Introduction to Hardware Security

Trey Austin Yifan Clare

Chris Max Jack Will Michael

Andrew

Engr 399/599: Hardware Security
Andrew Lukefahr
Indiana University

Adapted from: Mark Tehranipoor of University of Florida

Course Website

engr599.github.io

Passcode:

Room

2-3-5

Write that down!

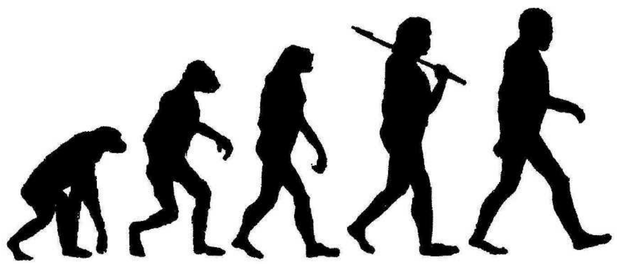
Why Hardware Security?

- ***Cybersecurity experts have traditionally assumed that the hardware underlying information systems is secure and trusted.***

- ***Such assumptions are not true.***

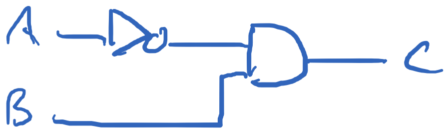
Evolution of Hardware Security and Trust

- **Prior to 1996:** Coating, encapsulation, labeling, 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
- **2012**: Senate Armed Services – National Defense Authorization Act (NDAA) 2012
- **2014**: DARPA SHIELD – Supply chain security
- **2015**: DARPA LADS
- More…



```
assign c = ~a & b;
```

Old Hardware Business Model



TI

design

synthesis

place/route

Intel

design (verilog)

↓

sythisis (netlist)

↓

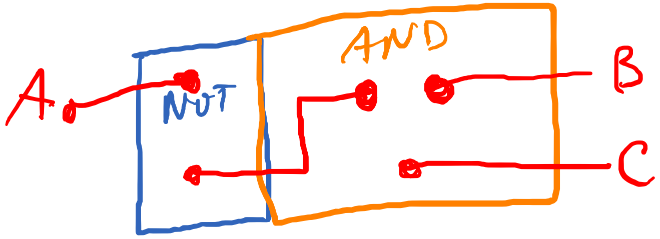
place/route

↓

factory/foundry

↓

Chip



Cutting-Edge foundries

TSMC

Samsung

Intel

New Hardware Business Model

Nvidia – fabless - semiconductor

Design of graphics (US)

Micron DDR4 controller (Germany)

Synopsys PCI-E Interface (Brazil)

↓

synthesis (US)

↓

place/Route (India)

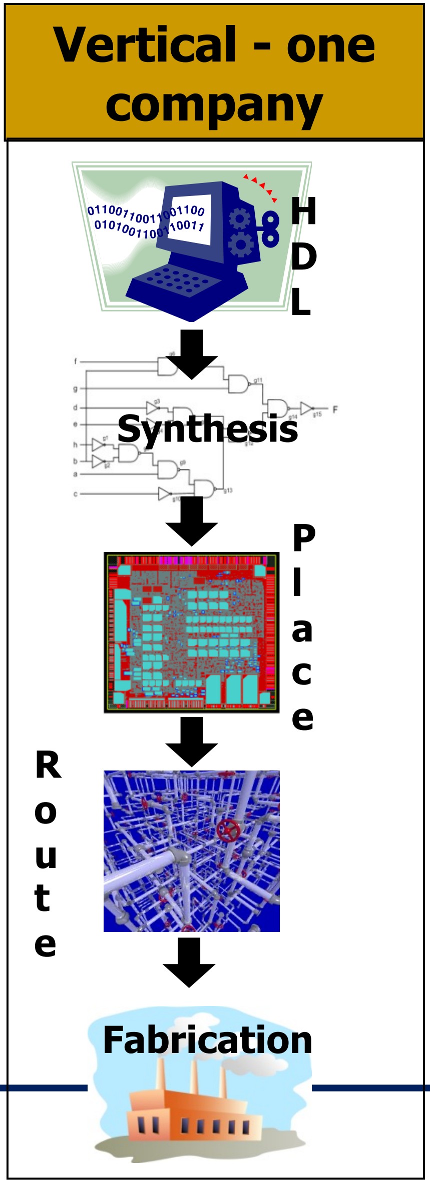
↓

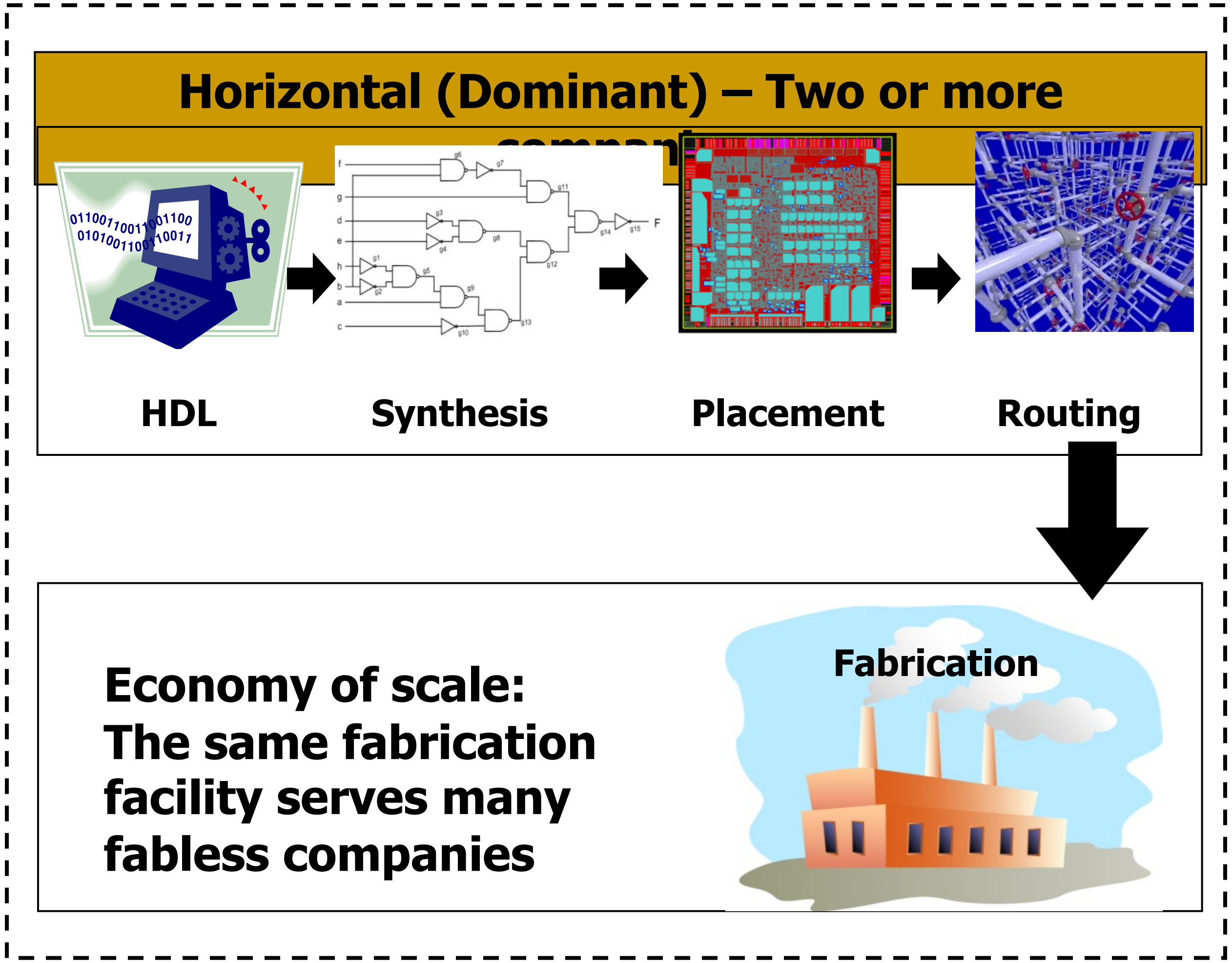
TSMC (Taiwan)

↓

Chip → Test (Singapoor) → Me!

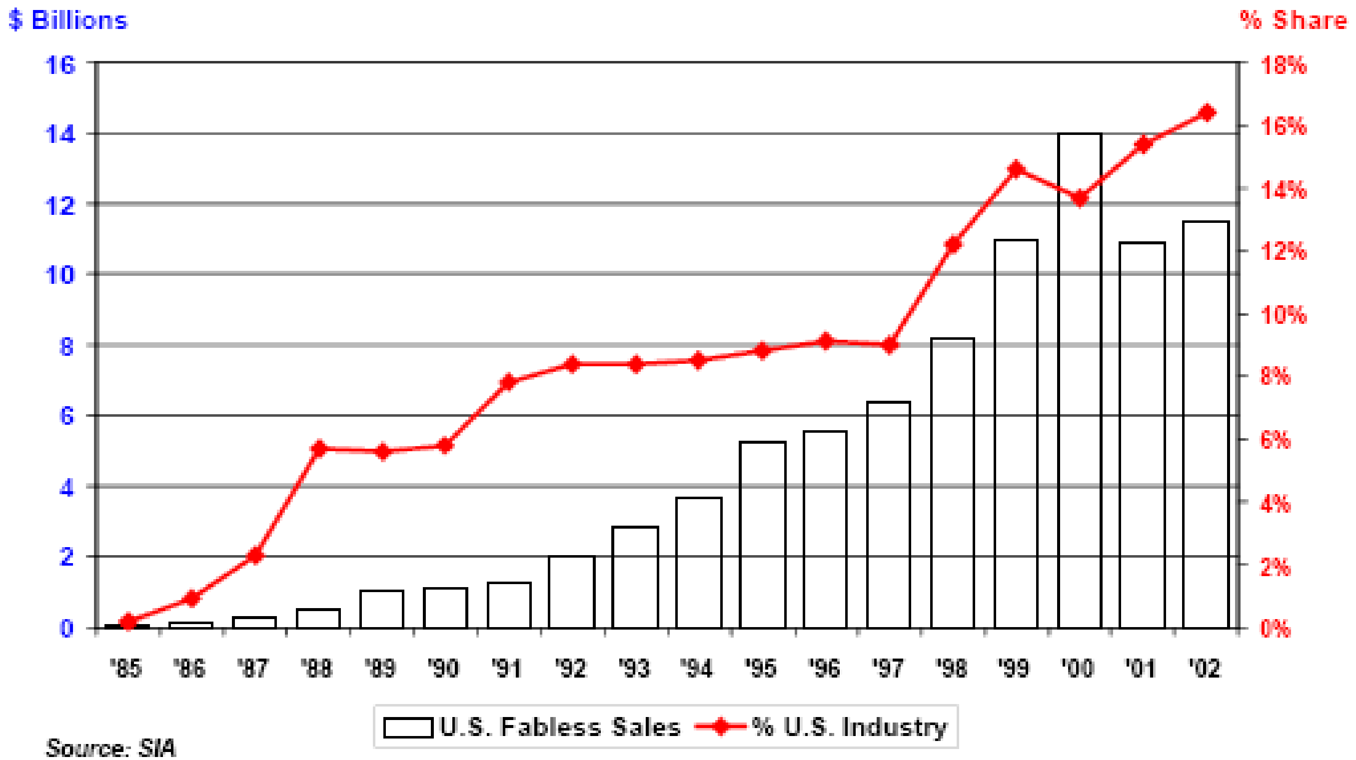
Shift in the Industry’s Business Model





Microelectronic Industry Business Model

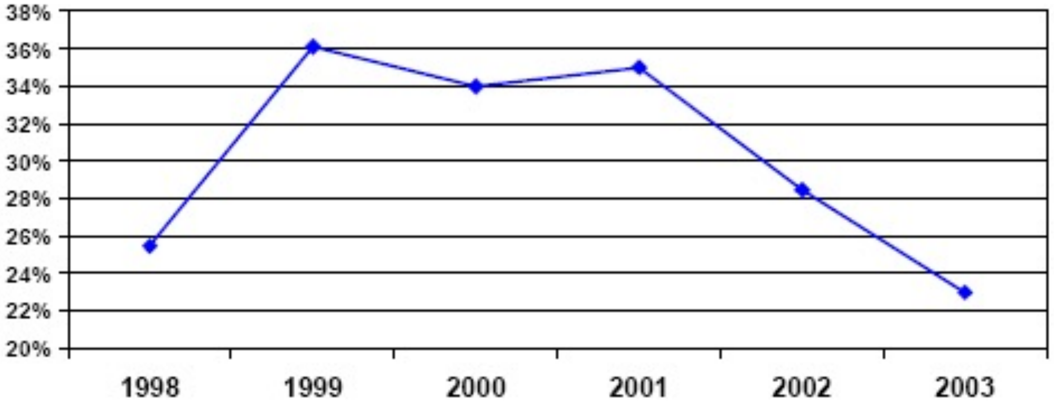
The fabless/foundry business model has grown to 16% of the U.S. chip industry. The trend is strongest in the leading process technology portion of the industry



Source: SIA

Leading-Edge Technology

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

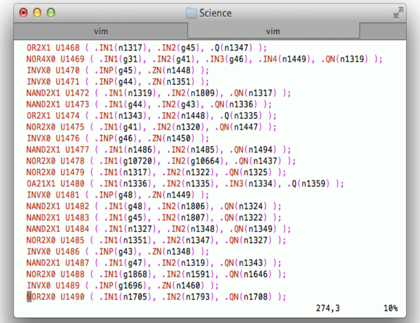


Leading Edge	< 0.4μ	< 0.3μ	< 0.3μ	< 0.2μ	< 0.2μ	< 0.16μ

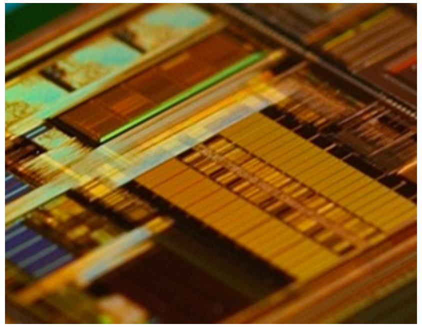
Source: SICAS/SIA

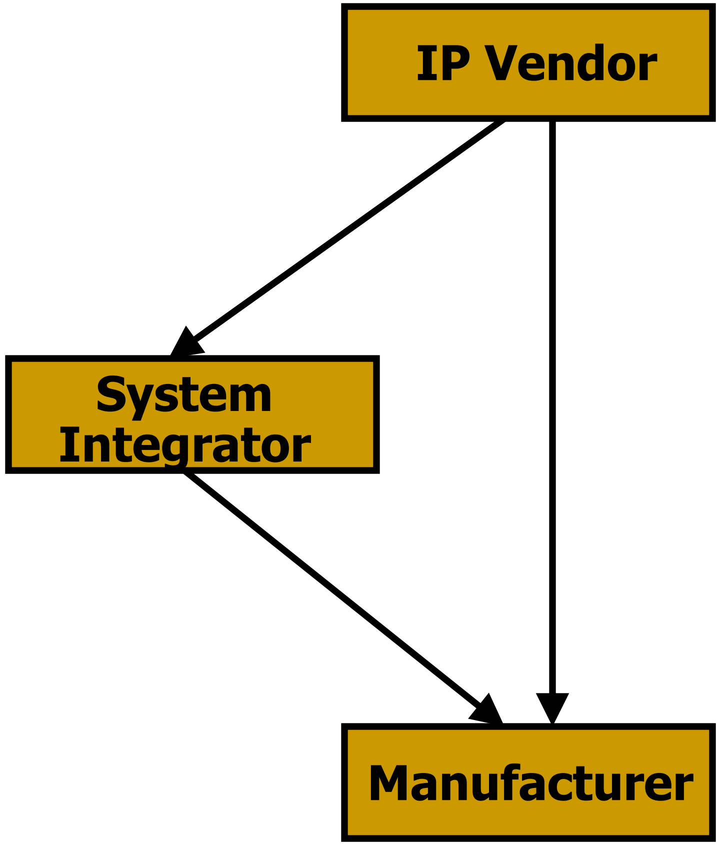
- The cost of building a full-scale, 300 mm wafer 65nm process chip fabrication plant is about $3bn

HW Threats


Science
vim
vim

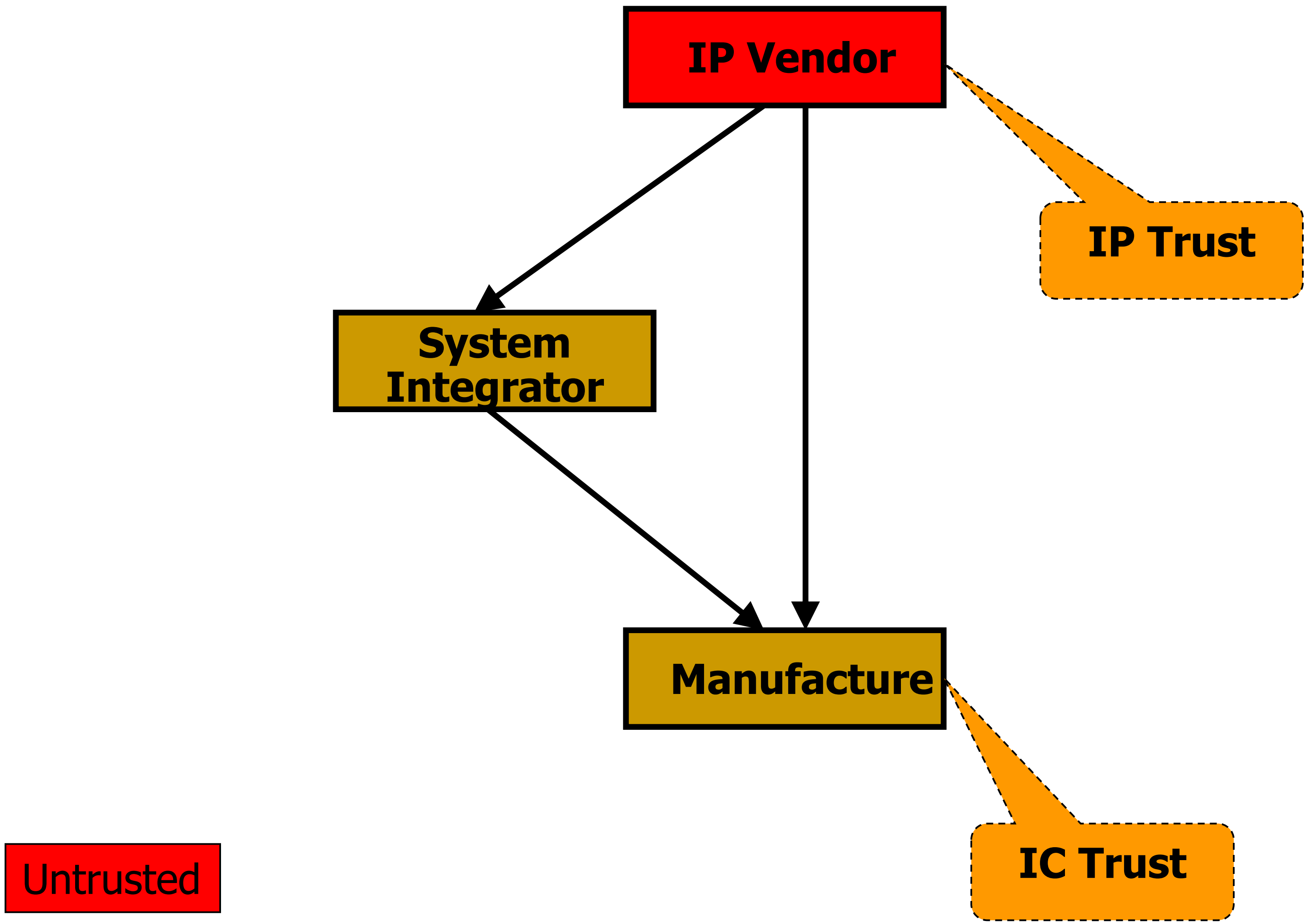
```
OR2X1 U1468 ( .IN1(n1317), .IN2(g45), .Q(n1347) );
NOR4X0 U1469 ( .IN1(g31), .IN2(g41), .IN3(g46), .IN4(n1449), .QN(n1319) );
INVX0 U1470 ( .INP(g45), .ZN(n1448) );
INVX0 U1471 ( .INP(g44), .ZN(n1351) );
NAND2X1 U1472 ( .IN1(n1319), .IN2(n1809), .QN(n1317) );
NAND2X1 U1473 ( .IN1(g44), .IN2(g43), .QN(n1336) );
OR2X1 U1474 ( .IN1(n1343), .IN2(n1448), .Q(n1335) );
NOR2X0 U1475 ( .IN1(g41), .IN2(n1320), .QN(n1447) );
INVX0 U1476 ( .INP(g46), .ZN(n1450) );
NAND2X1 U1477 ( .IN1(n1486), .IN2(n1485), .QN(n1494) );
NOR2X0 U1478 ( .IN1(g10720), .IN2(g10664), .QN(n1437) );
NOR2X0 U1479 ( .IN1(n1317), .IN2(n1322), .QN(n1325) );
OA21X1 U1480 ( .IN1(n1336), .IN2(n1335), .IN3(n1334), .Q(n1359) );
INVX0 U1481 ( .INP(g48), .ZN(n1449) );
NAND2X1 U1482 ( .IN1(g48), .IN2(n1806), .QN(n1324) );
NAND2X1 U1483 ( .IN1(g45), .IN2(n1807), .QN(n1322) );
NAND2X1 U1484 ( .IN1(n1327), .IN2(n1348), .QN(n1349) );
NOR2X0 U1485 ( .IN1(n1351), .IN2(n1347), .QN(n1327) );
INVX0 U1486 ( .INP(g43), .ZN(n1348) );
NAND2X1 U1487 ( .IN1(g47), .IN2(n1319), .QN(n1343) );
NOR2X0 U1488 ( .IN1(g1868), .IN2(n1591), .QN(n1646) );
INVX0 U1489 ( .INP(g1696), .ZN(n1460) );
NOR2X0 U1490 ( .IN1(n1705), .IN2(n1793), .QN(n1708) );
                                        274,3      10%
```



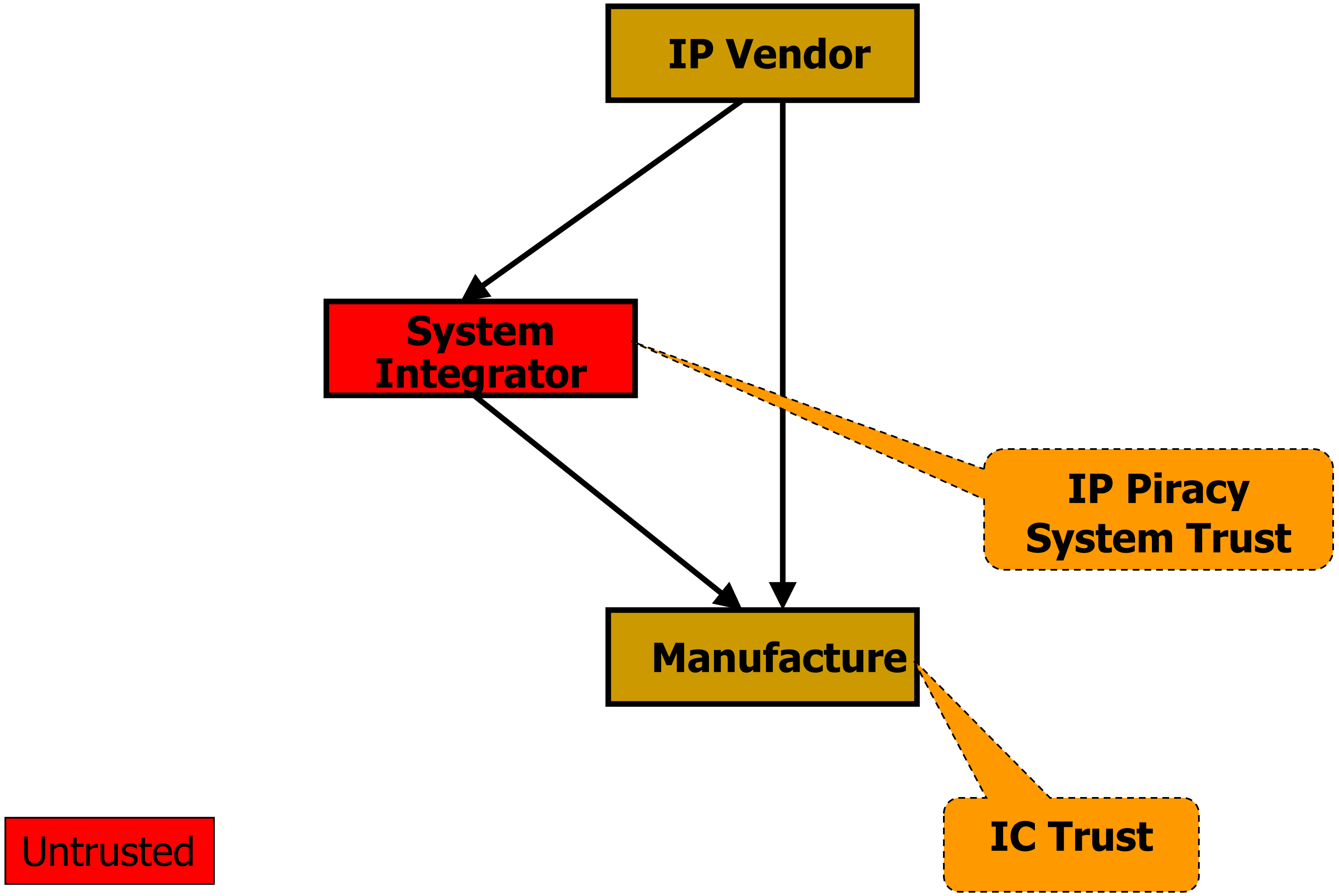


Any of these steps can be untrusted

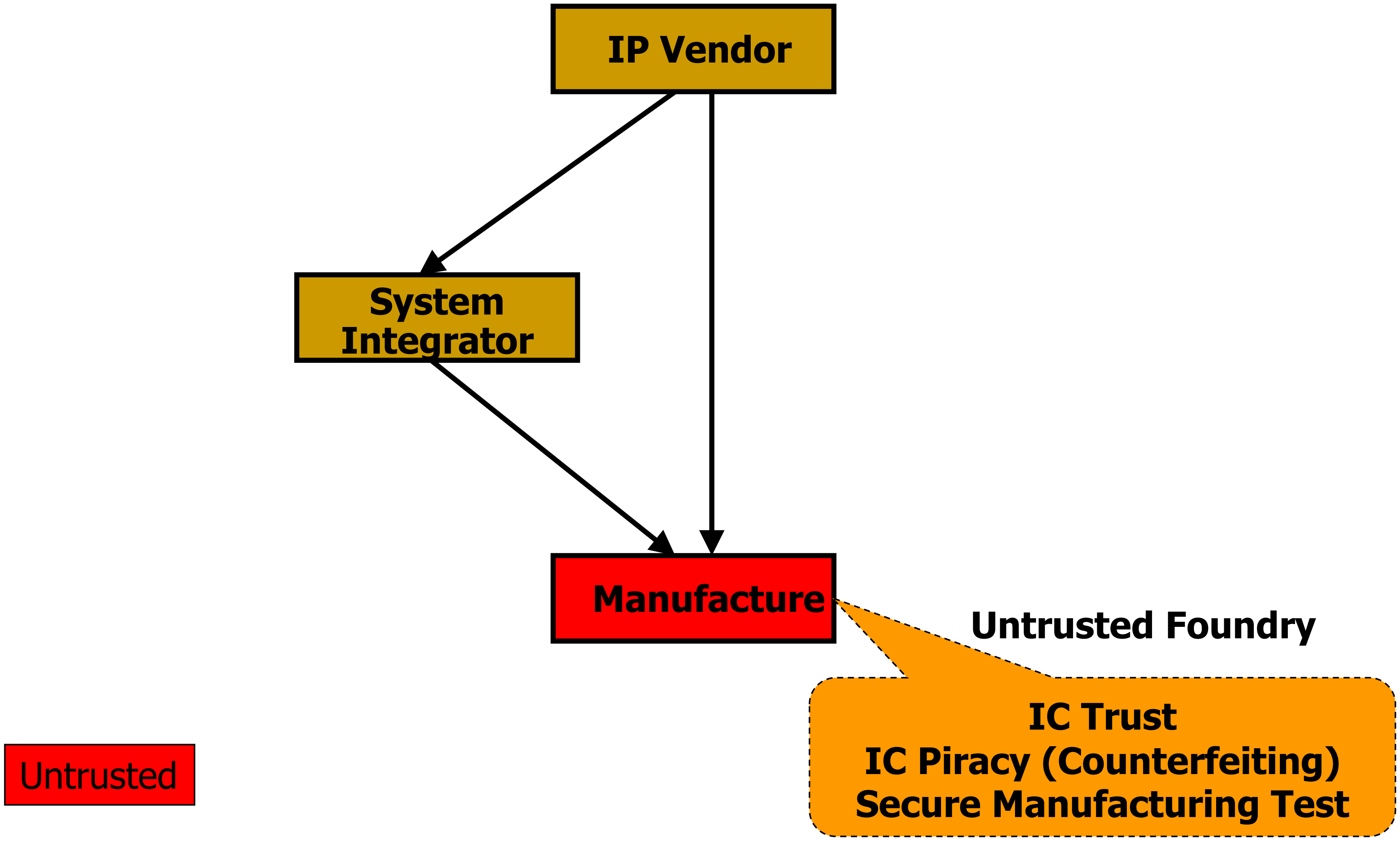
HW Threats


IP Vendor
IP Trust
System Integrator
Manufacture
IC Trust
Untrusted

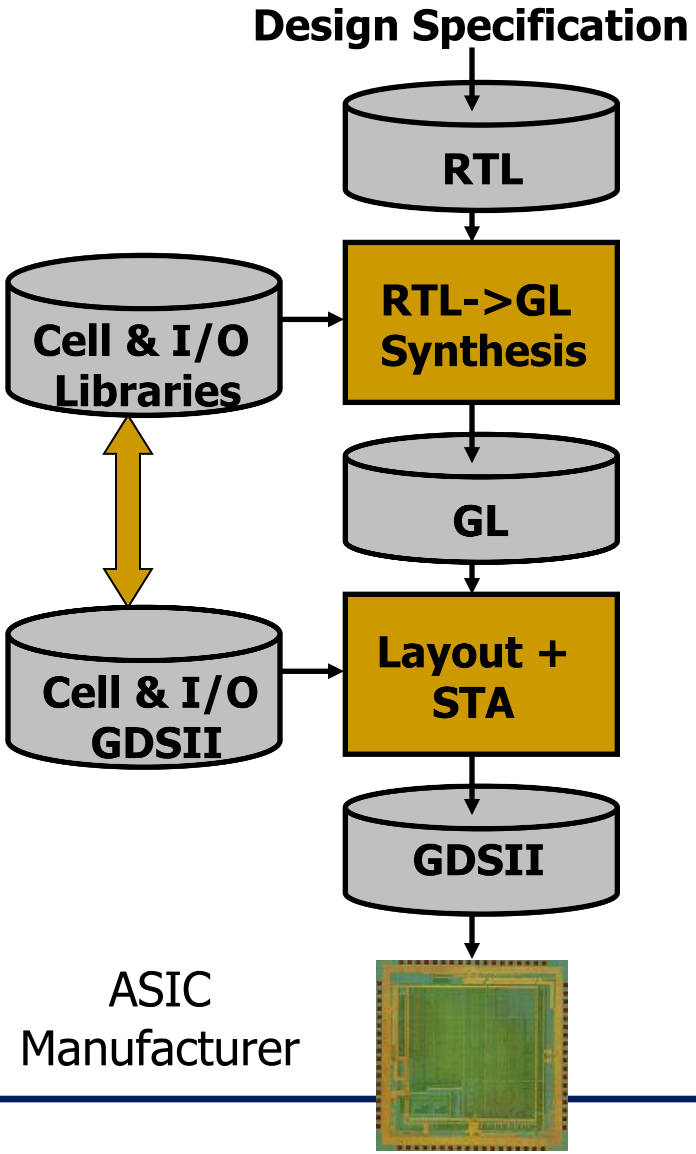
HW Threats


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

HW Threats

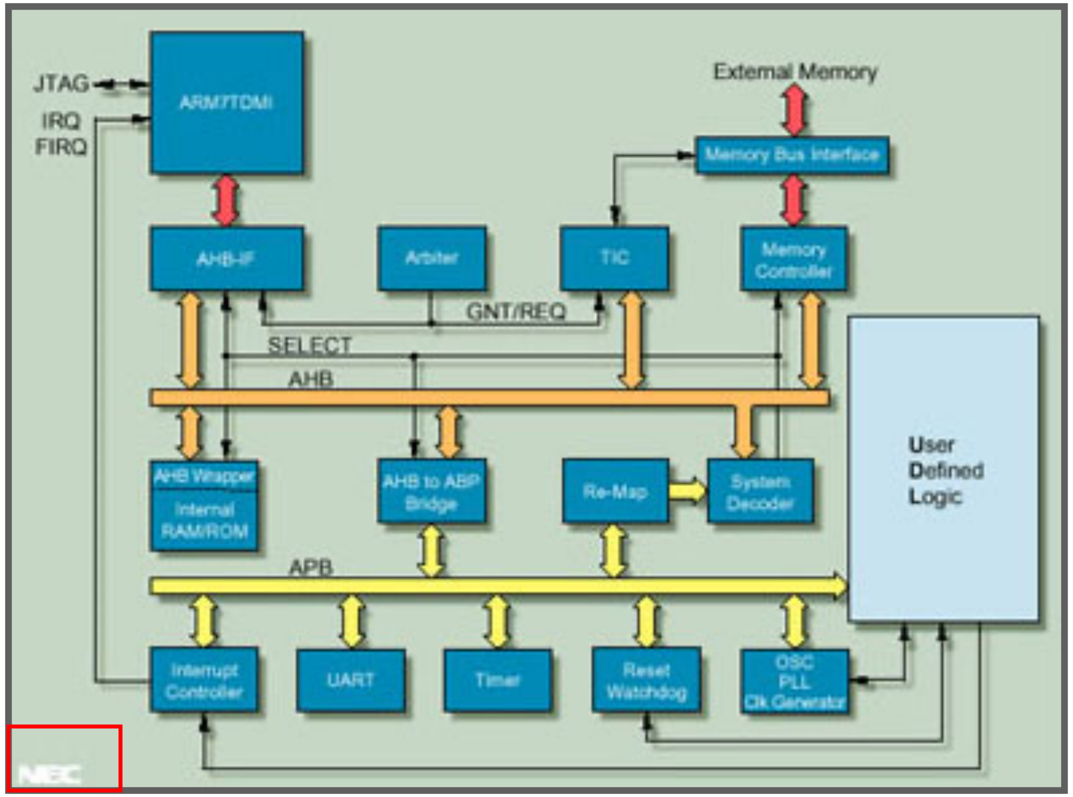

IP Vendor
System Integrator
Manufacture
Untrusted Foundry
IC Trust
IC Piracy (Counterfeiting)
Secure Manufacturing Test
Untrusted

Design Process – Old Way

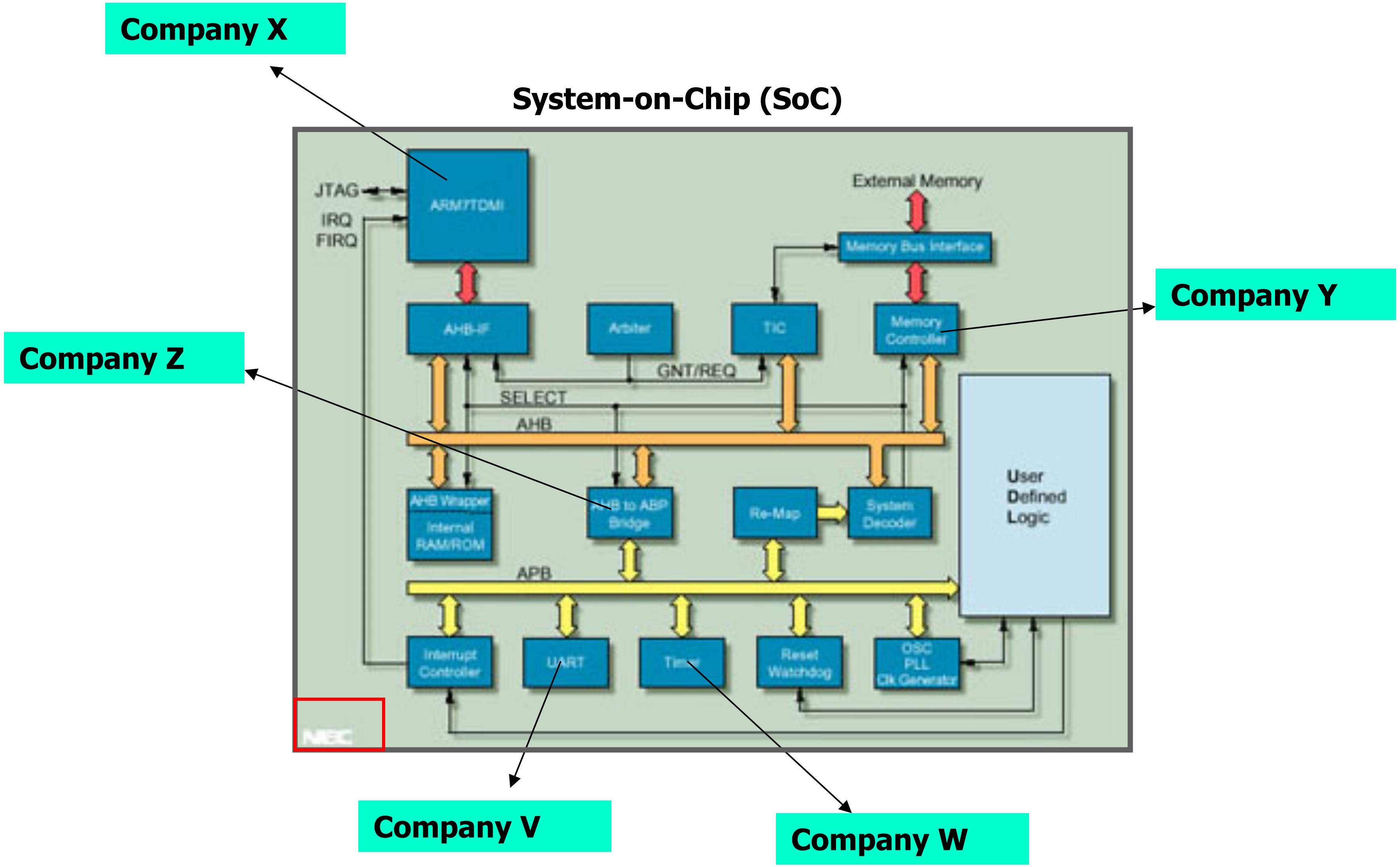


Issues with Third-Party IP Design

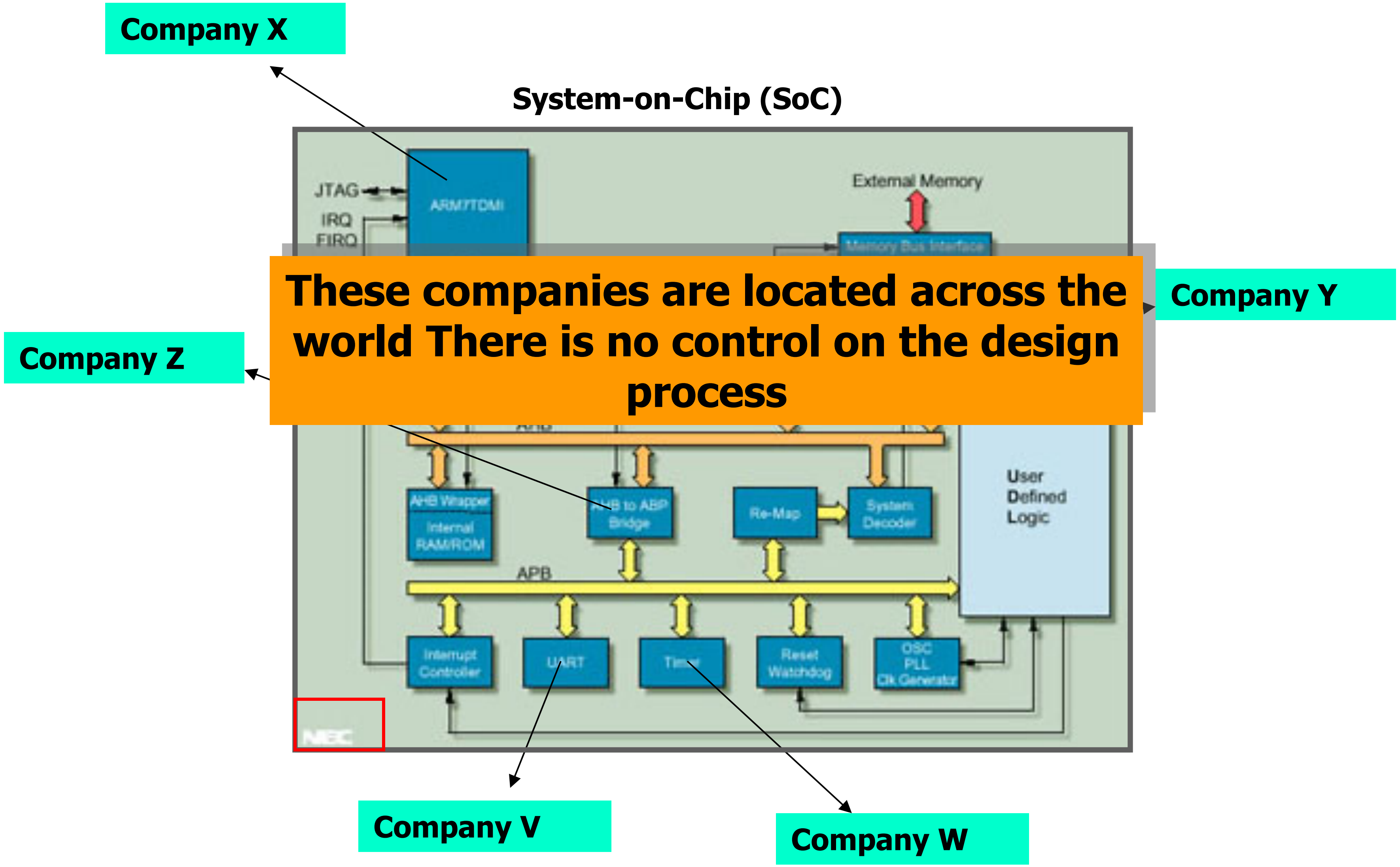
System-on-Chip (SoC)



Issues with Third-Party IP Design

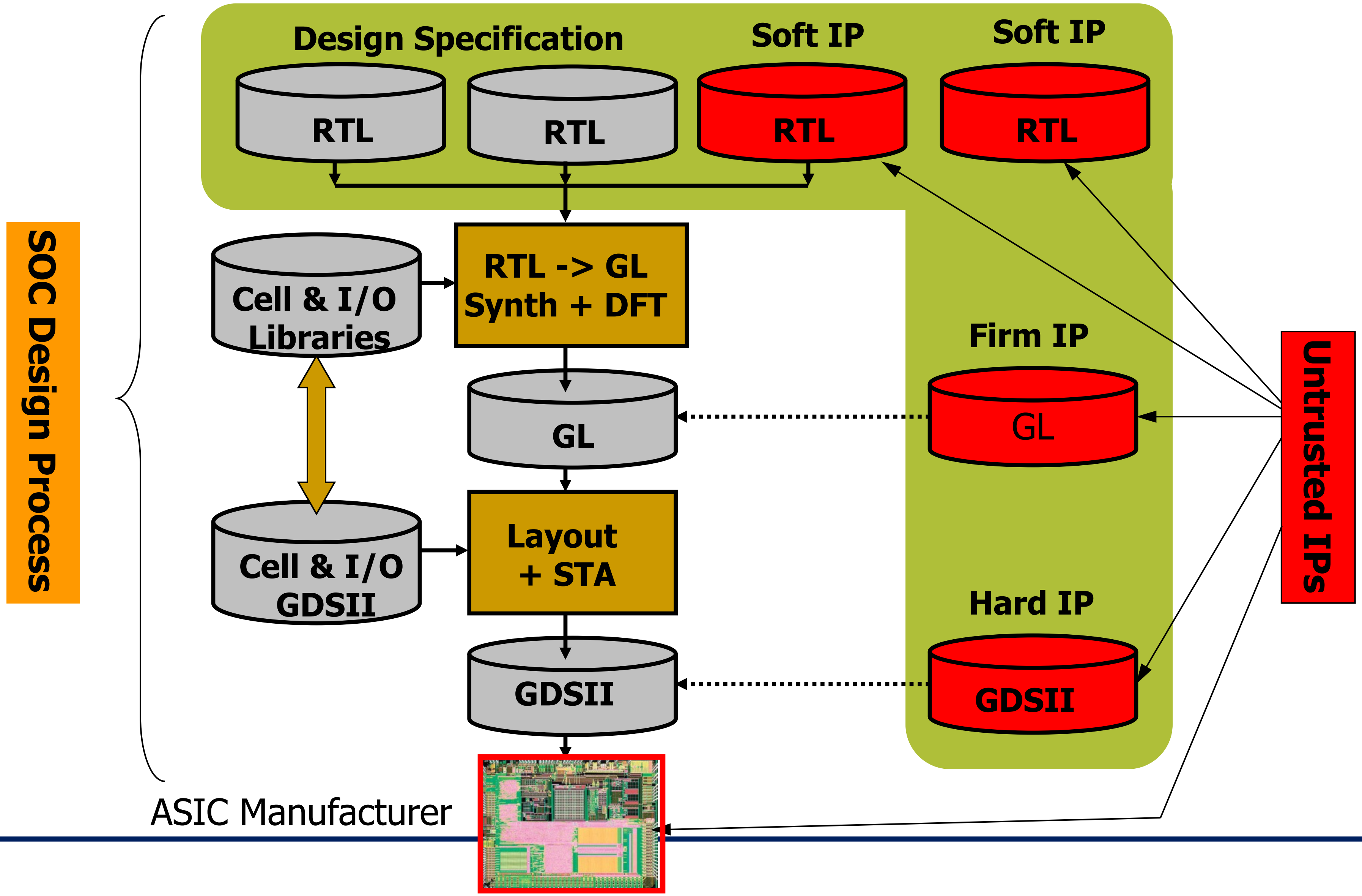


Issues with Third-Party IP Design



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

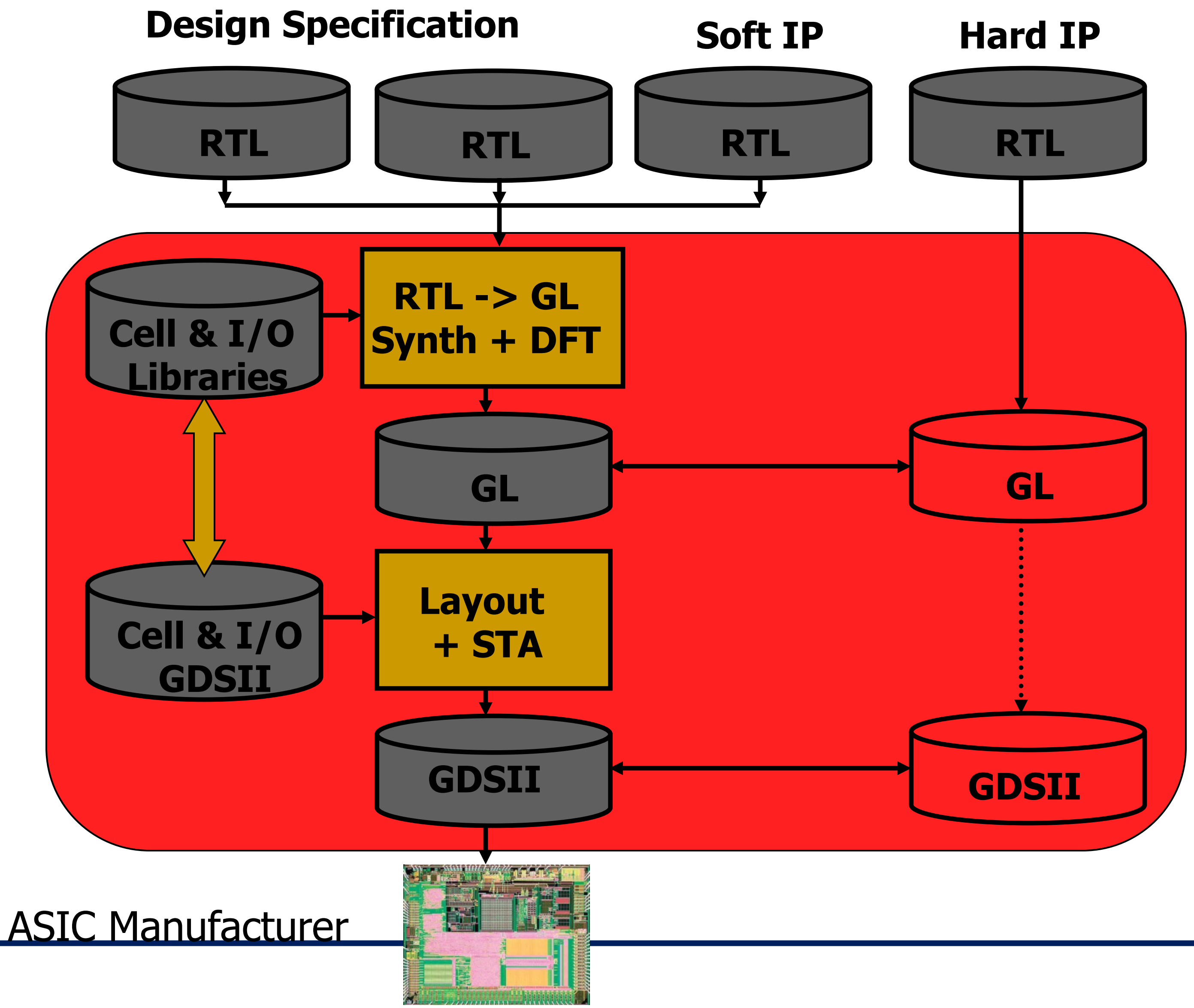
Design Process – New Way



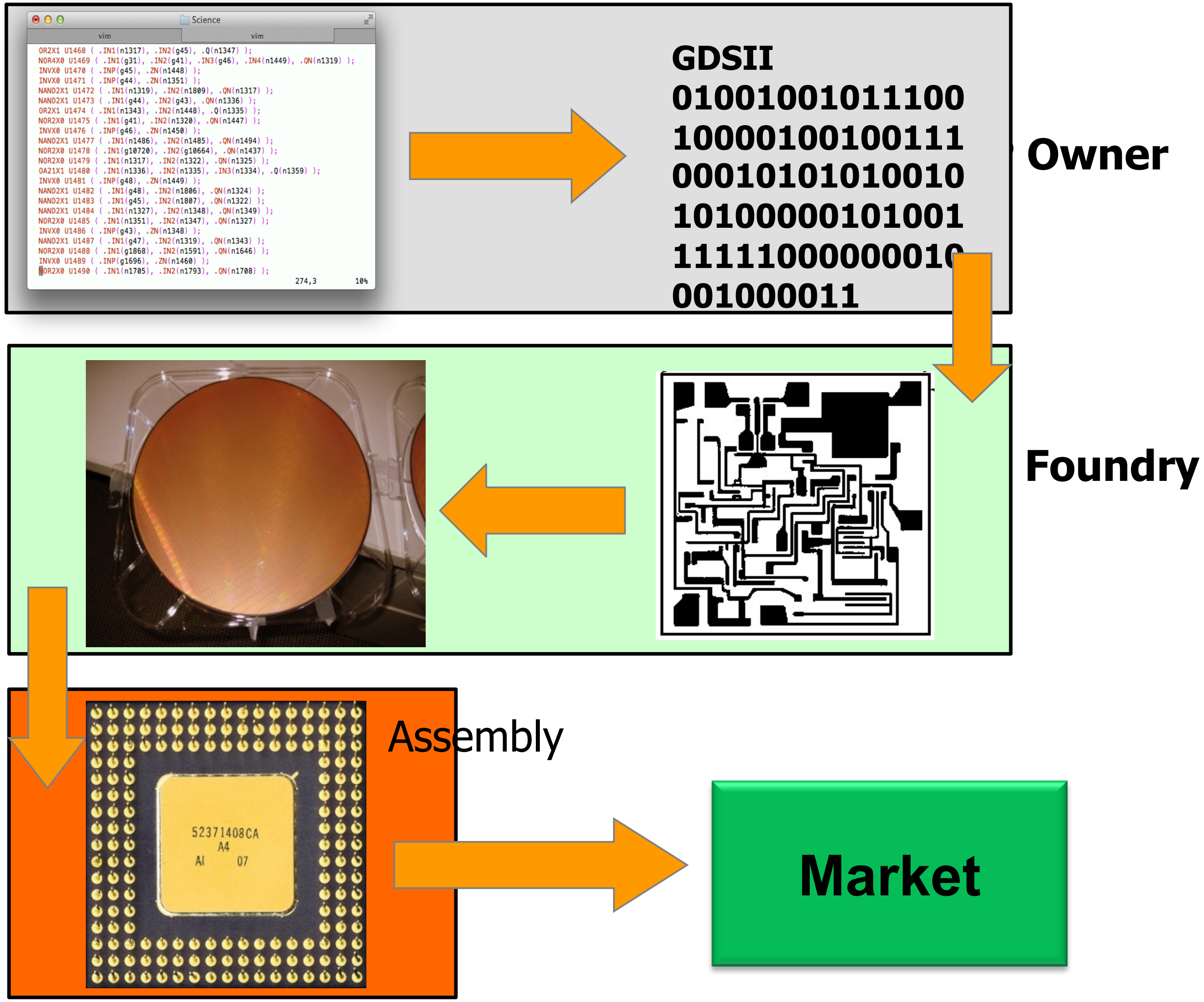
Who Develops the IPs? Who Designs the ICs? Who Fabricates Them?

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

Untrusted System Integrator

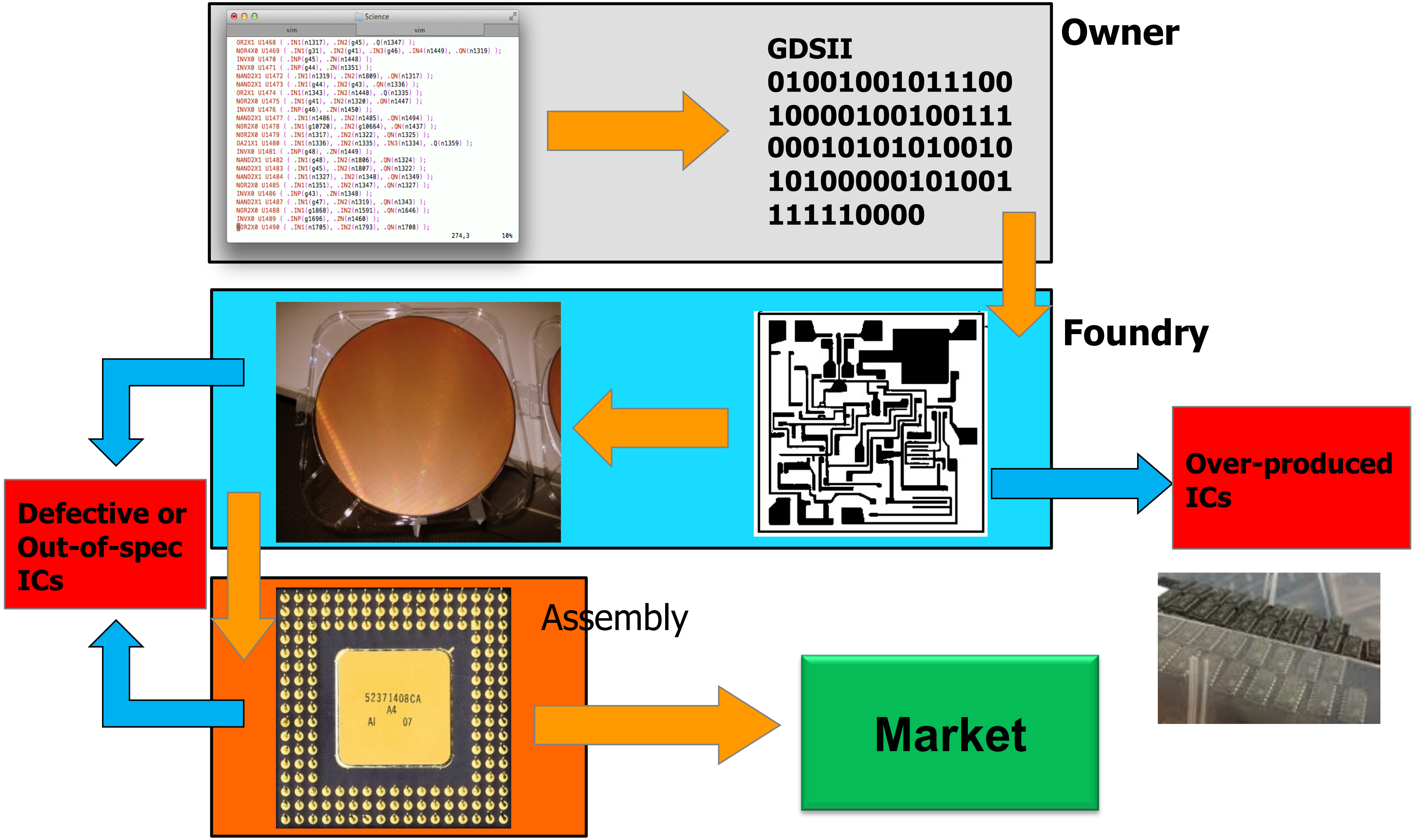


Counterfeiting



Google image

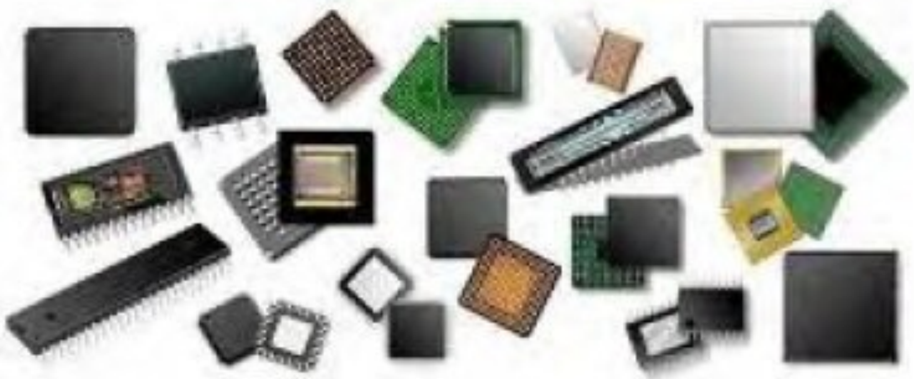
Counterfeiting



Google image

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

Defective parts

Cloned ICs

Recycled ICs

IC Recycling Process

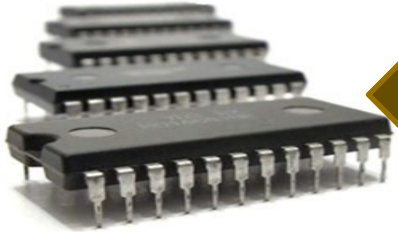
A recycling center

PCBs taken off of electronic systems

ICs taken off of PCBs

Refine recycled ICs

Resold as new



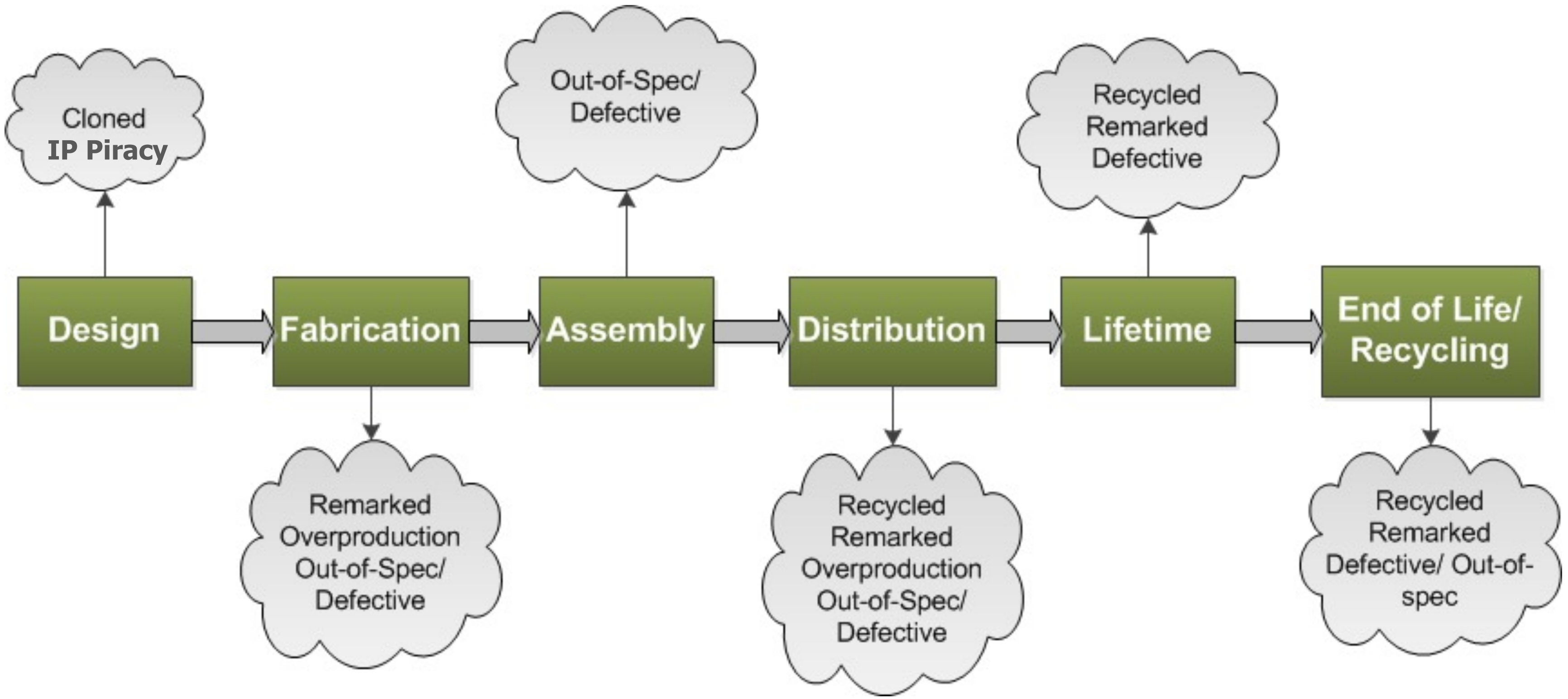
Identical:
Appearance, Function, Specification

Critical Application

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

Source: Images are taken from google

Supply Chain Vulnerabilities



Some Basic Definitions

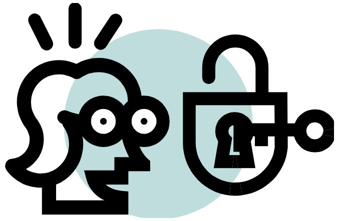
stop here!

- **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

Some Basic Definitions (Cont'd)

- **Cryptography**:
  - crypto (secret) + graph (writing)
    - the science of locks and keys
  - The keys and locks are mathematical
  - Underlying every security mechanism, there is a "secret"…
  - We are going to talk some about the traditional crypto, but we will also show new forms of security based on other forms of HW-based secret



What Does Secure Mean?

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

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 human 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

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
- **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

- **Individual, group 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, cloned, etc.

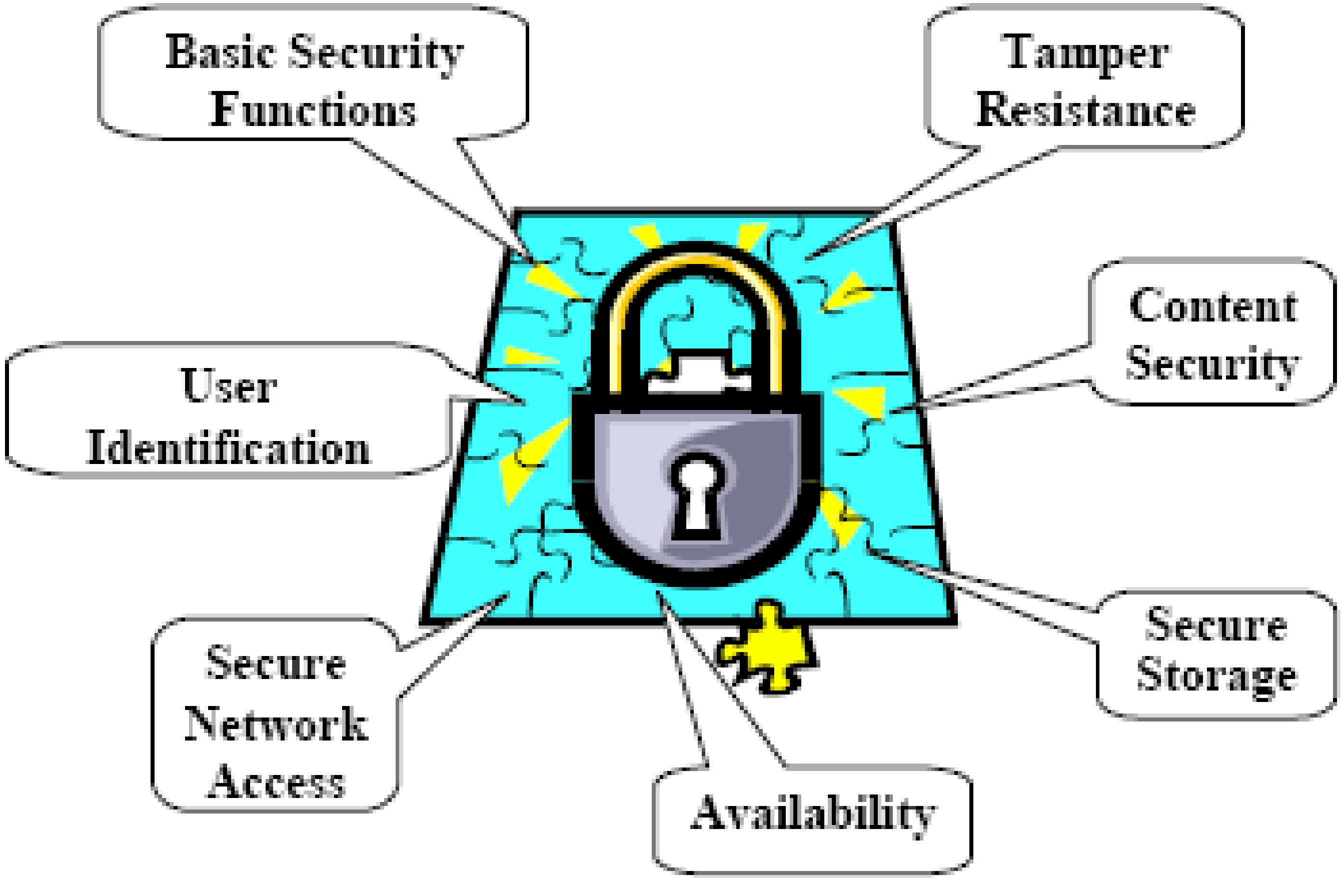
Hardware Controls for Secure Systems

- Hardware implementations of encryption
  - Encryption has to do with scrambling to hide
- Design locks or physical locks limiting the 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/IoTs

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

Security Requirements in the IoT Era



Secret

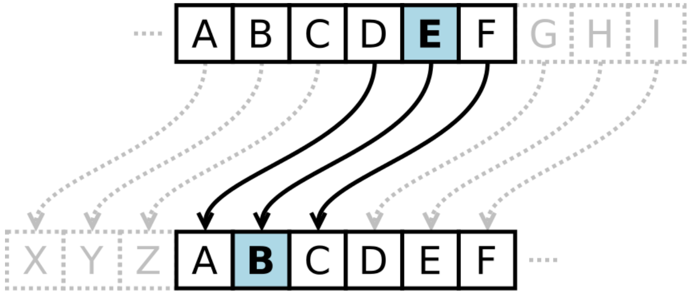
- **Underlying most security mechanisms or protocols is the notion of a “secret”**
  - Lock and keys
  - Passwords
  - Hidden signs and procedures
  - Physically hidden

Cryptography – History

- Has been around for 2000+ years
- In 513 B.C, Histiaeus of Miletus, shaved the slave’s head, tattooed the message on it, let the hair grow

Cryptography – Pencil & Paper Era

- Caesar's cipher: shifting each letter of the alphabet by a fixed amount!
  - Easy to break




```
Plaintext: THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
Ciphertext: QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD
```

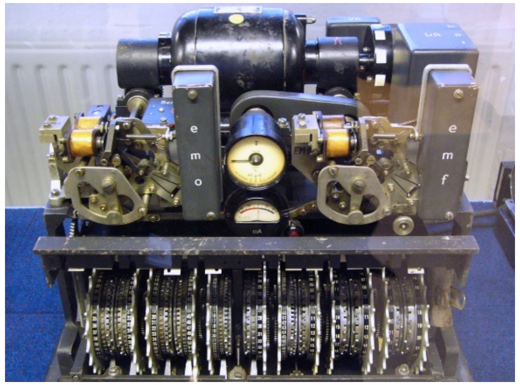
- Cryptoquote: simple substitution cipher, permutations of 26 letters
  - Using the dictionary and the frequencies, this is also easy to break

Cryptography – Mechanical Era

- Around 1900, people realized cryptography has math and stat roots
- German’s started a project to create a mechanical device to encrypt messages
- Enigma machine → supposedly unbreakable
- A few polish mathematicians got a working copy
- The machine later sold to Britain, who hired 10,000 people to break the code!
- They did crack it! The German messages were transparent to enemies towards the end of war
  - **Estimated that it cut the war length by about a year**
- British kept it secret until the last working Enigma!

Cryptography – Mechanical Era

- Another German-invented code was Tunny (Lorenz cipher system)
- Using a pseudorandom number generator, a seed produced a key stream *ks*
- The key stream xor'd with plain text p to produce cipher c: $c = p \oplus ks$
- How was this code cracked by British cryptographers at Bletchley Park in Jan 1942?
- A lucky coincidence!



German rotor stream cipher machines used by the German Army during World War II

Cryptography – Modern Era

- First major theoretical development in crypto after WWII was Shannon's Information Theory
- Shannon introduced the one-time pad and presented theoretical analysis of the code
- The modern era really started around 1970s
- The development was mainly driven by banks and military system requirements
- NIST developed a set of standards for the banks,
  - DES: Data Encryption Standard