MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU

FACULTE DE GENIE ELECTRIQUE ET DE L'INFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

THESE DE DOCTORAT EN SCIENCES

Spécialité : Electronique

Option : Microélectronique

Présentée par :

M^me^ AIT ABDELMALEK Ghania Ep. MOKDAD

Sujet :

Étude et modélisation de défauts des circuits fortement submicroniques sécurisés en vue du test

Soutenue le devant le jury composé de :

M. BELKAID Mohammed Said	Professeur	Université M. Mammeri, Tizi-Ouzou	President
M. ZIANI Rezki	Professeur	Université M. Mammeri, Tizi-Ouzou	Rapporteur
M. BENSIDHOUM M. Ou Tahar	M.C.A	Université M. Mammeri, Tizi-Ouzou	Examinateur
M. BENTERZI Hamid	Professeur	Université M. Bouguerra, Boumerdes	Examinateur
M. CHEMALI Hamimi	M.C.A	Université F. Abbas, Sétif	Examinateur
M. DJOUADI Djamel	Professeur	Université A. Mira, Bejaia	Examinateur

Remerciements

Je tiens à remercier tout particulièrement mon promoteur Monsieur Rezki Ziani, Professeur et chef de département électronique à l'UMMTO, de m'avoir confié ce travail et de l'avoir dirigé avec simplicité et objectivité, qu'il trouve ici l'expression de mon respect et de ma profonde reconnaissance.

Je remercie le Professeur Mohammed Said Belkaid, doyen de la faculté de génie électrique et informatique à l'UMMTO, pour l'honneur qu'il m'a fait en présidant ce jury.

Je remercie également Messieurs Mohand Outahar Bensidhoum, Maître de conférences A à l'UMMTO, Benterzi Hamid, Professeur à l'Université M. Bouguerra, Boumerdes, CHEMALI Hamimi, Maître de conférences A à Université F. Abbas, Sétif et Djouadi Djamel, Professeur à l'Université A. Mira, Bejaia, pour l'intérêt qu'ils ont porté à mon travail en acceptant de participer au jury.

Mes remerciements s'adressent aussi à toutes les personnes qui de près ou de loin m'ont aidé au cours de ces années, particulièrement :

Monsieur Mourad Laghrouche, Professeur à l'UMMTO, pour ses conseils et sa patience surtout à la fin de ma thèse.

Monsieur Ahcène Lakhlef, MCB à l'UMMTO, pour son aide précieuse et son soutien permanent.

Monsieur Aurel Gontean et son assistante Monica Chiosa de l'université Polytechnique de Timisoara en Roumanie, pour m'avoir accueillie pour quelques semaines au sein de son laboratoire afin de me lancer dans la validation expérimentale sur FPGA.

Je remercie également mes parents et ma sœur pour leur soutien et leurs encouragements.

Enfin, merci à toi mon mari, pour ton soutien indispensable, ton implication et ta patience.

Résumé

Compte tenu des récents progrès technologiques, les circuits sécurisés implémentés en contremesures WDDL et QDI apparaissent plus intéressants que les circuits synchrones, principalement pour sécuriser l'implantation des circuits intégrés contre les attaques par injection de fautes et par analyse de courant. Cependant, le manque de méthodes et d'outils de test a limité l'utilisation de ce type de circuits. L'objectif de ce travail de thèse est de présenter une méthode de test et de tolérance aux fautes de ces circuits sécurisées. Cette méthode montre que les modèles de fautes appliqués dans les structures CMOS classiques sont aussi applicables pour les structures sécurisées tolérantes aux fautes. Ces structures peuvent fonctionner correctement malgré la présence de deux défauts résistifs, les courts-circuits résistifs et les circuits ouverts résistifs. Les différentes mesures sont effectuées sous Spice de Cadence. Les résultats expérimentaux obtenus par FPGA valident la méthode proposée.

Mots clés: circuits asynchrones, circuits sécurisés, modèle de fautes, test, tolérance aux fautes

Due to recent technological advances, the secure circuits implemented in WDDL and in QDI countermeasures appear more interesting than synchronous circuits, mainly to secure the implementation of integrated circuits against attacks by fault injection and power analysis. However, the lack of method and test tool has limited the use of this type of circuits. The objective of this thesis is to present a method for testing and fault tolerance of these secure circuits. This method shows that the fault models applied in conventional CMOS structures are also applicable for secure structures fault tolerant, and as these structures can function correctly despite the presence of the two resistive defaults resistance faults, the resistive-bridge defect and the resistive-open defcet. The various measures are carried out under Spice Cadence. The experimental results obtained by FPGA validate the proposed methodology.

Key words: Asynchronous circuits, Secured circuits, fault models, testing, fault tolerance.

Sommaire

CHAPITRE 2 : ATTAQUES ET CONTREMESURES

CHAPITRE 3 Impact des défauts résistifs sur les circuits sécurisés

CHAPITRE 4 APPLICATION DE LA METHODE SUR DES CIRCUITS SECURISES IMPLEMENTES SUR FPGA

Liste des figures

Liste des Abréviations et Symboles

Abréviation	Description
AES	Advanced Encryption Standard
CMOS	Complementary Metal Oxide Semiconductor
DFR	Design For Reliability
DIMS	Delay-Insensitive Minterm Synthesis
DL	Defect Level
DPA	Differential Power Analysis
FPGA	Field-Programmable Gate Array
MDPL	Masked Dual-rail Precharge Logic
MTBF	Mean Time Between Failure
MTTF	Mean Time To Failure
NMR	N-Modular Redundancy
QDI	Quasi Delay-Insensitiv
R	Reliability
SABL	Sense Amplifier Based Logic
SPA	Simple Power Analysis
STTL	Secure Triple Track Logic
TMR	Triple Modular Redundancy
VHDL	HDL-Hardware Description Language
WDDL	Wave Dynamic Differential Logic
Y	Yield

Introduction générale

L’essor des nanotechnologies nécessite le développement de techniques de test et de tolérance aux fautes fiables pour répondre aux évaluations des risques potentiels et au contrôle après fabrication. En effet, avec l'avènement des technologies submicroniques, certains phénomènes physiques qui auparavant étaient négligeables deviennent prépondérants. Nous pouvons citer notamment la variation des paramètres des transistors (dimensions, dopages), les courants de fuite dus à la variation de la tension d’alimentation et de la température. Ces phénomènes pouvant induire des défaillances ont une répercussion directe sur la fiabilité et le rendement de fabrication. Par conséquent, l’obtention d’une fiabilité plus élevée ne peut être atteinte que par plusieurs tests approfondis des circuits et des systèmes intégrés. Beaucoup de travaux ont porté sur différentes méthodologies pour tester les circuits intégrés [Lat13, Sch02, Wen03, Tha11, Pap11, Ala10, Gro10, Ait12, Ait12a]. Pour tester efficacement un circuit intégré, il est impératif de définir des modèles de défaut en adéquation avec les défauts réels des technologies CMOS nanométriques actuelles et des technologies futures. Les défauts de court-circuit et de circuit-ouvert sont les types prédominants de défaut de fabrication. Les modèles précédents de ces défauts comprennent des modèles de fautes logiques et des modèles de fautes de retard, mais ignorent la résistance du défaut. La plupart des modèles des défauts de circuits ouverts résistifs [Rod02, Aru05, Li03] et des modèles des défauts de courts circuits résistifs [Hao91, Sha01, Li03a] sont utilisés pour décrire les défauts de circuit-ouvert résistif et de court-circuit résistif entre les nœuds logiques. Il est important de noter que la résistance de ces deux défauts est un paramètre aléatoire inconnu car il dépend des paramètres technologiques géométriques du défaut.

Si la modélisation des défauts pour les technologies CMOS classique est un domaine relativement maitrisé comme en témoigne une littérature assez riche sur ce sujet, de nombreuses questions se posent quant à la modélisation de défauts de circuits utilisant la technologie CMOS pour des applications spécifiques, telles que les circuits cryptographiques.

Dans les circuits de cryptographie nécessitant la sécurité et des liaisons de communication longue, il est important de considérer les tests d'interconnexion et leur fiabilité. Nous avons montré que les circuits sécurisés peuvent être testés avec des modèles de défauts similaires à ceux utilisés pour les circuits CMOS standard [Ait14, Ait16]. D’autres travaux ont proposé des algorithmes de routage tolérants aux fautes sous les défauts permanents pour applications spécifiques, tels que NoCs [[Fic09] Lehtonen [Leh07] et Almukharizim [Alm07] ont mis l'accent sur la faute d'interconnexion permanente dans les circuits asynchrones. Verdel et Makris [Ver02] ont proposé une méthode de duplication dans laquelle ils comparent les sorties des circuits dupliqués à l'intérieur d’un intervalle de temps spécifié

pour détecter les défauts transitoires et permanents. Cependant, les auteurs ont constaté que le circuit dupliqué ne peut pas fonctionner correctement sous les défauts permanents.

Dans [Ait12, Ait02a], nous avons évalué la tolérance aux fautes et la fiabilité des structures de redondance modulaire triple (TMR) sous fautes de collage. Nous avons montré que si un seul module est défectueux, les deux autres modules seront dominants. Par conséquent, la faute sera masquée et la TMR produit une sortie correcte, la TMR peut fonctionner correctement avec la présence d'un seul défaut permanent. Par contre, ces méthodes sont limitées à des applications spécifiques, telles que des circuits standard de type « benchmarks ISCAS85 et ITC99 ».

Ce travail de thèse évalue la robustesse de la TMR à base de circuits WDDL et à base de circuits QDI en injectant des défauts de courts-circuits résistifs et de circuits-ouverts résistifs au niveau transistor dans deux des trois modules de la TMR qui génèrent les mêmes sorties. Afin de détecter ces défauts résistifs et donc de savoir si la TMR est tolérante aux pannes ou non, nous avons analysé l'impact de ces deux défauts sur le comportement électrique de ce type de structure. Étant donné que les niveaux de tension de sortie V_{out} dans les conditions de présence de défauts résistifs sont supérieurs ou inférieurs à la tension de seuil à l'arrivée du front d'horloge des signaux d'entrée, la porte dans le port d'entrée peut reconnaître les défauts résistifs en comparant V_{out} avec une tension de seuil dont la valeur détermine si le défaut est une faute résistive ou pas. Si le défaut est détecté il n'est pas toléré. Par contre, s'il n'est pas détecté alors il est toléré. La détection de défauts peut être réalisée sur la base de la surveillance de la tension de sortie proposée.

Ce manuscrit se présente de la façon suivante :

Dans le premier chapitre, nous donnons un bref état de l'art sur la fiabilité des circuits intégrés, les différents types de défauts ainsi que leurs répartitions dans les circuits. Nous présentons les modèles de fautes utilisés, la simulation de fautes, l'injection de fautes, ainsi que les techniques de test utilisées. Nous décrivons également dans ce chapitre les méthodologies conceptuelles mises en œuvre en vue de fiabilité DFR « Design For Reliability » des circuits intégrés et tout particulièrement les structures de redondance modulaire triple TMR

Dans le deuxième chapitre, nous présentons les différentes attaques connues, ainsi que les principales contre-mesures à ces attaques. Nous détaillons celles spécifiquement destinées aux circuits logiques, et notamment les contremesures WDDL et les contremesures QDI.

Dans le troisième chapitre, nous décrivons dans un premier temps, notre méthode de détection des défauts résistifs pour évaluer la tolérance aux fautes des structures TMR sécurisées implémentées en WDDL et QDI contremesures. Dans un deuxième temps, nous étudions à l'aide des modèles de fautes injectés directement sur la schématiques de ces structures sous Spice de Cadence leur comportement et leur robustesse par rapport à la séquence de test appliquée et à la taille des défauts considérés.

Dans le quatrième chapitre nous décrivons l'implémentation de la méthode de détection proposée sur FPGA. Les résultats obtenus sont analysés, ce qui permet de valider notre approche pour l'application considérée.

Une conclusion générale donnera une synthèse du travail effectué et résumera les principaux résultats obtenus ainsi que les perspectives envisagées.

Chapitre 1

Fiabilité et défaillance des circuits intégrés

1.1 Introduction

À cause de la miniaturisation croissante des procédés de fabrication (90 nm, 65 nm, 45 nm,…), il est de plus en plus difficile de réaliser un circuit intégré sans aucun défaut de fabrication. Les objectifs de l'industrie des semi-conducteurs est d'assurer que le composant électronique mis sur le marché donnera satisfaction au client en terme de fonctionnalités et de fiabilité. Par exemple les fabricants d'automobiles exigent zéro défaut dans les composants électroniques. Des exigences similaires sont appliquées pour les systèmes critiques de la vie où la sécurité est le facteur principal pris en compte. Une meilleure qualité de dispositifs électroniques ne peut être obtenue que par des tests approfondis des composants fabriqués. Le test des circuits et systèmes intégrés est une étape fondamentale qui doit veiller à leur bon fonctionnement. De nombreux travaux ont concerné la mise en œuvre de différentes méthodologies pour tester les circuits intégrés. Pour développer une stratégie de test efficace, il est très important de définir des modèles de défaut les plus représentatifs des défauts réels des technologies CMOS actuelles et à venir.

L'objectif de ce chapitre est de rappeler les principes de base du test et de la fiabilité des circuits intégrés. Nous présentons les définitions et les propriétés essentielles relatives au test, à la simulation de fautes, aux modèles de fautes, ainsi que les techniques d'injection de fautes utilisées pour la caractérisation et la détection du défaut considéré.

1.2 Fiabilité et rendement des circuits intégrés VLSI

Le rendement et la fiabilité sont complémentaires, et cette complémentarité est d'autant plus forte en considérant le rendement et la mortalité infantile qui sont fortement corrélés [Chr03]. En effet, chacun d'eux est affecté par les mêmes défauts tels que les défauts d'oxyde, d'alignement des masques ou des défauts induits par la faiblesse du processus de fabrication comme le dépôt de particules.

1.2.1-Notion de fiabilité

La fiabilité «R» est un attribut de la sureté de fonctionnement [Cou08, Del10, Vil97] et correspond à la probabilité qu'un système accomplisse la fonction pour laquelle il a été conçu, dans des conditions données et pendant une durée donnée. Un indicateur de bonne fiabilité est caractérisé par un MTBF (Mean Time Between Failure, moyenne des temps de bon fonctionnement) le plus long possible. Dans le cas d'un système non réparable, on parlera plutôt de temps moyen avant une défaillance « MTTF : Mean Time To Failure » [Cou08].

L'équation liant la fiabilité d'un système à son taux de défaillance s'écrit :

$$\lambda(t)\, R(t) + \frac{dR(t)}{dt} = 0$$

Où t est le temps de mission en heure.et λ: le taux de défaillance, égal au nombre de défaillances par le nombre d'heures opérationnelles.

La résolution de cette équation donne

$R(t) = \exp(-\int_0^t \lambda(u)du)$, qui devient :

$R(t) = e^{-\lambda t}$ dans le cas de la loi exponentielle ($\lambda(t)$ = constante).

La figure 1.1 montre qu'avec un taux de défaillance constant, la probabilité de fonctionner sans défaillance pour un temps supérieur au MTBF est seulement de 36,78%. En effet, lorsque t = MTBF, la fiabilité du circuit chute et devient égale à :

$R(t) = e^{-\frac{1}{(mtbf)}.(mtbf)} = e^{-1} = 36{,}78\%$.

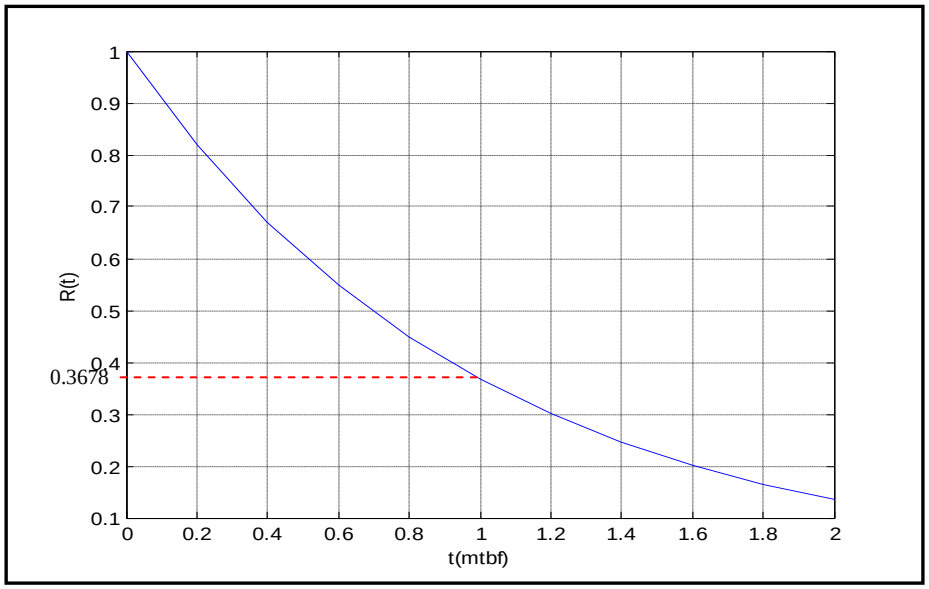


Figure 1.1 Relation entre fiabilité et le temps.

L'évolution du taux de défaillance d'un circuit VLSI durant son cycle de vie suit une courbe dite « en baignoire » représentée sur la figure 1.2. Cette courbe montre 3 phases distinctes :

Phase 1 : période dite de jeunesse, ou encore de mortalité infantile. Elle se caractérise par un taux de défaillance important mais décroissant. L'occurrence de défaillances durant cette période n'est pas aléatoire au cours du temps mais plutôt le résultat de défauts de

conception tels que par exemple des défauts d'isolation de grille. En général, on s'affranchit de l'étude dans cette zone par des tests de déverminage ou rodage.

Phase 2 : période de vie utile caractérisée par un taux de défaillance faible et relativement constant. Les circuits sont affectés par l'apparition de défauts aléatoires.

Phase 3 : période dite de vieillesse ou d'usure, caractérisée par un taux de défaillance croissant. L'occurrence de défaillances durant cette période est due à l'usure critique des circuits. Là aussi, on peut s'affranchir de l'étude dans cette zone, car on suppose que le circuit tombe en panne avant d'atteindre cette zone, ou alors il est remplacé avant.

Ceci justifie l'utilisation de la loi exponentielle (λ constante) dans les études de fiabilité.

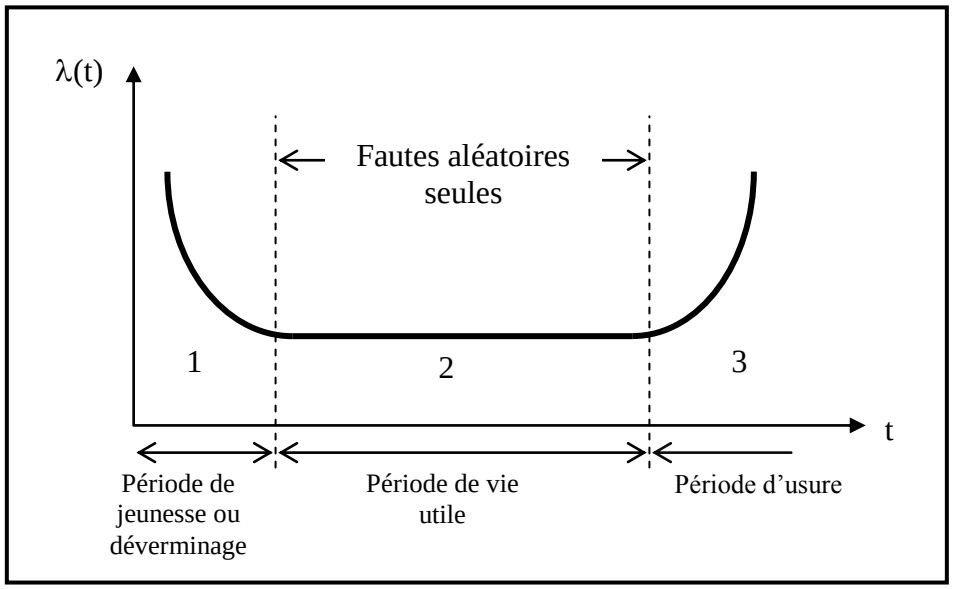


Figure 1.2 Évolution du taux de panne en fonction du temps.

1.2.2- Notion de rendement

La qualité du test dépend de la stratégie adoptée et de la technique mise en œuvre pour accomplir les tâches assurant la génération des vecteurs de test et le prélèvement des résultats. L'accomplissement de ces tâches dépend grandement de la possibilité d'accès offerte pour la réalisation de contacts avec les nœuds internes du système sous test. L'accessibilité aux circuits actuels est souvent difficile voire impossible. Il faut donc prendre en compte d'une part, le coût du développement des tests et le coût de leur mise en œuvre et d'autre part, les coûts entraînés par les produits défectueux non repérés lors des tests. Les tests doivent être mis en œuvre en parallèle avec la conception.

La qualité du test a une influence directe sur la fiabilité des circuits intégrés fabriqués. C'est pour cette raison, qu'il est indispensable d'introduire des métriques qui permettent d'évaluer la qualité du test de ces derniers. Ces métriques sont très utiles aussi bien pour le constructeur dans l'évaluation du test de production que pour le concepteur dans l'évaluation de sa technique de test. Dans le cas des fautes simples et des circuits numériques, le paramètre le plus utilisé est la couverture de fautes F qui correspond à la probabilité de détection de fautes dans le circuit. Cette probabilité est estimée comme suit

$$F = \frac{\text{le nombre de fautes détectées}}{\text{le nombre total de fautes}} \qquad (1.1)$$

Si on désigne par Y (Yield) le rendement de production de circuits corrects, par T l'efficacité des tests, le taux de produits défectueux DL (Defect Level) non détectés est donné par la relation (1 .2), définie pour la première fois par Williams et Brown [Wil81].

$$DL = 1 - Y^{(1-T)} \qquad (1.2)$$

$$DL = 1 - Y^{(1-T)} \iff 1 - T = \frac{\log(1-DL)}{\log(Y)} \qquad (1.3)$$

Soient n le nombre de soudures ou contacts sur une carte et *P* la probabilité pour que chacun d'entre eux soit en bon état. La probabilité pour que l'ensemble soit en bon état est donnée par :

$$Y = P^n \qquad (1.4)$$

Si les tests vérifient m contacts parmi les n, l'efficacité des tests est alors:

$$T = \frac{m}{n} \qquad (1.5)$$

La probabilité pour que les (n-m) contacts restants soient bons vaut $P^{(n-m)}$ et la probabilité de défaillance s'écrit [Mou00]:

$$DL = 1 - P^{n-m} = 1 - Y^{\frac{n-m}{n}} = 1 - Y^{(1-T)} \qquad (1.6)$$

1.3 Notions de base du test des circuits VLSI

Un circuit intégré est dit performant s'il est apte à réaliser sa fonction voulue avec un niveau de qualité et de fiabilité élevé. Pour garantir cette qualité de bon fonctionnement, il

faut tester et vérifier les circuits dès les premières étapes de conception. Une fois la conception validée, les circuits sont envoyés à la production pour en fabriquer des milliers d'échantillons. Pendant l'étape de fabrication dans les salles blanches, des défauts peuvent se produire (par exemple un court-circuit entre deux lignes métalliques parallèles ou entre les deux bornes d'un composant, un circuit-ouvert qui coupe la ligne métallique reliant deux composants etc.). Ces types de défauts rendent le circuit défectueux, d'où la nécessité d'une étape qui suit la fabrication. Cette étape consiste à tester tous les circuits fabriqués pour valider leur fonctionnalité ainsi que leurs spécifications prédéfinies afin de s'assurer que les circuits mis sur le marché donneront satisfaction au client en termes de fonctionnalité et de fiabilité. Parmi les différents types de test, le test de production est couramment utilisé lorsque le circuit fabriqué contient des défauts physiques ou de fabrication et par conséquent ne correspond pas au circuit conçu. Le test fonctionnel permet de détecter une erreur de conception lorsque le circuit conçu ne répond pas aux spécifications du cahier des charges.

1.3.1 Notion de vecteur de test

Le vecteur de test est définit comme étant une série de pulsations. Chaque pulsation i (figure 1.3) est caractérisée par sa largeur PWi et son temps d'échantillonnage t_i. La sortie du circuit sous test considérée dans le domaine transitoire est sensible à ces paramètres. L'analyse de sensibilité par rapport à ces paramètres est l'une des techniques les plus utilisées pour la génération de vecteurs de test dans la détection des fautes résistives [Var97]. L'algorithme de génération du vecteur de test optimal consiste à trouver le nombre optimal de pulsations, la largeur optimale et le temps d'échantillonnage optimal de chaque pulsation qui permettra la détection des fautes.

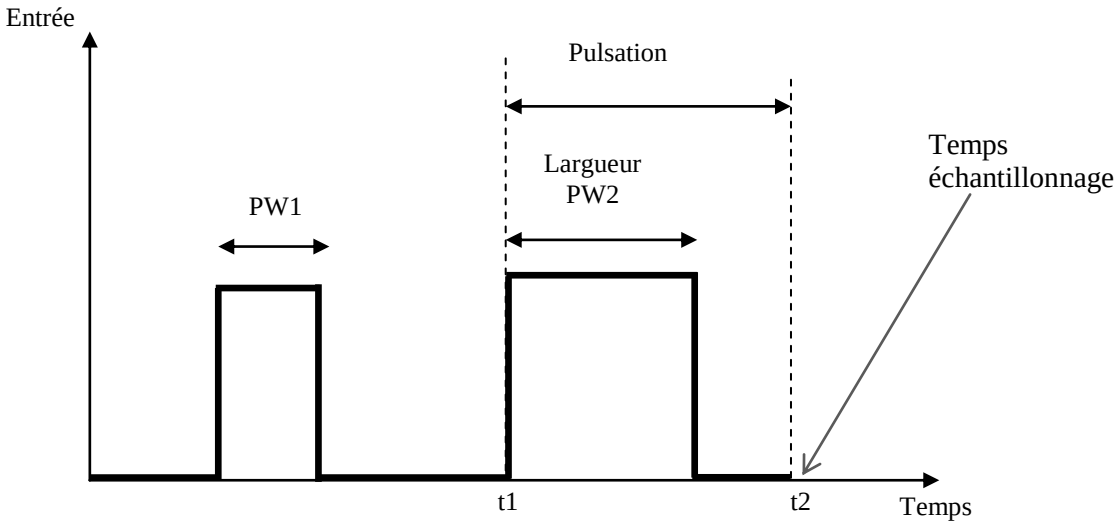


Figure 1.3 Vecteur de test à une série de pulsations de différentes largeurs.

1.3.2 Test fonctionnel

L'objectif d'un test fonctionnel est de vérifier toutes les fonctionnalités du circuit vu comme une boîte noire, avant de l'envoyer en fabrication. Il est effectué pour déterminer si le circuit réalise bien toutes les spécifications décrites dans le cahier de charges et faire le diagnostic en cas d'erreurs pour modifier sa conception. Il est couramment utilisé pour les petites puces analogiques et mixtes. Comme la fonctionnalité des circuits numériques devient de plus en plus complexe, il apparaît qu'il est pratiquement impossible de vérifier les fonctionnalités d'une puce, en particulier les composants numériques larges tels que les microprocesseurs. Ainsi, dans les circuits VLSI le test fonctionnel tend à être remplacé par le test structurel [Mac08]. Ce test améliore le taux de couverture de fautes.

1.3.3 Test de production

Le but de ce type de test est de déterminer si le circuit fabriqué ne contient pas de défauts de fabrication et de séparer les circuits défaillants des circuits fonctionnels. Avec un tel test, les circuits défaillants ne peuvent pas être réparés, ils seront écartés. Cependant le diagnostic s'effectue dans le but d'améliorer le rendement de la chaîne de fabrication. Le test de production comprend trois types de test :

- Le test alternatif, utilisé pour les circuits analogiques, mixtes et radiofréquences RF.
- Le test structurel (test logique), le circuit est vu comme une boîte blanche. Ce test est largement adopté pour le test des circuits numériques basé sur les modèles de fautes. Il permet d'utiliser un ensemble optimal de vecteurs de test et nécessite un minimum de temps de test, et par conséquent réduit efficacement le coût du test.
- Le test paramétrique ou de caractérisation sur plusieurs lots de circuits et prototypes pour déterminer les limites de fonctionnement du circuit. Ce type de test s'effectue à chaque nouvelle conception ou nouveau processus de fabrication sous différentes conditions.

1.4 Motivation et coût du test

Les différentes étapes de fabrication des circuits intégrés sont très complexes, et par conséquent des défauts dus aux procédés de fabrication, aux matériaux, ou introduits lors de l'encapsulation dans le boîtier peuvent survenir. Une meilleure qualité de circuits électroniques ne peut être obtenue que par des tests approfondis des composants fabriqués. Au niveau du coût, ces tests suivent la règle de dix (10). Plus un défaut est détecté tôt dans le processus de fabrication, moins le coût qu'il va induire est élevé. En effet, si un circuit intégré est détecté défectueux, le coût du boîtier, de son intégration dans un système et ensuite de la localisation de l'erreur dans ce système sont évités. La figure 1.4 présente le coût d'un défaut en fonction du moment où il est repéré.

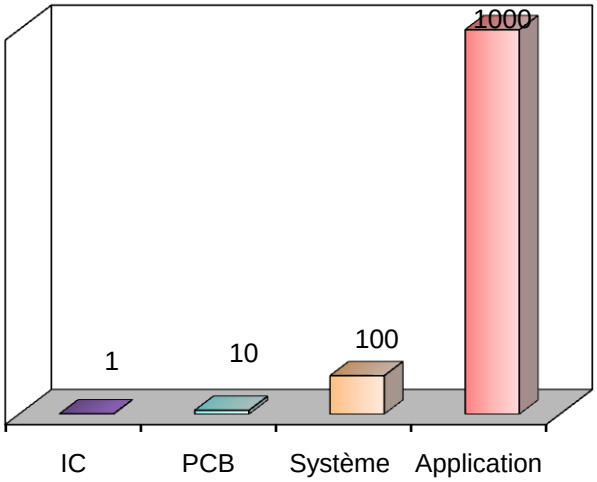


Figure 1.4 Motivation du test [Kho07].

1.5 Les différentes phases de test

Le circuit VLSI subit différentes phases de test illustrées à la figure 1.5, pendant son procédé de fabrication et dont la durée appelée temps de cycle est d'environ deux mois jusqu'à la mise en boîtier. La fabrication d'un circuit intégré passe par deux étapes principales, l'étape de conception ou de design et l'étape de fabrication. Dans chacune des étapes, les phases de test s'appliquent de la manière suivante :

- Test sur wafer « ∅=300mm » : réalisé par la machine « wafer prober » pour détecter les défauts de fabrication et éviter le montage en boîtier des circuits défectueux;
- Test du circuit encapsulé (Packaged) : pour détecter les défauts dus au processus d'encapsulation une fois les dices découpées et les circuits montés en boîtier ;
- Test du circuit sur la carte ;
- Test de la carte dans le système.

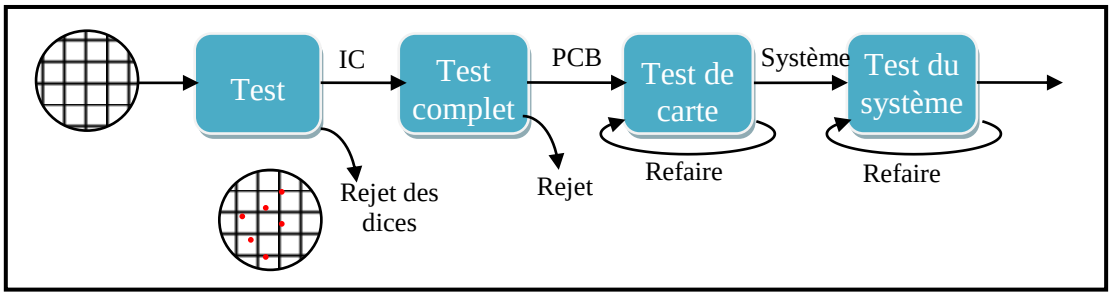


Figure 1.5 Phases de test

Dans les deux dernières phases on trouve le test de fonctions aux conditions nominales puis aux conditions limites d'environnement, le test des performances dynamiques et le test paramétrique (essentiellement les caractéristiques électriques des broches d'entrée/sortie) utilisé par exemple, pour mesurer le seuil du courant de fuite I_{DDQ} consommé par le circuit au

repos. Si le circuit sous test consomme moins que le courant de seuil, il est accepté, sinon, il est rejeté. Ce test détecte certaines défaillances que les tests classiques ne perçoivent pas. En effet, certains défauts, tels qu'un court-circuit entre polysilicium et oxyde de grille ou encore un défaut de pont entre deux pistes provoquent une surconsommation du courant I_{DDQ}. La détection de cette surconsommation nécessite une minuterie de capture pour effectuer la comparaison requise. Des solutions qui vont des capteurs de courants hors puce (off-chip sensors) aux capteurs de courant intégrés (built-in curent sensor BICS) pour des circuits à haute fiabilité sont utilisées aujourd'hui.

1.6 Défauts et fautes

Les défauts sont des pannes physiques qui affectent le layout d'un circuit [Kho07]. L'impact des défauts sur les caractéristiques électriques d'un circuit intégré déviant au-delà des valeurs spécifiées est appelée faute [Alb04, Eng00]. La présence d'un défaut dans un circuit ne conduit pas forcément à l'apparition d'une faute. En d'autres termes, le bon fonctionnement du circuit est assuré malgré la présence du défaut. Les défauts de fabrication qui peuvent avoir lieu dans un procédé CMOS sont dus à diverses sources.

1.6.1 Sources de défauts

Le procédé de fabrication est généralement la cause principale de la présence des fautes, que ce soit après fabrication ou bien après une durée de vie du circuit. Les fautes peuvent être aussi provoquées par le design et sont sensées être corrigées après la vérification des prototypes. Les sources qui peuvent être à l'origine de l'apparition de certains défauts sont [Kho07, Mil92(31)]:

1 Les erreurs humaines
   - Une partie d'un métal peut être discontinue provoquant un circuit ouvert.
   - Les dopants peuvent ne pas être diffusés avec la bonne concentration (non uniformité) ou aux zones appropriées altérant ainsi les caractéristiques des dispositifs ;
   - Mauvais alignement des masques ou contamination de ces derniers avec des particules de poussières, cheveux …etc.
   - Équipement défectueux
2 L'instabilité dans les conditions du process, en termes de changement de valeurs de n'importe quelle variable physique supposée constante.
3 L'instabilité du matériel, qui se rapporte à de petites variations dans les compositions chimiques utilisée dans la ligne du process.

4 Les points lithographiques, causés par des poussières dans les régions transparentes ou les rayures dans les régions opaques.

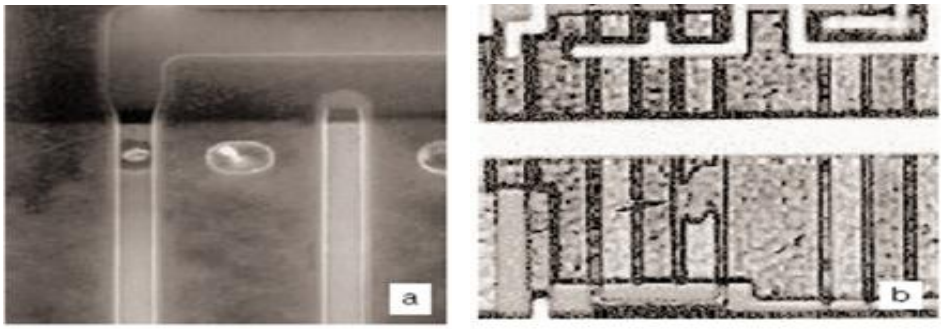
- Les contacts et les via résistifs
- Deux fils métalliques séparés pouvant être court-circuités;
- Les défauts d'oxyde de grille et les défauts dans les couches d'interconnexions.

1.6.2 Classes de fautes

Selon la surface atteinte par le mécanisme de défaillance, on distingue deux classes de défauts [Alb04, Eng00, Hue93, Mil98, Sun99] : les défauts globaux et les défauts locaux. Ces derniers peuvent causer des fautes structurelles et paramétriques. Parmi les fautes structurelles on trouve les fautes catastrophiques et les fautes paramètriques. Les fautes catastrophiques engendrent la déviation de toutes les spécifications et font que le circuit ne fonctionne pas. L'ensemble des fautes catastrophiques inclut les circuit-ouverts, les court-circuits. Par contre, les fautes paramétriques causent seulement la déviation des paramètres en dehors des spécifications sans changer la topologie du circuit.

1.6.2.1 Défaut de court-circuit

Les défauts de courts-circuits comprennent tous les défauts et les mécanismes de défaillance qui provoquent des connexions électriques non souhaitées entre deux ou plusieurs nœuds du circuit. Les travaux de Hawkins et al [Haw94] ont démontré que les courts-circuits ont des propriétés I-V non linéaires ou linéaires (résistives) avec une résistance de près de zéro à > 1 Mohm. Les défauts de court-circuit non linéaires comprennent les courts circuits de l'oxyde de grille (fig 1.6. a) et les courts circuits entre poly-silicium et oxyde de grille (fig. 1.6. b). Les courts circuits résistifs se produisent dans les motifs défectueux des circuits intégrés qui laissent des ponts de métal ou de poly-silicium (fig 1.6 b), dans une contamination ionique mobile, qui peut être concentrée dans une région particulière du circuit quand il est déformé, et dans certaines formes de court-circuit de l'oxyde de grille.



a. Court-circuit d'oxyde de grille causant 360µA d'Iddq additionné

b. Court-circuit entre poly-silicium et oxyde de grille causant 5mA d'Iddq additionné

Figure 1.6 Exemples de défauts de court-circuit causant une surconsommation d'I_{DDQ} [Fer98]

La résistance du défaut de court-circuit est le facteur prédominant dans les techniques de détection. Il existe une fonctionnalité booléenne correcte pour le signal du nœud affecté par un défaut de court-circuit lorsque le défaut dépasse une résistance critique. Cette résistance peut se situer dans une gamme allant de 10 Ohms à environ 5 KOhms [Haw94]. Il existe plusieurs classes de défauts de court-circuit : court-circuit entre les nœuds du transistor (grille, drain et source), court-circuit à l'intérieur d'une porte logique et court-circuit entre deux portes logiques. La figure 1.7 représente un exemple de court-circuit entre deux portes logiques. Les méthodes de test en tension et en courant sont utilisées pour la détection du défaut de court-circuit résistif.

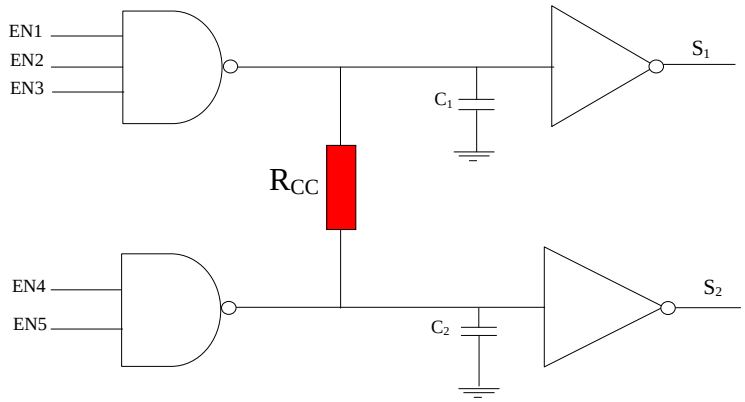
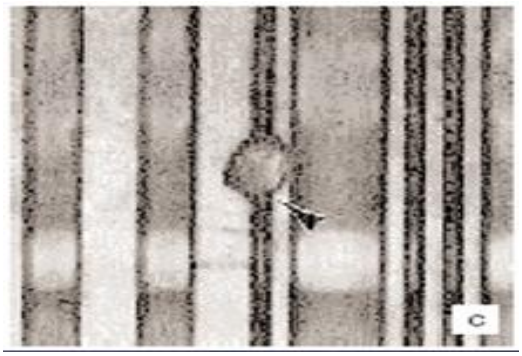


Figure 1. 7 Circuit logique affecté par un court-circuit résistif.

1.6.2.2 Défaut de circuit-ouvert

Les défauts de circuits ouverts sont des discontinuités électriques involontaires. Ils provoquent des comportements qui peuvent être difficiles à prévoir. Ces défauts comprennent des fils minces, des contacts mal formés (via), des fissures dans les siliciures, des contacts absents souvent causés par une gravure incorrecte, des trous d'oxyde, des vides dans les lignes métalliques (Figure1.8) ou le poly-silicium résultant des spots lithographiques.



Circuit- ouvert du métal causant 5 µA d'Iddq additionné.

Figure 1.8 Exemple de circuit-ouvert causant une surconsommation d'I_{DDQ}.

Les propriétés du défaut de circuit-ouvert dépendent principalement de la taille du défaut, de l'emplacement du défaut, de la structure locale électrique et de la variabilité du processus de fabrication. La figure 1.9 montre l'effet de l'emplacement du défaut lorsque le circuit-ouvert est dans la grille d'un seul transistor. Champa et al [Cha94] ont analysé ce défaut avec une puce de test. Un circuit-ouvert dans un seul transistor permet une forte capacité de couplage entre le drain, la grille et la source. Il est à noter que le circuit-ouvert sur un seul transistor de la figure 1.9 induit une augmentation du courant I_{DDQ} et est à 100 % détectable par la méthode de test I_{DDQ}. Le test en courant I_{DDQ} est basé sur la mesure du courant d'alimentation du circuit. Cependant, le circuit-ouvert sur le drain et le circuit-ouvert sur la source ont une probabilité de détection plutôt faible en utilisant des tests I_{DDQ}.

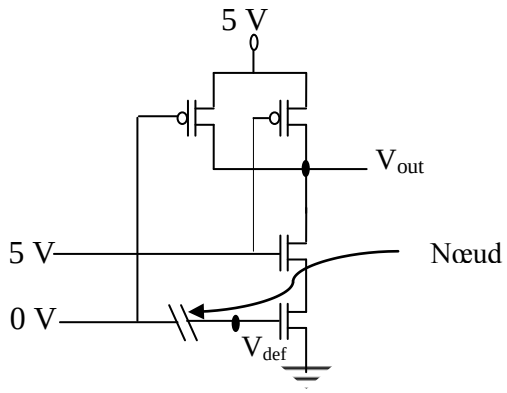


Figure 1.9 Circuit-ouvert sur la grille d'un transistor.

I.6.2.3 Défaut de retard paramétrique

Cette classe de défaut définit des défauts de retard qui ne sont généralement ni dans la catégorie des courts-circuits ni dans celle des circuits ouverts, bien que de nombreux défauts de circuit-ouvert ou de court-circuit entrainent des retards. Les défauts entrainent des retards dans les circuits intégrés CMOS de deux façons : l'affaiblissement des niveaux logiques, la modification des paramètres des chemins de transmission de signaux.

I.7 Simulation de fautes

La simulation de fautes est utilisée afin de déterminer la qualité d'une séquence de test T et d'évaluer une technique de test. Cette qualité s'exprime sous la forme d'un taux de couverture de fautes. Les modèles de fautes représentent les impacts des défauts réels sur le comportement du circuit. La simulation se fait avec des simulateurs de circuits analogiques de type SPICE, SPECTRE, etc. Elle comprend une phase de simulation du circuit sans fautes, une phase d'injection de fautes dans le circuit, une phase de simulation du circuit avec des fautes et enfin une phase de comparaison des résultats des deux simulations. .Un simulateur se caractérise par son efficacité, son temps d'exécution, et par la mémoire utilisée.

1.8 Modèles de fautes

Les modèles de fautes sont des circuits qui représentent le comportement électrique d'un défaut réel durant une simulation. Pour développer une stratégie de test efficace en termes d'outils de simulation de fautes, de génération de vecteurs de test, ou de diagnostic, des modèles de fautes représentatifs des défauts réels sont nécessaires. L'obtention d'un taux de couverture de 100 %, se fait en fonction de la représentativité du modèle de fautes utilisé. Plus le modèle de fautes est représentatif de la majorité des défauts physiques, plus il y aura de défauts détectés. De manière générale, les modèles de fautes des circuits numériques supposent que si la faute existe alors elle est unique (faute simple). Les fautes catastrophiques peuvent facilement être détectées par un simple test statique ou un test en courant I_{DDQ} [Har95]. Par contre, les fautes paramétriques produisent des déviations des paramètres de sortie du circuit et ces déviations peuvent être plus au moins grandes selon le paramètre du circuit considéré. En effet, il ne suffit pas de trouver les largeurs des pulsations des vecteurs de test qui activent la faute, il faut aussi trouver les meilleurs paramètres, comme par exemple les paramètres technologiques des transistors utilisés (w_i^n, L_i^n ,w_i^p, L_i^p), qui permettent d'avoir une déviation en sortie du circuit en dehors de l'intervalle de tolérance acceptable.

1.9 Modèle de fautes catastrophiques

La définition des fautes catastrophiques diffère d'un auteur à un autre. Pour certain auteurs, les fautes catastrophiques sont des fautes qui correspondent à des défauts de fabrication ponctuels et aléatoires (spot defect), celles qui résultent d'une particule de poussière sur un masque photo-lithographique entraînant des déformations locales comme les courts-circuits et les circuits-ouverts. En revanche, pour d'autres auteurs les fautes catastrophiques sont des fautes qui engendrent un fonctionnement du circuit complètement différent du fonctionnement normal, même si l'origine de la faute n'est qu'une variation d'un paramètre du circuit. Dans le cadre de ce travail, nous avons adopté la première définition, et nous nous sommes essentiellement intéressés aux modèles de fautes catastrophiques les plus utilisés : le court-circuit résistif et le circuit ouvert.

1.9.1 Modèle de court-circuit résistif

Montanes et al [Mon92] ont constaté que la plupart des courts circuits représentent une résistance significative entre les nœuds défectueux. Le modèle de défaut de court-circuit résistif insère une résistance entre les nœuds défaillants pour modéliser le court-circuit de façon plus réaliste. Lorsque la résistance augmente, l'impact du défaut est plus faible. Ainsi, des tensions intermédiaires sont au niveau des deux lignes défectueuses comme le montre la figure 1.10. V1 et V0 auront la même valeur dans le cas des courts circuits présentant une résistance nulle. Lorsque la résistance du court-circuit augmente à l'infini, aucune valeur défectueuse n'est générée. L'ensemble des modèles de courts-circuits étudié nécessite aussi

d'avoir des valeurs logiques qui soient opposées entre les deux lignes court-circuitées. Ainsi, les tests appliqués se basant sur les modèles de défauts traditionnels (un ET logique, un OU logique) ne peuvent pas garantir la détection des défauts de court-circuit résistif. Pour cette raison, Yamazaki [Yam96], Sar-Dessai et Walker [Sar98, Sar99] ont développé de nouvelles stratégies pour la détection de défaut de court-circuit résistif. Le test I_{DDQ} que nous avons cité précédemment est une option pour détecter le défaut de court-circuit résistif. En présence de défaut de court-circuit, I_{DDQ} causé par ce défaut varie en fonction de la résistance du court-circuit et dépend du nombre de transistors inclus dans le chemin V_{dd} à V_{ss}. Il est à noter que si la limite de courant utilisé pour distinguer entre un I_{DDQ} défectueux et un I_{DDQ} sans défaut est trop élevée, certains défauts peuvent ne pas être détectés. Par contre, si la limite de courant est basse, un circuit sans défaut sera incorrectement identifié comme étant défectueux. Par conséquent, un réglage précis de la limite actuelle est crucial pour rendre le test I_{DDQ} plus performant. Yamazaki et Miura [Yam99] ont étudié la testabilité du courant I_{DDQ} pour les défauts de court-circuit dans une variété de bascules. Ils ont utilisé une limite de courant statique qui est dérivée des valeurs de résistance de court-circuit, des facteurs de gain pour les transistors MOS, de la tension d'alimentation, des tensions de seuil et de la tension de grille-source. Il est clair que la limite actuelle dépend des valeurs de résistance des courts-circuits. Cependant, la résistance de court-circuit est un paramètre inconnu qui varie en fonction de la technologie, de la matière et de la gravité des défauts. Par conséquent, la limite de courant est un paramètre dynamique. L'analyse expérimentale peut aider à définir plus précisément la limite du courant. Le défaut de court-circuit résistif peut également conduire aux fautes de délais. En effet, Metra et al [Met93] ont identifié certains défauts produisant de petits retards de transition qui ne peuvent pas être détectés par un test logique ou un test I_{DDQ}.

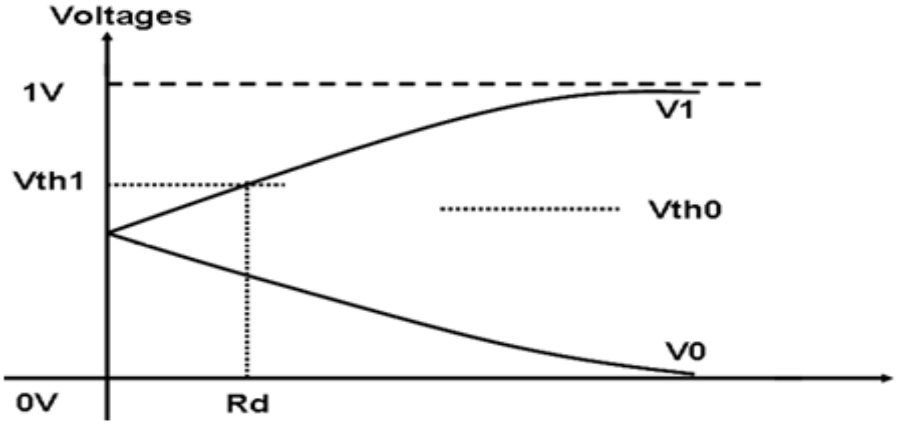


Figure 1.10 Comportement de défaut court-circuit résistif.

1.9.2 Modèle de circuit-ouvert résistif

Un défaut de circuit-ouvert se définit comme étant une imparfaite connexion de circuit qui peut être modélisé comme une résistance entre deux nœuds de circuit qui doivent être connectés [Jam01]. Le modèle de circuit-ouvert permet de détecter des défauts physiques qui ne sont pas détectés par le modèle des collages et de tester les fautes par des séquences de test du modèle des collages. Des recherches ont classé le circuit-ouvert en forte ouverture (> 10 MΩ) et en faible ouverture (≤10MΩ) [Rod02]. Les fortes ouvertures causent les fautes de collage (stuck-at) qui peuvent être détectées par le modèle de collage. Les faibles ouvertures engendrent les fautes de délais. Ces fautes ne peuvent pas être détectées par les modèles traditionnels de collage [Haw94] [Moo00]. Rodriguez-Montanes et Gyvez [Mon02] ont montré que dans la technologie moderne submicronique, le pourcentage des ouvertures faibles est largement élevé. La figure 1.11 montre une ligne défectueuse qui peut être modélisée par un circuit-ouvert résistif (R_{CO}). Le comportement du circuit dépend de la valeur de la résistance du défaut de circuit ouvert.

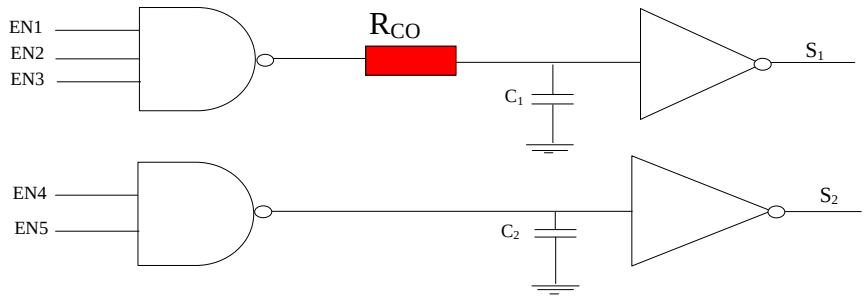


Figure 1. 11 Modèle de défauts de circuit-ouvert résistif.

Au fur et à mesure que la résistance diminue, le circuit défectueux aura le même comportement que celui d'un circuit sans défaut et la déconnexion n'est qu'une faible ouverture. Lorsque la résistance du circuit-ouvert augmente à l'infini, l'impact électrique du défaut est plus significatif et la déconnexion est complètement ouverte. Là aussi il existe une certaine valeur de la résistance, appelée valeur critique $R_{C,}$ à partir de laquelle une valeur logique défectueuse est produite et le comportement du circuit devient fautif. Le test de ce type de défaut se base sur la détermination d'un plus large intervalle de résistances pour lequel le circuit-ouvert est détecté et n'est pas toléré par le circuit. Cet intervalle de résistance pour lequel la valeur logique en sortie du circuit est fautive correspondant à l'intervalle [R_C, ∞ [, est appelé l'intervalle de détection DI et l'intervalle de résistance [0, R_C [est appelé l'intervalle de tolérance de circuit ouvert.

Le test en retard peut être utilisé pour détecter des défauts de circuits- ouverts résistifs qui créent des pannes temporelles à l'origine du mauvais fonctionnement d'un circuit à des

fréquences élevées. Les travaux de li et al [Li03] ont montré que le délai augmente presque linéairement avec la résistance de circuit ouvert. Le test en retard se fait en utilisant l'un des nombreux modèles de fautes de délai. Ces derniers ont été utilisés pour la première fois par Breuer [Bre74] afin de modéliser l'effet des défauts résistifs (court-circuit ou circuit-ouvert).

1.9.3 Modèle de fautes de délai

Dans le cas des fautes de délai, le défaut physique se traduit par un rallongement du temps de réponse du circuit [Bre74]. En effet, la réduction des dimensions des transistors induit celle de la section des interconnexions métalliques qui les lient entre eux ou à leur environnement. Ces interconnexions, séparées les unes des autres par des isolants, sont également de plus en plus proches à mesure que la largeur des transistors diminue. Le passage d'un nœud technologique à un nœud plus petit s'accompagne donc d'une augmentation de la résistance Ri des interconnexions et de leurs capacités parasites C_i, d'où un accroissement du délai RiCi de transmission de l'information entre les portes logiques au sein d'un circuit intégré, ou vers l'extérieur du circuit. Si R_i C_i devient plus grand que le temps de commutation d'une porte, les interconnexions vont conduire à limitation du transfert des données.

Les modèles traditionnels de défaut de court-circuit comprennent des modèles de fautes fonctionnelles ou des modèles de fautes de délai. Un modèle de défaut de court-circuit résistif incorporant à la fois la fonctionnalité et le retard est présenté par Li et al. [Li03a].

Les modèles les plus utilisés pour les fautes de délai sont les modèles des fautes de transition et les modèles des fautes de délai sur les chemins.

1.9.3.1 Modèle des fautes de transition

La faute de transition se traduit par un temps de transition qui est plus lent que les spécifications. Elle se produit lorsqu'une particule ionisante frappe un nœud sensible d'une cellule mémoire et entraine le basculement de la valeur logique mémorisée. Il existe deux temps de transitions, le temps de montée et le temps de descente. Pour chaque signal de sortie on distingue deux fautes: temps de montée plus lent « Slow-to-rise » et temps de descente plus lent « Slow-to-fall ».

Dans le circuit sain, chaque porte a un peu de retard nominal. Les fautes de délai se traduisent par une augmentation ou une diminution de ce retard. Selon le modèle de fautes de transition, le retard supplémentaire causé par le défaut est supposé être important pour empêcher la transition d'atteindre toute sortie primaire au moment de l'observation. En d'autres termes, la faute de délai peut être observée indépendamment si la transition se propage à travers un long ou un court chemin vers toute sortie primaire d'une porte (fig 1.12). Les défauts de retard de petite taille ne peuvent pas être détectés le long du chemin court. Ce modèle est aussi appelé modèle de faute de retard brut [Par87]. L'ensemble des modèles de courts-circuits étudiés nécessite aussi d'avoir des valeurs logiques qui soient opposées entre

les deux lignes court-circuitées. Pour détecter une faute transitoire dans un circuit combinatoire, il est nécessaire d'appliquer deux vecteurs d'entrée. Le premier vecteur initialise le circuit, tandis que le deuxième vecteur active le défaut et propage son effet à une certaine sortie primaire. Une faute de transition est considérée détectée si la transition se produit sur l'endroit du défaut et un chemin sensibilisé se produit à partir de l'endroit du défaut à une certaine sortie primaire.

Ce modèle présente cependant l'inconvénient de ne couvrir qu'une insignifiante partie des retards de petite taille. Ce point a notamment été souligné par Geilert [Gei90]. Dans les travaux de Tendolkar [Ten85], il a été montré que les fautes de retard couramment observées dans les circuits actuels sont d'une taille faible. Ceci permet de dire que le modèle de défaut de transition n'est pas toujours considéré comme réaliste.

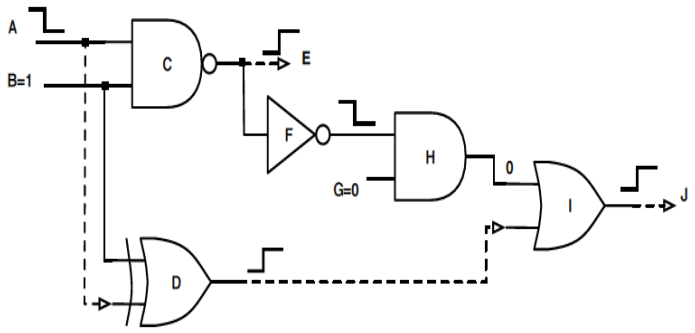


Figure 1.12 Faute de retard de transition. A-C-E: chemin court et A-D-I-J: chemin long [Ger09]

1.9.3.2 Modèle de fautes de retard de porte

La plupart des travaux [Krs98, Pra88, Hay83] sont fondés sur une approche à une faute de retard localisée sur une porte dans le circuit. Dans le modèle de faute de retard de porte, le retard de propagation à travers la porte défectueuse est plus long que prévu. Cette défaillance est modélisée par une faute de type Lent à monter ou de type Lent à descendre suivant le type de commutation sur les entrées ou les sorties d'une porte du circuit. Une faute de retard de type temps de montée plus lent ou temps de descente plus lent affectant une porte logique caractérise un retard de propagation d'une transition montante ou descendante supérieure à la valeur spécifique. La principale limitation de ce modèle de retard de porte est que tous les chemins sensibles entre l'endroit défectueux et une sortie primaire n'entrainent pas forcement une détection de l'erreur. En effet, même si une seule porte est lente, les performances du réseau peuvent ne pas être atteintes si la porte ne se trouve pas sur le chemin critique, à savoir le plus long chemin de l'entrée principale à la sortie principale du réseau. Il faut ainsi prendre en compte le retard de propagation de chaque chemin afin de choisir un chemin sensible qui peut entraîner la détection de la faute de retard.

1.9.3.3 Modèle de fautes de délai de chemin

Dans ce type de modèle, le défaut est dans un chemin qui contient unes série de portes. Un chemin d'accès est défectueux, si le retard de propagation à travers ce chemin est plus long que prévu [Krs98, Smi85, Lin87]. Comme dans le cas du modèle de stuck-on/open qui suppose que l'un des transistors de la porte logique se trouve dans un état permanant passant (stuck-on) ou ouvert (stuck-open), une paire de vecteurs de test est nécessaire pour détecter les défauts de retard. Pour tester un défaut de retard, nous avons besoin de lancer une transition au niveau des entrées qui va exciter la faute de collage, et de trouver un chemin de propagation entre l'endroit défectueux et une sortie primaire du circuit, et enfin de mesurer le temps de propagation de cette transition à la sortie. Le modèle de faute de retard de chemin est considéré le plus proche du modèle idéal pour les fautes de retard dans la mesure où il couvre la totalité des pannes du circuit mais ne peut être considéré comme efficace qu'à partir du moment où tous les chemins ont été testés. Le nombre de chemins dans le circuit peut être très grand (éventuellement exponentiel au nombre de portes). Pour cette raison, le test de toutes les fautes de retard de chemin n'est pas pratique. Il y a cependant un moyen simple permettant d'utiliser ce modèle. La sélection de l'ensemble des fautes de retard de chemin à tester se basant sur les analyses temporelles exhaustives du circuit est issue des travaux d'Hitchcock et al [Hit82] et Al-Hussein [Alh85]. Li [Li89] a proposé un algorithme qui permet de générer efficacement une séquence de test à partir du modèle de faute de délai de chemin. Le principe de cet algorithme est de sélectionner un nombre minimum de chemins, compris entre une entrée primaire et une sortie primaire du circuit sous test.

1.10 Injection de fautes

L'injection d'une faute est la technique qui permet d'ajouter au circuit sous test, pendant l'étape de simulation, un circuit (appelé faute) représentant le modèle de la faute dans le but de simuler un défaut réel. Il existe deux approches permettant d'injecter des fautes. La première approche se fait en modifiant le fichier netlist du circuit sous test. La deuxième approche [Ebe99, Rom03] consiste à modifier directement le schéma électrique du circuit à tester avant de générer la netlist, ce qui permet une diminution de la complexité de la procédure d'injection et par conséquent du temps de calcul. Nous allons nous intéresser à cette deuxième approche afin de faciliter l'injection de fautes résistives sous Spice de Cadence. Par exemple, un court-circuit résistif se modélise par une résistance variable d'une valeur très petite, et un circuit ouvert-ouvert résistif se modélise par une résistance variable d'une valeur très grande. En ce qui concerne, la manière dont ces modèles seront injectés, le court-circuit résistif s'injecte en parallèle entre deux connections d'un circuit. Par contre le circuit-ouvert résistif s'injecte en série à la sortie de l'un des segments d'une connexion d'un circuit.

1.11 Analyse de fiabilité, méthodes d'évaluation et prédiction de la fiabilité

L'analyse de fiabilité est utilisée pour étudier les incertitudes et la qualité d'un circuit électronique, en se basant sur le retour d'expérience, l'expertise et les modèles prévisionnels. Dans un contexte de mondialisation et de compétition industrielle toujours plus difficile, la maîtrise des coûts de développement, des délais de mise sur le marché et des performances du circuit le long du cycle de vie est une des clés du succès commercial de tout projet de lancement de nouveaux systèmes, d'où un besoin crucial de méthodes et outils d'évaluation des performances comportementales au plus tôt dans la phase de conception [Cou08, Ber04].

1.12 Méthodologies conceptuelles pour améliorer la fiabilité

Plusieurs méthodes ont été proposées dans la littérature [Ber04, Sie92] pour l'amélioration des performances comportementales des circuits intégrés.

Le développement d'un circuit fiable passe par l'utilisation d'un ensemble de méthodologies conceptuelles et structurelles qui peuvent être classées ainsi :

- Prévention de fautes : comment empêcher l'occurrence ou l'introduction de défauts lors de la fabrication du circuit;
- Tolérance aux fautes : comment assurer, par redondance, la continuité du service conduisant à la fiabilité du circuit en dépit de défauts ;
- Élimination de fautes : comment réduire la présence (nombre, sévérité) des défauts ;
- Prévision de fautes : comment estimer la présence, le taux futur et les possibles conséquences des défauts.

1.13 Choix d'une structure tolérante aux fautes

Les méthodes de tolérance aux fautes sont classées, selon leur type de redondance, en cinq familles [Kor07]: la redondance matérielle [Cho85], la redondance d'information [Amo88, Ple86, Mak86, Dum07, Maz95], la redondance temporelle [Lah83, Cho85], la redondance logicielle [Arl79, Bri93, Che78, Chr03, Lap90, Ran75] et la redondance mixte.

La structure la plus connue à avoir les qualités requises pour la correction de défauts permanents apparus dès le processus de fabrication et survenant même pendant le fonctionnement du circuit, est la structure NMR « N-Modular Redundancy».

Nous avons alors choisi de nous focaliser sur un type de structure NMR : la TMR «Triple Modular Redundancy».

1.13.1 La structure TMR

Une structure TMR ou 3MR telle que représentée à la figure 1.13, est la conception la plus simple et la plus utilisée, c'est un système composé de trois circuits « modules » identiques fonctionnant en parallèle et assurant une même fonction, et d'un voteur majoritaire [Kor07,

Lyo62] qui permet de détecter et corriger leurs erreurs éventuelles. Le voteur choisit les sorties des modules sains ce qui masque les modules défectueux.

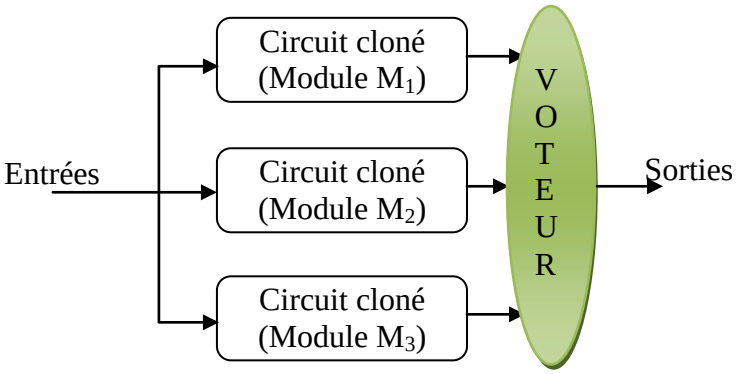


Figure 1.13 Structure d'un système TMR [Lyo62]

Le voteur est une structure combinatoire dont le nombre est égal au nombre de sorties des modules [Haf90]. Considérons par exemple la structure TMR de la figure 1.14, où les modules ont trois sorties. $S_{1,1}$, $S_{1,2}$, $S_{1,3}$ pour le premier module, $S_{2,1}$, $S_{2,2}$, $S_{2,3}$ pour le deuxième module et $S_{3,1}$, $S_{3,2}$, $S_{3,3}$ pour le troisième module. Les sorties $S_{x,1}$ sont votées ensemble ainsi que les sorties $S_{x,2}$ et $S_{x,3}$. La fonction réalisée par chacun des voteurs i est la suivante :

$$S_i = S_{1,i}.S_{2,i} + S_{1,i}.S_{3,i} + S_{2,i}.S_{3,i}$$

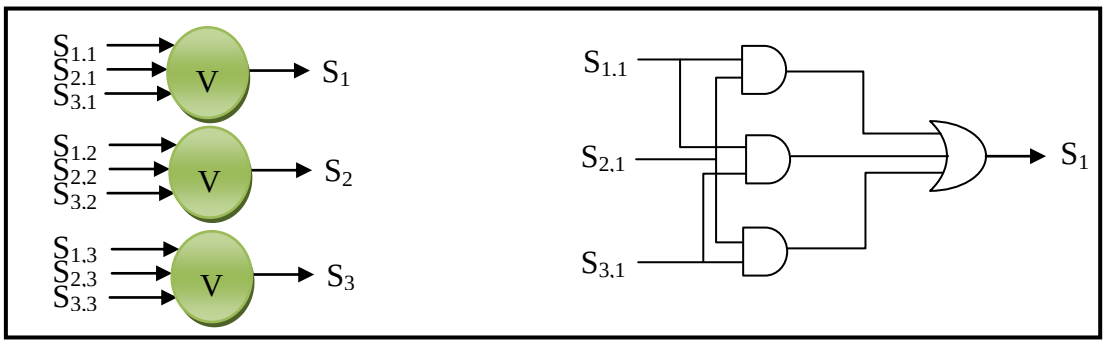


Figure 1.14 Voteur bit par bit [Lyo62]

Si un seul module est fautif, alors les deux autres seront dominants et la faute sera masquée. Si un module supplémentaire est fautif alors le résultat peut être erroné. Quant au voteur, la moindre faute présente est susceptible de fausser les sorties. Ceci dit, on verra par la

suite, que dans certains cas, la structure TMR peut fonctionner correctement même avec deux modules défaillants [Haf90].

Pour estimer la fiabilité de la structure NMR il faut prendre en compte deux cas, qui sont :

- **1er Cas :** Le voteur est sain. les défauts sont indépendants et n'affectent que les modules. La fiabilité de la structure NMR s'écrit [Sie92, Lyo62, Haf90, Ham05]:

$$R_{NMR}(t) = \sum_{i=M}^{N}\left(C_N^i \times R(t)^i[1-R(t)]^{N-i}\right) \quad \ldots\ldots (1)$$

Avec R(t) la fiabilité d'un module à l'instant t
$R_{NMR}(t)$, la fiabilité du circuit NMR à l'instant t
M, le nombre majoritaire de modules tel que :
M= (N+2)/2 si N est pair et ;M= (N+1)/2 si N est impair.

- **2ème Cas :** Le voteur peut être défectueux et les défauts sont corrélés, la fiabilité chute

Démonstration : La fiabilité R_{TMR} d'une structure TMR s'écrit :

$$\begin{aligned} R_{TMR}(t) &= R_{voteur} \times \sum_{i=2}^{3}\left(C_3^i \times R(t)^i[1-R(t)]^{3-i}\right) \\ &= R_{voteur} \times (3R(t)^2[1-R(t)] + R(t)^3) \\ &= R_{voteur} \times (3R(t)^2 - 2R(t)^3) \quad \ldots\ldots (2) \end{aligned}$$

.

Si on note R_v la fiabilité du voteur et R_m la fiabilité d'un module

$R_{TMR} > R_m$ revient à $3R_m^2 - 2R_m^3 > R_m / R_v$ ou $3R_m - 2R_m^2 - 1/R_v > 0$

Que l'on peut écrire $R_m^2 - 3/2\ R_m + 1/2\ R_v < 0$

ou $(R_m - 3/4)^2 < (9R_v - 8)/16R_v$

Pour avoir des solutions, le terme $(9R_v - 8)/16R_v$ doit être strictement supérieur à zéro.

Soit $9R_v - 8 > 0$ (car $16R_v > 0$)

Ce qui donne une valeur minimale pour $R_v \simeq 0{,}89$

La valeur minimale de $(R_m - 3/4)^2$ est zéro, ce qui correspond à $R_m = 3/4 = 0{,}75$

Ainsi, la structure TMR améliore la fiabilité, si et seulement si, la fiabilité minimale du voteur est égale à 0,89 et celle du module est égale à 0.75.

1.13.2 Tolérance aux défauts de fabrication

Lorsque les défauts sont corrélés, ils se manifestent par une erreur au même moment et engendrent la diminution de la fiabilité du circuit. Pour savoir quand et comment ces circuits sont aptes à tolérer les défauts de fabrication, on doit distinguer deux cas [Lau09] :

- Les défauts sont présents dans les modules de la structure TMR « partie redondante »;
- Les défauts sont présents dans le voteur « partie non redondante ».

1.13.2.1 Les défauts affectant les modules

Pour étudier la tolérance aux défauts de fabrication affectant les modules d'une structure TMR, nous distinguons plusieurs cas donnés par [Fan06, Lau09]:

1. Cas où un ou plusieurs défauts affectent un seul module ;
2. Cas où deux défauts affectent deux modules différents ;
3. Cas où plus de deux défauts affectent plusieurs modules différents.

- **1er Cas : un ou plusieurs défauts affectent un seul module**

Lorsqu'un ou plusieurs défauts de fabrication affectent un seul et même module (fig 1.15), alors ce défaut est toléré par la structure TMR. Il reste deux autres modules « sains », qui seront forcément majoritaires lors du vote.

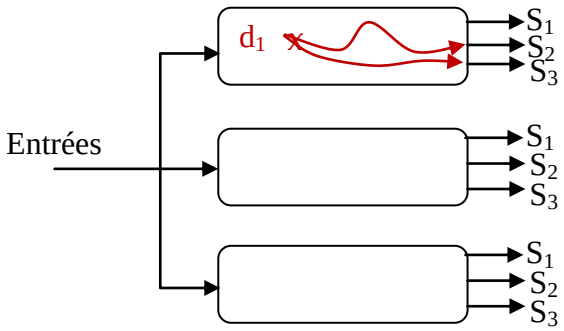


Figure 1.15 Présence d'un défaut de fabrication [Fan06, Haf90, Lau09]

- **2ème Cas : deux défauts affectent deux modules différents**

Si deux défauts de fabrication (d_1, d_2) sont présents dans deux modules différents (fig 1.16) alors ils peuvent être tolérés ou pas selon leurs effets, c'est-à-dire :

- Ils sont tolérés si aucun vecteur de test d'entrée ne peut propager deux erreurs jusqu'à deux sorties de modules communes (fig 1.16.a).
- Ils sont non tolérés, si deux erreurs sont propagées jusqu'à deux sorties de modules communes (fig 1.16.b).

Cependant, selon la nature du défaut, si les deux défauts propagent chacun une valeur logique complémentaire alors leurs effets s'annulent [Haf90], dans ce cas là, ce sont les

sorties non erronées du troisième module qui seront choisies. Ainsi, pour que deux défauts ne soient pas tolérés, il faut aussi que leurs effets ne se compensent pas.

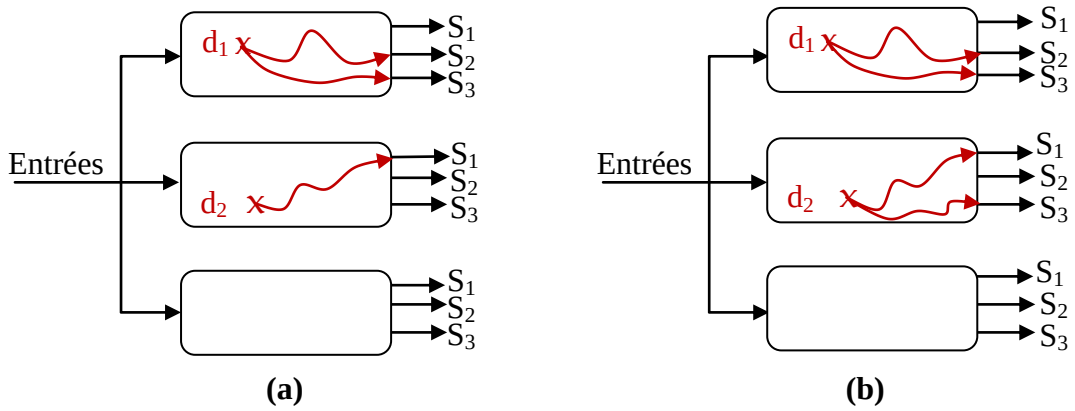


Figure 1.16 Deux défauts de fabrication sont (a) tolérés(b) non tolérés [Fan06, Lau09]

- **3ème Cas : plus de deux défauts affectent plusieurs modules**

Dans ce cas, nous pouvons regrouper les défauts en paires de défauts. Par exemple quatre défauts (d_1, d_2, d_3, d_4) peuvent être regroupés en six paires de défaut {(d_1, d_2), (d_1, d_3), (d_1, d_4), (d_2, d_3), (d_2, d_4) et (d_3, d_4)}.Ainsi, n défauts de fabrication peuvent être regroupés en C_n^2 paires de défauts et sont tolérés par la structure TMR si toutes les paires de défauts sont masquées par le voteur.

1.13.2.2 Défauts affectant le voteur

Le voteur ne contient pas de redondance. Il est donc susceptible de propager une erreur pour chacun des défauts de fabrication l'affectant. Le voteur est le point faible de la structure TMR puisque c'est la seule partie à ne pas être tolérante aux défauts de fabrication. Pour réduire son manque de fiabilité, plusieurs voteurs redondants peuvent être utilisés. Il peut également être réalisé avec une technologie plus robuste (par exemple, des règles de dessin plus larges) [Caz04] ou bien de manière logicielle lorsque cela est possible.

1.14 Conclusion

Ce chapitre a tout d'abord permis de rappeler quelques notions fondamentales de fiabilité, essentiellement fondées sur les techniques de test et sur la tolérance aux fautes, dans le contexte de la détection des défauts de fabrication de circuits intégrés. Pour cela nous avons étudié la modélisation des différents types de défauts existants, l'injection et la simulation de fautes. Ensuite, les différentes techniques de test ainsi que les métriques permettant d'évaluer ces tests seront introduits. Enfin, nous avons étudié les stratégies conceptuelles mises en œuvre pour améliorer la fiabilité et le rendement de fabrication des circuits intégrés. L'utilisation de la structure tolérante aux fautes via la redondance triple « TMR » semble être la plus avantageuse pour garantir un fonctionnement correct tout en préservant les avantages des avancées technologiques.

Par ailleurs, en ce qui concerne ces défauts, une étude bibliographique a montré qu'il était raisonnable de considérer que les défauts couramment observés dans les circuits actuels sont les courts circuits et les circuits ouverts. Au cours des prochains chapitres, nous nous intéresserons t aux défauts paramétriques (courts circuits résistifs et circuits ouverts résistifs).

Chapitre 2

Attaques et contremesures

2.1 Introduction

La conception d'un circuit intégré consiste à rechercher un modèle vérifiant un ensemble de spécifications. A titre d'exemple, on peut citer la consommation, le coût, la performance et la fonction. Un circuit cryptographique peut généralement se distinguer d'un circuit intégré classique selon ses spécifications qui doivent aussi intégrer des contraintes sécuritaires pour résister à une attaque particulière. Toute vulnérabilité non détectée très tôt dans la phase de conception entraîne un surcoût important en temps de développement et un retard de mise sur le marché. Par conséquent, ce coût induit à son tour une baisse importante du revenu de l'entreprise car 25% à 50% du chiffre d'affaire du marché de la sécurité est lié à l'introduction de nouveaux produits innovants et sécuritaires. Il est donc essentiel pour les concepteurs de circuits sécurisés de disposer d'un flot de conception permettant de valider aussi tôt que possible l'efficacité de leurs contremesures.

Ce chapitre a pour premier objectif de rappeler le principe des différentes attaques connues. Une attention particulière sera apportée aux attaques qui ne détruisent pas le composant, et en particulier les attaques par canaux cachés DPA qui se révèlent être les plus dangereuses car leur mise en œuvre nécessite peu de moyen pour être menées avec succès. Une analyse de leur efficacité sera proposée. Le second objectif est de présenter les principales contre-mesures à ces attaques. Nous détaillerons les contre-mesures spécifiquement destinées aux circuits logiques.

2.2 Attaques par canaux cachés

La technologie de l'information évolue rapidement. Des ordinateurs personnels, des téléviseurs et des téléphones mobiles sont utilisés quotidiennement par des millions de personnes dans le monde. L'intérêt pour la technologie des cartes à puces ne cesse de prendre de l'ampleur depuis 1990. Les cartes à puce présentent de nombreux avantages sécuritaires. Elles sont utilisées dans les domaines des services financiers (cartes de crédit), des télécommunications (cartes SIM, cartes prépayées), etc. Ceci est la raison de l'intérêt croissant pour de nouvelles méthodes d'attaques d'un côté et de nouvelles contremesures et de nouveaux algorithmes cryptographiques de l'autre côté.

Les algorithmes cryptographiques sont des blocs de construction de nombreux protocoles de sécurité et peuvent être mis en œuvre à la fois dans le logiciel et le matériel. Les solutions logicielles sont moins coûteuses et plus souples, tandis que les implémentations matérielles offrent une vitesse plus élevée et une sécurité intrinsèque. Un compromis dans le coût et la vitesse peut être obtenue par la co-conception matérielle et logicielle.

Les attaques sur les algorithmes cryptographiques sont divisées en attaques mathématiques et attaques d'implémentations. Ces dernières sont basées sur la faiblesse dans l'implémentation et peuvent être passives ou actives.

Les attaques passives ou non invasives n'endommagent pas le circuit et elles sont souvent aussi appelées attaques par canaux cachés. Les trois types les plus importants d'attaques par canaux cachés sont les attaques par analyse du temps de calcul [Koc96], les attaques d'analyse de puissance [Koc99], et les attaques électromagnétiques [Gan01, Qui01]. L'objectif de ces attaques est de déterminer la clé secrète d'un dispositif cryptographique par la mesure de son temps d'exécution, de sa consommation d'énergie, ou de son champ électromagnétique. La plupart des attaques non invasives peuvent être réalisées avec un équipement peu coûteux, et par conséquent, ces attaques constituent une menace sérieuse pour la sécurité des dispositifs cryptographiques.

Les attaques actives ou invasives sont réalisées sur le silicium du composant et peuvent donc endommager le circuit. Elles sont basées sur l'introduction de défauts, qui se traduisent par des calculs erronés conduisant à l'exposition de la clé secrète. L'injection de fautes repose sur des modifications anormales des paramètres externes du circuit tels que l'alimentation, l'horloge, la température, etc. Un attaquant pourrait également utiliser une sonde très fine avec des équipements tels que des sondes de la caméra ou d'un laser afin d'induire une faute.

Une attaque invasive commence généralement à extraire la puce de son support en plastique. Les différents composants du dispositif sont directement accessibles en utilisant une plateforme de sondage (figure 2.1). Cette partie d'une attaque invasive peut être passive si la plateforme de sondage est utilisée pour observer des signaux de données ou active si des signaux dans le dispositif sont changés pour modifier la fonctionnalité du dispositif.

En ce qui concerne les attaques, cette thèse se concentre exclusivement sur les attaques par injection de fautes, même si un aperçu général des autres types d'attaques est traité ci-après.

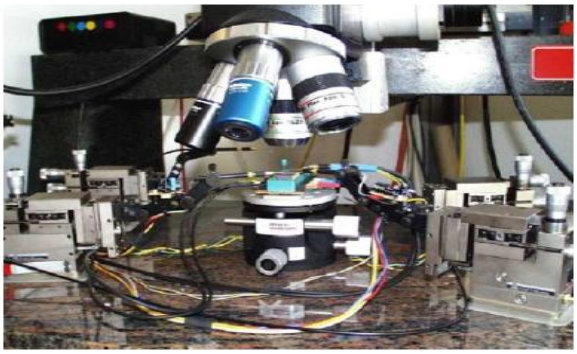


Figure 2.1 Attaque par sondage [Raz06]

2.2.1 Attaques par analyse du temps de calcul

Elles sont basées sur le fait que les algorithmes avec un temps d'exécution non constant peuvent permettre d'obtenir des informations secrètes. Un temps d'exécution non constant

peut être causé par des branchements conditionnels dans l'algorithme, et diverses techniques d'optimisation, etc. A la différence des attaques de puissance, les attaques par analyse du temps de calcul peuvent aussi être appliquées à un réseau de crypto-systèmes et à d'autres applications chaque fois que l'attaquant peut se procurer des informations de synchronisation.

La façon évidente de prévenir les attaques du temps de calcul est de mettre en œuvre des algorithmes cryptographiques avec un temps d'exécution constant. Presque toutes les implémentations modernes sont résistantes aux attaques de synchronisation, ce qui rend cette dernière impossible. Cependant, la menace reste en combinant des informations de synchronisation avec d'autres canaux cachés. Par exemple, des informations de synchronisation peuvent être utilisées par un attaquant afin de localiser des parties spécifiques de l'algorithme.

2.2.2 Attaques par analyse du courant de consommation

Aujourd'hui, la technologie CMOS est la plus couramment utilisée pour mettre en œuvre les circuits intégrés numériques. Le facteur dominant pour la consommation d'énergie d'une porte CMOS est la consommation d'énergie dynamique. Deux types de fuite de consommation d'énergie peuvent être observés. La fuite de comptage de transition donne des informations sur le nombre de bits modifiés, tandis que la fuite de poids de Hamming est liée au nombre de bits à 1 traités simultanément.

Deux types d'attaques d'analyse de puissance existent. Dans une attaque par analyse simple de la consommation SPA (Simple Power Analysis), un attaquant utilise les informations des canaux cachés pour déterminer la valeur d'une partie de la clé secrète. Dans l'attaque par analyse de puissance différentielle DPA (Differential Power Analysis), de nombreuses mesures sont utilisées pour filtrer le bruit. Alors que les attaques SPA exploitent la relation entre les opérations qui sont exécutées et la fuite de courant, les attaques DPA exploite la relation entre les données traitées et la fuite de courant. Dans DPA, un attaquant utilise d'abord un modèle du circuit attaqué en vue de prévoir plusieurs valeurs pour la sortie du canal caché d'un circuit, puis il compare ces valeurs à la sortie du canal caché mesuré du circuit. Pour chacune de ces attaques SPA et DPA, le modèle prédit la quantité de fuite du canal caché pendant un certain temps d'exécution.

Pour comprendre le fondement des attaques par analyse de consommation, il faut se référer aux caractéristiques de consommation de la technologie CMOS. Un circuit intégré conçu en technologie CMOS est composé de portes logiques qui elles mêmes sont composées de transistors agissant comme des interrupteurs. Les interconnexions entre les portes logiques, réalisées par des pistes parallèles au substrat, créent des condensateurs, couramment appelés de ligne, dont les valeurs sont proportionnelles à la longueur des interconnexions. Et chaque entrée d'une porte logique présente au fil qui lui est connecté un condensateur, dit d'entrée. La valeur de ce dernier est liée à la réalisation niveau transistor de la porte et au placement-

routage de celle-ci. La puissance absorbée du circuit est due aux condensateurs de ligne et d'entrée, et elle est définie par une puissance statique et une puissance dynamique [Ngu11]. La première est due au courant de fuite qui traverse les transistors qui composent la porte quand ils sont dans un état stable (I_{stat}). La seconde se produit lorsque ces transistors changent d'état provoquant un courant de court-circuit I_{cc} entre la masse et l'alimentation. Les condensateurs parasites qui sont connectés à la sortie de la porte sont chargés ou déchargés selon le sens de la commutation. Ils sont chargés par le courant (I_{cl}) en provenance de l'alimentation si la transition a lieu de l'état bas vers l'état haut. Par contre, ils se déchargent à travers la masse et donc aucun courant n'est absorbé si la transition a lieu de l'état haut vers l'état bas.

Nous allons nous placer dans le cas d'un circuit en pleine activité. La puissance absorbée est de la forme [Raz06] :

$$P = \alpha . C_L . V_{dd}^{2.} F \qquad (2.1)$$

où α correspond au taux d'activité de la porte, la constante C_L est la charge du condensateur,. F désigne la fréquence du circuit et le terme V_{dd} définit la tenson d'alimentation du circuit.

Le tableau 2.1 et la figure 2.2 illustrent les transitions et leur consommation associée pour un inverseur en technologie 45nm. Sur ce tableau, une transition vers un état haut consomme plus qu'une transition vers l'état bas, la différence entre les deux étant égale à la charge du condensateur parasite en sortie de l'inverseur.

Les résultats de simulation présentés sur la figure 2.2 montrent que les transitions [0-0] et [1-1] en sortie de l'inverseur ont une consommation nulle et ne génèrent aucun appel de courant sur les rails d'alimentation. Les transitions [0-1] et [1-0] induisent quant à elles la circulation de courants d'amplitudes plus ou moins importants. Cela confirme ce qui a été dit dans le tableau (2.1) sur les transitions [0-1] qui induisent des appels en courant nettement supérieur aux transitions [1-0]. Les attaques par analyse de consommation exploitent les variations instantanées du courant d'un circuit pour retrouver l'activité du circuit ou bien les données traitées. Ainsi, il est clairement établi que le fondement des attaques par analyse de consommation est la dépendance entre les données manipulées et les profils en courant.

Transition	Courant consommé
0 → 0	I_{stat}
0 → 1	$I_{cc} + I_{cl}$
1 → 0	I_{cc}
1 → 1	I_{stat}

Tableau 2.1 – Le courant consommé en fonction des transitions.

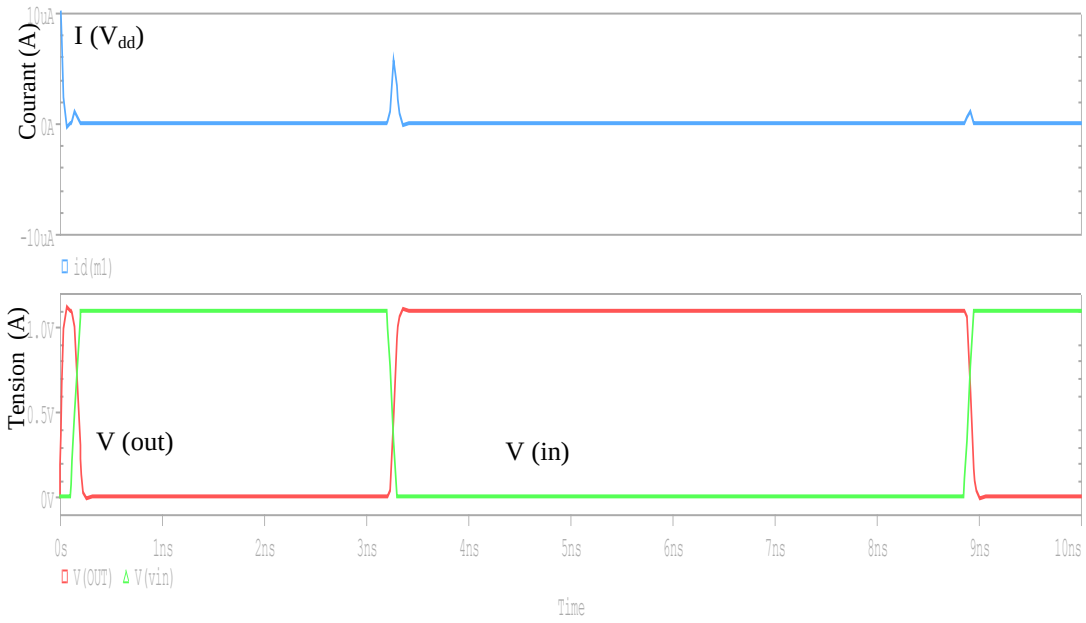


Figure 2.2 Simulation du courant consommé en fonction des transitions.

2.2.3 Attaques par analyse du champ électromagnétique

Ce type d'attaques exploite l'information contenue dans le champ électromagnétique qui est provoqué par les courants circulant dans chaque élément du dispositif cryptographique. Il existe deux types d'émission de champ électromagnétique : intentionnelle et non intentionnelle. Le premier type résulte du flux de courant continu. Le second type est causé par différents couplages, modulations (AM et FM), etc.

Ce type de fuites électromagnétiques est connu depuis les années 50. Les premiers travaux faits pour ce type d'attaques sont ceux de Quisquater [Qui01] et Gandol [Gan01]. Quisquater a montré qu'il est possible de mesurer le rayonnement électromagnétique à partir d'une carte à puce. Sa configuration de mesure comprend un capteur composé d'une bobine plate (figure

2.3), un analyseur de spectre ou un oscilloscope et une cage de Faraday. Les termes simple EMA (SEMA) et différentiel (DEMA) ont été également introduits dans [Qui01]. La faisabilité des attaques EMA et leur comparaison avec les attaques d'analyse de puissance (PA) ont été faits dans [Gan01]. A savoir, les émissions EM peuvent également exploiter les informations locales et les mesures peuvent être effectuées à distance. Ce fait permet d'élargir le spectre des cibles auxquelles les attaques par canaux cachés peuvent être appliquées.

Quisquater et Gandol ont traité uniquement les émissions intentionnelles. Par contre, les émissions non intentionnelles ont été explorées dans [Agr03], ce qui est un véritable avantage par rapport aux autres attaques par canaux cachés. Plus précisément, les fuites EM se composent de multiples canaux. Par conséquent, des informations compromettantes peuvent aussi être disponibles même pour les dispositifs résistants aux DPA pour lesquels aucune mesure de contact n'est disponible. A savoir, en plus d'explorer toutes les émissions EM disponibles, un attaquant peut également se concentrer sur une combinaison de deux ou plusieurs canaux cachés. Ces attaques par différents canaux cachés sont définies dans [Agr03a].

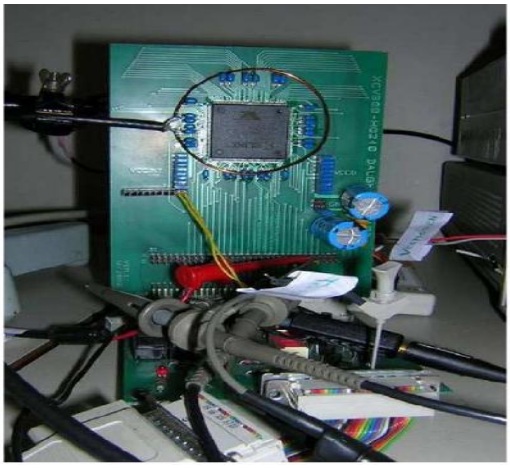


Figure 2.3 Exemple d'un banc d'analyse électromagnétique.

2.2.4 Attaques par injection de fautes

Les attaques par injection de fautes sont basées sur les fautes matérielles ; elles ont été introduites par Boneh et al [Bon97]. L'attaque est basée sur le fait que si un mauvais résultat est libéré l'attaquant peut utiliser cette information pour briser le crypto-système.

Boneh et al.ont classé les fautes injectées en deux classes. Le premier type est les fautes transitoires qui peuvent induire le crypto-système en erreur durant une fraction temporelle bien bornée correspondant à une opération bien spécifique du crypto-système que l'on cherche à corrompre. Le deuxième type est les défauts injectés pour lesquels l'accès physique

au matériel est nécessaire. À titre d'exemple, dans [Sco02], un simple flash d'appareil photo dont la lumière est concentrée par un microscope est utilisé sur un transistor pour changer l'état d'une cellule mémoire SRAM dans un microcontrôleur à une valeur constante. Les auteurs ont aussi suggéré d'utiliser le style de logique double rail pour contrer ces attaques, qui pourrait également aider à faire face contre les attaques d'analyse de puissance.

L'injection de fautes nécessite la définition de modèles de fautes tout comme des modèles de fautes sont générés pour effectuer le diagnostic des circuits fautifs. Contrairement au diagnostic des circuits, ces modèles de fautes ne sont pas utilisés pour retrouver le site des pannes mais pour retrouver des informations secrètes et plus particulièrement des portions de la clef secrète. Différents modèles sont utilisés pour modéliser les effets de perturbations décrites ci-dessus. Les différents modèles distinguent généralement la localisation de la faute dans le temps et l'espace et le type de fautes engendrées [Ngu11].

Les attaques par injection de défauts peuvent être considérées comme des attaques dangereuses car les contremesures incluent des techniques complexes qui ne sont pas faciles à mettre en œuvre sur un environnement contraint tel que les cartes à puce.

2.3 Les contremesures

Depuis que l'analyse de puissance différentielle constitue une menace réelle pour la sécurité de la carte à puce, les attaques DPA ont montré qu'il est possible de briser de nombreux algorithmes cryptographiques. Une grande variété de contremesures a été proposée pour prévenir les attaques d'analyse de puissance sur cartes à puce.

Les contremesures contre les attaques DPA peuvent être classées en deux groupes: dissimulation et masquage. Le but de la dissimulation est de supprimer la dépendance de données de la consommation d'énergie. Cela signifie que soit l'exécution de l'algorithme est aléatoire ou les caractéristiques de consommation d'énergie du circuit sont modifiées de manière à ce que l'attaquant ne puisse pas trouver facilement une dépendance de données. L'idée de base du masquage est de rendre aléatoire les valeurs intermédiaires qui sont traitées par le circuit cryptographique.

Ces contremesures peuvent aussi être classées selon le niveau sur lequel elles sont mises en œuvre, le niveau algorithmique ou le niveau matériel. Sur le niveau algorithmique, un masquage aléatoire des variables intermédiaires [Has01] est, par exemple, une technique largement utilisée. Ce sont là des contremesures qui dépendent de la plateforme et qui nécessitent un temps de traitement important. Les contremesures matérielles peuvent être classées en fonction du niveau de concept durant le flot de conception.

Les techniques au niveau du système comprennent l'ajout de bruit à la consommation d'énergie du circuit [Ben03], la duplication des logiques avec des opérations complémentaires [Sap03], la technique de filtrage du signal d'alimentation pour maintenir une consommation constante pendant le fonctionnement du circuit sécurisé [Sha00]. Certaines de ces techniques

ont un intérêt théorique puisque en raison de coût en surface important, elles ne peuvent pas être utilisées pour concevoir des cartes à puce d'autoprotection résistantes.

Les contremesures au niveau porte comprennent des techniques de circuiterie qui peuvent être mises en œuvre en utilisant des portes disponibles dans une bibliothèque standard de cellules logiques, par exemple masquage aléatoire [Gol04], pré-charge aléatoire [Buc03], les transitions d'état et l'équilibrage de poids de Hamming [Cun02].

Enfin, l'approche au niveau transistor pour empêcher les DPA est basée sur l'adoption d'une famille logique dont la consommation électrique est indépendante des données traitées. Bien que cette approche est reconnue la plus puissante des contremesures, son coût en terme de temps de conception est largement très élevé car une approche complète sur mesure est nécessaire.

.

2.3.1 Les contremesures algorithmiques

La plupart de ces attaques exploitent certaines caractéristiques spécifiques des implémentations logicielles d'algorithmes cryptographiques, et beaucoup de contremesures ont été conçues au niveau logiciel. Une des techniques logicielles la plus puissante pour contrer de telles attaques est de masquer toutes les entrées et les données intermédiaires afin de corréler toute fuite d'information à travers les canaux cachés de données secrètes réelles en cours de traitement [Cha99]. Le message et la clé sont masqués avec des valeurs aléatoires au début des calculs, et par la suite tout est presque comme d'habitude. La valeur du masque à la fin d'une certaine étape fixe doit être connue afin de rétablir la valeur attendue à la fin de l'exécution. Un exemple de masquage est de masquer les implémentations de l'algorithme AES (Advanced Encryption Standard) [Nat01]. Dans la section 2.3.2.2 est montré comment appliquer la technique de masquage de données au niveau des micro-opérations comme un ET logique.

2.3.2 Les contremesures matérielles

Les contremesures matérielles sont classées selon le niveau d'abstraction impliqué pendant le flot de conception. Nous allons donner une brève description des différentes solutions adoptées dans chaque niveau.

2.3.2.1 Contremesures au niveau système

Les contre-mesures au niveau du système sont une approche qui n'a aucune incidence sur la mise en œuvre de l'algorithme. Par exemple Shamir [Sha00] a proposé un procédé dans lequel l'alimentation électrique est isolée à partir du matériel cryptographique d'une carte à puce en utilisant des condensateurs pour fournir le courant. Deux condensateurs sont utilisés: l'un fournit du courant à la puce tandis que l'autre se recharge. L'examen de la ligne d'alimentation montrera seulement un motif résultant de la charge des condensateurs d'alimentation interne. Une autre approche, proposée dans [Rat04], agit comme un circuit

auxiliaire pour augmenter la difficulté d'analyse de puissance des attaques matérielles. Un circuit de suppression DPA qui peut être ajouté à des dispositifs matériels existants mettant en œuvre des algorithmes cryptographiques est présenté. L'idée est que DPA obtient des informations sous la forme de variations dans le courant d'alimentation. Si ces variations sont atténuées, DPA est plus difficile à effectuer. En d'autres termes, l'attaquant nécessite davantage d'échantillons de puissance pour distinguer la corrélation pointes de bruit. Le circuit de suppression est montré à la figure 2.4. Son principe de fonctionnement est que lorsque un courant instantané consommé par le dispositif sous protection est détectée, un courant approprié est shunté de sorte que le courant total de l'alimentation montre moins de variation.

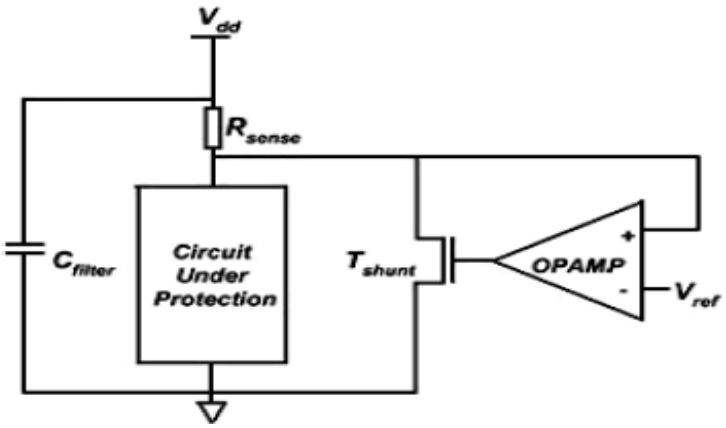


Figure 2.4 diagramme du bloc de circuit de suppression.

2.3.2.2 Contremesures au niveau porte

Le masquage au niveau de la porte en utilisant une logique masquée spéciale a été proposé dans [Tri02] et [Gol04], il a été démontré comment appliquer des techniques de masquage des données au niveau des micro-opérateurs logiques tels que ET logique, XOR, etc., et comment utiliser ces opérateurs comme éléments de base pour la mise en œuvre d'inversion dans les champs composites directement sur des données masquées. La principale contribution de ces travaux est la conception d'une porte ET masquée et son utilisation pour sécuriser les implémentations de l'AES. Le problème considéré, par exemple, dans [Men03] est de savoir comment calculer en toute sécurité dans le matériel, sur le niveau de la porte logique, la fonction masquée ET (Figure 2.5). Un autre exemple de contremesure matérielle au niveau porte est la technique proposée dans [Buc05], basée sur l'insertion de retards aléatoires sur les signaux d'entrée de chaque étage d'un pipeline du chemin de données d'un processeur en vue de rendre aléatoire la quantité de charge de l'alimentation. Dans la figure 2.6, la technique proposée pour brouiller la consommation de courant est représentée, en considérant un étage

de pipeline générique dans un processeur cryptographique, chaque entrée du réseau combinatoire est retardée par un temps aléatoire $\Delta_i = 1,\ldots, N$. Cela permet d'introduire une variance sur la forme d'onde, et de rendre également la quantité de charge transférée indépendante des données traitées grâce à la modification de la séquence interne de transitions due aux retards d'entrée.

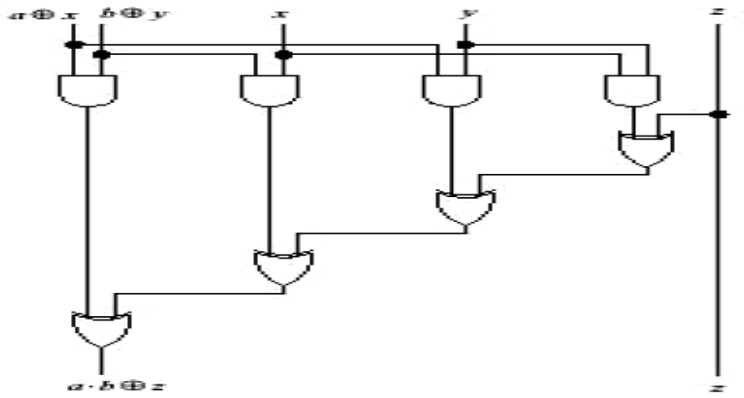


Figure 2.5 Exemple d'un ET masqué.

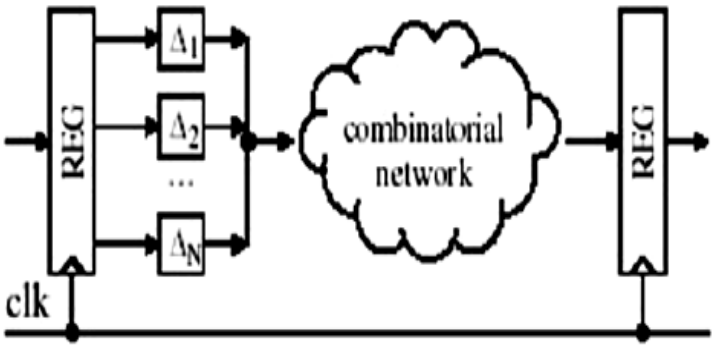


Figure 2.6 Etage d'un pipeline avec délais aléatoires.

2.3.2.3 Les contremesures au niveau transistor

La logique CMOS, qui est le style logique par défaut dans les bibliothèques de cellules standard utilisées pour les circuits sécurisés, ne consomme de l'énergie de l'alimentation que lorsque sa sortie a une transition 0-1. Pendant la transition 1-0, l'énergie précédemment stockée dans la capacité de sortie est dissipée et dans les deux événements d'une transition 0-0 ou 1-1 aucune puissance n'est utilisée. Cette demande de puissance asymétrique fournit les informations utilisées dans DPA pour la clé secrète.

Depuis l'introduction de DPA, plusieurs contre-mesures matérielles ont été proposées à différents niveaux logiques: contremesures au niveau système, au niveau porte et au niveau transistor.

L'approche au niveau du transistor est basée sur l'adoption d'un style logique dont la consommation d'énergie est constante ou indépendante des données traitées. La logique CMOS standard a une consommation d'énergie qui dépend fortement des données traitées. Pour affaiblir la relation entre les données traitées et la consommation d'énergie, deux solutions différentes ont été introduites. Une première solution est la logique dynamique (ou pré-charge), où chaque signal a une phase d'évaluation dans laquelle le signal prend la valeur logique en fonction de la fonction logique réalisée et une phase de pré-charge dans laquelle chaque signal passe à V_{DD}. Un signal d'horloge supplémentaire en entrée de la porte définit les différentes phases.

La deuxième solution est le style de logique double rail dans lequel chaque signal X est remplacé par la paire de signaux X et son inverse $\overline{X}$. Dans ce style logique, une porte OU à deux entrés possède quatre entrées (A, $\overline{A}$, B, $\overline{B}$) et deux sorties (S, $\overline{S}$). L'avantage de cette solution dans les applications cryptographiques, réside dans le fait que chaque fois qu'une sortie passe à l'état bas (0) l'autre passe à l'état haut (1) produisant une consommation d'énergie. Le premier inconvénient de cette solution est que chaque porte a besoin d'une surface additionnelle pour dupliquer la logique. Du point de vue de la sécurité, lorsque les entrées ne changent pas, la sortie ne change pas trop, comme dans CMOS. Ceci procure aux circuits doubles rails des propriétés intéressantes. A titre d'exemple, la consommation des circuits double rail est indépendante des données traitées, ce qui conduit, à l'accroissement de la robustesse des circuits aux attaques. Plusieurs mises en œuvre de cellules sécurisées en style de logique de pré-chargement double rail (DRP) ont été proposées dans la littérature pour contrer DPA. Nous citerons la logique SABL, (Sense Amplifier Based Logic) introduite dans [Tir02], la logique WDDL (Wave Dynamic Differential Logic) [Tir04], la logique STTL (Secure Triple Track Logic) [Raz07], la logique MDPL (Masked Dual-rail Precharge Logic) [Pop05] et la logique quasi insensible au délai (QDI), appelée également SecLib [Nas10].

Ces contremesures ont toutes une caractéristique commune, à savoir les signaux sont encodés en tant que deux fils complémentaires et la consommation d'énergie est constante sous l'hypothèse que les sorties différentielles de chaque porte commandent la même charge capacitive. La construction de deux fils équilibrés nécessite une approche personnalisée, augmentant ainsi les coûts de conception et d'entretien. Un style logique DRP peut être implémenté en utilisant des portes CMOS standard, comme dans le cas de la logique (WDDL) [Tir04], ou en utilisant une conception personnalisée dans laquelle chaque porte est conçue au niveau du transistor, comme dans le cas de Sense Amplifier Based Logic (SABL) [Tir02]. Des flots de conception semi-personnalisés supportant des familles logiques différentielles ont été proposés dans la littérature. Par exemple, une technique pour le routage

automatique de lignes complémentaires équilibrées a été introduite dans [Tir04a]. Même si un routage automatique peut réduire le temps de conception et augmenter la portabilité, la technique de routage équilibré proposée ne prend pas en compte la dépendance de la charge capacitive sur une ligne de l'état logique des fils adjacents et introduit par ailleurs des contraintes supplémentaires pour l'outil de routage limitant ainsi son efficacité et, possiblement, provoquant une surcharge de surface. Une autre technique proposée dans [Pop05, Pop06] est basée sur un style de logique double rail de pré-charge masquée (MDPL) où, en raison du masquage aléatoire au niveau de la porte, la consommation d'énergie est aléatoire. Mais aussi comme MDPL est une logique de pré-charge double rail, les changements sont évités et les fils complémentaires n'ont pas besoin d'être équilibrés, éliminant ainsi l'inconvénient principal des circuits double rail. Cependant, une première implémentation de MDPL montrait une fuite DPA due à la propagation précoce des données d'entrée par rapport aux masques [Pop07].

Une implémentation améliorée (aMDPL) a été proposée par Popp et al. [Pop07], où les bascules RS sont utilisées pour resynchroniser les entrées forçant ainsi une cellule combinatoire à évoluer uniquement lorsque toutes les entrées sont dans un état différentiel valide. Dans ce chapitre, deux familles de logiques différentes pour contrer les attaques par injection de fautes et DPA seront présentées. A partir des portes logiques CMOS standard, on montrera que chaque solution proposée constitue une amélioration par rapport à l'autre en ce qui concerne les critères de sécurité et de conception. La première solution proposée est le style de logique WDDL qui est basée sur deux opérations (pré-charge et évaluation), et qui repose sur l'utilisation de signaux avec deux états possibles: logique 1 (tension V_{DD}), logique 0 (tension GND). Une porte logique WDDL présente une consommation de puissance indépendante des données sous l'hypothèse idéale que les deux charges de sortie sont parfaitement équilibrées. La deuxième solution est une logique quasi-insensible au délai QDI. Elle est obtenue par introduction d'une porte de Muller pour assurer la synchronisation des signaux. Pour chaque modèle de logique, des détails d'implémentation et des résultats de simulation sur un ensemble de base de portes logiques sont d'abord rapportés. Des études de cas simples sont discutées.

2.4 La logique WDDL

La logique WDDL permet de protéger les circuits cryptographiques contre les attaques par injection de fautes et par l'analyse différentielle de la consommation de courant. Elle est issue des travaux de Tiri et Verbauwhede [Tir04]. Ces derniers ont montré qu'il était possible de réaliser une contremesure à base de portes spécifiques WDDL pour les dispositifs programmables de type FPGA en rendant la consommation de courant indépendante des transitions logiques, ce qui permet d'augmenter davantage la résistance des circuits aux attaques DPA. Néanmoins, pour qu'elle soit efficace, il faut que le routage des signaux

différentiels du circuit soit équilibré. Dans ce type d'équilibrage le circuit contient deux parties : sa partie originale C_t et sa partie duale C_f. Si f_t désigne une fonction logique du circuit ayant comme entrée x_t et comme sortie S_t, la fonction duale f_f vérifiera la propriété suivante $S_f = f_f(x_f) = \text{non}(f_t(xt)) = \text{non}(f_t(\text{non}(x_f)))$ si $x_f = \text{non}(x_t)$. Les deux fonctions sont réalisées à l'aide de réseaux superposables. À titre d'exemple, la partie gauche de la figure 2.7 représente la porte logique ET WDDL. Sa partie originale est constituée d'une porte logique ET et sa partie duale d'une porte logique OU. Ces parties sont superposables (l'une est le miroir de l'autre) lorsqu'elles sont représentées aux niveaux transistors comme indiqué sur la partie droite de la figure 2.7.

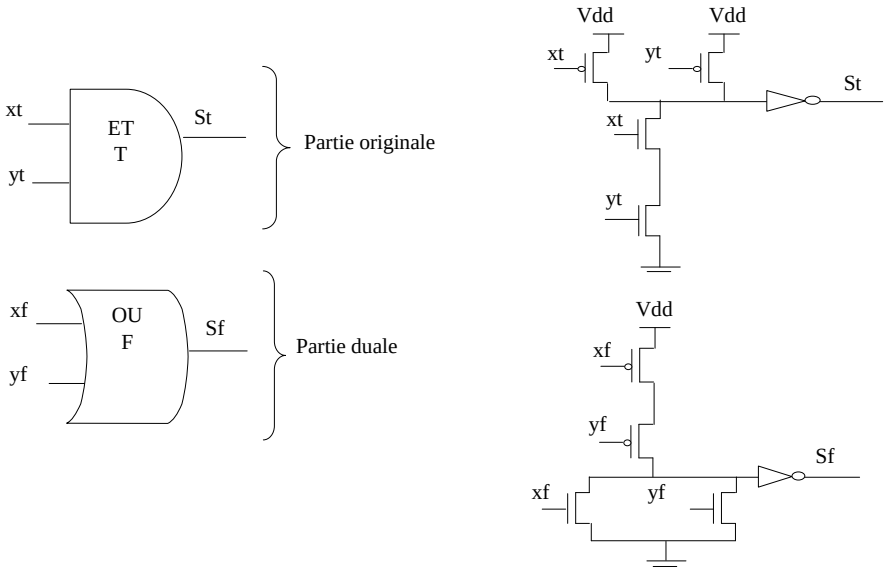


Figure 2.7 Porte ET WDDL (vue porte, à gauche et transistor, à droite)

2.5 Bibliothèque de cellules WDDL : conception et simulation

La technologie choisie pour la présente étude est 45nm CMOS. Des simulations du circuit ont été réalisées dans l'environnement CADENCE IC 16.3. Une alimentation de 1.1V a été supposée. Tous les transistors à canal n et canal p ont été dimensionnés pour une surface minimale. Le fonctionnement transitoire de la porte ET WDDL est illustré par la figure 2. 8. La consommation d'énergie de la porte ET WDDL a été aussi simulée en tenant compte d'une capacité d'interconnexion de 1.5 f F à la fois pour les sorties St et Sf.

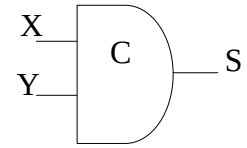
On voit que la consommation en courant est indépendante des données traitées, et que chaque bit est représenté par un couple de signaux et les calculs permutent entre la phase de pré-charge (PRE) et la phase d'évaluation (EVA). Dans la phase de pré-charge toutes les entrées sur la gauche sont mises à l'état logique 0, cela amène la vraie sortie S_t et la sortie fausse S_f à se mettre à l'état logique '0'. Dans la phase d'évaluation, après le basculement des entrées, seule S_t ou S_f sera mise à l'état logique '1'. Il est à noter que quelque soit la transition

temporelle, EVA à PRE ou PRE à EVA, et quelles que soient les données d'entrés, seulement l'une des sorties différentielles commute ce qui donne un nombre de transition constant. On voit sur la figure 2. 8 que le nombre de transitions est le même pendant la phase PRE à la phase EVA et vice-versa. Une transition ascendante de 0 à 1 indique que les deux entrées soient égales à 1. Par contre une transition descendante de la sortie de 1 à 0 ne contient pas suffisamment d'information sur l'état actuel de chacune des deux entrées. La seule information qu'elle fournit est qu'au moins une entrée est égale à 0. Pour éviter ce type de situation la méthode DIMS (Delay-Insensitive Minterm Synthesis) a été utilisée pour synchroniser toutes les valeurs possibles des entrées grâce à des portes de Muller.

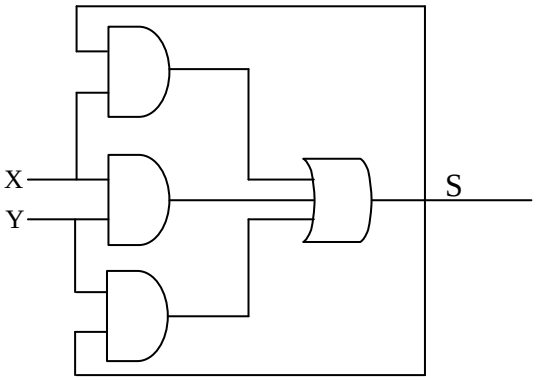
Figure 2.8 Réponse transitoire de ET WDDL.

2.6 Porte de Muller

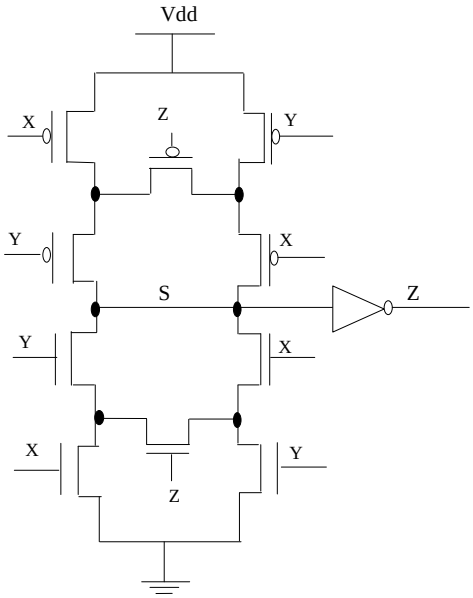
La porte de Muller appelée aussi C-element permet de synchroniser deux événements. Elle ne passe à 0 que lorsque ses deux entrées sont passées à 0, et ne repasse à 1 que lorsque ses deux entrées sont elles aussi repassées à 1. Elle est considérée comme un ET événementiel, ce qui explique le symbole de cette porte (figure 2.9 (a)), inspiré du ET logique. On peut réaliser cette porte à l'aide de portes standard à base d'une majorité dont la sortie reboucle sur l'une des entrés (Figure 2.9 (b)). Et si l'on veut faire plus simple avec des transistors en technologie CMOS, il faut une boucle d'inverseurs pour mémoriser la sortie lorsque X et Y ont des valeurs différentes (Figure 2.9 (b) et (c)). Sa réponse transitoire est donnée par la figure 2.9 (e).



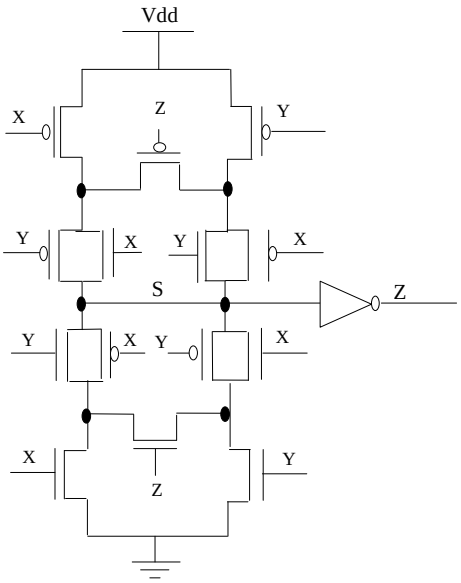
(a)



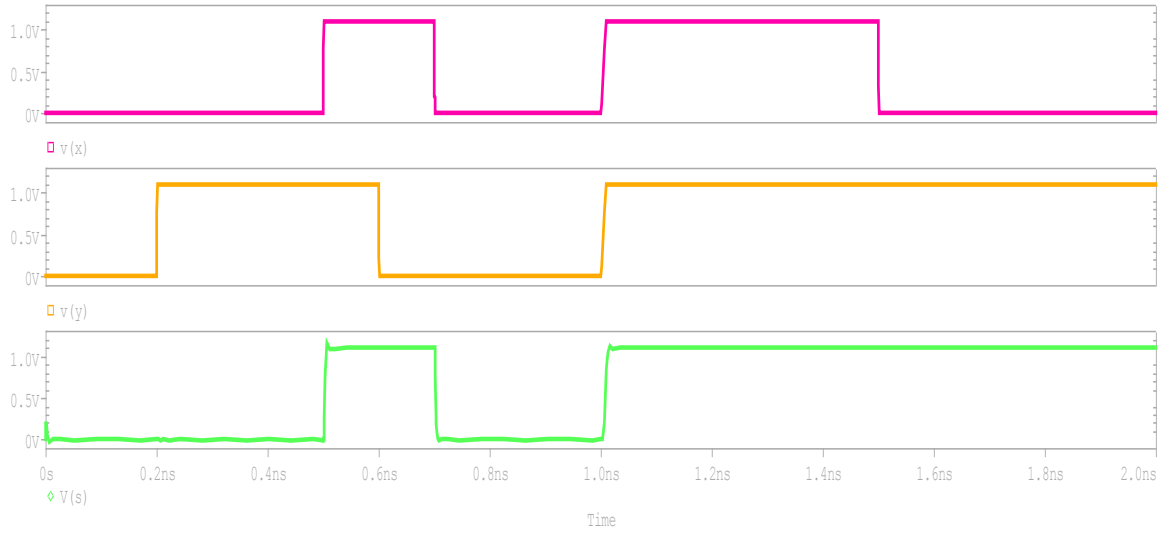
(b)



(c)



(d)



(e)

Figure 2.9 (a) Symbole C-element, C-element à base de portes standard (c) C-element régulier, (d) C-element sécurisé et
(e) Simulation Spice.

2.7 La logique QDI'

Ce type de logique offre l'avantage des temps de propagation dans les portes logiques et dans les interconnexions non bornées. Cette classe de circuits est couramment la plus utilisée dans la pratique. De nombreux microprocesseurs ont été fabriqués en technologie asynchrone QDI [Ouc11]. A titre d'exemple, les travaux de Shimoda [Shi05] ont proposé des solutions complètement asynchrones. Bien que les circuits asynchrones double rail et plus spécifiquement les circuits QDI semblent être les circuits les plus robustes aux attaques par injection de fautes et aux attaques différentielles en courant, la très grande majorité des circuits sécurisés conçu pour des applications cryptographiques sont aujourd'hui des circuits synchrones réalisés avec de la logique CMOS standard. Et cela revient particulièrement au manque d'outils de conception de circuits asynchrones. Les concepteurs de circuits asynchrones sont contraints alors d'utiliser les outils de conception de circuits synchrones. Cependant, ceci conduit à un autre obstacle, à savoir l'absence de bibliothèque de cellules contenant les primitives de base de la conception de circuits asynchrones comme par exemple les portes de Muller.

2.8 Propriétés intrinsèques des circuits QDI

Les propriétés intrinsèques des circuits QDI les rend plus attractifs. En effet, elles augmentent considérablement leur résistance aux attaques par injection de fautes et DPA. Parmi ces propriétés on trouve celles citées ci-dessous.

2.8.1 Codage des données de type 1 parmi n

Ce type de codage présente un certain avantage du fait qu'il permet un poids de Hamming constant quelles que soient les données manipulées. Par ailleurs, la dépendance entre ces dernières et le courant consommé est fortement réduite. De plus, il augmente aussi la résistance des circuits QDI aux attaques par injection de fautes en utilisant l'état invalide pour générer des alarmes en cas de détection de fautes.

2.8.2 Chemins de données équilibrées

Les circuits quasi asynchrones ont l'avantage de contrôler avec précision le nombre de transitions logiques dans chaque bloc de calcul. Cela rend les chemins de données plus équilibrées et assure ainsi une consommation indépendante des données sur chaque chemin.

2.8.3 Contrôle local

Le contrôle local a l'avantage d'offrir une répartition de l'activité du circuit dans le temps et de rendre plus difficile la synchronisation sur un événement particulier. Par conséquent, cela rend impossible toute attaque temporelle.

2.8.4 Protocole de communication

À l'inverse des circuits synchrones, les circuits asynchrones n'utilisent pas de signal d'horloge. La gestion des communications se fait de manière locale par une synchronisation entre blocs fonctionnels. Un des concepts les plus importants dans les circuits asynchrones est le contrôle local. Les échanges d'informations se font de manière bidirectionnelle et tout échange d'information doit être acquitté afin que l'émetteur puisse émettre à nouveau. Cela signifie que chaque unité se synchronise seulement avec les blocs dont la synchronisation a une signification fonctionnelle. De plus, elle se fait uniquement lorsqu'elle doit avoir lieu, indépendamment du reste du système. Par conséquent, pour garantir une synchronisation indépendante du temps, il est plus réaliste de considérer pour chaque bloc d'un circuit asynchrone des signaux explicites de synchronisation utilisant des protocoles de type requête/acquittement ou « poignée de main » avec les blocs voisins, comme représenté sur la figure 2.10. L'efficacité complète du circuit passe par un choix judicieux du protocole et du codage afin de minimiser la surface occupée et l'énergie utilisée. Pour ces raisons de surcoût, des protocoles quatre phases ont été développés.

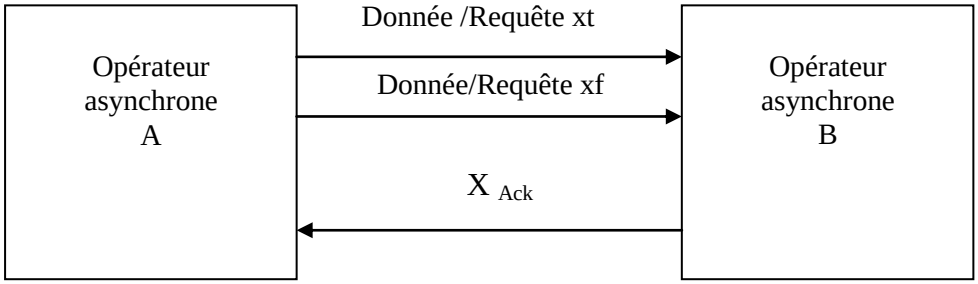


Figure 2.10 Communication de type requête/acquittement entre opérateurs asynchrones.

2.9 Protocole 4-phases

En ce qui concerne le protocole de communication, il apparaît que le protocole 4 phases soit le plus adapté pour la répartition du courant dans le temps et la réduction des pics de courant ainsi que l'émission électromagnétique tout en lissant la forme d'onde du courant. Le protocole 4-phases est un protocole d'acquittement des données, permettant au destinataire B de signaler à l'expéditeur A qu'il a bien reçu la donnée x que celui-ci lui a envoyé. Ceci est réalisé grâce à un signal d'acquittement x_{Ack} , comme présenté sur la figure 2.11. Le principe du protocole 4-phases est le suivant :

Phase 1. Lorsque x_{Ack} est à 0, A peut mettre une donnée valide sur la paire de fils (xt, xf) ;

Phase 2. Lorsque B a bien reçu les données, il met son acquittement x_{Ack} à 1 ;

Phase 3. Détectant l'acquittement à 1, A doit alors remettre sa donnée à l'état invalide ;

Phase 4. Une fois que B a bien reçu la donnée invalide, il relâche son acquittement qui retourne à 0. Ceci est schématisé par la figure 2.11, dans lequel les flèches grises symbolisent l'ordre chronologique des événements.

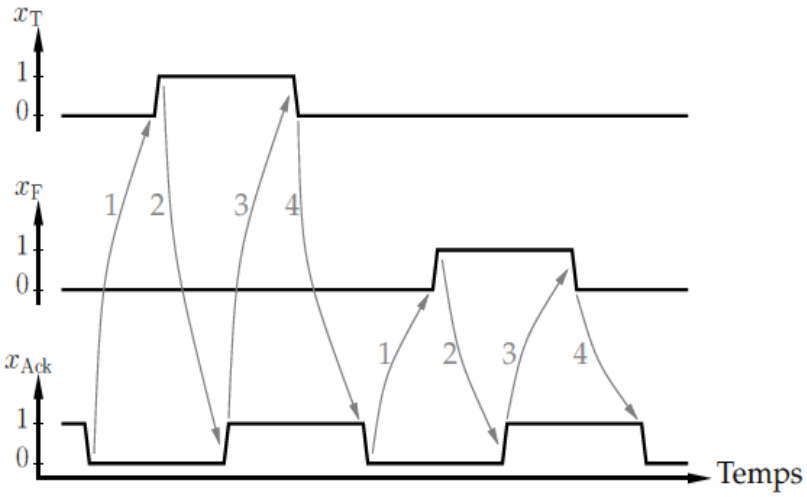
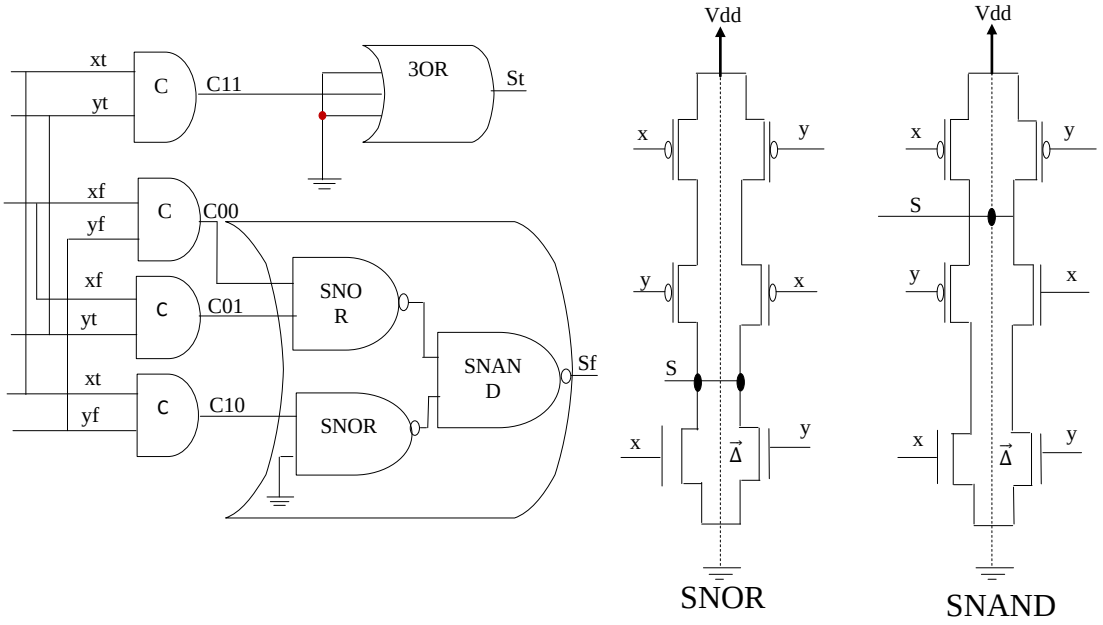


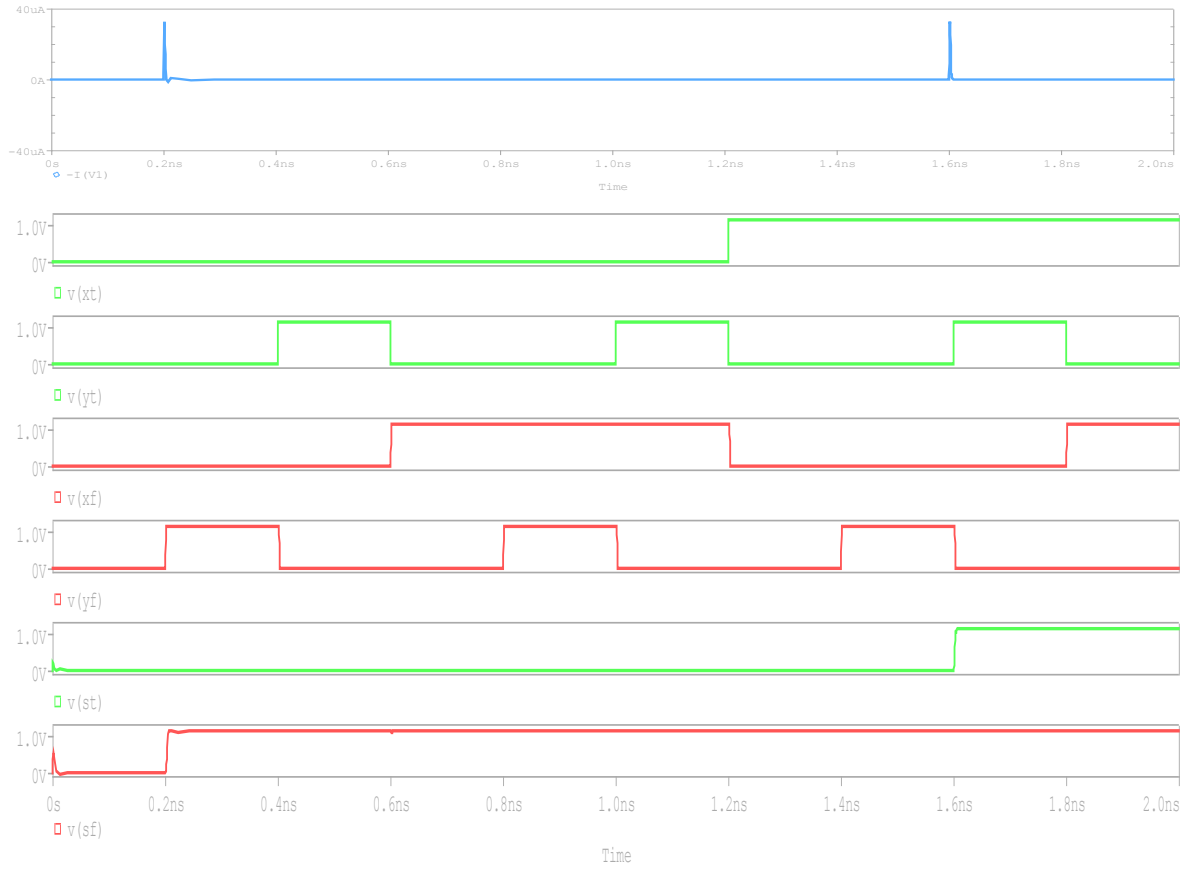
Figure 2. 11 Protocole 4 phases

2.10 Bibliothèque de cellules QDI: conception et simulation

Dans la logique QDI, les paramètres de conception et les outils de simulation sont les mêmes que ceux choisis pour ET WDDL. La consommation d'énergie de ET QDI a été aussi simulée en tenant compte d'une capacité d'interconnexion de 1.9 fF à la fois pour les sorties St et Sf. La porte ET QDI est composée de quatre portes de Muller et de deux portes 3OR constituées chacune de deux portes SNOR et une porte SNAND qui possèdent une architecture parfaitement symétrique comme le montre la Figure 2.12 , en gardant la même fonction logique des portes NOR et NAND de la bibliothèque des cellules standard. Les figures 2.12 (a) et (b) montrent comment réaliser le rendez-vous électrique de deux signaux à partir d'une porte complexe ET QDI. Les résultats de simulation de la porte ET QDI sont représentés par la figure 2.12 (c)**.** On constate sur cette figure que la puissance consommée est nettement indépendante des données d'entrées par rapport à la puissance consommée dans le cas de la porte ET WDDL (figure 2.8).



(a) (b)



(c)

Figure 2.12 Schema de (a) une ET QDI sécurisée, (b) l'architecture interne de la porte 3OR et (c) la simulation Spice de ET QDI.

2.11 Conclusion

Ce chapitre nous a permis tout d'abord de rappeler quelques attaques qui menacent la sécurité des systèmes sécurisés, fondées essentiellement sur les attaques logiques et les attaques matérielles. Ensuite les différentes contremesures matérielles ont été présentées. Parmi les attaques matérielles, les attaques par injection de fautes et en puissance sont considérées comme étant les plus dangereuses. Les contremesures implémentées en logique WDDL et QDI sont reconnues comme étant les plus efficaces contre les attaques par injection de fautes et DPA. Aussi, dans la suite de nos travaux, nous allons nous intéresser à ce type de contremesures et nous étudierons leur robustesse.

Chapitre 3

Impact des défauts résistifs sur les circuits sécurisés

3.1 Introduction

Ce chapitre porte sur l'analyse et la modélisation de l'effet des défauts résistifs sur le comportement des circuits sécurisés implémentés en WDDL et QDI contremesures. Nous étudierons deux types de défauts paramétriques, le défaut de circuit-ouvert résistif et le défaut de court-circuit résistif. Les défauts proposés sont évalués par une technologie CMOS 45nm avec une redondance modulaire triple (TMR). Pour cela, nous avons utilisé le modèle de fautes décrit au chapitre 1. L'étude porte sur l'analyse des temps de réponse et les intervalles de détection de défaut et donc de tolérance aux fautes. L'objectif est de rechercher la résistance maximale pour laquelle le défaut est considéré comme un court-circuit résistif et la résistance minimale pour laquelle le défaut sera assimilé à un circuit-ouvert détecté. Nous analyserons le comportement électrique de deux structures TMR conçues à base de deux types de portes sécurisées, la porte ET WDDL et la porte ET-QDI en présence de défauts résistifs. Ensuite l'étude sera étendue à une troisième structure TMR conçue à base d'un registre complet asynchrone double rail. Ces trois structures TMR sont implémentées en technologie CMOS 45 nm et ont une tension Vdd =1.1 V. L'ensemble des simulations sont réalisées avec le logiciel SPICE de l'environnement CADENCE.

3.2 Analyse électrique de l'effet du circuit-ouvert

Dans cette section, nous développons une méthode de tolérance aux fautes adaptée aux problèmes de test et de la fiabilité des circuits sécurisés WDDL et QDI. Pour analyser l'effet du défaut de circuit-ouvert résistif sur le comportement électrique de la TMR à base de la porte ET WDDL et de la TMR à base de la porte ET QDI, nous suivons la procédure ci-dessus montrée par la Figure 3.1. Tout d'abord, nous utilisons les portes ET WDDL et ET QDI, comme illustré sur la Figure 3.2 (a) et 3.2 (b), ensuite nous les transformons en structures TMR, dans lesquelles nous injectons le défaut de circuit-ouvert entre les lignes d'interconnexion des modules 2 et 3 (Fig 3.1), et enfin nous faisons plusieurs simulations SPICE avec différentes valeurs de la résistance pour comparer le comportement résultant avec le comportement du module 1 sans défaut afin de caractériser ses effets.

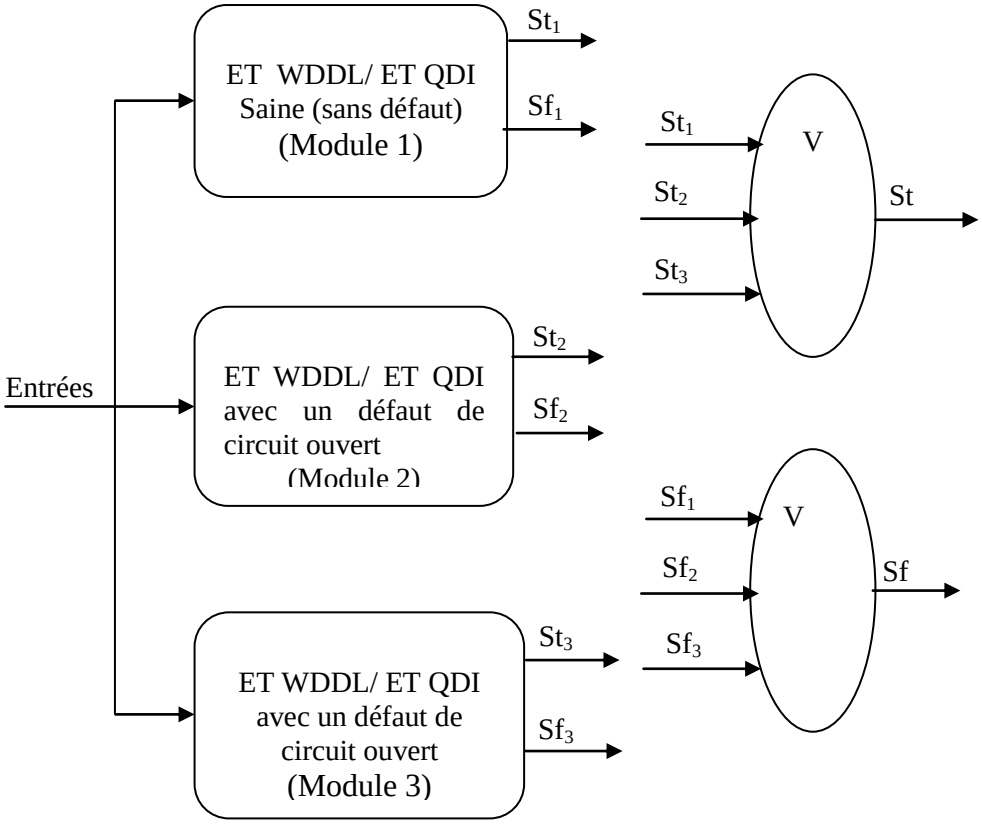
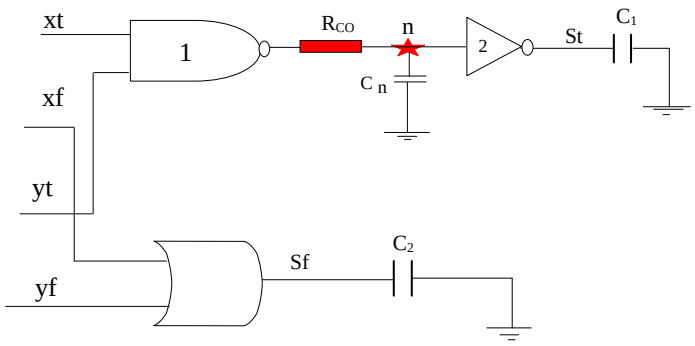
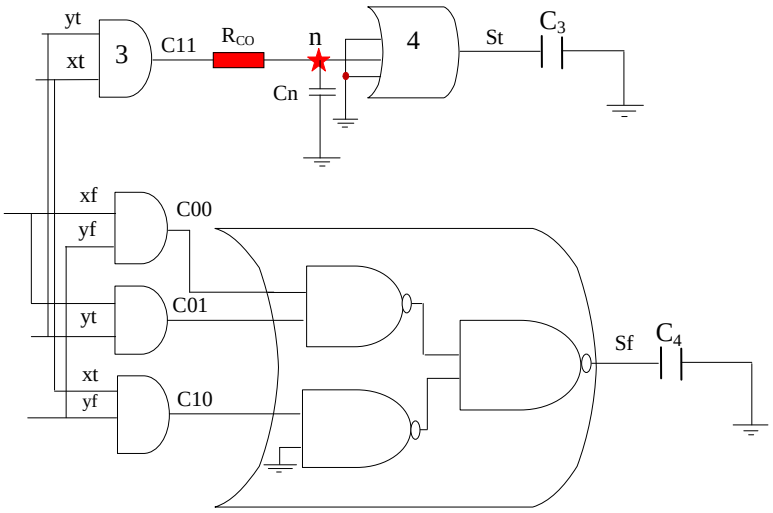


Figure 3.1 injection de deux défauts de circuit-ouvert dans la TMR.

Les deux portes affectées par un circuit-ouvert résistif représenté par la résistance R_{CO} sont montrées sur la Figure 3.2. Le nœud n est affecté par un circuit-ouvert résistif représenté par la résistance R_{CO}. Ces deux portes sont représentatives de ce qui peut se passer dans un circuit intégré sécurisé, voire une puce cryptographique actuelle, et les conclusions que nous tirerons de cette étude peuvent être extrapolées à des circuits complexes. Les deux portes sont composées de 4 entrées, notées xt, yt, xf, yf et de deux sorties notées St (sortie saine) et Sf (sortie fautive). La capacité C_n représente la charge créée par les portes en aval du défaut [Hou09]. D'un point de vue statique (cas du test booléen), il a été prouvé qu'un circuit-ouvert résistif ne peut pas être détecté du fait que le nœud fautif finit toujours par atteindre son niveau logique sain [Hou09]. Par contre, ce défaut modifie le comportement temporel du circuit et il peut donc être détecté par un test dynamique, autrement dit par un test en retard grâce à l'application d'une paire de vecteurs de test [Hou09].



a. ET WDDL fautive.

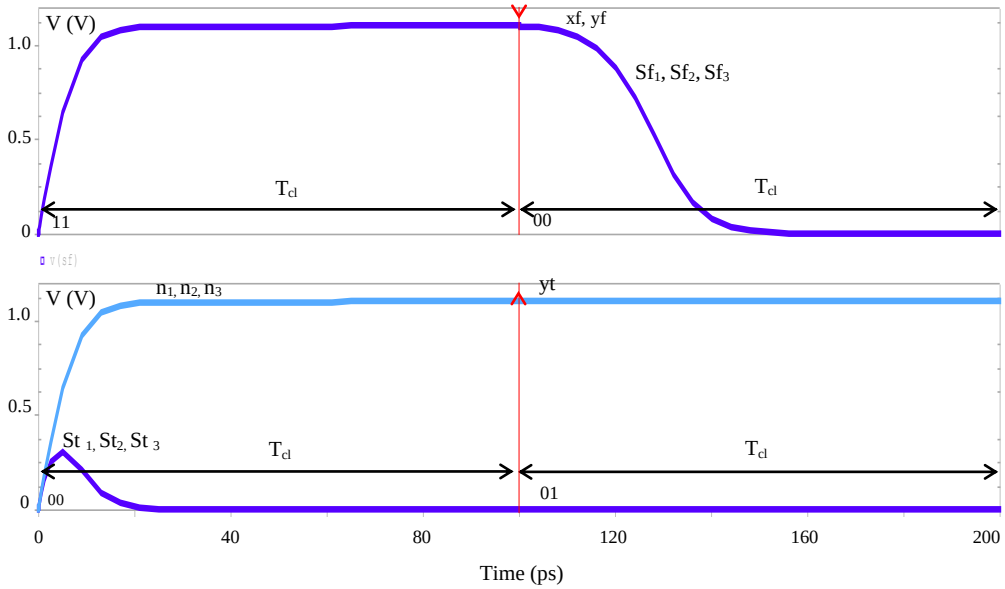


b. ET QDI fautive.

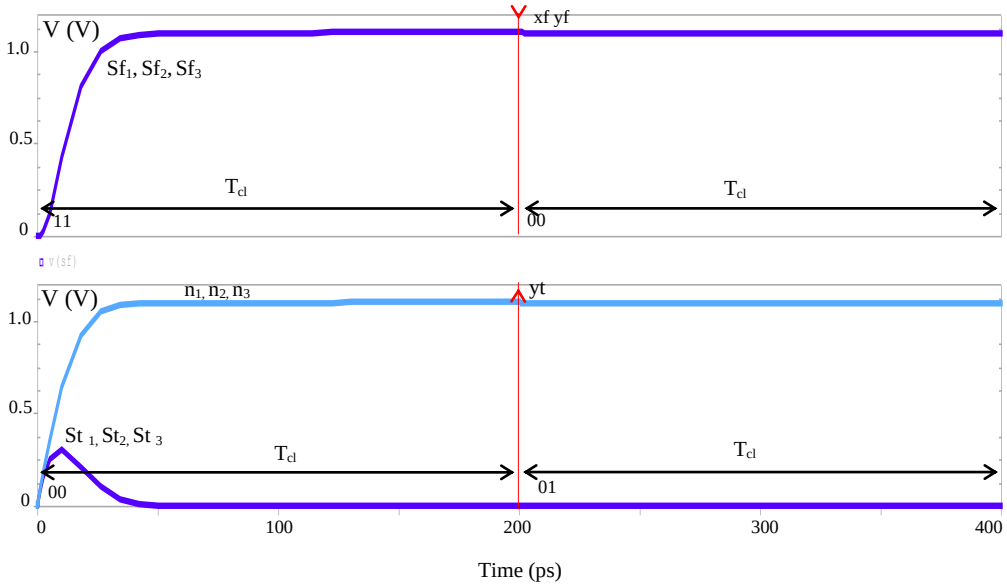
Figure 3.2 Portes affectées par un circuit-ouvert résistif

Les deux portes sécurisées restent toujours reliées mais par une ligne dégradée caractérisée par la résistance R_{CO}. Cette résistance imprévisible est le paramètre prépondérant de la modélisation du défaut, et pour illustrer son influence, on peut réaliser plusieurs simulations avec différentes valeurs de résistance. Mais avant, il est nécessaire de caractériser la réponse dynamique des deux TMR saines de manière à pouvoir raisonner en fonction d'une référence. La Figure 3.3 représente la réponse transitoire des deux modèles de TMR saines. L'état initial est donné par la séquence de test T0 = [xt yt xf yf] = [0011] et l'état final par la séquence T1= [0100]. Nous remarquons que les allures générales des caractéristiques des Figures 3.3.a et 3.3.b sont tout à fait similaires. Cependant, les ordres de grandeur des temps de propagation et des tensions de sortie notamment pour St ne sont pas identiques. Un facteur multiplicatif faible d'environ 0.4 existe et n'a qu'une très légère influence sur les caractéristiques. Cette amplification est due à la structure de chaque porte et au facteur d'échelle appliqué sur le

cycle d'horloge interne qui est de Tcl= 0.1ns pour la TMR à base de la porte ET WDDL et T_{cl} = 0.2ns pour la TMR à base de la porte ET QDI, ainsi qu'aux capacités parasites et au délai de propagation de chaque porte. Les entrées xt, yt, xf, yf commutent de 0 à V_{dd} et la transition est propagée à travers les portes 1 et 2 dans la porte ET-WDDL et à travers les portes 3 et 4 dans la porte ET-QDI. La sortie Sf commute de V_{dd} à 0.



a. TMR ET WDDL



b. TMR ET QDI

Figure 3.3 Réponse transitoire des TMR saines

Nous effectuons maintenant une série de simulations similaires avec une paire de séquences de test différente T0= [0011] et T1= [0111]. Dans les figures 3.4.a et 3.4.b nous choisissons une résistance de défaut assez petite : R_{CO} = 200 Ω pour la TMR à base de la porte ET WDDL et R_{CO}= 400 Ω pour la TMR à base de la porte ET QDI.

Les résultats de simulation sont montrés par la figure 3.4. On définit les temps de propagation suivants [Hou09]:

- T_{pav}, le temps de propagation avant le défaut,
- T_{pap}, le temps de propagation après le défaut,
- T_{ad}, le retard induit par le défaut,
- T_m, la marge temporelle du chemin yt => St.

On voit sur la figure que le front montant de l'entrée yt atteint le défaut au temps T_{pav}= 46.7 ps pour la TMR ET WDDL et au temps T_{pav}= 166.5 ps pour la TMR ET QDI. Ce temps est égal à la somme des différents retards T_{di} de propagation des portes.

$$T_{pav} \text{ pour ET WDDL} = T_{d1} + T_{d2} = 46.649 \text{ ps} \quad (1)$$

$$T_{pav} \text{ pour ET QDI} = T_{d3} + T_{d4} = 166.496 \text{ ps} \quad (2)$$

Il est important de rappeler que chaque retard de propagation T_{di} dépend [Hou09] :

- De la capacité du nœud défectueux C_n.
- Des paramètres technologiques des transistors utilisés (w_i^n, L_i^n, w_i^p, L_i^P).
- De la résistance R de la ligne affectée par le défaut.

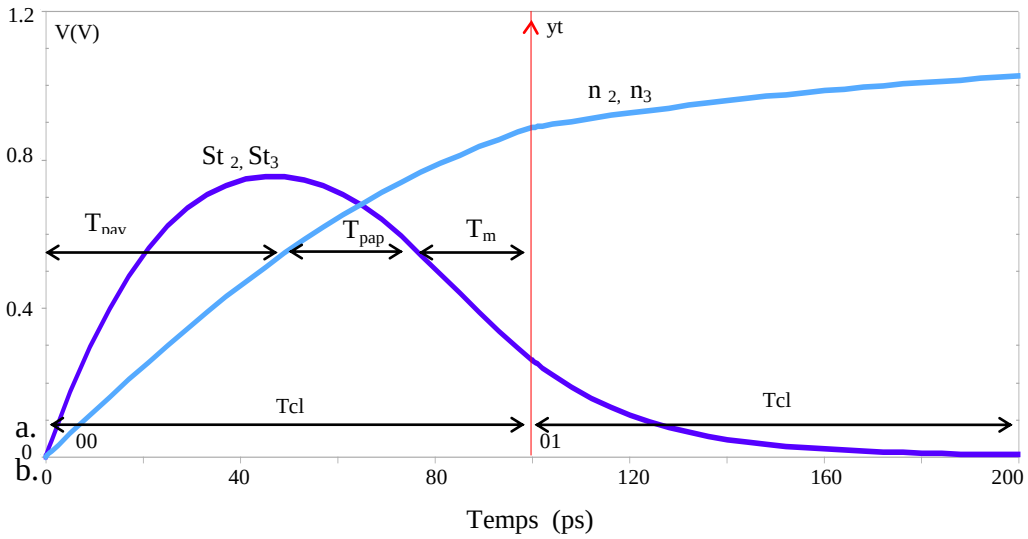
Pour la TMR à base de la porte ET WDDL, le défaut se propage jusqu'au sorties St_2 et St_3, dans une période de temps T_{pap}= 19.73ps, qui dépend du délai de propagation de portes existantes après le nœud n.

$$T_{pap} = T_{d4} = 19.73\text{ps} \quad (3)$$

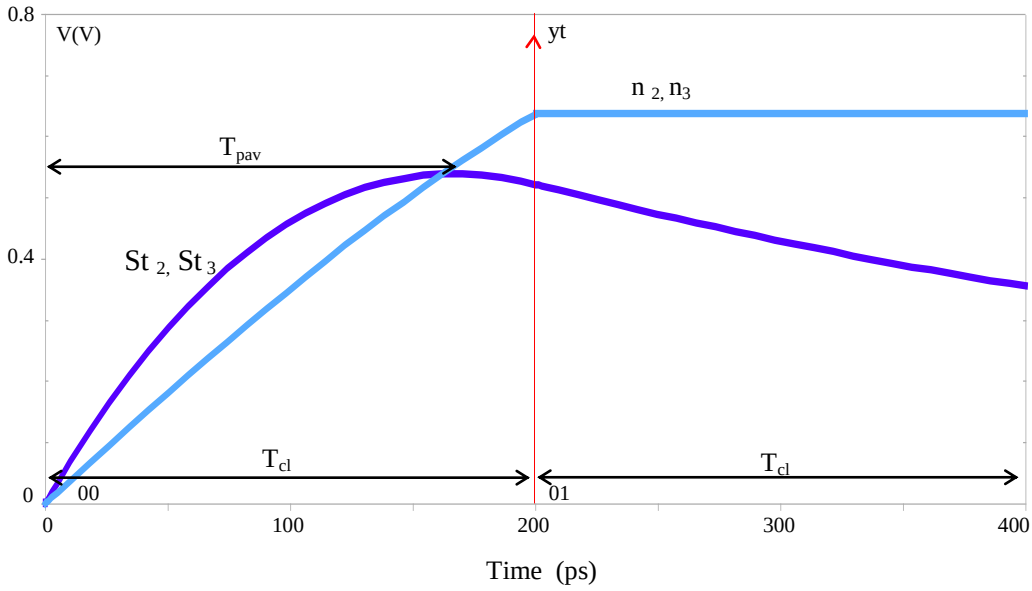
Puis la sortie St_2, St_3 reste stable pendant une période de temps T_m= 33.721ps.

Par contre dans la TMR à base de la porte ET QDI, la marge temporelle T_m n'est pas définie et donc de même pour T_{pap}, car la sortie St_2 et St_3 n'atteint jamais la tension de seuil. La sortie St des deux TMR est correcte et donc elles sont tolérantes aux deux défauts de circuit ouvert. Dans [Hou09], la relation liant les différents temps de propagation est donnée:

$$Tcl = Tpav + Tpap + Tm \quad (4)$$



a. TMR ET WDDL avec R_{CO} = 200 Ω



b. TMR à base de la porte ET QDI avec R_{CO} = 400 Ω

Figure 3.4 Comportement dynamique des TMR.

3.3 Détection et tolérance au défaut de circuit-ouvert résistif

Après avoir injecté des fautes de type circuit-ouvert résistif au niveau des TMR ET WDDL et TMR ET-QDI, nous allons observer et analyser son comportement électrique pour détecter les défauts. Nous allons vérifier si l'application d'une séquence de test à i largeurs de pulsations permettra de détecter les deux défauts résistifs.

3.3.1 Test et tolérance aux fautes avec un vecteur à une seule largeur de pulsation (PW1)

La figure 3.5 représente la simulation SPICE des deux TMR avec une séquence de test à une seule largeur de pulsation. Dans les figures 3.5.a et 3.5.b nous choisissons une résistance de défaut assez petite : R_{CO} = 2 kΩ pour la TMR ET WDDL et R_{CO} = 4kΩ pour la TMR ET QDI. L'état initial est donné par la séquence [xt yt] = [00] et la transition est créée en appliquant la séquence T1= [01]. Il apparait que la présence du circuit-ouvert ralentit la propagation du signal. Un retard additionnel est observé: T_{ad}= 16.213 ps pour $(ET\ WDDL)_2$ et $(ET\ WDDL)_3$ et T_{ad}= 7.494 ps pour $(ET\ QDI)_2$ et $(ET\ QDI)_3$. Cependant ce retard reste inférieur à la marge temporelle T_m= 16.812 ps pour $(ET\ WDDL)_2$ et $(ET\ WDDL)_3$ et T_m= 15.805ps pour $(ET\ QDI)_2$ et $(ET\ QDI)_3$. La sortie St des deux TMR est donc interprétée normalement et reste insensible à la présence des deux défauts, car les deux sorties St_2, St_3 restent correctes d'un point de vue logique. Une valeur correcte est sauvegardée dans le registre de sortie [Rod96], et les deux TMR fonctionnent correctement. En d'autres termes, les défauts sont masqués et les deux TMR sont tolérantes aux fautes.

$$T_{pav} + T_{ad} + T_{pap} < Tcl \qquad (5)$$

L'analyse de cette simulation permet donc de dire qu'un circuit-ouvert avec une petite résistance de défaut ne peut pas être détecté et les deux TMR fonctionnent correctement malgré la présence des deux défauts résistifs. Afin de faciliter la détection, il est nécessaire d'augmenter la valeur de la résistance des défauts. Nous allons nous intéresser au cas d'une résistance de défaut plus importante, R_{CO} = 5.325 kΩ pour la TMR ET WDDL et R_{CO} =5.713 kΩ pour la TMR ET QDI (Figures 3.5.c et 3.5.d). Dans ce cas, on constate que le retard additionnel T_{ad} est égal à la marge temporelle. La tension de sortie St_2, St_3 n'est pas descendue sous la valeur seuil de 0.55V lorsque survient le front d'horloge. On obtient donc une valeur 1 logique au lieu d'une valeur 0 logique. Une valeur fautive de la sortie S_t des deux TMR est capturée dans le registre de sortie et les deux défauts de circuit-ouvert peuvent être détectés ce qui permet de conclure que ces deux TMR ne sont pas tolérantes.

$$T_{pav} + T_{ad} + T_{pap} > T_{cl} \text{ pour (ET WDDL)} \qquad (6)$$

$$T_{pav} + T_{ad} + T_{pap} > T_{cl} \text{ pour (ET QDI)} \qquad (7)$$

Cela signifie qu'un circuit-ouvert résistif ne peut être détecté par une séquence de test à une largeur de pulsation [PW_1] que si et seulement si la valeur de la résistance du défaut R_{CO} est supérieure à une certaine valeur critique R_C. On associe aux deux défauts de circuit-ouvert un intervalle de détection DI associé à la séquence [PW1] défini par :

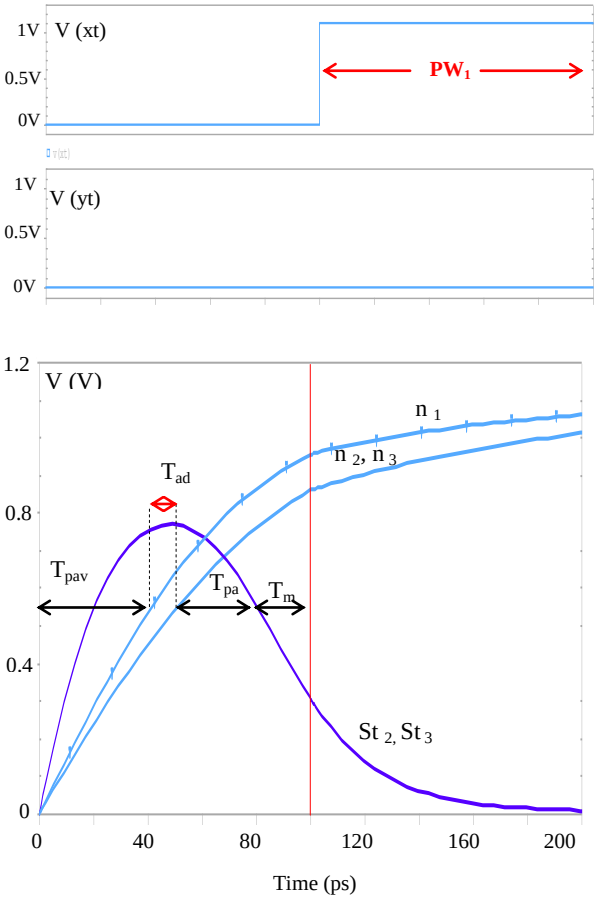
$$DI^{[PW\,1]} = [R_c^{[PW\,1]}, \infty[$$

$$DI = [R_c, \infty[= [5.325\ k\Omega, \infty[, \text{ pour TMR ET WDDL} \qquad (8)$$

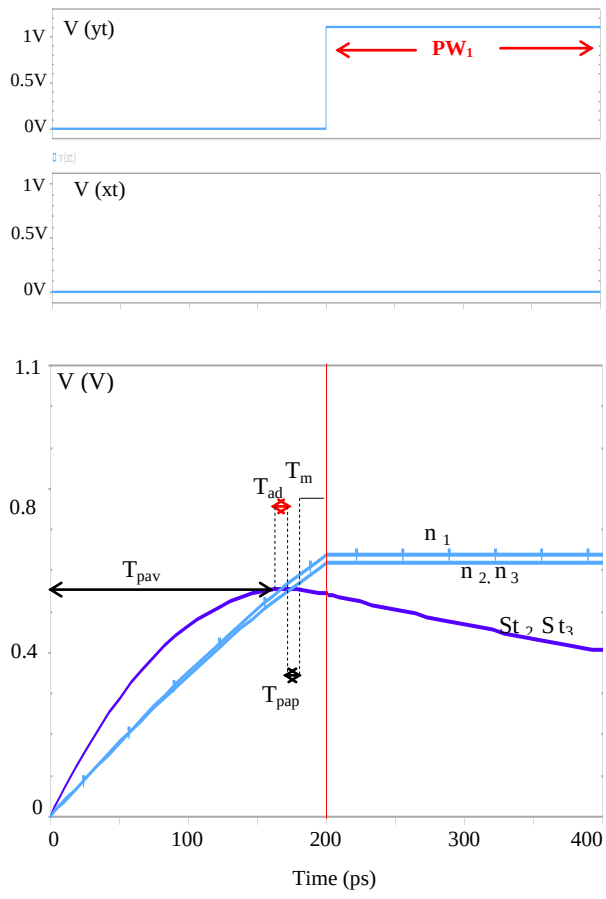
$$DI = [R_c, \infty [= [5.713\ k\Omega, \infty [, \text{ pour TMR ET QDI} \quad (9)$$

Nous constatons qu'il existe une légère différence entre les deux TMR. Ceci permet de dire que la TMR ET QDI est plus robuste que la TMR ET WDDL. Cependant, il est important de rappeler que cette valeur est associée à PW1 et qu'une autre séquence ayant une marge temporelle plus petite, pourrait détecter une résistance plus faible et donc un intervalle de tolérance plus étroit.

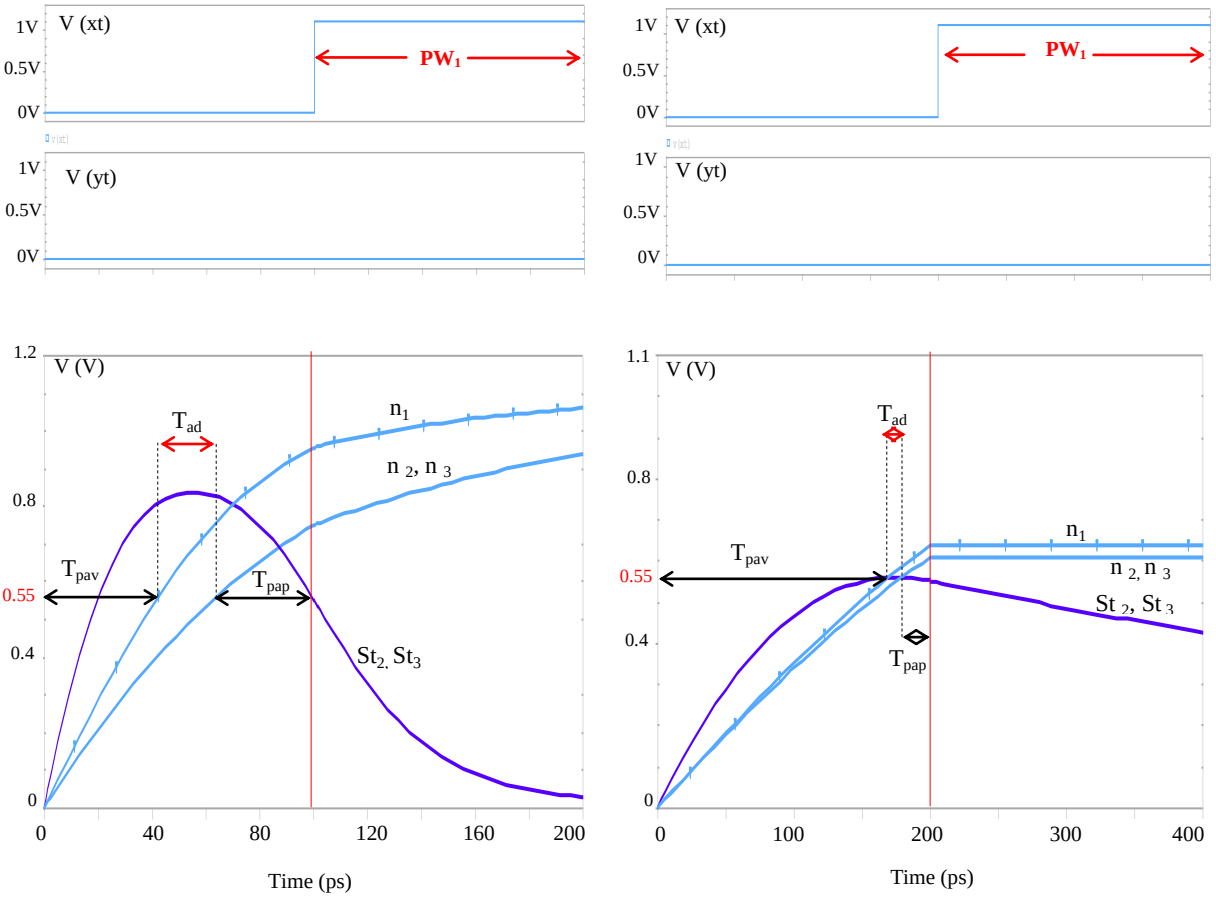
En résumé, pour $R_{CO} \in [5.325\ k\Omega, \infty [$ dans ET WDDL et pour $R_{CO} \in [5{,}713\ k\Omega, \infty [$ dans ET QDI, les deux TMR ne peuvent pas fonctionner correctement en présence des deux défauts de circuit ouvert. En d'autres termes, les deux défauts ne seront pas masqués et le voteur produit une sortie St fautive. La TMR ET WDDL et la TMR ET QDI ne sont pas tolérantes et donc elles ne sont pas fiables. Cependant, pour $R_{CO} \in [0, 5.325\ k\Omega [$ dans ET WDDL et pour $R_{CO} \in [0, 5.713\ k\Omega [$ dans ET QDI, les deux TMR fonctionnent correctement en présence des deux défauts résistifs. En effet, les deux défauts sont masqués et le voteur produit une sortie St correcte. Les deux TMR sont tolérantes aux fautes et donc elles sont fiables.



a. TMR ET WDDL avec R_{CO}=2 kΩ



b. TMR ET QDI avec R_{CO}=4 kΩ

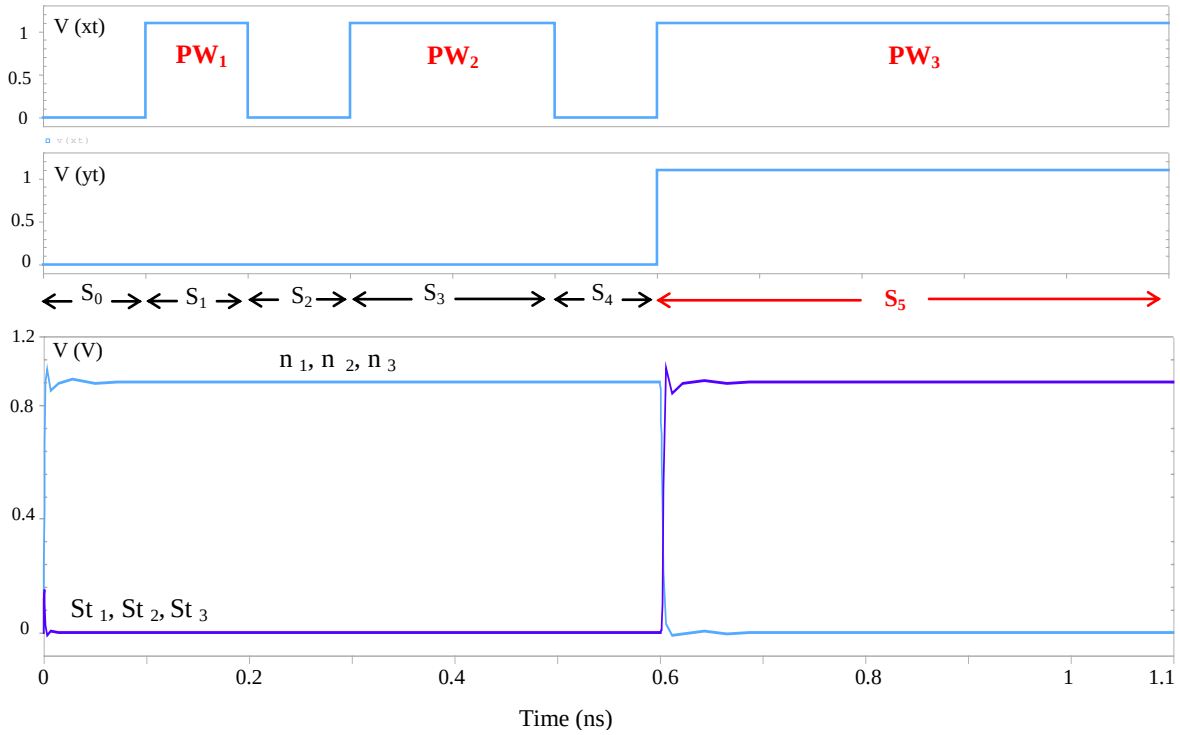


c. TMR ET WDDL avec R_{CO}= 5.329 kΩ d. TMR ET QDI avec R_{CO}= 5.713 kΩ

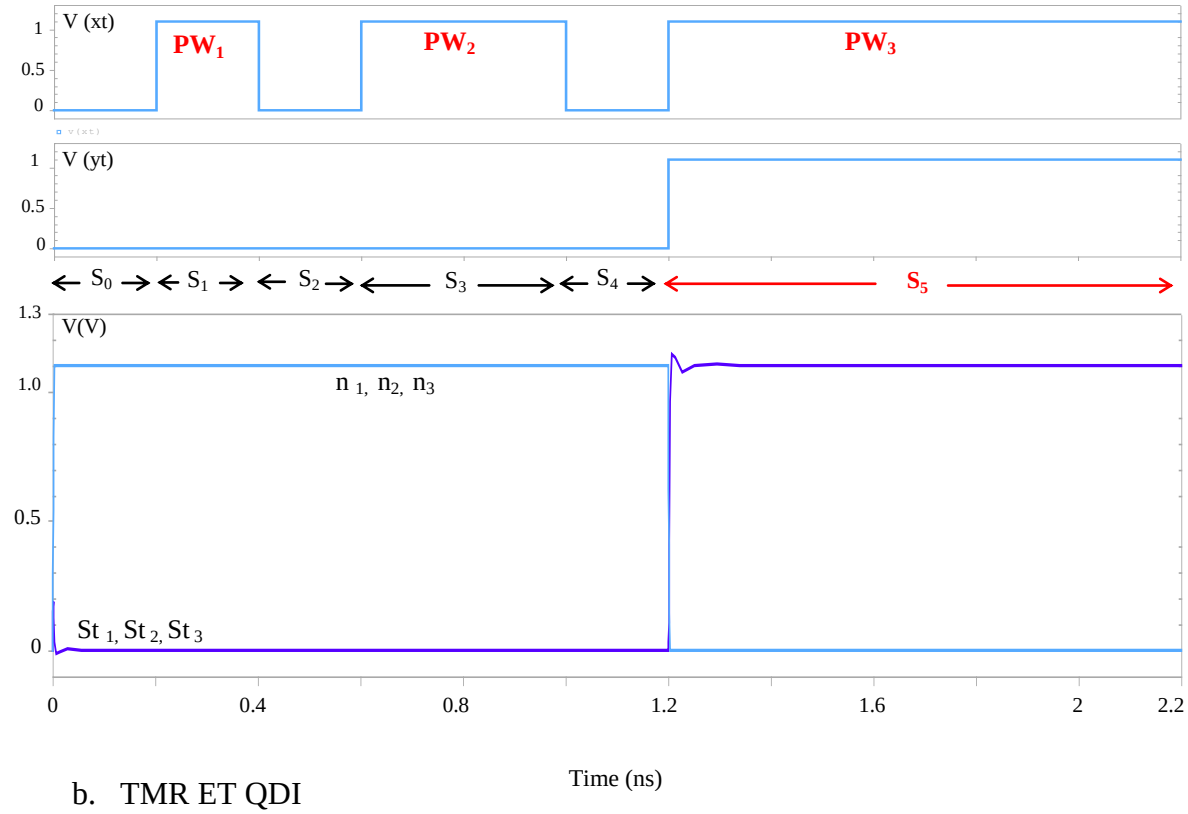
Figure 3.5 Comportement dynamique des TMR en présence de circuits ouverts résistifs.

3.3.2 Test et tolérance aux fautes avec un vecteur à i largeurs de pulsations (PWi)

Dans cette partie l'objectif est d'introduire une amélioration à la précédente technique de test avec un vecteur à une seule largeur de pulsation. Nous étudions la détection des défauts lorsque celui-ci a été testé avec une séquence de test complète. Nous avons considéré un temps de cycle d'environ T_{cl} = 0, 1 ns dans TMR ET WDDL et T_{cl} = 0, 2 ns dans TMR ET QDI. A partir d'une pulsation initiale donnée par PW1, une séquence de test complète de i pulsations est appliquée aux circuits TMR. Dans notre cas, nous essayerons de détecter les deux défauts de circuits-ouverts avec une séquence de test composée de trois largeurs de pulsations différentes [PW_1, PW_2, PW_3]. La transition créée par les pulsations [PW_1, PW_2] traverse les nœuds n_1, n_2 et n_3 et se propage à une sortie observable primaire et permet la détection des défauts. Les pulsations successives avant la pulsation PW_3 peuvent produire des transitions sur ces nœuds, mais ces transitions ne se propagent pas à une sortie primaire, c'est-à-dire que le défaut ne peut pas être détecté avant l'application de la séquence correspondant à PW_3. Le comportement dynamique des deux TMR sans défaut est présenté dans la Figure 3.6. On voit que dans le cas des TMR saines, les transitions surviennent à l'arrivée du front montant de la troisième pulsation PW_3.



a. TMR ET WDDL



b. TMR ET QDI

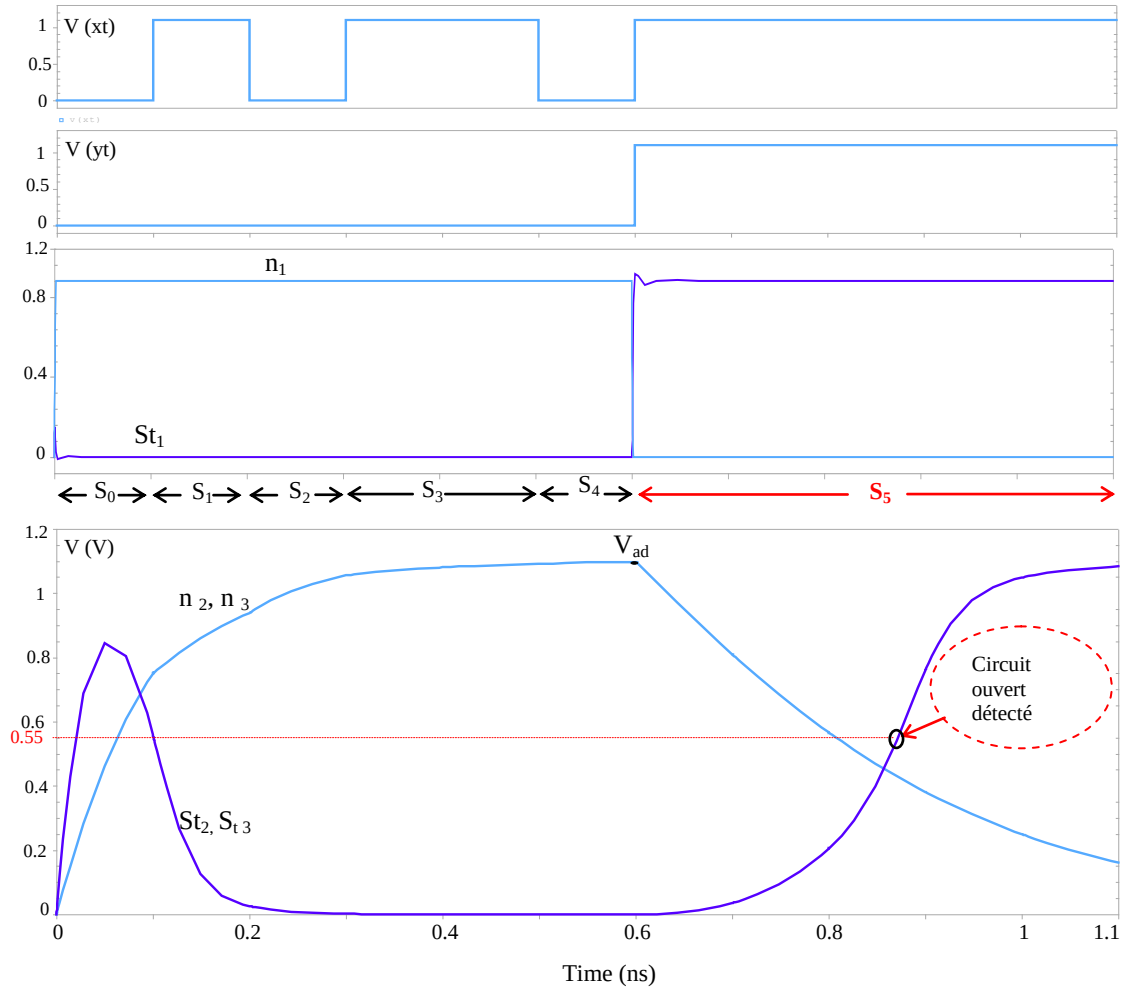
Figure 3.6 Comportement sain avec trios largeurs de pulsations (PW_3)

Les comportements des deux TMR défectueuses dans le cas de différentes résistances de défauts sont montrés à la figure 3.7. Les signaux sont ralentis par la présence des deux défauts de circuits ouverts. Dans TMR ET QDI, les défauts sont détectés au cours de PW_3. Lorsque la séquence PW_3 est appliquée, une transition se propage à partir des signaux d'entrée xt et yt jusqu'aux nœuds n_2 et n_3, cette transition est ralentie par les défauts et se propage finalement aux sorties St_2 et St_3. Les deux défauts sont détectés puisque les sorties St_2 et St_3 transitent juste après le front montant de la troisième pulsation correspondant à la séquence S_5 = [11]. La résistance critique minimale est égale à R_C = 19 kΩ dans TMR ET QDI. La tension finale de la phase avant détection (Vad) est égale à 1, 05 ≈ V_{DD}, qui constitue la meilleure condition de détection de défauts avec une résistance critique minimale [Hou09]. Le comportement dynamique associé aux résistances inférieures à 19 kΩ est insensible à la présence des deux défauts et donc les TMR sont tolérantes et fiables. Par contre, les comportements associés aux résistances supérieures à 19 kΩ sont très sensibles à la présence de défauts. En d'autres termes, on voit que les nœuds défectueux n_2 et n_3 ne sont observables que sur les signaux de sortie St_2 et St_3. Par conséquent, une erreur logique et un dysfonctionnement sont observés aux sorties St_2 et St_3 pendant la séquence S_5 = [11]. La séquence de test à trois largeurs de pulsations (PW_3) conduit à l'obtention d'une résistance critique supérieure à celle obtenue avec la séquence de test à une seule pulsation (PW_1). Cette observation avec trois largeurs de pulsations a permis de mettre en évidence une technique simple qui implique de trouver des intervalles de tolérance plus larges et donc d'accroître la fiabilité. Dans la TMR ET WDDL, la valeur de la résistance critique dépend également des pulsations appliquées car les défauts sont détectés par la troisième pulsation (PW_3) correspondant à la séquence S_5. La valeur de la résistance critique minimale trouvée est égale à 8,75 kΩ. Le potentiel Vad est égal à 1, 1 V = V_{DD}. Il est également montré que la valeur R_C est inférieure à celle trouvée dans TMD ET QDI, ce qui démontre une fois de plus que TMR ET QDI est plus robuste que TMR ET WDDL.

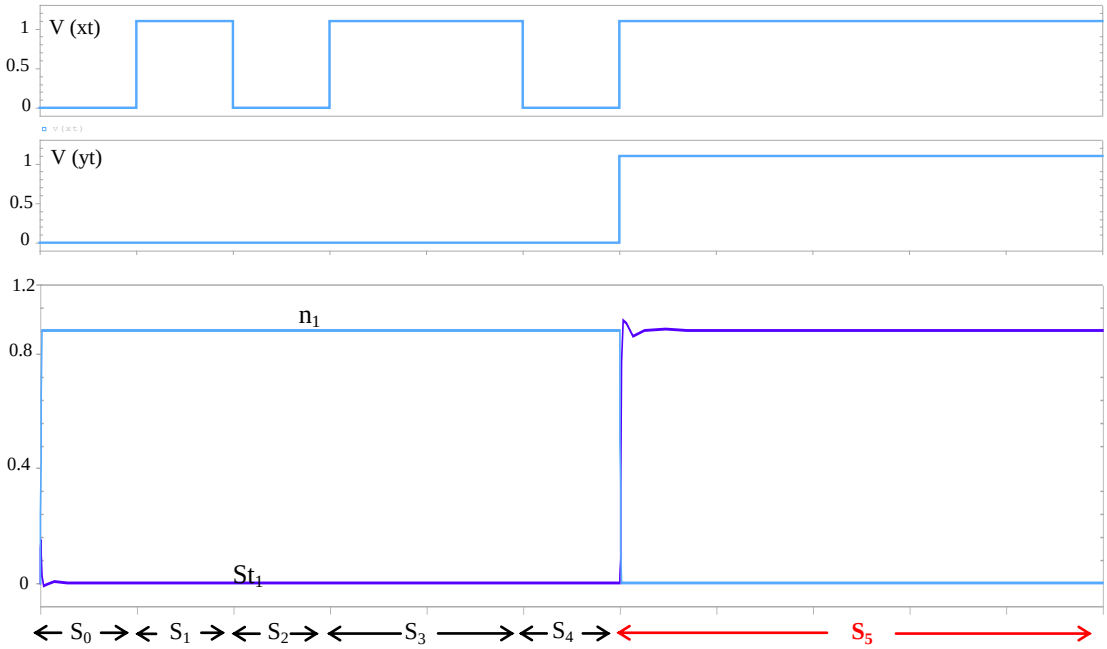
L'intervalle de détection (DI) et l'intervalle de tolérance (TI) sont définis ci-dessous:

$$DI_{TMR\ ET\ WDDL}^{\{PW_1, PW_2, PW_3\}} = DI^{\{PW_1\}} = [R_c^{\{PW_1, PW_2, PW_3\}}, \infty[= [8{,}75\ k\Omega, \infty[\Longrightarrow TI = [0, 8{,}75\ k\Omega[$$

$$DI_{TMR\ ET\ QDI}^{\{PW_1, PW_2, PW_3\}} = [R_c^{\{PW_1, PW_2, PW_3\}}[= [19\ k\Omega, \infty[\Longrightarrow\ TI = [0, 19\ k\Omega\ [$$


V (xt)
V (yt)
n1
St1
S0 S1 S2 S3 S4 S5
V (V)
Vad
n 2, n 3
St2, St 3
0.55
Circuit
ouvert
détecté
Time (ns)

a. TMR ET WDDL


V (xt)
V (yt)
n1
St1
S0 S1 S2 S3 S4 S5

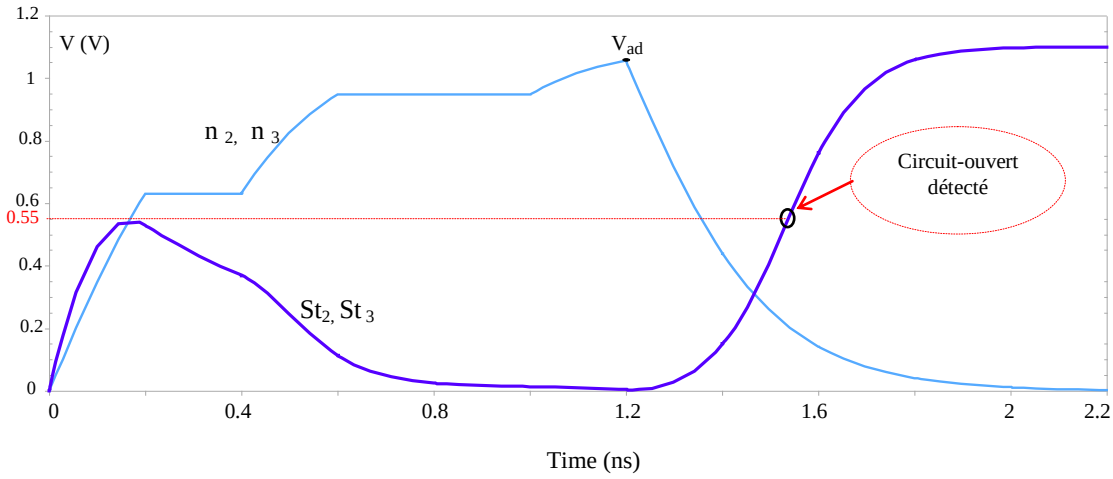


Figure 3.7 Comportement fautif avec trios largeurs de pulsations (PW_3)

3.4 Analyse électrique de l'impact du court-circuit résistif

Dans cette partie nous nous intéressons à l'étude de l'impact du court-circuit résistif sur les deux TMR à base des portes ET WDDL et ET-QDI. Le test a été limité à l'analyse des interconnexions avec le modèle RC. La capacité de couplage entre les interconnexions et les effets inductifs ont été négligés.

3.4.1 Analyse statique de l'effet de défaut de court-circuit résistif

Pour analyser l'impact du défaut de court-circuit sur le comportement statique des deux TMR, nous suivons la procédure illustrée sur la Figure 3.8. Dans un premier temps, nous injectons les deux défauts de court-circuit entre les lignes d'interconnexions St et Sf des modules 2 et 3, comme illustré par la Figure 3.9. Dans un second temps, nous comparons le comportement résultant au comportement du module 1 sans défaut afin de caractériser ses effets.

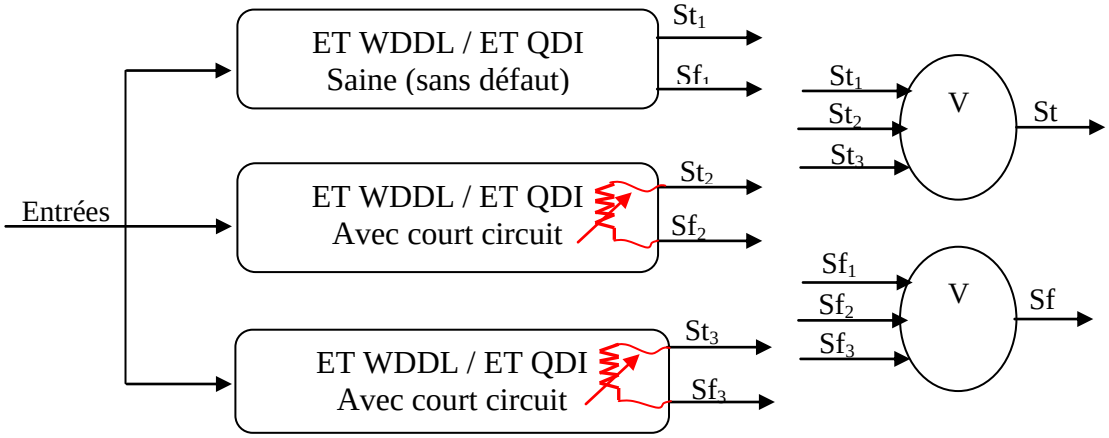


Figure 3.8 Injection de court-circuit résistif dans la TMR.

Les portes (ET WDDL) $_2$/ (ET WDDL) $_3$ et (ET-QDI) $_2$ / (ET-QDI) $_3$ de la Figure 3.9 sont affectées par un court-circuit résistif. Les interconnexions St et Sf sont court-circuitées et on suppose que la tension de seuil (V_{TS}) des deux portes 3OR est la même ($V_{TS} = V_{DD} / 2 = 0.55V$). Le court-circuit est représenté par la résistance R_{CC} dont la valeur est inconnue puisque dépendante de paramètres aléatoires tels que la topologie ou le matériau utilisé. Pour garantir la détection de ce défaut, son comportement électrique doit être analysé pour déterminer les conditions optimales de détection et de tolérance. L'impact d'un court-circuit résistif est tel que chaque nœud tente d'imposer sa valeur logique à l'autre. Lorsque le défaut est injecté entre deux nœuds qui sont au même niveau logique, les deux transitions sont dans la même direction, dans ce cas la présence du défaut de court-circuit résistif ne perturbe pas le fonctionnement des deux TMR. Il nous faut donc injecter le défaut entre deux nœuds de niveau logique différent. Deux séquences [1100] et [0011] sont appliquées successivement sur les entrées [xt yt xf yf] des deux TMR et nous observons leur comportement pour cinq valeurs discrètes de la résistance R_{CC}: 10 Ω, 100 Ω, 10 kΩ, 100 kΩ, 1000 kΩ (Figure 3.10).

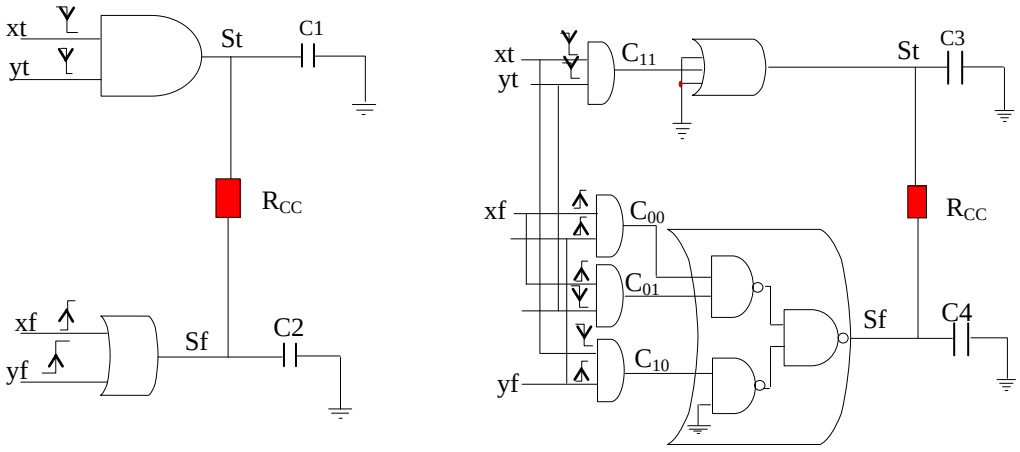


Figure 3.9 Portes sécurisées avec un défaut de court-circuitrésistif.

On voit que, le courant consommé est plus important dans le cas de la TMR ET WDDL, au fur et à mesure que la résistance du défaut diminue et les pics de consommation de courant ne sont plus équilibrés. Dans le module 1 sans défaut, Si $R_{CC} \in]$ 100 KΩ, ∞ [, un niveau de la tension de port de sortie V(Sf) $_1$devient élevé lorsque la transition est appliquée au niveau des entrées, tandis qu'un niveau de la tension de port de sortie V(St) $_1$ devient faible. Dans les modules 2 et 3 défectueux, les niveaux de ports de sortie, V(St) $_2$ et V(St) $_3$, deviennent faibles et des niveaux de sortie, V(Sf) $_2$ et V(Sf) $_3$, deviennent élevés lorsque la transition est appliquée au niveau des entrées. Ces niveaux de tension, V(St) et V(Sf), sont les mêmes dans les deux cas de sans défaut et de conditions des défauts de courts circuits résistifs. Par conséquent, les deux TMR fonctionnent correctement et les deux défauts ne sont pas détectés. La TMR à base de ET WDDL et la TMR à base de ET QDI sont tolérantes et donc fiables.

Il est important de noter que dans ce cas, les pics de courant de consommation sont presque les mêmes quelle que soit la transition effectuée par St_2, St_3, Sf_2 et Sf_3. Ainsi, les signaux de sorties sont indépendants des données appliquées à ses entrées, par conséquent la sécurité est maintenue et les TMR sont à l'abri des attaques par analyse de consommation

Si Rbr ∈] 100Ω, 100 kΩ], les deux TMR fonctionnent correctement. Avec la diminution de R_{CC}, les niveaux de tension, V (St) $_2$, V (St) $_3$ et V (Sf) $_2$, V (Sf) $_3$, se déplacent dans le sens opposé à V(St) $_1$ et V (Sf) $_1$, mais ils sont respectivement au-dessous et au-dessus de la tension de seuil, et ils sont donc toujours interprétés comme les valeurs logiques 0 respectivement 1. Donc, les tensions V(St) et V (Sf) sont les mêmes dans les deux cas considérés. Les défauts ne sont pas détectés et donc la TMR ET WDDL et la TMR ET QDI sont tolérantes et fiables. Cependant, le courant de consommation est déséquilibré. En effet, le courant I_{dd} n'est pas le même pour chaque changement d'entrée et il exploite très clairement la différence quand les sorties St_2, St_3 et Sf $_2$, Sf $_3$ changent d'état de 0 à 1 et de 1 à 0, comme le montre la Figure 3.9. L'ensemble des informations sur l'état de la sortie est visible à travers I_{dd}. Par conséquent, les deux TMR perdent leur sécurité contre les attaques par analyse de consommation.

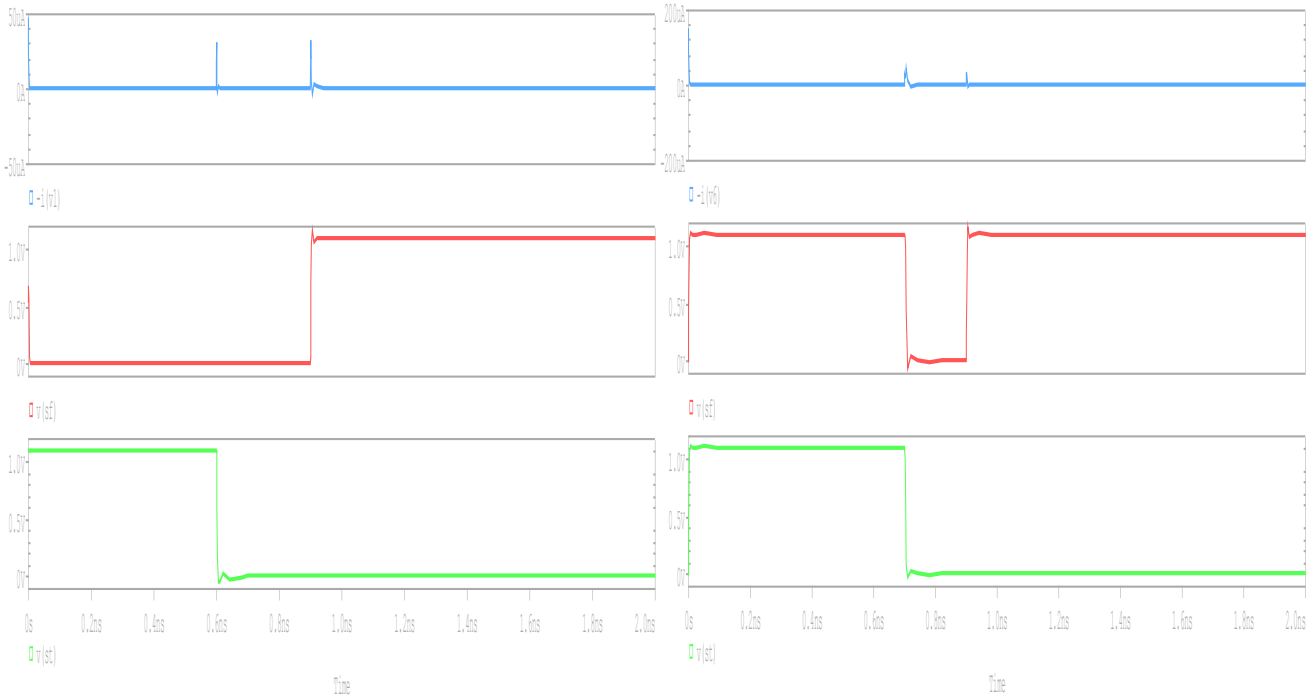
Si $R_{CC} \in [0, 100\ \Omega]$, on voit que le court-circuit est excité et provoque des effets fautifs et les deux TMR sont défectueuses. Là aussi, avec la diminution de R_{CC}, une tension de faible niveau apparaît à la sortie Sf $_2$, Sf $_3$ au lieu d'une tension de haut niveau et une tension de haut niveau apparaît à la sortie St $_2$, St $_3$ au lieu d'une tension de bas niveau. A titre d'exemple pour $R_{CC} = 100\ \Omega$, V(St) $_2$, V(St) $_3$ et V(Sf) $_2$, V(Sf) $_3$ ont une tension intermédiaire identique qui est égale à la tension de seuil. Par conséquent, V(St) $_2$ et V(St) $_3$ sont interprétées comme étant la valeur logique de 1 et V(Sf) $_2$, V(Sf) $_3$ comme étant la valeur logique de 0. La présence des deux défauts de court-circuit résistif produit dans ce cas une erreur logique.

Comme on le voit sur la Figure 3.10 la valeur de la résistance influe sur la détection des défauts. Le défaut est facilement détectable pour les valeurs de résistances faibles ($R_{CC} = 10\ \Omega$). La valeur de résistance maximale mise en évidence est de l'ordre de 100 Ω. Par ailleurs, les deux défauts de courts circuits résistifs ont également déséquilibré les profils de consommation des deux TMR fautives et les rend dépendants des données manipulées. Par conséquent, les deux TMR deviennent non sécurisées contre les attaques par analyse de consommation. Ceci permet d'affirmer qu'un court-circuit résistif peut être détecté par une séquence à deux vecteurs de test si et seulement si $R_{CC} \leq 100\ \Omega$. On peut associer à la valeur fautive (0/1 ou 1/0) un intervalle de détectabilité (DI), pour lequel les deux défauts sont détectés, et un intervalle de tolérance (TI) pour lequel les défauts sont tolérés.

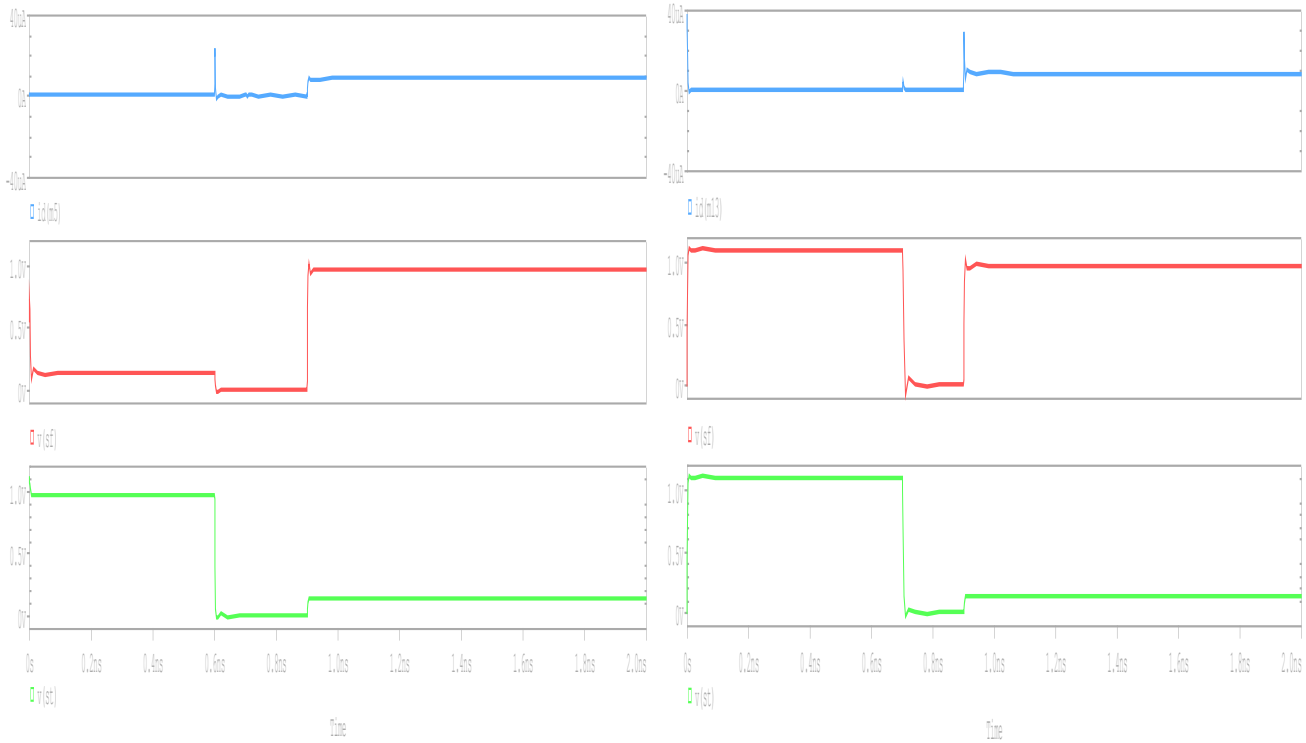
$$DI =]\ 0, R_C] =]\ 0, 100\ \Omega] \implies TI =]\ R_C, \infty\ [=]\ 100\ \Omega, \infty\ [$$

En résumé, pour $R_{CC} \in]\ 0, 100\ \Omega]$, les deux TMR ne peuvent pas fonctionner correctement en présence de deux défauts de courts circuits résistifs. Les deux défauts ne seront pas masqués et le voteur produit une sortie fautive. Pour $R_{CC} \in]\ 100\ \Omega, 100\ k\ \Omega]$, les deux TMR

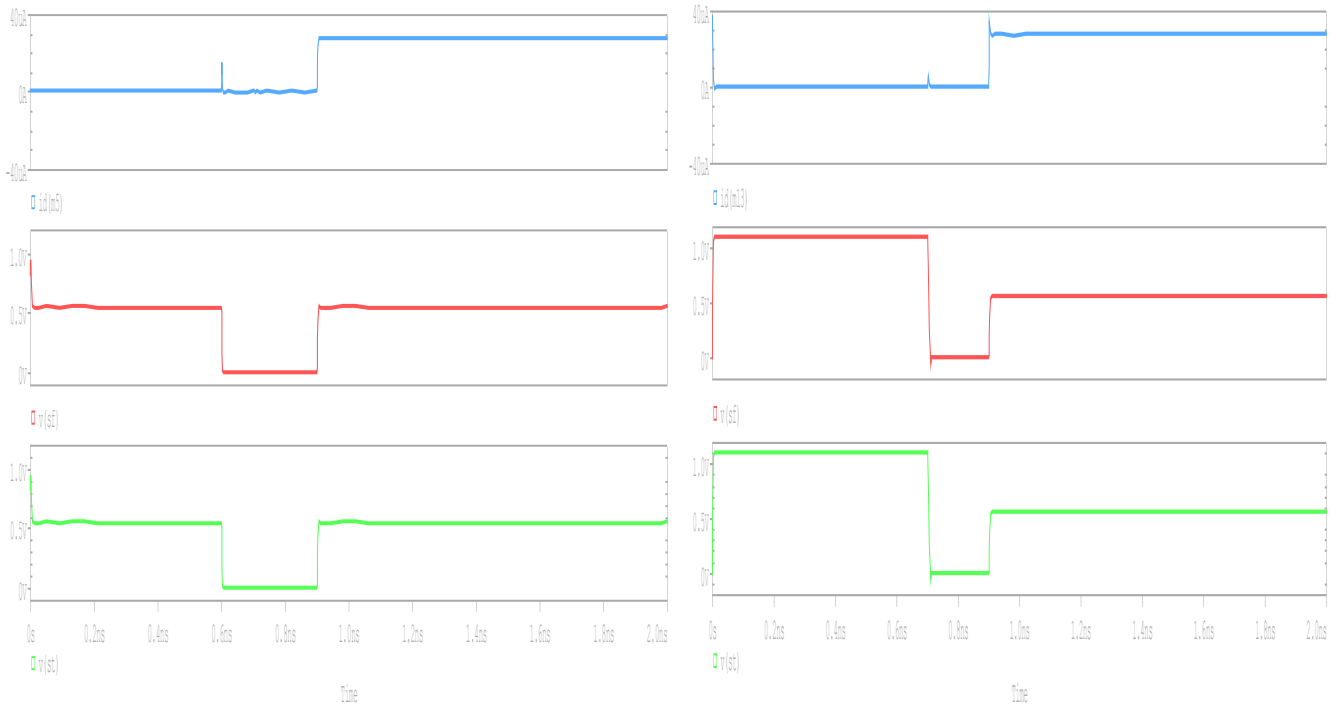
fonctionnent correctement mais elles ont perdu leur sécurité. Cependant, pour $R_{CC} \in]$ 100 kΩ, ∞ [, les deux TMR fonctionnent correctement en présence de deux défauts de court-circuit résistif. Elles sont dites sont sécurisées, tolérantes aux fautes et donc fiables. Les deux défauts de courts circuits résistifs sont masqués et le voteur produit une sortie correcte.



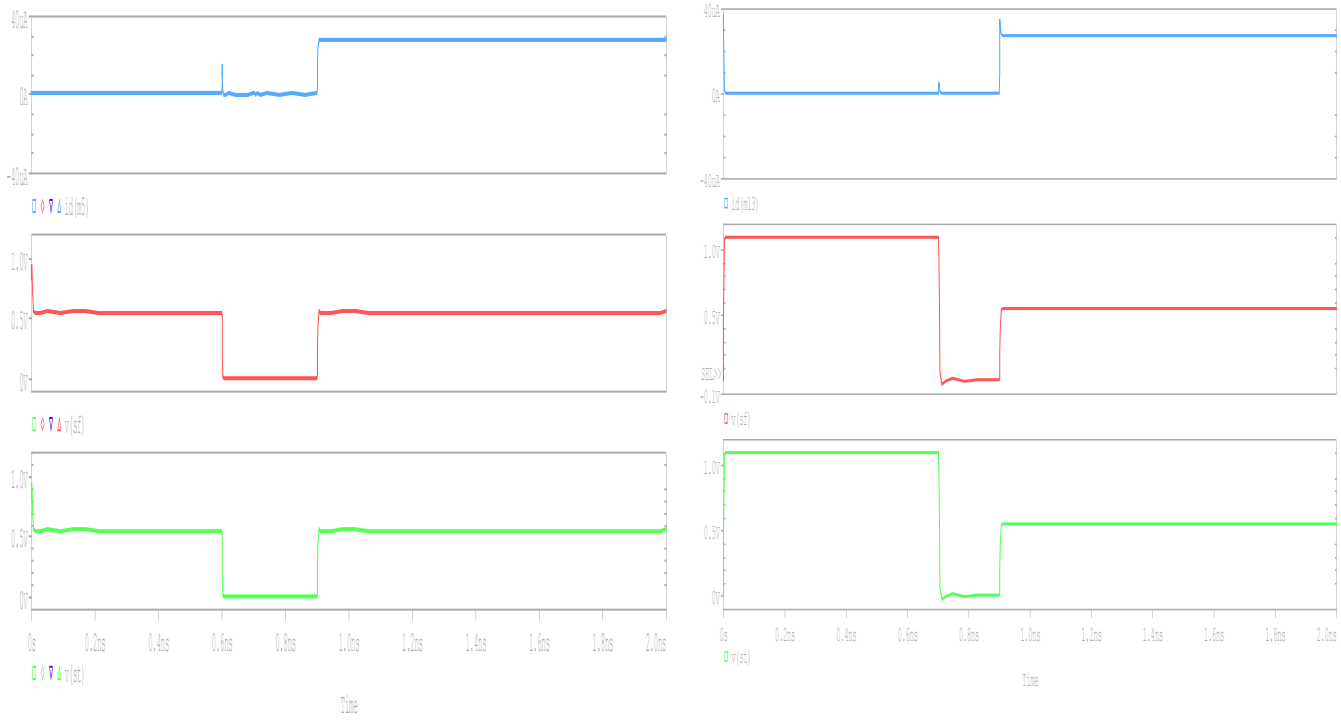
R= 1000 kΩ



R= 100 kΩ



R= 100 Ω



R= 10 Ω

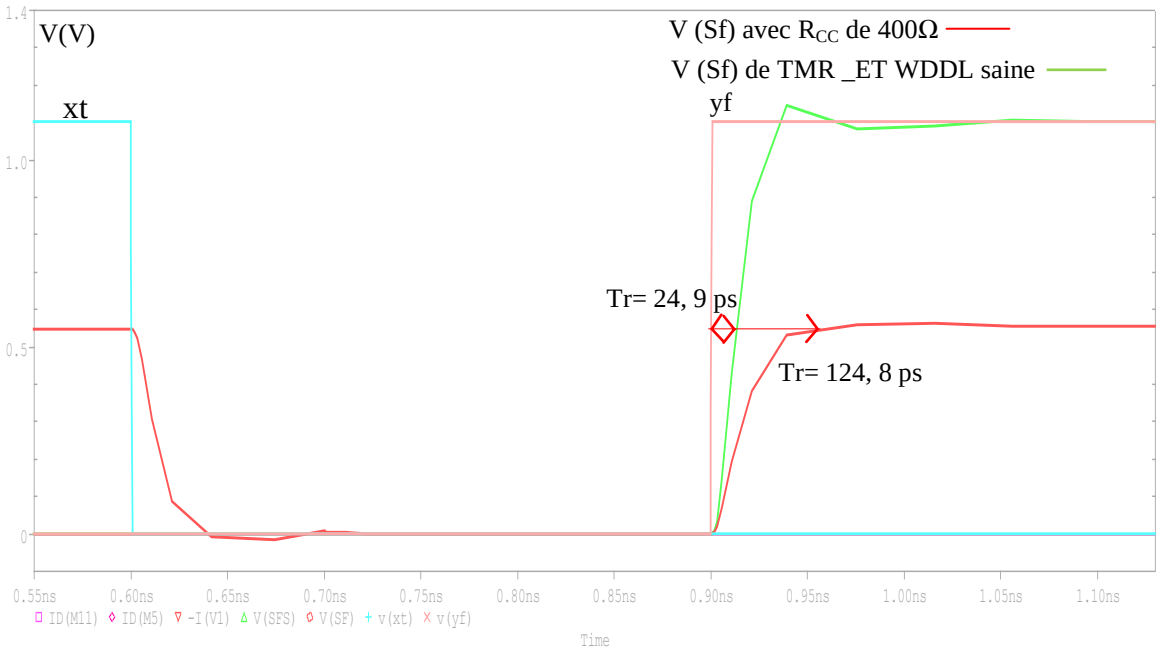
Figure 3.10 Réponse statique des TMR en fonction de la résistance du défaut.

3.4.2-Influence du court- circuit résistif sur le comportement dynamique des portes

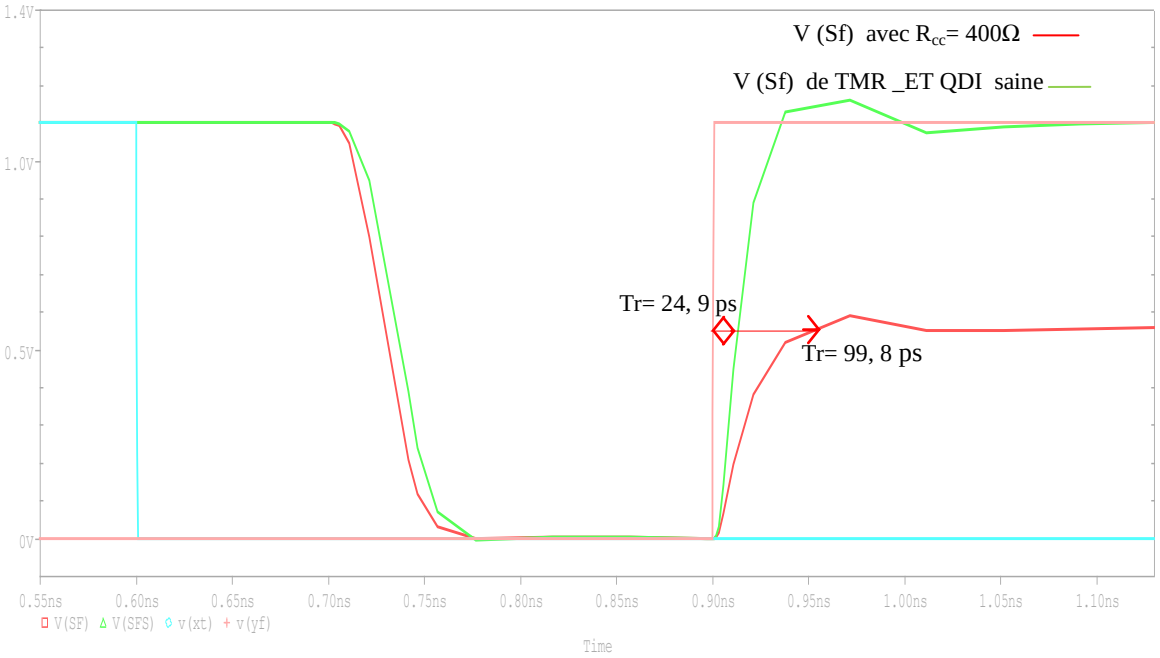
Le défaut de court-circuit résistif peut également changer le comportement dynamique du circuit par l'augmentation des retards de propagation. Intéressons-nous, à présent, au comportement dynamique des TMR affectées par deux défauts de courts-circuits résistifs. Nous appliquons successivement les séquences [1100] et [0011] sur les entrées des portes de la figure 3.7. La figure 3.11 montre que les effets des défauts sont similaires pour les deux TMR. Cependant, les deux séquences de test créent des conditions défavorables pour la transition sur Sf et donc un rallongement de ce signal, ce qui augmente le retard de propagation. Le retard mesuré pour les deux TMR saines est de 24.9 ps. Par contre, en présence de deux défauts de courts-circuits résistifs de 400 Ω, le retard est respectivement de 124,8 ps pour la TMR ET WDDL et de 99,8 ps pour la TMR ET QDI.

Analysons avec précision l'influence de la valeur de la résistance du court-circuit. Logiquement, plus la résistance du court-circuit est faible et plus son impact sur le comportement du circuit est important.

.



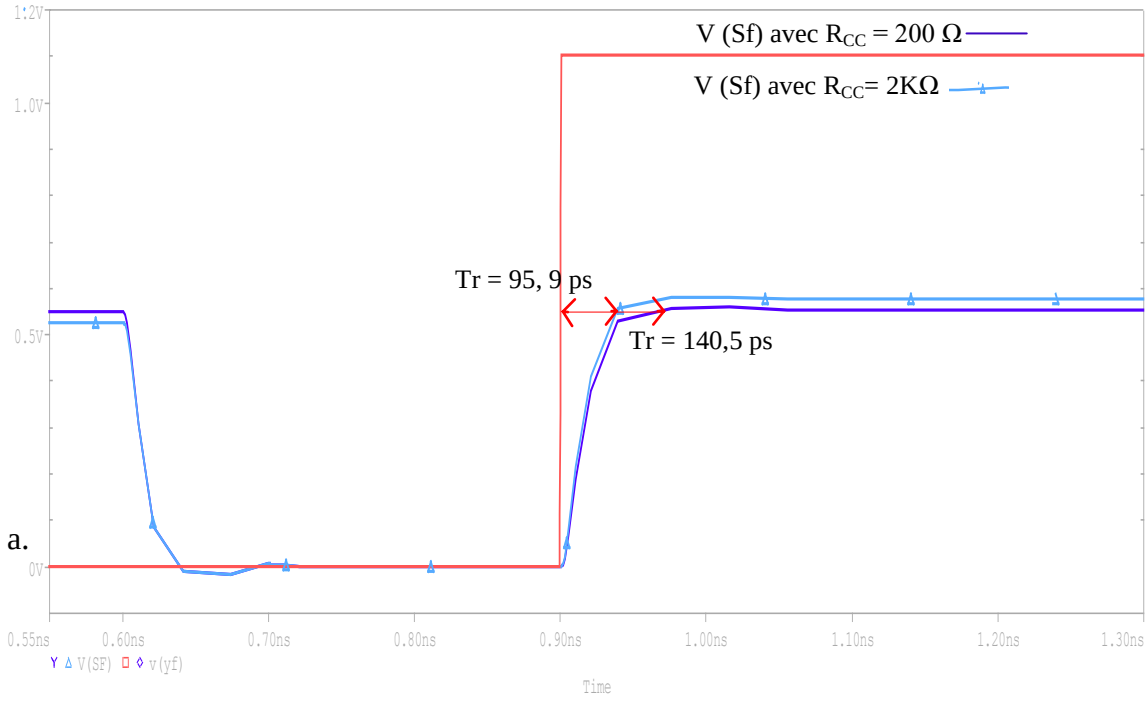
a. TMR ET WDDL



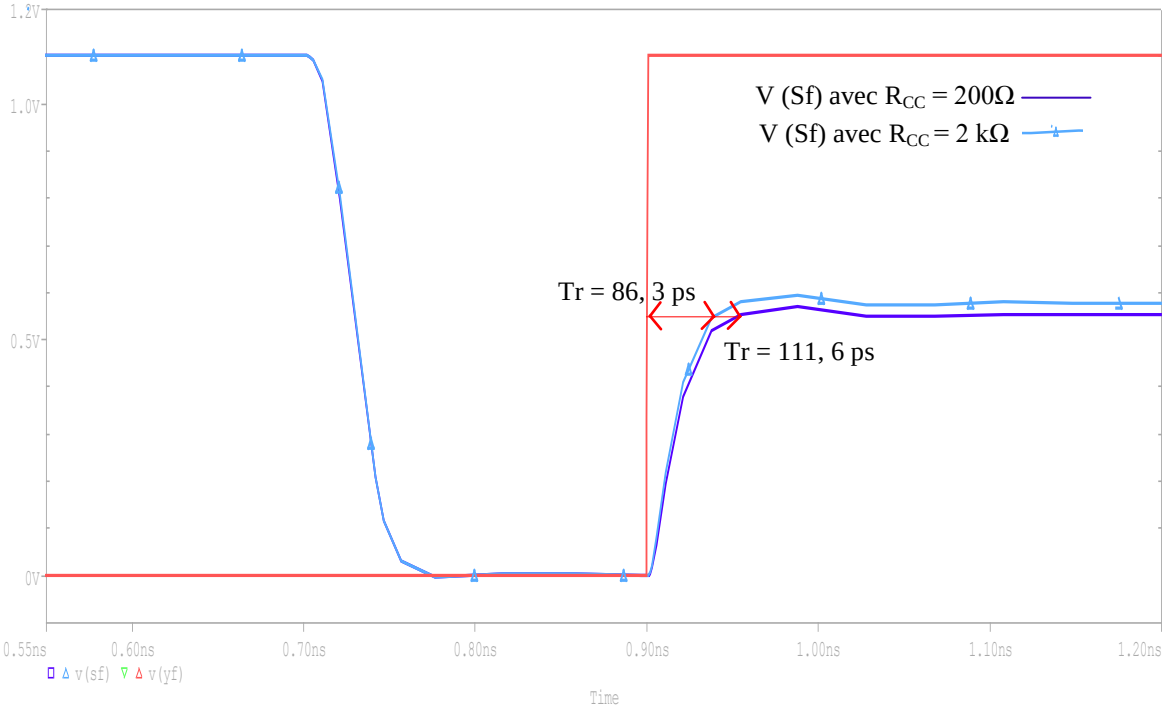
b. TMR ET QDI

Figure 3.11 Retard mesuré en fonction de R_{CC}.

Les résistances des nœuds d'interconnexion court-circuités sont typiquement en dessous de 500 Ω [21], mais les mesures faites sur le processus de contrôle de défauts des plaquettes wafers rapportent aussi de petits pourcentages dans la gamme de 500 Ω à 20 kΩ. En fait, par rapport à l'impédance d'entrée d'un transistor MOS, 500 Ω est très bas et 20 kΩ est trop élevé. Les travaux de Hawkins [Haw22] ont montré également que les valeurs de résistance de court-circuit résistif s'étendent de 800 Ω à 4.7 kΩ. Pour nous assurer que notre évaluation du défaut est représentative pour la gamme complète de la résistance de court circuit, nous avons choisi deux valeurs 200 Ω et 2 kΩ pour la résistance. La figure 3.12 montre que pour R_{CC} = 200 Ω, le délai créé sur la ligne Sf est de 140,5 ps pour la TMR ET WDDL et de 111.6 ps pour la TMR ET-QDI. Tandis que pour R_{CC} = 2 kΩ, le délai est de 95,9 ps pour la TMR ET WDDL et de 86.3 ps pour la TMR ET-QDI. En conclusion nous pouvons dire que le délai mesuré au niveau la TMR ET WDDL est plus significatif. Ainsi, ceci permet d'affirmer encore que la TMR ET QDI est plus robuste que la TMR ET WDDL.



a. TMR ET WDDL

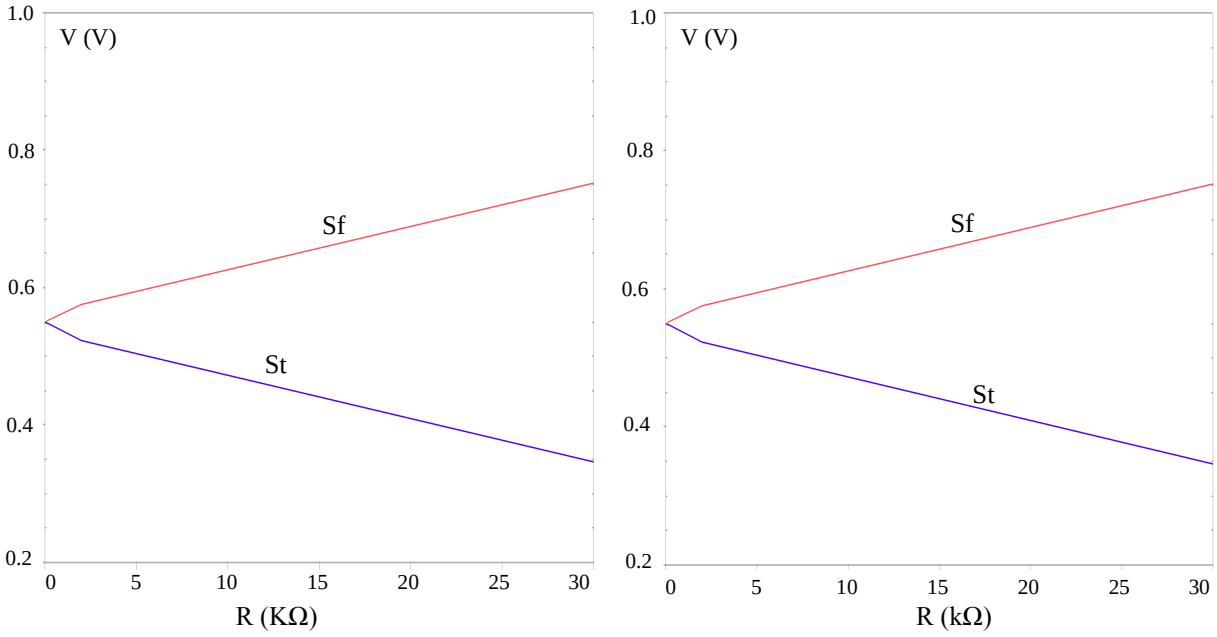


b. TMR ET QDI

Figure 3.12 Délai en fonction de R_{CC}.

3.5 Comparaison entre TMR ET WDDL et TMR ET-QDI

Les figures 3.13 et 3.14 représentent la variation des tensions V(St) et V(Sf), en fonction de la résistance R_{CC} et la variation du courant d'alimentation pour les deux TMR. On remarque que les deux cellules présentent un comportement similaire. On peut donc conclure que les TMR à base de circuits WDDL et QDI peuvent être testées avec des modèles de courts-circuits résistifs semblables à ceux utilisés pour les portes CMOS standard. La Figure 3.14 montre que la TMR en logique QDI consomme moins de courant que la TMR en logique WDDL, ce qui représente une certaine forme de protection et de tolérance pour les circuits sécurisés car les consommations de courant seront plus difficiles à observer pour un attaquant. C'est pourquoi dans ce qui suit, nous allons nous intéresser aux protocoles de communications des circuits QDI et nous allons analyser l'impact des ces défauts sur une structure TMR à base de circuits QDI plus complexes.



a. TMR ET WDDL b. TMR ET QDI

Figure 3.13 Les tensions de sortie en fonction de la résistance R_{CC}.

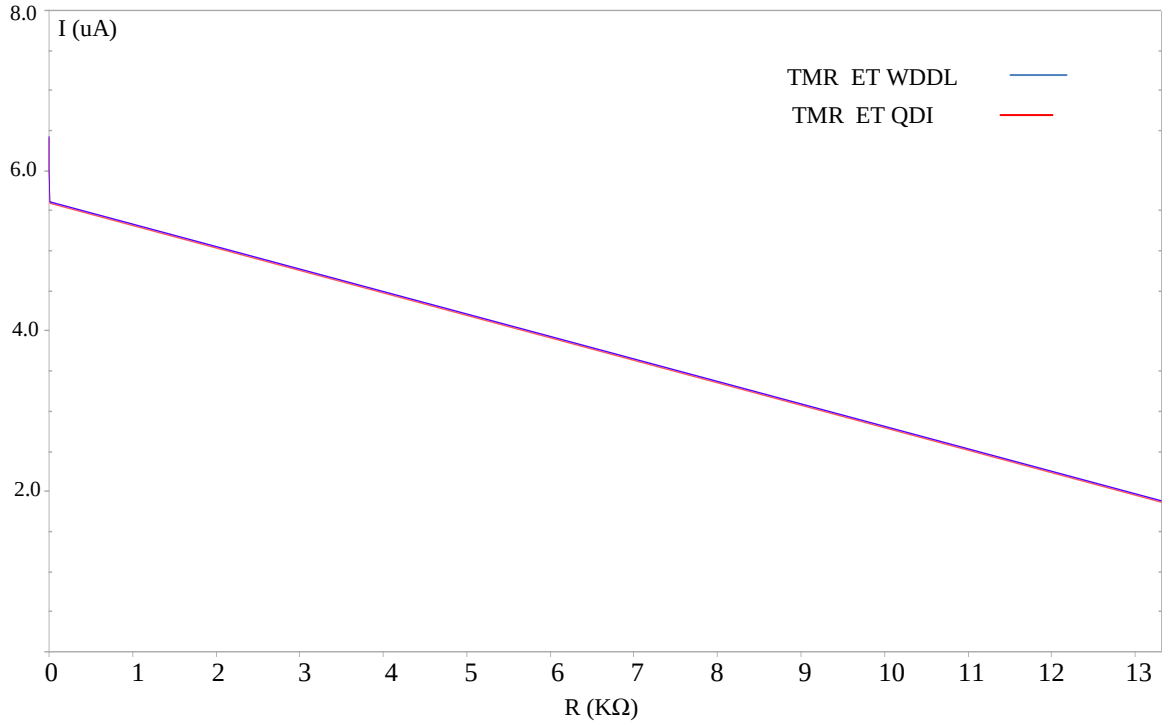


Figure 3.14 Consommation de courant en fonction de R_{CC}.

3.6 Influence du défaut de circuit-ouvert sur le comportement électrique de full buffer

Nous allons analyser l'impact des deux défauts de circuits-ouverts sur le comportement d'une structure TMR à base de registre complet asynchrone tout en prenant en compte les protocoles de communication (requête et acquittement).

3.6.1 Demi-registre asynchrone

La figure 3.15 représente un demi-registre asynchrone double rail. Les signaux d'acquittement E^{acq} et S^{acq} sont actifs au niveau bas et les canaux utilisent un codage « 1-parmi-N ». La figure 3.16 représente les résultats de simulation Spice de la réponse transitoire du demi-registre. On voit bien qu'après le signal de reset, tous les rails de données sont au niveau bas et les rails d'acquittement sont au niveau haut. Quand la donnée arrive, l'un des rails d'entrée (E0 ou E1) passe au niveau haut. La sortie de la porte de Muller correspondante (S0 ou S1) passe à 1, faisant passer E^{acq}. à 0. Ensuite S^{acq} passe à 0, accusant réception de la donnée. A l'entrée, l'environnement réagit par la remise à zéro des rails de données, .et en sortie les rails de sortie sont remis à l'état initial.

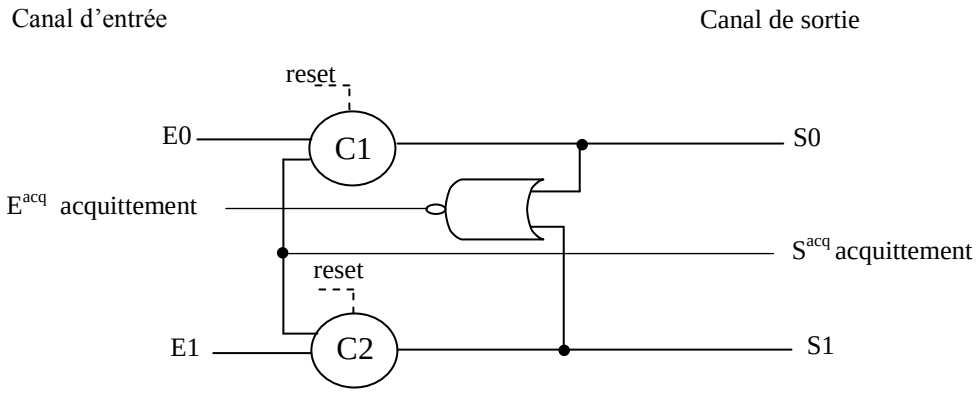


Figure 3.15 Implémentation du demi-registre double rails.

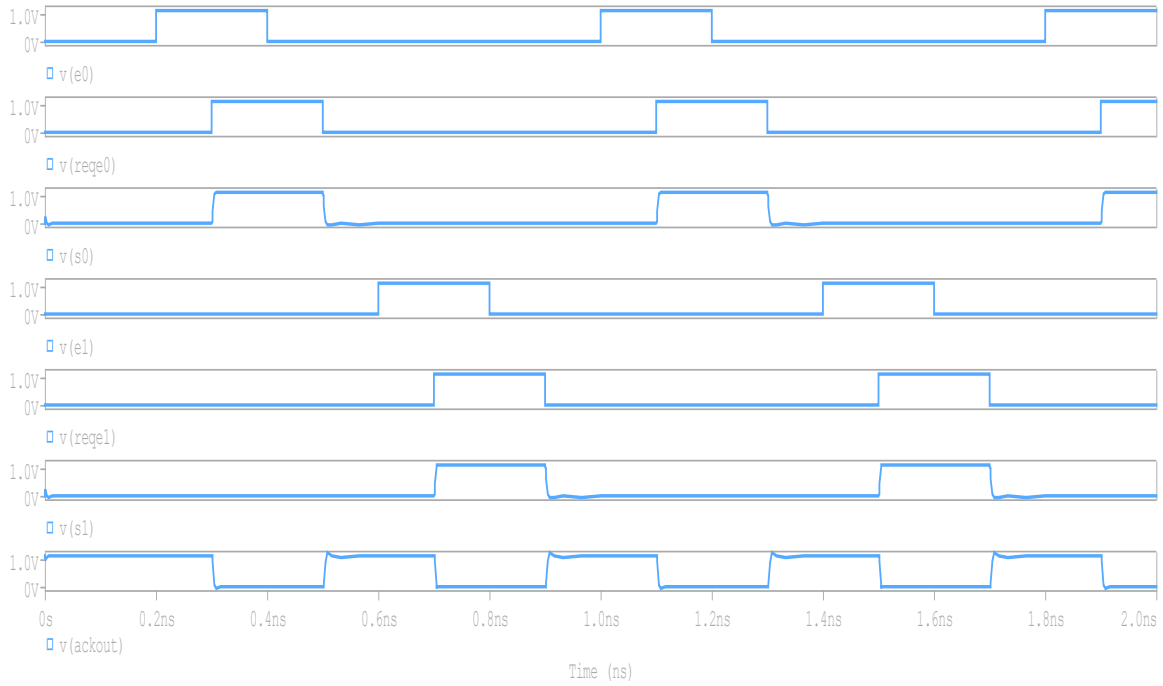


Figure 3.16 Simulation du demi-registre.

3.6.2 Architecture du registre complet

La figure 3.17 représente le dispositif d'un registre complet constitué de deux demi-registres double-rails [Raz11]. Ce registre complet possède trois canaux de communication. L'environnement d'entrée est supposé lent et émet une seule requête. Par contre, l'environnement de sortie est rapide et il accepte toutes les requêtes transmises par le registre. Les données présentes sur le canal d'entrée doivent être réémises dans l'ordre d'arrivée et sans dégradation sur le canal de sortie.

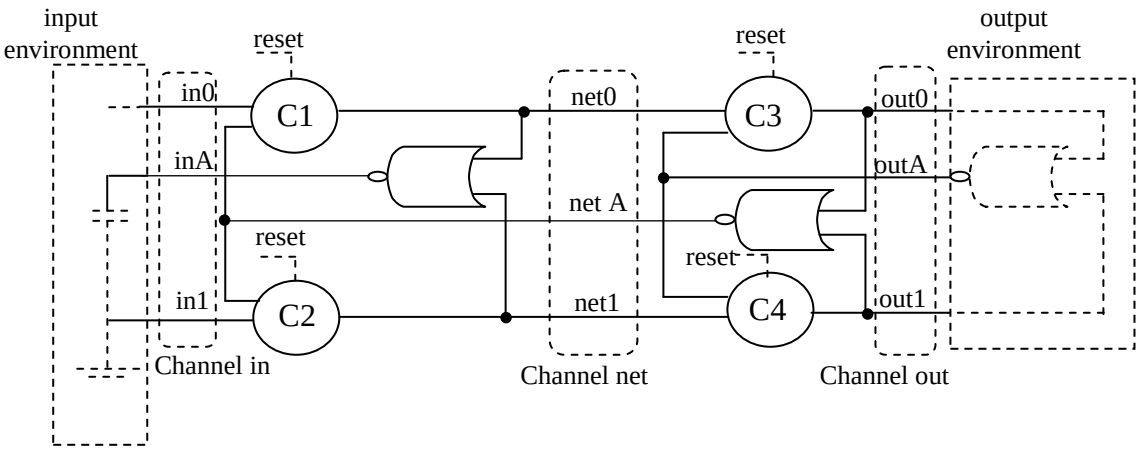


Figure 3.17 Dispositif du registre complet double rails.

Lorsque les conditions de fonctionnement normal sont respectées, un registre complet asynchrone doit émettre autant de jetons de données qu'il en a reçus [Raz11]. Dans le cas contraire, le circuit est en dysfonctionnement. Les travaux de Razafindraibe [Raz11] ont mis en évidence que seul un des rails des demi-registres est utilisé. Par conséquent, il est possible de simplifier encore le dispositif en supprimant le rail inutilisé, tel que représenté par la Figure 3.18. Le dispositif simplifié est utilisé en vue d'obtenir une TMR à base d'un registre complet asynchrone double rails. La figure 3.19 illustre les résultats de simulation Spice du registre complet sain.

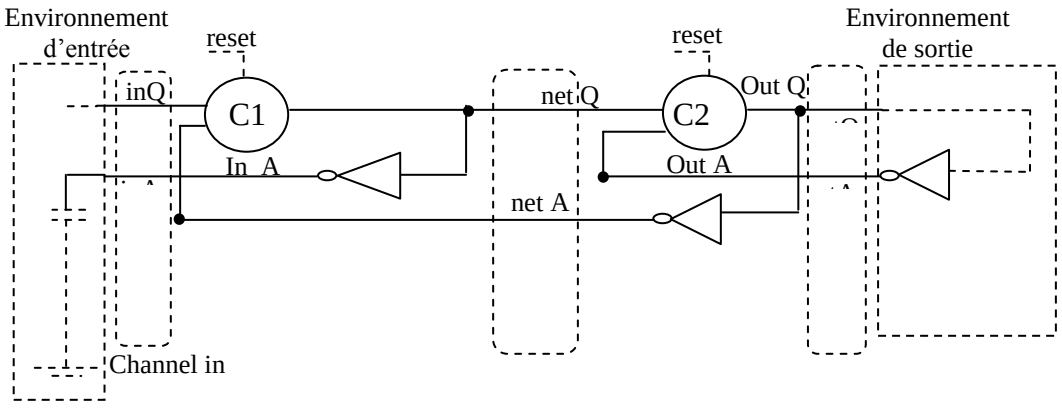


Figure 3.18 Registre complet simplifié sans défaut.

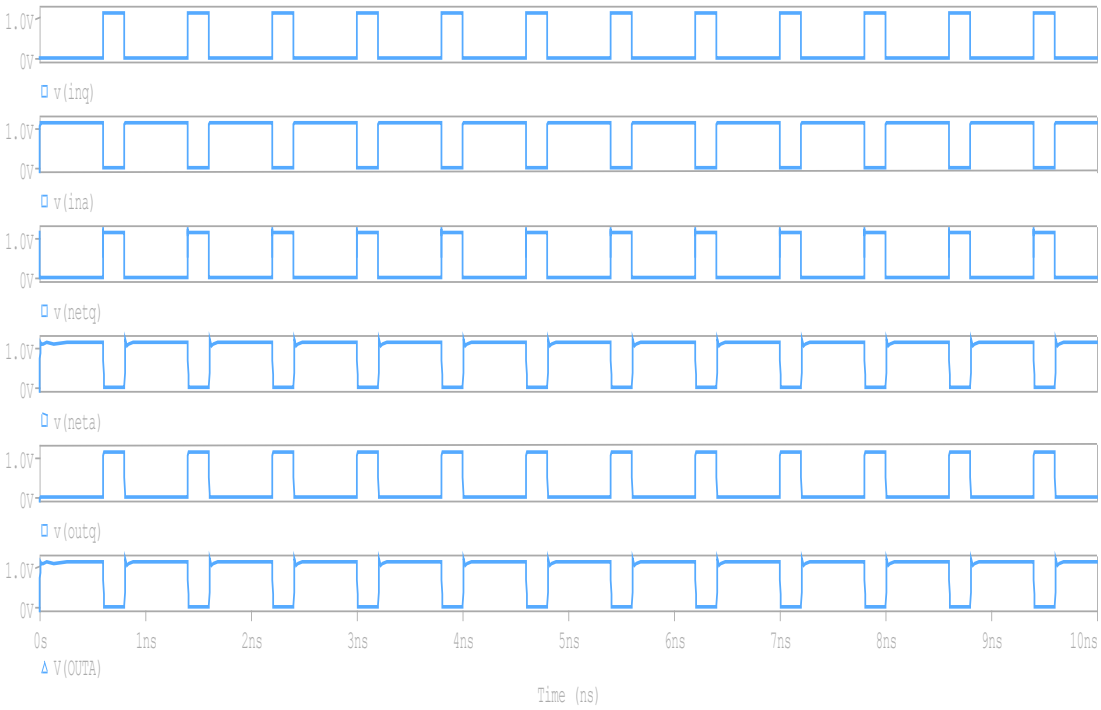


Figure 3.19 Réponse transitoire du registre complet sans défaut.

3.6.3 Effet de circuit-ouvert sur la TMR à base de registre complet

Pour analyser l'impact de deux défauts de circuits ouverts sur la TMR à base de registre complet, nous avons étudié le comportement électrique de cette structure pour les deux cas avant et après injection des défauts dans les lignes d'interconnexions des modules 2 et 3. La Figure 3.20 représente un registre complet où le nœud n est affecté par un circuit-ouvert résistif. Le circuit est composé de deux entrées notées InQ et InA et de deux sorties OutQ et OutA.

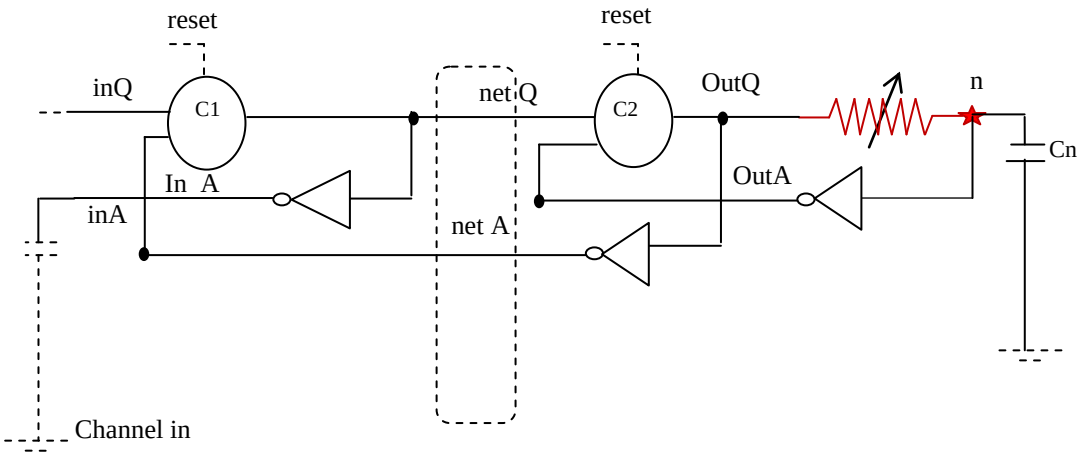


Figure 3.20 Registre complet fautif.

La figure 3.21 montre les résultats de simulation Spice de la TMR asynchrone à base de registre complet proposée lorsque les lignes d'interconnexion correspondant aux signaux OutQ2 et OutQ2 des modules 2 et 3 sont fautives. Les simulations ont été réalisées avec différentes résistances. La figure 3.21 représente les requêtes et acquittements mesurés avec un circuit-ouvert résistif de résistance critique égale à 8 kΩ pour lequel le défaut est détecté. Les sorties outQ et outA atteignent la tension de seuil à l'arrivée du front d'horloge du signal inQ. Pour faciliter la détection des deux défauts nous avons agrandi la zone d'activité 1 qui est visible dans la zone 2. En effet, on voit que lors de l'arrivé du front du signal d'entrée (transition de 0 à 1) les sorties de la TMR sont actives lors des transitions lentes.

Lorsque les données sont transmises à travers la ligne d'interconnexion affectée par un circuit ouvert, de nombreuses requêtes sont émises sur le canal intermédiaire net et transmises au canal de sortie out. Comme il a été démontré par Razafindraibe [Raz11], ces apparitions de requêtes peuvent empêcher la progression des données. A partir de la résistance critique trouvée, ces erreurs se traduiront par l'intolérance aux deux défauts de circuits ouverts et le dysfonctionnement de la TMR. En effet, tous les blocs logiques étant fortement synchronisés avec leurs voisins, la modification du comportement d'un des blocs affectera tout le circuit de proche en proche.

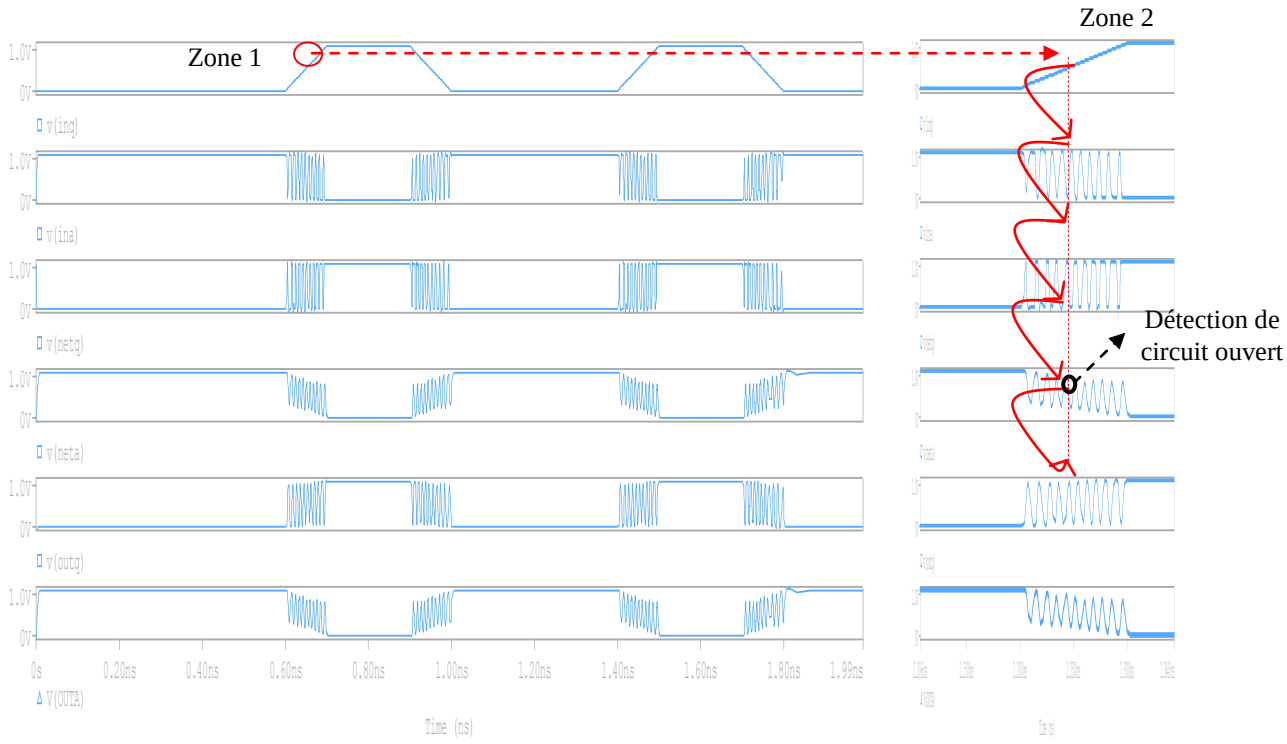


Figure 3.21 Détection du défaut avec R_{CO} = 8 kΩ

3.7 Conclusion

Dans ce chapitre, nous avons mis en évidence les propriétés électriques déterminantes pour la détection de défauts physiques de fabrication dans les TMR sécurisées. Nous avons d'abord analysé le comportement statique et dynamique de deux défauts paramétriques : le court-circuit résistif et le circuit-ouvert résistif. Les résultats de simulation ont confirmé que les mêmes modèles de faute des circuits CMOS standard sont aussi applicables pour les circuits sécurisés. La résistance aléatoire de défaut est le paramètre prépondérant de sa modélisation. Nous avons montré que selon la valeur de la résistance du court circuit, il existe trois intervalles de fonctionnement des TMR sécurisées. Les résultats ont également montré, d'une part, l'existence d'une résistance critique maximale au dessous de laquelle les deux défauts de courts circuits sont détectés et les deux TMR ne sont plus tolérantes aux défauts de courts circuits. D'autre part l'existence d'une résistance critique minimale à partir de laquelle les deux défauts de circuits ouverts sont détectés et les deux TMR ne sont plus tolérantes aux défauts de circuits ouverts. Nous avons aussi montré que la logique WDDL est moins robuste que la logique QDI et que le courant consommé devient plus significatif dans le cas des circuits sécurisés défectueux, ce qui permet d'obtenir facilement la séquence de données et ainsi briser la sécurité des circuits. Par la suite, nous avons fait la même analyse pour une TMR asynchrone double rail tout en prenant en compte les protocoles de communication (Requête et acquittement) et l'architecture associée en vue de connaître l'effet des deux défauts sur le dysfonctionnement et la tolérance des TMR sécurisées.

Afin de valider le comportement des circuits ouverts et des courts circuits des TMR sécurisées, le chapitre suivant sera consacré à la validation expérimentale de ces modèles de fautes sur des TMR sécurisés réelles.

Chapitre 4

Validation expérimentale

Application de la méthode de test sur des circuits sécurisés réels implémentés sur FPGA.

4.1 Introduction

La validation expérimentale comprend deux étapes. La première étape consiste en la division de la fréquence d'horloge de la carte FPGA, utilisée comme référence, au moyen d'un diviseur d'horloge pour surmonter les principales contraintes de conception de la réalisation expérimentale. Nous discutons de son intérêt et soulignons le fait qu'elle doit être adaptée à une application donnée, en fonction des connaissances générales des données à traiter. La seconde étape, qui représente l'originalité essentielle de ce travail, est tout d'abord consacrée à l'implémentation de deux types de TMR sécurisées à base des portes WDDL et QDI, et puis ensuite à l'injection de nos modèles de défaut développés de manière à faciliter la détection par surveillance des variations des tension de sorties. L'évaluation de cette technique permet de mettre en valeur sa capacité à détecter des défauts résistif de différentes valeurs dans une technologie CMOS sécurisée fortement submicronique (45nm).

4.2 Banc de test expérimental

Le schéma du dispositif expérimental de la méthodologie de test développée dans ce travail est présenté sur la figure 4.1. Ce dispositif est composé, d'une part, du système de programmation et, d'autre part, des éléments de contrôle et de pilotage indispensables à son fonctionnement. Une carte FPGA mise sous tension (deux tensions d'alimentation sont nécessaires: 3,3 V pour les entrées/sorties et 1,2V pour l'alimentation interne du FPGA), permet de générer les vecteurs de test de largeur de pulsation variant de 0.1ns à 0.2 ns. Ces signaux sont ensuite amplifiés en sortie de la carte FPGA avant d'être envoyés à l'oscilloscope. Les résistances et les capacités de différentes valeurs permettent l'injection de fautes réelles directement sur la schématique du circuit sous test et dans une description VHDL au niveau RTL. Un oscilloscope de large bande d'une fréquence d'échantillonnage très élevée (1 GHz) permet de visualiser les différents signaux d'entrée et de sortie à analyser. L'ensemble de ces éléments constituant le système de test sont contrôlés par un ordinateur de type PC. Il permet de piloter et de programmer la carte FPGA par l'intermédiaire d'un câble USB Adept.

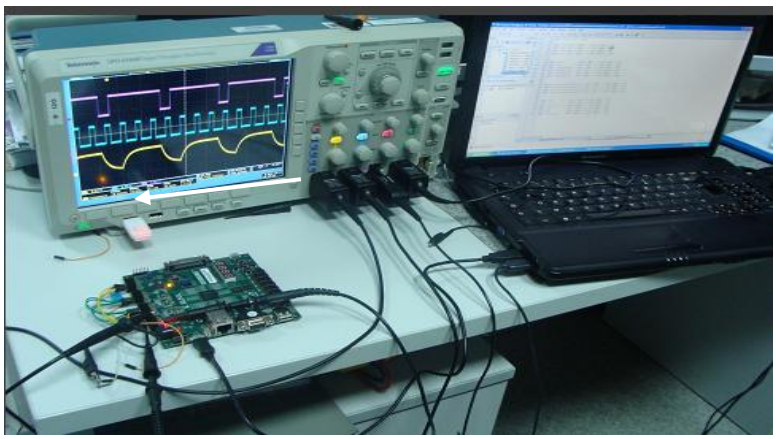


Figure 4.1 Dispositif expérimental

4.3 Principe de la méthode de test

Nous allons tout d'abord décrire le principe général de la méthode proposée, ce qui permettra de définir les différentes étapes du système de détection que nous souhaitons développer. Chacune de ces étapes sera ensuite détaillée.

Désignons par ET-WDDL, ET-QDI et le registre asynchrone complet les circuits sécurisés présentés au banc de test. L'objectif est de vérifier leur tolérance en présence des deux défauts résistifs: circuit-ouvert résistif et court-circuit résistif. Comme ceci fut précisé précédemment, nous optons pour une approche dite à une redondance modulaire triple (TMR). La détection et la vérification sont effectuées par comparaison de la caractéristique du signal de sortie des modules sains de la TMR, notés {(ET-WDDL) $_1$, (ET-QDI) $_1$ et (registre complet) $_1$} avec des exemplaires de sortie des autres modules défectueux de la TMR, notés {(ET-WDDL) $_{2,3,}$ (ET-QDI) $_{2,3}$ et (registre complet) $_{2,3}$}. Nous proposons d'implémenter et de transformer ET-WDDL, ET-QDI et le registre complet au moyen du langage VHDL et de l'application d'une perturbation électrique extérieure afin de faire apparaître une structure TMR spécifique.

- La partie logicielle consiste à développer un code VHDL adapté à chacune des superpositions entre un défaut de fabrication (perturbation électrique) et les vecteurs de test appliqués aux entrées des portes dans le but de détecter toute anomalie au niveau du signal de sortie des TMR sous test.
- La perturbation électrique extérieure (circuit RC) permet de faire apparaître l'impact électrique réel des modèles de fautes injectés sur les structures considérées. Ce choix est motivé par le fait que le retard crée par un défaut résistif peut être modélisé par un circuit RC. Les vecteurs de test associés aux différentes perturbations seront optimisés pour détecter les défauts selon deux analyses différentes (statique et dynamique).

Le fait d'appliquer chacune des deux transformations à ET-WDDL, ET-QDI et au registre complet conduit à l'obtention de la série des circuits transformés définie par l'ensemble {TMR saine à base ET-WDDL, TMR saine à base ET-QDI, TMR à base de registre complet sain, TMR fautive à base ET-WDDL, TMR fautive à base ET-QDI et TMR à base de registre complet fautif}. Ensuite, pour chaque transformation, on décide alors si le comportement électrique analysé est fautif, à l'aide de la surveillance de leur tension de sortie. Finalement, les décisions relatives aux différentes transformations vont faire apparaître les intervalles de tolérance. Les structures TMR sécurisées sont alors testées par le banc de test.
Le schéma de principe de la méthode proposée est donné par la figure 4.1. Au cours des sections suivantes, nous décrivons le banc de test, les deux transformations (programmation en VHDL et la technique d'injection de fautes), la technique de détection de défauts et finalement le principe de tolérance de ceux-ci.

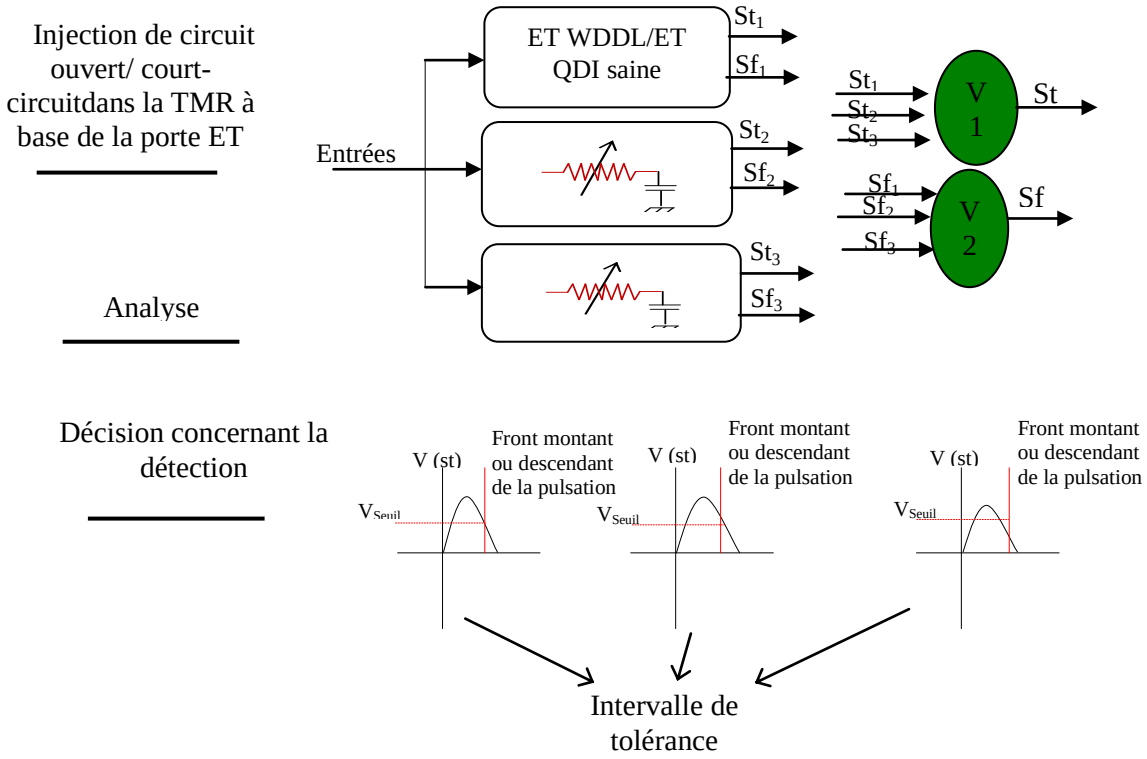


Figure 4.2 Méthode de test et de tolérance aux fautes.

4.4 Implémentation de circuits sécurisés

La méthode d'implémentation que nous proposons comprend deux étapes. La première consiste en une série de programmation VHDL. Il convient de les implémenter sur une carte FPGA de la famille Spartan 6 afin de tirer parti de la technologie utilisée dans cette dernière. Cette carte est couramment utilisée pour la grande variété d'entrées/sorties qu'elle offre et aussi pour sa facilité d'adaptation aux besoins de l'utilisateur. La seconde étape concerne la phase de l'exécution des programmes, exclusivement applicable sur l'interface graphique via

Digilent Adept. Du fait du nombre restreint d'opérations effectuées dans ce dernier cas, nous proposons de négliger les temps de traitement relatifs aux différentes exécutions.

4.4.1 Contraintes de conception

La technique de recherche de la fréquence d'horloge est à adapter en fonction du type de données, c'est-à-dire de l'application. La carte FPGA utilisée dans notre méthode a une fréquence d'horloge égale à 100 Mhz. Cette fréquence peut être multipliée ou divisée par 2, 4, 6 ou 8 grâce au réseau d'horloges intégrées dans le prototype FPGA, selon le besoin. En effet, dans le cadre de nos travaux de simulations SPICE, nous avons travaillé avec des temps d'horloge avoisinant la nanoseconde, d'où la nécessité de diviser la fréquence d'horloge de la carte FPGA. La procédure de réduction de la fréquence d'horloge est montrée par la figure 4. 2.

La suite de cette validation expérimentale sera l'implémentation des portes ET WDDL et ET QDI et d'un registre complet asynchrone (full buffer) sur ce même prototype FPGA en mettant en œuvre les protocoles de communication et l'architecture associée.

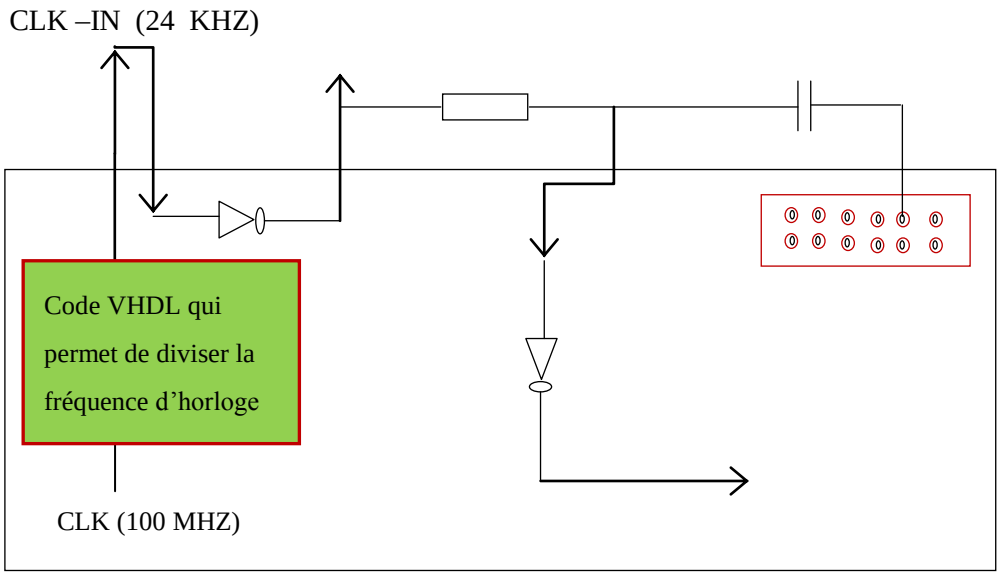


Figure 4.2 : Configuration de la carte FPGA dans le cas de diviseur de fréquence.

4.4.2 Implémentation de la porte ET WDDL

L'implémentation de la porte ET WDDL consiste à procéder en deux temps. Un programme VHDL donnant la description comportementale de la porte ET WDDL est effectué. Les différentes liaisons de la porte ainsi implémentée sur FPGA sont tout d'abord programmées sur la liste des réseaux (pinout_ucf.ucf) de la carte FPGA puis réalisées au moyen de petits fils conducteurs. Ainsi les entrées {xt, yt, xf, yf} qui constitue le vecteur de test sont connectées respectivement au {Pmod D9, Pmod C1, Pmod C2, Pmod C3}. Quant

aux sorties St et Sf, elles sont connectées aux Pmod C7 et Pmod C9. Il est à noter que les quatre signaux {S1, S2, S3, S4} générés à partir de la carte FPGA correspondent respectivement aux signaux d'entrées {yf, yt, xf, xt}. Cette implémentation est illustrée par la figure 4.3. La vue RTL et schématique de la porte ET WDDL est représentée sur la figure 4.4. La figure 4.5 donne la réponse transitoire de la porte ET-WDDL.

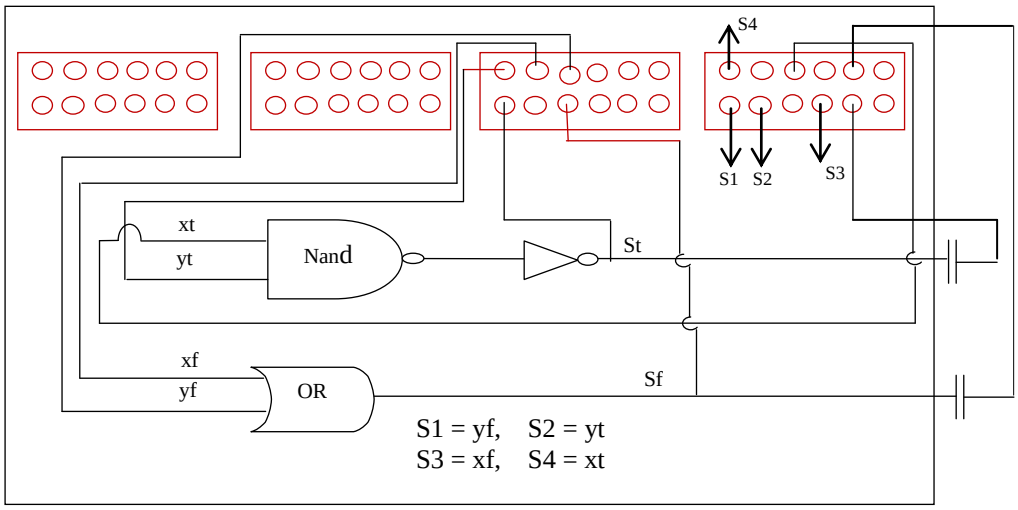


Figure 4.3 Configuration de la carte FPGA dans le cas de la porte WDDL–AND saine

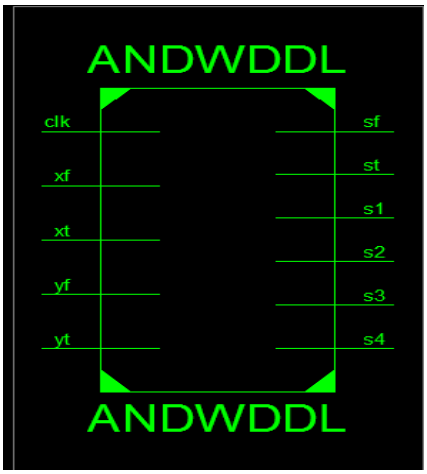


Figure 4.4 Vue RTL et schématique de ET WDDL.

Figure 4.5 Fonctionnement de la porte ET WDDL

4.4.3 Implémentation de la porte ET QDI

Pour implémenter la porte de Muller, nous avons effectué la même procédure d'implémentation décrite dans le cas de la porte ET WDDL. Sa vue RTL et schématique est représentée par la figure 4.6. L'évolution du signal de sortie en fonction du temps, est donnée par la figure 4.7. Il apparaît un fonctionnement anormal de la porte considérée. En effet, l'état logique de la sortie (S) change d'état logique chaque fois que l'une des deux entrées (a ou b) change d'état logique. Ce phénomène est souvent appelé boucle de rétroaction ou de retour. Ceci peut ainsi entrainer une désynchronisation des signaux d'entrée. C'est là la principale limitation de l'implémentation proposée. Il y'a cependant un moyen permettant de la surmonter. Il s'agit tout d'abord de localiser la zone qui crée la boucle de retour présente dans la porte de Muller considérée. Ensuite, cette porte de Muller est redéfinie comme étant égale à la porte de Muller initiale moins la zone contenant la boucle de retour. Enfin, on réapplique la technique d'implémentation pour cette nouvelle porte de Muller, comme cela est présenté par la figure 4.8. Le chronogramme de la porte de Muller illustré sur la figure 4.9 montre bien que le problème de boucle de rétroaction est bien supprimé et par conséquent la porte de Muller assure bien le rendez-vous entre les deux signaux a et b.

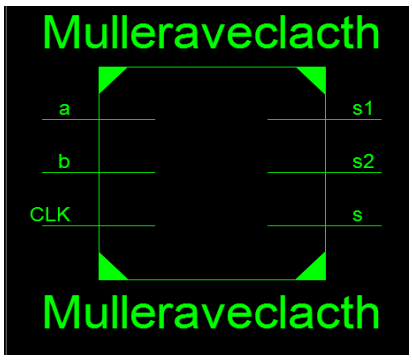


Figure 4.6 Vue RTL et schématique de C-element avec boucle de retour.

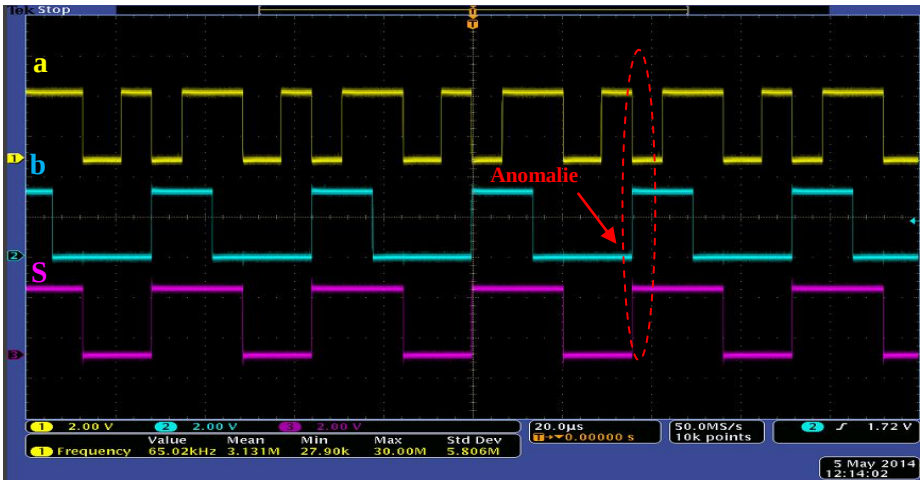


Figure 4.7 Porte de Muller avec boucle de retour.

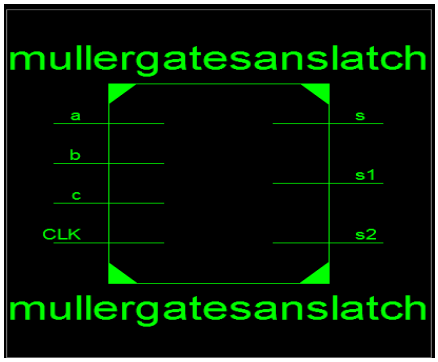


Figure 4. 8 Vue RTL et schématique de la porte de Muller.

Figure 4.9 Porte de Muller sans boucle de retour.

En ce qui concerne l'implémentation de la porte ET QDI, nous avons effectué la même procédure décrite dans le cas de l'implémentation de la porte ET WDDL. Nous faisons l'hypothèse que, dans le cadre de cette application, les signaux d'entrées {xt, yt, xf, yf} sont connectés respectivement aux {Pmod A10, Pmod A4, Pmod A9, Pmod A3}, les signaux de sorties {St, Sf} sont connectées aux {Pmod B1, Pmod B2}, et enfin les signaux appelés feedbacks {Fd1, Fd2, Fd3, Fd4} sont connectés aux {Pmod B3, Pmod B4, Pmod B9, Pmod10}. Le schéma de principe est représenté sur la figure 4.10. La vue RTL et schématique de la porte ET QDI est illustrée sur la figure 4.11. La réponse transitoire de la porte ET QDI est illustrée par la figure 4.12. On peut voir dans cette dernière le fonctionnement de la porte ETQDI pour des variations d'entrée données. Il est aussi constaté, d'après la reconstitution, que l'information contenue dans les différents signaux a été amplifiée. On note par ailleurs qu'en fonctionnement normal la porte ET QDI est programmée de façon à recevoir en entrée quatre signaux de niveau logique 1,1 V. Cette amplification des signaux correspond essentiellement aux niveaux logiques de sortie du prototype FPGA (3,3 V).

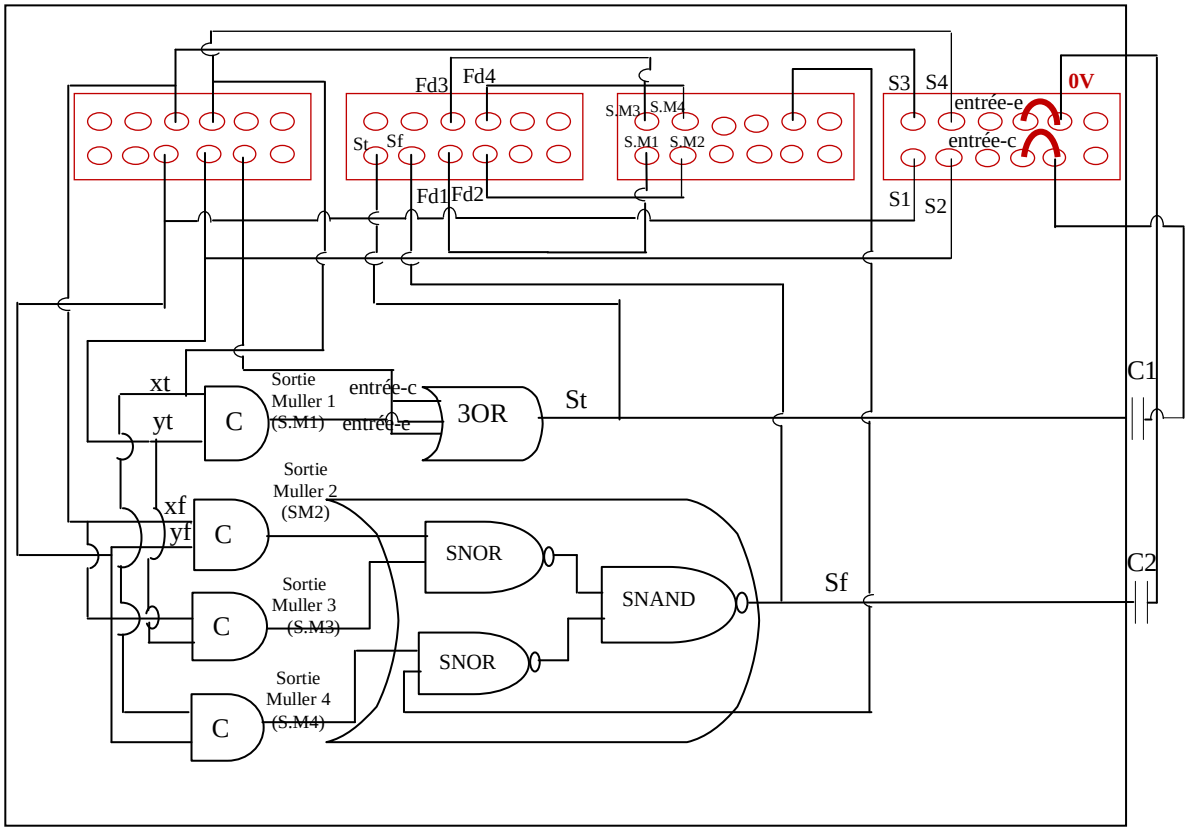


Figure 4.10. Configuration de la carte FPGA dans le cas de la porte ET QDI.

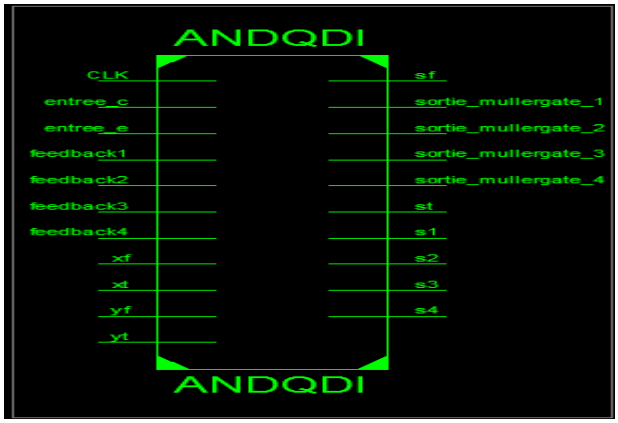


Figure 4.11 Vue RTL et schématique de ET QDI.

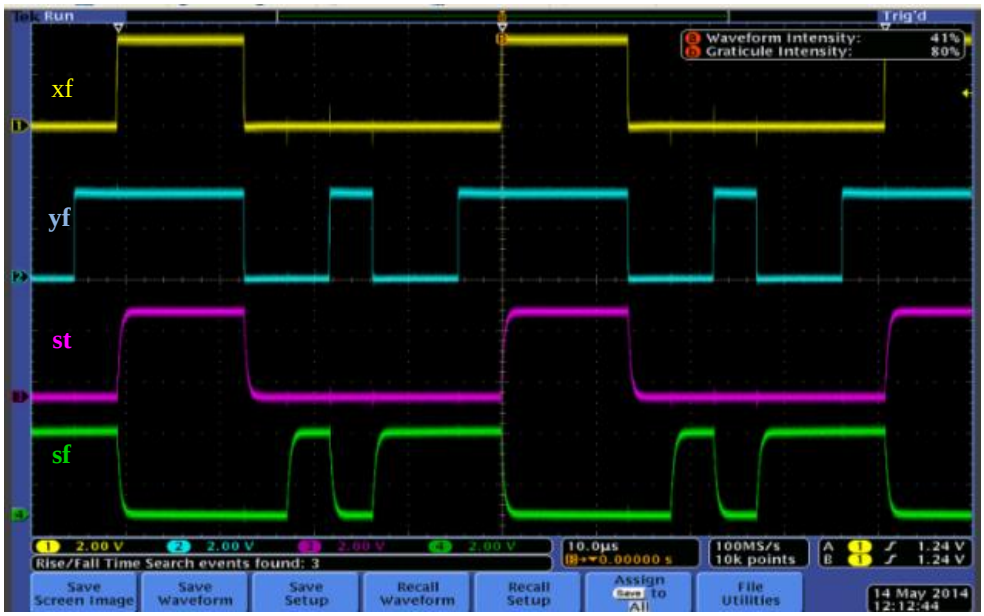


Figure 4.12 Fonctionnement de la porte ET QDI.

4.4.4 Implémentation du full buffer

La Figure 4.13 présente la configuration dans laquelle le registre complet sous test se trouve avant l'injection du circuit-ouvert résistif. Les entrées {inq, reqinq, reqsortie_mullergate_1} sont connectées respectivement au {Pmod JA10, Pmod JA3, Pmod JA9}. Quant aux sorties out A et in A, elles sont connectées au Pmod JB2 et Pmod JD8. Les trois signaux {S1, S2, S3} sont générés à partir du FPGA. La vue RTL et schématique du registre sont représentées par la figure 4.14. Quant à son fonctionnement il est montré sur la figure 4.15. On voit bien que son comportement est correct et ne comporte aucune anomalie.

4.5 Injection de fautes résistives

La technique d'injection de fautes au niveau comportemental que nous proposons est fondée sur le rajout des modèles de fautes résistifs réels sur la schématique du circuit mais aussi dans une *description VHDL* couramment utilisée pour représenter précisément des défauts réels et pour la simulation de fautes. Il existe principalement deux approches permettant d'injecter une faute catastrophique. La première approche consiste à trouver le modèle de faute qui modélise correctement le défaut considéré. La deuxième, consiste à trouver la manière dont ce modèle de faute sera injecté dans le circuit sous test. Il est à rappeler qu'un court-circuit résistif se modélise comme une résistance d'une valeur très petite et un circuit-ouvert résistif se modélise comme une résistance d'une valeur très grande. Concernant la manière dont ces modèles seront injectés, le court-circuit s'injecte en parallèle entre deux connections disjointes d'un circuit. Par contre, le circuit-ouvert s'injecte en série dans l'un des segments d'une connexion d'un circuit.

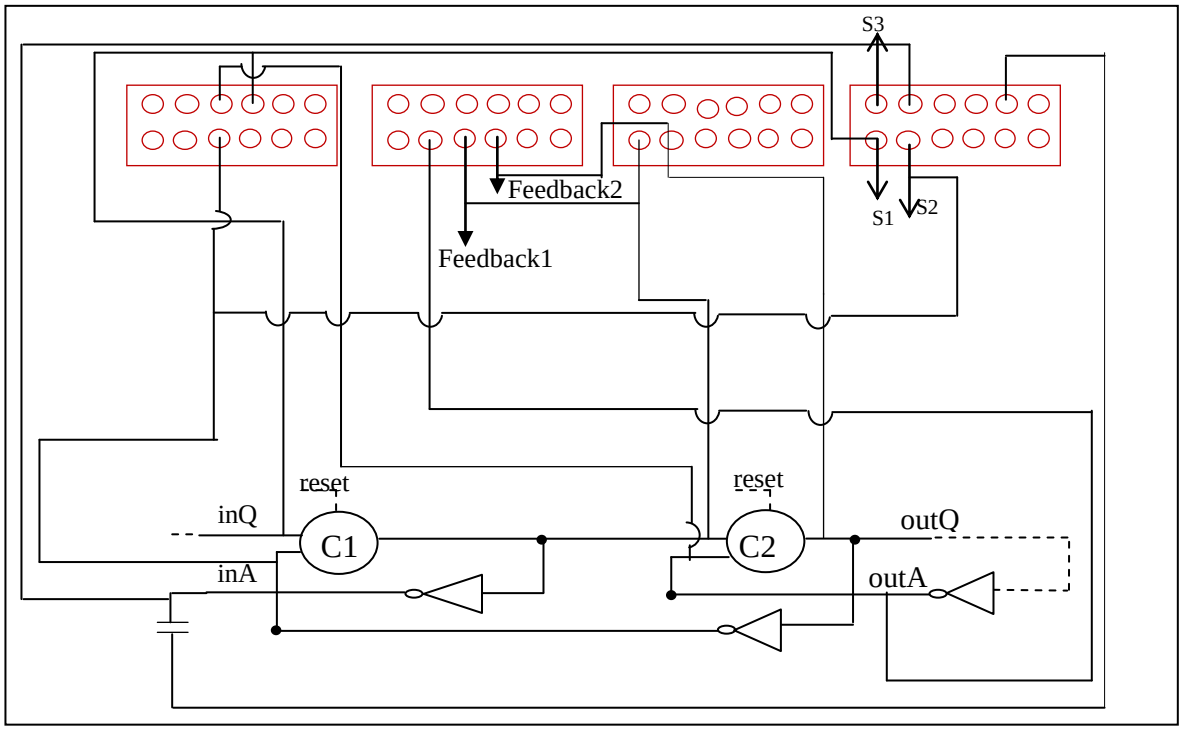


Figure 4.13 Configuration du FPGA dans le cas de registre complet.

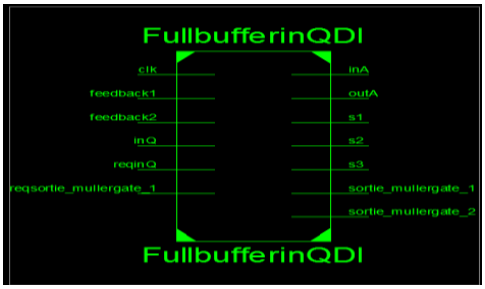


Figure 4.14 Vue RTL du registre complet sain.

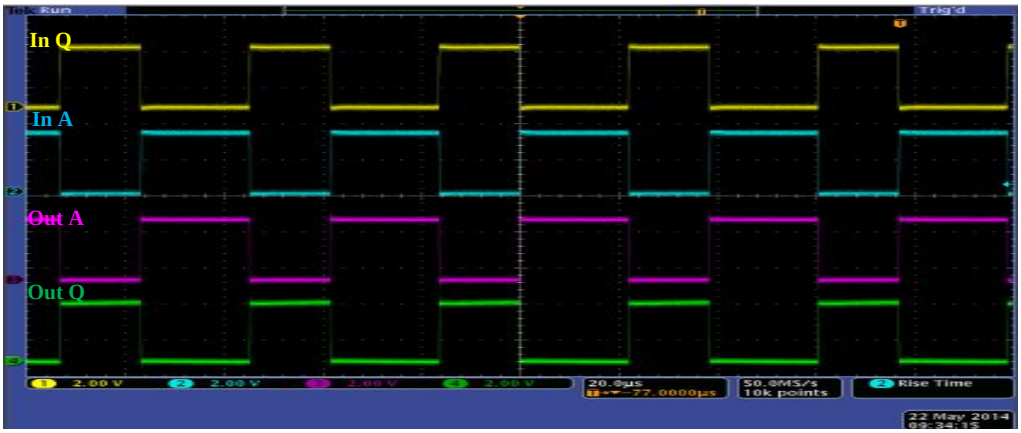


Figure 4.15 Comportement du registre complet sain.

4.5.1 Injection de court-circuit résistif

Les figures 4.16 et 4.18 illustrent cette technique d'injection de court-circuit résistif. La configuration des deux portes est légèrement modifiée. Les fils des deux sorties St et Sf sont respectivement portés à l'entrée et à la sortie de la résistance aléatoire du défaut. La carte FPGA va jouer le rôle de générateur de vecteur de test [xt yt xf yf]. Deux capacités de valeurs typiques de 5 pF sont placées en sortie de chaque sortie St et Sf. Un grand soin est accordé à la soudure des deux capacités de charge sur les deux extrémités de la résistance afin d'assurer un bon contact entre elles et donc une bonne conduction de courant. L'oscilloscope va jouer le rôle de récepteur, les signaux à la sortie FPGA seront visualisés sur l'écran de ce dernier. Nous rappelons aussi que pour créer des transitions de sens inverses sur les nœuds St et Sf, un vecteur de test composé de deux pulsations ayant la même largeur [0011] et [1100] est généré à partir du prototype FPGA. Ces vecteurs sont ensuite appliqués sur les entrées [xt yt xf yf] des portes sécurisées. Les vues RTL et schématique des deux portes ET WDDL et ET QDI sont présentées par la figure 4.17 et la figure 4.19, respectivement.

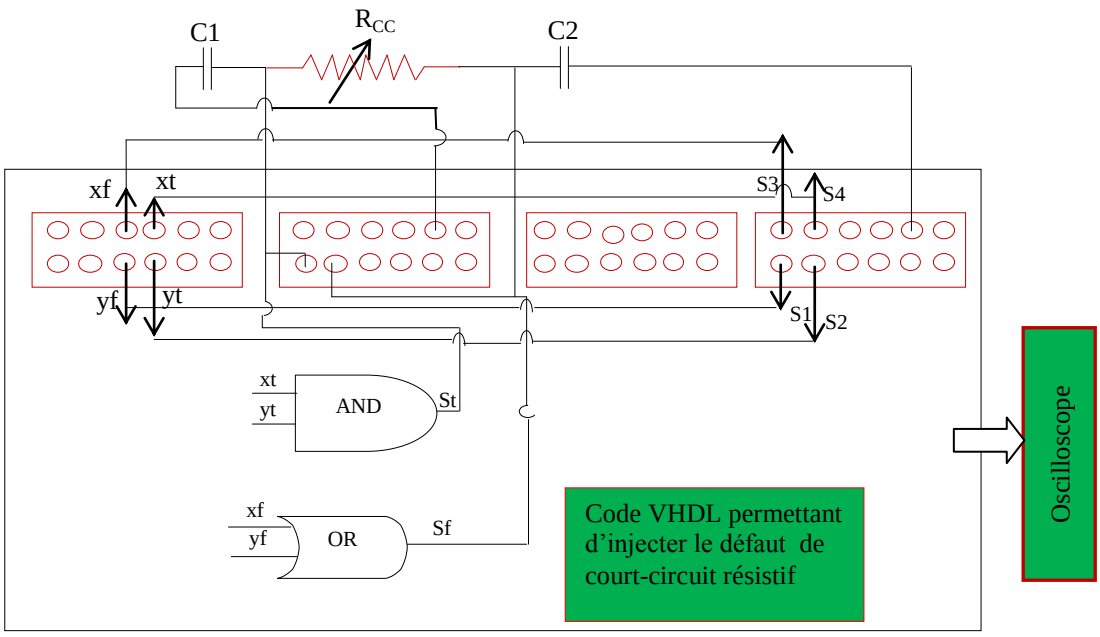


Figure 4.16 injection de court-circuit résistif dans ET WDDL.

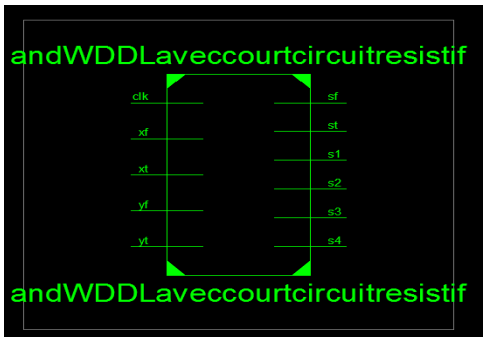


Figure 4.17 Vue RTL et schématique de la porte ET WDDL fautive.

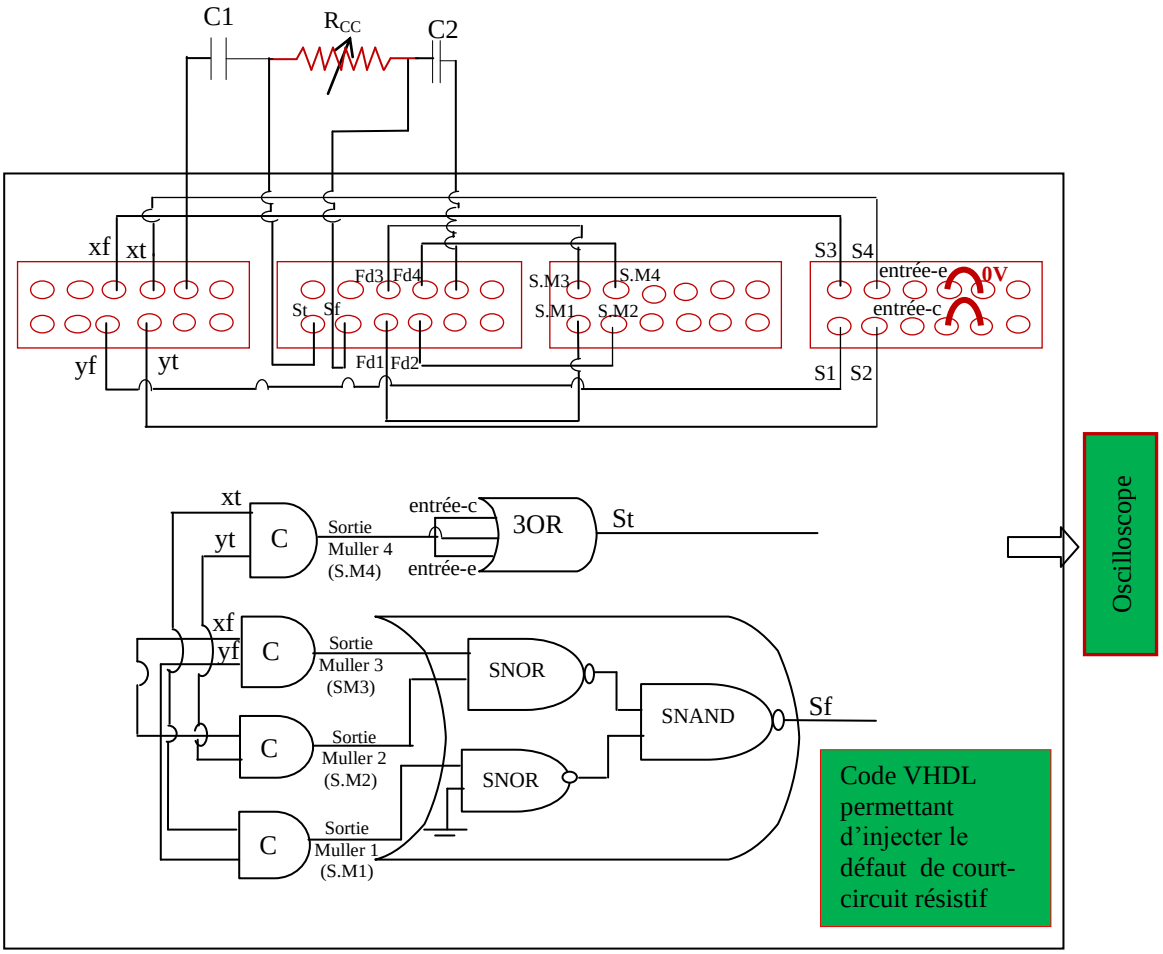


Figure 4.18 Configuration sur FPGA de l'injection de court-circuit dans ET QDI

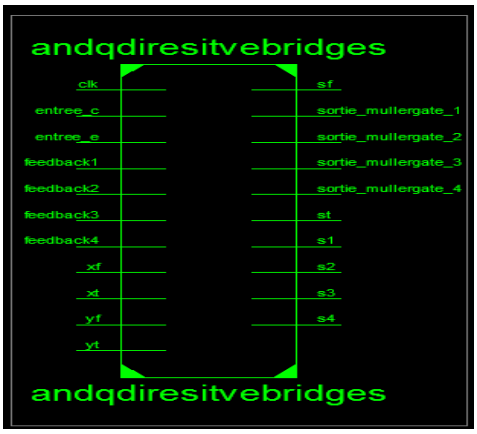


Figure 4. 19 Vue RTL et schématique de ET QDI fautive.

4.5.2 Injection de circuit-ouvert résistif

Nous allons tout d'abord injecter le circuit-ouvert dans les circuits sécurisés, sans tenir compte les protocoles de communication. Ensuite nous allons injecter le même défaut dans un circuit sécurisé prenant en compte les protocoles de communication.

4.5.2.1 Injection de circuit-ouvert résistif dans ET WDDL et ET QDI

Le processus d'injection du circuit-ouvert diffère de celui du court-circuit. nous proposons d'injecter la résistance variable entre la sortie de la porte Nand et l'entrée de l'inverseur dans la porte ET WDDL (figure 4.20), et entre la sortie de la quatrième porte de Muller et la deuxième entrée de la porte 3OR de la porte ET QDI (figure 21). Par ailleurs, dans la porte ET WDDL, la sortie de la porte NAND et l'entrée de l'inverseur sont respectivement portés à l'entrée et à la sortie de la résistance aléatoire du défaut. Dans la porte ET QDI, la sortie de la quatrième porte de Muller et la deuxième entrée de la porte 3OR sont respectivement portées à l'entrée et à la sortie de la résistance aléatoire du défaut. Deux capacités de valeurs 6,5 pF sont placées en sortie St et Sf. La vue RTL et schématique de ces deux portes défectueuses est représentée par la figure 4.22 et 4.23, respectivement.

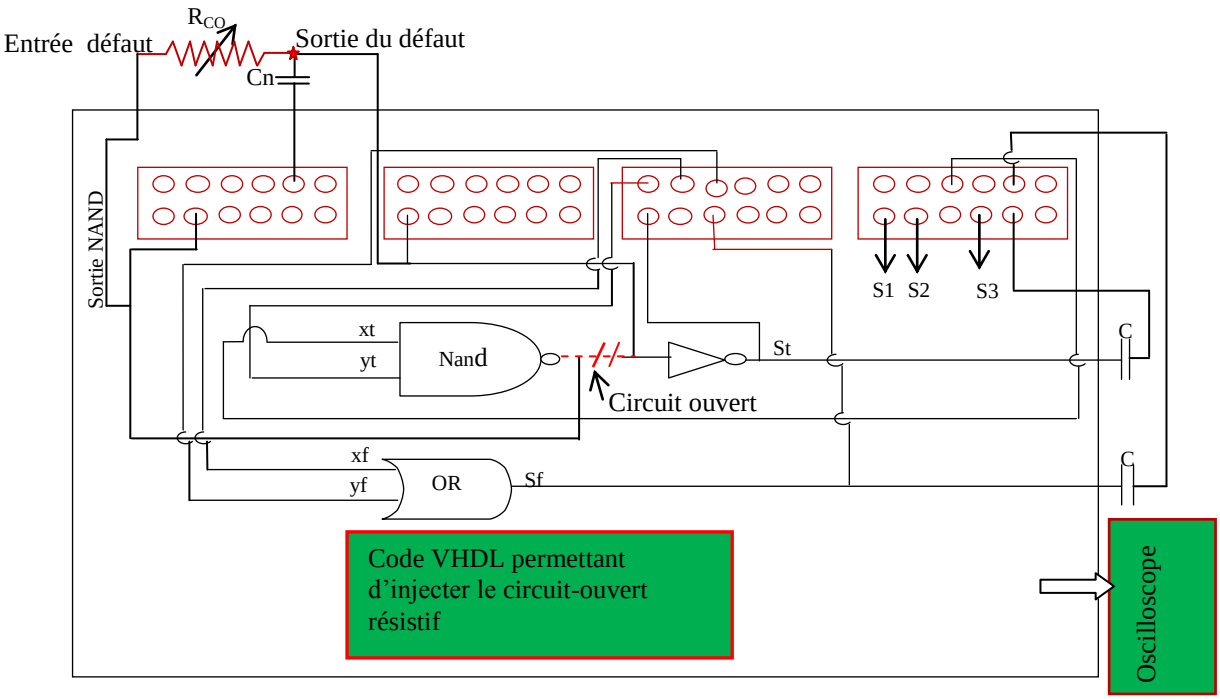


Figure 4.20 Configuration du FPGA de l'injection de circuit-ouvert dans ET WDDL.

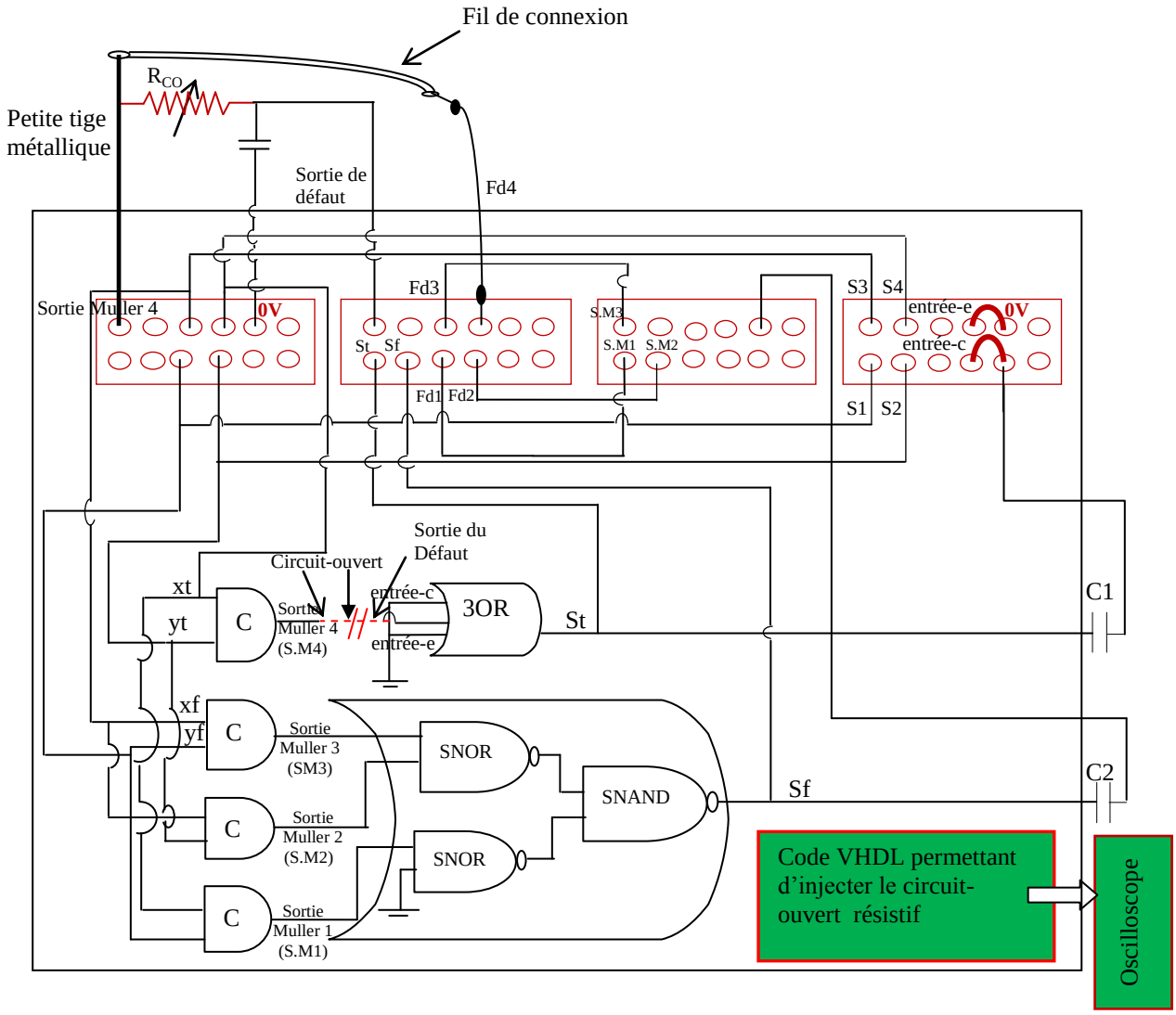


Figure 4. 21 Configuration du FPGA dans le cas d'injection de circuit-ouvert dans ET QDI.

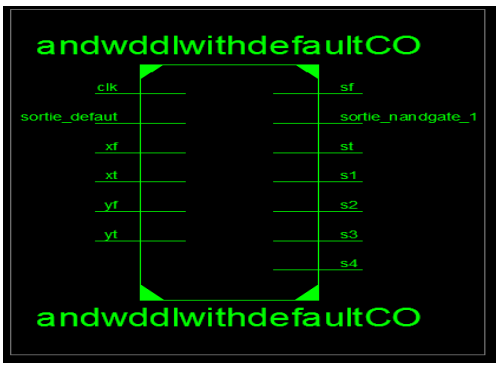


Figure. 4.22 Vue RTL et schématique de ET WDDL

Figure 4.23 Vue RTL et schématique de ET QDI

4.5.2.2 Injection de circuit-ouvert résistif dans le registre complet

Comme le montre les figure 4.24 et 4.25 nous avons d'abord injecté directement le circuit-ouvert résistif dans le registre complet. L'architecture du registre est aussi légèrement modifiée, la sortie de la porte de Muller 2 (ACK/Out Q) et l'entrée de l'inverseur 2 sont respectivement portés à l'entrée et à la sortie de la résistance aléatoire du défaut. Deux capacités de valeurs de 5 pF sont placées en sortie du signal inA et en sortie du défaut.

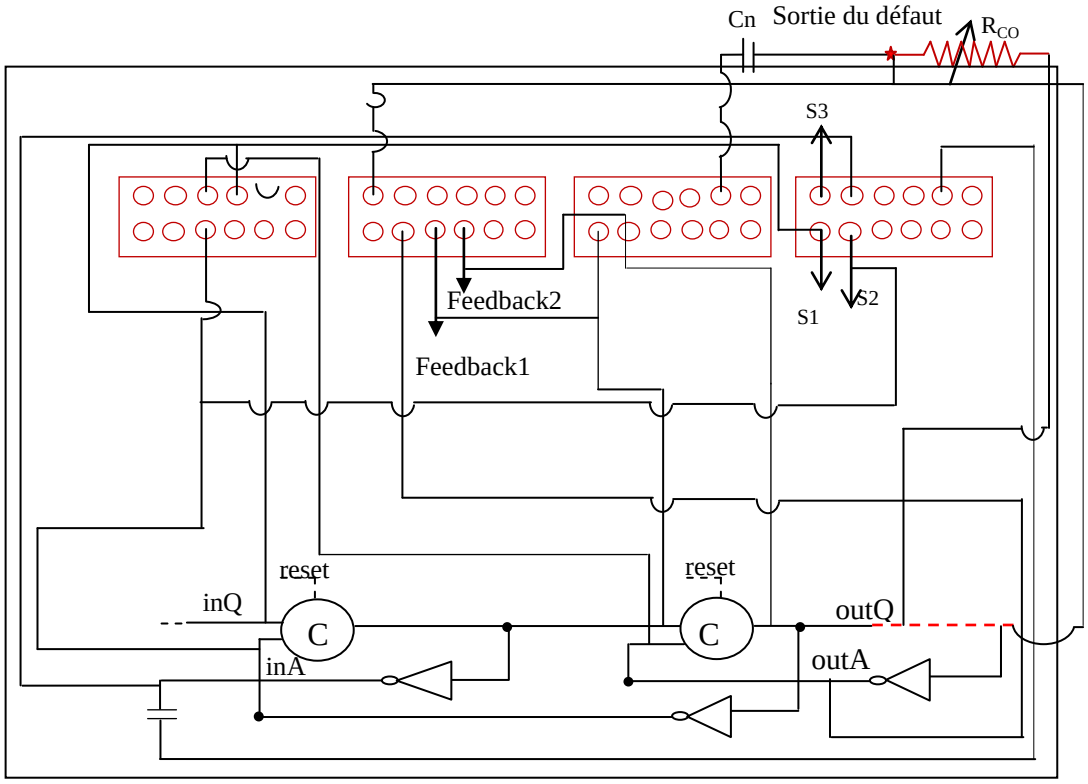


Figure 4.24 Configuration du FPGA dans le cas d'injection de circuit-ouvert dans le registre complet asynchrone.

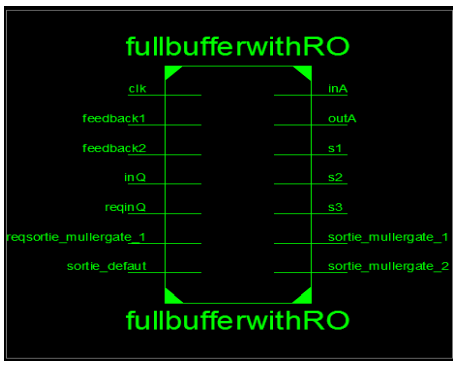
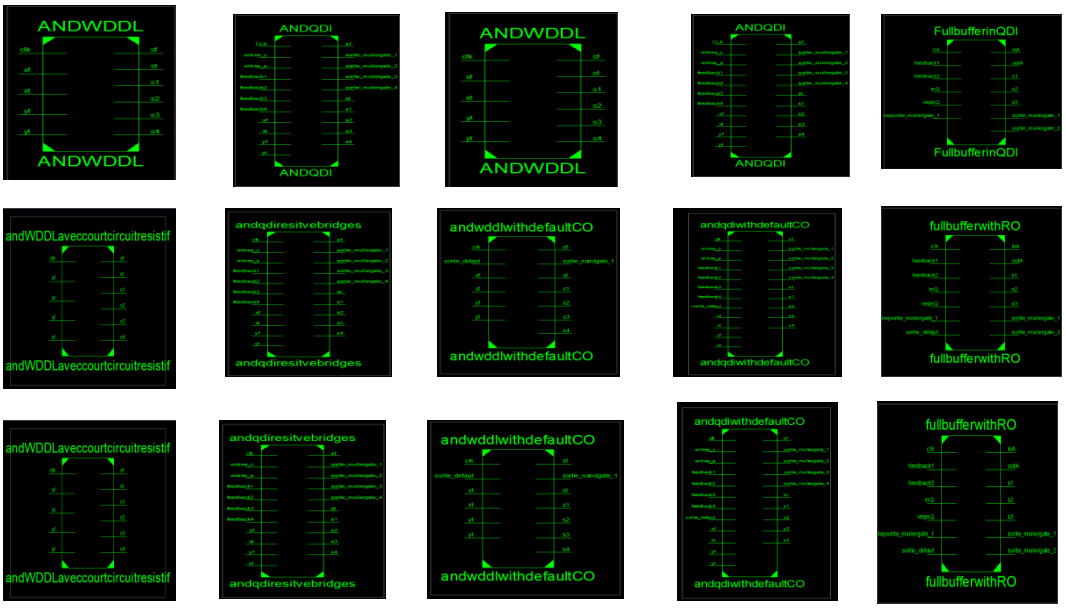


Figure.4.25 Vue RTL du registre fautif.

4.5.2.3 Injection de défauts résistifs dans les structures TMR

Cette injection consiste en la combinaison des circuits sécurisés implémentés précédemment pour obtenir les TMR de chaque cas considéré. La figure 4.26 illustre chaque TMR considérée chacune affectée de deux défauts résistifs dans les modules 2 et 3.



(a) TMR à base ET WDDL avec deux défauts de court circuit

(b) TMR à base ET QDI avec deux défauts de court circuit

(c) TMR à base ET WDDL avec deux défauts de circuit-ouvert

(d) TMR à base ET QDI avec deux défauts de circuit ouvert

(e) TMR à base de registre complet avec deux défauts de circuit-ouvert

Figure 4.26 Injection de défauts résistifs dans les TMR.

4.6 Résultats expérimentaux

L'évaluation des performances de la méthode de test proposée est effectuée en mesurant l'intervalle de tolérance TI, relatif aux valeurs de résistances de défauts tolérées, En d'autres termes, ceci revient à évaluer l'intervalle de détection DI, relatif aux valeurs de la résistance de défauts détectées.

La base des données du dispositif expérimental est tout d'abord décrite. Le protocole expérimental est ensuite présenté. Enfin, les résultats expérimentaux sont détaillés. Détaillons tout d'abord les résultats obtenus dans le cas des structures TMR à base ET WDDL et ET QDI, sans tenir compte des protocoles de communication. Le comportement électrique est analysé pour différentes valeurs du paramètre R. nous rappelons que ce paramètre R désigne la résistance du défaut type utilisée pour modéliser les défauts résistif décrit dans les sections précédentes.

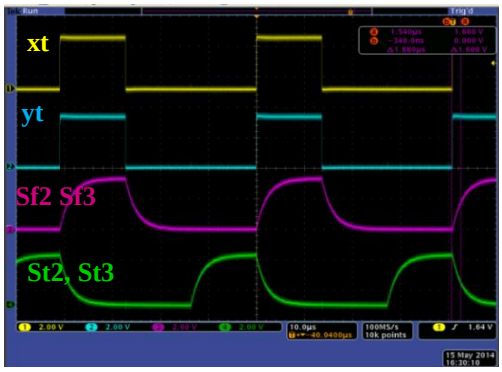
4.6.1 Analyse de l'impact des deux défauts de courts circuits sur les TMR

L'étape de détection de défauts début par la surveillance de la tension de sortie de la TMR considérée. Une tension de seuil de celle-ci est ensuite déterminée. Nous faisons l'hypothèse que la tension de seuil de chaque porte 3OR est la même. La tension de seuil V_{seuil} que nous proposons d'utiliser est défini par Vseuil = $V_{amplifiée}/2$, où $V_{amplifiée}$ est la tension en des sortie de la carte FPGA. La figure 4. 28 rapporte l'évolution du comportement dynamique de la TMR à base ET WDDL et de la TMR à base ET QDI en fonction de la résistance R du court-circuit. On observe tout d'abord un petit retard de propagation dans le signal $St_{1, 2,3}$ des portes saines (R= 0Ω), et il est de 1.18 μs pour la porte la TMR à base ET WDDL et de 780 ns pour la TMR à base ET QDI. Ces évolutions sont données pour différentes valeurs de la résistance du défaut (800 Ω, 400 Ω, 200 Ω, 100 Ω, 46 Ω). Il est observé que le comportement des structures TMR est fortement détérioré lorsque la résistance du défaut diminue. En effet, un ralentissement du signal $St_{2, 3}$ et $Sf_{2, 3}$ est observé. Cela se traduit par une augmentation du retard au fur et à mesure que la résistance du défaut décroît. Les retards mesurés pour les résistances 800 Ω, 400 Ω, 100 Ω sont respectivement de l'ordre de 3.40 µs, 3.88 µs et 4,08 µs dans la TMR à base ET WDDL. Dans le cas de la TMR à base ET QDI, ces retards mesurés peuvent être estimés comme étant égaux à 1.68 µs, 1,90 µs et 3,02 µs. On remarque que ces temps mesurés dans la TMR à base ET WDDL sont supérieurs aux temps mesurés dans la TMR à base ET QDI. Ceci permet de mettre en évidence la robustesse des circuits sécurisés implémentés en circuits QDI vis-à-vis des défauts de fabrication.

Il est à noter que pour ces résistances considérées, la tension de seuil n'a pas été déterminée à l'arrivée du front (montant ou descendant) des pulsations par notre technique de d'analyse et que notre méthode n'a pas conduit à la détection du défaut et aucun changement d'état logique en sorties St et Sf n'est observé et les TMR fonctionnent correctement et donc les deux défauts sont tolérés. Cependant, une observation précise des cas où la résistance 100 Ω dans la TMR à base ET WDDL et la résistance 46 Ω dans la TMR à base ET QDI a déterminé la tension de seuil à l'arrivée du coup d'horloge. De plus, dans ce cas, Il y a apparition d'une faute logique et le retard de propagation du signal $St_{2, 3}$ et $Sf_{2, 3}$ est plus important. Il est de 12,20 µs pour la TMR à base ET WDDL, et de 8,30 µs pour la TMR à base ET QDI. Ceci permet de montrer que les deux défauts sont détectés et que les deux TMR ne sont pas tolérantes. Ainsi les intervalles de tolérance de ces deux défauts déterminés par cette technique sont les suivants :

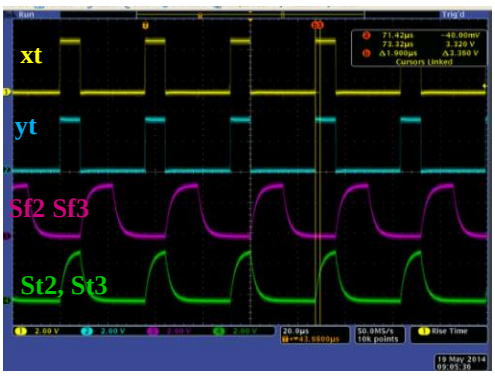
$$ID_{\text{TMR à base ET WDDL}} = [0,\ 100\ \Omega] \Rightarrow IT =]\ 100\ \Omega,\ \infty\ [$$

$$ID_{\text{TMR à base ET QDI}} = [0,\ 45\ \Omega] \Rightarrow IT =]\ 45\ \Omega, \infty\ [$$



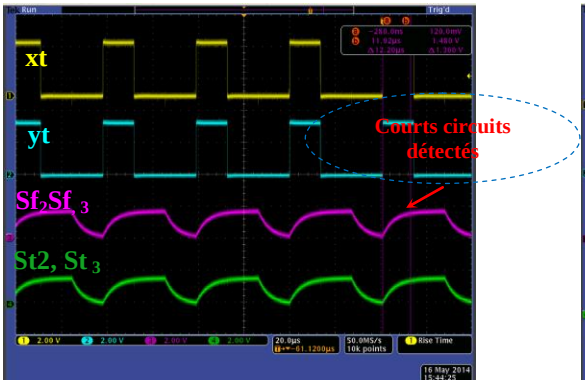
$R_{CC} = 0\ \Omega$

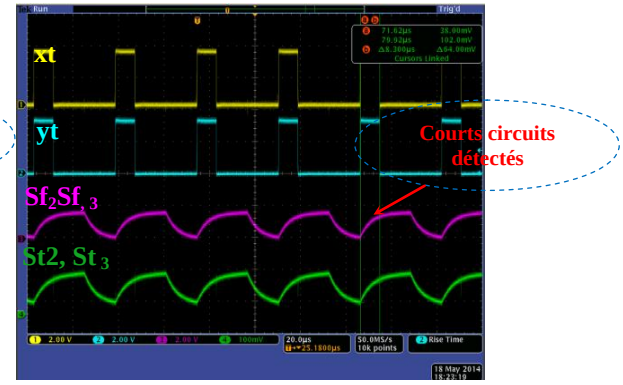
$R_{CC} = 800\ \Omega$



$R_{CC} = 400\ \Omega$

R_{CC} = 200 Ω





R_{CC} = 100 Ω

R_{CC} = 46Ω

a. TMR à base ET WDDL

b. TMR à base ET QDI

Figure 4.27 Retard mesuré en fonction de la valeur de R_{CC}.

4.6.2 Détection et tolérance de circuit-ouvert

L'objectif de cette section est d'évaluer l'efficacité de la technique de détection proposée en fonction de la valeur de la résistance du défaut de circuit-ouvert. La première partie de l'analyse est consacrée à l'estimation, à partir de mesures expérimentales, de la détection de défauts dans TMR à base ET WDDL (resp. à base ET QDI) avec une séquence de test à une largeur de pulsation (PW1), et puis par la suite avec une séquence de test à trois largeurs de pulsations (PW3). La seconde partie concerne la détection de circuits ouverts dans la TMR à base de registre complet asynchrone. Là aussi nous faisons l'hypothèse que la tension de seuil de chaque porte 3OR est la même.

4.6.2.1 Détection et tolérance avec une séquence à une seule largeur de pulsation PW1

Nous proposons d'analyser le comportement dynamique des structures TMR en fonction de la résistance du défaut de circuit ouvert. Nous allons analyser l'influence de la séquence de test appliquée aux entrées des structures TMR sur la qualité de détection. Considérons tout d'abord les structures TMR à base ET WDDL et à base ET QDI auxquelles nous appliquons une séquence de test à une seule largeur de pulsation (PW1) aux entrées [xt yt xf yf], en d'autres termes le vecteur initial V_0 = [0011] et le vecteur qui crée la transition est V_1 = [0 1 0 0]. La figure 4.29 montre la série des comportements des TMR ainsi générée en fonction de la résistance de défaut du circuit-ouvert. Pour chaque résistance, nous avons appliqué notre méthode de détection. La première ligne de la figure 4.28 représente les comportements obtenus pour une petite valeur de résistance égale à 2 kΩ. La seconde ligne de cette même figure donne les comportements obtenus pour une grande résistance égale à 3,5 kΩ dans la TMR à base ET WDDL et 4 kΩ dans la TMR à base ET QDI.

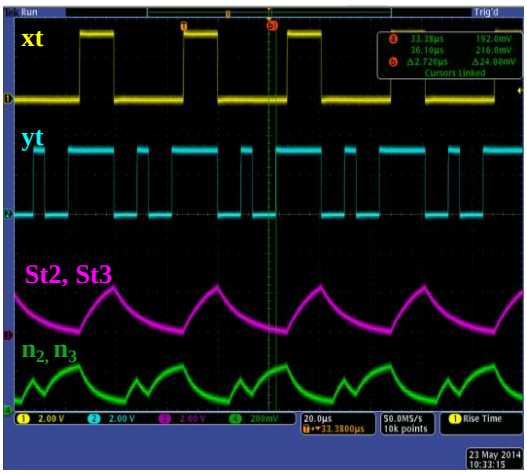
D'après la figure 4.29, on constate que, pour les comportements associés aux petites résistances les défauts ne sont pas détectés et sont tolérés, tandis que les grandes résistances entrainent une détection des défauts contenus dans les TMR. Dans le premier cas, on comprend bien que, même si on observe un ralentissement du signal St_2 et St_3 estimé à 2,72 µs et 1,39 µs, respectivement dans la TMR à base ET WDD et la TMR à base ET QDI, la valeur logique de la sortie St reste correcte et donc les deux défauts sont tolérés. Dans le second cas, la valeur logique du signal de sortie St est incorrecte ainsi ces résistances critiques conduisent à un dysfonctionnement des TMR et les défauts ne sont pas tolérés.

L'observation de ces images montre que cette technique permet de déterminer les intervalles de tolérance suivants :

$$ID_{\text{TMR à base ET WDDL}} = [3{,}5\ k\Omega,\ \infty[\Rightarrow IT = [0,\ 3{,}5\ k\Omega]$$

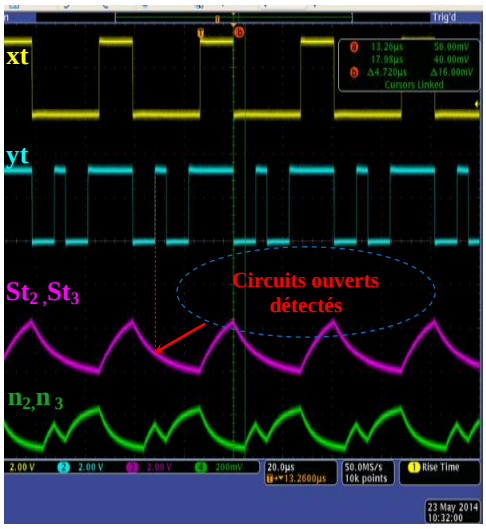
$$ID_{\text{TMR à base ET QDI}} = [4\ k\Omega,\ \infty[\Rightarrow IT = [0,\ 4\ k\Omega]$$

On constate que l'intervalle de tolérance le plus large correspond à la TMR à base ET QDI. La TMR à base ET WDDL est très sensible aux deux défauts de circuits ouverts. Par contre, la TMR à base ET QDI est nettement moins sensible.

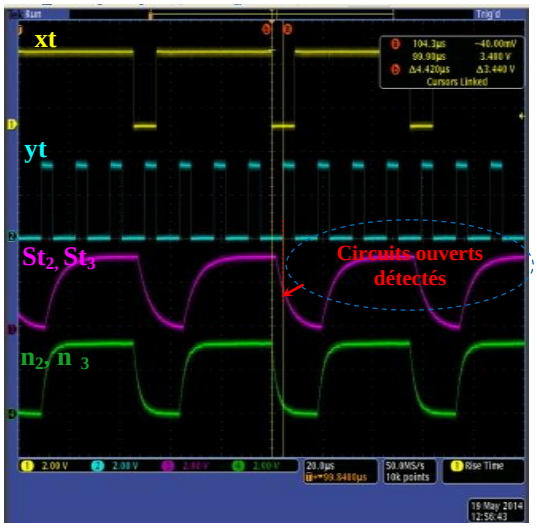


TMR à base ET WDDL
R= 2 KΩ

TMR à base ET QDI
R= 2 KΩ



TMR à base ET WDDL
R= 3,5 kΩ



TMR à base ET QDI
R= 4 kΩ

Figure 4.28 Détection et tolérance avec une séquence de test à PW1

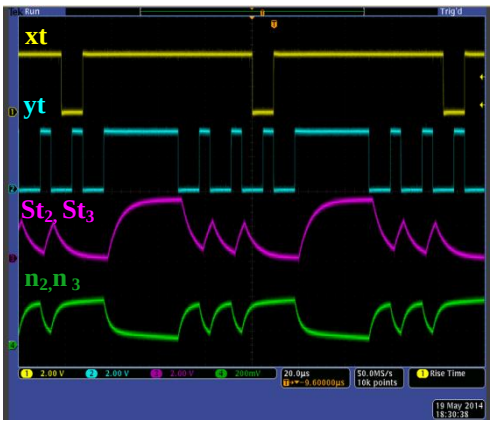
4.6.2.2 Détection et tolérance avec une séquence à trois largeurs de pulsation (PW3)

L'objectif de cette section est d'appliquer la méthode de génération d'une séquence de test qui peut être utilisée pour détecter les défauts. La technique de détection est à adapter en fonction de la largeur de pulsation et de la taille des défauts résistifs, c'est-à-dire de l'application. Considérons le cas de la TMR à base ET WDDL et de la TMR à base ET QDI soumises à une génération de n vecteurs de test et contenant des défauts de différentes tailles. Soit V= [V_0 $V_1V_2V_3$ V_4 V_5 V_6 V_7] la séquence à trois largeurs de pulsations (PW3 dans

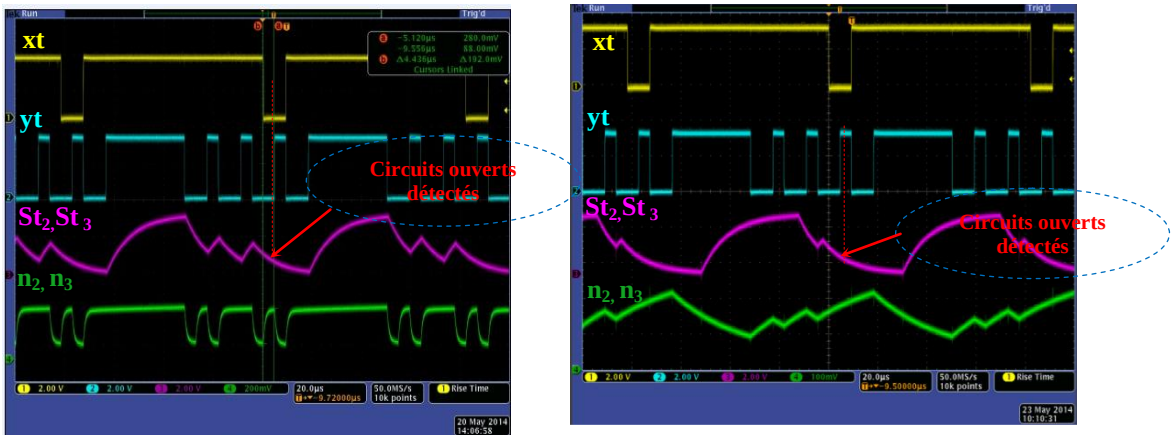
notre cas) ou bien les vecteurs ainsi générés. Le vecteur V7= [0 0] représente le vecteur de détection. Une tension de seuil V_{seuil} permettant de détecter les défauts est déterminée.
La figure 4.30 montre l'évolution du comportement des deux TMR dans le cas de différentes résistances de défaut. On constate que, les comportements dynamiques de la TMR à base ET QDI associés aux valeurs de résistance inférieures à 14,5 kΩ sont insensibles à la présence des deux défauts et donc la TMR est tolérante. Par contre, les comportements associés aux valeurs de résistances supérieures à 14,5 kΩ sont très sensibles à la présence des défauts. Par conséquent, des erreurs logiques et des dysfonctionnements sont observés au niveau du signal de sortie St et S_f durant le vecteur V7 = [00]. Dans ce cas, la résistance critique est égale R_C= 14,5 kΩ. L'augmentation du nombre de larguer de pulsation conduit à l'obtention d'une résistance critique ayant une valeur plus élevée que celle trouvée dans la détection avec une séquence de test à une seule largeur de pulsation. Autrement dit, cette observation faite avec une séquence de test à trois largeurs de pulsations a permis de mettre en évidence une technique simple qui consiste, par effet mémoire, à élargir l'intervalle de tolérance des deux défauts de circuit-ouvert.

$$ID = [14,\ 5\ k\Omega,\ \infty\ [\Rightarrow IT = [0,\ 14{,}5\ k\Omega\ [$$

Cependant, en ce qui concerne la TMR à base ET WDDL, le comportement du signal $St_{2,\ 3}$ reste correcte et le défaut n'est pas détecté et ceux quelle que soit la valeur de la résistance du défaut. Par conséquent, cela nous permet de dire que la détection avec une séquence de test à trois largeur de pulsation n'est pas efficace dans ce type d'architecture TMR à base ET WDDL. Cela confirme les résultats trouvés par les simulations Spice dans le chapitre précédent.



R= 10 kΩ



R= 14,5 kΩ

a. TMR ET WDDL b. TMR ET QDI

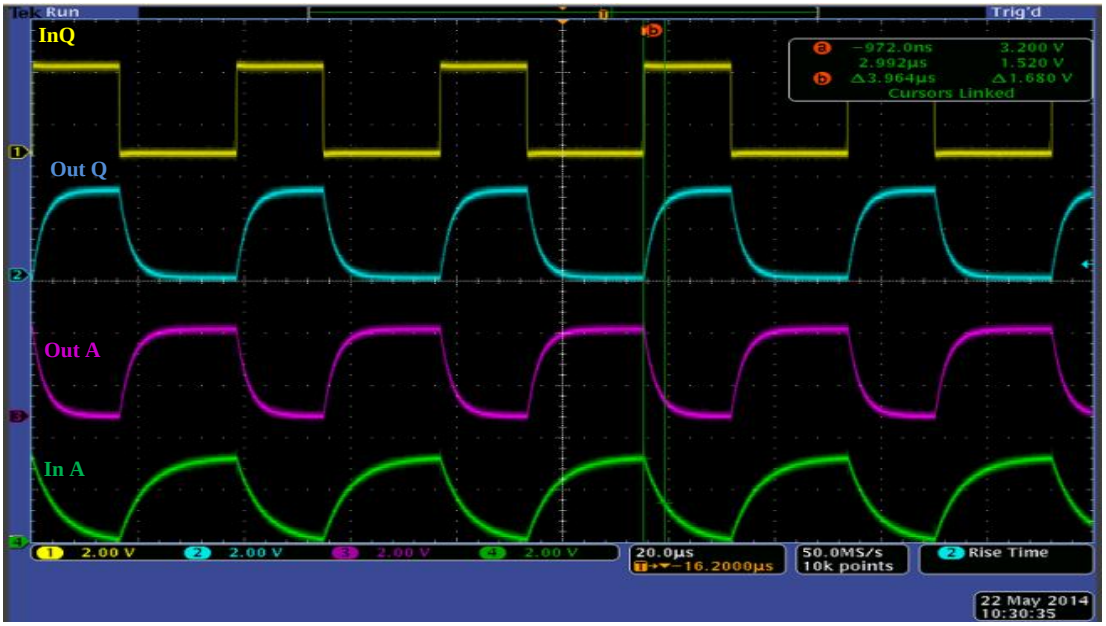
Figure 4.29 Détection et tolérance avec une séquence de test à PW3.

4.6.3 Détection et tolérance de circuit-ouvert dans le registre complet

Nous proposons d'appliquer la technique de détection avec une séquence de test à PW1 à une TMR à base de registre complet de la figure 4.26.e. Le critère de susceptibilité choisi étant le même, c'est-à- dire dès que le niveau de la sortie atteint la valeur de la tension de seuil au moment de l'arrivée du front de la pulsation, le circuit est considéré comme défaillant.

La figure 4.31 montre les résultats du comportement dynamique de la TMR ainsi traitée. Nous remarquons que la susceptibilité augmente quand la valeur de la résistance augmente, ce qui rejoint bien la théorie exposée précédemment. Pour une valeur de résistance appliquée égale à R= 3 kΩ, l'étude des signaux de sortie montre que ces derniers demeurent relativement sables mais à part un petit ralentissement des signaux et aucun changement anormal n'est détecté (figure 4.31.a). Le second cas de test consiste à augmenter la valeur de la résistance du défaut jusqu'à ce que les signaux en sortie soient dégradés. Le défaut est détecté pour une valeur de la résistance du défaut égale à 9,5 kΩ (Figure 4.36.b). Le signal de la sortie outA/ACK atteint la tension de seuil à l'arrivée du front de la pulsation du signal d'entrée InQ. Ainsi, le défaut est détecté pour cette valeur critique de R_{CO} = 9,5 kΩ. Les intervalles de détection et de tolérance sont est définis comme étant ID = [9,5 kΩ, ∞ [et IT = [0, 9,5 kΩ [.

En conclusion, nous pouvons confirmer que ce modèle de faute peut aussi être appliqué pour une structure TMR sécurisée contenant les protocoles de communication (Requête et acquittement).



a. R= 3 kΩ

b. R= 9,5 kΩ

Figure 4.30 Détection et tolérance de circuits ouverts dans la TMR à base de registre complet.

4.7 Conclusion

Nous avons présenté une méthode de test et de tolérance aux fautes des circuits sécurisés implémentés sur FPGA. Notre objectif était de concevoir et valider des modèles de fautes rapides de vérification, et utilisables pour représenter des défauts réels.

Les opérations considérées sont l'injection extérieure de fautes, permettant une analyse électrique des défauts réels, et plusieurs modifications de la description VHDL des TMR implémentées, chacune permettant de générer les vecteurs de test et de détecter les défauts selon une tension de seuil spécifique. Pour chacune des modifications, le défaut analysé est caractérisé par une série de résistances obtenue en variant la valeur de la résistance du modèle de fautes injecté.

Cette méthode a été validée sur une base de données composée de la TMR à base de circuits WDDL, de la TMR à base des circuits QDI et de la TMR à base de registre complet. Les résultats obtenus montrent l'intérêt d'une implémentation sur FPGA de la méthode que nous avons proposée. Son implémentation a été simulée en tenant compte des contraintes relatives au domaine de diviseur d'horloge. Il est fort probable que l'utilisation d'un multiplicateur d'horloge plus étendu améliore les performances de la carte FPGA. Les récents progrès technologiques, réalisés dans la conception et la fabrication des FPGA, montrent qu'une nouvelle génération de FPGA *Xilinx* procure une DCM (Digital Clock Managers) qui contient une PLL (Phase-Locked Loops) permettant la multiplication par 1000 MHz. Ces dispositifs sont pour le moment limités à un facteur de multiplication d'unités (1.5, 2, 2.5, 3, 4, 5, 8, ou 16), mais les avancées dans ce domaine laissent prévoir à moyen terme des FPGA à 1000 Mhz. Ceci permettrait d'effectuer la détection en un temps encore plus négligeable (quelques nanosecondes au lieu de quelques dizaines de nanosecondes), à condition que le dispositif d'acquisition suive la même cadence.

Nous avons démontré encore une fois que les mêmes modèles de faute utilisés pour les circuits CMOS standard peuvent être aussi appliqués pour des circuits réels sécurisés. Le banc de mesure relatif à la détection de défauts de fabrication peut être utilisé pour tout un système complexe sécurisé.

Conclusion générale

Avec la technologie de circuits intégrés actuels qui ne cesse de se développer intégrant de plus en plus de fonctionnalités complexes avec une forte densité d'intégration, l'apparition de nouveaux modes de défaillance devient importante, ce qui nécessite de nouvelles solutions de test, de fiabilité et de nouvelles techniques de détection de défauts. Par ailleurs, le test et la modélisation de défauts pour les technologies CMOS standard a reçu une attention particulière au cours de dernières années, y compris pour les technologies fortement submicroniques allant jusqu'à 45 nm. Par contre, très peu de travaux ont été menés pour le test et la modélisation de défauts des circuits utilisant la technologie CMOS classique pour des applications spécifiques, notamment dans le domaine de la sécurité (circuits cryptographiques). La solution que nous avons proposé a donc été de développer une méthode de test et de tolérance aux fautes des circuits sécurisés basée sur deux modèles de fautes de court-circuit résistif et de circuit-ouvert résistif.

Grâce aux simulations Spice réalisées, nous avons analysé l'impact de deux paires de défaut de courts-circuits résistifs et de circuits-ouverts résistifs sur le comportement électrique de la TMR à base de la porte ET WDDL et à base de la porte ET QDI. Nous avons montré que selon la valeur de la résistance de ces deux défauts de courts circuits, il existe trois intervalles de fonctionnement des TMR sécurisés. Les résultats ont également montré l'existence d'une résistance critique qui dépend de la séquence de test appliquée et pour laquelle les défauts sont détectés et les TMR ne sont pas tolérantes et donc ne sont pas fiables.

En effet, on a déterminé une résistance critique de 19 kΩ dans la TMR à base de ET QDI pour une séquence de test à trois largeurs de pulsations alors que dans la détection avec une séquence de test à une seule largeur de pulsation cette valeur critique n'était que de 5.713 kΩ. Ceci démontre que la détection et la tolérance de défauts de circuits ouverts dépend également du nombre de largeur de pulsation.

Il a été également montré que la TMR à base de ET QDI est plus robuste que la TMR à base de ET WDDL. A titre d'exemple, la valeur de la résistance critique des deux défauts de circuits ouverts mesurée dans la TMR à base de ET WDDL est légèrement inférieure à celle mesurée dans la TMR à base de ET QDI. Cette valeur est estimée à 5.325 kΩ pour la TMR à base ET WDDL et à 5,713 kΩ pour la TMR à base ET QDI.

Pour les retards de propagation engendrés par les défauts, nous avons démontré que le retard induit par ces défauts de courts-circuits résistifs et les circuits ouverts-résistifs dans la structure TMR à base de ET WDDL est très important par rapport au délai mesuré dans la TMR à base de ET QDI. Cela nous a démontré encore une fois que les structures TMR à base de circuits QDI sont les moins sensibles et les plus robustes en présence de défauts résistifs.

Pour valider cette méthode de test proposée, nous avons implémenté sur FPGA ces deux structures TMR et analysé leur comportement électrique en présence de ce type de paires de

défauts. Cela nous a permis de montrer que notre méthode de test pouvait aller encore plus loin en termes de précision donnée sur le résultat de détection

Les résultats obtenus par FPGA ont permis de montrer que notre méthode pouvait aller plus loin en précisant considérablement les conditions de détection de ces deux défauts, en réduisant les facteurs clefs, la résistance critique de détection et donc les intervalles de tolérance de défauts. Grâce à cela, les structures TMR sont suffisamment tolérantes aux défauts en particulier la structure TMR à base de ET QDI avec un intervalle de tolérance IT = [0, 4 kΩ [. L'application d'une séquence à trois largeurs de pulsations conduit à l'obtention des intervalles de tolérances plus large en particulier avec les structures TMR à base de circuits QDI.

La perspective pour nos travaux serait d'étudier et de modéliser les défauts qui affectent les technologies nanométriques sécurisées, et notamment les fluctuations des tensions de référence (ground bounce), les chutes de tension d'alimentation (IR drop) et les dérives de tension de seuil (Negative Bias Temperature Instability, NBTI).

Références bibliographiques

[Agr03] D. Agrawal, B. Archambeault, S. Chari, J. R. Rao and P. Rohatgi, "Advances in Side-Channel Cryptanalysis", RSA Laboratories Cryptobytes, Vol. 6, number 1, pages 20-32, 2003.

[Agr03a] D. Agrawal, J. R. Rao and P. Rohatgi, "Multi-channel attacks", in C. Walter, Ç. K. Koç and C. Paar, editors, Proceedings of 5th International Workshop on Cryptographic Hardware and Embedded Systems (CHES), number 2779 of LNCS, pages 2-16, 2003, Springer-Verlag.

[Ait12] G. Ait Abdelmalek, R. Ziani, M. Laghrouche, " Fault injection for verifying testability of fault tolerant structures at the Verilog level", IEEE XPLORE, Proceedings of The 24th International Conference of Microelectronics ICM 2012, December 17-20, 2012, Algiers

[Ait12] G. Ait Abdelmalek, R. Ziani and M. Laghrouche,"Study and modeling of defects in integrated circuits for their reliability analysis", IEEE XPLORE, Proceedings of the 24th International Conference of Microelectronics ICM 2012, December 17-20, 2012, Algiers.

[Ait14] G. Ait Abdelmalek, R. Ziani, "Impact Analysis of Resistive Bridge within Deep Submicron Secured CMOS Circuits", IEEE XPLORE, Proceedings of the 9th International Design and Test Symposium IDT 2014, December 16-18, 2014, Algiers.

[Ait16] G Ait Abdelmalek, R Ziani, M Laghrouche,"Testing and fault tolerance of secured circuits", International Journal of Circuits, Systems and signal processing Volume 10, 2016.

[Ala10] H. Al-Asaad, , "Efficient Techniques for Reducing Error Latency in On- line Periodic Built-in Self-Test", IEEE Instrumentation & Measurement Magazine, pp. 28-32, 2010.

[Alb04] H. Albustani, "Modelling Methods for Testability Analysis of analog Integrated Circuits Based on Pole-Zero Analysis", PhD thesis, Der Fakultät Ingenieurwissenschaften der Universität Duisburg-Essen, 06 Août 2004.

[Alh85] M.H. Al-Hussein,"Path-delay computation algorithms for VLSI systems", VLSI Design Conf., pp. 86–91, February 1985.

[All01] M.W. Allam, M.I. Elmasry, "Dynamic Current Mode Logic (DyCML): a New Low-Power High-Performance Logic Style", IEEE Journal of Solid State Circuits, vol 36, no. 3, pp 550-558, March 2001.

[Alm07] S. Almukharizim and O. Sinanoglu, "A Hazard-Free Majority Voter for TMR-Based Fault Tolerance in Asynchronous Circuits", Proc. Design and Test Workshop 2007, pp. 93-98, 2007.

[Arl79] J. Arlat, " Conception d'un microcalculateur tolérant aux fautes par diversification fonctionnelle", thèse de docteur- ingénieur, INP, Toulouse, April 1979.

[Aru05] D. Arumi, R.Rodriguez-Montanes, J. Figueras, "Defective Behaviors of Resistive Opens in Interconnect Lines", IEEE European Test Symposium, pp. 28-33, 2005.

[Ber04] M Berg, "Methodologies for Reliable Design Implementation", Washington, D.C, september 2004.

[Bon97] D. Boneh, R. A. DeMillo and R. J. Lipton, "On the Importance of Checking Cryptographic Protocols for Faults", in W. Fumy, editor, Advances in Cryptology: Proceedings of EUROCRYPT '97, number 1233 of LNCS, pages 37-51, Springer-Verlag.

[Bre74] [30] M. Breuer, " The effects of races, delays, and delay faults on test generation," IEEE Trans. on Computers, vol. c-23, pp. 1078–1092, October 1974.

[Bri93] D. Brière, P Traverse, "Airbus A320/A330/ A340 electrical flight controls- a family of tolerant systems", in Proc. 23 rd Int. Symp. On fault tolerant computing (FTCS-23), pp. 616-623, IEEE CS Press, 1993.

[Buc03] M. Bucci, L. Germani, R. Luzzi, A. Triletti, M. Varanonuovo, “A HighSpeed Oscillator-Based Truly Random Number Generator for Cryptographic Applications on a Smart Card IC”, IEEE Trans. Computers, vol. 52, no. 4, pp. 403-409, Apr. 2003.

[Buc05] M. Bucci, M. Guglielmo, R. Luzzi, A. Triletti, A Countermeasure against Differential Power Analysis based on Random Delay Insertion, Circuits and systems 2005, ISCAS 2005, Vol. 4, pp. 3547-3550, 2005.

[Caz04] J. M Cazeaux, D Rossi et C Metra, “New high speed Cmos self- cheking Voter”, Proc. of IEEE international on lin e testing symposium, pp. 58-63, 2004.

[Cha94] V. Champac et al., “Electrical model of the floating gate defect in CMOS ICs: Implications on I ddq testing”, IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems, vol. 13, No. 3, p. 359, 1994.

[Cha99] R.Chari. S. Jutla., , C. Rao, J. Rohatgi, “Towards sound approaches to counteract power-analysis attacks”, Proc. Advances in Cryptology-Crypto'99, volume 1666 of Lecture Notes in Computer Science, pp. 398-412, SpringerVerlag, 1999.

[Che78] L. Chen, A. Avizienis, “N-version programming: a fault tolerance approach to reliability of software operation”, in Proc.8 th Int. symp. On fault tolerant computing (FTCS-8), pp. 3-9, IEEE CS Press, 1978.

[Cho85] Y.H. Choi, M. Malek, “A tolerant FFT processor”, proceding of fault tolerant computing symposium, pp. 814-823, 1985.

[Chr03] M. Chrzanowska Jeske, “Between failure, reliability, yield and IC layout”, springer 2003.

[Cou08] A. Coulibaly, “ modélisation sémantique et évaluation de performances comportementales de produits en conceptoin”, mémoire d’habilitation à diriger des recherches, Université Louis Pasteur, Strasbourg I, 2008.

[Del10] D. Delahaye, "Evaluation quantitative", fascicule de cours sûreté de fonctionnement, 2009-2010.

[Ebe99] Y. Eben-Aimine, A. Richardson, C. Descleves, and K. Sommacal. GDS FaultSim, a Mixed- Signal IC Computer-Aided-Test (CAT) Tool. In IEEE Design and Test Conference in Europe, pages 232–238, Munich, Germany, March 1999.

[Eng00] N. Engin. Linking Mixed-Signal Design and Test : Generation and Evaluation of Specification-Based Tests, University of Twente in Enschede, the Netherland, 2000.

[Fic09] D. Fick, A. DeOrio, G. Chen, V. Bertacco, D. Sylvester and D. Blaauw, "A Highly Resilient Routing Algorithm for Fault Tolerant NoCs," Proc.Design, Automation and Test in Europe 2009, pp.21-26, 2009.

[Fan06] L Fang, M.S Hsiao,“Bilateral Testing of Nano-scale Fault Tolerant Circuits”, Proc. of IEEE Defect and Fault Tolerance in VLSI Systems, pp.309-317, 2006.

[Fer98] A. Ferre, “I_{DDQ} testing: state of the art and future trends”, Integration, the VLSI journal 26, pp 167-196, 1998.

[Gan01] K. Gandolfi , C. Mourtel and F. Olivier, “Electromagnetic Analysis: Concrete Results”, in Ç. K. Koç, D. Naccache and C. Paar, editors, Proceedings of 3rd International Workshop on Cryptographic Hardware and Embedded Systems (CHES), number 2162 of LNCS, pages 251-261, 2001, Springer-Verlag.

[Gei90] M. Geilert, J. Alt, and M. Zimmermann, “On the efficiency of the transition fault model for delay faults,” Int. Conf. on Computer-Aided Design, pp. 272–275, November 1990.

[Ger09] José Luis Garcia Gervacio,“An Aware Methodology to Evaluate Circuit Testability for Small Delay Defects“, thèse de doctorat Tonantzintla, Puebla, Mexico, 2009.

[Gol04] J. Dj. Golic and R. Menicocci,“Universal masking on logic gate level”, Electronics Lett., vol. 40, no. 9, April 2004.

[Gro10] M. Grosso, M.S. Reorda, M. Portela-Garcia, M. Garcia-Valderas, C. Lopez-Ongil, L. Entrena, “An On-line Fault Detection Technique Based on Embedded Debug Features”, IEEE 16th International On-Line Testing Symposium (IOLTS),pp. 167-172, 2010.

[Haf90] M. Hafezparast, “Fault tolerant hardware designs and their reliability analyses”, thèse de doctorat, Brunel university, the university of west London, 1990.

[Ham05] K.Hamidi, O. Malassé and J.F.Aubry, “Coupling of information-flow aggregation method and dynamical model for a more accurate evaluation of reliability”. In Proc. of the European Safety and Reliability Conference (ESREL05), Poland, June 2005.

[Hao91] H. Hao and E.J. McCluskey, “Resistive shorts within CMOS gates”, International Test Conference, pp. 292–301, 1991.

[Har95] R. Harvey, A. Richardson, and H. Kerho, “Defect Oriented Test Developement Based on Layout inductive Fault Analysis”, In IEEE International Mixed-Signal Testing Workshop (IMSTW’05), pages 2–9, 1995.

[Has01] M. A. Hasan, “Power Analysis Attacks and Algorithmic Approaches to Their Countermeasures for Koblitz Curve Cryptosystems”, IEEE Trans. Computers, vol. 50, no. 10, pp. 1071-1083, Oct. 2001.

[Haw94] C.F. Hawkins et al, “Defect classes - an overdue paradigm for CMOS IC testing”, ITC, p. 413, 1994.

[Hay83] T. Hayashi, K. Hatamaya, K. Sato, and T. Natabe, “A Delay Test Generator for Logic LSI,” IEEE International Test Conference, pp. 560–571, 1983.

[Hit82] R. B. Hitchcock, G. L. Smith, and D. D. Cheng, “Timing analysis of computer hardware”, IBM Journal Research and Development,vol. 26, no. 1, pp. 100–105, January 1982.

[Hou09] N. Houarche, “Modélisation de défauts paramétriques en vue de tests statiques et dynamiques”, thèse de doctorat, Université Montpellier II, Octobre 2009.

[Hue93] J. Huertas, “Test and Design for Testability of Analog and Mixed-Signal Integrated Circuits: Theoretical Basis and Pragmatical Approaches”. In In Circuit Theory and Design : Selected Topics in Circuits and Systems. D.G. Haigh, J.L. Huertas, P.A. Humblet, M. Kunt, Elsevier Science Publishers, 1993.

[Jam01] C. M. James, Li, Chao-Wen Tseng, E.J. McCluskey, “Testing for Resistive Opens and Stuck Opens”, ITC, 2001, 1049-1058

[Kho07] A. Khouas, “Test de systèmes électroniques”, fascicule de cours, École polytechnique Montréal, Automne 2007.

[Koc96] P. C. Kocher, “Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems”, In Neal Koblitz, editor, Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings, number 1109 in Lecture Notes in Computer Science, pages 104-113. Springer, 1996.

[Koc99] P. Kocher., Jaffe J., and B. Jun, “Differential power analysis”, Proc. Advances in Cryptology (CRYPTO '99), Lecture Notes in Computer Science, vol. 1666, Springer-Verlag, 1999, pp. 388-397

[Krs98] A. Krstic and K.-T. T. Cheng, “Delay Fault Testing for VLSI Circuits”. Kluewer Academic Publishers, 1998.

[Lah83] S. Laha, J.H. Patel, "Error correction in arithmetic operations using time redundancy", proceeding of fault tolerant computing symposium, pp. 298-305, 1983.

[Lat13] A. Latoui, F. Djahli , “An Optical BILBO for On-Line Testing of Embedded Systems “, IEEE design & test of computers , Vol. PP, N°: 99, March 2013, pp. 1-12.

[Leh07] T. Lehtonen, P. Liljeberg and J. Plosila, "Online Reconfigurable Self-Timed Links for Fault Tolerant NoC," VLSI Design, vol. 2007, Article ID 94676, 2007.

[Li89] W. N. Li, S. M. Reddy, and S. K. Sahni, “On path selection in combinational logic circuits,” IEEE Trans. on Computer-Aided Design, vol. 8, no. 1, pp. 56–63, January 1989.

[Li03] Z. Li, X. Lu, W. Qiu, W. Shi, and D. M. H. Walker, “A circuit level fault model for resistive opens and bridges,” VLSI Test Symposium, pp. 379–384, 2003.

[Li03a] Z. Li, X. Lu, W. Qiu, W.Shi, and D.M.H. Walker, “A Circuit Level Fault Model for Resistive Bridges”, ACM Transactions on Design Automation of Electronic Systems, Vol. 8, No. 4, October 2003.

[Lin87] J. C. Lin and S. M. Reddy, “On Delay Fault Testing in Logic Circuits,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 6, pp. 694–703, 1987.

[Lyo62] R. E.Lyons, W. Vanderkulk, “The Use of Triple-Modular Redundancy to Improve Computer Reliability", IBM Journal of Research and Development, 6 (2), pp.200-209, Avril 1962. http://www.ccs.neu.edu/course/csg712/resources/Lyons-Vanderkulk-62.pdf

[Mak86] G. Maki, P. Owsley, K. Cameron, J. Venbrux, "VLSI reed solmon decoder design", military communications conference, IEEE volume 3, pp.46.5.1- 46.5.2, octobre 1986.

[Men03] R. Menicocci and J. Pascal, “Elaborazione crittografica ca di dati digitali mascherati”, Italian patent IT MI0020031375A, July 2003.

[Met93] C. Metra, M. Favalli, P. Olivo, B. Ricco, “Testing of Resistive Bridging Faults in CMOS Flip-Flop”, Proc. Europe Test Conference, pp. 530-531, 1993.

[Mil92] L. Milor, Fault-driven analog testing. Ph.d. dissertation, University of California, Berkeley, Calif, 1992.

[Mil98] L.-S. Milor. A tutorial introduction to research on analog and mixed-signal circuit testing. In IEEE transactions on Circuits and Systems-II : Analog and Digital Signal Processing, 45(10) :1389–1407, October 1998.

[Mon02] R.Rodriguez-Montanes and J. P. de Gyvez, “Resistance characterization for weak open defects ” , IEEE Design and Test , Sept.2002,pp:18-25 .

[Moo00] W. Moore, G. Gronthoud, K. Baker and M.Lousberg, Delay-fault testing and defects in sub-micron Ics-does critical resistance really mean, anything, ITC,2000,95-104.

[Mou00] S. Mourad and Y. Zorian, “Principles of Testing Electronic Systems”, John Wiley & Sons, Somerset, NJ, 2000.

[Nat01] National Institute of Standards and Technology, FIPS -197: Advanced Encryption Standard, November 2001.

[Pap11] G. Papa, A.T.T. Garbolino, “ Optimal On-Line Built-In Self-Test Structure for System-Reliability Improvement”, IEEE Congress on Evolutionary Computation (CEC), pp. 222-229, 2011.

[Par87] E. S. Park and M. R. Mercer, “Robust and Nonrobust Test for Path Delay Faults in a Combinational Circuit,” IEEE International Test Conference, pp. 1027–1034, 1987.

[Ple86] V. Pless, "Decoding the golay codes", Information theory, IEEE transactions on volume 32, Issue 4, pp.561-567, juillet 1986.

[Pop05] T. Popp and S. Mangard, “Masked Dual-Rail Pre-Charge Logic: DPAResistance without Routing Constraints”, Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES '05), Lecture Notes in Computer Science, vol. 3659, Springer-Verlag, pp. 172-186, 2005.

[Pop06] T.Popp and S. Mangard,“Implementation Aspects of the DPA-Resistant Logic Style MDPL”, Proc. IEEE Int.l Symp. Circuits and Systems (ISCAS '06), pp. 2913-2916, 2006.

[Pop07] T. Popp, M. Kirschbaum, T. Zefferer and S. Mangard, “Evaluation of the Masked Logic Style MDPL on a Prototype Chip”, Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES '07), Lecture Notes in Computer Science, vol. 4727, Springer-Verlag, pp. 81-94, 2007.

[Pra88] A. K. Pramanick and S. M. Reddy, “On the Detection of Delay Faults”, IEEE International Test Conference, pp. 845–856, 1988.

[Qui01] J. Quisquater and D. Samyde, “Electromagnetic analysis (EMA): Measures and countermeasures for smart cards”, in I. Attali and T. Jensen, editors, Proceedings of Smart Card Programming and Security (E-smart 2001), number 2140 of LNCS, pages 200-210, 2001, Springer-Verlag.

[Ran75] B. Randell, “System structure for software fault tolerance”, IEEE transactions on software engineering, SE-1, SE-1(2), pp. 220-232, juin 1975.

[Ran03] W. Rankl and W. Effing, “Smart Card Handbook” Third Edition, John Wiley & Sons, 2003.

[Rat04] G.B. Ratanpal, R.D. Williams and T.N. Blalock, “An On-Chip Signal Suppression Countermeasure to Power Analysis Attacks”, IEEE Transactions On Dependable And Secure Computing, Vol. 1, no.3, July-September 2004.

[Rod02] R. Rodriguez-Montanes, P. Volf and J. Pineda de Gyvez, “Resistance characterization for weak open defects”, IEEE Design & Test of Computers , Vol. 19, n°5, pp. 18-26, 2002.

[Rom03] C. Roman, S. Mir, and B. Charlot, “Building an analog fault simulation tool and its application to MEMS”, In Microelectronics Journal, 34(10) :897–906, 2003.

[Sar98] V.R. Sar-Dessai and D.M.H. Walker, “Accurate Fault Modeling and Fault Simulation of Resistive Bridges”, International Symposium Defect and Fault Tolerance in VLSI Systems, pp. 102-107, 1998.

[Sar99] V.R. Sar-Dessai and D.M.H. Walker, “Resistive Bridge Fault Modeling, Simulation and Test Generation”, Proc. International Test Conference, pp. 596-605, 1999.

[Sch02] S. Schulz, J. W. Rozenblit, K.J. Buchenrieder, “Multilevel Testing for Design Verification of Embedded Systems”, IEEE design and test of computer, pp.60-69, 2002.

[Sco02] S. P. Scorabogatov and R. J. Anderson, “Optical fault induction attacks”, in B. S. Kaliski Jr., Ç. K. Koç and C. Paar, editors, Proceedings of 4th International Workshop on Cryptographic Hardware and Embedded Systems (CHES), number 2523 of LNCS, pages 2-12, 2002, Springer-Verlag.

[Sha00] A. Shamir, “Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies”, Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES '00), Lecture Notes in Computer Science, vol. 1965, Springer-Verlag, pp. 71-77, 2000.

[Sha01] D. Shaw, D. Al-Khalili, and C. Rozon, “Accurate CMOS bridge fault modeling with neural network-based VHDL saboteurs”, International Conference on Computer Aided Design, pp. 531–536, 2001.

[Shi05] T. Shimoda,“Introduction of TFT R&D Activities in Seiko Epson Corporation”, 2005. http://www.holtronic.ch/White_papers/SE2005_1.pdf.

[Sie92] D. P. Siewiorek, R.S.Swarz, “Reliable Computer Systems, Design and Evaluation”, second edition, 1992.

[Smi85] G. L. Smith, “Model for Delay Faults Based upon Path”, IEEE International Test Conference, pp. 342–349, 1985.

[Sun99] S. Sunter and N. Nagi, “Test metrics for analog parametric faults”. In 17th IEEE VLSI Test Symposium, pages 226–234, 1999.

[Ten85] N. N. Tendolkar, “Analysis of timing failures due to random ac defects in VLSI modules,” Design Autom. Conf., pp. 709–714, June 1985.

[Tha11] H.D. Thacker, O.O. Ogunsola, , A.V. Muler, , J.D. Meindl, , “Wafer Testing of Optoelectonic–Gigascale CMOS Integrated Circuits”, IEEE Journal of Selected Topics in Quantum Electronics, VOL. 17, NO. 3, pp. 659-670, 2011.

[Tir02]K. Tiri, M. Akmal, and I. Verbauwhede, “A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards”, in Proc. of ESSCIRC '02, 2002.

[Tir04] K. Tiri and I. Verhauwhede, “A Logic Design Methodology for a Secure DPA Resistant ASI C or FPGA Implementation”, in Proc.Design, Automation and Test in Europe Conference andExpositionDATE 04), pp. 246-251, 2004.

[Tir04a] K. Tiri and I. Verbauwhede, “Place and route for secure standard cell design”, Proc. Smart Card Research and Advanced Application IFIP Conf. (CARDIS '04), 2004.

[Tri02] E. Trichina, E. De Seta, L. Germani, “Simplified Adaptive Multiplicative Masking for AES and its secure implementation”, in Cryptographic Hardware and Embedded Systems: CHES 2002, Vol. 2523 of Lecture Notes in Computer Science, pp. 277-285, Springer-Verlag, 2002.

[Var97] P. Variyam and A. Chatterjee. Test Generation for Comprehensive Testing of Linear Analog Circuits Using Transient Response Sampling. In International Conference on Computer- Aided Design (ICCAD ’97), p.p. 382–385, 9-13 Novembre 1997.

[Ver02] T. Verdel and Y. Makris, “Duplication-Based Concurrent Error Detection in Asynchronous Circuits:Shortcomings and Remedies”, Proc. IEEE Int. Symp.Defect and Fault Tolerance in VLSI Systems 2002. pp.345-353, 2002.

[Vil97] A. Villemeur, “Sureté de fonctionnement des systèmes industriels”, Edition Eyrolles, 1997.ISSN : 0399-4198.

[Wen03] J. Wen-Ben, H. Der-Chen and S.R. Das, “An Efficient BIST Method for Non-Traditional Faults of Embedded Memory Arrays”, IEEE Transactions on Instrumentation and Measurement, Vol. 52, NO. 5, October 2003

[Wil81] T. Williams and N. Brown, “Defect Level as a Function of Fault Coverage”, IEEE Transactions on Computers, Vol. C-30, N°.12, 1981, pp. 987–988.

[Yam96] H. Yamazaki, and Y. Miura, “IDDQ Testability of Flip-flop Structures”, IEEE International Workshop on IDDQ Testing, pp.29-33, 1996.

PRODUCTION SCIENTIFIQUE

G. Ait Abdelmalek, R Ziani, M Laghrouche, "Testing and fault tolerance of secured circuits", International Journal of Circuits, Systems and signal processing Volume 10, 2016.

G. Ait Abdelmalek, R. Ziani, "Impact Analysis of Resistive Bridge within Deep Submicron Secured CMOS Circuits", IEEE XPLORE, Proceedings of The 9th International Design and Test Symposium IDT 2014, December 16-18, 2014, Algiers.

G. Ait Abdelmalek**,** R. Ziani, M. Laghrouche, "Fault injection for verifying testability of fault tolerant structures at the Verilog level", IEEE XPLORE, Proceedings of The 24th International Conference of Microelectronics ICM 2012, December 17-20, 2012, Algiers

R. Ziani, G. Ait Abdelmalek, M. Laghrouche, "Study and modeling of defects in integrated circuits for their reliability analysis", IEEE XPLORE, Proceedings of The 24th International Conference of Microelectronics ICM 2012, December 17-20, 2012, Algiers

G. Ait Abdelmalek**,** R. Ziani, M. Laghrouche, "Testing and fault tolerance of integrated circuits", American Academic & Scholarly Research Journal, Vol. 4, N° 5, Sept 2012

G. Ait Abdelmalek, R. Ziani**,** "Design for Reliability and Manufacturing Yield", World Academy of Science, Engineering and Technology issue 71 2012, pp. 1498-1501, Proceedings of the International Conference on Electrical, Computer, Electronics, Communication Engineering, ICECECE 2012, November 28-29, 2012, Paris