Project Number: FP7-611404

D2.2.1 - Characterization of failure mechanisms for future systems (preliminary)

Authors[1]

S. Ozdemir (INTEL), N. Aymerich (INTEL), M. Riera (UPC), R. Canal (UPC), A. González (UPC), M. Kaliorakis (UoA), S. Tselonis (UoA), N. Foutris (UoA), D. Gizopoulos (UoA), A. Benso (POLITO), S. Di Carlo (POLITO)

Version 1.4 – 31/10/2014

Lead contractor: UPC
Contact person: Antonio González Dep. of Computer Architecture Universitat Politècnica de Catalunya Campus Nord UPC, Cr. Jordi Girona 1-3, 08034 Barcelona (ES) E-mail: antonio@ac.upc.edu
Involved partners[2]**:** UoA, INTEL, THALES, YOGITECH, POLITO, UPC, ABB, CRNS
Work package: WP2
Affected tasks: T2.1

Nature of deliverable[3]	R	P	D	O
Dissemination level[4]	PU	PP	RE	CO

[1] *Authors listed here only identify persons that contributed to the writing of the document.*

[2] *List of partners that contributed to the activities described in this deliverable.*

[3] ***R**: Report, **P**: Prototype, **D**: Demonstrator, **O**: Other*

COPYRIGHT

© COPYRIGHT CLERECO Consortium consisting of:

- Politecnico di Torino (Italy) – Short name: POLITO
- National and Kapodistrian University of Athens (Greece) - Short name: UoA
- Centre National de la Recherche Scientifique - Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier (France) - Short name: CNRS
- Intel Corporation Iberia S.A. (Spain) - Short name: INTEL
- Thales SA (France) - Short name: THALES
- Yogitech s.p.a. (Italy) - Short name: YOGITECH
- ABB (Norway) - Short name: ABB
- Università politecnica della Catalunya (Spain) – Short name: UPC

CONFIDENTIALITY NOTE

THIS DOCUMENT MAY NOT BE COPIED, REPRODUCED, OR MODIFIED IN WHOLE OR IN PART FOR ANY PURPOSE WITHOUT WRITTEN PERMISSION FROM THE CLERECO CONSORTIUM. IN ADDITION TO SUCH WRITTEN PERMISSION TO COPY, REPRODUCE, OR MODIFY THIS DOCUMENT IN WHOLE OR PART, AN ACKNOWLEDGMENT OF THE AUTHORS OF THE DOCUMENT AND ALL APPLICABLE PORTIONS OF THE COPYRIGHT NOTICE MUST BE CLEARLY REFERENCED

ALL RIGHTS RESERVED.

[4] ***PU**: public, **PP:** Restricted to other program participants (including the commission services), **RE** Restricted to a group specified by the consortium (including the Commission services), **CO** Confidential, only for members of the consortium (Including the Commission services)*

INDEX

COPYRIGHT **2**

INDEX **3**

1. Introduction **7**

2. Target technologies and Modeling **8**

2.1. Technologies Review **8**

2.2. Modeling **8**

3. Description of Failure mechanisms **9**

3.1. Random Dopant Fluctuations (RDF) **10**

3.2. Line Edge Roughness (LER) **11**

3.3. Random Telegraph Noise (RTN) **12**

3.4. Electromigration (EM) **13**

3.5. Metal Stress Voiding (MSV) **14**

3.6. Gate Oxide Wearout (GOW) **15**

3.7. Hot Carrier Injection (HCI) **16**

3.8. NBTI/PBTI Aging **17**

3.9. Radiation Induced Faults (RIF) **18**

3.10. SOI Self-Heating (SHE) **20**

3.11. Other Sources **21**

3.12. Sources of Failure mapped with technologies **21**

4. Characterization of Different Sources of Failure **22**

4.1. Soft Errors **23**

4.1.1. Methodology to Analyze Soft Error Rates 23

4.1.2. Analysis of SRAM Cells 25

4.1.3. Analysis of Latches 27

4.1.4. Tasks Summary 29

5. Conclusions **30**

6. Additional material on CLERECO SVN Repository **31**

7. Acronyms **32**

8. Bibliography 33

Scope of the document

This document is an outcome of task T2.1, "***Reliability failure mechanisms for future systems***", elaborated in the description of work (DoW) of the CLERECO project under the Work Package 2 (WP2).

Figure 1 depicts graphically the goal of this deliverable, its main results, the inputs it uses and which work packages will use its outputs.

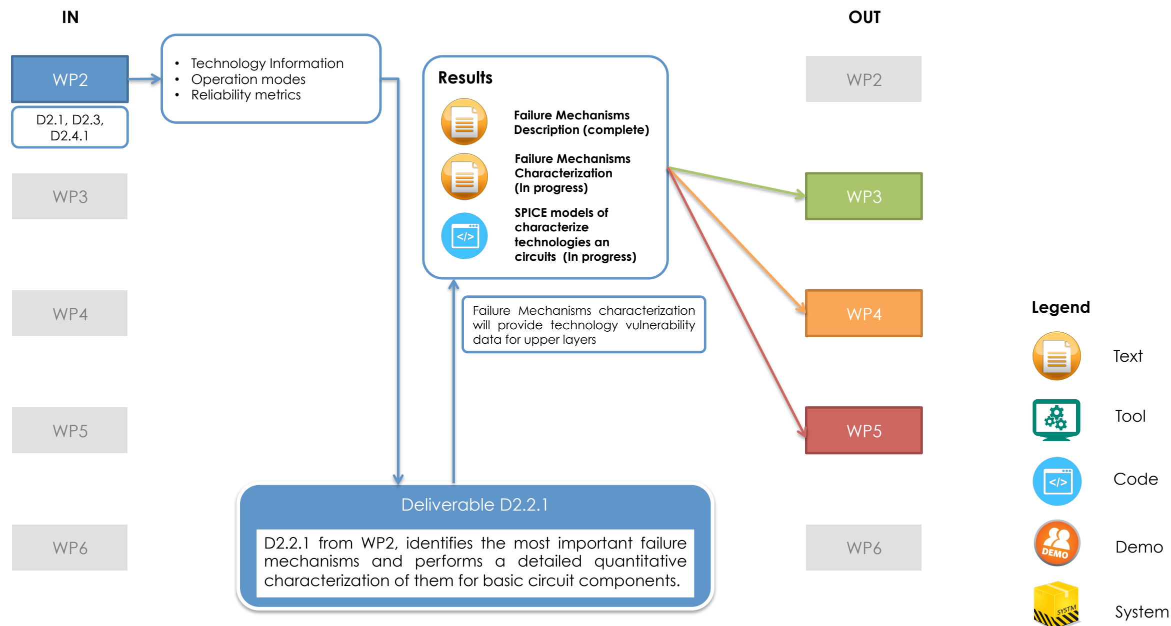

Figure 1: Deliverable summary

D2.2.1 focuses on describing the most important failure mechanisms in current and future technologies, and performs a characterization (preliminary at this stage of the project) of how these failure mechanisms affect the reliability of basic circuit components. The technologies considered in this deliverable are those identified in deliverable D2.1 (Report on future technologies that may be used in future computer systems) and their characterization is performed taking into account the reliability metrics identified in deliverable D2.4.1 (Report on system level reliability metrics v.1). Environmental conditions are also considered as described in deliverable D2.3 (Definition of operation modes for future systems).

This deliverable produces two main outcomes for the CLERECO project. First a detailed list of failure mechanisms that may arise in future technology. These failure mechanisms represent the main source of unreliability of complex system. Second, a characterization of the characteristic of each considered failure mechanism in order to compute vulnerability data to be exploited for the upper layers (e.g., error rates, etc.). The characterization is performed through a set of SPICE models and circuits listed in Table 7, that are provided as additional material to this deliverable.

The outputs of this deliverable will be strongly exploited within WP3, WP4 and WP5 activities.

It has to be pointed out that CLERECO project does not deal with software bugs/errors but only with the effect of hardware faults and their propagation to software layers.

The document is organized in the following sections:

- **Introduction**. This section sets the background for the document. The objectives of the document and the investigations made for its development are included.

- **Target Technologies and Modeling.** This section makes a review of the most promising future technologies and how they are modeled.
- **Description of Failure Mechanisms.** This section describes the most important failure mechanisms divided in a subchapter per source of failure, and maps the sources of failure with the technologies affected.
- **Characterization of different sources of failure.** This section explains how the different sources of failure can be characterized to obtain the vulnerability factor at technology level, focusing, at this moment, on soft errors.
- **Conclusions.** This section summarizes the document and takes some conclusions on how this part of the project is going on.
- **Acronyms and Definitions.** A section containing a list of the most important acronyms used in the document and their definitions.
- **Bibliography.** A section containing a list of the references used to make this part of the project and this document.

1. Introduction

System reliability has become an important design aspect for computer systems due to the aggressive technology miniaturization, which introduces a large set of different sources of failure for hardware components [1][2][3][4][5][6][7]. Errors are strongly related to the technology used to build the hardware blocks composing the system and are caused by effects such as physical fabrication defects, aging or degradation (e.g., NBTI), environmental stress (e.g., radiations), etc.

After a raw fault manifests in a given hardware block, it can be propagated through the different hardware structures composing the full system and reach the software layer by corrupting either data or instructions composing a software application.

The reliability stack depicted in Figure 1.1 summarizes the basic idea of system reliability evaluation of CLERECO. Every system is split into three main layers: (1) technology, (2) hardware and (3) software. CLERECO's goal is to contribute with a full system reliability estimation methodology, which takes into consideration all these factors to provide an accurate estimate of the expected reliability of the system as early as possible during design.

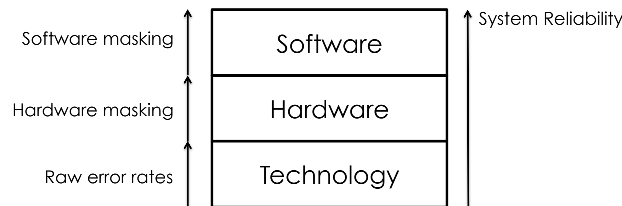

Figure 1.1: CLERECO reliability stack

Each layer included in Figure 1.1 defines an interface with the upper layer, which in turns sets how the errors can be propagated from one layer to the next one. In this deliverable we focus on errors that can cross the interface between the technology and the hardware layer. The main relevant elements required to analyze the impact of technology on the reliability of a system are shown in Figure 1.2.

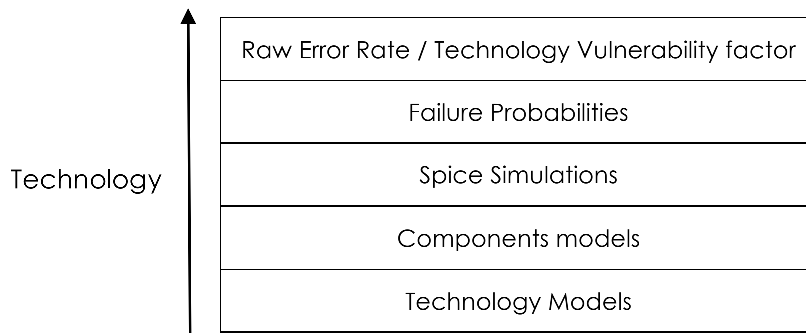

Figure 1.2: The technology layer

In this document, the most important failure mechanisms are described and in this preliminary version we will focus on the characterization of soft errors. The first step is to find predictive models for future technologies and develop models for the components that need to be analyzed. Next step is to perform Spice simulations to test the reliability of these components in the new technologies in order to compute failure probabilities and derive the Technology Vulnerability Factor (TVF) that will be required for the next layers of the stack.

2. Target technologies and Modeling

There are several technologies that are strong candidates to be used in a near future. In this chapter, the most promising technologies are briefly reviewed, and then we discuss how these new technologies are modeled and tested for this project. A detailed list of these technologies is provided in deliverable D2.1.

2.1. Technologies Review

Planar CMOS technology is still being used and will stay here for a long time. Planar CMOS has been scaled down during many generations but physical limitations and reliability problems are starting to be a serious challenge for newer technology nodes. As planar CMOS have their limitations, other technologies such as multi gate FinFET transistors are gaining interest and are analyzed in this project. FinFETs [9] have the conduction channel wrapped by a thin silicon "fin" which forms the body. The thickness of the fin is the major challenge for FinFETs fabrication as it determines the effective length of the channel. Another technology being used nowadays is silicon on insulator (SOI), which refers to the use of layered silicon-insulator-silicon substrate instead of the conventional silicon substrate to reduce parasitic capacitance and improve performance. Finally, newer technologies that are still being investigated such as III-V HEMT will be considered in this project.

2.2. Modeling

Transistors are modeled using compact models with predicted parameters [13][14]. In the area of predictive modeling, the Berkeley Predictive Technology Model (BPTM) [10] and the Arizona State University (ASU) [11] PTM were developed for Planar CMOS technology nodes up to 7nm based on the BSIM models, which are commonly used. BPTM was developed by empirically extracting model parameters from early stage silicon data while ASU PTM improved the methodology by taking into account significant physical correlations among model parameters. Both groups also developed PTM models for multi-gate transistors, mainly FinFETs, for sub-20nm technology nodes.

All the predicted models are developed based on the scaling theory of planar CMOS and multi-gate devices, physical models and the International Technology Roadmap for Semiconductors (ITRS) [12] projections, which recollects data of the industry and makes projections about the future technologies.

In Table 2.1, there is a list of the circuit components, technologies and technology nodes that are planned to be analyzed in this project at transistor level. The technologies marked in bold are available to be analyzed by today as we have compact models available, and efforts are being made to find models for the rest of technologies.

Circuits	Technology	Technology Nodes
SRAM Cells 6T/8T/10T	**Bulk Planar CMOS**	16nm (Planar CMOS)
DRAM Cell 1T	**MultiGate FinFET**	22nm (Planar CMOS)
Flip Flop - D	Silicon On Insulator (SOI)	14nm (FinFET)
Latch	Flash	20nm (FinFET)
Ring Oscillator	III-V HEMT	7nm and 10nm (FinFET)

Table 2.1: Circuits, Technologies and Nodes to be analyzed

3. Description of Failure mechanisms

The first step of this project is to select the failure mechanisms that will be analyzed. In order to do that, we have made a study from the literature looking for the failure mechanisms that may have a highest impact on the vulnerability of current and future technologies. The results are described in this section.

Faults, errors and failures [16] are terms that are often confused but have different meanings. A fault is a defect that may trigger an error or stay dormant. Faults in hardware structures could arise from defects, imperfections, or interactions with the external environment. Examples of faults include manufacturing defects in silicon chip or bit flips caused by cosmic ray strikes.

Faults are usually classified into three categories: permanent, intermittent and transient. Permanent faults remain for indefinite periods till corrective action is taken. Oxide wearout leading to a transistor malfunction is an example. Intermittent faults appear, disappear, and then reappear and are often early indicators of permanent faults. Finally, transient faults are those that appear and disappear in a very short period of time (typically one cycle). Bit flips or gate malfunctions due to an alpha particle or a neutron strike are examples of transient faults. A fault in a particular system layer may not show up at the user level. This may be because the fault is being masked in an intermediate layer, a defective transistor may affect performance but not the correct operation, or because any of the layers may be designed to tolerate some faults.

Errors are manifestation of faults. Faults could cause an error, but not all faults show up as errors, as they may be masked or tolerated. Errors can be classified in the same way as faults, so a permanent fault may cause a permanent error and so on. The final term, failure, is defined as a system malfunction that causes the system not to meet its correctness, performance, or other guarantees. Figure 3.1 summarizes this terms in the way of when they can arise. As an example, Figure 3.2 shows the different types of SRAM failures, which can arise from manufacturing defects, process variations and alpha particles or neutron strikes.

Figure 3.1: Summary of fault, error and failure terms

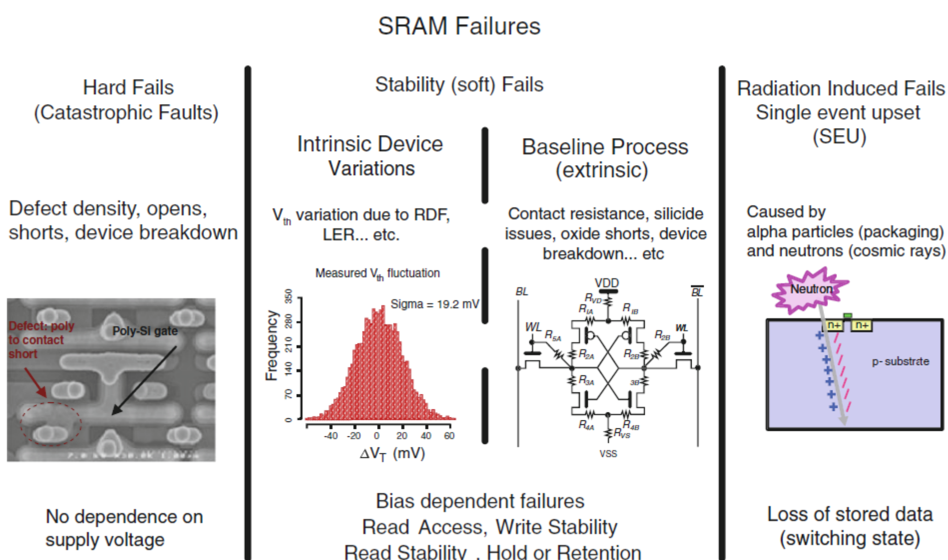

Figure 3.2: Different types of SRAM failures

3.1. Random Dopant Fluctuations (RDF)

Random Dopant Fluctuations (RDF) [15][8] is a type of process variation that may cause a failure, and are primarily caused due to the random fluctuation in the number of dopant atoms in the channel gate and their placement. The effect is more pronounced as devices are scaled down, as the total number of dopant atoms in the depletion region decreases with subsequent technology nodes. This fluctuation in the number of dopants in the transistor channel results in variations in the threshold voltage (V_{th}) for the device.

The problem of RDF has been well documented over the last three decades and has been predicted to be a major challenge for controlling device performance. Due to the random nature of this phenomenon, the threshold voltage (V_{th}) of the transistor undergoes significant variation. This is because the intrinsic value of V_{th} is dependent on the charge of the ionized dopants in the depletion region. The standard deviation of V_{th} follows the inverse square law of the device area. In other words, with scaling of technology, σV_{th} dependent on RDF increases for transistors with smaller area. The variation in V_{th} due to RDF has been demonstrated to follow a Gaussian distribution with its standard deviation derived as:

$$\sigma_{V_{th}} = \left(\sqrt[4]{2q^3 \varepsilon_{Si} N_a \phi B}\right) x \frac{T_{ox}}{\varepsilon_{ox}} x \frac{1}{\sqrt{3WL}}$$

where q represents electron charge, ε_{Si} and ε_{ox} are permittivity of silicon and gate oxide, N_a is the channel dopant concentration, ϕB is the difference between Fermi level and intrinsic level, T_{ox} is the gate oxide thickness, W and L are the channel width and length of the transistor, respectively.

The trend to reduce the total number of dopant atoms when reducing device dimensions is shown in Figure 3.3. It is evident that reducing the total number of dopant atoms in subsequent process nodes makes σV_{th} increase significantly. Even two equal transistors with the same number of dopants can have different voltage thresholds due to their position in the channel. As RDF is inversely proportional to the device area, SRAM cells, which are usually constructed with the minimum geometry transistors available, are intrinsically the most susceptible to this type of variation.

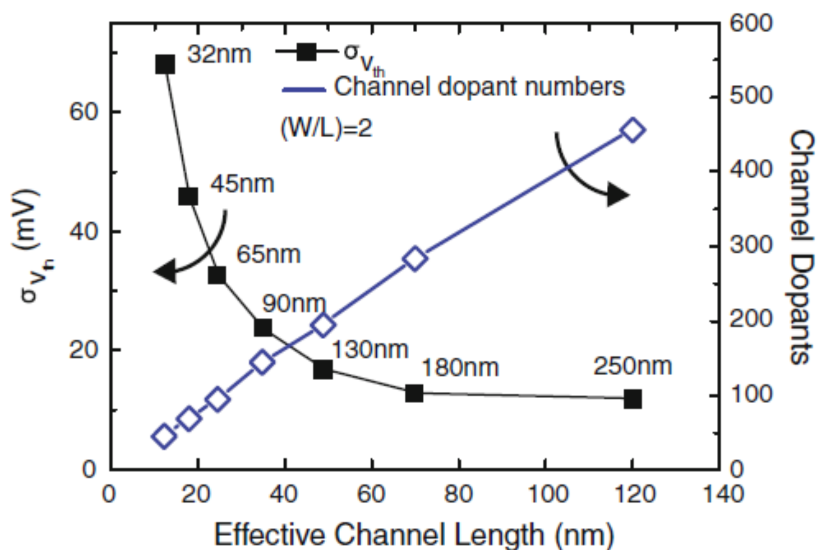

Figure 3.3: Impact of RDF on Vth variation and number of dopants of a MOSFET

3.2. Line Edge Roughness (LER)

Line-edge roughness (LER) [15][8] is caused by the change in the shape of the gate along the channel width direction as can be seen in Figure 3.4. This roughness in the edge of the gate is caused by the inherent characteristics of the materials forming the gate and additional process steps such as etching and imperfection in lithography.

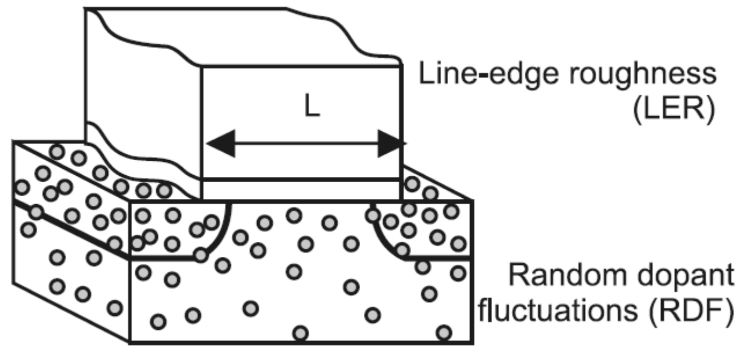

Figure 3.4: Primary sources of variation: RDF and LER

The impact of this phenomenon is more pronounced at technologies below 50nm, as process technologies use light sources with wavelengths much higher than the minimum feature size, increasing gate variation due to LER. LER impacts directly on Vth variation following a Gaussian distribution, and is inversely proportional to the gate width of the transistor. The impact of LER when changing the device dimension from W1 to W2 on σV_{th} is given by the following equation:

$$\sigma_{V_{th}\,|\,W_2} = \sqrt{W_1/W_2}\,\sigma_{V_{th}\,|\,W_1}$$

Figure 3.5 shows the impact of LER on Vth fluctuation while scaling transistor widths. As explained in [8], the variance of this phenomenon does not decrease with technology scaling despite improvements in the underlying manufacturing technology. As a result, the problem can become critical for devices such as memory cells that are extremely susceptible to Vth mismatch.

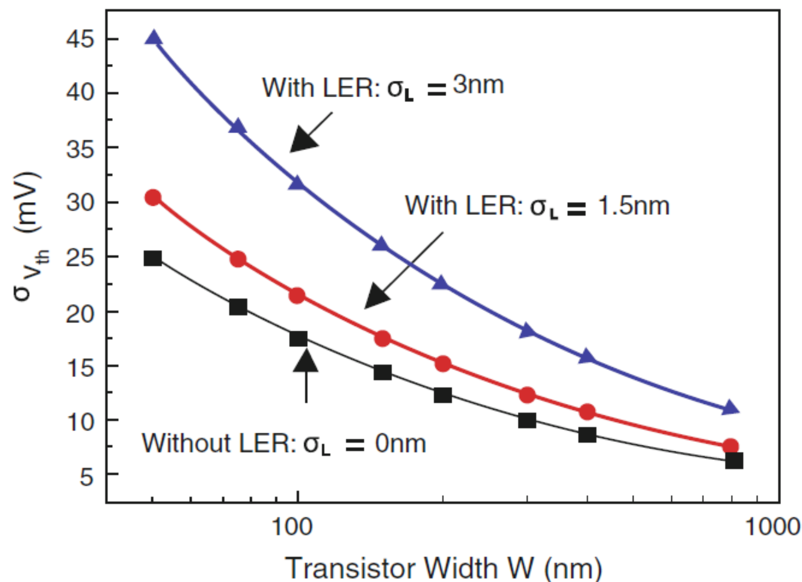

Figure 3.5: Combined effect of LER and RDF on Vth variation

3.3. Random Telegraph Noise (RTN)

Random Telegraph Noise (RTN) [8], also known as random telegraph signal (RTS), is a random fluctuation in the device drain current due to the trapping and detrapping of channel carriers in the dielectric traps at the oxide interface, as shown in Figure 3.6, which causes variation in Vth. The fluctuation in drain current is caused by the change in the number of carriers as well as the changes in surface mobility due to scattering by the trapped charges in the gate dielectric.

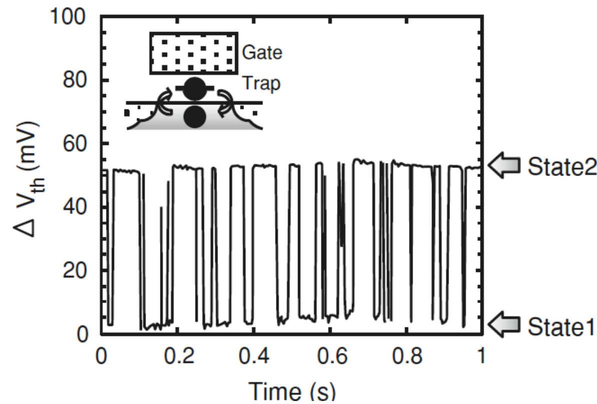

Figure 3.6: RTN Vth variation is caused by trapping and detrapping of charges in the channel

Both RTN and RDF arise due to discreteness in charges, however, RTN differs from RDF in that is time dependent, and fewer charges are involved. Technology scaling increases RTN due to reduction in the number of channel carriers caused. The impact of RTN on V_{th} variations can be estimated as follows:

$$\Delta V_{th,RTN} = \frac{q}{W_{eff} L_{eff} C_{ox}}$$

where q is the elementary charger, L_{eff} and W_{eff} are the effective channel length and width, respectively, and Cox is the gate capacitance per unit area. The equation shows that V_{th} variation is inversely proportional to device area, and can become a serious concern for highly scaled technologies and a critical problem for SRAM cells. Figure 3.7 shows that V_{th} variation due to RTN has a non-Gaussian distribution with a long tail, which is a critical concern related to RTN, and RTN may exceed RDF in design impact.

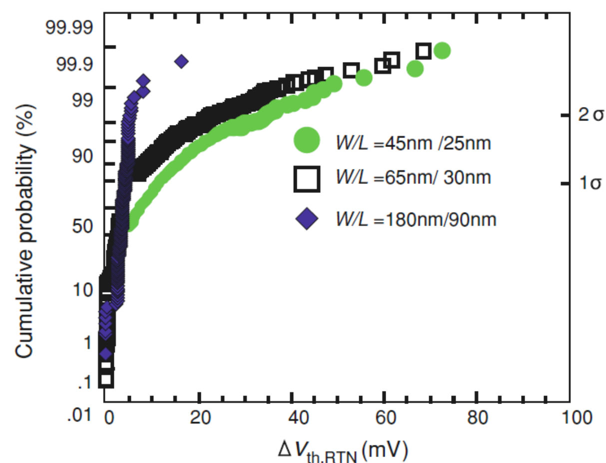

Figure 3.7: Distribution of Vth fluctuation due to RTN in 22nm technology

3.4. Electromigration (EM)

Electromigration (EM) [16] is a failure mechanism that causes voids in metal lines or interconnects in semiconductor devices. Often, these metal atoms from the voided region create an extruding bulge on the metal line itself. EM is caused by electron flow and exacerbated by rise in temperature. As electrons move through metal lines, they collide with the metal atoms. If these collisions transfer sufficient momentum to the metal atoms, these atoms may get displaced in the direction of the electron flow. The depleted region becomes the void, and the region accumulating these atoms forms the extrusion. Figure 3.8 shows the Electromigration effect and Figure 3.9 shows a real example of voids caused by these phenomena.

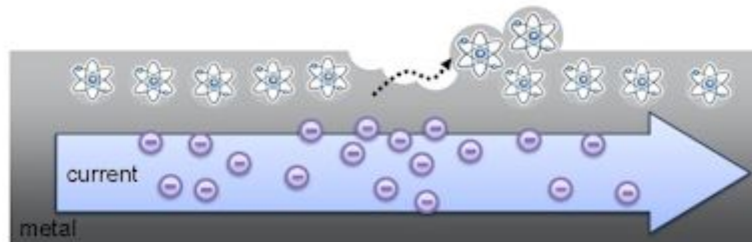

Figure 3.8: Electromigration

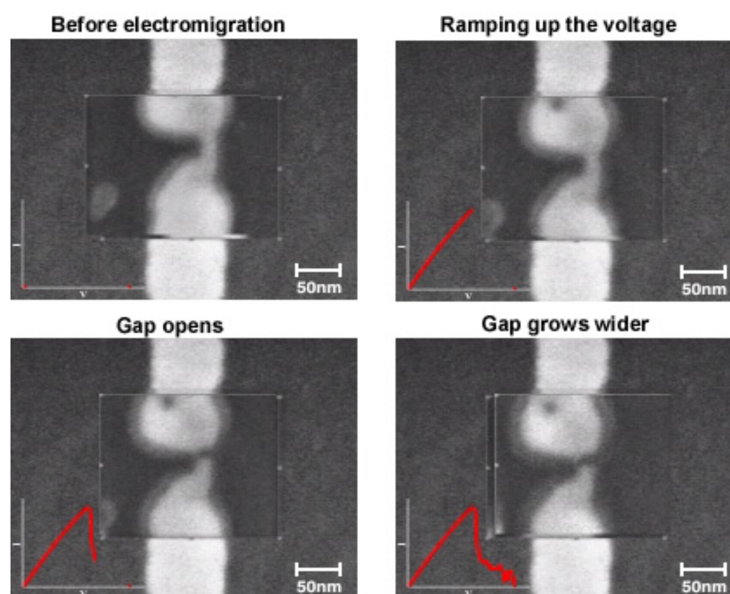

Figure 3.9: Example of a Void due EM [17]

Black's law is commonly used to predict the Median Time to Failure (MeTTF) of a group of aluminum interconnects. This law was derived empirically and applies to a group of metal interconnects, so cannot be used to predict the TTF of an individual wire. The equation is as follows:

$$MeTTF_{EM} = \frac{A_0}{j_e^2} e^{\frac{E_a}{kT}}$$

where A_0 is a constant dependent on technology, j_e is electron current density (A/cm^2), T is the temperature (K), E_a is the activation energy (eV) for EM failure and k is the Boltzmann constant.

As technology shrinks, the current density usually increases, so designers need effort to keep the current density at acceptable levels to prevent EM. Nevertheless, the exponential temperature term has a more serious effect on MeTTF than current density.

3.5. Metal Stress Voiding (MSV)

Metal stress voiding (MSV) [16], also known as Stress Migration, causes voids in metal lines due to different thermal expansion rates of metal lines and the passivation material they bond to. This can happen during the fabrication process itself, when deposited metal reaches very high temperatures (400 ^{0}C or more) for a passivation step, and the metal lines expand and tightly bond to the passivation material. However, when cooled to room temperature, enormous tensile stress appears in the material due to the differences in the thermal coefficient of expansion of the two materials. If the stress is large enough, then it can pull a line apart and the void can show up immediately or years later. Figure 3.10 shows an example of a void caused by stress migration.

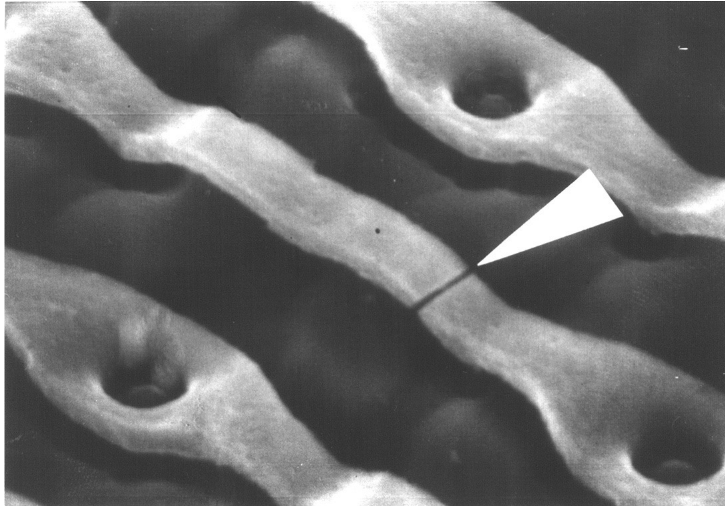

Figure 3.10: Example of a void due to Stress Migration

The Mean Time to Failure (MTTF) due to MSV is given by the following equation:

$$MTTF_{MSV} = \frac{B_0}{(T_0 - T)^n} e^{\frac{E_b}{kT}}$$

where T is the temperature, T_0 is the temperature at which the metal was deposited, B_0, n, and E_b are material dependent constants, and k is the Boltzmann constant. For copper, n = 2.5 and E_b = 0.9. The higher the operating temperature, the lower the term $(T_0 - T)$ is and the higher the MTTF is. However, the exponential term drops rapidly with a rise in the operating temperature and usually has the more dominant effect.

In general, copper is more resistive to EM and MSV than aluminum and for this reason has replaced aluminum for metal lines in the semiconductor industry. However, copper can cause severe contamination in the fab and therefore needs a more controlled process.

3.6. Gate Oxide Wearout (GOW)

Gate oxide reliability has become an increasing concern in the design of high performance silicon chips. Gate oxide consists of thin noncrystalline and amorphous silicon dioxide (SiO_2). In a bulk CMOS transistor the gate oxide electrically isolates the polysilicon gate from the substrate or bulk of the transistor as can be seen in Figure 3.11. The switching speed of a CMOS transistor is a function of the gate oxide thickness. As technology shrinks, the supply voltage is reduce to maintain the overall power consumption, but this reduces the switching speed. To increase the switching speed, the gate oxide thickness is reduced and rapidly approaches molecular dimensions. Oxides with such a low thickness are referred to as ultrathin oxides and introduce some failure mechanisms.

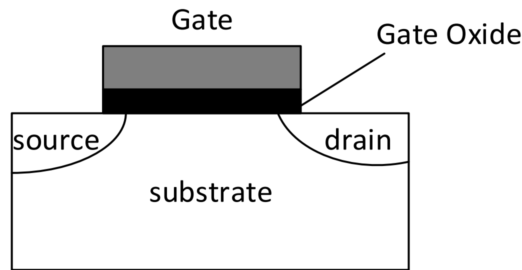

Figure 3.11: Structure of a bulk CMOS transistor

Ultrathin oxide breakdown [16] causes a sudden discontinuous increase in conductance often accompanied by an increased current noise, causing a reduction in the current of the transistor. Gradual oxide breakdown may initially lead to intermittent faults but may eventually cause a permanent fault in the device.

The breakdown is caused by gradual buildup of electron traps, which are oxide defects produced by missing oxygen atoms. The breakdown occurs when a statistical distribution of these traps is vertically aligned and allows a thermally damaging current to flow through the oxide. This is known as the *percolation* model of wearout and breakdown and the time to breakdown for a gate oxide can be expressed with the following equation:

$$T_{bd} = Ce^{\gamma(\alpha t_{ox} + \frac{E_a}{kT_j} - V_G)}$$

where C is a constant, t_{ox} is the gate oxide thickness, Tj is the average junction temperature, Ea is the activation energy, VG is the gate voltage, and γ and α are technology dependent constants. Therefore, the time to breakdown decreases with decreasing oxide thickness but increases with decreasing V_G. This model is still an area of active research.

3.7. Hot Carrier Injection (HCI)

Hot Carrier Injection (HCI) [16] arises from impact ionization when electrons in the channel strike the silicon atoms around the drain-substrate interface. This could happen from one of several conditions, including a higher power supply or short channel lengths, among others. HCI results in a reduction of the maximum operating frequency of the chip.

The ionization produces electron-hole pairs in the drain as can be seen in Figure 3.12. Some of these carriers enter the substrate increasing the substrate current. A small fraction of these carriers may have sufficient energy to cross the oxide barrier and enter the oxide causing damage. Because these carriers have a high mean equivalent temperature, they are referred to as hot carriers. However, HCI becomes worse as ambient temperature decreases due to the corresponding increase in carrier mobility.

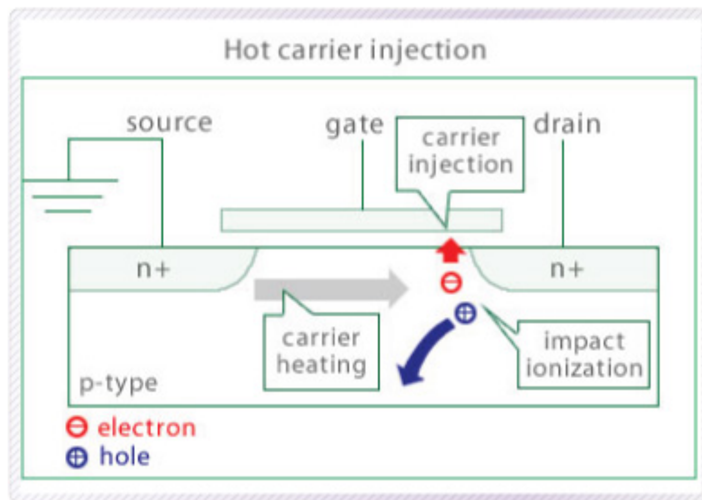

Figure 3.12: HCI Effect

The drain saturation current (I_{Dsat}) degradation is used to measure HCI degradation as is one of the key transistor parameters that most closely approximates the impact on circuit speed and because HCI damage occurs only when the transistor is in saturation.

Frequency guardbanding is a typical measure to cope with HCI related degradation. The expected lifetime of a chip is often between 5 and 15 years, and the frequency degradation during the expected lifetime is between 1% and 10%. Hence, the chips are rated to run at a few percentage points below what they actually run at, calling this reduction as frequency guardband.

Transistor lifetime degradation (τ) due to HCI can be specified with the following equation:

$$\tau = Constant \frac{\frac{W}{I_D}}{(\frac{I_{sub}}{I_D})^{3'}}$$

where W is the transistor width, I_D is the drain current, and I_{sub} is the substrate current. The I_D and I_{sub} parameters are estimated for the use condition of the chip.

3.8. NBTI/PBTI Aging

Negative Bias Temperature Instability (NBTI) [16], like HCI, causes degradation of the maximum frequency of the chip. However, while HCI can affect both nMOS and pMOS transistors, NBTI only affects short channel pMOS transistors. Under stress, like high temperatures, highly energetic holes bombard the channel-oxide interface, electrochemically react with the oxide interface, and release hydrogen atoms by breaking the silicon-hydrogen bonds. These free hydrogen atoms combine with oxygen or nitrogen atoms to create positively charged traps at the oxide-channel interface.

NBTI causes a reduction in mobility of holes and a shift in the pMOS threshold voltage towards the more negative direction. These effects cause the transistor drive current to degrade, slowing down the transistor device. The term "instability" refers to the variation of threshold voltage with time. There is active research to look for models that can predict how NBTI will manifest in future process generations.

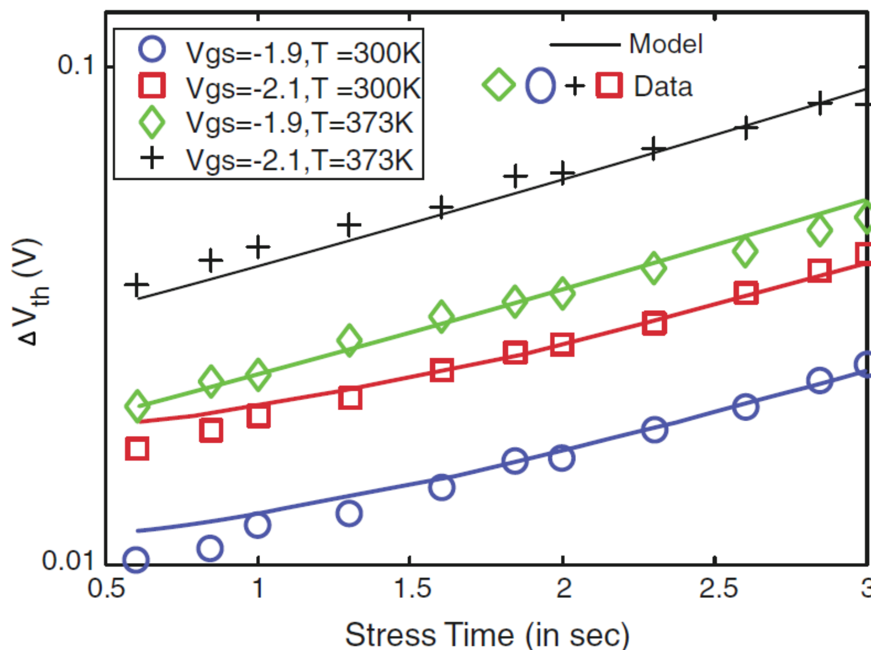

Figure 3.13: Vth degradation under static NBTI for different temperatures and Vgs for 90nm technology

Figure 3.13 shows V_{th} degradation under static NBTI for 90nm technology at different temperature and voltage conditions. NBTI shift recovers slightly after the stress condition is removed. There are some models for V_{th} shift that take account of recovery and dynamic stress.

For newer technologies using high-K dielectrics, nMOS devices suffer from a similar reliability problem due to Positive Bias Temperature Instability (PBTI).

3.9. Radiation Induced Faults (RIF)

Radiation induced transient faults [16][19] can be produced due to different types of sources: alpha particles from packaging and neutrons from the atmosphere. Most of the faults described in this chapter can be taken care before a chip is shipped. In contrast, radiation faults are addressed with fault detection and error correction circuitry.

An alpha particle consists of two protons and two neutrons bound together into a particle. Alpha particles are emitted by radioactive nuclei, such as uranium or radium, in a process known as alpha decay. Alpha particles have kinetic energies of a few MeV, which is lower than those of neutrons that affect CMOS chips. Nevertheless, alpha particles can affect semiconductor devices because they deposit dense track of charge and create electron-hole pairs as they pass through the substrate. Alpha particles can arise from radioactive impurities used in chip packaging such in the solder balls or contamination of semiconductor processing materials. Alpha particles are difficult to eliminate completely from the chip so chips need fault detection and error correction techniques.

The neutron is one of the subatomic particles that make up an atom. Atoms are considered the basic building blocks of matter and consists of three types of subatomic particles: protons, neutrons and electrons. A proton is positively charged, a neutron is neutral and an electron is negatively charged. An atom consists of an equal number of protons and electrons and hence it is neutral itself. The neutrons that cause soft errors arise when atoms break apart into protons, electrons and neutrons. Protons have a long half-life so can persist for long durations before decaying and constitute the majority of the primary cosmic rays that bombarded the earth's outer atmosphere. When these protons and associated particles hit atmospheric atoms, they create a shower of secondary particles named secondary cosmic rays. Untimely, the particles that hit the earth's surface are known as terrestrial cosmic rays.

Alpha particles and neutrons slightly differ in their interactions with silicon crystals. Charged alpha particles interact directly with electrons. In contrast, neutrons interact with silicon via inelastic or elastic collisions. Inelastic collisions cause the incoming neutrons to lose their identity and create secondary particles, whereas elastic collisions preserve the identity. Inelastic collisions cause the majority of the soft errors due to neutrons.

When an alpha particle penetrates a silicon crystal, it causes strong field perturbations, creating electron hole-pairs in the substrate of a transistor. The electric field near the p-n junction, the interface between the bulk and diffusion, can be high enough to prevent the electron-hole pairs from recombining. Then, the excess carriers could be swept into the diffusion regions and eventually to the device contacts, registering an incorrect signal.

One key concept to explain the interaction of alpha particles with silicon is the stopping power. Stopping power is defined as the energy lost per unit track length, which measures the energy exchanged between an incoming particle and electrons in a medium. Stopping power quantifies the energy released from an interaction between alpha particles and silicon crystals, which in turn can generate electron-hole pairs. About 3.6 eV of energy is required to create one such pair. Whether the generated charge can actually cause a malfunction or a bit flip depend on two factors named charge collection efficiency and critical charge of the circuit that will be explained later.

Neutrons do not directly cause a transient fault because they do not directly create electron hole-hole pairs in silicon crystals (their stopping power is zero). Instead, these particles collide with the nuclei in the semiconductor resulting in the emission of secondary nuclear fragments. These fragments could consist of particles such as pions, protons, neutrons, deuteron, tritons, alpha particles and others. These secondary fragments can cause ionization tracks that can produce a sufficient number of electron-hole pairs to cause transient faults in the device. The probability of a collision that produces these secondary fragments is very small so a greater

number of neutrons is necessary than alpha particles to produce the same number of transient faults.

Stopping power explains why and how many electron-hole pairs may be generated by an alpha or a neutron strike, but it does not explain if the circuit will malfunction. The charge accumulation needs to cross a certain threshold before an SRAM cell, for example, will flip the charge stored in the cell. This minimum charge necessary to cause a circuit malfunction is termed as the critical charge of the circuit represented as Qcrit. Typically, Qcrit is estimated in circuit models by injecting different current pulses till the circuit malfunctions.

Hazucha and Svensson [18] proposed the following model to predict neutron induced Soft Error Rate (SER):

$$Circuit\ SER = Constant\ x\ Flux\ x\ Area\ x\ e^{-\frac{Qcrit}{Qcoll}}$$

Constant is a constant parameter dependent on the process technology and circuit design style, Flux is the flux of neutrons at the specific location, Area is the area of the circuit sensitive to soft errors, and Qcoll is the charge collection efficiency, which is the ratio of collected and generated charge per unit volume. Qcoll depends strongly on doping and Vcc and is directly related to the stopping power, so the greater is the stopping power, the greater is Qcoll. Qcoll can be derived empirically using either accelerated neutron tests or device physics models, whereas Qcrit is derived using circuit simulators. This equation can also be used to predict the SER of alpha particles. Figure 3.14 shows a diagram illustrating the effects of soft errors.

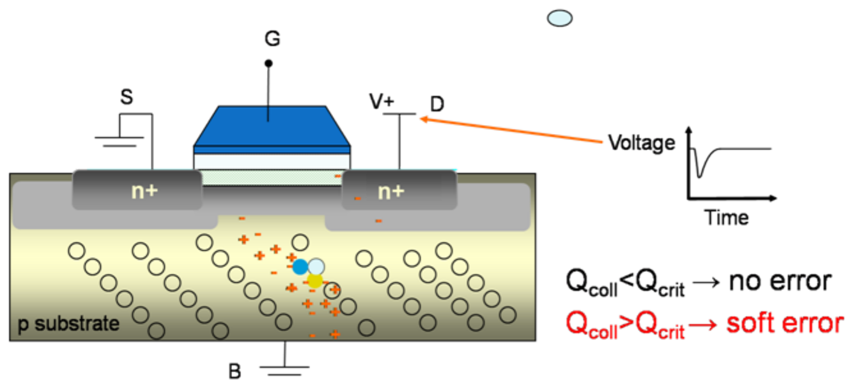

Figure 3.14: Diagram of soft errors effects

With every process generation, the area of the same circuit goes down, so this should reduce the effective SER from one process generation to the next. However, Qcrit also decreases because the voltage of the circuit goes down across process generations. Therefore, for some elements like latches and logic, this effect appears to cancel each other out, resulting in a constant SER across generations. However, if Qcrit is sufficiently low, such in SRAM devices, then the impact of the area begins to dominate. This is referred as saturation effect, where the SER decreases with process generations. However, the circuit is highly vulnerable to soft errors in the saturation region. In the extreme case, as Qcrit approaches to zero, almost any amount of charge produced by alpha or neutron strikes will result in a transient fault.

When a charge produced by an alpha particle or neutron strike is sufficient to overwhelm a circuit, then it may malfunction. At the gate or cell level, this malfunction appears as a bit flip. For storage devices, when a bit residing in a storage cell flips, a transient fault is said to have occurred. For logic devices, a change in the value of the input node feeding a gate or output node coming out of a gate does not necessarily mean a transient fault has occurred. Only when this fault propagates to a forward latch or storage cell does one say a transient fault has occurred.

3.10. SOI Self-Heating (SHE)

Silicon on insulator (SOI) [20] technology possesses some advantages over bulk silicon technology such as the reduction of parasitic capacitance, excellent, sub-threshold slope, elimination of latch up and resistance to radiation. Hence, it is preferred for high speed, high temperature and low power devices by some manufacturers.

SOI MOS devices employ a buried insulating thin layer usually made of silicon dioxide to electrically isolate the devices from the bulk of the semiconductor. Due to the poor conductance of SiO2, the buried dielectric layer also thermally insulates the MOSFETs from the bulk. Consequently, the heat generated in the SOI MOSFETs causes a larger temperature rise than in bulk devices under similar conditions, and the self-heating effect that results in reduced carrier mobility and corresponding decrease in the drain current transconductance and speed becomes an inherent issue for MOSFETs built in SOI. As the device geometries diminish and transconductance as well as current density increase with MOS scaling, the self-heating effect becomes more pronounced. There are some theoretical models to evaluate the effect of self-heating in SOI which are used by some simulators. Figure 3.15 and Figure 3.16 shows the effect of SOI self-heating with the ATLAS simulator.

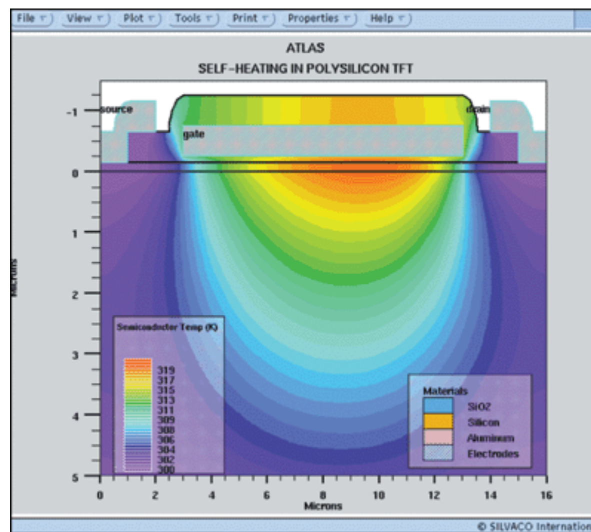

Figure 3.15: Self-heating in SOI transistors [21]

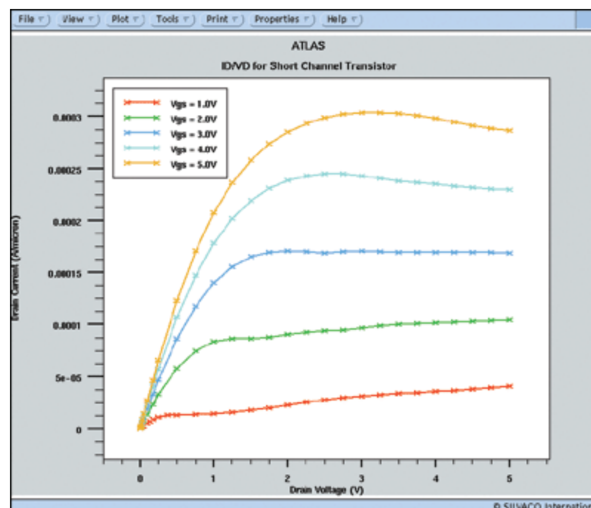

Figure 3.16: Effect of Self-heating on output characteristics [21]

3.11. Other Sources

RDF and LER are currently dominant sources of process variations but there are several other sources, which may become important for future technologies. Below there is a list of other sources of variations:

- **Oxide Charges Variation**: Interface charges can also cause V_{th} variations that may be significant with the recent adoption of high-K gates.
- **Mobility Fluctuation**: Variations in a transistor's drive current can be caused by mobility fluctuations. Mobility fluctuations can arise from several complex mechanisms such as fixed oxide charges, doping or inversion layer, among others.
- **Gate Oxide Thickness Variation**: Any variation in oxide thickness affects many electrical parameters, especially V_{th}.
- **Channel Width Variation**: Due to lithography limitations, transistor channel width also varies similarly to LER variations. Width variations can cause V_{th} variations, but as W is 2-4 times larger than L, its impact on V_{th} is smaller than the impact due to L variation.

3.12. Sources of Failure mapped with technologies

The described sources of failures can affect different technologies in different ways. For example, RDF and LER are critical for CMOS SRAM cells while FinFETs are more resistant to RDF but adds fin thickness variations [22], even some of them may only affect specific technologies. In Table 3.1, there is a summary of the sources of failure described, with their type, and the technologies that may be most affected by these failures.

Sources	Fault Type	Technology
Random Dopant Fluctuations (RDF)	Permanent	All
Line Edge Roughness (LER)	Permanent	All
Random Telegraph Noise (RTN)	Intermittent	All
Metal Stress Voiding (MSV)	Permanent	All
Electromigration (EM)	Permanent	All
Hot Carrier Injection (HCI)	Intermittent/Permanent	All
Gate Oxide Wearout (GOW)	Intermittent/Permanent	All
NBTI/PBTI Aging	Intermittent/Permanent	All
Radiation Induced Faults (RIF)	Transient	All
Self-Heating (SHE)	Intermittent/Permanent	SOI

Table 3.1: Sources of failure mapped with technologies

4. Characterization of Different Sources of Failure

In this chapter, we present the characterization of the previously described sources of failure. This characterization includes preliminary data that will be used within the project. Before that, some general considerations are made below.

The circuit components being tested in this project have been previously listed in Table 2.1of chapter 2. These components have been modeled and analyzed with SPICE. For this purpose, we developed a description of the necessary circuits at transistor level and use a predictive technology model (PTM) of the technology node be analyzed.

Depending on the circuit, some transistors may need to be resized for correct operation or better performance. In the case of Planar CMOS, the resizing means to specify the length and the width of the transistor in lambdas or nanometers. Examples of most circuits for 32nm or higher technology nodes can be found in the literature. These examples have been used as starting point and then linearly scaled down at the technology nodes that we want to analyze. In a similar way, the transistors for FinFETs have been resized in terms of number of fins from a starting point taken from the literature.

Environmental factors can also impact the characteristics or behavior of a source of failure. Table 4.1 shows different environmental factors and describes how these factors impact on the different types of errors. In this project, these environmental factors will not be taken into account in a first step and for simulation purposes the default temperature (25 ^{0}C) of SPICE will be used.

Factors	Impact on transient errors	Impact on Intermittent errors	Impact on Permanent errors
Temperature	Increase in transient failures with higher temperatures due to higher energetic particles and increased leakage	Increase in intermittent failures due to device degradation (e.g. NBTI effects) and thermal stress	Increase in permanent failures due to device degradation effects (e.g. Electromigration effects) and thermal stress(e.g. wear out effects)
Humidity / Dust / Acid / Salt	N/A	N/A	Increase in permanent failures due to corrosion/shorting on contacts
Vibration / Shock / Pressure / Gravity / Explosion	N/A	May cause intermittent failures depending on the strength of the effect	Increase in permanent failures due to mechanical stress and contact/solder breaks
EMC / EMI / Radiation / Altitude	Increased soft errors due to increased interferences (e.g. IR effects, magnetic storage technologies)	May cause intermittent failures for unshielded components that last throughout the exposure period (e.g. solar EMP)	Oxide failure or metal melt due to ESD; power surges due to HEMP and HPM; device degradation effects (Total Ionizing Dose) and destructive effects (Single-Event Latch-Up)

Table 4.1: Environmental factors and their effects on different types of errors

The rest of this chapter is mainly focused on the characterization of soft errors, since this is the type of errors that have been analyzed so far. We focus first on soft errors as their impact on the reliability of new systems is increasing and are becoming a major concern in the industry. Below we report the studies performed for the circuits and technologies mentioned in chapter 2.

4.1. Soft Errors

As described in chapter 3.9, for an alpha particle or a neutron to cause a soft error, the strike must flip the state of a bit. Whether the bit flip eventually affects the final outcome of a program depends on whether the error propagates without being masked, and whether there is some error detection and correction scheme. Architecturally, the error detection and correction mechanisms create two categories of errors: Silent Data Corruption (SDC) and Detected Unrecoverable Error (DUE) [16].

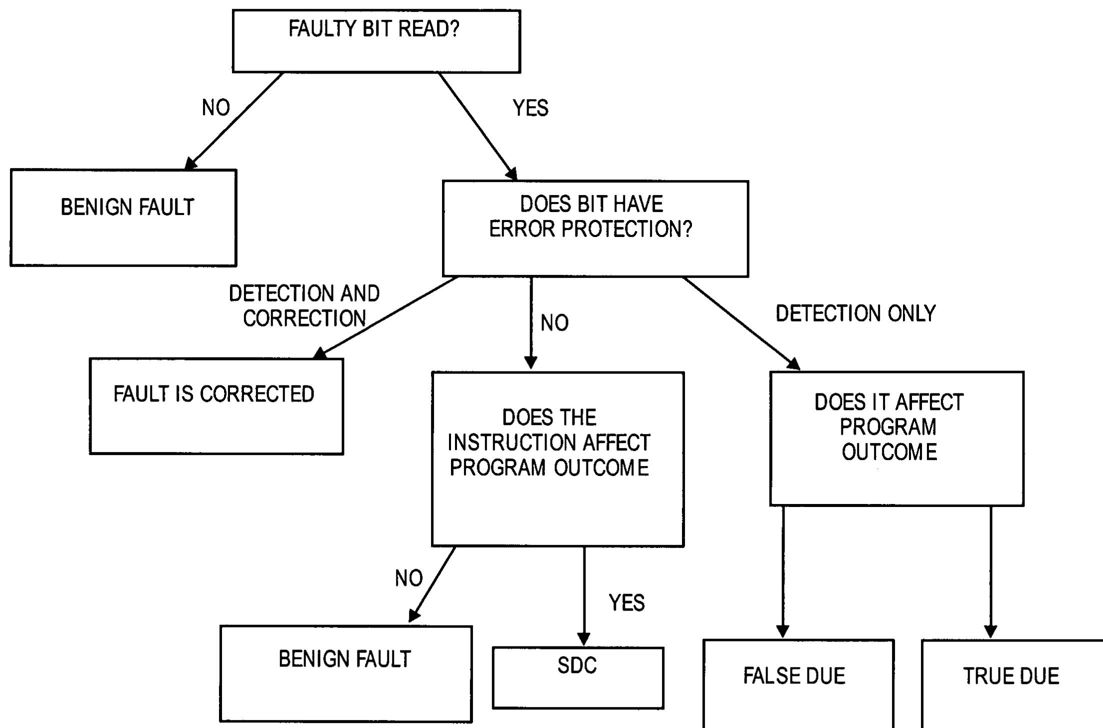

Figure 4.1: SDC and DUE Classification Scheme

Figure 4.1 shows the different outcomes of a bit flip. The most insidious form of error is SDC since a fault induces the system to generate erroneous outputs. SDC rates can be expressed as either FIT or MTTF. To avoid SDC, designers use basic error detection mechanisms, such as parity. The ability to detect a fault but not correct it avoids generating incorrect outputs, but prevents from finalizing the task. Therefore, simple error detection does not reduce the overall error rate but does provide fail-stop behavior and avoids data corruption. Errors in this category are called DUE, and can also be quantified using FIT and MTTF. Industry normally specifies SERs in terms of SDC and DUE numbers. DUE events are further divided according to whether the detected fault would have affected the final outcome of the execution or not, calling them true and false DUE respectively.

The following subsections describe the methodology that we follow to characterize Soft Error Rates (SER), the work that has been done until now, which is basically the computation of Qcrit for SRAM cells and Latches, and the work that still has to be done in the future in this project.

4.1.1. Methodology to Analyze Soft Error Rates

SER will be expressed in FIT rate and can be computed with the following experimental formula:

$$SER_{raw}\ \alpha\ Constant\ x\ Flux\ x\ Area\ x\ e^{-\frac{Qcrit}{Qcoll}}$$

The components of the previous equation have been described in chapter 3.9. The exponential part of the formula is the technology vulnerability factor (TVF). Therefore, the first step is to compute the critical charge (Qcrit) for each component, using HSPICE simulations [23][24]. When a particle strikes a sensitive node of a circuit, it produces a time dependent current pulse that can be modeled with the following equation:

$$I(t) \propto \frac{Q}{T}\ x\ \sqrt{\frac{t}{T}}\ x\ \exp\left(-\frac{t}{T}\right)$$

Where Q is the charge collected from a particle strike and T is a technology dependent parameter. This current pulse can be used in simulators, like HSPICE, to gauge the impact of a particle strike and compute Qcrit.

Reviewing the literature we can find experimental data, such as Figure 4.2 and Figure 4.3, and fitting parametric models that enable performing this calculation and find the probability of some strike to generate a charge greater than the computed Qcrit, obtaining the TVF.

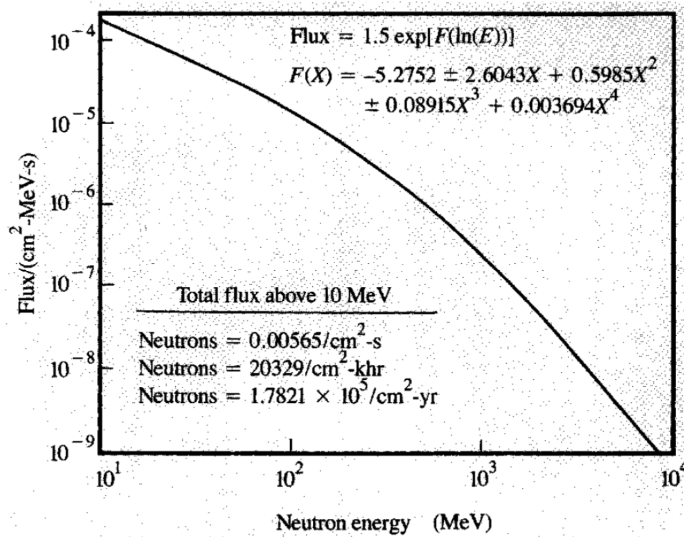

Figure 4.2: Neutron Energy as function of the flux [26]

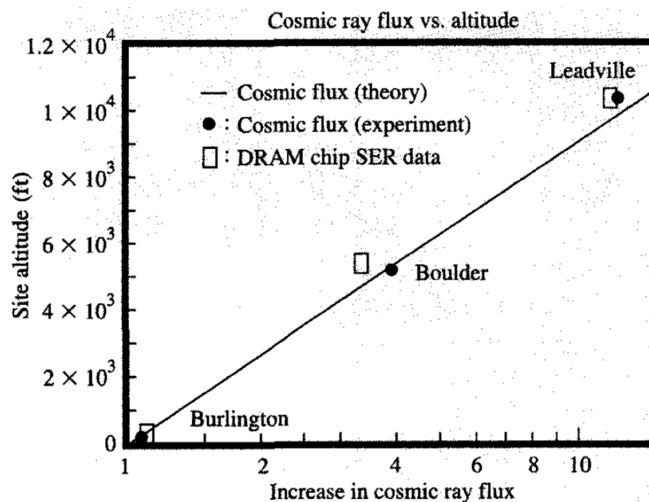

Figure 4.3: Cosmic Ray flux depending on the altitude [27]

Using these data, given an energy range (E_1, E_2), since flux is a cumulative metric we can calculate the raw SER of particles, without masking effects, with energies inside this range as:

$$SER_{raw} = (SER_{raw}(E1) - SER_{raw}(E2))$$

To sum up, this first step is based on state-of-the-art information and provides us a parametric model based on experimental data that allows us to calculate the raw SER per node given specific ranges of particle energies.

In the case of combinatorial logic, the masking effects have to be taken into account. There are two makeable effects that can be analyzed at technology level. The first one is the electrical masking, meaning that the signal may be attenuated before reaching the output. The second effect is the latch-window masking, where the error is propagated only if the value is latched. The final SER for a logic component can be computed adding the SER of all the nodes. However, considering the number of basic components in the cell libraries and possible path combinations, it is practically impossible to have an exhaustive study of all the nodes of each component.

Because CLERECO project aims at providing an early and accurate estimation of the system reliability, we propose generating estimation functions that can predict the circuit vulnerability factor (CVF) numbers with high accuracy given a small subset of circuit characteristics such as number of gates, number of inputs and outputs, logic depth, topology, etc. The experimental study comprises the use of a set of benchmark circuits from ISCA'85 and ISCA'89, and a regression model to extrapolate the information obtained for the rest of combinatorial logic depending on the number of gates, etc., to calculate the CVF. This approach is still in a very early stage and has to be properly studied to validate it.

4.1.2. Analysis of SRAM Cells

SRAM is a type of memory widely used in current CPUs. For example, it is used in cache memories and register files of the processor. SRAMs are made of arrays of cells, each one storing a bit of memory. There are different types of cells depending on the number of transistors used to make the cell, being 6T, 8T and 10T the most common ones. They are depicted in Figure 4.4, Figure 4.5 and Figure 4.6 respectively, and these will be the ones analyzed.

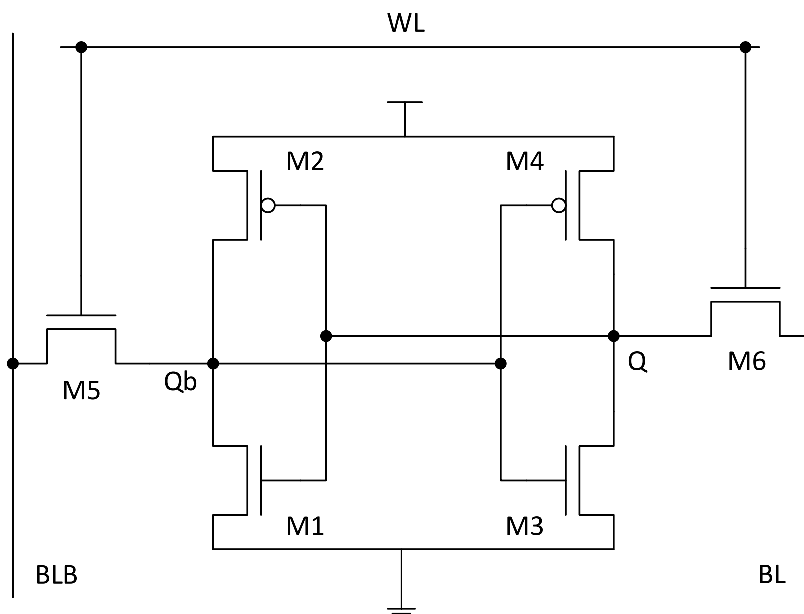

Figure 4.4: Scheme of a 6T Cell

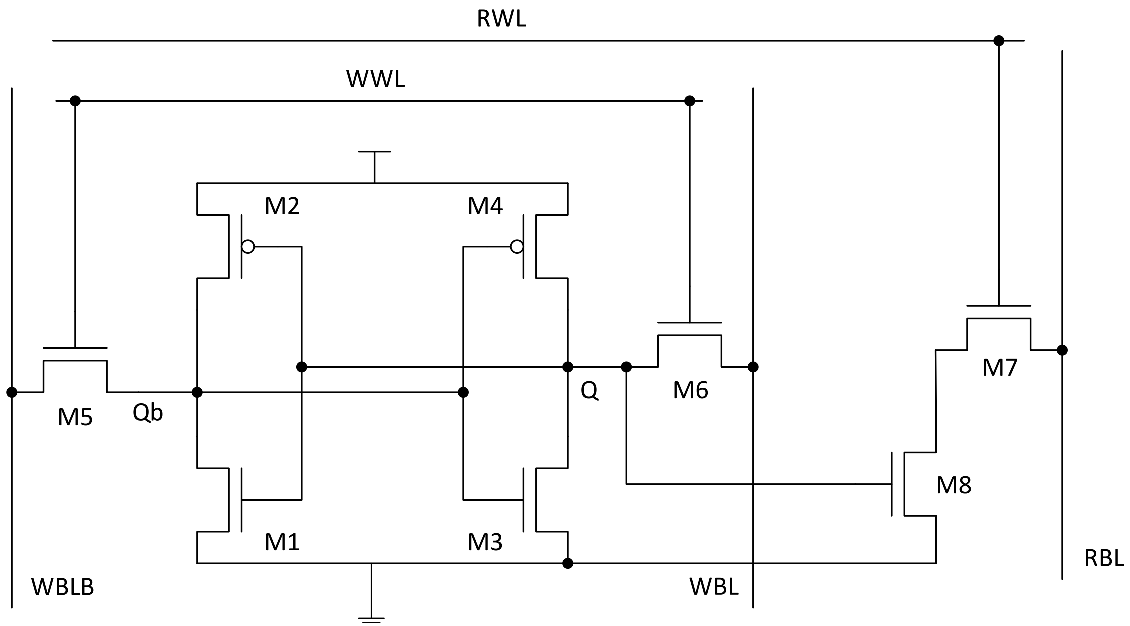

Figure 4.5: Scheme of an 8T Cell

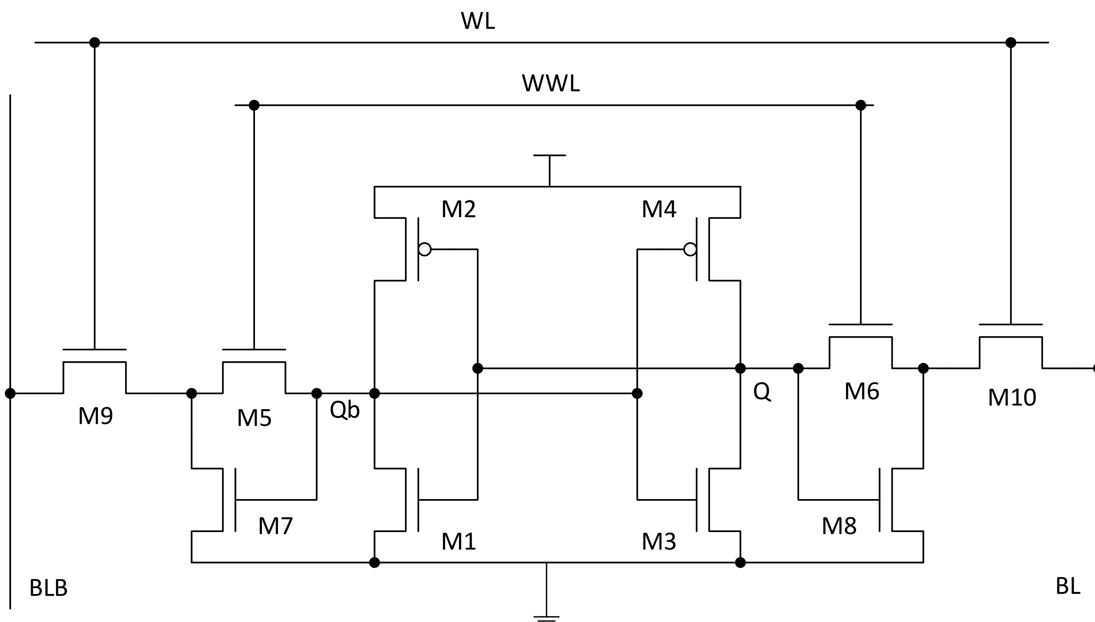

Figure 4.6: Scheme of a 10T Cell

As described above, to obtain the Soft Error Rate (SER) of an SRAM cell and therefore the vulnerability factor, the critical charge (Qcrit) is needed [25]. Qcrit represents the minimum charge needed to cause an upset in the SRAM cell, that is, a soft error.

Qcrit can be obtained doing simulations with HSPICE by inserting a current pulse in the sensible nodes of the cell, which are the storage nodes Q and Qb, and testing when an upset is produced. The current pulse will represent the charge produced by the impact of an alpha particle or cosmic ray. The current pulse can be modeled in different ways. In this analysis we use an exponential pulse with a fall time constant of 200ps, while different rise time constants has been tested (2ps, 16ps, 33ps and 90ps).

Qcrit can be computed using an approximation of the integral of the current pulse function using HSPICE. In this analysis, Qcrit is computed by measuring the time from the start of the pulse to 80% of its maximum when discharging, and then, this time is multiplied by 80% of the maximum current of the pulse. Therefore, we are measuring the area below the pulse in a rectangular form. This methodology may require some tuning depending on the time constants used and the technology being analyzed. Figure 4.7 shows a graphical example of the measures done to compute Qcrit with a negative current pulse.

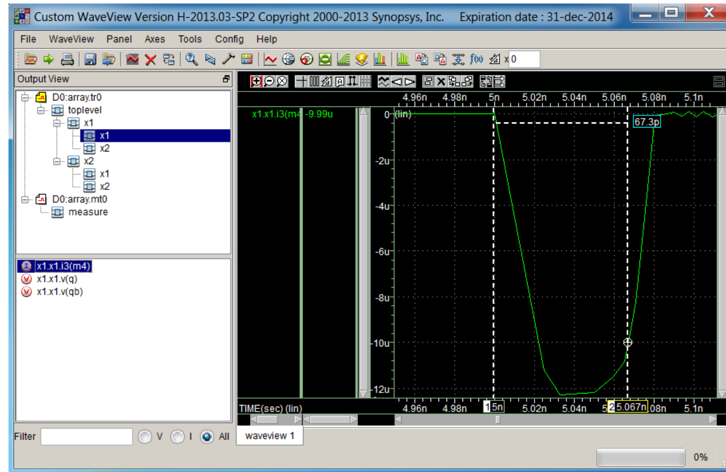

Figure 4.7: Graphical measure of Qcrit

The values of Qcrit obtained have been summarized in Table 4.2, showing the maximum, the minimum and the average Qcrit for each type of cell and technology. In this table we can see that the latest technology nodes have usually lower critical charge than their predecessors. However, different types of technologies, such as FinFETs improve in this aspect and have a higher Qcrit. Probably the best way to compute the vulnerability factor is to focus in the worst case, which is the minimum critical charge.

Qcrit Values of different SRAM Cells and Technologies			
SRAM Cell Types	**Maximum (fC)**	**Minimum (fC)**	**Average (fC)**
6T Planar 22nm	6,61	0,62	2,58
6T Planar 16nm	3,84	0,38	1,52
6T FinFET 20nm	26,71	4,62	12,19
6T FinFET 14nm	32,88	4,51	13,91
8T Planar 22nm	6,68	0,96	2,65
8T Planar 16nm	3,85	0,54	1,53
8T FinFET 20nm	26,76	4,71	11,33
8T FinFET 14nm	32,63	4,42	13,60
10T Planar 22nm	4,87	0,95	2,32
10T Planar 16nm	2,80	0,54	1,33
10T FinFET 20nm	22,67	4,62	10,23
10T FinFET 14nm	32,92	4,55	13,29

Table 4.2: Qcrit values obtained from HSPICE simulations

4.1.3. Analysis of Latches

Latches are the most basic sequential logic elements. Their output values depend not only in the current inputs but also in the previous ones. Therefore, latches are used to store data like state information. Figure 4.8 shows the scheme of the latch used in this analysis.

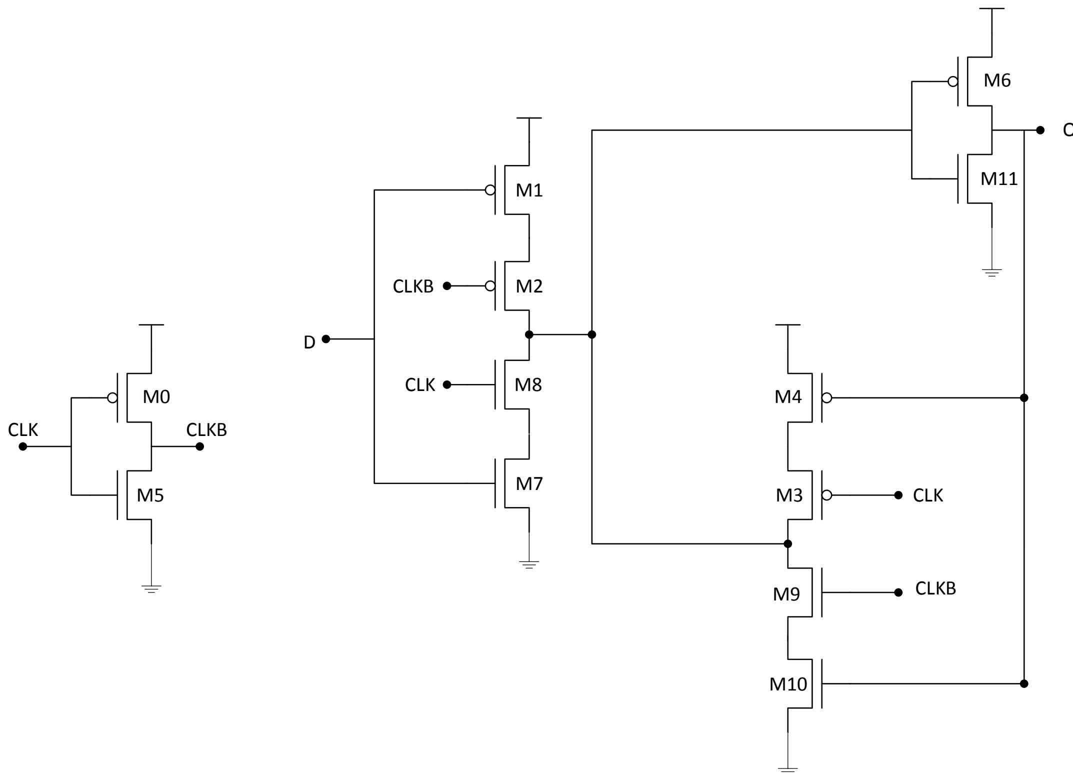

Figure 4.8: Scheme of a Latch

The methodology used to compute Qcrit for Latches is similar to the methodology used for SRAM cells. The sensible node studied is the intermediate node of the Latch [28][29]. As the latch can be in different modes, the current pulse has been introduced to test two cases. The first case is when the latch is in opaque mode, and the second case is when the latch is in transparent mode during the setup. Figure 4.9 shows a chronogram with the timings and modes of a static latch like the latch that has been analyzed.

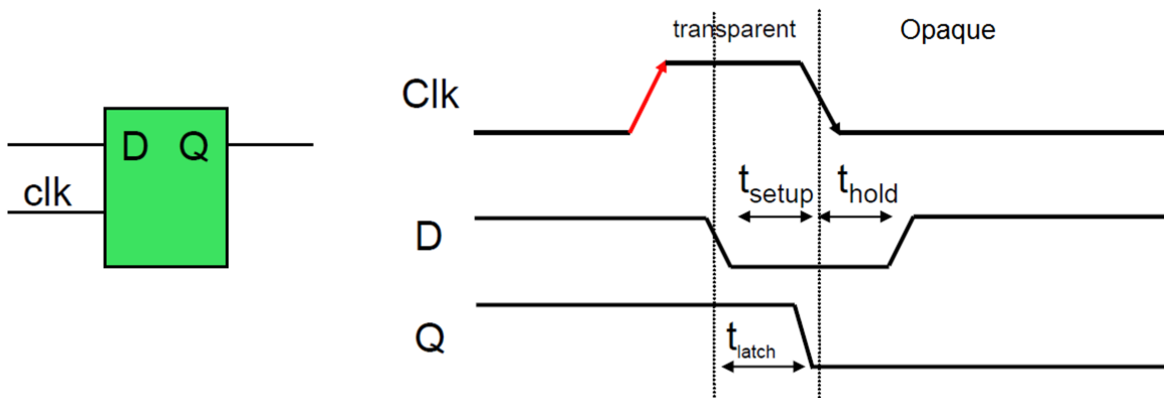

Figure 4.9: Time diagram showing the Latch modes and timing

Table 4.3 shows the Qcrit values obtained for the latch and different technology nodes. Similarly to SRAM cells, FinFET technology is more robust by having a higher Qcrit.

Qcrit Values of the Latch			
Technology	**Maximum (fC)**	**Minimum (fC)**	**Average (fC)**
Planar 22nm	7,79	1,87	3,12
Planar 16nm	4,64	1,00	1,83
FinFET 20nm	8,62	2,43	4,88
FinFET 14nm	8,63	3,47	5,64

Table 4.3: Qcrit values obtained for the Latch for different technology nodes

4.1.4. Tasks Summary

Up until this point of the project, the Qcrit computations of SRAM Cells and Latches has been completed for two technology nodes of planar CMOS and two technology nodes of FinFETs. However, there is still a lot of work to be done, mainly the Qcrit computation of Flip flops and combinatorial logic elements and the computation of the vulnerability factors. Table 4.4 summarizes the tasks that have been completed and the tasks that are to be done.

Tasks	Status
Analysis of previous work	Done
Circuit models	Done
Predictive Models	In progress (Trying to find some models for newer technologies)
Qcrit of SRAM Cells	Done
Qcrit of Latches	Done
Qcrit of Flip Flops	In progress
Qcrit of combinatorial logic	Not started
Find probability distributions of the charge of Alpha particles and neutron strikes	In progress
Compute the Technology Vulnerability factor (TVF)	Not started
Experimental study for the combinatorial logic	Not started
Technology contribution to SER Computation	Not started

Table 4.4: Tasks status

5. Conclusions

In this preliminary document, some technologies being used now or expected to be used in the near future have been reviewed, in addition to different possible source of failures that may be critical for these technologies. The work that has been done until now is mainly related to the characterization of soft errors. Not many conclusions can be drawn at this preliminary stage, but looking at some of the preliminary results, it is obvious that as technology scales down Qcrit is lower so the elements may become more vulnerable to soft errors. On the other hand newer technologies such as multi-gate FinFETs are more resistant to this effect. In conclusion, there is still a lot of work to do but preliminary studies suggest that newer technologies can reduce some of the current system vulnerabilities whereas planar CMOS is becoming more vulnerable due to the scaling down of its components.

6. Additional material on CLERECO SVN Repository

This section provides a link to tools, code and models developed in the framework of the activities described in this deliverable that are available through the CLERECO SVN Repository. This material, listed in Table 7 must be considered as integral part of the deliverable.

The CLERECO SVN repository is accessible through a web browse clicking on the links reported in Table 7. The access to the material requires authentication. Reviewers can access it using the following credentials:

- **Username**: clerecoreviewers
- **Password**: fp7-611404

Table 7: Additional Material

Item No.	Description	Link to the CLERECO SVN Repository
AM1	**SPICE Public Technology Compact Models used for fault characterization in CLERECO**	http://www.clereco.eu/clereco_svn/Deliverables/D2.2.1/PublicTechnologyCompactModels/
AM2	**SPICE models for basic circuits characterized in this deliverable**	http://www.clereco.eu/clereco_svn/Deliverables/D2.2.1/SPICE_models_for_basic_circuits/

7. Acronyms

The following table shows a list of the acronyms used in this document and their meaning:

Acronym	Definition
TVF	Technology Vulnerability Factor
CVF	Circuit Vulnerability Factor
CMOS	Complementary Metallic Oxide Semiconductor
FinFET	Fin-Shaped Field Effect Transistor
PTM	Predictive Technology Model
ITRS	International Technology Roadmap for Semiconductors
RDF	Random Dopant Fluctuations
LER	Line Edge Roughness
RTN	Random Telegraph Noise
EM	Electromigration
MeTTF	Median Time to Failure
MSV	Metal Stress Voiding
MTTF	Mean Time to Failure
GOW	Gate Oxide Wearout
HCI	Hot Carrier Injection
NBTI/PBTI	Negative/Positive Bias Temperature Instability
RIF	Radiation Induced Faults
SER	Soft Error Rate
Qcrit	Critical charge
SOI	Silicon On Insulator
SHE	Self-Heating
SDC	Silent Data Corruption
DUE	Detected Unrecoverable Error
FIT	Failure In Time

8. Bibliography

[1] R. Baumann, "Soft Errors in Advanced Computer Systems", IEEE Design & Test of Computers, vol. 22, no. 3, pp. 258-266, May/June, 2005

[2] S. Borkar et al., "Design and Reliability Challenges in Nanometer Technologies", IEEE DAC, pp. 75-75, 2004

[3] P. Shivakumar, M. Kistler, "Modeling the effect of technology trends on the soft error rate of combinational logic", IEEE DSN, 2002

[4] S. S. Mukherjee, C. Weaver, J. Emer, S.K. Reinhardt, T. Austin, "A systematic methodology to compute the architectural vulnerability factors for a high-performance microprocessor", MICRO, pp. 29-40, 2003

[5] D. Ernst et al., "Razor: circuit-level correction of timing errors for low-power operation", IEEE MICRO, Vol. 24, no. 3, pp. 10-20, 2004

[6] R. Vadlamani et al., "Multicore soft error rate stabilization using adaptive dual modular redundancy", IEEE DATE, pp. 27-32, 2010

[7] Kaliorakis, M.; Tselonis, S.; Foutris, N.; Gizopoulos, D., "D3.1 – Report on major classes of hard- ware component"

[8] M. H. Abu-Rahma, M. Anis. "Variability in Nanometer Technologies and Impact on SRAM", Springer New York, 2013

[9] P. Mishra, A. Muttreja, N. K. Jha, "FinFET Circuit Design", Springer Science, 2011

[10] Berkeley Predictive Technology Model and BSIM, http://www-device.eecs.berkeley.edu/bsim/

[11] Arizona State University (ASU) PTM, http://ptm.asu.edu/

[12] International Technology Roadmap for Semiconductors (ITRS) projections, http://www.itrs.net/

[13] Y. Cao, "Predictive Technology Model for Robust Nanoelectronic Design", Integrated Circuits and Systems, Springer, 2011

[14] D. Lu, "PhD Dissertation: Compact Models for Future Generation CMOS", Electrical Engineering and Computer Sciences University of California at Berkeley, 2011

[15] Shrikanth, "Reliability In The Face of Variability in Nanometer Embedded Memories", UPC Thesis, March, 2014

[16] S. Mukherjee. "Architecture Design for Soft Errors", Morgan Kaufmann, 2008

[17] Ralph Group nanoscale Physics, http://people.ccmr.cornell.edu/~ralph/projects/emig_movies/

[18] P. Hazucha and C. Svensson, "Impact of CMOS Technological Scaling on the Atmospheric Neutron Soft Error Rate", IEEE Transactions on Nuclear Science, Vol. 47, No. 6, pp.2586-2594, December 2000

[19] Q. Ding, R. Luo, H. Wang, H. Yang, Y. Xie, "Modeling the Impact of Process Variation on Critical Charge Distribution", IEEE, 2006

[20] Paul K. Chu, "Novel Silicon-on-Insulator Structures for Reduced Self-Heating Effects", IEEE Circuits and Systems magazine, 2005

[21] A. Armstrong, Self-Heating in SOI, http://www.ee.qub.ac.uk/nisrc/simulations/shsoi.htm

[22] X. Wang, A. R. Brown, B. Cheng, A. Asenov, "Statistical Variability and Reliability in Nanoscale FinFETs", IEEE, 2011

[23] H. Cha, et al., "A Gate-Level Simulation Environment for Alpha-Particle-Induced Transient Faults", IEEE Transactions on Computers, 45(11), 1996

[24] Z. Kalbarczyk, et al., Hierarchical Simulation Approach to Accurate Fault Modeling for System Dependability Evaluation, IEEE Transactions on Software Engineering, 25(5), 1999.

[25] R. Naseer, S. DasGupta. "Critical Charge Characterization for Soft Error Rate Modeling in 90nm SRAM", IEEE, 2007

[26] J. F. Ziegler, "Terrestrial cosmic rays", IBM journal of research and development, 1996

[27] J. F. Ziegler, et al.,"IBM experiments in soft fails in computer electronics (1978-1994)", IBM journal of research and development, 1996

[28] S. Lin, Y. Quim, F. Lombardi, Soft-Error Hardening Designs of Nanoscale CMOS Latches, 27th IEEE VLSI Test Symposium, 2009

[29] S. A. Tawfik, V. Kursun, Characterization of New Static Independent-Gate-Biased FinFET Latches and Flip-Flops under Process Variations, 9th International Symposium on Quality Electronic Design, IEEE, 2008