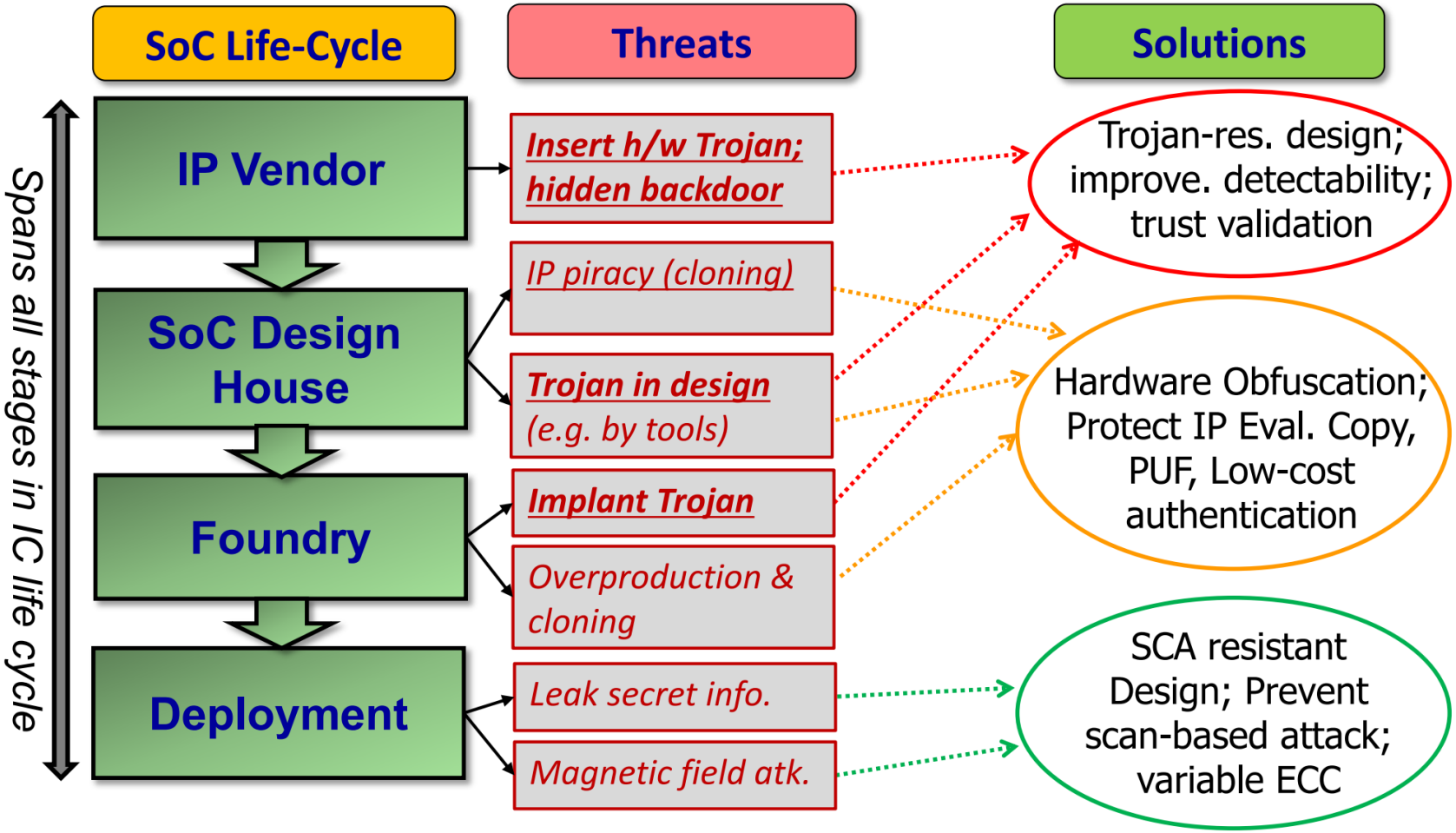
Hardware Trojan

Yu Bi

ELE594 – Special Topic on Hardware Security & Trust

University of Rhode Island

IP 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; variable ECC

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

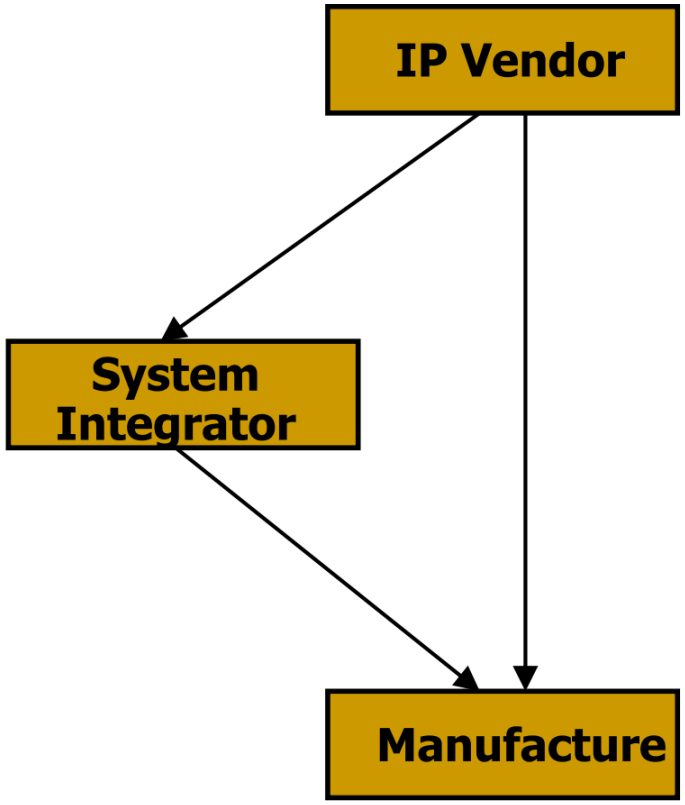
IP Threats

- 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*

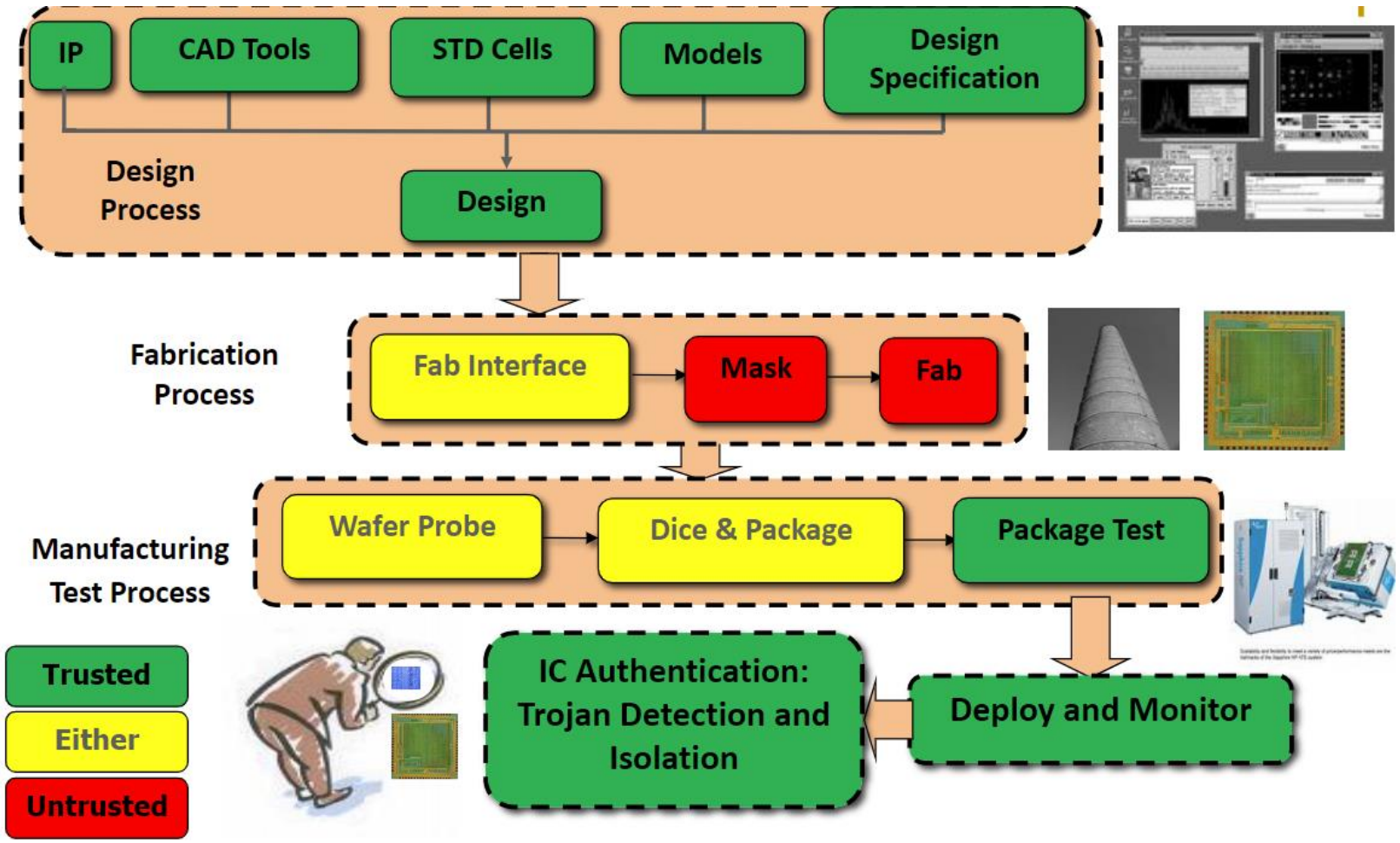
- **Designer and Foundry:**
  - Foundry may place a Trojan in the layout design.
  - *IC Trust problem*

Hardware Trojan Threats

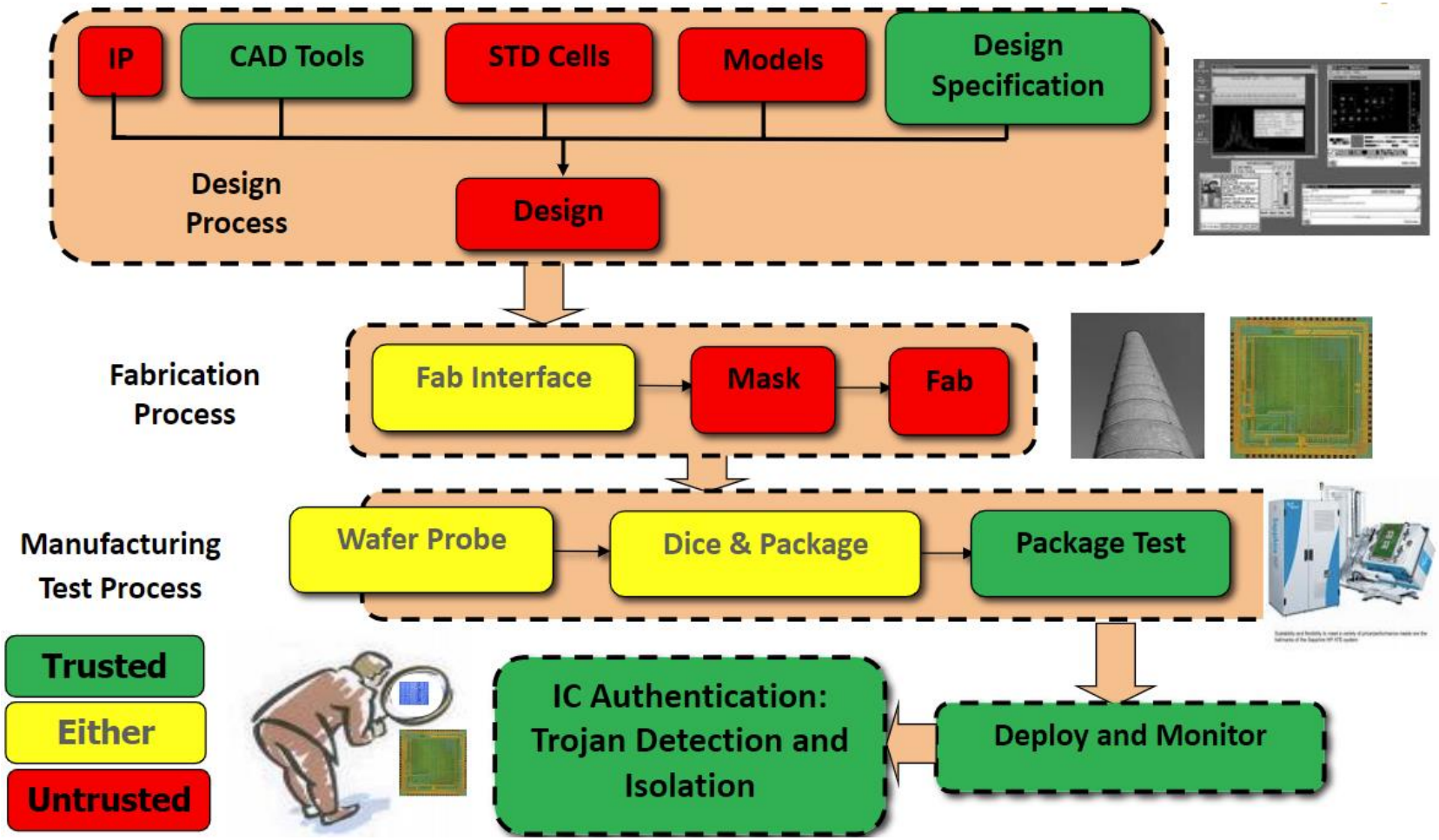


Any of these steps can be untrusted

Untrusted Foundry

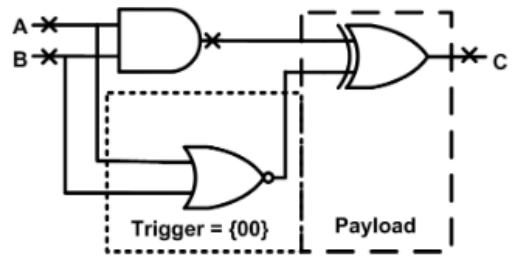


Untrusted Designer

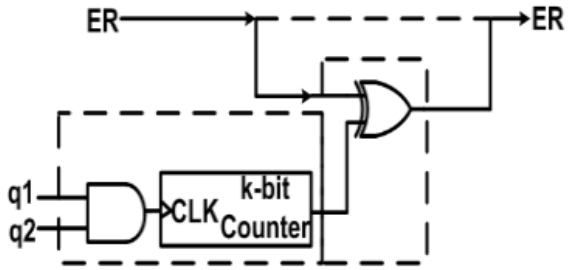


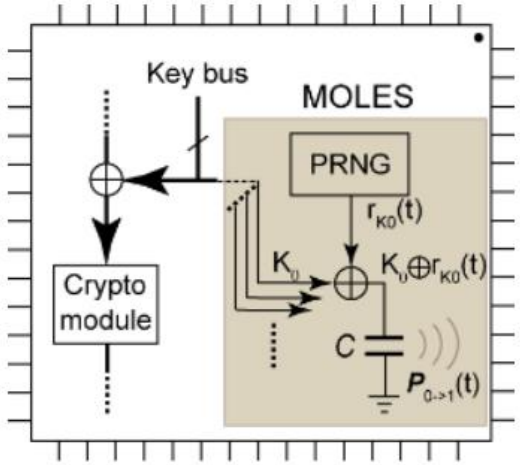
Hardware Trojan Examples

Comb. Trojan Example

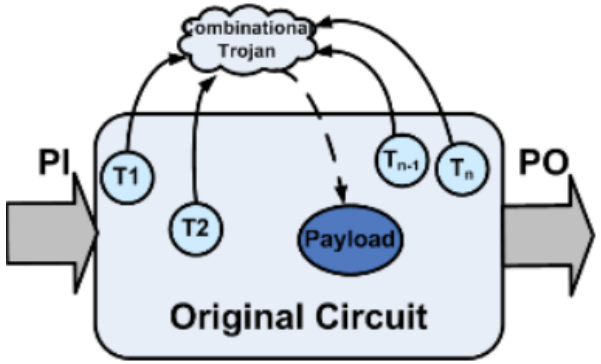


Seq. Trojan Example

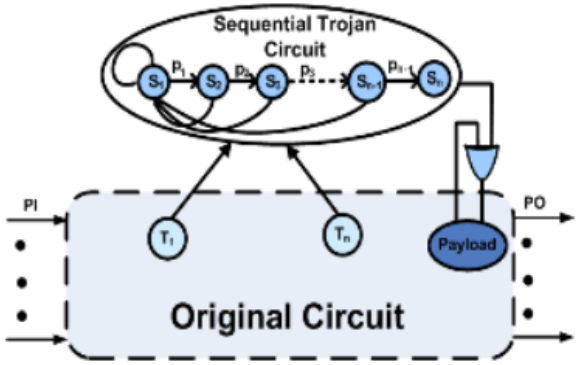




Comb. Trojan model



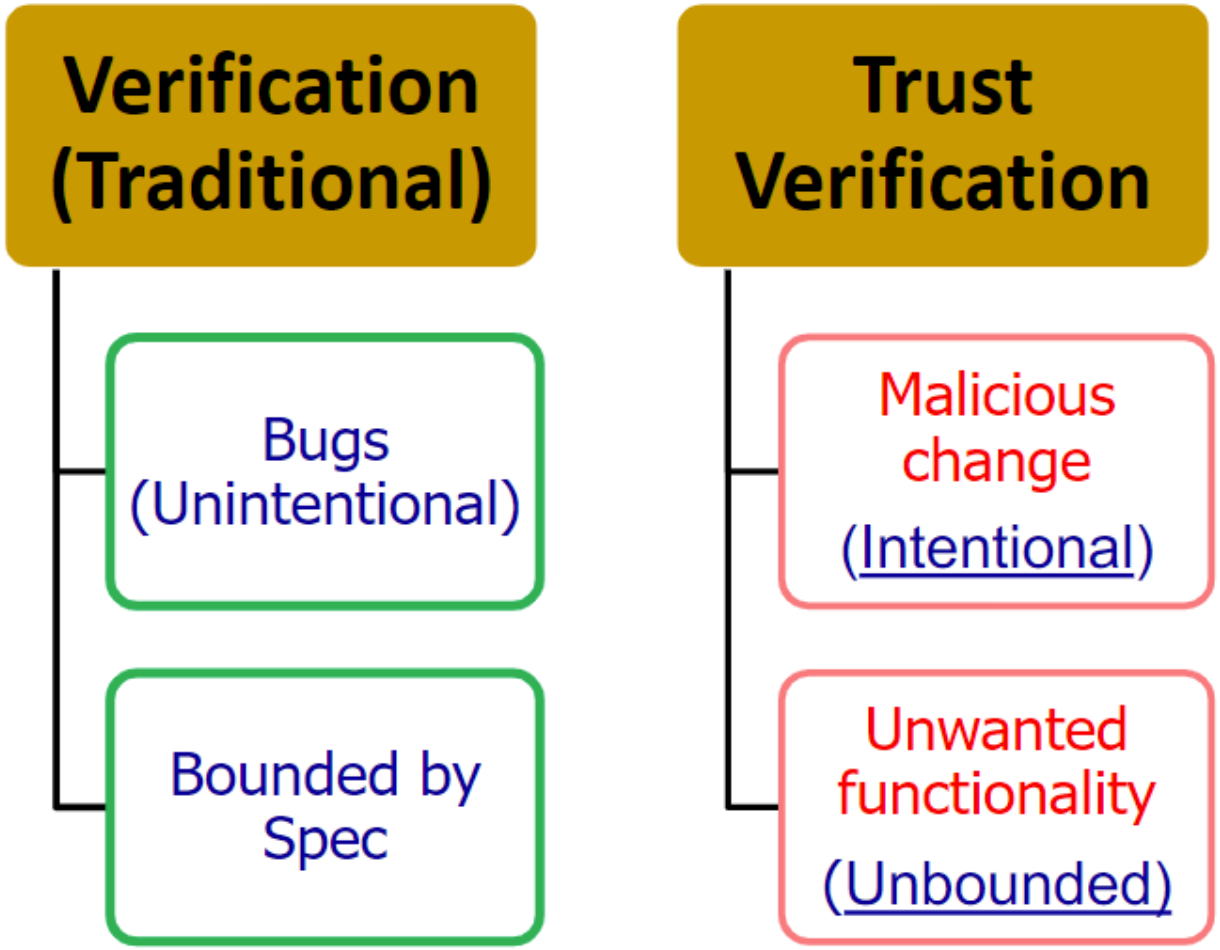
Seq. Trojan Model



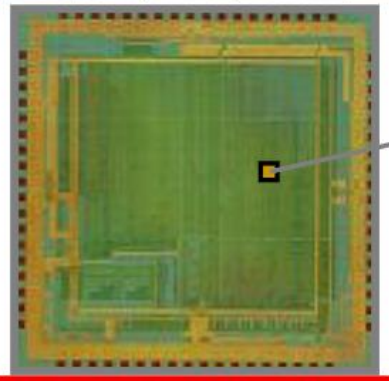
Fishy Chips: Spies Want to Hack-Proof Circuits

HW Trojan evidence!

Bug vs. Trojan

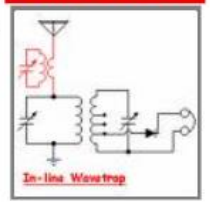


Backdoor



Untrusted Hardware

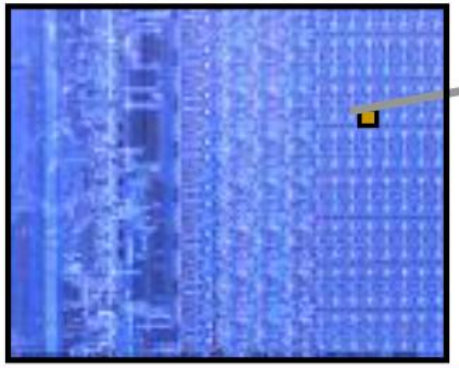
Antenna



- 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.

Time Bomb



Untrusted Hardware

Counter

Finite state machine (FSM)

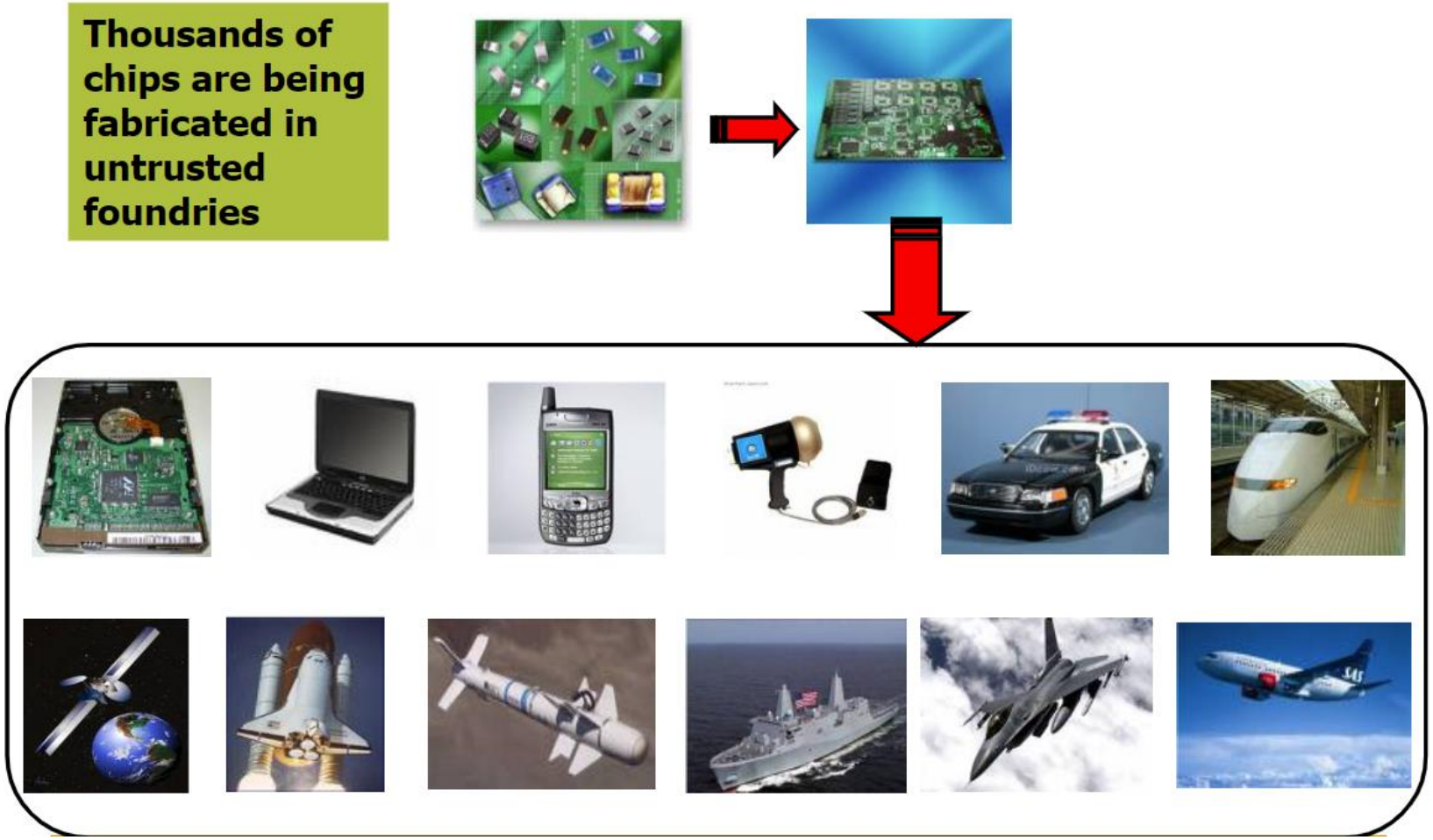
Comparator to monitor key data

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

Hardware Trojan Threats

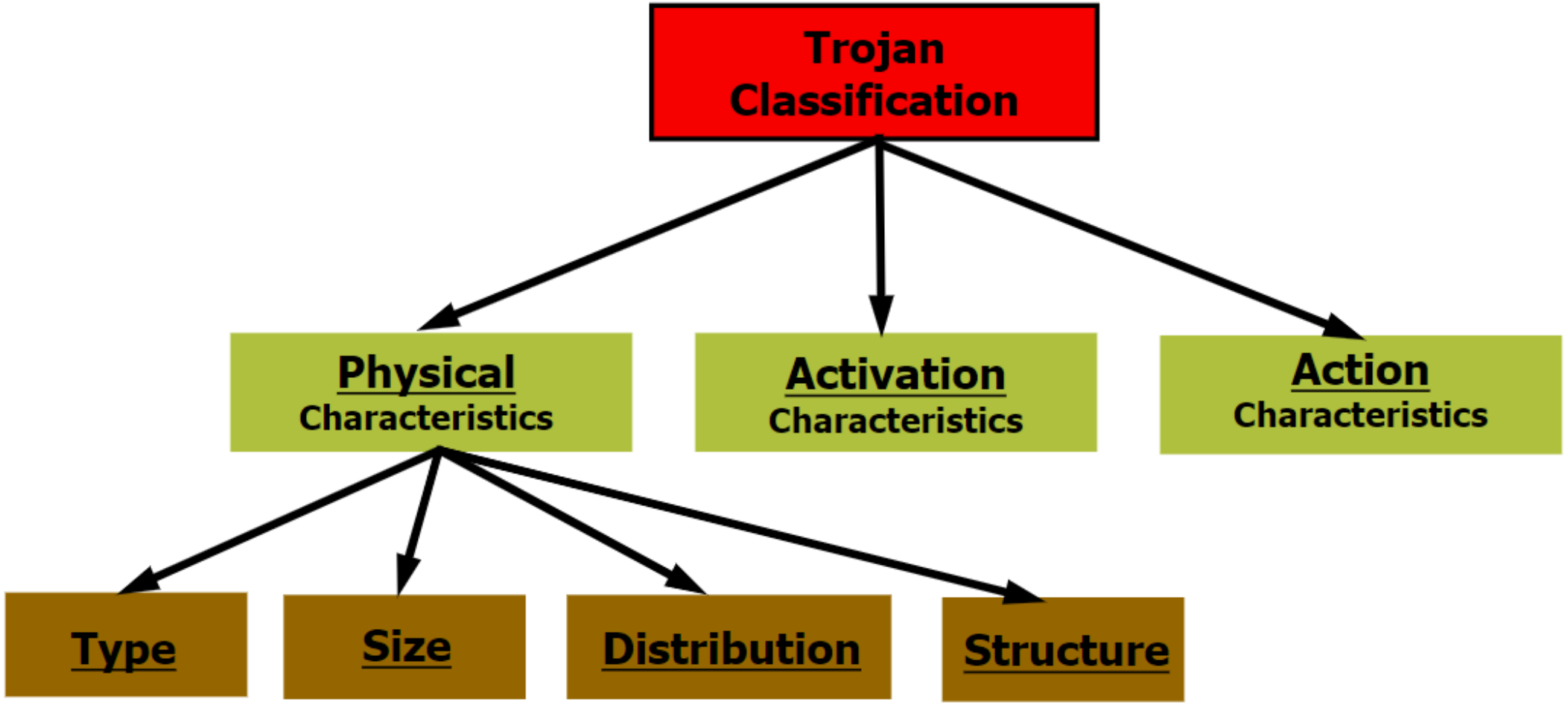
Thousands of chips are being fabricated in untrusted foundries



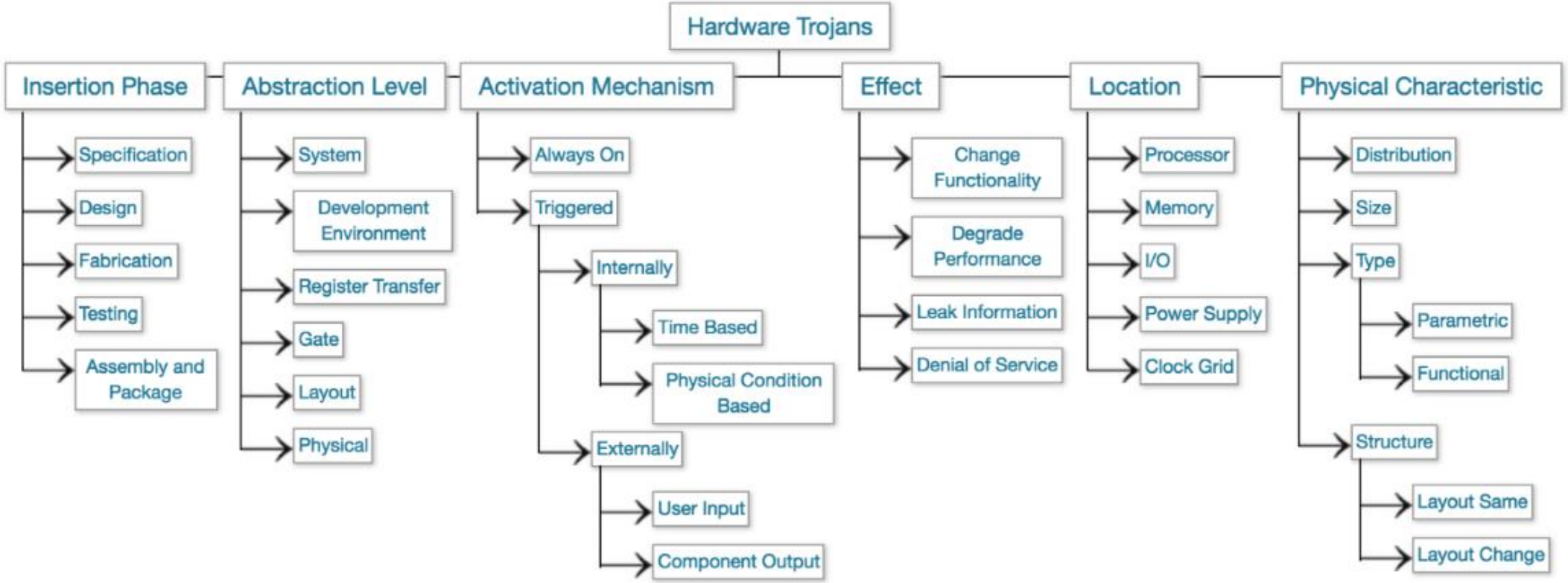
Threat Models

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

Trojan Taxonomy

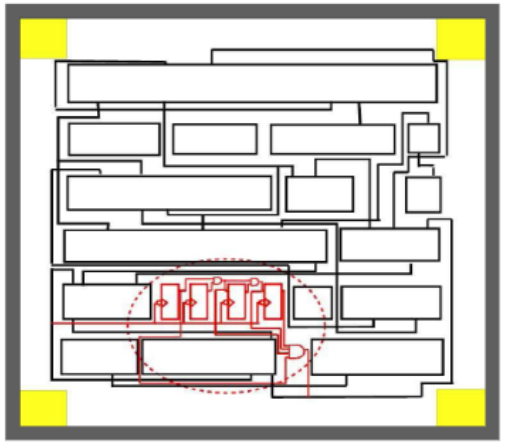


Trust-Hub

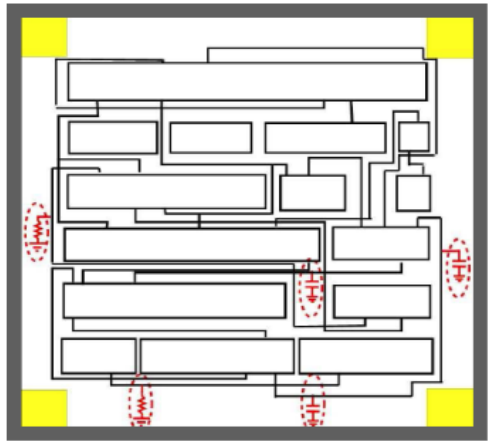

Hardware Trojans
Insertion Phase
Specification
Design
Fabrication
Testing
Assembly and Package
Abstraction Level
System
Development Environment
Register Transfer
Gate
Layout
Physical
Activation Mechanism
Always On
Triggered
Internally
Time Based
Physical Condition Based
Externally
User Input
Component Output
Effect
Change Functionality
Degrade Performance
Leak Information
Denial of Service
Location
Processor
Memory
I/O
Power Supply
Clock Grid
Physical Characteristic
Distribution
Size
Type
Parametric
Functional
Structure
Layout Same
Layout Change

Layout-layer Trojan

Functional



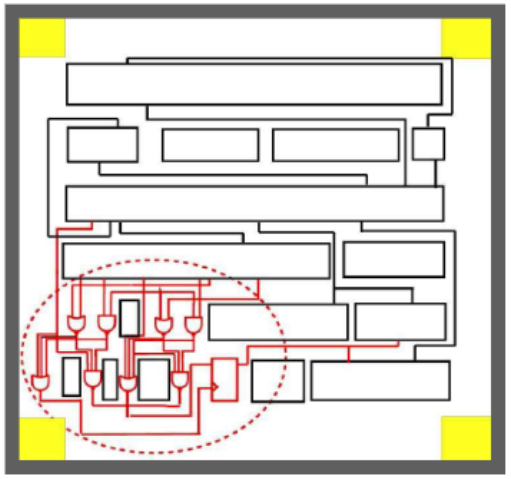
Parametric



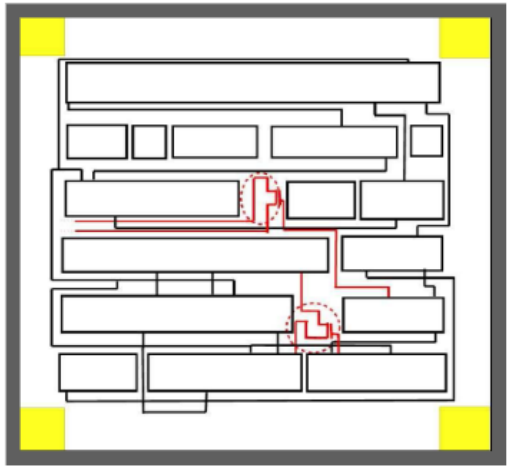
- **Functional**
  - Addition or deletion of components
  - Sequential circuits
  - Combinational circuits
  - Modification to function or no change
- **Parametric**
  - Modifications of existing components
    - Wire: e.g. thinning of wires
    - Logic: Weakening of a transistor, modification to physical geometry of a gate
    - Modification to power distribution network
  - Sabotage reliability or increase the likelihood of a functional or performance failure

Layout-layer Trojan

Big



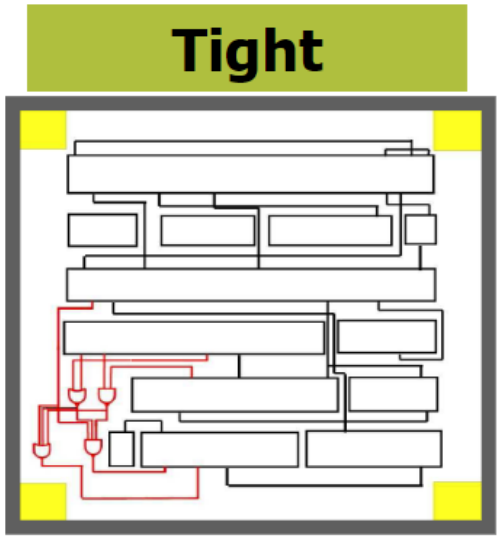
Small

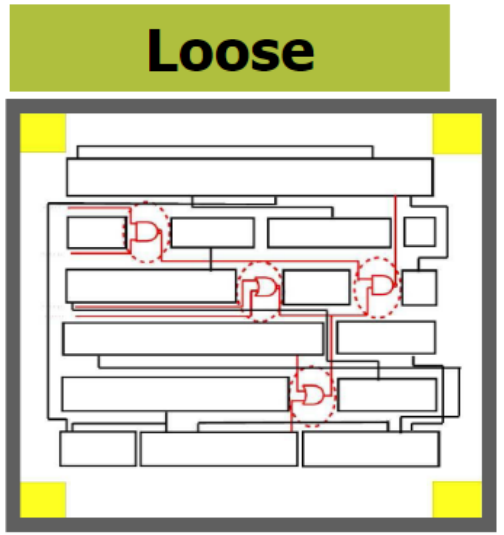


- **Size:**
  - **Number of components added to the circuit**
    - **Small transistors**
    - **Small gates**
    - **Large gates**

- **In case of layout, depends on availability of:**
  - **Dead spaces**
  - **Filler cells**
  - **Decap cells**
  - **Change in the structure**

Layout-layer Trojan



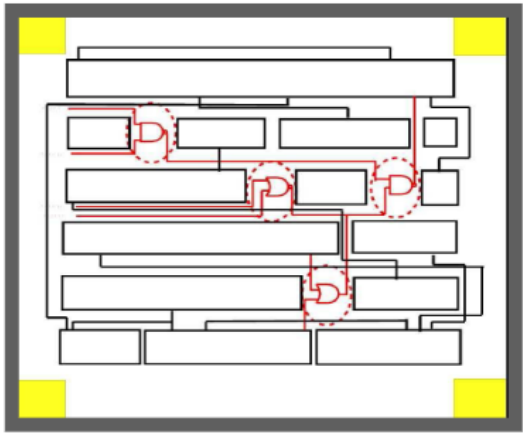


- **Tight Distribution**
  - Trojan components are topologically close in the layout
- **Loose Distribution**
  - Trojan components are dispersed across the layout of a chip

- **Distribution of Trojans depends on the availability of dead spaces on the layout**

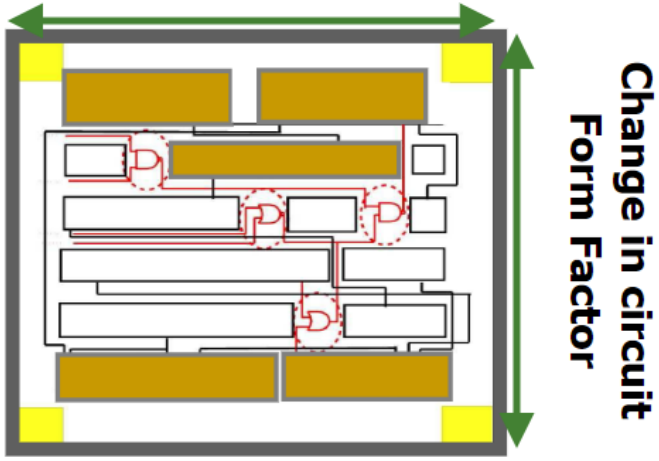
Layout-layer Trojan

No-change



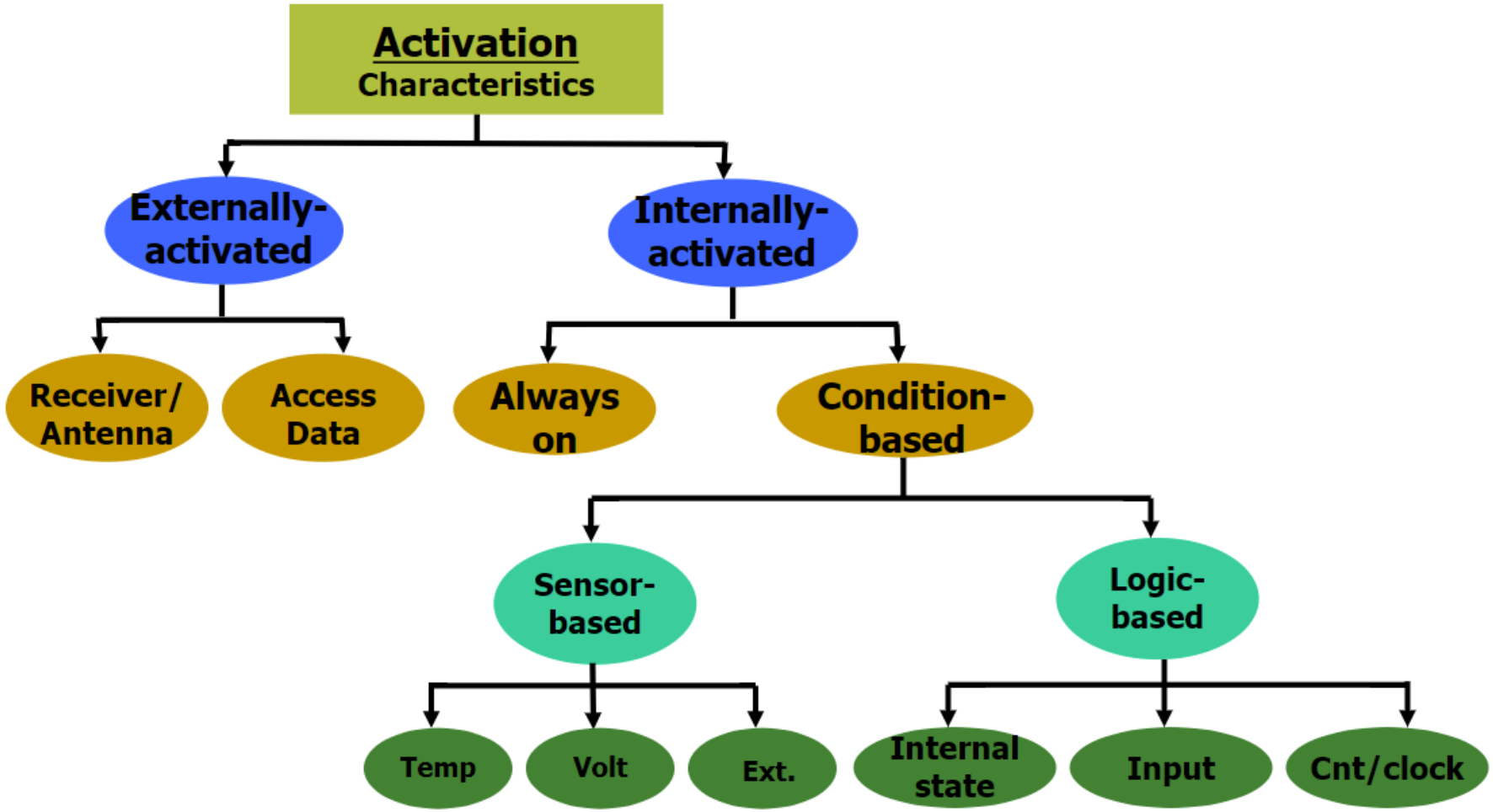
- The adversary may be forced to regenerate the layout to be able to insert the Trojan, then the chip dimensions change
  - It could result in different placement for some or all the design components

Modified Layout

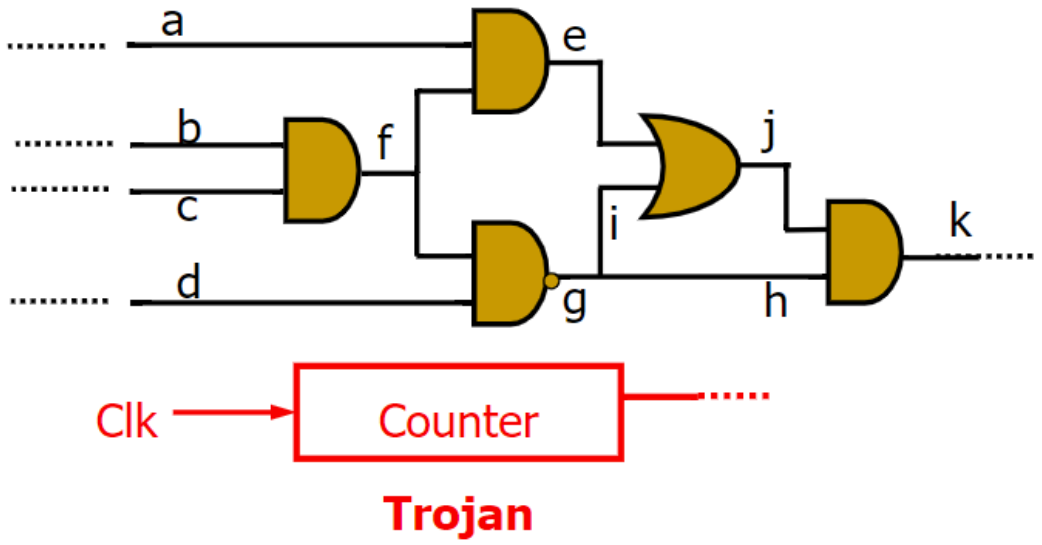


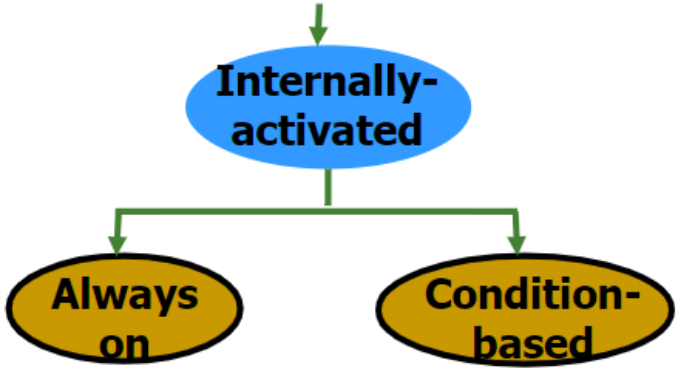
- A change in physical layout can change the delay and power characteristics of chip
  - It is easier to detect the Trojan

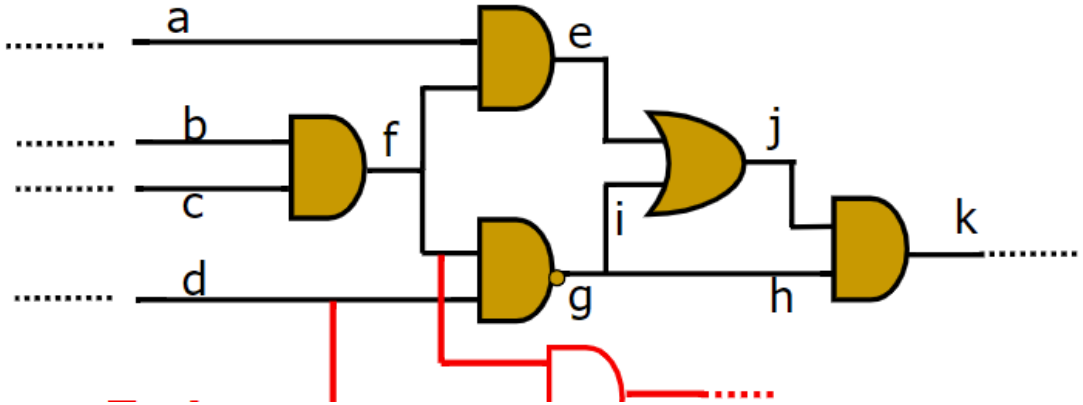
Trojan Activation



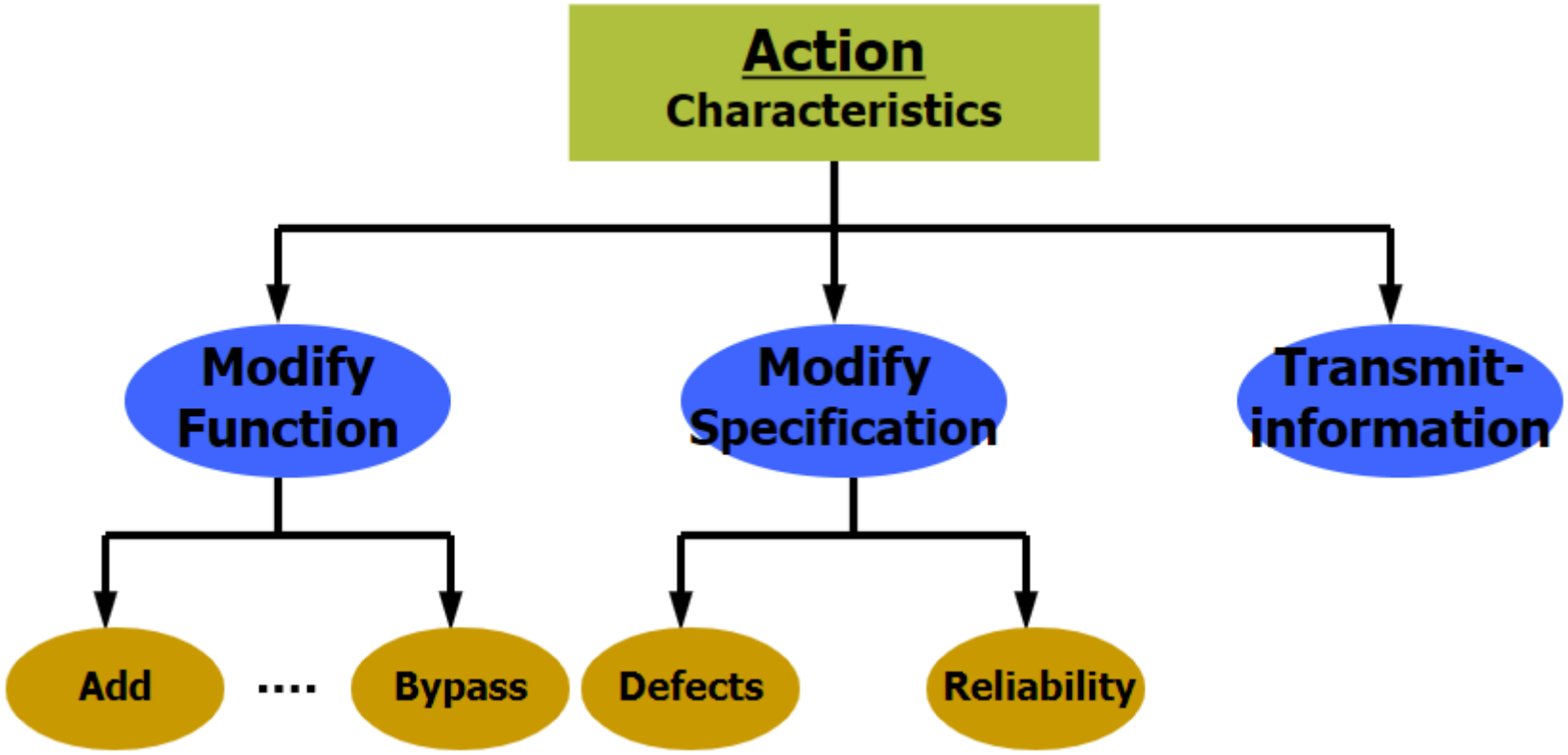
Trojan Activation



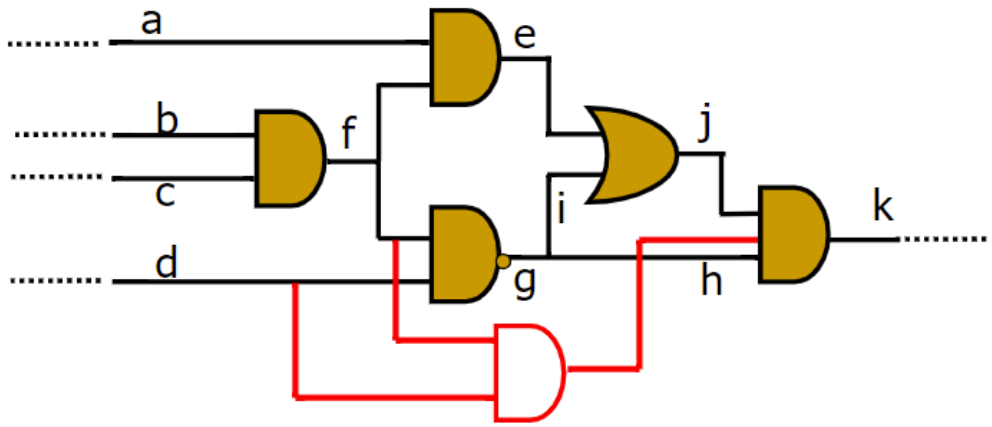




Trojan Activation



Trojan Activation



Modify Function

Modify Specification:

Noise, Delay and Temperature