Simulating and modeling the effects of laser fault injection on integrated circuits

Raphael Andreoni Camponogara-Viera

THÈSE POUR OBTENIR LE GRADE DE DOCTEUR DE L'UNIVERSITE DE MONTPELLIER

En microélectronique

École doctorale : Information, Structures, Systèmes (I2S)

Unité de recherche : Laboratoire d'Informatique, Robotique et Microélectronique (LIRMM)

Simulating and Modeling the Effects of Laser Fault Injection on Integrated Circuits

Présentée par Raphael A. C. VIERA

Le 02 octobre 2018

Sous la direction de Philippe MAURINNE

Devant le jury composé de

Jean-Luc DANGER, Professeur, Telecom ParisTech	Rapporteur
Jean-Michel PORTAL, Professeur, IM2NP	Rapporteur
Guy CATHEBRAS, Professeur, LIRMM	Examinateur
Bruno ROUZEYRE, Professeur, LIRMM	Président du jury
Philippe MAURINE, Maître de conférences HDR, LIRMM	Directeur de thèse
Jean-Max DUTERTRE, Maître de conférences HDR, EMSE	Co-Encadrant de thèse
Rodrigo POSSAMAI BASTOS, Maître de conférences HDR, TIMA	Co-Encadrant de thèse

UNIVERSITÉ DE MONTPELLIER

To You

Acknowledgements

I want to thank first and foremost my parents, Edison and Cecília for their unconditional love and for challenging me to rise above the comfort and security of the ordinary, and for my siblings, Christian and Lucas for their love. I am grateful for my grandmother Carmen who, like my parents always encouraged me to go further.

I want to express special gratitude to my wife Suzane for her support and patience throughout this project. I also express my gratitude to my wife's family for their support and friendship, namely Elda, Gelson, Norton and Priscilla.

I wish to give a big thanks to my childhood friend Alonso for his true friendship since we were seven years old. I also thank his family for always receiving me with open arms.

I would like to thank my supervisors Jean-Max Dutertre, Philippe Maurine and Rodrigo Possamai Bastos for their guidance, insights and encouragement throughout my thesis.

I would like to thank Jean, Leonel, Otto, Rodrigo and Thiago, my colleagues from the TIMA Laboratory, in Grenoble. And my colleagues from the SAS Laboratory in Gardanne, Mounia, Elias, Paul and Noèmie for their friendship, comments and insights.

My research was supported by the Brazilian National Council for Scientific and Technological Development (CNPq Brazil). I would like therefore to thank all the CNPq's staff for their support during this project.

ISBN: 978-2-11-129250-5

Table of Contents

ISBN: 978-2-11-129250-5

List of Figures

ISBN: 978-2-11-129250-5

List of Tables

ISBN: 978-2-11-129250-5

Abstract

Laser fault injections induce transient faults into ICs by locally generating transient currents that temporarily flip the outputs of the illuminated gates. Laser fault injection can be anticipated or studied by using simulation tools at different abstraction levels: physical, electrical or logical. At the electrical level, the classical laser-fault injection model is based on the addition of current sources to the various sensitive nodes of MOS transistors. However, this model does not take into account the large transient current components also induced between the VDD and GND of ICs designed with advanced CMOS technologies. These short-circuit currents provoke a significant IR drop that contribute to the fault injection process. This thesis describes our research on the assessment of this contribution. It shows by simulation and experiments that during laser fault injection campaigns, laser-induced IR drop is always present when considering circuits designed in deep submicron technologies. It introduces an enhanced electrical fault model taking the laser-induced IR-drop into account. It also proposes a methodology that uses standard CAD tools to allow the use of the enhanced electrical model to simulate laser-induced faults at the electrical level in large-scale circuits. On the basis of further simulations and experimental results, we found that, depending on the laser pulse characteristics, the number of injected faults may be underestimated by a factor as large as 3 if the laser-induced IR-drop is ignored. This could lead to incorrect estimations of the fault injection threshold, which is especially relevant to the design of countermeasure techniques for secure integrated systems. Furthermore, experimental and simulation results show that even though laser fault injection is a very local and accurate fault injection technique, the induced IR drops have a global effect spreading through the supply network. This gives experimental evidence that the effect of laser illumination is not as local as usually considered.

Keywords: Laser fault injection, design for test & security, transient faults, methodologies for EDA, hardware security implementation.

ISBN: 978-2-11-129250-5

Résumé

Avec la réduction d'échelle des systèmes intégrés, l'augmentation de leur robustesse face aux perturbations environnementales ou anthropiques entraîne des défis de conception considérables. Le vieillissement, les particules alpha libérées par les impuretés radioactives, et les neutrons provenant des rayons cosmiques sont des exemples d'événements environnementaux [60]. D'autre part, les attaques par injection de fautes dans le but de récupérer les données secrètes utilisées par les applications de sécurité ou de désactiver des fonctions de sécurité [62] sont des attaques humaines qui permettent aux attaquants d'obtenir des informations fondamentales pour les méthodes de cryptanalyse ou d'activer les chevaux de Troie matériels [47] malicieusement insérés dans les systèmes.

Une attaque par injection de fautes peut être utilisée pour désactiver les mécanismes de sécurité des systèmes embarqués. La variété des techniques connues pour injecter des fautes dans des circuits intégrés (CIs) est grande et continue de grandir [15, 16]. Parmi eux, il est possible de trouver des techniques pour perturber le signal d'horloge [6, 66], pour induire des variations brusques de la tension d'alimentation [7] ou de polarisation du substrat [75], et pour injecter des courants parasites en utilisant de puissantes perturbations électromagnétiques ou des éclairs de lumière intense [16, 36].

L'efficacité des attaques optiques a d'abord été démontrée en utilisant le flash d'un appareil photo [109]. Cependant, afin d'influencer indépendamment chaque cellule logique, et ainsi de mieux contrôler les fautes injectées, des sources focalisables de rayonnements ionisants sont préférables. Les sources laser sont un exemple de telles sources. En effet elles permettent de contrôler finement les fautes injectées grâce à leurs hautes résolutions spatiale et temporelle. Dans les années 1960, l'illumination laser a commencé à être utilisée comme un moyen d'émuler l'effet des particules ionisantes puisque les propriétés des courants transitoires qu'ils induisent sont similaires [48, 52, 77, 80, 118]. S. Skorobogatov [107, 109] a signalé l'utilisation du laser comme outil pour attaquer les circuits sécurisés au début des

ISBN: 978-2-11-129250-5

années 2000. Suite à ce travail, la conception de circuits robustes contre les injections de fautes laser est apparue comme une nécessité dans la communauté de la sécurité matérielle.

Des modèles et des méthodologies sont donc nécessaires pour prévoir les effets des attaques laser sur les CIs. Les méthodologies développées pour la simulation de fautes peuvent être réalisées à différents niveaux d'abstraction du flux de conception (par exemple, niveau de transistor, niveau de porte logique, niveau de registre, et même au niveau de logiciel). Les niveaux d'abstraction plus bas offrent la plus grande précision.

Lorsqu'un laser éclaire un CI, il génère un courant parasite (photoélectrique) [58] et, par conséquent, une tension transitoire indésirable. Cet effet peut se propager à travers la logique vers l'entrée d'un registre (bascules de type D) et, s'il est toujours présent lorsque le front d'horloge montante suivant se produit, une valeur de bit incorrecte est memorisée, produisant une soft erreur (SE). Au niveau électrique, il a été démontré [59, 121] qu'un tel courant transitoire est efficacement modélisé par une source de courant (IPh) délivrant un signal avec une forme en double exponentielle. Ensuite, une simulation de niveau électrique, visant à prendre en compte les effets de l'illumination laser, est réalisée en ajoutant une source de courant à la netlist de la cellule éclairée par le faisceau laser. Dans cette thèse, nous appelons ce modèle le modèle électrique classique.

Ce modèle a été créé à une époque où l'utilisation de sources laser délivrant des faisceaux de diamètre $1\,\mu m$ ou $5\,\mu m$ permettait de ne viser qu'une seule jonction PN sensible à la fois (ce sont les jonctions PN d'un circuit qui constituent les zones sensibles à l'éclairement laser). Pour les technologies avancées actuelles, ce modèle est discutable. En effet, pour des cellules standard de technologies plus récentes éclairées par une source laser avec un diamètre de spot de $5\,\mu m$, le tir laser éclaire simultanément plusieurs portes à la fois et donc plusieurs jonctions PN lors d'un même tir. En conséquence, un courant transitoire (IPh_{Psub_nwell}) qui passe directement de V_{DD} à G_{ND} est toujours induit. Ce courant est induit dans la jonction biaisée inversée $Psub$ - $Nwell$ polarisée en inverse qui entoure chaque $Nwell$. Même si le faisceau laser est dirigé vers un NMOS sensible, le faisceau laser induit également des porteurs de charge qui seront suffisamment proches d'une jonction $Psub$ - $Nwell$ pour induire IPh_{Psub_nwell}. Ce courant, qui n'est pas pris en compte par le modèle classique, peut avoir un effet significatif sur le mécanisme d'injection de fautes en induisant une chute de tension d'alimentation (IR drop).

Nous avons démontré par simulation et au moyen d'expérimentations la précision du modèle électrique amélioré proposé. Pour ce faire, le modèle classique

et le modèle amélioré ont été appliqués, sur une base de simulation, à un oscillateur en anneau (ring oscillator - RO). Un RO a également été implémenté sur un FPGA afin d'effectuer une illumination laser et de les comparer avec des résultats expérimentaux. La simulation et les résultats expérimentaux sont caractérisés par un haut niveau de corrélation, ce qui met en évidence la plus grande précision du modèle électrique amélioré proposé dans cette thèse par rapport au modèle de fautes classique.

La remarque ci-dessus implique que les modèles [39, 44, 54, 70] utilisés jusqu'ici pour simuler les effets d'un tir laser sur des CIs conçus dans des technologies avancées manquent de précision. De plus, les effets de propagation des courants photoélectriques et de l'IR drop associée ne peuvent être simulés avec précision qu'à des niveaux d'abstraction plus bas – en tenant compte de la topologie du circuit cible (en particulier de son réseau d'alimentation et de polarisation des substrats) pour mieux représenter le phénomène physique – dans le cadre d'un système entier. La simulation doit donc être effectuée sur des circuits complexes et pas seulement dans une (ou quelques) cellules CMOS et en prenant en compte le layout et les parasites.

Au meilleur de nos connaissances, parmi les simulateurs de fautes proposés précédemment [31, 46, 55, 70, 82, 100], le plus récent [71] est basé sur le code open source nommé Lifting [22]. Ces simulateurs de fautes s'appuient sur des modèles électriques [39, 44, 93, 101] qui dépendent de la configuration individuelle de plusieurs paramètres technologiques. Par exemple, le modèle proposé dans [50] inclut les jonctions bipolaires parasitaires verticales (inhérentes aux MOSFETs) dans le processus d'injection de fautes qui peuvent conduire à des effets de IR drop. Cependant, [50] se concentre uniquement sur l'étude d'un seul inverseur. En effet, dimensionner le réseau RC de rails d'alimentation est une tâche difficile, car les valeurs RC dépendent de plusieurs paramètres de la technologie. Par exemple, la taille des cellules, la position des prises de tension sur les rails et les parasites RC. Aucune de ces travails ne considère l'effet de l'IR drop induit par laser.

Ce qui a été observé jusqu'ici est qu'il y a eu des améliorations des modèles électriques des courants transitoires induits par laser ces dernières années. Cependant, ces modèles ont été développés au niveau d'une seule porte, ignorant ainsi les effets des courants induits par laser au niveau de la puce. En ce qui concerne les simulateurs de fautes laser, ils utilisent généralement des modèles électriques simples tels que le modèle électrique classique, dans lequel des sources de courant sont attachées au drain et à la masse des transistors sensibles au laser.

Afin d'utiliser le modèle électrique proposé qui prend en compte la contribu-

tion de IR drop induite par le courant (IPh_{Psub_nwell}) créé entre la jonction $Psub$ - $Nwell$, il est nécessaire de modéliser par un réseau RC les rails d'alimentation. Modéliser le réseau RC pour quelques portes devrait être faisable, le faire pour un grand circuit n'est pas une tâche à effectuer manuellement. Compte tenu de cette limitation, à savoir que les simulateurs de fautes laser actuels ne peuvent utiliser des modèles de faute complets et précis, nous proposons une méthodologie de simulation d'injection laser utilisant un outil CAO d'electromigration et IR drop pour fournir automatiquement le réseau RC d'un design donné. Il fournit également la tension transitoire qui se propage le long des rails d'alimentation à la suite du courant IPh_{Psub_nwell}. La méthodologie peut être utilisée pour tout circuit conçu dans n'importe quelle technologie prise en charge par les outils de CAO standard.

Les résultats de simulation fournis par la méthodologie proposée mettent en évidence la manière dont les effets de l'IR drop induits par le laser contribuent de manière significative à l'injection de fautes. La méthodologie a été appliquée à une puce de test, qui a utilisé le modèle électrique amélioré lors de simulations afin de démontrer comment l'IR drop facilite l'apparition des fautes en amplifiant les perturbations induites par laser sur les signaux logiques. Les zones sensibles à l'injection de fautes laser et la durée de sensibilité au laser sont toutes deux augmentées.

Une comparaison entre les résultats de simulation obtenus avec notre méthodologie et les résultats expérimentaux obtenus avec un FPGA Virtex 5 a permis de déterminer la supériorité du modèle proposé par rapport au modèle classique. Les résultats présentés ont également révélé que le IR drop induite par le laser contribue fortement au processus d'injection de fautes car il amplifie la tension transitoire induite dans le drain des transistors sensibles. Cette amplification réduit la quantité de charge nécessaire pour provoquer une faute transitoire, diminuant ainsi le seuil d'injection de faute. Les résultats ont révélé que le fait d'ignorer le IR drop induite par le laser peut entraîner une sous-estimation du risque d'injection de fautes, sans parler de l'estimation incorrecte du seuil d'injection de fautes. En effet, pour la puce test évaluée par la méthode de simulation, une augmentation du nombre de fautes d'un facteur de 2,38 (resp. 3,03) a été observée pour un diamètre de spot laser égal à $5\,\mu m$ (resp. $1\,\mu m$) lorsque les IR drops sont pris en compte. Ce résultat est particulièrement pertinent pour la conception de techniques de contre-mesures pour des systèmes intégrés sécurisés.

Dans ce contexte, la contribution principale de cette thèse est : premièrement, la mise en évidence par simulation d'injection de fautes et par des expériences d'irradiation laser que lors d'un tir laser, une composante de courant supplémen-

taire provoquant un IR drop avec un effet significatif sur l'opération cible est toujours présente lorsque l'on travaille avec des circuits conçus dans des technologies CMOS avancée. Deuxièmement, cette thèse introduit un modèle électrique de faute transitoire amélioré qui prend en compte l'IR drop induite par laser pendant les simulations. Troisièmement, il est dérivé, à partir du modèle de fautes améliorées, une méthodologie de simulation basée sur des outils de CAO standard (en tenant compte l'IR drop induite par laser) pour prévoir l'effet des injections laser dans les circuits à grande échelle.

En plus, cette thèse introduit une méthode basée sur la simulation pour évaluer l'efficacité des techniques de détection d'erreurs simultanées (Concurrent Error Detection Techniques) dans l'identification des fautes transitoires provoquées dans les blocs logiques combinatoires. Des profils de fautes typiques sont simulés dans des campagnes d'injections reproduisant des scénarios de sortie de circuits combinatoires. De plus, une technique de détection d'erreur simultanée est proposée et comparée à des stratégies de pointe en utilisant la méthode présentée. Les résultats montrent les capacités de toutes les techniques étudiées, fournissant un classement en termes de leur efficacité dans la détection des fautes transitoires induites dans les circuits logiques combinatoires, et analysant les situations dans lesquelles les SEs sont produites dans les éléments de mémoire.

Institutions impliquées

Cette thèse a reçu le soutien financier du Conseil National de Développement Scientifique et Technologique (CNPq Brésil) et a été réalisée en collaboration avec trois laboratoires :

- *Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier* (LIRMM) : un laboratoire de recherche public mixte du *Centre National de Recherche Scientifique* (CNRS) et *Université de Montpellier* .

- *Systèmes et Architectures Sécurisés* (SAS) : une équipe commune de recherche et de développement conjointe entre *l'École des Mines de Saint-Étienne* (EMSE) et le *Commissariat à l'Énergie Atomique et aux alternatives* (CEA).

- *Laboratoire de Techniques de l'Informatique et de la Microélectronique pour l'Architecture des Systèmes Intégrés* (TIMA) : un laboratoire public mixte de recherche du *Centre National de Recherche Scientifique* (CNRS), *Université*

Joseph Fourier (UJF), et *Institut Polytechnique de Grenoble* (Grenoble INP), tous membres de *l'Université de Grenoble*

La première partie de la thèse, de septembre 2015 à mai 2017, s'est déroulée à Grenoble au laboratoire TIMA. Et la deuxième partie de la thèse, de juin 2017 à septembre 2018, a été réalisée à Gardanne, au laboratoire SAS.

Mots-clés : Injection de faute par laser, fautes transitoires, conception pour test & sécurité, méthodologies pour EDA, implémentation de sécurité matérielle.

Chapter 1

Introduction

With the downscale of integrated systems, increasing their robustness against environmental or human-induced perturbations motivates considerable design challenges. Aging, alpha particles released by radioactive impurities, and more importantly, neutrons from cosmic rays are examples of environmental events [60]. On the other hand, fault injections to the end of retrieving secret data from security applications or disabling embedded secure protocols [62] are human attacks, which allow attackers obtaining fundamental information for cryptanalysis methods or to activate hardware trojans [47] maliciously inserted in systems.

Fault injection attack can be used to defeat the security mechanisms of embedded devices. The variety of known techniques to inject faults into integrated circuits (ICs) is large and keeps on growing [15, 16]. Among them it is possible to find techniques to disrupt the clock signal [6, 66], to induce sudden variations of the supply voltage [7] or of the substrate biasing [75], and to inject parasitic currents using powerful electromagnetic disturbances or intense light flashes [16, 36].

The efficiency of optical attacks was first demonstrated using the flash of a camera [109]. However, in order to influence each logic cell independently, and thus to better control the injected faults, focusable sources of ionizing radiations are preferable. Laser sources are an example of such sources. Indeed they allow to finely control the injected faults thanks to their high spatial and temporal resolutions. In the 1960s, laser illumination started to be used as a way to emulate the effect of ionizing particles since the properties of the transient currents they both induce are similar [48, 52, 77, 80, 118]. S. Skorobogatov [107, 109] however, reported the use of laser as a tool to attack secure circuits in the early 2000s. Following this work, designing robust circuits against laser fault injections has emerged as a necessity in the hardware security community.

ISBN: 978-2-11-129250-5

Models and methodologies are thus demanded to forecast the effects of laser-based attacks on ICs. The methodologies developed for fault simulation can be performed at different abstraction levels of the design flow (e.g. transistor level, gate level, RTL level, and even software level). However, low abstraction levels provide the highest accuracy.

When a laser illuminates an IC, it generates a parasitic (photoelectric) current [58] and, consequently, an undesired transient voltage. This effect may propagate through the logic toward the input of a register (D-type Flip-Flops) and, if it is still present when the next rising clock edge occurs, an incorrect bit value is latched, producing a soft error (SE). At the electrical level, it has been demonstrated [59, 121] that such transient current is efficiently modeled by a current source delivering a signal with a double exponential shape. Then, an electrical-level simulation, aiming to take into account effects of laser illumination, is performed by adding a current source to the netlist of the cell illuminated by the laser beam.

If such a current source-based model has been considered relevant for submicron CMOS technologies, it is questionable for more recent deep-submicron technologies. Indeed, with the increasing transistor density, laser illumination does not affect a single transistor (or CMOS gate) but rather illuminates multiple gates at a time. In this case, a laser shot also induces a current that flows from V_{DD} to G_{ND} causing a temporary power supply voltage drop (IR drop), which is a source of timing failures due to the violation of specified timing constraints [8, 33, 114]. In this case, we have demonstrated [117] that the induced IR drop may be of significant amplitude and duration, thus it has to be taken into account while simulating laser fault injection.

The above remark implies that the models [39, 44, 54, 70] used so far for simulating the effects of a laser shot on ICs designed in advanced technologies lack accuracy. Furthermore, the propagation effects of the photoelectric currents and of the related IR drop can only be simulated with accuracy at low abstraction levels –taking into account the layout topology to better represent the physical phenomenon– in the scope of a whole system. The simulation must thus be performed on complex circuits and not just in one (or few) CMOS cells.

To the best of our knowledge, among the formerly proposed fault simulators [31, 46, 55, 70, 82, 100], the most recent one [71] is based on the open-source code named Lifting [22]. These fault simulators rely on electrical models [39, 44, 93, 101] that depend on individually setting several technology parameters. For instance, the model proposed in [50] includes the vertical parasitic bipolar junctions (inherent to MOSFETs) in the fault injection process that may lead to IR drop effects. However, [50] focuses only on the scope of a single inverter. In fact, dimensioning

ISBN: 978-2-11-129250-5

the RC network of power/ground rails is a difficult task, since the RC values depend on several parameters of the technology, for example, the size of cells, the position of voltage taps on the rails and the RC parasitics. None of these formerly works consider the effect of the laser induced IR drop.

Within this context, the main contribution of this thesis is threefold. Firstly, it reveals by both fault injection simulation and irradiation experiments that during a laser shot, an additional current component causing an IR drop with a significant effect on the target operation is always present when working with circuits designed in deep submicron CMOS technologies. Secondly, this thesis introduces an improved transient fault model that takes laser-induced IR drop into account for simulation purposes. Thirdly, it is derived, from the enhanced fault model, an adequate simulation methodology based on standard CAD tools (taking the induced IR drop into account) to forecast the effect of laser fault injections in large scale circuits.

In addition, this thesis also introduces a simulation-based method for evaluating the effectiveness of Concurrent Error Detection (CED) techniques in identifying transient faults provoked in combinational logic blocks. Typical fault profiles are simulated in campaigns of injections that reproduce output scenarios of faulted combinational circuits. Furthermore, a CED technique is proposed and compared to State-of-the-Art strategies by using the presented method. Results show the capabilities of all studied techniques, providing a rank in terms of their effectivenesses in detecting transient faults induced in combinational logic circuits, and analyzing the situations in which soft errors are produced in memory elements.

The rest of this thesis is organized as follows. Chapter 2 gives a detailed background on the effects of laser illumination on ICs. Furthermore, this chapter recalls the current literature about transient-fault detection techniques for protecting integrated systems against transient faults (TFs) induced by fault injection techniques.

In the following, Chapter 3 presents the method for evaluating the effectiveness of the CED techniques (introduced in Chapter 2) in detecting TFs. The performance and costs of all detection techniques are summarized in a table, thus giving a direct insight of the effectiveness of each technique. Also, in this chapter, another CED technique is introduced and compared among the other techniques.

A background and discussion about the limitations of the previous proposed laser fault models [39, 50, 93, 101] are given in Chapter 4 before introducing our enhanced electrical fault model. Then, gate level simulations and experimental results of laser injections are given in order to demonstrate the existence of laser-induced IR drops and also to confirm the correctness of the proposed enhanced model.

Chapter 5 details the method allowing to simulate laser-induced faults in large-

ISBN: 978-2-11-129250-5

scale circuits. Simulation results provided by the proposed method are presented. A discussion regarding the contribution of the laser-induced IR drop is given by comparing simulation and experimental results at system level before concluding the thesis in Chapter 6.

Involved Institutions

This thesis has the financial support of the National Council for Scientific and Technological Development (CNPq Brazil) and it was done in collaboration with three labs:

- *Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier* (LIRMM): a public joint research laboratory of the *Centre National de la Recherche Scientifique* (CNRS) and *Université de Montpellier*.
- *Systèmes et Architectures Sécurisés* (SAS): a joint research and development team between the *École des Mines de Saint-Étienne* (EMSE) and the *Commissariat à l'Énergie Atomique et aux énergies alternatives* (CEA).
- *Laboratoire de Techniques de l'Informatique et de la Microélectronique pour l'Architecture des systèmes intégrés* (TIMA): a public joint research laboratory of the *Centre National de la Recherche Scientifique* (CNRS), *Université Joseph Fourier* (UJF), and *Institut Polytechnique de Grenoble* (Grenoble INP), all members of the *Université de Grenoble*

The first part of the thesis, from September, 2015 to May, 2017 was done in Grenoble at TIMA laboratory. And the second part of the thesis, from June, 2017 to September 2018, was done in Gardanne, at SAS laboratory.

ISBN: 978-2-11-129250-5

Chapter 2

Introduction to Hardware Security

In 1978, Intel Corporation was unable to deliver an order containing microchips to AT&T as the chips were not working as expected. Eventually, later that year, Intel was able to trace the problem to their chip packaging modules. These packaging modules got contaminated with Uranium-235, Uranium-238 and Thorium-230 from an old uranium mine located upstream on Colorado's Green River from the new ceramic factory that made these modules. In the same year, a landmark publication by May and Woods [76] described Intel's problem with alpha particle contamination. These particles create a charge in sensitive chip areas causing bits to flip. This was the first report of faults being injected into a chip.

Since then, several fault induction methods have been discovered and used to attack secure systems. By attack we mean the use of proper tools to extract confidential data of secure systems in order to, for example, steal a service. The first attack that used induced faults to derive secret information targeted the Rivest-Shamir-Adleman (RSA) public-key cryptosystem [21].

Although hardware security includes the study of side channel attacks based on observing the target's activity [11, 19, 37, 57, 61, 64, 65, 81, 108, 110, 119], this thesis focuses on fault injection attacks [10, 13, 14, 18, 36, 56, 63, 67, 72, 73, 74, 102] and more specifically on the use of laser pulses to induce faults into secure integrated circuits [15, 20, 44, 96, 109, 116].

To be more precise, this thesis focuses on the assessment of the effects of laser illumination on ICs rather than attack methods using laser fault injection. Therefore, the next section reports in details the effects of laser illumination on ICs. Section 2.2 presents several transient-fault detection techniques aiming the protection of integrated systems against TFs provoked in combinational logic blocks. Such TFs can be induced by laser fault injection.

ISBN: 978-2-11-129250-5

2.1 Laser Illumination Effects on ICs

Lasers have been used since the 1960s in order to emulate the effects caused by radiation on semiconductors [48]. In the early 2000s, S. Skorobogatov [44, 109] reported the use of laser illumination to induce faults into secure integrated circuits. As this thesis focuses on laser fault injection, this section provides in details a background on the effects of laser illumination on ICs.

2.1.1 Effect of a Laser Shot at Transistor Level

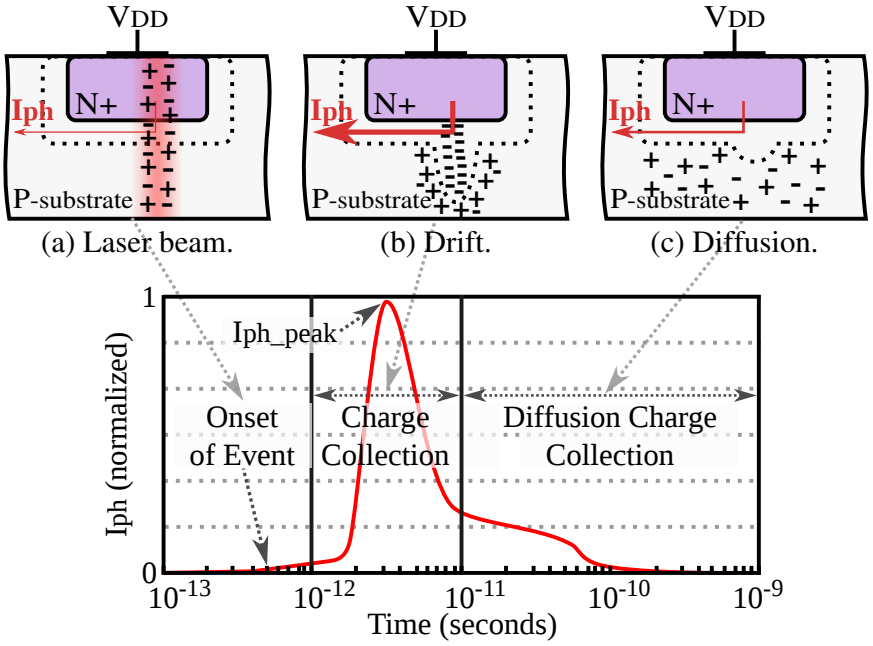
ICs are known to be sensitive to induced transient currents. Such currents may be caused by a laser beam passing through the device, creating electron-hole pairs along the path of the laser beam [58]. These induced charge carriers generally recombine without any significant effect, unless they reach the strong electric field found in the vicinity of reverse biased PN junctions (the reverse biased junction is the most laser-sensitive part of circuits) [17]. In this case, the electrical field puts these charges into motion and a transient current flows from the reversed biased PN junction (drain of NMOS or PMOS transistor) to the $P_{substrate}$ biasing contact.

Each induced transient current has its proper characteristics such as amplitude and duration that depend basically on the laser energy, the laser shot location, the device technology, the device supply voltage, the output load, etc. The nature of these currents was first studied in the case of radioactive particles [48, 52, 77, 80, 118]. Laser illumination started then to be used as a way to emulate the effect of ionizing particles since the properties of the transient currents they both induce are similar.

Fig. 2.1 translates to the case of laser illumination the results of [17].

As shown in Fig. 2.1a, at the onset of an event caused by a laser shot, a track of electron hole pairs with high carrier concentration is formed along the path of the laser beam. When the resultant track traverses or comes close to the depletion region of a reverse biased PN junction, carriers are rapidly collected by the electric field creating a current/voltage transient at that node. An interesting feature of the event is the distortion of the potential into a funnel shape [52, 53]. This funnel enhances the efficiency of the drift collection by extending the field depletion region deeper into the substrate (Fig. 2.1b). The profile of the funnel (size and distortion) depends on the substrate doping. This collection phase is completed in the picosecond range and followed by a phase where diffusion begins to dominate the collection process (Fig. 2.1c). Additional charge is collected as electrons diffuse into the depletion region on

ISBN: 978-2-11-129250-5



(d) Induced transient current.

Fig. 2.1: Charge generation and collection phases in a reverse-biased PN junction and the resultant transient current caused by the passage of a laser beam.

a longer time scale (nanoseconds range) until all excess carriers have been collected, recombined, or diffused away from the junction area. A laser-induced transient current is thus called 'photocurrent' [59, 121]. The current pulse $I_{Photocurrent}$ (I_{Ph}) resulting from these three phases is shown in Fig. 2.1d. The red arrows in Fig. 2.1 represent the transient current flowing from the sensitive drain to the $P_{substrate}$ biasing contact tied at GND.

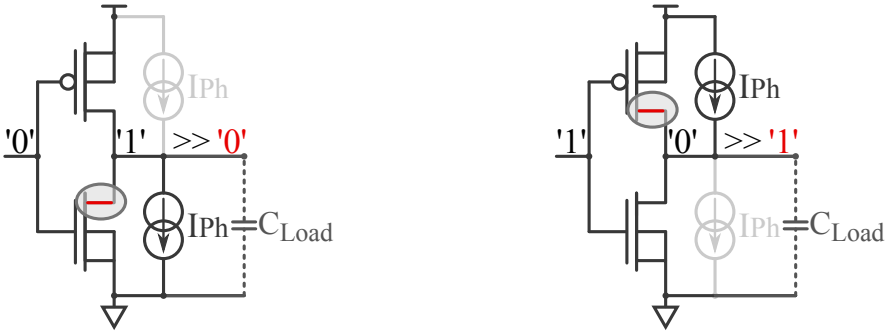
2.1.2 Effect of a Laser Shot at Gate Level

The effects of a laser shot are recalled in Fig. 2.2 which illustrates in the case of an inverter where laser shots may generate photocurrents at gate level. In case the inverter input is low (Fig. 2.2a), the most laser-sensitive part of the inverter is the drain of the NMOS transistor due to a reverse biased PN junction between the drain and the $P_{substrate}$. Thus, an induced transient current (I_{Ph}) flows from the drain of the NMOS to the $P_{substrate}$ biasing contact (at GND). A similar reasoning can be made when the inverter input is high (Fig. 2.2b). In that case, the susceptible part of the inverter is the drain of the PMOS transistor.

In case of Fig. 2.2a (resp. Fig. 2.2b), a part of the induced photocurrent (I_{Ph}) discharges (resp. charges) the inverter output capacitance. As a result the inverter

ISBN: 978-2-11-129250-5

output goes to low voltage (resp. high voltage), thus a so called voltage transient occurs. As can be observed from the above analysis, the laser-sensitive areas of an IC is data dependent since it will depend if the drain of a NMOS or PMOS transistor is biased at V_{DD} or G_{ND}.



(a) NMOS sensitive drain. (b) PMOS sensitive drain.

Fig. 2.2: Classical Electrical model of laser-induced transient currents applied to a CMOS inverter.

The beam diameter is one of the most important attribute of a laser beam in a class of commonly measured parameters (beam diameter, spatial intensity distribution, beam quality factor etc.). A commonly used definition of the laser beam diameter is derived from the bivariate normal distribution of its intensity leading to measure the beam diameter at 13.5% of its maximum value [25], or a drop to $\frac{1}{e^2}$ from its peak value.

The effects of a near infrared laser beam have been modeled in [41] and later in [101]. In the latter work, it is shown that the induced photocurrent (I_{Ph} in Fig. 2.1d), which is spatially distributed as a bivariate normal distribution, has a peak amplitude I_{ph_peak} that follows the empirical equation (2.1):

$$I_{Ph\_peak} = (a \times V + b) \times \alpha_{gauss(x,y)} \times Pulse_w \times S \tag{2.1}$$

where V is the reverse-biased voltage of the exposed PN junction, a and b are constants that depend on the laser power. $\alpha_{gauss(x,y)}$ is a term related to the bivariate distribution of the laser beam amplitude in space, $Pulse_w$ is a term allowing to take into account the laser pulse duration and S is the area of the PN junction. Additional details on the above parameters are provided by [101].

By way of illustration, Fig. 2.3 shows a three-dimensional view of the normalized amplitude of a laser spot. Beam intensity at a given (x,y) represents the amount of power delivered by the laser source at this specific coordinate.

ISBN: 978-2-11-129250-5

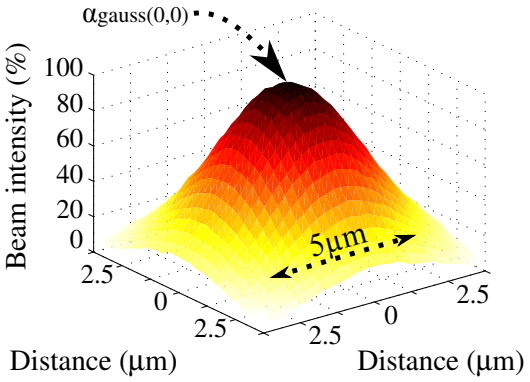


Fig. 2.3: Three-dimensional view of a laser beam in terms of intensity per area. 100% of laser beam intensity represents the epicenter of the laser spot.

When considering the layout of the circuit and the footprint of the laser effect in the illuminated zone, different areas of the circuit are affected with different intensities since the laser effect area is spatially distributed as a bivariate normal distribution (eq. 2.1). In order simulate the effects of a laser considering the layout topology, the current sources (Fig. 2.2) modeling the classical electrical model should be applied with different profiles for each transistor's PN junction. Fig. 2.4 illustrates this process using as example three inverter cells being illuminated by a laser. In this case it is also considered only three points of the laser beam effect. For each of these points, a current source is thus applied with the same width but different amplitudes (I_{Ph_peak}). In Chapter 5 a methodology allowing to simulate laser-induced faults in large-scale circuits will show in details the simulation procedure that takes the circuit layout into account.

ISBN: 978-2-11-129250-5

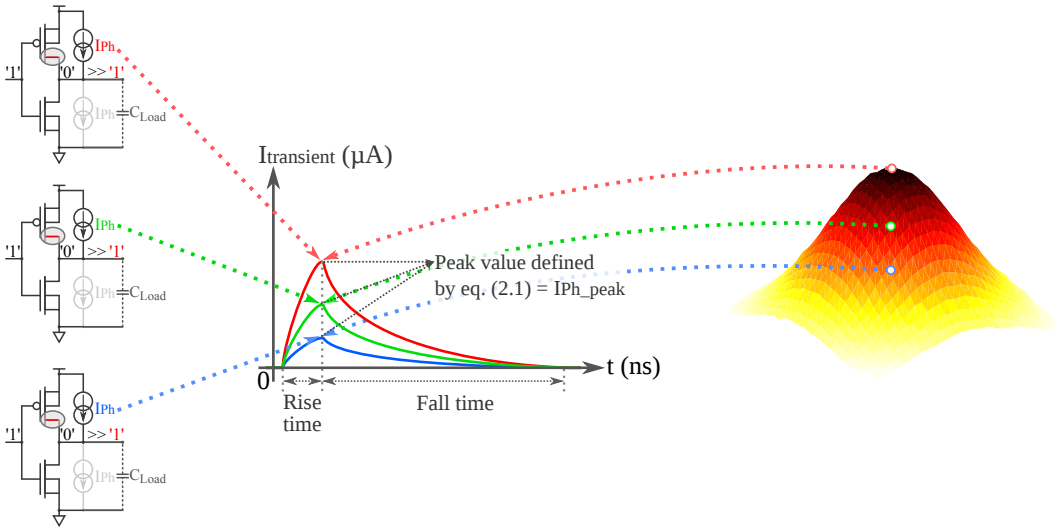


Fig. 2.4: Laser-induced currents modeled by current sources with a double exponential profile. The current amplitude of each current source is defined by eq. (2.1). The current width is always fixed.

2.2 State-of-the-Art Techniques for Concurrent Error Detection

This section gives an overview of different transient-fault detection techniques aiming the protection of integrated systems against TFs provoked in combinational logic blocks. TFs that can be induced by fault injection techniques, such as laser fault injection.

Radiation exposure and environmental variations are able to induce parasitic transient currents in integrated circuits as well as optical sources like laser beams or even flashlights [44, 109]. Laser beams allow finely controlling the injected current thanks to their high spatial and temporal resolutions [16]. The induced transient faults, which are indeed temporarily voltage level modifications, are active only for a short duration of time, and their occurrence are not predictable when caused by the environment. Therefore, TFs need to be detected and corrected at run-time before provoking SEs in stored results of system operations.

Several concurrent error detection (CED) techniques have been proposed [12, 23, 35, 40, 85, 86, 88, 98, 103, 106] with the intent to design more reliable computing systems. In this section, State-of-the-Art CED techniques are classified into four categories: spatial redundancy, temporal redundancy, Transition Detector (TD)-based schemes, and Built-In Current Sensors (BICSs). We could still mention a fifth category – information redundancy – in which its structure is similar to a spa-

ISBN: 978-2-11-129250-5

tial redundancy; however, instead of a copy block, a code prediction block and a coder are added [91]. Furthermore, we highlight the well-known acronym CED is indeed a misuse of language as there exist concurrent detection schemes able to detect TFs not necessarily producing errors. The detection of TFs that are masked – not resulting in hard or soft errors – is also of importance for secure applications. All these approaches are implementable at different abstraction levels of a design. This work is interested on techniques implemented at the hardware level.

This work introduces a simulation-based method for evaluating the effectiveness of Concurrent Error Detection (CED) techniques in identifying transient faults provoked in combinational logic blocks. Typical fault profiles are simulated in campaigns of injections that reproduce output scenarios of fault-affected combinational circuits. Furthermore, a CED technique is proposed and compared to State-of-the-Art strategies by using the method presented herein. Results show the capabilities of all studied techniques by providing a rank in terms of their effectivenesses in detecting transient faults induced in combinational logic circuits, and analyzing the situations in which soft errors are produced in memory elements.

2.2.1 Spatial redundancy

2.2.1.1 Duplication With Comparison

The Duplication With Comparison (DWC) technique [103], illustrated in Fig. 2.5, is conceptually the simplest CED scheme. Based on the principle of spatial redundancy, the outputs $D_{<1>}$ and $D_{<1>}copy$ (duplication of one bit of the circuit's logic) are connected to two D-type Flip-Flops (DFFs), which have their outputs compared by an XOR gate, generating an error signal (Err_1) in case of difference.

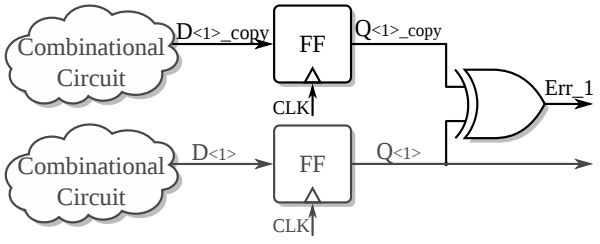


Fig. 2.5: Duplication With Comparison: general scheme.

This type of technique guarantees a high level of error detection. Fig. 2.6 shows an example in which a TF (red) reaches the input of a DFF (signal $D < 1 > \_copy$) without being masked electrically, logically or temporally. The TF is thus captured by the DFF and appears as a soft error (red) at the output $Q < 1 >$. The XOR gate

ISBN: 978-2-11-129250-5

(comparator) raises an error signal Err_1 in order to notify the presence of such an error that could be further processed by an error correction procedure (ECP) in the subsequent clock cycles.

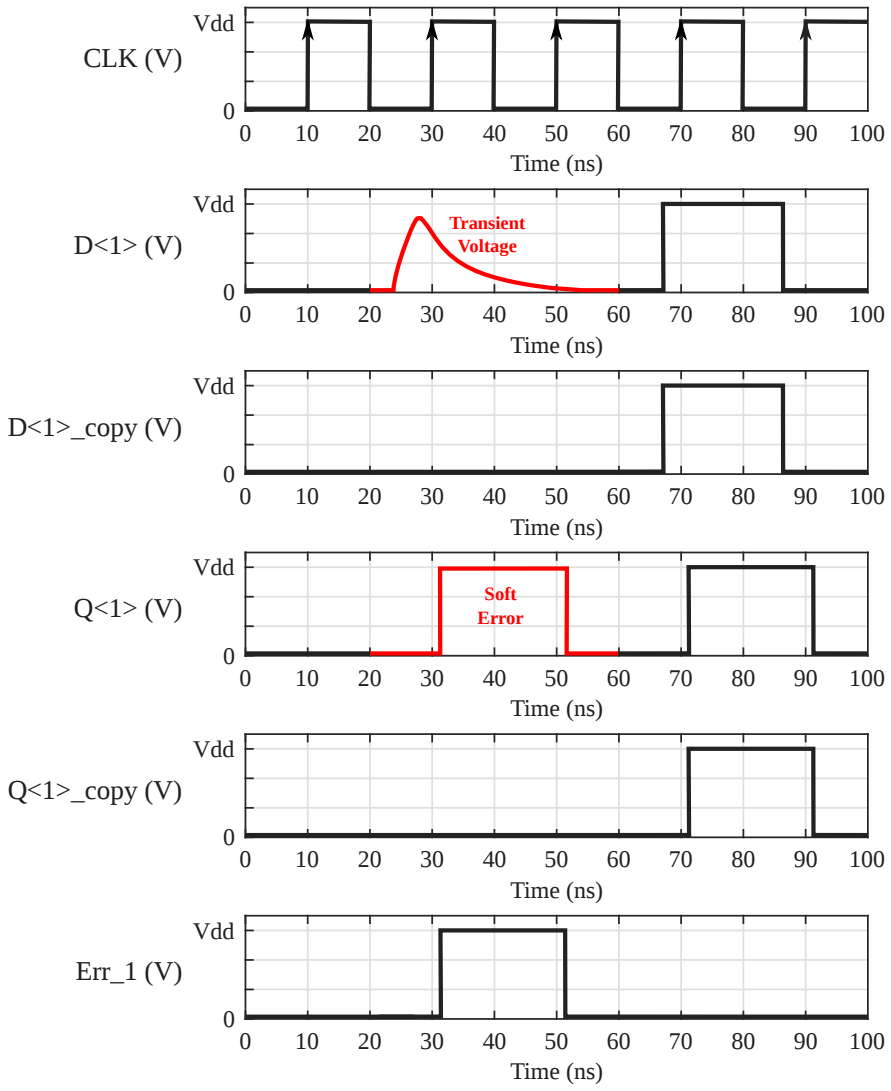


Fig. 2.6: Duplication With Comparison: single induced transient voltage propagation and detection.

ISBN: 978-2-11-129250-5

2.2.2 Temporal redundancy

2.2.2.1 Time Redundancy

The basic idea behind the Time Redundancy (TR) scheme is to repeat twice the same computation with the same hardware at two different instants, and to compare the two results [86].

TR architectures can be implemented at different abstraction levels: system, algorithmic, micro-architectural, logical, or electrical. At system and algorithmic levels, the computation is started with the input data to store the result in a temporary variable, then to repeat the same computation with the same data, and finally to check the results. The system delivers the results only if they are identical. In these cases, the delay between two computations is usually in the order of several clock cycles. Therefore, TR at such abstraction levels can be very effective with low additional area costs but huge and permanent time penalties.

However, in case of logical, and electrical levels, TR architectures can exhibit some issues. In this case, the circuit where TR takes effect is composed of a single combinational logic block. The register at its outputs is duplicated as Fig. 2.7 illustrates. The additional register receives the output data $D < 1 >$ after a delay ($D < 1 >\_delay$). The outputs of the two registers are compared, and in case of discrepancy the circuit raises an error flag (Err_1). The delay between the two computations minus the flip flop's setup time and hold time corresponds to the maximum TF duration that can be detected by this solution.

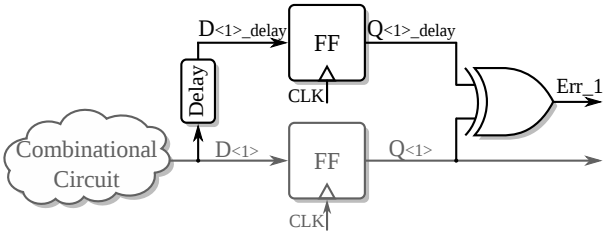


Fig. 2.7: Time Redundancy: general scheme.

Fig. 2.8 details the operation of the TR scheme. In this case, a transient voltage is propagated trough the logic (signals $D_{<1>}$ and $D_{<1>}\_delay$). The signal $D_{<1>}\_delay$ is a delayed copy of the signal $D_{<1>}$. Looking at the output of both flip flops (signals $Q_{<1>}$ and $Q_{<1>}\_delay$), it is possible to observe that the delayed signal is correct and the original signal was temporarily bit flipped due to the transient voltage. Both signals $Q_{<1>}$ and $Q_{<1>}\_delay$ are then compared by an XOR gate and the error signal Err_1 is raised, thus successfully detecting the transient

ISBN: 978-2-11-129250-5

voltage that caused a soft error.

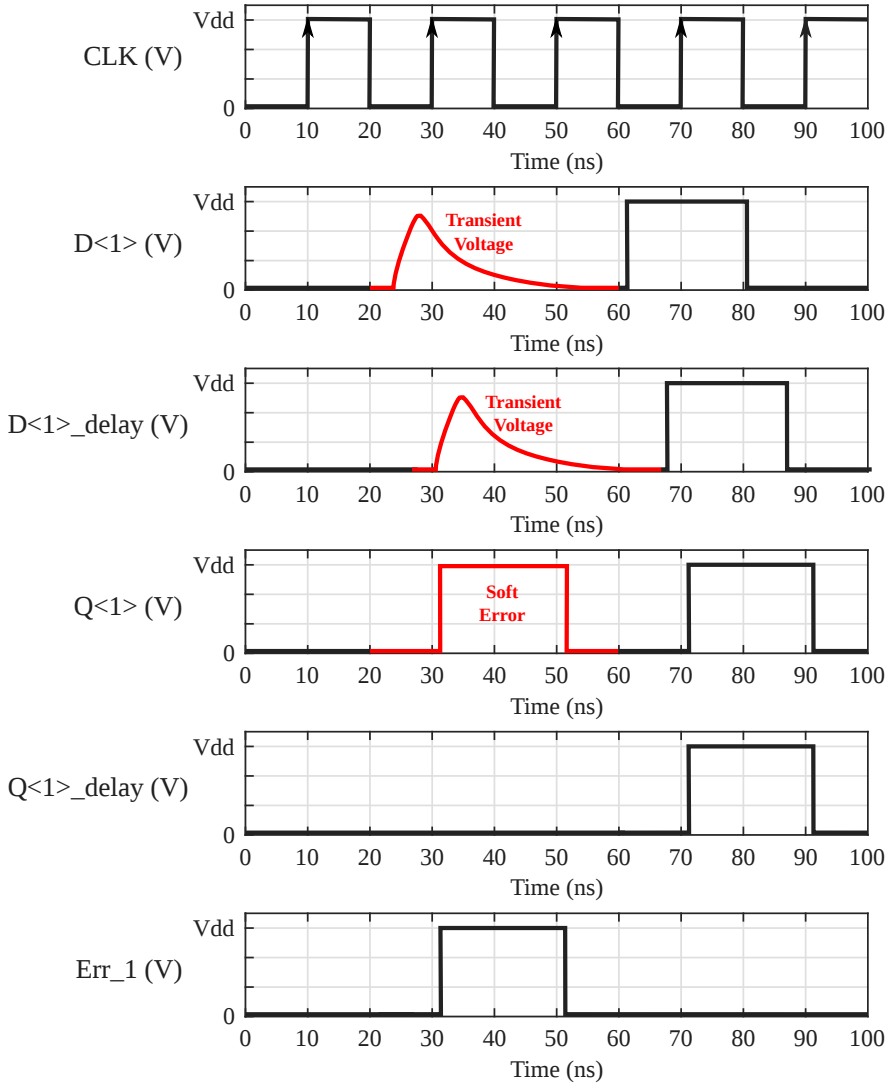


Fig. 2.8: Time Redundancy: single induced transient voltage propagation and detection.

ISBN: 978-2-11-129250-5

2.2.3 Transition Detector

2.2.3.1 RAZOR-II

RAZOR-II [35] is a Transition Detection (TD)-based technique dedicated to detect Delay Errors (DEs) but also the advent of SEs. A TD circuit is a simple circuit with one input and one output. The circuit creates a short pulse when a defined edge, rising, falling, or both depending on the data, is detected.

The architecture and the principle of operation of the Razor-II are illustrated in Fig. 2.9 and Fig. 2.10 respectively. It uses a single positive level-sensitive latch, augmented with a transition-detector controlled by a detection clock generator. The latch output $\overline{Q}_{<1>}$ is connected to a TD block that is thus able to detect TFs. A legitimate transition occurs when data is setup to the latch input before the rising edge of the clock. In this case, the output $Q_{<1>}$ of the latch transitions at the rising edge after a delay equal to the CLK-to-Q delay of the latch, to reflect the state of data being captured. In order to prevent legitimate transitions being flagged as timing errors, a short negative pulse (signal DC) on the detection clock is used to disable the transition detector for at least the duration of the CLK-to-Q delay after the rising edge.

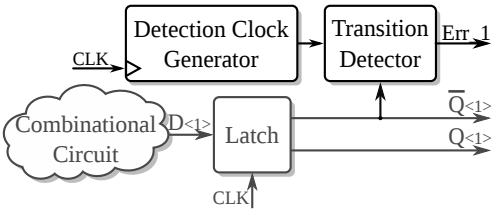


Fig. 2.9: Razor-II: general scheme.

ISBN: 978-2-11-129250-5

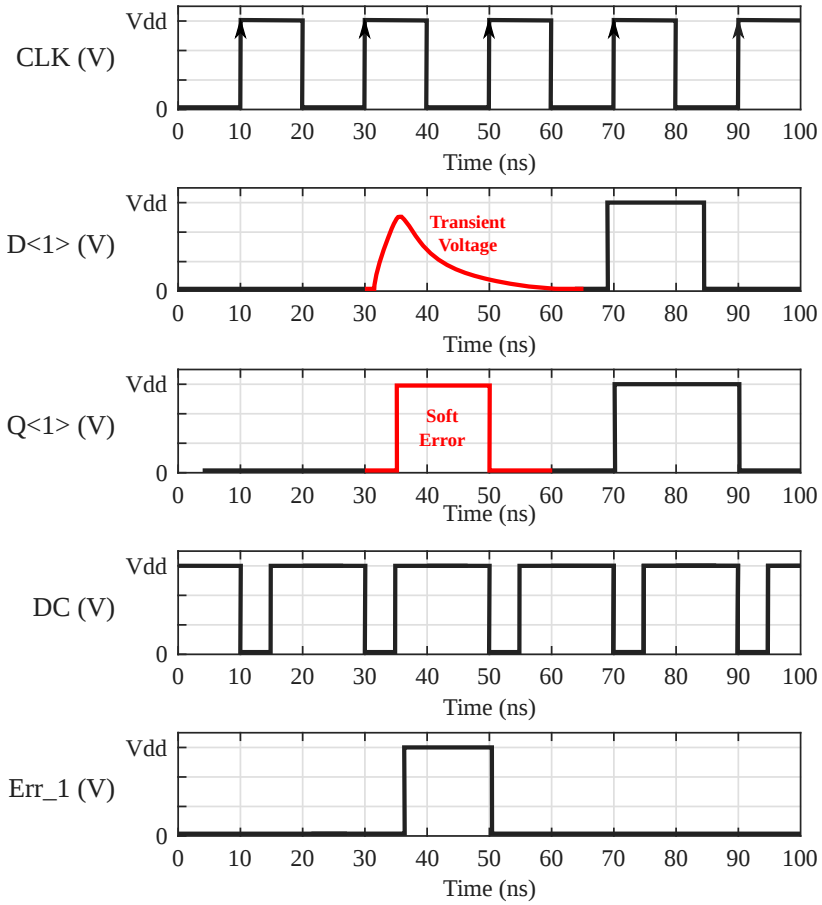


Fig. 2.10: Razor-II: single induced transient voltage propagation and detection.

2.2.3.2 Transition Detector With Time Borrowing

This technique [23] is similar to Razor-II. The Transition Detector With Time Borrowing (TDTB) consists in the coupling of a latch and a TD as illustrated in Fig. 2.11.

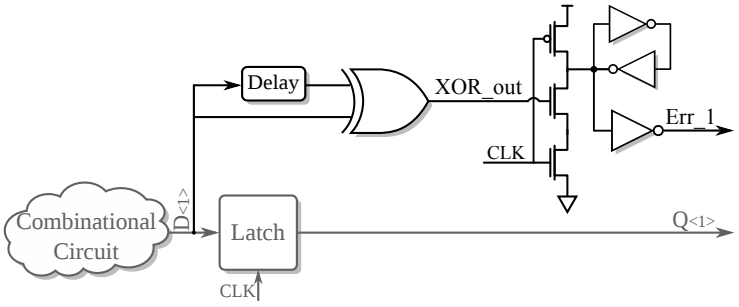


Fig. 2.11: Transition Detector With Time Borrowing: general scheme.

Fig 2.12 illustrates the operation of TDTB. The transition detector raises the error signal Err_1 for any input transitions (XOR_{out}) during the high state of the

ISBN: 978-2-11-129250-5

clock ($\overline{CLK}$), thus requiring the signal $D_{<1>}$ to be stable before the high level of the clock. It is also possible to detect transient voltages during the low state of the clock by using CLK instead of $\overline{CLK}$ at the input of the latch. In this case, the signal must be stable after the high level of the clock.

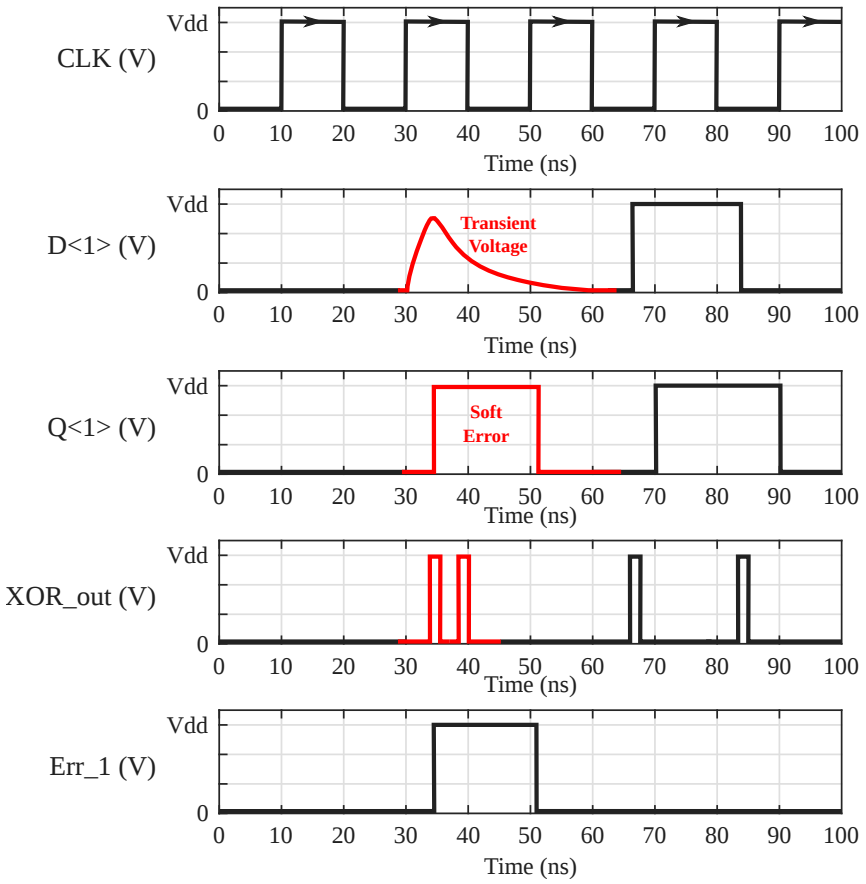


Fig. 2.12: Transition Detector With Time Borrowing: single induced transient voltage propagation and detection.

ISBN: 978-2-11-129250-5

2.2.3.3 Double Sampling With Time-Borrowing

This technique [23] presented in Fig. 2.13 is similar to the TDTB scheme although a shadow master flip-flop (MFF) replaces the TD block.

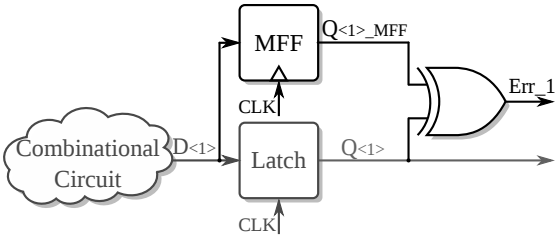


Fig. 2.13: Double Sampling With Time-Borrowing: general scheme.

An illustration of the operation mode of Double Sampling With Time-Borrowing (DSTB) in presented in Fig. 2.14.

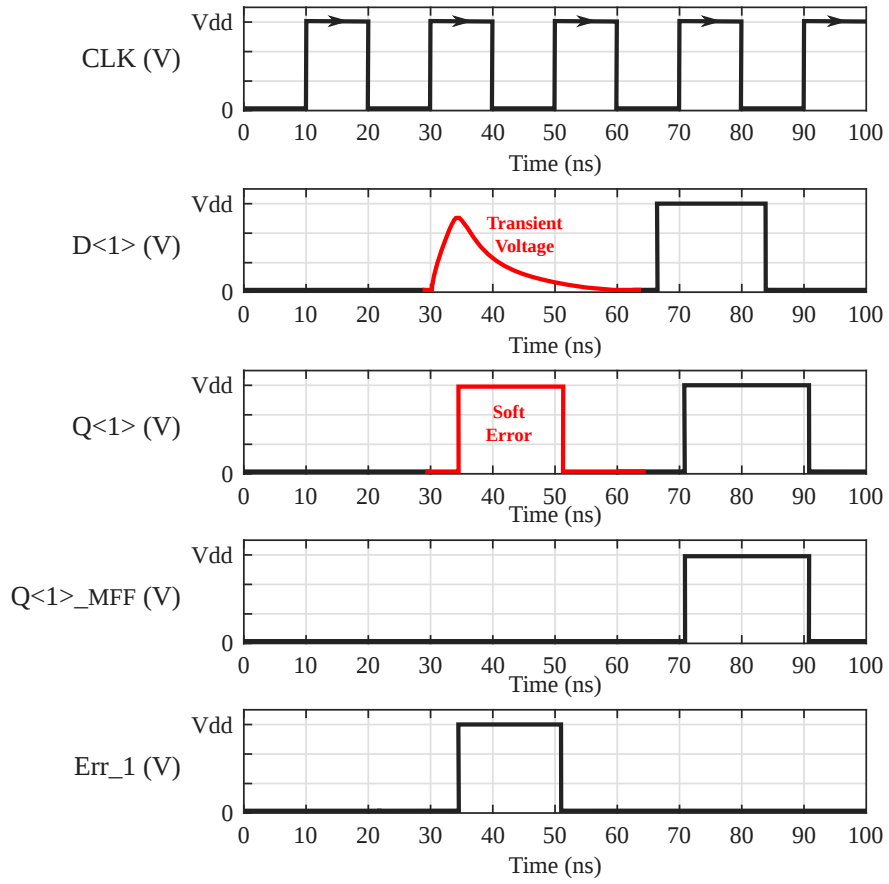


Fig. 2.14: Double Sampling With Time-Borrowing: single induced transient voltage propagation and detection.

As shown in Fig. 2.14, DSTB double samples signal $D_{<1>}$ and compares the latch and shadow flip-flop outputs ($Q_{<1>}$ and $Q_{<1>\_MFF}$) to generate the error sig-

ISBN: 978-2-11-129250-5

nal. Furthermore, DSTB retains the time-borrowing feature of TDTB to eliminate metastability.

2.2.3.4 Transient Fault Monitoring Scheme

The Transient Fault Monitoring Scheme (TFMS) was proposed by [98] aiming the detection of TFs affecting the DFF input such as signal $D_{<1>}$[1] in Fig. 2.15. As shown in this figure, this scheme includes a *Transition Detector* (TD) made by an XOR gate and a delay block. The TD block generates a high signal when there is a TF inside the *Detection Window* (signal DW). The *Sticky Block* is used to validate TFs occurring only when the signal DW is at its high state. The *Sticky Block* is also used to merge the error signal (Err_1) since the TD produces two pulses.

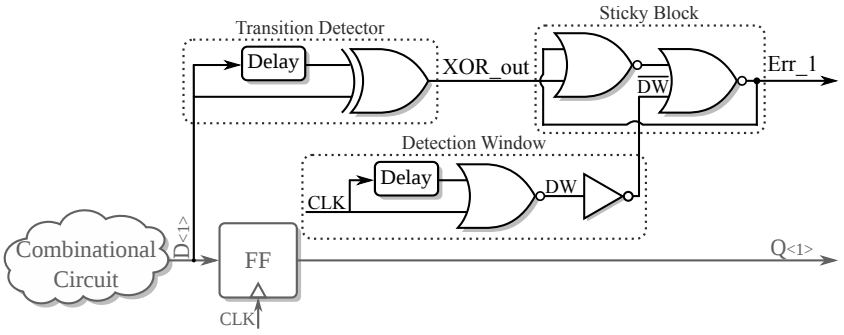


Fig. 2.15: Transient Fault Monitoring Scheme: general scheme.

The operation mode of TFMS is illustrated in Fig. 2.16. In this example a transient voltage is observed on signal $D_{<1>}$. This transient induces a soft error on signal $Q_{<1>}$ as it is sampled by the flip flop. Since the transient voltage is rising when DW is at V_{DD}, the error signal Err_1 is raised indicating a fault.

[1] $D_{<1>}$ represents 1 bit of N bits of a system.

ISBN: 978-2-11-129250-5

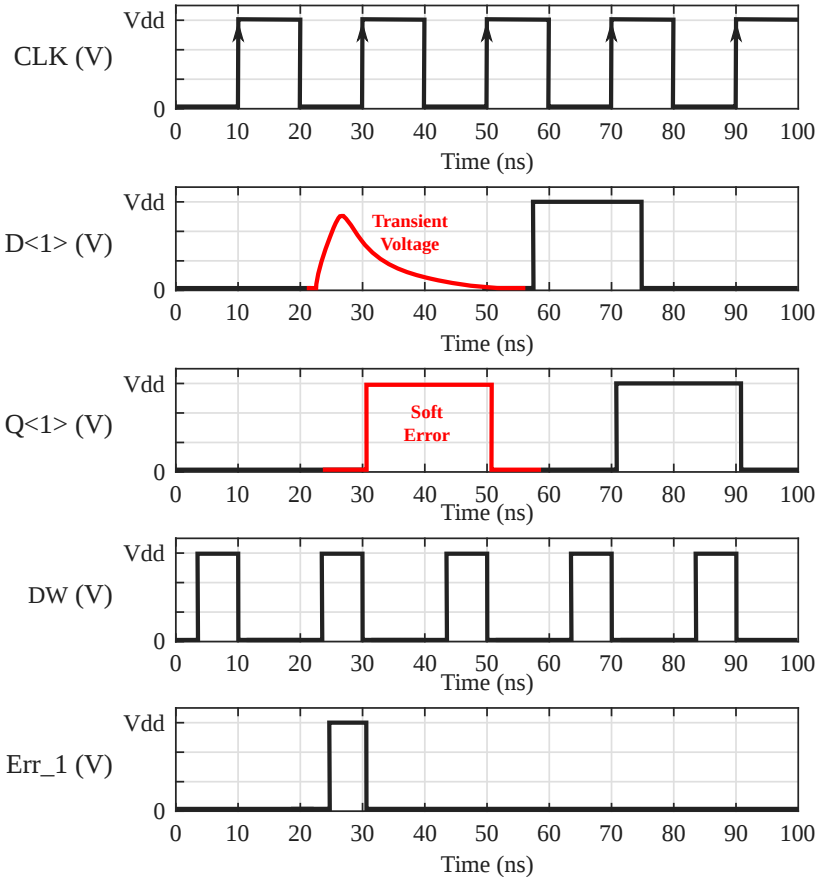


Fig. 2.16: Transient Fault Monitoring Scheme: single induced transient voltage propagation and detection.

2.2.4 Bulk Built-In Current Sensors

2.2.4.1 Single Bulk Built-In Current Sensor

The Single Bulk Built-In Current Sensor (SBBICS) architecture is based on the principle of Built-In Current Sensors (BBICS) proposed by [85], which is designed to monitor radiation- or laser-induced transient currents passing through the bulk of transistors. SBBICS allows monitoring simultaneously pull-up and pull-down CMOS networks [40, 92]. Fig. 2.17 shows the SBBICS connection scheme where the bulks of monitored transistors ($Bulk\_N$ and $Bulk\_P$) are tied to SBBICS instead of G_{ND} and V_{DD} directly. SBBICS will thus be responsible to provide the correct biasing for the bulk of the monitored transistors.

Fig. 2.18 shows the SBBICS CMOS schematic view. The circuit mainly comprises two cross-coupled inverters to perform the function of an asynchronous latch. When the system operates in normal conditions, node *out* stays at '0' (G_{ND}), however, when a fault is detected, node *out* is set to '1' (V_{DD}). The SBBICS connection

ISBN: 978-2-11-129250-5

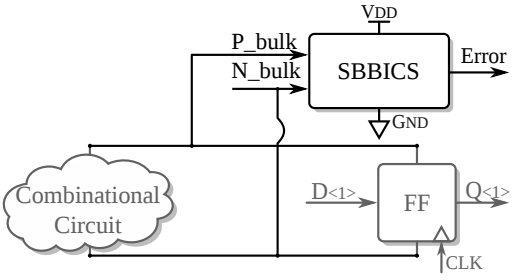


Fig. 2.17: Single Bulk Built-In Current Sensor: circuit monitored by the current sensor.

to the bulks of the monitored transistors ($Bulk\_N$ and $Bulk\_P$ in Fig. 2.17) is used as a bias contact to G_{ND} and V_{DD} through transistors M_{N1} and M_{P1} respectively. When there exists an induced current flowing through the PN junction of the sensitive NMOS or PMOS transistors, this current is perceived in the input of the sensor (N_Bulk or P_Bulk in Fig. 2.18). Since this current flows through the drain of transistor M_{N1} or M_{P1}, the voltage in node N_Bulk goes from 0 V to +$V_{transient}$ and the voltage in node P_Bulk goes from V_{DD} to V_{DD}-$V_{transient}$, thus transistors M_{N2} or M_{P2} enter in the saturation region of operation making the latch to flip its value, i.e., node out change its value from '0' (G_{ND}) to '1' (V_{DD}) indicating a fault. Transistors M_{N_t} and M_{P_t} are passing transistors used to provide a voltage drop and thus facilitate the flipping of the latch state. Finally, transistors M_{N_rst} and M_{P_rst} are used to reset the latch to the initial condition after a fault is detected.

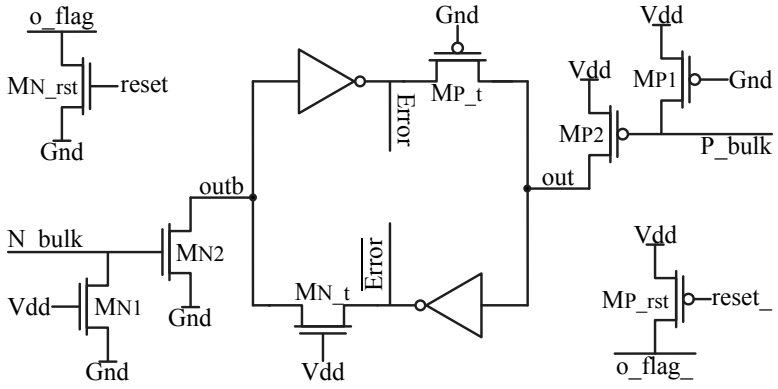


Fig. 2.18: Single Bulk Built-In Current Sensor: CMOS schematic view.

The basic operation of SBBICS is illustrated in Fig. 2.19. Since the bulk of the monitored PMOS and NMOS transistors are not connected directly to the ground/power supply, SBBICS is responsible for providing it. In this way, all current passing through SBBICS is monitored (signals P_Bulk and N_Bulk) and a flag (signal $Error$) is raised indicating a fault. Whether SBBICS is capable or not

ISBN: 978-2-11-129250-5

to detect the induced transient current depends exclusively on its sensitivity threshold (or detection threshold). Signal *Error* stays at V_{DD} until the *Reset* signal is applied.

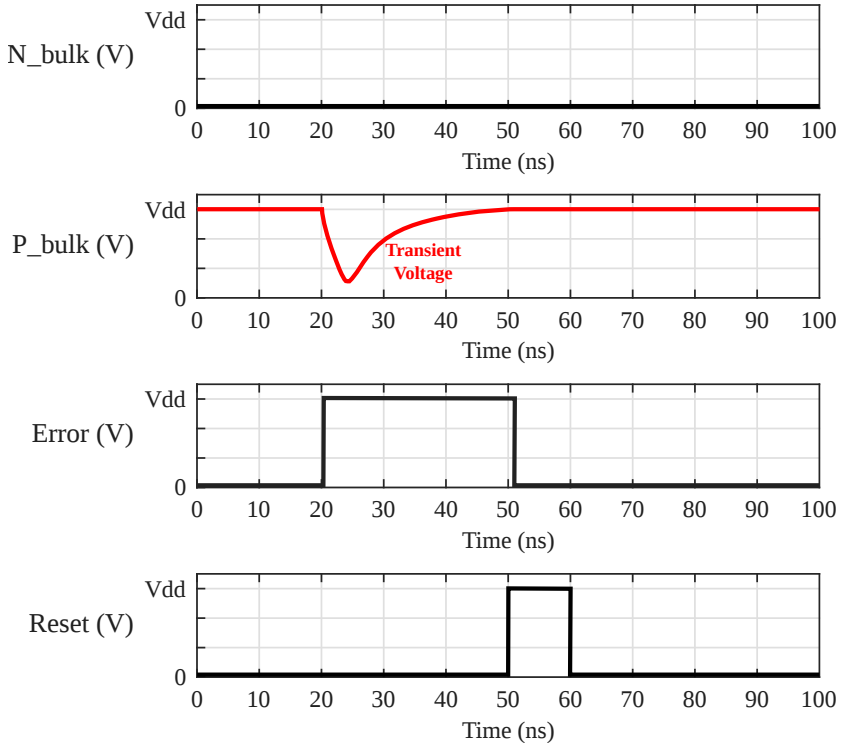


Fig. 2.19: Single Bulk Built-In Current Sensor: Single induced transient voltage occurrence and detection.

2.2.4.2 Dynamic Bulk Built-In Current Sensor

The Dynamic Bulk Built-In Current Sensor (DBBICS) [106] operates similarly to SBBICS, although it features a dynamic memory cell. Fig. 2.20a depicts the basic scheme for a version of DBBICS intended to monitor NMOS transistors (another complementary DBBICS is required to monitor PMOS transistors).

Fig. 2.20 shows the DBBICS CMOS schematic. At the beginning, P0 is switched ON by $\overline{Reset}$ signal and briefly shorts P1 gate to V_{DD}, thus ensuring P1 is OFF. N2 acts as a load for P1, setting signal *Error* to '0' (G_{ND}). Transistor N0 acts as a sensing resistor. The voltage drop over N0, caused by the induced transient current in the bulk of the monitored transistors, activates N1 when that voltage is greater than the threshold voltage of N1. Conduction of N1 connects P1 gate to ground, charging its gate-source capacitance up and turning P1 ON. Once P1 goes to ON state, signal *Error* is set to '1' (V_{DD}) because P1 has a higher current driving

ISBN: 978-2-11-129250-5

capability than the "always ON" transistor N2.

N1 goes OFF when Ibulk returns to its normal value after the current pulse vanishes. Since there is no DC path to allow discharging of gate charge, P1 remains ON until P0 is turned ON again by the $\overline{Reset}$ signal (which must be periodic), sent by the system as soon as the $Error$ signal is acquired and recognized. Thus, N1 discharges P1 gate charge and forces P1 to OFF state. Fig. 2.21 depicts a typical set of waveforms for DBBICS in operation.

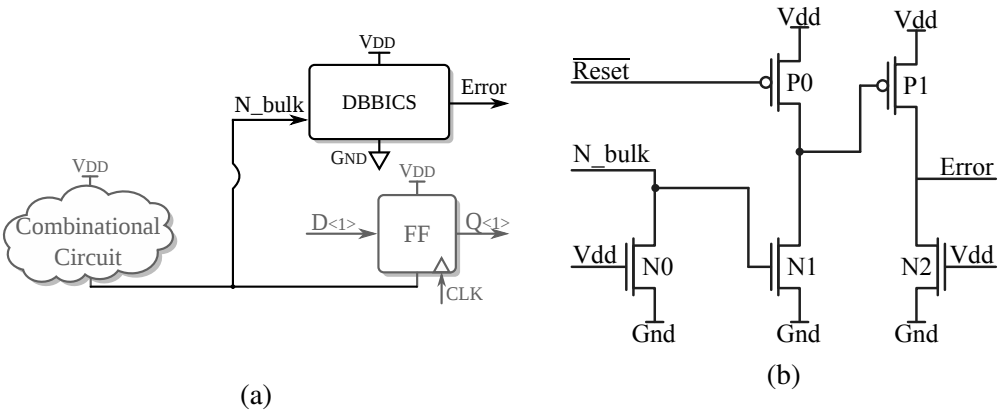


Fig. 2.20: Dynamic Bulk Built-In Current Sensor architecture: (a) Circuit monitored by the current sensor (b) CMOS schematic.

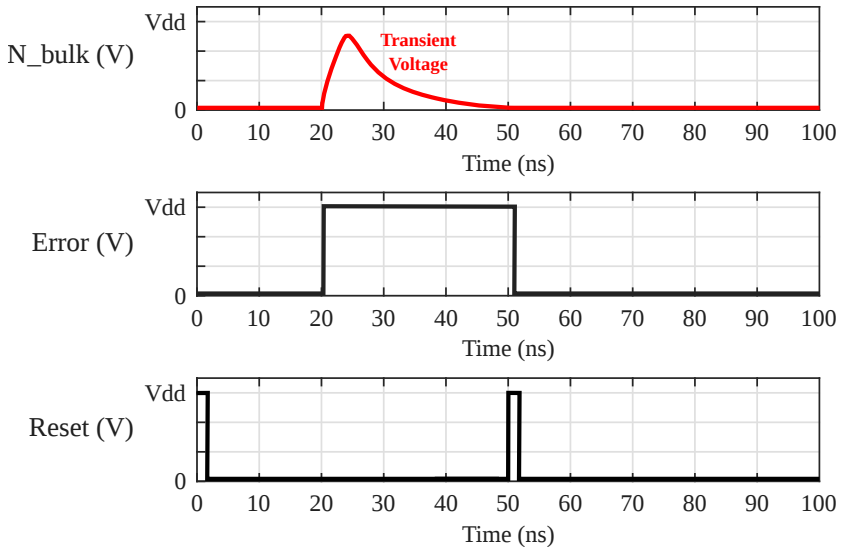


Fig. 2.21: Dynamic Bulk Built-In Current Sensor: single induced transient voltage occurrence and detection.

ISBN: 978-2-11-129250-5

2.3 Summary

By focusing the studies on laser fault injection, this chapter presented in Section 2.1 a detailed background on the effects of laser illumination on ICs. In addition, several techniques for concurrent error detection were also reviewed in Section 2.2.

The next chapter introduces a simulation-based method for evaluating the effectiveness of the CED techniques in identifying transient faults provoked in combinational logic blocks. Typical fault profiles are simulated in campaigns of injections that reproduce output scenarios of fault-affected combinational circuits. Furthermore, another CED technique is proposed and compared to State-of-the-Art strategies by using the method presented in the next chapter. Results show the capabilities of all studied techniques, providing a rank in terms of their effectivenesses in detecting transient faults induced in combinational logic circuits, and analyzing the situations in which soft errors are produced in memory elements.

ISBN: 978-2-11-129250-5

Chapter 3

Effectiveness of Concurrent Error Detection Techniques in Identifying Transient Faults

Several CED techniques were reviewed in the last chapter (Section 2.2). These techniques mainly differ in their detection capabilities and in the constraints they impose on the system design. This chapter presents a simulation-based method to evaluate and to compare different detection techniques regarding their effectivenesses in detecting TFs arisen in combinational logic blocks and resulting in SEs. The method proposes 32 different scenarios of TF injection. Results of all detection techniques studied here are summarized in a table that provides a direct insight of the effectiveness of each technique. Furthermore, in this chapter, another CED technique is introduced and compared among the other techniques. It uses an effective Transition Detector (TD) and a controllable adaptive detection window (DW). As a result, the introduced technique offers increased SE detection capability but also allows the detection of Delay Errors (DEs).

Section 3.1 of this chapter details the proposed CED technique. In the following, Section 3.2 presents the method for evaluating the effectiveness of CED techniques. Section 3.3 gives simulation results and Section 3.4 provides a comparative analysis of the CED techniques.

The works reported in this chapter were presented in the European Symposium on Reliability of Electron Devices, Failure Physics and Analysis (ESREF) 2017 and published in the international journal Microelectronics Reliability 2017 [3].

ISBN: 978-2-11-129250-5

3.1 Proposed Concurrent Error Detection Technique

The technique presented in this section is proposed to improve the effectiveness of TD-based schemes at detecting transient faults. The operation mode is similar to [98] (Section 2.2.3.4). However the devised 1-bit TD circuit is formed by a latch instead of the delay block suggested in [98], as Fig. 3.1 shows. In addition, our proposition combines the error signals of each 1-bit TD circuit (Err_1 to Err_N) with the help of a single dynamic OR gate (Fig. 3.2), and not using parity trees (i.e. XOR trees) that may electrically filter TFs and prevent the possibility of detecting them.

The proposed TD circuit and dynamic OR gate are particularly activated during a Detection Window (DW) in which the monitored combinational circuit's output $D_{<1>}$ (i.e. D-type Flip-Flop (DFF) input) is prone to present TF-induced illegal transitions. Therefore, any abnormal transition at $D_{<1>}$ within DW would be detected. We denote our technique herein as Latch Based Transient-Fault Detection (LBTFD). The scheme in Fig. 3.3 is used to create the signal called DW.

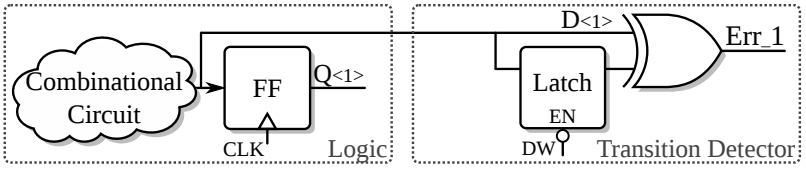


Fig. 3.1: The proposed scheme for detecting transient faults that result in illegal transitions at combinational circuit's outputs like the bit $D_{<1>}$.

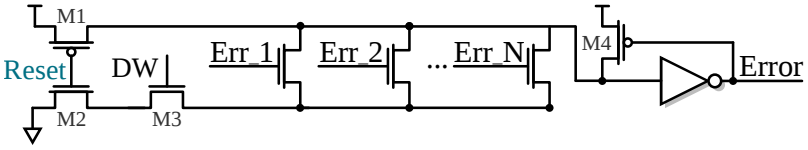


Fig. 3.2: Dynamic OR gate for combining error signals from transition detector circuits.

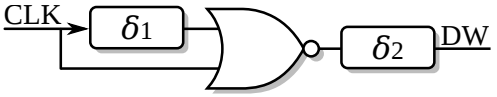


Fig. 3.3: Detection window generator.

One of the advantages in using a latch as a TD is that only one pulse is generated by the error signal output. In the case of a TD, as the one used in [98], the transition

ISBN: 978-2-11-129250-5

detection block produces two pulses, therefore, needing to resort to an additional block to merge the two generated pulses. A second advantage is the ability to detect TFs also during the hold time (thus TFs inducing SE). An additional increase in $\delta 2$ will permit the detection to cover all SEs and DEs. Furthermore, the use of a latch in a TD will guarantee the detection of TFs in recent technologies since TDs using inverters connected to a XOR gate [23] need an increased delay in order to be triggered, thus, having more static power consumption and higher area overhead.

3.1.1 Defining the Detection Window

In order to choose a proper configuration for Detection Window (DW), Fig. 3.4a refers to a data-path with a clock period denominated clk_per. Labels t_{setup} and t_{hold} define the DFF setup and hold times respectively. The setup time is the minimum amount of time before the clock edge during which the signal D must be valid and steady, whereas the hold time is the minimum amount of time after the clock edge during which the signal D must be valid for a correct operation of the DFF. δ_{DW} is the time overhead due to the DW. According to the width of TFs (TF_W), the width of the DW (DW_{width}) can be designed in a way in which only faults resulting in SEs are detected:

$$DW_{width} = (t_{setup} + t_{hold}) \tag{3.1}$$

The width of DW (DW_{width}) can also be designed in a way in which TFs resulting or not in SEs are detected:

$$DW_{width} = (t_{setup} + t_{hold}) + \delta_{DW}. \tag{3.2}$$

Note that, the greater the δ_{DW} (lower $\delta 1$ in Fig. 3.3), the earlier the signal D must be steady. Indeed it must reach its final steady state $(t_{setup} + \delta_{DW})$ before the rising clock edge. For a DW configuration as the one in Fig. 3.4a the maximum operating clock frequency of the circuit is penalized, however, $\delta 2$ allows the detection window generator to shift DW meanwhile maintaining its same width as can be seen in Fig. 3.4b, thus allowing an increased operation frequency of the circuit. In fact there are many ways to design DW to cope with timing specifications. The main advantage in having $\delta_{DW} \neq \emptyset$ is the possibility to detect of transient faults with $TF_W \leq (t_{setup} + t_{hold} + \delta_{DW})$ that will cause a SE as DW will also cover the t_{hold} time. Note that, if the TF width is larger than the designed DW, a few SEs will pass undetected by LBTFD.

ISBN: 978-2-11-129250-5

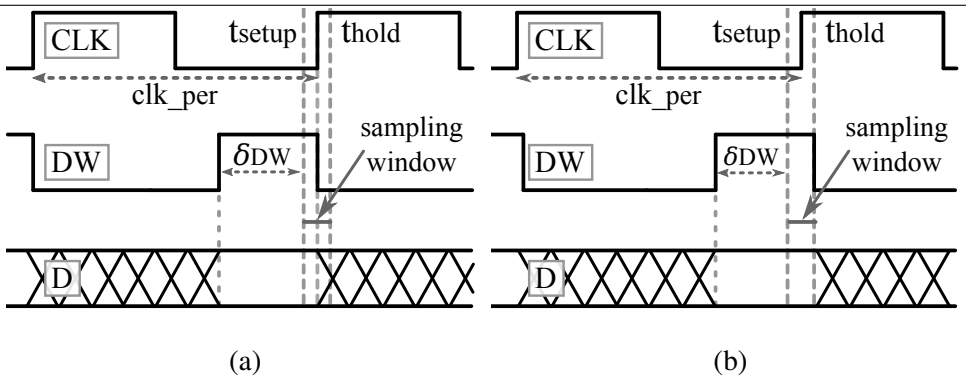


Fig. 3.4: Detection window configuration: (a) $\delta 1 \neq 0$ and $\delta 2 = 0$ (b) $\delta 1 \neq 0$ and $\delta 2 \neq 0$.

3.1.2 Verification by Electrical Simulation

The operation of the proposed technique was verified by electrical simulation to detect the advent of a single induced transient fault arriving at node D as presented in Fig. 3.5. The simulation was performed in a FD-SOI 28 nm technology with V_{DD} = 1 V. The magnitude of the injected transient current was such that it creates a transient voltage with an amplitude equivalent to 100 % of V_{DD}, i.e., 1 V. The rise time was shorter than the fall time to keep the traditional shape of transient faults [30]. The consequent induced transient fault width was around 150 ps. The transient current was injected from the PMOS sensitive drain to its Nwell bulk, i.e., the current was applied when signal D was steady at 1 V. It could be clearly noted that any variation inside the DW is sufficient to trigger the error signal independently of its polarity (rising or falling). Therefore, any fault occurring in the NMOS or PMOS sensitive drains within the DW is detectable.

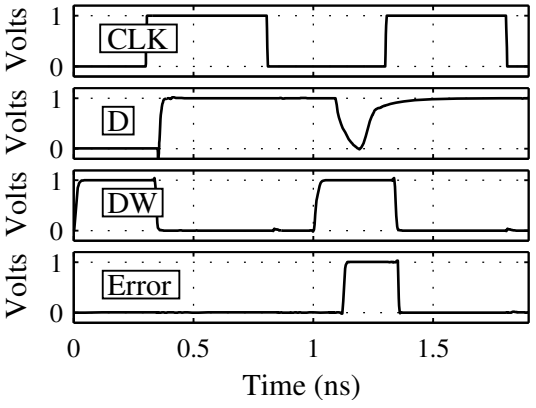


Fig. 3.5: Electrical simulation of the proposed technique detecting a single TF (width of around 150 ps) injected on node $D_{<1>}$.

ISBN: 978-2-11-129250-5

3.2 Method for evaluation of Concurrent Error Detection Techniques

The method proposed in this section evaluates the effectiveness of the CED techniques (section 2.2 and 3.1) in detecting single TFs by taking into account four facts:

- (1) the harmful consequence of TFs induced in a combinational circuit under protection of a CED circuitry is the generation of a SE in one or several DFFs;
- (2) TFs induced inside a combinational circuit (in the worst case) propagate up to an input $D_{<1>}$[1] of one or several DFFs flipping their bits (SEs);
- (3) TFs partially or fully propagated up to $D_{<1>}$ produce a profile of TF on $D_{<1>}$ that is perfectly representable by profiles of single TFs injected directly on $D_{<1>}$; and
- (4) TFs induced inside a combinational circuit and fully mitigated by a logical or electrical masking effect [60] has no effect on $D_{<1>}$. These TFs are indeed attenuated by the target combinational circuit, and not by the CED technique protecting it.

With these four TF-related facts in mind, the evaluation of the CED technique effectiveness can be simplified by injecting TFs only on $D_{<1>}$. Furthermore, as the goal is to evaluate the degree to which a CED technique is successful in detecting TFs —and not the ability of the target combinational circuit in masking TFs— the logic function of the target combinational circuit is not relevant. Latching-window masking effects, otherwise, have to be considered because the sampling window of DFFs is directly related to the design of most CED techniques included into systems synchronized by a clock.

The proposed simulation-based method applies, therefore, only on $D_{<1>}$ a double exponential current source with parameters configurable in function of the classical model of transient faults. Diversified profiles of single TFs are thus injected on $D_{<1>}$ at different times, and the results of the TF-injection campaigns are synthesized through evaluation metrics.

[1] $D_{<1>}$ represents 1 bit of N bits, e.g., a system of 32 bits would require the inclusion of 32 CED circuitries.

ISBN: 978-2-11-129250-5

3.2.1 Description of simulation experiments

In order to simulate the effects of single TFs on a complex system, the critical path of an ARM 7 processor, designed in a commercial FD-SOI 28-nm technology, has been extracted as this is potentially the critical part of the system. Fig. 3.6 summarizes the extracted data path represented by the *ARM 7 Critical Path* block connected to the input $D_{<1>}$ of a DFF.

Two current sources are shown in Fig. 3.6 because depending on the input $Di_{<1>}$ of the *ARM 7 Critical Path* block, the injected transient current will follow a path from the NMOS sensitive drain to its Pwell bulk or from the PMOS sensitive drain to its Nwell bulk.

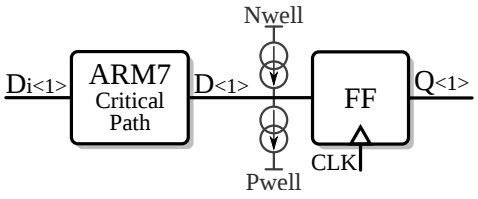


Fig. 3.6: Simulated circuit: the critical path of an ARM 7 processor in a commercial FD-SOI 28-nm technology.

3.2.2 Profiles of Injected Transient Faults

Campaigns of single current injection reproduce 32 scenarios having different profiles of TFs: transient faults with different widths, different amplitudes, and different polarities. Additionally, the slack time of the simulated circuit is changed to verify how a timing path with a different slack behaves when submitted to diverse TF profiles. The rise times of the injected double exponential current sources have been set on the order of 5 ps to keep the typical shapes of TFs: short rise time and longer fall time [38, 42]. For each scenario, a total of one thousand TFs were injected across a clock period of 1 ns, resulting in a simulation step of 1 ps.

The 32 scenarios are summarized in Table 3.1. By considering a simulation start time of 0 ns, the TF start column represents the instant at which the first transient fault begins to be injected on node $D_{<1>}$. Note that the combination of each column in the table comprises a different scenario, resulting in a total of 32 scenarios, for instance, the eight scenarios in the first row (1, 2, 9, 10, 17, 18, 25 and 26) have the following configurations: TF width of 10 ps, TF start at 0.2 ns or 0.58 ns, sensitive drain of PMOS or NMOS and TF amplitude of 60% V_{DD} or 100% V_{DD}.

ISBN: 978-2-11-129250-5

Table 3.1: Profiles of injected TFs

Scenario	TF width	TF start	Sensitive Drain	TF amplitude
1, 9, 17, 25 2, 10, 18, 26	10 ps	0.20 ns	PMOS	60 % of V_{DD}
3, 11, 19, 27 4, 12, 20, 28	50 ps			
5, 13, 21, 29 6, 14, 22, 30	200 ps	0.58 ns	NMOS	100 % of V_{DD}
7, 15, 23, 31 8, 16, 24, 32	450 ps			

3.2.3 Analysis of Injected Transient Fault Effects

The injection of single TFs on $D_{<1>}$ is able to induce four effects:

- (1) TFs that completely overlap the sampling window always produce a SE in the DFF [84];
- (2) TFs that rise and fall inside the sampling window are either masked or they cause a DE or a SE;
- (3) TFs that partially overlap with the sampling window provoke a CLK→Q time variation, i.e. a DE;
- (4) TFs that do not overlap with the sampling window are always masked [84].

In order to evaluate the proposed scenarios in function of time and their consequences, Fig. 3.7 defines three color bars in a rage of 1000 points as the simulation step is 1 ps and the clock period is 1 ns. Each point represents the moment at which the transient fault begins. In this case each color corresponds to:

- Green color bar: Masked Fault (MF): the injected single TF do not perturb the output Q of the monitored DFF, i.e. no SE is induced.
- Blue color bar: Delay Error (DE): the injected single TF increases the CLK→Q delay of the DFF by more than 10% with regard to the typical CLK→Q delay under normal operation.
- Red color bar: Soft Error (SE): the injected single TF provokes a SE.

ISBN: 978-2-11-129250-5

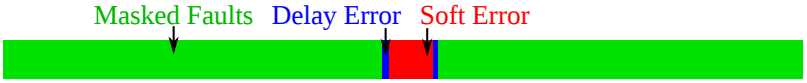


Fig. 3.7: Definition of color bars for masked faults (green), delay errors (blue) and soft errors (red).

Figure 3.8 shows, for each considered scenario the clock signal CLK, the monitored data signal $D_{<1>}$ and the color bars representing the behavior of eight scenarios regarding the TF profile. Note that, due to the different slack time values, the earliest TF for each scenario are injected at a specific time. For scenario 1, the TF begins at 0.2 ns, the same instant in which the signal $D_{<1>}$ reaches its high voltage level (1 V), however, for scenario 2, the TF begins at 0.58 ns since, due to a different slack time value, signal $D_{<1>}$ has its high voltage level at this time. For the others scenarios, the same principle applies, i.e., for each scenario there is a difference in the slack time provided, in the TF polarity, in the width, or in the amplitude of the TF. It can be noted that the number of SEs caused in each scenario is highly dependent on the width of the injected transient fault.

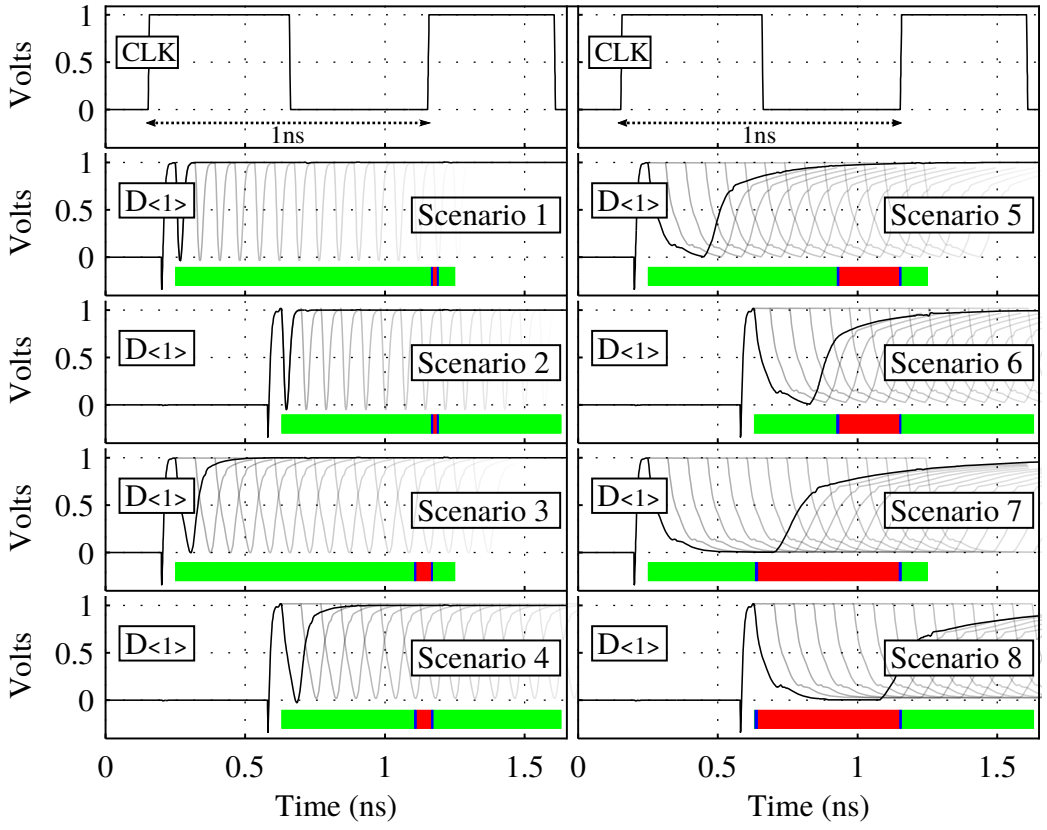


Fig. 3.8: Fault injection scenarios and color bars for masked faults, delay errors, and soft errors.

ISBN: 978-2-11-129250-5

3.2.4 Evaluation metrics

Figures of merit are defined herein to better compare and quantify the effectiveness of the CED techniques. For a total of 1000 single TFs of a scenario, the first metric below measures how many times the CED technique has detected the injected single TF:

$$TF_{\ Detection\ Ratio} = \frac{\#TF_{detected}}{\#TF_{injected}} \tag{3.3}$$

where $\#TF_{detected}$ represents the number of detected TFs by the CED technique for a particular scenario and $\#TF_{injected}$ represents the number of injected TFs, in this case, 1000.

The second and third metrics measure the CED technique effectiveness in detecting injected single TFs that induce SEs and DEs, respectively:

$$SE_{\ Detection\ Ratio} = \frac{\#SE_{detected}}{\#SE_{induced}}. \tag{3.4}$$

$$DE_{\ Detection\ Ratio} = \frac{\#DE_{detected}}{\#DE_{induced}}. \tag{3.5}$$

$\#SE_{detected}$ and $\#DE_{detected}$ represent the number of detected SEs and DEs, respectively, by the CED technique for a particular scenario. $\#SE_{induced}$ and $\#DE_{induced}$ represent the number of TFs causing a SE or a DE. In this case, the number of induced SEs or DEs varies for each scenario as it directly depends on the width of the injected TF.

The fourth metric measures how many times the CED technique is able to detect an injected single TF that induces a SE or a DE:

$$SE + DE_{\ Detection\ Ratio} = \frac{(\#SE + \#DE)_{detected}}{(\#SE + \#DE)_{induced}}. \tag{3.6}$$

Finally, global metrics are defined by taking into account all the 32 scenarios described in previous subsections, and not only a specific scenario as the evaluation metrics 3.3, 3.4, 3.5, and 3.6 do consider. These global metrics are formalized as the arithmetic mean of the results over 32 scenarios, or if S is the total number of scenarios and $X_{\ Detection\ Ratio}$ is one of the evaluation metrics 3.3, 3.4, 3.5, and 3.6, we have:

$$X_{\ Detection\ Ratio\ Global} = \frac{\left(\sum_{i=1}^{S} X_{\ Detection\ Ratio[i]}\right)}{S} \tag{3.7}$$

ISBN: 978-2-11-129250-5

3.3 Simulation results and comparative analysis

Simulation results and comparative analysis of the CED techniques described in previous sections are provided herein by using the proposed evaluation method detailed in section 3.2.

3.3.1 A Comparative analysis

Comparative results are analyzed in this subsection for scenario 5 of the method described in section 3.2, i.e. TFs on NMOS with 200 ps of width and amplitude of V_{DD} (cf. Table 3.1). Fig. 3.9 shows the instants at which a TF with such a profile starts to be formed and a CED technique is able to detect it (orange) or not (light gray). The rising edge of the clock happens at 1.2 ns. The orange color means, therefore, the error signal of the CED scheme raised, and the light gray color means the opposite. Each row of Fig. 3.9 is composed of 1000 simulated points, meaning that 1000 simulations were performed for each scenario and for each CED technique. Taking as example the results of the DWC scheme in Fig. 3.9, the DWC's error signal is raised only when a TF reaches the monitored memory element causing a SE. Consequently, the orange part matches with the red one. For the proposed scheme (LBTFD), the error signal is raised when there are transitions within the detection window, which has been calibrated to accommodate TFs with width up to 450 ps. Therefore, the LBTFD's error signal is also raised at instants when there is no occurrence of soft error.

As seen in Fig. 3.9, each technique has a different detection profile, however the majority is able to detect all TFs causing a SE for this scenario. Depending on the application, the designer can for example, choose a technique that is able to detected the maximum amount of TFs, however, in this case, the system may be frequently interrupted in order to restore the computation.

ISBN: 978-2-11-129250-5

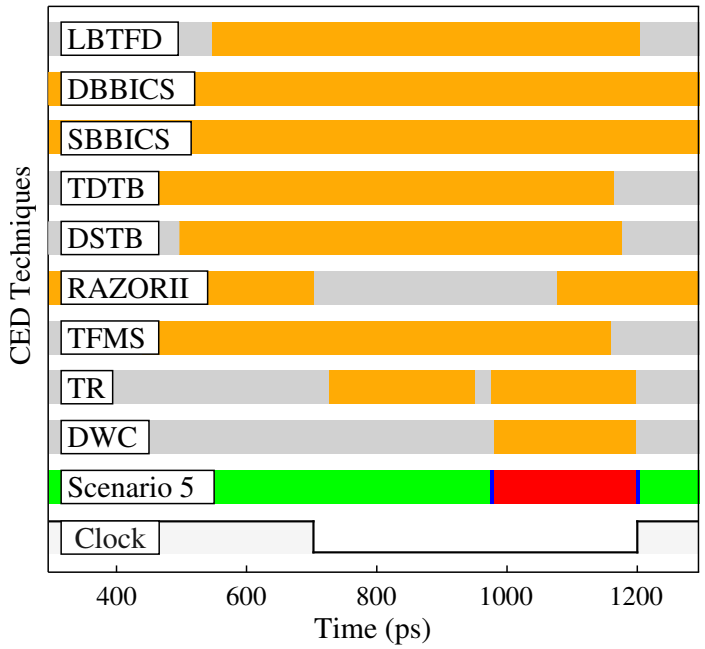


Fig. 3.9: Detection results regarding scenario 5.

3.3.2 Global comparative analysis

Simulation results for each CED technique regarding its effectiveness in detecting single TFs as well as its total power consumption (dynamic plus static analysis) are provided in Table 3.2. For a global comparative analysis, Table 3.2 present results that take into account the 32 scenarios, i.e. the global metrics detailed in subsection 3.2.4. If a CED technique, for instance, works better in scenario 1 than scenario 3, Table 3.2 is not suitable to analyze it. However, as the aim of this work is also to provide an insight of the global effectiveness of a CED technique in different scenarios of TFs, Table 3.2 is a great asset to it.

Note in Table 3.2 the results of the TFMS technique. It shows that 87.39% of SEs and 44.97% of DEs were detected, meanwhile the proposed technique LBTFD (aiming at detecting only SEs) was able to detect 100% of the injected TFs that result in SEs. However, if the TF width is larger than the designed DW, a few SEs will pass undetected by LBTFD. Even though, results are interesting if compared to the other CED techniques. Moreover, the design of the proposed LBTFD is easier than BBICS-based techniques as only standard cells can be used, implicating directly in less time to conceive the circuit. Although SBBICS was able to detect 100% of the injected TFs, it is not a known standard cell and requires to isolate the substrate into islands with separated Nwell and Pwell regions.

ISBN: 978-2-11-129250-5

Table 3.2: Total power and effectivenness of the CED techniques under analysis

CED Technique	**Power (μW)**	$\frac{\mathbf{TF_{detected}}}{\mathbf{TF_{injected}}}$	$\frac{\mathbf{SE_{detected}}}{\mathbf{SE_{induced}}}$	$\frac{\mathbf{DE_{detected}}}{\mathbf{DE_{induced}}}$	$\frac{\mathbf{(SE+DE)_{detected}}}{\mathbf{(SE+DE)_{induced}}}$
DWC [5]	$>$ 100 %	16.69 %	100.00 %	0.34 %	28.87 %
TR [6]	3.86 /bit	23.64 %	74.47 %	16.04 %	33.16 %
SBBICS [12]	6.56	100.00 %	100.00 %	100.00 %	100.00 %
DBBICS [11]	5.65	94.23 %	100.00 %	94.75 %	96.38 %
RAZORII [8]	199.21 /bit	43.70 %	72.53 %	37.82 %	47.95 %
TDTB [9]	3.32 /bit	77.98 %	95.54 %	75.32 %	81.49 %
DSTB [9]	3.26 /bit	47.02 %	83.70 %	45.25 %	56.94 %
TFMS [13]	3.02 /bit	50.50 %	87.39 %	44.97 %	57.92 %
LBTFD [this]	2.64 /bit	57.17 %	100.00 %	100.00 %	100.00 %

3.4 Summary

A technique capable to detect TFs has been presented and analyzed in this chapter. Furthermore, a simulation-based method for classifying and evaluating CED techniques has been defined. For the considered scenarios, the proposed CED technique is able to detect all the TFs that result in SEs or DEs in the DFF. The ability to detect all TFs resulting in SEs and DEs is essential as these errors modify the circuit computation. SEs and DEs may be induced by accident (caused by radiation for example) or human-induced perturbations (e.g. caused by laser fault injection), which in this case the goal can be the extraction of confidential information from the chip.

The evaluation method takes into account only single TFs that survive the attenuation of logical or electrical masking effects in order to compare exclusively the effectiveness of the different CED techniques and not the ability of target combinational circuits in masking TFs. This evaluation strategy allows, therefore, to quickly analyze a CED technique independently of the logic complexity of the system. Results in Table 3.2 enable designers to choose the CED technique (or techniques) that suit best for their purposes. The decision can be made based on the detection capability of each technique and on the easiness to implement such technique.

ISBN: 978-2-11-129250-5

Chapter 4

Upgrading the Electrical Model of Laser Effects on ICs

As this thesis focuses on the effects of laser illumination on ICs, a detailed review about this subject was given in Chapter 2. Improvements of the classical electrical model for simulating the effects of laser shots on ICs that were previously proposed are discussed in Section 4.1. Following the State-of-the-Art concerning the electrical model, Section 4.2 details the limitations of the previous proposed models. In view of these limitations, Section 4.3 introduces an enhanced electrical fault model that takes the laser-induced IR drop into account for simulation purposes. Section 4.4 discusses the consequences of the enhanced electrical model on the laser-induced fault injection mechanism, i.e., how a laser shot can cause a SE and what is the influence of the enhanced model when compared to the classical model. In Section 4.5, simulations and experimental results of laser injections are compared in order to confirm the accuracy of the proposed enhanced fault model.

The works reported in this chapter and in Chapter 5 were published and presented in three different conferences:

- International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design (SMACD) 2017 [2]
- Euromicro Conference on Digital System Design (DSD) 2017 [1]
- International Symposium on Physical Design (ISPD) 2018 [5]
- A more detailed study on the contribution of laser-induced IR drop in the fault injection process was later submitted to the IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (IEEE TCAD) [4]

ISBN: 978-2-11-129250-5

4.1 Previous Works on Electrical Models of Laser Injection

After introducing the classical electrical model to simulate the effects of laser illumination on ICs in Chapter 2, more advanced electrical models proposed afterwards are also presented in this section.

4.1.1 Electrical Model Proposed in 1999 by V. Pouget et. al.

In this work [93], V. Pouget et. al. define an electrical model of a MOSFET illuminated by a laser. The definition of the model starts by a detailed analysis of the shapes of the transient currents induced by radiation (obtained from numerical device simulations) to extract characteristic physical behaviors, including capacitive and bipolar effects. A schematic is then deduced and the transients it generates are compared to those of a two dimension silicon device level simulator [105]. Good agreement is achieved between device level curves and SPICE level ones, for the four electrodes of the device. Benefits in using this enhanced model are finally explored with its application to the simulation of single-event upsets in a SRAM, and comparisons with results provided by common simplified models.

The electrical model proposed in [93] is given in Fig. 4.1. This model is based on the classical electrical model [121] to which is added a degraded bipolar transistor for simulating the related effect. The small capacitance C_2 (typically a few fF) is also added to improve reaction of the gate-bulk capacitance Cgb of the MOS transistor. Finally, a bulk network is also added. It is composed by a capacitance and two resistors to adjust the bulk current. The R_2-C_1 branch represents the dielectric relaxation time. R_3 controls the long time bulk response and represents the resistance of the conduction path through the bulk from drain to bulk contacts. This passive network is a key component of the model since it controls the potential of the internal bulk node.

4.1.2 Electrical Model Proposed in 2005 by A. Douin et. al.

In 2005, A. Douin et. al. [39] (from the same research group of V .Pouget et. al. [93]) presented similar electrical models of laser-induced currents in a NMOS transistor for different laser pulse durations. Their models were validated by mixed-mode device simulations of a laser-induced fault in a SRAM cell for different laser pulse durations ranging from 100 fs to 10 ns.

ISBN: 978-2-11-129250-5

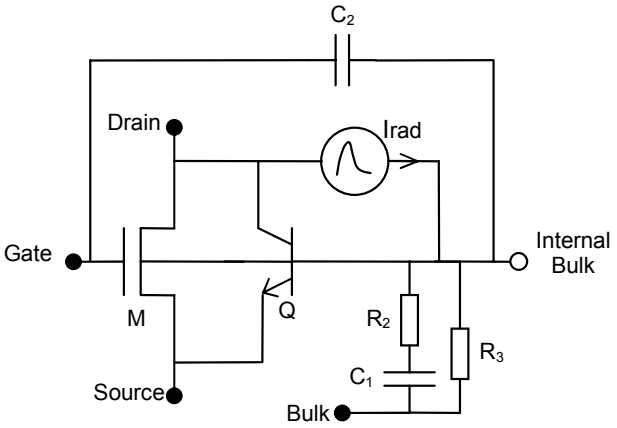


Fig. 4.1: Schematic of the electrical model of an irradiated MOSFET for short pulse duration.

In the case of short pulse durations (femtosecond to picosecond), the authors recommend the electrical model shown in Fig. 4.1. However, in case of long pulse durations (nanosecond to microsecond), the authors suggest the use of the electrical model presented in Fig. 4.2.

The main difference between the models proposed by [93] (Fig. 4.1) and [39] (Fig. 4.2) lies in the activation or not of the parasitic bipolar transistor and the variations or not of potentials lines in the substrate. That is why the parasitic bipolar transistor and capacitance C_2 between gate and internal-bulk do not appear in Fig. 4.2 . So it is based on the exponential current source.

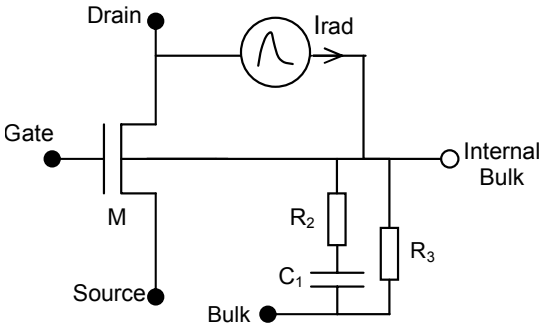


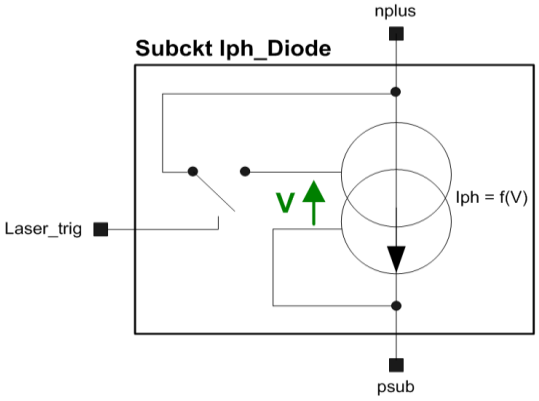
Fig. 4.2: Schematic of the electrical model of an irradiated MOSFET for long pulse duration.

4.1.3 Electrical Model Proposed in 2013 by A. Sarafianos et. al.

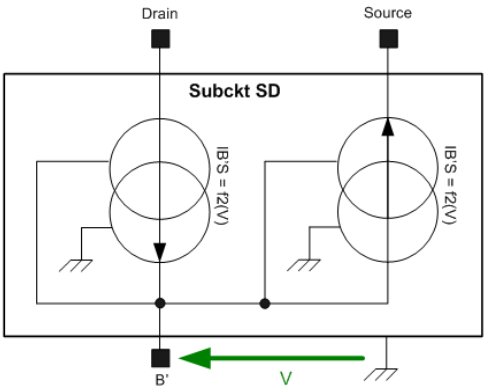
This work [101] presents measurements of pulsed photoelectric laser stimulation of an NMOS transistor in 90 nm technology. According to the authors of [101], a proper modeling of the effects of pulsed laser sources on an NMOS transistor involved two

ISBN: 978-2-11-129250-5

subcircuits denominated *Subckt Iph-Diode*: one for the Source/Bulk junction and another for the Drain/Psubstrate junction (c.f. Fig. 4.3). It must also involve the effect of a local increase of the Psubstrate's voltage which may trig the parasitic bipolar transistor. This is modeled by *Subckt SD* in Fig. 4.4. Resistance Rb and capacitance Cb are used to set the time constant of that phenomenon. This constant describes the time of dielectric relaxation [39].



(a) Electrical model of a PN junction under pulsed laser embedded in a sub circuit called *Subckt Iph_Diode*.



(b) Electrical model of the parasitic bipolar effect under pulsed laser embedded in a sub circuit called *Subckt SD*.

Fig. 4.3: Subcircuits used in the electrical model presented in Fig. 4.4.

4.1.4 Electrical Model Proposed in 2013 by L. Heriveaux et. al.

In 2005, A. Douin et. al. [39] wrote: "for technologies more integrated than the one studied in this work, it may be important to consider complementary charge collection mechanisms. As an example, a laser pulse impacting on the drain of a transistor smaller than the spot size may generate enough carriers directly in the source of the transistor to induce significant current in this junction."

Following this hypothesis, the electrical model published by L. Heriveaux et. al. [50] demonstrated the significant contribution of the current induced by the vertical parasitic bipolar transistors inherent to MOSFETs. Fig. 4.5 presents the electrical model of laser-induced transient currents applied to a CMOS inverter [50].

The electrical model shown in Fig. 4.5 is based on the inverter circuit with a load capacitor (C_{load}) acting as the input of the next stage. The model used for the two MOS transistors is that of an ideal switch. The NMOS is modeled by an open circuit (OFF-state) and the PMOS by a resistor or a current source (ON-state) according to V_{GS} (gate-to-source bias) and V_{DS} (drain-to-source bias) values. The

ISBN: 978-2-11-129250-5

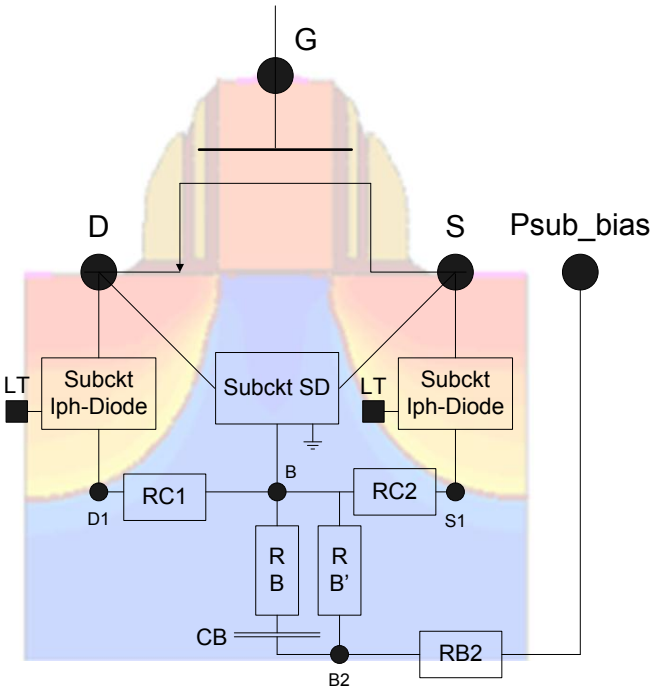


Fig. 4.4: Electrical model of an NMOS transistor under pulsed laser source. Electrical model proposed in [101].

model considers that leakage currents of MOS transistors have a negligible impact in the simulations.

The two parasitic PNP-BJTs inherent to the Nwell process are arranged between the drain, source and bulk of the PMOS. Emitters are naturally at the P-type active region according to their higher doping concentration. Bases and collectors are tied to each other and they follow respectively at Nwell and P-substrate. The bases are biased to the high supply line through the well-resistor (R_{NWell}) and the collectors are biased to the low supply line through the substrate resistors (R_{sub1} and R_{sub2}). The amplification factor $\beta = \frac{I_C}{I_B}$ of the PNP-BJTs is set to 5. This value is based on the literature [45, 87] suggesting that β ranges between 2 and 10.

In bulk process, the well-substrate junction and the drain junction of the OFF MOS transistor are reverse biased. Consequently, these junctions are more sensitive to photoelectrical stimulation and generate photocurrents accordingly to the injected light power. Both photocurrents are modeled by a controlled current source between bases and collectors of the PNP-BJTs for the well-substrate junction (I_P) and between the output and the substrate resistors for the drain-NMOS junction (I_N). The injected photocurrent is considered constant when junctions are reverse biased and linearly decreases when junctions are forward biased due to the counterbalancing forward current of diodes. The injected photocurrent magnitude and the ratio be-

ISBN: 978-2-11-129250-5

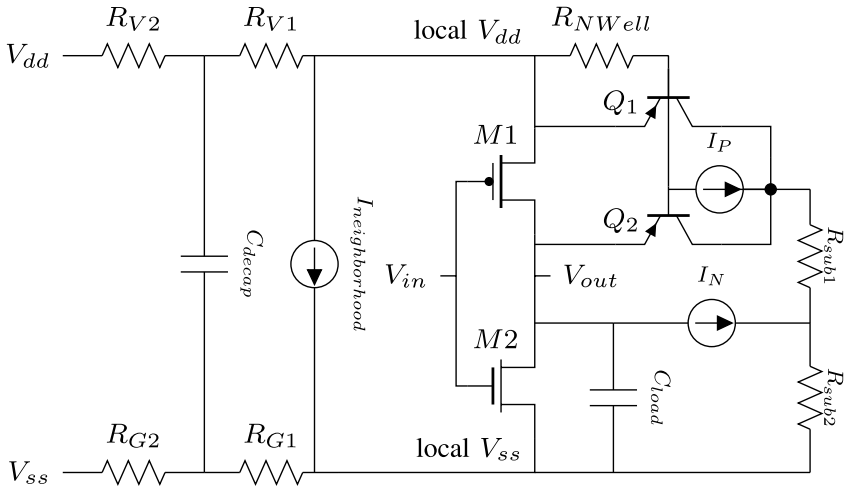


Fig. 4.5: Electrical model of a CMOS inverter with parasitic bipolar transistors.

tween I_P and I_N are also based on the literature [101]. The size of the structure studied in [101] was taken into account and injected currents were roughly scaled down linearly to a 1 μm wide transistor. The relationship between power density and current is also based on the studies published by [101].

The injected photocurrents are expected to flow through the power supply line (V_{DD} = 1.2 V, V_{SS} = 0 V) and generate a voltage drop on the local cells' supply. To study this effect, the power supply lines were modeled by a passive network including rail resistors (R_{G1}, R_{V1}, R_{G2} and R_{V2}) and a decoupling capacitor (C_{decap}) between the power supply and the Device Under Test [79, 112].

Laser spot size is modeled with an additional leakage current ($I_{neighborhood}$) on the power supply lines and corresponds to neighboring cells' photocurrent ending in power rail lines. Because the laser beam spot has a Gaussian shape and because the cells' biasing is not known, the correlation of the supplementary injected photocurrents with the number of cells exposed is not straightforward.

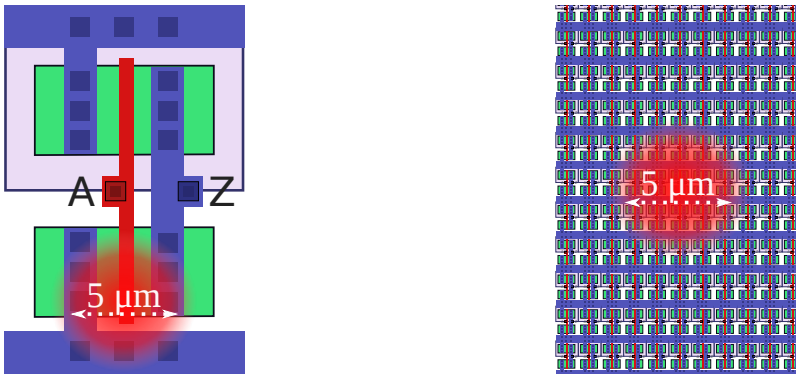
4.2 Limitations of Previous Electric Fault Models

The last section presented the improvements made [39, 50, 93, 101] over the classical electrical model [80] to simulate laser effects on ICs. The next sections detail the limitations of all the models presented so far. Furthermore, these limitations justify the need for a new model when considering deep submicron technologies.

ISBN: 978-2-11-129250-5

4.2.1 Limitations of the Classical Electrical Fault Model

The classical fault model (Fig. 2.2) uses current sources attached to the drain of laser sensitive transistors since these currents are the root cause of the transient fault injection mechanism. This model was created at a time when laser sources with 1 μm to 5 μm spot diameter were able to target only one sensitive PN junction, as Fig. 4.6a illustrates. For advanced technologies this model is questionable. Indeed, looking at Fig. 4.6b, which shows standard cells of a 28 nm CMOS technology being illuminated by a laser source with 5 μm spot diameter, one may observe that the laser shot simultaneously illuminates at least 10 gates at a time and therefore not only a single PN junction.



(a) 250 nm technology.
Standard cell height: 12.5 μm

(b) 28 nm technology.
Standard cell height: 1.2 μm

Fig. 4.6: Standard cells being illuminated by a 5 μm laser spot diameter.

As a consequence, a transient current that flows directly from V_{DD} to G_{ND} is always induced. In fact this direct current from V_{DD} to G_{ND} also flows in older technologies for which the laser spot is able to illuminate only one PN junction. However the effect is negligible when comparing to more advanced technologies. Fig. 4.7 illustrates the additional current component, named IPh_{Psub_nwell}. This current is induced in the reversed biased $Psub$-$Nwell$ junction that surrounds every $Nwell$. Even if the laser beam is directed toward a sensitive NMOS, the laser beam also induces charge carriers sufficiently close to a $Psub$-$Nwell$ junction to induce a transient current IPh_{Psub_nwell}. This current, which is not taken into consideration by the classical model (Fig. 2.2), can have a significant effect on the fault injection mechanism by inducing a supply voltage drop [40].

ISBN: 978-2-11-129250-5

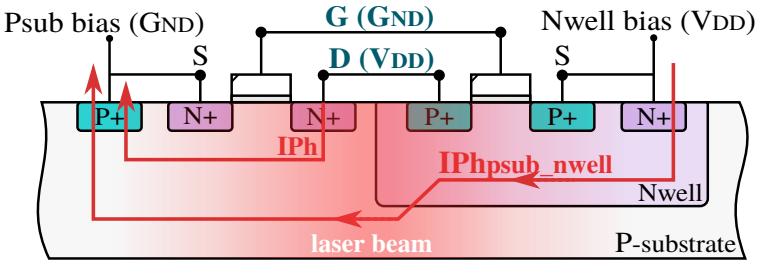


Fig. 4.7: Laser-induced current components. Cross-section of a CMOS inverter.

4.2.2 Limitations of State-of-the-Art Electrical Models

The models proposed by [39, 93, 101] improved the classical fault model by including bipolar transistors for simulating the parasitic bipolar effect, capacitances and resistances in the bulk to adjust the bulk current and to represent the dielectric relaxation time. These models in fact have a better correlation between electrical simulation and a two dimension silicon device level simulator [105]. However, as in the case of the classical model and, as mentioned in the last section, these models consider that the laser beam illuminates only one sensitive PN junction.

A. Douin et. al. [39] wrote that laser illumination nowadays may generate enough carriers directly in the source of the transistor to induce significant current in this junction leading to secondary effects such as IR drop. Following this work, L. Heriveaux et. al. [50] proposed an electrical model including the significant contribution of the current induced by vertical parasitic bipolar junctions inherent to MOSFETs that may lead to IR drop effects. As complete as this electrical model seems to be, in their original publication [50], the authors used values taken from other works and made ideal assumptions which limits the accuracy of the model and render difficult its implementation at circuit level as they did not extended their work beyond the scope of a single inverter. From their own words they emphasize: "because the laser beam spot has a Gaussian shape and because the cells' biasing is not known, the correlation of the supplementary injected photocurrents with the number of cells exposed is not straightforward".

In view of all the aforementioned limitations, an enhanced electrical model is presented in the next section. The proposed model aims at being as accurate and simple as possible to be implemented to simulate complex designs and not only a single standard cell.

ISBN: 978-2-11-129250-5

4.3 Proposed Transient Fault Model of a Cell Under Laser Illumination

Fig. 4.8 shows, in case of an inverter, the proposed enhanced electrical model taking into account the laser-induced IPh_{Psub_nwell} current component. This current has no direct effect on the gate output as it draws current from the gate's power-grid model (or power distribution network – PDN). As a result, the targeted gate power supply (V_{DD}) undergoes an IR drop and its ground supply (G_{ND}) experiences a ground bounce. Furthermore, as neighboring cells are subject to similar transient currents, their effects add up and can propagate to distinct cells via the PDN. In addition, because the supply voltage is not anymore constant and below its normal value, one may expect a non linear effect due to surrounding logic gates that can start consuming current.

However, the proposed electrical model (Fig. 4.8) is useless if the power supply grid is assumed ideal, i.e. if V_{DD} and G_{ND} are connected to ideal supply sources via ideal nets. It must thus be used in conjunction with an accurate model of the PDN. This explains why we recommend to use this model in a simulation flow based on an Electromigration / IR drop (EMIR) CAD tool. This kind of tool automatically provides the power-grid model for each cell in the design.

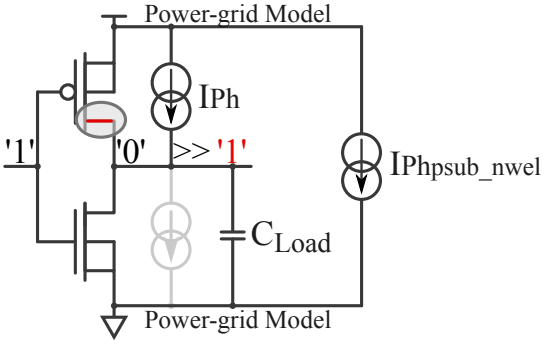


Fig. 4.8: Proposed laser-induced transient fault model (applied to an inverter with input biased at V_{DD}) to take into account the supply voltage drop/bounce induced by the IPh_{Psub_nwell} parasitic current.

The current sources in Fig. 4.8 have a profile of a double exponential, such as the one illustrated in Fig. 2.1d. The currents have a peak amplitude defined by equation (2.1). The parameter S (area of the PN junction) corresponds to the PMOS drain area for I_{Ph}, while it is equal to the $Nwell$ area for the IPh_{Psub_nwell} component. IPh_{Psub_nwell} is usually larger than I_{Ph} since the drain area is significantly smaller than the $Nwell$'s area.

ISBN: 978-2-11-129250-5

The IPh_{Psub_nwell} current source is attached to the biasing contacts of the $Nwell$ and the $P_{substrate}$ (for standard cells without embedded biasing contacts, the current source is connected to the closest). The various IPh_{Psub_nwell} currents add up and flow from V_{DD} to G_{ND} trough the power/ground networks of the device under illumination. Because the power grid is resistive and capacitive, local voltage drops and ground bounces occur thus suddenly reducing the voltage swing seen by standard cells in the close vicinity of the laser spot. This laser-induced voltage drop can by itself cause timing errors (timing constraint violations) or even data disruptions leading to the sampling of erroneous data by the registers. Furthermore, the IPh_{Psub_nwell} current deprives the ON transistor of the inverter from its ability to compensate for the effect of IPh. As a result, the output capacitance is more easily discharged (or charged) by the photocurrent. Te transient fault is thus easier to induce and has a stronger amplitude.

The above observations highlight the importance of considering the spatial distribution of the laser beam energy on the IC surface. It also highlights the importance of accurately modeling the power/ground network to simulate laser effects on ICs with accuracy. Considering the above, this thesis also provides a method based on standard CAD tools to take at chip level the effect of laser-induced IR drops into account. The method will be presented in details in Chapter 5.

4.4 Effects of the Enhanced Electrical Model on the Laser-induced Fault Injection Mechanism

4.4.1 Soft-Error occurrence due to a laser shot

By considering both the classical and enhanced models, this section clarifies how a laser-induced transient fault can cause a soft error in three different situations. First, it is shown in section 4.4.1.1 the influence of the I_{Ph} current component, which corresponds to the classical model. Then, section 4.4.1.2 explains how the IPh_{Psub_nwell} current component alone can cause timing errors. Section 4.4.1.3 takes into account the enhanced electrical model to show the influence of I_{Ph} and IPh_{Psub_nwell} current components at the same time, thus illustrating the effect of IPh_{Psub_nwell} over I_{Ph}.

The diagrams presented in Fig. 4.9a to4.11a show the timing paths to be analyzed. FF_i is the source register, FF_o is the destination register, and between, the combinational logic.

ISBN: 978-2-11-129250-5

4.4.1.1 Influence of the I_{Ph} current component - Classical model

Fig. 4.9b illustrates where laser shots may generate an undesired transient current/-voltage (in red) in a CMOS inverter according to the classical model. If this inverter is part of a combinational logic like the one Fig. 4.9a illustrates, the transient voltage propagates through the logic toward the input of sequential cells (registers or latches). Depending on the transient voltage characteristics (width and amplitude) the induced transient can still be present at the input (signal D_o in Fig. 4.9c) of the DFF (FF_o) when the rising clock edge occurs. In that case a SE is induced by the laser illumination: there is thus a flipping of the correct output of the register (signal Q_o of Fig. 4.9c).

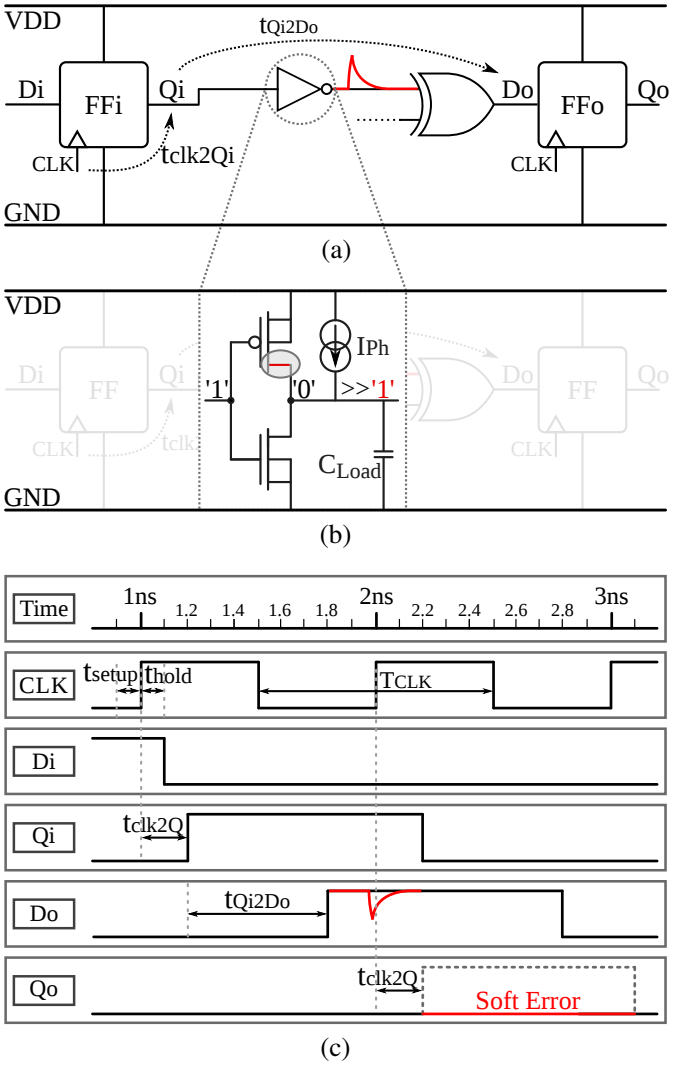


Fig. 4.9: Propagation of a corrupted signal along the data path and sampling of the corrupted signal at the next rising clock edge inducing a soft error.

ISBN: 978-2-11-129250-5

4.4.1.2 Influence of the IPh_{Psub_nwell} current component

IR drops caused by the switching of transistors can reach up to 20% of the nominal power supply voltage [125]. However, when a laser illuminates a circuit, IR drops are even more accentuated in the affected cells. With this decrease of the power supply voltage, the speed of critical paths also reduces [120]. In particular, delays of some specific gates increase largely due to IR drops [90]. Therefore, IR drop can induce timing errors and even data disruptions.

In case of timing errors, the timing constraints for a synchronous design are violated. This constraint known as the setup time constraint, requires that the minimum clock period T_{CLK} (Fig. 4.10c), necessary for the circuit to operate correctly, must be superior or at least equal to:

$$T_{CLK} \geq t_{clk2Qi} + Q_i2D_o + t_{setup} \tag{4.1}$$

where t_{clk2Qi} is the FF_i clock-to-Q delay. Q_i2D_o is the maximum data path propagation delay and t_{setup} represents the setup time (minimum amount of time before the clock edge during which the signal D_o must be steady at its valid state).

Figure 4.10a shows the timing paths to be analyzed. Fig. 4.10b illustrates where laser shots may generate an undesired current IPh_{Psub_nwell}. Both Fig. 4.10a and 4.10b depict an illustration of a voltage drop and ground bounce induced by the current IPh_{Psub_nwell}. The voltage drop and ground bounce depicted on the left part of the power/ground rails occurs due to the switching of transistors composing the FF_i cell. The voltage and ground bounce occurring on the right part of the power/-ground rails is essentially due to the laser-induced current IPh_{Psub_nwell}. Fig. 4.10c gives an example in which a voltage drop induced only by the current IPh_{Psub_nwell} causes a setup time violation in the data path.

ISBN: 978-2-11-129250-5

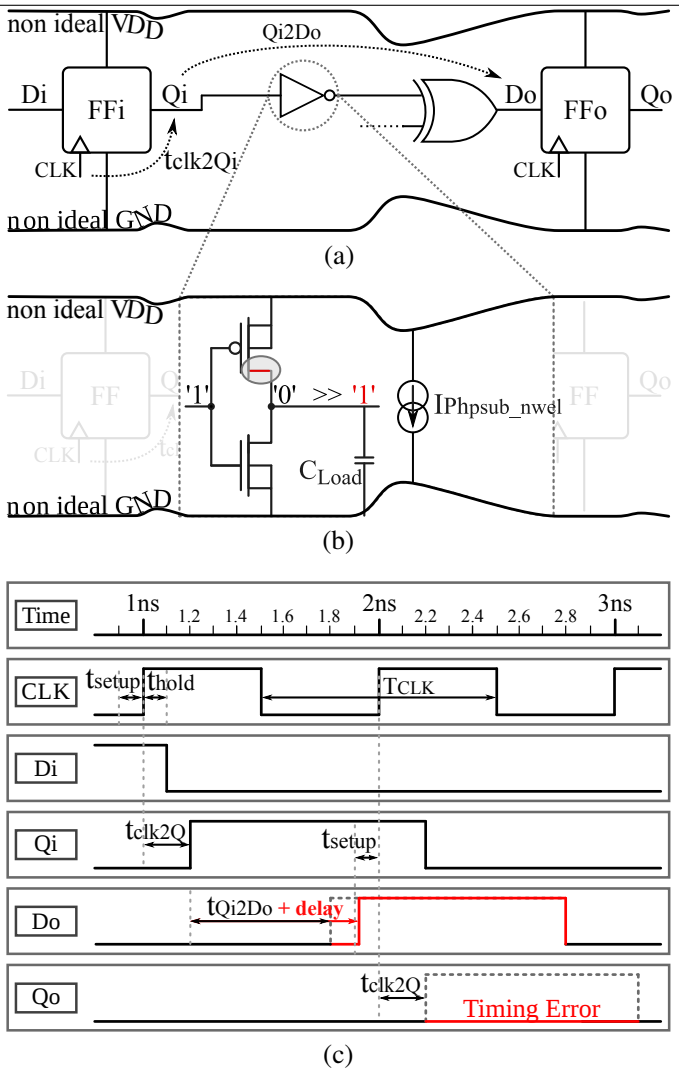


Fig. 4.10: Propagation of a signal along the data path and its sampling at the next rising clock edge with increased delay leading to a timing error due to the IR drop.

4.4.1.3 Influence of I_{Ph} and IPh_{Psub_nwell} current components

Until now, the influences of the current I_{Ph} and IPh_{Psub_nwell} have been considered separately. In Fig. 4.11c both components are taken into account. As a result, signal D_o shows a different profile of transient fault than the same signal in Fig. 4.9c. The principle behind the observed amplification of the amplitude and width of the transient fault profile will be addressed in the next section. However, Fig. 4.11c suggests that the contribution of both current components increase the total number of soft/timing errors observed in the circuit because the induced perturbations have higher amplitude and width.

ISBN: 978-2-11-129250-5

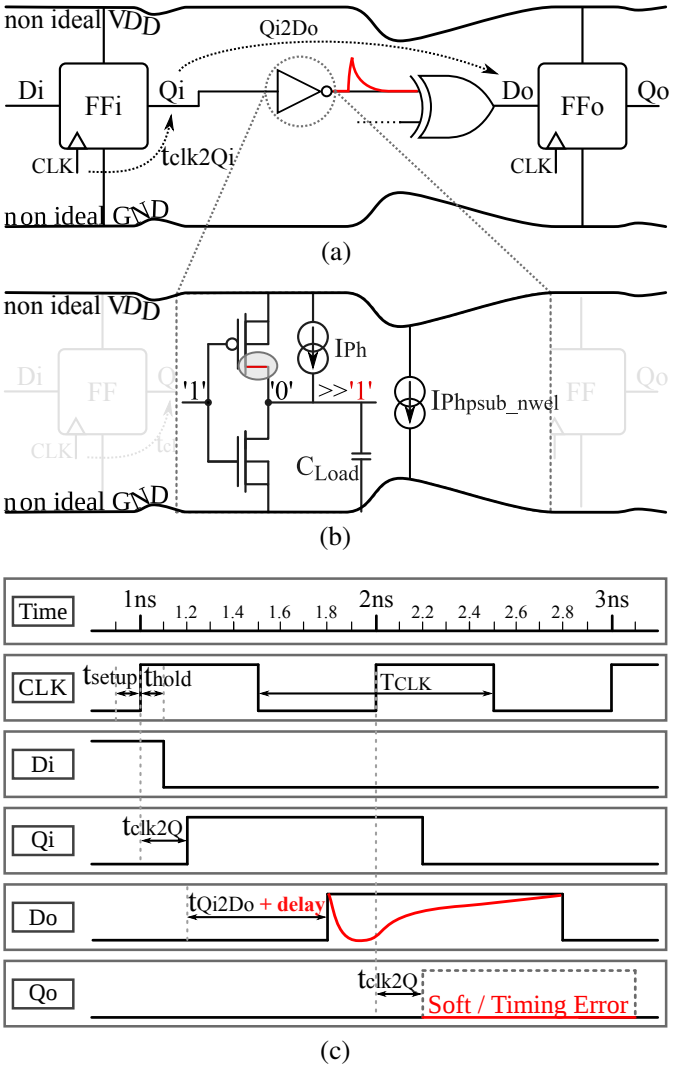


Fig. 4.11: Propagation of the corrupted signal along the data path and sampling of the signal at the next rising clock edge plus increased delay leading to a soft/timing errors due to IR drops.

4.4.1.4 Threshold for the Occurrence of Soft Errors

In the three models presented in Fig. 4.9 to 4.11, there is no fixed thresholds on the laser shot characteristics (power, pulse width, etc.) indicating when a soft error occurs or not. In fact, the occurrence of a SE depends on the cells that have been illuminated by the laser beam and also on many design parameters such as the clock period, the timing slack, etc. A key parameter is also the value of the handled data which fixes the maximal propagation time and thus the localization of the laser-sensitive areas. Similarly, in the models presented in Fig. 4.10 to 4.11, in which the influence of the current component IPh_{Psub_nwell} is considered, the occurrence of SE also depends on the logical depth of the considered data path. The instant when

ISBN: 978-2-11-129250-5

the laser is activated plus the slack time of the affected datapath thus determine if the induced currents cause a soft error or a timing error.

4.5 Simulation and Experimental Evidence of Laser-induced IR Drop

Before describing the core of this work: the use of standard CAD tools to simulate the effect of laser fault injections in large-scale circuits by taking into account the IR drop component, the accuracy of the proposed enhanced model is first put to proof in this section. To achieve this, the classical and the enhanced model were applied (on simulation basis) on a ring oscillator (RO). A RO was also implemented on a FPGA in order to perform laser illumination and them to compare simulation with experimental results.

For the sake of clarity, Table 4.1 depicts the order in which the results are presented. Section 4.5.2 presents simulation and experimental results for both models and for a laser illuminating an area targeting the standard cells of the RO. Then, Section 4.5.3 reports simulation and experimental results for both classical and enhanced models in case of a laser illuminating a region near the RO. In this case the laser spot does not illuminate the standard cells of the RO. Thus, according to the classical fault model, if the latter is correct, it is expected that the behavior of the RO remains unchanged. If this is not observed in practice, the classical model is lacking of representativity and accuracy.

Table 4.1: Presentation order of the results of Section 4.5

Laser spot in the RO (Section 4.5.2)	**Laser spot close to the RO (Section 4.5.3)**
Simulation: classical model	Simulation: classical model
Simulation: enhanced model	Simulation: enhanced model
Experimental: laser shot on a RO	Experimental: laser shot near a RO

The results presented in this section are of fundamental importance as they give for the first time, evidence that laser-induced IR drop does exist and should not be neglected during the design of secure systems. The results also justifies the work presented in Chapter 5.

ISBN: 978-2-11-129250-5

4.5.1 Design Under Test

A RO was chosen as the Design Under Test (DUT) since its oscillation frequency varies linearly with the supply voltage over a wide range of V_{DD} [49, 51, 78]. This characteristic renders such a structure particularly interesting to experimentally monitor potential voltage drops caused by laser shots by measuring the evolution of their oscillation frequency [68]. The next paragraphs (Sections 4.5.1.1 and 4.5.1.2) give details on how the RO was implemented electrically in order to perform simulations and on FPGA to launch experimental campaigns with a laser source (setup details are given in Section 4.5.1.3).

4.5.1.1 Electrical model of the ring oscillator used during simulations

The RO of Fig. 4.12a was designed using a 65 nm technology. It features an AND2 gate, a BUFFER gate, and seven inverters. Its nominal oscillation frequency is equal to 148 MHz. The oscillation frequency was fixed to be in accordance with that of the RO considered during the experiments described in the next paragraphs so that to ease the joint analysis of experimental data and simulation results.

Fig. 4.12b shows a basic example of a series RLC distributed model [99] of the supply voltage V_{DD} between the supply pad and the inverters in Fig. 4.12a. The RLC network allows to consider the decoupling effect of the power grid as well as its inductance and resistance. This model therefore takes laser-induced IR drops into account during simulations by setting $IPh_{Psub\_nwell} > 0$.

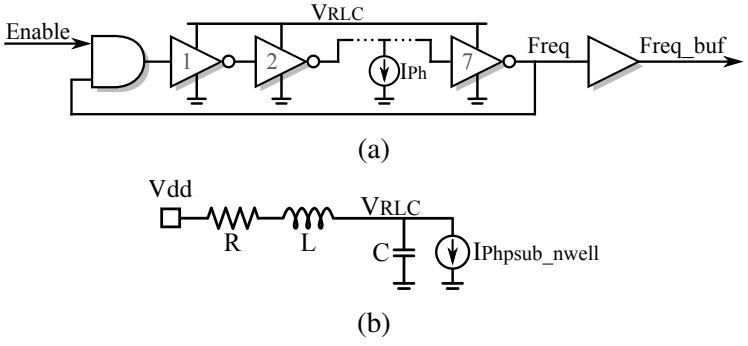


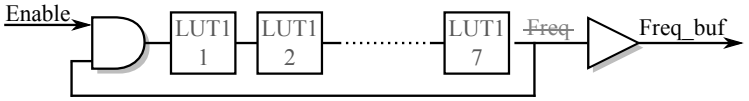
Fig. 4.12: Ring oscillator used during simulations. (a) RO block diagram including the IR drop contribution (non-ideal V_{DD}) for a given power-grid model. (b) Lumped elements of a series RLC network with IPh_{Psub_nwell} current connected in parallel.

ISBN: 978-2-11-129250-5

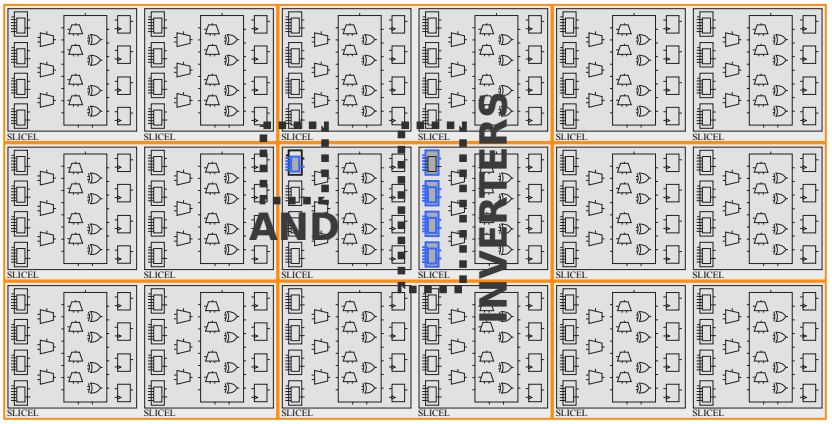
4.5.1.2 Ring oscillator implemented on FPGA

A RO, similar to the one used to perform simulations, was implemented on a Virtex-5 FPGA [124] in order to launch experimental campaigns and also to ascertain the existence of a laser-induced IR drop.

The topology of the RO mapped into the Virtex-5 is presented in Fig. 4.13a. It is composed of five LUTs and has a nominal frequency equal to 148 MHz. Fig. 4.13b shows the placement of the LUTs in two different slices of the FPGA. The LUTs used to implement the inverters were placed in the same slice (the one on the right) while the LUT used to implement the AND2 gate was placed in another slice to avoid disabling the RO during laser shots. The output buffer is associated with the IO port of the FPGA, thus having a fixed position (not shown in Fig. 4.13b).



(a)



(b)

Fig. 4.13: RO implemented on a Virtex-5 FPGA. (a) RO block diagram. (b) Placement of the ring oscillator using the PlanAhead design tool [123].

4.5.1.3 Laser setup for the experimental fault injection

After implementing the RO on the Virtex 5, the chip was exposed to laser shots by removing its encapsulation. For the experiments reported in this thesis the thickness of the substrate was kept intact (approximately 300 μm). The board was then put in place with the setup illustrated in Fig. 4.14.

The following list details the role of each equipment used for the experimental fault injection:

ISBN: 978-2-11-129250-5

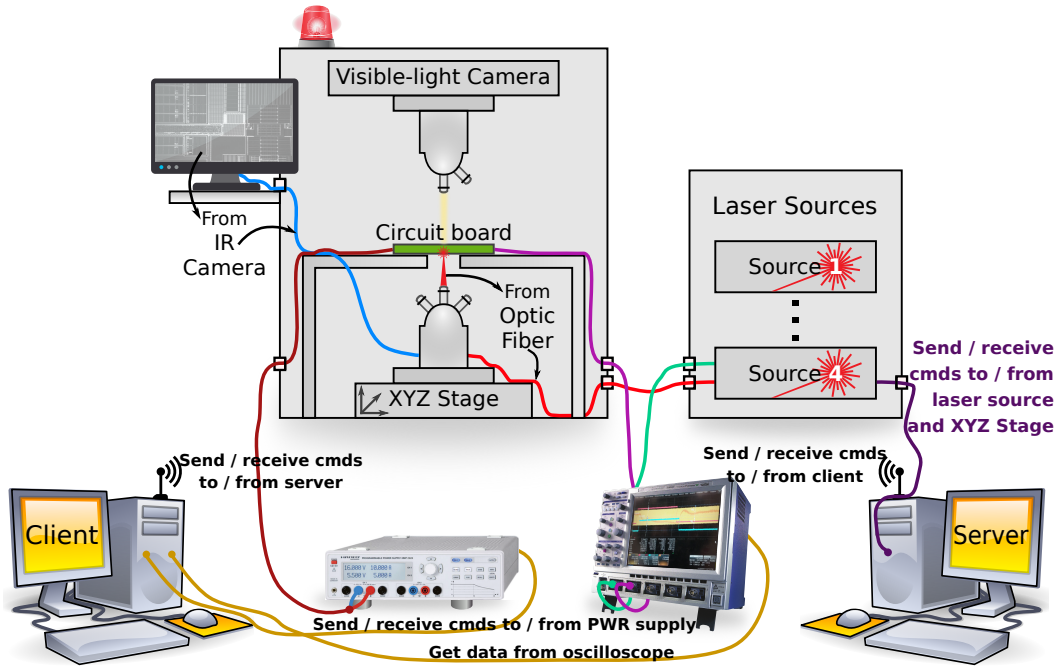


Fig. 4.14: Laser setup used for the experimental results reported in this thesis.

- Visible-light camera: provides a visible-light beam at one side of the chip that helps to centralize it with regard to the lens used for the laser injection located at the other side of the same chip (target).
- Infrared camera: allows to see the internal structure of the circuit and to adjust the focus of the laser spot.
- Oscilloscope: it monitors the oscillation frequency of the RO and the laser pulse in order to know when the laser is active with regard to the circuit operation.
- Power supply: used to reset the FPGA whenever a permanent fault is observed, i.e. when the RO stops oscillating after a laser shot and remains in that state even if the laser is inactive.
- Laser sources: there are four difference laser sources available with different characteristics (power, pulse duration, etc.). For the experiments reported in this thesis, a laser source with 1064 nm wavelength (infrared range) was used to generate laser pulse of duration equal to 5 μs and of power equal to 1.04 W (considering 57.84% of the transmission coefficient of the lens).
- Lenses: different lenses provide different laser spot diameters. For the experiments reported in this thesis, a lens with 20x amplification giving a spot diameter equal to 5 μm was chosen.
- XYZ stage: the lens used to perform laser injection are mounted on a mo-

ISBN: 978-2-11-129250-5

torized XYZ stage in order to automatically perform laser-testing scans of its surface and thus to draw fault maps. The board [122] containing the Virtex-5 remained fixed.

- Server computer: it communicates with the laser source, the XYZ stage and the client computer. It receives from the client computer the specified laser parameters and send them to the laser source so the laser shot will be done with these specifications. The server computer also controls the XYZ stage in order to illuminate a specific part of the circuit.
- Client computer: it communicates with the server computer, the oscilloscope and the power source. The client computer contains a set of scripts used to communicate with the server computer. In these scripts, the user can define the laser parameters such as the laser power, the pulse duration, the displacement step of the XYZ stage as well as its step precision (being 0.1 μm the minimum precision). The client computer also reads from the oscilloscope the waveforms from the RO and from the laser shot to be analyzed afterwards and provide the results reported herein. Finally, the client computer sends a signal to the power supply in order to hard reset the FPGA in case of a permanent fault.

After preparing the sample with the setup illustrated in Fig. 4.14, the laser sensitivity map as depicts Fig. 4.15 was drawn. The map covered all the surface of the FPGA comprising an area of 10 mm x 10 mm. In this case, the displacement step of the XYZ stage was set to X: 100 μm and Y: 100 μm, resulting in 10,000 laser shots. Each of the 10,000 points plotted in Fig. 4.15 correspond to the lowest output frequency of the RO observed on the oscilloscope in a time window of 10 μs enclosing the laser shot. The parameter Z of the XYZ stage was kept fixed to maintain the focus of the laser beam with relation to the illuminated PN junctions. As mentioned earlier, a laser source with 1064 nm wavelength was used to generate a laser pulse of duration equal to 5 μs and power equal to 1.04 W. The laser spot diameter was equal to 5 μm.

The pulse duration equal 5 μs was chosen so that to be able to observe the effects caused by the laser-induced IR drop in a long period of time. The observed window on the oscilloscope was 10 μs, which represents in this case around 750 periods for the assessed RO with frequency equal to 148 MHz. The laser power was fixed to the minimum value capable to stop the operation of the RO (frequency output reaching 0 MHz) and to avoid permanent faults in sensitive areas of the FPGA. For powers superior to 1.04 W, some illuminated areas of the FPGA were affected in a way that

ISBN: 978-2-11-129250-5

only reseting the FPGA could restore the correct execution of the RO. As we do not know the internal structure of the FPGA we can only speculate why this happened. In this case for example, the laser beam might have corrupted the configuration bits of the FPGA resulting in permanent errors in the mapped design [29].

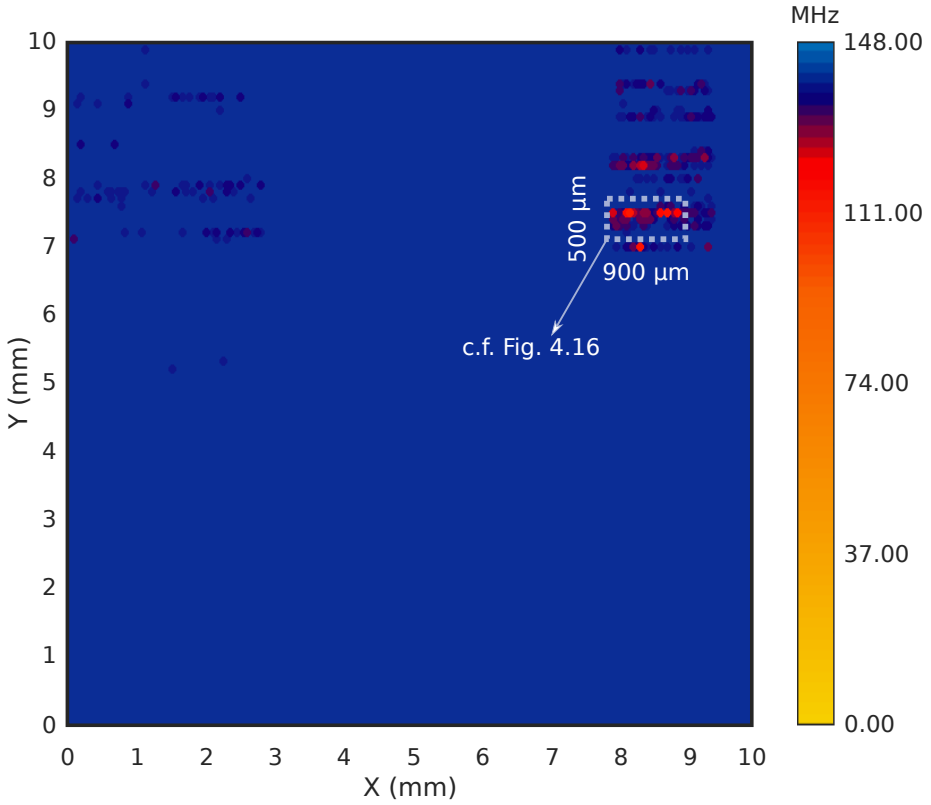


Fig. 4.15: Laser sensitivity map of the DUT, profiled by mapping the output frequency of the RO implemented on FPGA: each point corresponds to the lowest output frequency of the ring oscillator observed on the oscilloscope during a 10 μs time window. Laser pulse duration: 5 μs. Laser power: 1.04 W. Laser spot diameter: 5 μm. (X,Y) displacement step: 100 μm. Covered area: 10 mm x 10 mm.

The orange points in Fig. 4.15 correspond to a drop on the RO's output frequency. This means that when the laser illuminates these regions of the FPGA, the frequency of the RO is affected. As the displacement step used in this sensitivity map is probably several times larger than the area occupied by the RO, several other sensitivity maps were done with smaller displacement steps. This allowed to discover with more precision the location of the LUTs used to implement the RO.

Figure 4.16 also shows the sensitivity map of the DUT, but now, a smaller region of the FPGA is addressed. The (X,Y) displacement step in this case was set to 5 μm. The yellow points should correspond to the placement of the RO (Fig. 4.13b) as the laser shot stops its operation when the laser illuminates that region, i.e., the output

ISBN: 978-2-11-129250-5

frequency of the RO reaches level zero.

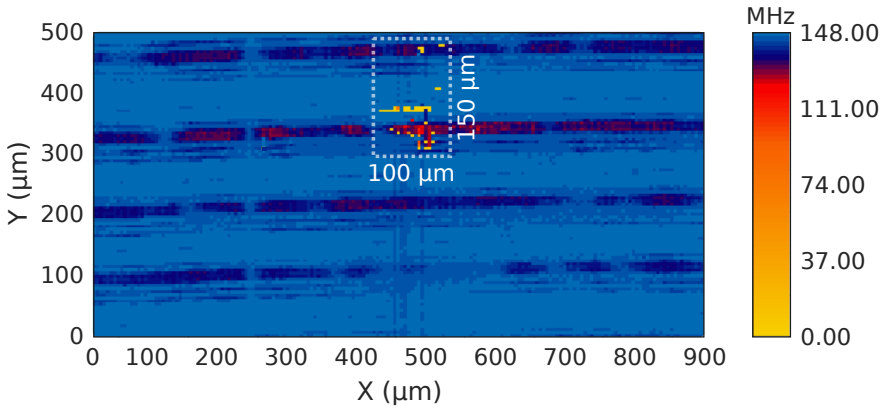


Fig. 4.16: Laser sensitivity map of the DUT, profiled by mapping the output frequency of the RO implemented on FPGA: each point corresponds to the lowest output frequency of the ring oscillator observed on the oscilloscope during a 10 μs time window. Laser pulse duration: 5 μs. Laser power: 1.04 W. Laser spot diameter: 5 μm. (X,Y) displacement step: 5 μm. Covered area: 900 μm x 500 μm.

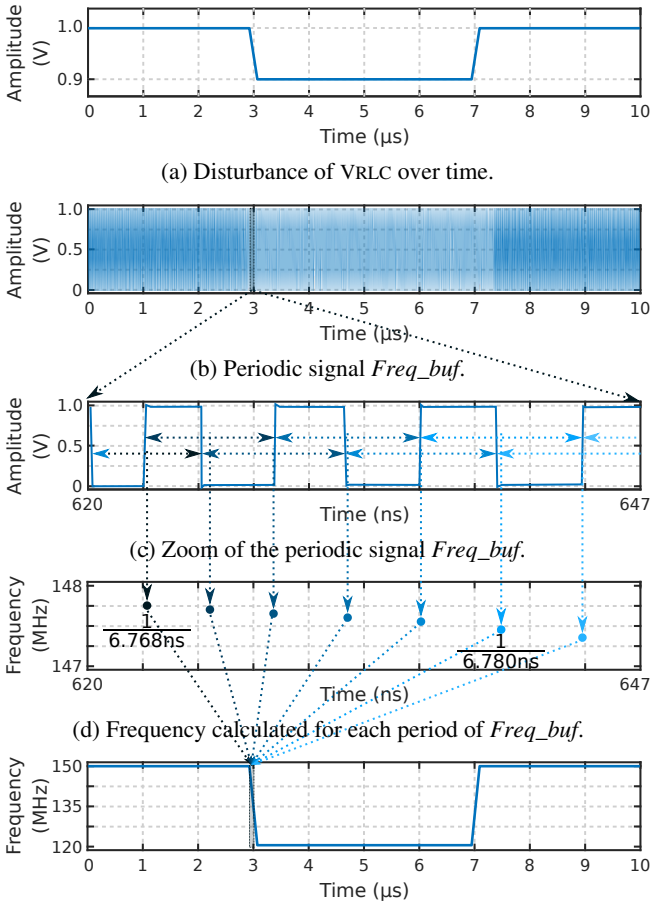
4.5.1.4 Method used to observe the laser-induced IR drop

For the electrical simulations, it is easy to probe any node of the circuit. It is as easy to observe voltage drops in the power supply of the RO (e.g. signal VRLC in Fig. 4.12). In the case of the FPGA, we could not probe the local power supply of the LUTs implementing the RO to monitor local voltage drops occurring in the affected region. We then resort to the fact that the RO's oscillation frequency varies linearly with the supply voltage over a wide range of V_{DD} [49, 51, 78]. In this way, instead of monitoring a voltage drop, we monitored a frequency drop.

The behavior of this effect is illustrated in Fig. 4.17 with a trapezoidal shape voltage drop. For this illustration based on simulation, the amplitude and the duration of the drop were fixed at $100mV$ and $4\ \mu s$ respectively.

Fig. 4.17 gives the obtained results. More precisely, Fig. 4.17a shows the voltage drop considered during the simulation. Fig. 4.17b reports the evolution of the RO's output. Fig. 4.17c is a zoom on the beginning of the voltage drop showing the gradual decrease of the RO's oscillation frequency. By measuring it at half the supply voltage value between all successive pairs of rising and falling edges of $Freq\_buf$ signal, Fig. 4.17d was drawn. It displays the evolution of the frequency as a function of time as well as the effect of the voltage drop which falls from 148 MHz to 120 MHz (Fig. 4.17e).

ISBN: 978-2-11-129250-5



(a) Disturbance of VRLC over time.

(b) Periodic signal *Freq_buf*.

(c) Zoom of the periodic signal *Freq_buf*.

(d) Frequency calculated for each period of *Freq_buf*.

(e) Disturbance of the frequency over time (reconstruction of VRLC).

Fig. 4.17: Simulated effect of a voltage drop on the oscillation frequency of a RO.

4.5.2 Simulation and experimental results for a laser shot applied directly on a Ring Oscillator

The next paragraphs give simulation and experimental results related to a laser shot illuminating directly the RO.

4.5.2.1 Simulation result: classical fault model

According to the classical fault model, only the transient current I_{Ph} is induced by the laser illumination in this case. In order to understand by simulation the effect of a laser shot on a RO according to this classical model, IPh_{Psub_nwell}, R, C and L are not considered in this model. Consequently the power supply is assumed ideal (no IR drop can occur) and all effects on the oscillation frequency are due to the increase of the illuminated inverters' propagation delay.

ISBN: 978-2-11-129250-5

For the related simulation, I_{Ph} current source (Fig. 4.18a) was tuned to provide the parasitic current for $5\mu s$ as depicted in Fig. 4.18b. The resulting periodic signal $Freq\_buf$ is given by Fig. 4.18c in which the lighter blue region represents a time interval of roughly $5\mu s$ when $Freq\_buf$ has a frequency lower than 148 MHz. This lowering of the RO's output frequency is quantified in Fig. 4.18d. As illustrated, the frequency falls from 148 MHz to 100 MHz.

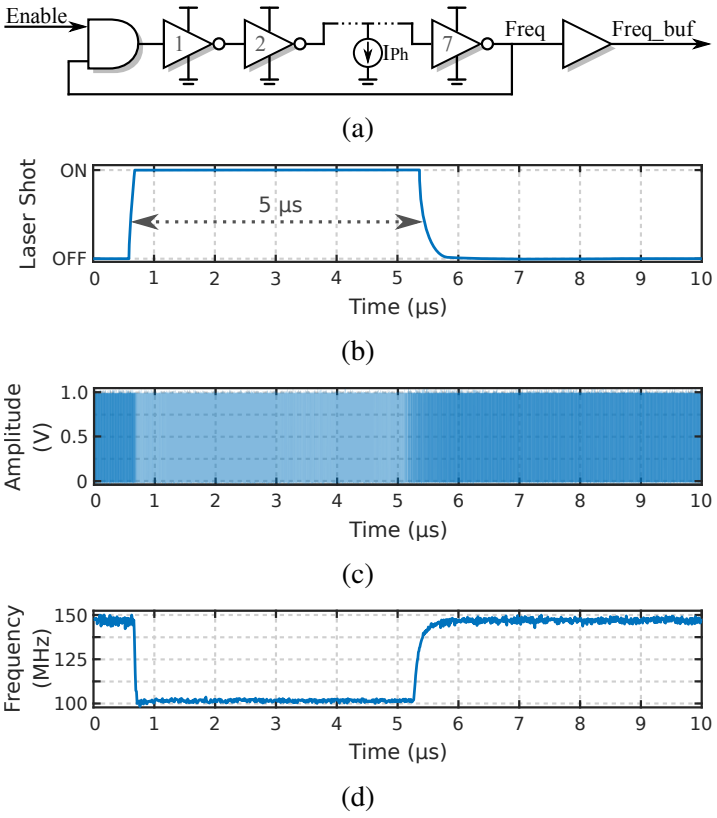


Fig. 4.18: Simulation, according to the classical fault model. Effect of a laser shot illuminating directly a region of the RO. (a) RO block diagram - contribution of I_{Ph} current component only. (b) Laser shot with pulse duration equal 5 μs. (c) Periodic signal $Freq\_buf$. (d) Disturbance of the frequency over time.

4.5.2.2 Simulation result: enhanced fault model

According to the enhanced fault model, a laser shot also induces a direct flow of current between V_{DD} and G_{DD} modeled by IPh_{Psub_nwell} (Fig. 4.19a). By simply setting $I_{Ph} > 0$ (Fig. 4.19a – same current amplitude as in Fig. 4.18a), $IPh_{Psub\_nwell} > 0$ and $(R, L, C) > 0$ (Fig. 4.19a) it is thus possible to get an idea by simulation of the effect of a laser shot according to the enhanced model.

Fig. 4.19b depicts the shape of both I_{Ph} and IPh_{Psub_nwell} currents of duration

ISBN: 978-2-11-129250-5

equal to 5 μs and normalized amplitudes. Fig. 4.19c shows the periodic signal $Freq\_buf$. In this figure a region where the signal $Freq\_buf$ if forced to zero appears. It is due to joint effects of the photoelectric effect I_{Ph} and of the laser-induced IR drop provoked by IPh_{Psub_nwell}. This leads to the evolution of the $Freq\_buf$ frequency shown in Fig. 4.19d. In this case, by considering the enhanced fault model, the RO stops oscillating for $5\mu s$. This indicates that the IR drop induced by IPh_{Psub_nwell} amplifies the effect of I_{Ph} on the RO. This amplification effect will be further analyzed in Section 5.4.1.

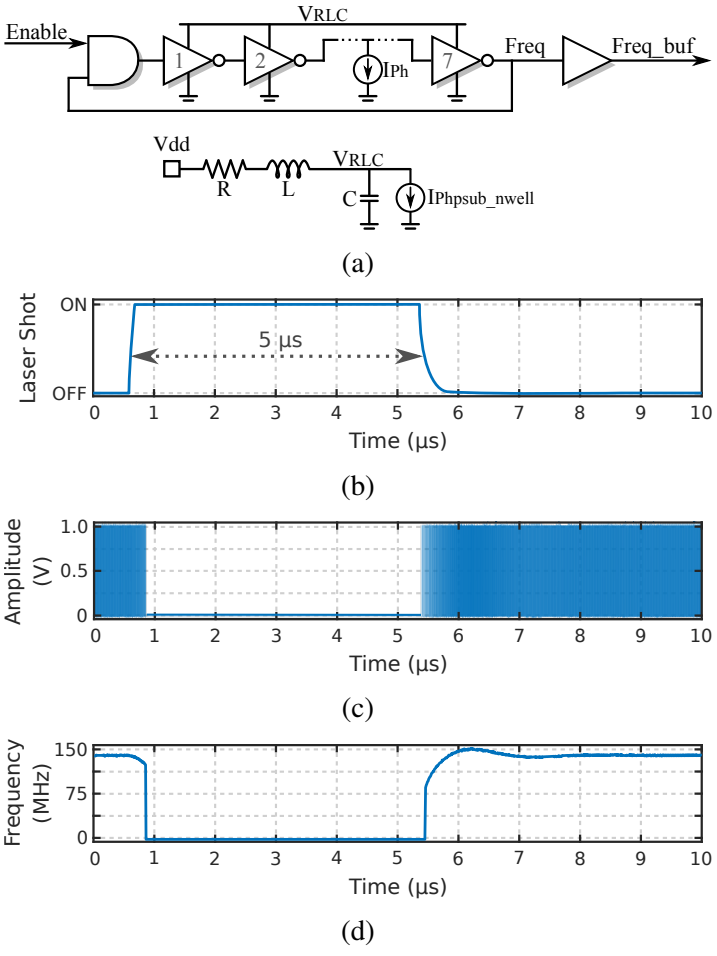


Fig. 4.19: Simulation, according to the enhanced fault model. Effect of a laser shot illuminating directly a region of the RO. (a) RO block diagram - contribution of I_{Ph} and IPh_{Psub_nwell} current components. (b) Laser shot with pulse duration equal 5 μs. (c) Periodic signal $Freq\_buf$. (d) Disturbance of the frequency over time.

ISBN: 978-2-11-129250-5

4.5.2.3 Experimental result: laser shot applied directly on a ring oscillator

After the simulation steps described above, experimental campaigns were launched in order to measure the laser shot effect of the RO oscillation frequency when the laser spot illuminated directly the RO, or part of it.

Fig. 4.20a illustrates the area illuminated by the laser beam, which was applied directly over the RO. Fig. 4.20b depicts the laser shot with duration of 5 μs. The resulting periodic signal $Freq\_buf$ measured on the Virtex-5 is shown in Fig. 4.20c.

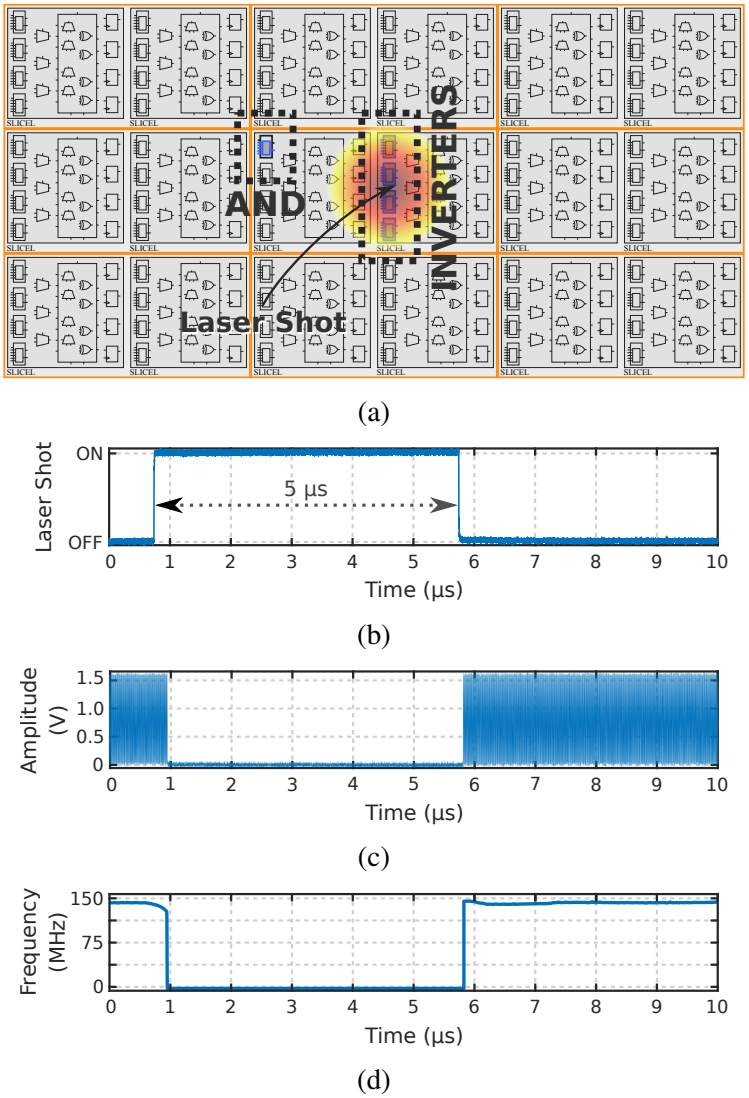


Fig. 4.20: Measured effect (on an FPGA) on the RO oscillation frequency of a laser shot illuminating it directly. (a) Placement of the ring oscillator using the PlanAhead design tool [123]. Here, the laser beam is illuminating the RO. (b) Laser shot with pulse duration equal 5 μs. (c) Periodic signal $Freq\_buf$. (d) Disturbance of the frequency over time.

ISBN: 978-2-11-129250-5

It can be observed in Fig. 4.20c that during the laser shot the signal $Freq\_buf$ stops oscillating. This experimental observation is in accordance with electrical simulation results using the enhanced laser fault model. This is a first element in favor of a better accuracy of the enhanced model over the classical model. Additional evidences were obtained and will be shown in the next section to conclude that the enhanced fault model is in fact more accurate than the classical one.

4.5.3 Simulation and experimental results for a laser shot applied near a ring oscillator

The next paragraphs discuss the effects of laser shots when they do not directly illuminate the RO but rather illuminate part of the IC close to the RO. In this case, the only disturbance able to affect the RO is that of the induced IR drop provoked by IPh_{Psub_nwell} current if this transient current exists.

4.5.3.1 Simulation result: classical fault model

When applying the classical fault model in case of a laser shot striking the IC near the RO, no simulation is required because $I_{Ph} = 0$ and V_{DD} is considered ideal. In this case the classical fault model predicts that there is no effect of the laser shot on the RO behavior as the PN junctions of the sensitive transistors' drain are not illuminated, thus no current is induced. For illustration purpose, Fig. 4.21d shows that the RO's frequency is considered unaffected by the laser shot. If this prediction is not confirmed by experimental results this means that the classical fault model is incomplete and underestimates the spatial distribution of the laser shot effects on ICs. This also indicates that the enhanced model is more adequate.

ISBN: 978-2-11-129250-5

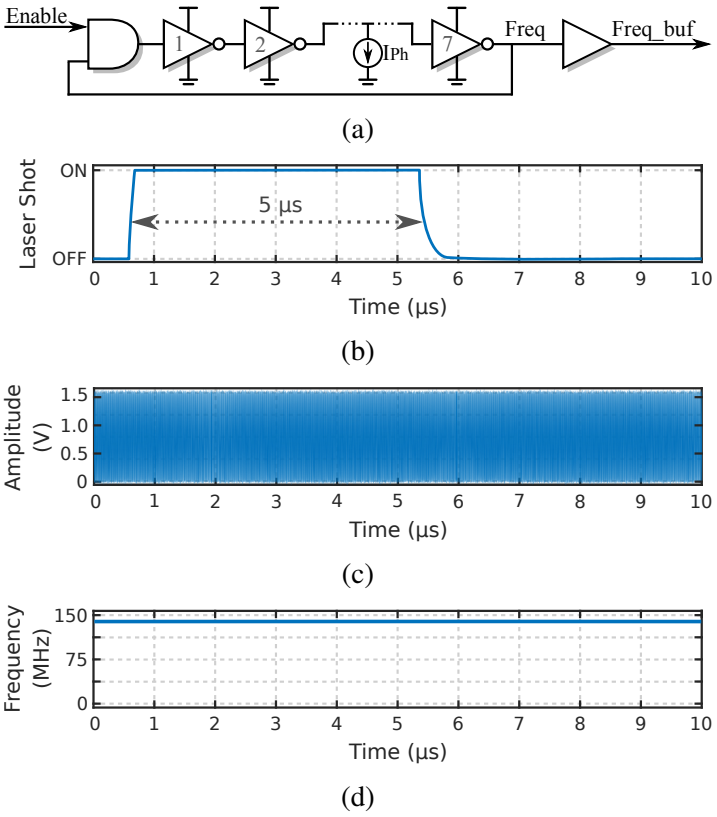


Fig. 4.21: Simulation, according to the classical fault model. Effect of a laser shot illuminating a region near the RO. (a) RO block diagram - contribution of I_{Ph} current component only. (b) Laser shot with pulse duration equal 5 μs. (c) Periodic signal $Freq\_buf$. (d) Undisturbed RO's output frequency over time.

4.5.3.2 Simulation result: enhanced fault model

When choosing the enhanced model instead of the classical model, a simulation has to be run to get an insight on the effect of a laser shot near the RO. Indeed, even if there is no photocurrent injected directly in the RO ($I_{Ph} = 0$ in the simulation), the IPh_{Psub_nwell} current flowing close to the RO alters its supply and thus its operation.

Fig. 4.22 shows the simulation results obtained in the case of a laser shot of duration equal to 5 μs as in former considered cases. The amplitude of IPh_{Psub_nwell} is such that it generated a maximum frequency drop of around 38 MHz (from 148 MHz to 110 MHz). This drop can be observed in Fig. 4.22d that reports the complete evolution of the oscillation frequency. As shown, the evolution has a smoother profile than that observed in previous cases. This is due to the RC filtering effect of the supply voltage network. Frequency bounces are observed around the steady values, which are due to the inductance of the power network. Finally, the profile of Fig. 4.22d shows that the RLC network was designed to have an under-damped response

ISBN: 978-2-11-129250-5

[9].

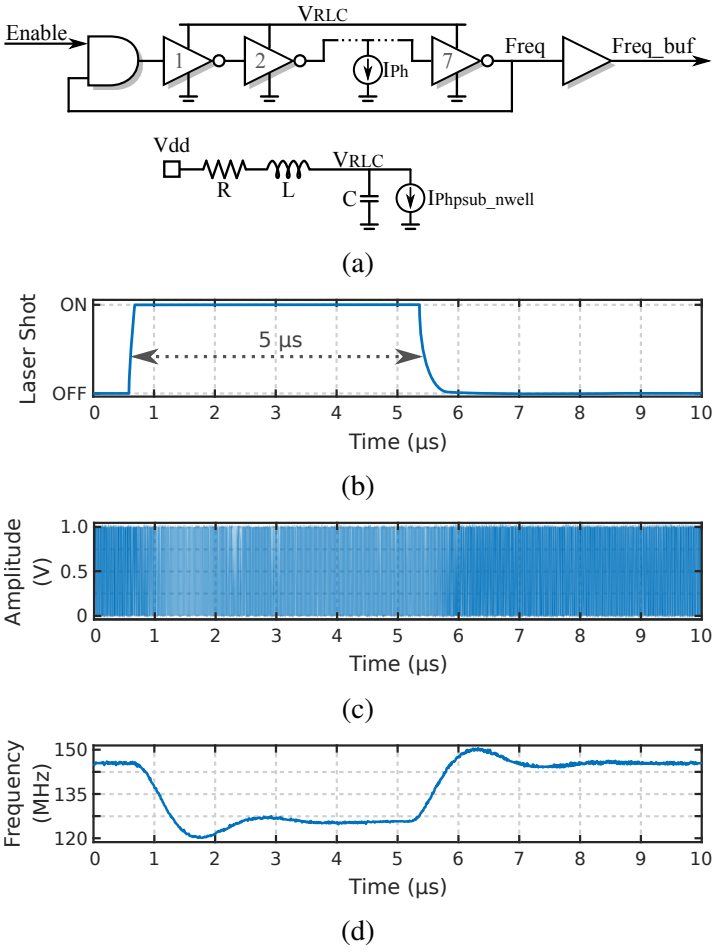


Fig. 4.22: Simulation, according to the enhanced fault model, of a laser shot near the RO. (a) RO block diagram - contribution of IPh_{Psub_nwell} current component. (b) Laser shot with pulse duration equal 5 μs. (c) Periodic signal $Freq\_buf$. (d) Disturbance of the frequency over time.

4.5.3.3 Experimental result: laser shot near a ring oscillator

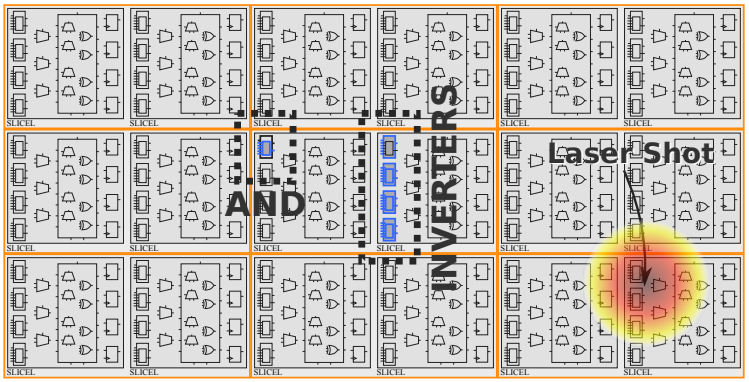
To experimentally observe the effect of a laser shot near a RO, several regions around it (but not over it) were illuminated. This allowed, by monitoring directly the output of the RO with a digital sampling oscilloscope, to locate the $Psub$-$Nwell$ junctions physically interconnected with the LUTs used to implement the RO but also to identify laser spot positions associated to an illumination of the PN junctions related to its design.

Figure 4.23a illustrates that the laser beam is not applied directly over the RO. Fig. 4.23b depicts the laser shot with duration of 5 μs. Fig. 4.23c shows the periodic

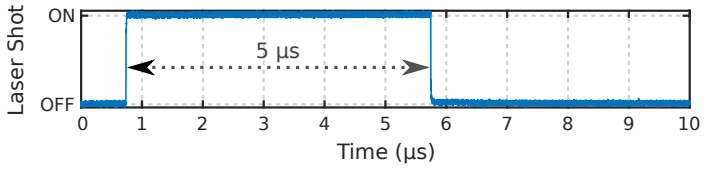
ISBN: 978-2-11-129250-5

signal $Freq\_buf$ typically observed with the oscilloscope when illuminating a region close to the RO. In this figure, a region in lighter blue is visible. It corresponds to an increase of $Freq\_buf$ period. This behavior is similar to the one obtained by simulation in Fig. 4.18c.

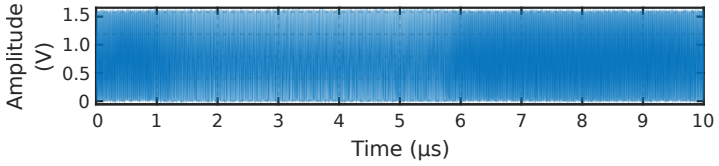
Figure 4.23d shows the evolution of the RO frequency $Freq\_buf$, when the laser is active. As in the simulation, this evolution has a smooth profile due to the RC filtering effect of the supply voltage network. It is also possible to observe, as in the simulation (Fig. 4.22d), the bounces caused by the inductance.



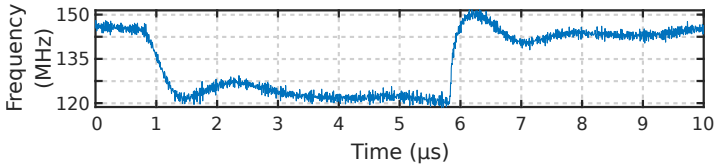
(a)



(b)



(c)



(d)

Fig. 4.23: Measured typical effect on the RO oscillation frequency of a laser shot illuminating a region close to it. (a) Placement of the ring oscillator using the PlanAhead design tool [123]. Here, the laser beam is not illuminating the RO. (b) Laser shot with pulse duration equal to 5 μs. (c) Periodic signal $Freq\_buf$. (d) Disturbance of the frequency over time.

ISBN: 978-2-11-129250-5

4.5.4 Summary

Because we can ascertain (following the work described in [24]) the RO position with preliminary experiments we can be sure that Fig. 4.23d and Fig. 4.20d gives the responses of the RO in two radically different situations (laser spot locations).

In the case associated to Fig. 4.23d the laser was not illuminating directly the RO, thus only inducing current in the Psub-Nwell junctions (IPh_{Psub_nwell}) close to the laser spot location and away from the RO gates. On the contrary, in case of Fig. 4.20d, the laser beam was directly illuminating several gates of the RO's logic, thus activating both I_{Ph} and IPh_{Psub_nwell}.

The comparison of the experimental results with simulation results are characterized by a high level of correlation. Especially the comparison of Fig. 4.23d that gives experimental results of a laser shot near the RO, and Fig. 4.22d that gives simulation results, according to the enhanced fault model, of a laser shot near the RO. These results demonstrate that laser-induced IR drops must not be neglected. This also highlights therefore the superiority of the enhanced fault model proposed in this thesis over the classical fault model. Despite this evidence of the existence and importance of laser induced IR-drop, results suggest that these laser induced IR-drops amplify the effect of I_{Ph}. Indeed, instead of having a drop in frequency of 48 MHz (Fig. 4.18d) when considering only this current (classical model), the frequency falls to zero (Fig. 4.19d and Fig. 4.20d) when the IR drop is taken into account.

Therefore, the IPh_{Psub_nwell} current has to be considered for accurate simulations. This requires to model the PDN. Extracting the PDN for a few gates should be feasible. Doing it for larger circuits requires the use of a proper method capable to automatically provide the PDN for each cell in the circuit. This explains why the next chapter presents a standard CAD tool-based method allowing to simulate laser-induced faults in large-scale circuits.

Together with simulation results, performed by the proposed method, other experimental results will be used to emphasize on the existence of the IPh_{Psub_nwell} current component. More importantly, the relevance of simulating this current will be shown by observing experimentally the phenomena pointed out by simulations and carried out with the proposed simulation flow, which is based on the enhanced fault model.

ISBN: 978-2-11-129250-5

Chapter 5

Standard CAD Tool-Based Method for Simulation of Laser-Induced Faults in Large-Scale Circuits

Laser fault injection may be anticipated or studied by using simulation tools at different abstraction levels: physical, electrical or logical. In Section 5.1, previous works that proposed laser fault simulation tools are reviewed in order to justify the need for the methodology presented in Section 5.2.

5.1 Previous Works on Laser Fault Simulation

5.1.1 Logic Level

The authors of [89] proposed a methodology for multiple fault injection at the Register Transfer Level (RTL). The methodology reduces the fault space of laser fault injection campaigns by using the locality characteristic of laser fault through a partitioning of the RTL description of the circuit. Their efforts involve the development of an RTL fault injection approach more representative of laser attacks than random multi-bits fault injections. Unfortunately, as a RTL fault simulator, the fault model is defined as a logic pulse with different widths. This is not sufficient to take into account neither the laser parameters nor IR drop effects.

5.1.2 Electrical Level

Laser fault simulation at the electrical level is a good tradeoff between speed (logical level) and accuracy (physical level). Therefore, it is possible to represent the laser

ISBN: 978-2-11-129250-5

physical phenomenon in the scope of a whole system. Although the simulation time might be an issue, today's electrical simulators are up to 100x faster than baseline SPICE simulators without loss of accuracy. Furthermore when large circuits are simulated, it is possible to take advantage of hybrid simulations in which only the affected zone of the IC is simulated with SPICE accuracy while the non affected is simulated with gate level accuracy. Section 5.3.8 reports simulation times for the circuit under analysis using different electrical simulators.

To the extent of our knowledge, the most recent fault simulator at the electrical level was proposed by [71]. This simulator is based on the open-source Lifting [22], which allows both 0-delay and delay-annotated simulations of digital circuits using layout information to derive the laser spot location. They also use multi-level simulation to trade speed for accuracy. The major issue with this fault simulator is that it relies on electrical models [39, 44, 101] that are technology dependent. Even though it is possible to dimension these models, it is hard to obtain accurate results when dealing with new technologies.

For instance, the contribution of IR drop effects play a significant role in the fault injection process as reported in the last chapter [117]. The authors of [50] modeled a RC network in the power/ground rails to demonstrate the significant contribution of the current induced by vertical parasitic bipolar junctions inherent to MOSFETs in the fault injection process. However, they did not study the effect of the IR drop induced by laser shots, i.e., its impact in the fault injection mechanism. They also did not extend their work beyond the scope of a single inverter since they manually dimensioned the values of the RC components, which would be a difficult task to do for a large circuit.

5.1.3 Physical Level

Physical level simulations are based on Technology Computer Aided Design (TCAD), which is the simulation of semiconductor processing, device operation and interconnect characterization for technology development and manufacturing. The authors in [69] characterized and analyzed photoelectric effects induced by static 1064 nm wavelength laser on a 90 nm technology NMOS transistor. In [43], Silicon-Germanium Heterojunction Bipolar Transistor (SiGe HBT) models are used in TCAD to investigate single event transients induced by heavy-ion broadbeam and pulsed-laser sources. Although TCAD is the ultimate tool to simulate laser effects on ICs, this simulator is extremely CPU consuming and can only be applied to individual transistors or small circuit areas.

ISBN: 978-2-11-129250-5

5.1.4 Summary

What has been observed so far is that there are improvements of laser fault models in the last years. However these models were developed at the level of a single gate, ignoring thus the effects of laser-induced IR drops at chip level. Regarding laser fault simulators, they usually use the simple fault model in which current sources are attached to the drain and bulk of laser sensitive transistors [59, 121]. This fault model was created at a time in which laser sources with 1 μm to 5 μm spot diameter were used to target only one sensitive PN junction at a time. For advanced technologies this model is questionable. For a 28 nm technology for example, the standard cells have a height value of about 1.2μm, meaning that even lasers with 1 μm spot diameter also illuminate the $Psub$-$Nwell$ junction (see Fig. 4.7) and thus induce significant IR drop in the area surrounding the laser spot.

In order to use a fault model that takes into account the IR drop contribution induced by the current component (IPh_{Psub_nwell}) created between the $Psub$-$Nwell$ junction, it is necessary to model by a RC network the power/ground rails. Modeling the RC network of a large circuit is not a task to be performed manually. In view of this limitation, i.e., that current laser fault simulators do not use complete and accurate fault models, we propose a fault simulation methodology that uses an Electromigration IR drop (EMIR) CAD tool to automatically provide the RC network of the power/ground rails for a given design. It also provides the transient voltage that propagates along the power rails as a result of the IPh_{Psub_nwell} current. The methodology can be used for any circuit designed in any technology supported by the standard CAD tools. Next section presents in details the proposed methodology.

5.2 Proposed Methodology for Laser Fault Simulation Using Standard CAD Tools

This section presents the developed methodology to simulate laser effects on ICs at the electrical level using the enhanced electrical fault model proposed in the last chapter. The simulation flow, which allows to take laser-induced IR drops into account during the simulation of large scale circuits is given in Fig. 5.1. This methodology is based on standard CAD tools: Cadence® Voltus^{TM} [28] for EMIR simulation and Cadence® Spectre® XPS [27] for the electrical/hybrid simulation. The proposed methodology provides: the ability to draw laser-induced IR drop sensitivity maps and fault maps that can help the designer to decide how to harden designs

ISBN: 978-2-11-129250-5

against laser fault injection. It also provides the ability to validate the efficiency of embedded countermeasures.

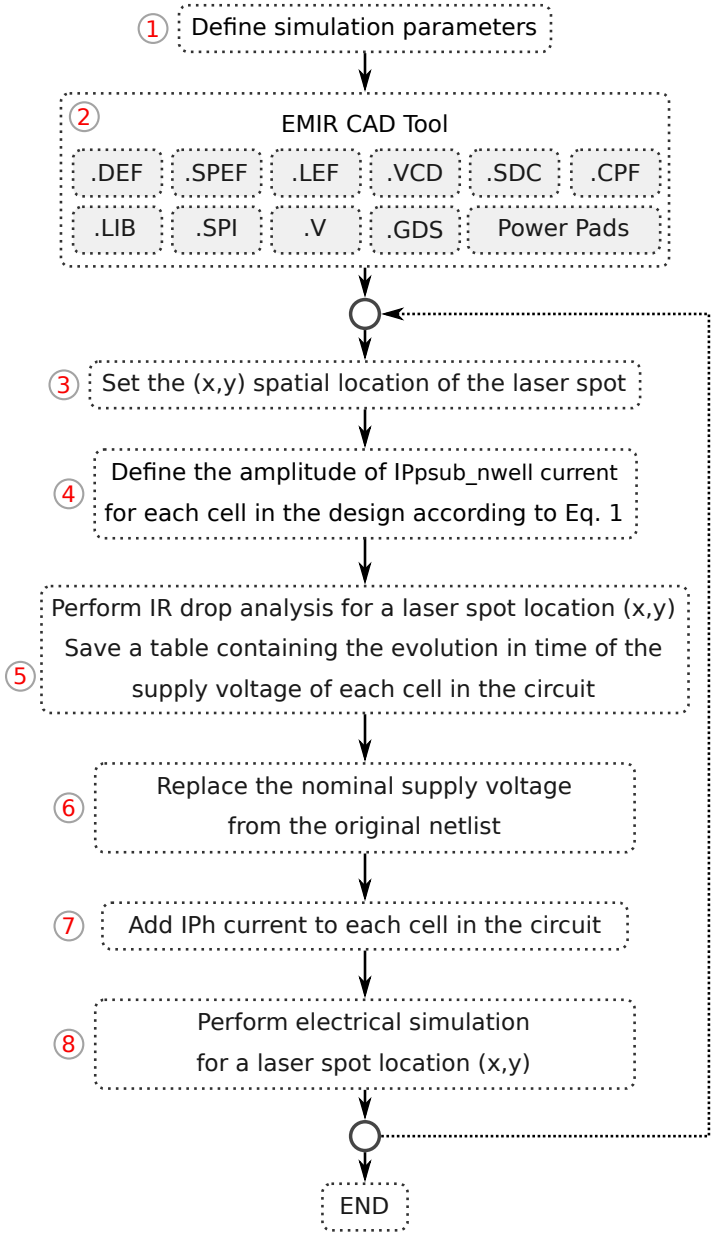


Fig. 5.1: Proposed methodology to simulate the effects of a laser shot on ICs with the enhanced fault model.

This methodology can be quite easily adapted to provide supplementary results to the ones reported in this work. To the best of our knowledge, this is the first methodology allowing to simulate the effects of a laser shot on ICs that simultaneously takes into account the design, the layout in its whole and the laser induced IR drops that have been proven in Chapter 4 to be important and thus have a significant role on the occurrence of faults.

ISBN: 978-2-11-129250-5

Although Cadence tools [26, 27, 28] were used, any other tools [94, 95] able to perform IR drop analysis and SPICE like simulations can be used. Fig. 5.1 is subdivided in steps that are described in the following paragraphs.

Step 1: Defining simulation parameters

In the first step, a shell script file (named 'main.scr') is filled by the user. It defines the parameters characterizing the laser beam. Among them, the user can specify:

- the laser beam diameter,
- the laser power,
- the laser pulse duration,
- the time at which the laser illumination occurs with regard to the zero of the simulation,
- the $(\Delta X, \Delta Y)$ displacement steps of the laser spot when one aims at drawing a fault sensitivity map (details are given in Section 5.3.5.2),
- the initial position of the laser spot being $(X, Y) = (0, 0)$ the default value, which corresponds to the bottom-left part of the layout.

This script is also responsible for calling the necessary tools and scripts for the correct execution of the simulation flow.

Step 2: Data preparation for the EMIR CAD tool

The inputs that are inside the dashed rectangle "EMIR CAD Tool" of Fig. 5.1 are either files automatically generated by the design CAD tool (Cadence® Innovus [26]) or obtained from the design kit of the considered CMOS technology. These files are required to model the RC networks of the power/ground rails and to perform IR drop analysis with Cadence® Voltus^{TM}.

A brief explanation of the content of each file imported into Cadence® Voltus^{TM} is given bellow:

- Design Exchange Format (.DEF): the .DEF file contains information in ASCII format allowing representing the layout of an IC. It represents the netlist and circuit layout. DEF is used in conjunction with LEF to represent complete physical layout of an IC while it is being designed;
- Standard Parasitic Exchange Format (.SPEF): the .SPEF is an ASCII format file listing all parasitic data (R, L, C) of wires of a circuit. This file is used

ISBN: 978-2-11-129250-5

for delay calculation and ensuring signal integrity of a chip which eventually determines its speed of operation;

- Library Exchange Format (.LEF): the .LEF is an ASCII format file containing the representation of a physical layout of an IC. It includes design rules and abstract information about the cells;
- Value Change Dump (.VDC): the .VDC file is used to store information about value changes during simulation for nets and registers, i.e., used to annotate activity at primary inputs of the design;
- Synopsys Design Constraints (.SDC): the .SDC file contains data used to specify the design intent, including the timing, power and area constraints for a design;
- Common Power Format (.CPF): the .CPF file specifies power-saving techniques early in the design process;
- Timing Library Format (.lib): the .lib file contains timing and logical information about a collection of cells;
- SPICE sub-circuits (.spi): SPICE netlist for all cells in the design along with the SPICE models;
- Graphic Database System (.GDS): the .GDS is a binary file containing industry standard for data exchange of IC layout artwork. Used together with SPICE subckts to calculate accurate capacitance and current distribution for the cell;
- Power pad: this file has no standard extension and can be described by the user. It contains power and ground voltage source (X,Y) location or power pad cell names to use during analysis;
- Verilog (.V): the .V file is the verilog netlist consisting of a list of the electronic components in a circuit and a list of the nodes they are connected to.

In the remainder of the thesis, an implementation of the ARM 7 processor (Fig. 5.2) with an area of $110\,\mu m \times 70\,\mu m$ is considered as a test case. More details about the ARM 7 processor are provided in Section 5.3 as for now it will only serve as illustration purposes to simplify the explanation of the proposed methodology. Fig. 5.2 also shows by using a flip-flop cell (DFF) as an example the power-grid network composed of resistors, capacitors and a current source. The latter models the current consumed during the activity of the transistors that compose that cell. This current induces IR drop exclusively due to the switching activity of the transistors.

ISBN: 978-2-11-129250-5

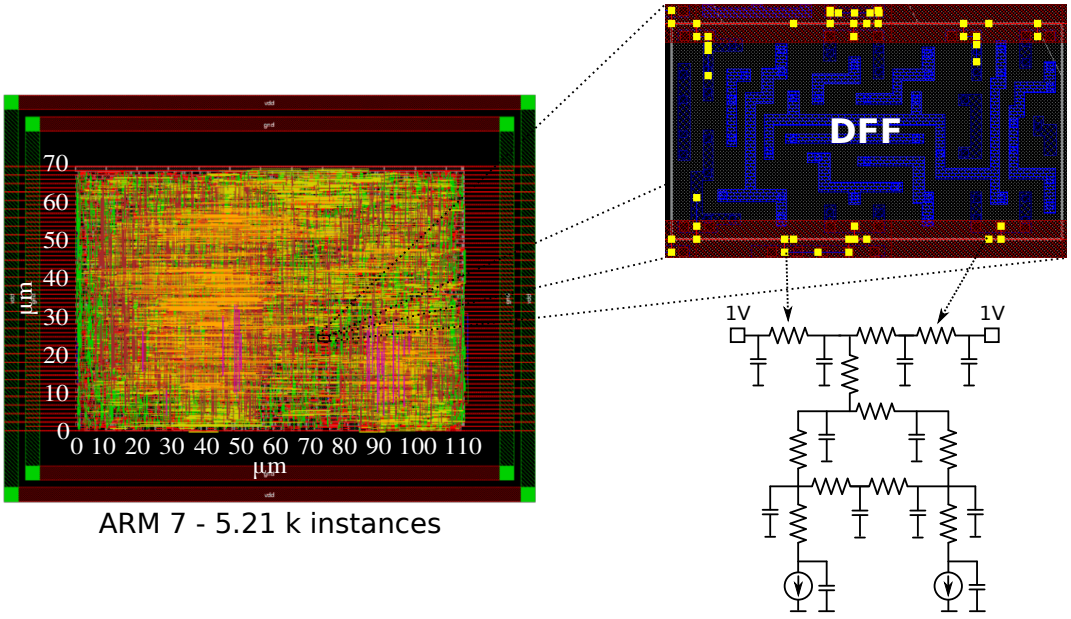


Fig. 5.2: ARM 7: model of the RC network of the power/ground rails provided by Cadence® Voltus^{TM}. In evidence, the RC network of a DFF.

Step 3: Spatial location of the laser spot

This step defines the position of the laser shot with respect to the circuit layout. If the user decides during step 1 to draw a fault cartography, then step 3 (this one) to step 8 are repeated n times, n being the number of simulations required to cover the whole IC surface according to the value of the laser spot displacement step defined during step 1.

For the test case chosen for this thesis (ARM 7 processor depicted in Fig. 5.2), choosing displacement steps $\Delta x = \Delta y$ equal to $5\mu m$ to sweep the whole design surface with the laser spot, beginning at $(x, y) = (0, 0)$ and ending at $(x, y) = (110, 70)$, implies launching $n = 345$ laser shot simulations as Fig. 5.3 illustrates.

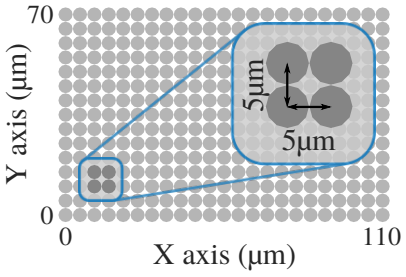


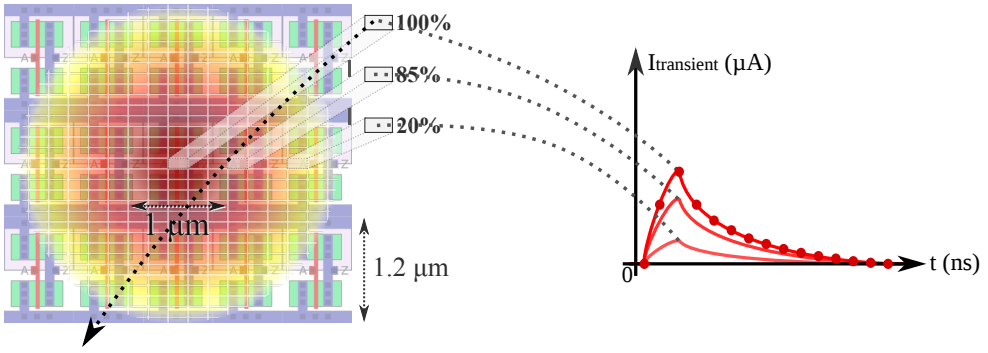
Fig. 5.3: Illustration of the cartography process: each point corresponds to a laser spot position, each position requires a simulation (steps 3 through 8).

ISBN: 978-2-11-129250-5

Step 4: Definition of the IPh_{Psub_nwell} amplitude

The simulation of the effect of a laser shot starts by specifying the amplitude of the different current sources constituting the laser fault model (Fig. 4.8) applied to all standard cells in the circuit illuminated by the laser. Therefore it is necessary to know which instances of the DUT are affected by the laser.

Several ways can be adopted to fix the values of these current sources. The proposed methodology takes advantage of a Cadence® Voltus^{TM} feature. It allows to apply an amount of current to a defined region. In this way, several small rectangular regions are defined to draw the footprint of the laser shot on the IC surface. The amplitude of the small rectangular regions is then set so that the footprint follows the binormal distribution of the photocurrent defined by (2.1). Fig. 5.4 illustrates how the rectangular regions can be used to apply the laser power (current induced by the laser) to each rectangle. The rectangular regions are only applied to areas where Nwell is present. Therefore, if a rectangular region, is for example, over a NMOS transistor or at the edge of the IC (in this case the laser illuminates only part of the IC), no current will be induced in that area as there is no Psub-Nwell junction.




```
create_current_region -current {1.500ns 0.000mA 1.505ns 0.820mA 1.510ns 1.000mA
                                1.515ns 0.950mA ... 1.800ns 0.000mA}
                      -layer M2
                      -intrinsic_cap C
                      -loading_cap C
                      -region "1.50 1.50 1.75 1.75"
```

Fig. 5.4: Laser-induced current regions applied over standard cells of a CMOS 28 nm technology. The current amplitude of each region is defined by eq. (2.1).

The code snippet in Fig. 5.4 represents the characterization of the rectangle located at the center of the laser spot. This code describes piecewise linearly a current with a double exponential shape. In this example, the time step is equal to $5\,ps$, the peak value of the current (I_{Ph_peak}) which starts rising at $1.500\,ns$ occurs at $1.510\,ns$ and is equal to $1\,mA$. Other parameters such as capacitances are extracted from .lib

ISBN: 978-2-11-129250-5

and .spi files of the technology for each illuminated instance. The resolution of each rectangle (square in this example) is $250\,nm$ as shown by the last parameter of the code: -region "$x1$ $y1$ $x2$ $y2$", therefore $x2 - x1$ = 1.75 μm - 1.50 μm = $250\,nm$ (the same is valid for $y2$-$y1$). The dimension of the rectangle can be changed accordingly to the precision needed to model the laser spot. Except for the current amplitude, the same other characteristics are applied to all rectangles. Each rectangle therefore has its own amplitude defined by the binormal distribution of the photocurrent (equation 2.1).

Step 5: IR drop analysis

In this step, Cadence® Voltus^{TM} is used to perform a laser-induced IR drop simulation for the laser spot location defined in step 3. All other simulation parameters being kept constant (spot diameter, intensity, etc).

To clarify, IR drop can be defined as the power supply noise induced by currents flowing through the resistive parasitic elements of the power distribution network. In this work, the laser-induced IR drop is also considered, meaning that the laser-induced current IPh_{Psub_nwell} will accumulate with the dynamic current of a cell, thus increasing its IR drop while the laser and the IC are active ($IPh_{Psub\_nwell} \neq 0$).

Figure 5.5a gives three IR drop cartographies associated to three laser spot locations. The spot locations number (130, 132 and 137) corresponds to the simulation number. Considering a displacement steps $\Delta x = \Delta y$ equal to $5\mu m$, then simulation 1 represents $(x, y) = (0, 0)$. Simulation 130 represents $(x, y) = (70, 30)$ and so on and so forth until the last simulation 345 ($(x, y) = (110, 70)$).

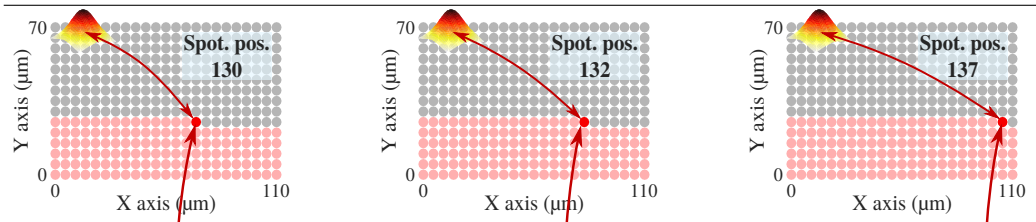
Figure 5.5b shows the maximum IR drop and ground bounce for a laser shot applied to the three positions given as an example (130, 132 and 137). The effects caused by the laser and observed in this figure, will be further explained in details in section 5.3 as for now this section focuses on discussing the methodology and not the simulation results.

Figure 5.5c shows one of the instances used as example (U205). The location of this instance is pointed out by a small white rectangle in Figure 5.5b.

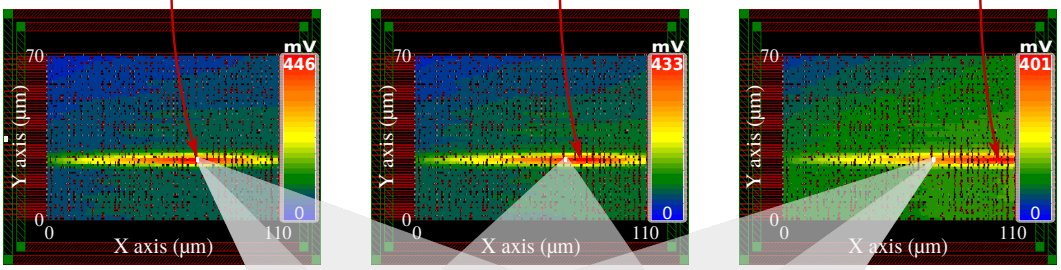
For each iteration of this step, a table containing the evolution in time of each instance's voltage swing amplitude (V_{DD} - IR drop - G_{ND} bounce) is saved for future analyses since different instances are affected by the laser shot. Table 5.1 gives the remaining voltage swing of three different instances at the peak of the transient current (Fig. 2.1d) induced by three laser shots applied at the considered locations.

In this example, for the laser spot position no. 130 (cf. Table 5.1) the instances

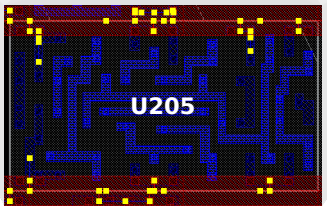
ISBN: 978-2-11-129250-5



(a) Illustration of the cartography process: each point corresponds to a laser spot position, each position requires a simulation (steps 3 through 8). In this example, the system is ready to simulate positions 130, 132 and 137.



(b) Maximum IR drop + ground bounce after simulatng three different laser spot positions as defined in step 3.



(c) Instance U205 (flip-flop) used as example.

Fig. 5.5: Laser-induced IR drop cartographies for three different laser spot locations. The laser spot diameter is equal to 5 μm in this example.

Table 5.1: Voltage swing of three instances of the DUT at the apex of three different laser shots. The nominal voltage swing is equal to 1 V

Spot pos. 130 Voltage Swing	**Spot pos. 132 Voltage Swing**	**Spot pos. 137 Voltage Swing**
U205: 0.554 V	U205: 0.670 V	U205: 0.815 V
U1942: 0.554 V	U1942: 0.677 V	U1942: 0.818 V
U1088: 0.555 V	U1088: 0.669 V	U1088: 0.814 V

are more affected (lower voltage swing) as the epicenter of the laser spot is closer to these three instances (the same can be observed in Fig. 5.5). For laser spot positions nos. 132 and 137, the instances are less affected since the laser spot is increasingly more distant. To illustrate this effect, the evolution in time of U205's voltage swing amplitude is shown in Fig. 5.6 for the three laser spot positions nos. 130, 132 and 137.

ISBN: 978-2-11-129250-5

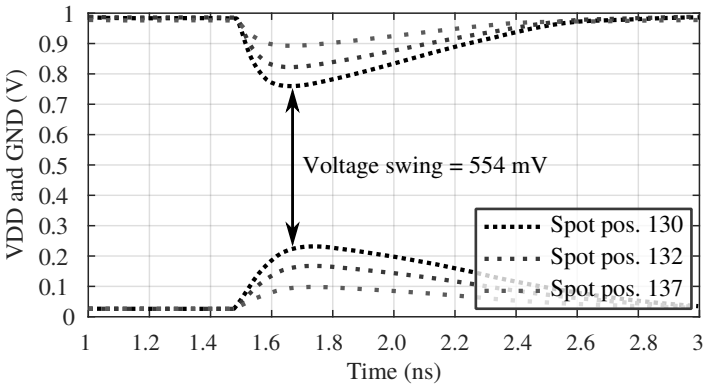


Fig. 5.6: The evolution in time of U205's voltage swing amplitude.

Step 6: Replacing the ideal supply voltage by estimated V_{DD} and G_{ND} waveforms

After the estimates with Cadence® Voltus^{TM} of the IR drops induced in the power/ground rails by the IPh_{Psub_nwell}, a shell script is used to replace the ideal V_{DD} and G_{ND} sources in the original SPICE netlist of the DUT by the IR drop waveforms saved during step 5 for each instance in the circuit. Fig. 5.7 illustrates this process using an inverter as an example. This figure shows the creation of two voltage sources (PWL type) for the instance U527. One voltage source is used to model the ground bounce (GND_U527) and the other is used to model the IR drop (VDD_U527). Similar voltage sources are created for all the illuminated instances of the circuit.

ISBN: 978-2-11-129250-5

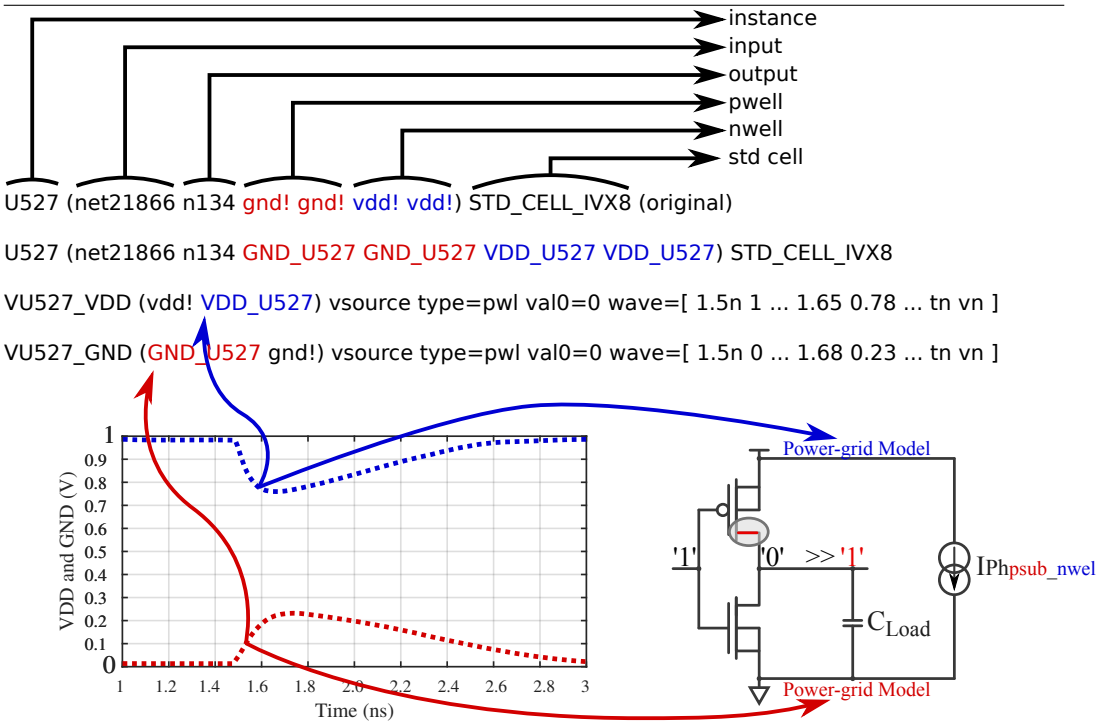


Fig. 5.7: Illustrating the process of replacing the ideal V_{DD} and G_{ND} in the original SPICE netlist of the DUT by the IR drop waveforms saved in step 5 for each instance of the circuit.

Step 7: inserting I_{ph}

After inserting the effects of IPh_{Psub_nwell} (IR drop and ground bounce) in the original spice netlist, a shell script is used in order to add current sources between the drain and bulk of illuminated PMOS and NMOS transistors. They model the classical I_{ph} currents causing the voltage transient at the output of the illuminated gates. It should be noticed that only some of these current sources are activated depending on which drain's PN junction are reversely biased or not. To determine which of them should be turned ON, it is thus necessary to run a fault free electrical simulation and save a golden table with the inputs and outputs of each instance as a function of time. Fig. 5.8 illustrates the process of adding the current source I_{ph} to an inverter. At this point, the proposed model has been applied to each instance of the circuit.

Knowing that the IPh_{Psub_nwell} current is defined as a $factor \times I_{ph}$ because of the parameter S in eq. (2.1) which is related to the area of Nwells and the area of transistors drains, it is possible to compute the $factor$ value to be applied to each instance by analyzing the .lef and netlist files that contain informations regarding each available standard cell. This allows to estimate the area of the affected PN

ISBN: 978-2-11-129250-5

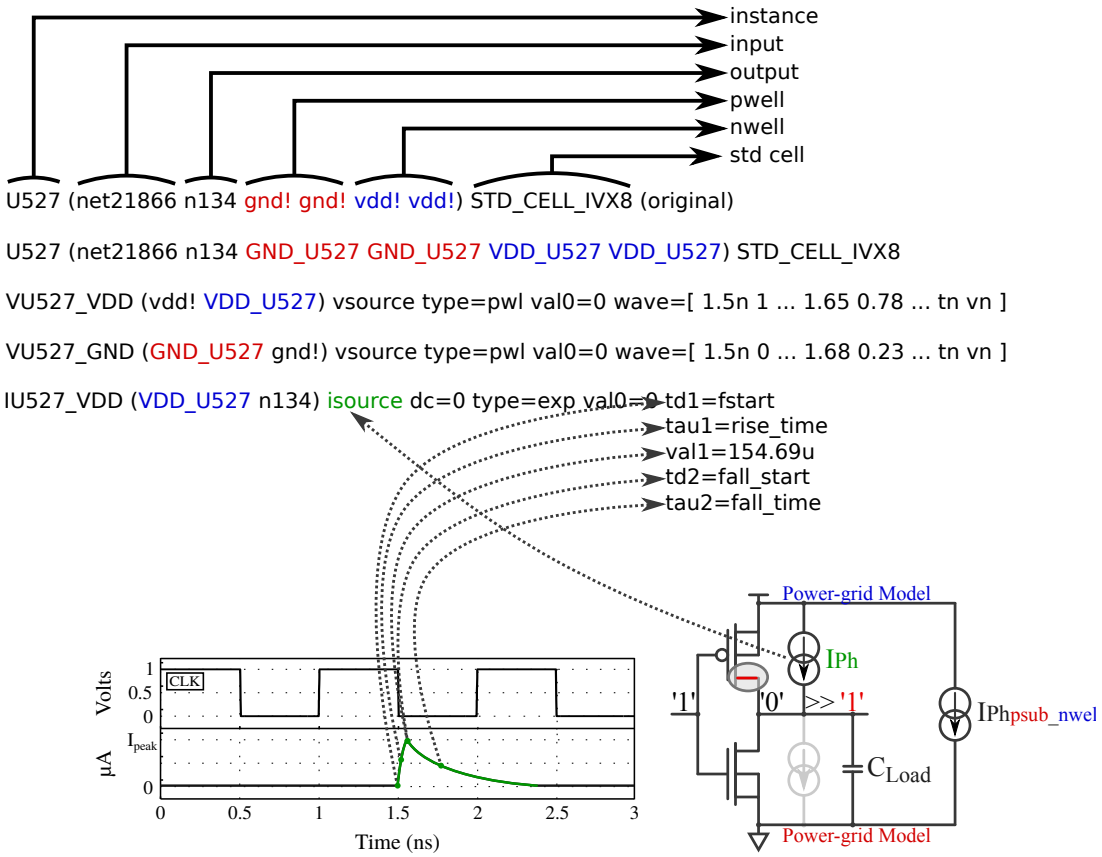


Fig. 5.8: Illustrating the process of adding a current source I_{ph} between the drain and bulk of an instance. This procedure is applied to all illuminated instances of the circuit.

junction of a particular transistor's drain as well as the area occupied by the $Nwell$, and thus deduce a rational estimate of S (eq. 2.1).

Step 8: Electrical/hybrid fault simulation

This step consists in running an electrical simulation of the modified spice netlist for each laser shot position specified at step 3. However, because electrical simulations are time consuming, hybrid simulations are performed to decrease the overall simulation time.

In these hybrid simulations, run with Cadence® Spectre® XPS simulator, solely the region of the circuit containing the mostly affected instances by the laser shot are simulated with SPECTRE accuracy. To delimit this region a threshold voltage, th, is defined based on all voltage swing values (V_{DD}-G_{ND}) provided by tables likeTable 5.1. If the remaining voltage swing value of an instance is higher than V_{DD}-th, it is considered as not affected by the laser shot. This is the case of instances which are

ISBN: 978-2-11-129250-5

far away from laser spot epicenter (Table 5.1). For example, if th is set equal to 5% of the nominal $V_{DD} = 1\,V$, then all instances with a residual voltage swing higher than $950\,mV$ are simulated at the logic abstraction level.

Table 5.2 gives the number of instances simulated at the logic abstraction level for different th values and different spot locations. The considered spot locations were randomly selected with the purpose to show that the number of affected instances changed depending on the laser spot location. As shown, increasing the th value allows managing the trade off between speed (increasing the number of gates simulated at the logic abstraction level) and accuracy.

Table 5.2: Number of instances simulated at the logic abstraction level for different th values and three spot locations. Laser spot diameter equal to 5 μm in this example (5.21k instances in the circuit).

th % of V_{DD}	No. of instances (spot loc. 130)	No. of instances (spot loc. 137)
5%	1676	1646
10%	4744	4866
15%	4878	5033
20%	5005	5152

After this step is completed, the methodology returns to step 3 to simulate the effects of a laser shot in another position. Steps 3 through 8 are repeated 345 times (in this case) until the cartography process finishes. After all simulations have been performed, the methodology provides the user with several kinds of results for analysis. These results are presented in the next section.

5.3 Laser Fault Simulation Results

In order to simulate the effects of laser-induced faults on complex systems, simulations were performed on different circuits. However only the results obtained for an ARM 7 processor are shown in details. All circuits were synthesized using a 28 nm CMOS technology.

5.3.1 Circuit Inventory

The nominal supply voltage of the DUT is 1 V and the clock period is $1\,ns$. The ARM 7 has an area equal to $110\,\mu m \times 70\,\mu m$ occupied by 5.21 k instances, 5.34 k

ISBN: 978-2-11-129250-5

nets and 90 k nodes. The power-grid model generated by Cadence® Voltus^{TM} has 100 k resistors and 90 k capacitors.

5.3.2 Laser Spot Diameter

Laser sources used to produce faults can be characterized by their beam diameter equal to 1 μm, 5 μm or 20 μm and a wavelength of 1064 nm. Although the minimum diameter of a laser spot is 1 μm (given the laws of optic) its effect area extends far beyond [34, 97]. Consequently, a laser spot does not induce a single transient current in a single cell, but several transient currents at different sensitive nodes of the target. Without loss of generality, a spot diameter of 1 μm and 5 μm were chosen for the experiments reported below.

5.3.3 Spatial Distribution of the Laser-induced IR Drop

Laser illumination induces IR drops, which effect spreads over the IC surface. It is thus not limited as indicated by the classical fault model to the few transistors or logic gates illuminated by the beam. One can thus wonder how far and how the effect of a laser shot spread (the shape of its effect area). To give a first insight about this spreading, Fig. 5.9a to 5.9c give the IR drop maps obtained with Voltus for the considered test case in presence or not of a laser shot.

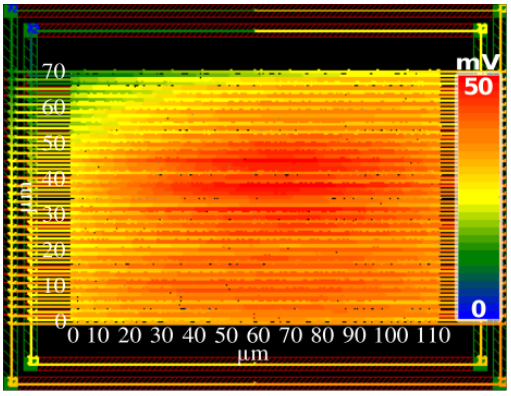
In Fig. 5.9a, the IR drop across the rails reach the maximum value of $50\,mV$. This drop, which is uniquely due to the normal switching activity of the transistors, seems to affect quite uniformly almost the whole circuit surface. Indeed, there is no specific spot at which the IR drop is significantly stronger.

Fig. 5.9b (obtained at the end of step 5 of the proposed method) illustrates how the laser effect propagates on the circuit. In presence of a single laser shot with a spot diameter of 5 μm at coordinates x=68 μm, y=25 μm, the effect area extends along the X axis through the power-grid main metal lines for more than 100 μm. It has a shape that is stretched horizontally along the power supply rails (standard cell rows) as they provide a propagation path to the laser-induced IR drop and ground bounce. Whereas its extension along the Y axis is only approximately 7 μm ($\approx$ 6 standard cell row height). The peak value of the induced drop in the power lines is 446 mV (Fig. 5.9b). At this time, the voltage swing is reduced to 554 mV, a value far below the nominal core voltage of 1 V.

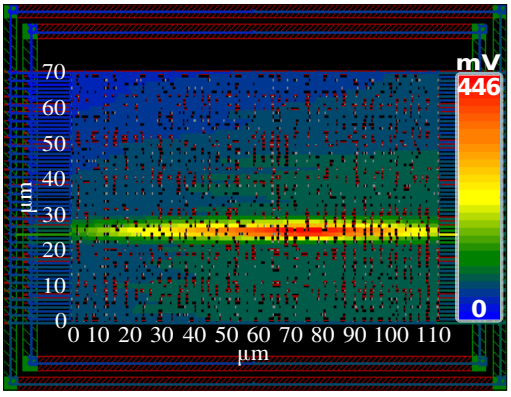
Fig. 5.9c has similar characteristics to Fig. 5.9b. In case of Fig. 5.9c however, the laser spot diameter is equal to 1 μm and the peak value of the induced voltage

ISBN: 978-2-11-129250-5

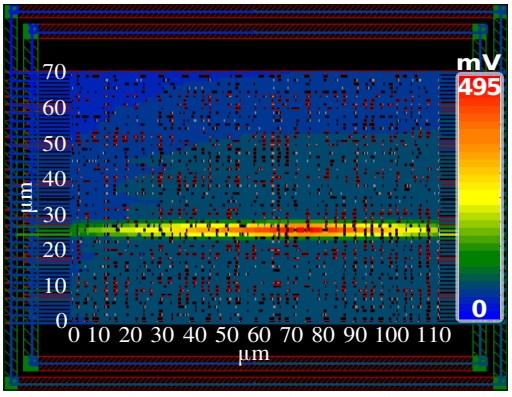
drop in the power lines is 495 mV. Thus reducing the voltage swing to only 505 mV.



(a) Normal operation conditions. Voltage drop due to the switching of the transistors only.



(b) Laser shot with a spot diameter equal to 5μm.



(c) Laser shot with a spot diameter equal to 1μm.

Fig. 5.9: Maximum supply voltage drop of ($V_{DD} - G_{ND}$) for the ARM 7 layout with 5k+ instances.

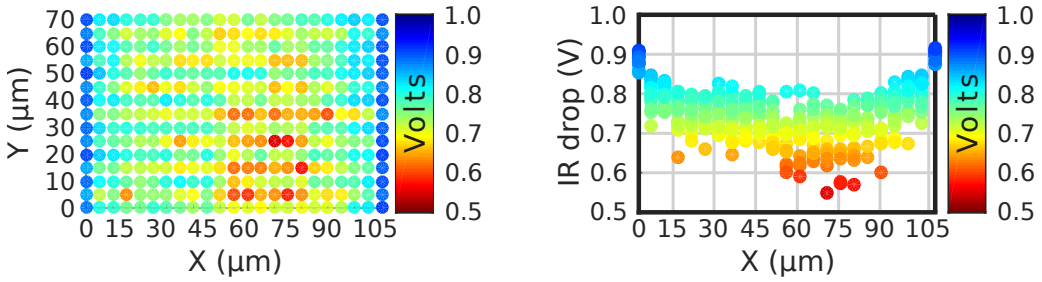
From the above observations, depending on the laser power, laser shots can induce faults in the circuit, such as timing errors or even data disruption quite far from the laser spot location. Indeed, dozens of standard cells are inside the laser effect area when considering a 28 nm technology, and hundreds of them can experience a significant voltage drop even for a spot diameter equal to 1μm.

5.3.4 Laser-induced Sensitive Zones

This section gives an insight on how to use some results obtained from the proposed method to harden the design against laser-fault injection. Fig. 5.10a and 5.11a show the maximum laser-induced IR drop for simulations considering a laser spot diameter equal to 5 μm and 1 μm respectively. Each point in both figures correspond to a laser shot. Fig. 5.10b and 5.11b show the same results as Fig. 5.10a and 5.11a,

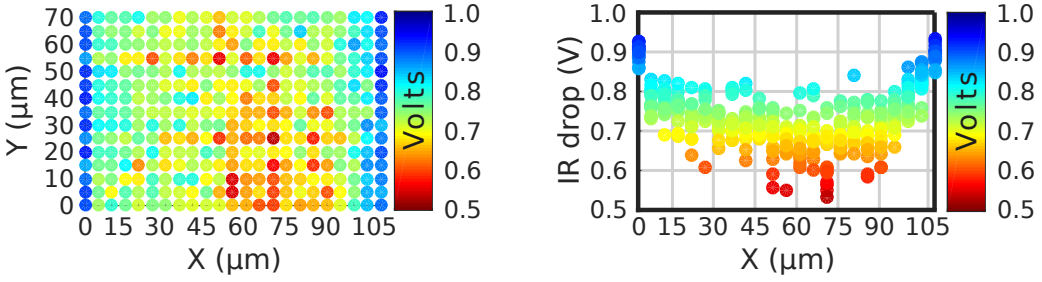
ISBN: 978-2-11-129250-5

however in a different perspective, in this case x axis by z axis (IR drop). With these figures a designer can address the zones of the IC where more IR drop are observed. An example of how to address these sensitive zones will be given in the next paragraphs.



(a) X,Y plane. (b) X,Z plane.

Fig. 5.10: ARM 7: maximum laser-induced IR drop for a laser spot diameter equal to 5 μm. Each point corresponds to a laser shot.



(a) X,Y plane. (b) X,Z plane.

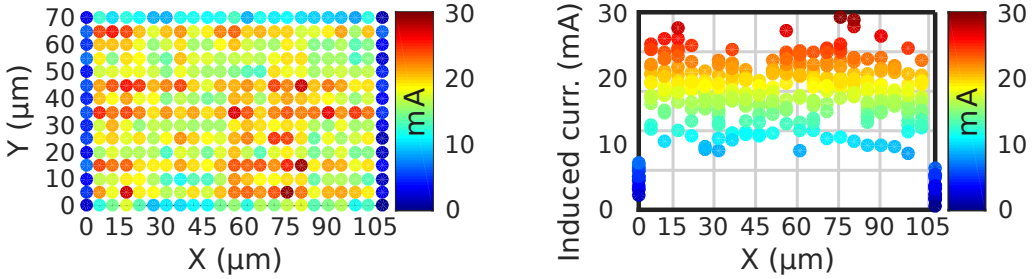
Fig. 5.11: ARM 7: maximum laser-induced IR drop a laser spot diameter equal to 1 μm. Each point corresponds to a laser shot.

The total current consumption for the circuit under normal operation is 13.202 mA. The total induced current when considering the maximum laser-induced IR drop (worst case) is 24.408 mA and 20.398 mA for laser spot diameters equal to 5 μm and 1 μm respectively (Fig. 5.12a and 5.13a). An additional of 11.206 mA and 7.196 mA is thus induced by the laser shot applied at particular coordinate (x=68 μm, y=25 μm in Fig. 5.9b and Fig. 5.9c) when considering both laser spot diameters of 5 μm and 1 μm respectively.

The figures for the maximum laser-induced current (Fig. 5.12a and 5.13a) do not correspond exactly with the figures reporting the maximum laser-induced IR drop (Fig. 5.10a and 5.11b). This happens because the standard cells have the same heights but different widths, therefore, larger standard cells induced more current (IPh_{Psub_nwell}) as their Nwell have a larger area. This observation is directly related

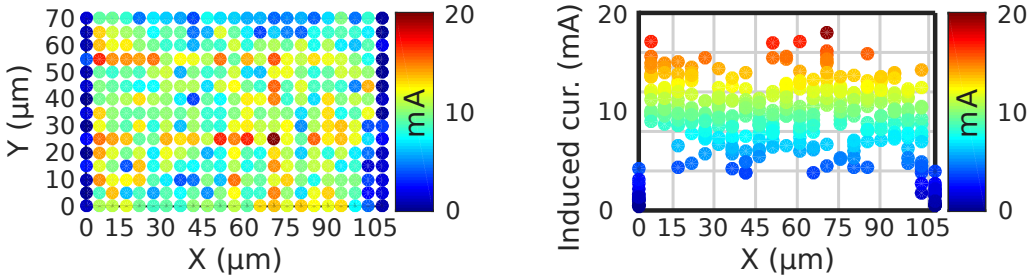
ISBN: 978-2-11-129250-5

with the parameter S of equation (2.1). Another important factor is the presence of empty spaces between the standard cells (when a filler cell is not placed), in this case, current is induced only in adjacent regions where biasing contacts are present.



(a) X,Y plane. (b) X,Z plane.

Fig. 5.12: ARM 7: maximum laser-induced current (IPh_{Psub_nwell}) a laser spot diameter equal to 5 μm. Each point corresponds to a laser shot.



(a) X,Y plane. (b) X,Z plane.

Fig. 5.13: ARM 7: maximum laser-induced current (IPh_{Psub_nwell}) a laser spot diameter equal to 1 μm. Each point corresponds to a laser shot.

Table 5.3 provides some useful information that can be used in combination with Fig. 5.10a and 5.11a (spot $\varnothing$ equal 5 μm and 1 μm) to harden sensitive zones of the circuit against IR drops. It give the number of violations of the voltage guard bands, i.e. the number of cells with a voltage swing lower than 0.9 V (V_{DD} = 1 V). It also gives the total coupling capacitance of the circuit, which is composed of:

- Grid coupling capacitance: this is the capacitance between power and ground stripes in the design. This capacitance is extracted using the .QRC technology file provided by the foundry. It takes into account effects of all the neighboring geometries. Generally, this capacitance is equivalent to around 5% of the total capacitance offered by the die.
- Gate coupling capacitance: this is the cell intrinsic capacitance (or gate capacitance) between the power and ground pin. Non-switching cells act as

ISBN: 978-2-11-129250-5

decoupling capacitors and offer this intrinsic capacitance to the power-grid. This capacitance is extracted with the SPICE netlist and SPICE models of the cell by running an AC sweep. It could account for about 50% of total capacitance in the design, although it is design dependent.

- Loading coupling capacitance: this is the output pin loading capacitance which comes from the .SPEF file. It includes signal wire loading and pin capacitance from the .lib file. Loading capacitance and on-resistance is calculated per instance basis. The loading capacitance could account for up to 50% of total capacitance in the design, although it is also design dependent. This loading capacitance is connected through the MOSFET on-resistance, which is generally high and diminishes the effect of loading capacitance during IR drop analysis.

Figure 5.14 illustrates the aforementioned capacitances used during IR drop analysis. By applying a voltage to a capacitor, and thus measuring its charge, the ratio of the charge Q to the voltage V will provide the capacitance value, which is given as: $C = Q/V$.

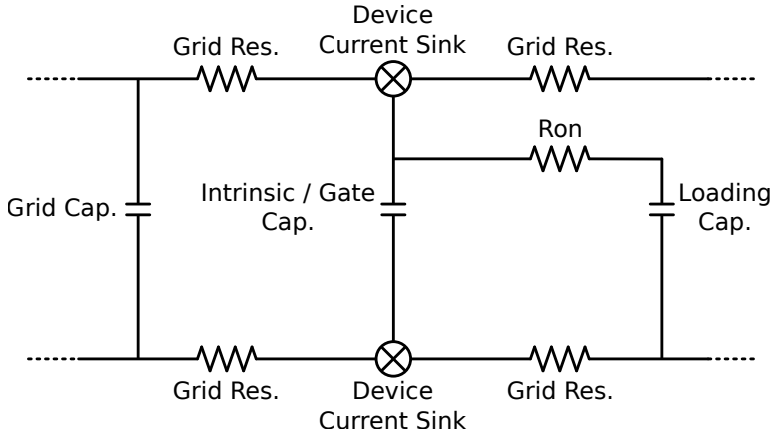


Fig. 5.14: Abstraction of a power distribution network. In evidence the three types of capacitors used during IR drop analysis: grid capacitance, gate capacitance and loading capacitance.

This explains why the values of gate coupling capacitance and loading coupling capacitance change (Table 5.3) according to the amount of IR drop in that region. For instance, for the laser spot diameter equal to 5 μm, more cells are affected, therefore the total amount of induced IR drop in this case is higher than in the case of a laser beam with diameter equal to 1 μm.

To better clarify, in Table 5.3 the maximum voltage swing for a 5 μm laser spot diameter is equal to 0.554 V (IR drop equal to 0,446 V), which is lower than the

ISBN: 978-2-11-129250-5

maximum voltage swing in the case of a 1 μm laser spot diameter (0.505 V). This value is accounted for only one standard cell that observed this voltage drop. However, when considering all the affected zones by the laser, more cells experience an increased IR drop in the case of a 5 μm laser spot diameter.

Table 5.3: ARM 7: IR drop, power and capacitance analysis of the design in normal operation and under laser illumination.

Attribute	**Normal op.**	**Spot ⌀ = 5 μm**	**Spot ⌀ = 1 μm**
Peak Dynamic Current	13.202 mA	24.408 mA	20,398 mA
Minimum Voltage Swing	0.957 V	0.554 V	0.505 V
# Violations ($< 10\%$ V_{DD})	0	2030	1913
Grid Coupling Cap.	1.438 pF	1.438 pF	1.438 pF
Gate Coupling Cap.	0 pF	2.920 pF	0.960 pF
Loading Coupling Cap.	36.974 pF	39.894 pF	37.934 pF
Total Coupling Cap.	38.412 pF	44.252 pF	40.332 pF
Additional Cap. Required	0 pF	42.125 pF	39.845 pF

For simplicity, the analysis that follows will be made only for a laser spot diameter equal to 5 μm. The decoupling capacitors (decap) optimization method discussed in this section computes the additional decap required in the design to meet the IR drop threshold of the design. The additional decap required is translated into additional explicit decap cells that can be placed in the design, which would provide the necessary intrinsic capacitance to meet the IR drop threshold.

Cadence® Voltus^{TM} analyzes each node voltage in the design. Based on user-specified voltage limit, whenever the node voltage is below the limit within a clock cycle, it computes the additional charge required to put back the charge onto the grid. If more than one clock period is simulated, Voltus^{TM} computes the total required charge for the node for each clock period and picks the maximum total charge that was computed for any one clock cycle. In this way, the additional charge is computed for each node in the design.

As suggested in Table 5.3, an additional 42.125 pF of decoupling capacitance is required to meet the voltage swing threshold of 0.9 V for the given laser parameters. Decaps operate as charge reservoirs to stabilize the power/ground grid and to minimize transient voltages. Before the advent of 90 nm technology, design teams would typically add a significant number of decoupling capacitors between the power and ground rails to smooth any transient voltage on the rails and to minimize transient voltage spikes caused by the switching of cells. As a result, the noise on the power

ISBN: 978-2-11-129250-5

grid was minimized [32, 83, 113]. For circuits designed below 90 nm, however, the increased leakage from decoupling capacitors begins to add to the power consumption, so it was no longer possible to liberally add them to minimize transient voltages. For low-power and designs below 90 nm, analyzing where to add decoupling capacitors is of critical importance [8, 33, 104, 114].

The challenge for a design team thus become the optimization of the size and location of the decoupling capacitors, to make sure IR drop do not cause timing failure, while managing on-chip leakage power since each added decap cell add to the overall leakage.

Indeed, a lower density of decaps in the design can translate to increased dynamic IR drop which can lead to possible functional and timing problems in the design. Adding too many decaps in the design translates to prolonged recovery time, lower resonant frequency, yield degradation and higher leakage current. This makes it imperative that the optimum usage of decaps should be achieved to balance the power distribution in the design.

A solution to this problem is proposed by Voltus^{TM} that allows placing automatically the right decaps at the right places. An engineering change order (ECO) file is generated with a list of filler cells to be replaced by decap cells. The ECO file is then imported into Cadence® Innovus to generate a new and hardened layout against IR drops. The following is an excerpt from Cadence® Voltus^{TM}, where an additional of 42.125 pF is successfully added into the circuit.

```
##############################################
 x1    y1    x2    y2 (micron) # Total Decap (fF)
##############################################
 87    43    130   87          #       42,115.3
 130   43    174   87          #       9.64625
##############################################
# Total decoupling capacitances: 42.125pF
```

The name of the cells are not shown in the excerpt above due to non-disclosure agreement. The origin (x=0,y=0) in this case is the bottom-left part of Fig. 5.9a. A total of 816 instances were swapped from filler cells to decap cells. However, this amount was not sufficient to provide the required additional decaps. The additional decap required is translated into additional explicit decap cells that can be placed outside the original design to provide the necessary amount of charge to keep the voltage swing higher than 0.9 V. However, the method of adding explicit decap cells

ISBN: 978-2-11-129250-5

may not be convenient for a specific design as it will increase the die area, thus it should be analyzed carefully.

Fig. 5.15 shows the distribution of filler cells in the design. As can be seen, there are no filler cells on the edges of the design's core, except at the top. By lacking filler cells able to act as decaps, this region is prone to be more susceptible to laser fault injection. To support this assumption, the fault injection maps reported in Section 5.3.5.2 should present faults in these regions even though laser illumination induces less IR drop at the edges of the design (Fig. 5.17 and Fig. 5.18).

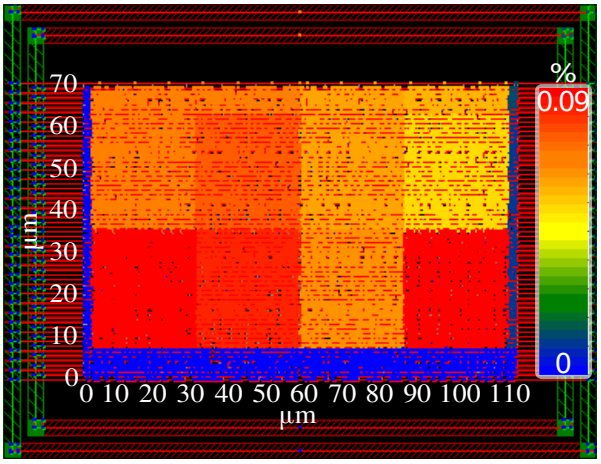


Fig. 5.15: ARM 7: distribution of filler cells in the design.

5.3.5 Drawing Fault Sensitivity Maps

5.3.5.1 Simulated Scenarios

The proposed simulation flow was applied to various scenarios. Among all these scenarios, only six of them are considered hereafter for the sake of simplicity. They are illustrated in Fig. 5.16. This figure shows in the first line the clock signal waveform used as a time reference (clock frequency equal to 1 GHz). The two other lines give the proposed scenarios applied to the proposed methodology.

The second line of Fig. 5.16 reports the results when the classical fault model (only I_{Ph}) is used during simulations. This line gives typical evolutions observed during simulations of the signal Q_x. This signal represents the output of the cell 'x' under illumination, in three different cases. These cases correspond to laser shots with a duration equal to $250\,ps$ applied respectively at 1.5 ns, 1.7 ns and 1.9 ns (corresponding respectively to scenarios 1, 2 and 3). They are thus starting closer and closer to the next rising clock edge that occurs at 2 ns.

ISBN: 978-2-11-129250-5

The third line of Fig. 5.16 gives results obtained with the enhanced model (I_{Ph} and IPh_{Psub_nwell} are considered). In this case, the laser fault injection also begins at 1.5 ns, 1.7 ns and 1.9 ns (corresponding respectively to scenarios 4, 5 and 6). As can be observed in the third line, the curves have a smoother double exponential waveform when compared to that of the second line. This is due to the RC filtering effect of the supply voltage network.

These scenarios allow us to directly compare the results between the classical electrical model and the proposed enhanced electrical model. As the width and amplitude of the transient voltage are larger when using the enhanced model, the number of induced faults for scenarios 4, 5 and 6 should also be increased. The next sections reports the results for each of the six proposed scenarios. A discussion is then given about the influence of the proposed model in the laser fault injection process.

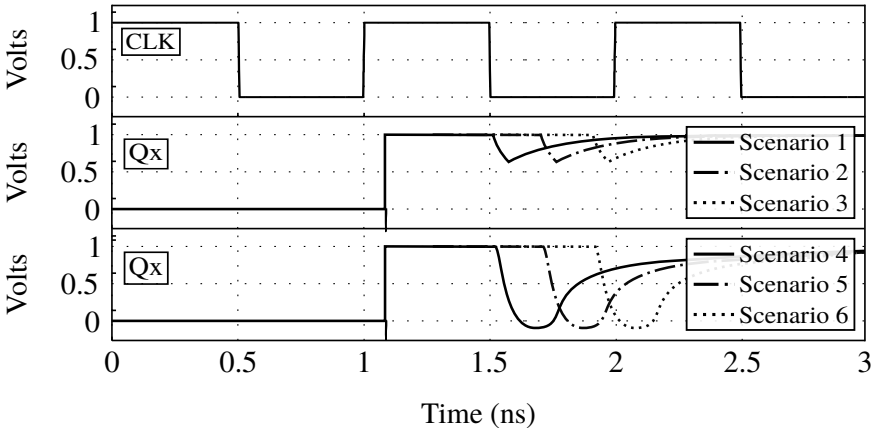


Fig. 5.16: Typical waveforms observed during simulations at the output of an arbitrary gate illuminated by a laser beam. Line 1: clock signal. Line 2: waveforms observed when considering I_{Ph} contribution only. Line 3: waveforms observed when considering both I_{Ph} and IPh_{Psub_nwell} contributions.

5.3.5.2 Fault Injection Maps

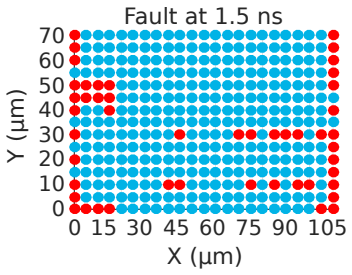
For the purpose of assessing the contribution of the laser-induced IR drop to the fault injection mechanism, fault sensitivity maps were drawn on simulation basis using the proposed methodology. The simulations were done both with the classical and enhanced fault models. They were also performed for locations of the laser spot so that to sweep the whole circuit area (110 μm x 70 μm) with X and Y displacement steps of 5 μm. This resulted in programing 345 simulations to obtain each figure (each dot corresponds to the location of a simulated laser shot).

ISBN: 978-2-11-129250-5

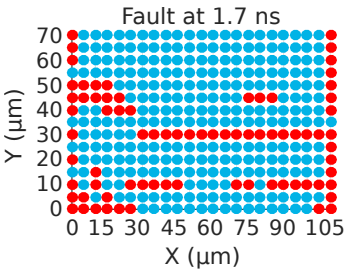
Figures 5.17 and 5.18 report the fault maps obtained considering a laser spot diameter equal 5 μm and 1 μm respectively. In both figures, results obtained with both the classic (Fig. 2.2) and the enhanced electrical models (Fig. 4.8) are shown. The red dots correspond to laser spot locations leading to a faulty result (a SE was induced) and blue dots to the absence of faults. Only bit-flip faults were considered, i.e. faults corresponding to the flipping (with reference to normal operation) of the output state of one or more flip-flops.

5.3.5.3 Simulations with the Classical Fault Model

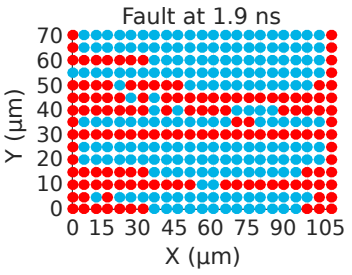
Fig. 5.17a, 5.17b and 5.17c (resp. Fig. 5.18a, 5.18b and 5.18c) report simulations performed considering the classical fault model, in which only the I_{Ph} current component with a width of 250 ps is considered. The current begins to rise at 1.5 ns, 1.7 ns and 1.9 ns respectively (scenarios 1, 2 and 3). Note that the closer to the flip-flop sampling window (time window of width t_{setup} + t_{hold} centered on the rising edge) the laser shot is, the more faults are induced (this is in fact independent of the considered fault model).



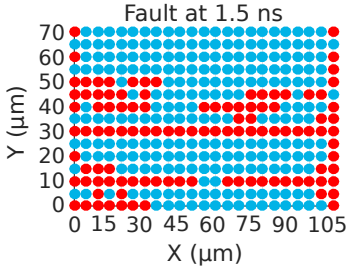
(a) I_{Ph} only Classical model. #faults: 48



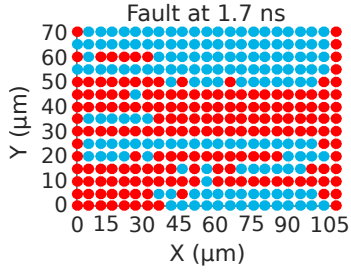
(b) I_{Ph} only Classical model. #faults: 76



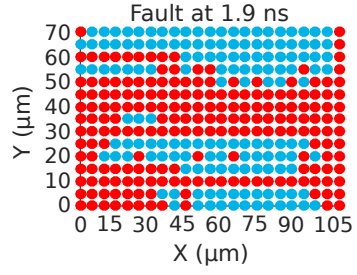
(c) I_{Ph} only Classical model. #faults: 140



(d) I_{Ph} + IPh_{Psub_nwell} Enhanced model. #faults: 108



(e) I_{Ph} + IPh_{Psub_nwell} Enhanced model. #faults: 181



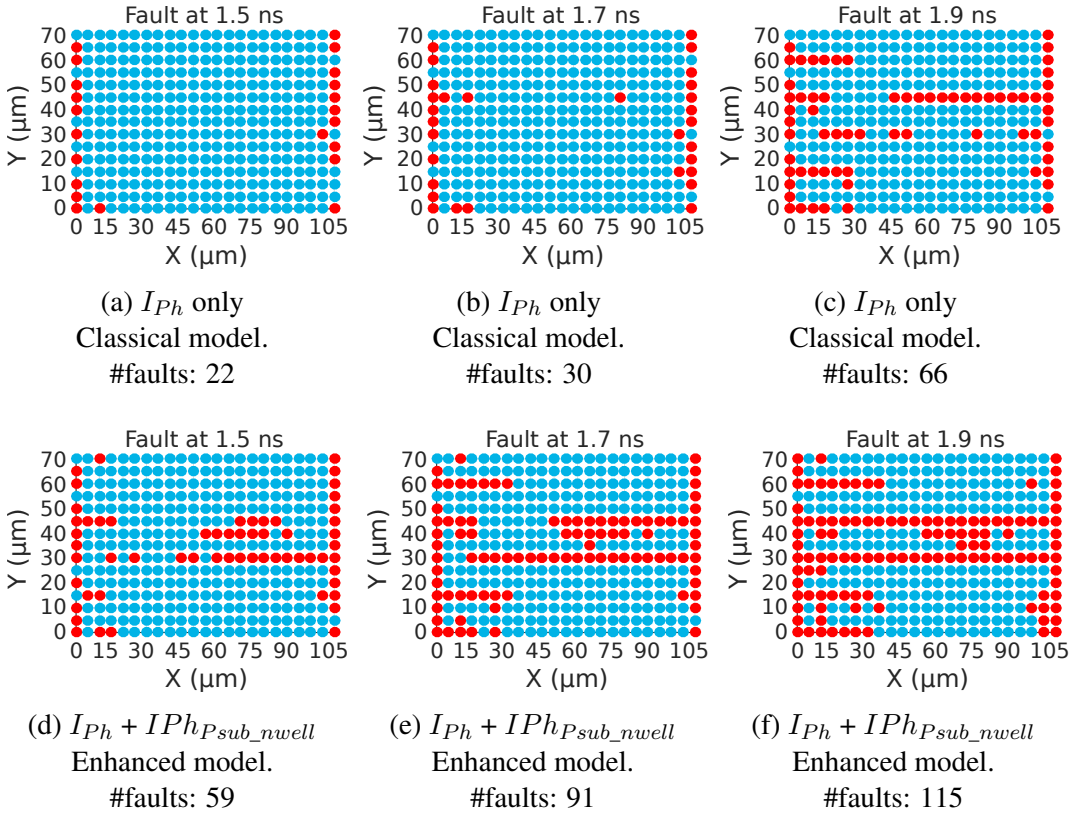
(f) I_{Ph} + IPh_{Psub_nwell} Enhanced model. #faults: 198

Fig. 5.17: Maps of laser-induced faults for the simulated scenarios. Laser spot diameter: 5 μm.

ISBN: 978-2-11-129250-5

5.3.5.4 Simulations with the Enhanced Fault Model

Fig. 5.17d, 5.17e and 5.17f (resp. Fig. 5.18d, 5.18e and 5.18f) report the fault maps obtained with the same settings but using the enhanced fault model (scenarios 4, 5 and 6) instead of the classical one. The comparison of these maps with that of the first line reveals that the fault areas are wider. The current amplitude applied to I_{Ph} remains the same as the one used in the classical model. The IR drop induced mainly by IPh_{Psub_nwell} amplify the effect of I_{Ph} current and thus the number of faults. It also unveils an extension of the laser sensitivity in time. Indeed, the number of faults is increased respectively by a factor of 2.25, 2.38 and 1.41 for the laser applied at 1.5 ns, 1.7 ns and 1.9 ns.



(a) I_{Ph} only
Classical model.
#faults: 22

(b) I_{Ph} only
Classical model.
#faults: 30

(c) I_{Ph} only
Classical model.
#faults: 66

(d) I_{Ph} + IPh_{Psub_nwell}
Enhanced model.
#faults: 59

(e) I_{Ph} + IPh_{Psub_nwell}
Enhanced model.
#faults: 91

(f) I_{Ph} + IPh_{Psub_nwell}
Enhanced model.
#faults: 115

Fig. 5.18: Maps of laser-induced faults for the simulated scenarios. Laser spot diameter: 1 μm.

In the case of the enhanced model, the highest amplification factor was for a laser shot beginning at 1.7 ns as the transient fault is wider. However, due to the RC filtering effect, the rise time has also changed and can be in the order of 100 ps depending on the affected cell. If so, when the laser is applied at 1.9 ns some faults are logically masked by the flip flop, which is not the case when the laser is applied at 1.7 ns. In this case even if the rise time has a duration of around 100 ps, the flip

ISBN: 978-2-11-129250-5

flop will be able to sample the transient voltage if it has sufficient amplitude.

Table 5.4 and 5.5 summarize the number of injected faults for each simulated scenario and for both 5 μm and 1 μm laser spot diameters, respectively. The results show that IR drops induced by laser shots play an important role in the occurrence of soft errors as, for the assessed scenarios, it amplifies the number of faults by a factor of 2.38 in the case of a 5 μm laser spot diameter and by a factor of 3.03 in the case of a 1 μm laser spot diameter. Not taking the laser-induced IR drop into account leads to over optimistic results regarding the threshold of fault injection and the number of injected faults.

Table 5.4: Number of injected faults for each simulated scenario. Simulations considering a laser spot diameter equal to 5 μm

	Number of faults Classical elect. model	**Number of faults Enhanced elect. model**	**Amplification factor**
Fault at 1.5 ns	48	108	2.25
Fault at 1.7 ns	76	181	2.38
Fault at 1.9 ns	140	198	1.41

Table 5.5: Number of injected faults for each simulated scenario. Simulations considering a laser spot diameter equal to 1 μm

	Number of faults Classical elect. model	**Number of faults Enhanced elect. model**	**Amplification factor**
Fault at 1.5 ns	22	59	2.68
Fault at 1.7 ns	30	91	3.03
Fault at 1.9 ns	66	115	1.74

5.3.6 First-order Approximation of the IR Drop Contribution to the Fault Injection Mechanism

To understand how the superposition of the effects of IR drop and of the current sources involved in the classical model creates the strong amplification effect depicted in the 3^{rd} quadrant of Fig. 5.16 and 5.17d (resp. Fig. 5.18d), consider the case of an inverter depicted in Fig. 5.19.

In normal operation with its input at zero, the current flowing in the PMOS transistor during the steady state (which is in its linear mode of operation) is equal to zero. For the sake of simplicity, consider that the laser-induced photocurrent has

ISBN: 978-2-11-129250-5

a constant amplitude $I_{Ph_{NMOS}}$, as described by equation (2.1). Thus, this current flows through the ON PMOS transistor and a voltage ΔV_{out} occurs across the PMOS as expressed by equation (5.1):

$$\Delta V_{out}(withoutIR) = \frac{I_{Ph_{NMOS}}}{\frac{\mu \cdot C_{ox} \cdot W}{L}(V_{DD} - V_T)} \tag{5.1}$$

in which $I_{Ph_{NMOS}}$ is the photocurrent amplitude, W and L the width and the length of the PMOS transistor, μ the hole mobility, C_{ox} the oxide thickness and V_T the threshold voltage.

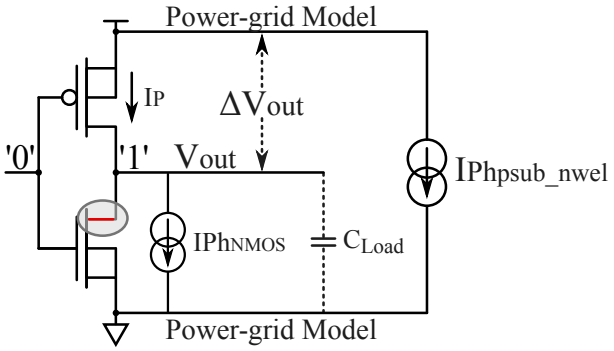


Fig. 5.19: Inverter with a low input signal under laser illumination.

In the above simple calculation, the supply voltage was considered unaffected by the laser shot and thus equal to V_{DD}. Considering now that the laser shot simultaneously generates an IR drop reducing V_{DD} by V_{drop}. This IR drop in turn affect the voltage across the PMOS, ΔV_{out}, which can be approximated by:

$$\Delta V_{out}(withIR) = V_{drop} - \frac{I_{Ph_{NMOS}}}{\frac{\mu \cdot C_{ox} \cdot W}{L}(V_{DD} - V_{drop} - V_T)}, \tag{5.2}$$

As shown by equation (5.2), the effect of the IR drop on the ΔV_{out} is non linear. The voltage drop induced by the laser shot has thus an important effect and cannot be neglected. This is especially true for ICs designed in advanced technologies for which the supply voltage is low with respect to the threshold voltages, as shown by:

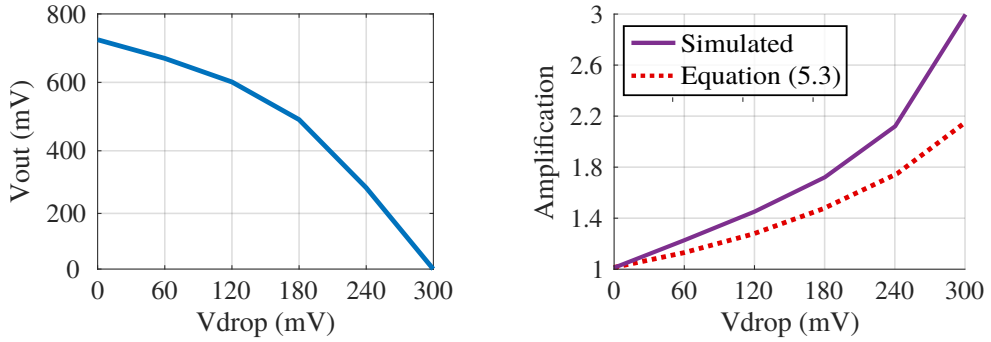
$$\frac{\Delta V_{out}(withIR)}{\Delta V_{out}(withoutIR)} = \frac{1}{1 - \frac{V_{drop}}{V_{DD} - V_T}} \tag{5.3}$$

that gives the amplification by the IR drop of the laser induced perturbation at the gate output.

By way of illustration, Fig. 5.20a gives some simulated values of V_{out} for different V_{drop} values in case of a basic 28nm CMOS inverter. As expected from the above

ISBN: 978-2-11-129250-5

equation, the higher the V_{drop}, the lower V_{out} is. Similarly, Fig. 5.20b gives, for the same inverter, the simulated and calculated IR drop induced amplification of the perturbations. The obtained trend is in accordance with (5.3) even if the modeling of the IR drop effect remains of first order and could thus be improved.



(a) (b)

Fig. 5.20: (a) Simulated V_{out} values with regard to V_{drop} (b) IR drop amplification according to (5.3) and electrically simulated.

5.3.7 Probability of Soft Error Occurrence

The occurrence of SEs due to a laser shot depends on several parameters. Among them, one can enumerate: the laser spot diameter, the transient fault profile, the time when the laser shot is applied in the circuit with regard to the clock signal, the position of the affected cells in the circuit and the handled data.

Considering these parameters fixed, the probability of a SE occurrence depends on the data path propagation delay of a particular signal.

On simulation basis, Fig. 5.21 shows the probability an SE occurs on two signals affected by a laser shot at fixed position (x,y). The output of the observed signals were saved with a time step of 50 ps in a range of two clock cycles, i.e. 2 ns. Note in the fourth line of Fig. 5.21 how the probability of soft/timing error occurrence due to the contribution of I_{Ph} + IPh_{Psub_nwell} (proposed model) is always equal to 1 on wider time ranges than the contribution of I_{Ph} alone (classical model). Furthermore, the time when the laser shot is applied causing a SE is more unpredictable due to the delay caused by the IPh_{Psub_nwell} current component that induces IR drops in the power rails.

ISBN: 978-2-11-129250-5

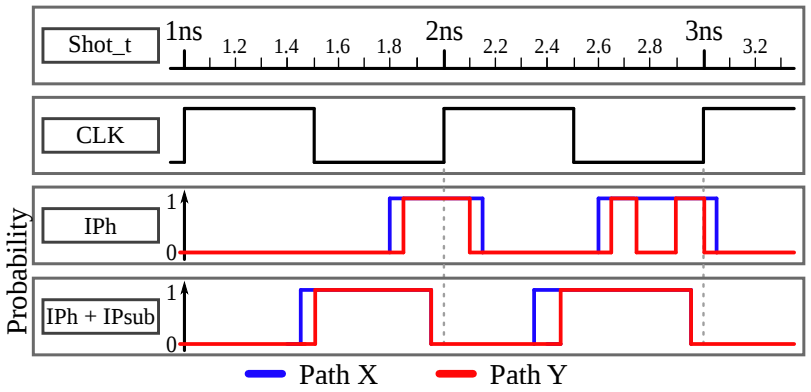


Fig. 5.21: Probability of SE occurrence. $Shot_t$: Laser shot time. I_{Ph}: I_{Ph} contribution only. I_{Ph} + IPh_{Psub}: I_{Ph} + IPh_{Psub_nwell} contribution.

5.3.8 Simulation Performance

The performance of the simulation directly depends on the available computing resources and the complexity of the simulated circuit. The processor used to perform simulations was an Intel® Xeon® E5630@2.53 GHz with two cores and 16 GB of RAM. Table 5.6 gives the simulation performance of the four assessed circuits and for two laser spot diameters: 1 μm and 5 μm. Note how the simulation time does not increase proportionally with the number of instances in the circuit. Since the proposed method deals with simulations of laser-induced fault injection, other factors such as the laser spot diameter, its power and the duration of the laser shot impact the simulation time. Indeed, these parameters directly:

- fix the number of instances experiencing a supply voltage lower than V_{DD}-th and thus the number of instances that have to be simulated with Spectre accuracy,
- reduce the time step of simulations because V_{DD} and G_{ND} are no more at a constant value.

Table 5.6: Simulation performances for different circuits regarding one laser shot.

Benchmark circuit	**Number of instances**	**Simulation time spot ⌀ = 5 μm**	**Simulation time spot ⌀ = 1 μm**
ARM 7	5,210	1min 02s	51s
S38584 (ISCAS'89)	20,705	1min 20s	1min 05s
B18 (ITC'99)	52,601	3min 05s	2min 37s
B19 (ITC'99)	105,344	6min 35s	5min 53s

ISBN: 978-2-11-129250-5

5.4 Additional Evidences of the Importance of Laser-induced IR Drop

5.4.1 Lessons from Simulations

Figure 4.22d (copied here as Fig. 5.22a for convenience), which reports simulation results related to a laser shot *near* the RO obtained considering the enhanced fault model, shows a frequency drop of 38 MHz. This frequency drop is due to the laser-induced IR drop and to its propagation through the supply network, from the laser impact point to the RO's gates. This propagation capability suggests that a laser shot can affect the behavior of a structure which it is not illuminating directly.

In the same way, Fig. 4.18d (or Fig. 5.22b) which gives simulation results related to a laser shot *over* the RO obtained considering the classical fault model shows a frequency drop of 48 MHz.

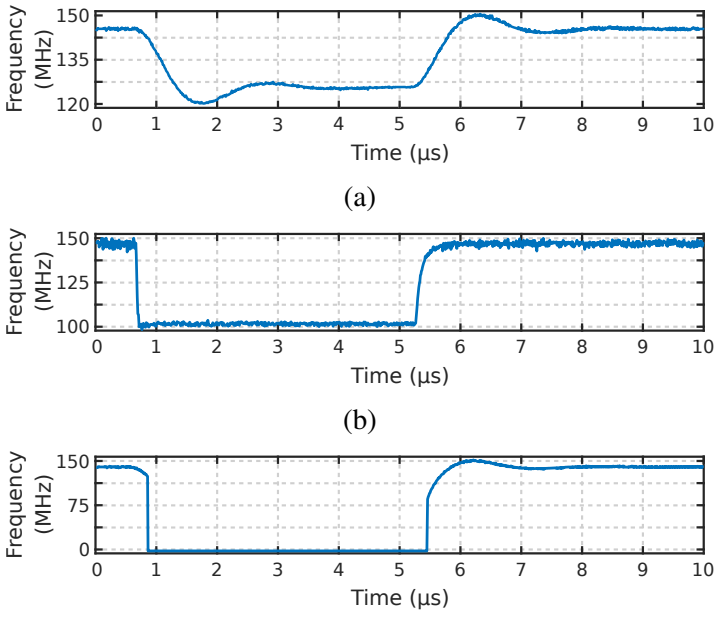


Fig. 5.22: Disturbance of the RO frequency over time. Laser shot with pulse duration equal 5 μs. (a) Simulation, according to the enhanced fault model. Effect of a laser shot illuminating a region near the RO. Contribution of I_{Ph} and IPh_{Psub_nwell}. (b) Simulation, according to the classical fault model. Effect of a laser shot illuminating directly a region of the RO. Contribution of I_{Ph} only. (c) Simulation, according to the enhanced fault model. Effect of a laser shot illuminating directly a region of the RO. Contribution of I_{Ph} and IPh_{Psub_nwell}.

Considering the two above results, one can think that simulating with the up-

ISBN: 978-2-11-129250-5

graded model a laser shot *over* the RO would give a frequency drop equal to 38 MHz + 40 MHz=78 MHz. However, as shown in Fig. 4.19d (or Fig. 5.22c) that gives the result of such a simulation, this is not the case. Indeed, the frequency falls down to zero during the laser shot. This suggests the existence of an amplification by the IR drop (due to IPh_{Psub_nwell}) of the amplitude of the transient fault generated by I_{Ph}.

We can thus conclude that the enhanced fault model points out the importance of the laser-induced IR drop in the fault injection process. Indeed, according to the above simulation results and the ones given in the last section (Fig. 5.17 and 5.18), these IR drops play an important role in the fault occurrence process by either amplifying the transient voltages generated by I_{Ph} or by directly disrupting the behavior of gates or datapaths far from the laser spot location because IR drops propagate through the PDN.

This importance of the laser-induced IR drops (and thus of the related amplification effect) has been highlighted by results of Fig. 5.17 showing that the fault areas of the ARM 7 surface are larger than that obtained with the classical fault model.

At that stage of this thesis, one may wonder if the lessons related to laser shot effects (amplification and propagation effects) learned from simulations hold in practice even if some experimental evidences of the validity of the enhanced model have been already given in Section 4.5.

5.4.2 Experimental Results - Ring Oscillator implemented on FPGA

To make meaningful comparisons of the results obtained with the proposed simulation methodology, fault maps of an FPGA Virtex 5 embedding a RO were drawn. More precisely, two sets of laser scans were performed.

During the first set of scans, only a RO, placed as shown in Fig. 4.13b, was implemented in the Virtex 5. During the second set of scans the same implementation of the RO was considered. However, extra logic (chain of inverters without any kind of logic connection with the RO) was placed around it. The result of the second place and route of the related topology is depicted in Fig. 5.23.

In Fig. 5.23, LUTs in blue are the ones used to implement the RO while LUTs in green form an inverters chain. This chain takes as input the output of an internal clock source of the FGPA, which switches at a fixed frequency equal to $50\,MHz$. It is important to highlight that LUTs in green are not logically connected with the RO. The only role of this constantly switching extra logic is to generate an additional IR drop in the RO.

ISBN: 978-2-11-129250-5

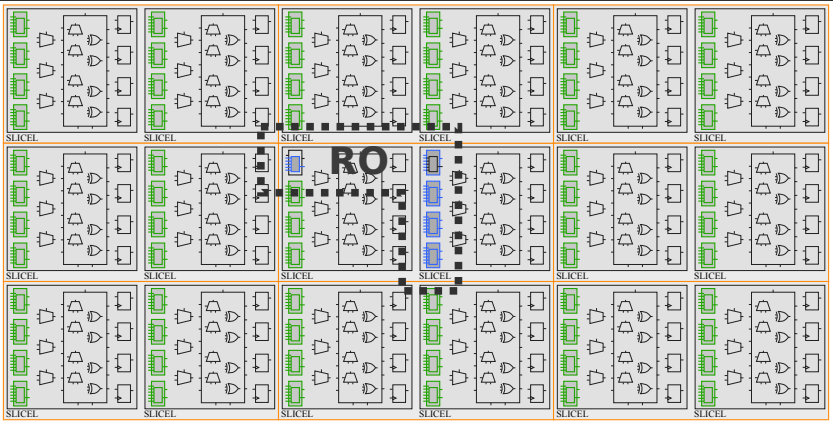


Fig. 5.23: Placement of the ring oscillator (blue) and the logic surrounding the ring oscillator without logical connection with it (green).

Fig. 5.24 groups all experimental results, validating the lessons learned from simulations, lessons related to the existence of an amplification effect by the laser-induced IR drop and of a propagation effect related to the affected region by the laser beam on the surface of the IC.

Fig. 5.24a shows for each laser spot location the frequency drift induced by the laser shot. The scanned surface was equal to $900\,\mu m \times 500\,\mu m$ and enclosed the RO without surrounding logic, as shows Fig. 4.13b. For this scan, the laser spot diameter was $5\,\mu m$ and the laser power was set to $1.04\,W$, value which is near the minimum threshold to induce faults in the RO (fault means, in this case, a frequency equal 0 MHz). The x and y displacement steps were set to $5\,\mu m$ resulting in a total of 18000 points. Each point of the cartography corresponds to a RO frequency measured over a time window of $10\,\mu s$, beginning shortly before the laser shot (c.f. Fig. 4.23b). The minimum frequency found over this window of $10\,\mu s$ was saved along with the corresponding (x, y) position of the laser shot. The color bar ranges from 148 MHz (the nominal frequency) down to 0 MHz. The dark/red stripes in Fig. 5.24a correspond to the positions of biased $Psub\text{-}Nwell$ junctions.

Fig. 5.24b and 5.24c show the same results than Fig. 5.24a after application of a rotation to only show y and z axis, z being the frequency of the RO. Fig. 5.24c and 5.24b only differ by their considered frequency range (color bar scale).

Fig. 5.24d to 5.24f give the same types of fault maps than Fig. 5.24a to 5.24c but for the RO with the aforementioned surrounding logic. In this case the nominal frequency of the RO dropped from 148 MHz to 145 MHz due to the IR drop caused by the additional logic.

ISBN: 978-2-11-129250-5

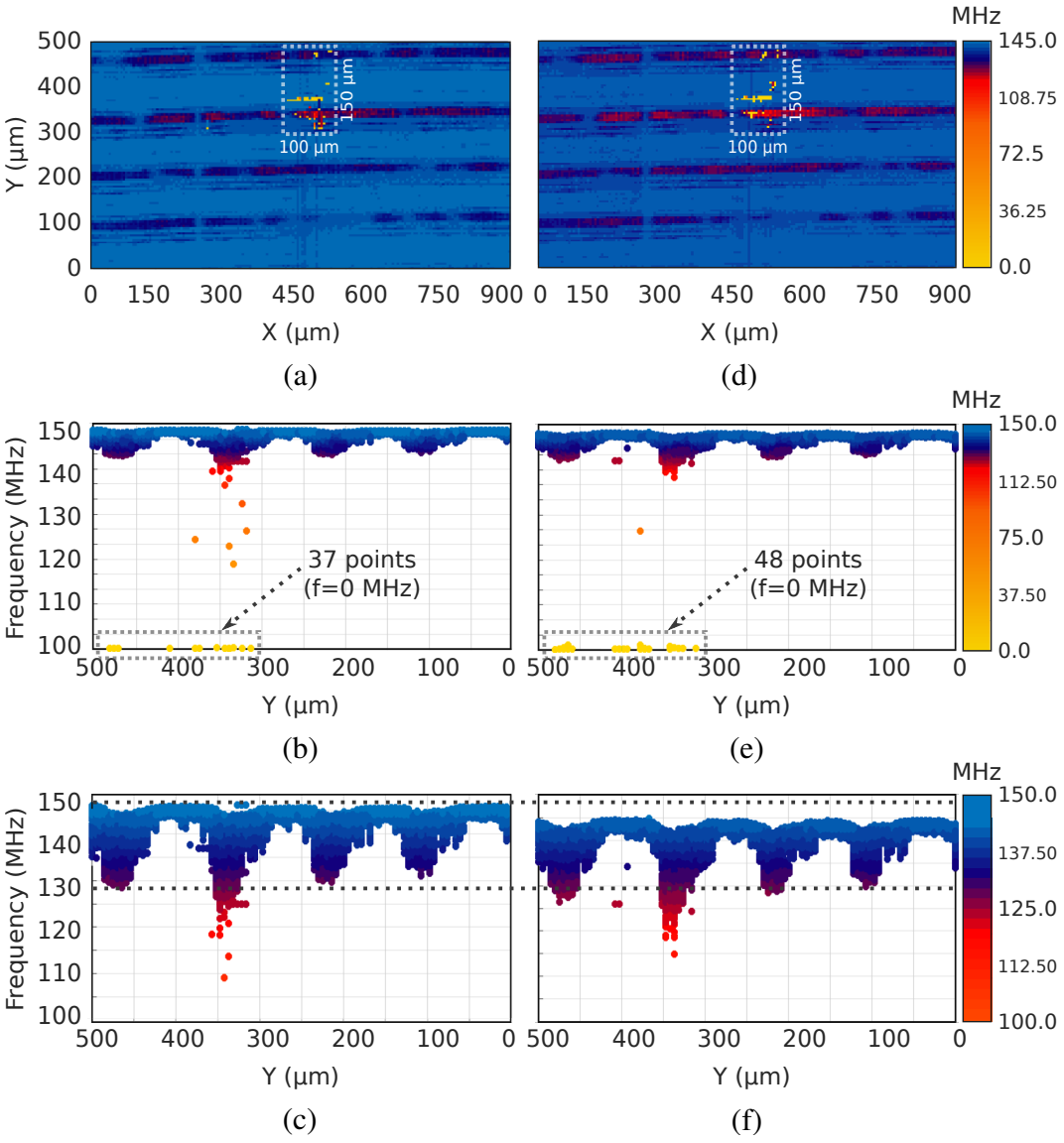


Fig. 5.24: Maps of laser-induced frequency drops of the RO implemented on FPGA: each point corresponds to the output frequency of the ring oscillator observed on the oscilloscope. Laser pulse duration: 5 μs. Laser power: 1.04 W. Laser spot: 5 μm. (X,Y) displacement step: 5 μm. (a-c) Ring oscillator implemented alone. (d-f) Ring oscillator implemented with logic surrounding it causing additional IR drop due to switching activity.

The two maps (Fig. 5.24a to 5.24c and Fig. 5.24d to 5.24f) experimentally demonstrate the existence of laser induced IR drops. Indeed, on both maps, frequency drops occur at many points of the scanned surface even if the RO occupies only a really small fraction of it ($100\,\mu m \times 150\,\mu m$). This is a direct experimental evidence that the effect of laser illumination is not as local as usually considered (the classical model is unable to predict these maps).

ISBN: 978-2-11-129250-5

One can observe that the horizontal propagation of the frequency drop is similar to the voltage drop propagation shown in Fig. 5.9b (propagation that follows the power grid). The effect of laser illumination is thus more global than previously thought. Additionally, the points in yellow corresponds to laser shots completely stopping the operation of the RO (frequency equal to zero). Thus, the yellow points should correspond to the placement of the RO (Fig. 4.13b) or really close to it.

The amplification of the laser shot effect by the laser-induced IR drop can be observed by comparing the first column of Fig. 5.24 (Fig. 5.24a-c) with its second column (Fig. 5.24d-f). Indeed, by taking a closer look at Fig. 5.24a and Fig. 5.24d, it is possible to observe that the number of red and yellow points is larger in Fig. 5.24d. This means that in the case of Fig. 5.24d more points have a frequency value below a certain threshold (or a null frequency).

Table 5.7 reports the number of points below or equal to a given frequency. The nominal frequency of the RO is equal to $148\,MHz$. To give an example, consider a threshold of 5% of the nominal frequency ($148\,MHz$ - $7.4\,MHz$ = $140.6\,MHz$). In this case, Table 5.7 reports a number of points equal to 3363 (frequency below or equal to $140.6\,MHz$) for the cartography reported in Fig. 5.24a (RO alone). And 3453 points for the cartography reported in Fig. 5.24d (RO with surrounding logic). Similar results are given in Table 5.7 for different thresholds.

The numerical results given in Table 5.7 demonstrates quantitatively that even a small additional IR drop (of few mV) caused by the switchings of extra cells, increases the impact of laser shots. More precisely, it increases the frequency drop experienced by the RO when using the same laser power. Hence the amplification of the transient current I_{Ph} by the laser-induced IR drops.

Table 5.7: Number of points below or equal to a given frequency (nom. freq. = 148 MHz for Fig. 5.24a-c and nom. freq. = 145 MHz for Fig. 5.24d to 5.24f)

Frequency value (nom freq - x % of nom. freq.)	**No. of points Fig. 5.24a to 5.24c**	**No. of points Fig. 5.24d to 5.24f.**
nom freq - 0 % of nom. freq.	18000	18000
nom freq - 5 % of nom. freq.	3363	3453
nom freq - 10 % of nom. freq.	468	563
nom freq - 100 % of nom. freq.	37	48

ISBN: 978-2-11-129250-5

5.4.3 Influence of the pulse duration on the laser-induced IR drop

This section presents simulation and experimental results regarding the influence of the laser pulse duration on the characteristics of laser-induced IR drops.

To analyze the effect of laser pulse duration, three laser shots with duration equal to 1 μs, 5 μs and 10 μs were applied to the Virtex 5 embedding the RO. The output frequency of the RO was measured during the experiments.

Fig. 5.25 shows the applied pulses and the related evolutions of the oscillation frequency of the RO. One can observe on this figure that for short pulses the amplitude of the frequency drop, and thus the one of the IR drop, is lower than the frequency for long pulses. This could be explained by the role of decoupling capacitances that are able to provide enough charges to the PDN to counterbalance for short pulses (lower than 1 μs) of the induced IR drop. For longer pulses however, the charge stored in the decoupling capacitances are not enough important to counterbalance the laser induced IR drop, thus the IR drop settles to a constant value after approximately 1 μs.

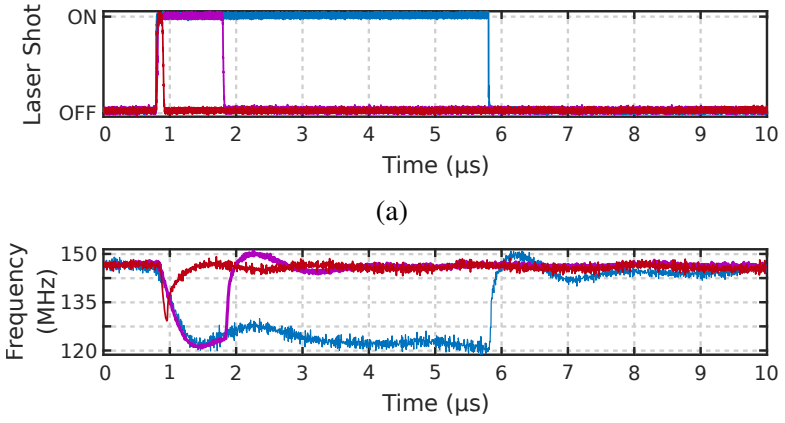


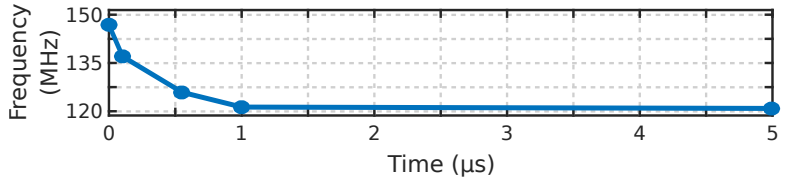
Fig. 5.25: Experimental results: maximum drop in frequency for different pulse durations. (a) The three considered laser shots with different pulse durations: 100 ns, 1 μs and 10 μs. (b) Disturbance by the laser of the RO's frequency over time.

Several other pulse durations were characterized by simulation and experimentally. Fig. 5.26 gathers the obtained results. For the FPGA Virtex 5, the external and internal decoupling capacitances are sufficient to limit the amplitude of IR drop for pulse durations lower than 1 μs. Regarding the simulation results related to the ARM 7 the decoupling capacitances compensate the effects of laser shots for durations lower than 0.5 ns. The gap between this value and that obtained for the FPGA

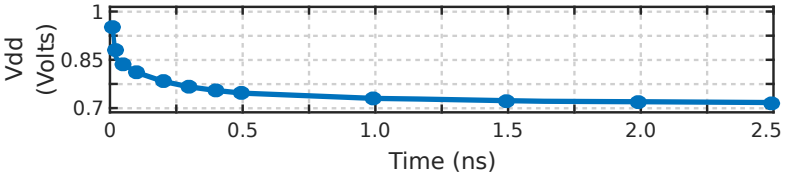
ISBN: 978-2-11-129250-5

can be explained by the absence of external decoupling capacitance, the technology geometry (28 nm for the ARM 7 and 65 nm for the FPGA), and the reduced size of the ARM 7 ($110\,\mu m \times 70\,\mu m$) with regard to the Virtex 5 ($10\,mm \times 10\,mm$).

The method proposed in this thesis takes all the aforementioned characteristics into account, i.e., it is able to predict the minimum pulse duration that will cause an attenuation on the induced IR drop depending on the technology, circuit size and amount of decoupling capacitors. This is an important result since the design can be modified, based on this observation, to harden sensitive parts of the circuit as described in Section 5.3.4.



(a) Experimental results: Ring oscillator implemented on a Virtex-5 FPGA.



(b) Simulation results: ARM 7 implemented on a 28 nm technology.

Fig. 5.26: Influence of the pulse duration on the maximum laser-induced IR drop.

5.5 Summary

Former works that proposed laser fault simulation tools were reviewed in Section 5.1 of this chapter. These fault simulators, or at least the ones performing simulation at the electrical level, usually use the classical electrical fault model or enhanced models that do not take into account the IR drop contribution. For that, it is necessary to model the RC network in the power/ground rails of each cell in the circuit. In view of this limitation, we proposed in this chapter a fault simulation methodology that uses an EMIR CAD tool to automatically provide the RC network of the power/ground rails for a given design.

Section 5.2 of this chapter detailed the proposed methodology allowing to simulate laser-induced faults in large-scale circuits. The methodology is based only on standard CAD tools making it easy to be applied in other design environments such as Cadence, Synopsys and Menthor Graphics.

ISBN: 978-2-11-129250-5

Section 5.3 reported simulation results provided by the proposed methodology. The results highlighted how laser-induced IR drop effects significantly contribute to fault injection. The methodology was applied to a test-chip, which used the enhanced electrical model during simulations in order to demonstrate how IR drop facilitate the occurrence of SEs by amplifying laser induced perturbations on logic signals. Both the areas sensitive to laser-fault injection and the time span of laser sensitivity are increased.

In Section 5.4 were compared simulation results obtained with our methodology with experimental results obtained with an FPGA Virtex 5. Both simulation and experimental results helped to ascertain the superiority of the proposed model over the classical one. The results presented in this section also revealed that the laser-induced IR drop is a strong contributor to the fault injection process as it amplifies the transient voltage induced in the drain of sensitive transistors. This amplification reduces the amount of charge needed to cause a transient fault, thus decreasing the fault injection threshold. This result reveals that laser-induced IR drop has to be considered in order to not underestimate fault sensitivity.

ISBN: 978-2-11-129250-5

University of Montpellier, LIRMM
ISBN: 978-2-11-129250-5

Chapter 6

Conclusions and Perspectives

In today's complex and highly automated society, semiconductor chips are everywhere around us. They are present in airplanes, cars, computers, TV sets, mobile phones, smart cards etc. With constantly growing demand for security, silicon chips started to be used not only for control purposes but for protection as well. As a consequence, a continuous battle is waged between manufacturers and hackers. The manufactures invent new security solutions and the hackers are constantly trying to break the implemented protections. It is thus crucial for the designers to have a convenient and reliable method for testing secure designs before fabrication.

In this context, Chapter 2 reported a detailed background on the effects of laser illumination on ICs, as this thesis focuses on laser fault injection. In addition, several concurrent error detection techniques were also reviewed. These techniques aim at protecting integrated systems against transient faults that can be induced by fault injection techniques.

In the sequence, Chapter 3 presented a method for classifying and evaluating the effectiveness of the concurrent error detection techniques introduced in Chapter 2. Another technique capable to detect transient faults was proposed in this chapter. The evaluation method take into account only single transient faults that survived the attenuation of logical or electrical masking effects. This allowed to directly compare the effectiveness of each concurrent error detection technique. The results of all detection techniques were summarized in Table 3.2, giving a direct insight of the effectiveness of each technique. This enable designers to choose the concurrent error detection technique that suit best for their purposes.

Improvements of the classical electrical model proposed in the current literature for simulating the effects of laser illumination on ICs were discussed in Chapter 4. This chapter also detailed the limitations of formerly proposed models before

ISBN: 978-2-11-129250-5

introducing our enhanced electrical fault model. The proposed model takes laser-induced IR drop into account for simulation purposes since for new deep submicron technologies, a laser shot simultaneously illuminates the $Psub$-$Nwell$ junction thus inducing a transient current directly flowing from V_{DD} to G_{ND} (a massive short circuit current).

Consequences of the proposed and classical electrical models on the laser-induced fault injection mechanism were then compared. Putting it differently, it was clarified how a laser-induced transient voltage propagates through the logic toward the input of sequential cells, thus causing a soft / timing error when considering both classical and proposed electrical models.

Then, simulation and experimental results of laser injections were presented in order to confirm the superiority of the proposed enhanced fault model. The results revealed that, when an IC —fabricated in a relatively new technology node (Virtex-5 FPGA - 65 nm)— is illuminated by a laser beam, it induces IR drops. The induced IR drops have a global effect spreading through the supply network. This gives experimental evidence that the effect of laser illumination is not as local as usually considered, i.e., laser illumination does not only affect the drain's PN junction of sensitive transistors. It also affects the $Psub$-$Nwell$ junction of all transistors interconnected by the same power rail.

Chapter 5 proposed a methodology which allows the simulation of laser fault injection at the electrical level in large-scale circuits by using standard CAD tools. The proposed enhanced electrical fault model that takes laser-induced IR drop into account was used by the methodology during simulations. The enhanced model was applied only to the illuminated instances of the assessed test-chip to reduce simulation time, thus, the non affected instances were simulated with the logic abstraction level as the circuit perform only binary (digital) operations. The use of the proposed enhanced model allowed to demonstrate how the induced IR drop facilitates the occurrence of SEs by amplifying laser-induced perturbations on logic signals.

Simulation results obtained with the proposed methodology as well as experimental results revealed that ignoring the laser-induced IR drop may outcome in underestimating the risk of fault injection, not to mention the incorrect estimation of the fault injection threshold. Indeed, for the test-chip assessed by the simulation methodology, an increase in the number of faults by a factor of 2.38 (resp. 3.03) was observed for a laser spot diameter equal to 5 μm (resp. 1 μm) when IR drops are taken into account. This result is especially relevant for the design of countermeasure techniques for secure integrated systems.

Further scientific work in our plan includes testing a microchip fabricated in FD-

ISBN: 978-2-11-129250-5

SOI 28 nm technology in partnership with ST Microelectronics [111] and Tiempo [115]. Different circuits were integrated in order to validate:

- The overall behavior of a dynamic bulk built-in current sensor, which is a promising concurrent error detection technique when it comes to hardware security. Due its high detection ability, the dynamic bulk built-in current sensor is able to detect more than 99% of injected transient faults in the monitored circuit (cf. Table 3.2). The bulk built-in current sensor is able to detected transient faults induced by, for example, laser illumination or even radiation exposure.

- A RO in order to have additional results regarding the laser-induced IR drop occurring in a different technology. In this case, the IR drop is expected to be more accentuated as the amount of decaps in this design and technology is much smaller the amount of decaps in the Virtex 5 designed in a 65 nm technology.

In addition, following the work of Sarafianos [101], PN junctions with different areas should be characterized for other technologies. The bivariate normal distribution used in this thesis (equation 2.1) is based on empirical studies made by Sarafianos [101] for the 90 nm technology. Similar results for different technologies will better calibrate the proposed methodology regarding the relationship between power density and current. This was in fact the main difficulty while developing the proposed methodology as the other ratios are given automatically by the methodology. Ratios such as the area of the drain / Nwell of each transistor and the amount of capacitance and resistance in the power / ground rails for each cell in the circuit.

Using an inverter cell as an example, if the area of the Nwell of the inverter is 10x larger than the area of the sensitive transistor's drain, then the current IPh_{Psub_nwell} is 10x larger than the induced current I_{Ph}. However, it is not straightforward to know how many mA corresponds to a certain power density for a specific PN junction, thus we had to rely on the results reported by Sarafianos [101]. Nevertheless, the most important aspect is the ratio between the currents IPh_{Psub_nwell} and I_{Ph} as well as the capacitors and resistors. These ratios will give a better correlation between simulation and experimental results and not the absolute amount of current induced by the laser. In this case, it is just a matter of playing with the power of the laser source to match the induced current for a given laser pulse duration and laser spot diameter.

ISBN: 978-2-11-129250-5

University of Montpellier, LIRMM
ISBN: 978-2-11-129250-5

Glossary

A

AES Advanced Encryption Standard.

AC Alternating Current.

ADC, A/D Analog-to-Digital Converter.

AND Boolean-logic function.

ASIC Application-Specific Integrated Circuit.

B

BBICS Bulk Built-In Current Sensor.

BICS Built-in Current Sensor.

C

CAD Computer-Aided Design

CED Concurrent Error Detection

CMOS Complementary Metal-Oxide-Semiconductor

CPLD Complex Programmable Logic Device

CPF Common Power Format

CPU Central Processor Unit

ISBN: 978-2-11-129250-5

D

DoS Denial-of-Service.

DAC, D/A Digital-to-Analog Converter.

DBBICS Dynamic Bulk Built-In Current Sensor.

DC Direct Current.

DE Delay Error.

DEF Design Exchange Format.

DES Data Encryption Standard.

DPA Differential Power Analysis.

DUT Design Under Test.

DRAM Dynamic Random-Access Memory.

E

EEPROM, E^2PROM Electrically Erasable Programmable ROM.

EM Electromagnetic.

EMIR Electromagnetic IR drop.

ECO Engineering Change Order.

EPROM Electrically Programmable ROM.

F

FET Field-Effect Transistor.

FIB Focused Ion Beam.

FPGA Field-programmable gate array.

ISBN: 978-2-11-129250-5

G

GDS Graphic Database System.

I

IC Integrated Circuit.

IO Input/Output.

IP Intellectual Propriety.

I_{Ph} I (current) Ph (photo). Photocurrent between the drain and the substrate of a sensitive transistor.

$IPh_{Psub-nwell}$ Photocurrent between Nwell and P-type substrate.

IR InfraRed. Light with longer wavelengths than those of visible light.

ISO International Organisation for Standardisation. ISO/IEC 7816 is a smartcard standard.

L

LEF Library Exchange Format.

LIVA Light-Induced Voltage Alterations. Failure analysis technique.

MF Masked Fault.

NIR Near-Infrared. Region of infrared light close to the visible light.

NOR Not OR. Boolean-logic function.

OBIC Optical Beam Induced Current. Failure analysis technique.

OR Boolean-logic function.

P

PCB Printed Circuit Board.

PDN Power Distribution Network.

ISBN: 978-2-11-129250-5

R

RO Ring Oscillator.

RSA Rivest–Shamir–Adleman. Cryptographic algorithm invented by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1977.

RTL Register Transfer Level.

S

SBBICS Single Bulk Built-In Current Sensor.

SVT Standard Threshold Voltage.

SDC Synopsys Design Constraints.

SDF Standard Delay Format.

SE Soft Error.

SPEF Standard Parasitic Exchange Format.

SPICE Simulation Program with Integrated Circuit Emphasis.

SRAM Static Random-Access Memory.

T

TCAD Technology Computer-Aided Design.

TD Transition Detector.

TF Transient Fault.

TFMS Transient Fault Monitoring Scheme.

V

VCD Value change dump.

V_{th} Threshold Voltage.

ISBN: 978-2-11-129250-5

X

XNOR Exclusive NOR. Boolean-logic function.

XOR Exclusive OR. Boolean-logic function.

ISBN: 978-2-11-129250-5

University of Montpellier, LIRMM
ISBN: 978-2-11-129250-5

Bibliography of Author's Publications

[1] R. A. C. Viera, J. M. Dutertre, R. P. Bastos, and P. Maurine. Role of laser-induced ir drops in the occurrence of faults: Assessment and simulation. In *2017 Euromicro Conference on Digital System Design (DSD)*, pages 252–259, Aug 2017.

[2] R. A. C. Viera, P. Maurine, J. M. Dutertre, and R. P. Bastos. Importance of ir drops on the modeling of laser-induced transient faults. In *2017 14th International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design (SMACD)*, pages 1–4, June 2017.

[3] R.A. Camponogara Viera, R. Possamai Bastos, J.-M. Dutertre, P. Maurine, and R. Iga Jadue. Method for evaluation of transient-fault detection techniques. *Microelectronics Reliability*, 76-77:68 – 74, 2017.

[4] Raphael A.C. Viera, Jean-Max Dutertre, Philippe Maurine, and Rodrigo Possamai Bastos. Simulation and experimental demonstration of the importance of ir-drops during laser fault-injection. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2018.

[5] Raphael A.C. Viera, Jean-Max Dutertre, Philippe Maurine, and Rodrigo Possamai Bastos. Standard cad tool-based method for simulation of laser-induced faults in large-scale circuits. In *Proceedings of the 2018 International Symposium on Physical Design*, ISPD '18, pages 160–167, New York, NY, USA, 2018. ACM.

ISBN: 978-2-11-129250-5

University of Montpellier, LIRMM
ISBN: 978-2-11-129250-5

References

[6] AGOYAN, M., DUTERTRE, J.-M., NACCACHE, D., ROBISSON, B., AND TRIA, A. When clocks fail: On critical paths and clock faults. In *CARDIS* (2010).

[7] AHMADI, R., AND NAJM, F. N. Timing analysis in presence of power supply and ground voltage variations. In *ICCAD-2003. International Conference on Computer Aided Design* (Nov 2003), pp. 176–183.

[8] AJAMI, A. H., BANERJEE, K., MEHROTRA, A., AND PEDRAM, M. Analysis of ir-drop scaling with implications for deep submicron p/g network designs. In *Fourth International Symposium on Quality Electronic Design, 2003. Proceedings.* (March 2003), pp. 35–40.

[9] ALEXANDER, C., AND SADIKU, M. *Fundamentals of Electric Circuits*, 4th ed. McGraw Hill Higher Education, 2008.

[10] ANDERSON, R., AND KUHN, M. Tamper resistance – a cautionary note. In *IN PROCEEDINGS OF THE SECOND USENIX WORKSHOP ON ELECTRONIC COMMERCE* (1996), pp. 1–11.

[11] ANDREOU, A., BOGDANOV, A., AND TISCHHAUSER, E. Cache timing attacks on recent microarchitectures. In *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)* (May 2017), pp. 155–155.

[12] ANGHEL, L., AND NICOLAIDIS, M. Cost reduction and evaluation of a temporary faults detecting technique. In *Proceedings Design, Automation and Test in Europe Conference and Exhibition 2000 (Cat. No. PR00537)* (2000), pp. 591–598.

[13] BALASCH, J., ARUMÍ, D., AND MANICH, S. Design and validation of a platform for electromagnetic fault injection. In *2017 32nd Conference on Design of Circuits and Integrated Systems (DCIS)* (Nov 2017), pp. 1–6.

ISBN: 978-2-11-129250-5

[14] BAR-EL, H. Known attacks against smartcards.

[15] BAR-EL, H., CHOUKRI, H., NACCACHE, D., TUNSTALL, M., AND WHELAN, C. The sorcerer's apprentice guide to fault attacks. *Proceedings of the IEEE 94*, 2 (Feb 2006), 370–382.

[16] BARENGHI, A., BREVEGLIERI, L., KOREN, I., AND NACCACHE, D. Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures. *Proceedings of the IEEE 100*, 11 (Nov 2012).

[17] BAUMANN, R. C. Radiation-induced soft errors in advanced semiconductor technologies. *IEEE Transactions on Device and Materials Reliability 5*, 3 (Sept 2005), 305–316.

[18] BAYON, P., BOSSUET, L., AUBERT, A., FISCHER, V., POUCHERET, F., ROBISSON, B., AND MAURINE, P. Contactless electromagnetic active attack on ring oscillator based true random number generator. In *Constructive Side-Channel Analysis and Secure Design* (Berlin, Heidelberg, 2012), W. Schindler and S. A. Huss, Eds., Springer Berlin Heidelberg, pp. 151–166.

[19] BIHAM, E., AND SHAMIR, A. Differential fault analysis of secret key cryptosystems. In *Advances in Cryptology — CRYPTO '97* (Berlin, Heidelberg, 1997), B. S. Kaliski, Ed., Springer Berlin Heidelberg, pp. 513–525.

[20] BLÖMER, J., AND SEIFERT, J.-P. Fault based cryptanalysis of the advanced encryption standard (aes). In *Financial Cryptography* (Berlin, Heidelberg, 2003), R. N. Wright, Ed., Springer Berlin Heidelberg, pp. 162–181.

[21] BONEH, D., DEMILLO, R. A., AND LIPTON, R. J. On the importance of checking cryptographic protocols for faults. In *Advances in Cryptology — EUROCRYPT '97* (Berlin, Heidelberg, 1997), W. Fumy, Ed., Springer Berlin Heidelberg, pp. 37–51.

[22] BOSIO, A., AND NATALE, G. D. Lifting: A flexible open-source fault simulator. In *2008 17th Asian Test Symposium* (Nov 2008), pp. 35–40.

[23] BOWMAN, K. A., TSCHANZ, J. W., KIM, N. S., LEE, J. C., WILKERSON, C. B., LU, S. L. L., KARNIK, T., AND DE, V. K. Energy-efficient and metastability-immune resilient circuits for dynamic variation tolerance. *IEEE Journal of Solid-State Circuits 44*, 1 (Jan 2009), 49–63.

ISBN: 978-2-11-129250-5

[24] BREIER, J., HE, W., BHASIN, S., JAP, D., CHEF, S., ONG, H. G., AND GAN, C. L. Extensive laser fault injection profiling of 65 nm fpga. *Journal of Hardware and Systems Security 1*, 3 (Sep 2017), 237–251.

[25] BUCHNER, S., MILLER, F., POUGET, V., AND MCMORROW, D. Pulsed-laser testing for single-event effects investigations. *IEEE Transactions on Nuclear Science* (2013).

[26] CADENCE. Innovus implementation system. Software, https://www.cadence.com/content/cadence-www/global/en_US/home/tools/digital-design-and-signoff/hierarchical-design-and-floorplanning/innovus-implementation-system.html [accessed 2017-12-07]. (December 3, 2017).

[27] CADENCE. Spectre extensive partitioning simulator. Software, https://www.cadence.com/content/cadence-www/global/en_US/home/tools/custom-ic-analog-rf-design/circuit-simulation/spectre-extensive-partitioning-simulator-xps.html [accessed 2017-12-07]. (December 3, 2017).

[28] CADENCE. Voltus IC power integrity solution. Software, https://www.cadence.com/content/cadence-www/global/en_US/home/tools/digital-design-and-signoff/silicon-signoff/voltus-ic-power-integrity-solution.html [accessed 2017-12-07]. (December 3, 2017).

[29] CANIVET, G., MAISTRI, P., LEVEUGLE, R., CLÉDIÈRE, J., VALETTE, F., AND RENAUDIN, M. Glitch and laser fault attacks onto a secure aes implementation on a sram-based fpga. *Journal of Cryptology 24*, 2 (Apr 2011), 247–268.

[30] CHA, H., AND PATEL, J. A logic-level model for alpha;-particle hits in cmos circuits. In *Computer Design: VLSI in Computers and Processors, 1993. ICCD '93. Proceedings., 1993 IEEE International Conference on* (Oct 1993), pp. 538–542.

ISBN: 978-2-11-129250-5

[31] CHA, H., RUDNICK, E. M., PATEL, J. H., IYER, R. K., AND CHOI, G. S. A gate-level simulation environment for alpha-particle-induced transient faults. *IEEE Transactions on Computers 45*, 11 (Nov 1996).

[32] CHEN, H. H., AND LING, D. D. Power supply noise analysis methodology for deep-submicron vlsi chip design. In *Proceedings of the 34th Design Automation Conference* (June 1997), pp. 638–643.

[33] CHEN, H. T., CHANG, C. C., AND HWANG, T. Reconfigurable eco cells for timing closure and ir drop minimization. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems 18*, 12 (DECEMBER 2010), 1686–1695.

[34] DARRACQ, F., LAPUYADE, H., BUARD, N., MOUNSI, F., FOUCHER, B., FOUILLAT, P., CALVET, M. C., AND DUFAYEL, R. Backside seu laser testing for commercial off-the-shelf srams. *IEEE Transactions on Nuclear Science* (2002).

[35] DAS, S., TOKUNAGA, C., PANT, S., MA, W. H., KALAISELVAN, S., LAI, K., BULL, D. M., AND BLAAUW, D. T. Razorii: In situ error detection and correction for pvt and ser tolerance. *IEEE Journal of Solid-State Circuits 44*, 1 (Jan 2009), 32–48.

[36] DEHBAOUI, A., DUTERTRE, J.-M., ROBISSON, B., AND TRIA, A. Electromagnetic Transient Faults Injection on a hardware and software implementations of AES. In *FDTC 2012* (Leuven, Belgium, Sept. 2012), p. 7.

[37] DHEM, J.-F., KOEUNE, F., LEROUX, P.-A., MESTRÉ, P., QUISQUATER, J.-J., AND WILLEMS, J.-L. A practical implementation of the timing attack. In *Smart Card Research and Applications* (Berlin, Heidelberg, 2000), J.-J. Quisquater and B. Schneier, Eds., Springer Berlin Heidelberg, pp. 167–182.

[38] DODD, P. E., SHANEYFELT, M. R., FELIX, J. A., AND SCHWANK, J. R. Production and propagation of single-event transients in high-speed digital logic ics. *IEEE Transactions on Nuclear Science 51*, 6 (Dec 2004), 3278–3284.

[39] DOUIN, A., POUGET, V., LEWIS, D., FOUILLAT, P., AND PERDU, P. Electrical modeling for laser testing with different pulse durations. In *11th IEEE IOLTS* (July 2005), pp. 9–13.

ISBN: 978-2-11-129250-5

[40] DUTERTRE, J.-M., POSSAMAI BASTOS, R., POTIN, O., FLOTTES, M.-L., ROUZEYRE, B., DI NATALE, G., AND SARAFIANOS, A. Improving the ability of Bulk Built-In Current Sensors to detect Single Event Effects by using triple-well CMOS. *Microelectronics Reliability 54* (Sept. 2014), 2289 – 2294.

[41] ENLOW, E. W., AND ALEXANDER, D. R. Photocurrent modeling of modern microcircuit pn junctions. *IEEE Transactions on Nuclear Science 35*, 6 (Dec 1988), 1467–1474.

[42] FERLET-CAVROIS, V., PAILLET, P., GAILLARDIN, M., LAMBERT, D., BAGGIO, J., SCHWANK, J. R., VIZKELETHY, G., SHANEYFELT, M. R., HIROSE, K., BLACKMORE, E. W., FAYNOT, O., JAHAN, C., AND TOSTI, L. Statistical analysis of the charge collected in soi and bulk devices under heavy lon and proton irradiation mdash;implications for digital sets. *IEEE Transactions on Nuclear Science 53*, 6 (Dec 2006), 3242–3252.

[43] FLEETWOOD, Z. E., LOURENCO, N. E., ILDEFONSO, A., WARNER, J. H., WACHTER, M. T., HALES, J. M., TZINTZAROV, G. N., ROCHE, N. J. H., KHACHATRIAN, A., BUCHNER, S. P., MCMORROW, D., PAKI, P., AND CRESSLER, J. D. Using tcad modeling to compare heavy-ion and laser-induced single event transients in sige hbts. *IEEE Transactions on Nuclear Science 64*, 1 (Jan 2017), 398–405.

[44] GODLEWSKI, C., POUGET, V., LEWIS, D., AND LISART, M. Electrical modeling of the effect of beam profile for pulsed laser fault injection. *Microelectronics Reliability* (Aug. 2009).

[45] GOH, W.-L., YEO, K.-S., LAZUARDI, S., PENG, W., LEONG, K.-C., CHAN, L., AND SEE, A. Latchup characterization of 0.18-micron sti cobalt silicided test structures. *Microelectronics Journal 32*, 9 (2001), 725 – 731.

[46] GREENSTEIN, G. S., AND PATEL, J. H. E-proofs: A cmos bridging fault simulator. In *1992 IEEE/ACM ICCAD* (Nov 1992), pp. 268–271.

[47] GUIMARÃES, L. A., BASTOS, R. P., DE PAIVA LEITE, T. F., AND FESQUET, L. Simple tri-state logic trojans able to upset properties of ring oscillators. In *2016 International Conference on Design and Technology of Integrated Systems in Nanoscale Era (DTIS)* (April 2016), pp. 1–6.

ISBN: 978-2-11-129250-5

[48] HABING, D. H. The use of lasers to simulate radiation-induced transients in semiconductor devices and circuits. *IEEE Transactions on Nuclear Science 12*, 5 (Oct 1965), 91–100.

[49] HAJIMIRI, A., LIMOTYRAKIS, S., AND LEE, T. H. Jitter and phase noise in ring oscillators. *IEEE Journal of Solid-State Circuits 34*, 6 (1999).

[50] HERIVEAUX, L., CLEDIERE, J., AND ANCEAU, S. Electrical modeling of the effect of photoelectric laser fault injection on bulk cmos design. In *39th ISTFA ASM* (2013).

[51] HERZEL, F., AND RAZAVI, B. A study of oscillator jitter due to supply and substrate noise. *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing 46*, 1 (Jan 1999), 56–62.

[52] HSIEH, C. M., MURLEY, P. C., AND O'BRIEN, R. R. A field-funneling effect on the collection of alpha-particle-generated carriers in silicon devices. *IEEE Electron Device Letters 2*, 4 (April 1981), 103–105.

[53] HSIEH, C.-M., MURLEY, P. C., AND O'BRIEN, R. R. Collection of charge from alpha-particle tracks in silicon devices. *IEEE Transactions on Electron Devices 30*, 6 (Jun 1983), 686–693.

[54] HUANG, H. M., LIN, Y., AND WEN, C. H. P. Fast-yet-accurate variation-aware current and voltage modelling of radiation-induced transient fault. In *DATE* (2016).

[55] HUBERT, G., VELAZCO, R., AND PERONNARD, P. A generic platform for remote accelerated tests and high altitude seu experiments on advanced ics: Correlation with musca sep3 calculations. In *2009 15th IEEE International On-Line Testing Symposium* (June 2009), pp. 180–180.

[56] I. HAYASHI, Y., HOMMA, N., SUGAWARA, T., MIZUKI, T., AOKI, T., AND SONE, H. Non-invasive emi-based fault injection attack against cryptographic modules. In *2011 IEEE International Symposium on Electromagnetic Compatibility* (Aug 2011), pp. 763–767.

[57] JIANG, Z. H., AND FEI, Y. A novel cache bank timing attack. In *2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)* (Nov 2017), pp. 139–146.

ISBN: 978-2-11-129250-5

[58] JOHNSTON, A. H. Charge generation and collection in p-n junctions excited with pulsed infrared lasers. *IEEE Trans. Nucl. Sci.* (1993).

[59] JORDAN, A. G., AND MILNES, A. G. Photoeffect on diffused p-n junctions with integral field gradients. *IRE Transactions on Electron Devices 7*, 4 (Oct 1960), 242–251.

[60] KARNIK, T., AND HAZUCHA, P. Characterization of soft errors caused by single event upsets in cmos processes. *Dependable and Secure Computing, IEEE Transactions on 1*, 2 (April 2004), 128–143.

[61] KELSEY, J., SCHNEIER, B., WAGNER, D., AND HALL, C. Side channel cryptanalysis of product ciphers. In *Computer Security — ESORICS 98* (Berlin, Heidelberg, 1998), J.-J. Quisquater, Y. Deswarte, C. Meadows, and D. Gollmann, Eds., Springer Berlin Heidelberg, pp. 97–110.

[62] KIM, C. H., AND QUISQUATER, J.-J. Faults, injection methods, and fault attacks. *Design Test of Computers, IEEE 24*, 6 (Nov 2007), 544–545.

[63] KIM, C. H., AND QUISQUATER, J. J. Faults, injection methods, and fault attacks. *IEEE Design Test of Computers 24*, 6 (Nov 2007), 544–545.

[64] KOCHER, P. C. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In *Advances in Cryptology — CRYPTO '96* (Berlin, Heidelberg, 1996), N. Koblitz, Ed., Springer Berlin Heidelberg, pp. 104–113.

[65] KOCHER, P. C., JAFFE, J., AND JUN, B. Differential power analysis. In *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology* (London, UK, UK, 1999), CRYPTO '99, Springer-Verlag, pp. 388–397.

[66] KÖMMERLING, O., AND KUHN, M. G. Design principles for tamper-resistant smartcard processors. In *Proceedings of the USENIX WOST* (Berkeley, CA, USA, 1999), USENIX Association, pp. 2–2.

[67] KRAKOVINSKY, A., BOCQUET, M., WACQUEZ, R., COIGNUS, J., AND PORTAL, J. M. Thermal laser attack and high temperature heating on hfo2-based oxram cells. In *2017 IEEE 23rd International Symposium on On-Line Testing and Robust System Design (IOLTS)* (July 2017), pp. 85–89.

ISBN: 978-2-11-129250-5

[68] LECOMTE, M., FOURNIER, J. J. A., AND MAURINE, P. Thoroughly analyzing the use of ring oscillators for on-chip hardware trojan detection. In *2015 ReConFig* (Dec 2015), pp. 1–6.

[69] LLIDO, R., SARAFIANOS, A., GAGLIANO, O., SERRADEIL, V., GOUBIER, V., LISART, M., HALLER, G., POUGET, V., LEWIS, D., DUTERTRE, J. M., AND TRIA, A. Characterization and tcad simulation of 90 nm technology transistors under continous photoelectric laser stimulation for failure analysis improvement. In *2012 19th IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits* (July 2012).

[70] LU, F., NATALE, G. D., FLOTTES, M. L., AND ROUZEYRE, B. Laser-induced fault simulation. In *Euromicro Conference on Digital System Design* (2013).

[71] LU, F., NATALE, G. D., FLOTTES, M. L., ROUZEYRE, B., AND HUBERT, G. Layout-aware laser fault injection simulation and modeling: From physical level to gate level. In *2014 9th IEEE International Conference on Design Technology of Integrated Systems in Nanoscale Era (DTIS)* (May 2014).

[72] MAISTRI, P., LEVEUGLE, R., BOSSUET, L., AUBERT, A., FISCHER, V., ROBISSON, B., MORO, N., MAURINE, P., DUTERTRE, J. M., AND LISART, M. Electromagnetic analysis and fault injection onto secure circuits. In *2014 22nd International Conference on Very Large Scale Integration (VLSI-SoC)* (Oct 2014), pp. 1–6.

[73] MARC SCHMIDT, J., AND HUTTER, M. Optical and em fault-attacks on crt-based rsa: Concrete results, 2007.

[74] MAURINE, P. Techniques for em fault injection: Equipments and experimental results. In *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography* (Sept 2012), pp. 3–4.

[75] MAURINE, P., TOBICH, K., ORDAS, T., AND LIARDET, P. Y. Yet Another Fault Injection Technique : by Forward Body Biasing Injection. In *YACC'2012: Yet Another Conference on Cryptography* (Porquerolles Island, France, Sept. 2012).

[76] MAY, T. C., AND WOODS, M. H. A new physical mechanism for soft errors in dynamic memories. In *16th International Reliability Physics Symposium* (April 1978), pp. 33–40.

ISBN: 978-2-11-129250-5

[77] MAY, T. C., AND WOODS, M. H. Alpha-particle-induced soft errors in dynamic memories. *IEEE Transactions on Electron Devices* (Jan 1979).

[78] MCNEILL, J. A. Jitter in ring oscillators. *IEEE Journal of Solid-State Circuits 32*, 6 (Jun 1997), 870–879.

[79] MENG, X. Decoupling capacitor design issues in 90 nm cmos. msc thesis, university of british columbia.

[80] MESSENGER, G. C. Collection of charge on junction nodes from ion tracks. *IEEE Transactions on Nuclear Science* (1982).

[81] MESSERGES, T. S., DABBISH, E. A., AND SLOAN, R. H. Investigations of power analysis attacks on smartcards. In *Proceedings of the USENIX Workshop on Smartcard Technology on USENIX Workshop on Smartcard Technology* (Berkeley, CA, USA, 1999), WOST'99, USENIX Association, pp. 17–17.

[82] MEYER, W., AND CAMPOSANO, R. Active timing multilevel fault-simulation with switch-level accuracy. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 14*, 10 (Oct 1995).

[83] MORRISON, R. *Digital Electronics*. Wiley-IEEE Press, 2007, pp. 240–.

[84] MUKHERJEE, S. *Architecture Design for Soft Errors*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2008.

[85] NETO, E., RIBEIRO, I., VIEIRA, M., WIRTH, G., AND KASTENSMIDT, F. Using bulk built-in current sensors to detect soft errors. *Micro, IEEE 26*, 5 (Sept 2006), 10–18.

[86] NICOLAIDIS, M. Time redundancy based soft-error tolerance to rescue nanometer technologies. In *VLSI Test Symposium, 1999. Proceedings. 17th IEEE* (1999), pp. 86–94.

[87] OKAZAKI, Y., KOBAYASHI, T., KONAKA, S., MORIMOTO, T., TAKAHASHI, M., IMAI, K., AND KADO, Y. Characteristics of a new isolated p-well structure using thin epitaxy over the buried layer and trench isolation. *IEEE Transactions on Electron Devices 39*, 12 (Dec 1992), 2758–2764.

[88] PALFRAMAN, D. J., KIM, N. S., AND LIPASTI, M. H. Time redundant parity for low-cost transient error detection. In *2011 Design, Automation Test in Europe* (March 2011), pp. 1–6.

ISBN: 978-2-11-129250-5

[89] PAPADIMITRIOU, A., HELY, D., BEROULLE, V., MAISTRI, P., AND LEVEUGLE, R. A multiple fault injection methodology based on cone partitioning towards rtl modeling of laser attacks. In *2014 Design, Automation Test in Europe Conference Exhibition (DATE)* (March 2014), pp. 1–4.

[90] PENG, K., HUANG, Y., GUO, R., CHENG, W.-T., AND TEHRANIPOOR, M. Emulating and diagnosing ir-drop by using dynamic sdf. In *2010 15th ASP-DAC* (Jan 2010), pp. 511–516.

[91] POSSAMAI BASTOS, R., DI NATALE, G., FLOTTES, M.-L., LU, F., AND ROUZEYRE, B. A new recovery scheme against short-to-long duration transient faults in combinational logic. *Journal of Electronic Testing 29*, 3 (Jun 2013), 331–340.

[92] POSSAMAI BASTOS, R., SILL TORRES, F., DUTERTRE, J.-M., FLOTTES, M.-L., DI NATALE, G., AND ROUZEYRE, B. A single built-in sensor to check pull-up and pull-down cmos networks against transient faults. In *Power and Timing Modeling, Optimization and Simulation (PATMOS), 2013 23rd International Workshop on* (Sept 2013), pp. 157–163.

[93] POUGET, V., LAPUYADE, H., LEWIS, D., DEVAL, Y., FOUILLAT, P., AND SARGER, L. Spice modeling of the transient response of irradiated mosfets. In *1999 Fifth European Conference on Radiation and Its Effects on Components and Systems. RADECS 99 (Cat. No.99TH8471)* (1999), pp. 69–74.

[94] POWER, S. I. Em/ir, thermal reliability and power integrity. Website, https://www.silvaco.com/products/analog_mixed_signal/inVar/invar.html [accessed 2018-06-25]. (June 25, 2018).

[95] REDHAWK, A. Power integrity and reliability analysis. Website, https://www.ansys.com/products/semiconductors/ansys-redhawk [accessed 2018-06-25]. (June 25, 2018).

[96] ROSCIAN, C., DUTERTRE, J., AND TRIA, A. Frontside laser fault injection on cryptosystems - application to the aes' last round -. In *2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)* (June 2013), pp. 119–124.

[97] ROSCIAN, C., SARAFIANOS, A., DUTERTRE, J. M., AND TRIA, A. Fault model analysis of laser-induced faults in sram memory cells. In *FDTC, 2013 Workshop on* (Aug 2013), pp. 89–98.

ISBN: 978-2-11-129250-5

[98] ROSSI, D., OMANA, M., AND METRA, C. Transient fault and soft error on-die monitoring scheme. In *Defect and Fault Tolerance in VLSI Systems (DFT), 2010 IEEE 25th International Symposium on* (Oct 2010), pp. 391–398.

[99] RUBINSTEIN, J., PENFIELD, P., AND HOROWITZ, M. A. Signal delay in rc tree networks. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 2*, 3 (July 1983), 202–211.

[100] SANTOS, M. B., AND TEIXEIRA, J. P. Defect-oriented mixed-level fault simulation of digital systems-on-a-chip using hdl. In *DATE Conference and Exhibition, 1999. Proceedings (Cat. No. PR00078)* (1999).

[101] SARAFIANOS, A., GAGLIANO, O., SERRADEIL, V., LISART, M., DUTERTRE, J. M., AND TRIA, A. Building the electrical model of the pulsed photoelectric laser stimulation of an nmos transistor in 90nm technology. In *IRPS, 2013 IEEE International* (April 2013), pp. 5B.5.1–5B.5.9.

[102] SCHMIDT, J. M., HUTTER, M., AND PLOS, T. Optical fault attacks on aes: A threat in violet. In *2009 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)* (Sept 2009), pp. 13–22.

[103] SELLERS, F., XIAO, M., AND BEARNSON, L. *Error detecting logic for digital computers*. McGraw-Hill, 1968.

[104] SHEPARD, K. L., AND NARAYANAN, V. Noise in deep submicron digital design. In *Proceedings of International Conference on Computer Aided Design* (Nov 1996), pp. 524–531.

[105] SILVACO. 2d silicon device simulator. Software, https://www.silvaco.com/products/vwf/atlas/spisces/spisces_br.html [accessed 2018-04-14]. (April 14, 2018).

[106] SIMIONOVSKI, A., AND WIRTH, G. Simulation evaluation of an implemented set of complementary bulk built-in current sensors with dynamic storage cell. *IEEE Transactions on Device and Materials Reliability 14*, 1 (March 2014), 255–261.

[107] SKOROBOGATOV, S. Optical fault masking attacks. In *2010 Workshop on Fault Diagnosis and Tolerance in Cryptography* (Aug 2010), pp. 23–29.

ISBN: 978-2-11-129250-5

[108] SKOROBOGATOV, S., AND WOODS, C. In the blink of an eye: There goes your aes key. Cryptology ePrint Archive, Report 2012/296, 2012. https://eprint.iacr.org/2012/296.

[109] SKOROBOGATOV, S. P., AND ANDERSON, R. J. Optical fault induction attacks. In *4th International Workshop on Cryptographic Hardware and Embedded Systems* (London, UK, 2002), Springer-Verlag, pp. 2–12.

[110] SPREITZER, R., MOONSAMY, V., KORAK, T., AND MANGARD, S. Systematic classification of side-channel attacks: A case study for mobile devices. *IEEE Communications Surveys Tutorials 20*, 1 (Firstquarter 2018), 465–488.

[111] STMICROELECTRONICS. Stmicroelectronics - life.augmented. Website, http://www.st.com [accessed 2018-05-04]. (May 04, 2018).

[112] STRINGFELLOW, D., PEDICONE, J., AND PROFESSIONAL SERVICES, S. Decoupling capacitance estimation, implementation, and verification: A practical approach for deep submicron socs. *SNUG San Jose* (01 2007).

[113] TAO, Y., AND LIM, S. K. Decoupling capacitor planning with analytical delay model on rlc power grid. In *2009 Design, Automation Test in Europe Conference Exhibition* (April 2009), pp. 839–844.

[114] TEHRANIPOOR, M., AND BUTLER, K. M. Guest editors' introduction: Ir drop in very deep-submicron designs. *IEEE Design Test of Computers 24*, 3 (May 2007), 214–215.

[115] TIEMPO. Tiempo secure. Website, http://www.tiempo-secure.com [accessed 2018-05-04]. (May 04, 2018).

[116] VAN WOUDENBERG, J. G. J., WITTEMAN, M. F., AND MENARINI, F. Practical optical fault injection on secure microcontrollers. In *2011 Workshop on Fault Diagnosis and Tolerance in Cryptography* (Sept 2011), pp. 91–99.

[117] VIERA, R. A. C., DUTERTRE, J. M., BASTOS, R. P., AND MAURINE, P. Role of laser-induced ir drops in the occurrence of faults: Assessment and simulation. In *2017 Euromicro Conference on Digital System Design (DSD)* (Aug 2017), pp. 252–259.

[118] WANG, F., AND AGRAWAL, V. D. Single event upset: An embedded tutorial. In *21st International Conference on VLSI Design* (Jan 2008).

ISBN: 978-2-11-129250-5

[119] WANG, W., YU, Y., STANDAERT, F. X., LIU, J., GUO, Z., AND GU, D. Ridge-based dpa: Improvement of differential power analysis for nanoscale chips. *IEEE Transactions on Information Forensics and Security 13*, 5 (May 2018), 1301–1316.

[120] WANG, X., AND SU, D. On-chip emi monitoring for integrated circuits of 55nm and below technologies. In *General Assembly and Scientific Symposium (URSI GASS), 2014 XXXIth URSI* (Aug 2014), pp. 1–4.

[121] WIRTH, J. L., AND ROGERS, S. C. The transient response of transistors and diodes to ionizing radiation. *IEEE Transactions on Nuclear Science 11* (1964).

[122] XILINX. Ml501 evaluation platform. Software, https://www.xilinx.com/support/documentation/boards_and_kits/ug226.pdf [accessed 2018-04-24]. (April 24, 2018).

[123] XILINX. Planahead design and analysis tool. Software, https://www.xilinx.com/products/design-tools/planahead.html [accessed 2017-12-07]. (January 8, 2018).

[124] XILINX. Virtex-5 overview. Software, https://www.xilinx.com/support/documentation/data_sheets/ds100.pdf [accessed 2017-12-07]. (December 7, 2017).

[125] ZHAO, S., AND ROY, K. Estimation of switching noise on power supply lines in deep sub-micron cmos circuits. In *VLSI Design, 2000. Thirteenth International Conference on* (2000), pp. 168–173.

ISBN: 978-2-11-129250-5