Hardware Trust

Giorgio Di Natale, Elena Ioana Vatajelu

21.09.2023

License Information

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Motivation

- **Hardware/software security** and **trust** play nowadays critical roles as computing is intimately integrated into many infrastructures that we depend on

- Hardware Security
  - dealing with (secret) data in hardware devices
- Hardware Trust
  - dealing with design, manufacturing and life cycle of devices

Overview

- Introduction
- The product life-cycle chain
- Counterfeiting types
- Counterfeiting detection
- Counterfeiting prevention

Counterfeiting

- Counterfeiting of integrated circuits has become a major challenge
  - deficiencies in the existing test solutions
    - due also to the extremely high complexity of systems
  - lack of low-cost and effective avoidance mechanisms in place
- Numbers:
  - $50 billion lost in revenue in 2021 (in semiconductors)
  - E.g., in 2021 over 20% of mobile phone devices sold across the world are counterfeit products (around 180million devices yearly)

Which is the cause?

- Complexity of the electronic systems significantly increased over the past few decades

- Everything in this picture is now in your pocket

Which is the cause?

- Complexity of the electronic systems significantly increased over the past few decades
  - To **reduce production cost**, they are mostly fabricated and assembled globally
- This **globalization** has led to an illicit market willing to undercut the competition with counterfeit and fake parts
- Poorly controlled **E-waste**

Facts

- In November 2011, Semiconductor Industry Association (SIA) President Brian Toohey said:
  - …as many as **15%** of all spare and replacement semiconductors purchased by the Pentagon are **counterfeit**
- E-waste is considered the fastest-growing waste stream in the world
  - 44.7 million tonnes generated in 2016
    - equivalent to 4500 Eiffel towers!
  - In 2019 an estimate of 53.6 million tonne of e-waste was reported, with a 7.3 kg per capita average
  - In 2021, less than 20% of the e-waste is collected and recycled

http://www.semiconductors.org/news/2011/11/08/news_2011/sia_president_testifies_at_senate_armed_services_committee_on_dangers_of_counterfeit_chips/

Stories

- November 8, 2011, the United States Committee on Armed Services held a hearing on an investigation of counterfeit electronic parts in the defense supply chain
- The investigation had revealed alarming facts: materials used to make counterfeit electronic (a.k.a. e-waste) parts are shipped from the United States and other countries

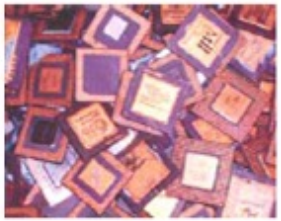
http://www.industryweek.com/procurement/ticking-time-bomb-counterfeit-electronic-parts

Stories (2)

- The e-waste is sent to cities like Shantou, China, where:
  - It is disassembled by hand, washed in dirty river water, and dried on the city sidewalk
  - It is sanded down to remove the existing part number or other markings that indicate its quality or performance
  - False markings are placed on the parts that lead the average person to believe they are new or high-quality parts

Millions of Scrap Boards

Component Removal



Sorted by size, similarity and lead count

Re-processed

Good

Clean facilities

Packaging

Testing

Marking

Good vs. Bad

Clean facilities

Packaging

Testing

Marking

De-soldering

De-packaging

Re-marking

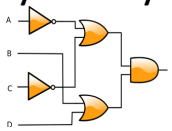
Overview

- Introduction
- The product life-cycle chain
- Counterfeiting types
- Counterfeiting detection
- Counterfeiting prevention

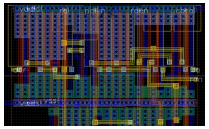
Microelectronics Industry

HW Description Language

Synthesys



Place and Route



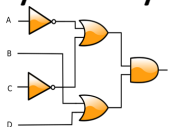
Silicon Foundry
(Fabrication)

Distribution

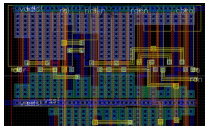
Microelectronics Industry

HW Description Language

Synthesys



Place and Route



Silicon Foundry
(Fabrication)

Distribution

One company

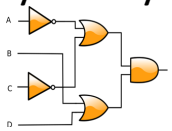
- Design specifications
- Design tools
- Fabrication process
- IC test
- IC lifetime behavior
- IC distribution

Trusted Product

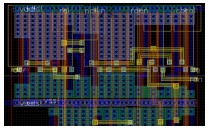
Microelectronics Industry

HW Description Language

Synthesys



Place and Route



Silicon Foundry (Fabrication)

Distribution

One company
- Design specifications
- Design tools
- Fabrication process
- IC test
- IC lifetime behavior
- IC distribution

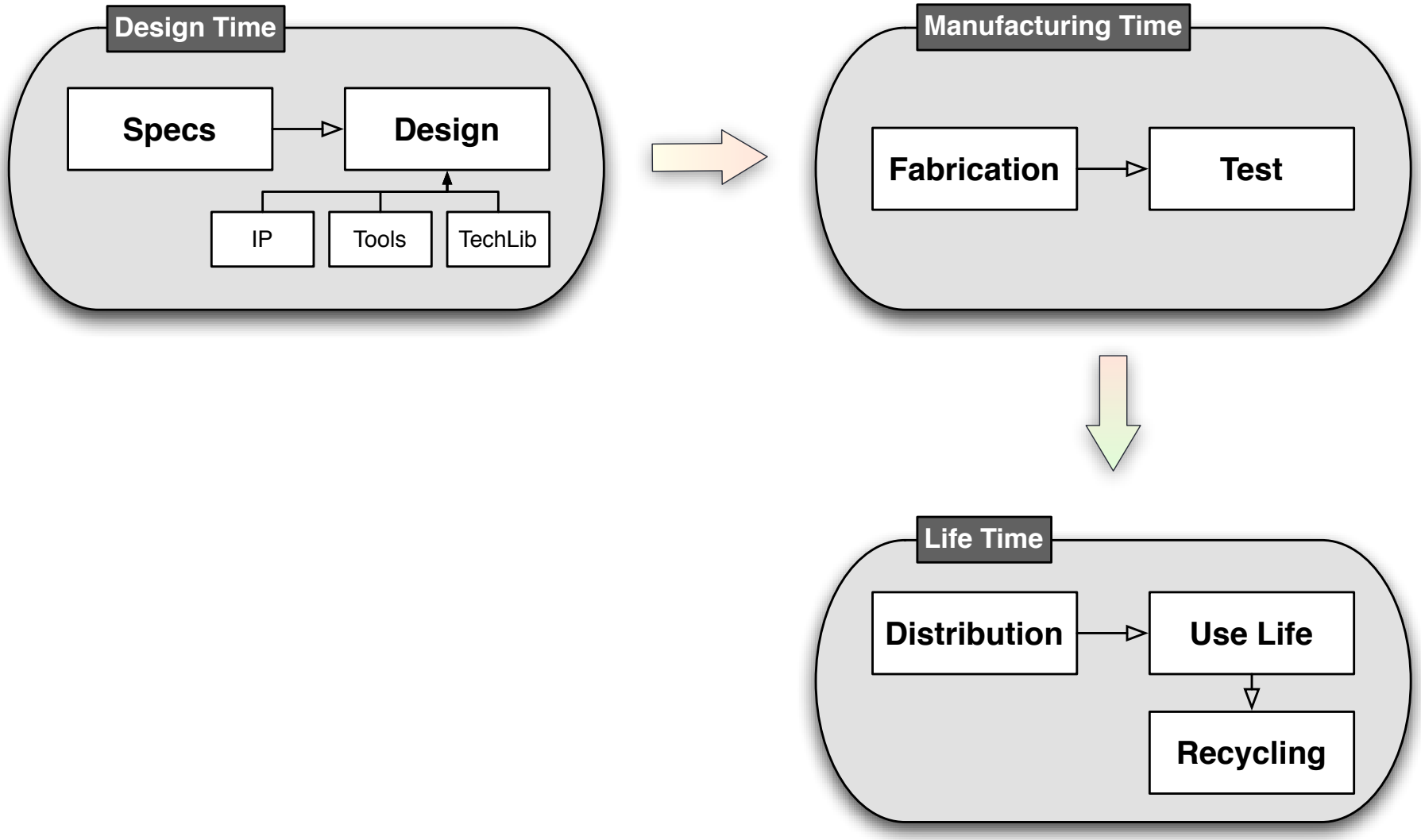
Trusted Product

Multiple companies
- C1: Design specifications
- C2*: Design tools
- C3*: Fabrication process
- C4*: IC test
- C4*: IC lifetime behavior
- C1: IC distribution

Untrusted Product

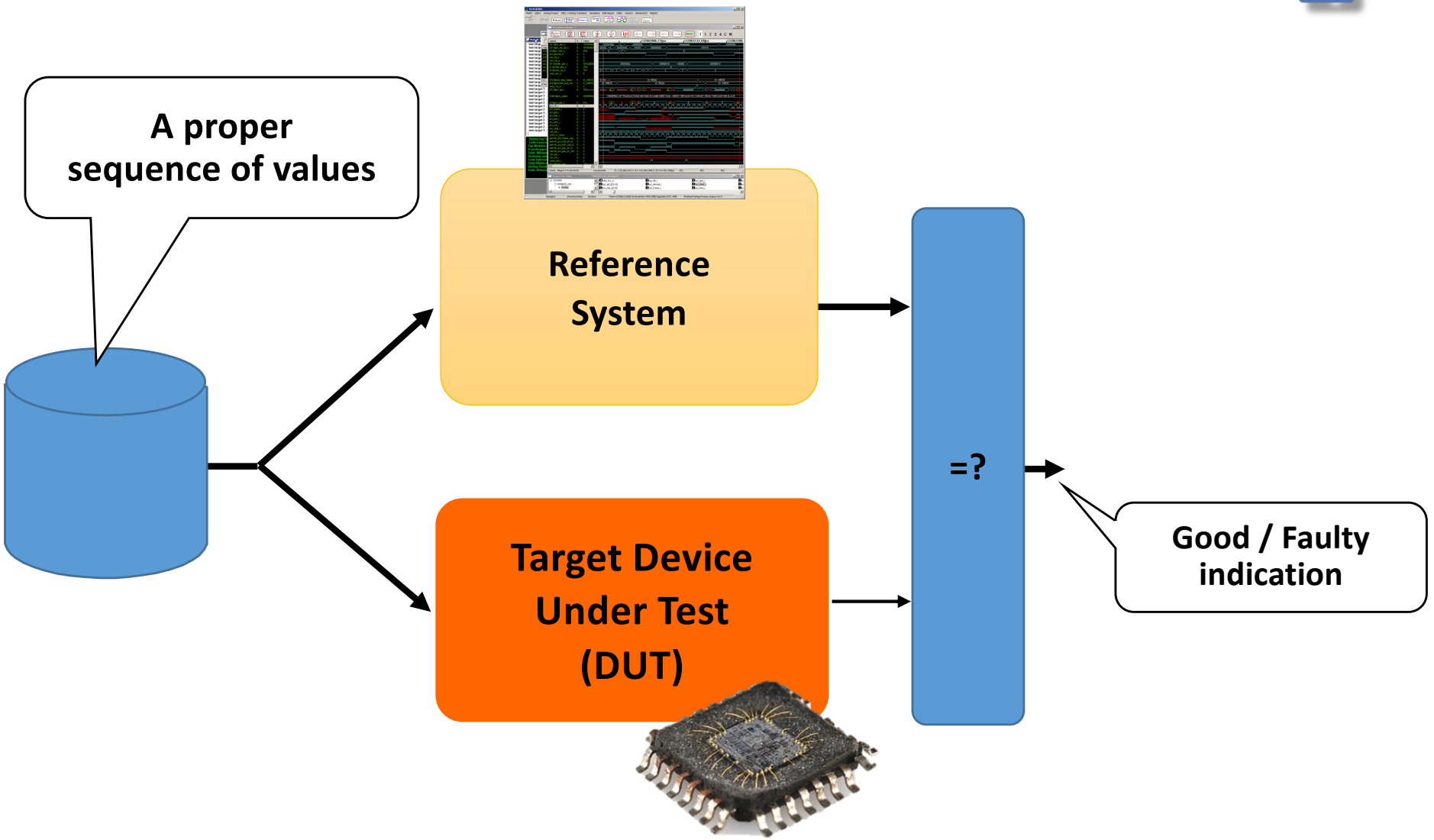
M. Tehranipoor, "Introduction to Hardware Security and Trust"

The Trusted Chain



VLSI Testing

The basic approach to Testing

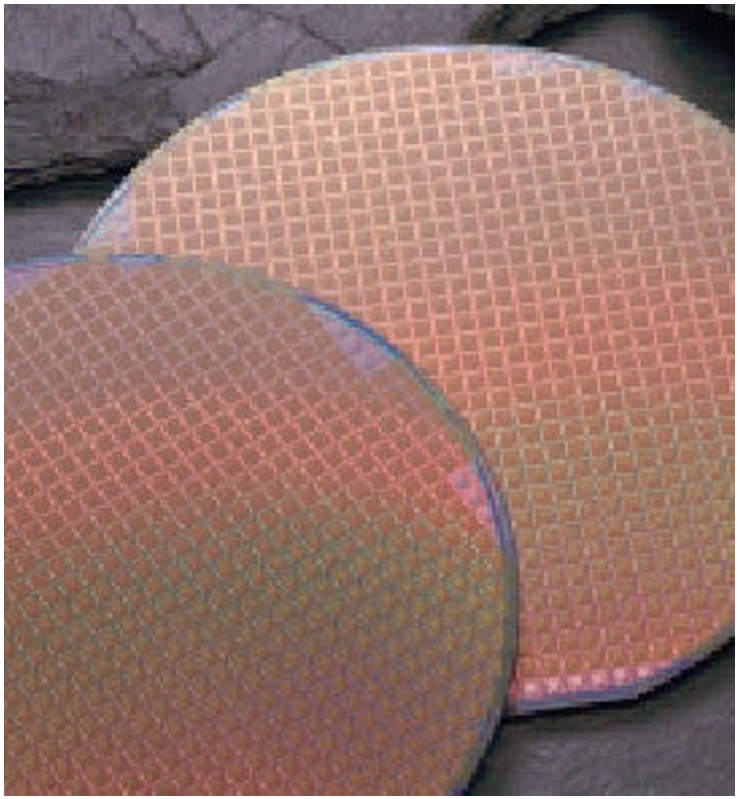


IC production test

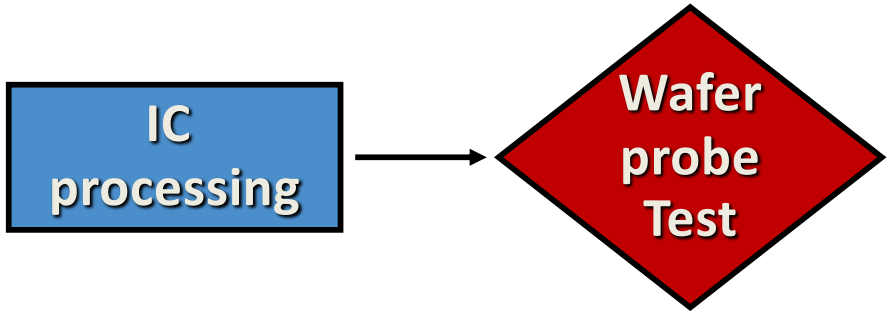
IC processing

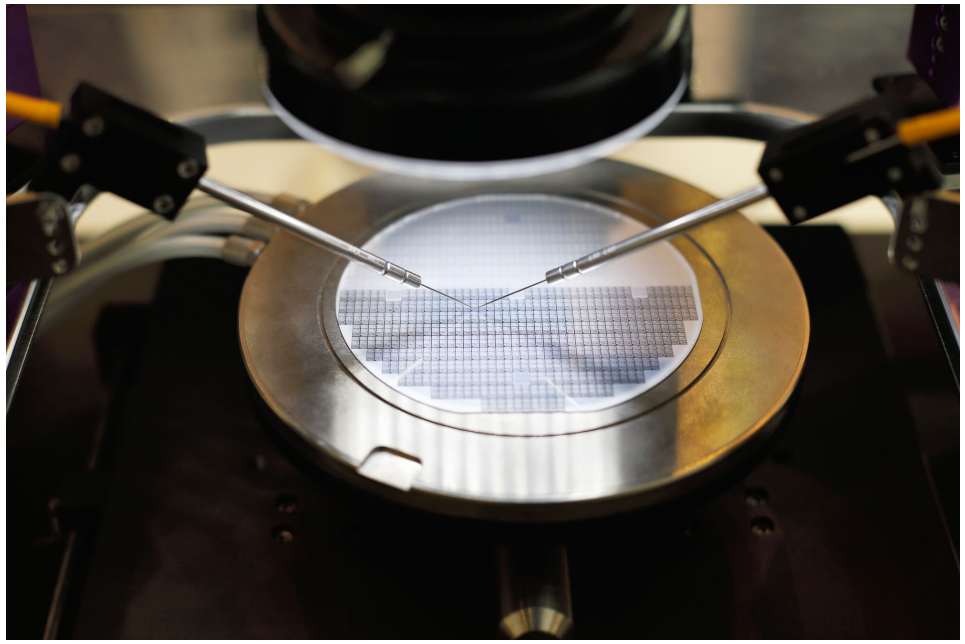
IC production test

IC processing

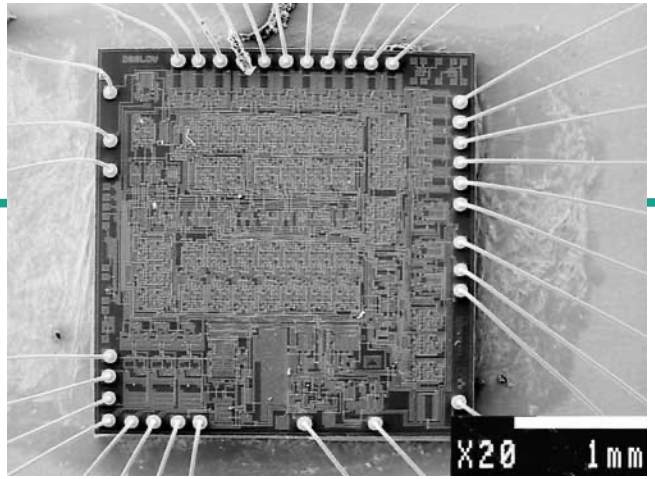


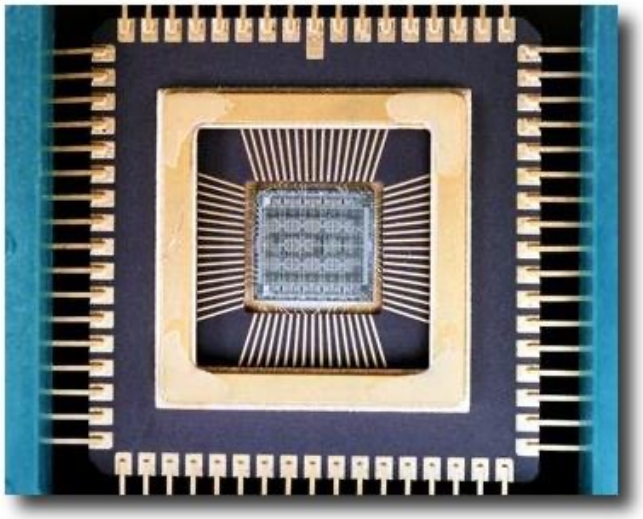
IC production test



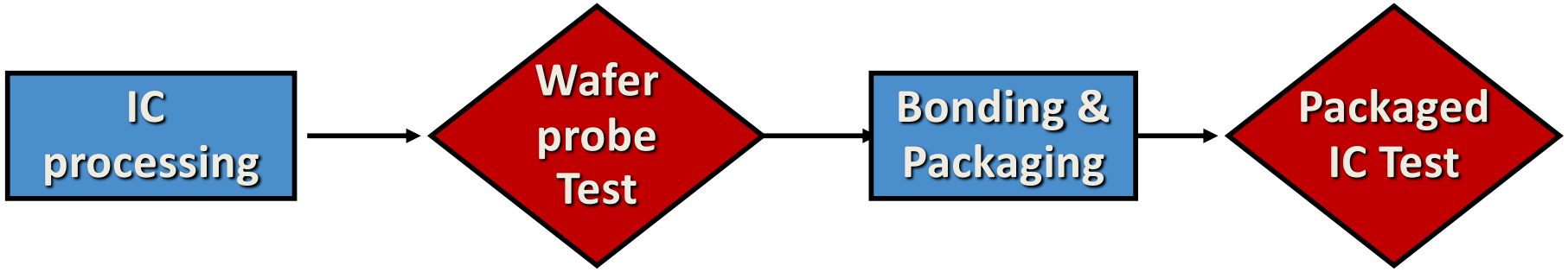


IC production test

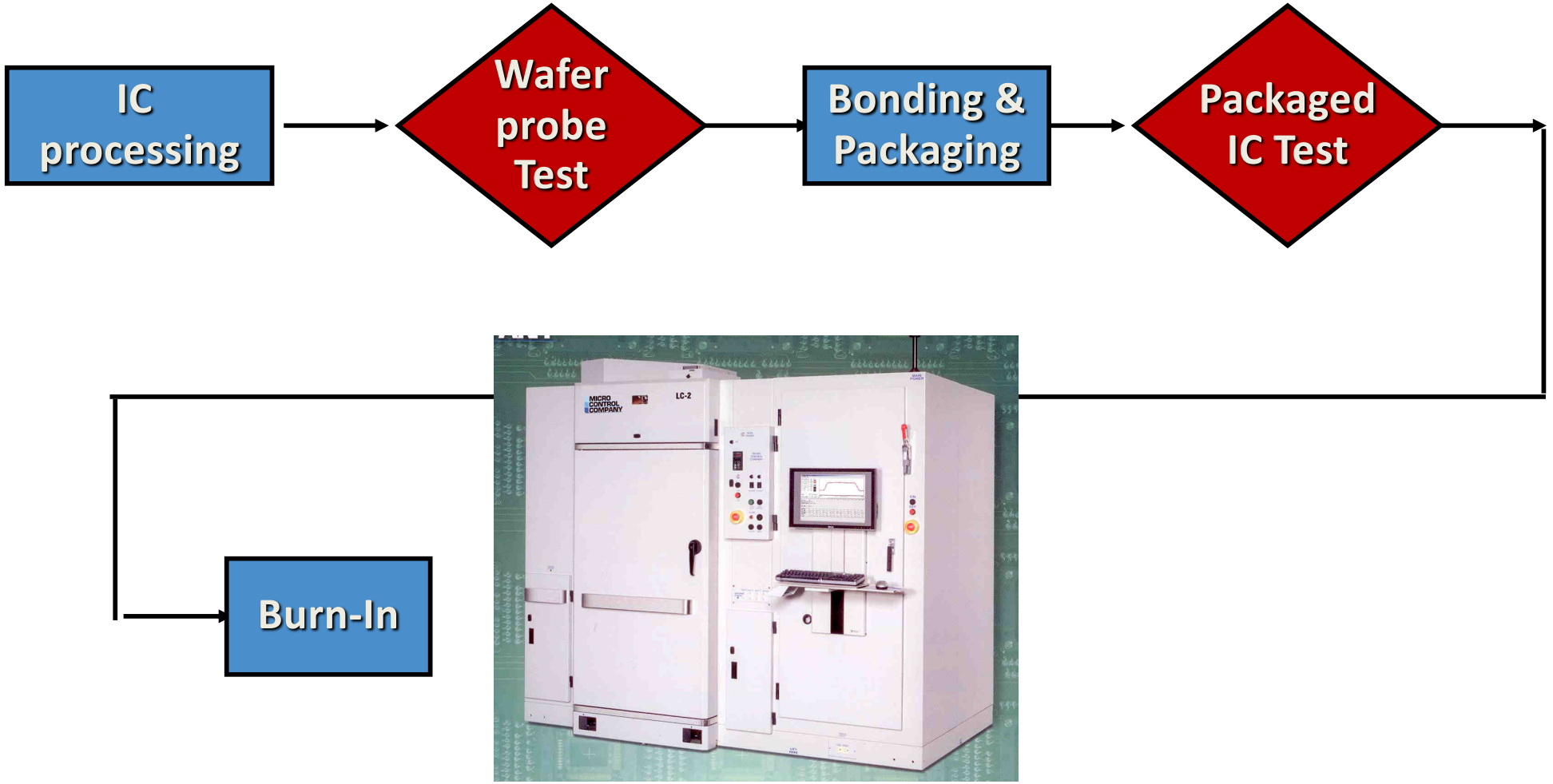




IC production test



IC production test



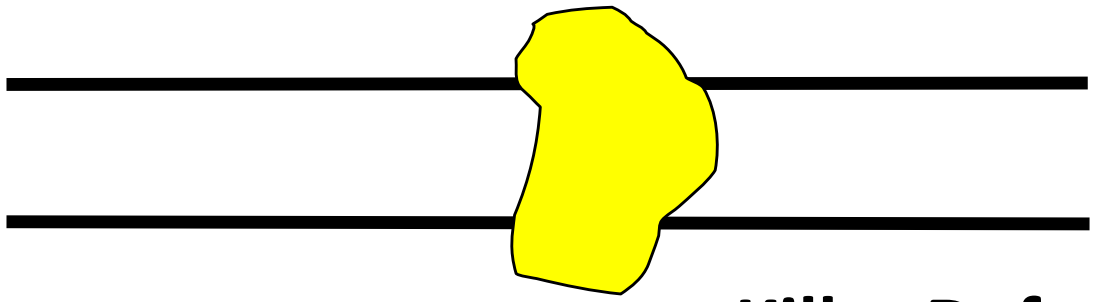
Burn-in tests

- Between 1% and 0.1% of circuits that pass wafer probe testing have latent defects

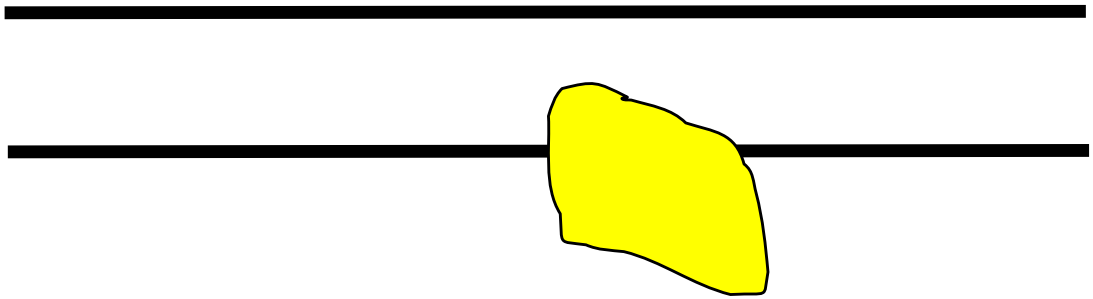
  >> 10,000 to 1000 DPM

- Must be screened by Burn-in tests

The Problem of Latent Defects

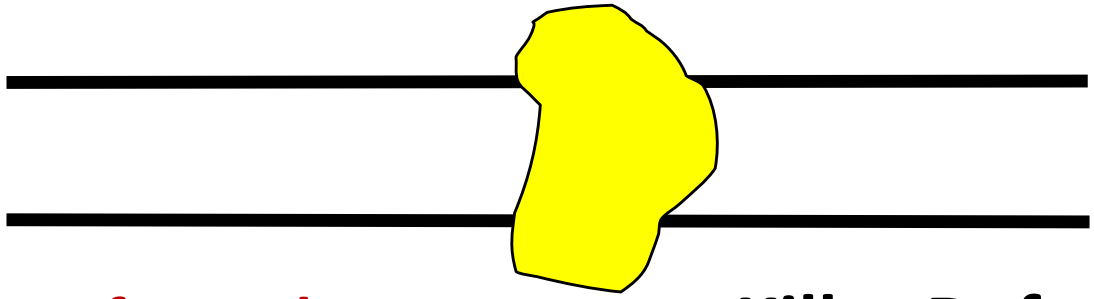


Killer Defect



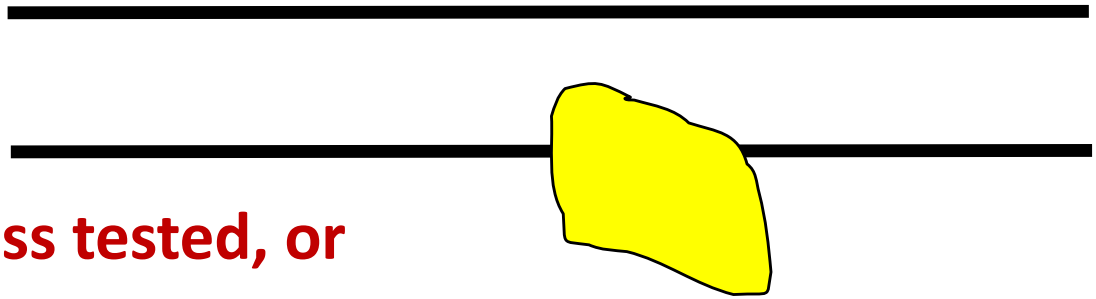
Latent Defect

The Problem of Latent Defects



Detected at wafer probe

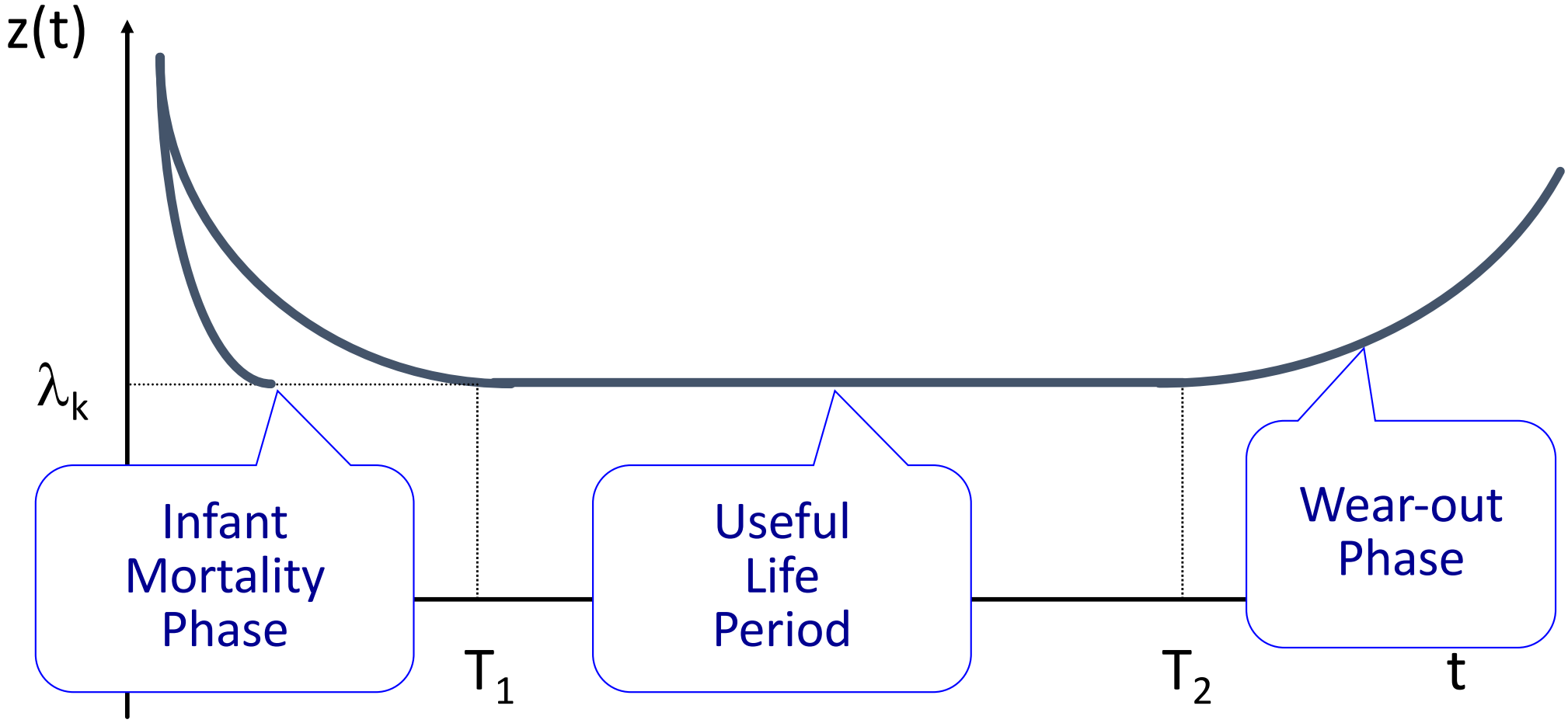
Killer Defect



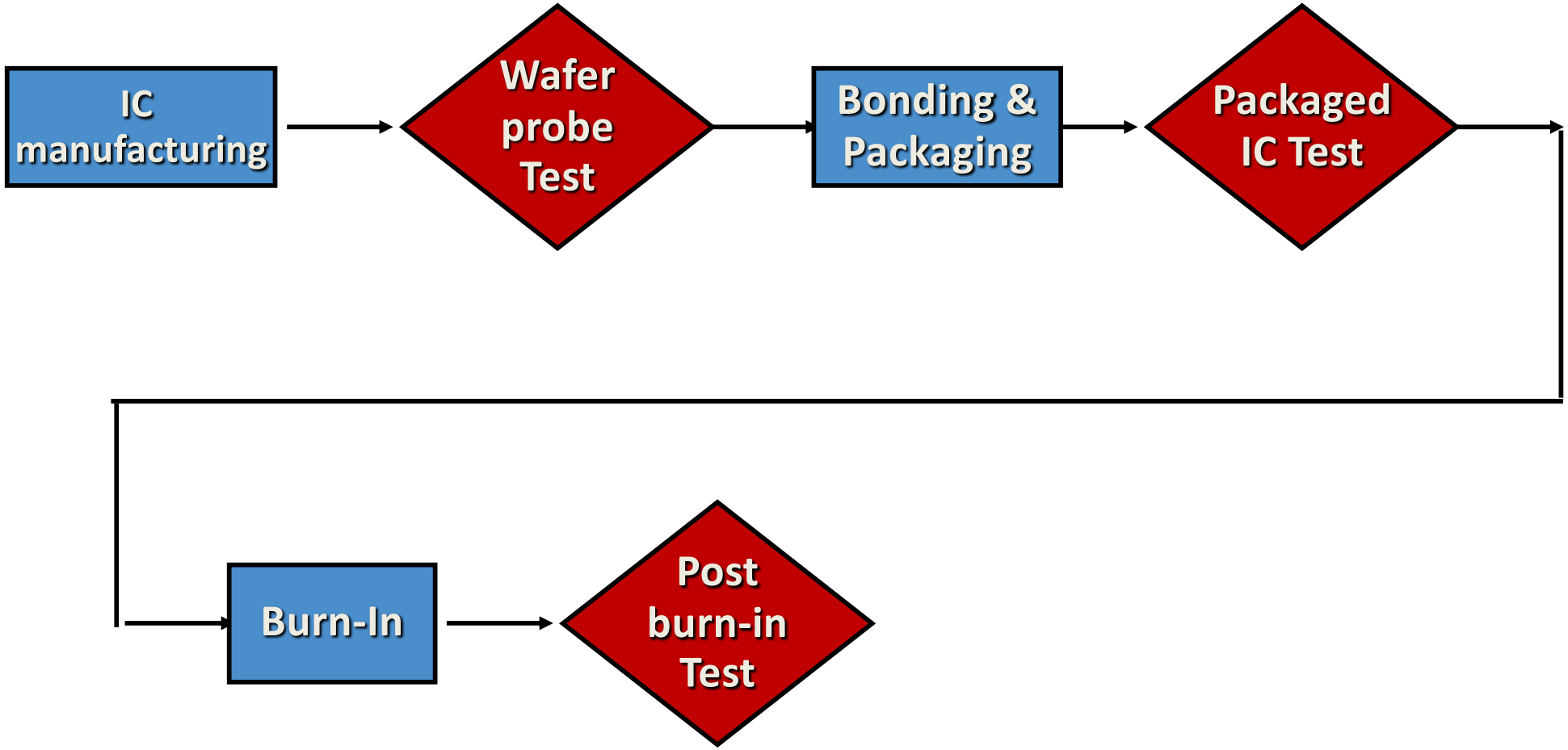
Must be stress tested, or screened

Latent Defect

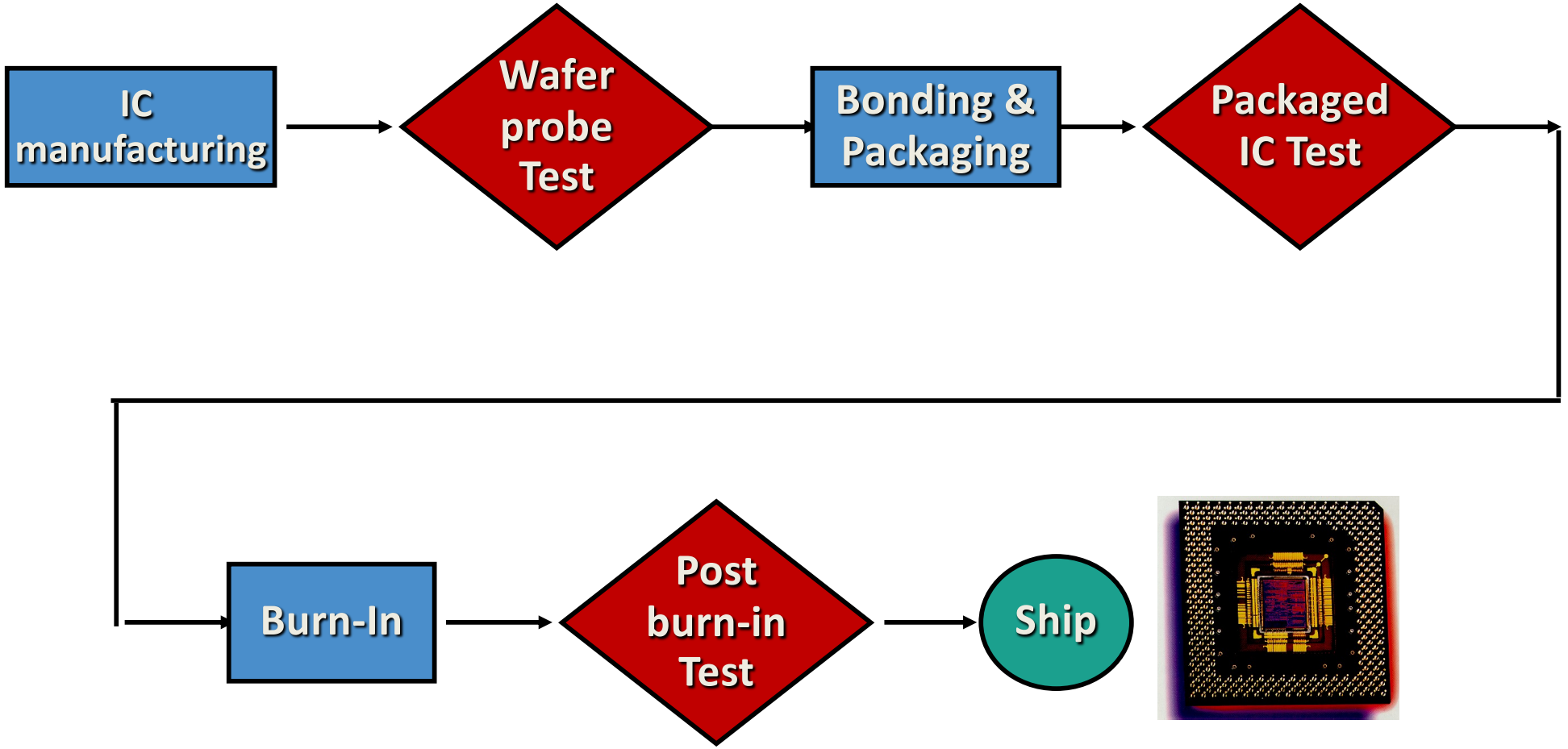
Failure Rate Function (Bathtub curve relationship)



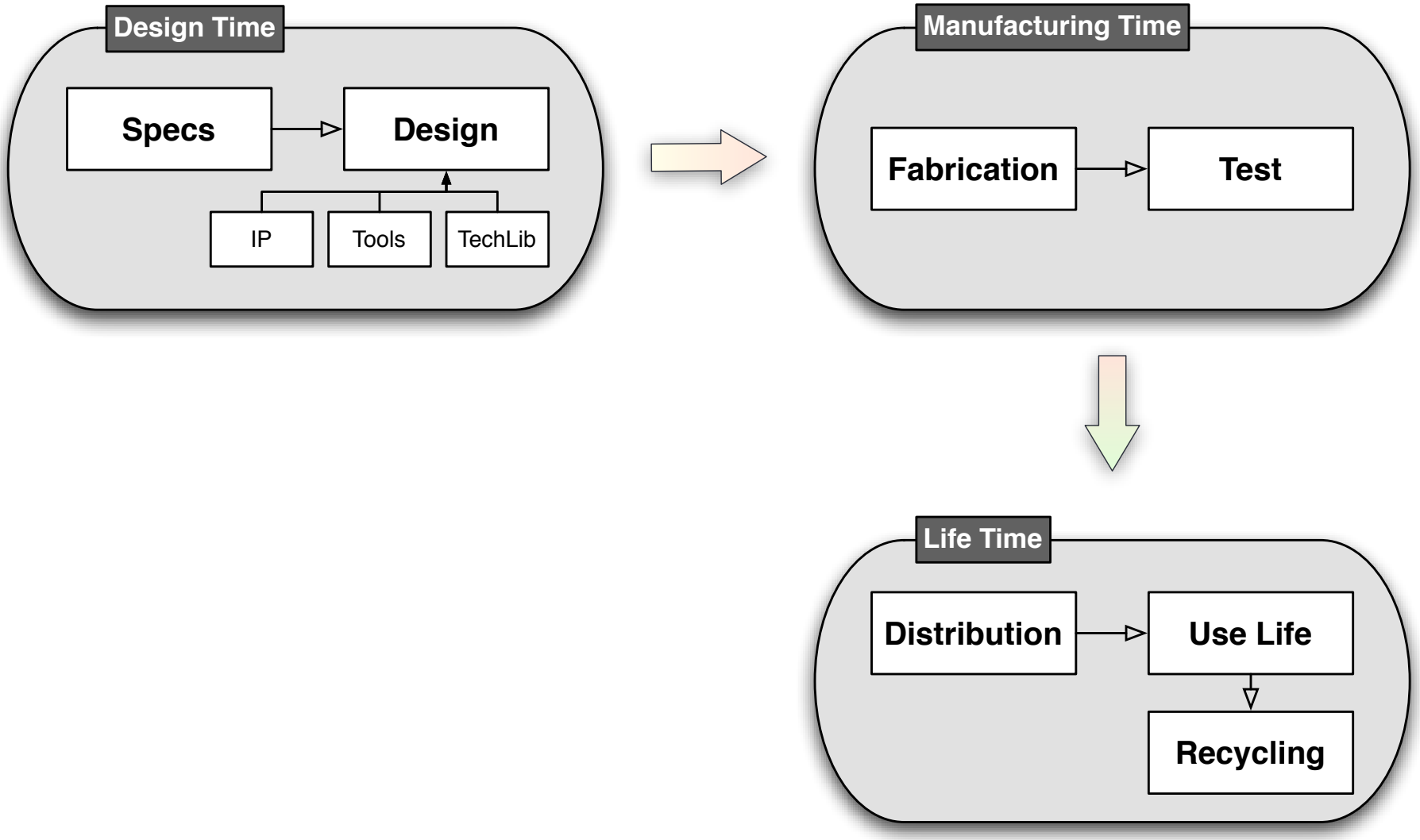
IC production test



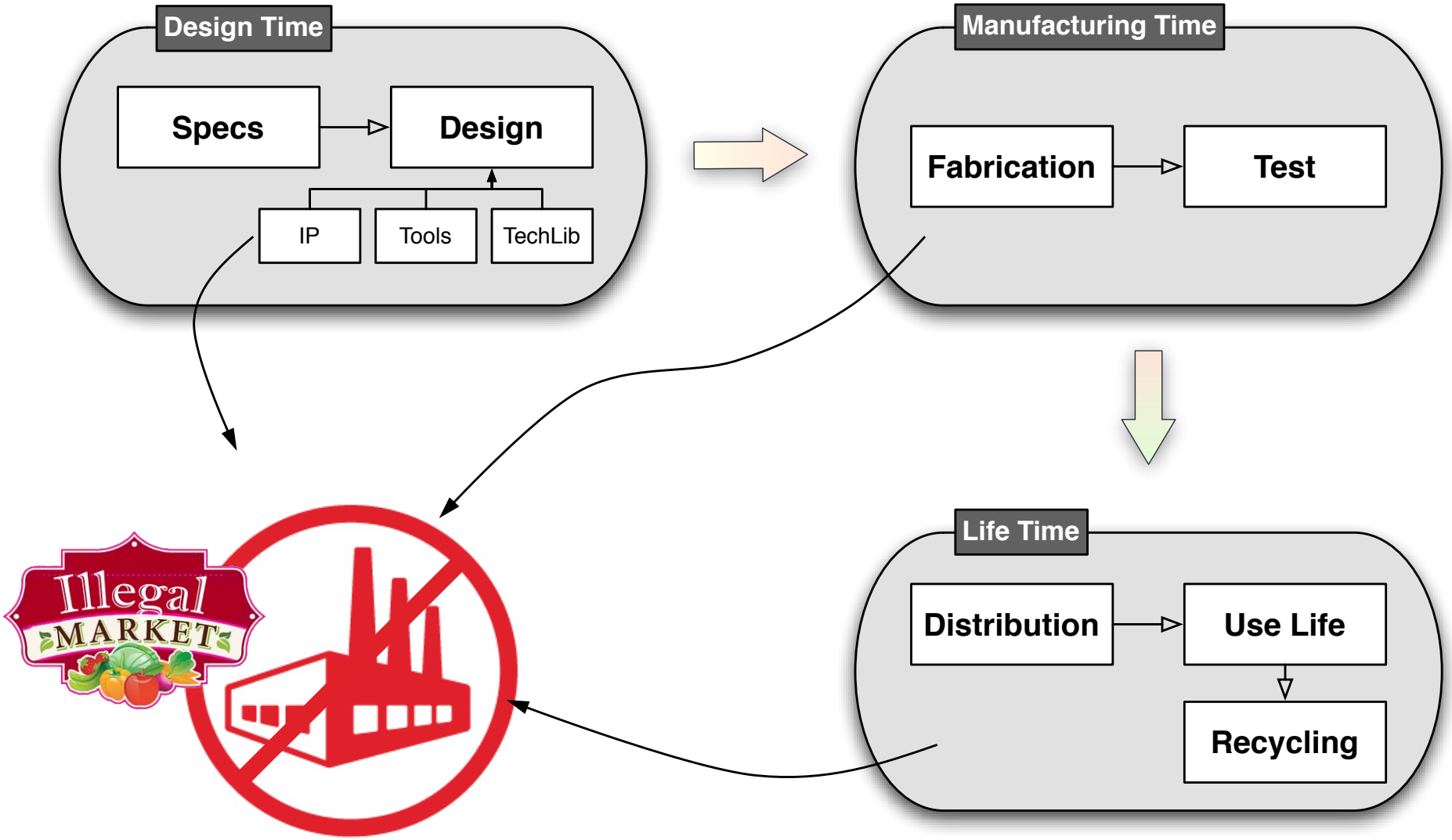
IC production test



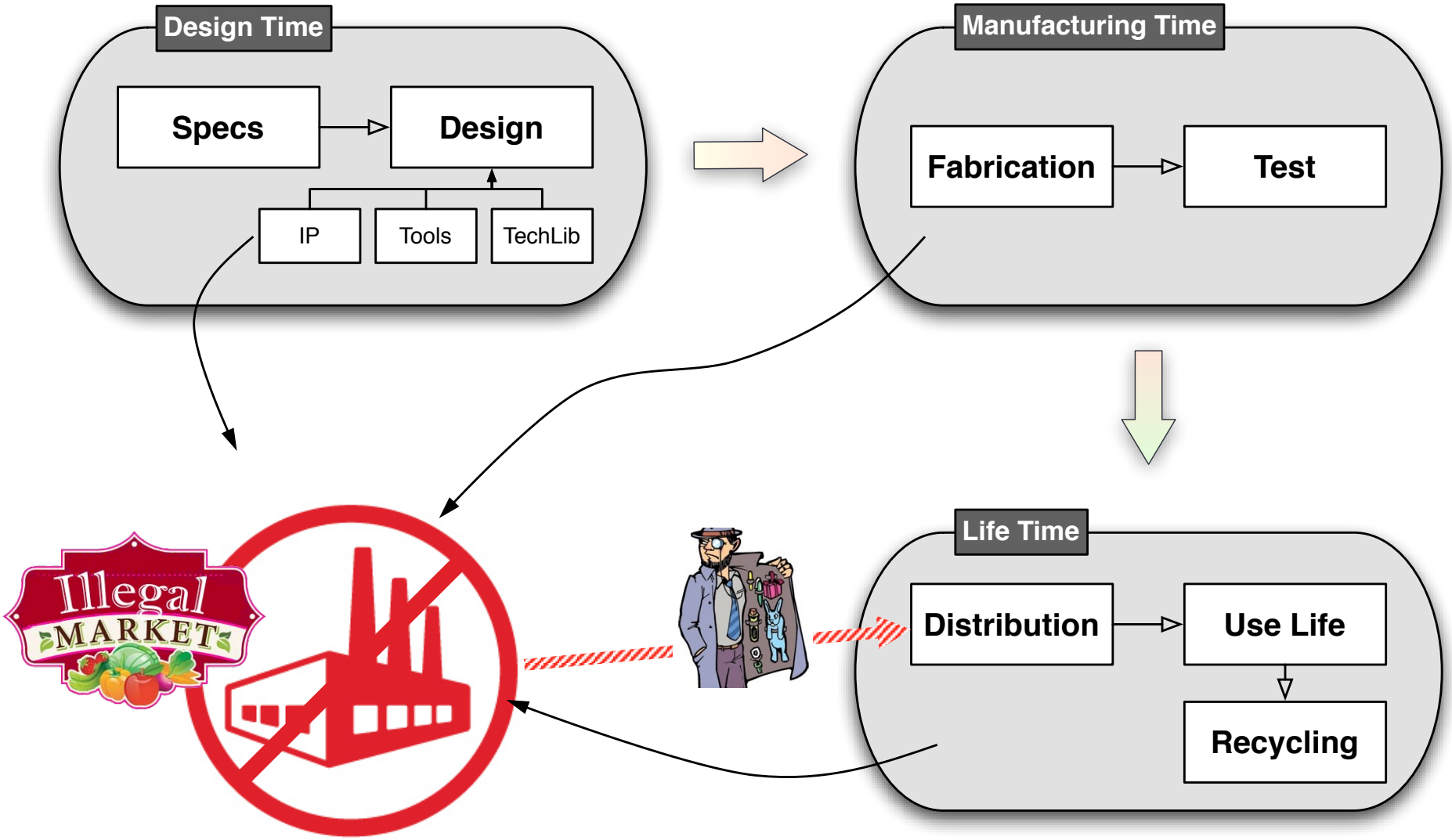
The Untrusted Chain



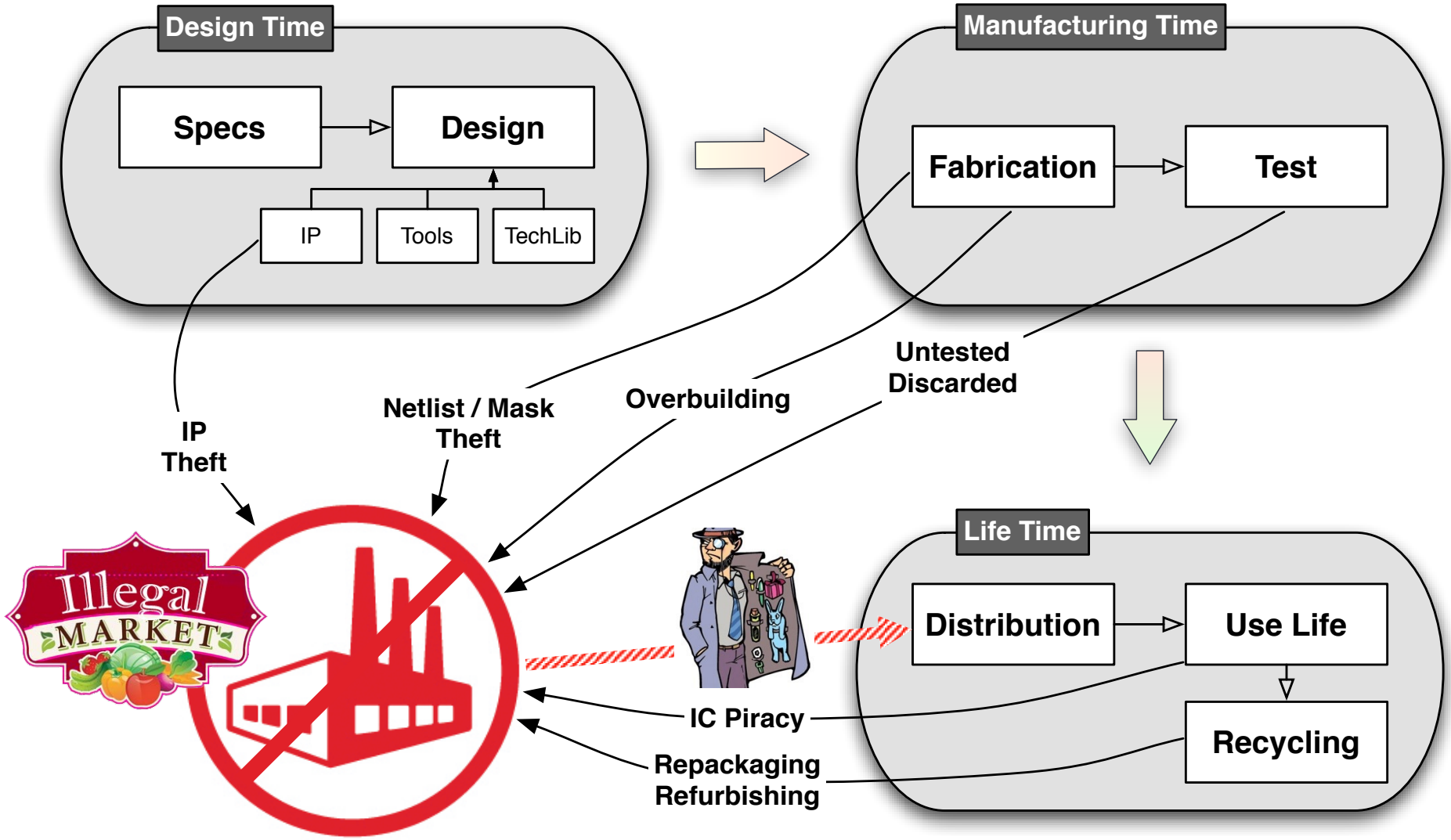
The Untrusted Chain



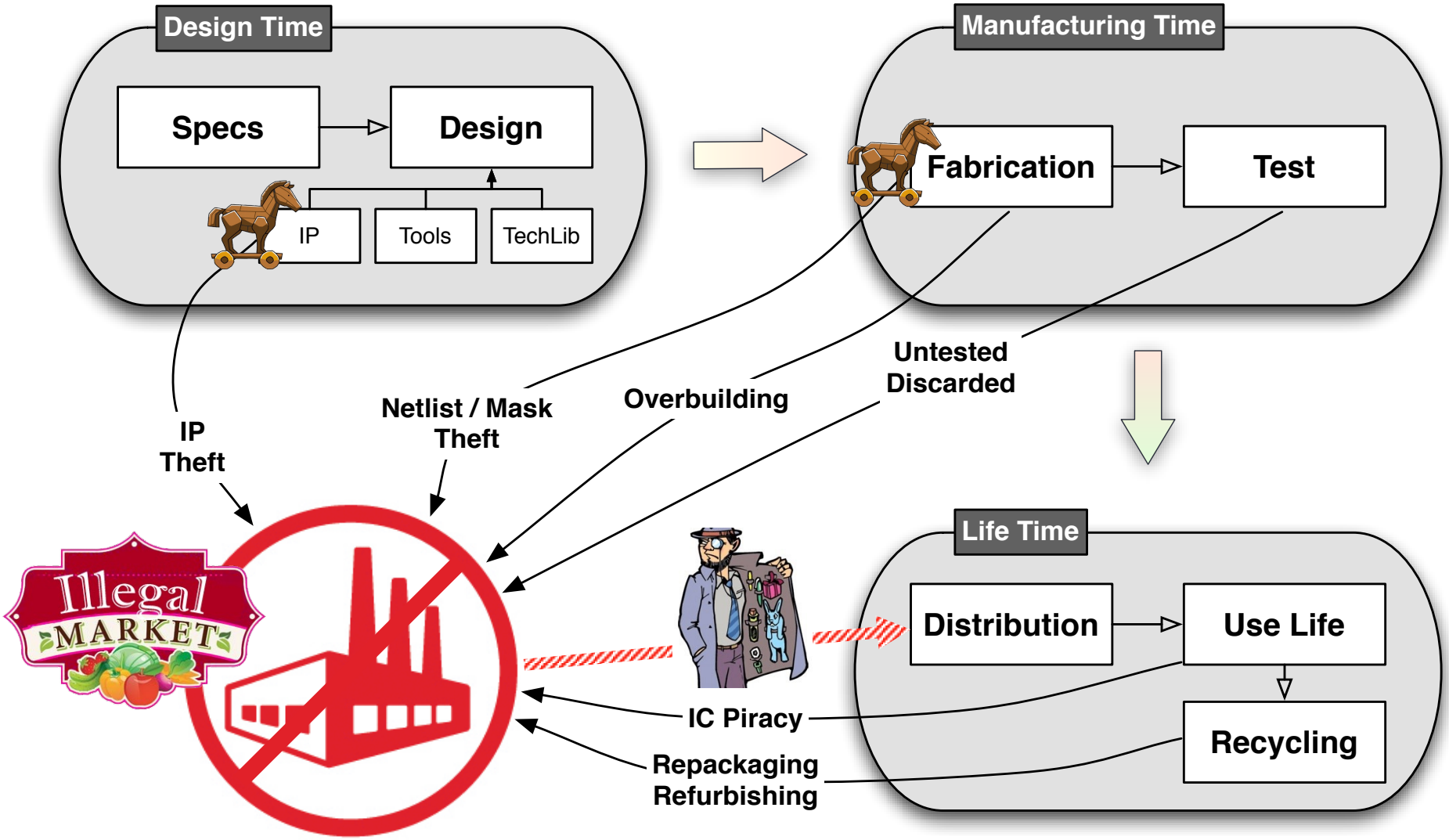
The Untrusted Chain



The Untrusted Chain



The Untrusted Chain



Overview

- Introduction
- The product life-cycle chain
- Counterfeiting types
- Counterfeiting detection
- Counterfeiting prevention

Counterfeiting Types

- Recycled
- Remarking
- Overproduced
- Defective
- Cloned
- Tampered

Counterfeit types – Recycled

- Electronic component that is recovered from a system and then modified to be misrepresented as a new component.
- Problems:
  - lower performance
  - shorter lifetime
  - damaged component, due to the reclaiming process (removal under very high temperature, aggressive physical removal from boards, washing, sanding, repackaging, etc.)

Counterfeit types – Recycled

- Electronic component that is recovered from a system and then modified to be misrepresented as a new component.
- Consequences:
  - Market loss (…and also unemployment)
  - Brand image loss
  - Lack of security
  - Lack of reliability

Counterfeit types – Remarked

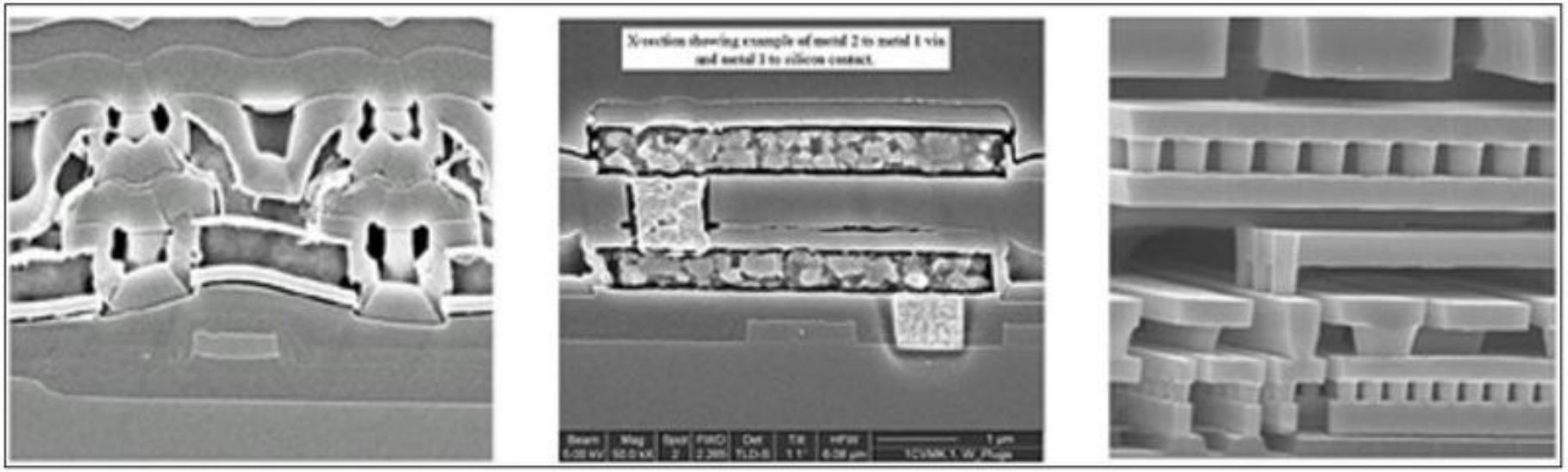
- Chemically or physically removing the original marking
- Goal:
  - to drive up a component's price on the open market
  - to make a dissimilar lot fraudulently appear homogeneous
- Consequences:
  - Brand image loss
  - Lack of security
  - Lack of reliability

Counterfeit types – Overproduced

- Overproduction occurs when foundries sell components outside of contract with the design house
- Problems:
  - reliability threats since they are often not subjected to the same rigorous testing as authentic parts
- Consequences:
  - loss in profits for the design and IP owner
  - Lack of security
  - Lack of reliability

Counterfeit types – Defective

- A part is considered defective if it produces an incorrect response to post-manufacturing tests
- Method:



Counterfeit types – Defective

- Method:
  - These parts should be destroyed, downgraded, or otherwise properly disposed of
  - However, if they can be sold on the open markets, either knowingly by an untrusted entity or by a third party who has stolen them

…there are internal notices about the issue that instruct engineers not to disclose this memory issue. The company was worried about creating a perception within the customer base that they had quality issues.

Source: http://www.bradreese.com/blog/2-16-2014.htm

Counterfeit types – Cloned

- A copy of a design, in order to eliminate the large development cost of a part

Counterfeit types – Cloned

- A copy of a design, in order to eliminate the large development cost of a part
- Methods:
  - Reverse engineering
    - https://www.youtube.com/watch?v=r8Vq5NV4Ens
  - By obtaining IP illegally (also called IP theft)
  - With unauthorized knowledge transfer from a person with access to the part design

Counterfeit types – Tampered

- Components modified in order to cause damage or make unauthorized alterations
- Examples:
  - time bombs that stop the circuit functionality at a critical moment
  - Backdoors that give access to critical system functionality or leak secret information

Counterfeit types – Tampered

Trojan Horses

- A Hardware Trojan Horse is a malicious modification of an integrated circuit
  - Performed at any design and/or manufacturing step
  - A hardware Trojan is completely characterized by its physical representation and its behavior.
- Is it a real threat?
  - ~~Few~~ Some real cases
  - A big fear!!

Counterfeit types – Tampered

Trojan Horses

- What hardware Trojans can do?
  - Change the functionality
  - Reduce the reliability
  - Leak valuable information
- Applications that are likely to be targets
  - Military applications
  - Aerospace applications
  - Civilian security-critical applications
  - Financial applications
  - Transportation security
  - IoT devices
  - Commercial devices
  - More

Counterfeit types – Tampered

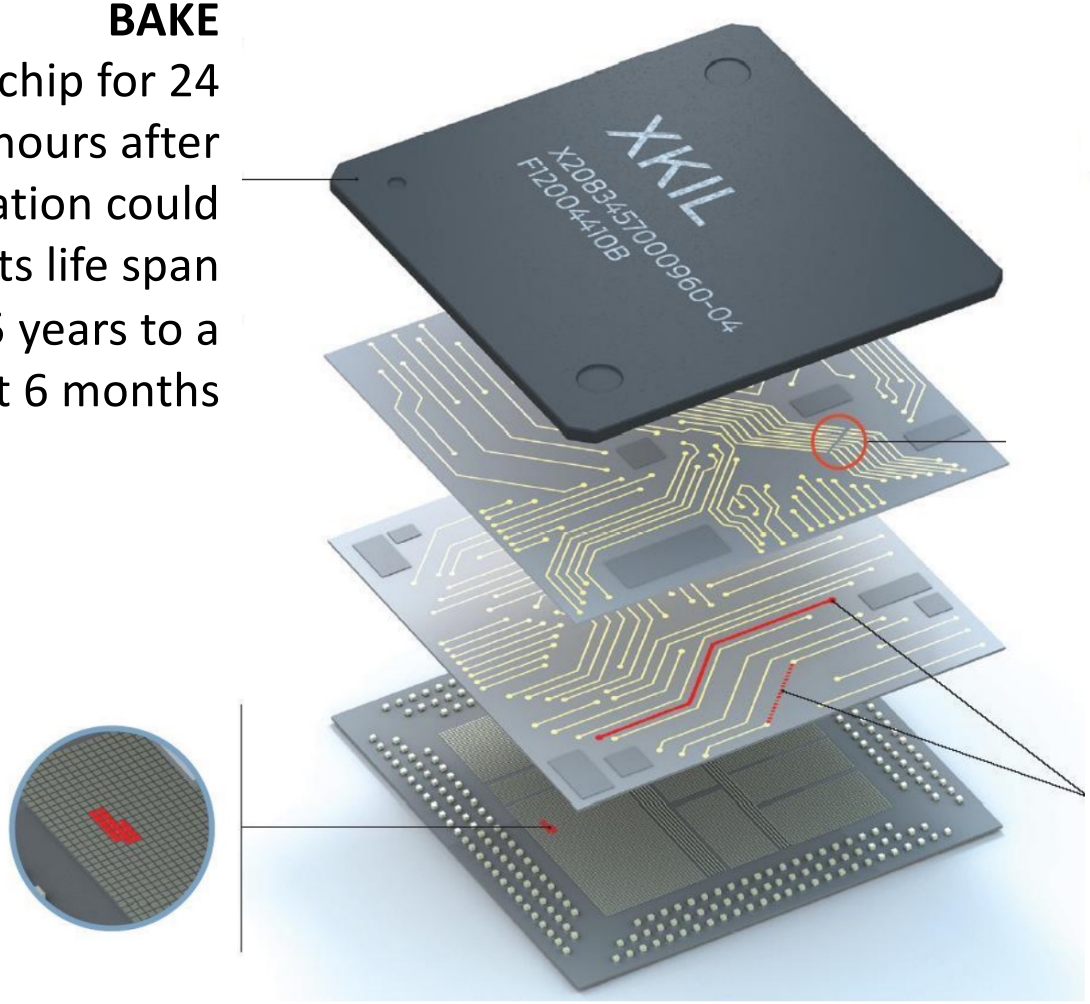
Trojan Horses

- 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*

Counterfeit types – Tampered

Trojan Horses – at manufacturing time

BAKE
Baking a chip for 24 hours after fabrication could shorten its life span from 15 years to a scant 6 months

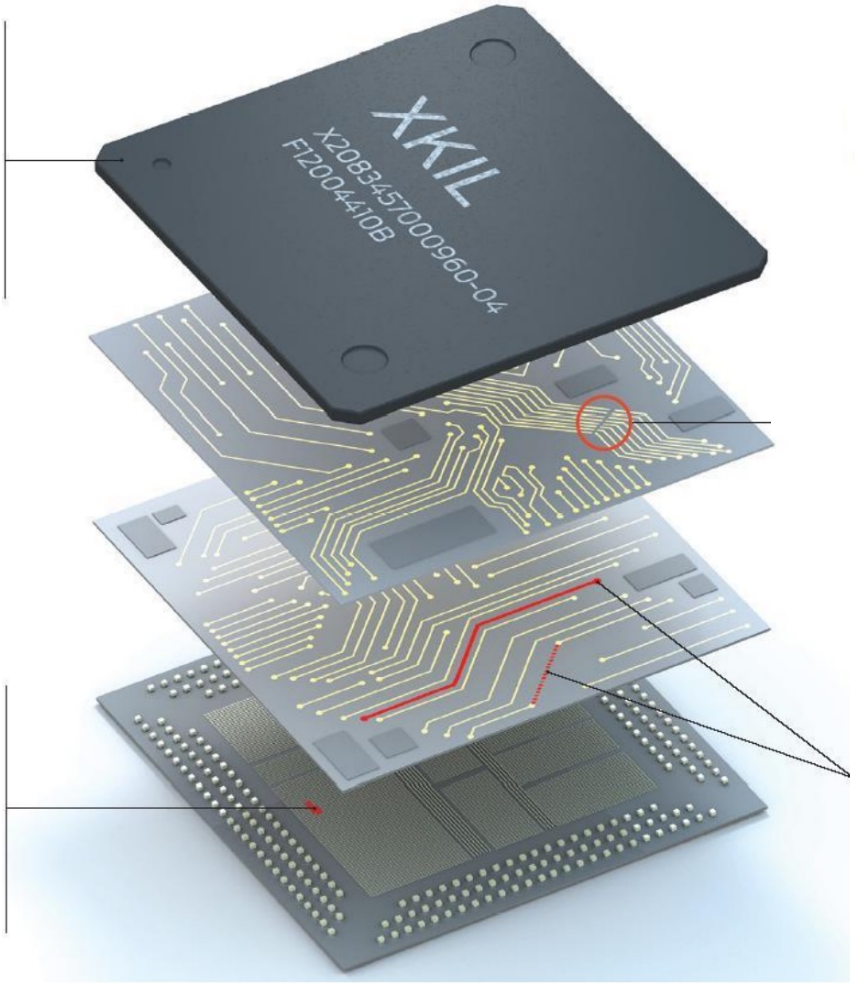


IEEE Spectrum

Counterfeit types – Tampered

Trojan Horses – at manufacturing time

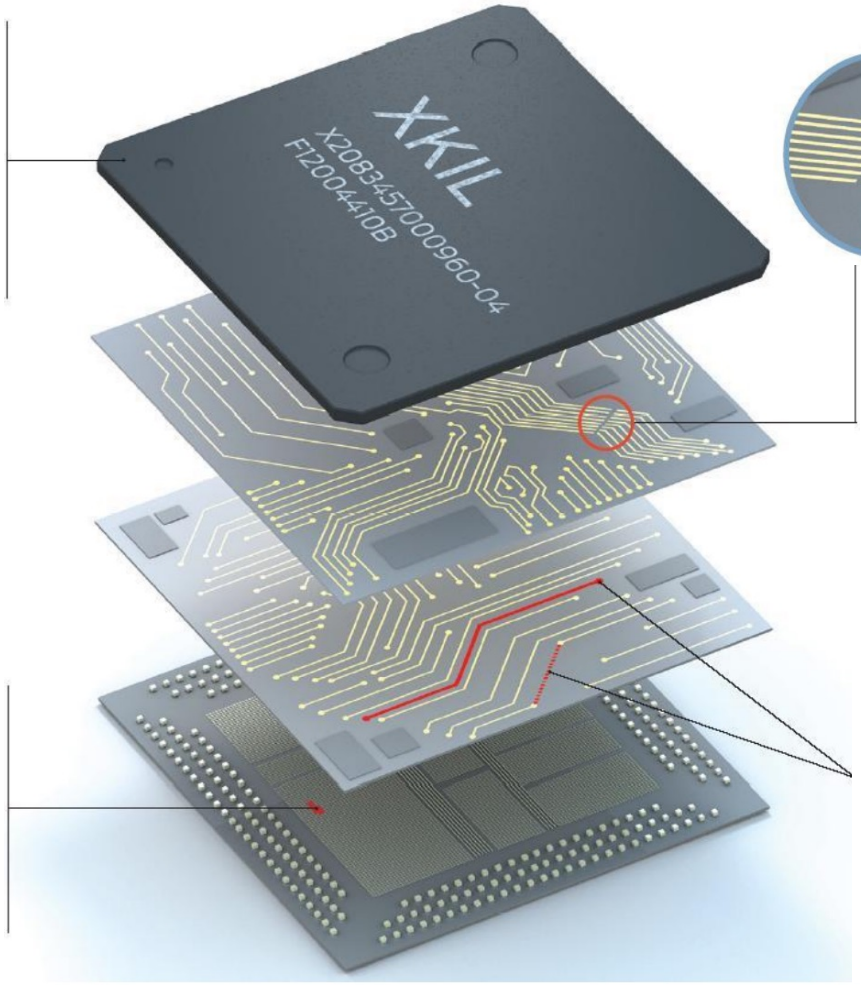
ADD EXTRA TRANSISTORS
Adding just 1000 extra transistors during either the design or the fabrication process could create a kill switch or a trapdoor. Extra transistors could enable access for a hidden code that shuts off all, or part of the chip.



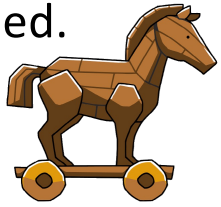
IEEE Spectrum

Counterfeit types – Tampered

Trojan Horses – at manufacturing time



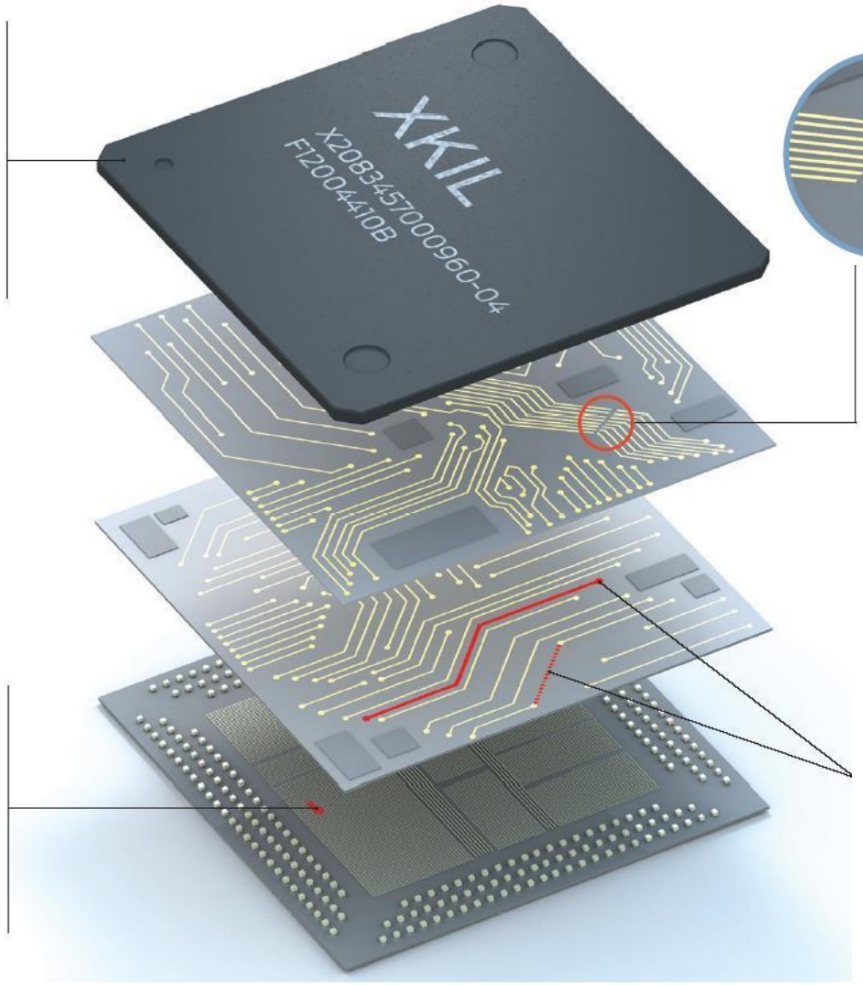
NICK THE WIRE
A notch in a few interconnects would be almost impossible to detect but would cause eventual mechanical failure as the wire became overloaded.



IEEE Spectrum

Counterfeit types – Tampered

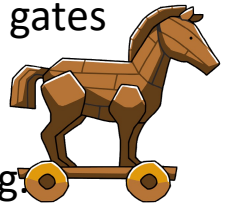
Trojan Horses – at manufacturing time



IEEE Spectrum

ADD OR RECONNECT WIRING

During the layout process, new circuit traces and wiring can be added to the circuit. A skilled engineer familiar with the chip's blueprints could reconnect the wires that connect transistors, adding gates and hooking them up using a process called circuit editing.

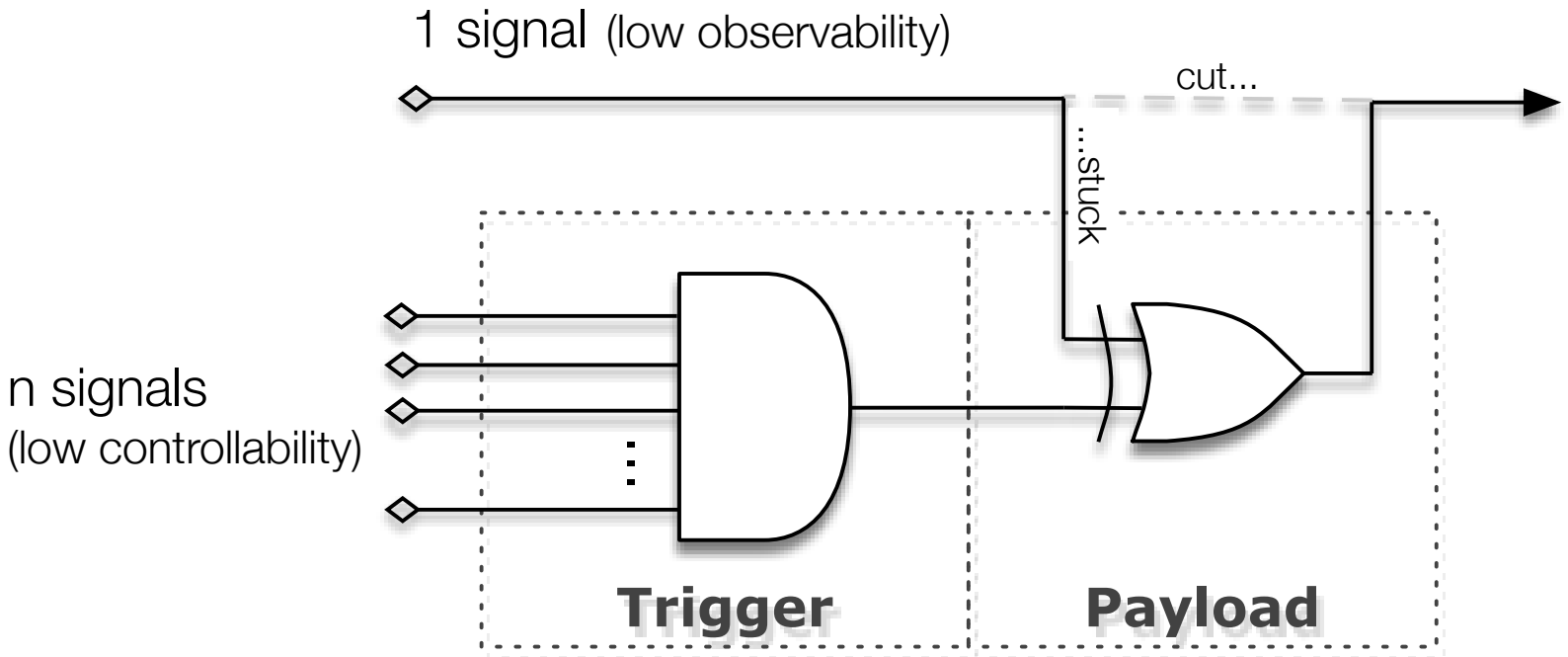


Counterfeit types – Tampered

- The **payload** of an HT is the entire activity that the Trojan executes when it is **triggered**.
- Trojans bypass or disable the security fence of a system:
  - leak confidential information by radio emission
  - disable, derange or destroy the entire chip or components of it.

Counterfeit types – Tampered

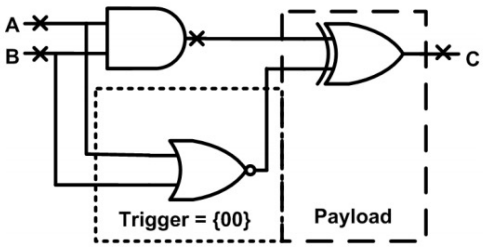
Trojan Horses – basic model



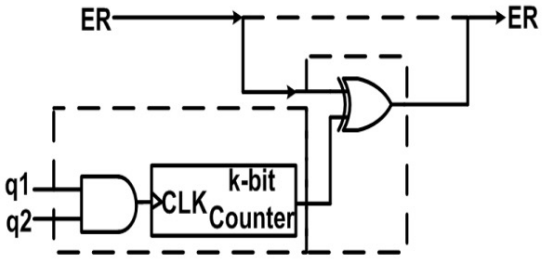
Counterfeit types – Tampered

Trojan Horses – examples

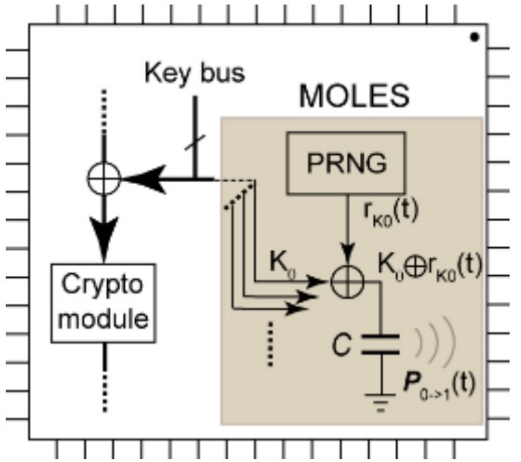
Comb. Trojan Example



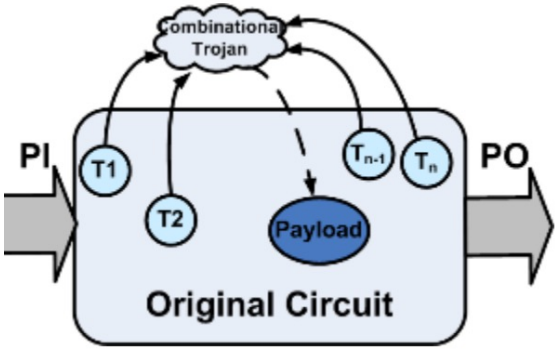
Seq. Trojan Example



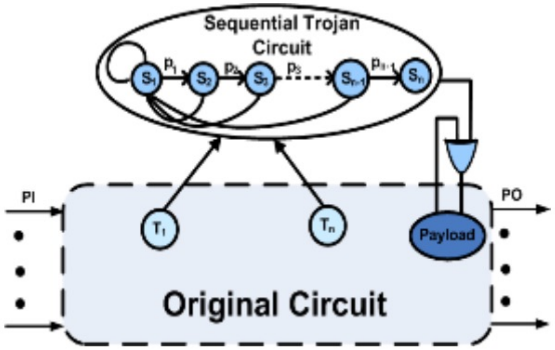
MOLES*: Info Leakage Trojan



Comb. Trojan model



Seq. Trojan Model



Counterfeit types – Tampered

- An HT can be characterized by several methods:
  - physical representation
    - functional or parametric
  - activation phase
    - triggered by sensors, internal logic states, a particular input pattern or an internal counter value
  - action phase
    - modify the chip's function or changes the chip's parametric properties

Counterfeit types – Tampered

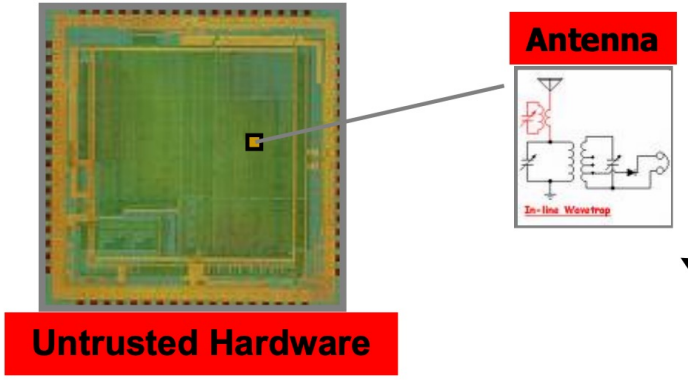
Trojan Horses – Examples

Silicon Back-door:

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

HOW?

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



Counterfeit types – Tampered

Trojan Horses – Examples

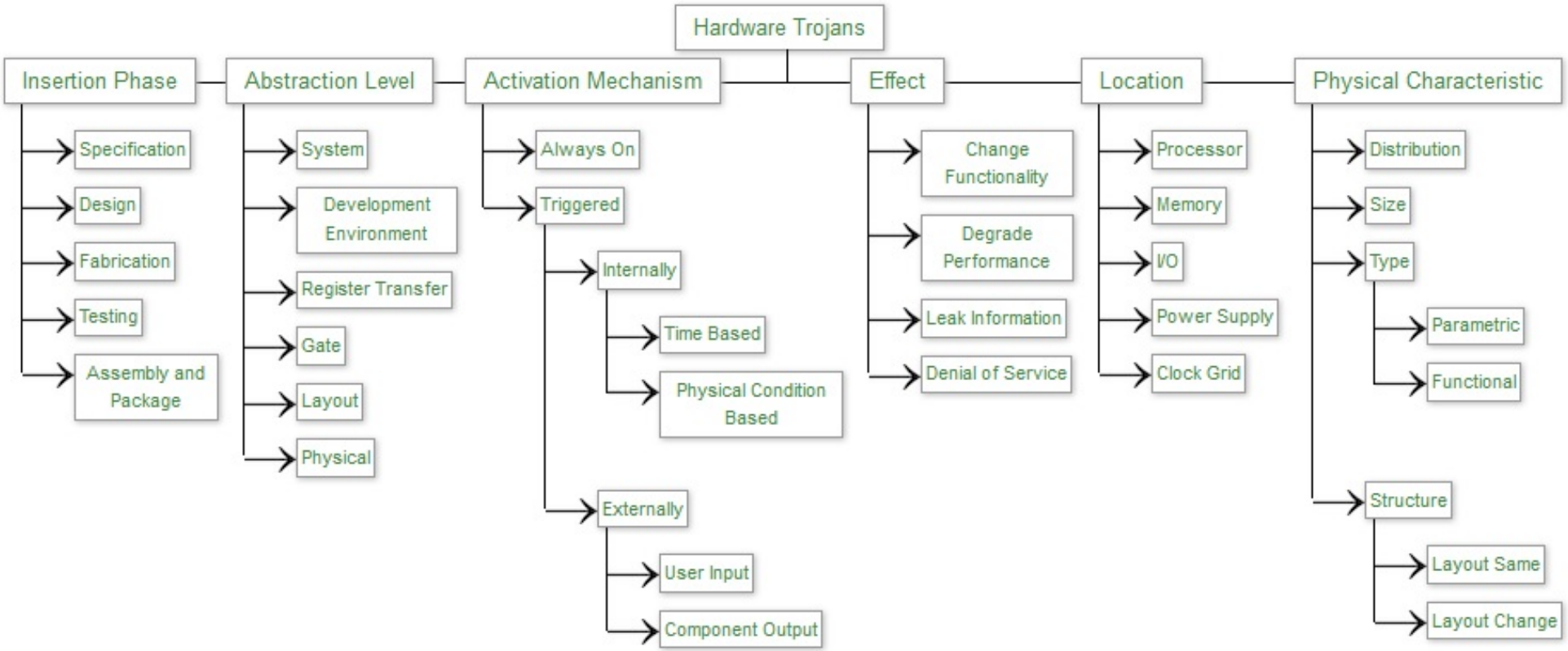
Silicon Time bomb:

- 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

Counterfeit types – Tampered

Trojan Horses – Taxonomy



Overview

- Introduction
- The product life-cycle chain
- Counterfeiting types
- Counterfeiting detection
- Counterfeiting prevention

Counterfeiting detection

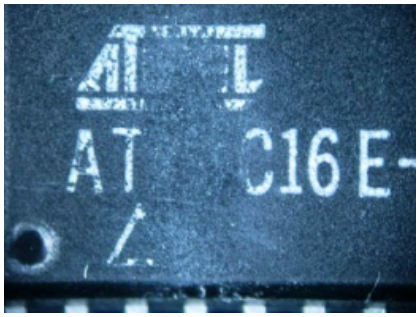
- Cleaning, visual inspection
- Microscope & X Ray Inspections
- Side-Channel

Counterfeiting detection

Cleaning, visual inspection

Before cleaning

After cleaning

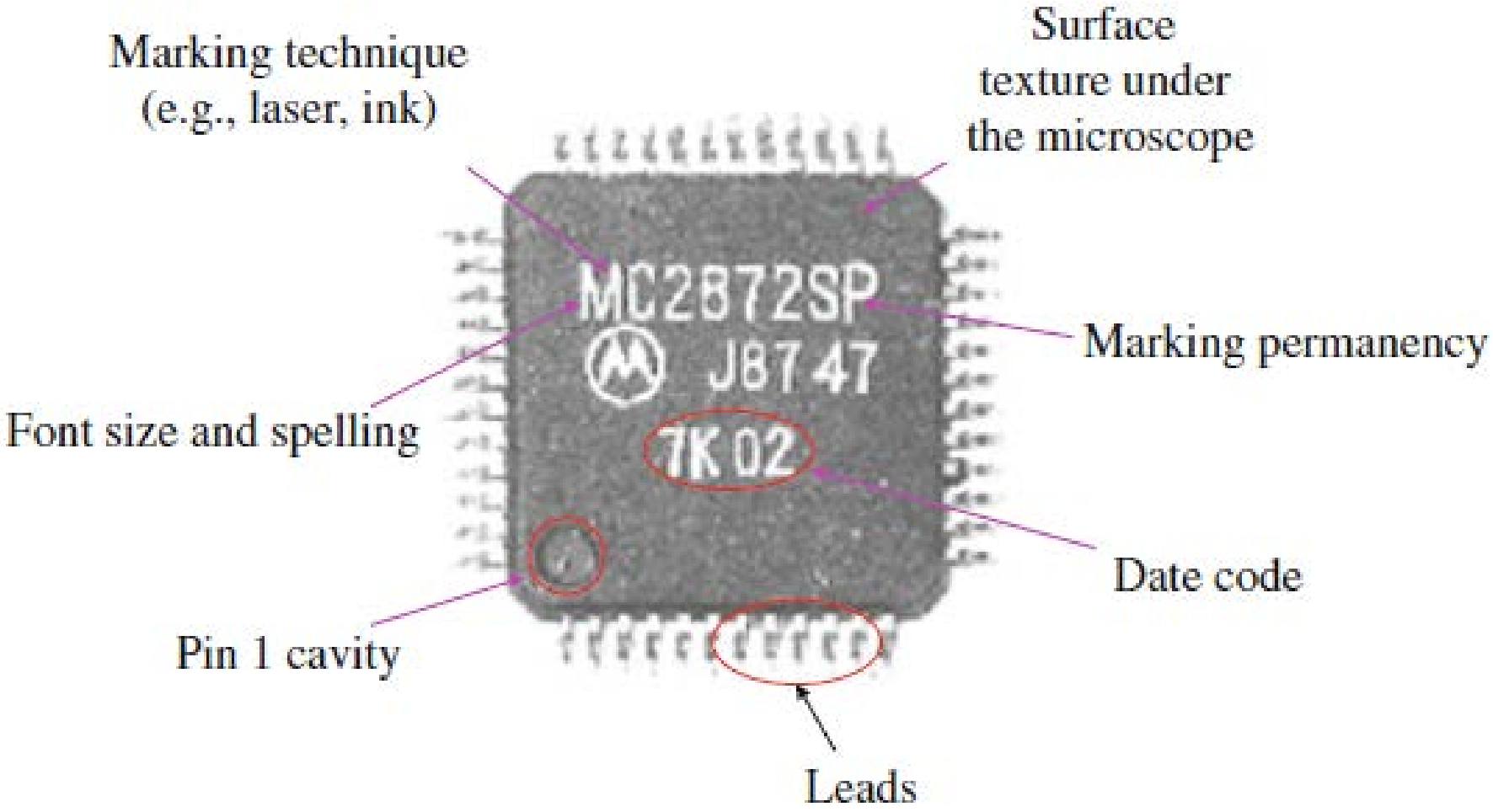


Fake Atmel

Fake Motorola

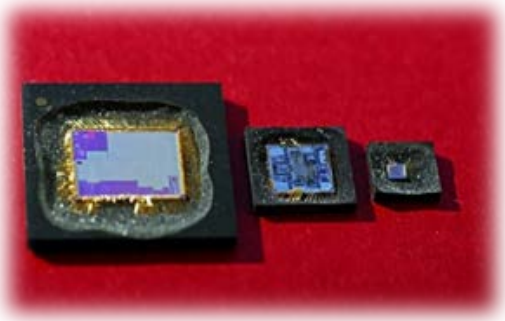
Counterfeiting detection

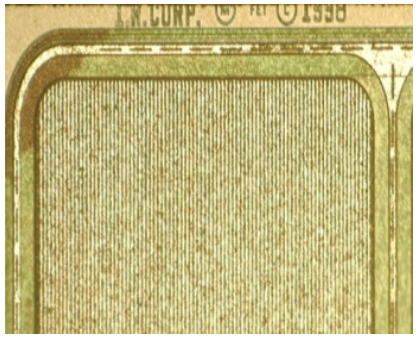
Cleaning, visual inspection

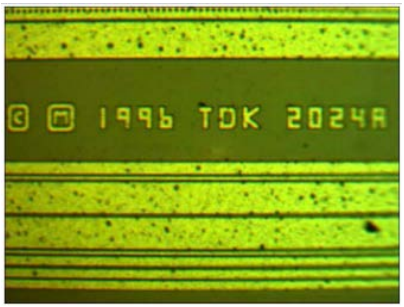


Counterfeiting detection

Inspection by microscopes



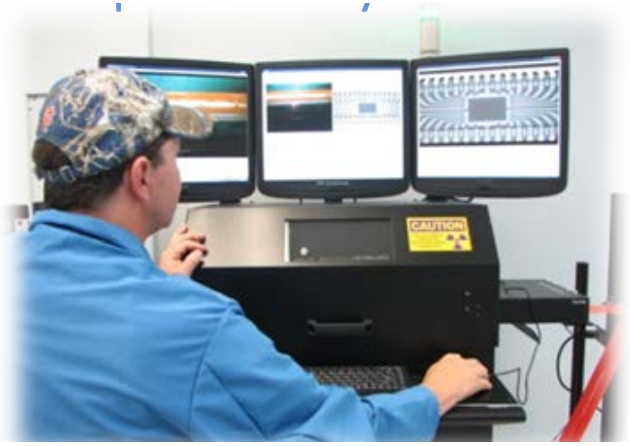


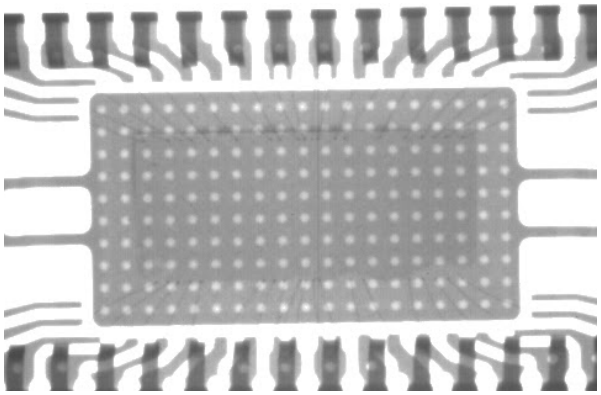


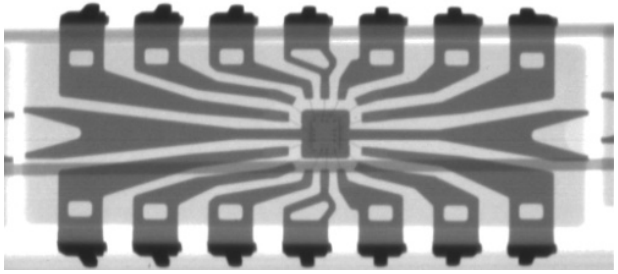
https://www.youtube.com/watch?v=RVTME7DzEj0

Counterfeiting detection

Inspection by X Ray



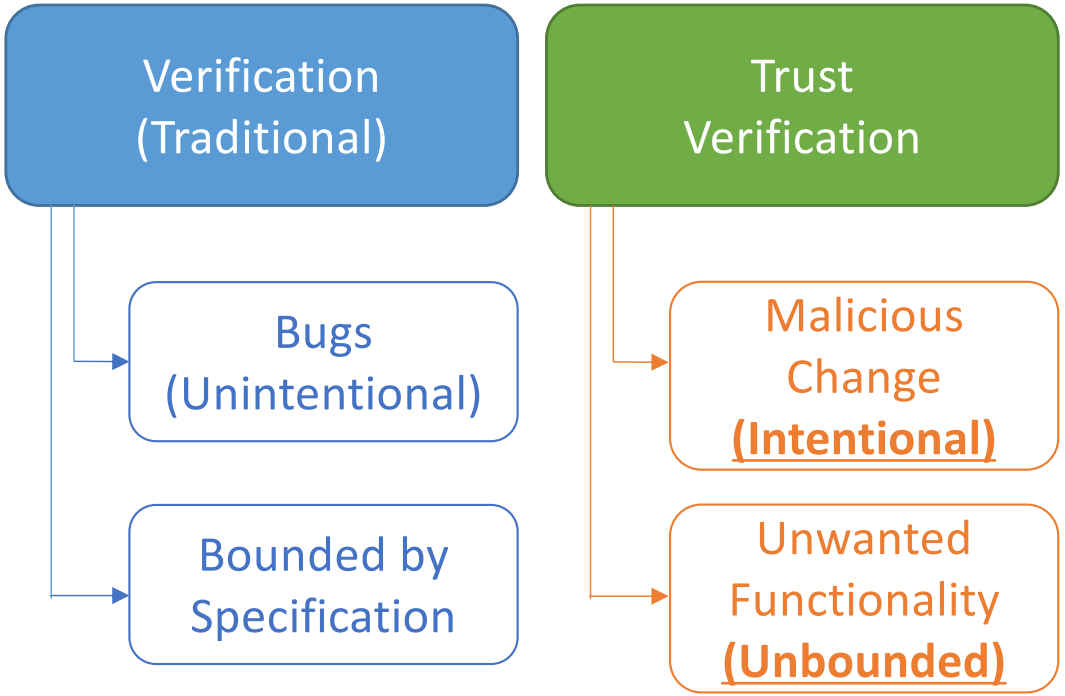




https://www.youtube.com/watch?v=RVTME7DzEj0

Counterfeiting detection

Hardware Trojan Detection - Challenge



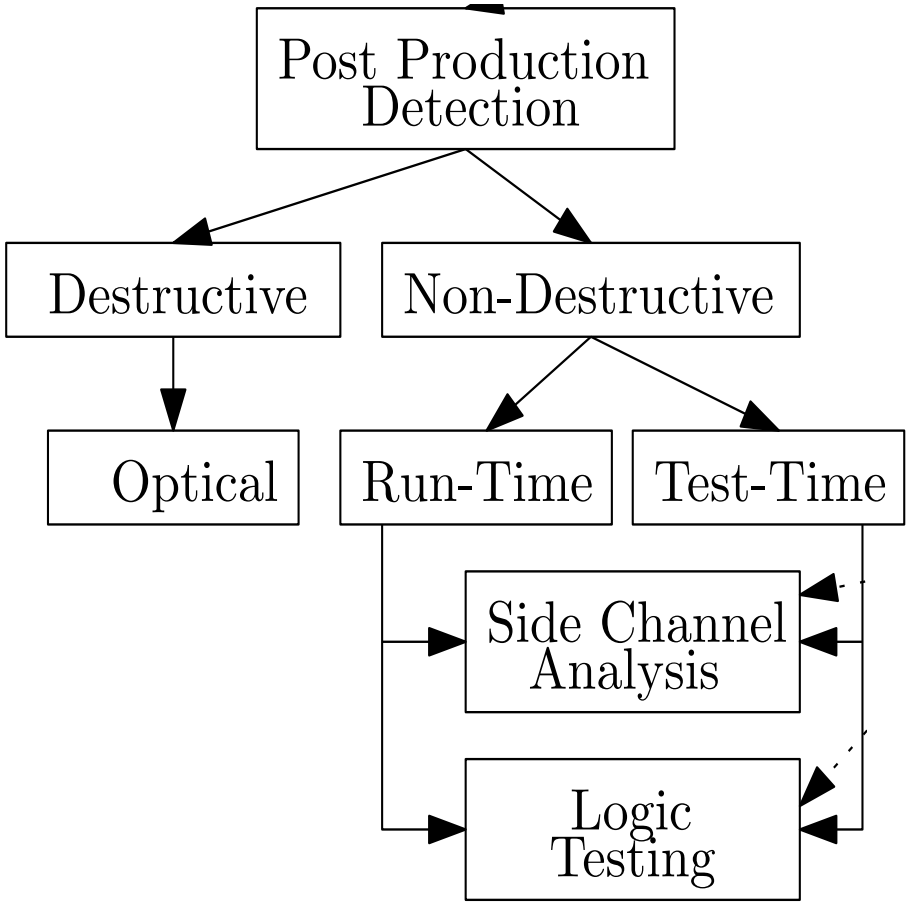
Counterfeiting detection

Hardware Trojan Detection - Challenges

- Objective:
  - Ensure that the fabricated chip/system will carry out only our desired function and nothing more.
- Challenges:
  - Tiny: several gates to millions of gates
  - Quiet: hard-to-activate (rare event) or triggered itself (time-bomb)
  - Hard to model: human intelligence
  - Conventional test and validation approaches fail to reliably detect hardware Trojans.
    - Focus on manufacture defects and does not target detection of additional functionality in a design

Counterfeiting detection

Hardware Trojan Detection

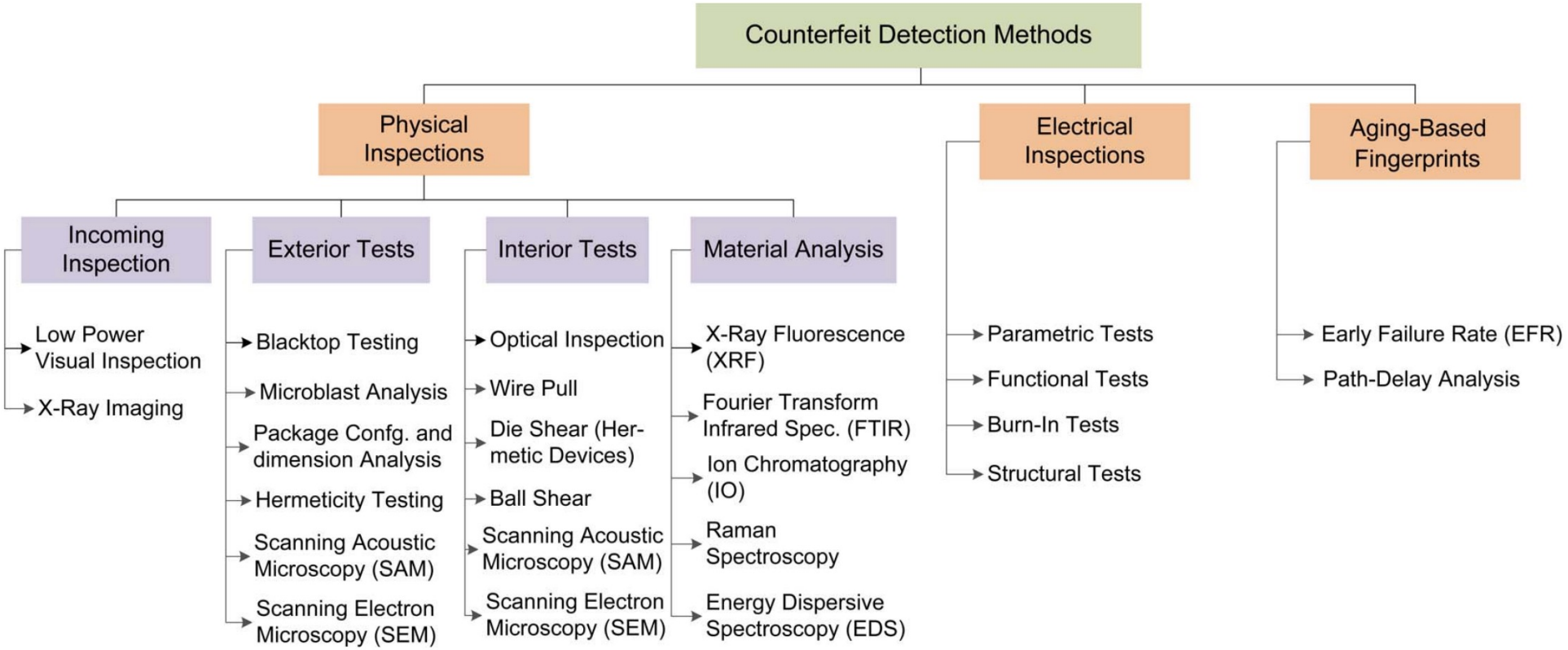


Counterfeiting detection

Hardware Trojan Detection

- **Destructive Approach**: Expensive and time consuming
  - Reverse engineering to extract layer-by-layer images by using delayering and Scanning Electron Microscope
  - Identify transistors, gates and routing elements by using a template matching approach – needs golden IC/layout
- **Non-destructive Approach**
  - Run-time monitoring: Monitor abnormal behaviour during run-time
    - Exploit pre-existing redundancy in the circuit
    - Compare results and select a trusted part to avoid an infected part of the circuit.
  - Test-time Detection: Detect Trojans throughout test mechanisms
    - Logic-testing-based approaches
    - Side-channel analysis-based approaches

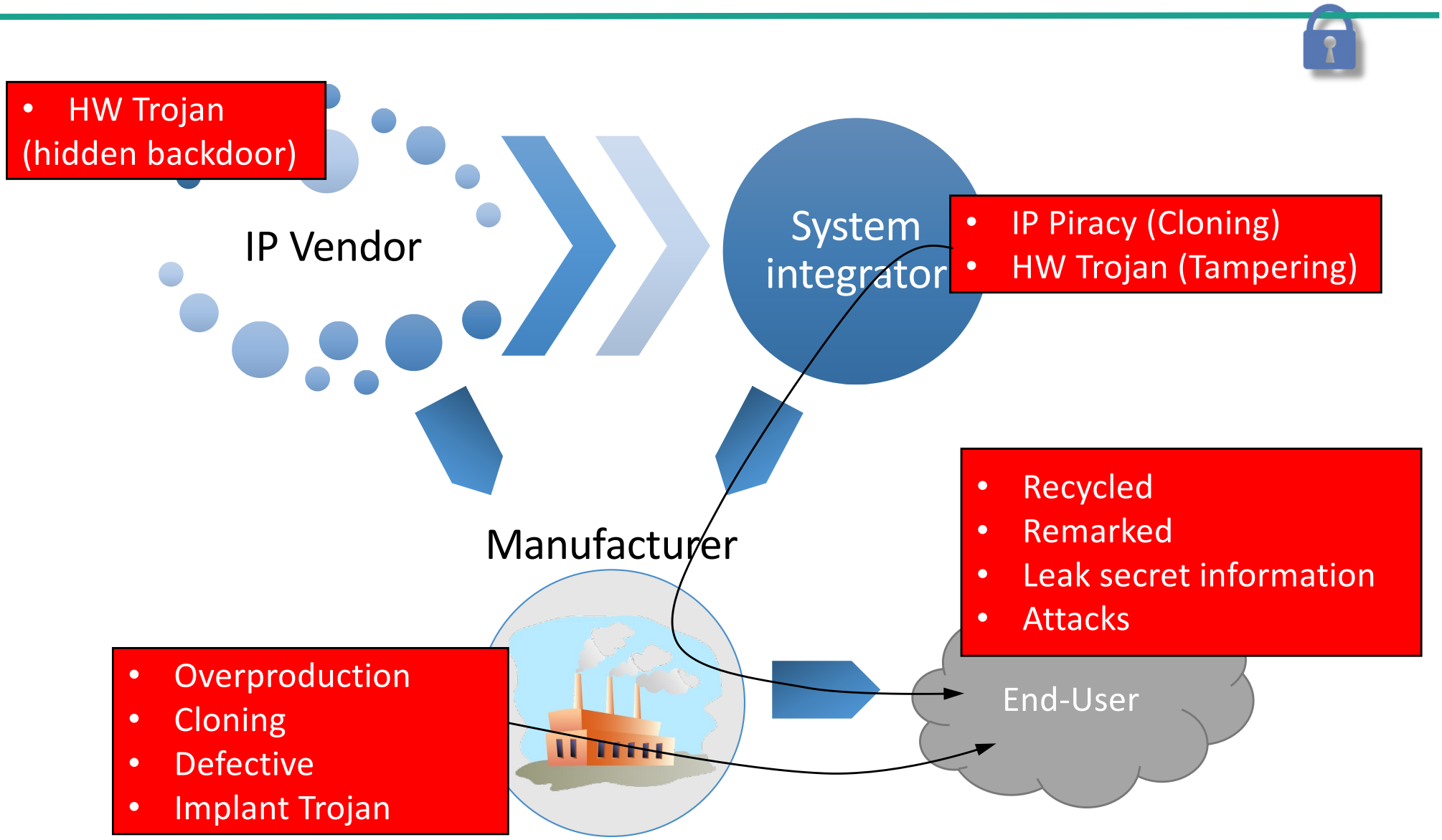
Counterfeiting detection



Overview

- Introduction
- The product life-cycle chain
- Counterfeiting types
- Counterfeiting detection
- Counterfeiting prevention

Microelectronics Industry



Counterfeiting prevention

- Aging detectors
- Hardware metering
  - Post-manufacturing activation
  - “Secret” power-on procedure
  - Logic encryption
- IC Camouflage
- IC Authentication
- HT Prevention
  - Split manufacturing
  - Online detection

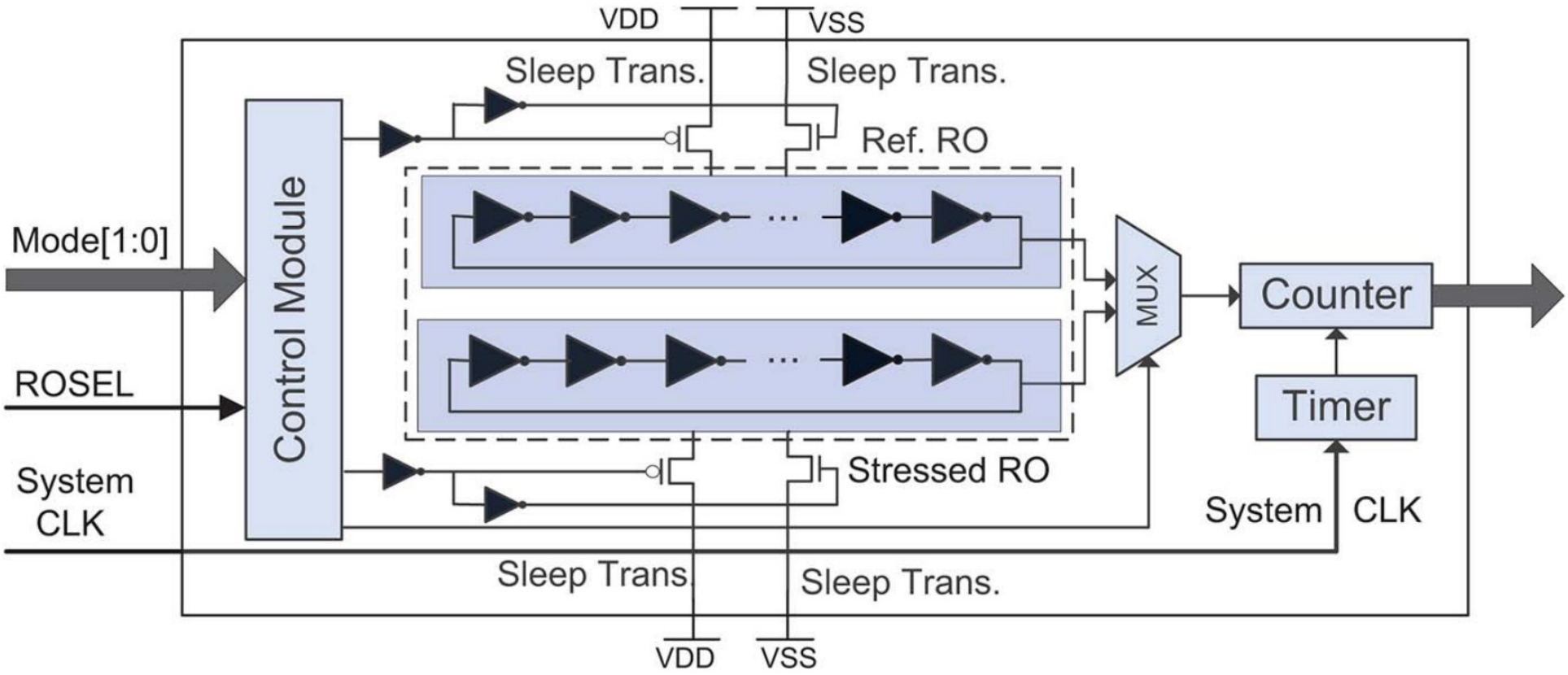
Counterfeiting prevention

Aging Detectors

- Sensors in the chip to capture the usage of the chip in the field
  - It relies on aging effects of MOSFETs to change a ring oscillator frequency in comparison with the golden one embedded in the chip.
- Antifuse-based Technology for Recording Usage Time

Counterfeiting prevention

Aging Detectors
CDIR (combating die and IC recycling)



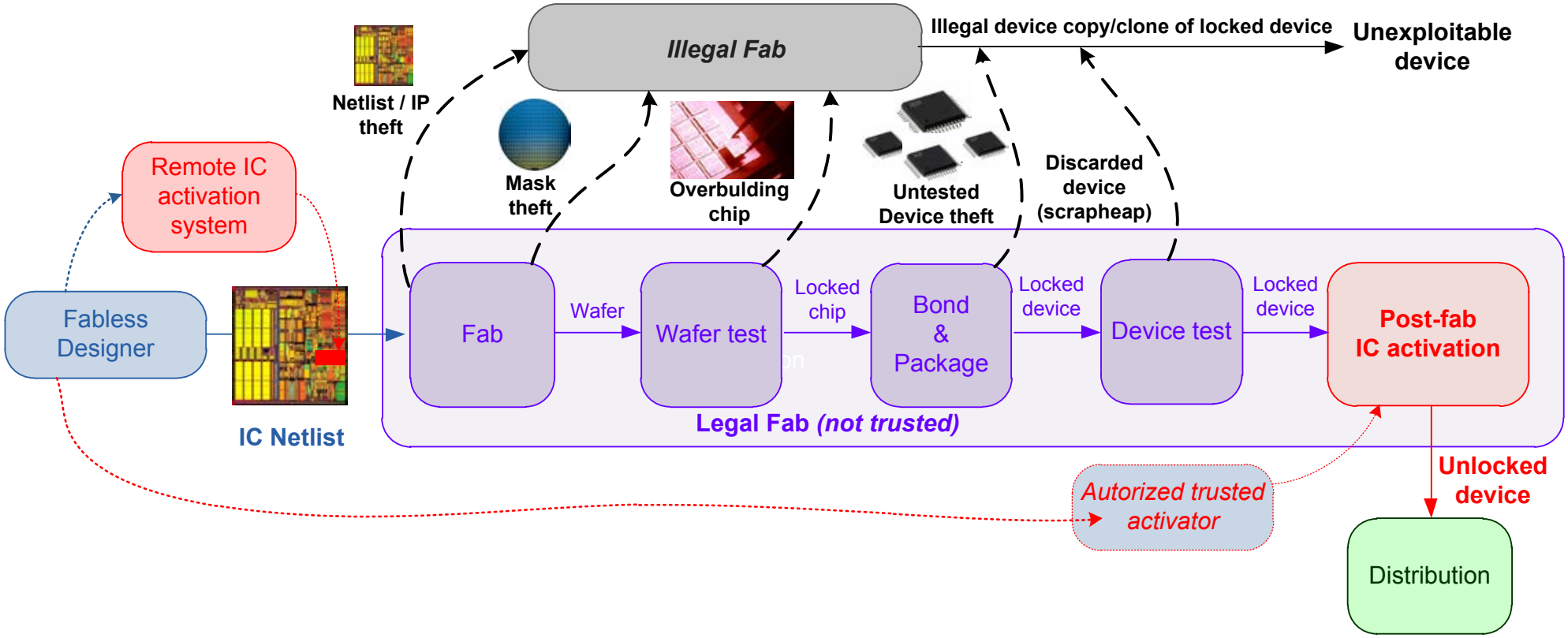
Counterfeiting prevention

Hardware Metering

- A set of security protocols that enable the design house to achieve the post-fabrication control of the produced ICs to prevent overproduction
  - Post-Manufacturing Activation
  - Adding a Finite-State Machine (FSM) which is initially locked and can be unlocked only with the correct sequence of primary inputs
  - Logic Encryption
- Final customer is possibly not aware of all this!!

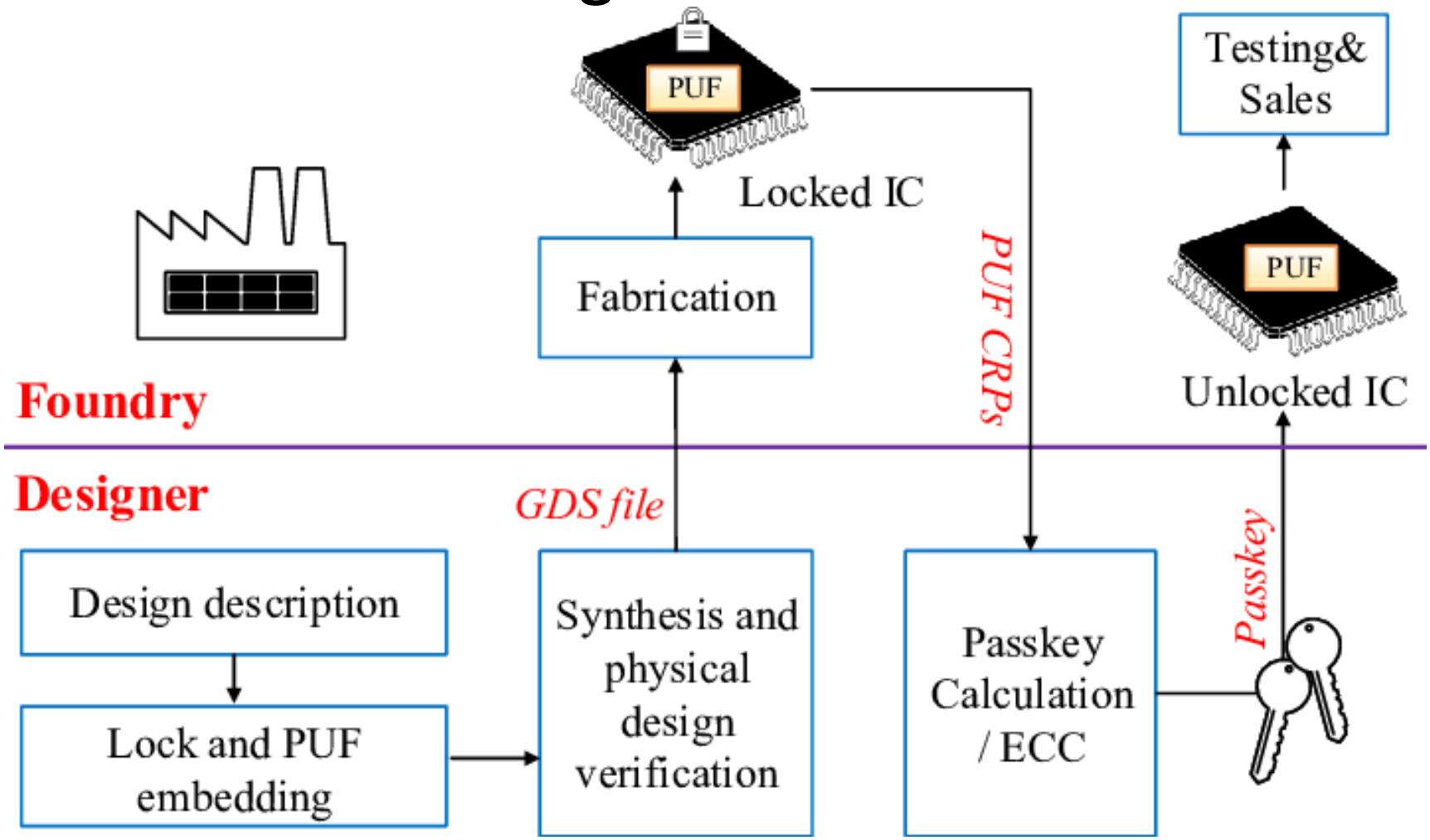
Counterfeiting prevention

Hardware Metering – Integrated Circuits Activation



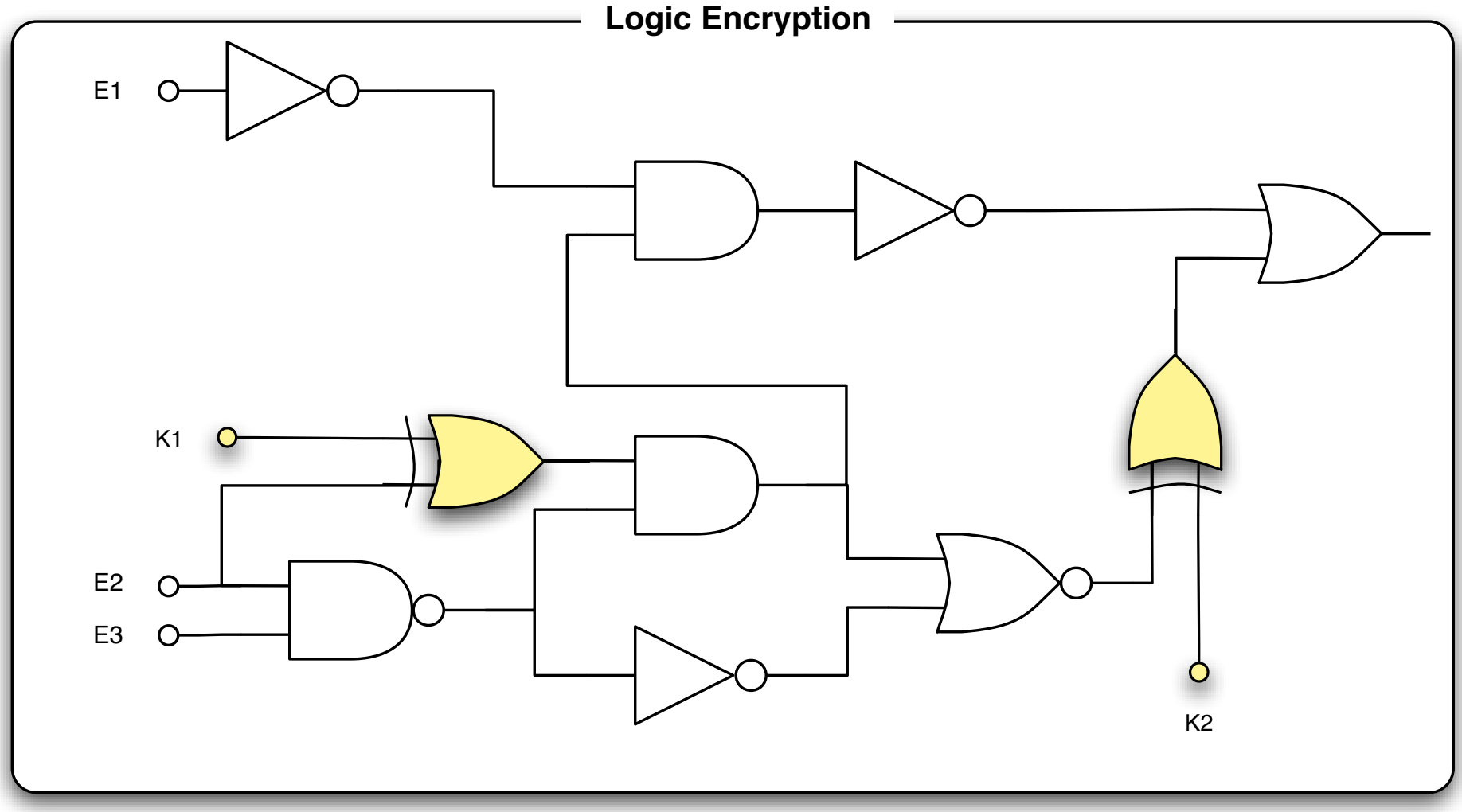
Counterfeiting prevention

Hardware Metering



Counterfeiting prevention

Hardware Metering – Logic Encryption



Counterfeiting prevention

Secure Split Test

- Secure split test (SST) secures the manufacturing test process to prevent counterfeits, allowing the design house to protect and meter their IPs
- SST introduces hardware components for cryptography and locking mechanisms to block the correct functionality of an IC until it is activated by the IP owner during or after the test.
- SST brings design houses back into the manufacturing test process.

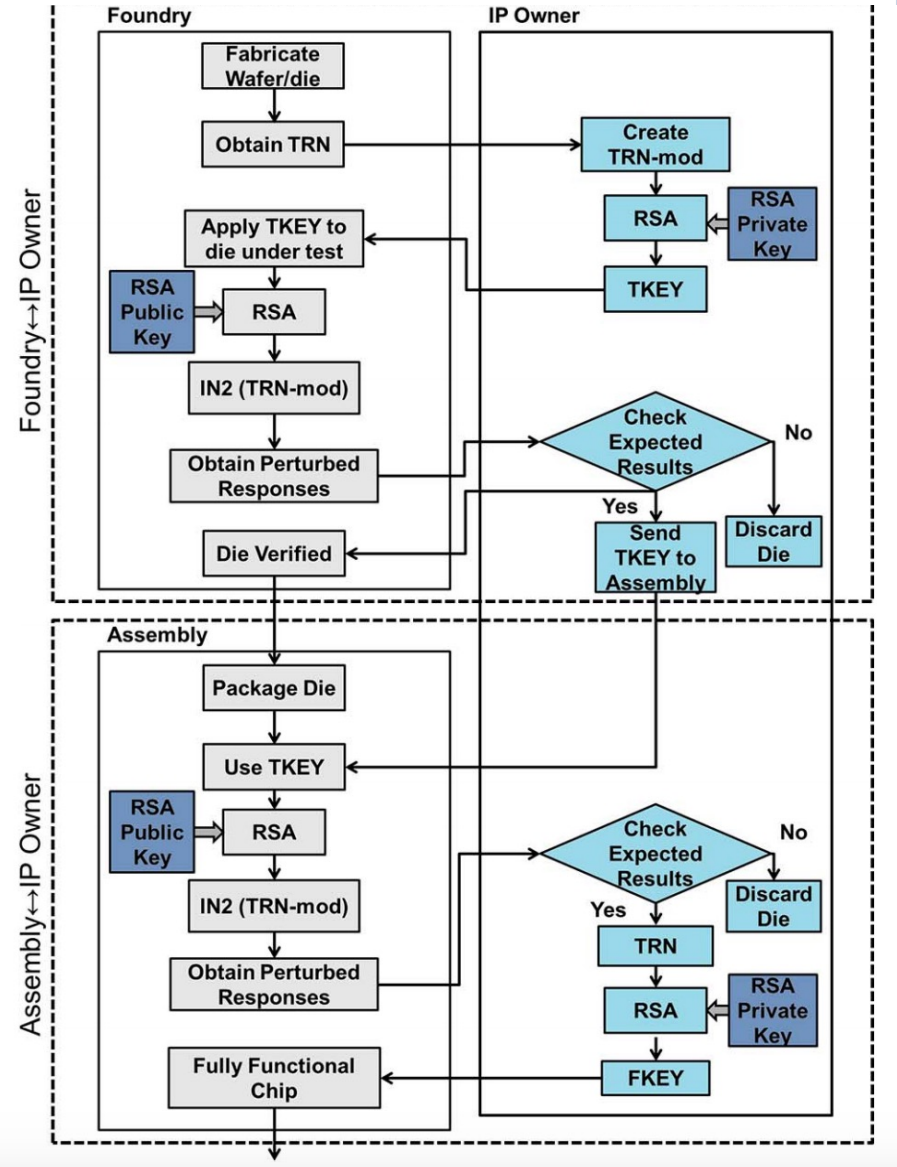
Counterfeiting prevention

Secure Communication

- Secure Split-Test enhances communication between the IP owner and foundry.

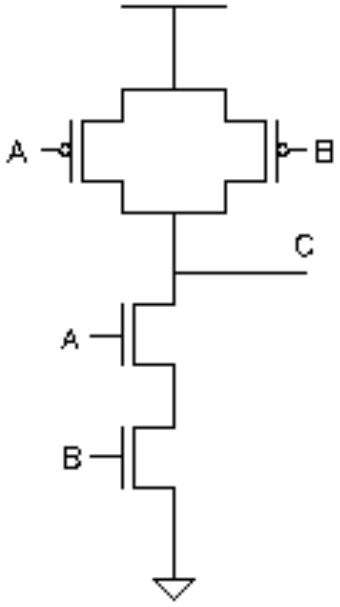
- The IP owner gets test results from the foundry and determines whether an IC is operating correctly.

- IC design becomes more secure because it gives the IP owner the decision over passing or failing ICs without the need of being physically present.

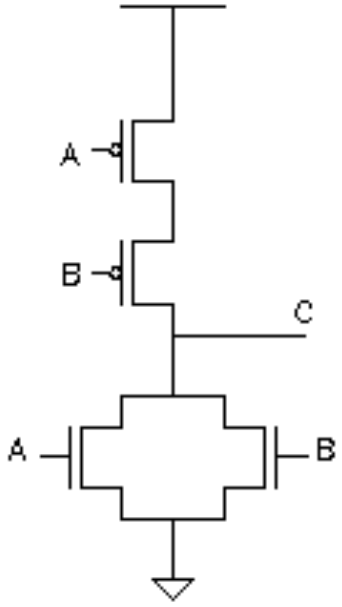


Counterfeiting prevention

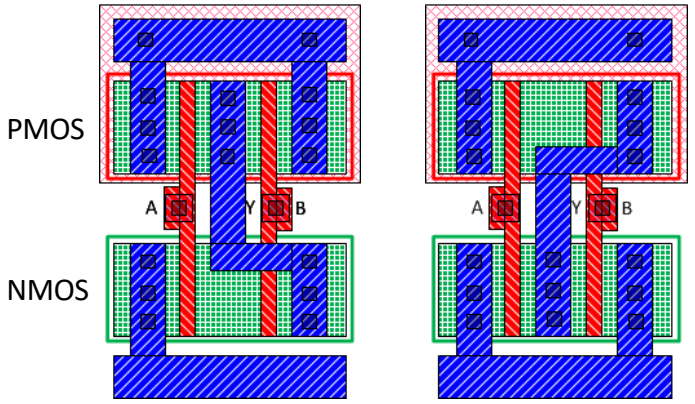
IC Camouflage



NAND



NOR

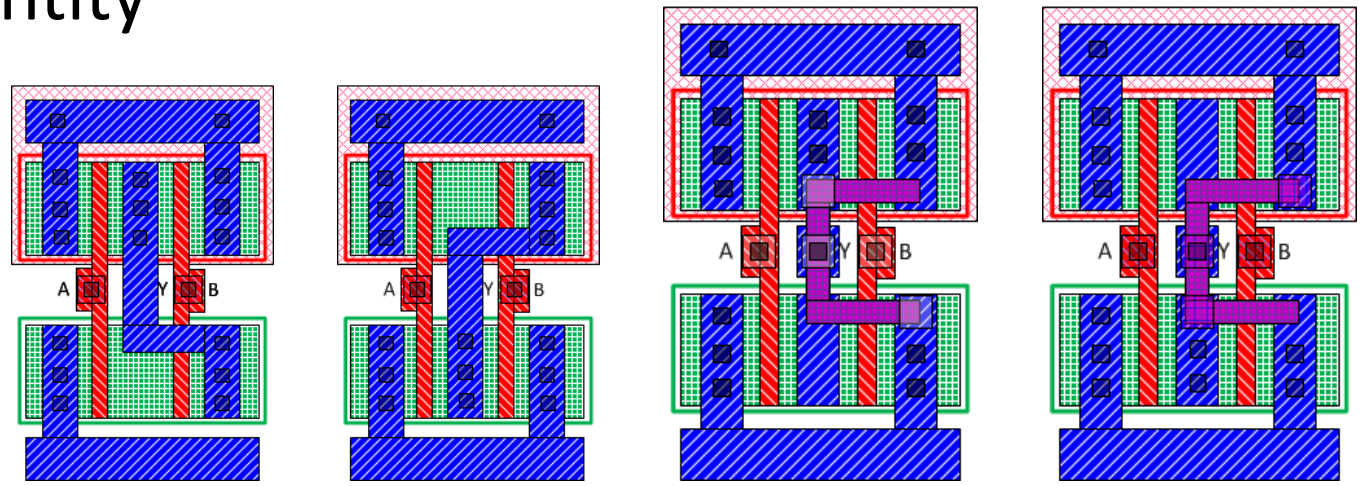


NAND NOR

Counterfeiting prevention

IC Camouflage

- Standard-cells are re-designed not to disclose their identity

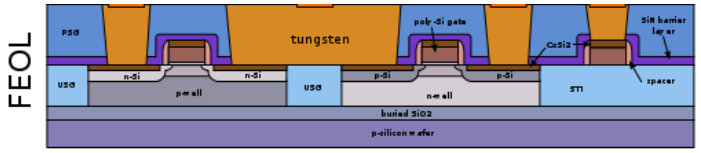


NAND NOR Camouflaged NAND Camouflaged NOR

Hardware Trojan prevention

Split Manufacturing

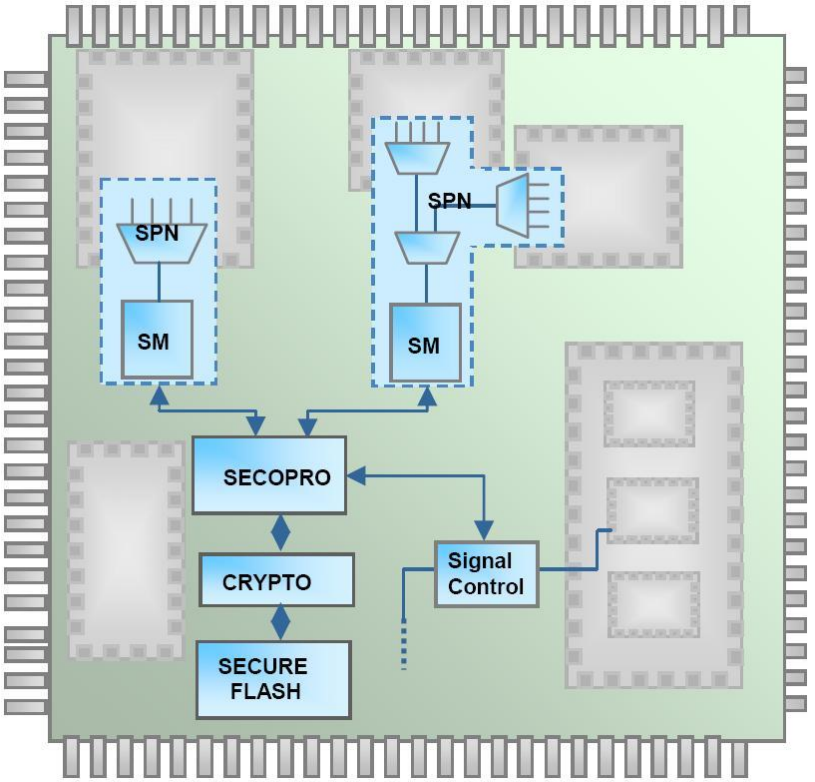
- Front End Of Line (FEOL) layers (transistor and lower metal layers) are fabricated in an untrusted foundry
- Back End Of Line (BEOL) in a trusted low-end fab
- It is considered secure against reverse engineering as it hides the BEOL connections from an attacker in the FEOL foundry



Hardware Trojan prevention

Online Detection

- Online monitoring to check:
  - Critical operations
  - Idle mode
  - Security policies
  - Performances
- Costly!!



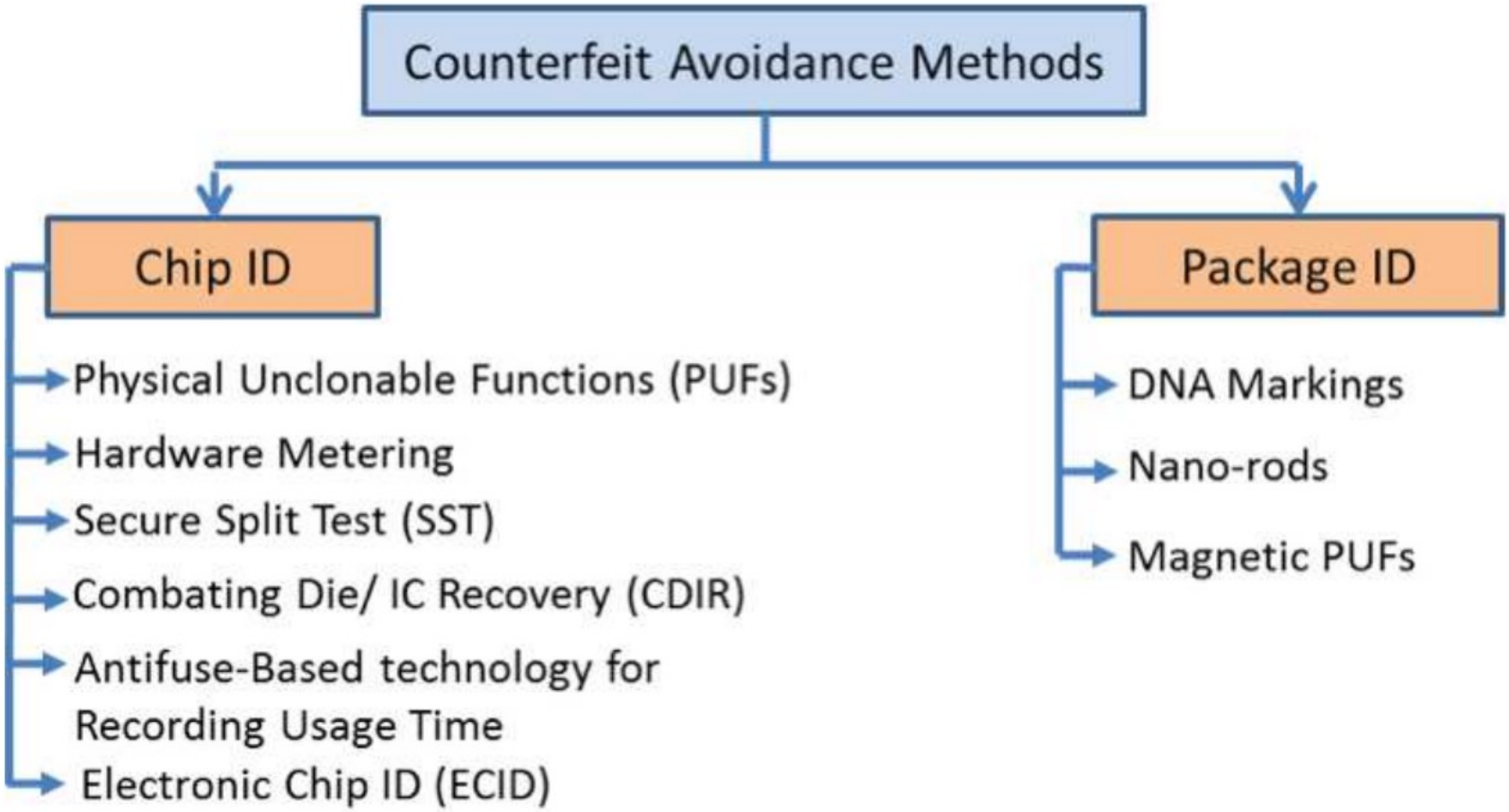
Counterfeiting prevention

IC Authentication

- Strong PUF
  - Many CRPs
- After manufacturing, each device is challenged by **several random** challenges
- Responses are stored in a secure database
- To authenticate the device, some of the challenges are used during mission mode

Counterfeiting prevention

Summary



Summary

Counterfeit Types

Counterfeit Detection	Overproduction	Recycling	Cloning	Trojans
HW Metering	Y		Y	y
IC Camouflage			Y	y
Aging Detectors		Y		
PUFs	y		Y	
Split Manufacturing	Y		Y	Y
Test methods		y		Y
Side-Channel				Y
Reverse Engineering			As mean	Y

Ujjwal Guin · Daniel DiMase · Mohammad Tehranipoor,
Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead,
J Electron Test (2014) 30:9–23

Physically Unclonable Functions

Physical(ly) Unclonable Functions

- To have a built-in mechanism that generates **one stable different** ID for **each identical device**
  - without the need of programming the ID value
  - without the need of storing the value!
- Advantages:
  - No reverse engineering can be applied
  - Even if you discover an ID in one circuit, you cannot program another circuit

Motivation & Goal

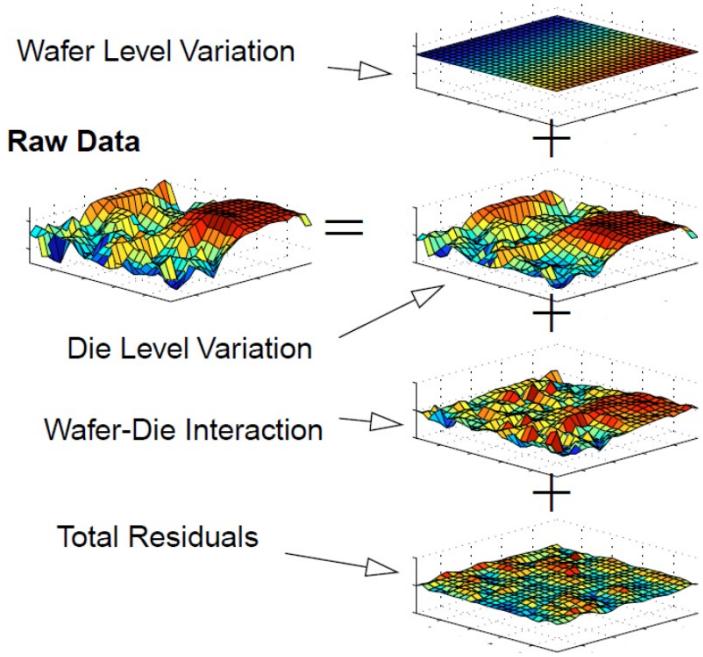
- PUFs can serve as a root of trust
- PUFs can provide a key which cannot be easily reverse engineered.
- PUFs provide every device with an individual fingerprint, characterized and stored in a data base during the production phase.
  - At a later stage, every device can be identified in the field using this PUF fingerprint information.

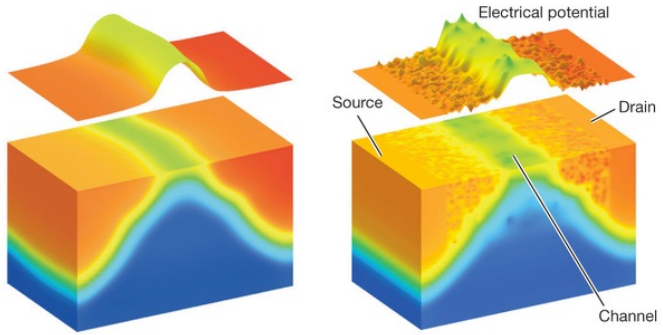
Physically Unclonable Functions

- PUFs are based on the comparison of **nominally-identical** physical characteristics
- Examples:
  - Delay of some networks
    - Ring Oscillator PUF
    - Arbiter PUF
  - Content of SRAMs at power-up
  - Resistance of STT-MTJs elements
  - Capacitance of TSVs

Process Variability

- Silicon PUFs exploit inherent physical variations (process variations) that exist in modern ICs
  - variations are uncontrollable and unpredictable, making PUFs suitable for IC identification and authentication

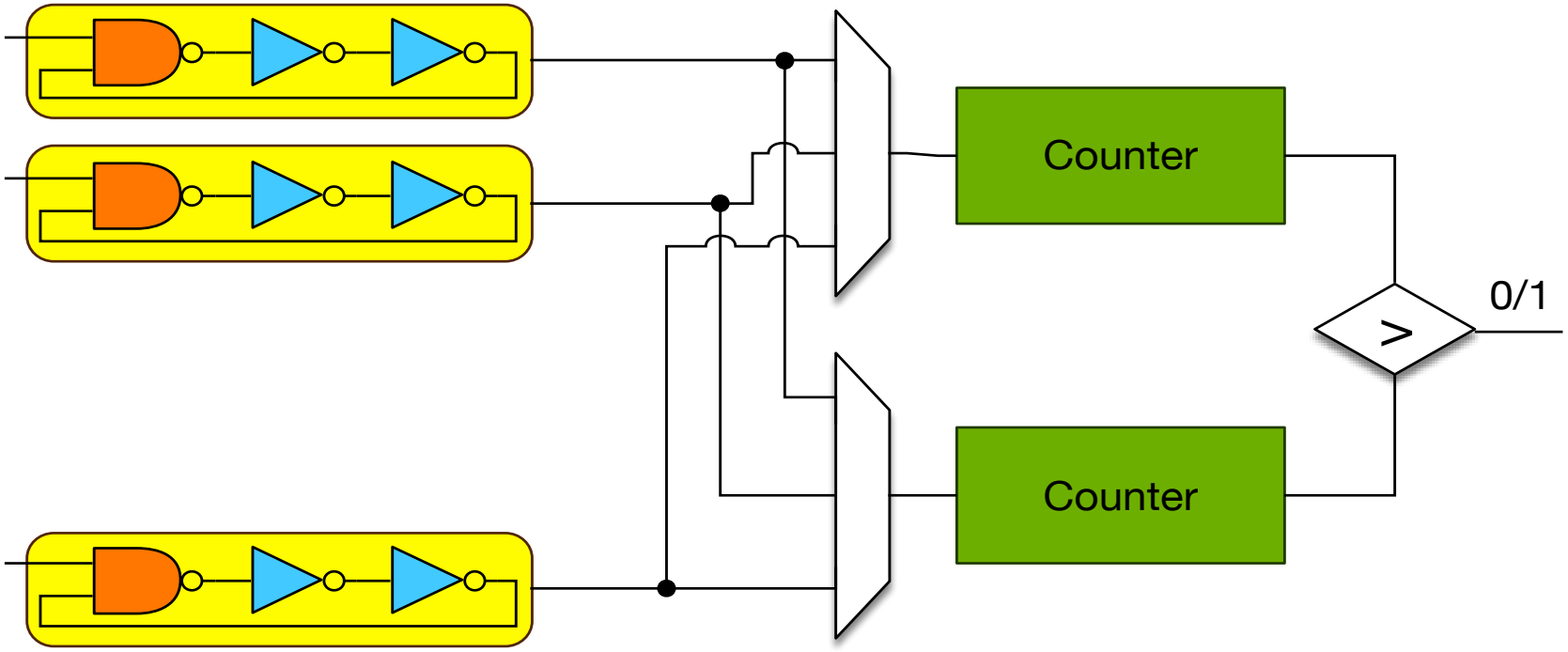




Random Dopant Fluctuation

Igor L. Markov, Limits on fundamental limits to computation, Nature 2014

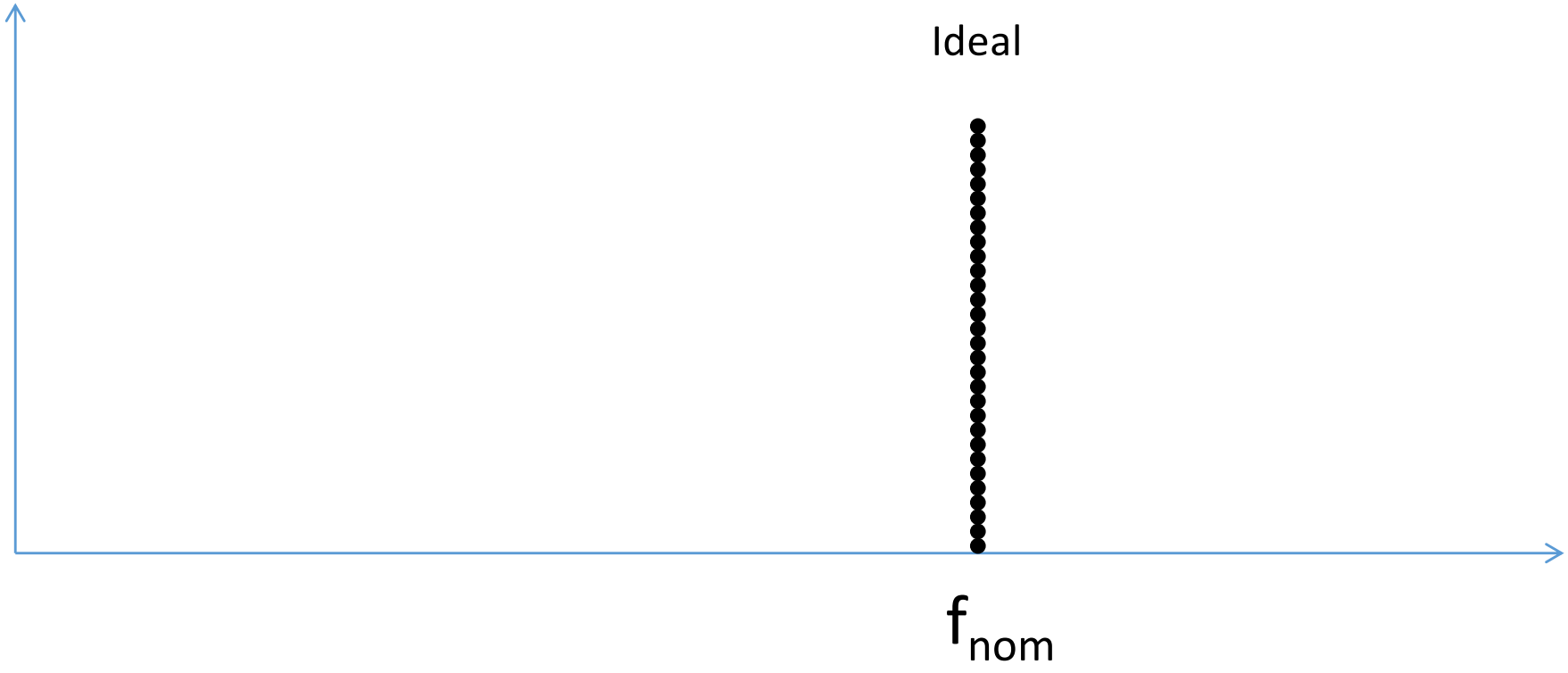
Ring Oscillator PUF



- Ideal: Frequencies of all Ring Oscillators identical

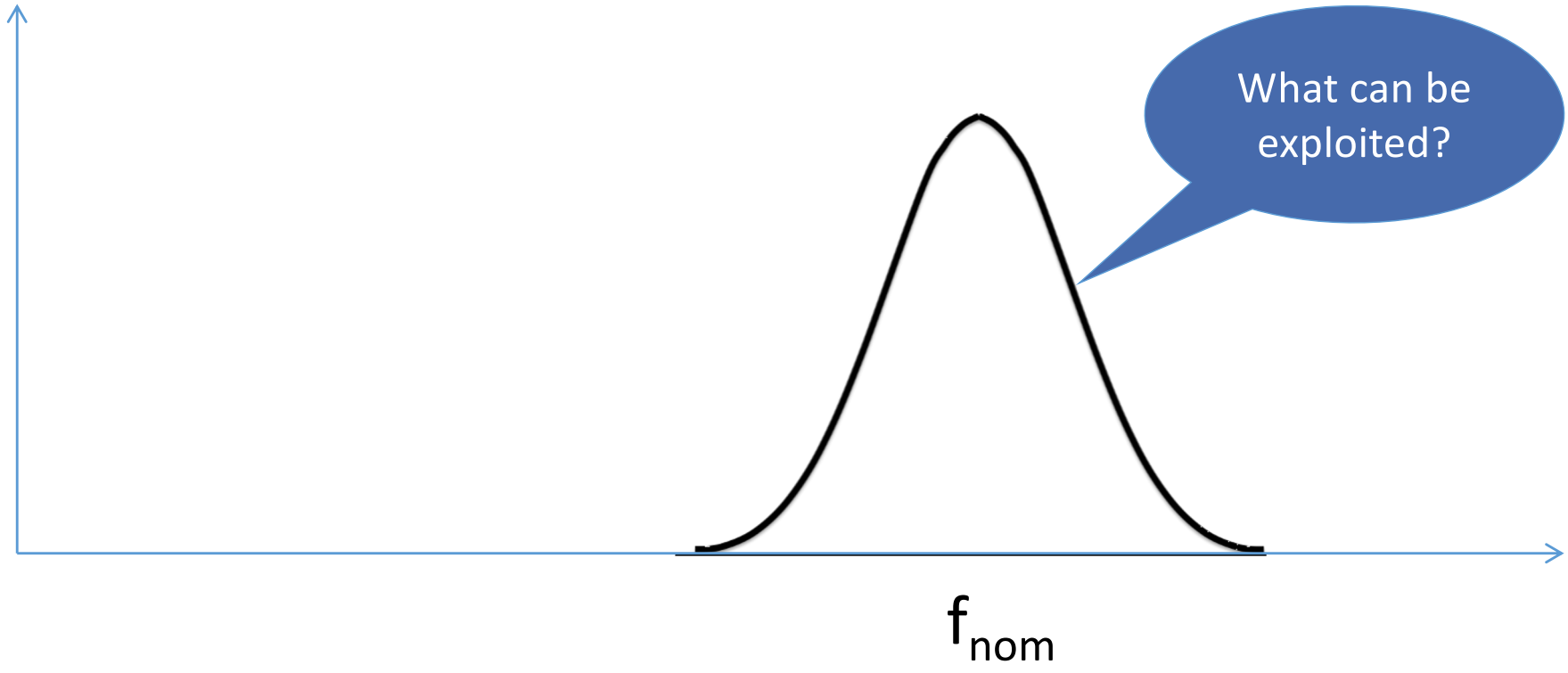
Process Variability

- Example: frequency of **identical** ring oscillators

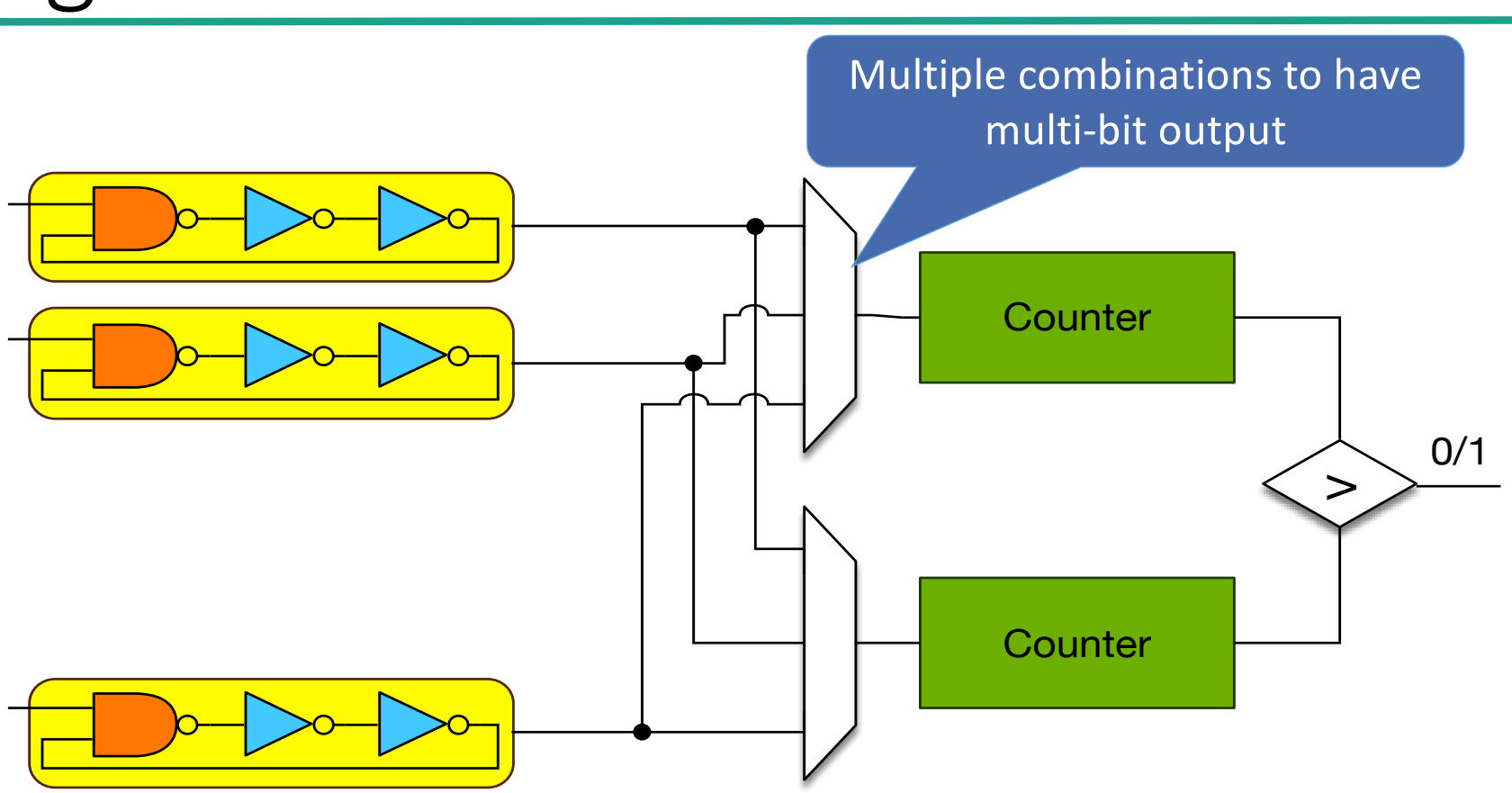


Process Variability

- Example: frequency of **identical** ring oscillators

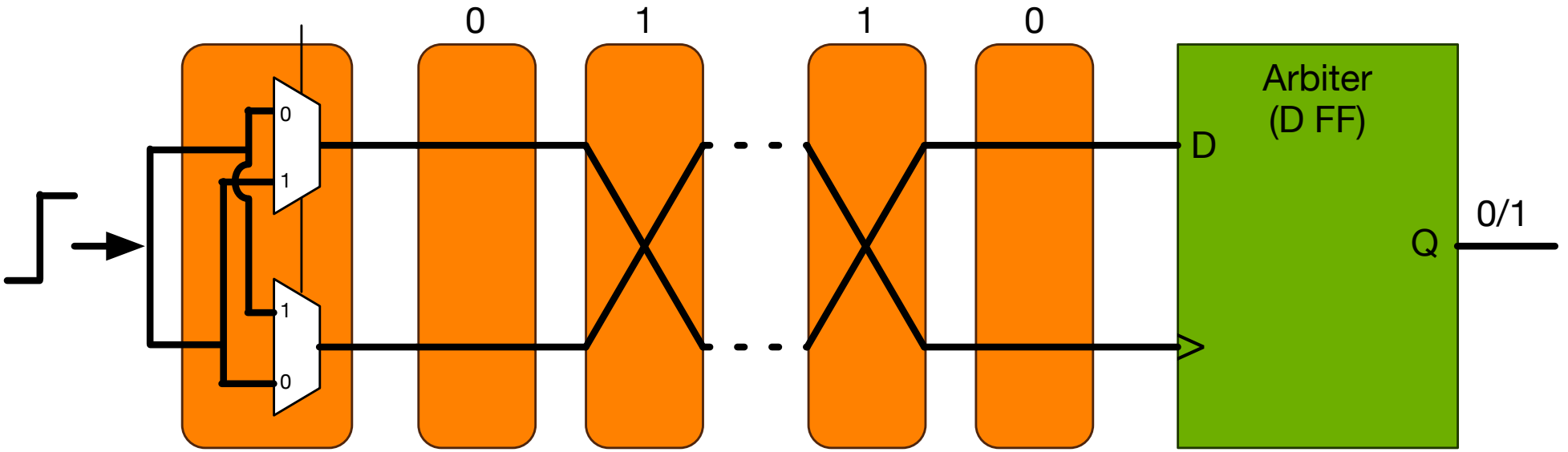


Ring Oscillator PUF



- Ideal: Frequencies of all Ring Oscillators identical
- Reality: because of process variations, all different!

Arbiter PUF



- Ideal: Delays of all the paths from input to output identical
- Reality: because of process variations, all different!

SRAM-based PUF

Power Up

- “Strength” of all inverters: identical
- Reality: because of process variations, all different!

Techniques of Informatics and Micro-electronics for integrated systems Architecture

http://tima.univ-grenoble-alpes.fr

Giorgio Di Natale

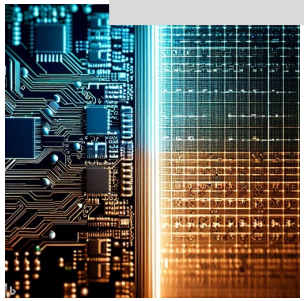
Techniques de l'Informatique et de la Microélectronique pour l'Architecture des systèmes intégrés

Micro and Nano Electronics

Digital, Analog, RF
Devices, Circuits
MEMS, Sensors
CMOS, FPGA, …

Microprocessors
Architectures
Embedded OS and SW
Algorithms

Computer Science



Specification, Design, Verification, Test for Integrated Circuits and Systems

To meet Energy, Cost, Performance, Quality, Dependability (Reliability, Safety, Security)

To enable Design Automation (Design Methods, CAD Tools)

TIMA

- Total: 100 ÷ 150
  - Faculty/Researchers: 34
  - Admin/Technical Staff: 14
  - PhD Students: ~50
  - Postdoc: ~5
  - Internship: 0 ÷ 50

Our research topics, goals and challenges

Digital ICs and systems

SLS
- System-Level Synthesis
- Hardware/Software co-design
- Simulation and verification

CDSI
- Low power design
- Asynchronous design
- MEMS, Smart Sensors and Actuators

Analog/mixed-signal/RF/mmW devices, circuits, systems

RMS
- Low power design
- Modeling, control and calibration

Dependability issues

AMfoRS
- Robustness, safety, reliability and test
- Hardware security and embedded trust

Goals:
Energy efficiency,
Cost, Performance,
Reliability, Resilience,
Safety, Quality,
Security, Trust,
Design Automation

Technologies:
CMOS, FDSOI
ASIC, FPGA
Emerging Memories
MEMS
Quantum

New challenges:
End of Moore's law
New technologies
New applications

Our research topics

- **Circuit and System Design and Test**
  - Digital, Asynchronous, Analog, AMS, RF, Beyond 5G and sub-THz communications, 3D
  - MEMS and Smart Sensors
- **CAD tools**
- **Properties:**
  - Energy, Cost, Performance, Quality, Dependability
  - Hardware Security
  - Sovereignty, Trust of Supply Chain
  - Safety, Robustness
- **Environmental responsibility**
  - Ultra Low Power and Ultra Low Voltage Digital, AMS, RF circuits
  - Energy harvesting
- **Applications:**
  - Secure Hardware
  - IA (embedded, new technologies)
  - RISC-V
  - Cryo-CMOS electronics, Quantum computing
  - Smart self-adaptable systems
  - Haptic Systems
  - Medical

https://tima.univ-grenoble-alpes.fr/