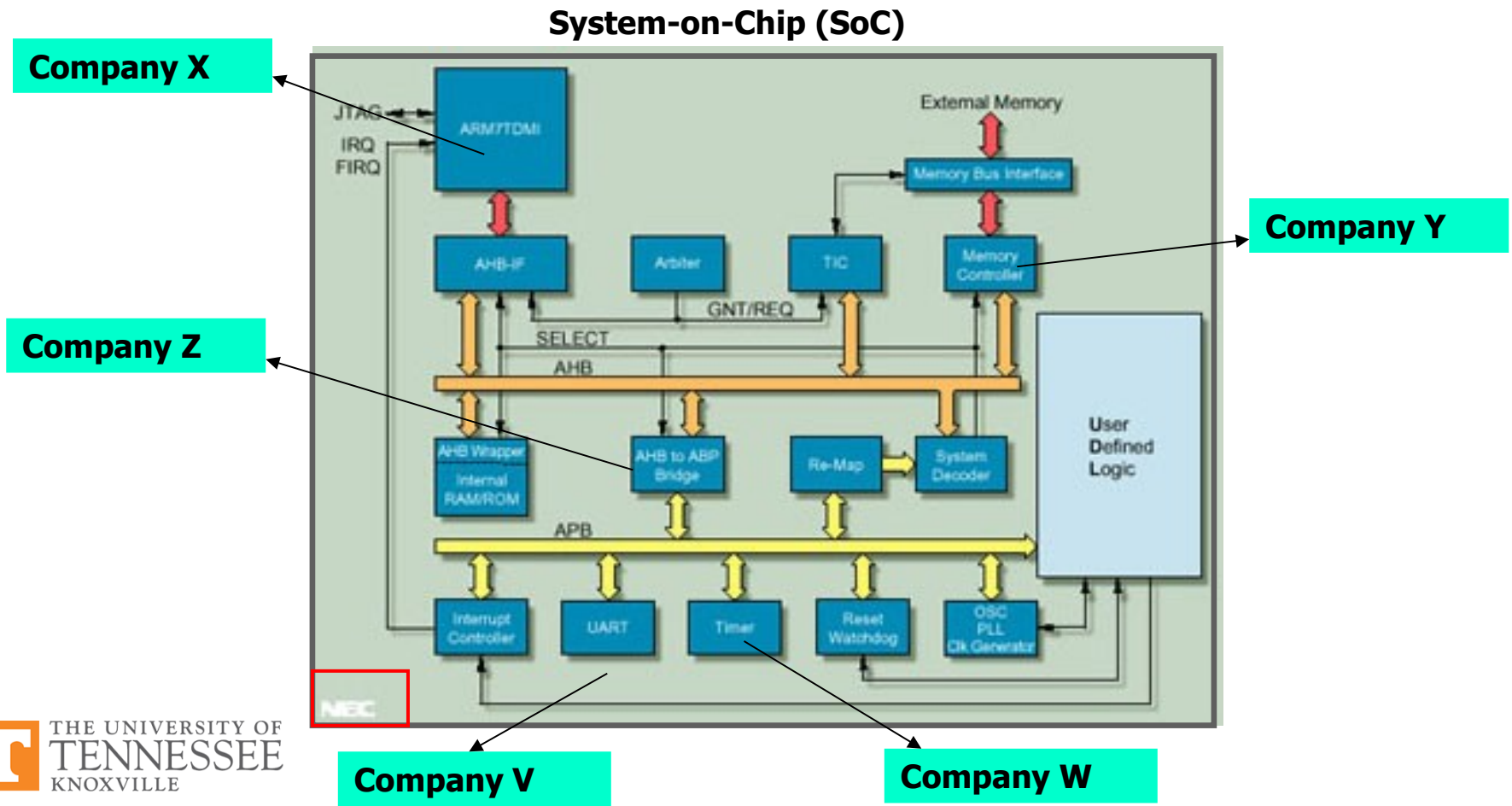


Issues with Third Party IP

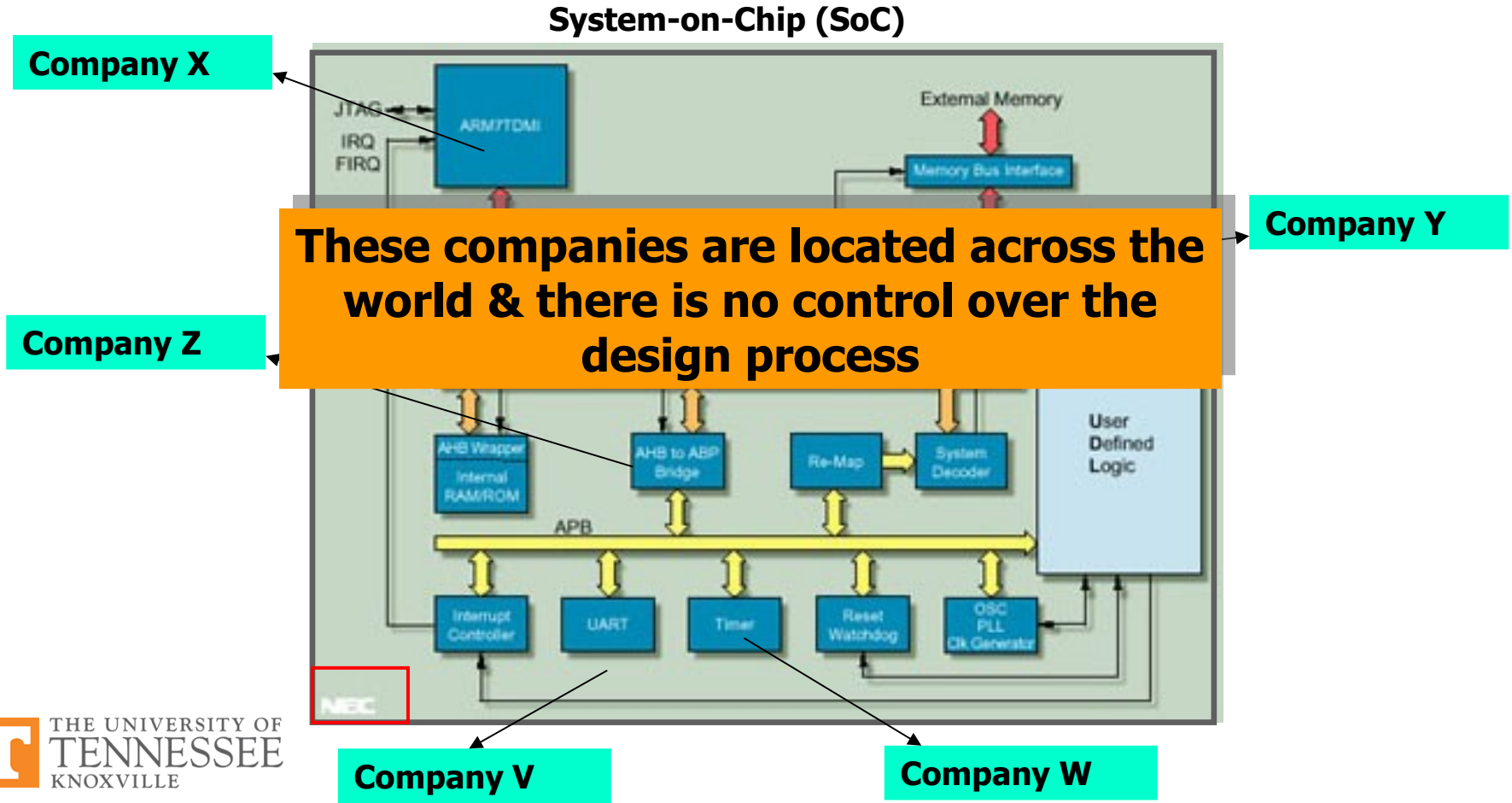
System-on-Chip (SoC)



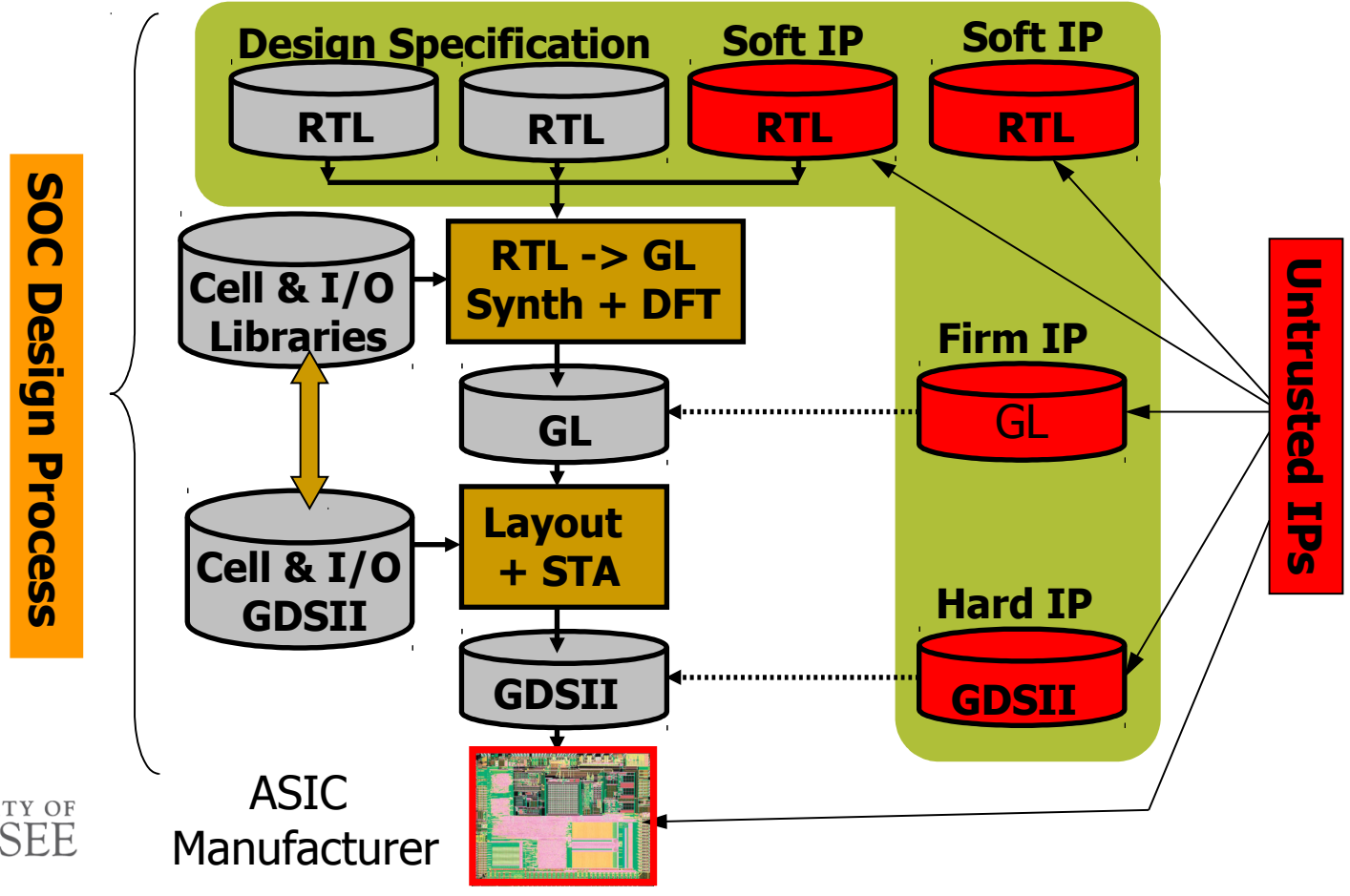
Issues with Third Party IP



Issues with Third Party IP

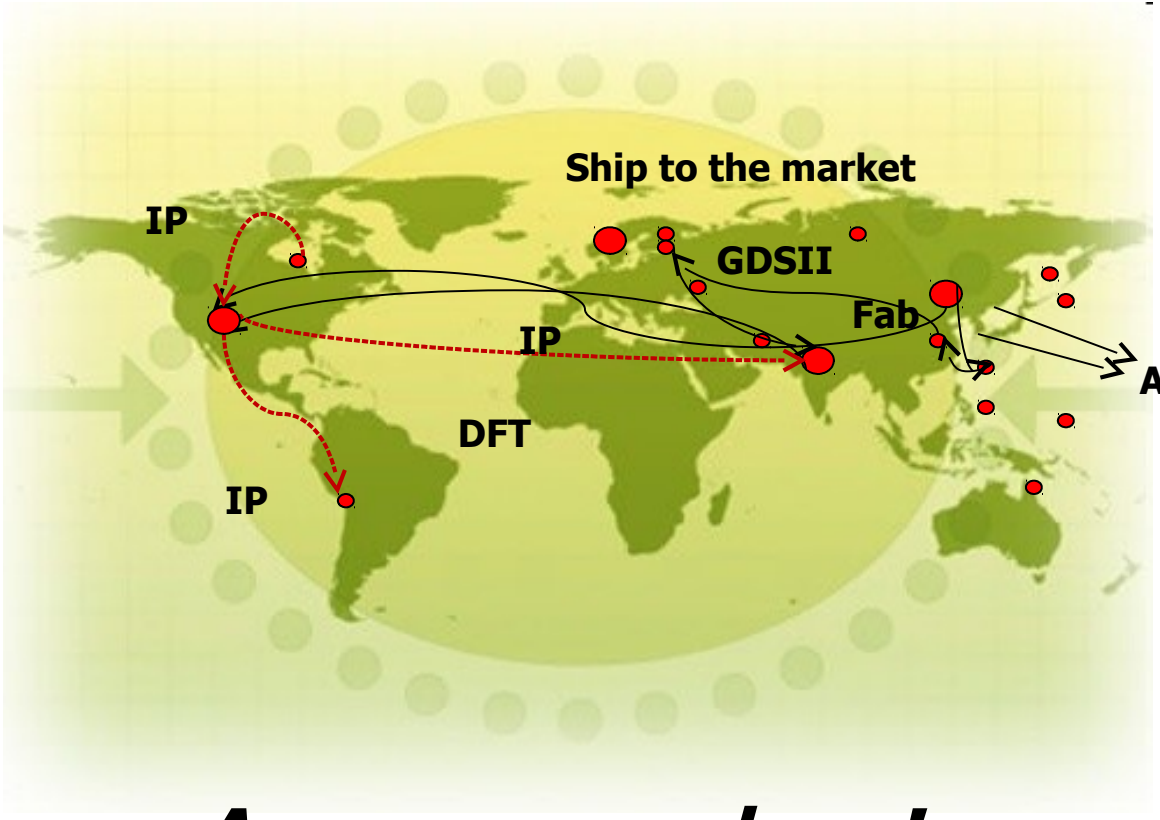


Design Flow – The New Way



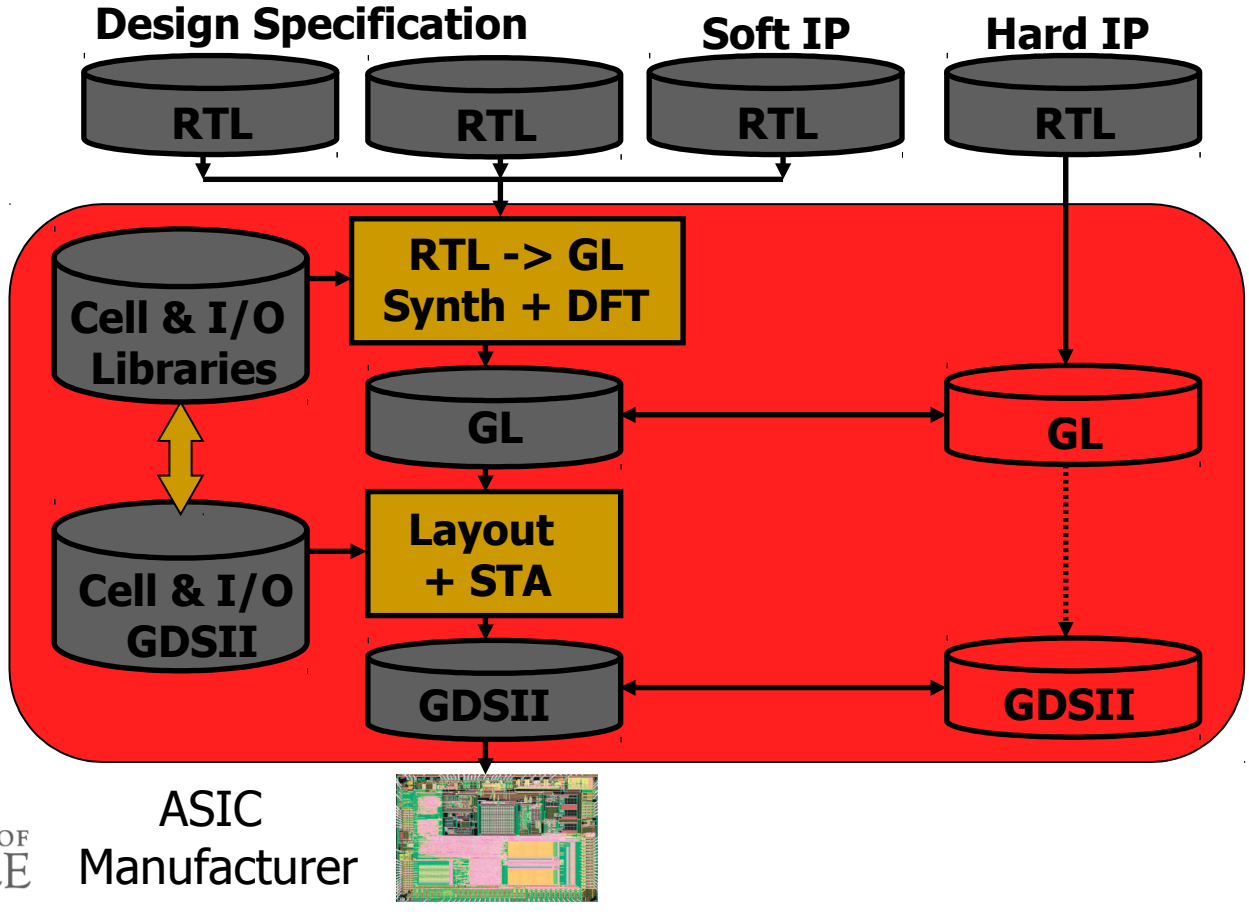
Who Develops the IP? Who Designs the IC? Who Fabricates?

Who Develops the IP? Who Designs the IC? Who Fabricates?

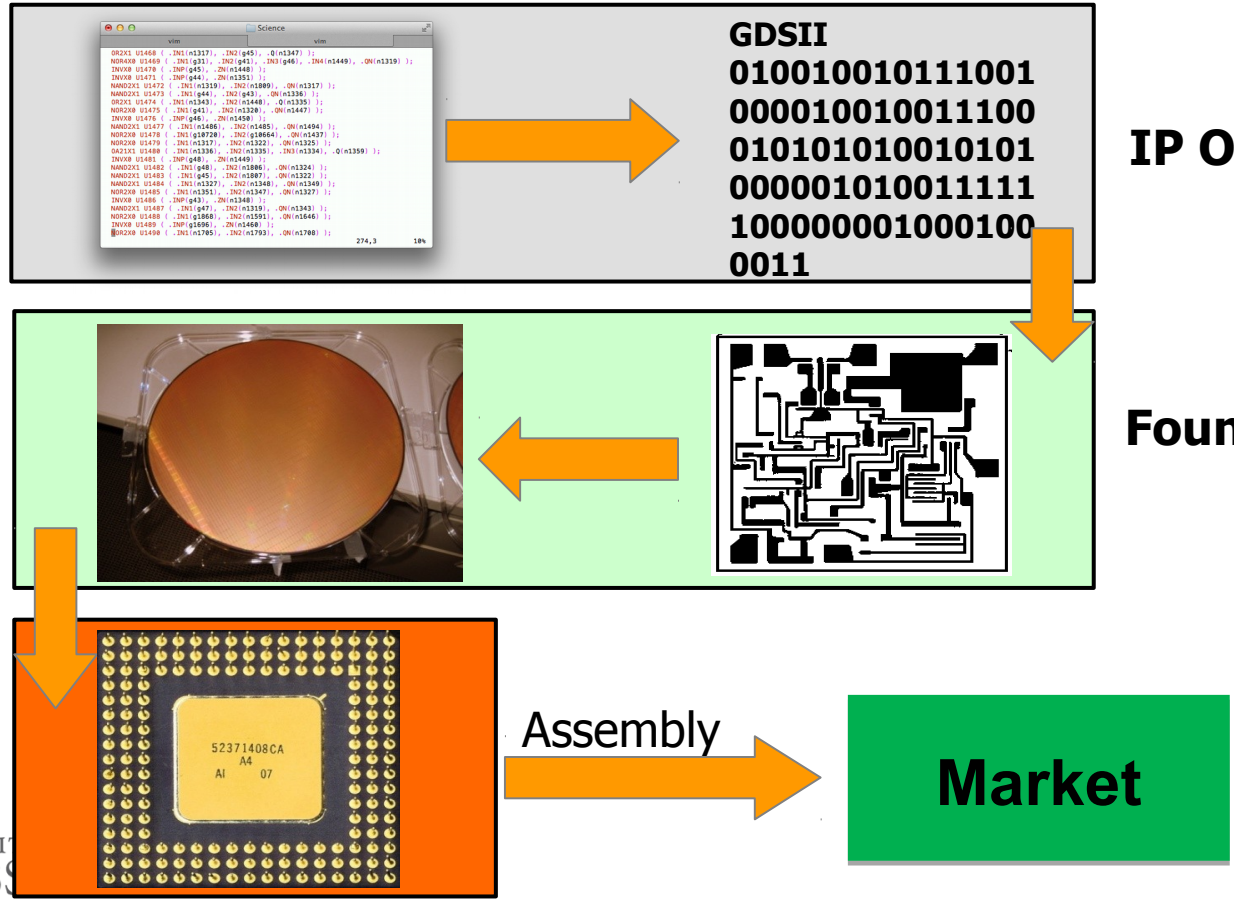


Anyone, anywhere!

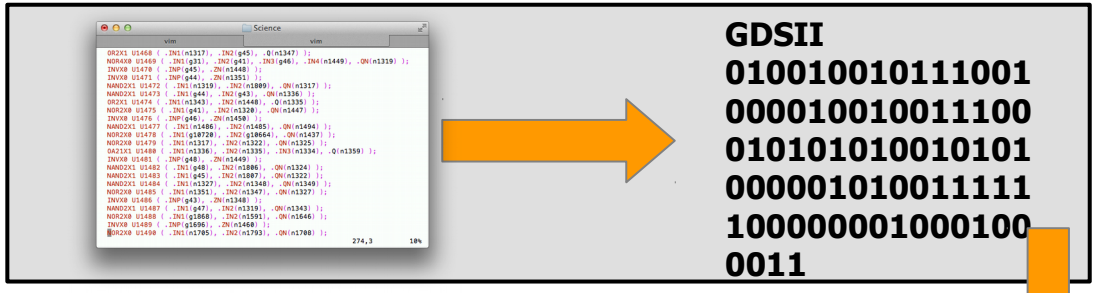
Untrusted System Integrator



Counterfeiting

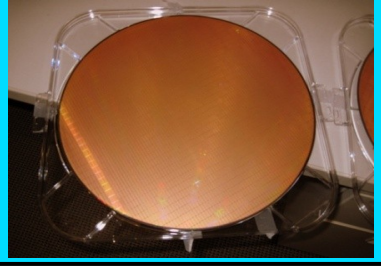


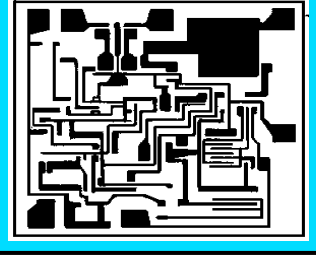
Counterfeiting



GDSII
0100100101110010000100100111000101010100100101000001010011111100000000100010000011

IP Owner

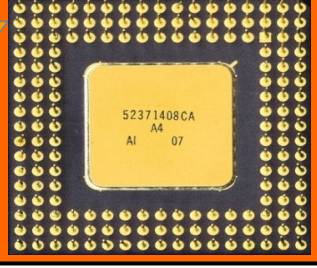




Foundry

Over-produced ICs

Defective or Out-of-spec ICs



Assembly

Market

IC Counterfeiting

- Most prevalent attack today!
- Unauthorized production of wafers
- Estimated that counterfeiting costing semiconductor industry more several billion dollars per year

Over production

Off-spec parts

Defective parts

Cloned ICs

Recycled ICs

IC Recycling Process

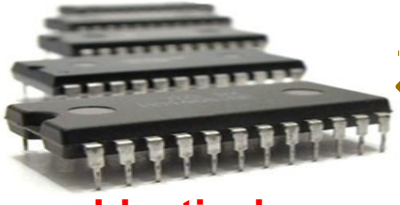
A recycling center

PCBs taken off of electronic systems

ICs taken off of PCBs

Refine recycled ICs

Resold as new



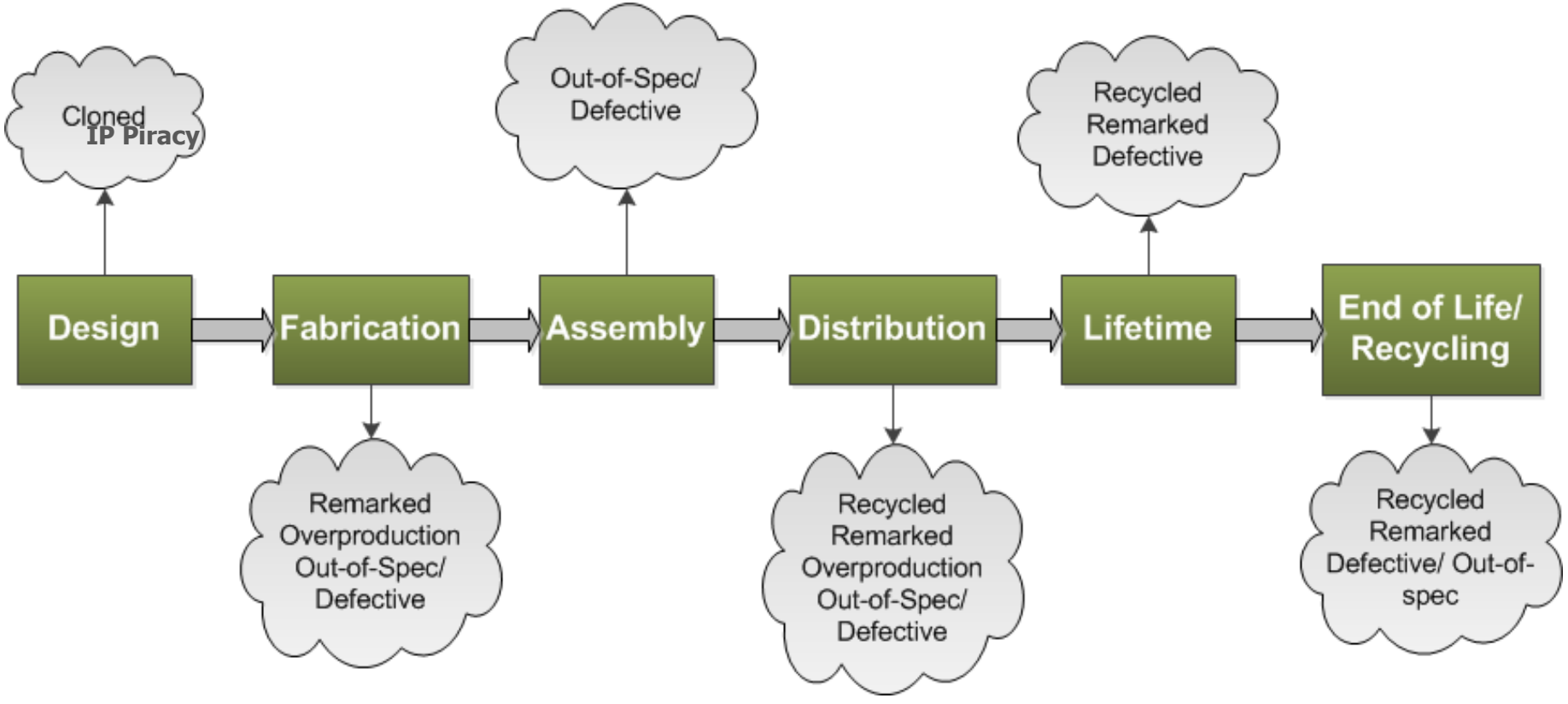
Identical:

Appearance, Function, Specification

Critical Application

Consumer trends suggest that more gadgets are used in much shorter time – more e-waste

Supply Chain Vulnerabilities



Piracy – A True Story…

- In 2000, Chen Jin, finished his Ph.D. in computer engineering at the University of Texas at Austin
- He then returned to China, first to Motorola Research and then to Jiaotong University as a faculty member
- In 2003, he supervised a team that created one of China's first homegrown DSP ICs
- Chen was named one of China's brightest young scientists, funded his own lab, received a huge grant from the government
- In 2006, it was revealed that he faked the chip, having stolen the design from Texas Instruments!

Ref.: “In a Scientists Fall, China Feels Robbed of Glory,” New York Times, May 2006. (link)

Another Story: "The Athens Affair"

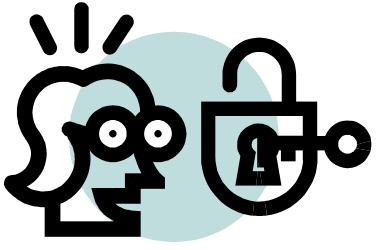
- In March 8, 2005, Costas Tsalikidis, a 38 year old engineer working for Vodafone Greece committed suicide, linked to scandal
- The next day, the prime minister was notified that his cell phone – and those of other high ranking officials – was hacked!
- Earlier, in January, investigators had found rogue software installed on the Vodafone Greece phones by "parties unknown"
- The scheme did not depend on the wireless nature of the devices
- A breach in storing keys in a file – Vodafone was fined €76 million!

Some Basic Definitions

- **Intellectual property** represents the property of your mind or intellect – proprietary knowledge
- The four legally defined forms of IP:
  - **Patents** – register invention with the government, gain legal right to exclude others from manufacturing or marketing it
  - **Trademark** – a name, phrase, sound or symbol used in association with services or products
  - **Copyright** – protections for written or artistic forms of expression fixed in a tangible medium
  - **Trade secrets** – formula, pattern, device or compilation of data that grants user an advantage over competitors

Some Basic Definitions (cont'd)

- **Cryptography**:
  - crypto (secret) + graph (writing)
    – the science of locks and keys
  - The keys and locks are mathematical
  - Behind every security mechanism, there is a “secret” …



  - Locks and keys very useful in security
  - We will discuss more about traditional cryptography, but will also show new forms of security based on HW-based secrets