

Any questions so far?

27/02/2025

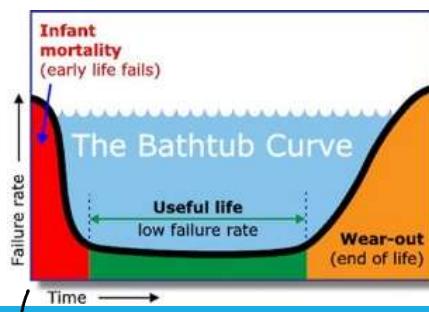
Hardware and Embedded Security - Prof. Daniele Rossi

31

31

Recycled Components & Aging Phenomena

- More than 80% of the counterfeit components are recycled
- Most of the recycled parts are at the end of life → damaged considerably due to usage and aging



Failure rate as time goes on:
for a short lifetime period we have chips may stop working
properly very soon: this is for production defects. Production
is complex and we cannot avoid defects

27/02/2025

Hardware and Embedded Security - Prof. Daniele Rossi

32

32

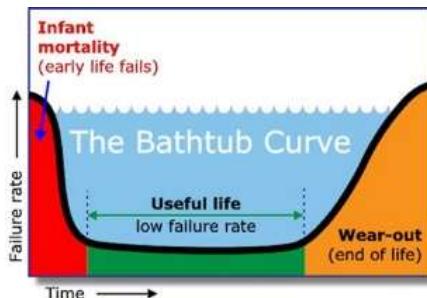
So these chips should be avoided. So we test chips to try to identify as many chips as possible. We can either destroy them or do failure analysis: understand what went wrong. So we now are in the useful life region.

After a bit, though, your system is going to wear out.

14

Recycled Components & Aging Phenomena

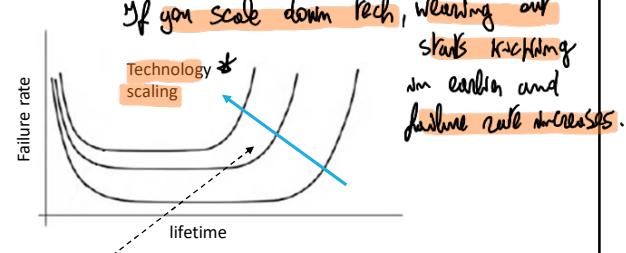
- More than 80% of the counterfeit components are recycled
- Most of the recycled parts are at the end of life → damaged considerably due to usage and aging



27/02/2025

Hardware and Embedded Security - Prof. Daniele Rossi

33



New aging mechanisms:

- Negative and Positive Bias temperature instability (NBTI, PBTI) (Muniby meghni)
- Hot carrier injection (HCI) ①
- Time dependent dielectric breakdown (TDDB)
- ...

- 33 ① HCl = highly energetic
 ② In MOS we have dielectric very thin, that can eventually (not abruptly) break down.
 * With scaling we refer to the size of transistors (the channel): $I_D \propto \frac{W}{L}$



DRO
 Injected carriers vs Trapped carriers; dielectric gets weaker as electric fields are applied over it.

Basics on Transistor Aging Phenomena

- When the chip operates in functional mode, the transistors age mainly due to **NBTI (Negative Bias Temperature Instability)**, and **HCI (Hot Carrier Injection)**.
- The aging effects of NBTI and HCI can cause **parametric shifts** and circuit failures
- NBTI occurs when a negative gate-to-source voltage is applied at the pMOS transistors (i.e., when they are ON), which breaks Si-H bonds generating the interface traps → **NBTI is data dependent!**
- These interface traps can get electrically charged and increase the absolute value of the pMOS threshold voltage (V_{th}), resulting in reduced transistor current and increased gate delay
- HCI occurs in nMOS devices caused by the trapped interface charge at Si-SiO₂ surface near the drain end during switching that results a non-recoverable V_{th} degradation

27/02/2025

Hardware and Embedded Security - Prof. Daniele Rossi

34

34

- NBTI, PBTI could really be neglected with larger components. But for tech nodes before 80-60nm, those are impacting.
- Problem is related

defects we can find for transistors. Related to potential wells

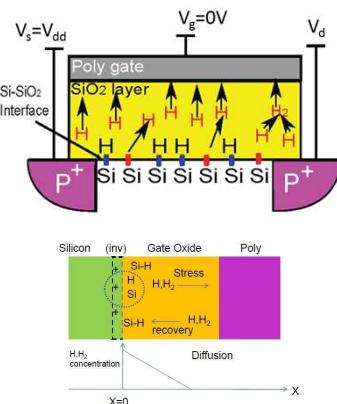
That are able to trap electrons (due to impurities you have during production)

Because of quantum phenomena like tunnel effect that makes electrons fall in

What happens to MOS transistors as they age? (I)

the well without having potential. So effect is that threshold voltage increases, so I_o smaller.

- Aging effects: physical description



$$\Delta V_{th} = \frac{qN_{it,NBTI}(t)}{C_{ox}} \quad N_{it,NBTI}: \text{interface traps generated by NBTI}$$

- A similar effect takes place for HCI:

- HCI occurs when the electron or hole in the transistors gains sufficient energy to overcome the silicon dioxide barrier in order to break an interface state → interface traps are generated

$$\Delta V_{th} = \frac{qN_{it,HCI}(t)}{C_{ox}} \quad N_{it,HCI}: \text{interface traps generated by HCI}$$

27/02/2025

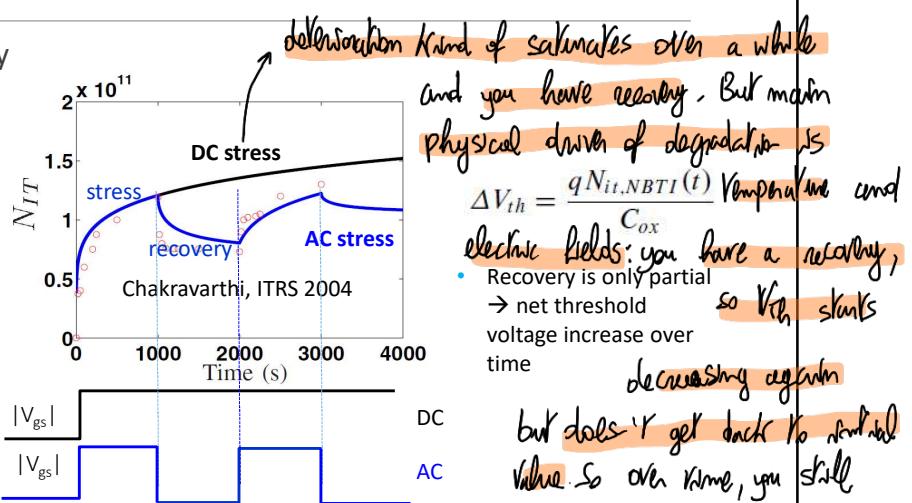
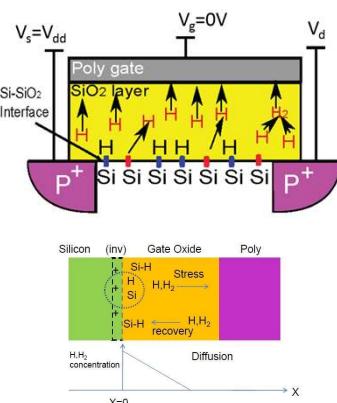
Hardware and Embedded Security - Prof. Daniele Rossi

35

35

What happens to MOS transistors as they age? (II)

- NBTI: stress and recovery



27/02/2025

Hardware and Embedded Security - Prof. Daniele Rossi

36

36 have degradation. Transistor degrades when $|V_{gs}|$ is on, partially recovers when $|V_{gs}|$ is off. Degradation of a component is date dependent. (Recovery happens for trapped charges)

NMOS is on with logic 1 and off with logic 0. Depends on the workload we are going to process. This is bad for designers.

To tackle this problem, designers make systems slower. You lose performance at the very beginning of course.

You can even adjust frequency of circuits overtime. Systems embed performance monitors overtime to look at your degradation rate and slow down clock signals or voltage supply.

Temperature worsen device degradation; $\alpha = \text{stress ratio}$: components are mostly on: α high.

What happens to MOS transistors as they age? (III)

- NBTI: analytical modelling

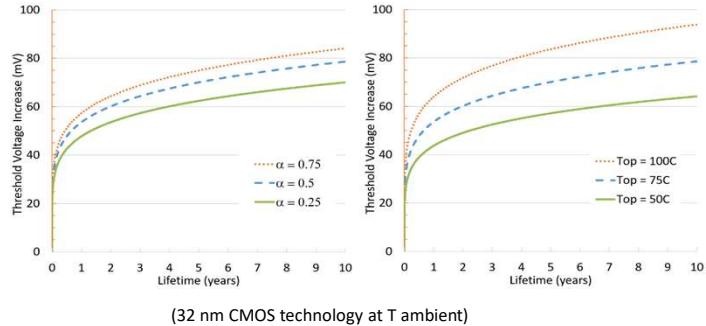
$$\Delta V_{th} = \xi K \sqrt{C_{ox}(V_{gs} - V_{th0})} e^{-\frac{E_a}{kT}(\alpha t)^{\frac{1}{6}}}$$

α : stress ratio

T : operating temperature

t : operating time (lifetime)

E_a : activation energy



Stress ratio: ratio between the amount of time during which the device is under stress (ON) and the overall operating time → Stress ratio accounts for NBTI aging data (workload) dependency

27/02/2025

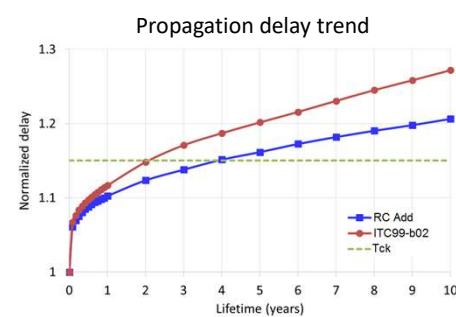
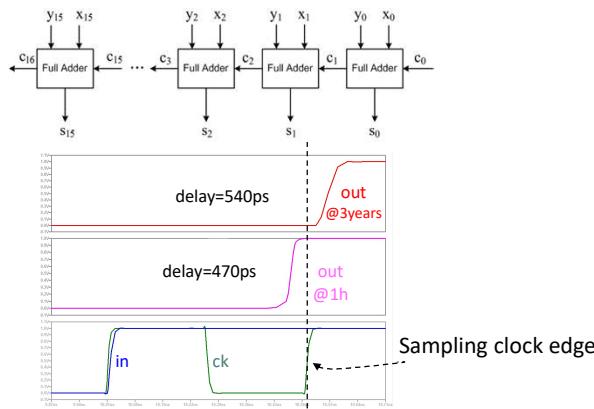
Hardware and Embedded Security - Prof. Daniele Rossi

37

37

Aging Effects in Electronic Circuits Performance (I)

- The overall (and well characterized) effect is that electronic circuits get slower



- Propagation delay degradation can lead to the sampling of a wrong data → reliability issue → Lifetime (LT) reduction

27/02/2025

Hardware and Embedded Security - Prof. Daniele Rossi

38

38

You can use the model up there as a model for ΔV_{th} over time.

C_{ox} = oxide capacitance

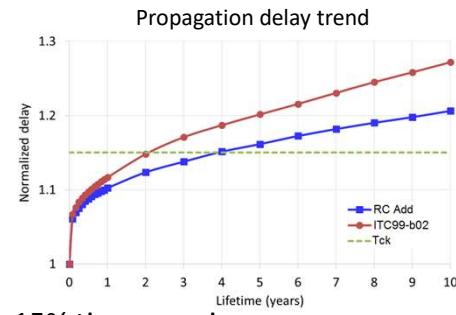
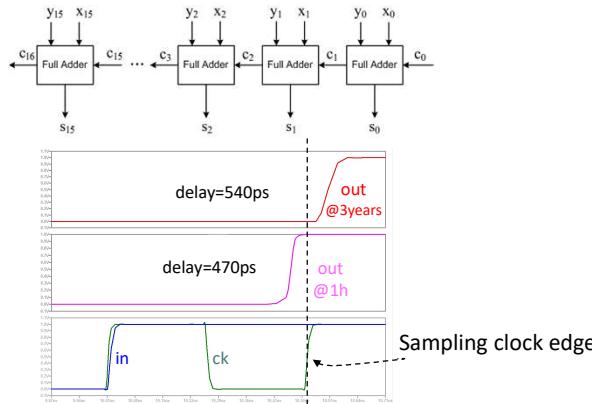
Example of simulation on apple carry adder. You do a simulation for the worst case propagation delay $T_{PD} \rightarrow$ this leads you to the minimum $T_{CK_{min}}$ \rightarrow then you select the real $T_{CK} = T_{CK_{min}}(1 + \%)$

↳ percentage of slack

NOTE: What is the signal that is experiencing the worst prop. delay? C_{16} is the one. And after NRI estimation, we have a delay of 170 ps in th, but in 3 years you get 540 ps. If you want to have an idea of survival time, you can plot propagation delay over time (this is the worst case). So you can increase the slack to get better results.

Aging Effects in Electronic Circuits Performance (II)

- The overall (and well characterized) effect is that electronic circuits get slower



- 15% time margin:

- $LT_{itc} = 2.1$ years
- $LT_{add} = 4$ years

27/02/2025

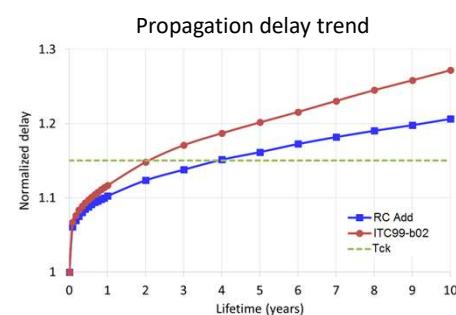
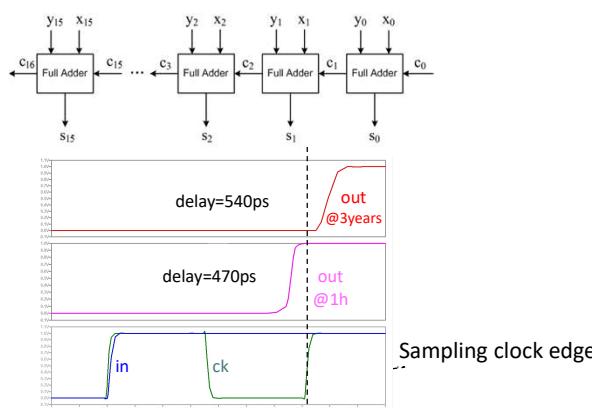
Hardware and Embedded Security - Prof. Daniele Rossi

39

39

Aging Effects in Electronic Circuits Performance (III)

- The overall (and well characterized) effect is that electronic circuits get slower



- 20% time margin:

- $LT_{itc} = 4.8$ years
- $LT_{add} = 9$ years

27/02/2025

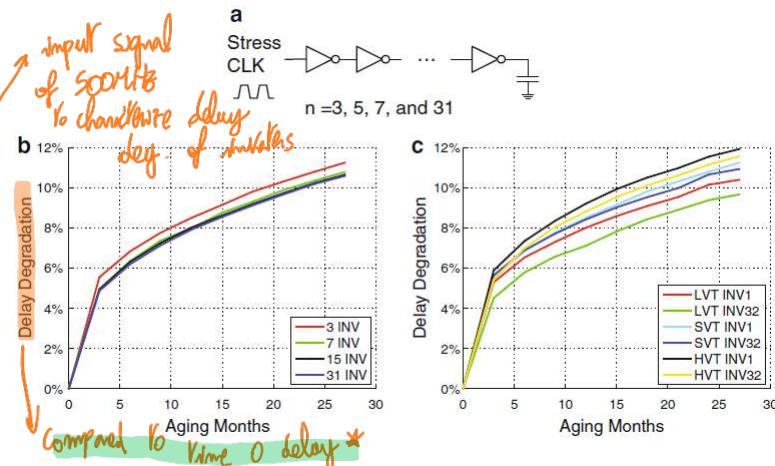
Hardware and Embedded Security - Prof. Daniele Rossi

40

40

Aging Effects Analysis for Recycled IC Detection (I)

- Example: inverter chain
- Inverter chains with the same capacitive load and the same stress coming from a 500 MHz clock
- These chains are composed of 3, 7, 15, and 31 standard, high, and low threshold voltage (SVT, HVT, and LVT) inverters



27/02/2025

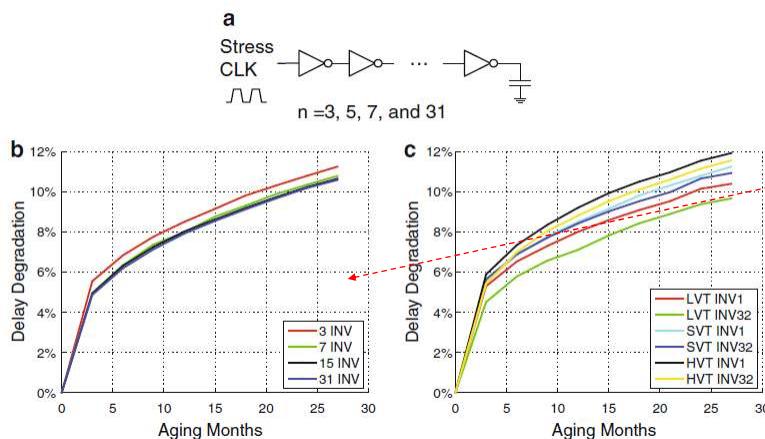
Hardware and Embedded Security - Prof. Daniele Rossi

41

41

*Relative degradations doesn't depend much from the chain length of inverters. What has a bigger impact (red plot), we have a simulation of inverters with different threshold voltage: Standard VT, High, Low. HVT used in low power design (Tradeoff for performance) => static power for leakage decreases if VT is higher. ①

Aging Effects Analysis for Recycled IC Detection (II)



- Delay degradation of inverter chains under clock stress for up to 27 months with no interruption

Fig. b: the **number of inverters** does not have a **significant impact** on the degradation of these chains since they receive the same stress, and each inverter's speed degrades at the same rate

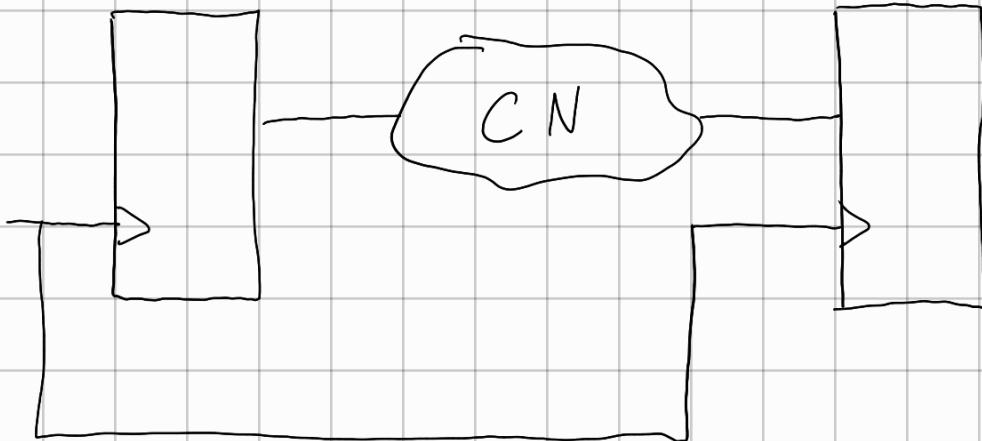
27/02/2025

Hardware and Embedded Security - Prof. Daniele Rossi

42

42

① Components with higher threshold voltage are experiencing highest levels of degradation. This is for construction physical defects.

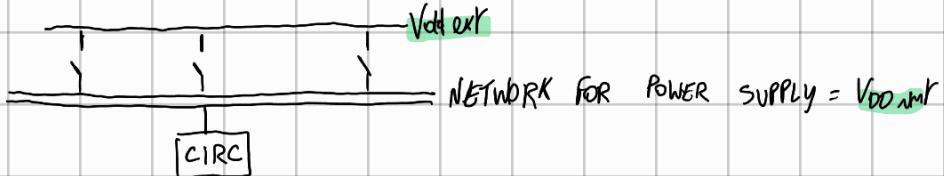


CK

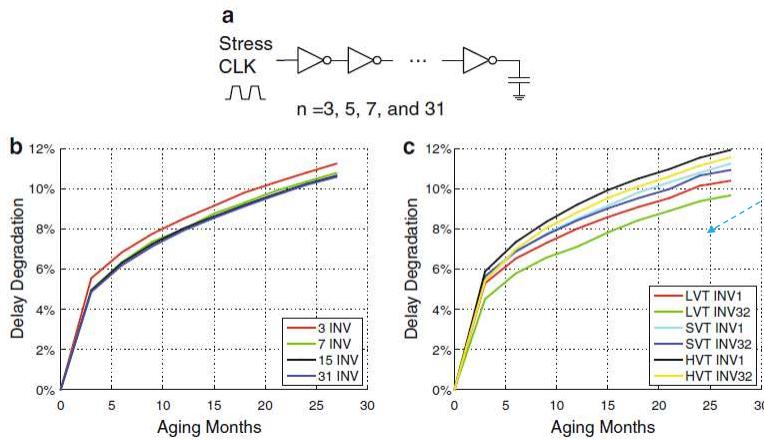
switching from 0 to 1, even if CN doesn't have anything useful for a while. So you can turn off the clock and save power:



- This is called clock gating. This reduces dynamic power.
- To reduce static power consumption, you can turn off voltage supply! Power gating



Aging Effects Analysis for Recycled IC Detection (III)



- Delay degradation of inverter chains under clock stress for up to 27 months with no interruption
- Fig. c: the chain with the **HVT inverters** experiences **more degradation** than the chains with the SVT or LVT inverters,
- the **INVX1** inverter chain has a **larger degradation** than the **INVX32** inverter chain

27/02/2025

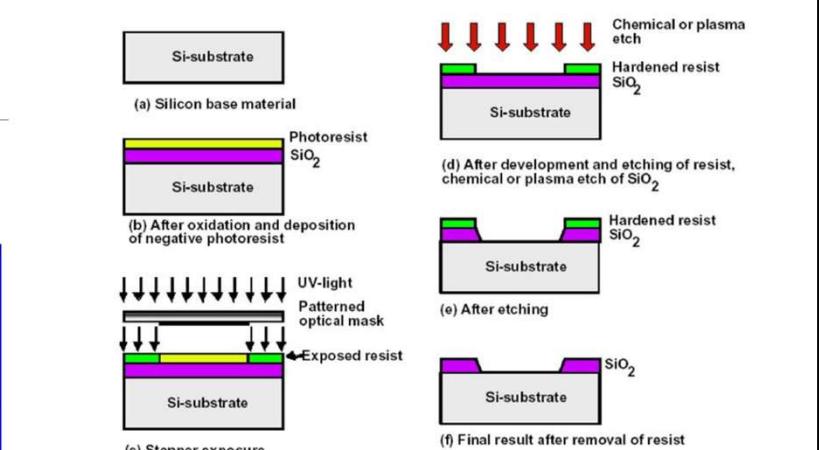
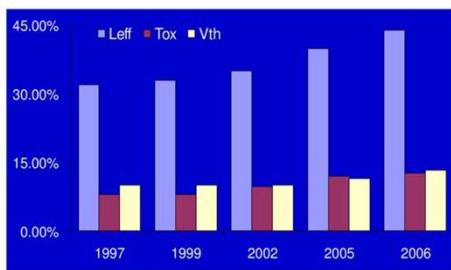
Hardware and Embedded Security - Prof. Daniele Rossi

43

43

Lithography Manufacturing Process

Process variations trend



- As technology scales, all kinds of sources of variations
- Critical dimension (CD) control for minimum feature size
 - Doping density
 - Masking

27/02/2025

Hardware and Embedded Security - Prof. Daniele Rossi

44

44

Another interesting phenomenon: process variations. When you scale down the technology, the manufacturing mechanisms become increasingly complex.

Photolithography is one of the main manufacturing mechanisms that need to be performed, and defining component parameters precisely gets harder.

Components are characterised by W , L , V_{TH} ..., that have impact on performance.

Problem is that these parameters cannot be really defined very precisely.

So in complex circuits we will have transistors ideally the same, but upon closer looks, we don't have a specific value.



Effect: Components that should behave the same, will have different performances.

If we pick a component in A and B, A will be more performing than B.

- This is process variation (for one IC, you have one value in this distribution)

Idea: I can compare component with a new one to see if they are recycled.

But for a new component I don't know precisely the performances!

And as we scale down, this difference is even bigger.

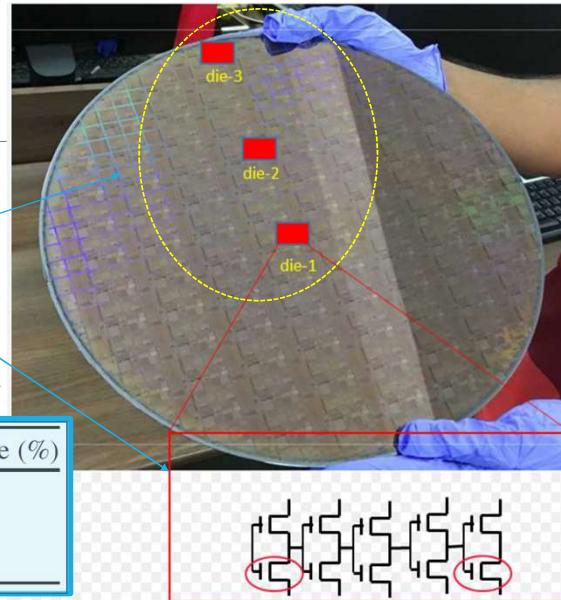
As a reference, assume I am in A with a new component I take another that falls in B. How can I tell if I was unlucky and component is new or if I have a recycled one?

You have different chips within a wafer and they exhibit different variations.

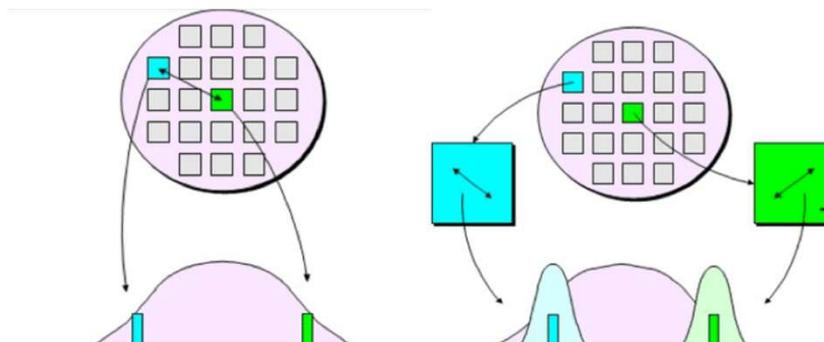
Process Variations

- There can be both
 - Die-to-Die (D2D), or **inter-die** variations, and
 - Within-Die (WID), or **intra-die** variations

Parameter	Inter-die (%)	Intra-die (%)
Threshold voltage (V_{th})	20	5
Channel length (L)	8	2
Oxide thickness (T_{ox})	4	1



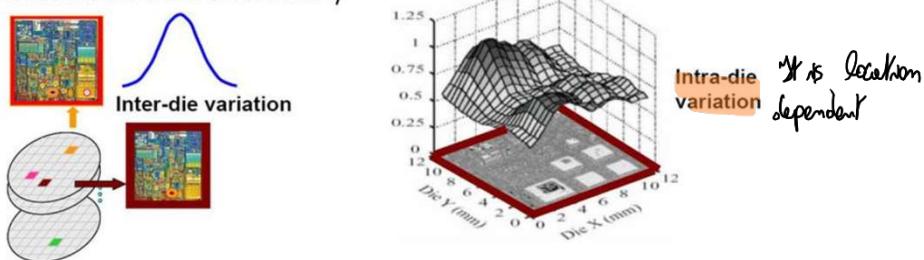
Process Variations



- Die-to-Die (D2D), or **inter-die** variations
- Within-Die (WID), or **intra-die** variations

Process Variations

- **Inter-die vs intra-die variation**
 - Inter-die variation: same devices at different dies are manufactured differently
 - Intra-die (spatial) variation: same devices at different locations of the same die are manufactured differently



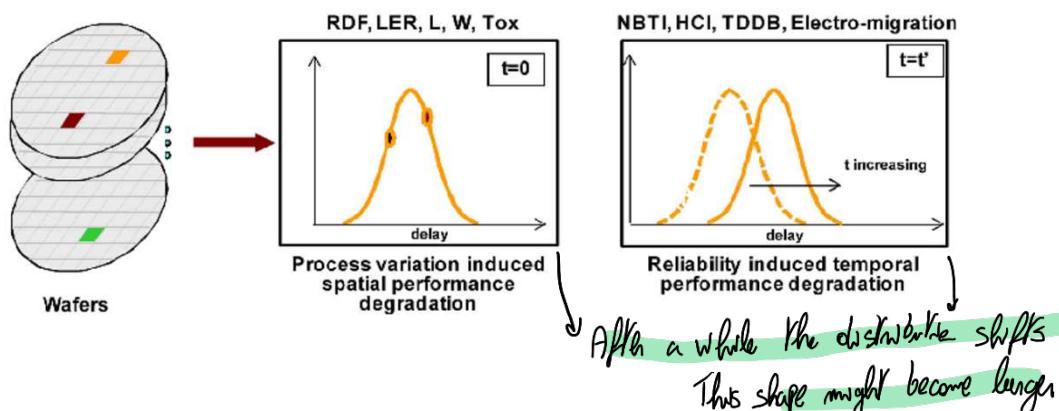
27/02/2025

Hardware and Embedded Security - Prof. Daniele Rossi

47

47

Process Variations and Aging



27/02/2025

Hardware and Embedded Security - Prof. Daniele Rossi

48

48 Intel characterizes processes based on their performance. They run tests and sell components on the left as max operating frequency components at maximum power. Tests are called speed binning.

Some interesting videos

- What's inside a microchip? <http://www.youtube.com/watch?v=GdqbLmdKgw4>
- Zoom Into a Microchip <http://www.youtube.com/watch?v=Fxv3JoS1uY8>
- Counterfeit Electronics Could Be Dangerous, Funding Nefarious People
<http://www.youtube.com/watch?v=dbZlUe6guxc>
- How Computers and Electronics Are Recycled (about proper electronic waste management)
<http://www.youtube.com/watch?v=lw4g6H7alvo>
- Counterfeit Electronic Components Process
http://www.youtube.com/watch?v=5vN_7NJ4qYA
- Counterfeit Visual Inspection <http://www.youtube.com/watch?v=MbQUvu2LN6o>
- Gold from waste circuit electronics <http://www.youtube.com/watch?v=ZkhOuNvkuu8> (no longer available)

Any questions?