Hardware & Embedded Security

Part 2

Academic Year: 2024-2025

Prof Daniele Rossi


Via G. Caruso 16, room B-1-03


daniele.rossi1@unipi.it


050 221 7611

1

Detection of Counterfeit ICs

Lecture 2 - DR

2

Brief Outline

- Counterfeit detection
  - Basics on IC test processes

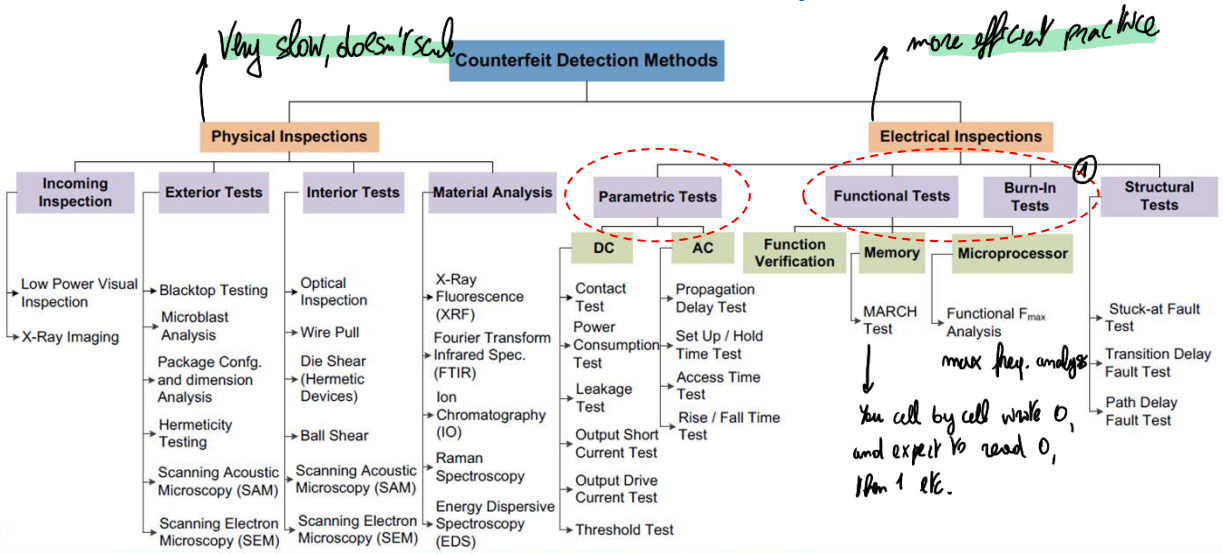
We can run some test procedures to detect counterfeit components

3

Basics on Electrical Tests for Integrated Circuits

4

Detection Method Taxonomy



5

① Burn-in test: related to infant mortality. You can't afford to test a component for days/months. Tests must last hours at max. But how to identify defects that will make components fail shortly. So you can try to "accelerate" occurrence of malfunctions. You stress them in a non-nominal condition: higher temperature, electric stress etc. This is the Burn-in test. But you don't want to exhaggerate and damage components.

Electrical Tests

- Mainly focus on large scale integrated circuits
  - Microprocessor, Memory, and Programmable Logic chips account for almost 35% of counterfeits
- As these are **high-cost parts**, counterfeiter will probably **put much effort to counterfeit** and **physical detection** will be **extremely difficult** (merely impossible)
- No definite test methodology either electrical or physical (without destroying the chip) to detect counterfeit with 100% confidence level

Even after carrying out tests ↑ Same for defects

6

There is a parameter to quantify manufacturing process called "Yield".
For established processes, Y can be higher than 96%. For new processes even 60%

VLSI Chip Yield

- Electrical tests are mainly applied to test for manufacturing defects after chip fabrication
- A manufacturing defect in the fabrication process causes electrically malfunctioning circuitry
- A chip with no manufacturing defect is called a **good chip**; the defective ones are called **bad chips**
- Percentage of good chips produced in a manufacturing process is called the **yield**
- Yield is denoted by symbol Y

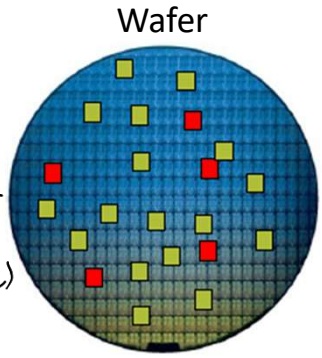
$$Y = \frac{\#\ of\ good\ chips}{\#\ of\ all\ manufactured\ chips}$$

- How can we distinguish bad chips from good chips? Yield is denoted by symbol Y

Ideally → **we test all chips!** Or we work with samples to save $ and Y

Why test matters?

- In simple terms, TEST identifies the defective chips
- Some bad chips (■) are easy to find
- Some other are difficult (■)



- Test is associated with
  - Cost and Return On Investment (ROI)
    → n ¥ € $ - Money.

They cost but they allow you to save money: higher return on investment vs no damage to reputation (warranty replace)

- Since counterfeit ICs can be considered as defective chips (and they actually are defective!)

→ **Principles and methods from "manufacturing" testing can be applied to identify counterfeits!**

Electrical Tests

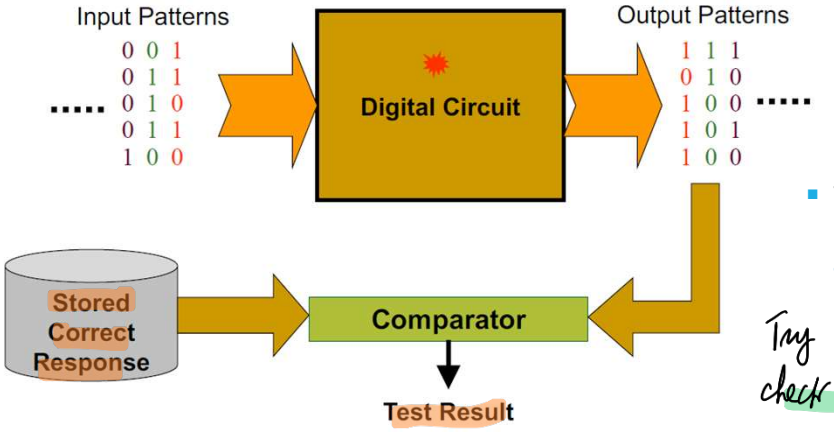
Two main types of electrical test:

- **Parametric test (DC & AC)**
  - It targets the testing of the electric properties of a component
- **Functional test**
  - It targets the (logic) functionality of a component

9

FOR DIGITAL SYSTEMS: you know the correct response to expect for every input pattern.

Testing Principles



- This is the process usually adopted for **functional testing**

Try input patterns and check if output patterns = expected patterns.

10 BUT: Digital circuit can also be a sequential circuit, you can have millions of different internal states. You cannot guarantee to detect all possible functional conditions for your system. But even for a very simple circuit (CN), you may have a huge number of inputs.

If you want to test properly, you need to design your test properly to avoid false positives and false negatives.

Functional Tests

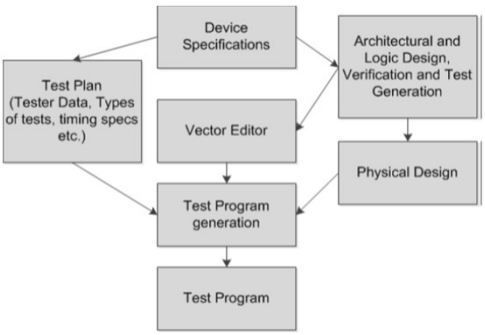
- **Functional testing** is the most efficient way of verifying the functionality of a component.
- **Function Verification** of a Component
  - Determines whether individual components, possibly designed with different technologies, function as a system and produce the expected response.
- **Memory Tests**
  - Read/write operations are performed on a memory to verify its functionality. MARCH tests can be applied for counterfeit detection.
- **Microprocessor Tests**
  - Microprocessors are binned in different groups depending on the maximum functional frequency (fmax).

11

Electrical Tests

Tester: ATE (Automated Test Equipment)

- Specification:
  - Speed (clock rate of the device)
  - Timing (strobe) accuracy
  - Number of input/output pins, etc.
- Test Programming
- Limitation
  - HDL description of test module must be available to test ICs
  - No definite methodology to detect counterfeit ICs



12

Parametric Test

- **DC Parametric test**
  - Contact Test
  - Power Consumption Test
  - Leakage Test
  - Output Short Current Test
  - Output Drive Current Test
  - Threshold Test
- **AC Parametric test**
  - Propagation delay test
  - Setup/hold time test
  - Access time test
  - Rise and fall time test

13

Parametric Test: DC Examples

Contact Test

1. Set all inputs to 0 V
2. Force current I (e.g. I ~ 10s μA) out of pin
3. Measure pin voltage Vpin and calculate pin resistance R
   - R ≈ 0 Ω → Contact short (R = 0 Ω) → OK!
   - R >> 0 Ω (huge) → Pin open → problem due to no or poor contact

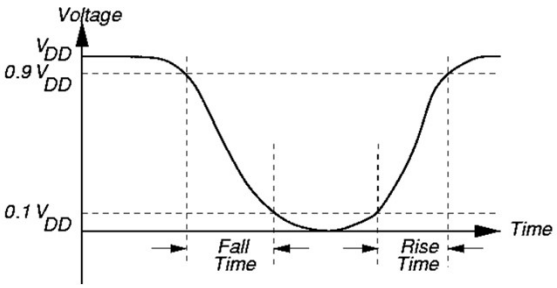
Output short current test

1. Make chip output a 1
2. Short output pin to 0 V in a precision measurement unit (PMU)
3. Measure short current (but not for long, or the pin driver burns out)
   - Short current > I_f (~ μA) → OK
   - Short current ≤ I_f → fails!

14

Parametric Test: AC Examples

Rise/fall time test



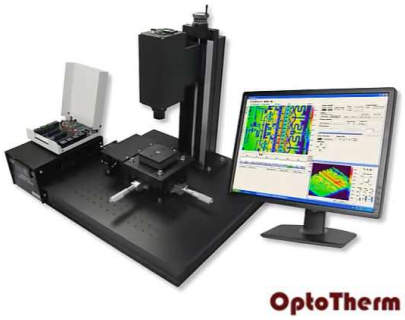
Propagation delay test

1. Apply standard output pin load
2. Apply input pulse with specific rise/fall
3. Measure propagation delay from input to output
   - Delay in expected range → OK!
   - Delay outside expected range → fails!

15

Temperature Cycling/ Burn-In

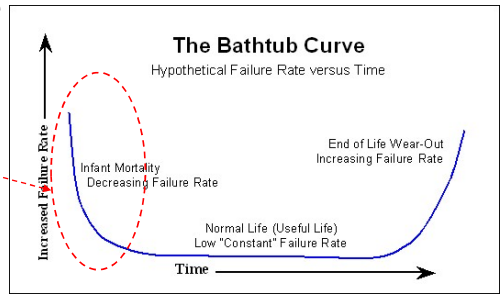
- Testing the chip at extremes of operating range:
- Tester ranges:
  - Military Grade: -65°C to 175°C
  - Industrial Grade: -25°C to 85°C
  - Commercial Grade: -10°C to 70°C



16

Temperature Cycling/ Burn-In

- **Burn-in**
  - The device is operated at an elevated temperature (Stressed condition)
  - To find infant mortality failures and unexpected failures to assure reliability.
- Test methods
  - MILSTD-883 for integrated circuits and
  - MIL-STD-750 for other discrete components.
- Very useful as **it can easily weed out the commercial grade components marked as military grade**.



17

Summary on Electrical Tests

- **Parametric tests** – determine whether pin electronics system meets **digital logic voltage, current, and delay time specs**
- **Functional tests** – determine whether internal **logic/analog sub-systems behave correctly**
- **ATE Cost** Problems
  - Pin inductance (expensive probing)
  - Multi-GHz frequencies
  - High pin count
- **Test Cost Reduction**
  - **Design for Test(ability) - DFT** - methods (like Built-In Self-Test) → additional circuitry added to ICs just to facilitate their test (e.g., scan chains)

18

Downsides of Physical and Electrical Tests

- Both physical and electrical tests/inspections
  - **Require specialised, often costly, equipment** → not everybody can afford to go through these kind of processes in a systematic way
  - **Can be (are) very time consuming** → suitable for checking a limited number of ICs
  - As a result, these processes are **not scalable**!

- Recently, the use of **hardware metering** techniques or the introduction of additional circuitry into the ICs (like for DFT) to facilitate the identification of counterfeits is gaining momentum!

19

Thank you!

Any questions?

20