Hardware Security and Trust

Yu Bi

ELE594 – Special Topic on Hardware Security & Trust

University of Rhode Island

ELE594

- **Title**: “Special Topic on Hardware Security and Trust”
- **Instructor**
  - Yu Bi, Assistant Professor, ECBE Department
- **Class Time**
  - 12:30 – 1:45 pm Tuesday, Swan Hall 213
  - 12:30 – 1:45 pm Thursday, Online (Zoom)
- **Prerequisites**
  - Digital or analog circuit design
  - Self-contained
  - A brief overview of digital/VLSI design will be provided

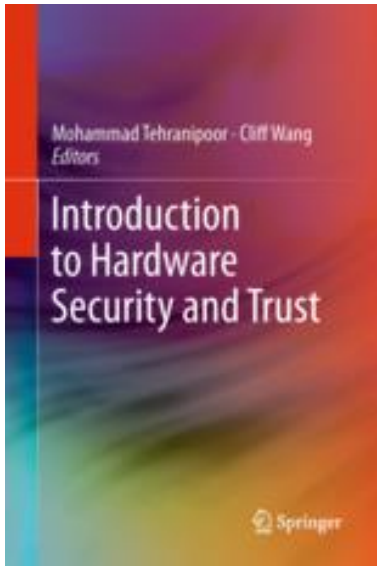
ELE594

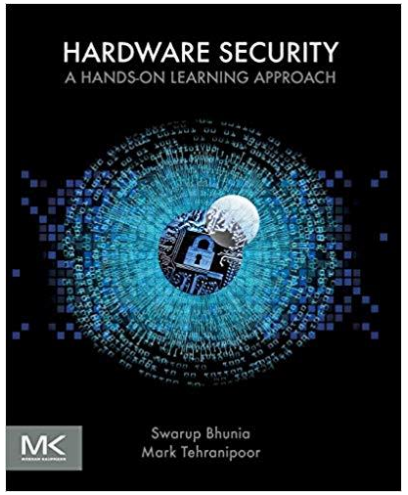
- **Office Hours**
  - 2:00 – 4:00 pm Tuesday&Thursday
  - Fascitelli Center 410
- **Textbooks** (not required):
  - P, Mishar, S. Bhunia, and M. Tehranipoor, “Hardware Security: A Hands-on Learning Approach”, Elsevier, 2018.
  - M. Tehranipoor and C. Wang, “Introduction to Hardware Security and Trust”, Springer, 2011.
  - Collections of papers and reports will be distributed
- **Supplementary**
  - Trust-hub, https://www.trust-hub.org/
  - Opencores, https://opencores.org/

Textbooks and Materials

- Textbooks (not required):
  - Introduction to Hardware Security and Trust, Springer, 2011.
  - Hardware Security: A Hands-on Learning Approach, Elsevier, 2018.

- Reading Materials
  - Conferences: IEEE HOST, IEEE/ACM DAC, DATE, IEEE ICCAD; IEEE S&P, ACM CCS, USENIX Security. etc.
  - Journals: IEEE TIFS, IEEE TDSC, IEEE TCAD, IEEE TC, IEEE TVLSI etc.
  - A collection of papers will also be provided.





Course Overview

- Overviews and Basics of VLSI Design
- Hardware Attacks:
  - Invasive, non-invasive, physical etc.
- Security based on PUFs and TRNGs
- Hardware Trojan
- Hardware IP Protection
  - Metering, logic obfuscations and encryption etc.
- FPGA Security
- AI/System Security

Objectives

- Learning the state-of-the-art security primitives and methods as well as emerging technologies and security trends
- Better understanding of attacks and providing countermeasures against them
- Better understanding of the electronic component supply chain vulnerabilities
- Integration of hardware security as a design metric for any hardware design flows
- Exploration of hardware and software co-design to enhance the integrity of hardware IP

More Interesting Resources

- The hunt for the kill switch https://spectrum.ieee.org/tag/hardware+Trojan
- Old Trick Threatens the Newest Weapons https://www.nytimes.com/2009/10/27/science/27trojan.html?_r=2&emc=eta1
- Hardware Trojans: Lessons Learned after One Decade of Research https://dl.acm.org/doi/10.1145/2906147
- Supergeek pulls off 'near impossible' crypto chip hack https://www.nzherald.co.nz/technology/news/article.cfm?c_id=5&objectid=10625082&pnum=0
- Three Ways to Hack a Printed Circuit Board https://spectrum.ieee.org/computing/hardware/three-ways-to-hack-a-printed-circuit-board
- The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies https://shorturl.at/fhxO2

. . . . . .

Interesting Video

- What's inside a microchip? https://www.youtube.com/watch?v=GdqbLmdKgw4
- Zoom into a chip https://www.youtube.com/watch?v=Fxv3JoS1uY8
- Counterfeit electronics could be dangerous https://www.youtube.com/watch?v=dbZiUe6guxc
- How computers and electronics are recycled https://www.youtube.com/watch?v=Iw4g6H7alvo
- Counterfeit electronic components process https://www.youtube.com/watch?v=5vN_7NJ4qYA
- Couterfeit inspection https://www.youtube.com/watch?v=MbQUvu2LN6o

……

Grading

- Grading
  - One Midterm Exam: 30%
  - Student Presentation: 30%
  - Final Project and Demo: 40%

- Project
  - Individual or a group of max two students
  - Propose or select from a given list of projects
  - Experiment might need hardware component (e.g. fpga boards)
  - Project should be presented and video recorded.

Tools for Projects

- Tools
  - Xilinx Vivado Synthesis
  - Verilog, VHDL, High-level Synthesis (e.g. C++), Python etc.
  - You may need to run some statistical analysis (e.g. python or matlab)

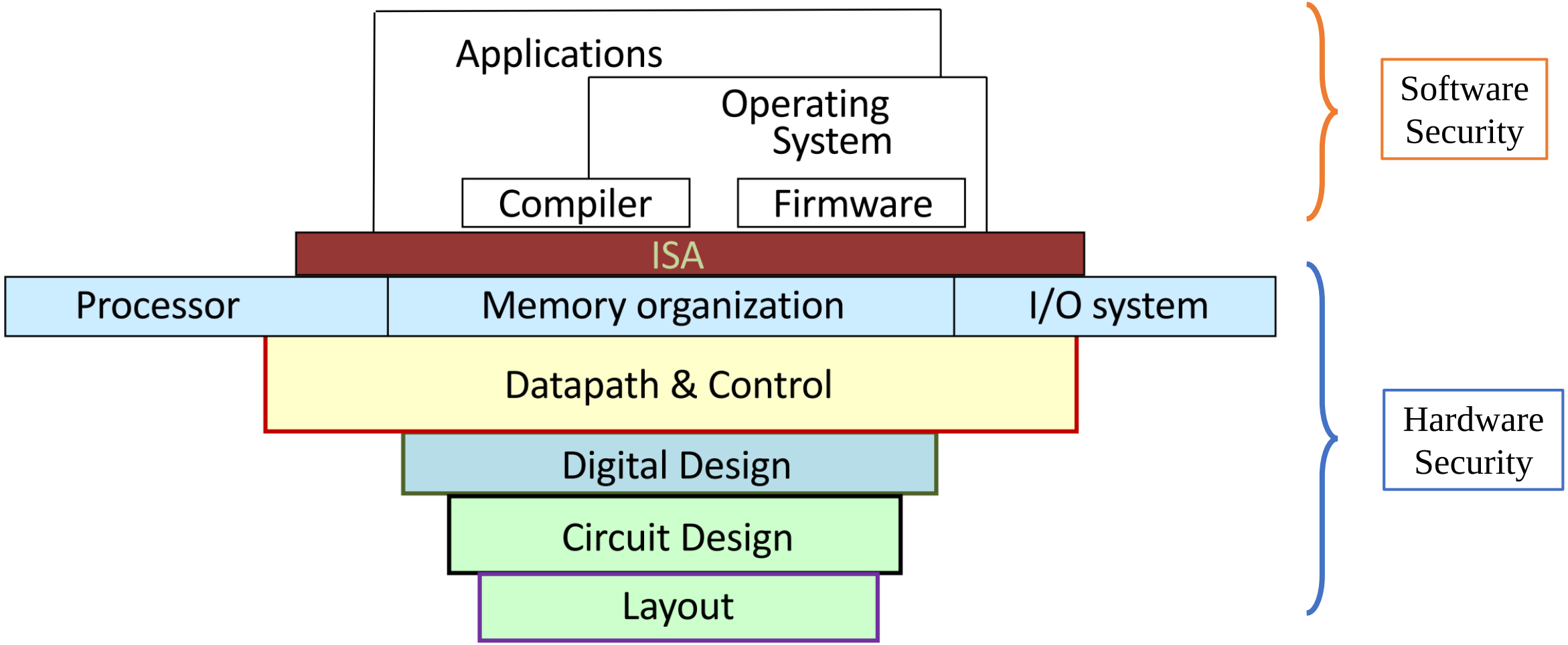
- Hardware
  - Project running on hardware, e.g. FPGA and Microcontroller.

- **Talk to me before you start the project**.
- **Start as early as possible.**

Hardware Security

- Hardware security in general definition includes any study/research under the micro-architecture level;
- The underlying hardware has long been considered secure and trust by software experts;
- Such assumption is no longer true;
- Moving forward, a software and hardware co-design is required to maintain the integrity of computer systems.

Computer System Overview



Motivation: Why the 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 EVoting 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
  - **Apple hardware back-door (spy chips), The Guardian, 10/04/18**
  - **New Evidence of Hacked Supermicro Hardware Found in U.S. Telecom, 2018**
  - **A Critical Intel Flaw Breaks Basic Security for Most Computers, 2018**

  ……

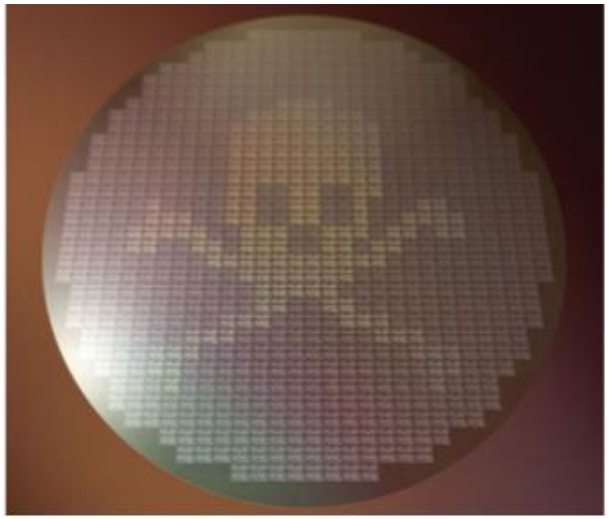
Example Hardware Attacks

DHS: Imported Consumer Tech Contains Hidden Hacker Attack Tools

- Top homeland securities have admitted instances where along with software, hardware components that are being imported from foreign parties and used in different US systems are being compromised and altered to enable easier cyber-attacks.

The Hunt for Kill Switch, IEEE Spectrum 2008

- Increasing threat to hardware due to globalization
- Extremely difficult to detect kill switches (utilized by enemies to damage/destroy opponent artillery during critical missions) as well as intentional backdoors (to enable remote control of chips without user knowledge)
- Example: Syrian's Radar during Israeli attack, French Government using kill switches intentionally as a form of active defense to damage the chips if they fall in hostile hands, and more …



Example Hardware Attacks

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

Energy Theft Going From Bad to Worse

- Tampering with “smart” meters
  - Oil, electricity, gas, …
- $1B loss in CT because of electricity theft

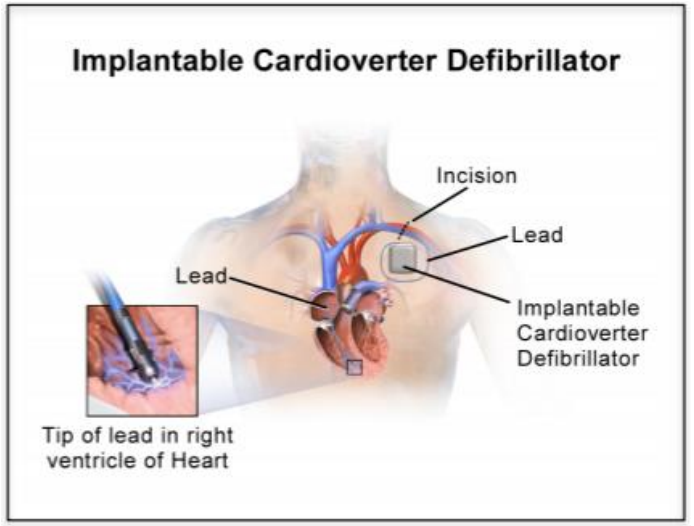
Example Hardware Attacks

The deadly world of fake medicine – CNN.com

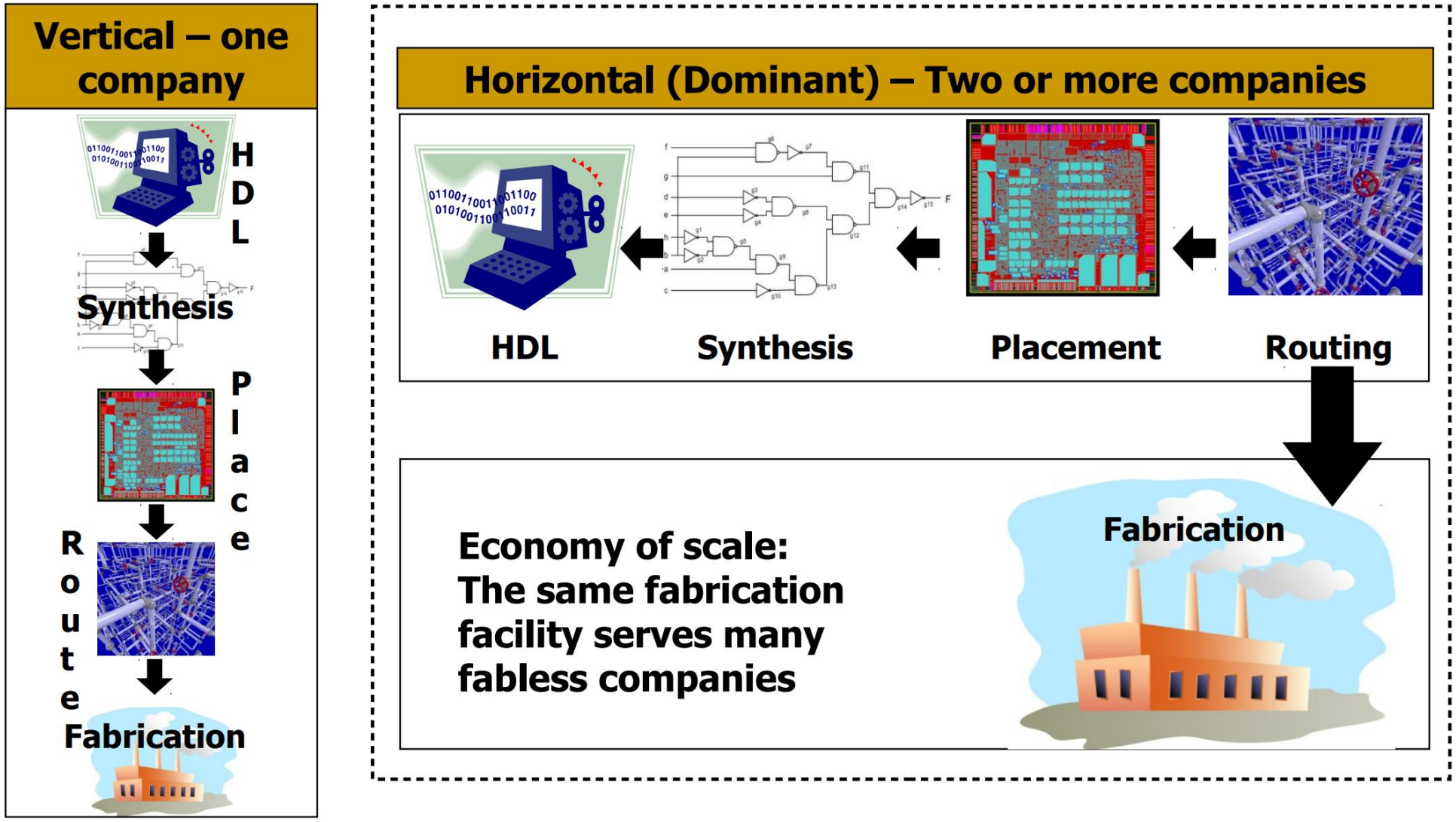
- A **counterfeit medication** or a counterfeit drug is a medication or pharmaceutical product which is produced and sold with the intent to deceptively represent its origin, authenticity or effectiveness

Medical Device Security

- Incorporating security is sometimes considered expensive
- Implantable devices: e.g., Heart rate monitor
  - Incorporating Security could potentially reduce the life-time of the device by 30%
  - Attacking these device could result in loss of lives

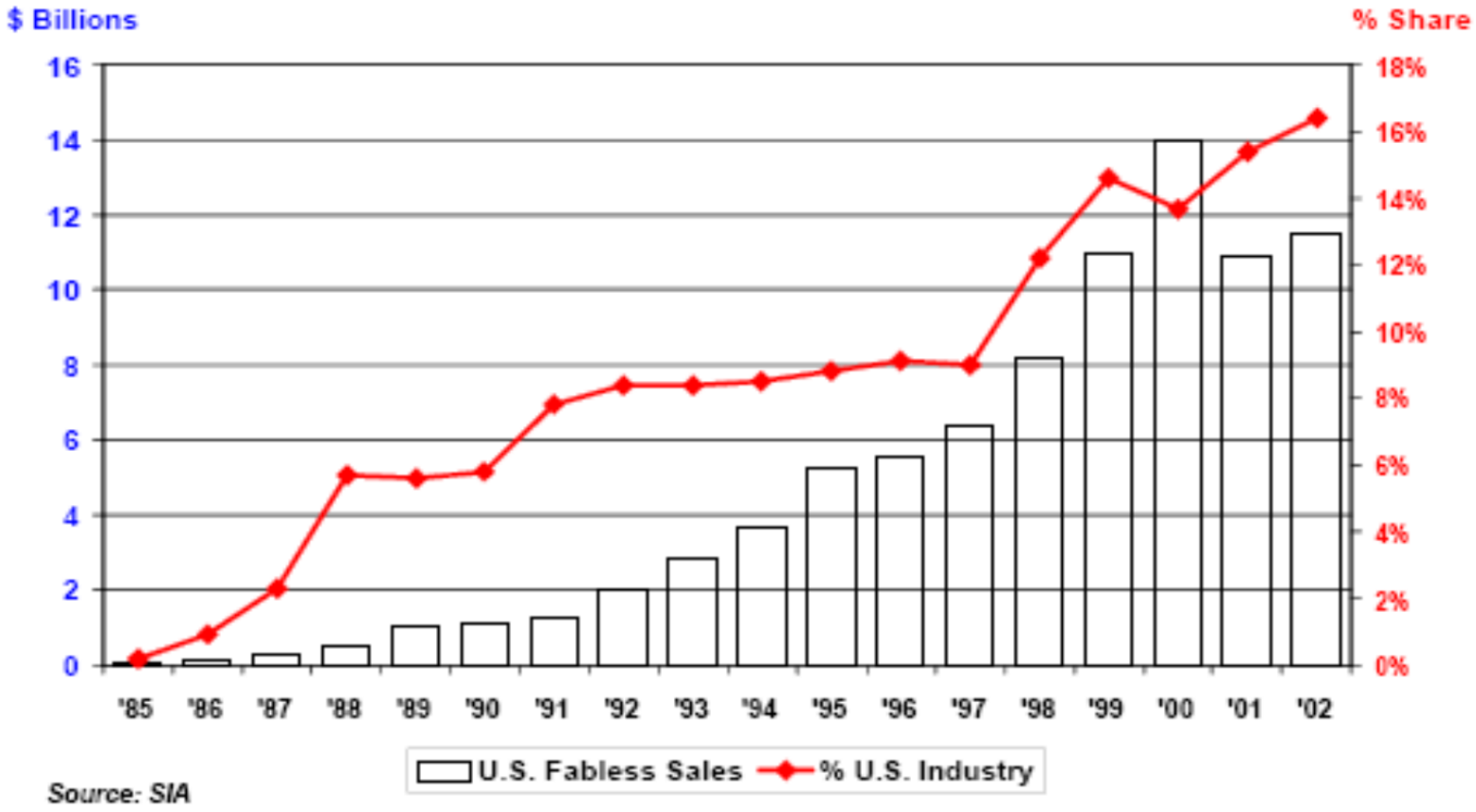


Semiconductor Industry



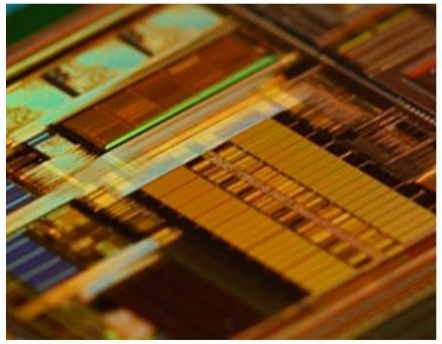
Semiconductor Industry

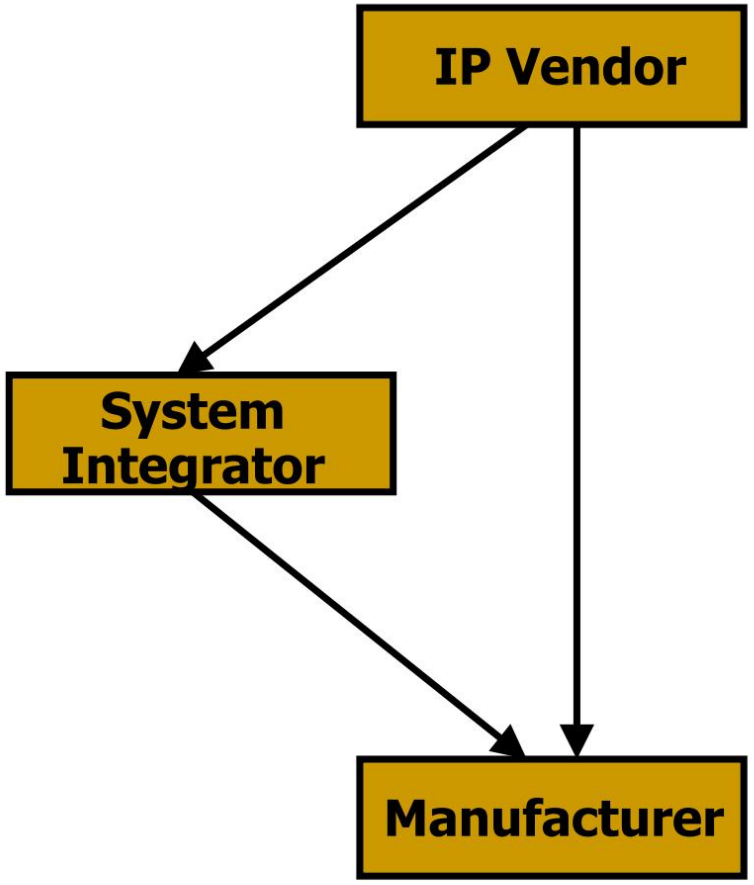
The fabless/foundry business model has grown to 16% of the U.S. chip industry. The trend is strongest in the leading process technology portion of the industry

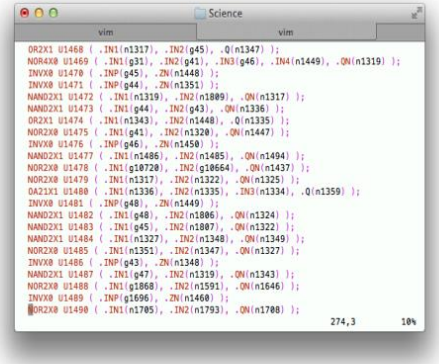


Source: SIA

Hardware Threats

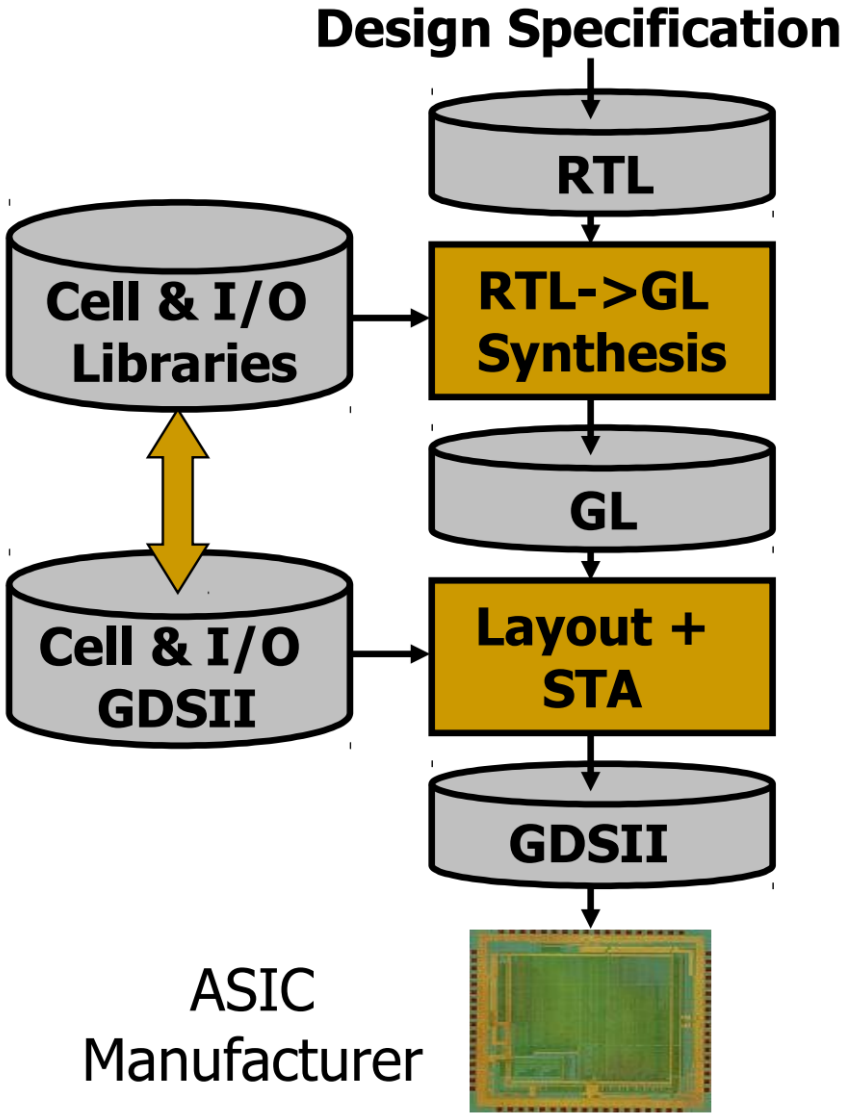




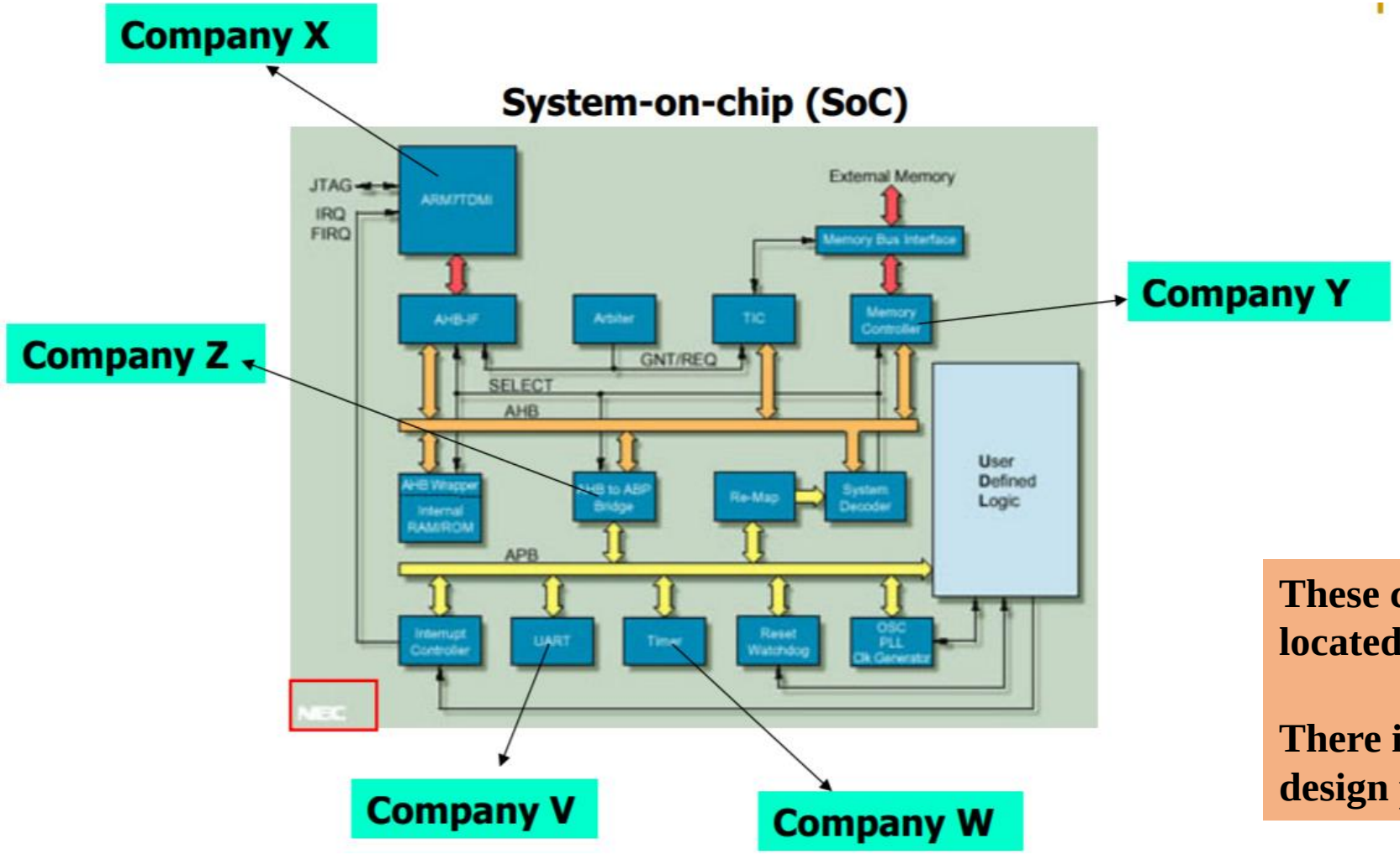


Any of these steps can be untrusted

Design Flow


Design Specification
RTL
Cell & I/O Libraries
RTL->GL Synthesis
GL
Cell & I/O GDSII
Layout + STA
GDSII
ASIC Manufacturer

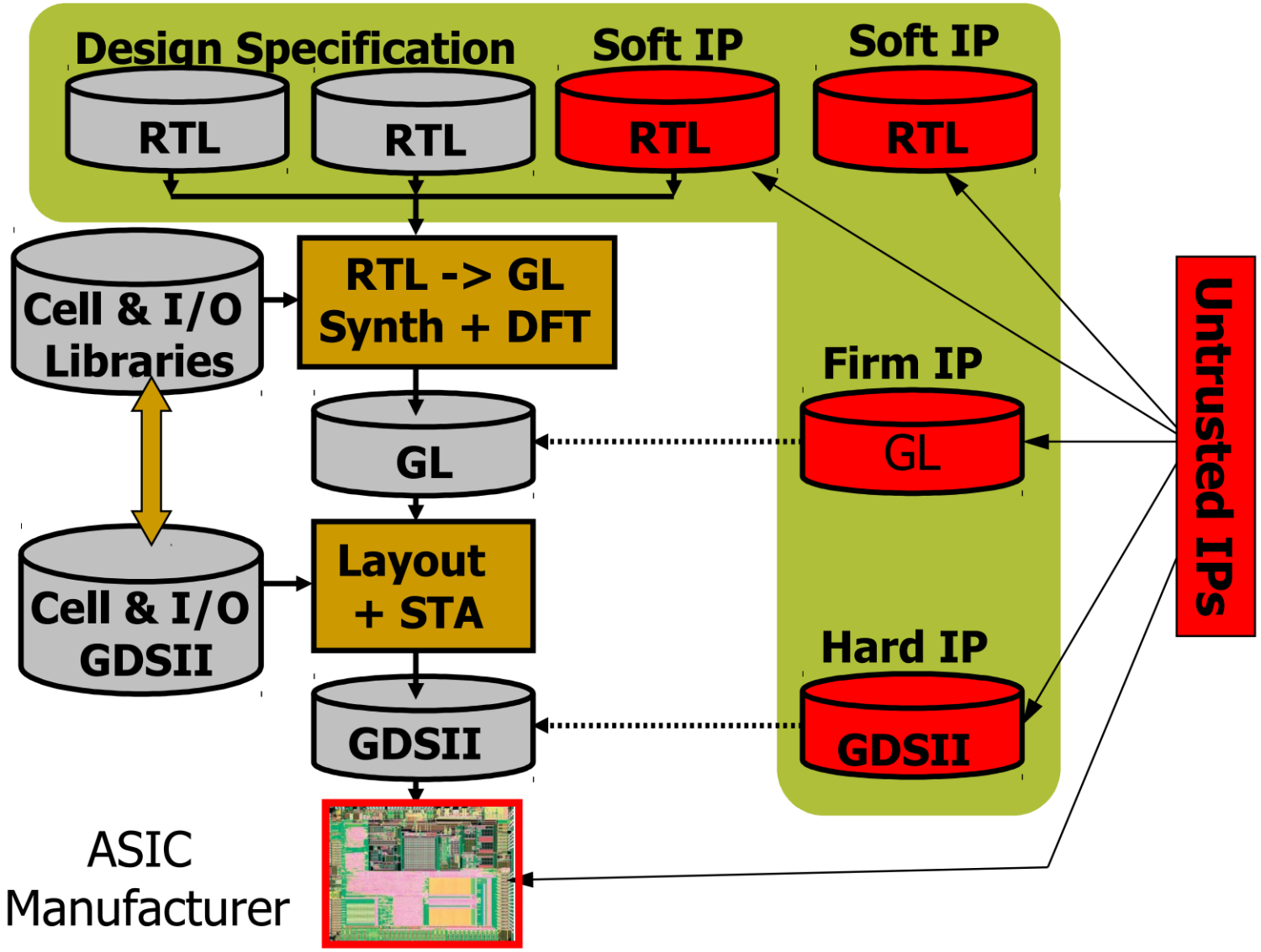
SoC based on Third Party



These companies are located across the world.

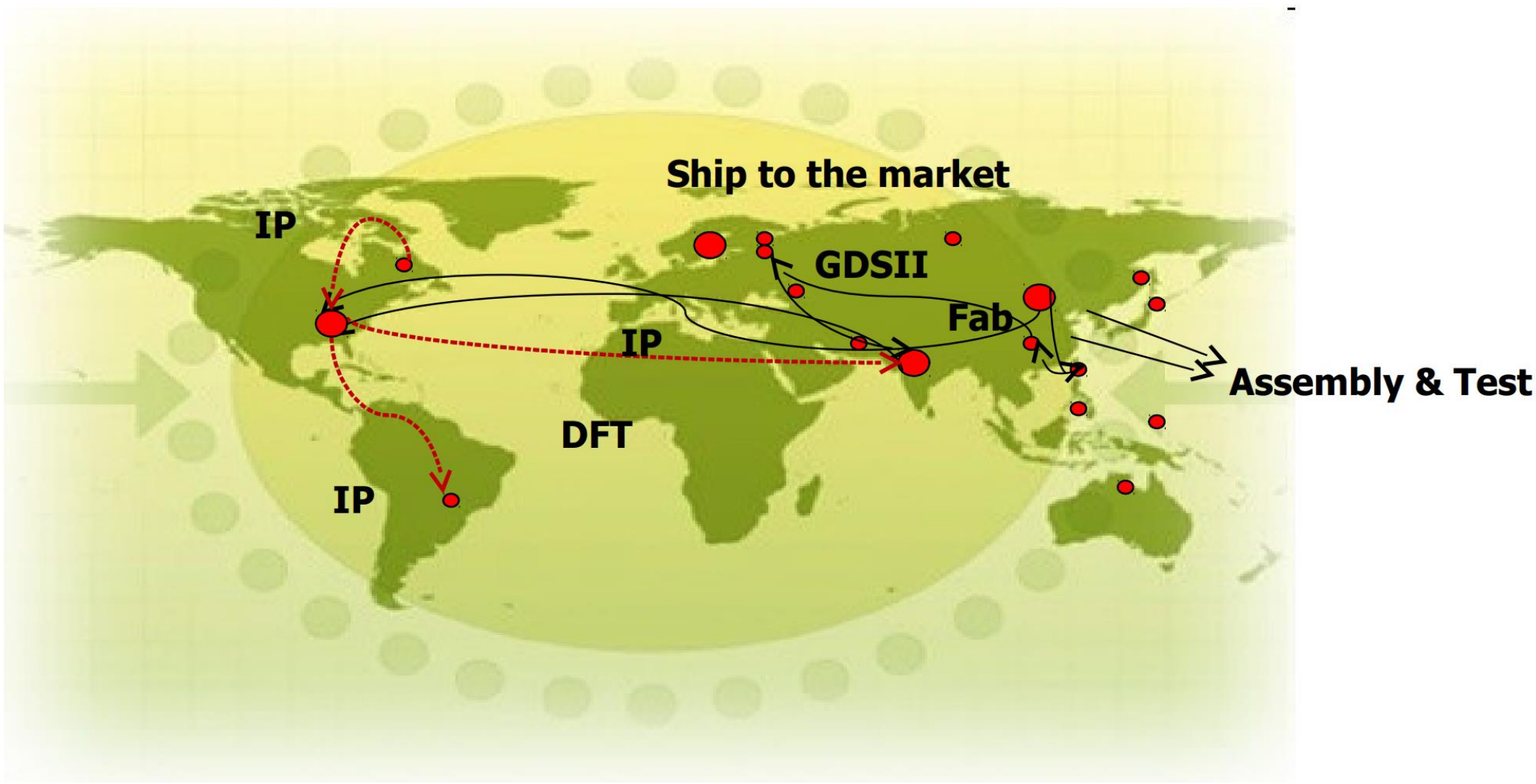
There is no control on the design process

Design Flow – New Way



Semiconductor Business Landscape

Semiconductor Business Landscape



Hardware Threat Models

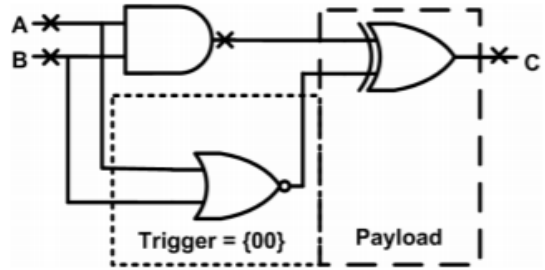
- Individual or Government
  - Pirating the IPs – illegal use of Ips
  - Inserting backdoors, or malicious circuitries
  - Implementing Trojan horses
  - Reverse engineering of ICs
- System integrators
  - Pirating the IPs
- Fabrication Facilities
  - Pirating the IPs/ICs
- Counterfeiting parties
  - Recycling, cloned, etc

Goal of Hardware Defense

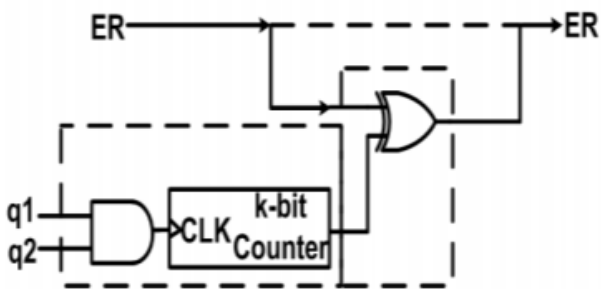
- Hardware implementations of encryption
  - Encryption has to do with scrambling to hide
- Design locks or physical locks limiting the access
- Devices to verify the user identities
- Hiding signatures in the design files
- Intrusion detection
- Hardware boards limiting memory access
- Tamper resistant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

HW Trojan Examples/Models

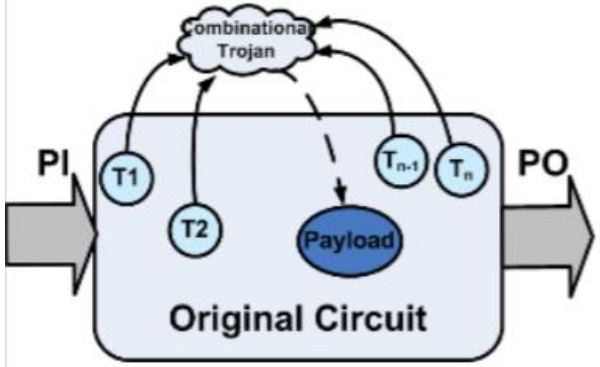
Comb. Trojan Example



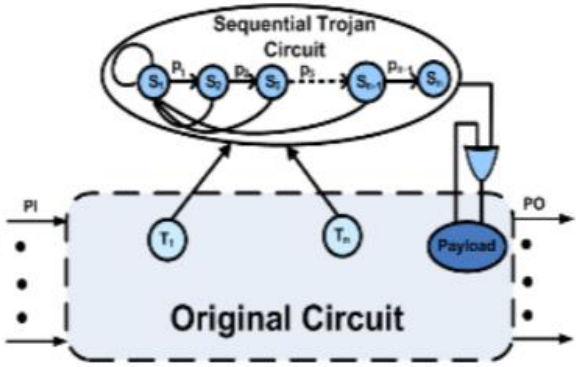
Seq. Trojan Example



Comb. Trojan model



Seq. Trojan Model




Fishy Chips: Spies Want to Hack-Proof Circuits

HW Trojan evidence!

HW Trojan Demo

- https://youtu.be/LtoOgiZcZT8