Conception des interfaces sécurisées pour contrôle-commandes de puissance

N. Zaidan

INSTITUT NATIONAL POLYTECHNIQUE DE GRENOBLE

N° attribué par la bibliothèque

/__/__/__/__/__/__/__/__/__/__/

THESE

Pour obtenir le grade de

DOCTEUR DE L'INPG

Spécialité : Microélectronique

Préparée au laboratoire : **T**echniques de l'**I**nformatique et de la **M**icroélectronique pour l'**A**rchitecture d'ordinateurs

dans le cadre de **l'Ecole Doctorale : «** ELECTRONIQUE, ELECTROTECHNIQUE, AUTOMATIQUE, TELECOMMUNICATIONS, SIGNAL **»**

présentée et soutenue publiquement

par

Nidal ZAIDAN

Le 27 mai 2002

CONCEPTION DES INTERFACES SECURISEES POUR CONTRÔLE-COMMANDES DE PUISSANCE

Directeur de thèse : Michel NICOLAÏDIS

Jury

M. René DAVID	Président
M. Abbas DANDACHE	Rapporteur
M. Stanislaw J. PIESTRAK	Rapporteur
M. Michel NICOLAÏDIS	Directeur de thèse
M. Dominique BIED-CHARRETON	Examinateur

A mon fils……..Nawar

Remerciements

Le travail présenté dans cette mémoire a été effectué au sein de l'équipe « Systèmes Intégrés Sûrs» du laboratoire Technique de l'Informatique et de la Microélectronique pour l'Architecture d'ordinateur (TIMA) de l'Institut National Polytechnique de Grenoble (INPG)

Je suis très honoré d'avoir préparé cette étude au laboratoire TIMA dirigé par Monsieur Bernard COURTOIS, directeur de recherche au CNRS, directeur du laboratoire TIMA que je remercie de m'avoir accueilli dans son laboratoire.

Je suis très reconnaissant envers Monsieur Michel NICOLAÏDIS, mon directeur de thèse, pour ses conseils, ses encouragements, son aide et sa bonne humeur, qui m'ont été d'un soutien très précieux que je n'oublierai jamais, « Merci chef ».

Je suis très honoré de la présence à mon jury de thèse et je tiens à remercier :

- Monsieur René DAVID, directeur de recherche au CNRS, pour l'honneur qu'il m'a fait en acceptant de présider mon jury de thèse.

- Monsieur Abbas DANDACHE, professeur à l'université de Metz, ainsi que Monsieur Stanislaw J. PIASTRAK, professeur à l'université de Wroclaw de Pologne, pour l'honneur qu'ils m'ont fait d'avoir accepté d'examiner mon travail et de participer à mon jury de thèse en qualité de rapporteur.

- Monsieur Dominique BIED-CHARRETON, Ingénieur à l'Institut National de Recherche sur les Transports et leurs Sécurités (INRETS) pour l'honneur qu'il m'a fait d'avoir participé à mon jury de thèse.

Enfin, je voudrais remercier tous les membres du laboratoire TIMA et tous les amis que j'ai côtoyés durant cette thèse.

TABLE DES MATIERES

INTRODUCTION GENERALE ……...1

I. INTERFACES SECURISEES IMPLEMENTEES EN VLSI.……4

I.1 INTRODUCTION…….6

I.2 INTERFACES DE CONTROLE D'ACTIONNEURS A HAUTE SECURITE INTEGREES EN VLSI.……...6

I.2.1 DEFINITIONS DE BASE..……..7

I.3 CIRCUITS STRONGLY FAIL-SAIFE UTILISANT UN CODAGE EN FREQUENCE...…….....10

I.4 MECANISME DE VERROUILLAGE A L'ETAT SUR..……...13

I.4.1 INDICATEURS D'ERREUR STABLES..…… …13

I.4.2 CIRCUIT DE CONVERSION D'INDICATION D'ERREUR..…… …...16

I.4.3 FONCTIONS COMPLEXES STRONGLY FAIL-SAFE ET STRONGLY SAFE-DISJOINT..……..18

I.4.4 IMPLEMENTATION DU CONVERTISSEUR D'INDICATION D'ERREUR..……...20

I.5 CONCLUSION..…….…24

II. LE CAPTEUR DE COURANT INTEGRE..…….25

II.1 INTRODUCTION..…….26

II.2 UTLISATION DES CAPTEURS DE COURANT DANS DES SYSTEMES CRITIQUES EN SECURITE..…….…..26

II.3 ESTIMATION DE COURANT DE FUITE..……29

II.3.1 LA METHODE D'ESTIMATION DU COURANT I_{DDQ}..……30

II.3.1.1 LE COURANT I_{REF}..……..33

II.4 CONCEPTION D'UN CAPTEUR DE COURANT INTEGRE (BICS).....34

II.4.1 CONFIGURATION D'UN COMMUTATEUR DUAL (BYPASS DUAL)..38

II.4.2 LE COMPARATEUR DU BICS..……..40

II.5 IMPLEMENTATION ELECTRIQUE DU BICS..……..42

II.5.1 CONCEPTION DU PREMIER BY-PASS BS1 ET SON CIRCUIT DE COMPENSATION CBC..……...43
II.5.2 CONCEPTION DU COMPARATEUR..……44
II.6 CONCLUSION..……..46
III. LES TECHNOLOGIES DE PUISSANCE INTELLIGENTES..……..….48
III.1 INTRODUCTION..……..49
III.2 L'ISOLATION BASSE TENSION / PUISSANCE..…….51
III.2.1 LA TECHNIQUE DE L'ISOLATION PAR JONCTION..…….51
III.2.2 LA TECHNIQUE DE L'ISOLATION DIELECTRIQUE..……54
III.2.3 LA TECHNIQUE DE L'ISOLATION RESURF..……..55
III.2.4 LA TECHNIQUE D'AUTO-ISOLEMENT...……..55
III.3 LE CHOIX D'UNE TECHNOLOGIE DE PUISSANCE INTELLIGENTE..……57
III.4 LE COMMUTATEUR DE PUISSANCE EN TECHNOLOGIES DE PUISSANCE INTELLIGENTES..……..58
III.4.1 LE TRANSISTOR DE PUISSANCE LDMOS..…….61
III.4.1.1 LE REGIME DE FONCTIONNEMENT..……..…..61
III.4.1.2 AIRE DE SECURITE..……...63
III.4.2 COMMANDE DE GRILLE DE TRANSISTOR DMOS..……..64
III.5 LA TECHNOLOGIE 0.8 MM HV CMOS DE AMS..……..70
III.6 CONCLUSION..……...….71
IV. INTERFACE SECURISEE DE PUISSANCE DANS LE CADRE DE PROJET ISIS..……73
IV.1 INTRODUCTION..……..74
IV.2 INTERFACE DE CONTROLE D'ACTIONNEUR POUR LES SYSTEMES DUPLIQUES..…….……...74
IV.3 INTERFACE SFAS DE CONTROLE D'ACTIONNEUR POUR LES SYSTEMES TMR..……...76
IV.4 RECAPITULATIF DES MECANISMES ASSURANT L'OBJECTIF « ULTIMATE FAIL-SAFE »..……77
IV.5 IMPLEMENTATION POUR UNE SECURITE ACCRUE..……78
IV.5.1 IMPLEMENTATION DE CONTROLEUR DOUBLE-RAIL..……...……79

IV.5.2 L'IMPLEMENTATION D'INDICATEUR D'ERREUR..……...80
IV.5.3 L'INSERTION DU BICS DANS L'INTERFACE..…….82
IV.5.4 L'IMPLEMENTATION DE CONVERTISSEUR LOGIQUE BASSE TENSION / PUISSANCE..……86
IV.5.5 IMPLEMENTATION DE CONVERTISSEUR PUISSANCE / LOGIQUE BASSE TENSION..……...88
IV.6 COMPATIBILITE DES INTERFACES FAIL-SAFE AVEC DES SYSTEMES ELECTRONIQUES SECURISES..……...91
IV.7 METHODOLOGIE DE DEMONSTRATION DE LA SECURITE..……...94
IV.8 DYNAMISATION..……..100
IV.8.1 LA COUVERTURE DES FAUTES..……..……....106
IV.9 LAYOUT GLOBAL ET CONCLUSION..…….……....107
CONCLUSION GENERALE…….109

INTRODUCTION GENERALE

Au cours de ces dernières années, les techniques de test des circuits intégrés ne cessent de croître pour répondre d'une part, aux exigences de qualité, de fiabilité et de sécurité imposées par le marché, et d'autre part, aux progrès de la technologie des circuits intégrés qui sont devenus de plus en plus complexes. Par ailleurs, dans certaines applications de sécurité, un mauvais fonctionnement d'un élément du circuit, aussi infime, peut engendrer des situations critiques ou même catastrophiques. Une défaillance, dont l'effet local n'est pas critique peut, si elle n'est pas détectée, contaminer d'autres unités du système, et de ce fait, avoir une conséquence catastrophique. Il est donc essentiel de considérer le test des circuits intégrés dès leur conception non seulement pour assurer la détection de fautes de fabrication, mais aussi pour garantir en cas de fautes survenant pendant la durée de vie du circuit, un niveau de fiabilité requis pour l'application donnée. Cette exigence est d'autant plus importante s'il s'agit d'une application critique en sécurité. Pour une telle application, il sera indispensable d'assurer qu'une défaillance ne produira pas des situations dangereuses. Des techniques de test en-ligne pourront mettre en place lors de la conception du circuit pour garantir cette propriété.

POSITION DU PROBLEME

Le but de cette étude est de développer et de valider une famille de circuits d'interfaces sécurisées produisant des sorties de puissance, et pouvant être utilisés comme périphériques assurant le contrôle des actionneurs dans les transports ferroviaires. Une stratégie d'intégration de ce type d'interface sécurisée sera élaborée.

Les architectures informatiques sont maintenant largement utilisées dans les transports guidés pour réaliser des fonctions de sécurité : signalisation, contrôle de vitesse, pilotage automatique et commande-contrôle des itinéraires. Ces architectures peuvent être décomposées en deux parties : le cœur qui réalise les traitements par le biais des divers logiciels et la périphérie qui permet de communiquer avec l'extérieur. Ces communications sont de plusieurs types :

- acquisition ou générations de grandeurs booléennes (Tout ou Rien : TOR),

- échange de messages codés,

- lecture de balises situées le long de la voie,

- élaboration de la position instantanée des mobiles.

Le cœur est constitué de plusieurs unités centrales architecturées et/ou programmées de façon à obtenir le niveau de sécurité requis ; la périphérie se compose d'un grand nombre de cartes. Ces cartes sont réalisées en sécurité intrinsèque au moyen de composants discrets ou de circuits hybrides[1].

Le fait de pouvoir disposer de cartes électroniques d'acquisition des entrées et de génération de sorties plus compactes, devrait pouvoir conduire non seulement à une réduction des volumes occupés, mais également, par le fait même, à une augmentation de disponibilité et à une réduction des coûts. Cette considération du volume occupé et de son impact sur les coûts est important pour les raisons suivantes :

- à bord des trains, on a généralement un nombre limité d'entrées et de sorties TOR, mais en revanche, on dispose de très peu de place.

- dans les équipements au sol, le volume occupé n'est pas une donnée critique ; en revanche, le nombre d'entrées et de sorties TOR est très élevé puisqu'il faut acquérir la position des trains, commander la signalisation ainsi que les itinéraires et de plus effectuer les contrôles nécessaires au fonctionnement de l'ensemble en sécurité.

Les équipements développés en France sont souvent à base de processeur codé et n'utilisent donc que des cartes spécifiques. Lorsqu'il s'agit de traiter des séquences codées, on peut utiliser des circuits intégrés du commerce ou des ASIC [2] ; en revanche, dans tous les autres cas, la technologie utilisée est soit à base de composants discrets, soit à base de circuits hybrides étant donné la difficulté de concevoir des circuits intégrés capables en cas de défaillance de produire des signaux qui prennent soit des valeurs correctes soit des valeurs non dangereuses. Il est toutefois clair que le gain en volume, la disponibilité et le coût, qui peuvent apporter une technologie, permettent de réaliser ces parties par des circuits intégrés.

Grâce aux techniques de conception des interfaces « Fail-Safe » développées au laboratoire TIMA au sein du groupe « Systèmes Intégrés Sûrs », l'implémentation en technologie de puissance intelligente des interfaces d'entrée et de sortie devient possible. Ces interfaces appelées, « Fail-Safe »**,** ne délivrent que des informations correctes ou sûres. Les travaux présentés dans ce manuscrit concernent la conception de telles interfaces conçues dans une technologie de type « Smart Power », afin de générer de commandes d'actionnaires

sécurisés et fournissant le niveau de puissance requis pour contrôler divers type d'actionneurs utilisés le contrôle ferroviaire.

Ces travaux ont été menés au laboratoire TIMA dans le cadre du projet ISIS (Interface de Sécurité Intégrée sur Silicium) sous le contrôle technique de l'INRETS (Institut national de recherche sur les transports et leurs sécurités), qui a assuré par ailleurs son financement

Le premier chapitre de cette mémoire présente les alternatives de conception des interfaces de sécurité en VLSI qu'on peut envisager pour atteindre un très haut niveau de sécurité requise.

Le deuxième chapitre est réservé à la présentation du circuit de capteur du courant dénommé BICS dans les publications anglo-saxonnes. Ce circuit permet de mesurer le courant de fuite d'un sous-circuit. On peut détecter par ce dispositif les défauts qui pourront produire des niveaux indéterminés, par un phénomène de division de tension**.**

Le troisième chapitre présente les technologies de puissance intelligentes « Smart Power »**,** développées par plusieurs fabricants des semi-conducteurs. Ces technologies permettent d'intégrer sur la même puce des circuits logiques et analogiques complexes de basse tension, ainsi qu'une gamme étendue d'éléments de commutation de haute tension et de puissance. L'intégration des circuits d'interfaces sûre en technologies de puissance intelligentes, permet de réduire leur coût d'implémentation et d'optimiser leurs performances.

Le quatrième chapitre montrera une architecture d'interface sécurisée de puissance, développée dans le cadre du projet ISIS. Les différentes unités de cette interface utilisées afin d'atteindre un très haut niveau de sécurité, seront présentées en détail.

PREMIER CHAPITRE

INTERFACES SECURISEES IMPLEMENTEES EN VLSI

1 INTRODUCTION

Chaque actionneur d'un système sécuritaire doit être contrôlé par un signal unique qui doit rester sûr en présence de défaillances *(Fail-Safe)*, c'est à dire qu'en cas de défaillance son état est soit correct, soit sûr. Les systèmes intégrés auto-contrôlables en ligne (*Self-Checking*) fournissent des groupes de signaux codés en sortie. Ces groupes de signaux ne permettent pas d'assurer le contrôle direct des actionneurs, car chaque actionneur est contrôlé par un seul signal qui doit être individuellement sûr. A cause de cette exigence particulière, il n'était pas possible dans le passé d'implémenter en VLSI toutes les parties d'un système sécuritaire.

En fait, les systèmes sécuritaires existants sont divisés en deux parties : un système auto-contrôlé ou tolérant aux pannes (qui utilise par exemple un code détecteur d'erreur, une technique de duplication, triplication ou un processeur codé), et une interface Fail-Safe utilisant des composants discrets. Cette interface transforme les sorties du système de traitement en signaux *Fail-Safe*. Outre l'inconvénient des interfaces à composants discrets d'être très encombrantes et coûteuses, la probabilité de défaillance est augmentée et la durée de vie du système est diminuée par rapport à l'implémentation VLSI, ce qui limite la disponibilité du système. Il est donc intéressant d'intégrer en VLSI les interfaces *Fail-Safe*, capables d'assurer le contrôle sécuritaire des actionneurs.

2 INTERFACES DE CONTROLE D'ACTIONNEURS A HAUTE SECURITE INTEGRES EN VLSI

Cette étude décrit une famille d'interfaces sécuritaires implémentables en VLSI pour le contrôle direct des actionneurs. Ces interfaces utilisent soit un codage en fréquence soit un codage de puissance pour représenter l'état non-sûr, permettant ainsi d'éviter les états non-sûrs dus aux défaillances affectant les sorties de l'interface (e.g. collages des sorties au niveau logique '0' ou '1'). Des techniques de redondance sont rajoutées pour éviter les états non-sûrs dus aux fautes affectant les composants de l'interface. Des mécanismes d'autocontrôle sont adoptés ensuite pour détecter les fautes et assurer le blocage irréversible du circuit dans l'état sûr.

Dans un premier temps, la nouvelle technique de conception d'interfaces sécuritaires est utilisée pour réaliser une fonction simple, à savoir le comparateur *Strongly Fail-Safe* (SFaS). Pour les fonctions plus complexes (e.g. circuit de vote majoritaire, indicateur d'erreur) les valeurs des signaux d'entrée utilisées durant l'opération de l'interface ne peuvent révéler qu'une partie des fautes. Pour contourner ce problème, ces fonctions complexes seront implémentées en utilisant plusieurs branches de comparateurs SFaS. Les sorties de ces branches sont combinées par une logique générant la sortie de la fonction complexe (logique de recombinaison). Un théorème [3], discuté dans la section 4.3 montre que la fonction complexe est SFaS, si chacune des branches est SFaS. Ainsi la conception des fonctions complexes SFaS peut reposer sur la conception SFaS de la fonction simple du comparateur. On exploite ensuite cette technique pour implémenter les fonctions de surveillance des interfaces sécuritaires livrant des signaux de puissance, qui sont donc aptes de contrôler les actionnaires sans utilisation de circuits intermédiaires.

2.1 DEFINITIONS DE BASE

Avant de présenter les détails des implémentations proposées, quelques définitions sont nécessaires pour garantir la sécurité de façon formelle.

Définition 1 : un circuit G est sécurisé en présence de faute pour un ensemble de fautes F, si pour chaque faute f de cet ensemble et pour tout vecteur d'entrée du circuit G, sa sortie est soit correcte soit sûre.

L'ensemble f doit inclure toutes les fautes susceptibles de survenir dans une technologie donnée. Selon la définition 1, si une faute f_1 appartenant à F survient, le circuit G produira soit des sorties sûres soit des sorties correctes. La sécurité est ainsi assurée pour une première faute. Néanmoins, si la première faute reste indétectable pour longtemps, une deuxième faute f_2 pourra survenir. Mais, en présence de la faute double f_1, f_2, il n'est pas garanti que le circuit produit toujours des sorties correctes ou sûres. La propriété d'autotest, définie ci-dessous, prend alors tout son intérêt.

Définition 2 : un circuit G est auto-testable (*Self-Testing*) pour un ensemble de fautes F, s'il dispose d'un mécanisme de détection de fautes tel que, pour chaque faute f appartenant

à F, il y a au moins un vecteur d'entrée de G qui déclenche la détection de F par ce mécanisme de détection.

En combinant la propriété *Fail-Safe* et *Self-Testing* on obtient la propriété *Totally Fail-Safe* (TFS).

Définition 3 : un circuit est *Totally Fail-Safe* pour un ensemble de fautes F s'il est à la fois *Fail-Safe* et *Self-Testing* pour F.

Un circuit TFS pourra produire une sortie erronée sans pour autant déclencher un signal de détection d'erreur. Cette erreur non détectable ne compromet pas la sécurité tant qu'elle aboutit à un état de sortie sûre. En se basant sur cette observation, on peut définir l'objectif dont les circuits TFS cherchent à assurer.

Totally Fail-Safe Goal : Jusqu'à la première détection de faute toutes les sorties erronées sont sûres.

Les circuits TFS assurent cet objectif si on assume l'hypothèse suivante :

Hypothèse H1 :

1. Les fautes de l'ensemble F surviennent une par une.
2. Entre l'occurrence de deux fautes successives il se passe un temps suffisamment long pour que tous les vecteurs nécessaires pour détecter les fautes de F surviennent sur les entrées de G.

Cette hypothèse est réaliste étant donné que les mécanismes de défaillances sont des phénomènes lents. Ainsi la probabilité d'apparition simultanée de deux ou plusieurs fautes est très faible, et l'intervalle de temps qui s'écoule entre l'occurrence de deux fautes est suffisamment grand pour permettre l'application d'un ensemble d'entrées détectant toutes les fautes. Néanmoins, le concepteur doit veiller à éviter les causes de fautes en mode commun et doit s'assurer d'une dynamisation régulière et fréquente des entrées du circuit.

Les circuits TFS représentent une sous-classe de circuits assurant l'objectif TFS. La classe la plus large de circuits assurant cet objectif est défini ci-dessous. La définition est récursive similairement aux définitions *Strongly fault secure* [4][5] et *strongly code disjoint* (SCD) [6] utilisées dans la théorie des circuits auto-contrôlables.

Définition 4 *:* un circuit G est SCD pour un ensemble de fautes F si, pour toute faute f appartenant à F, soit :

1. G est TFS soit,
2. G est *Fail-Safe* et si une nouvelle faute appartenant à F survient, alors, pour la faute multiple résultant, le cas 1 ou le cas 2 est vrai.

L'objectif dit TFS goal assure la propriété *Fail-Safe* jusqu'au moment où la première détection de faute survient. Néanmoins, le but ultime est de s'assurer que le système ne produit pas des sorties erronées non sûres, même après la première détection de faute, et malgré de nouvelles fautes qui pourraient éventuellement survenir. Cet objectif est présenté ci-dessous.

***Ultimate Fail-Safe Goal* :** Tant que le système est en service, toute sortie erronée est sûre.

En pratique, afin d'assurer cet objectif la première détection de faute sera exploitée pour bloquer le système dans l'état sûr de façon irréversible, c'est-à-dire indépendamment des événements qui pourraient se produire par la suite (tels que occurrence de nouvelles fautes par exemple). Le mécanisme utilisé convertit le signal de détection de faute en un signal *Fail-Safe* qui coupe l'alimentation du circuit de façon irréversible par l'intermédiaire de circuits externes conçus en sécurité intrinsèque.

3 CIRCUITS STRONGLY FAIL-SAFE UTILISANT UN CODAGE EN FREQUENCE

Les interfaces développées au sein de l'équipe « Systèmes Intégrés Sûrs » fourniront des signaux *Fail-Safe* destinés au contrôle des actionneurs. Afin de s'affranchir d'une électronique coûteuse, l'interface sera donc réalisée dans une technologie permettant d'implémenter dans un seul circuit intégré des fonctions logiques et analogiques de basse tension ainsi que des composants de puissance. On s'intéresse donc à des interfaces dont l'état non sûr en sortie est codé par la présence d'une puissance (P = V x I) élevée.

Néanmoins, la surveillance de ces interfaces sera réalisée par un mécanisme produisant une sortie *Fail-Safe* codée en fréquence. Ce mécanisme de surveillance est d'une

importance capitale dans la démarche de sécurité adoptée. On commence donc par étudier les circuits *Fail-Safe* codés en fréquence, car ces circuits seront utilisés pour réaliser le mécanisme de surveillance.

Etant donné que dans les circuits intégrés on a une probabilité non négligeable qu'un nœud soit collé à l'une ou à l'autre des valeurs logiques 0 ou 1, l'état non sûr des sorties de l'interface ne peut pas être codé dans une valeur logique. On peut choisir donc de représenter l'état non sûr par la présence d'une fréquence ou d'un niveau de puissance élevé. L'utilisation d'un codage en fréquence est considéré dans cette section, c'est-à-dire la présence d'impulsions d'une gamme de fréquence *Fe* est utilisée pour représenter le niveau logique non-sûr (par convention, '1') et l'absence de cette fréquence représente le niveau logique sûr (par convention, '0'). Une interface *Fail-Safe* réalise la conversion des signaux codés en voltage (*S1, S2, … Sn*) en signaux codés en fréquence (*O1, O2, … On*).

Une première solution pour assurer la propriété *Fail-Safe* d'une sortie *Oi* ($i \in \{1,2, \ldots n\}$) est d'utiliser une porte AND qui déconnecte la sortie *Oi* du générateur d'impulsions de fréquence *Fe* chaque fois que le système de traitement fournit un signal de commande Si correspondant à l'état sûr (niveau logique 0). Dans ce cas, une faute *stuck-on* 1 du signal Si connecte la sortie de manière permanente au signal de fréquence *Fe*. Cela conduit à la présence permanente de l'état non-sûr en sortie. Donc, le circuit d'interface codé en fréquence n'est pas *Fail-Safe*. Pour éviter ce type de faute nous pouvons recourir à l'utilisation des portes doubles connectées en série, qui coupent le transfert de fréquence de la source *Fe* à la sortie *Oi* en deux points distincts, chaque fois que Si est à l'état sûr. Ainsi, une faute ne peut connecter le signal de fréquence *Fe* à la sortie *Oi* si les signaux d'entrée portent l'état sûr. La Figure 1 représente un exemple d'interface *Fail-Safe* codée en fréquence pour un système dupliqué (comparateur *Fail-Safe*).

Ce schéma utilise une porte NAND et une porte NOR pour contrôler la coupure du signal de fréquence *Fe*. Le fonctionnement normal du système fait propager la fréquence *Fe* à la sortie de l'interface pour les valeurs $S_1 = 1$, $S_1^* = 1$, correspondant à l'état non-sûr. Les valeurs $S_1 = 0$, $S_1^* = 0$ donnent l'état sûr qui déconnecte la fréquence *Fe* de la sortie. Une vérification simple montre qu'il n'y a pas de faute simple qui connecte la fréquence *Fe* en sortie. Donc, l'interface est sûre pour les fautes simples.

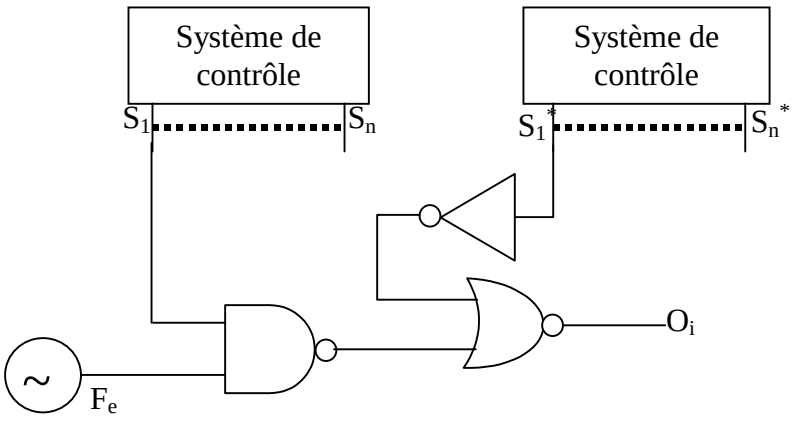


Fig. (1) : Interface autocontrôlable pour un système dupliqué.

Pour implémenter la propriété SFaS, nous utilisons, comme mentionné précédemment, une approche autocontrôlable (*Self-Checking*). Une façon d'assurer ce contrôle consiste à dupliquer l'interface et à comparer les deux parties pour détecter l'apparition de fautes. Pour assurer la validité de la technique, il est nécessaire ensuite d'imposer deux contraintes supplémentaires :

1) Durant le fonctionnement normal du système, les éléments de l'interface reçoivent tous les signaux nécessaires pour détecter les fautes qui, autrement non détectées, pourront invalider sa propriété SFaS.

2) Les effets des fautes (les erreurs générées) sont propagés aux nœuds observables des circuits dupliqués (et par la suite aux entrées du circuit d'autocontrôle).

Un premier constat est que la condition 1 n'est pas assurée par l'interface de la Figure 1. En fait, le système de la Figure 1 ne peut pas vérifier, durant le fonctionnement normal, si la porte NOR déconnecte la sortie O_1 du générateur de fréquence *Fe*. Cependant, la porte NAND est vérifiée de manière exhaustive durant l'opération normale du système. Ainsi, la condition 1 est respectée pour cette porte. D'autre part, la porte NOR reçoit les valeurs d'entrée 00, 01 et 11, mais elle nécessite l'application des valeurs d'entrée 00, 01 et 10 pour qu'elle soit testée. Cette condition est accomplie suite à l'inversion du signal de sortie de la porte NAND, comme présenté en Figure 2. En outre, pour assurer la condition 2, l'interface est dupliquée et les sorties des portes NANDs et NORs sont vérifiées par un circuit contrôleur double-rail, comme celui proposé en [7] vérifiant la propriété *Totally Self-Checking*. Ce

circuit vérifie toutes les branches de l'interface correspondant aux sorties O_1, O_2, … O_n, et fournit sur g_1, g_2 une indication d'erreur codée en double-rail (g_1g_2 = 10 ou 01 pour l'indication de fonctionnement correct et g_1g_2 = 11 ou 00 pour l'indication d'erreur).

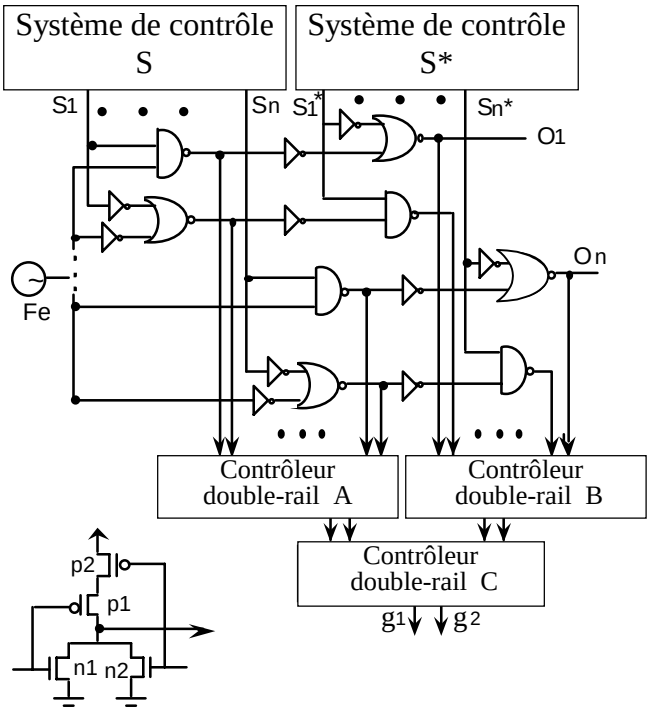


Fig. (2) : Comparateur SFaS pour un système dupliqué à *n* sorties

et schéma électrique d'une porte NOR CMOS.

Proposition 1: L'interface de figure 2 est SFaS pour les fautes du type collage logique de ligne (*stuck-at)*, transistor collé passant (*stuck-on)* et transistor collé ouvert (*stuck-open).*

La démonstration de cette proposition est fournie en [3]. La démonstration ne considère pas les court-circuits pour lesquels une simulation électrique ainsi qu'une action au niveau topologique doivent être faites. Cette analyse sera considérée pendant la phase de génération du 'layout'.

4 MECANISME DE VERROUILLAGE A L'ETAT SUR

Comme illustré dans la section précédente, l'interface *Fail-Safe* devient SFaS par le biais des fautes détectées par le contrôleur double-rail et signalées aux sorties g_1, g_2. Cette propriété garantit l'objectif TFS. Pourtant, pour assurer l'objectif *Ultimate Fail-Safe*, nous devons nous assurer que, après la première détection de faute, les signaux de sortie de l'interface sont *Fail-Safe* pour toute nouvelle faute ou séquence de fautes survenues dans n'importe quelle partie du système. Pour assurer ce but, la détection de faute indiquée par les signaux g_1, g_2 sera utilisée pour bloquer le système de manière irréversible dans l'état sûr, même si de nouvelles fautes surviennent plus tard, affectant n'importe quelle partie du système, y compris des fautes affectant le mécanisme de blocage. Ce mécanisme est basé sur l'utilisation d'un circuit d'autocontrôle - l'indicateur d'erreur - qui mémorise toute indication d'erreur signalée par les signaux g_1, g_2. Ensuite, un circuit transpose l'indication d'erreur codée en double-rail en signal codé en fréquence. Finalement, un circuit réalisé en sécurité intrinsèque coupe l'alimentation du système si le signal codé en fréquence indique une erreur.

4.1 INDICATEURS D'ERREUR STABLES

Dans un premier temps une détection de faute signalée par les signaux d'indication d'erreur g_1g_2 doit être mémorisée afin d'avoir le temps de couper l'alimentation et décharger les capacités des lignes d'alimentation du circuit. Tant que ces capacités ne sont pas déchargées le circuit pourra sortir de cet état de blocage.

La mémorisation de la détection d'erreur est effectuée par un circuit appelé indicateur d'erreur. Plusieurs configurations d'indicateurs d'erreur ont été décrites dans la littérature publiée. Gaitanis [8] propose, par exemple, un indicateur d'erreur asynchrone composé d'un contrôleur double-rail et de quatre circuits latch. Nanya et Kawamura [9] utilisent deux portes logiques XOR et quatre circuits latch D dans une configuration d'indicateur d'erreur synchrone. Pour nos besoins, nous avons adopté un circuit synchrone utilisant un contrôleur double-rail et deux bascules D[3], présenté dans la figure 3.

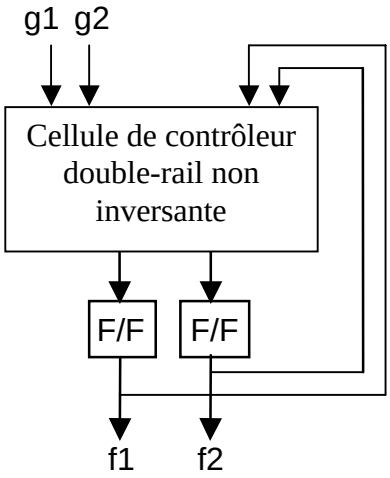


Fig. (3) : Le circuit indicateur d'erreur

La cellule du contrôleur double-rail utilise une configuration de non inversion (au nombre pair d'inversions logiques entre les entrées et les sorties de la cellule). Quatre implémentations possibles sont présentées en Figure 4.

Un indicateur d'erreur conçu comme montré dans les figures 3 et 4 possède les propriétés suivantes :

1) Concernant une détection de faute externe à l'indicateur d'erreur :

a) Dès qu'une détection de faute est signalée aux entrées (code g1g2 = 00 ou 11), les sorties f1, f2 sont aussi commutées dans un des deux états détecteurs d'erreur 00 ou 11 et ils sont verrouillés dans ces états pour tout changement ultérieur aux entrées g1, g2. Cela signifie que l'indication d'erreur est mémorisée.

b) Si l'indication d'erreur est mémorisée, l'état des sorties f1, f2 peut changer seulement une fois : de 00 à 11 pour les cellules 11-dominantes des figures 4a et 4b et de 11 à 00 pour les cellules 00-dominantes des figures 4c et 4d.

2) Détecte et mémorise les fautes affectant ses nœuds internes :

a) Les fautes de type nœud collé affectant la cellule de contrôleur double-rail ou les latches de sortie sont détectables. Ils génèrent l'indication hors-code 00 ou 11 aux sorties f1, f2 si le code d'entrée g1g2 est 10 ou 01. Une séquence d'entrée 01, 10, 01, 10 appliquée aux entrées g1, g2 résulte dans l'application de quatre combinaisons du code d'entrée de la cellule du contrôleur double-rail, indépendamment de l'état initial des latches D. Ceci permet, par la

suite, de détecter toutes les fautes internes. D'une manière plus générale, toute séquence d'entrée incluant d'une part au moins deux codes 10 et d'autre part au moins deux codes 01 séparés par un nombre impair de codes 10, détecte toutes les fautes mentionnées précédemment. Cela signifie que l'indicateur d'erreur est auto-testable suite à l'utilisation des valeurs caractérisant l'opération normale du système.

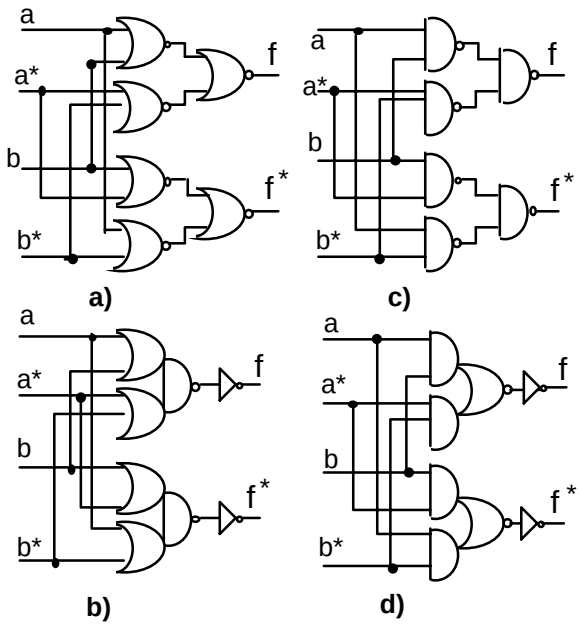


Fig. (4) : Contrôleur double-rail au nombre pair d'inversions en implémentation CMOS : (a), (b) 11-dominant et (c), (d) 00-dominant.

b) L'état d'indication d'erreur en sortie suite à la détection de faute décrite au 2.a est mémorisé dans les latches D de sortie.

c) Les signaux hors-code obtenus aux sorties f1, f2 ne changent pas : ils gardent indéfiniment les valeurs mémorisées, 00 ou 11.

Un indicateur d'erreur caractérisé par les propriétés 1.b et 2.c sera dénommé indicateur d'erreur stable.

Il est à noter que les cellules du contrôleur double-rail de la figure 4 sont SCD pour les stuck-at [7]. Elles le sont aussi pour les stuck-open car ces fautes sont détectables si on applique les vecteurs de test des stuck-at dans un ordre spécifique (cet ordre sera assuré par

les circuits de dynamisation). Concernant les stuck-on, la cellule a- de la figure 4 est aussi SCD à cause de la faible résistance du réseau des transistors n par rapport au réseau des transistors p [10]. Pour des raisons similaires, la cellule b- est aussi SCD pour les stuck-on. Dans cette cellule le réseau p présente une résistance inférieure à celle du réseau n (un seul transistor connecte la sortie de la porte NAND au Vdd, tandis que cette sortie est connectée à la masse par l'intermédiaire de deux transistors n en série).

4.2 CIRCUIT DE CONVERSION D'INDICATION D'ERREUR

L'indication d'erreur mémorisée sur les sorties *f1*, *f2* de l'indicateur d'erreur doit être utilisée pour bloquer/verrouiller le système à l'état sûr de manière irréversible, (c'est-à-dire même en cas d'occurrence de nouvelles fautes dans le système). Pour ce faire, le signal d'indication d'erreur sera transposé en signal *Oe* codé en fréquence. Les valeurs *f1f2 =01* ou *10* sont transposées en la présence d'une fréquence *Fe* sur *Oe* tandis que les valeurs *f1f2 = 00* ou *11* sont transposées en l'absence de cette fréquence sur *Oe*. Afin de faire cette conversion de façon sécuritaire le circuit de conversion doit vérifier certaines propriétés, définies dans la suite.

En premier lieu, un convertisseur d'indication d'erreur doit transformer les valeurs du code double-rail (*01* et *10*) en une sortie non sûre (e.g. fréquence *Fe*), et les valeurs en dehors du code double-rail (i.e. 00 et 11) en une sortie sûre (absence de *Fe*). Cette correspondance disjoint de valeurs de code/hors-code en valeurs non sûres/sûres détermine la propriété *Safe-Disjoint* d'un circuit de conversion.

Définition 7: Un circuit est '*Safe-Disjoint*' s'il convertit chaque valeur appartenant à son code d'entrée en une sortie non-sûre, et chaque valeur n'appartenant pas à son code d'entrée en une sortie sûre.

En cas d'une détection de faute (correspondant en une valeur en dehors du code d'entrée du convertisseur), le convertisseur *Safe-Disjoint* produit l'état sûr à sa sortie (e.g. absence de *Fe*). Cette valeur est utilisée pour bloquer le système à l'état sûr. En cas de non-détection de faute (i.e. valeur dans le code d'entrée de convertisseur), le convertisseur *Safe-Disjoint* fournit à sa sortie l'état non-sûr (présence de *Fe*). Cette valeur de sortie laisse le système libre de délivrer aux actionneurs les résultats de ces opérations. Ainsi, si l'état sûr est

produit par erreur à la sortie du convertisseur, au moment ou une indication d'erreur est livrée à l'entrée du convertisseur, le système peut délivrer des valeurs dangereuses aux signaux de contrôle des actionneurs. Cette situation dangereuse peut survenir à cause d'une faute affectant le convertisseur. Pour éviter une telle situation le convertisseur peut posséder la propriété *self-testing*. Un convertisseur *Safe-Disjoint* et *Self-Testing* sera appelé *Totally Safe Disjoint* (TSD).

Néanmoins, il ne sera pas nécessaire de détecter toutes les fautes du convertisseur. Sa mission étant de transposer une entrée hors code en une sortie sûre, les fautes ne compromettant pas cette mission, peuvent rester indétectables. On arrive de façon naturelle à la propriété *Strongly Safe Disjoint* (SSD)

Définition 8 *Strongly Safe-Disjoint* (SSD) : Un circuit de conversion G est *Strongly Safe-Disjoint* pour un ensemble de fautes F s'il est *Safe-Disjoint* et si pour toute faute $f \in F$ il est :

a) auto-testable (*self-testing*), ou

b) il reste capable de convertir chaque entrée hors code à une sortie sûre, et si une nouvelle faute appartenant à F survient, le cas a) ou b) est vrai.

La propriété définie ci-dessus permet la détection des fautes dangereuses affectant le convertisseur. L'indication d'erreur produite par le convertisseur doit aussi bloquer le système à l'état sûr. Pour ce faire cette indication doit être injectée dans le convertisseur. De plus, ce dernier, bien qu'il soit affecté par une faute, doit transposer cette indication d'erreur en une sortie sûre. La définition suivante décrit la propriété requise.

Définition 9 *Strongly Fault-Safe Disjoint* (SFSD) : Un convertisseur de signaux G est *Strongly Fault-Safe Disjoint* pour l'ensemble F de fautes s'il est *safe-disjoint* et, pour toute faute $f \in F$,

il est auto-testable (*Self-Testing*) et il reste capable de convertir toute entrée hors code à l'état sûr de sortie, ou

il reste capable de convertir toute entrée hors-code à l'état sûr de sortie, et si une nouvelle faute survient, le cas 1 ou 2 est vrai.

Nous pouvons observer qu'un circuit SSD qui, après l'occurrence de la première faute détectable, préserve sa capacité de fournir le niveau sûr en sortie pour toute entrée hors code est un circuit SFSD.

4.3 FONCTIONS COMPLEXES STRONGLY FAIL-SAFE ET STRONGLY SAFE-DISJOINT

La propriété SFaS du comparateur de systèmes dupliqués de la figure 2 est atteinte car il a été possible d'obtenir une implémentation assurant le test de portes logiques par les entrées appliquées au comparateur durant son utilisation normale. Cependant, pour des fonctions plus complexes, il sera pratiquement impossible d'atteindre ce but. Deux théorèmes de base présentés dans [3] nous permettent de résoudre ce problème. Le premier théorème concerne la construction de fonctions complexes ayant la propriété SFaS en utilisant des fonctions simples SFaS. Ce théorème est utilisé dans [3] pour construire des circuits de vote SFaS en utilisant comme brique de base le comparateur SFaS. Par la suite, nous nous sommes intéressés au deuxième Théorème qui concerne les convertisseurs SSD. Il sera utilisé pour construire le convertisseur d'indication d'erreur. La définition suivante est nécessaire pour introduire ensuite le théorème.

Définition 10 *Fail-Passif* (FP) : Un circuit G est *Fail-Passif* (FP) par rapport à un état de sortie E et à un ensemble de fautes F si et seulement si, pour toute faute simple ou multiple de F, l'état E n'est jamais reproduit aux sorties de G, sauf si E est appliqué sur une ou plusieurs entrées de G.

Le terme *Fail-Passif* est utilisé en analogie aux notions bien connues des circuits actifs et passifs (e.g. filtres passifs). En effet, un circuit électrique passif n'est pas connecté aux lignes d'alimentation. Ainsi, il ne peut fournir de l'énergie à ses sorties que si l'énergie est appliquée sur ses entrées. De manière similaire, un circuit *Fail-Passif* ne fournit pas l'état E en sortie (correspondant généralement à l'état non-sûr), même si le circuit est défaillant, sauf si l'état E est également appliqué à ses entrées. Le circuit *Fail-Passif* peut être réalisé en choisissant un état E qui peut être produit seulement si un certain signal portant cet état est connecté aux entrées du circuit.

Un circuit de conversion complexe G peut être réalisé en utilisant un bloc qui combine les sorties de plusieurs convertisseurs plus simples $f_1, f_2, \ldots f_k$ qui sont SSD

Théorème : On considère un convertisseur G réalisé à l'aide de plusieurs convertisseurs élémentaires $f_1, f_2, \ldots, f_k$ de telle manière que :

1) G a le même état non-sûr en sortie que les convertisseurs $f_1, f_2, \ldots, f_k$.

2) Durant son opération en absence de faute, la sortie de G est à l'état non-sûr chaque fois que la sortie d'un ou plusieurs convertisseurs élémentaires $f_1, f_2, \ldots, f_k$ est à l'état non-sûr.

3) L'union des espaces des codes d'entrée de tous les convertisseurs f_i est égale à l'espace de code d'entrée de G.

4) G est implémenté en recombinant les sorties des convertisseurs $f_1, f_2, \ldots, f_k$ par le biais d'un bloc (dénommé bloc de recombinaison par la suite) qui est *Fail-Passif* par rapport à l'état non-sûr, et aucune source de l'état non-sûr n'est connectée à ce bloc mis à part les sorties des fonctions de $f_1, f_2, \ldots, f_k$.

Alors, si les implémentations des fonctions $f_1, f_2, \ldots, f_k$ vérifient la Définition 6, l'implémentation de G est un convertisseur SSD.

Ce théorème est démontré dans [3].

Dans la section suivante, nous allons utiliser ce théorème pour concevoir une implémentation SSD pour la fonction XOR, utilisée dans le convertisseur d'indication d'erreur. Cette fonction ne reçoit pas tous les vecteurs nécessaires pour son test durant le fonctionnement normal. Ainsi, des fautes qui détruisent la propriété SSD demeurent non-détectables. Pour contourner ce problème, la structure de convertisseur établie utilise le comparateur SFaS présenté dans la section 3 et une logique de recombinaison. Toutes les fautes non-testées durant le fonctionnement normal sont concentrées dans la logique de recombinaison, et grâce au théorème précèdent nous n'avons pas besoin de nous occuper de ces fautes.

Ce théorème nécessite aussi l'implémentation d'un bloc de recombinaison *Fail-Passif*. Cette contrainte peut être satisfaite facilement pour la plupart des états non-sûrs utilisés dans la pratique. Par exemple, l'état non-sûr correspond à une source de tension

d'alimentation élevée et/ou de haute puissance. Dans ce cas, la propriété *Fail-Passif* peut être obtenue automatiquement grâce au principe de conservation d'énergie. Dans le cas où on utiliserait une gamme de fréquences pour représenter l'état non-sûr, alors les fautes de type *stuck-at*, *stuck-on* ou *stuck-open* ne peuvent pas entraîner cette fréquence à la sortie d'un circuit logique tant que cette fréquence n'est pas appliquée à l'une de ses entrées. D'autre part, les fautes de type court-circuit peuvent créer des boucles de contre-réaction. Si une telle boucle a une parité d'inversion impaire, elle pourra conduire à une oscillation. Dans ce cas, nous pouvons déterminer par simulation les fréquences d'oscillation produites par ces fautes. La gamme de fréquences correspondant à l'état non-sûr est ensuite choisie de manière à ne pas inclure ces fréquences. Des changements de conception topologique du circuit peuvent être également utilisés pour éviter l'apparition de court-circuits induisant des boucles d'oscillation. Suite à tels changements nous pouvons garantir la propriété de passivité du circuit en présence de fautes (*Fail-Passiveness*).

4.4 IMPLEMENTATION DU CONVERTISSEUR D'INDICATION D'ERREUR

L'indication d'erreur mémorisée aux sorties *f1 f2* de l'indicateur d'erreur sera convertie de façon sécuritaire en un signal *Oe* codé en fréquence.

Le signal *Oe* sera utilisé pour couper de façon irréversible l'alimentation du système en tension continue. Les valeurs de code *f1f2* = 01 ou 10 (*f1* XOR *f2* = 1) connectent la sortie *Oe* au générateur de fréquence *Fe*, et les valeurs hors-code *f1f2* = 00 ou 11 (*f1* XOR *f2* = 0) coupent le signal de fréquence *Fe* et isolent la sortie *Oe*. En d'autres termes, pour générer le signal *Oe*, nous pouvons utiliser une porte XOR qui reçoit aux entrées les signaux *f1*, *f2*. Le niveau 0 en sortie de la porte XOR est utilisé pour déconnecter *Oe* de *Fe*. Pour que la propriété SSD soit assurée, la voie du signal *Fe* est déconnectée de *Oe* en deux points. Une manière directe de satisfaire cette contrainte est d'utiliser deux indicateurs d'erreur, deux portes XOR et deux portes de transmission contrôlées par les deux sorties des portes XOR. Cependant, les portes XOR ne sont pas testées, car *f1* et *f2* prennent seulement les valeurs 10 et 01 durant le fonctionnement normal (sans défaillance), alors que toutes les quatre séquences d'entrée 10, 01, 00, 11 sont nécessaires pour tester une fonction XOR à deux

entrées. On constate également que la porte de transmission contrôlée par la sortie d'une porte XOR n'est pas testée, car la sortie XOR prend toujours la valeur logique 1 durant le fonctionnement normal. Cette situation nous suggère l'utilisation du théorème présenté dans la section précédente. La figure 5 présente le schéma du convertisseur double-rail/codage fréquence obtenue en utilisant ce théorème.

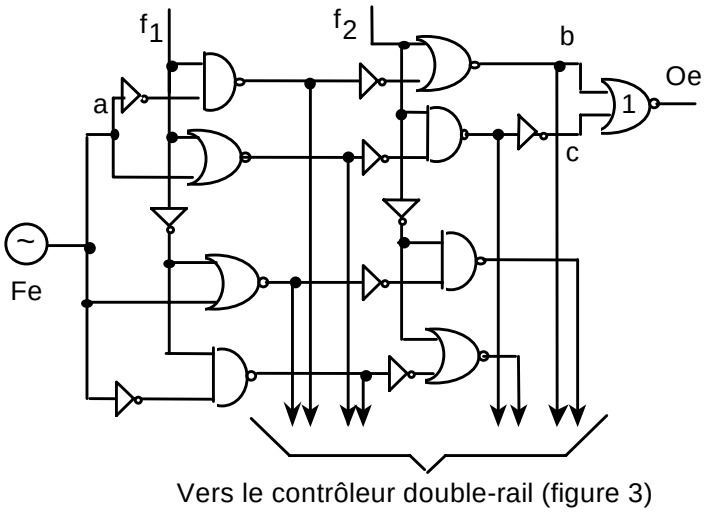


Fig. (5) : Implémentation SSDdu convertisseur de signal double-rail en signal codé en fréquence

Pour appliquer ce théorème, nous avons partagé la fonction en deux branches. Chaque branche a une fonction similaire au circuit de la figure 2. Une des branches propage la fréquence *Fe* pour le code d'entrée *f1f2* = 01. Ainsi, la combinaison logique 01 représente l'espace de code d'entrée pour cette branche et les trois autres combinaisons forment l'espace hors-code. L'autre branche propage la fréquence *Fe* pour *f1f2* = 10 (l'espace de code).

Nous pouvons facilement vérifier que chaque branche est *Safe-Disjoint*. Les sorties des deux branches sont recombinées à l'aide d'une fonction logique NOR (marquée 1 en figure 5) pour générer le signal *Oe*. Cette porte est nommée logique de recombinaison. De façon similaire à la figure 2, deux branches redondantes sont rajoutées, comme montré en figure 5. Chaque branche et sa paire redondante sont testées à l'aide de l'espace de code d'entrée *f1f2* = 10 et *f1f2* = 01 correspondant au fonctionnement normal, de la même manière que le circuit de la figure 2 est testé par les codes d'entrée 11 et 00. Ainsi, chaque branche est un

convertisseur TSD. Nous pouvons maintenant vérifier facilement que le convertisseur double-rail/codage en fréquence vérifie toutes les conditions du théorème de la section 4.4. Par conséquent, il est SSD.

Il reste à noter que la coupure simultanée des deux branches de signal, a-b et a-c, est sûre et stable en régime statique pour les deux combinaisons d'entrées hors-code, *f1f2* = 00 et *f1f2* = 11, mais les transitions éventuelles entre les deux combinaisons hors-code 00 et 11 peuvent générer des aléas en b ou c dus aux temps de propagation des signaux. Ces aléas vont apparaître en *Oe*. Si des transitions successives de signaux hors-code *f1f2* de 00 à 11 et de 11 à 00 se succèdent à des fréquences de répétition particulières, cela peut résulter en la présence d'un signal de fréquence *Fe* à la sortie *Oe*. Cependant, les propriétés 1b et 2c de l'indicateur d'erreur stable donnent, pour une conception respectant les schémas des figures 3 et 4, tout au plus une transition, de 00 à 11 ou de 11 à 00 (indicateurs d'erreurs stables). Ainsi, une situation d'aléas dynamiques telle que décrite précédemment ne peut pas apparaître. Cette propriété n'est pas assurée si l'indicateur d'erreur est implémenté par une cellule de contrôleur double-rail ayant un nombre impair d'inversions. Dans une telle situation, les valeurs logiques en sorties f1, f2 peuvent changer de 00 à 11 et de 11 à 00 sans restriction. De tels indicateurs d'erreur ne doivent pas être utilisés pour implémenter le mécanisme proposé. Nous observons également en figure 5 que les quatre paires de signaux double-rail ont des valeurs corrélées, ce qui fait que, s'ils sont injectés aux entrées d'un contrôleur double-rail, celui-ci ne sera pas testé exhaustivement. En effet, ces signaux sont injectés au contrôleur double-rail de la figure 2. En fusionnant les signaux double-rail de la figure 5 et ceux de la figure 2 et en les vérifiant à l'aide des contrôleurs A et B, toutes les cellules des contrôleurs seront dynamisées.

Tel qu'il est représenté, le convertisseur de la figure 5 est SSD. Néanmoins un convertisseur doit être SFSD (Définition 9) pour garantir que la détection de ses propres fautes assure le verrouillage du circuit dans l'état sûr. Comme discuté au dernier paragraphe de la section 4.2, un convertisseur SSD qui après l'occurrence de la première faute détectable, reste capable de convertir toutes les entrées hors-code en sorties sûres, est un convertisseur SFSD. Pour notre implémentation, cette propriété sera obtenue en utilisant deux convertisseurs double-rail/codage en fréquence connectés en série, comme montré en figure 6. Ainsi, quand la première faute détectable survient dans un des deux convertisseurs, elle

n'affecte pas la capacité de l'autre convertisseur de couper la propagation de la fréquence *Fe* à la sortie *Oe*.

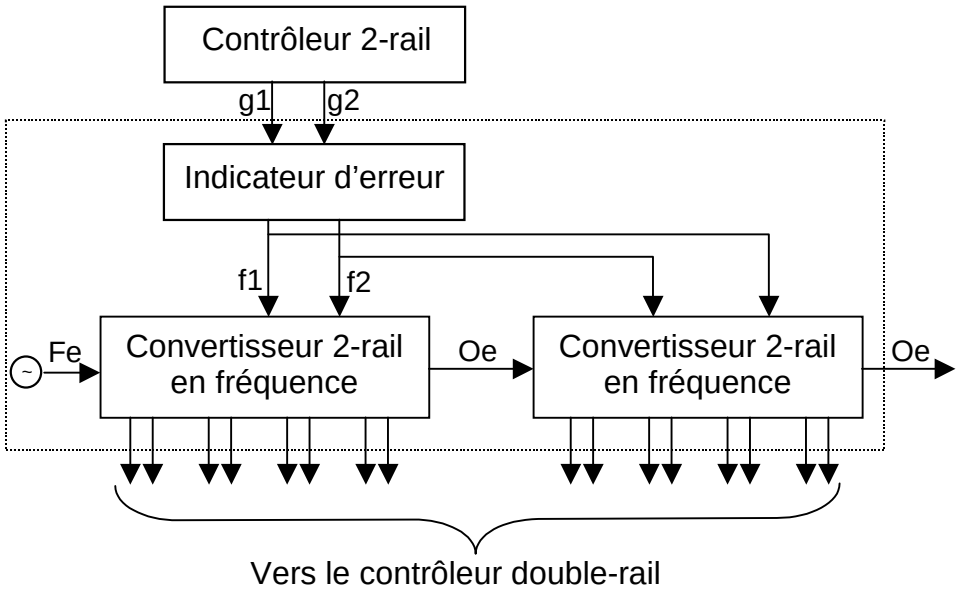


Fig. (6) : Indicateur d'erreur SFSD

Dans la figure 6 on peut aussi voir comment le convertisseur se connecte avec l'indicateur d'erreur et le contrôleur double-rail. Le dernier assure la fusion en une seule paire de signaux double-rail *g1g2*, de tous les signaux double-rail de l'interface, y compris ceux fournis par le convertisseur. Cette indication d'erreur unique (*g1g2*) est mémorisée par l'indicateur d'erreur. Ce circuit fournit l'indication d'erreur mémorisée (*f1f2*) qui compose les entrées du convertisseur. Ce dernier transforme cette indication d'erreur (*f1f2*) en une sortie *Oe* codée en fréquence. *Oe* génère un état sûr (absence de fréquence Fe) quand une faute est détectée dans n'importe quelle partie du système.

Le signal de sortie en fréquence *Oe* est utilisé pour couper la tension d'alimentation du système en cas de défaillance. La coupure de l'alimentation est activée par l'absence du signal de fréquence *Fe* à la sortie *Oe*. Le verrouillage du système, en cas de défaillance, est irréversible dans l'état sûr, et ceci même en cas d'occurrence de fautes ultérieures.

5 CONCLUSION :

Dans ce chapitre, nous nous sommes intéressés à étudier l'implémentation des interfaces *Fail-Safe* en VLSI. Cette implémentation nous permet d'éviter les inconvénients majeurs des interfaces à composants discrets tels que l'encombrant et le coût élevé.

Après avoir présenté le concept de démonstration de sécurité d'une telle interface implémentée en VLSI, nous nous sommes rappelés de quelques définitions de base. Par la suite, la technique d'implémentation des interfaces sécuritaires a été abordée afin de réaliser finalement une interface SFSD. La sécurité requise suggère, en cas de défaillance, de verrouiller le système de manière irréversible dans l'état sûr, en coupant la tension d'alimentation du système.

DEUXIEME CHAPITRE

LE CAPTEUR DE COURANT INTEGRE (BICS)

1 INTRODUCTION :

L'implémentation des capteurs de courant intégrés dans des circuits utilisés dans une application critique en sécurité, permet de détecter les défauts créant des valeurs non déterminées, qui pourraient échapper à la détection par les techniques conventionnelles utilisant des circuits d'autocontrôle vérifiant des valeurs logiques. D'autre part, ces capteurs pourraient être utilisés en phase de test de production, pour effectuer des tests de courant destinés à détecter les défauts non détectables par des tests logiques. Ces tests sont normalement effectués en observant les lignes d'alimentation externes du circuit intégré. Néanmoins, avec les technologies sub-microniques avancées, les forts courants de fuite ne permettent plus de distinguer le courant statique normal du courant statique induit par une défaillance. Les capteurs de courant intégrés(BICS) permettent un partitionnement du circuit en blocs suffisamment petits, de façon à ce que le courant de fuite observé par chaque capteur soit bien plus faible que le courant produit par les défauts. Néanmoins ce problème ne se pose pas pour la technologie choisie dans le cadre du projet ISIS. Les capteurs de courant internes sont utilisés principalement ici pour pouvoir faire un test de courant rapide pendant le fonctionnement du circuit dans l'application, et pour ne pas complexifier la carte en rajoutant des capteurs de courant externes.

Nous considérons dans ce chapitre le cas d'utilisation de capteur de courant intégré dans des systèmes critiques en sécurité, afin de détecter les défauts créant des niveaux indéterminés. Dans ce contexte, le conception d'un capteur de courant intégré nécessite de calculer son courant de seuil (le courant de référence de BICS). La méthode utilisée pour estimer ce courant sera présenté dans la section 3. Nous allons détailler, par la suite, la conception d'un capteur de courant intégré en prenant compte les contraintes les plus importantes limitant son utilisation.

2 UTILISATION DES CAPTEURS DE COURANT DANS DES SYSTEMES CRITIQUES EN SECURITE :

Les techniques d'autocontrôles assurent la détection en-ligne des fautes générant des niveaux erronés logiques aux entrées et aux nœuds internes du circuit *Fail-Safe*. Elles assurent, par la suite, en cas de défaillance, le maintien des sorties à l'état sûr. Cependant, une

classe importante de mécanismes de défaillance dans les circuits CMOS statiques (*stuck-on*, courts-circuits) induisent des niveaux indéterminés, pouvant échapper à la détection. En fait, un niveau indéterminé sur un nœud du circuit peut être interprété comme incorrect par le circuit suivant et comme correct par le contrôleur utilisé pour assurer l'autocontrôle. Cette situation peut conduire à un état dangereux.

En effet, les circuits CMOS statiques ont une consommation quasi-nulle en phase de repos. La raison étant qu'une porte CMOS statique possède un réseau de transistors PMOS connectant la sortie au Vdd et un réseau de transistors NMOS connectant la sortie à la masse. En cas de fonctionnement sans défaillance, le Vdd est isolé de la masse, car la connexion des réseaux PMOS et NMOS est exclusive. Ainsi les seuls courants existant dans le circuit sont les courants de fuite, généralement très faibles, de l'ordre du nano-ampère. Un défaut induisant un niveau indéterminé crée une connexion entre la masse et le Vdd (exemple : un court-circuit entre deux nœuds portant des valeurs opposées, un *stuck-on* d'une porte logique). Le courant qui en résulte est de plusieurs ordres de grandeur supérieur au courant de fuite (de plusieurs dizaines voire de centaines de micro-ampères). En technologie CMOS 0.8 µm de AMS, les simulations sur la bibliothèque de cellules donnent des courants dépassant les 100 micro-ampères pour toute faute donnant un niveau intermédiaire, même en considérant des fautes qui maintiennent un niveau logique correct (exemple : 4,8 volts au lieu de 5 volts). Des niveaux de courant de cet ordre peuvent être détectés aisément par un capteur de courant intégré BICS. Ils peuvent donc être utilisés en complément d'un autocontrôle en-ligne logique du type (*self-checking*)[10].

La figure 1 montre le principe d'utilisation d'un capteur de courant intégré BICS contrôlant le courant I_{DDQ}. Ce capteur de courrant est connecté sur la masse ou Vss d'un bloc interne d'un circuit CMOS intégré sous-test, appelée dans cette configuration Vss virtuel et notée Vs dans la figure 1.

Un transistor ou commutateur by-pass, connecte la ligne Vs sur la Vss durant la phase de transition du circuit et la déconnecte durant la phase de repos. Le BICS mesure le courant durant la phase de stabilité desintrées en le comparant à un seuil V_{REF} par le biais d'un comparateur. Cette mesure doit être effectuée durant le fonctionnement du circuit, soit sur chaque cycle de l'horloge, soit périodiquement pendant des phases spécifiques dédiées au test de courant. Dans les circuits rapides, on ne peut effectuer le test de courant que de façon

périodique, le capteur de courant étant plus lent que le circuit sous test. Ainsi durant les phases de test, la vitesse de fonctionnement est ralentie, permettant le fonctionnement du BICS. Ce ralentissement n'est pas nécessaire dans notre cas car ISIS utilise une horloge lente (100 kH_z).

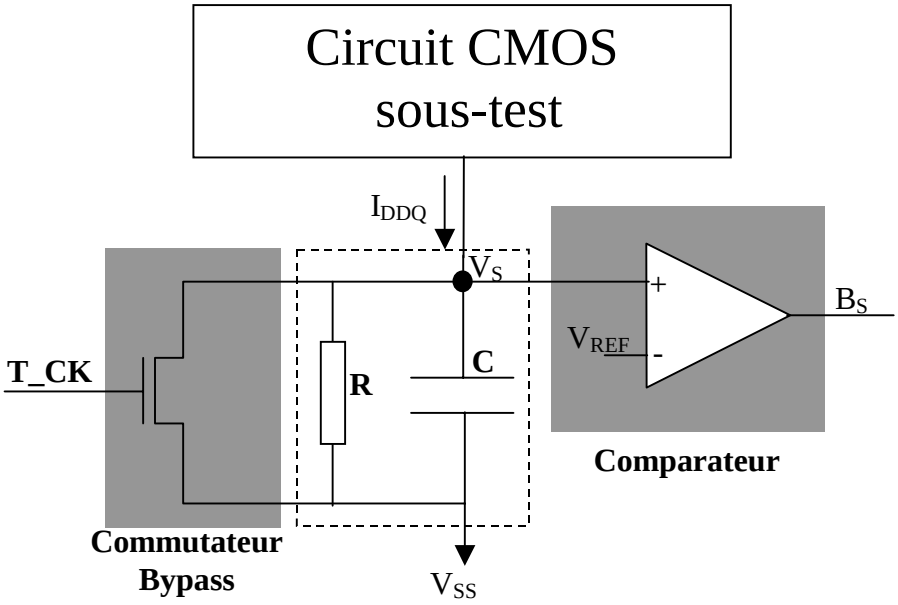


Fig. (1) : L'insérétion de capteur de courant intégré pour mesurer le courant I_{DDQ} d'un circuit CMOS sous-test

Un test périodique conventionnel peut ne pas être suffisant dans le contexte d'une application de haute sécurité. En fait, un test de courant permet de détecter une défaillance très tôt dans sa phase de développement, dès qu'un courant de fuite anormal apparaît dans le circuit, c'est à dire avant que la défaillance ne se manifeste par une faute fonctionnelle. En fait, les mécanismes des défaillances étant des phénomènes très lents, on peut aisément choisir une période de test permettant la détection de défaillances avant que le fonctionnement du circuit n'en soit affecté.

3 ESTIMATION DU COURANT DE FUITE D'UN CIRCUIT CMOS :

Le test de courant I_{DDQ} est très utilisé dans le processus de fabrication des circuits intégrés CMOS depuis beaucoup d'années. En effet, les techniques traditionnelles de test ne sont pas efficaces pour certaines fautes ou modes de défaillances dans les circuits intégrés actuels.

Plusieurs défaut comme : les ouvertures dans l'oxyde, les fautes de type *stuck-on* au niveau transistor, la porte flottante d'un transistor et les courts-circuits ne se manifestent pas comme des fautes logiques faciles à détecter avec des tests logiques. Par contre, ces types de défauts dégradent les performances électriques d'un circuit CMOS. Le test d'I_{DDQ} basé sur la mesure du courant statique permet la détection de ces types de fautes.

Par le test I_{DDQ} on mesure le courant sur les lignes d'alimentation (Vdd, Gnd) à l'état de repos du circuit, après que les signaux sont stabilisés. Les défauts qui entraînent une augmentation du courant I_{DDQ} seront ainsi détectés.

D'autre part, l'utilisation du BICS dans un circuit intégré, nécessite un courant de référence I_{ref}. La valeur de ce courant détermine l'état de fonctionnement de ce circuit. Autrement dit, si le courant de fuite venant du circuit intégré sous-test est inférieur à cette valeur, la sortie de BICS indique un fonctionnement correct du circuit. Par contre l'augmentation de ce courant au-delà de ce seuil signifie qu'il y a une défaillance dans le circuit. Ainsi, l'estimation de la valeur du courant de fuite constitue une étape capitale afin de tester le circuit intégré par un BICS. Cependant, plusieurs techniques ont été proposées dans la littérature pour mesurer le courant I_{DDQ} [11][12][13]. Ces études reposent sur des simulations électriques, dont chacune est consacrée à un seul type de défauts. De plus, chacun de ces défauts génère un courant anormal dans le circuit. Le courant de référence du BICS sera égal au courant minimal de l'ensemble des défauts.

Ces techniques considèrent le paramètre du défaut (e.g. la valeur de la résistance du court-circuit) connu. L'inconvénient de ces techniques réside d'une part, en un temps de simulations élevé, et d'autre part, en une estimation de la valeur de la résistance du défaut pouvant largement varier d'un circuit à l'autre[14]. De plus, des études ont montré que le

courant de fuite dépend de la température. Plus précisément, la variation de la température de 0°C à 70°C fait décroître de courant de 20%[15]. Par conséquent, l'estimation du courant de fuite par les techniques précédentes ne garantit pas la détection des défaillances dans le circuit.

Pour faire face à ce problème, une nouvelle méthode a été proposée dans [16]. Cette méthode repose sur le fait que la résistance d'un défaut peut prendre une valeur comprise entre 0 et +∞. D'une telle façon, nous pouvons détecter n'importe quelle défaillance conduisant à un fonctionnement indésirable.

3.1 LA METHODE D'ESTIMATION DU COURANT I_{DDQ} :

La nouvelle approche permet de déterminer le courant I_{DDQ} minimal équivalent à une défaillance paramétrique d'un élément du circuit intégré. Ce courant déterminera à son tour le courant I_{ref} du BICS associé à ce circuit afin de détecter la moindre défaillance dans le circuit sous-test, et éviter ainsi les sorties dangereuses du système.

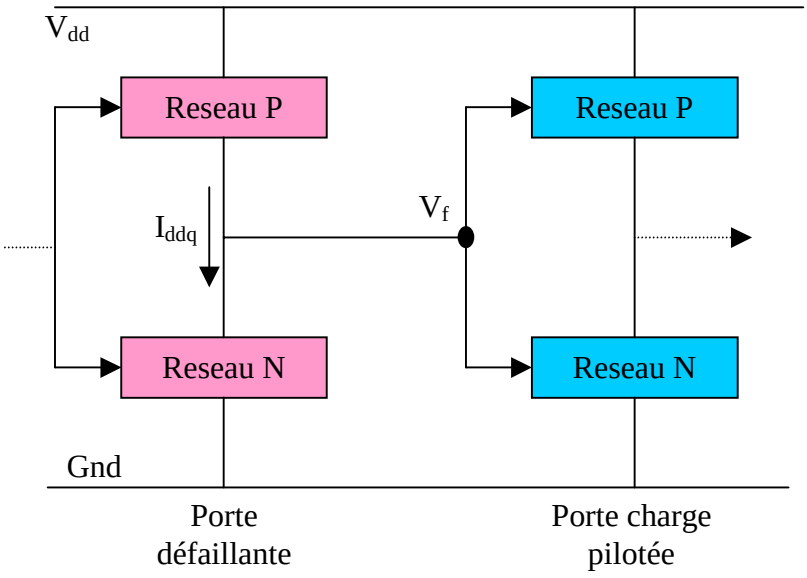


Fig. (2) : La structure de portes CMOS.

Le principe de cette méthode repose sur l'utilisation des niveaux des tensions de sortie de porte logique pour calculer le courant I_{DDQ}, en prenant compte la valeur de résistance

équivalente de l'élément défaillant. Le concepteur précise tout d'abord les niveaux de tension aux sorties qui peuvent être acceptés comme '1' logique et '0' logique.

Dans la technologie CMOS, chaque porte se compose de deux réseaux : le réseau P et le réseau N, comme illustré à la figure (2).

Supposons maintenant qu'il y a un défaut dans une porte (soit le réseau P, soit le réseau N est défaillant). La tension de sortie de cette porte prend la valeur V_f, alors que le courant passant par cette porte est égal à I_{DDQ}. La tension de sortie V_f peut prendre une valeur entre Vss et V_{dd}. Considérons que U_{bas} et U_{haut} constutient les deux tensions limitant la zone indéterminée de la tension de sortie. Suivant la valeur de $V_{f,}$ nous pouvons distinguer trois intervalles du fonctionnement indésirables (figure 3) :

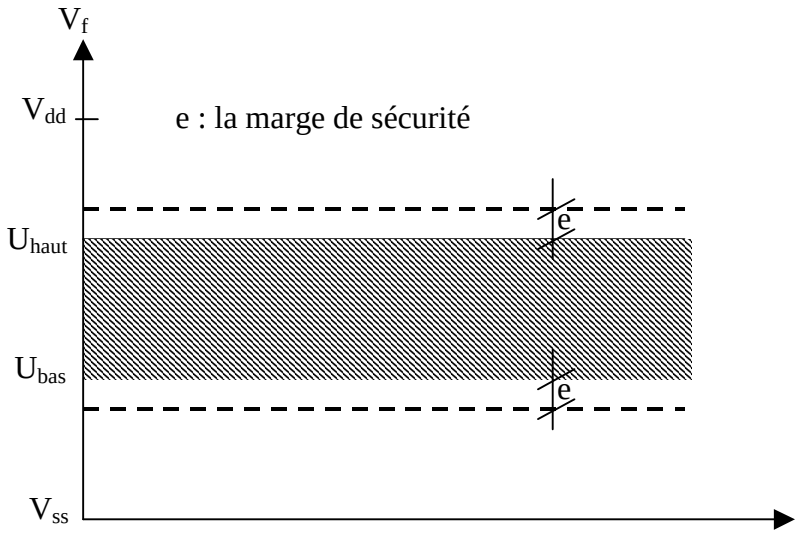


Fig. (3) : Les zones des fonctionnements indésirables

1- La valeur correcte de la sortie de la porte est '0' ('1'), et la tension de sortie V_f à cause de la faute est $V_f > U_{haut}$ ($V_f < U_{bas}$). C'est une erreur logique détectable par un contrôleur logique.

2- La valeur correcte de la sortie de la porte est '0' ou '1', et la tension de la sortie V_f de cette porte défaillante est $U_{haut} > V_f > U_{bas.}$ Le fonctionnement du circuit est dans ce cas indésirable, et la porte suivante de cette porte peut interpréter cette valeur de V_f comme '1' ou '0' logique. Ceci peut par conséquent conduire à un fonctionnement incorrect, que l'on ne soit pas sûr de détecter par un contrôleur logique.

3- La valeur correcte de la sortie de la porte est ‘0’ (‘1’), et la tension de sortie V_f de cette porte défaillante est $V_f < U_{bas}$ ($V_f > U_{haut}$). Ainsi, la différence $\Delta V_f = U_{bas} - V_f$ ($\Delta V = U_{haut} - V_f$) = e, où e présente la sensibilité de la porte vis-à-vis du bruit. Une valeur très petite de cette différence rend le circuit de mauvaise qualité.

Finalement, les trois cas de fonctionnement indésirable expliqués au-dessus sont déterminés par les valeurs des résistances R_p et R_n correspondant respectivement aux résistances du réseau P et du réseau N. Ces résistances connectent la sortie de porte CMOS à V_{dd} ou à V_{ss} comme le montrer la figure (4).

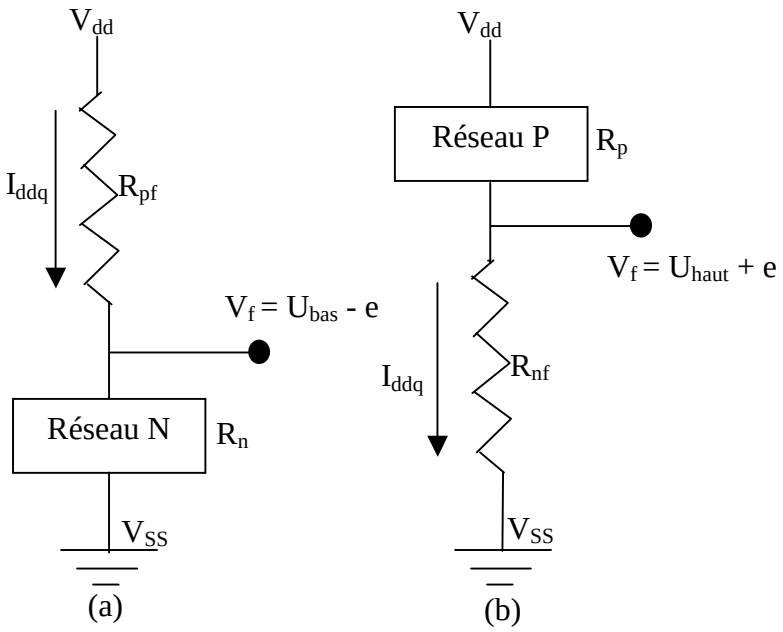


Fig. (4) : Le modèle de défaillance dans une porte logique

(a) dans le réseau P, (b) dans le réseau N

Cependant, un défaut se produisant dans une porte CMOS change la valeur de la résistance R_p ou R_n. D’autre part, nous avons vu que la résistance équivalente d’un réseau défaillant peut prendre une valeur entre 0 et +∞, le courant minimal I_{DDQ} sera calculé en prenant en compte la résistance la plus élevée (la valeur maximum de la résistance génère une valeur minimale du courant I_{ddq}). Ceci correspond au troisième cas du fonctionnement indésirable présenté auparavant où ΔV_f = e (la marge de sécurité). Par exemple, si la résistance R_p est correcte et la résistance R_n est incorrecte, la valeur de la résistance R_p est

connue alors que la valeur de la résistance R_n peut prendre une valeur de 0 à +∞, le calcul du courant I_{DDQ} minimal sera fait pour une résistance R_n maximale qui produira un fonctionnement indésirable. Ceci correspond au cas où ΔV_f = e, autrement dit le troisième point des cas de fonctionnement indésirable.

3.1.1 LE COURANT I_{REF} :

Nous avons vu que le calcul du courant I_{DDQ} repose sur la valeur de tension de sortie V_f de la porte défaillante, en prenant en considération des valeurs des résistances R_p et R_n. La figure (4) illustre deux portes défaillantes : (a) est une porte défaillante dans le réseau P et (b) est une porte défaillante dans le réseau N. Les résistances R_{pf} et R_{nf} présentent les valeurs erronées des résistances R_p et R_n respectivement.

Dans le premier temps, nous allons considérer que le réseau N est défaillant, le courant I_{DDQ} correspondant à ce défaut est égal :

$$I_{DDQ}=\frac{V_{dd}}{R_p+R_{nf}} \quad \text{……(1-2)}$$

$$R_{nf}=R_p\frac{V_f}{V_{dd}-V_f}$$

Où $V_f = U_{haut} + e$

De la même manière, si la défaillance est dans le réseau P, le courant I_{DDQ} correspondant à ce défaut est égal :

$$I_{DDQ}=\frac{V_{dd}}{R_{pf}+R_n} \quad \text{……..(2-2)}$$

$$R_{pf}=R_n\frac{(V_{dd}-V_f)}{V_f}$$

Où $V_f = U_{bas} - e$.

Des équations (1-2) et (2-2), nous pouvons ainsi déterminer le courant I_{DDQ} d'une porte défaillante, en utilisant les valeurs des résistances R_p, R_n. En fait, cette détermination du courant I_{DDQ} requière seulement deux simulations électriques. Cependant, une simulation

SPICE est nécessaire afin de déterminer les conductance r_p, r_n de transistors P et N respectivement dans le mode statique.

Pour une porte CMOS, le courant I_{ref} sera égal à la valeur du courant I_{DDQ} la plus petite des deux courants I_{DDQ} résultant des équations (1-2) et (2-2). Ainsi, pour une bibliothèque de portes CMOS, le courant de référence I_{ref} de cette bibliothèque sera déterminé par la valeur du courant I_{DDQ} le plus petit des courants I_{DDQ} résultant en appliquant les équations (1-1), (2-2) pour l'ensemble des portes utilisées dans le circuit.

Les valeurs des résistances R_p, $R_{n,}$ en état passant du réseau P ou N d'une porte CMOS, dépendent des valeurs des entrées de cette porte. Par exemple, pour une porte NOR à deux entrées, la valeur de R_p égale à $2r_p$ (r_p : est la valeur de résistance du transistor PMOS à l'état passant) car, en état passant, dans le réseau P de porte NOR, on doit considérer les deux transistors PMOS connectés en série. D'autre part, la valeur de R_n est égale à r_n (r_n : est la valeur de résistance du transistor NMOS à l'état passant) si les entrées étaient 01 et 10, et $r_n/2$ si les entrées étaient 11. Cependant, le courant de référence considéré est le courant I_{DDQ} le plus petit qui correspond à la valeur de résistance R_p et R_n le plus élevée. Cette valeur sera alors égale à $2r_p$ dans le cas de la porte NOR.

En se basant sur cette technique nous avons simulé toutes les portes utilisées dans le circuit ISIS et établi le courant I_{ref}.

4 CONCEPTION D'UN CAPTEUR DE COURANT INTEGRE (BICS) :

Nous avons vu que le capteur du courant intégré (BICS) est une solution possible pour la détection des fautes dans les circuit CMOS sub-microniques. Ce capteur du courant doit être simple, conçu pour fonctionner à faible tension d'alimentation. De plus, l'impact de l'introduction de ce capteur sur les performances du circuit doit être insignifiant.

Cependant, pour éviter la dégradation des performances (vitesse, consommation) due à l'introduction du BICS sur les lignes d'alimentation, nous allons utiliser un transistor NMOS de grande taille comme élément de commutateur (by-pass). Mais, la commutation du by-pass, peut induire un grand bruit de courant au nœud Vs connectant le commutateur by-pass au circuit. Ceci est dû au phénomène de l'injection de charge, de plus, l'intégration du

courant de bruit sur la capacité Cs de ce nœud peut déclencher le comparateur du BICS, et peut être interprétée ainsi comme un courant produit par un défaut. Pour éviter ce problème, un circuit de compensation et un deuxième by-pass peuvent réduire ces effets indésirables, et augmenter la vitesse de fonctionnement du BICS. Ainsi, la vitesse du test d'I_{DDQ}, et la précision de la mesure d'I_{DDQ} seront améliorées.

Une caractéristique très importante du BICS est la flexibilité du choix du niveau de courant de seuil I_{DDQ}, seulement en jouant sur la fréquence d'horloge.

Le comparateur du courant de BICS doit respecter des contraintes telles que : un niveau bas de tension d'alimentation, une fréquence de fonctionnement élevée, et une grande précession de mesure.

La figure (5) présente un schéma d'un capteur du courant proposé pour tester un circuit CMOS. De point de vue structurel, il est composé de trois parties:

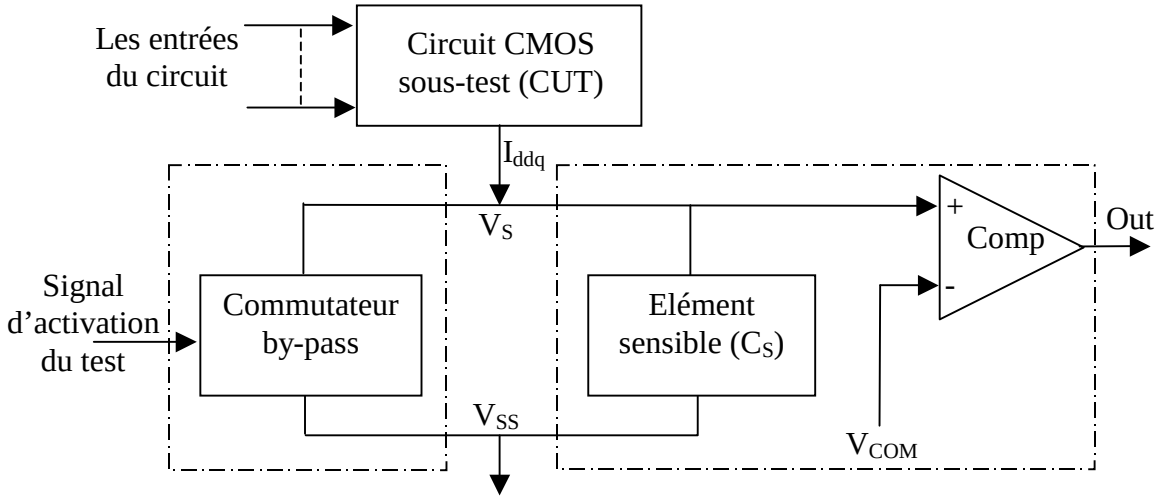


Fig. (5) : Le schéma d'un capteur de courant BICS

1- Le commutateur ou l'élément de by-pass qui connecte la masse réelle Vss avec la masse virtuelle Vs. Ici, on appelle masse virtuelle le nœud où on connecte les sources de tous les transistors NMOS du circuit sous - test.

2- L'élément sensible (Cs), dans ce cas l'élément est la capacité parasite du circuit sous-test au nœud Vs.

3-Le circuit de détection , dans ce cas un comparateur analogique.

Le comparateur analogique fonctionne de la façon suivante :

- Lorsque Vs > V_{COMP}, la sortie Out = 1. Ceci signifie que le courant de fuite est plus grand que celui du seuil. Cette détection présent une défaillance dans le circuit sous-test.

- Lorsque Vs < V_{COMP}, la sortie Out = 0. Dans ce cas, le courant de fuite du circuit sous-test est inférieur à celui du seuil. Le circuit fonctionne donc correctement.

En effet, le BICS peut être vu comme un contrôleur de la commutation de la source d'alimentation d'une part, et comme un contrôleur de courant de fuite I_{DDQ} d'autre part.

Dans le premier cas on prend en compte des contraintes de dessin imposées par des simulations de dissipation de puissance, tandis que dans le deuxième cas, les contraintes sont obtenues à partir des simulations de fautes I_{DDQ}.

Deux paramètres sont très importants dans le processus de conception du BICS:

1- La taille du circuit sous-test CUT, qui détermine le courant maximum de fuite à détecter avec le BICS. De plus les caractéristiques fonctionnelles du circuit sous-test vont déterminer les courants transitoires qui vont passer par le commutateur by-pass, et les temps de synchronisation du commutateur.

2- La capacité parasite Cs au nœud virtuel Vs, qui limite la vitesse et la précision de la mesure des courants I_{DDQ} avec le BICS. Plus la capacité est grande, plus le temps de test est long, puisque cela prend plus de temps pour permettre au courant de défaut de la charger à un niveau de tension détectable par le comparateur.

La décision plus importante pendant la phase de la conception du BICS est le choix de la taille du commutateur by-pass. Normalement deux types de courant passent par le BICS :

-Le courant transitoire qui passe par le by-pass.

-Le courant de fuite qui doit être détecté par le comparateur. L'intérêt principal dans le processus de conception du BICS est que la résistance de l'élément de by-pass soit très faible, afin que la tension entre les nœuds Vs et Vss reste près de 0V. Ceci est possible si la taille du transistor utilisé pour la construction du by-pass est très grande. La tension sérielle réduite assure un fonctionnement normal du circuit sous-test sans dégradation des

performances. Des solutions moins coûteuses en surface existent, mais elles ne sont pas optimales pour l'opération à faible tension d'alimentation et grande vitesse.

Les éléments linéaires sont impraticables pour le by-pass à cause de la dégradation de la précision de mesure. Les solutions avec des diodes induisent une augmentation de la tension sérielle pour le passage d'un courant élevé (VD = Vs - Vss = 0.7V). Les solutions avec les transistors bipolaires sont éliminées du choix à cause du temps significatif de commutation du transistor bipolaire et d'une capacité de conduction du courant assez faible.

Le comparateur est la dernière partie à dimensionner dans la phase de conception du BICS. Sa fonction est très dépendante de la conception du commutateur (by-pass). Le circuit de détection des courants I_{DDQ} doit satisfaire des conditions différentes comme par exemple : un niveau bas de tension d'alimentation, une fréquence de fonctionnement élevée pour des niveaux faibles des courants I_{DDQ}, et une grande précision de mesure.

Pour cela, on a conçu un comparateur avec des miroirs de courant, rapide et sensible à la sélection du courant de seuil I_{DDQ} pour satisfaire ces différentes conditions, et pour ajouter la flexibilité et la vitesse de fonctionnement.

La mesure du courant I_{DDQ} avec une plus grande précession permet de :

- échantillonner la sortie de BICS plusieurs fois pendant la période de test. Chaque instance d'échantillonnage correspond à un niveau de courant I_{DDQ} diffèrent, cette opération permet une analyse de fiabilité très précise.

- offrir à l'utilisateur la possibilité d'exécuter les tests d'I_{DDQ} à des vitesses plus élevées. On peut tester le circuit à une grande vitesse, si on augmente le seuil de détection de courant I_{DDQ}.

- offrir à l'utilisateur l'option de décider à tout moment les niveaux de courant I_{DDQ} qui sont considérés comme provenant des défauts, cette opération peut être faite en jouant sur la vitesse du test I_{DDQ}.

- proposer un comparateur de courant très facile à intégrer dans le circuit à tester avec une faible tension d'alimentation, et une faible consommation.

4.1 CONFIGURATION D'UN COMMUTATEUR DUAL (BYPASS DUAL) :

Pendant l'opération normale du circuit sous-test, le premier by-pass (BS1) connecte le nœud Vs au nœud Vss. Si le circuit sous-test fonctionne en mode test I_{DDQ} (quand on envoie des vecteurs de test I_{DDQ}), le transistor MB1 du premier by-pass passe à l'état bloqué, et quand le circuit arrive à l'état de repos, on commence la mesure I_{DDQ}.

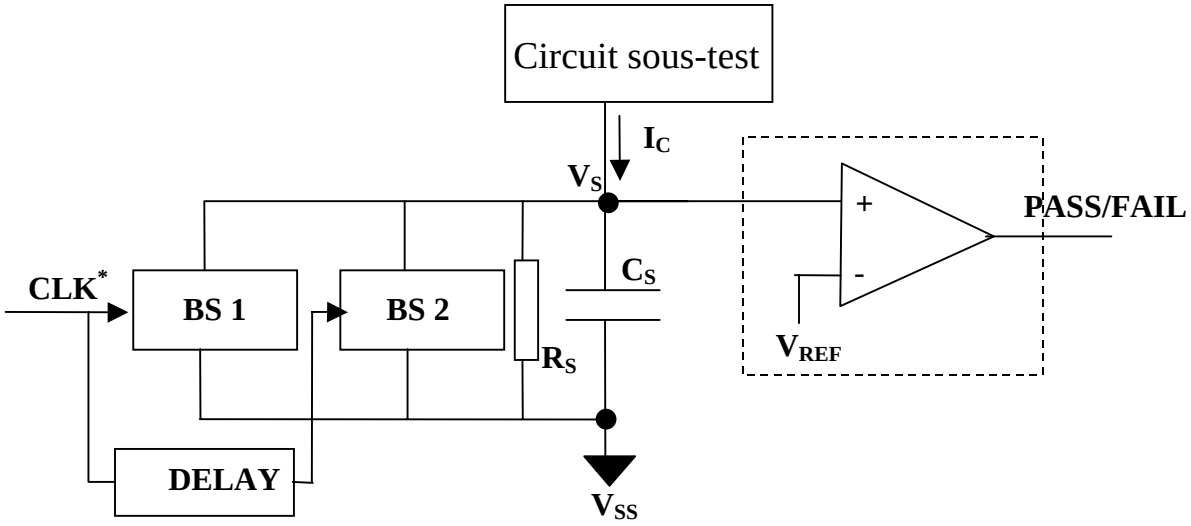
Mais la commutation du transistor MB1 de l'état passant à l'état bloqué peut induire un grand bruit de courant au nœud Vs à cause du phénomène de l'injection de charge. L'intégration du courant de bruit sur la capacité Cs peut déclencher le comparateur du BICS, et peut être interprétée ainsi comme un courant produit par un défaut.

Typiquement, on utilise un circuit de compensation afin de réduire les effets de l'injection de charge au nœud Vs. Mais parce qu'il est très difficile d'estimer la taille précise du circuit de compensation et le bruit du by-pass, on a rajouté un autre by-pass retardé pour diminuer le bruit, et pour augmenter la vitesse de fonctionnement du BICS.

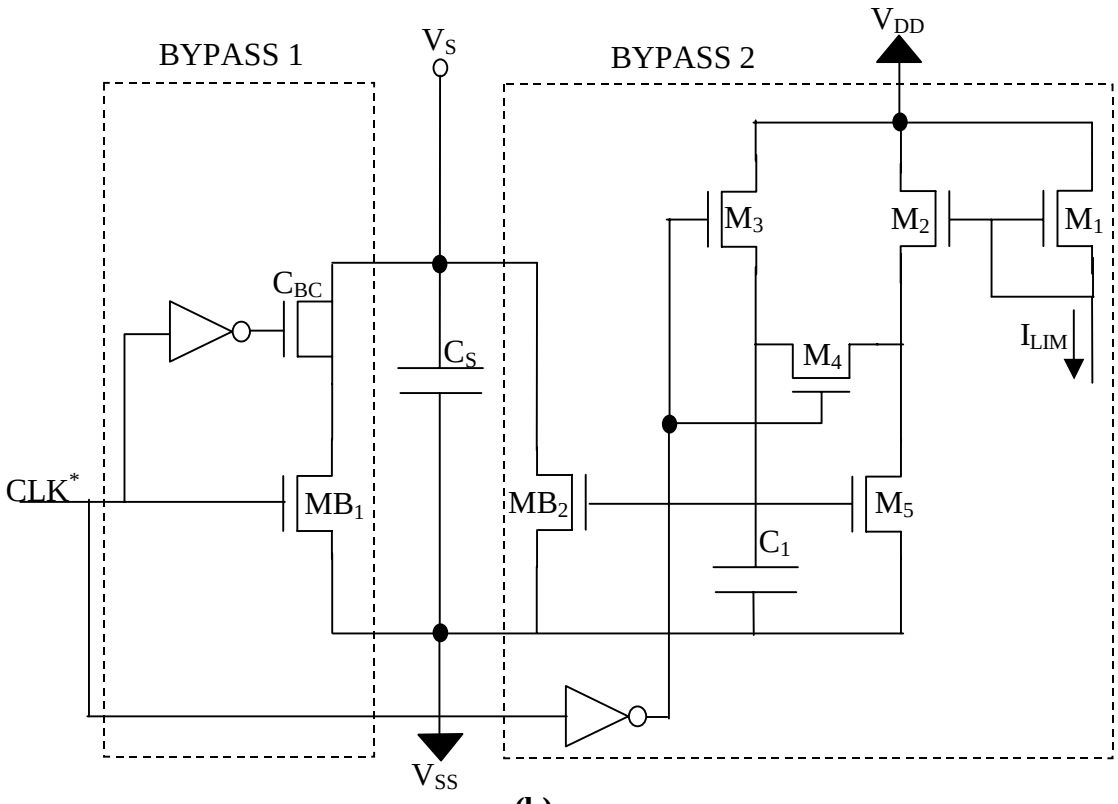
La figure 6 présente un by-pass dual qui se compose de deux by-pass :

1- le by-pass principal (BS1), qui se compose d'un grand transistor NMOS (MB1) avec un circuit de compensation d'injection de charge (un transistor NMOS, le drain et la source en court-circuit, configuré comme une capacité "C_{BC}"). Le by-pass BS1 est contrôlé par un signal d'horloge inversé.

2- le deuxième by-pass retardé (BS2) représenté par le transistor MB2 reliant la masse virtuelle Vs à la masse réelle Vss pendant que MB1 est à l'état passant et peu de temps après qu'il passe à l'état bloqué'. MB2 est progressivement désactivé par un circuit de contrôle qui se compose des transistors M1-M5, qui aident à la décharge de la capacité C1 par la résistance équivalente du groupe (M4 - M5).



(a)



(b)

Fig. (6) : Un shéma de by-pass dual

(a): Le circuit sous-test connecté au BICS, (b): Le commutateur dual

La figure (7) montre la variation du courant transitoire au nœud V_S et présente les trois phases précédentes du fonctionnement du BICS. La mesure du courant I_{DDQ} commence en troisième phase.

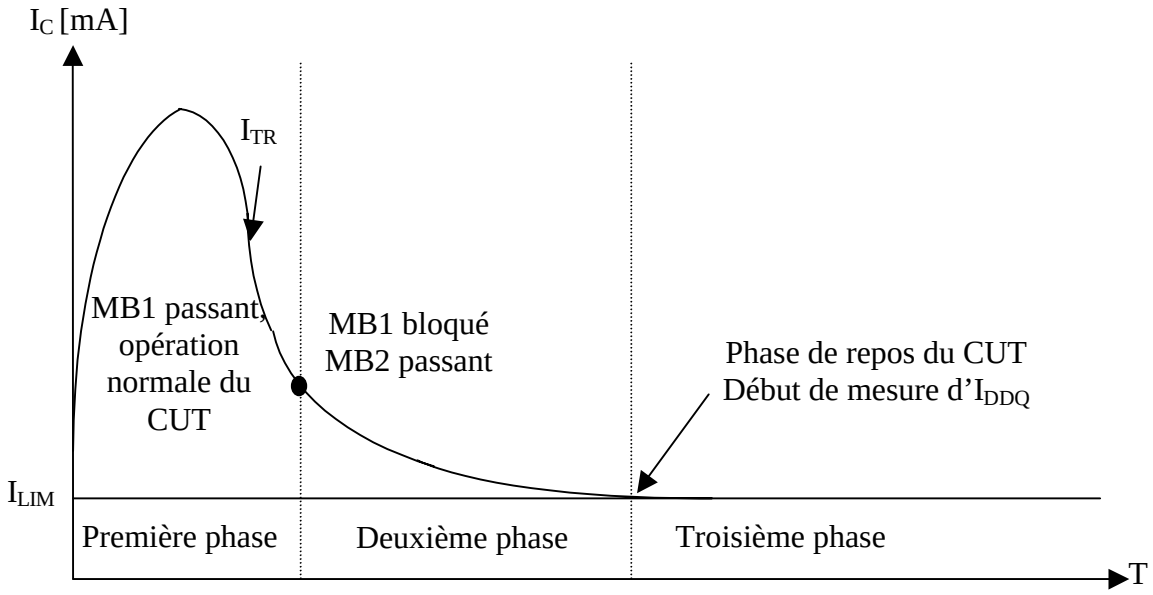


Fig.(7) : le courant au nœud V_S

La connexion Vs au Vss par le deuxième by-pass est donc un complément efficace au circuit de compensation d'injection de charge. Le deuxième by-pass conduit à la masse le courant transitoire résiduel afin de permettre une mesure plus rapide d'$I_{DDQ.}$

Ainsi, MB2 accélère le passage du courant transitoire à la masse et réduit rigoureusement le bruit de commutation injecté par la commutation du MB1 au nœud Vs. A la fin du passage du courant transitoire résiduel à la masse et le déchargement du nœud C1 (la période du fonctionnement du deuxième by-pass), MB2 fonctionne comme un miroir de courant qui soustrait le courant I_{LIM} (limite du test d'I_{DDQ}) du nœud virtuel Vs.

4.2 LE COMPARATEUR DU BICS

La conception du comparateur pour une détection rapide des courants I_{DDQ} dans les circuits CMOS sub-microniques doit également satisfaire les conditions de faible tension d'alimentation, et de faible bruit. La figure (8) présente un nouveau comparateur contrôlé en tension qui satisfait les conditions nécessaires pour la conception du BICS et qui fournit un message d'erreur de type tension (V_{ERR}) et /ou courant (I_{ERR}).

On observe qu'un courant extérieur est fourni I_{REF} , et deux autres courants I_{LIM} et I_{SENS}, qui sont générés à partir de ce courant. Ces deux courants et les tailles des transistors appartenant aux miroirs de courant définissent la sensibilité du comparateur. Le niveau anormal de courant I_{DDQ} est détecté par une petite augmentation de la tension de Vs qui déclenche le fonctionnement du comparateur.

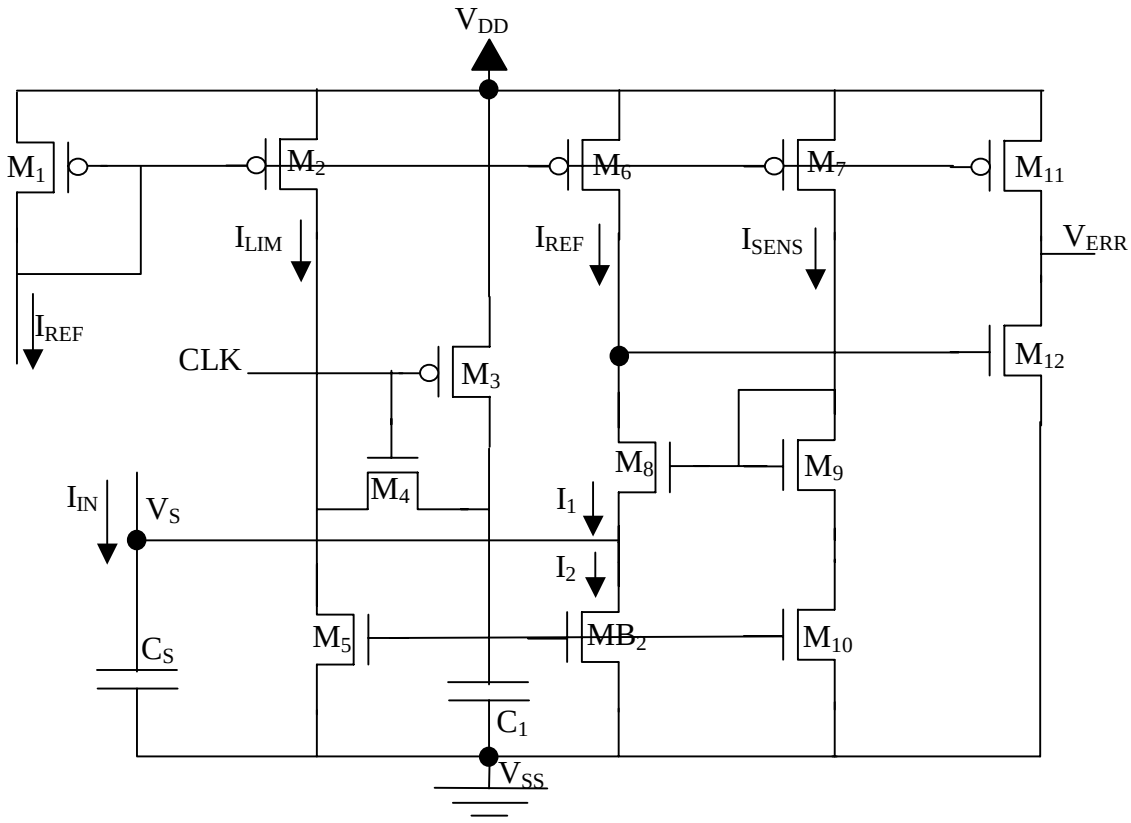


Fig.(8) : Le comparateur contrôlé en tension

Les valeurs des courants I_1 et I_2 sont partiellement déterminées par le courant I_{REF}, et par les tailles des transistors, mais elles sont aussi dépendantes du courant d'entrée I_{IN} fourni par le circuit sous-test (CUT).

Le transistor MB_2 conduit le maximum de courant quand le signal de CLK est au niveau logique '0'. Quand ce signal passe à '1', découplant le premier by-pass, le courant qui passe par le MB_2 est progressivement réduit jusqu'à ce que le courant I_1 soit égale à I_{LIM}. Cela permet d'éviter d'avoir la masse virtuelle Vs comme un nœud flottant, de réduire la sensibilité du comparateur face au bruit de commutation du MB_1, et de conduire les courants de fuite

(c'est à dire les courants des défauts) I_{DDQ} à la masse réelle Vss (comme on a vu au section 5.1). La vitesse et la sensibilité du comparateur sont essentiellement définies par les courants I_{LIM}, I_{REF}, I_{IN}, et Cs et Vs.

5 IMPLEMENTATION ELECTRIQUE DU BICS :

Dans le paragraphe précédent, nous avons discuté le principe de conception d'un capteur de courant intégré. La réalisation du schéma électrique de ce capteur en utilisant la technologie 0.8µm d'AMS fait l'objet de ce paragraphe. Le schéma d'implémentation électrique du BICS est présenté dans la figure (9). Les tailles des transistors sont calculées en faisant le choix du niveau de courant I_{DDQ} qu'on veut détecter, la surface du BICS et la sensibilité de la mesure du courant.

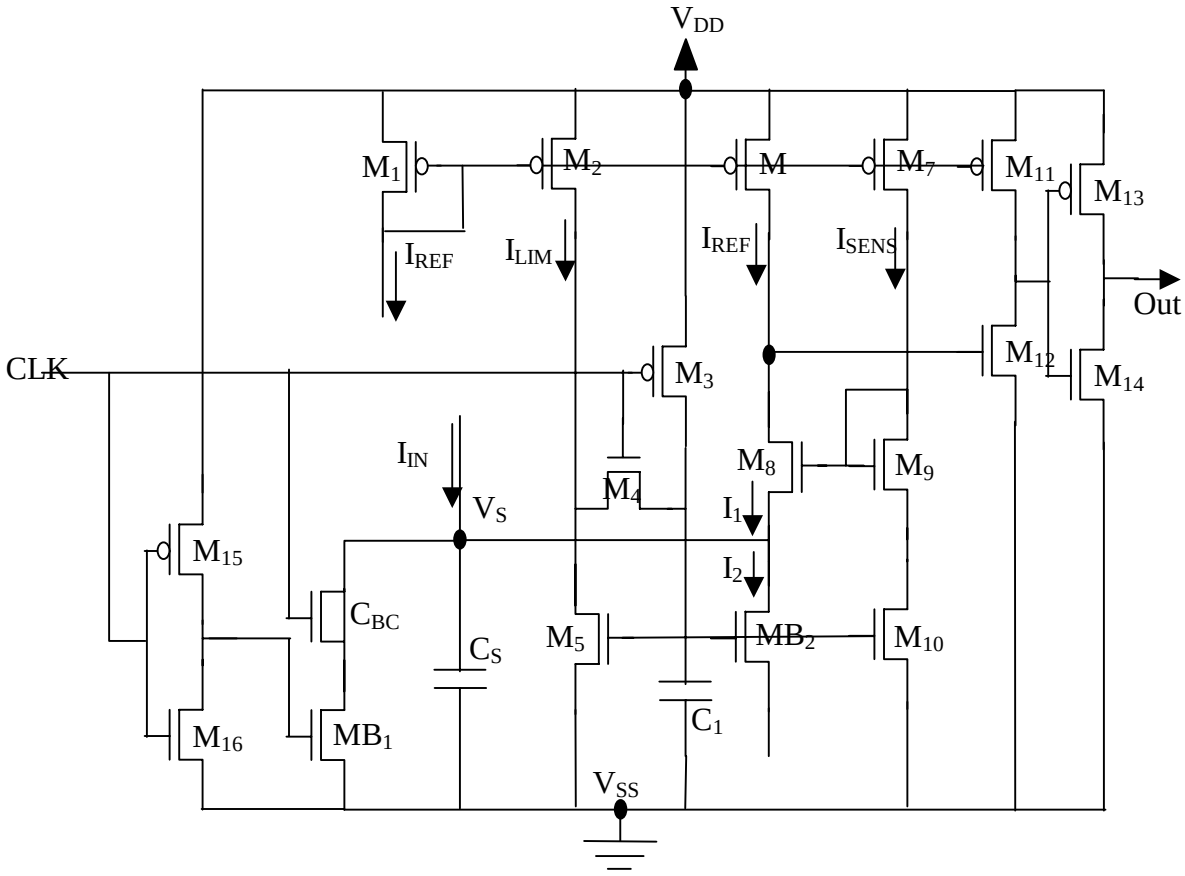


Fig. (9) : Le schéma électrique du BICS

Pendant le calcul des tailles des transistors deux étapes essentielles sont étudiées avec attention :

1- La conception du premier by-pass BS1 et de son circuit de compensation(C_{BC})

2- La conception du comparateur.

5.1 : CONCEPTION DU PREMIER BY-PASS BS1 ET DE SON CIRCUIT DE COMPENSATION CBC :

La figure 10 présente le premier by-pass avec son circuit de compensation (C_{BC}) :

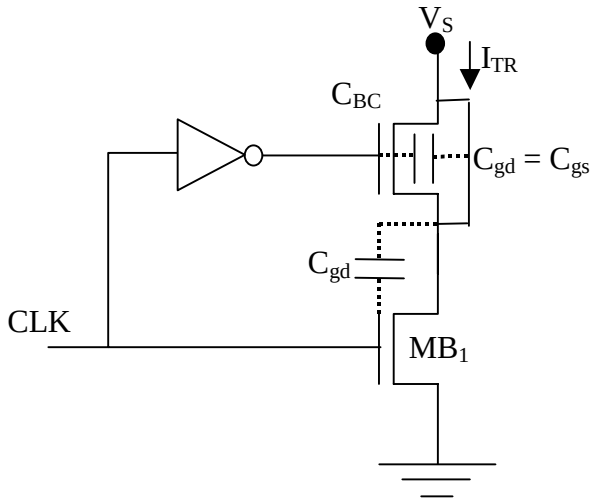


Fig. (10) : Le bypass BS1

Normalement le premier by-pass connecte le nœud Vs au Vss durant la phase de transition de courant du circuit sous-test. Le choix du transistor MB1 dépend de la valeur du courant transitoire I_{TR}. La valeur de ce courant permet de dimensionner le transistor MB1 et la capacité C_{BC}.

Le courant I_{SAT} dans la région de saturation d'un transistor NMOS est :

$$I_{SAT}=K\frac{W}{L}(V_{GS}-V_T)^2 \quad \text{……..(3-2)}$$

$$K=\frac{\xi.\mu_n}{2t_{ox}} \quad \text{…….(4-2)}$$

ξ : permittivité du SiO2

μ_n : mobilité des électrons,

t_{ox} : épaisseur du SiO2,

W : largeur du transistor,

L : longueur du transistor,

Les paramètres ξ, μ_n, t_{ox} sont déterminés par la technologie utilisée. Le courant I_{SAT} sera calculé à partir de l'équation (3-2) avec le choix des paramètres W et L. L'équation (3-2) indique également que pour chaque changement de W ou L, il y aura changement de la valeur d'I_{SAT} pour des valeurs stables de V_{GS} et V_T.

Le circuit de compensation de charge (C_{BC}) est en effet un transistor NMOS (le drain et la source en court-circuit), et un inverseur à l'entrée. Cette capacité doit être suffisamment grande pour compenser le bruit de commutation de la capacité Cgd du transistor MB1 (premier by-pass).

La valeur de Cgd du MB1 est donné par la formule :

$$Cgd=Cgs=\frac{C_{ox}}{2}*(W.L)=\frac{\xi}{2.t_{ox}}*(W.L) \quad \text{……(5-2)}$$

La valeur de C_{BS} doit être près de la valeur de Cgd, pour compenser le bruit de cette capacité. La réalisation de cette compensation sera effectuée par le choix de W et L du transistor configuré comme capacité C_{BC}

5.2 CONCEPTION DU COMPARATEUR :

Le comparateur de courant est composé de trois miroirs de courant :

1- un miroir de courant composé des transistors NMOS (M5-MB2), reliés à la masse Vss .

2- un miroir de courant composé des transistors PMOS (M1-M6), relié à la Vdd.

3- un miroir de courant flottant composé des transistors NMOS (M8-M9).

Les deux miroirs de courant NMOS sont dominants, parce qu'ils génèrent des courants plus élevés que le miroir de courant PMOS. Le courant I_{OUT} du comparateur est dépendant de la valeur de courant généré par le miroir PMOS et du miroir flottant NMOS. La figure 8 présente les trois miroirs de courant .

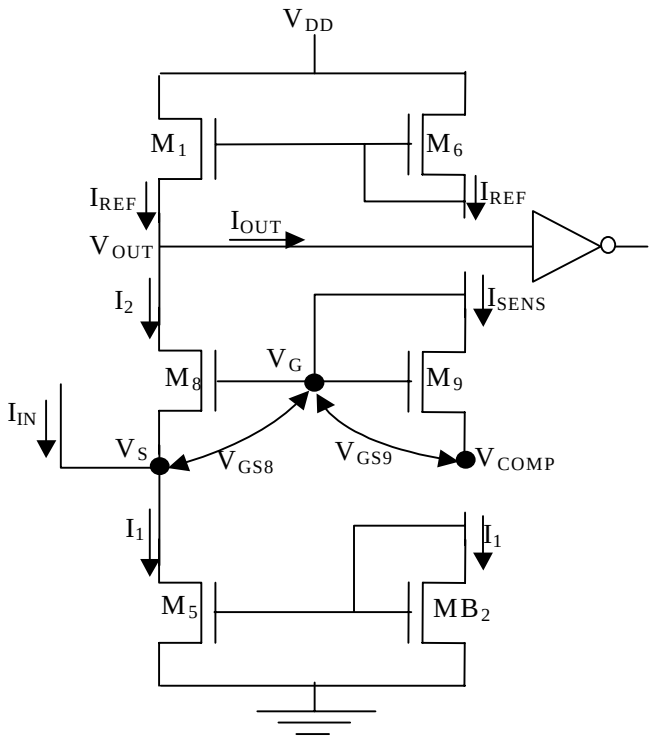


Fig. (11): Le comparateur de courant avec les miroirs de courant NMOS et PMOS.

Le nœud VS (la source du transistor M8) contrôle la tension de grille-source V_{GS8} du transistor M8. La grille de M8 a une tension stable V_G, déterminée par le tension V_{COMP} et le courant I_{SENS} du miroir flottant (M8-M9).

Le courant I_{SENS} du miroir de courant (M8-M9) est :

$$I_{SENS}=K.\frac{W_9}{L_9}(V_{GS9}-V_T)^2 \quad \text{……..(6-2)}$$

$$I_2=K.\frac{W_8}{L_8}(V_{GS8}-V_T)^2 \quad \text{……(7-2)}$$

Avec : $V_{GS9} = V_G - V_{COMP}$

$$V_{GS8} = V_G - V_S \quad \text{……..(8-2)}$$

$$K=\frac{\xi.\mu_n}{2t_{ox}}$$

Au début de la mesure I_{DDQ} les tensions V_{COMP} et V_S sont égales. Mais, si la valeur de V_S change de ΔV_S, alors la valeur du courant I_2 est:

$$I_2 = m.I_{SENS} - 2K\frac{W_8}{L_8}.\Delta V_S(V_G - V_T - V_S) \text{ ……..(9-2)}$$

où m est la relation entre les tailles de transistors M9 et M8. Pour L8 = L9, m=W8/W9.

C'est à dire que le courant I_2 est sensible au changement du V_S. Alors la valeur de I_2 est reliée à la valeur de V_S.

Le courant de sortie est :

$$I_{OUT} = I_{REF} - I_2, \text{ où……..(10-2)}$$

$$I_2 = I_1 - I_{IN} \text{……(11-2)}$$

Le niveau du courant I_1 est déterminé par le courant I_{REF} et les tailles de transistors M5, MB2.

Si la valeur du courant d'entrée I_{IN} fournie par le circuit sous-test augmente, (donc la tension de Vs augmente), la valeur du courant I_2 diminue (9-2) et la valeur du courant de sortie I_{OUT} augmente, indiquant l'erreur.

D'une part, les trois courants I_{REF}, I_1 et I_2 déterminent le courant d'erreur ou le seuil de détection, d'autre part ces courants sont contrôlés par les tailles des transistors de chaque miroir. On peut donc changer le seuil de détection des courants I_{DDQ} en changeant :

- le courant I_{REF} : par le choix des tailles des transistors pour le générateur d'I_{REF}.

- le courant I_1 : par le contrôle du rapport (WB2/W5) pour LB2=L5 (les tailles des transistors pour le miroir (M5-MB2))

- le courant I_2 : par le contrôle du rapport (W8/W9) pour L8=L9 (les tailles des transistors pour le miroir (M8-M9)).

6 CONCLUSION

La réalisation électrique du BICS prouve que les contraintes les plus importantes limitant son utilisation, comme l'impact sur la vitesse du circuit, la précision de mesure et le bruit au nœud V_S dû au phénomène de l'injection de charges, peuvent être éliminées.

Le BICS permet une vitesse de test assez élevée, mais elle dépend du niveau de courant de défauts I_{DDQ} qu'on veut détecter. Cette flexibilité du choix de niveau de courant de défaut est très important pour les tests de production, mais aussi pour les tests périodiques pendant le fonctionnement normal d'un circuit sub-micronique.

Le test I_{DDQ} pendant le fonctionnement normal du circuit sous-test offre, de plus, une meilleure couverture des fautes et un très bon diagnostic. Mais cela n'est pas toujours possible, sauf si la fréquence d'horloge est réduite pendant la phase de test I_{DDQ}. Dans ce cas, on utilise les entrées normales du circuit afin d'effectuer les tests I_{DDQ}, ou on utilise des vecteurs de test I_{DDQ} pour augmenter l'efficacité du test. Comme les mécanismes de défauts se développent lentement, on peut faire des cycles courts de test I_{DDQ} pendant des longs cycles d'opération normale du circuit sous-test. Alors, la dégradation des performances devient très faible.

Le test de courant I_{DDQ} sera de plus en plus important au fur et à mesure que les technologies CMOS s'approchent du domaine nanometrique. Mais, en même temps, les courants des fautes augmentent proportionnellement, et rendent impraticable le test I_{DDQ}.

Une solution possible est l'utilisation des captures de courant BICS, parce que la plus importante limitation du BICS est l'introduction de l'élément de by-pass qui affecte les performances du système sous-test.

TROISIEME CHAPITRE

LES TECHNOLOGIES DE PUISSANCE INTELLIGENTES

1 INTRODUCTION.

L'objet de ce chapitre est de présenter les principes de base des technologies de puissance intelligente " *Smart power* ". Ces sont des technologies VLSI mixtes de puissance de type BCDOM (Bipolaire - CMOS - DMOS " *Double-dfflused Metal Oxide Semiconductor*"), récemment développées par plusieurs fabricants des semi-conducteurs, permettent d'intégrer sur la même puce des circuits logiques et analogiques complexes de basse tension ainsi qu'un ou plusieurs interrupteurs de puissance avec leurs circuits de contrôle et de protection [17][18].

Depuis le début des années 1980, ces technologies et leur domaine d'applications n'ont depuis considérablement cessé de croître. Ces technologies ont d'abord pour but de remplacer les technologies de puissance purement bipolaires qui commençaient à montrer leurs limites. La consommation de puissance, liée au fonctionnement du transistor bipolaire, et la taille incompressible de ce type de composant sont les deux facteurs limitatifs incompatibles avec la demande toujours croissante de fonctions logiques de plus en plus complexe. Les composant CMOS répondent mieux a ces nouvelles exigences avec un niveau de consommation faible et une grande densité d'intégration.

De plus, les industriels ont commencé à introduire des telles technologies pour réaliser une gamme étendue d'applications qui couvrent les domaines suivants : les systèmes électroniques et informatiques portables, équipements de communications avec ou sans fil, l'électronique pour l'automobile, les systèmes de contrôle industriel, les systèmes embarqués pour l'aéronautique et les applications spatiales, et récemment pour améliorer les performances et la fiabilité des contrôleurs d'interface de puissance sûr adaptés aux systèmes d'actionneurs pour le transport ferroviaires.

Aujourd'hui, les circuits de puissance intelligents sont largement répandus, ils peuvent réaliser des fonctions dites "fonctions système" dont les performances sont meilleures que leur homologues en technologie discrète, et le coût quant à lui, est relativement bas et ceci pour une surface de silicium de plus en plus réduite.

Les fonctions d'un circuit de puissance intelligente consistent, d'une part, à réaliser l'interface entre la logique de contrôle et la charge à commander, et d'autre part, à assurer sa propre protection vis à vis des diverses perturbations générées par un environnement extérieur.

Nous retrouvons généralement, les éléments suivants sur la même puce afin de réaliser les fonctions de circuit intégré de puissance intelligente :

1- Une circuiterie logique chargée d'échanger des données avec le microprocesseur.

2- Un ou plusieurs composants de puissance chargés de contrôler une puissance de sortie.

3- Des circuits analogiques de commandes et de protection du dispositif de puissance.

Il est clair que les performances du système ainsi que la fiabilité de la partie fonctionnant en basse tension ne doivent pas être affectées par l'intégration de la partie de puissance et celle de haute tension. Pour cela, les technologies de puissance intelligentes assurent une meilleure isolation entre la région de puissance où le courant peut arriver à quelques centaines de mA sous quelques dizaines de volts, et la région de petit signal qui véhicule au plus des mA sous quelques volts.

Il existe plusieurs familles de technologies de puissance intelligente. Ces différentes familles peuvent être classées en fonction de la technologie d'isolation (isolation diélectrique, isolation par jonction, isolation RESURF " *Reduced Surface Field* ", auto-isolation), ou bien en fonction du composant de puissance (DMOS, Bipolaire, IGBT " *Insulated-Gate Bipolar Transistors* ").

Le choix d'une de ces technologies dépend de l'application. Dans le cas des applications où les tensions exigées sont relativement faibles, inférieures à 100V, et les courants varient entre 0.1A à quelques ampère, le composant de puissance DMOS couvre parfaitement ces spécifications et constitue donc le composant de choix.

2 L'ISOLATION BASSE TENSION-PUISSANCE :

Dans un circuit intégré de puissance intelligente, les composants de puissance et leurs circuits de commande ainsi que les circuits logiques de contrôle sont intégrés sur la même puce. L'isolement entre ces composants de puissance et les circuits de basse tension est alors le problème majeur à résoudre. Par ailleurs, il est nécessaire de distinguer deux problèmes d'isolement le premier statique et le deuxième dynamique.

En technologie CMOS, l'isolement statique peut être facilement réalisé puisque toutes les jonctions des transistors de puissance et ceux de basse tension, sont polarisées en inverse. Par contre l'isolement dynamique est également nécessaire lors des commutations très rapides des éléments de puissance ou de la réponse provoquée par la charge. L'épitaxie N^- situés sous la région du transistor de puissance, sera soumise à des fluctuations de tension et de courant rapide qui se propageront à travers toute l'épitaxie. Ces fluctuations de tension transitoires peuvent être transmises par couplages capacitifs dans le puits P^- de la logique et déclenche des dysfonctionnements dans cette partie logique. Ce dysfonctionnement est constitué essentiellement par le phénomène de *lach-up*.

Les solutions technologiques envisagées pour réaliser cet isolement sont la technique de l'isolation par jonction, de l'isolation diélectrique, de l'isolation RESURF, et d'auto isolement.

2.1 LA TECHNIQUE D'ISOLATION PAR JONCTION :

La technique d'isolation par jonction est couramment utilisée en technologie bipolaire. Cette technique est basée sur le principe d'utilisation des puits profonds de type P^+ polarisés au même potentiel que le substrat, afin de séparer totalement les éléments de puissance, de haute tension, et des circuits de basse tension, l'un des autres, comme le montre la figure (1). Dans cette figure, nous voyons un élément de puissance constitué d'un transistor DMOS latéral à électrodes coplanaires, et une structure CMOS de basse tension.

Une des méthodes comporte une double couche épitaxie de type N^- et P^- sur substrat de N^+, et consiste de réaliser des diffusions profondes d'impuretés P^+ dans l'épitaxie de type

N^- de manière à créer des îlots isolés du reste du circuit [19]. Les transistors PMOS et NMOS sont fabriqués dans des zones séparées de la puissance.

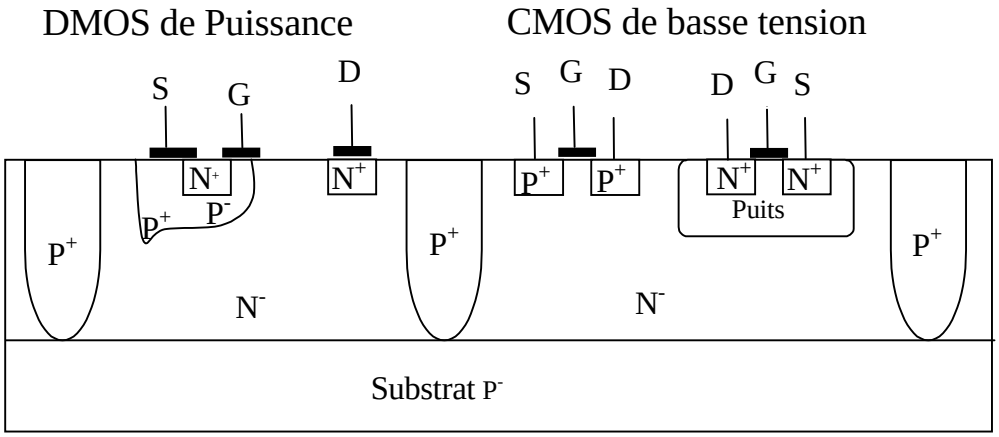


Fig. (1) :Le principe de la technique d'isolation par jonction

Une couche enterrée de type N^+ doit être réalisée sous le drain du MOS de puissance pour permettre au courant de transiter verticalement figure (2). Cette technique d'isolation a l'avantage de permettre de travailler en multi-interrupteurs en ramenant le courant du drain en surface du silicium. Par contre le tenu en tension maximum est limitée par la possibilité de diffuser profondément les mure d'isolations verticales P^+.

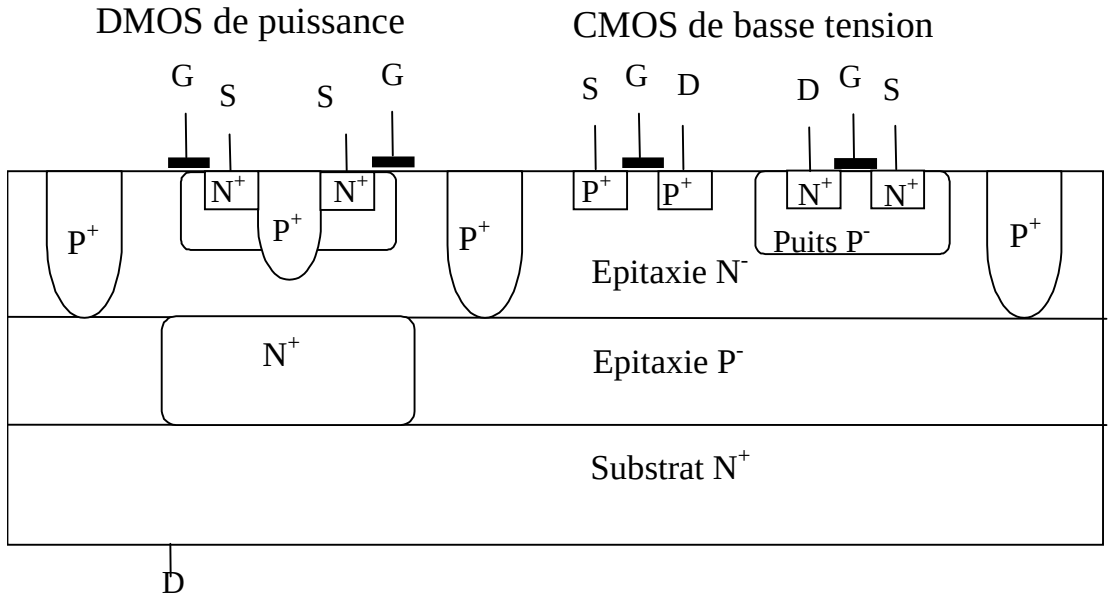


Fig. (2) : L'isolation par jonction. Double épitaxie

Une autre méthode comporte une seule épitaxie N^-, réalisée en deux étapes, sur un substrat N^+. Une couche enterrée de type P^+ est réalisée sous la région où la logique de contrôle va être hébergée après la première étape d'épitaxie [20]. Après la reprise d'épitaxie, des jonctions P^+ profondes diffusées jusqu'à cette couche enterrée définissent un caisson d'isolation de la logique par rapport à l'élément de puissance figure (3). L'avantage de cette deuxième méthode est que l'épaisseur du drain de l'élément de puissance est aussi l'épaisseur de l'épitaxie N^- qui n'est pas limitée par des considérations technologiques. Elle est bien adaptée aux éléments de puissance qui doivent tenir une très haute tension.

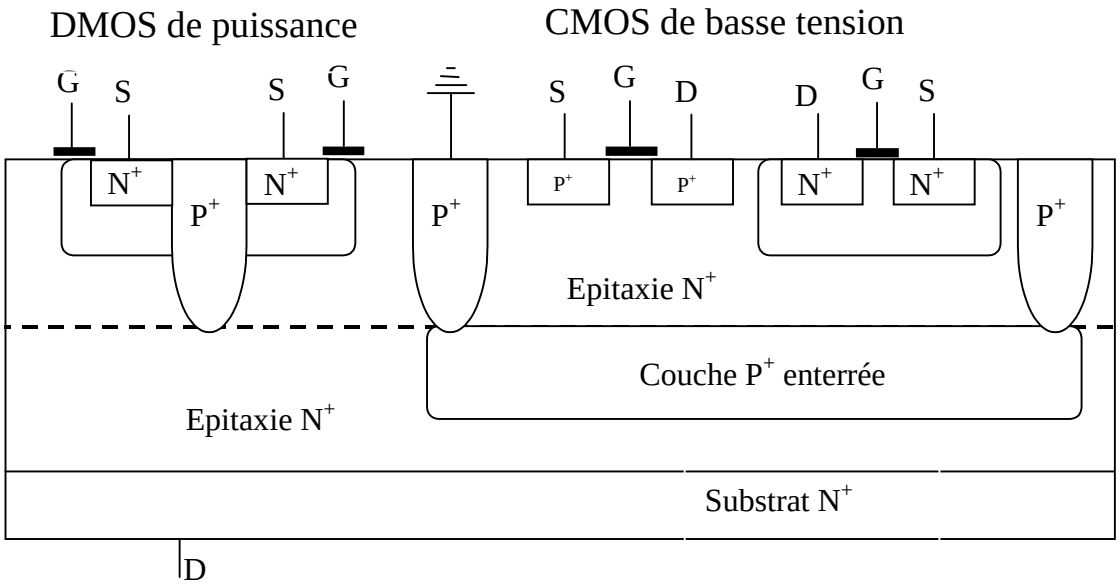


Fig.(3) : L'isolation par jonction. Reprise d'épitaxie

Ces technologies offrent une bien meilleure isolation aussi bien en statique qu'en dynamique. Cependant, des structures parasites de type bipolaire, sont susceptibles de se déclencher lors de forte transitoires en dV/dt. La conception d un tel circuit nécessite donc un certain nombre de précaution et présente donc des difficultés non négligeables.

L'intégration sur la même puce de plusieurs interrupteurs intelligents DMOS est possible sans aucune contrainte sur les connexions de drains, sources et grilles. Cette technologie, véritablement multi-interrupteurs, permet la réalisation de commandes de moteur en pont avec des niveaux de puissance de sortie élevés (400W) [21].

2.2 LA TECHNIQUE DE L'ISOLATION DIELECTRIQUE :

La technologie de l'isolation diélectrique consiste à réaliser sur le même substrat plusieurs caissons diélectriques totalement indépendants, destinés à héberger soit des dispositifs de puissance, soit la circuiterie de petit signal figure (4). En contrôlant l'épaisseur de la couche de diélectrique, cette technique permet ainsi de réduire les couplages entre les divers éléments du circuit tout en conservant une densité d'intégration élevée.

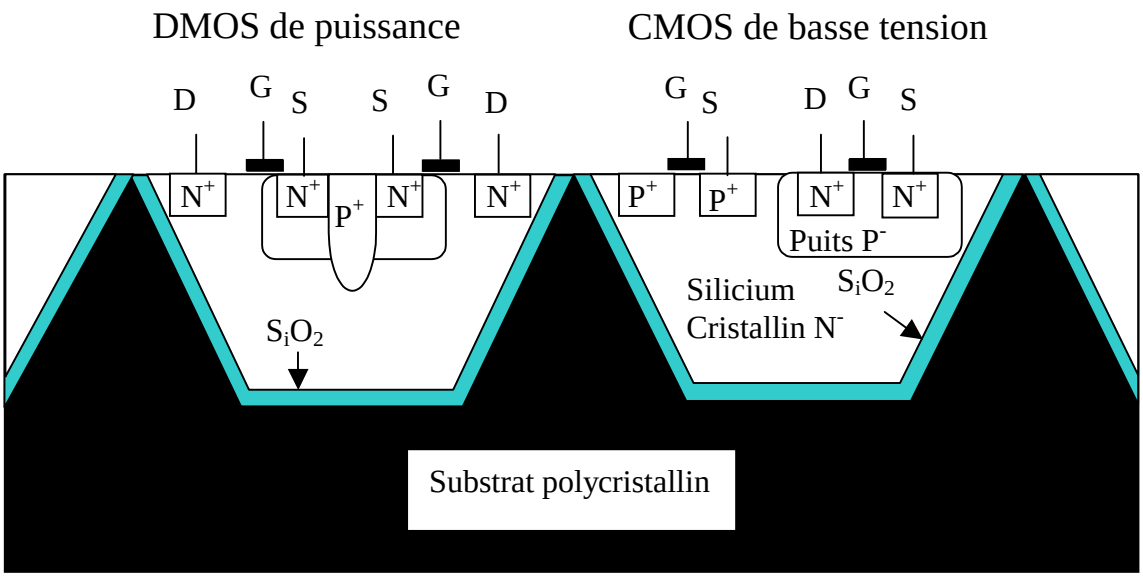


Fig. (4): la technique de l'isolation diélectrique

Ce procédé est généralement utilisé dans des applications haute tension [22] (>100V) faible puissance (les courants sont de l'ordre de 100mA). En effet, si le composant de puissance se trouve dans cette configuration isolée électriquement de la circuiterie petit signal, il l'est aussi thermiquement du radiateur fixé sur la face arrière de la puce[23].

L'isolation diélectrique est une technologie capable d'intégrer des dispositifs de différente nature sur une même puce tout en gardant une forte rapidité, une grande densité d'intégration et une bonne immunité au *latch-up*. En effet, la couche de diélectrique permet d'éliminer les structure bipolaires parasites responsables de l'initialisation du latch-up. Dans le cas d'un circuit de puissance intelligente, il s'agit d'isoler une logique de contrôle CMOS d'un élément de puissance.

2.3 LA TECHNIQUE DE L'ISOLATION RESURF :

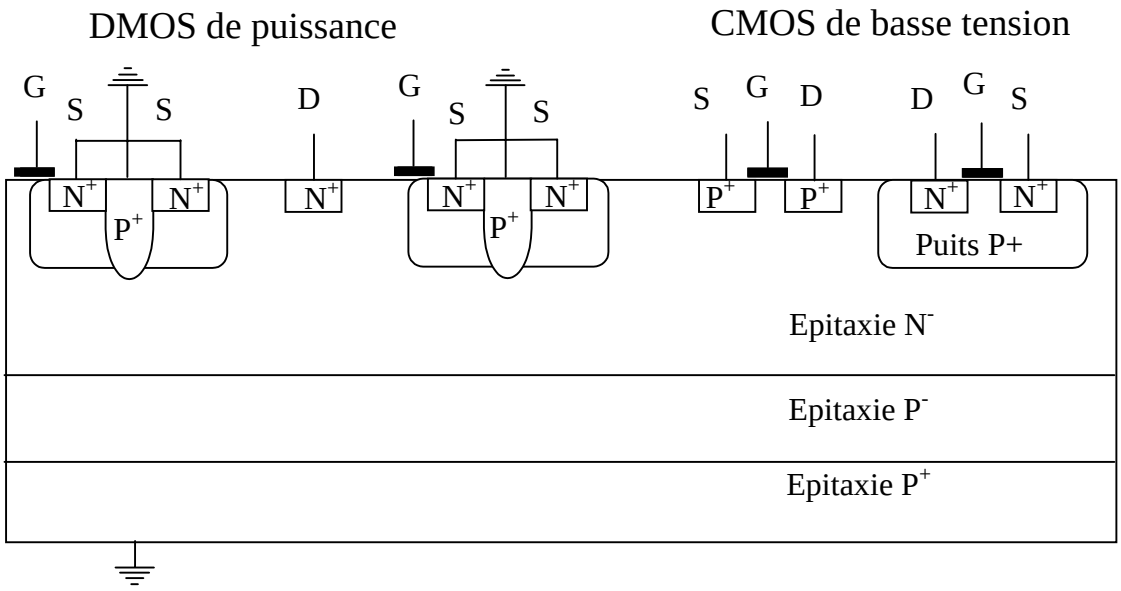


Fig. (5) :La technique de l'isolation RESURF

Il s'agit d'une nouvelle technique utilisée pour l'isolation entre une logique CMOS et un transistor latéral de puissance LDMOS (*Lateral Double Diffused Metal Oxide Semiconductor*). Deux couches épitaxiées, P^- et N^-, sont réalisées sur un substrat P^+ [24][25].

L'isolation est obtenue grâce à la polarisation à la masse du substrat P^+ et du puits P figure (5). La région épitaxie sous l'élément de puissance est alors fortement dépeuplée, ce qui a pour effet d'atténuer les perturbations en tension et courant survenant lors de la coupure de la mise en conduction de l'élément de puissance et permet donc d'implanter à côté de l'élément de puissance une logique CMOS isolée.

2.4 LA TECHNIQUE DE L'AUTO-ISOLEMENT :

Une des technologies de puissance intelligente basse tension la plus simple qui puisse être élaborée est l'association d'un transistor vertical DMOS de puissance avec une technologie CMOS puits P implantée directement sur le substrat N^- du DMOS qui constitue le drain de VDMOS [26]. Cette implantation directe sans autre forme d'isolation est possible du

fait du fonctionnement normal du transistor MOS qui conserve à tout moment ses jonctions en inverse d'où le terme de technique d'auto-isolée. Cette propriété, vraie en régime statique, n'est pas toujours vérifiée en régime dynamique lors des commutations de l'interrupteur DMOS.

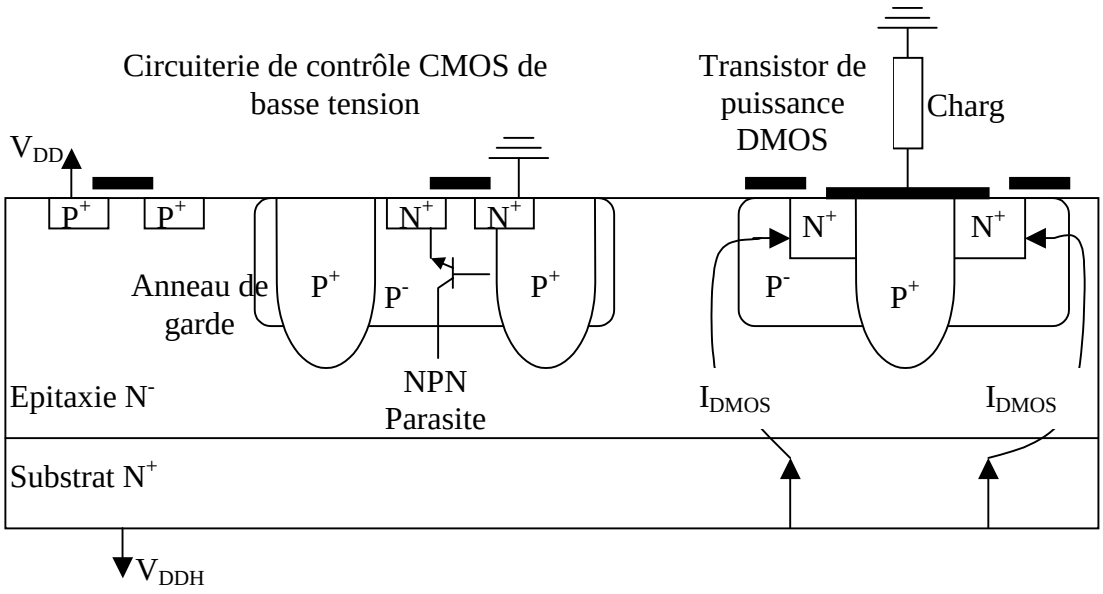


Fig. (6) : Technologie CMOS/DMOS auto-isolée et la technique de puits flottant

En effet, comme le montre la figure (6), le substrat N^- du DMOS est alors le siège de transistors en tension , dV/dt, qui par couplage capacitif, peuvent induire le déclenchement des transistors bipolaires de la technologie CMOS et initialiser le phénomène du latch-up. La solution préconisée, contrairement à la technique d'attache ferme à la masse du puits P de la technologie par des contacts ohmique, consiste à laisser au potentiel du puits la liberté de flotter en régime dynamique tout en restant proche de la masse en régime statique. Ceci est obtenu en utilisant la diffusion de P^+ profonde nécessaire à la fabrication du DMOS, pour réaliser un anneau de garde qui entoure le transistor NMOS et recouvre légèrement sa source pour former une jonction N^+/P^+ [14]. En régime statique, c'est cette jonction qui permet une polarisation du puits proche de la masse et garantit une tenue en tension proche de celle d'un puits attaché à la masse. L'efficacité de cette technique de puits flottant a été montrée expérimentalement sur la base d'une technologie développée au LAAS [27][28][21].

Cette technologie présente le choix technologique le moins chère, mais l'inconvénient de cette technique est qu'elle ne permet pas de travailler en multi-interrupteur et seulement en configuration haute.

3 LE CHOIX D'UNE TECHNOLOGIE DE PUISSANCE INTELLIGENTE

Nous venons de voir les différentes techniques permettant d'obtenir un isolement efficace entre les régions de puissance et celles de petit signal. Cependant, le choix de l'une ou d'autre de ces technologies dépendra d'une part, des caractéristiques de tenu en tension et de calibre en courant désirées, et d'autre part du facteur du coût.

Les technologies de puissance intelligentes possèdent des caractéristiques très différentes. La technique diélectrique, bien que dispensant la meilleure isolation et s'avérant très appropriée aux applications hautes tension, demeure très coûteuse. L'isolation par jonction est la technique la plus largement adoptée en matière de puissance intelligente, car elle est en réalité bien moins chère que l'isolation diélectrique et offre au concepteur sensiblement les mêmes possibilités. L'inconvénient de cette technique d'isolation par jonction constitue de ne pas être applicable aux dispositifs verticaux IGBT de puissance, qui semble être actuellement les composants de puissance haute tension les plus prometteurs.

En effet, le choix d'une telle technologie doit être fait en tenant compte de différents facteurs, comme le coût de fabrication, les performances des circuits et le type de montage (configuration basse ou haute, multi-interrupteur ou non).

Le coût de fabrication de ces techniques d'isolation dépend principalement de deux facteurs, le nombre de masques et d'étapes critiques, qui doit être maintenu faible, et d'autre part, le surface, qui doit rester réduite. Le coût de la technologie utilisée représente une forte limitation dans une application de puissance. La moins coûteuse des techniques décrites ici est bien évidemment celle de l'auto-isolement

Les performances des circuits réalisés avec ces techniques d'isolation sont entre autres, leur reproductibilité, leur vitesse de réponse et leur consommation sur le plant

électrique. Cependant, dans les applications de puissance intelligente, pour maintenir ces performances il faut assurer un bon isolement de la logique de commande contre différentes perturbations. Ces perturbations peuvent être internes, c'est-à-dire, en provenance de la partie de puissance et externes, c'est-à-dire, en provenance de l'environnement bruyant comme c'est le cas, par exemple, de l'application automobile.

L'isolation dynamique, lors des commutations très rapides de l'élément de puissance ou de la réponse provoquée par une charge inductive, pose un problème majeure à résoudre. L'épitaxie N^- située sous la région du transistor de puissance, sera soumise aux fluctuations de tension et des courants rapides qui se propageront à travers toute l'épitaxie. Ces fluctuations de tension transitoires peuvent être transmises par couplage capacitif dans le puits P^- de la logique et déclencher le phénomène de *latch-up* dans cette partie logique. Ce problème peut être résolu dans le cadre d'une technique d'isolation diélectrique.

4 LA COMMUTATRUES DE PUISSANCE EN TECHNOLOGIES DE PUISSANCE INTELLIGENTES :

Les circuits d'interface pour le contrôle des actionneurs aux contraintes de sûreté en fonctionnement utilisent généralement des éléments de puissance et de haute tension en sortie. L'intégration des actionneurs à haute tension d'alimentation et puissance dissipée dans les systèmes micro-électronique intégrés en silicium est devenue récemment possible en utilisant les commutateurs de puissance intégrés en technologie BCDMOS.

Il y a quelques années, les transistors bipolaires étaient les principaux composants actifs utilisés comme interrupteurs ainsi que dans les amplifications de puissance, étant donnée le fort courant qu'ils peuvent délivrer et bon contrôle géométrique de la largeur de zone active de transistor (base). De récent progrès dans les processus technologiques et l'introduction de nouvelles structures ont apporté des améliorations considérables relatives aux calibres en courant et en tension ainsi qu'à la puissance délivrée en sortie.

Deux familles de composants de puissance intégrés compatibles aux technologies MOS viennent de remplacer les transistors bipolaires de puissance dans la plupart des applications. Ces deux familles de dispositifs sont les transistors MOSFET de puissance et les

transistors bipolaires à porte isolée IGBT. Ils utilisent la même surface pour les même caractéristiques de puissance et nécessitent une dissipation de puissance beaucoup plus réduite pour le circuit de contrôle. Les processus de fabrication sont similaires pour les transistors MOSFET de puissance et pour les IGBT, sauf la polarité du substrat.

Dans le cas des applications où les tensions exigées sont relativement faibles, inférieures à 100V, et les courants varient entre 0.1A à quelques ampère, le composant de puissance DMOS couvre parfaitement ces spécifications et constitue donc le composant de choix.

Le développement des composants DMOS a été essentiellement lié à une conception technologique particulière :

- utilisation de la technique de double diffusion permettant d'obtenir des longueurs de canal faibles, ainsi que l'auto-alignement canal-drain.

- existence d'une région faiblement dopée entre le canal proprement dit (région inversée) et le drain N+, qui supporte le potentiel appliqué entre la source et la grille.

La configuration du transistor de puissance DMOS peut être présentée de deux manières, telles que la configuration haute (dans laquelle le drain du transistor de puissance est relié à l'alimentation), et la configuration basse (dans laquelle la charge est reliée à l'alimentation). La figure (7) montre ces deux types de configurations.

Enfin, la forte résistance d'entrée du transistor DMOS simplifie son circuit de commande en ne réclamant en régime statique aucune puissance continue, sa grille, exclusivement capacitive, est simplement pilotée en tension. Le principal avantage de ce type de transistors est la vitesse de commutation des porteurs majoritaires, qui ne risque pas de se dégrader par les problèmes de stockage des charges des porteurs minoritaires rencontrés dans les transistors bipolaires. Le transistor DMOS de puissance à canal N est préféré à celui à canal P, en raison de la forte mobilité des électrons par rapport aux trous, le transistor DMOS à canal N requiert pour la même résistance passante environ trois fois moins de surface

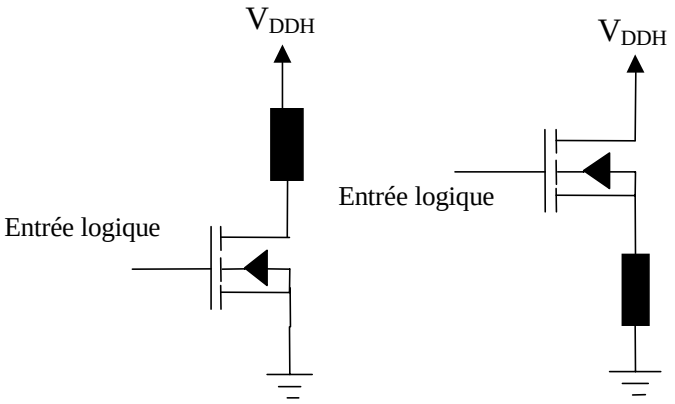


Fig. (7) : Configurations de transistor de puissance DMOS

Deux configurations sont utilisées dans la technologie DMOS afin de réaliser la fonction d'interrupteur dans les circuits intégrés de puissance. Ce sont, d'une part, les structures verticales VDMOS (*Vertical Double-diffused Metal Oxide Semiconductor*) utilisé en tant que "mono-interrupteur" où le drain est situé à la face arrière de la puce, et d'autre part, les structures horizontales LDMOS (*Lateral Double-diffused Metal Oxide Semiconductor*) assuré une fonction multi-interrupteur où les électrodes sont coplanaires et le flot de courant est horizontal.

La structure VDMOS se caractérise par les points suivants : grille en poly silicium enterrée sous la métallisation de source, canal horizontal, accès au drain par la couche accumulée sous la grille suivie par une région de drift faiblement dopée. En ce qui concerne l'intégration de ce type de composants, il semble être limité à la famille de puissance intelligente, utilisant un seul interrupteur. Il est en effet impossible d'isoler les drains de deux VDMOS réalisés sur la même puce.

Le transistor LDMOS possède l'avantage par rapport au transistor à configuration vertical VDMOS d'avoir intrinsèquement ses trois électrodes coplanaires [29], ce qui le rend favorable à l'intégration. Il est également compatible avec les technologies BiCMOS avancées, ce qui fait de lui un candidat idéal pour assurer la partie de puissance, c'est-à-dire la fonction d'interrupteur dans un circuit intégré ainsi que la solution la moins chère.

4.1 LE TRANSISTOR DE PUISSANCE LDMOS :

Les dispositifs horizontaux, dont une coupe technologique est donnée dans la figure (8) sont en général des transistors MOS latéraux double diffusé LDMOS. Ce sont en principe des composants à faible calibre en courant de l'ordre de 200 à 500 mA. La structure d'un LDMOS se caractérise tout d'abord par un substrat massif N-/N+, puis une région de drift faiblement dopée situé entre la fin du canal et le drain. Le contact de drain se situe sur la face supérieure de la puce. Cette structure est donc à électrodes coplanaires.

La résistance passante de transistor des structures latérales LDMOS est plus grande que celle dans les structures verticales VDMOS (environ trois fois), et dépend, d'une part, des données géométriques (la largeur et la longueur de la grille et particulièrement les dimensions de zone de drift), et d'autre part, de la polarisation de grille-source. Par ailleurs, la tenu en tension d'une telle structure peut monter jusqu'à 350V, et la tension de seuil jusqu'à 0.67V.

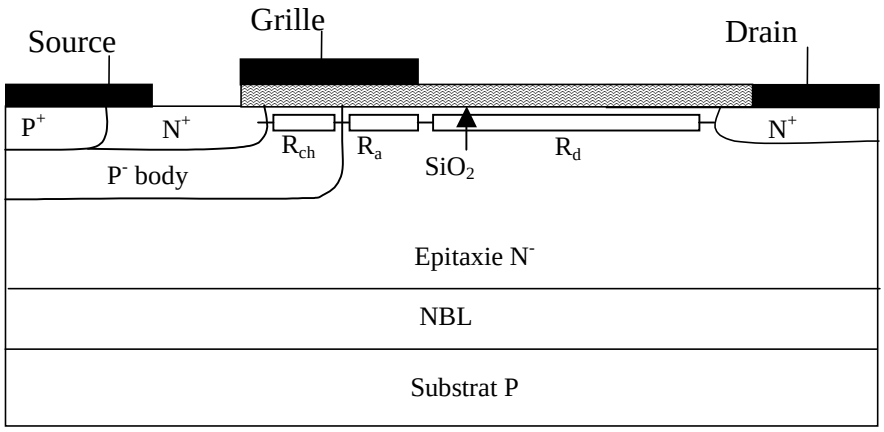


Fig.(8) : Coupe technologique du transistor LDMOS

4.1.1 LE REGIME DE FONCTIONNEMENT :

Dans le transistor LDMOS à canal N, polarisé en directe, le fonctionnement est régi par la contribution de trois zones :

1- La zone active de canal qui assure la conduction du courant électrique de drain, ce canal d'inversion est formé par les porteurs minoritaires (électrons) induits en surface de la

zone P^- (body), sous l'effet d'une polarisation positive appliquée entre la grille et la source du transistor. Les caractéristiques physiques et technologiques de cette zone telles que la longueur du canal, la mobilité, et le dopage de diffusion P, gèrent le niveau du courant de drain. Cette zone présente la résistance du canal R_{ch}. En général, le poids de cette résistance est négligeable devant la résistance à l'état passant pour les composants de haute tenue en tension.

2- La zone d'accès qui se forme sous l'électrode de grille dans la région superficielle N^-, fonctionnant en régime accumulé. Sa présence est induite par une polarisation grille-drain positive. Cette zone présente la résistance d'accumulation $R_{a.}$ Cette résistance dépend également des données géométriques et de la polarisation de grille et a un effet résistif qui agit sur les formes des caractéristiques statiques de sortie du transistor. Cette résistance a été longuement étudiée par J. L. Sanchez [30], elle suit une loi identique à la résistance du canal inversé.

3- La zone drift qui correspond à la zone épitaxie faiblement dopée de type N^-, qui permet aux électrons du canal de circuler latéralement afin d'accéder au drain, cette zone permet d'assurer la tenu en tension du dispositif. Autrement dit, plus la tension de claquage du composant est élevée, plus la résistivité et l'épaisseur de cette zone sont élevées. Cette zone présente la résistance de drift R_d.

En régime de commutation, les deux états de fonctionnement du transistor DMOS sont : l'état passant et l'état bloqué. Chacun de ces régimes de fonctionnement est régi par les paramètres géométriques et technologiques du composant. L'état passant se caractérise par la formation d'un canal d'inversion qui se crée grâce à l'application d'une tension positive entre la source et la grille du transistor par conséquent, par la circulation d'un courant dans la structure. Alors que l'état bloqué se caractérise par l'application entre la grille et la source d'une tension inférieure à celle de seuil.

Lorsque le transistor est à l'état passant, le canal formé en surface de la région P^- (body), assure la continuité de la nature des porteurs entre la source et le drain. Lorsque le transistor fonctionne à l'état passant, il se comporte comme une résistance, notée $R_{ds\text{-}on}$, qui est la somme des trois résistances suivantes :

$$R_{ds\_on} = R_{ch} + R_a + R_d \text{.....(1-3)}$$

Cette résistance impose une chute de tension aux bornes du composant de puissance. Cette chute de tension a pour expression :

$$V_{DS} = R_{ds\_on} . I_D \text{.....(2-3)}$$

Les pertes de puissance sont :

$$P = V_{DS} . I_D = R_{ds\_on} . I_D \text{.....(3-3)}$$

Il est clair que la résistance à l'état passant est le paramètre le plus important : plus faible elle sera, plus faibles seront les pertes.

Les résultats expérimentaux montrent que la résistance à l'état passant varie en fonction de la tension grille-source du composant. Plus la tension grille-source augmente, plus la résistance à l'état passant décroît.

4.1.2 AIRE DE SECURITE :

La figure (9) montre l'aire de sécurité d'un transistor MOS de puissance. Les limites de la zone de fonctionnement sont définies par :

1)- La tension de claquage du transistor V_{DBR}, imposée par les conditions d'avalanche.

2)- L'hyperbole de dissipation de puissance (V_{DS}*I_D = constante), correspondant à une température de la puce, choisie pour une raison de fiabilité, de l'ordre de 150°C.

3)- Le courant maximal de drain, correspondant au maximum de tension de polarisation appliquée sur la grille.

4)- Le lieu de seconde claquage.

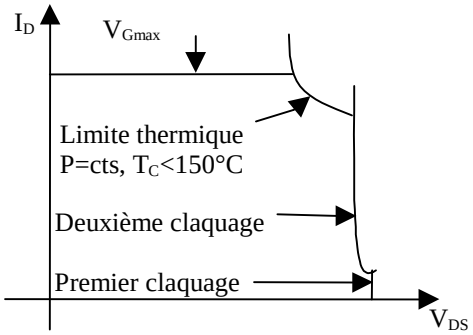


Fig ; (9) : Aire de sécurité d'un transistor MOS de puissance

4.2 COMMANDE DE GRILLE DU TRANSISTOR DOMS:

Le rôle des circuits de commande rapprochée du transistor de puissance, consiste à convertir un signal logique d'entrée 5V en un signal de commande haute-tension, avec des vitesses de commutation, à la mise en conduction et au blocage, les plus courts possibles (tout en restant compatible avec les contraintes de compatibilité électromagnétique). Ces temps de transition, lorsqu'ils sont inférieurs à une cinquantaine de microsondes, permettent de minimiser les pertes au moment de la commutation de l'interrupteur de puissance et d'éviter ainsi toute surchauffe excessive de la puce de puissance.

Les capacités de grille des transistors DMOS varient d'une centaine de picofarads à une dizaine de nanofarafds, le circuit de commande de grille doit ainsi être capable de délivrer des courants pics de 1 mA à 1 A en fonction de l'application.

La configuration haute de l'interrupteur de puissance que nous allons adopter pour notre application nécessite, pour commuter aux bornes de la charge la quasi-totalité de la tension d'alimentation, de porter la grille du DMOS à canal N à une tension supérieure à celle de l'alimentation. D'ailleurs, une valeur très importante de la tension de grille augmente également les temps de commutation et par conséquent la puissance dissipée par le composant de puissance.

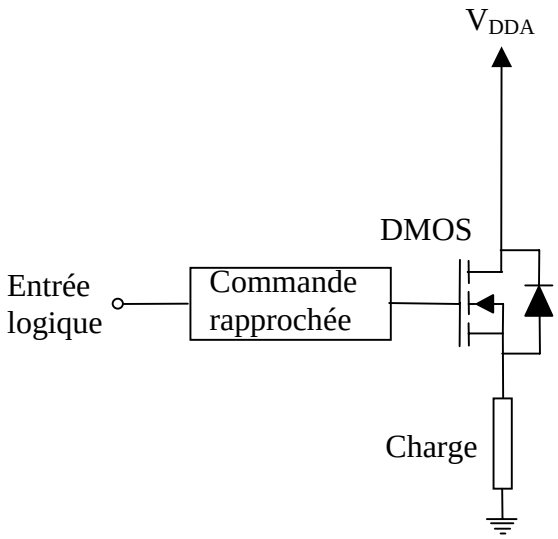


Fig. (10) : La configuration haute de transistor DMOS en technologie de puissance intelligente.

Le circuit de commande de transistor DMOS de puissance en configuration haute présenté dans la figure (10) doit donc fournir sur la grille du transistor de puissance une tension bien supérieure à celle d'alimentation avec une vitesse de commutation inférieure à 50µs.

Afin de piloter la grille de transistor DMOS de puissance par une tension bien supérieur à celle d'alimentation, nous aurons besoin d'un circuit de multiplieur de tension. Ce type des circuit est présenté dans la figure (11), chaque multiple de tension s'articule invariablement autour de trois éléments indissociables, ce sont une source de tension I, une capacité de couplage C_c et un interrupteur S.

Lorsque le signal de l'oscillateur est à un potentiel proche de la masse, la capacité C_c est chargée par la source de courant eu potentiel V_{in} alors que l'interrupteur est ouvert. Durant la demi-période suivante, précisément sur le front montant du signal d'oscillateur d'amplitude V_{in}, la différence de potentiel positif aux bornes de la capacité tend à se conserver. Ainsi, la tension à l'entrée de l'interrupteur prend une valeur supérieure à celle de V_{in} (en théorie le double de V_{in}) et une impulsion de courant traverse l'interrupteur pour charger la capacité de forte valeur C_{ch}.

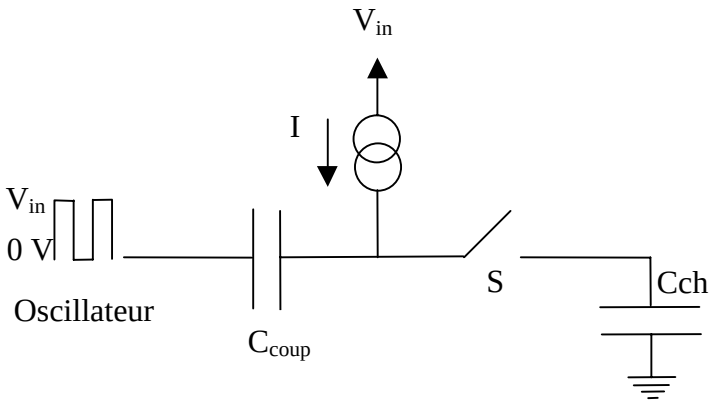


Fig. (11) : Le principe de pompe de charge

Le principe de fonctionnement de ce type de circuit reposant sur le transfert de charges d'une capacité de faible valeur vers une capacité de plus forte valeur, plusieurs périodes d'horloges successives sont donc nécessaires pour réaliser la charge complète de C_{ch} au potentiel $2V_{in}$. c'est pourquoi ces circuits de multiplieurs de tension sont souvent appelés "pompes de charges".

Plusieurs circuits ont été présentés dans ce domaine, entre autre, le multiple de tension classique utilisé en discret pour des applications haute-tension faible courant (10KV-50µA par exemple) [31], les multiples de tension intégrés pour les applications automobile[32][33]. Etant donnée que ces circuits utilisent des diodes isolées, et des capacités, ils possèdent un inconvénient important lié à la technologie utilisée dans cette approche. Le circuit de commande de grille, basé sur des diodes isolées, est conçu dans une technologie différente de celle de transistor de puissance. Il requiert donc une technologie mixte BiMOS, plus onéreuse et moine dense qu'une technologie simple entièrement MOS.

Un autre type des circuits de multiplieurs de tension est apparu dans le cadre des circuits logiques intégrés CMOS VLSI. Ce sont des circuits de pompes de charges basés sur le même principe de transfert de charges, et générant des tensions situées hors de la gamme d’alimentation, aussi positives que négatives.

Un premier type de circuit de pompe à charges négatives, appelé plus spécifiquement «générateur de tension de polarisation de substrat» [34], a pour but de réduire les valeurs des capacités parasites de jonctions drain-substrat en augmentant la polarisation en inverse de ces jonctions et en autorisant de plus faibles dopages de substrat.

Une seconde famille de circuits de pompe à charges CMOS trouvant dans les mémoires, fournit sur la ligne d'écriture des niveaux de tension supérieurs à celle d'alimentation positive, qui permettent de mémorise correctement le bit transmis au niveau de la cellule NMOS. La figure (12) présente une pompe à charges positive fonctionnant sur le même principe de la pompes de charges déjà décrit, où les transistors NMOS N1, N2 jouent ici les rôles respectifs de la source de courant destinée à charger la capacité C à V_{DD} et de l'interrupteur pour transférer les charges sur la ligne lors du front montant de l'oscillateur [35]. La capacité de couplage C est réalisée à l'aide d'un transistor NMOS à enrichissement, à drain et source reliés.

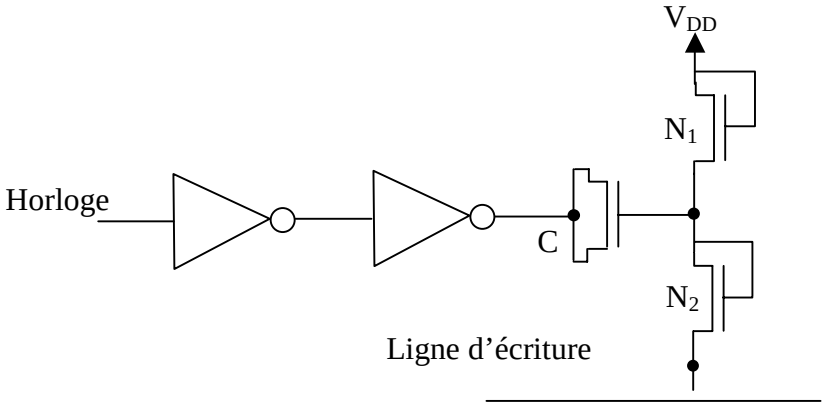


Fig. (12) : Cellule d'écriture NMOS des circuits de mémoires

Le circuit de pompe de charges CMOS utilisé classiquement dans les mémoires est celle de GUPTA [35] figure(13). Il repose sur les charges et décharges successives de la capacité C_{pomp} de faible valeur, au rythme d'oscillations imposées à la sortie d'un décaleur de niveaux, chargé de convertir les oscillations issues de la logique basse-tension en signaux haute-tension d'alimentation.

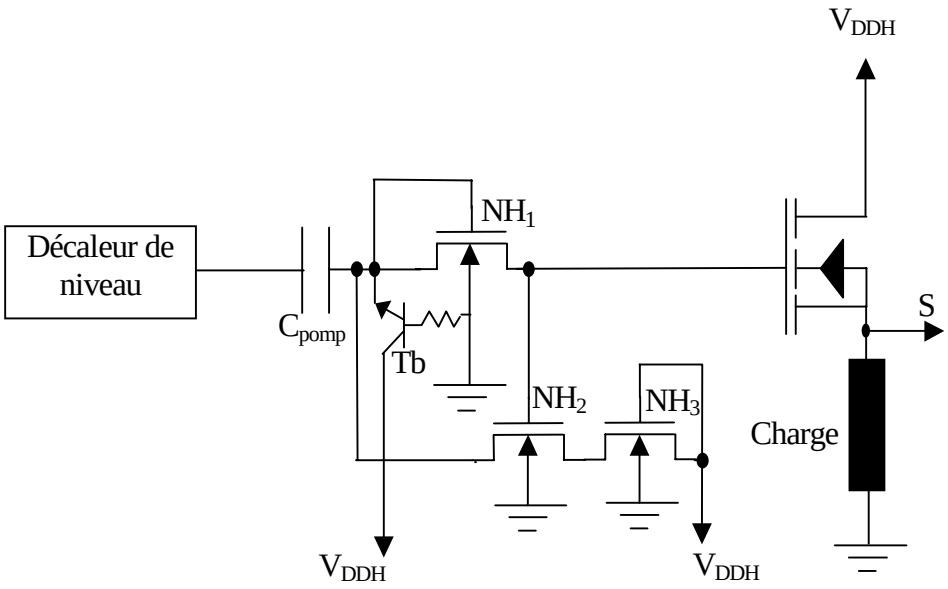


Fig. (13) : Pompe de charges de GUPTA

sur le front descendant du décaleur de niveau, la charge de C_{pomp} est réalisée par la source du courant NMOS constituée des transistors NH2, NH3, ce dernier permet d'éviter tout le courant de fuite en direction de l'alimentation, lord de la décharge de C_{pomp} à travers l'interrupteur NH1, tandis que le niveau de conduction du transistor NH2 est décuplé par la connexion de sa grille à celle du DMOS.

sur le front montant du décaleur de niveau, le potentiel du nœud N est entraîné vers une valeur supérieure à l'alimentation V_{DDH} et la capacité C_{pomp} est décharge sur la grille du transistor DMOS de puissance à travers l'interrupteur NH1, dont le puit P^- est polarisé à la masse.

Le transistor Tb représente un transistor bipolaire vertical NPN parasite associé au drain du transistor NH1, son émetteur est défini par la diffusion N^+ de drain de NH1, sa base par le puits P^- attaché à la masse et son collecteur par le substrat N^- connecté à l'alimentation V_{DDH}. Un des inconvénients de cette pompe de charges CMOS est lié à ce transistor parasite, qui est susceptible de déclencher le phénomène du *latch-up* sur les premiers fronts descendant du signal d'horloge.

Par contre, dans le cas d'applications de puissance intelligente, la tension haute d'alimentation impose au transistor NH1 un effet substrat important, qui réduit la quantité de

charges transmises vers le transistor DMOS. La source du courant réalisée par les transistors NH2, NH3, est également soumise à un fort effet substrat, qui diminue ces performances dynamiques.

L'effet substrat imposé aux transistors NH1, NH2 et NH3 qui réduit les performances dynamiques de pompe de charges dans le cas d'applications de puissance intelligente, ainsi que les risques liés à l'initialisation du phénomène du *latch-up* sont les deux problèmes de cette structure de pompe de charges pour constituer une solution viable pour la commande de grille de transistor DMOS en configuration haute dans des applications de puissance intelligente.

Dans le cadre de la technologie CMOS/DMOS d'auto-isolé une nouvelle version de cette pompe de charges a été construite [36] Elle est basée sur le principe de pompe de charges de GUPTA, utilise le concept de puits flottant pour la réalisation de deux fonctions clés telles que l'interrupteur NMOS et la source de courant. Ce concept permet de réduire l'effet substrat de l'interrupteur NMOS NH3 en chargeant le puits P- (nœud B) au potentiel V_{BAT} de la batterie grâce au transistor PMOS haute-tension, ainsi d'utiliser le transistor bipolaire vertical parasite, associé à la diffusion de drain de l'interrupteur NMOS, comme une source du courant compacte, rapide et performante. La figure (14) présente l'architecture de cette pompe de charges.

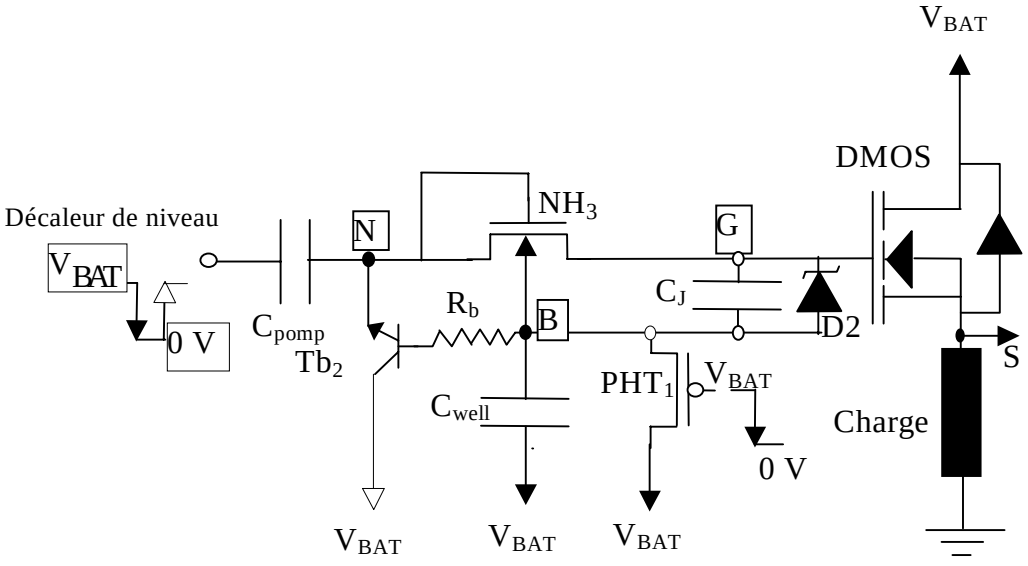


Fig. (14) : Circuit de pompe de charges CMOS basée sur le concept de puits flottant

Les phases successives de la charge et de décharge de la capacité de pompe de charges Cpomp sont respectivement les suivantes:

Sur le front descendant du décaleur de niveau, le transistor bipolaire NPN Tb2, dont le collecteur relié à l'alimentation V_{BAT}, charge la capacité Cpomp au potentiel V_{BAT} moins un seuil de diode Vbe. Dans ce cas de figure, le transistor NMOS à enrichissement, équivalant à un interrupteur ouvert, isole la grille du transistor DMOS de la capacité Cpomp.

Sur le front descendant du décaleur de niveaux, grâce au couplage assuré par la capacité Cpomp, la tension du nœud N est portée à une tension supérieure à celle de la batterie et l'interrupteur NMOS NH3, devenant fortement conducteur, permet la décharge rapide de la capacité Cpomp vers la grille du transistor DMOS de puissance.

Cependant, le déclenchement du phénomène du *latch-up* est évité en limitant les temps de conduction du transistor bipolaire vertical Tb2 à une valeur inférieur au temps minimal de régénération du *latch-up* de l'ordre de 50 ns [37].

5 LA TECHNOLOGIE 0.8 µ HV CMOS DE AMS

Dans le développement d'une famille de circuits de puissance intelligente, le choix de la technologie est une étape capitale, à partir de laquelle se dessinent les principales caractéristiques des circuits. Nombre de critères, directement dépendant de l'application, décident de ce choix technologique, comme le coût de fabrication, les performances de l'élément de puissance et le type de montage (configuration basse ou haute, multi-interrupteur ou non).

La technologie 0.8 µm HV CMOS de AMS, que nous avons retenue pour le projet de ISIS, est une technologie VLSI mixte, qui nous permet d'intégrer sur une seule puce de silicium un ensemble important de fonctions logiques et analogiques complexes à basse tension, ainsi que des éléments de puissances fonctionnant à haute tension d'alimentation (jusqu'à 50 V).

Les transistors de haut voltage de cette technologie pouvant fonctionner jusqu'à une tension de 50 Volts couvrent facilement les besoins d'une tension de 24 Volts visées dans le

projet ISIS, non seulement ça mais aussi la plupart des besoins requises dans le domaine ferroviaire, qui se limitent des signaux de contrôle des actionneurs ne dépassant pas la tension de 50 Volts.

Le transistor Gap-DMOS HV Mid-Oxide N-Channel de 0.8 CMOS HV permet d'implémenter aisément les interrupteurs de puissance de l'interface Fail-Safe développée dans le cadre de projet ISIS. De plus, compte tenu de sa faible résistance à l'état passant (24 KΩμm [38]) ainsi que de ses trois électrodes coplanaires, l'implémentation de plusieurs interrupteurs de puissance sur la même puce est possible.

Concernant le courant fourni et le nombre des signaux de sortie, on doit prévoir une surface de 0.5 mm^2 pour une sortie de 100 mA. Par conséquent, une surface de 8 mm^2 est suffisante pour implémenter 16 sorties de puissance, fournissant chacune un courant de 100 mA. D'autre part, une logique de 250 portes occupera une surface de 0.25 mm^2, ce qui est largement suffisant pour implémenter une double chaîne de surveillance "*Fail-Safe*" permettant d'atteindre un niveau de sécurité très élevée.

6 CONCLUSION :

Dans ce chapitre, nous étions intéressés d'étudier les technologies de puissance intelligente. Par ces technologies, nous intégrons sur la même puce des fonctions logiques et analogiques de basse tension ainsi que des interrupteurs de puissance. Lors de commutations des composants de puissance, des fluctuations de tension et de courrant rapide peuvent se propager à travers du substrat. Ceci produit des dysfonctionnements dans la partie de basse tension notamment le déclenchement du phénomène du *latch-up*. Pour éviter ces dysfonctionnements, nous devons séparer les partie de puissance de celles de basse tension. Les différentes façons actuellement connues pour isoler les parties logiques et analogiques de basse tension de celles de puissance ont été analysées.

Dans un deuxième temps, nous allons présenter les dispositifs de puissance de la technologie de puissance intelligente. Nous avons vu que le transistor DMOS de puissance répond parfaitement aux contraintes imposées par le projet ISIS d'être coplanaire. Ce qui nous permet d'intégrer plusieurs interrupteurs avec leurs circuits de commandes sur la même puce.

Enfin, nous avons présenté la technologie AMS 0.8 HV CMOS de puissance intelligente adoptée pour implémenter l'interface " *Fail-Safe* " de puissance dans le cadre de projet ISIS.

7 BIBLIOGRAPHIE DE CE CHAPITRE

[1] A. ANDREINI, C. CONTIERO, and P. GALBIATI « A New Integrated Silicon Gate Technology Combining Bipolar Linear, CMOS logic, and DMOS Power Parts » IEEE Trans. Electron Devices, Vol. ED-33, pp. 2025-2030, Décembre 1986.

[1] S. KRISHAN, J. KUO, and I.S. GAETA "An Analog Technology Integrates Bipolar, CMOS, and High-Voltage DMOS Transistors" IEEE Trans. Electron Devices, Vol. ED-31, pp. 89-95, Jan. 1984.

[3] C .CONTERO, P. GALBIATI, A. ANDREINI. European Patent Application, 0267882, date de publication 18.05.1988.

[4] R. ZEMBRANO, "Isolation Technique in Power IC's with Vertical Current Flow" ESSDERC, 1987, pp.653-656.

[5] P. GIVELIN, "Bibliothèque Compatible CMOS/DMOS de Fonctions de Commande et de Protection Pour les Application Automobiles de Puissance Intelligente », Thèse de 3ème cycle, INSAT, 1994.

[6] C. LU et al., « An analog/digital BCDMOS technologique with dielectric isolation-devices and processes », IEEE Trans. Electron Devices, Vol. 35, N° 2, Février 1988, pp. 230-237.

[7] B. MURARI, « La puissance intégrée n'a pas dit son dernier mot », Electronique, N° 23, Décembre 1992, pp. 26-28.

[8] N. AZZOUZ, « Composant LDMOS pour Circuits Intégrés Haute tension », Thèse de doctorat de l'université de Paul Sabatier (Toulouse), Juin 1989.

[9] M.A. BOUANANE, « Conception et Optimisation des Composants DMOS Latéraux Haute Tension en Technologie Resurf », Thèse de doctorat de l'université de Paul Sabatier (Toulouse), décembre 1992.

[10] Ingénieur de l'automobile, numéro spécial, juin 1986, pp. 91-108.

[11] M. BAHLEUR, J. BUXO, Ph. GIVELIN, M. PUIG VIDAL, V. MACARY, G. SARRABAYROUSE, "application of a floatting well concept to a latch-up free, low cost, smart power high-side switch technology", IEEE J. of Solid State Circuits, Vol. 40, N° 7, July 1993, pp. 1340-1342.

[12] M.PUIG VIDAL, "Immunité au latch-up d'une technologie de puissance intelligente CMOS/DMOS basée sur un concept de puits flottant », Thèse de Doctorat de l'université Paul Sabatier (Toulouse), Février 1993.

[13] T. EFLAND, « Lateral DMOS Structure Development for Advanced Power Technologies », Technical Joural, Vol. 11, N° 2, pp. 10-23, Mars- Avril 1994.

[14] J.L. SANCHEZ, « Propriétés à l'Etat Passant des Transistors DMOS de puissance Coplanaires et Verticaux », Thèse de 3ème cycle, INSAT, 1984.

[15] W. WILLS, « Get high voltag with low-cost multipler », Electronic designe, N° 13, 21 Juin 1974, pp.64-68.

[16] J.F. DICKSON, "On-chip high-voltage generation in MNOS integrated circuits using an improved voltage multiplier technique", IEEE J. Solid-State Circuits, Vol. 11, N° 3, Juin 1976, pp. 374-378.

[17] W.C. DUNN, "Driving and protection of high side NMOS power switches", IEEE Trans. Industry Applications, Vol. 28, N°1, Janvier/Février 1992, pp. 26-30.

[18] W.L. MARTINO et al., "An on-chip back-bias generator for MOS dynamic memory", IEEE J. Solid-state Circuits, Vol. 15, N° 5, Octobre 1980, pp. 820-825.

[19] A. GUPTA, T. CHIU, M. CHANGE, A. RENNINGER et G. PERLEGOS, « A 5V-only 16K EEPROM utilizing oxynitride dielectrics and EPROM redundancy », Proc. ISCCC Février 1982, pp. 184-185.

[20] M. BAFLEUR, Ph. GIVELIN, M. PUIG VIDAL, J. BUXO, et V. MACARY, “Cost-effective Smart Power CMOS/DMOS technology: Design of Main Drining and protection functions”, Analog Integrated Circuits and Signal Processing 8, pp. 133-246 1995.

[21] R.D. RUNG et H. MOMOSE, “DC holding and dynamic triggering characteristics of bulk CMOS latch-up”, IEEE Trans. Electron Devices, Vol. 30, N° 12, Décembre 1983, pp. 1647-1655.

[22] T. FUJIHIRA et al., “Self-isolation NMOS-DMOS technology for automotive low-side switches” Proc. Symp. High Voltage end Smart Power IC’s, 1989, pp. 392-397.

[23] B. MURARI, “Power integrated circuits : problems, tradeoffs and solutions”, IEEE J. Solid-State Circuits, Vol. 13, N° 3, Juin 1978, pp. 307-319.

[24] C.E. CORDONNIER, “Le Sensefet : un MOS à miroir de courant », Electronique de puissance, N°18, Décembre 1986, pp.34-38.

[25] Austria Mikro Systeme Inernational AG « 0.8 µm HV CMOS Process Parameters », June 1999.

1 INTRODUCTION. 49

2 L'ISOLATION BASSE TENSION-PUISSANCE : 51

2.1 LA TECHNIQUE D'ISOLATION PAR JONCTION : 51

2.2 LA TECHNIQUE DE L'ISOLATION DIELECTRIQUE : 54

2.3 LA TECHNIQUE DE L'ISOLATION RESURF : 55

2.4 LA TECHNIQUE DE L'AUTO-ISOLREMENT : 55

3 LE CHOIX D'UNE TECHNOLOGIE DE PUISSANCE INTELLIGENTE 57

4 LA COMMUTATRUES DE PUISSANCE EN TECHNOLOGIES DE PUISSANCE INTELLIGENTES : 58

4.1 LE TRANSISTOR DE PUISSANCE LDMOS : 61

4.1.1 le régime de fonctionnement : 61

4.1.2 aire de sécurité : 63

5 LES FONCTIONS DE PUISSANCE ITELLIGENTE :ERREUR ! SIGNET NON DEFINI.

5.1 COMMANDE DE GRILLE DU TRANSISTOR DOMS: 64

5.2 PROTECTION DU TRANSISTOR DMOS DE PUISSANCE CONTRE LA TEMPERATURES EXCESSIVES : ..... **ERREUR ! SIGNET NON DEFINI.**

5.3 PROTECTION DU TRANSISTOR DMOS DE PUISSANCE CONTRE LE SURCHARGE EN COURANT : ..... **ERREUR ! SIGNET NON DEFINI.**

6 LA TECHNOLOGIE 0.8 µM HV CMOS DE AMS 70

7 CONCLUSION : 71

8 BIBLIOGRAPHIE DE CETTE CHAPITRE 73

QUATRIEME CHAPITRE

INTERFACE SECURISEE DE PUISSANCE DANS LE CADRE DU PROJET ISIS

1 INTRODUCTION :

La plupart des actionneurs utilisés dans les systèmes électromécaniques nécessitent l'utilisation des signaux de contrôle de puissance en courant continu. Les technologies microélectroniques de puissance intégrée récentes permettent la génération de signaux aux niveaux de puissance et tension élevés capables d'assurer le contrôle direct des actionneurs, ainsi que l'intégration des fonctions logiques et analogiques en silicium. L'intégration des interfaces fournissant des sorties de puissance présente un avantage significatif pour le coût et la sûreté en fonctionnement de l'application. L'utilisation de composants externes pour transformer les signaux de contrôle codés en fréquence en signaux de puissance et courant continu pour l'attaque de l'actionneur est ainsi évitée. Une structure typique d'interface de puissance pour les systèmes dupliqués (comparateur) sera présentée, et une interface pour les systèmes tripliqués sera décrite (circuit de vote majoritaire). Ensuite, la conception d'interface fail-safe pour les systèmes dupliques, développée dans le cadre de projet ISIS sera détaillée, en présentant la conception de ces deux parties, la partie logique et la partie de puissance.

2 INTERFACE DE CONTROLE D'ACTIONNEUR POUR LES SYSTEMES DUPLIQUES :

Le mécanisme de verrouillage SFSD à l'état sûr d'un système défaillant, décrit dans la chapitre I section 4, coupe l'alimentation de manière irréversible suite à la première détection d'un signal erroné. Ainsi, il n'est plus nécessaire d'utiliser des composants redondants pour isoler à deux ou plusieurs endroits les sorties de la source de l'état non sûre. Pour l'interface de la Figure 2 de premier chapitre, par exemple, la porte NOR contrôlée par le signal *Si* et la porte NAND contrôlée par le signal *Si** peuvent être éliminées. Cette simplification est particulièrement adaptée au cas où les signaux de haute puissance sont utilisés comme des signaux non sûrs, car les transistors utilisés pour transférer les signaux de puissance vers l'actionneur ont des coûts très élevés en surface de silicium. L'utilisation de deux transistors de puissance connectés en série, multiplie par quatre la surface occupée pour assurer les mêmes performances en puissance.

Un exemple de comparateur SFaS avec sorties de puissance est présenté en figure 1. L'acquisition des sorties *S1* et *S1** des systèmes de traitement *S* et *S** est effectuée sur les niveaux actifs des signaux d'horloge *ck* et *ck**. Après son acquisition, le signal logique *S1* est converti en signal de haute puissance par le bloc convertisseur de niveau logique en niveau de puissance L.L./H.P. (*Logic Level to High Power translator*). Le signal *O1* obtenu, a comme état non sûr, l'état de haute puissance correspondant à une valeur élevée du produit V_{DDH} * I, où V_{DDH} est le niveau élevé de tension en sortie et I est le courant correspondant à cet état.

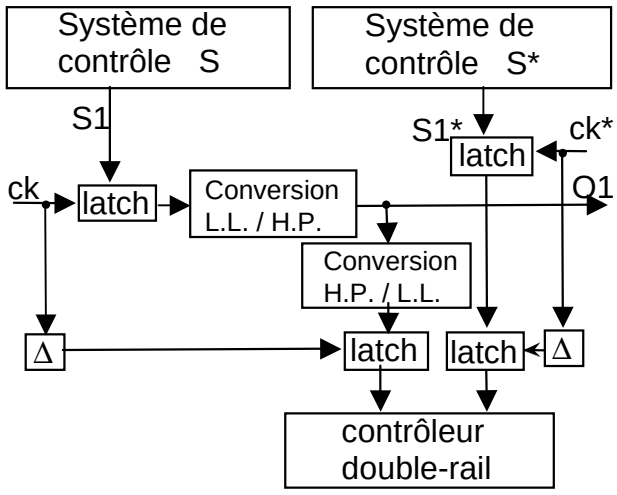


Fig. (1) : Comparateur fortement sûr en présence de défaillances (SFaS) aux sorties de puissance

Ainsi, durant l'état non-sûr du signal *S1*, la sortie *O1* génère une puissance élevée (nécessaire, par exemple, pour enclencher un actionneur) et durant l'état sûr de *S1*, *O1* est à 0V (connectée à la masse). Le signal *O1* contrôle l'actionneur et il est également connecté à un circuit de conversion des niveaux de haute puissance en niveaux logiques conventionnels H.P./L.L. (*High Power to Logic Level translator*). La sortie de ce dernier circuit est verrouillée dans un circuit latch à l'aide d'un signal d'horloge retardé pour obtenir un niveau logique correspondant à l'état stable du signal de contrôle de l'actionneur *O1*. Un deuxième latch au signal d'horloge retardé est utilisé pour synchroniser *S1** à ce signal. Les deux signaux ainsi obtenus sont comparés par un contrôleur double-rail. La sortie de ce contrôleur est connectée aux entrées du mécanisme de verrouillage d'erreur présenté dans le premier chapitre, section 4. La sortie Oe de ce mécanisme sera utilisée pour couper les deux

alimentations du circuit (alimentation Vdd de la partie logique et alimentation V_{DDH} de la partie de puissance).

La transformation du signal *O1* en un signal logique (bloc H.P./L.L.“convertisseur de haute puissance en niveau logique”) doit se faire avec précaution. En effet, il est important de transformer en niveau logique '1' tout niveau électrique sur la sortie *O1* qui pourrait activer l’actionneur (état non sûr). Dans le cadre du projet ISIS, les actionneurs sont activés par des signaux de 24 volts. Néanmoins, à cause d’un phénomène d’hystérisis, ils peuvent rester actifs même si cette tension baisse à un niveau de 0.7 volts. Ainsi, un niveau supérieur ou égal à 0.7 volts doit être transformé au niveau logique '1'. Afin d’avoir une marge de sécurité confortable on va en effet transformer tout niveau électrique supérieur ou égal à 0.7 volt au niveau logique '1'. Ce niveau minimal, qui doit être transposé au niveau logique '1', sera appelé seuil du niveau non sûr (SNNS).

En comparaison avec le circuit de la figure I.2, il n’y a pas de redondance utilisée pour éviter l’apparition de l’état non sûr sur *O1* en cas d’une faute simple. En effet, dans la figure 1, l’état de la sortie *O1* est déterminé à partir du seul signal *S1*. Ainsi une erreur mettant *S1* sur la valeur non sûre, va produire l’état non sûr sur *O1*. Néanmoins, dans ce cas l’état de *O1* sera incohérent avec l’état de *S1**. Il y aura donc détection de l’erreur par le contrôleur double-rail, qui enclenchera la coupure des alimentations et le blocage du circuit à l’état sûr. Le circuit intégré ayant un temps de réaction beaucoup plus rapide que les actionneurs, ce passage à l’état sûr surviendra avant qu’une action dangereuse soit déclenchée. La coupure des alimentations est irréversible, ce qui assure l'objectif de *Ultimate Fail-Safe goal.*

3 INTERFACES SFAS DE CONTROLE D'ACTIONNEURS POUR LES SYSTEMES TMR :

Dans les architectures des systèmes à redondance modulaire triple (TMR), les circuits de vote majoritaire SFaS peuvent être également adaptés au contrôle intégré des actionneurs de haute puissance. Le principe consiste à utiliser trois comparateurs SFaS comme celui de la figure 1, et un bloc de recombinaison, comme illustré en Figure 2. La logique de recombinaison utilise trois diodes à la cathode commune connectée à la sortie *O1* et les trois anodes connectées aux sorties des comparateurs. Les conditions du théorème présenté dans

[3] sont facilement vérifiables pour cette configuration de vote majoritaire, qui satisfait donc à la propriété SFaS.

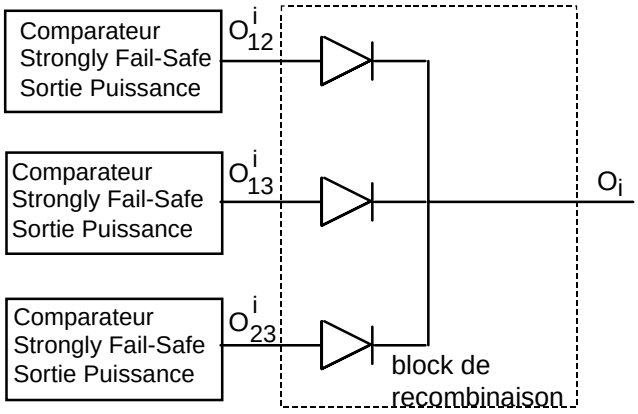


Fig. (2) : Circuit de vote SFaS pour actionneurs de puissance

Pour rajouter des propriétés de tolérance aux fautes au circuit de vote et augmenter ainsi la disponibilité de l'application, chaque indication d'erreur sera utilisée pour couper seulement l'alimentation du comparateur correspondant.

4 RECAPITULATIF DES MECANISMES ASSURANT L'OBJECTIF 'ULTIMATE FAIL-SAFE :

Considérons dans un premier temps ce qui se passe si la fréquence *Fe* n'est pas présente sur *Oe*. Etant donné que le circuit de coupure d'alimentation décrit en Figure 7 du premier chapitre est *Fail-Safe* en présence de défaillances simples et multiples, l'alimentation est coupée si le signal de fréquence *Fe* n'est pas présent à la sortie *Oe*. Sans alimentation le circuit ne peut, en aucun cas et pour aucune combinaison de nouvelles fautes, générer un signal *Fe* à sa sortie *Oe*. Donc, l'alimentation du circuit ne peut jamais être rétablie sans intervention externe. La coupure irréversible de l'alimentation implique l'impossibilité de générer les fréquences représentant l'état non-sûr aux sorties *O1*, *O2*, … *On*. Par conséquent, ceci assure un verrouillage du système à l'état sûr global.

Récapitulons les conséquences des fautes affectant les différentes parties de l'interface.

a) **Fautes dans l'indicateur d'erreur** : Nous avons montré que ces fautes sont détectées. Leur détection génère des combinaisons f1f2 hors-code qui se stabilisent sur la valeur 00 ou 11. Pour ces valeurs, *Oe* est déconnectée de *Fe* et le système est bloqué à l'état sûr et irréversible.

b) **Fautes dans le contrôleur double-rail** : Elles génèrent également des signaux hors-code à l'entrée de l'indicateur d'erreur qui les mémorise, ce qui mène de nouveau à l'état sûr et irréversible.

c) **Fautes dans les convertisseurs double-rail en fréquence** : L'analyse de fautes dans les convertisseurs du code double-rail en code de fréquence a montré que les convertisseurs sont SSD. Ainsi, pour chaque convertisseur, nous savons qu'avant la première détection de faute interne, il génère en sortie des signaux soit corrects, soit sûrs. Donc, il garde sa capacité de déconnecter *Oe* de *Fe* pour des fautes affectant les autres parties du système. Nous avons vu également que la propriété SFSD est obtenue par la redondance, en utilisant deux convertisseurs connectés en série. Ainsi quand la première faute détectable survient sur l'un des convertisseurs, une indication d'erreur est générée sur f1, f2, et par la suite le deuxième convertisseur déconnecte *Oe* de *Fe*. Ce qui mène au blocage dans l'état sûr et irréversible

d) **Fautes dans le comparateur SFaS de la figure 1** : Ces fautes peuvent amener à la génération d'un état erronée non-sûr sur la sortie *O1*. Néanmoins, la surveillance de cette sortie par une chaîne dupliquée permet de détecter l'erreur et de bloquer l'interface dans l'état sûr et irréversible, avant que l'actionneur soit déclenché.

5 IMPLEMENTATION POUR UNE SURETE ACCRUE

Le système décrit précédemment atteint l'objectif *Ultimate Fail-Safe Goal* si on retient l'hypothèse de défaillances simples. Cette hypothèse suppose aussi que les fautes surviennent une à la fois. Si plusieurs fautes surviennent simultanément, la sûreté du système peut être mise en cause.

Pour augmenter le niveau de sûreté face aux fautes multiples, nous pouvons adopter des techniques de redondance supplémentaires, en utilisant un deuxième convertisseur de niveau logique à partir de la sortie de haute puissance *O1* (convertisseur de puissance en

niveau logique). Le signal d'entrée *S1* est également copié une nouvelle fois à l'aide d'un deuxième latch. Les deux paires des signaux ainsi obtenues sont comparées à l'aide de deux contrôleurs double-rail. La sortie de chaque contrôleur est contrôlée par un indicateur d'erreur. Ces indicateurs erreurs contrôlent à leur tour deux convertisseur double-rail en fréquence (figure 3). Les deux convertisseur double-rail en fréquence seront connectés en série pour fournir la fréquence *Fe* sur la sortie *Oe*. Ce signal va couper les deux lignes d'alimentation V_{dd} et V_{DDH} quand un ou plusieurs contrôleurs signalent une erreur.

De cette façon, on aura deux chaînes de surveillances, chaque chaîne se compose d'un contrôleur double-rail, un indicateur d'erreur et un convertisseur double-rail en fréquence. On peut facilement vérifier que le nombre minimum de fautes simultanées nécessaires pour détruire la sûreté est de trois.

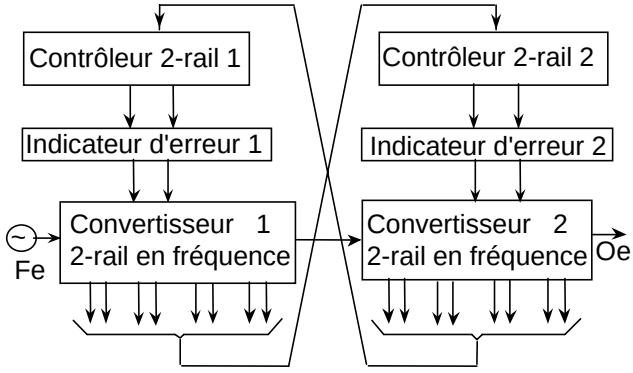


Fig. (3) : Indicateurs d'erreur SFSD à sûreté accrue.

5.1 IMPLEMENTATION DE CONTROLEUR DOUBLE-RAIL :

Le contrôleur 2-rail de la figure (3) peut être implémenté en utilisant des cellules du contrôleur 2-rail comme le montre la figure (4). Cependant, cette structure arborescente a un inconvénient majeur de ne pas être dynamisable. A cause de cet inconvénient, ce contrôleur n'assure pas la sûreté en fonctionnement. Une nouvelle architecture dynamisable sera décrit dans le paragraphe (9). Cette architecture assure non seulement le contrôleur double-rail mais aussi toutes les parties composant la chaîne de surveillance telles que l'indicateur d'erreur et le convertisseur double-rail en fréquence.

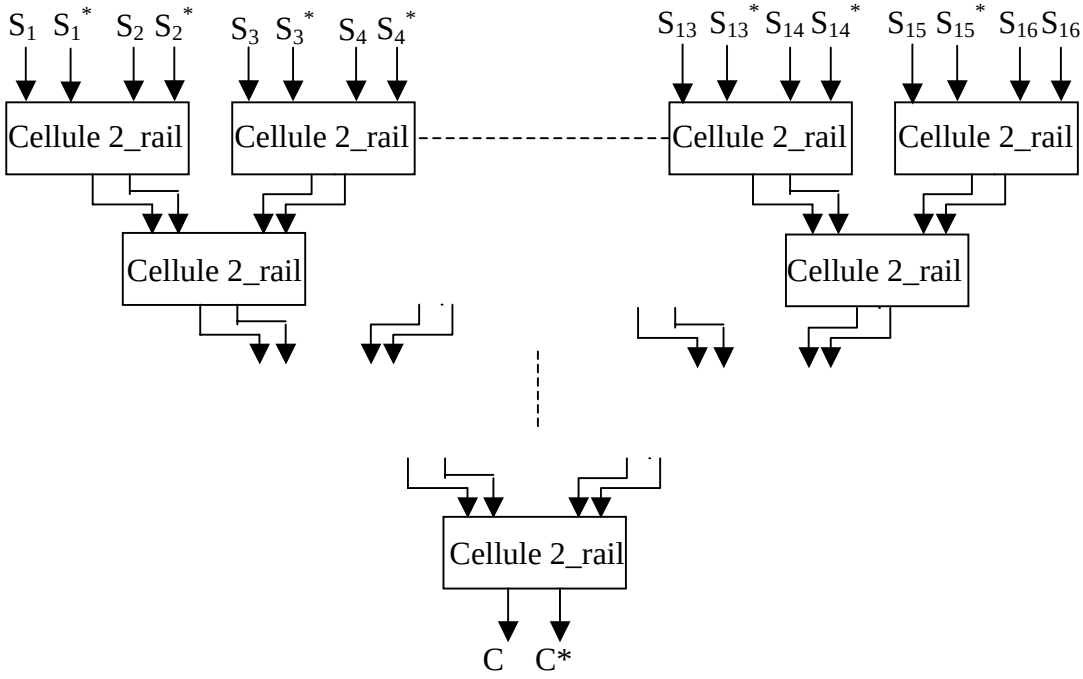


Fig. (4) : Le contrôleur 2-rail non dynamisable

5.2 IMPLEMENTATION D'INDICATEUR D'ERREUR :

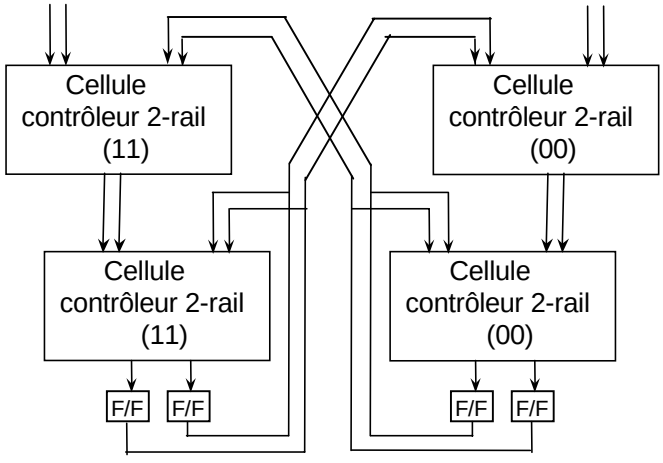


Fig. (5) : Indicateurs d'erreur couplés.

Les deux indicateurs d'erreur peuvent être couplés comme dans la Figure (5)[39]. Ce couplage permettra une plus grande sécurité vis-à-vis des fautes multiples. Pour une diversification de conception, l'un de ces indicateurs d'erreurs utilisera des cellules du

contrôleur double-rail à dominance 11 et l'autre à dominance 00. Les cellules du contrôleur double-rail dominantes 11 et 00 sont déjà présentées dans le premier chapitre, figure (4).

L'implémentation du convertisseur double-rail en fréquence était établie dans le premier chapitre section 4.4.

Il est à noter qu'on peut obtenir un niveau encore plus accru de protection du système en rajoutant des coûts modérés. En effet, le système précédemment développé représente une solution peu coûteuse, car elle nécessite l'utilisation d'un nombre modéré de portes logiques et permet le remplacement des implémentations réalisées en composants discrets. Par exemple, une interface de 16 sorties nécessite 144 portes logiques. Si on utilise une seconde chaîne de comparaison, elle nécessitera 252 portes logiques. Ce coût est négligeable dans une implémentation VLSI. Le coût restera négligeable si on rajoute une troisième ou une quatrième chaîne de comparaison. De toute façon la majorité de la surface sera occupée par la partie de puissance. Cela nous permet d'augmenter la sûreté en présence de fautes multiples, de telle sorte que n'importe quel niveau de sécurité souhaité peut être atteint. Pour ce faire, on augmente le nombre N des éléments de coupure de fréquence connectés en série, comme montré en figure 3 (où N = 2). Ainsi, le signal de fréquence *Fe* est coupé en N points, et le degré de sûreté (le nombre de fautes simultanées nécessaires pour permettre la propagation erronée du signal *Fe*) est augmenté en progression linéaire avec la complexité de l'implémentation.

Cependant, la sûreté est augmentée pour les fautes multiples affectant l'interface, et non pour les fautes affectant les signaux d'entrée *S1, S1** ou les systèmes de traitement qui les génèrent. Pour augmenter la protection des systèmes de traitement, le niveau de redondance utilisé pour leur implémentation doit être également augmenté (e.g. détection de fautes par les biais d'une triplication, d'une duplication renforcée avec le codage de parité, d'un mono-processeur codé au niveau logiciel). Notons aussi que les signaux de clock et d'initialisation des latches seront au moins dupliqués, pour éviter qu'une faute affectant un de ces signaux ne crée pas une situation dangereuse. Par exemple, l'utilisation de deux signaux d'initialisation pour les deux latches de la figure 3 du premier chapitre (signaux de ré-armement), permet de s'assurer que lors d'un défaut affectant un de ces signaux, la faute produit une indication d'erreur déclenchant la coupure d'alimentation. Bien sûr, comme pour les signaux d'entrée *S1,*

*S1**, une redondance plus élevée peut être envisagée afin d'augmenter le niveau de sécurité[39].

5.3 L'INSERTION DU BICS DANS L'INTERFACE :

Nous avons vu dans le deuxième chapitre que l'implémentation des capteurs de courant intégrés BICS dans des circuits utilisés dans une application critique en sécurité, permet de détecter les défauts créant des valeurs non déterminées, qui pourront échapper à la détection par une technique conventionnelle. Cette technique utilise des circuits d'autocontrôle. Le principe de test par un BICS repose sur la comparaison du courant de fuite venant du circuit sous-test avec le courant de référence du BICS.Ce courant sera déterminé selon la méthode expliquée au deuxième chapitre, section 3.1.

Le circuit d'interface en question se compose de deux chaînes de surveillances (figure 3). Chaque chaîne inclue un ensemble de latches d'entrées, un contrôleur double-rail, un indicateur d'erreurs et un convertisseur double-rail en fréquence. La chaîne de surveillance fait transporter de son entrée *Fe* à sa sortie *Oe* un signal de fréquence. En cas de détection d'une faute, la fréquence n'est plus transportée sur *Oe*, et son absence coupe l'alimentation du circuit.

Suivant cette architecture on implémente deux BICS, c'est à dire un BICS par chaque chaîne de surveillance. Cependant, dans cette configuration du BICS, un signal complémentaire Btest fournit la valeur '1' logique durant la phase du test, où dans cette phase la sortie du BICS Bs doit être égal à '0' s'il n'y a pas de défaillance dans la chaîne de surveillance ainsi que dans le BICS lui-même. Par conséquent les deux signaux Btest et la sortie du BICS Bs, forment une paire de signaux double-rail.

La sortie du BICS et le signal complémentaire Btest de l'une des chaînes seront injectés au contrôleur double-rail de l'autre chaîne, et vice-versa. Ainsi, en cas de défaillance sur une chaîne de surveillance le BICS associé pourra signaler cette dernière, et la seconde chaîne de surveillance (supposée sans défaut) permettra de couper la fréquence *Fe* (figure 6).

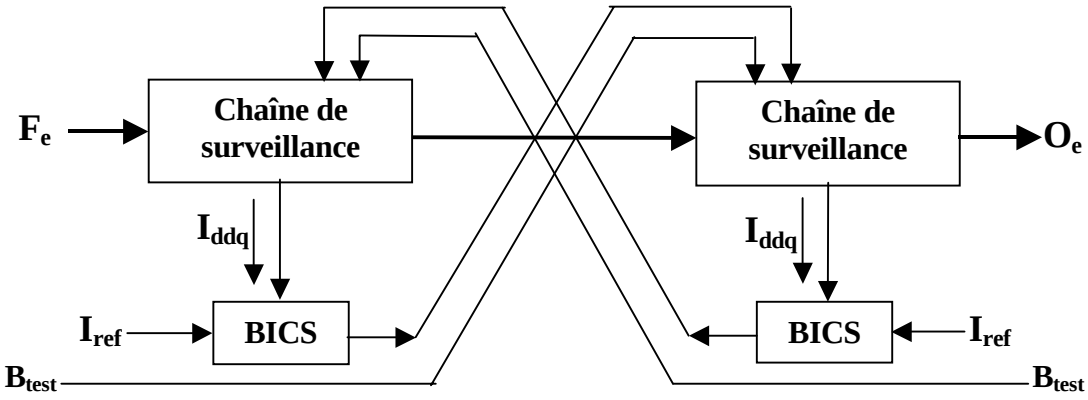


Fig. (6) : Insertion de BICS dans l'interface

L'insertion du BICS dans le circuit d'interface « *Fail-Safe* », a pour l'objectif de tester cette interface, en mesurant le courant venant des chaînes de surveillances. D'une manière générale, une défaillance dans une de ces chaînes de surveillances propage un courant supérieur au courant de fuite, généralement très faible, de l'ordre du micro-ampère. Un test périodique effectué en phase de stabilité des entrées permet, en cas de défaillance, de détecter l'augmentation lente de ce courant, et de couper la tension d'alimentation en mettant la sortie en état sûr, avant qu'une faute de fonctionnement se produise dans l'interface.

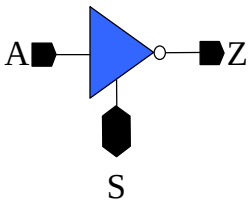
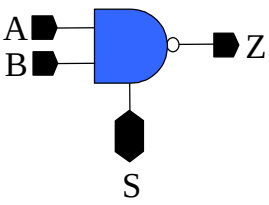
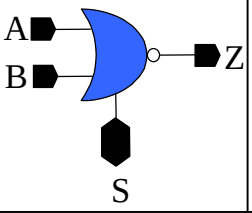
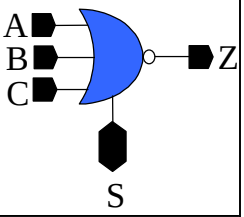
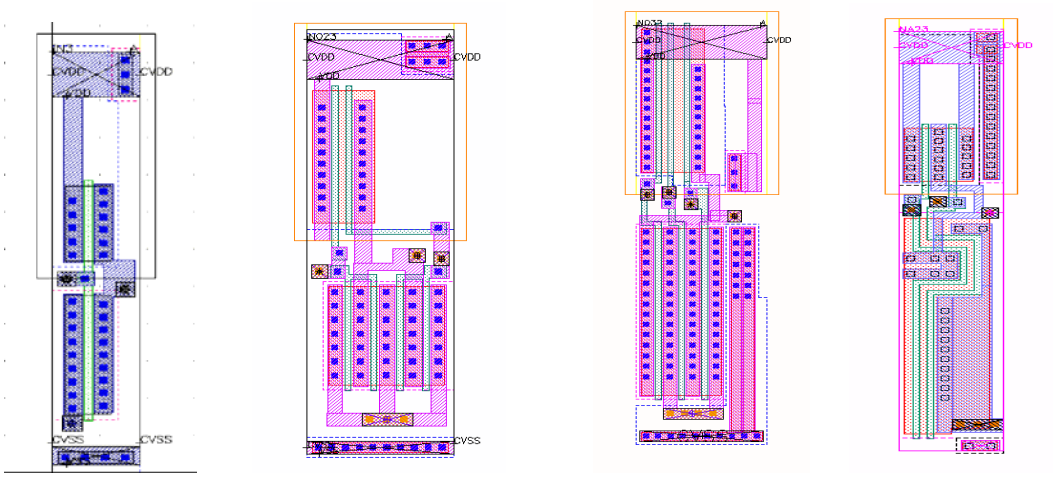
				
W_p	10 um	10 um	20 um	25.7 um
W_n	30 um	50 um	30 um	30 um
$L_{p, n}$	0.8 um	0.8 um	0.8 um	0.8 um

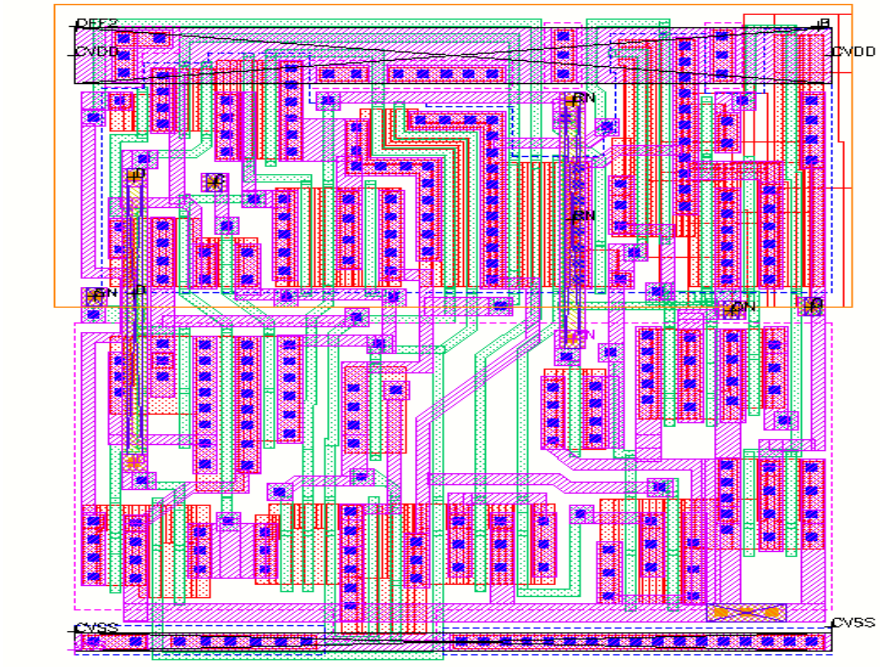
Fig. (7) : les cellules de nouvelle bibliothèque

Etant donné que les cellules standards de la technologie CMOS 0.8 µm haute voltage de AMS adoptée pour le prototype, ne possèdent pas des connexions indépendantes des sources, le fait de mesurer le courant de fuite est impossible. Pour faire face à ce problème,

nous avons créé plusieurs cellules. Ces cellules possèdent la connexion du substrat est séparée de celle de la source comme le montre la figure (7).



Inverseur NOR 2 NOR 3 NAND



Latch D

Fig. (8) : Les layouts des nouvelle cellules

Les layouts de ces cellules ont été réalisés au cours de cette thèse (figure 8), en respectant les règles de dessin de la technologie adoptée, ainsi les dimensions des transistors utilisés pour implémenter ces cellules**.**

D'une telle façon, pour mesurer le courant de fuite d'une des chaînes de surveillance, nous pouvons insérer le BICS en connectant les sources de toutes les cellules de cette chaîne entre elles avec l'entrée du BICS associée qui présente la masse virtuel V_S de la figure II.1, alors que la connexion du substrat de ces cellules est liée à la masse générale du circuit V_{SS}.

Dans le cadre de projet ISIS, afin de pouvoir préciser la valeur du courant de référence du BICS, nous avons tout d'abord déterminé les niveaux des signaux pire cas qui peuvent être acceptés comme « 0 » et « 1 » logique. Le niveau minimal de tension acceptable pour '1' logique est de 4.5 volts, alors que le niveau de tension maximal acceptable pour '0' logique est de 0.5 volt. Ceci pour pouvoir mesurer le courant de fuite venant de la chaîne de surveillance par un BICS et détecter ainsi toute l'augmentation anormale de ce courant dû à un défaut dans le circuit à tester.

Le courant de référence du BICS utilisé sera égal au courant I_{DDQ} minimal résultant de l'application des équations (1-2) et (2-2) (chapitre 2) pour toutes les cellules de la nouvelle bibliothèque. Les résultats obtenus sont illustrés dans le tableau ci-dessous, et ceux ci montrent que le courant I_{ddq} minimal est égal à 17.85 µA.

	Faute dans le réseau N				**Faute dans le réseau P**			
	r_p[KΩ]	**R_p**	**R_{nf}**	**I_{ddq}[µA]**	**r_n[KΩ]**	**R_n**	**R_{pf}**	**I_{ddq}[µA]**
NOT	14	r_p	$9r_p$	35.7	12.5	r_n	$9r_n$	40
NAND2	14	r_p	$9r_p$	35.7	8	$2r_n$	$18r_n$	31.25
NOR2	14	$2r_p$	$18r_p$	**17.85**	12.5	r_n	$9r_n$	40
NOR3	4.5	$3r_p$	$27r_p$	37	12.5	r_n	$9r_n$	40

Fig. (9) : le courant I_{DDQ} minimal

En fait, le courant minimal I_{DDQ} considéré comme un courant de référence I_{ref} du BICS associé à une chaîne de surveillance doit être inférieur au courant total venant de cette chaîne en cas de fonctionnement normal. Le courant de fuite total d'une chaîne de surveillance est égal à l'ensemble des courants de fuites des portes logiques composants cette chaîne. En sachant que chaque chaîne de surveillance se compose de 200 portes logiques, et que le courant de fuite de chaque porte ne dépasse pas quelques dizaines de nano-ampères, en cas du fonctionnement normal, nous pouvons donc estimer le courant de fuite total de cette chaîne à quelques micro-ampères. Par conséquent, pour chaque chaîne de surveillance, nous remarquons que le courant de référence I_{ref} du BICS est largement supérieur à celui de fuite en cas de fonctionnement normal. Cela fait une marge suffisamment large entre le seuil du courant de fuite passant au BICS en cas du fonctionnement normal et celui de référence du BICS dû à la détection des défaillances dans le circuit.

5.4 IMPLEMENTATION DE CONVERTISSEUR DU NIVEAU LOGIQUE EN NIVEAU DE PUISSANCE :

Dans le troisième chapitre, nous avons présenté les technologies de puissance intelligentes. Les interrupteurs de puissance sont les éléments capitaux pour réaliser la fonction de puissance. La configuration haute du transistor de puissance que nous avons adoptée pour notre application, nécessite pour commuter aux bornes de la charge la quasi-totalité de la tension d'alimentation, de porter la grille du transistor DMOS à canal N une tension supérieure à celle de l'alimentation. La commande de grille de transistor de puissance assurant un bon fonctionnement du transistor DMOS de puissance, constitue une fonction clé des circuits intégrés de puissance intelligentes. Cette fonction consiste à convertir un signal logique d'entrée de 5V en une tension de commande de haute tension. Le circuit intégré assurant cette fonction se compose d'un décaleur du niveau et d'une pompe de charges.

Dans le cadre de projet ISIS, La commande de la grille du transistor de puissance est obtenue par conversion du signal logique de basse tension en signal de haute tension, avec des vitesses de commutation, à la mise en conduction et au blocage, les plus courts possibles. Ce temps de transition, lorsqu'il est inférieur à une cinquantaine de microsondes, permet de minimiser les pertes au moment de la commutation de l'interrupteur de puissance et d'éviter

ainsi toute surchauffe de la puce. Le décaleur de niveau utilisé pour cette conversion se compose de deux transistors NMOS (NH_1, NH_2) de haute voltage du type MOS HV Mid-Oxide N-Channel (NMOSMH) et de deux transistors PMOS(PH_1, PH_2) de haut voltage du type MOS HV Mid-Oxide P-Channel (PMOSMH). Les transistor (NH_3, NH_4, et NH_5) et la capacitance Cpom constitue la pompe de charge. Les dimensions de ces transistors sont calculées pour obtenir, d'une part, une tension de polarisation de grille de transistor DMOS de puissance choisie afin de garder ce transistor à l'intérieur de son aire de sécurité, et d'autre part, des vitesses de commutation courtes pour réduire les pertes induites par ces commutations.

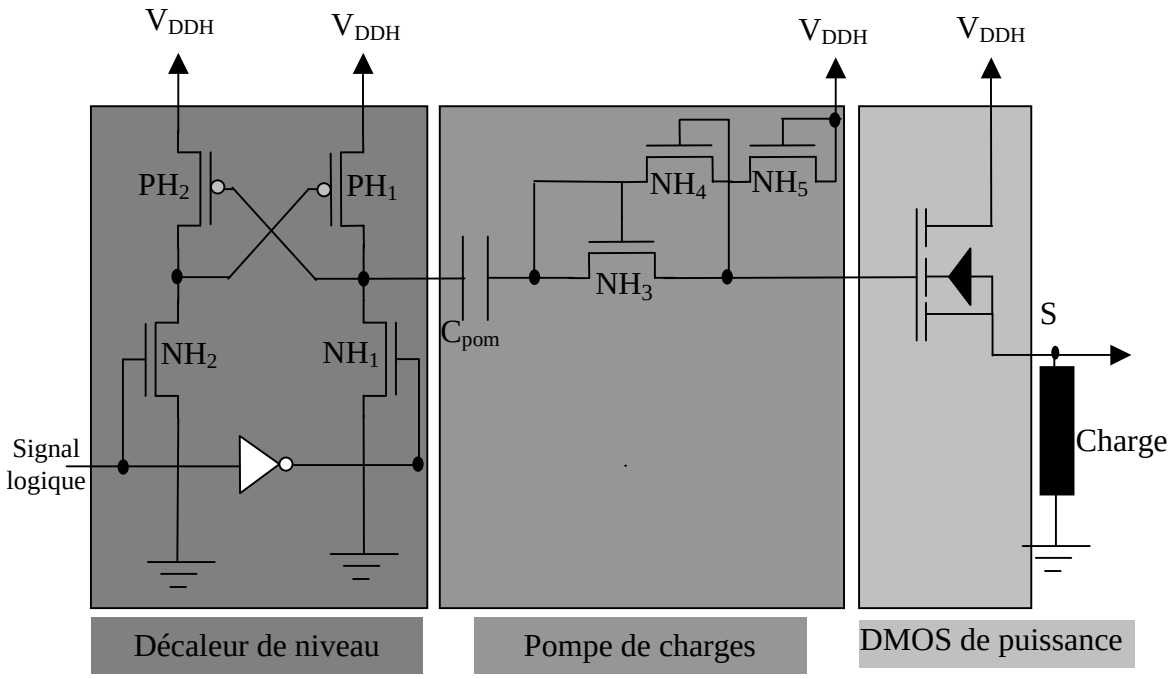


Fig. (10) : Le schéma électrique du convertisseur logique basse tension/puissance

Le schéma électrique de la partie de puissance est illustré dans la figure (10). Nous remarquons dans ce schéma les trois fonctions telles que le décaleur de niveau, la pompe de charges et le transistor DMOS de puissance, permettant de convertir le signal logique en signal de puissance (le bloc L.L./H.P. de la figure 1).

La figure (11) présente les résultats des simulations électriques de ce convertisseur. Ces résultats ont été obtenus pour une fréquence d'horloge de 5 MHz, une charge résistive de 250 Ω (ce qui correspond à la charge du circuit ISIS) connectée à la source du transistor

DMOS de type Gap-DMOS HV Mid-Oxide N-Channel de la technologie adoptée. Le dimensionnement des transistors utilisés dans ce circuit ont été choisis pour atteindre un temps de montée de 5 µs, pour une tension d'alimentation de 24.5 V.

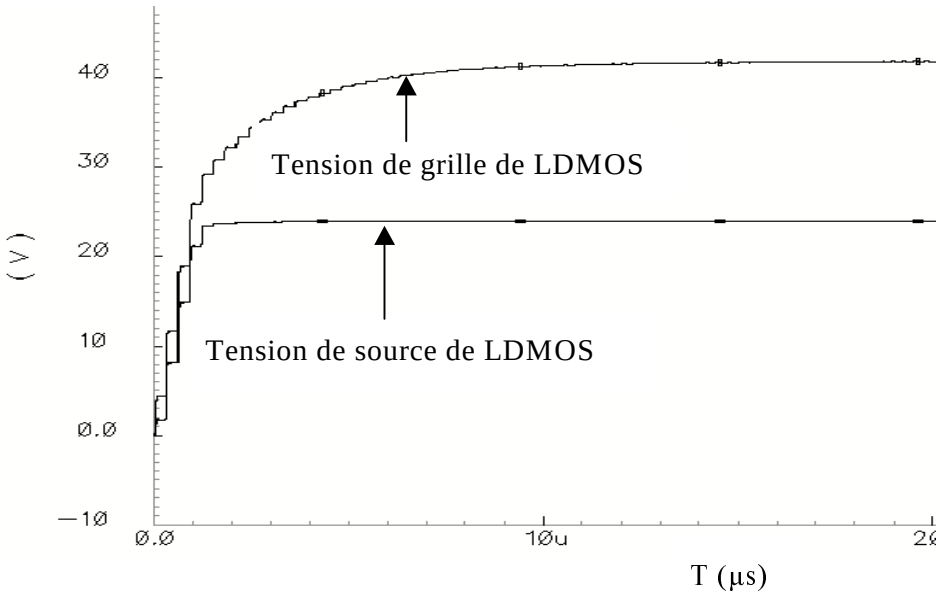


Fig. (11) : Résultats de simulation électrique du convertisseur

logique basse tension/puissance

5.5 IMPLEMENTATION DE CONVERTISSEUR PUISSANCE/LOGIQUE BASSE TENSION :

La transformation du signal de puissance à la sortie en niveau logique s'effectue par l'intermédiaire d'une résistance de forte valeur (la résistance de mesure) introduite en série avec le transistor de puissance (en parallèle avec la charge) permettant de prendre une image exacte du courant qui passe par la charge, et d'un comparateur de seuil (figure 12). La technologie adoptée permet d'implémenter aisément ces fonctions grâce aux composants logiques, analogiques et de puissance qu'elle comporte.

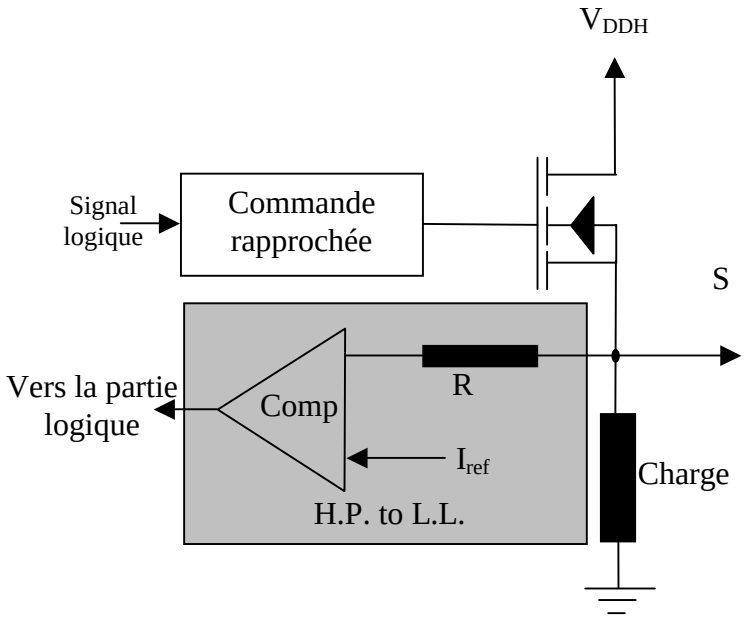


Fig. (12): Le convertisseur puissance/basse tension

Le schéma électrique du comparateur de courant est présenté dans la figure II.9. Les tailles des transistors ont été choisies pour détecter un courant supérieur au courant de référence. La valeur du courant de référence a été déterminée à 28 μA. Cette valeur correspond au courant qui peut passer dans le comparateur quand la tension de sortie S est égale à 0.7 Volts (le seuil à partir duquel l'état est considéré non sûr). Pour la résistance R, nous avons choisi une valeur de 25 KΩ. Cette valeur est suffisamment grande pour empêcher la destruction du comparateur de seuil quand la sortie prend sa valeur maximale (aux alentour de 25 volts). Ainsi le courant maximal est de l'ordre de 1 mA.

La figure (13) présente le layout du circuit de la figure 12.

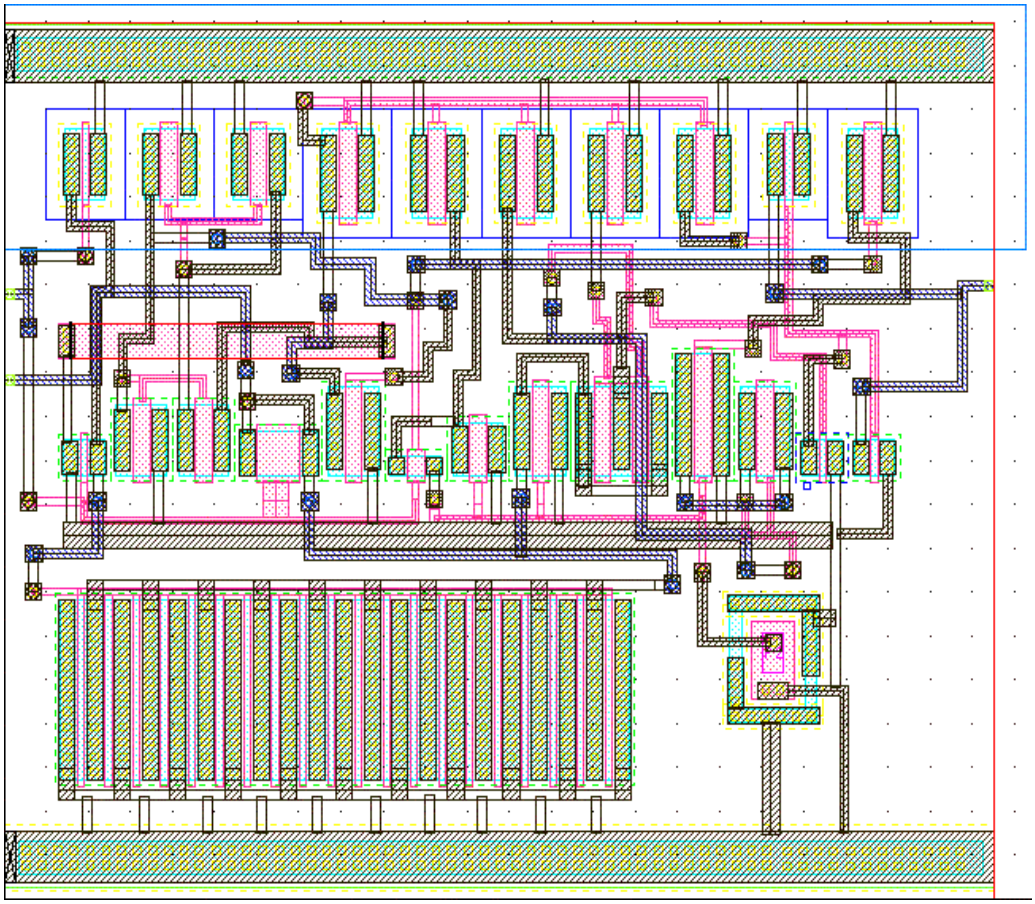


Fig. (13) : Le layout du comparateur du courant

En associant les différents blocs décrits auparavant, on aboutit à un synoptique plus détaillé pour l'interface intégrée (figure 14).

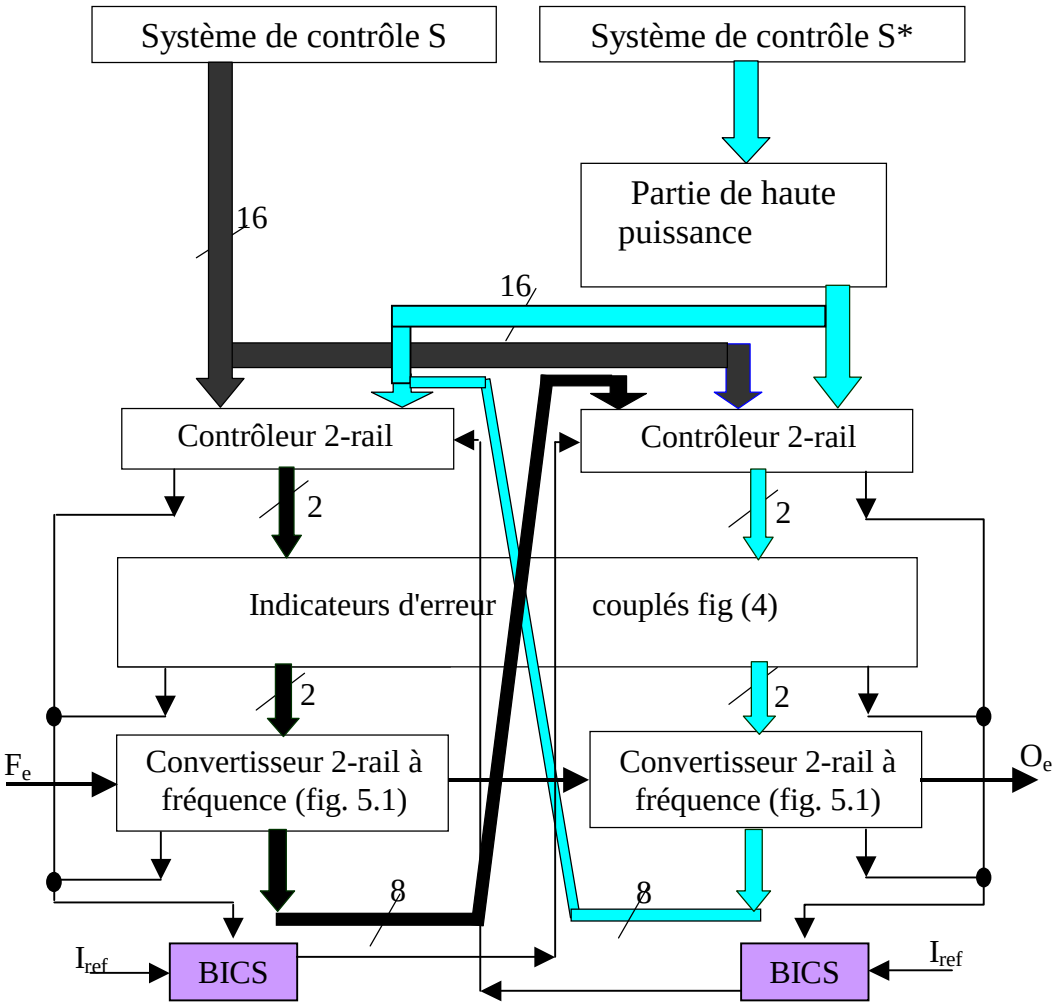


Fig. (14) : Synoptique de l'interface

6 *COMPATIBILITE DES INTERFACES FAIL-SAFE AVEC DES SYSTEMES ELECTRONIQUES SECURISES*

La figure (15) montre la structure de base de l'interface développée dans ce projet. Selon cette figure, le système de calcul sécurisé délivre des signaux dupliqués (éventuellement générés par des systèmes de calcul dupliqués). L'interface inclut un bloc destiné à la transformation des signaux dupliqués $S_{(i)}$, $S^*_{(i)}$, en signaux fail-safe *Oi*. Ce circuit

est contrôlé par un contrôleur double-rail qui procure une indication d'erreur codée sur deux signaux *g1*, *g2*. Ces signaux sont transformés en un signal Fail-Safe *Oe*, utilisé pour couper l'alimentation de l'interface en le bloquant de façon irréversible à l'état sûr.

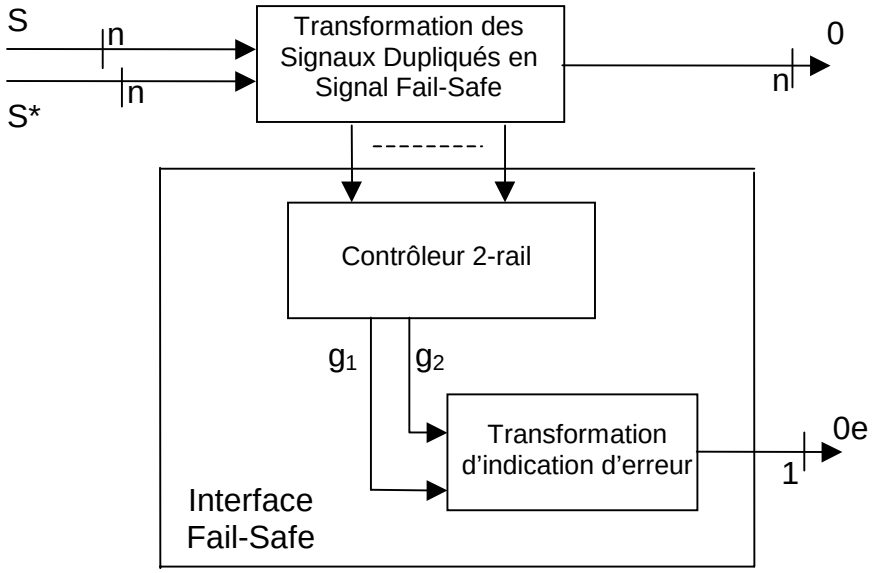


Fig. (15) : Interface *Fail-Safe* pour Systèmes Dupliqués

Le choix d'une interface compatible avec des signaux dupliqués a été fait tout d'abord à cause de l'utilisation très fréquente du principe de la duplication dans les systèmes de sécurité, mais surtout parce qu'une telle interface peut être adaptée très facilement aux autres architectures de sécurité. Le principe général de cette adaptation est présenté dans la figure 16.

Selon cette figure, le système de calcul délivre des sorties qui sont sécurisées par le biais d'un code (Sorties Codées). Ce code peut être autre que la duplication. Par exemple, un des codes souvent utilisés dans les circuits *self-checking* (code de Berger, code m-parmi-n, parité, etc.) ou un code utilisé dans une approche de codage logiciel (e.g. processeur codé). Le Contrôleur des sorties codées garantit qu'en cas de génération par le système de calcul sécurisé de sorties hors code, l'erreur est détectée. Cette détection d'erreur est propagée aux

sorties *g1 g2* du contrôleur double-rail qui implique la disparition de la fréquence *Fe* sur la sortie *Oe*, en mettant le système dans un état sûr.

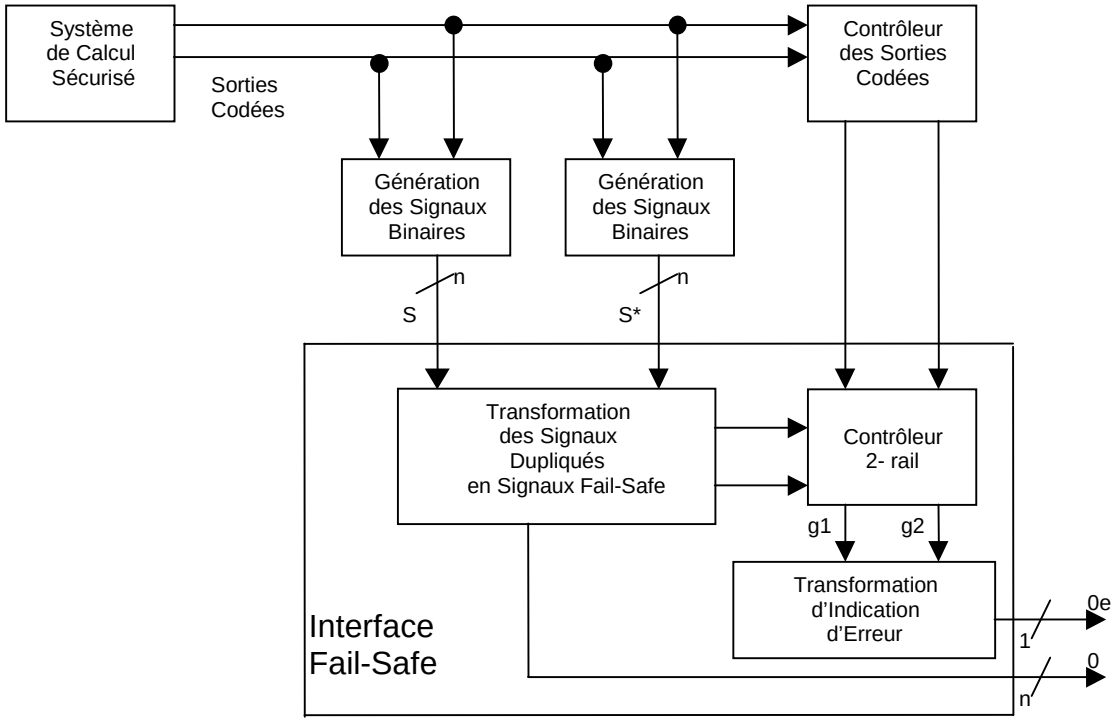


Fig. (16) : Interface *Fail-Safe* pour Système Sécurisé

Bien sûr, le contrôleur des sorties codées doit être conçu de façon à détecter ses propres fautes (contrôleur auto-contrôlable). De tels contrôleurs sont connus dans la littérature pour nombreux codes (e.g. parité, Berger, m-parmi-n, duplication etc.). Si nécessaire, le niveau de sécurité obtenu par un tel contrôleur peut être augmenté davantage en utilisant un deuxième contrôleur. Les signaux *S* et *S** sont générés par des blocs dupliqués, garantissant qu'un seul de ces signaux est affecté en cas de panne simple. Les fautes affectant les sorties du système de calcul sécurisé, et pouvant affecter les signaux *S* et *S** en même temps, sont détectées par le contrôleur des sorties codées. Comme précédemment, si nécessaire, le niveau de sécurité peut être davantage augmenté en augmentant le nombre de blocs de Génération des Signaux Binaires (e.g. utilisation de 3, 4, … blocs).

Une fois que les signaux binaires *S* et *S** sont générés de façon sécuritaire, le reste de la figure 16 peut être réalisé en utilisant l'interface que nous développons dans ce projet.

Le système de la figure 16 est schématique. Le contrôleur des sorties codées et les blocs de génération de signaux binaires peuvent être fusionnés, comme par exemple dans MAPS [40], où un processeur complexe est utilisé pour contrôler les signaux délivrés par le processeur codé [41] et générer les signaux binaires de façon sécuritaire. Ce circuit combine des techniques d'autocontrôles, de la duplication, et du test périodique afin d'obtenir un niveau de sécurité très poussé. Dans un contexte d'un circuit intelligent, comme MAPS [40], il sera envisageable que le contrôleur des sorties codées délivre au contrôleur double-rail une indication de détection d'erreur dès le premier cycle où un mot hors code est généré par le système de calcul sécurisé. Cec,i bien sûr, va réduire la disponibilité du système. Pour éviter ce problème il est aussi envisageable que le contrôleur des sorties codées ne délivre pas une indication de détection d'erreur à la réception du premier mot hors code. Il peut attendre dans ce cas le cycle suivant pour qu'il soit sûr que la faute est permanente, et nécessite un verrouillage du système à l'état sûr. Dans tous les cas de figure, l'interface développée ici pourra être utilisée, les différents choix n'affectant que les autres parties de la figure 13.

7 METHODOLOGIE DE DEMONSTRATION DE LA SECURITE

La démonstration de la sécurité s'effectue en quatre étapes :

- première étape purement théorique avec des théorèmes et des définitions ; compte tenu des différentes propriétés de chacun des blocs, on peut affirmer que l'ensemble permet d'atteindre le *UFS Goal*.

- seconde étape au niveau porte élémentaire : il faut concevoir chaque bloc avec un agencement de portes qui permet de respecter les différentes propriétés annoncées. De plus, chaque porte doit être conçue de telle sorte qu'on ait toujours en sortie un niveau logique et non pas un niveau douteux (qui entraînerait le risque d'interprétation différente par les portes situées en aval). L'utilisation d'un capteur de courant intégré (BICS), peut être aussi envisagée pour se protéger contre ces fautes.

- troisième étape au niveau implémentation : on élimine les courts-circuits qui auraient pour effet le non-respect de l'objectif *UFS Goal*.

- quatrième étape : on vérifie si les conditions de dynamisation de chaque bloc sont suffisantes pour détecter toutes les pannes dont les combinaisons avec d'autres fautes pourraient être dangereuses.

Les trois premières étapes sont discutées plus en détails dans la suite. La quatrième étape est discutée dans la section suivante.

La démonstration de sécurité de l'interface sera basée sur la considération des fautes rencontrées dans les technologies des circuits intégrés. A savoir les collages logiques (*stuck-at*), les transistors collés passants *(stuck-on*) les transistors collés ouverts (*stuck-open*), les courts-circuits (*shorts*) et les coupures.

L'impact de ces fautes sur le fonctionnement du circuit est souvent dépendant de l'implémentation finale. Ainsi la démonstration de sécurité ne se fera de façon définitive qu'une fois le circuit implémenté. Néanmoins, l'ensemble des fautes considérées agit à des niveaux différents de la description du circuit. La sécurité d'interface vis-à-vis de chacun de ces types de fautes, doit être considérée au moment où le niveau de la description correspondant est fixé. Ainsi, la sécurité vis-à-vis des collages logiques sera considérée lors de la description du circuit au niveau des portes logiques. La sécurité vis-à-vis des fautes telles que stuck-on, stuck-open et les coupures, sera considérée lors de la description du niveau des transistors. Néanmoins, étant donné qu'une description au niveau portes logique définit en même temps la description au niveau transistor (dans le cas ou le circuit utilise des portes CMOS standards), la sécurité vis-à-vis des pannes des transistors, pourrait être prise en compte lors de la description au niveau portes. Ceci est possible au moins pour les fautes dont le comportement ne dépend pas du dimensionnement des transistors (telles que les *stuck-open* par exemple). Pour les autres fautes, on doit attendre l'implémentation au niveau électrique pour s'assurer que l'objectif de sécurité est atteint. La simulation de fautes au niveau électrique (SPICE) sera utilisée à ce niveau pour vérifier la sécurité. Si certaines fautes compromettent la sécurité, un changement du dimensionnement de transistors permettra d'atteindre l'objectif de sécurité.

Finalement, l'impact des courts-circuits peut être déterminé une fois que les niveaux électrique et topologique sont définis. Le niveau topologique est nécessaire pour déterminer les courts-circuits qui peuvent réellement survenir. Le niveau électrique est nécessaire pour

simuler leur comportement. Pour les courts-circuits compromettant la sécurité du système, des modifications au niveau électrique peuvent être utilisées pour modifier le comportement dangereux. Alternativement, des modifications au niveau topologique peuvent être utilisées pour éliminer les courts-circuits dangereux, par éloignement des lignes mise en jeux.

Etant donné que l'implémentation au cours de cette étude est réalisée au niveau logique, l'analyse de la sécurité prend d'ores et déjà en compte les collages logiques, et les *stuck-open*. Les *stuck-on* sont aussi considérés afin de donner le type de dimensionnement des transistors qui nous permettra d'éliminer un comportement compromettant la sécurité du système.

Dans l'ensemble, l'assurance de la sécurité pour les *stuck-at* est la partie la plus critique. Si la sécurité n'est pas assurée pour les *stuck-at*, elle ne pourra pas être assurée pour les autres fautes. Par contre, si elle est assurée pour les *stuck-at*, elle pourra l'être pour les autres fautes en agissant sur le niveau électrique et topologique du circuit, ainsi que le séquençage des valeurs appliquées aux entrées du circuit.

Pour mieux comprendre la démarche, notons qu'il y a les situations suivantes à prendre en compte pour chaque faute :

1) Les erreurs produites par une faute ne génèrent pas des sorties erronées correspondant à l'état non-sûr.

2) La faute doit être :

soit 2.1) détectable (pour ne pas affecter la sécurité si une nouvelle faute survient plus tard se combinant avec la première.

soit 2.2) sa combinaison avec une nouvelle faute ne doit pas conduire à des états erronés non-sûrs.

3) Le mécanisme de sécurité déclenché par la détection d'une faute ne doit pas être mis à l'épreuve par l'occurrence de nouvelles fautes.

Le cas 1 est traité en utilisant une chaîne de surveillance basée sur la duplication. Ainsi une faute sur la chaîne de génération des sorties, conduisant à une valeur de sortie erronée et non-sûre, sera détectée par la chaîne de surveillance. La détection forçant le circuit à l'état sûr global supprime la valeur erronée non-sûre.

Le cas 3 est traité en utilisant un mécanisme qui, suite à une détection d'erreur, rentre dans un état passif dans lequel il n'y a plus de sortie possible par cause d'absence de source d'énergie.

Le cas 2.2 est garanti en s'assurant que les fautes non détectables vérifient des propriétés formelles (théorème de la section 4.3 du premier chapitre) qui garantissent que leurs combinaisons avec de nouvelles fautes ne peuvent pas conduire à des états erronés non-sûrs.

Pour le cas 2.1 on montre que les fautes *stuck-at* sont détectables par des valeurs d'entrée survenant durant le fonctionnement normal du circuit. Cette détection permet aussi de s'assurer que les fautes *stuck-open* sont aussi détectables. En fait, considérons une porte logique CMOS incluant un transistor *stuck-open*. Pour détecter ce *stuck-open* on doit d'abord appliquer une valeur qui initialise la sortie de la porte logique à l'état 1 (pour un *stuck-open* de NMOS) ou à l'état 0 (pour un *stuck-open* de CMOS), ces valeurs peuvent être les valeurs qui détectent le *stuck-at* 0 ou le *stuck-at* 1 de la sortie de la porte logique affectée. Ensuite on doit appliquer la valeur qui détecte le *stuck-at* 1 (pour un NMOS) ou le *stuck-at* 0 (pour un CMOS) de la sortie de la porte. On voit donc que si les *stuck-at* sont détectables, les *stuck-open* le sont aussi à condition qu'il n'y ait pas de restriction empêchant d'appliquer les valeurs dans l'ordre requis.

Concernant les *stuck-on*, on peut aussi montrer qu'ils sont détectables par les valeurs détectant les *stuck-at*. En fait le *stuck-on* d'un NMOS est détecté par le vecteur détectant le *stuck-at* 0 de sa porte, tandis que le *stuck-on* d'un PMOS est détecté par le vecteur détectant le *stuck-at* 1 de sa porte. Néanmoins, cette détection n'est pas garantie car la valeur à la sortie de la porte logique peut prendre des valeurs intermédiaires dont l'interprétation dépendra de l'environnement et notamment du bruit. Bien sûr, si le test est répété plusieurs fois (ce qui se passera de façon régulière lors de l'utilisation de l'interface), la probabilité de détection augmente. Ce problème sera résolu au niveau de la description électrique, en imposant que lors de la conduction simultanée du réseau P et du réseau N d'une porte logique, la sortie prendra une valeur logique. De plus, l'implémentation d'un capteur de courant intégré (BICS), permettant la détection de ces fautes par le biais d'une consommation de courant anormale [7] [42] [43]. En fait, un circuit BICS vérifie la consommation de courant pendant la phase de repos du circuit. Cette consommation est extrêmement faible dans les circuits CMOS. Etant

donné que un *stuck-on* crée une connexion entre l'alimentation Vdd et la masse Gnd, le courant en excès est facilement détectable.

La détection de court-circuits nécessite entre autre de mettre l'une des lignes affectées à l'état 1 et l'autre à 0. Ceci n'est pas forcément vrai en cas de valeurs détectant les *stuck-at*. Néanmoins une bonne dynamisation du circuit permettra d'obtenir ces conditions, ayant toujours un dernier recours sur un éloignement topologique des lignes affectées.

Un deuxième problème concerne, comme pour les *stuck-on*, la possibilité de génération de valeurs indéterminées en cas de court-circuit. Cette possibilité est éliminée par l'utilisation des portes logiques de la nouvelle bibliothèque des cellules que nous avons créé. Dans cette bibliothèque, on a suffisamment grandit la largeur des transistors du réseau N. De ce fait, les sorties de ces portes logiques prennent une valeur logique « 0 » en cas de conduction simultanée du réseau N et du réseau P, une situation qui se présente en cas d'un court-circuit ou d'une faute de type *stuck-on*. Les résultats obtenus pour une telle faute dans les cellules de la nouvelle bibliothèque sont montrés dans la figure (17). Ces résultats montrent qu'en cas d'une telle situation, le niveau maximal de tension est égal à 0.467 Volts. Cette valeur est suffisamment basse pour être toujours interprétée comme un niveau logique « 0 » par les autres portes du circuit.

Un problème supplémentaire concerne les court-circuits créant des boucles de contre réaction à parité d'inversion impaire. Ils peuvent créer des oscillations et peuvent compromettre la sécurité s'ils affectent la sortie *Oe*. La sécurité sera aussi affectée par des court-circuits entre *Oe* et une ligne portant la fréquence Fe. Des précautions topologiques permettant l'élimination de telles fautes, seront utilisés lors de l'implémentation au niveau layout.

Finalement, les coupures des lignes ou de contacts se manifestent par des fautes de type *stuck-at* 0 ou *stuck-at* 1. Elles sont prises en compte dans l'analyse des *stuck-at*. Des valeurs indéterminées pourraient aussi apparaître sur les lignes coupées. Elles auraient pour conséquence de mise en conduction simultanée des réseaux N et P des portes suivantes. L'utilisation de portes dont l'un des réseaux est plus conductif que l'autre (comme pour les *stuck-on*) réduira l'effet d'indéterminisme, rendant la majorité de ces fautes détectables. Une

bonne dynamisation du circuit pourra réduire à des niveaux très faibles la probabilité de non-détection.

Comme pour les *stuck-on*, un capteur de courant intégré permettra de détecter les court-circuits et les coupures, par le biais d'une consommation de courant anormale.

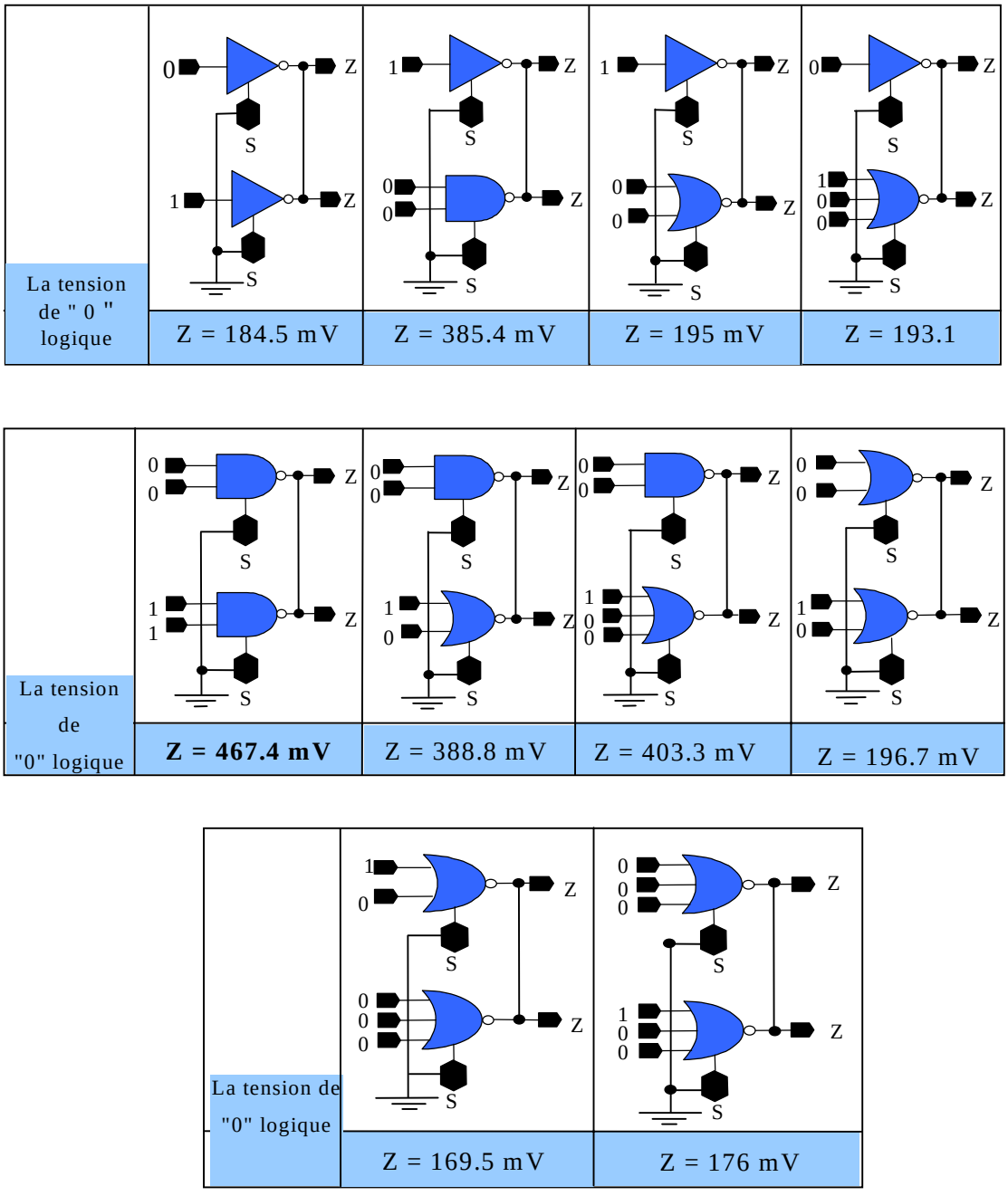


Fig. (17) : Le niveau « 0 » logique en cas de fautes de collages

8 DYNAMISATION

L'analyse précédente vise à démontrer que les fautes sont détectables par des valeurs survenant lors du fonctionnement normal du circuit. Néanmoins, rien n'oblige que ces valeurs vont réellement apparaître et de façon fréquente dans tous les cas d'utilisation de l'interface. Des moyens de dynamisation seront par conséquent indispensables. Pour des raisons de sécurité, il sera prudent de ne pas créer de chemins supplémentaires par lesquels on appliquera les vecteurs de test en connectant périodiquement le circuit sur ces chemins. On préférera donc utiliser les chemins normaux. Ainsi, le système de calcul pourra de temps à autre envoyer des valeurs de test de courte durée (n'activant donc pas les actionneurs), pour s'assurer que les deux valeurs logiques 0 et 1 sont appliquées à chacune des entrées de l'interface. Notons qu'il est exclu d'assurer cette dynamisation par l'intermédiaire du processeur codé. Néanmoins, l'interface n'étant connectée au Processeur Codé que par l'intermédiaire d'un circuit du type MAPS [40], ce dernier pourra assurer la tâche de dynamisation. Cette tâche est parfaitement compatible avec la nature du contrôleur MAPS, étant donné que son cycle de fonctionnement comporte une phase de calcul et une phase de génération des tests.

Il sera aussi utile, lors de ces tests, de réduire le niveau de l'alimentation de puissance (V_{DDH}), pour s'assurer que la chaîne de surveillance reconnaît bien le seuil à partir duquel un niveau de tension sur une sortie *Oi* est considéré comme la valeur non-sûre. Ce seuil est fixé par INRETS de 0.7 Volt, en prenant en compte du comportement des actionneurs (niveau de tension minimum qui active l'actionneur).

Il sera de la même façon possible d'appliquer des tests périodiques pour les autres parties de l'interface, en utilisant le système de calcul. Néanmoins, ces tests seront plus longs que les précédents et peuvent être indésirables. Pour éviter ces tests, une dynamisation interne à l'interface peut être utilisée. Elle aura l'avantage d'être permanente et non périodique. Donc, une latence de fautes extrêmement faible pourra être obtenue. Comme précisé auparavant on devrait éviter de basculer les circuits de l'interface sur des ressources de test. Pour assurer ces contraintes on exploitera le fait qu'à l'exception de la chaîne de puissance et du convertisseur de l'indication d'erreur, l'interface est construite en utilisant des contrôleurs double-rail. On utilisera donc le principe de la figure 18 pour dynamiser ces parties.

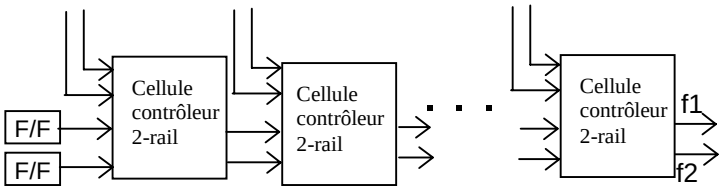


Fig. (18) : Dynamisation d'un contrôleur double-rail réalisé en arbre linéaire

Dans cette Figure, le contrôleur double-rail est réalisé en connectant ses cellules en configuration d'arbre linéaire. Toutes les entrées du contrôleur sont réservées au contrôle des signaux de l'interface, sauf pour une paire d'entrées qui reçoit les sorties d'une paire de *latches*. Ces *latches* changent leur état à chaque coût d'horloge. Ce changement d'état assure la dynamisation de toutes les cellules du contrôleur, même si les valeurs appliquées aux autres paires d'entrées sont corrélées entre elles.

L'inconvénient de la Figure 18 est que l'arbre linéaire est lent. Il pourra donc affecter la vitesse de fonctionnement d'un circuit. Dans un tel cas, un arbre plus rapide peut être utilisé. Néanmoins, un plus grand nombre de *latches* (en configuration LFSR) doit être utilisé, et un plus grand nombre de paires d'entrées doit être dédié à la dynamisation [44].

Le contrôleur de la figure(19) reçoit sur ses entrée un ensemble des signaux venant du système du traitement (S), de la partie de puissance (S*) et du convertisseur double-rail à fréquence (H, H*). Cette structure arborescente non linéaire assure la rapidité du fonctionnement. Cependant, la dynamisation de ce circuit est faite en utilisant la technique présentée dans [44].

Chaque branche verticale de ce contrôleur se compose des cellules 2-rail connectées entre elles en configuration d'arbre linéaire. La dynamisation de cette branche est réalisée en appliquant la méthode expliquée ci-dessus. Autrement dit, toutes les entrées de cette branche sont réservées au nombre limité des paires (SS*) (HH*), sauf une seule paire qui reçoit la combinaison logique (Y1Y0) venant d'un générateur de vecteurs de test

De la même manière, la dynamisation de la branche horizontale constituant la base de ce contrôleur sera effectuée en appliquant la paire (X1X0) d'un générateur de vecteurs de test sur la première cellule double-rail.

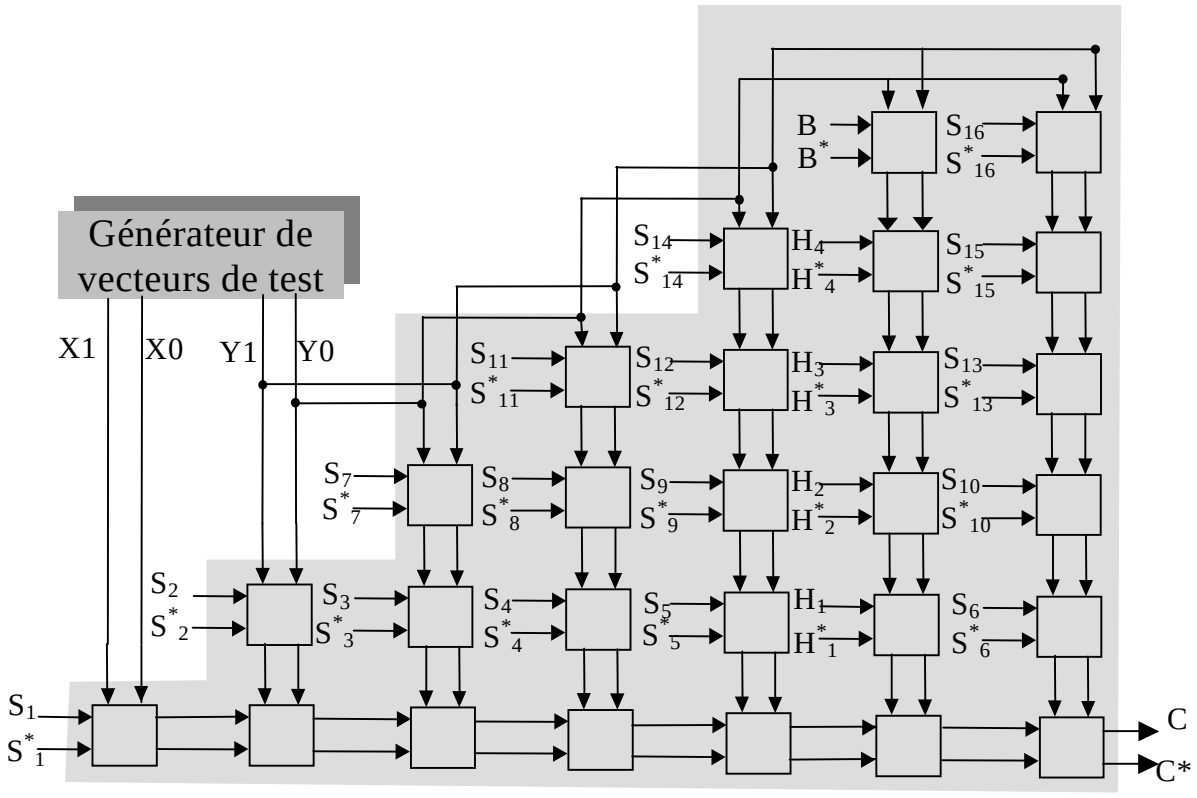


Fig. (19) : Le contrôleur double rail

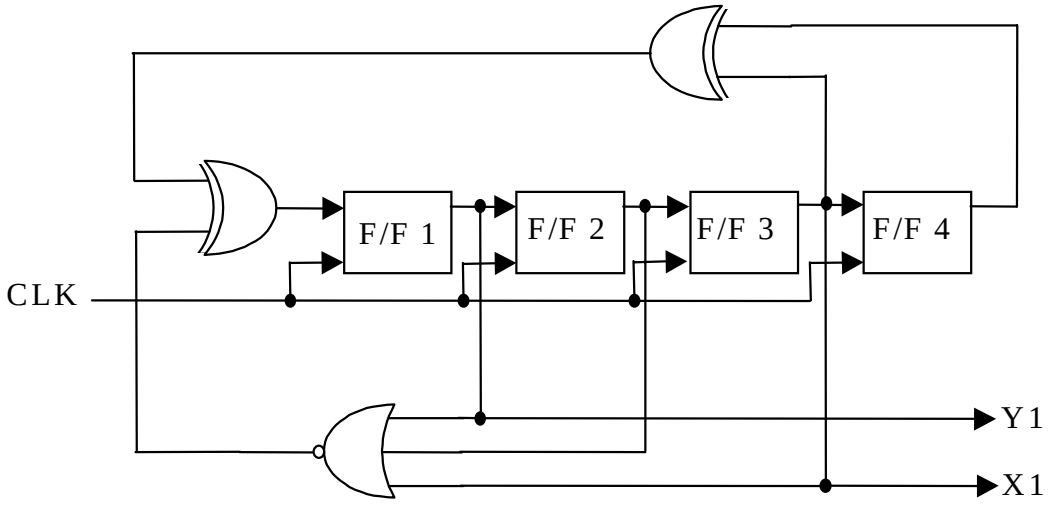


Fig. (20) : Le générateur de vecteurs de test

La réalisation du générateur de vecteurs de test est faite de la manière de LFSR comme montré dans la figure (20). Ce circuit génère les signaux XI, Y1. La duplication de ce

circuit en prenant les sorties inversées des bascules (F/F 1 et F/F 3) on peut obtenir les signaux X0, Y0. Le circuit comprenant les deux LFSR permet de générer toutes les combinaisons possibles d'un couple de signaux.

Finalement, la dynamisation du contrôleur présentée au-dessus assure également la dynamisation des différents circuits de la partie logique tels que le convertisseur double-rail à fréquence et l'indicateur d'erreur

Une dernière partie de cette chaîne qui reste à dynamisée est la partie de conversion des niveaux de puissance (sorties Oi) en niveaux logiques. Comme précisé dans la section 4.1, le niveau haut des sorties (24 volts) doit être transformé en '1' logique et le niveau bas (0 volt), doit être transformé en '0' logique. Il est donc tout d'abord nécessaire de déterminer le seuil de tension SNNS qui sépare le niveau logique « 0 » de celui de « 1 ». De cette façon, toutes les valeurs des tensions au-delà de ce seuil génèrent l'état non sûr en sortie, et toutes les valeurs des tensions de sortie qui sont inférieurs à ce seuil présentent l'état sûr en sortie. Ce seuil a été fixé par l'INRETS à 0.7 V.

La transformation du signal de puissance à la sortie en niveau logique s'effectue par l'intermédiaire d'une résistance de forte valeur R (la résistance de mesure) introduite en série avec le transistor de puissance, ainsi que d'un comparateur du courant Comp. Cependant, la résistance de mesure permet de transformer la tension à la sortie O_i en courant I_{test}, alors que le comparateur du courant convertit le courant I_{test} en signal logique, en utilisant un courant de référence I_{ref} (où la valeur de ce courant est égal à la tension du seuil SNNS divisée par la valeur de résistance de mesure). Dans ce cas, lorsque la valeur du courant I_{test} est inférieure à celle du I_{ref} (état sûr où la tension de sortie O_i est inférieure au seuil SNNS), un signal de « 0 » logique apparaît sur la sortie du comparateur. Dés que la valeur du courant I_{test} est supérieure à celle du I_{ref} (état non sûr où la tension de sortie O_i est supérieure au seuil SNNS), la sortie du comparateur s'affiche le « 1 » logique.

En cas du fonctionnement normal du circuit, lorsque l'entrée est mise au niveau « 1 » logique, la sortie O_i sera en état non sûr**.** D'autre part, lorsque l'entrée est mise au niveau « 0 » logique, la sortie O_i devrait être en état sûr. Mais à cause d'une défaillance quelconque dans le circuit, rien n'empêche la sortie de se mettre à un niveau supérieur au seuil SNNS, en déclenchant l'état non sûr. Dans ce cas, la sécurité sera assurée par l'intermédiaire du

convertisseur de niveau puissance/basse tension, qui produira une valeur différente de la valeur d'entrée. La détection de cette différence par le contrôleur double-rail aura comme conséquence la coupure de l'alimentation de l'interface, qui ramènera ses sorties à l'état sûr. Il est évident que le convertisseur joue un rôle crucial dans cette chaîne de sécurité. S'il est défaillant, il risque de ne pas détecter la valeur erronée non sûre sur la sortie O_i. on utilisera alors un test périodique pour vérifier son bon fonctionnement**.**

La solution proposée pour dynamiser le convertisseur puissance/basse tension, et pour détecter toute augmentation anormal de la tension de O_i au delà du seuil SNNS est montrée dans la figure (21). Dans cette figure, la résistance de mesure R est réalisée par deux résistances R_1 et R_2 ($R=R_1+R_2$), connectées en série. Les trois générateurs des courants connectés en parallèle fournissent les courants I_{in1}, I_{in2}, I_{in3}. Ces courant seront injectés sur le nœud M qui connecte R_1 et R_2.

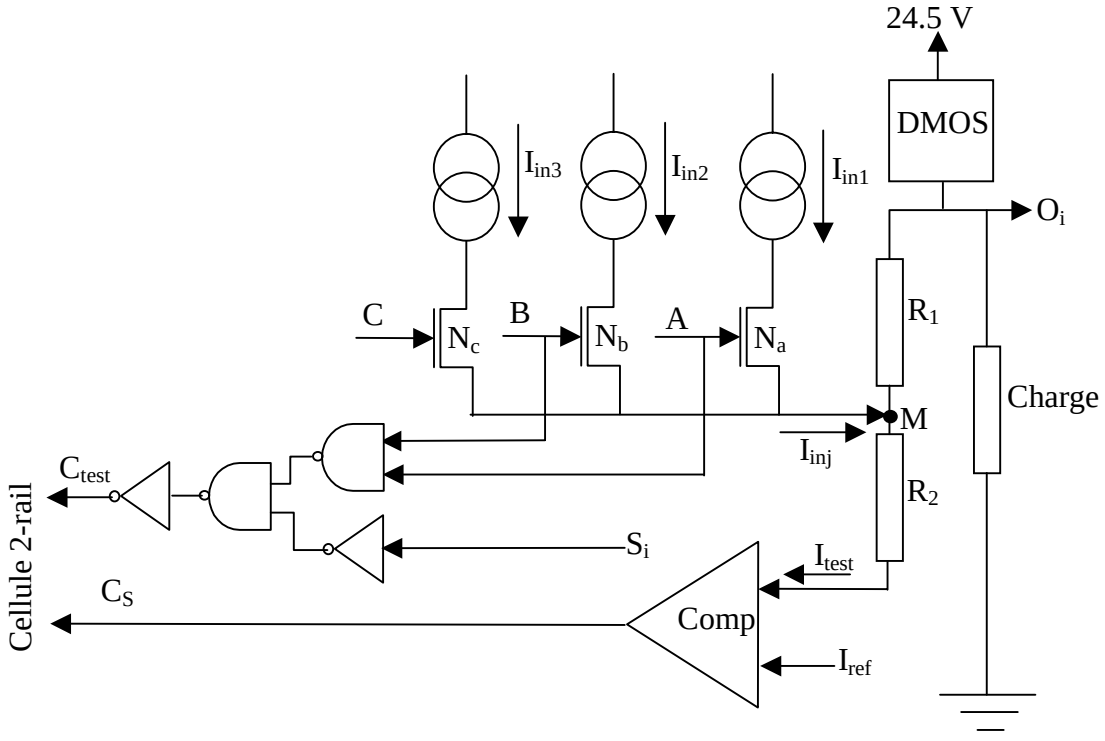


Fig. (21) : Dynamisation du convertisseur H.L. to L.L.

L'injection des courants fournis par les générateurs du courant est contrôlée par les signaux A, B, C, qui contrôlent respectivement les interrupteurs N_a, N_b, N_c.

On effectue le test quand S_i est 0. Le courant injecté au point M (I_{inj}) sera divisé en deux courants. Le premier passe par la résistance R_2, constituant le courant I_{test}. Le deuxième courant I_{R1} va passer par la résistance R_1, et la résistance de la charge (les deux résistances sont connectées en série entre le point M et la masse). Les équations suivantes déterminent les deux courants :

$$I_{test}=I_{inj}\frac{R_1+R_{charge}}{R_1+R_2+R_{comp}+R_{charge}}\approx I_{inj}\frac{R_1}{R_1+R_2} \quad \text{.....(1)}$$

$$I_{R_1}=I_{inj}\frac{R_2}{R_1+R_2+R_{comp}+R_{charge}}\approx I_{inj}\frac{R_2}{R_1+R_2} \quad \text{.....(2)}$$

Nous avons utilisé une valeur très élevée pour la résistance R (R_1 = 10 KΩ, R_2 = 15 KΩ). Dans ce cas les termes R_{comp} et R_{charge} peuvent être ignorés, comme dans les équations (1) et (2).

On choisie des valeurs de R_1, I_{in1}, I_{in2}, et I_{in3} telles que $I_{in1}*R_1$ = 0.4 volts, et $I_{in2}*R1= I_{in3}*R_1$ = 0.2 volts. Ainsi quant on injecte le courant I_{in1} + I_{in2} +I_{in3}, on a $I_{test}=\frac{0.8Volts}{R_1+R_2}$. Ceci est 15% supérieur au courant de seuil de comparateur ($\frac{0.7Volts}{R_1+R_2}$), qui correspond au seuil de l'état non-sûr sur la sortie O_i (0.7 volts). D'autre part, quand on injecte le courant I_{in1} + I_{in2} ou I_{in1} + I_{in3}, le courant $I_{test}=\frac{0.6Volts}{R_1+R_2}$. Ceci est 15% inférieur du seuil du comparateur.

La valeur du courant I_{inj}, et par conséquent du courant I_{test}, dépend des valeurs appliquées sur les nœuds A, B et C.

- Lorsque A = 0, B = 0, C = 0, les interrupteurs sont bloqués, aucun courant n'est injecté au point M. Donc le courant I_{test} est égal à 0.

- Lorsque A = 1, B = 1, C = 0 ou A = 1, B = 0, C = 1, la valeur du courant injectée au point M est égal à I_{in1} + I_{in2} = I_{in1} + I_{in3} , et le courant I_{test} est $\frac{0.6}{R_1+R_2}$.

- Lorsque A = 1, B = 1, C = 1, la valeur du courant injectée au point M est égal à I_{in1} + I_{in2} + I_{in3}, et le courant I_{test} est $\frac{1}{R_1+R_2}$.

D'une telle façon, nous pouvons dynamiser le comparateur du courant, et la résistance de mesure, ainsi que les générateurs des courants eux-même.

8.1 LA COUVERTURE DES FAUTES :

Nous avons vu que la dynamisation de cette partie est faite pendant la période de stabilité des entrées. Dans ce cas, la sortie C_{test} est décrite par l'équation logique suivante :

$$C_{test} = (S_i)^*.(A.B)^*$$

Dans le cas du fonctionnement sans faute, le tableau ci-dessus décrit les cas possibles pour les signaux A, B et C ainsi que pour les entrées S_i afin de dynamiser l'ensemble des éléments constituant ce circuit

	S_i	A	B	C	I_{test}, I_{ref}	C_{test}	C_s	Etat de fonctionnement
1	0	0	0	0	$I_{test}= (0) < I_{ref}$	1	0	Correcte
2	0	1	1	0	$I_{test} = 0.6\ V/(R_1+R_2) < I_{ref}$	1	0	Correcte
3	0	1	0	1	$I_{test} = 0.6\ V/(R_1+R_2) < I_{ref}$	1	0	Correcte
4	0	1	1	1	$I_{test} = 0.8\ V/(R_1+R_2) > I_{ref}$	0	1	Correcte
5	1	×	×	×	$I_{test} > I_{ref}$	0	1	Correcte

Fig. (22) : Tableau de dynamisation

Les cas de 2 à 4 détecteront les défaillances dans les générateurs de courants, dans la résistance R ($R = R_1 + R_2$), et dans le comparateur du courant, comme dans la suite :

- les défaillances dans un des générateurs des courants:

les fautes augmentant le courant I_{in1}, I_{in2}, I_{in3} seront détectées par les cas numéro 2 et 3. La faute est détectée si elle augmente le courant $I_{in1} + I_{in2}$ ou $I_{in1} + I_{in3}$ de plus de 15%. Dans les deux cas, le courant I_{test} sera supérieur au courant I_{ref}. Alors la sortie C_s prend la valeur 1 logique, tandis que la sortie C_{test} prend une valeur de 1 logique (A = 1, B = 0 ou A = 0, et B = 1) ; la cellule double-rail détecte cette erreur. Cette détection est importante car elle garantit que le courant $I_{in1} + I_{in2} + I_{in3}$ utilisé dans le test 3 ne devient pas trop grand par rapport au seuil $I_{ref.}$ D'autre part, le test 3 teste les fautes qui auront pour conséquence la diminution des courants. Néanmoins le teste de dynamisation des courants n'est pas important du point de vue sécurité.

- les défaillances dans la résistance de mesure :

Les tests 2, 3 et 4 vérifient aussi les modifications des résistances R_1, et R_2. Du point de vue sécurité, il est important de vérifier que R_1 et R_2 n'ont pas augmenté leurs valeurs de façon significative, car elles pourront empêcher le convertisseur de voir une valeur sur O_i dépassant le seuil. Les tests 2 et 3 vérifient si la résistance R_2 a diminué sa valeur ou la résistance R_1 l'a augmenté. Le test 4 vérifie si la résistance R_2 a augmenté sa valeur ou la résistance R_1 l'a diminué.

- les défaillances dans le comparateur :

les tests 2, 3 et 4 vérifient si le comparateur de seuil est capable de produire le niveau 1 à sa sortie quand son entrée dépasse le seuil (ceci est vérifié par le test 4) et s'il est capable de produire le niveau 0 à sa sortie quand son entrée est inférieure au seuil.

Du point de vue sécurité, le premier test est le seul qui est important, car il permettra de vérifier si le comparateur du seuil va fonctionner correctement dans le cas de la situation dangereuse où l'état non-sûr est présenté de façon erronée sur la sortie O_i.

9 LAYOUT GLOBAL ET CONCLUSIONS

En plaçant le layout final de différents blocs présentés auparavant et en les interconnectant, nous avons obtenu le layout global du circuit montré dans la figure 23. La surface occupée par ce circuit est faible ($13.31mm^2$. Il s'agit donc à une solution très économique qui implémente dans un seul circuit les composants de sécurité ainsi que des composants de puissance. Elle remplace ainsi des parties réalisées auparavant par des composants discrets, qui sont très volumineux, coûteux et ont une disponibilité très inférieure d'un circuit intégré. Par ces qualités, l'interface que nous avons conçu devient intéressant pas seulement pour des applications ferroviaires mais aussi pour des applications de sécurité à grand volume de production, telles que les fonctions critiques en sécurité les automobiles pour lesquelles la sécurité doit être assurée par des composants à faible coût.

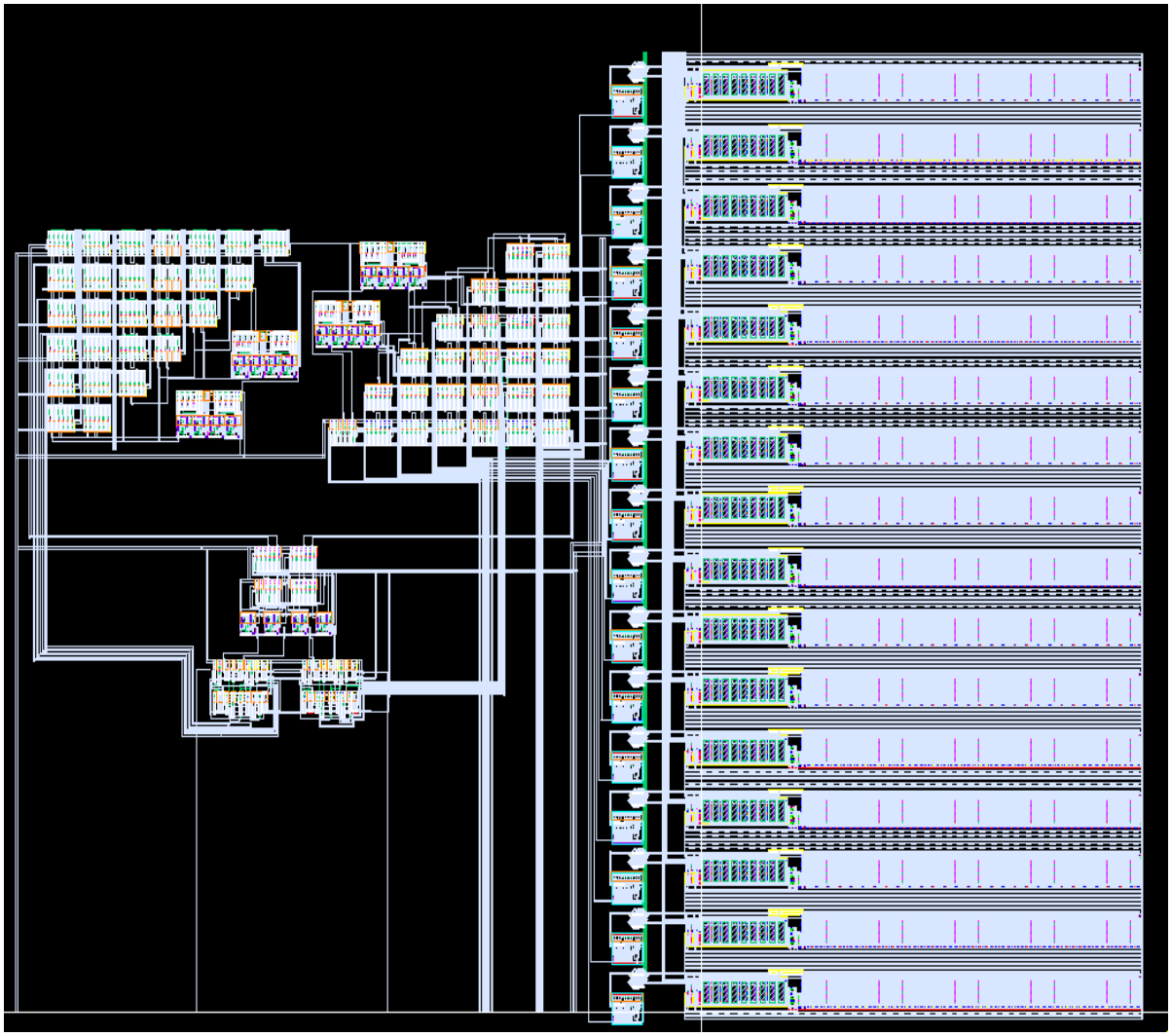


Fig. (23) : Le layout complet du circuit ISIS

CONCLUSION GENERALE

Dans cette mémoire, nous avons conçu dans une technologie « Smart Power » une interface sécurisée basée sur une théorie proposée et développée au sein de l'équipe RIS au laboratoire TIMA. Cette théorie permet l'intégration d'une interface appelée « Fail-Safe » dont les sorties sont soit sûres soit correctes. La conception d'un tel circuit est reposée sur deux concepts de base telles que la propriété d'auto contrôle et la propriété de *strongly Fail-Safe.*

Pour chaque sortie de l'interface, l'état non-sûr est représenté par la présence d'un état de puissance. Tout autre état en sortie est considéré comme sûr. L'interface transforme des signaux binaires de type 0 volts, 5 volts en signaux de puissance. Les signaux binaires sont générés par un système dupliqué, et sont codés dans le code double-rail. Si l'interface est affectée par une faute ou si les signaux binaires ne sont pas codés en double-rail, l'interface fournie des sorties qui sont soit correctes soit sûres (propriété *fail-safe*). De plus, l'interface est conçue en utilisant des circuits autocontrôlables qui permettent de détecter les fautes et assurer la propriété *strongly fail-saife*. Un intérêt majeur de ces interfaces est lié au fait qu'elles peuvent être implémentées en VLSI, évitant ainsi la complexité, l'encombrement et les coûts des interfaces conventionnelles réalisés en composants discrets.

L'architecture de l'interface assure la détection en-ligne des fautes logiques aux entrées et aux nœuds internes du circuit. Une telle détection coupe l'alimentation du circuit et bloque les sorties à l'état sûr de façon irréversible. Cependant, les défaillances produisant des niveaux logiques indéterminés, pourraient échapper à la détection et se combiner avec des défaillances survenant plus tard, pour conduire le circuit à un état dangereux. Pour éviter cette situation, nous avons conçu des cellules. Ces cellules ont été dimensionnées de façon à augmenter la force du niveau logique « 0 » qui s'impose en cas d'un court-circuit ou d'une faute de stuck-on. On évite ainsi l'occurrence des niveaux indéterminés. De plus, ces nouvelles cellules utilisent une connexion indépendante de la source. Ainsi, elles permettent l'utilisation d'une alternative supplémentaire afin de renforcer la sécurité. Cette alternative se repose sur l'utilisation d'un test par mesure de courant statique, en associant un circuit de BICS par chaîne de surveillance. De cette façon, nous pouvons, en phase de stabilité des entrées, mesurer le courant de fuite venant de chaque chaîne de surveillance et détecter ainsi, en cas de défaillance quelconque, l'augmentation anormale du courant de fuite.

Les technologies de puissance intelligentes récemment développées par plusieurs fabricants de semi-conducteurs nous ont permit d'intégrer aisément les différents bloques logiques de cette interface ainsi que les commutateurs de puissance et leurs circuits de commandes. Ceci est fait pour une gamme étendue d'applications dans les domaines du transport ferroviaire.

L'objectif final de ces implémentations est d'assurer un niveau élevé de protection pour une application donnée, ce qui signifie que le système ne fournit pas des sorties erronées non sûres tout au long de sa durée de service.

BIBLIOGRAPHIE

[1] D. BIED-CHARRETON, “Sécurité intrinsèque et sécurité probabiliste dans les transports terrestres » . Synthèse INRETS N° 31, Novembre 1998.

[2] P. FORIN « Une nouvelle génération du processeur codé ». Revue générale des Chemins de Fer, Juin 1996.

[3] M. NICOLAIDIS “Fail-Safe Interface for VLSI : Theoretical Foundations and Implementations”, IEEE Transactions on Computers, Vol. C-14, N° 1, January 1998, pp. 62-77.

[4] R. DAVID, P. THEVENOD-FOSSE “Design of totally self-checking asynchronous modular circuits”, J. Des. Automat. Fault Tol. Comput. Vol. 2, N° 4, October 1978, pp 271-287.

[5] J. VIAUD, R. DAVID, “Sequentially self-checking circuit”, The 10th International Symposium on Fault-Tolerant Computing, Kyoto, October 1-3, 1980, Digest of papers. New York, IEEE, 1980, PP 263-268.

[6] M. NICOLAÏDIS, I. JANSCH, B. COUTROIS, « Strongly code disjoint checkers » The 14th International Symposium on Fault-Tolerant Computing, Kissimmee, June 20-22, 1984, Digest of papers. New York, IEEE, 1984, PP 16-21, IEEE Trans. on Comp. June 1988

[7] W. CARTER, P. SCHNEIDER “design of dynamically checked computer”, IFIP Congress, Edinburgh, 1968, Information Processing ’68, Amsterdam, North Holland, 1969. Vol. 2, pp. 878-883.

[8] N. GAITANIS “A totally self checking error indicator”, IEEE Transactions on Computers, Vol. C-34, N° 8, pp. 753-761, August 1985.

[9] T. NANYA, T. KAWAMURA “On error indication foe totally self checking systems”, IEEE Transactions on Computers, Vol. C36, N° 1, pp.1389-1392, Novembre 1987.

[10] J-L. LO, J. C. DALY, M. NICOLAIDIS, “Design of Static CMOS Celf Checking Circuits Using Built-In Current Sensing”, In Proc. IEEE International Symposium on Fault Tolerant Computing, Boston, AM, July 8-10, 1992.

[11] C. L. HENDERSON, J. M. SODEN, C. F. HAWKINS, “The behavior and Testing Implications of CMOS IC Logic Gate Open Circuits“, Proc. of International Test Conference, 1991.

[12] T. M. STOREN, W. MALY, “CMOS Bridging Fault Detection”, Proc. of International Test Conference, 1990.

[13] W. MALY, F. J. FERGUSON, J. P. SHEN, “Systematic Characterization of Physical Defects for Fault Analysis of CMOS IC Cells”, Proc. of International Test Conference, 1984.

[14] R. RODRIGUEZ-MONTANES, E.M. BRULS, J. FIGUERAS, « Bridging Defects Resistance Measurements in a CMOS Process », Proc. of International Test Conference, pp. 892-899,October 1992,.

[15] R. RODRIGUEZ-MONTANES, J. A. SEGURA, V. H. CHAMPAC, J. FIGUERAS, J. A. RUBIO, « Bridging Faults in CMOS : Possibilities of Current Testing », Proc. Of European Solid-Stats Circuits Conference, 1990.

[16] F. L. VARGAS, M. NICOLAIDIS, B. HAMDI, “Quiescent Current Estimation Based on Quality Requirements”, IEEE Comput. Soc. Press, Los Alamitos, CA, USA; 1993.

[17] A. ANDREINI, C. CONTIERO, and P. GALBIATI « A New Integrated Silicon Gate Technology Combining Bipolar Linear, CMOS logic, and DMOS Power Parts » IEEE Trans. Electron Devices, Vol. ED-33, pp. 2025-2030, Décembre 1986.

[18] S. KRISHAN, J. KUO, and I.S. GAETA “An Analog Technology Integrates Bipolar, CMOS, and High-Voltage DMOS Transistors” IEEE Trans. Electron Devices, Vol. ED-31, pp. 89-95, Jan. 1984.

[19] C. CONTERO, P. GALBIATI, A. ANDREINI. European Patent Application, 0267882, date de publication 18.05.1988.

[20] R. ZEMBRANO, “Isolation Technique in Power IC’s with Vertical Current Flow” ESSDERC, 1987, pp.653-656.

[21] P. GIVELIN, “Bibliothèque Compatible CMOS/DMOS de Fonctions de Commande et de Protection Pour les Applications Automobiles de Puissance Intelligente », Thèse de 3ème cycle, INSAT (Institut National des Sciences Appliques de Toulouse), 1994.

[22] C. LU et al., « An analog/digital BCDMOS technologique with dielectric isolation-devices and processes », IEEE Trans. Electron Devices, Vol. 35, N° 2, Février 1988, pp. 230-

237.

[23] B. MURARI, « La puissance intégrée n'a pas dit son dernier mot », Electronique, N° 23, Décembre 1992, pp. 26-28.

[24] N. AZZOUZ, « Composant LDMOS pour Circuits Intégrés Haute tension », Thèse de doctorat de l'université de Paul Sabatier (Toulouse), Juin 1989.

[25] M.A. BOUANANE, « Conception et Optimisation des Composants DMOS Latéraux Haute Tension en Technologie Resurf », Thèse de doctorat de l'université de Paul Sabatier (Toulouse), Décembre 1992.

[26] Ingénieur de l'automobile, numéro spécial, juin 1986, pp. 91-108.

[27] M. BAHLEUR, J. BUXO, Ph. GIVELIN, M. PUIG VIDAL, V. MACARY, G. SARRABAYROUSE, "Application of a floating well concept to a latch-up free, low cost, smart power high-side switch technology", IEEE J. of Solid State Circuits, Vol. 40, N° 7, July 1993, pp. 1340-1342.

[28] M.PUIG VIDAL, "Immunité au latch-up d'une technologie de puissance intelligente CMOS/DMOS basée sur un concept de puit flottant », Thèse de Doctorat de l'université Paul Sabatier (Toulouse), Février 1993.

[29] T. EFLAND, « Lateral DMOS Structure Development for Advanced Power Technologies », Texas Insruments Technical Joural, Vol. 11, N° 2, pp. 10-23, Mars- Avril 1994.

[30] J.L. SANCHEZ, « Propriétés à l'Etat Passant des Transistors DMOS de puissance Coplanaires et Verticaux », Thèse de 3ème cycle, INSAT, 1984.

[31] W. WILLS, « Get high voltag with low-cost multipler », Electronic design, N° 13, 21 Juin 1974, pp.64-68.

[32] J.F. DICKSON, "On-chip high-voltage generation in MNOS integrated circuits using an improved voltage multiplier technique", IEEE J. Solid-State Circuits, Vol. 11, N° 3, Juin 1976, pp. 374-378.

[33] W.C. DUNN, "Driving and protection of high side NMOS power switches", IEEE Trans. Industry Applications, Vol. 28, N°1, Janvier/Février 1992, pp. 26-30.

[34] W.L. MARTINO et al., "An on-chip back-bias generator for MOS dynamic memory",

IEEE J. Solid-state Circuits, Vol. 15, N° 5, Octobre 1980, pp. 820-825.

[35] A. GUPTA, T. CHIU, M. CHANGE, A. RENNINGER et G. PERLEGOS, « A 5V-only 16K EEPROM utilizing oxynitride dielectrics and EPROM redundancy », Proc. ISCCC Février 1982, pp. 184-185.

[36] M. BAFLEUR, Ph. GIVELIN, M. PUIG VIDAL, J. BUXO, et V. MACARY, "Cost-effective Smart Power CMOS/DMOS technology: Design of Main Driving and protection functions", Analog Integrated Circuits and Signal Processing 8(3), pp. 233-246 1995.

[37] R.D. RUNG et H. MOMOSE, "DC holding and dynamic triggering characteristics of bulk CMOS latch-up", IEEE Trans. Electron Devices, Vol. 30, N° 12, Décembre 1983, pp. 1647-1655.

[38] Austria Mikro Systeme Inernational AG « 0.8 µm HV CMOS Process Parameters », June 1999.

[39] M. NICOLAIDIS, N. ZAIDAN, T. CALIN, D. BIED CHARRETON " ISIS : A Fail-Safe Interface Realised in Smart Power Technology " 6th IEEE International On-Line Testing Workshop, July 2000, Palma de Mallorca, Spain,

[40] G. CHAUMONTET " Etude de Faisabilité d'un Microcontrôleur de très Hautes Sécurité " Thèse Doctorat, Institut Polytechnique de Grenoble, octobre 1990.

[41] J. MARTIN, C. GALIVEL " Le Processeur Codé: Un Nouveau Concept Appliqué à la Sécurité des Systèmes de Transport ", Revue Générale des Chemins de Fer, Juin 1990.

[42] M. NICOLAIDIS " Finitely Self-Checking Circuits and their Application on Current Sensors " 11th IEEE VLSI Test Symposium, April 1993, Atlantic City, USA".

[43] M. NICOLAIDIS, F. VARGAS, B. COURTOIS " Design of Built-In Current Sensors for Concurrent Checking in Radiation Environments " IEEE Transactions on Nuclear Science, December 1993.

[44] M. NICOLAIDIS "Fault Secure Property Versus Strongly Code Disjoint Checkers" IEEE Transactions on Computer-Aided Design, Vol. 13, No 5, pp. 651-658, May 1994.

Résumé :

Chaque actionneur d'un système sécuritaire doit être contrôlé par un signal sûr en présence de défaillances (fail-safe), c'est à dire que en cas de défaillance son état est soit correct, soit sûr. Les systèmes intégrés auto contrôlables en ligne (self-checking) fournissent des groupes de signaux codés en sortie. Ces groupes de signaux ne permettent pas d'assurer le contrôle direct des actionneurs, car chaque actionneur est contrôlé par un seul signal qui doit être individuellement sûr. A cause de cette exigence particulière, il n'était pas possible d'implémenter en VLSI toutes les parties d'un système sécuritaire. En fait, tous les systèmes sécuritaires existants sont divisés en deux parties : un système auto contrôlé (self-checking) ou tolérant aux pannes (qui utilise par exemple un code détecteur d'erreur, une technique de duplication, triplication ou un processeur codé), et une interface fail-safe utilisant des composants discrets. Cette interface transforme les sorties du système de traitement en signaux fail-safe. Outre l'inconvénient des interfaces à composants discrets d'être très encombrantes et coûteuses, la probabilité de défaillance est augmentée et la durée de vie (MTTF) du système est diminuée dans ce cas par rapport à l'implémentation VLSI, ce qui limite la disponibilité du système. Il est donc intéressant d'intégrer en VLSI les interfaces fail-safe, capables d'assurer le contrôle sécuritaire des actionneurs.

Dans cette mémoire, nous présentons une interface sécurisée de puissance réalisée en technologie de puissance intelligente. Cette interface transforme les signaux de contrôles codés en fréquence en signaux de puissance pour le contrôle sécuritaire des actionneurs dans les transports ferroviaires. Elle repose sur l'utilisation du concept de fail-safe, et d'autocontrolable pour atteindre un haut niveau de sécurité.

Mots clès : Fail-safe, Auto contrôlable, Capteur de courant intégré (BICS), Puissance intelligente.

Abstract:

Each actuator of a fail-safe system must be controlled by a fail-safe signal, (i. e. a signal which in presence of failures is either correct or safe). Self-checking systems deliver groups of encoded signals and are not adequate for driving these actuators (since each actuator is controlled by a single signal, which must be fail-safe individually). Due to this particular requirement it was not possible to implement fail-safe systems in VLSI. Therefore all existing fail-safe systems are composed of a self-checking or fault tolerant processing system (e. g. using error detection codes, duplication, triplication etc.), and of a fail-safe interface implemented using discrete components. This interface transforms the outputs of the processing system into fail-safe signals. The drawback of these interfaces is that they are very cumbersome and have a high cost. Furthermore using discrete components results in lower MTTF with respect to VLSI implementations, so that the system availability is reduced. It is therefore mandatory to implement fail-safe interfaces in VLSI.

The present work describes a fail-safe interface realised in a smart power technology. It transforms the groups of encoded signals into high-level power signals for driving thus actuators. It combines fail-safe concepts, self-checking design and current monitoring to achieve high levels of safety.

Key words: Fail-safe, Self-checking, Built-In Current Sensor (BICS), Smart power.

ISBN : 2-913329-73-X Format électronique

ISBN : 2-913329-72-1 Broché