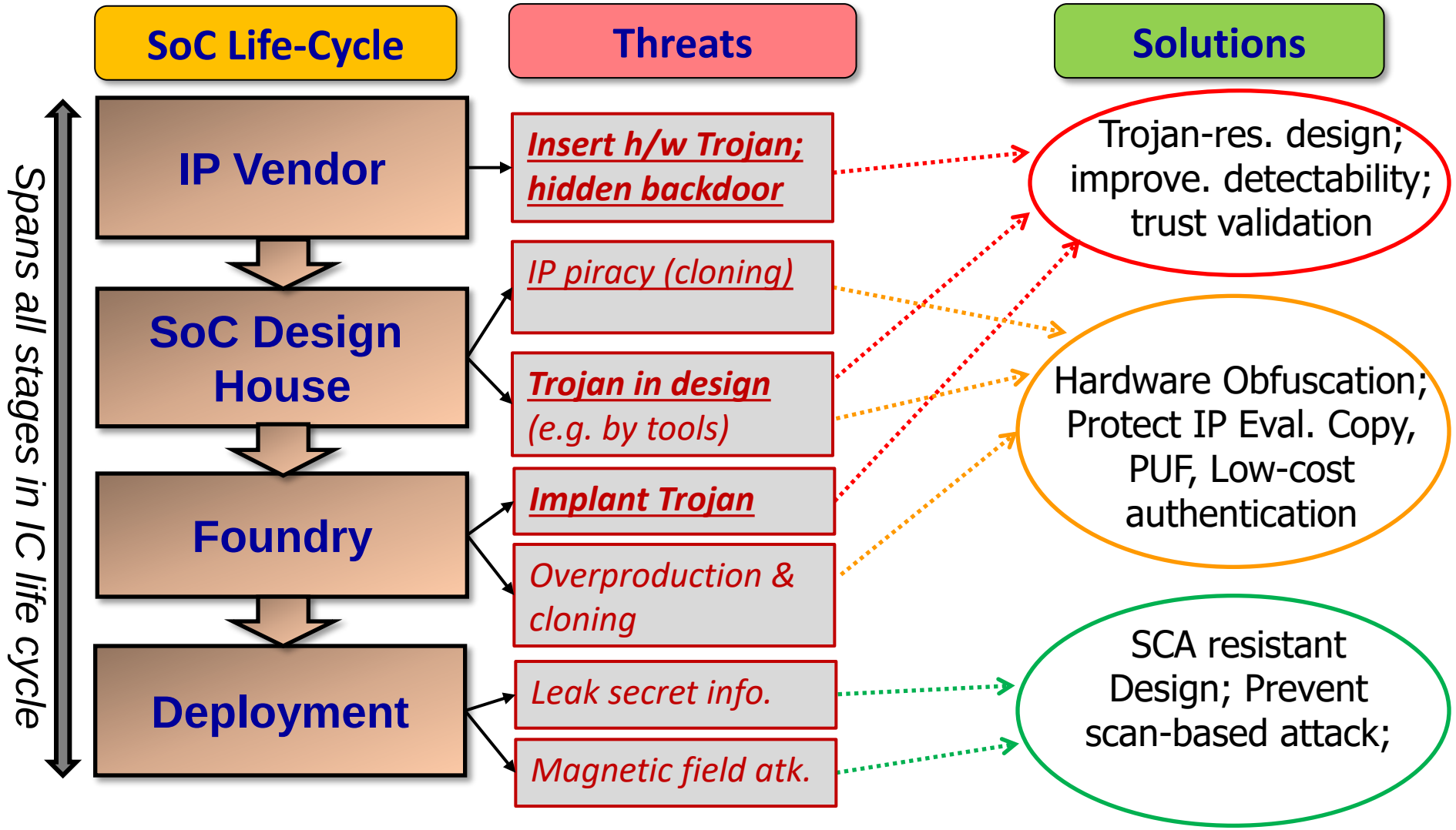
Chapter 5

Hardware Trojan

Threats


SoC Life-Cycle
Threats
Solutions
Spans all stages in IC life cycle
IP Vendor
SoC Design House
Foundry
Deployment
Insert h/w Trojan; hidden backdoor
IP piracy (cloning)
Trojan in design (e.g. by tools)
Implant Trojan
Overproduction & cloning
Leak secret info.
Magnetic field atk.
Trojan-res. design; improve. detectability; trust validation
Hardware Obfuscation; Protect IP Eval. Copy, PUF, Low-cost authentication
SCA resistant Design; Prevent scan-based attack;

What is Hardware Trojan?

- **Hardware Trojan:**
  - A malicious addition or modification to the existing circuit elements.
- **What hardware Trojans can do?**
  - Change the functionality
  - Reduce the reliability
  - Leak valuable information
- **Applications that are likely to be targets for attackers**
  - Military applications
  - Aerospace applications
  - Civilian security-critical applications
  - Financial applications
  - Transportation security
  - IoT devices
  - Commercial devices
  - More

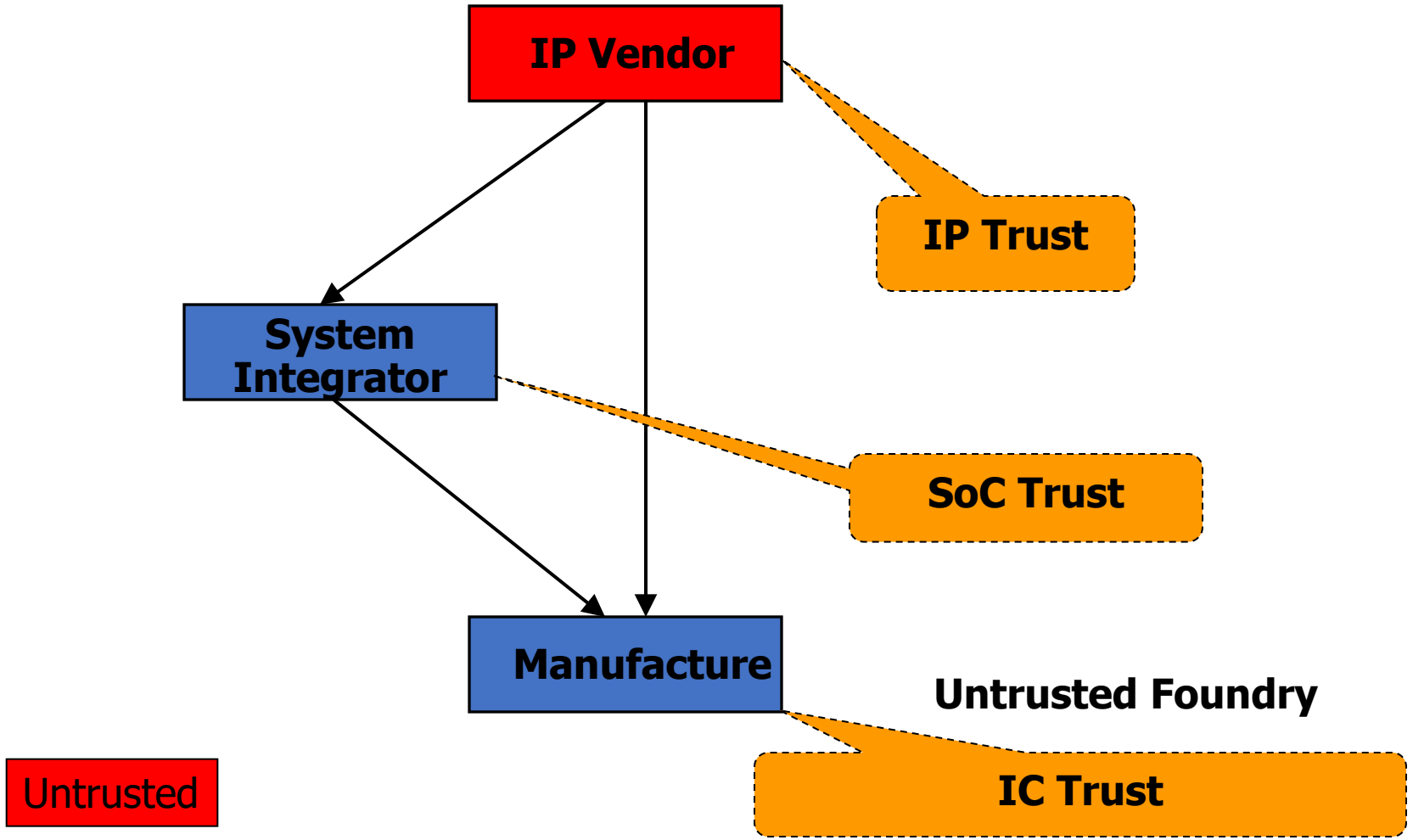
IC/IP Trust Problem

- Chip design and fabrication has become increasingly vulnerable to malicious activities and alterations with globalization.

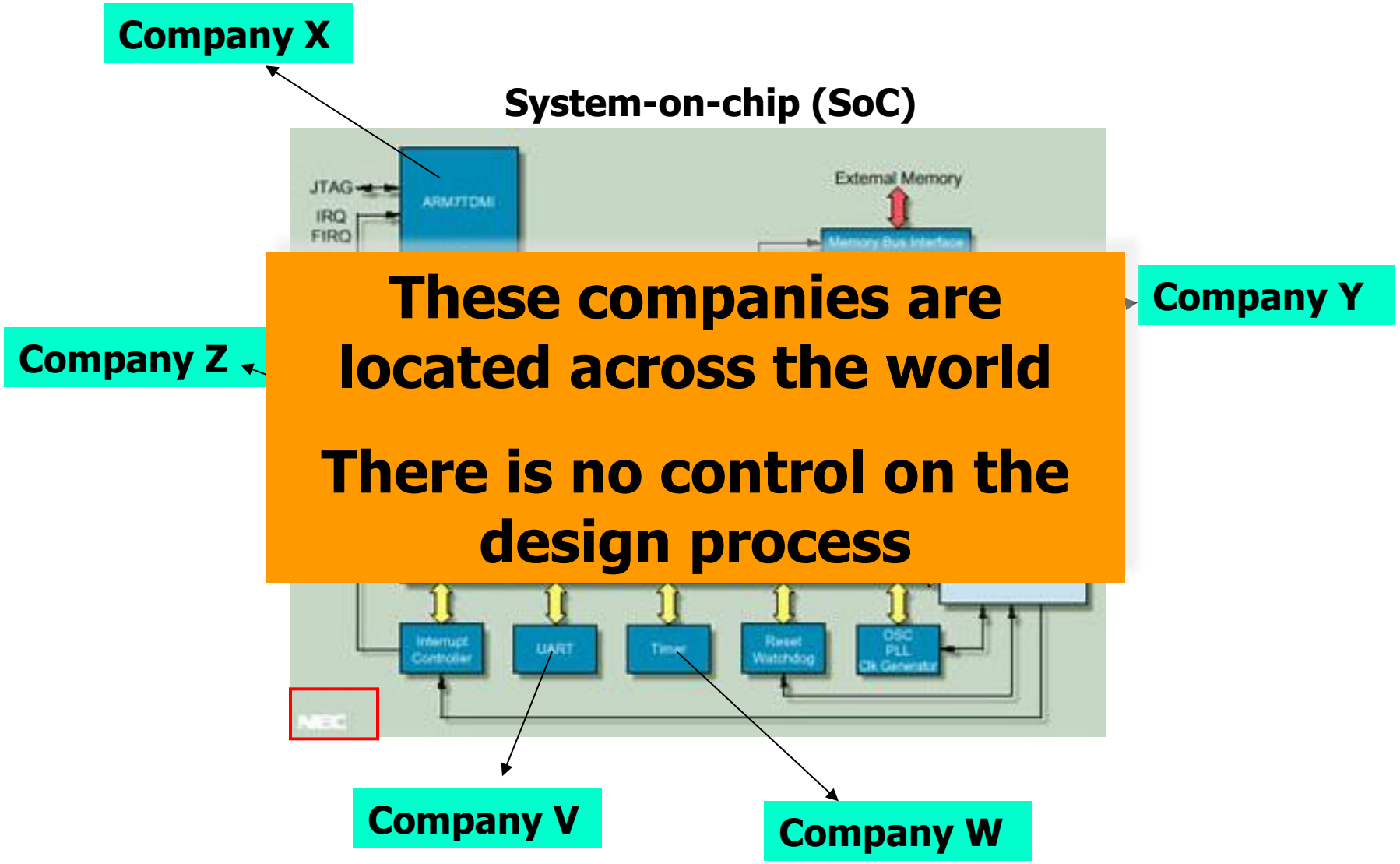
- **IP Vendor and System Integrator:**
  - IP vendor may place a Trojan in the IP
  - *IP Trust problem*

- **Designer and Foundry:**
  - Foundry may place a Trojan in the layout design.
  - *IC Trust problem*

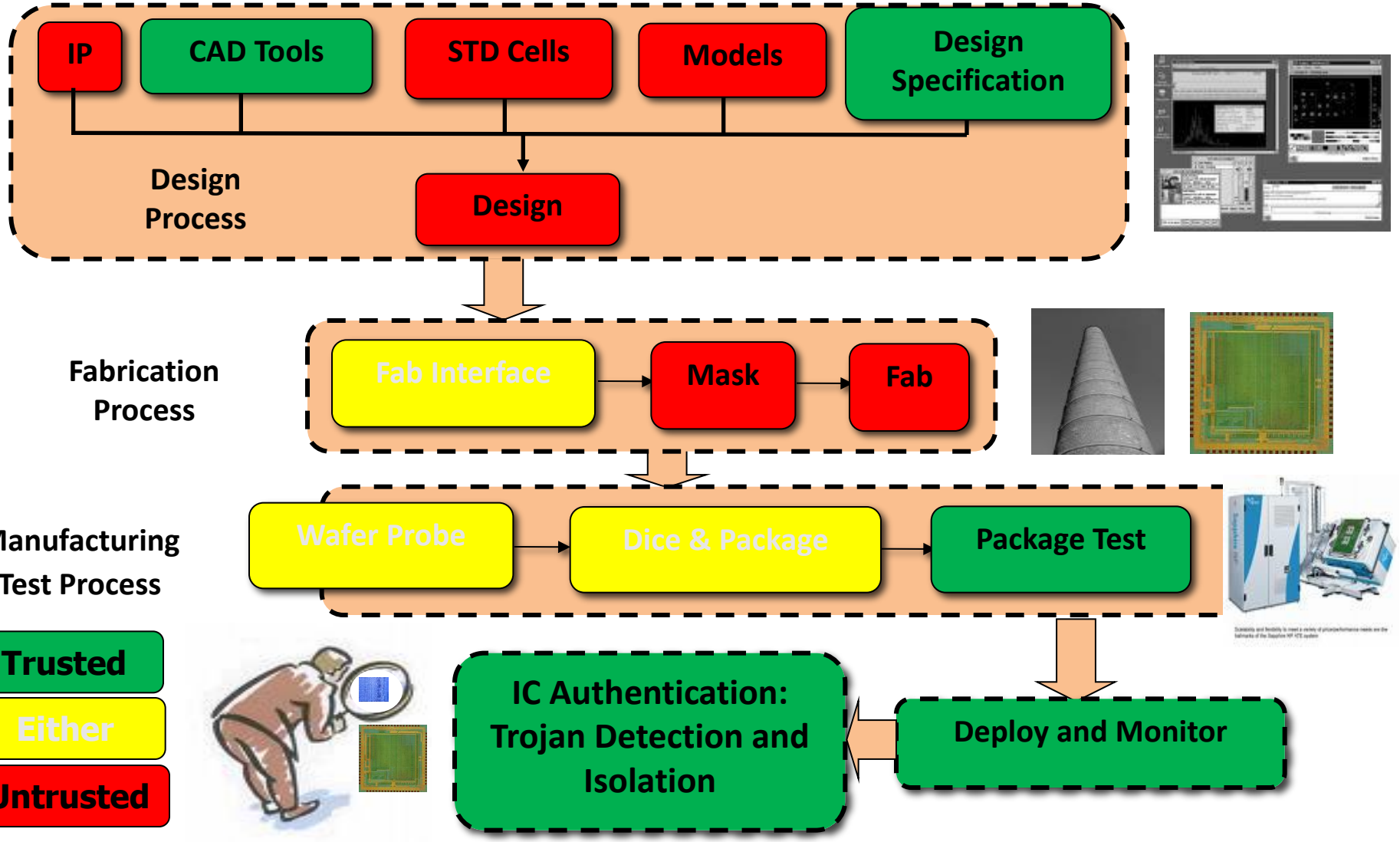
Hardware Trojan Threat



Issues with Third IP Design

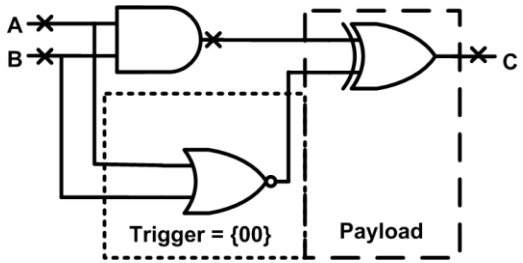


Untrusted Designer and Foundry

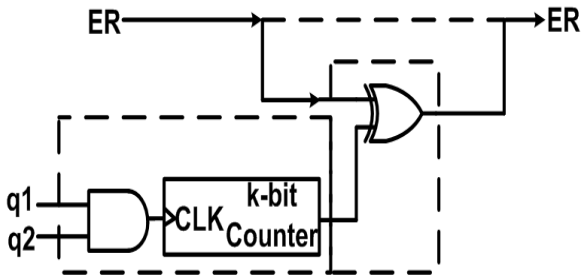


HW Trojan Examples / Models

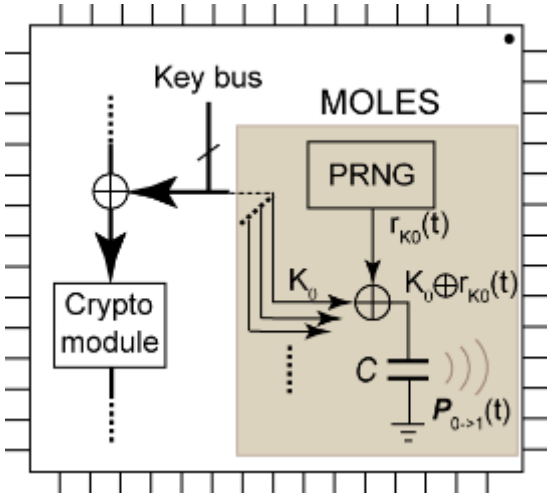
Comb. Trojan Example



Seq. Trojan Example

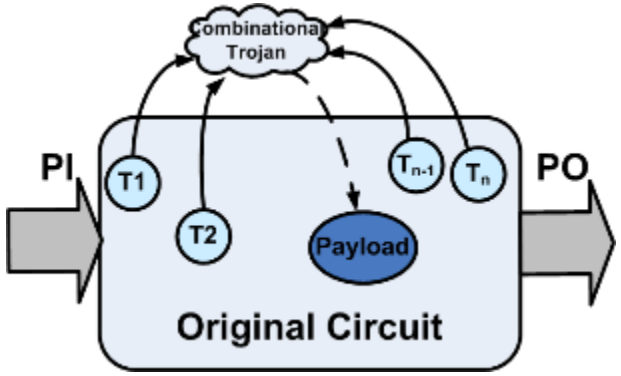


MOLES*: Info Leakage Trojan

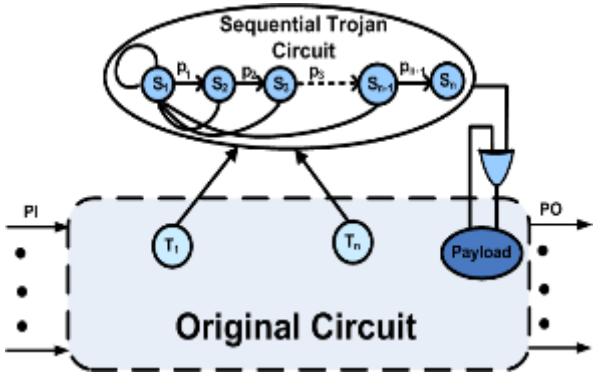


Malicious Off-chip Leakage Enabled by Side-channels

Comb. Trojan model



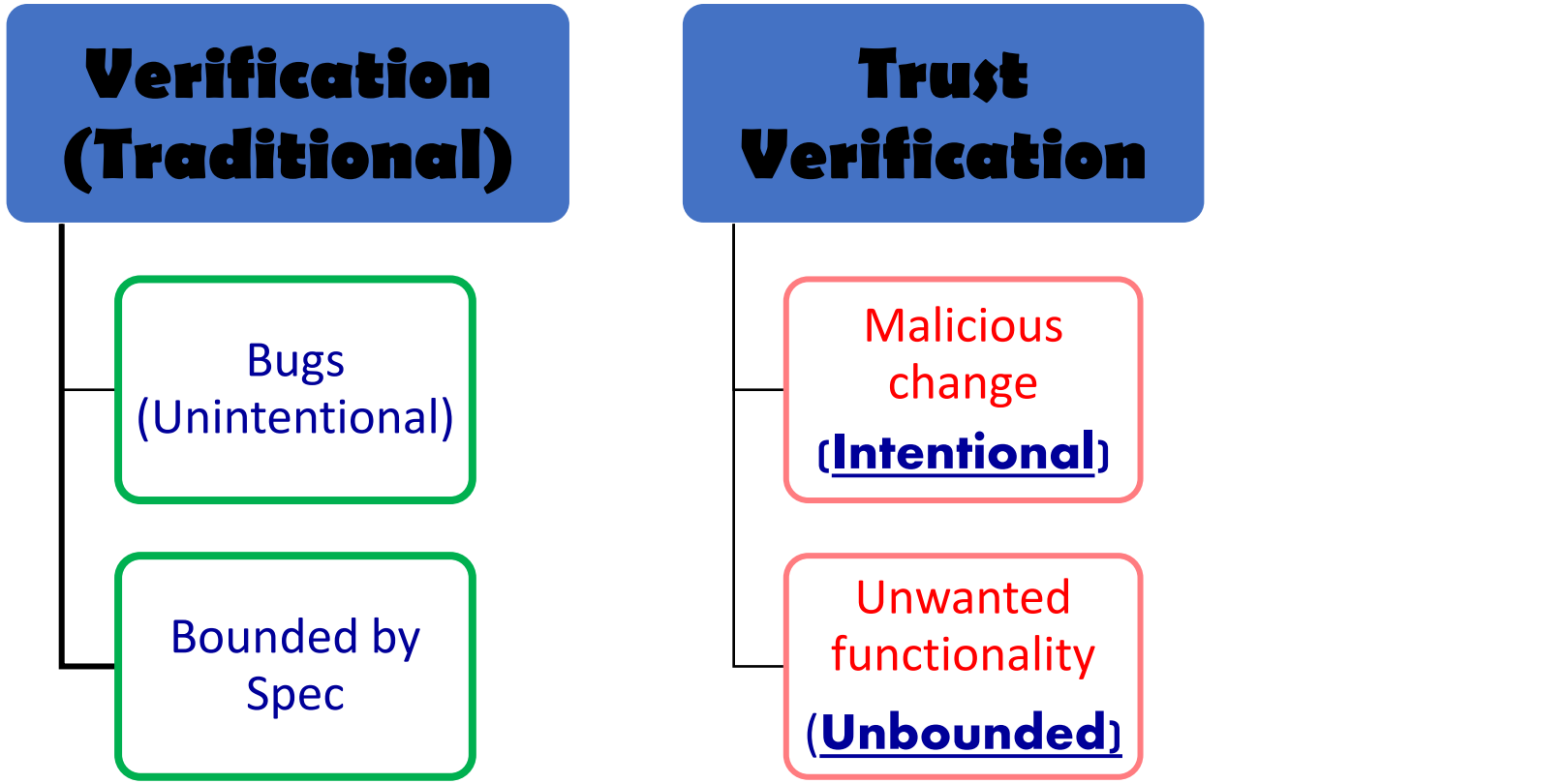
Seq. Trojan Model



**Lin et al, ICCAD 2009*

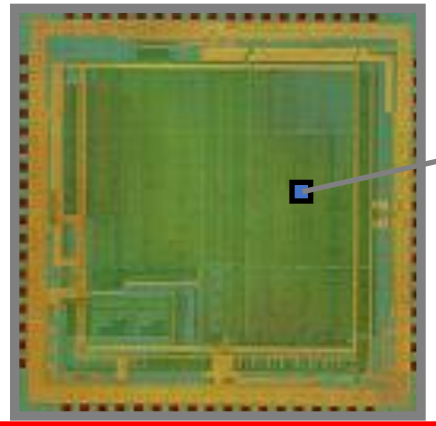
Why is detection of hardware Trojans very difficult?

Bug vs. Malicious Change



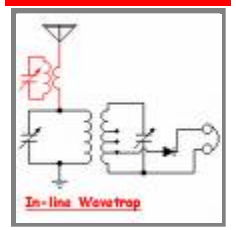
Trojan Attacks → BIGGER verification challenge!

Silicon Back Door



Untrusted Hardware

Antenna



- Adversary can send and receive secret information
- Adversary can disable the chip, blowup the chip, send wrong processing data, impact circuit information etc.

- Adversary can place an Antenna on the fabricated chip
- Such Trojan cannot be detected since it does not change the functionality of the circuit.

Silicon Time Bomb

Untrusted Hardware

Counter

Finite state machine (FSM)

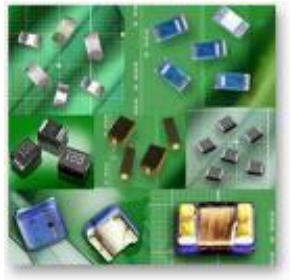
Comparator to monitor key data

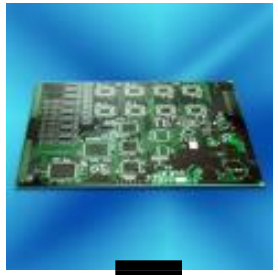
Wires/transistors that violate design rules

- **Such Trojan cannot be detected since it does not change the functionality of the circuit.**
- **In some cases, adversary has little control on the exact time of Trojan action**
- **Cause reliability issue**

Applications and Threats

Thousands of chips are being fabricated in untrusted foundries





Comprehensive Attack Model

Model	Description	3PIP Vendor	SoC Developer	Foundry
A	Untrusted 3PIP vendor	Untrusted	Trusted	Trusted
B	Untrusted foundry	Trusted	Trusted	Untrusted
C	Untrusted EDA tool or rogue employee	Trusted	Untrusted	Trusted
D	Commercial-off-the-shelf component	Untrusted	Untrusted	Untrusted
E	Untrusted design house	Untrusted	Untrusted	Trusted
F	Fabless SoC design house	Untrusted	Trusted	Untrusted
G	Untrusted SoC developer with trusted IPs	Trusted	Untrusted	Untrusted