BETA

Introduction to Hardware Security

Alessandro Savino

Politecnico di Torino

Acknowledgement

Most of the original Slides are Prof. Mark Tehranipoor's and his collaborators' property.

Hardware Security

Cybersecurity experts have traditionally assumed that the hardware underlying information systems is secure and trusted. However, such an assumption is no longer true.

Example Attack

Roy Zoppoth stands over a Xerox 914 copy machine, the world's first, which was used in soviet embassies all over the world. The machine was so complex that the CIA used a tiny camera designed by Zoppoth to capture documents copied on the machine by the Soviets and retrieved them using a "Xerox repairman" right under the eyes of soviet security.

Motivation – HW 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
- Facebook group on Hardware Security

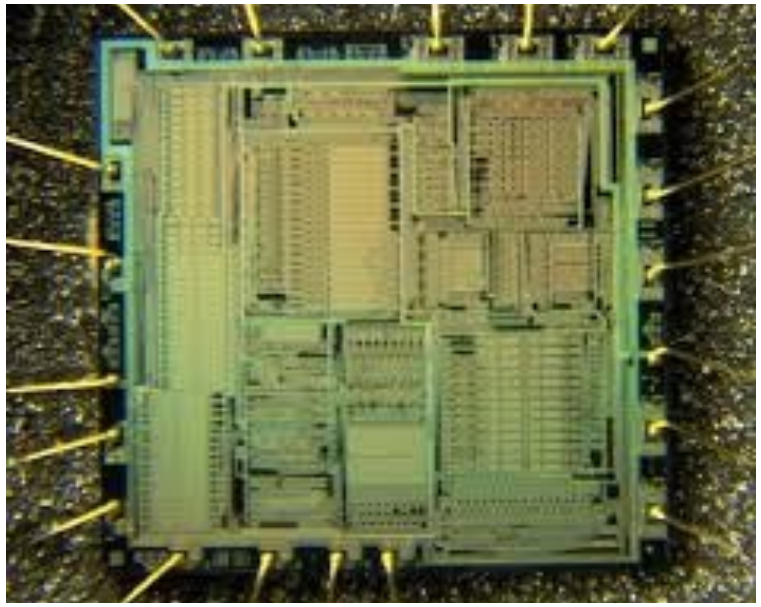
Example Attack

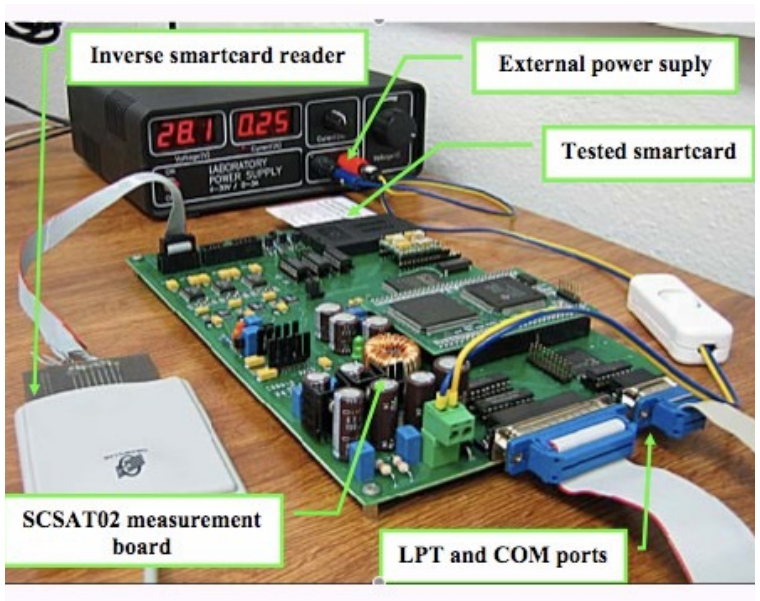
Fake Cisco routers risk "IT subversion"

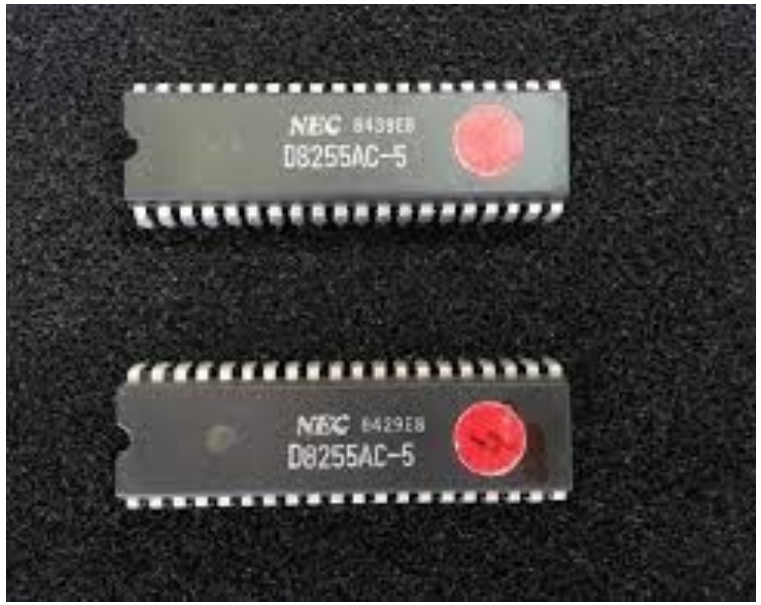
- An internal Federal Bureau of Investigation presentation states that counterfeit Cisco routers imported from China may cause unexpected failures in American networks. The equipment could also leave secure systems open to attack through hidden backdoors.
- $76 million fake Cisco routers

Example Attack

- Physical Attacks on Chip IDs
  - Extracting secret keys
- Side-Channel Attacks
  - Power Analysis, Timing Analysis, EM Analysis
- Tampering with Electronic Devices
  - Captured Drone by Iran
- Counterfeit Integrated Circuits
  - Multi-billion-dollar business



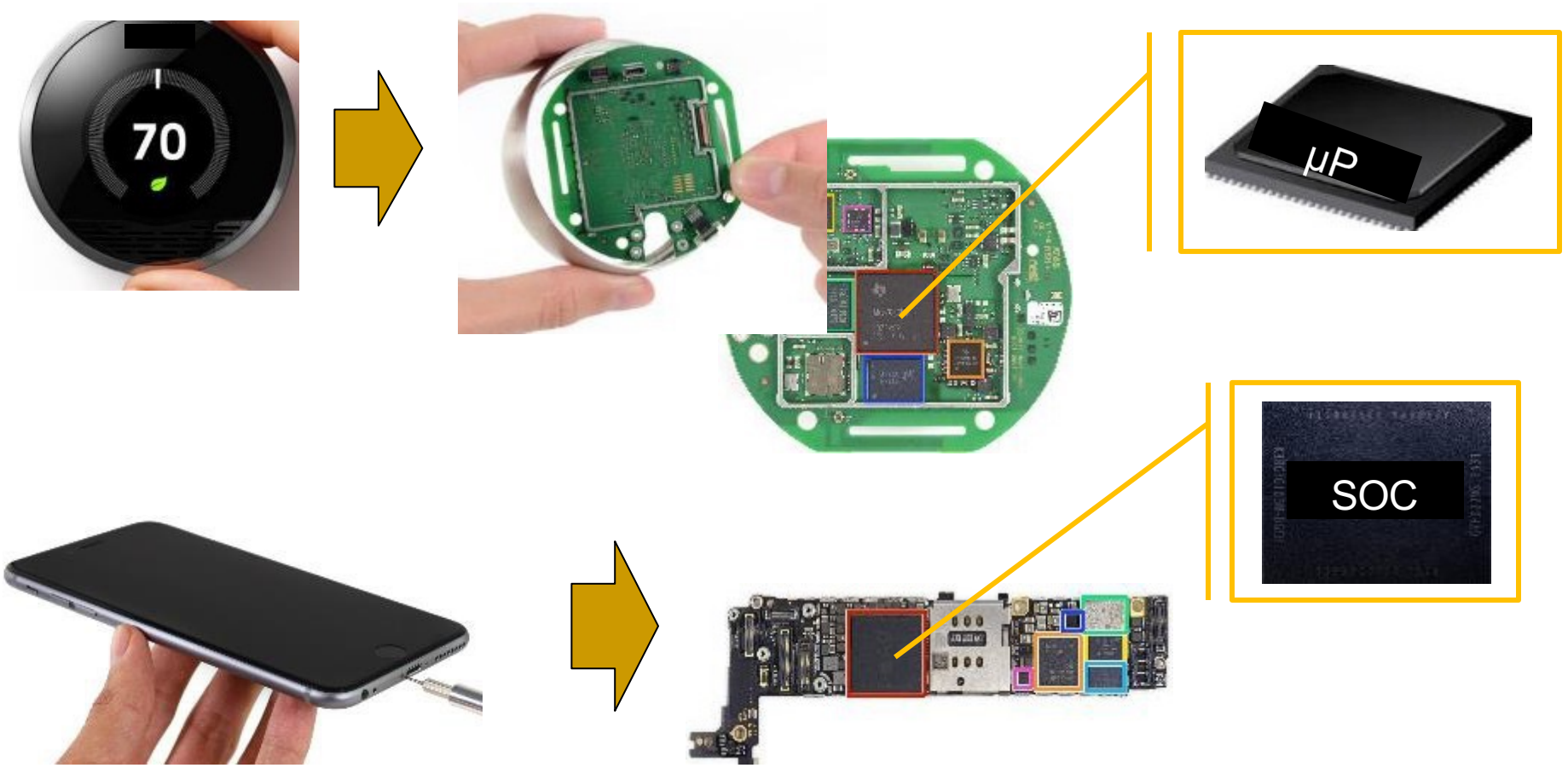




RFIDs

- 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 that are light enough to be suitable for the RFIDs?

What is Hardware?



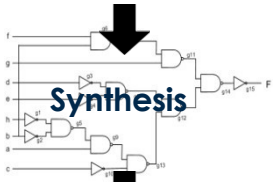
- Electronic System
- System Hardware – acts as the ***"root-of-trust"***: PCB → IC (SoC | μP)

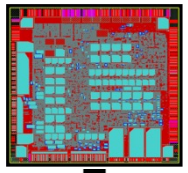
Evolution of Hardware Security and Trust

- Before 1996: Coating, encapsulation, labelling, taping, … still many companies don't spend much for securing their hardware
- 1996: Extracting secret keys using power analysis – started the side-channel signal analysis era
- 1998: Hardware unique ID
- 2002: Physically Unclonable Functions (PUFs), True Random Number Generation (TRNG), Hardware tagging
- 2004-2007: DARPA TRUST, Hardware trust
- 2008: DARPA IRIS Program – Reverse engineering, tampering, and reliability
- 2008: Counterfeit ICs
- More…

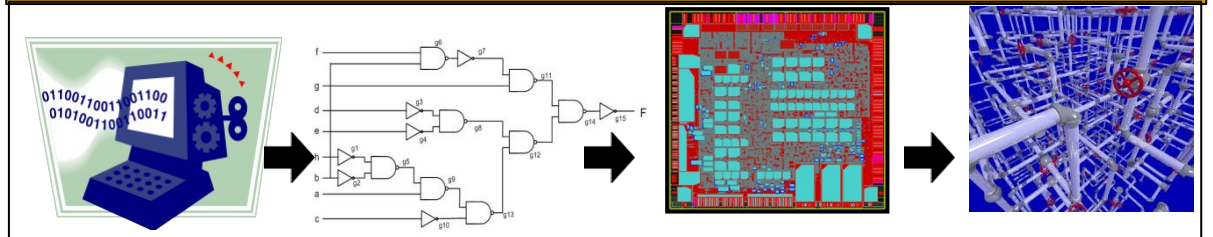
Shift in the Industry's Business Model

Vertical - one company





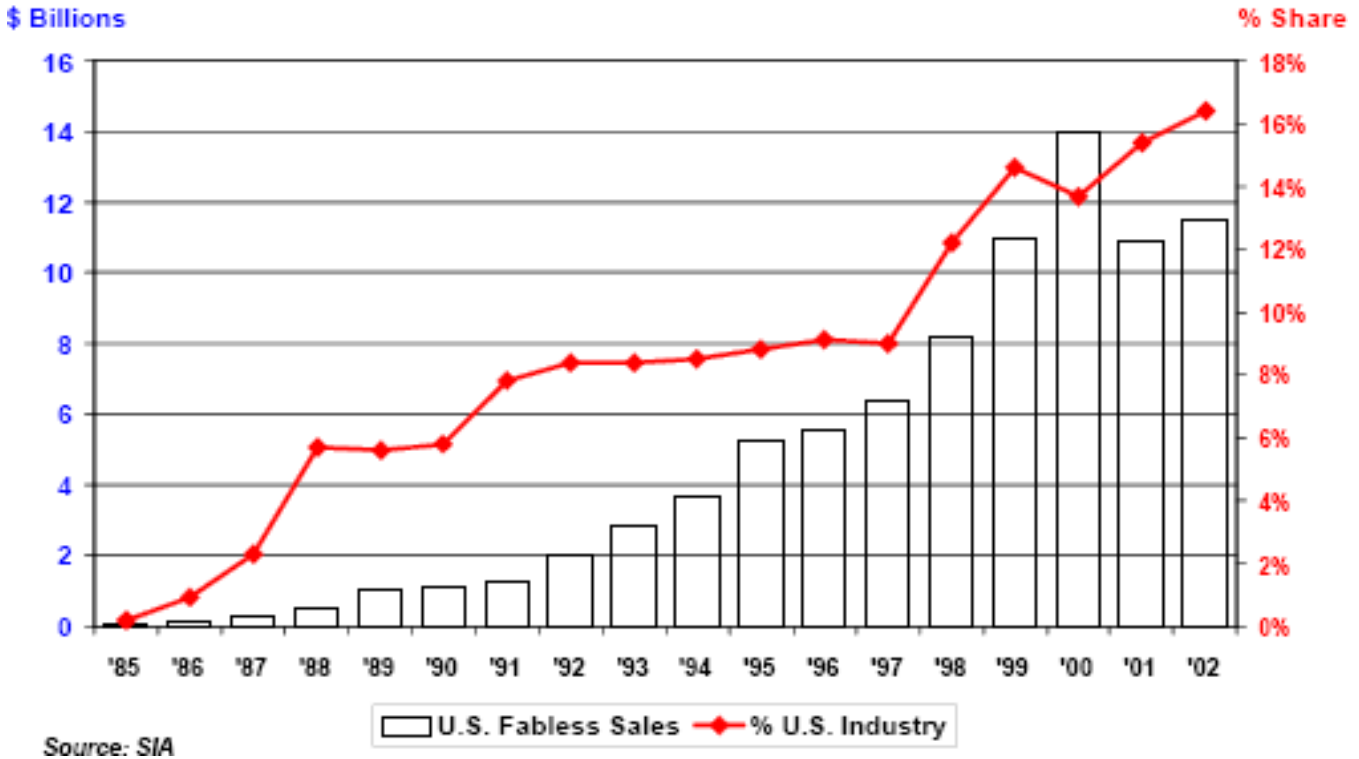
Horizontal (Dominant) – Two or more companies



Economy of scale: The same fabrication facility serves many fabless companies

Microelectronic Industry Business Model

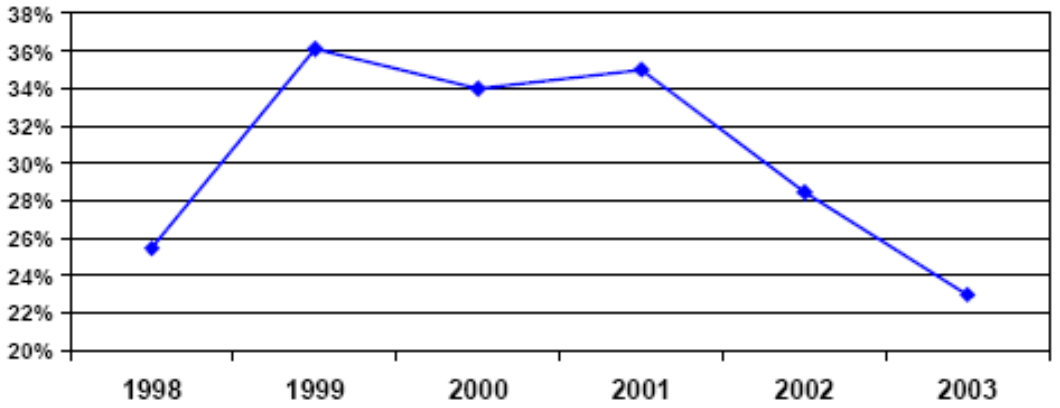
The fabless/foundry business model has grown to 16% of the U.S. chip industry. The trend is strongest in the leading process technology portion of the industry



Source: SIA

Leading-Edge Technology

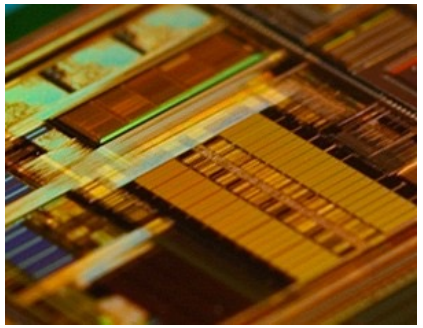
U.S. industry's share of capital expenditures falling and in leading edge semiconductor manufacturing capacity.

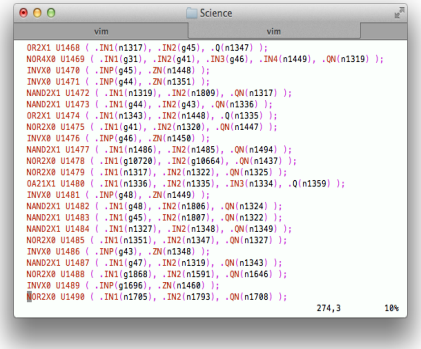


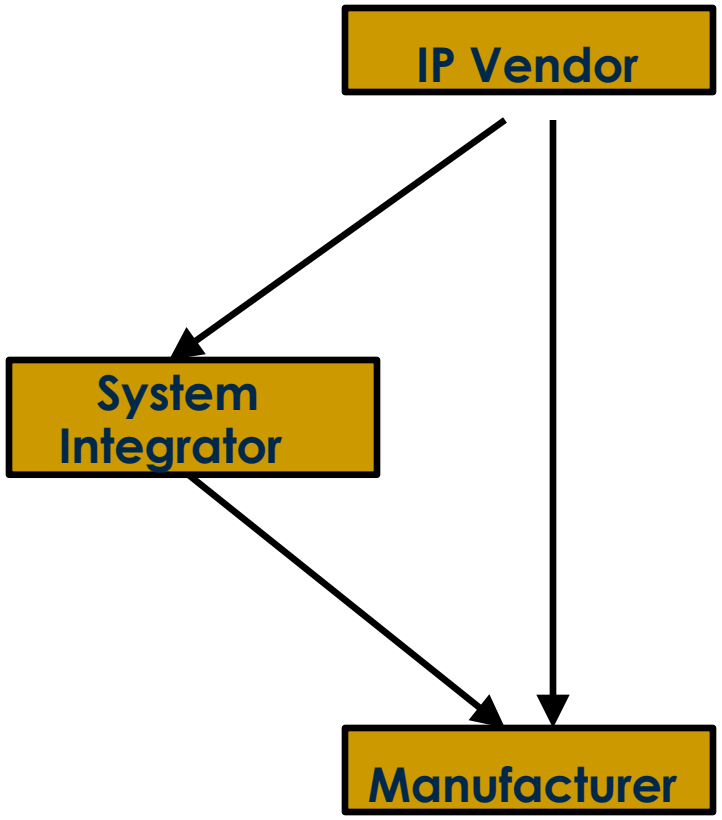
Source: SICAS/SIA

- The cost of building a full-scale, 300 mm wafer 65nm process chip fabrication plant is about $3bn

HW Threats

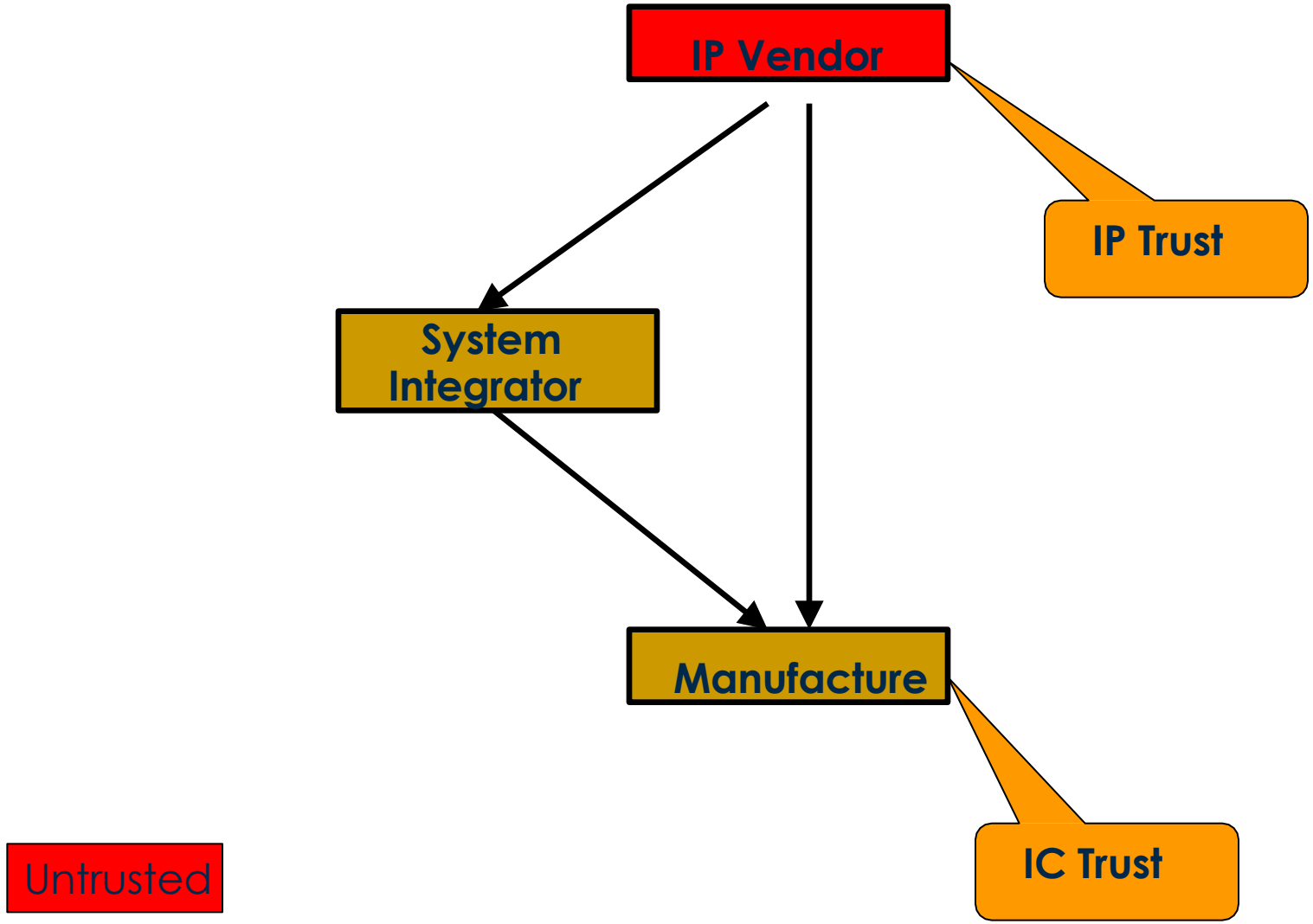




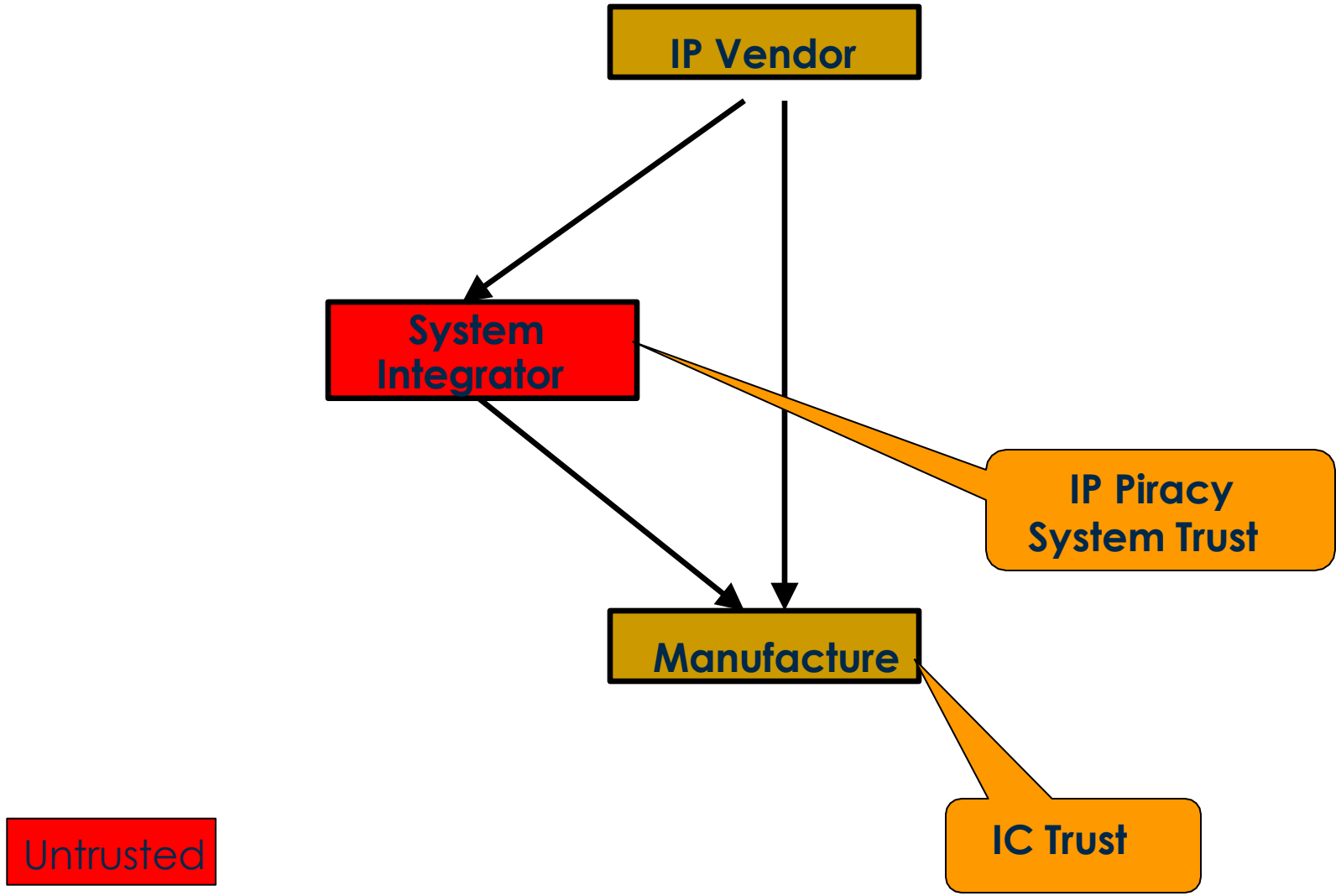


Any of these steps can be untrusted

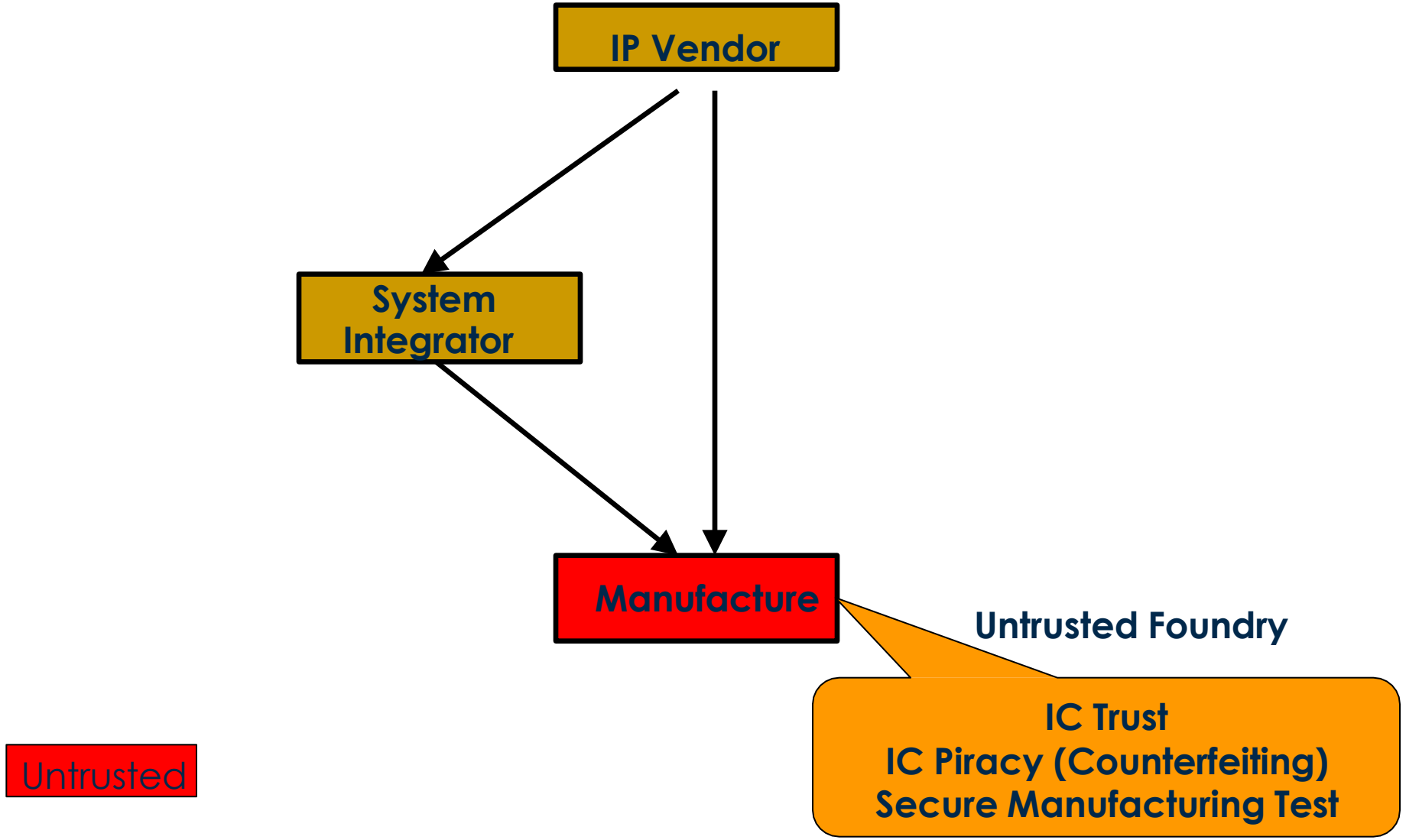
HW Threats


IP Vendor
IP Trust
System Integrator
Manufacture
IC Trust
Untrusted

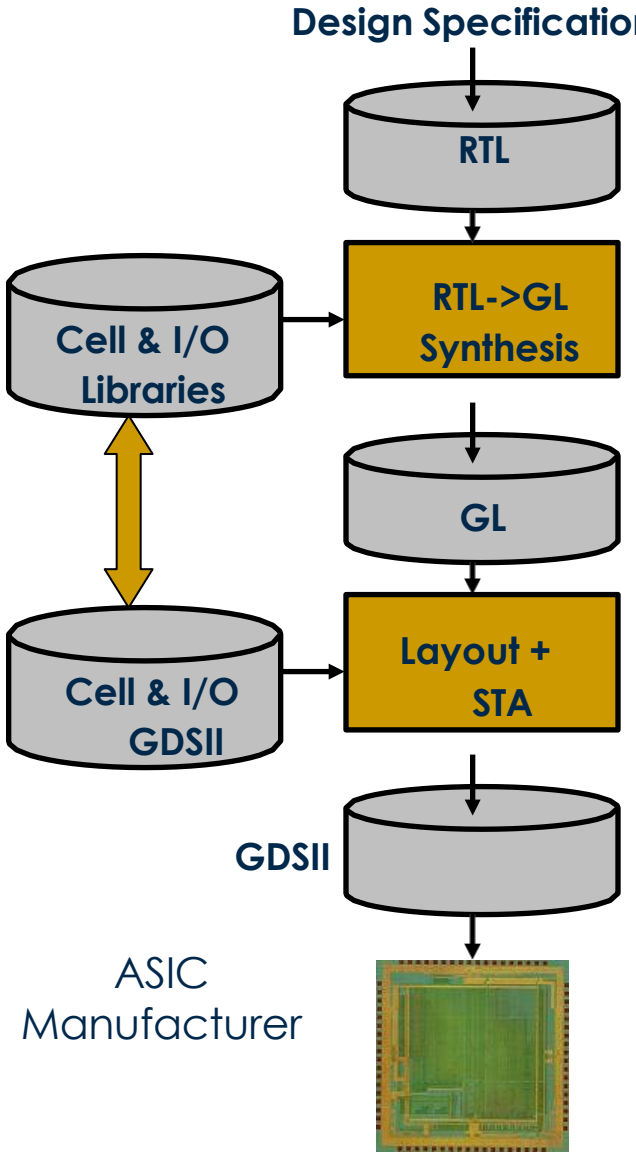
HW Threats


IP Vendor
System Integrator
IP Piracy
System Trust
Manufacture
IC Trust
Untrusted

HW Threats

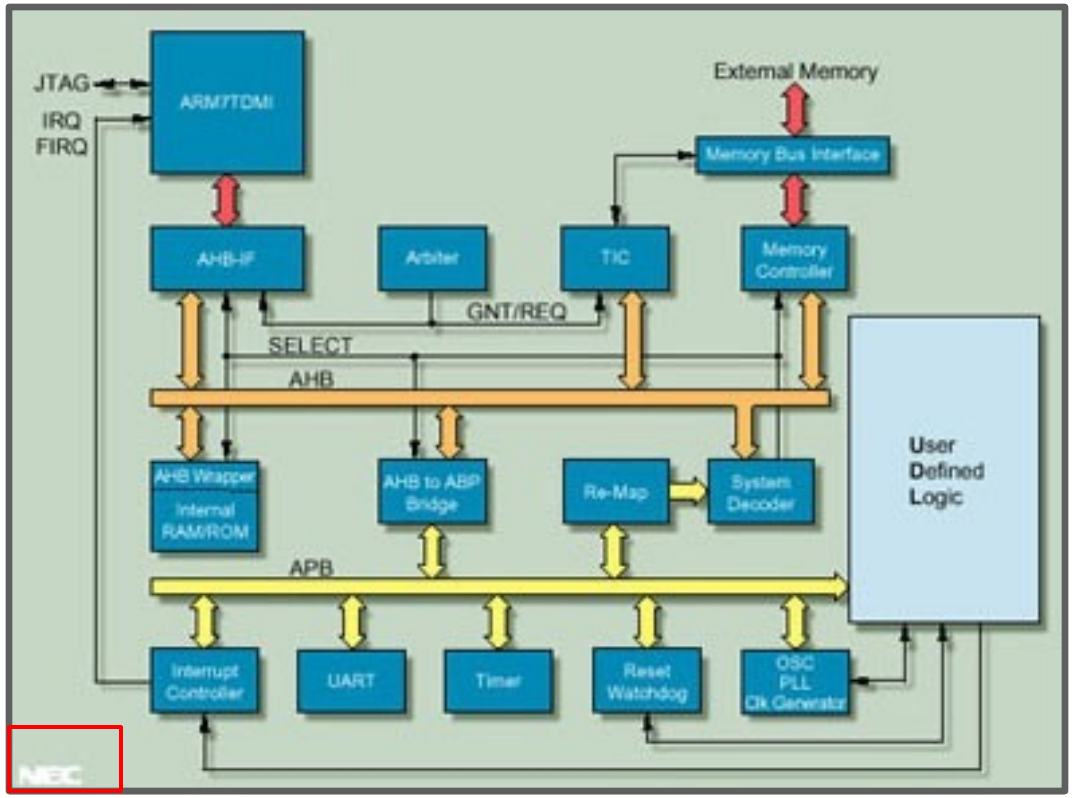

IP Vendor
System Integrator
Manufacture
Untrusted Foundry
IC Trust
IC Piracy (Counterfeiting)
Secure Manufacturing Test
Untrusted

Design Process – Old Way



Issues with Third-Party IP Design

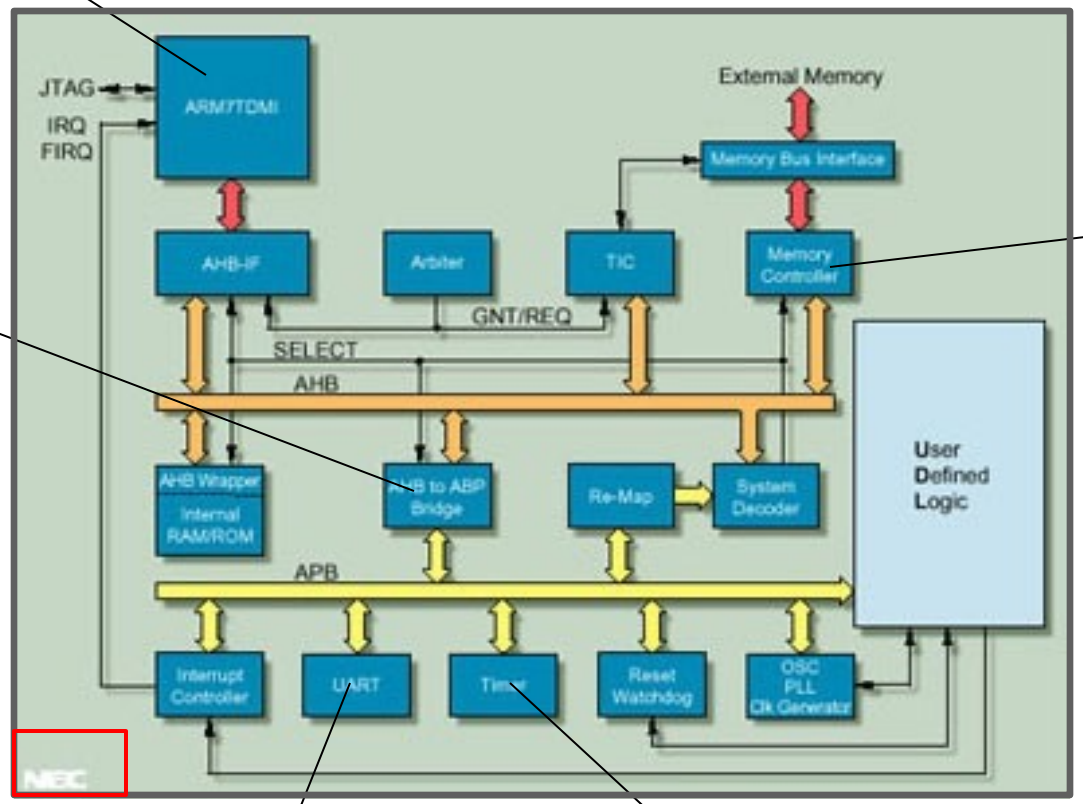
System-on-Chip (SoC)



Issues with Third-Party IP Design

Company X

System-on-Chip (SoC)



Company Y

Company Z

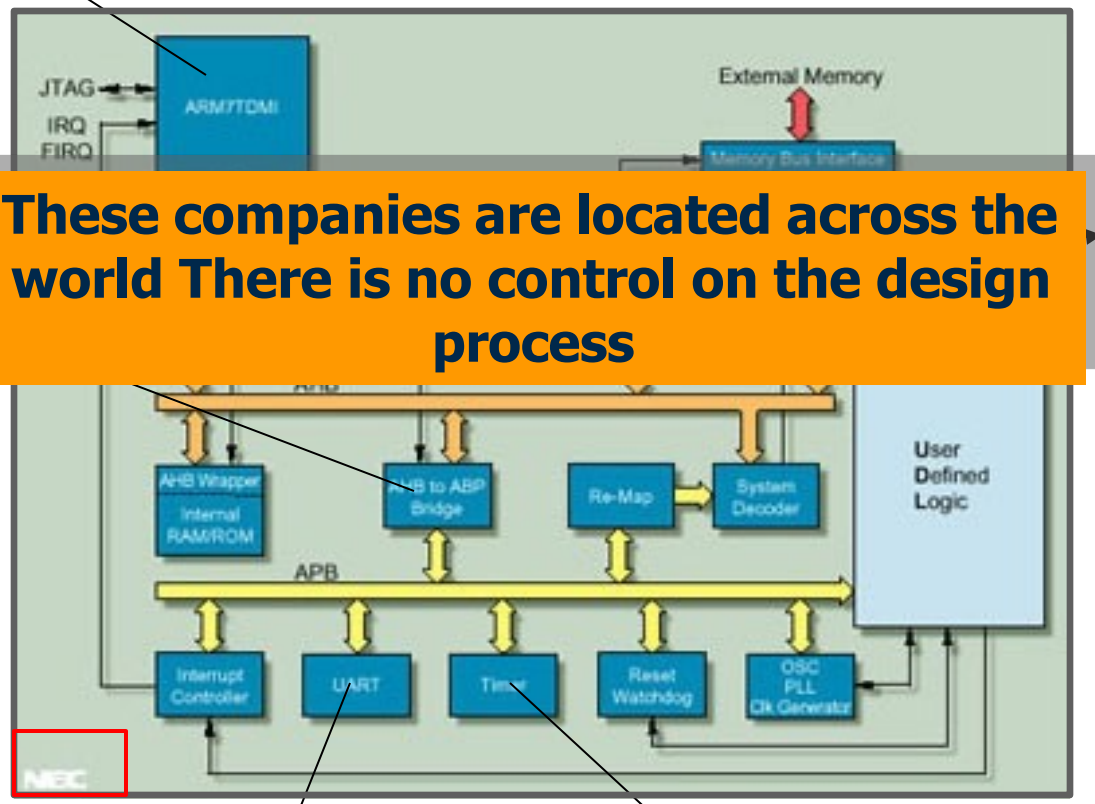
Company V

Company W

Issues with Third-Party IP Design

Company X

System-on-Chip (SoC)



These companies are located across the world There is no control on the design process

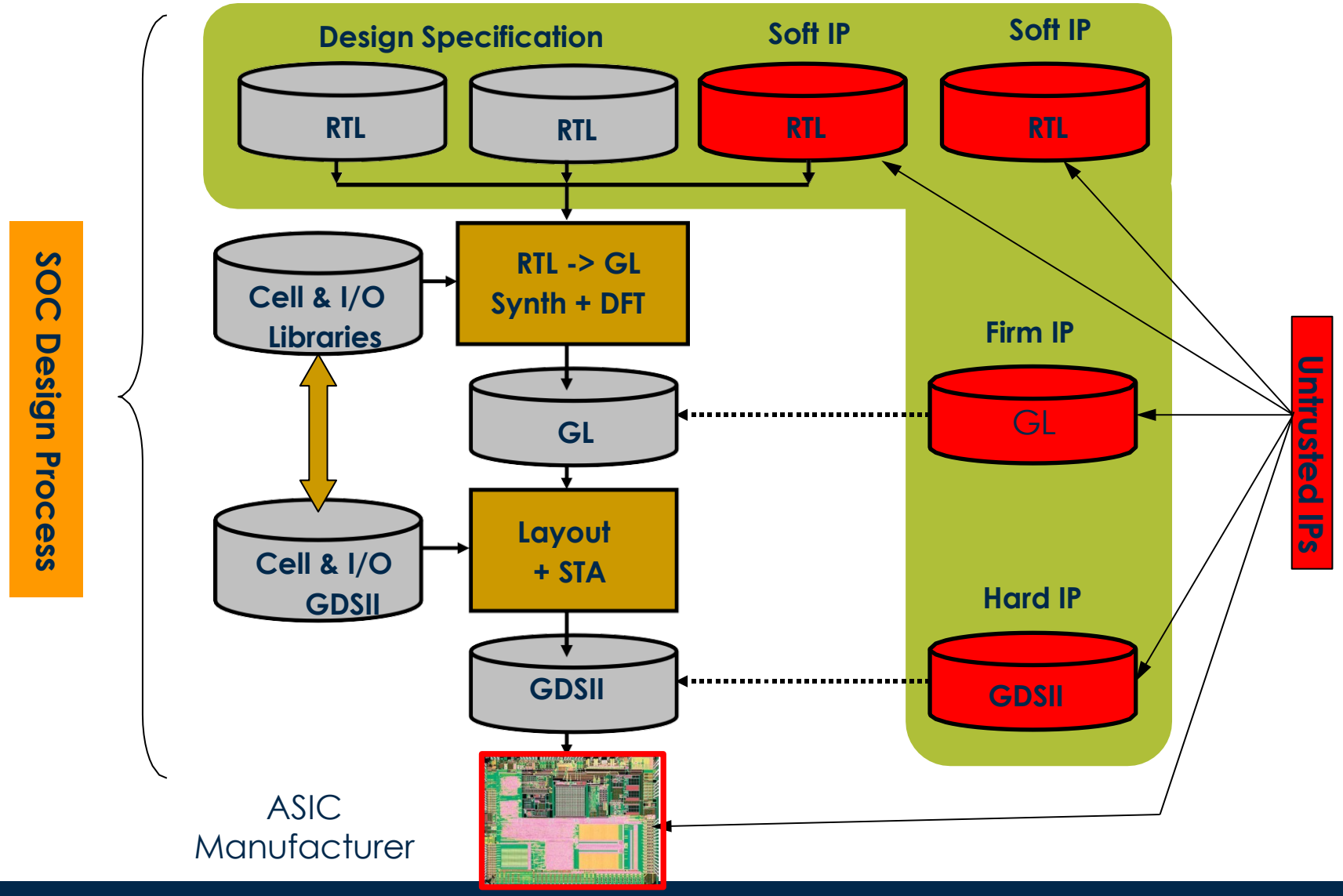
Company Y

Company Z

Company V

Company W

Design Process – New Way

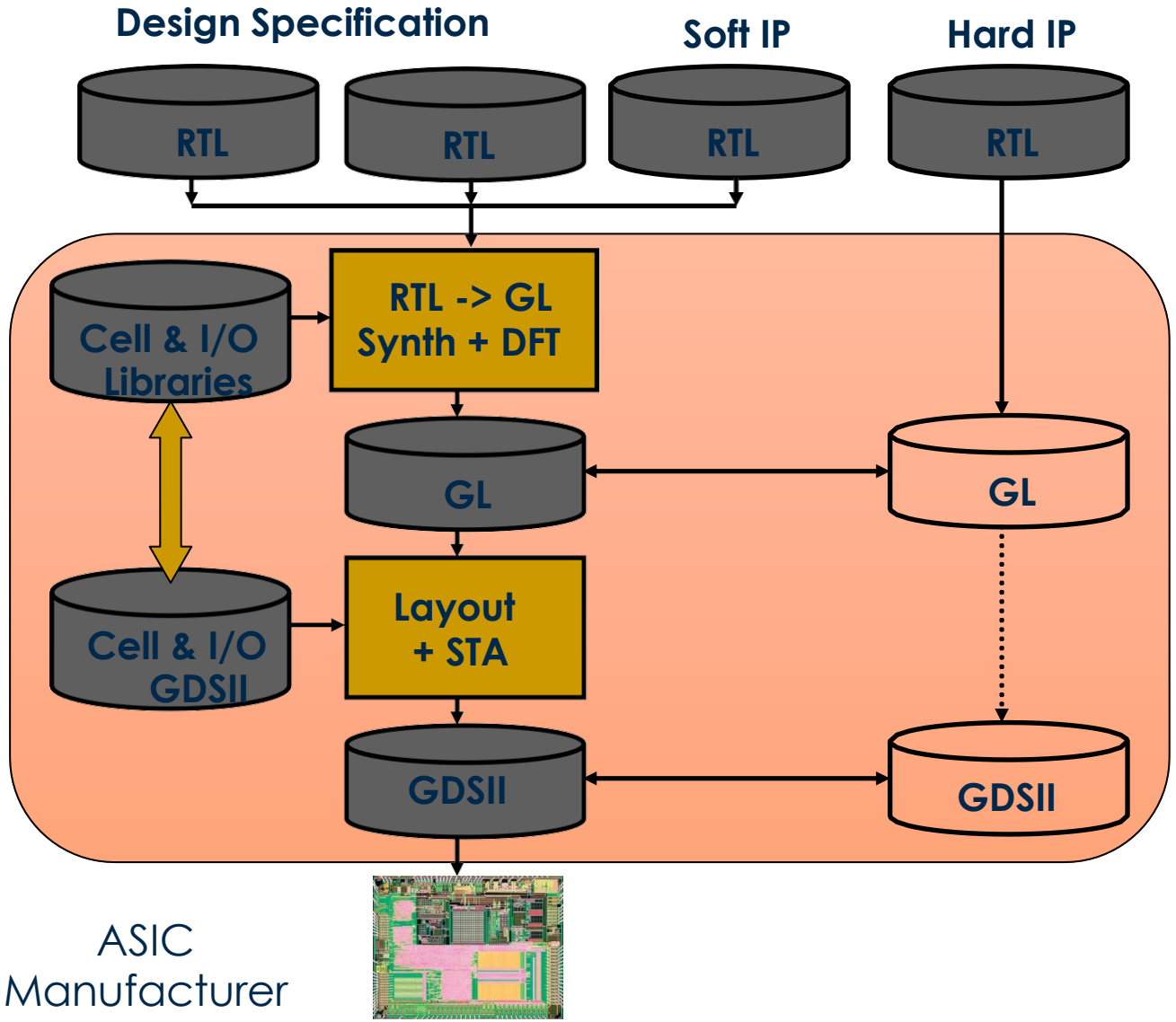


Who Develops the IPs? Who Designs the ICs? Who Fabricates Them?

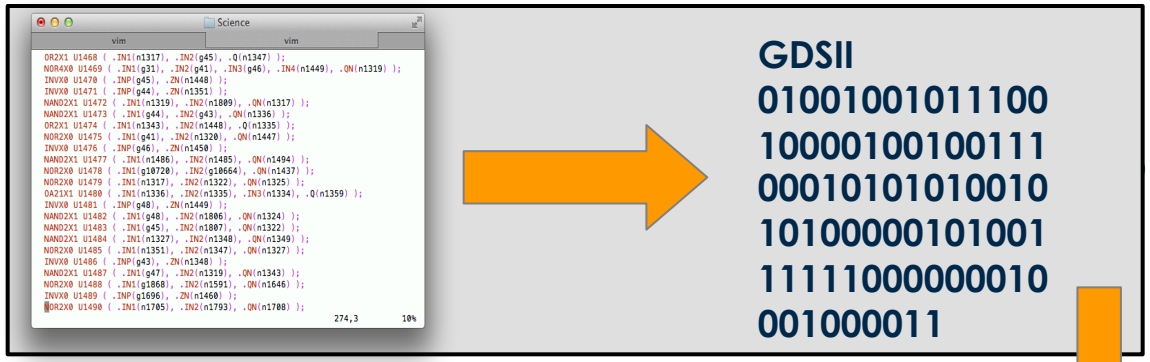
Who Develops the IPs? Who Designs the ICs? Who Fabricates Them?

Every Where!

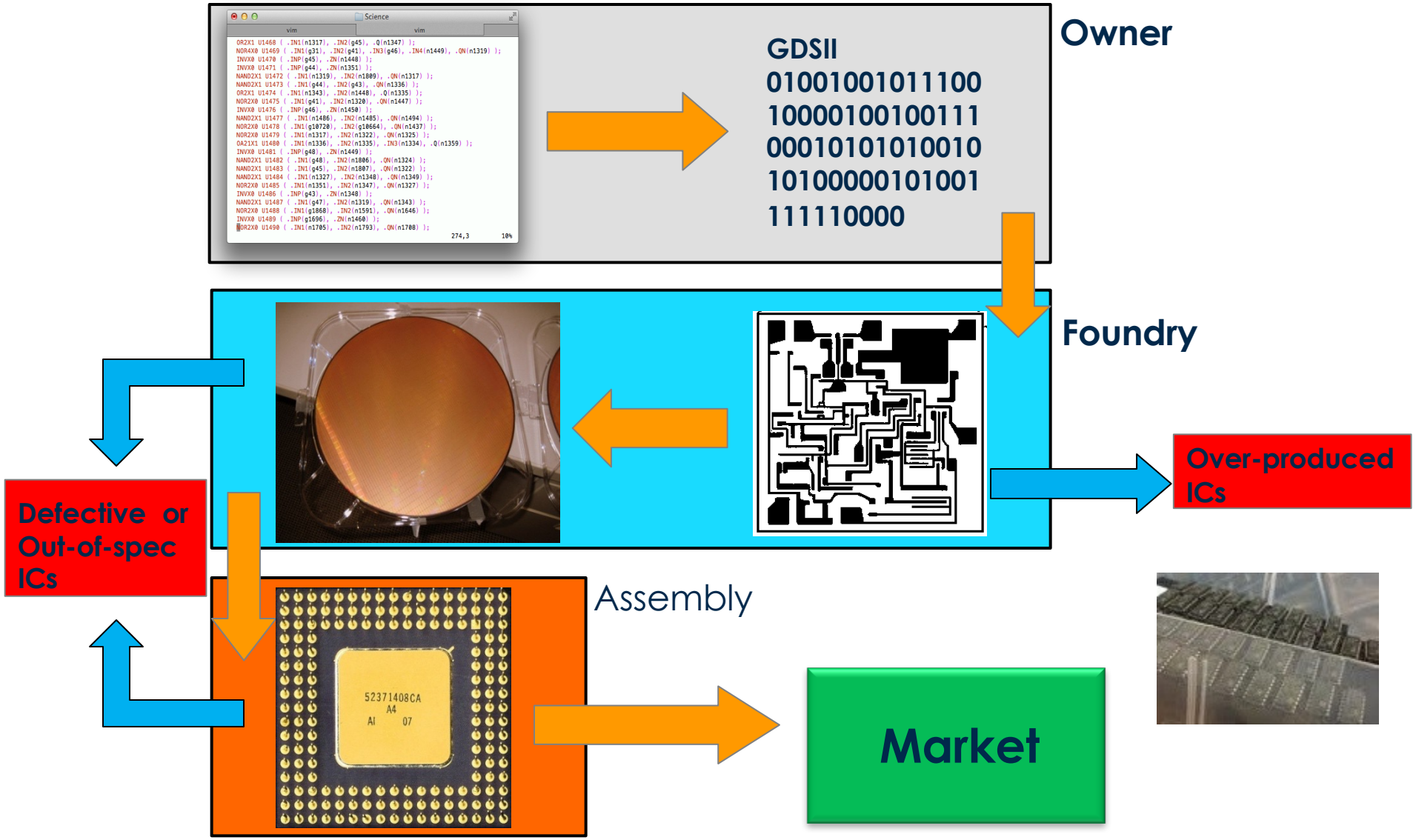
Untrusted System Integrator



Counterfeiting

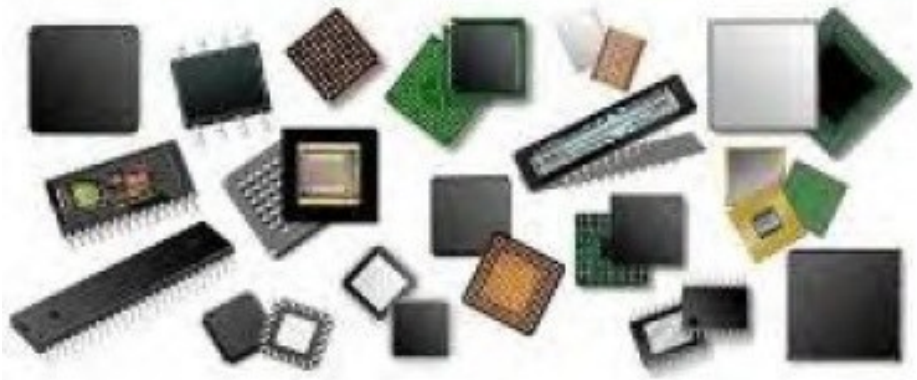


Counterfeiting



IC Counterfeiting

- Most prevalent attack today
- Unauthorized production of wafers
- It is estimated that counterfeiting is costing semiconductor industry more than several billion dollars per year



Over production

Off-spec parts

Recycled ICs

Defective parts

Cloned ICs

IC Recycling Process

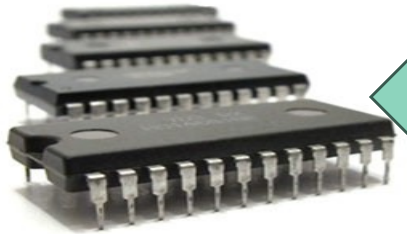
Recycling Center

PCB extracted

ICs extracted from PCBs

Refine ICs

Resold as new

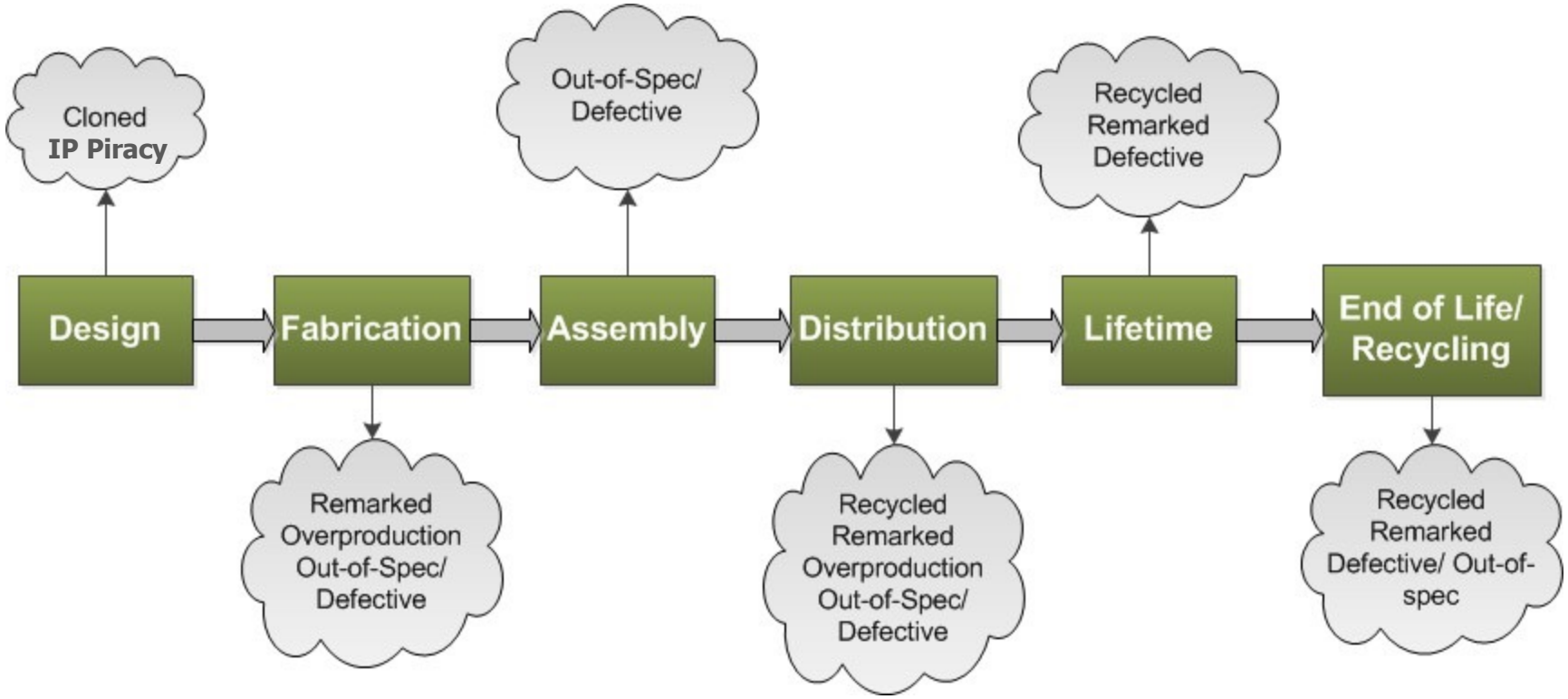


Identical:
Appearance, Function, Specification

Critical Application

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

Supply Chain Vulnerabilities



Some Basic Definitions

Intellectual property represents the property of your mind or intellect - proprietary knowledge

The four legally defined forms of IP

- **Patents**: When you register your invention with the government, you gain the legal right to exclude anyone else from manufacturing or marketing it
- **Trademarks**: A trademark is a name, phrase, sound, or symbol used in association with services or products
- **Copyrights**: Copyright laws protect written or artistic expressions fixed in a tangible medium
- **Trade** secrets: A formula, pattern, device, or compilation of data that grants the user an advantage over competitors

Politecnico di Torino

Security and Protection Objectives, Attacks

Overview

Definitions

- What does secure mean?
- Attacks
- Computer security
- Adversaries
- Methods of Defense

Security in embedded systems, design challenges

- "Secret" -- root of cryptography

What Does Secure Mean?

- It has to do with an asset with some value – think of what can be an asset!
- There is no static definition for “secure”
- It depends on what it is that you are protecting your asset from
- Protection may be sophisticated and unsophisticated
- Typically, a breach of one security makes the protection agent aware of its shortcomings

Typical Cycle in Securing a System

- Predict potential breaches and vulnerabilities
- Consider possible countermeasures or controls
- Either actively pursue identifying a new breach or wait for a breach to happen
- Identify the breach and work out a protected system again

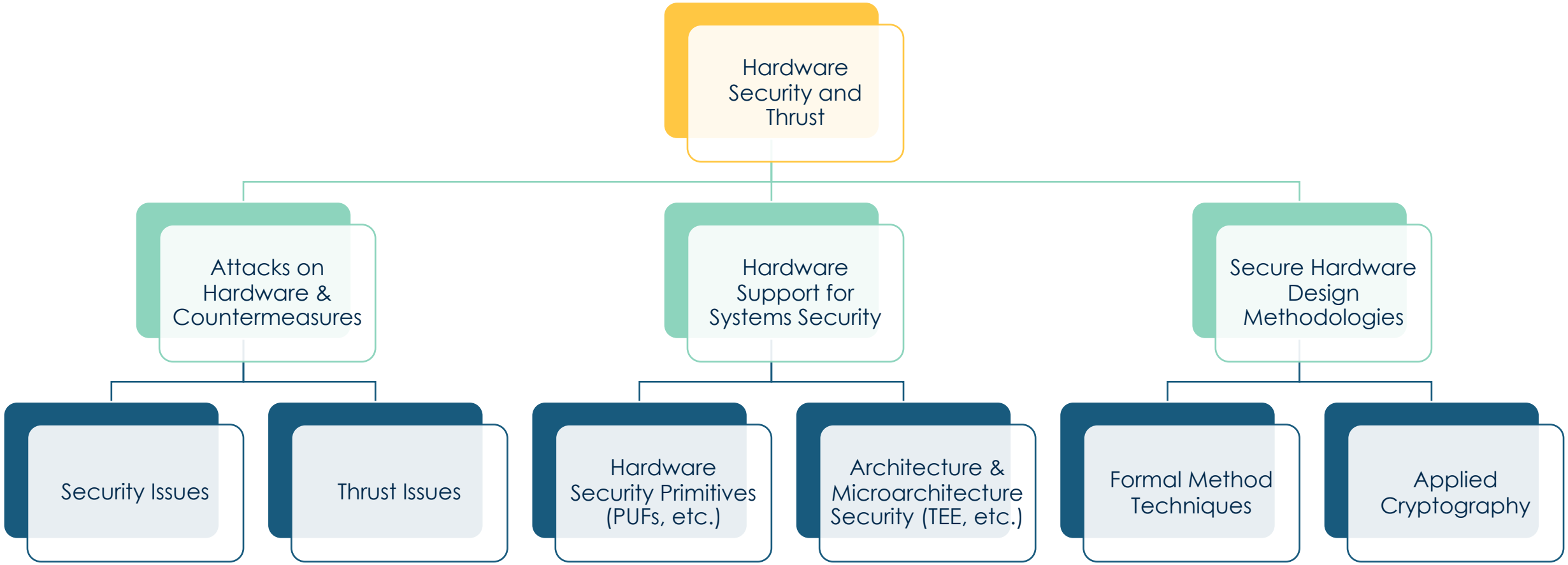
Computer Security

No matter how sophisticated the protection system is – simple breaches could break-in

A computing system is a collection of hardware (HW), software (SW), storage media, data, and humans interacting with them

- Security of SW, data, and communication
- HW security is important and challenging
  - Manufactured ICs are obscure
  - HW is the platform running SW, storage and data
  - Tampering can be conducted at many levels
  - Easy to modify because of its physical nature

Harware Security and Thrust



Definitions

- **Vulnerability**: Weakness in the secure system
- **Threat**: set of circumstances that has the potential to cause loss or harm
- **Attack**: The act of a human exploiting the vulnerability in the system
  - **Attack Surface**: the sum of all possible risk exposures.
- Computer security aspects
  - **Confidentiality**: the related assets are only accessed by authorized parties
  - **Integrity**: the asset is only modified by authorized parties
  - **Availability**: the asset is accessible to authorized parties at appropriate times

Hardware Vulnerabilities

- Physical Attacks
- Trojan Horses
- IP Piracy
- IC Piracy & Counterfeiting
- Backdoors
- Tampering
- Reverse Engineering

Adversaries

Individuals, groups, or governments
- Pirating the IPs – illegal use of IPs
- Inserting backdoors or malicious circuitries
- Implementing Trojan horses
- Reverse engineering of ICs
- Spying by exploiting IC vulnerabilities

System integrators
- Pirating the IPs

Fabrication facilities
- Pirating the IPs
- Pirating the ICs

Counterfeiting parties
- Recycling, cloning, etc.

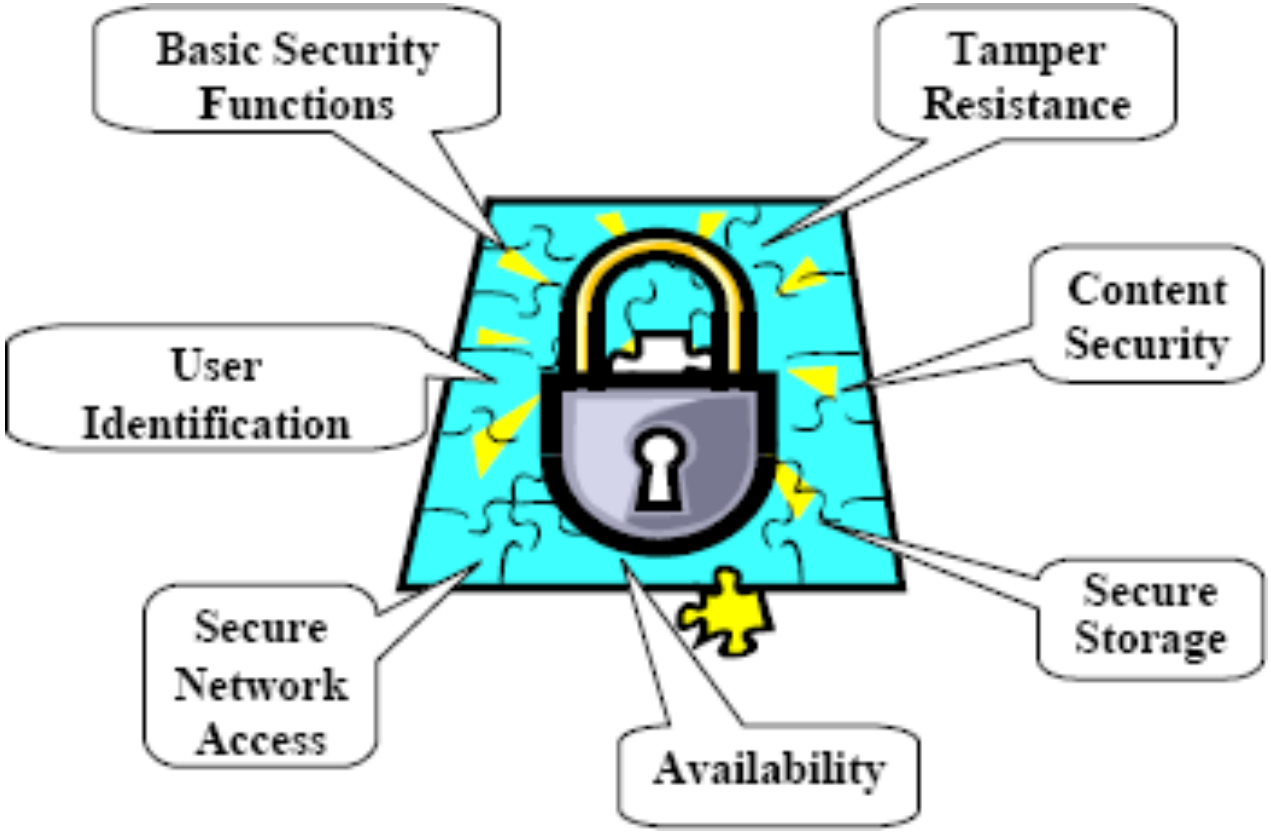
Hardware Controls for Secure Systems

- Hardware implementations of encryption
  - Encryption has to do with scrambling to hide
- Design locks or physical locks limiting access
- Devices to verify the user identities
- Hiding signatures in the design files
- Intrusion detection
- Hardware boards limiting memory access
- Tamper-resistant
- Policies and procedures
- More …

Embedded Systems Security

- Security processing adds overhead
  - Performance and power
- Security is challenging in embedded systems
    - Size and power constraints and operation in harsh environments
- Security processing may easily overwhelm the other aspects of the system
- Security has become a new design challenge that must be considered at the design time, along with other metrics, i.e., cost, power, area

Security Requirements in the IoT Era



Secure Embedded Systems - Design Challenges

- Processing gap
- Battery gap
- Flexibility
  - Multiple security objectives
  - Interoperability in different environments
  - Security processing in different layers
- Tamper resistance
- Assurance gap
- Cost

Secret

Underlying most security mechanisms or protocols is the notion of a “secret”

- Lock and keys
- Passwords
- Hidden signs and procedures
- Physically hidden