Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mouloud MAMMERI
Faculté du Génie Electrique et de l'Informatique
Département d'Electronique

Mémoire de fin d'études

Présenté en vue de l'obtention du diplôme
d'Ingénieur d'Etat en Electronique
Option : Communication

Thème

Etude de la compatibilité électromagnétique des circuits intégrés

Proposé et dirigé par :
Mr. H. KANANE

Etudié par :
Mr. Mohand Said KHENNOUCHE
M^elle^ Dehbia HABAREK

Année universitaire 2008/2009

Remerciements :

Nous souhaitons témoigner toute notre reconnaissance à notre encadrant, Mr. ***Hocine Kanane*** *pour le soutien et les conseils qu'il nous a apportés durant tout notre parcours. Pour cela, nous voudrions lui adresser de chaleureux remerciements pour la confiance qu'il nous a accordée mais aussi pour son enthousiasme, sa joie de vivre et la manière unique avec laquelle il a su encadrer notre travail. Nous le remercions enfin pour l'effort de correction qu'il a apporté à ce mémoire.*

Nous remercions également les membres de jury qui nous feront l'effort de juger et de critiquer notre modeste contribution afin de l'améliorer davantage.

Dédicaces :

Je dédie ce mémoire à ma mère, décédée, qui pendant toute sa vie, se sacrifiait pour me rendre la vie plus facile. Elle m'a accordé une confiance infaillible et m'a appris à affronter la vie. Sans ses efforts, ce travail n'aurait certainement pas pu se faire avec moi. Je la remercie pour toute la fierté qu'elle exprimait à chaque étape de ma vie qui s'achevait par un succès aussi modeste pouvait-il être. Pour toutes ces raisons et d'autres que je ne pourrai dénombrer, je ne la remercierais jamais assez.

Je remercie, en deuxième lieu, ma camarade de travail et amie, Dehbia, pour sa patience et ses efforts. Je ressentais vraiment qu'elle se surpassait. Pendant toute la durée de notre travail, elle faisait passer notre intérêt commun avant le sien. Je n'oublierai jamais son dévouement.

Je souhaite remercier également mes amis qui m'ont aidé à donner le meilleur de ce que j'avais à offrir. Je remercie notamment Karim, Malik, Aghilas, El Hadi et Mourad pour leur soutien et leur fidélité.

Said

Dédicaces :

Je dédie ce mémoire à toutes les personnes qui me sont proches et que j'aime :

- *Mes très chers parents*
- *Ma grande sœur Djouher, son mari Omar et leur fille Lisa*
- *Mon frère SAID*
- *Ma petite sœur Doudouche*
- *A mon camarade SAID*
- *Ma grand-mère maternelle*
- *Mes oncles et tentes maternelles*
- *Mes copines de chambre à la cité universitaire :Djouher, Safia et Ferial*

Dehbia

SOMMAIRE

Chapitre II : Evolution historique de la CEM des circuits intégrés et de leur conception :

Chapitre III : Solutions générales pour améliorer la CEM des circuits intégrés

Chapitre IV : Amélioration de l'immunité des circuits intégrés par des logiciels défensifs

Chapitre V : Réduction des émissions des circuits intégrés numériques en utilisant la version asynchrone

Introduction générale :

Les puces microélectroniques sont, de nos jours, présentes partout autour de nous : téléphone mobile, ordinateur, lecteur mp3, etc. On les retrouve également dans des domaines touchant directement à notre sécurité : automobile, aviation, médecine ...

Du fait de sa fiabilité et de l'économie en matières premières et donc d'argent, qu'elle assure par une intégration de plus en plus poussée, la microélectronique a gagné en intérêt et est devenue indispensable à l'apparition de toute nouvelle technologie.
Cependant, même si cette miniaturisation en évolution était nécessaire pour construire des systèmes qui n'auraient jamais pu exister autrement, elle a posé de nouveaux problèmes. En effet, la construction de circuits de plus en plus denses faisant rapprocher proportionnellement les différents blocs les constituant, favorise les couplages parasites. Ces nouveaux circuits devenaient donc de plus en plus vulnérables.

Avec des circuits intégrés de plus en plus « fragiles », l'utilisation de plus en plus intensives des ondes électromagnétiques (radars militaires ou civils, de nouveaux réseaux de télécommunications sans fil tels que le GSM ou l'UMTS, etc.) a accentué le problème d'autant. D'un autre côté, l'évolution de la microélectronique a permis la construction de circuits intégrés numériques de plus en plus rapides. Mais des commutations plus rapides signifient plus d'émission parasite.

En résumé, les nouveaux circuits intégrés sont plus fragiles ou plus susceptibles et rayonnent plus. Ils sont plus vulnérables à leur environnement extérieur et nuisent plus aux circuits environnants. Tous ces problèmes ont induit inévitablement à un intérêt extraordinaire pour la compatibilité électromagnétique, qui traite justement ces deux problèmes. De ce fait, une étude préalable de la compatibilité électromagnétique de tout nouveau produit (nouveau circuit) est devenue indispensable. Plus loin encore, elle est même devenue une condition imposée par tous les gouvernements sur les entreprises spécialisées, par l'intermédiaire d'une législation adéquate. La compatibilité électromagnétique est devenue un véritable gage de sécurité dans des domaines aussi critiques que l'aéronautique ou l'automobile, où un dysfonctionnement pourrait entrainer la perte de plusieurs vies humaines.

Le problème de compatibilité électromagnétique des circuits est particulièrement difficile, puisque ceux-ci sont en évolution rapide. En outre, les nouveaux circuits intégrés imposent de nouvelles contraintes, donc les normes de leur compatibilité doivent également évoluer. Cependant, avec des tailles plus petites qu'un micron, les contraintes actuelles sont très difficiles à satisfaire et celles du futur sont encore plus difficiles à satisfaire.

Dans ce mémoire, nous essayons d'apporter des solutions qui permettent d'augmenter l'immunité des circuits intégrés et de réduire leur émission parasite.

Notre étude sera divisée en cinq chapitres :

- Dans le premier chapitre, nous introduisons les notions de base nécessaires à la compréhension des problèmes rencontrés en compatibilité électromagnétique des circuits intégrés.

- Dans le second chapitre, nous évoquons l'évolution historique de la compatibilité électromagnétique des circuits intégrés et l'état de l'art de leur conception.

- Dans le troisième chapitre, nous proposons des solutions d'ordre général, pouvant soit réduire l'émission parasite des circuits intégrés, soit améliorer leur résistance face aux perturbations extérieures.

- Le quatrième chapitre traite des méthodes logicielles pouvant être appliquées aux microcontrôleurs ou microprocesseurs afin de rendre les systèmes les utilisant plus immunisés aux interférences extérieures.

- Le dernier chapitre évoque la possibilité de remplacer des circuits numériques synchrones par des circuits numériques asynchrones. Ces derniers étant moins perturbateurs mais moins connus, leur architecture est évoquée afin de les faire mieux connaître.

Chapitre I :

Problèmes de la compatibilité électromagnétique des circuits intégrés

Introduction :

Aujourd'hui, plus que jamais, les concepteurs des circuits intégrés sont confrontés à des défis de plus en plus importants. Leur principal défi est de rendre ces circuits intégrés compatibles, du point de vue électromagnétique. Il s'agit, d'une part, de les faire fonctionner correctement dans un environnement pollué par des ondes électromagnétiques ; et d'autre part, de tenir compte et de diminuer les perturbations électromagnétiques qu'ils génèrent, cette fois-ci, eux-mêmes. Ce problème se trouve accentué par la multiplication des sources de perturbation avec l'évolution technologique. En effet, les radars ne sont plus utilisés que dans les applications militaires ou dans le trafic aérien uniquement, il est, à présent, utilisé même dans le trafic routier. Les réseaux sans fils se multiplient, ce qui a pour conséquence, une occupation plus importante du spectre de fréquence. D'un autre côté, des phénomènes naturels sont plus dangereux, telles que la foudre, qui a une attention particulière de l'industrie aéronautique. Tous les problèmes évoqués et d'autres auxquels on ajoute le fait de l'obligation d'une miniaturisation de plus en plus importante, rendent le problème de la compatibilité électromagnétique des circuits intégrés particulièrement complexe. Avec une miniaturisation extrême, il y a rapprochement plus important entre les différentes composantes du circuit ce qui augmente l'importance des couplages parasites entre celles-ci. En résumé, pour qu'un circuit intégré fonctionne, il faut diminuer les couplages entre ses blocs internes, et entre lui-même et d'autres sources externes naturelles ou d'origine humaine.

Vu les applications dans lesquelles les circuits intégrés jouent un rôle prépondérant, les enjeux étaient si importants que la compatibilité électromagnétique des circuits intégrés s'est dotée de normes.

1) Définitions préliminaires relatives à la compatibilité électromagnétique :

1-1) Définition de la compatibilité électromagnétique :

La compatibilité électromagnétique d'un circuit intégré signifie l'aptitude d'un dispositif, d'un appareil ou d'un système à conserver sa fonction dans un environnement électromagnétique, tout en produisant un niveau de perturbations compatible avec son environnement. En conséquence, l'art de la CEM (Compatibilité ElectroMagnétique) consistera à faire cohabiter harmonieusement divers matériels pour lesquels un effort de "durcissement" aura été réalisé, de manière à limiter leurs perturbations émises, et à améliorer leur insensibilité aux agressions venant de l'extérieur.

1-2) Perturbation électromagnétique et différents types de couplages :

On qualifie de perturbateur, tout signal indésirable produit par un matériel susceptible de gêner le fonctionnement d'autres équipements, la perturbation étant un signal se propageant par rayonnement ou par conduction.

On dénombre deux types de propagation de ce signal parasite :

- la propagation par rayonnement, (on parlera de couplage en mode rayonné).
- la propagation par conduction (couplage en mode conduit).

❖ **Couplage en mode rayonné :**

Il est défini comme étant un couplage par onde électromagnétique engendré par des courants et des tensions variables.

❖ **Couplage en mode conduit :**

Il est défini comme étant un couplage se faisant par les conducteurs et leurs composants électriques associés (parasites ou réels). Il faut donc disposer, au préalable, d'un schéma équivalent faisant apparaître tous les composants, même ceux qui ne sont pas intentionnellement destinés à faire partie du circuit (les composants modélisant des parasites).

2) Problèmes rencontrés en CEM :

Un problème classique rencontré par les concepteurs de systèmes électroniques, intégrés ou pas, est la possibilité que celui-ci cause le dysfonctionnement d'autres systèmes. Le système ainsi construit est qualifié d'agresseur (voir la figure I-1) et en termes de CEM, le système émet, soit en mode conduit, soit en mode rayonné. Les spécialistes de la CEM appellent ce problème, un problème d'émission. Réciproquement, un système électronique peut être « victime » (voir la figure I-2) de perturbations extérieures. Le problème posé-là, s'agit d'un problème de susceptibilité. La susceptibilité d'un système peut être perçue comme un problème de résistance maximale ou de sensibilité aux émissions conduites et rayonnées issues de systèmes électroniques ou d'autres sources que nous allons évoquer succinctement plus loin.

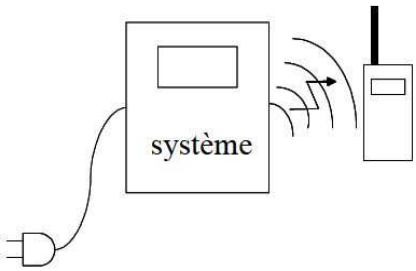


Figure I-1 : Tout système électronique peut se comporter comme une source de bruit.

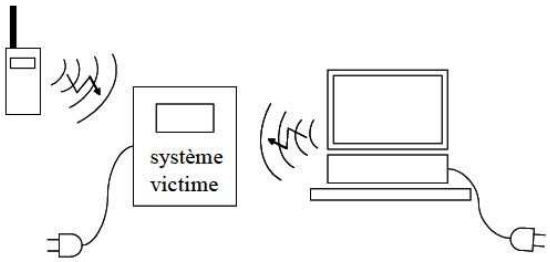


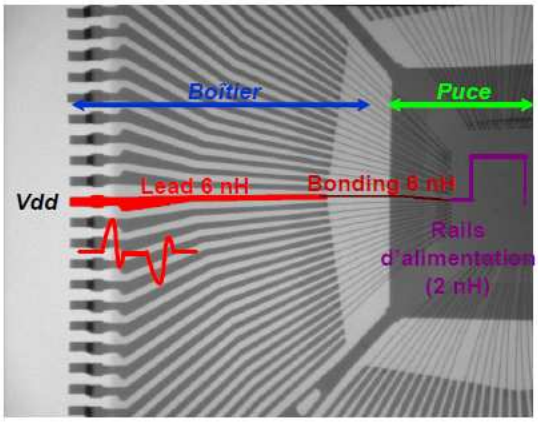
Figure I-2 : Tout système peut être perturbé par son environnement.

3) Emission parasite des circuits intégrés :

L'émission parasite issue d'un circuit intégré peut trouver son origine dans plusieurs sources. Nous allons évoquer ces sources de la façon suivante : une partie évoquera le bruit de commutation simultanée (SSN ou Simultaneous Switching Noise), une deuxième partie parlera des sources d'émission parasite les plus fréquentes. Cela se justifie par le fait que la commutation simultanée représente le mécanisme par lequel les sources d'émission parasite émettent, et perturbent ainsi les circuits environnants.

3-1) Le bruit de commutation simultanée (SSN ou Simultaneous Switching Noise) :

Les émissions électromagnétiques des systèmes électroniques trouvent leur origine au cœur des circuits intégrés. Ce phénomène provient du bruit de commutation simultanée ou *Simultaneous Switching Noise* (SSN) généré par les appels de courant dus à la commutation des différentes portes logiques du circuit. Des pics de courant transitoires apparaissant lors des commutations de l'état haut à l'état bas ou inversement des signaux logiques. Les alimentations et les références de masse parviennent aux circuits par l'intermédiaire d'un ensemble d'interconnexions, formées par les broches des boîtiers et le réseau d'alimentation interne. Toutes ces lignes représentent autant d'inductances et de résistances parasites qui, dès qu'elles sont traversées par un courant variables, induisent une variation de potentiel. Le boîtier représente le contributeur majeur de l'inductance parasite, tandis que le réseau d'alimentation interne est plus résistif. La figure I-3 [2] décrit l'ensemble des inductances et des capacités parasites à l'intérieur d'un circuit intégré qui sont responsables de l'apparition de SSN, avec les valeurs des éléments parasites introduits par différents types de boîtiers couramment utilisés.



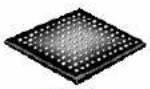
Boîtier	Nombre max de broches	Pitch min (mm)	Inductance boîtier (nH)	Capacité boîtier (pF)
 SOIC	90	0.4	1 –7	1 – 7
 QFP	300	0.4	3 – 7	2 – 5
 BGA	2000	0.5	0.5 – 10	1 – 10
 Stacked flip chip	1800	0.15	0.3 – 2	0.2 – 0.4

Figure I-3 : Inductances parasites liées aux interconnexions d'un circuit intégré (à gauche) et caractéristiques électriques des différents types de boitiers (à droite).

Le bruit lié au passage du courant de commutation des circuits au travers des inductances parasites des différentes interconnexions est appelé ΔI noise dont l'amplitude peut être évaluée à partir de l'équation suivante [2] :

$$V_{\Delta I\ noise} \approx L \times \frac{di}{dt}$$ Equation I-1

Avec : L : Inductance parasite du chemin d'alimentation.
di/dt : Pente du courant traversant les interconnexions.

Néanmoins, le chemin d'alimentation est aussi constitué d'une petite résistance parasite, variant de 100 mΩ à 10 Ω suivant la technologie et la taille du circuit. Le bruit lié au passage du courant appelé lors de la commutation des circuits au travers des résistances parasites est appelé IR noise. Avec l'augmentation de la résistance des interconnexions à chaque nœud technologique, le IR noise devient un problème de plus en plus contraignant.
Alors que le ΔI noise entraîne une fluctuation de tension, le IR noise entraîne une chute de potentiel et dégrade les vitesses de commutation des portes logiques, faisant ainsi apparaître des délais parasites. Cependant, l'ajout de résistances sur les rails d'alimentation permet d'amortir les oscillations produites par le ΔI noise et de réduire le bruit de commutation. Ainsi, la cumulation de ces deux effets permet de calculer l'amplitude du bruit de commutation en fonction du courant appelé par le circuit.

$$V_{SSN} = R \times i + L \times \frac{di}{dt}$$ Equation I-2 [2]

La figure 1-4 [2] décrit le phénomène de génération de bruit de commutation simultanée et la variation de tension d'alimentation produite.

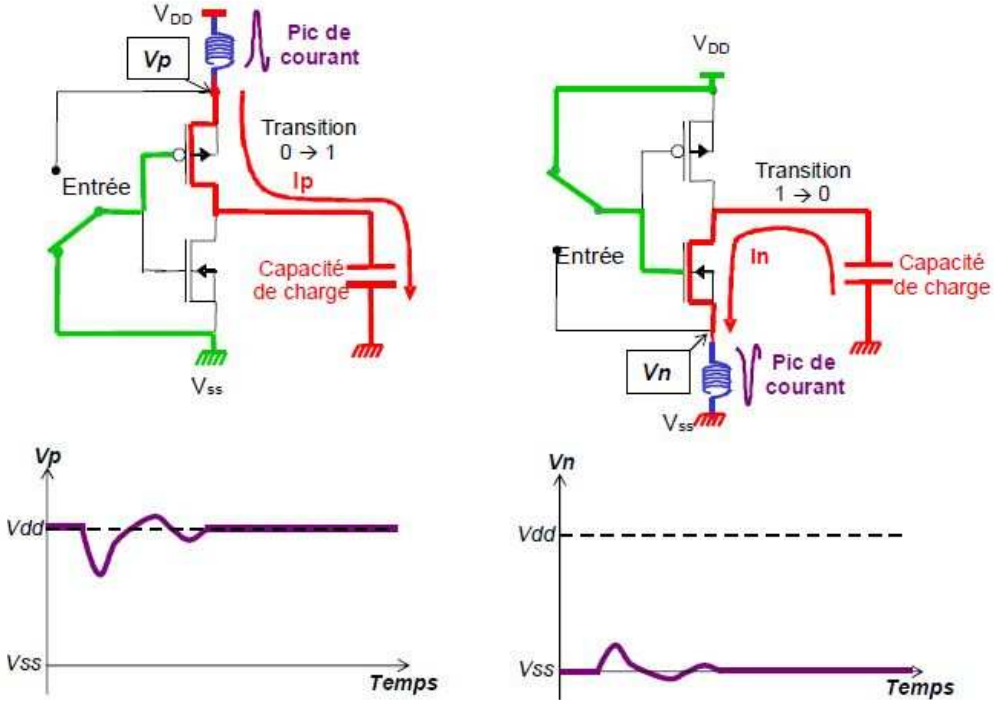


Figure I-4 : Courant circulant dans un inverseur CMOS lors de sa commutation et génération de bruit de commutation simultanée sur les lignes d'alimentation.

De nombreux modèles ont été développés afin de prédire l'amplitude du bruit de commutation. Celui-ci dépend d'un certain nombre de facteurs:

- La forme de l'appel de courant.
- Les paramètres technologiques et géométriques des transistors.
- Le nombre de portes commutant simultanément.
- L'impédance du chemin d'alimentation ou de masse.
- La disposition des plans d'alimentation et de masse.
- La capacité de charge.

Le tableau I-1 [2] présente les appels de courant typiques en fonction des technologies. Il apparaît clairement que l'amplitude du pic de courant et donc le bruit de commutation simultanée augmentent avec l'évolution technologique. On peut remarquer que, même si le pic de courant généré par porte ainsi que la tension d'alimentation diminuent, l'appel de courant total augmente puisque les circuits deviennent de plus en plus denses.

Technologie	Tension d'alimentation (V)	Densité de portes (/mm²)	Pic de courant (mA/porte)	Capacité (fF/porte)	Pic de courant (A/mm²)
1.2 µm	5	8K	1.1	60	8.8
0.8 µm	5	15 K	0.9	40	13.5
0.5 µm	5	28 K	0.75	30	21
0.35 µm	5 – 3.3	50 K	0.6	25	30
0.25 µm	5 – 2.5	90 K	0.4	20	36
0.18 µm	3.3 – 2	160 K	0.3	15	48
0.12 µm	2.5 – 1.2	240 K	0.2	10	48
90 nm	2.5 – 1	480 K	0.1	7	48
65 nm	2.5 – 0.8	1000 K	0.07	5	50
45 nm	1.8 – 0.8	2000 K	0.05	3	55

Tableau I-1 : Evolution des pics des courants en technologie CMOS.

La figure 1-5 [2] présente un exemple de bruit de commutation simultanée ainsi que sa transformée de Fourier. La forme de cet appel de courant peut être représentée en première approximation par un triangle. Ce bruit est caractérisé par des temps de montée et de descente rapides lui conférant de nombreuses composantes harmoniques à haute fréquence. L'analyse de son spectre montre qu'il couvre quasiment deux décades du spectre radiofréquence.

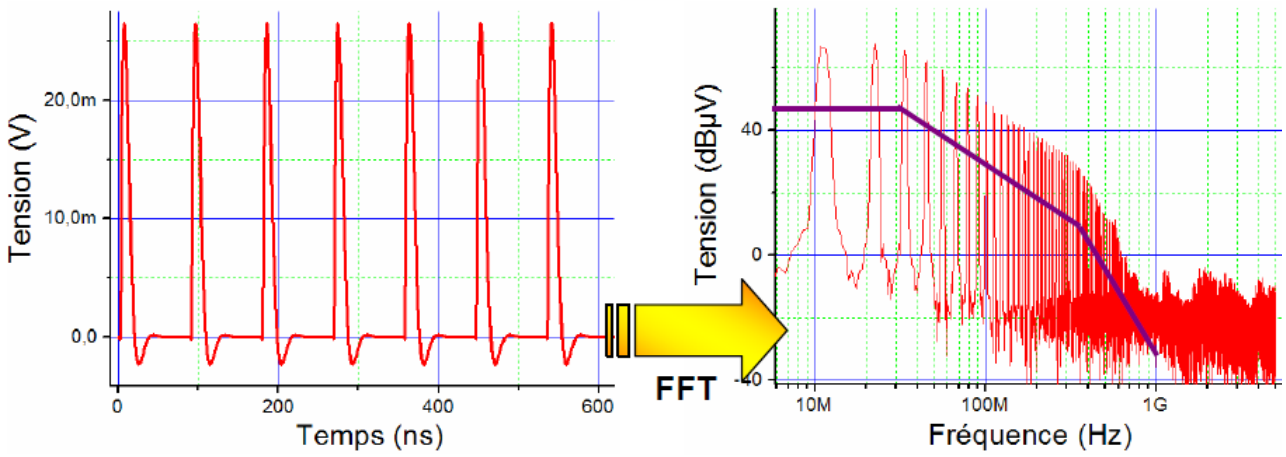


Figure 1-5 : Exemple de bruit de commutation simultanée et son spectre de fréquence.

3-2) Les sources d'émission électromagnétique parasite d'un circuit intégré :

Les circuits qui se caractérisent par des commutations nombreuses et simultanées, et en général, qui connaissent des variations de courants trop brusques et les appels de courant les plus importants, sont les plus bruyants. Certains blocs dans un circuit intégré sont plus bruyants que d'autres, et entre autre, les blocs les plus perturbateurs et qui sont donc assimilés aux sources des émissions parasites sont :

- ❖ Les blocs digitaux synchrones qui créent un appel de courant à chaque front de l'horloge de synchronisation. Le bruit est causé principalement par l'activité des cœurs numériques qui augmente à chaque nouvelle génération de circuit.
- ❖ Les entrées/sorties : Le bruit produit par la commutation des entrées/sorties est très important puisque celles-ci sont constituées de transistors MOS capables de fournir un courant important. Leurs états logiques dépendent des données qu'elles transportent à l'intérieur ou à l'extérieur du circuit intégré. Plus le nombre d'entrées/sorties commutant en même temps augmente et plus elles sont rapides, plus le bruit généré augmente.
- ❖ Les arbres d'horloge, qui distribuent le signal d'horloge et propagent le bruit à l'ensemble du circuit.
- ❖ Certains blocs analogiques tels que des amplificateurs de puissance ou des PLL, qui peuvent produire des émissions parasites concentrées sur quelques harmoniques.

Ces différents blocs peuvent être intégrés à l'intérieur du même circuit, comme dans un microcontrôleur qui intègre des blocs digitaux, des entrées/sorties, des convertisseurs analogique numérique (ADC ou Analog Digital Converter en anglais), des PLL et des blocs analogiques. La figure I-6 [2] présente une vue du placement des différents blocs ou floorplan d'un microcontrôleur. 16 bits.

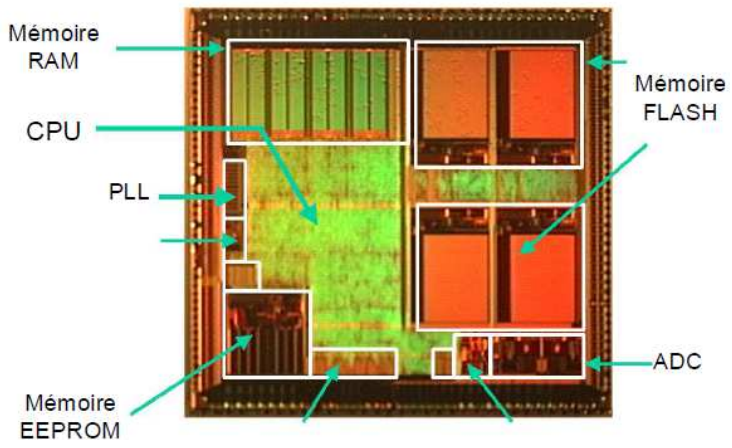


Figure 1-6 : le floorplan (disposition des blocs) d'un microcontrôleur 16 bits.

3-3) La propagation du bruit émis :

a) Conséquences et effets du bruit émis sur les circuits environnants :

Une fois le bruit généré, celui-ci va pouvoir se propager à travers tout le circuit ou aux circuits environnants, soit par couplage conduit, soit par couplage rayonné, comme l'illustre la figure I-8. A l'intérieur même du circuit, des problèmes d'auto-susceptibilité risquent d'apparaître (figure I-7), c'est-à-dire qu'un bloc bruyant pourra perturber un bloc sensible. Par exemple, la commutation de plusieurs entrées/sorties dans un circuit peut générer du bruit de commutation simultanée sur les lignes d'alimentation des entrées/sorties. Une partie de ce bruit peut se coupler au bus d'alimentation dédié aux parties analogiques, et induire des erreurs sur le résultat de conversion d'un convertisseur analogique numérique (figure I-7). Les circuits intégrés sont montés sur des cartes (PCB ou Printed Circuit Board) et partagent aussi un ensemble de pistes communes. Le bruit peut aussi se propager à travers toute la carte et venir perturber les circuits environnants. Par exemple, imaginons une carte de contrôle moteur sur laquelle se trouve un hacheur piloté par un microcontrôleur. Le hacheur produit de très forts appels de courants induisant un bruit important. Une partie de ce bruit peut venir se coupler sur les lignes d'alimentation du microcontrôleur et perturber son fonctionnement.

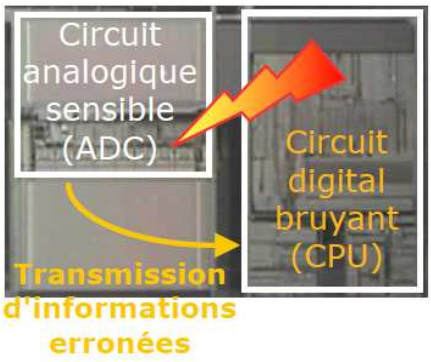


Figure I-7 : Illustration de l'auto-susceptibilité des microcontrôleurs.

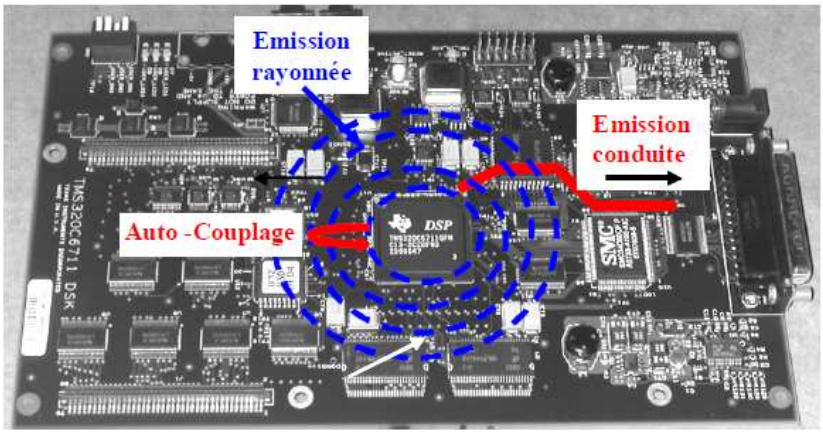


Figure I-8 : Propagation du bruit généré par un circuit intégré.

b) Mécanismes de propagation conduite :

Le bruit se propage principalement à l'intérieur des circuits ou sur les PCB par couplage conduit. Les lignes d'alimentation ou de masse des cœurs digitaux ou des entrées sortie sont les principaux vecteurs de propagation, puisque la commutation des cœurs numériques ou des entrées sorties génère des fluctuations de tension sur les alimentations. Une modélisation complète des résistances et des inductances parasites des interconnexions permettent de déterminer l'amplitude du bruit conduit. La propagation peut se faire aussi par couplage entre interconnexions voisines. Ce couplage, appelé aussi diaphonie ou *crosstalk*, il peut être soit de nature inductive, soit de nature capacitive. La figure I-9 décrit Le phénomène.

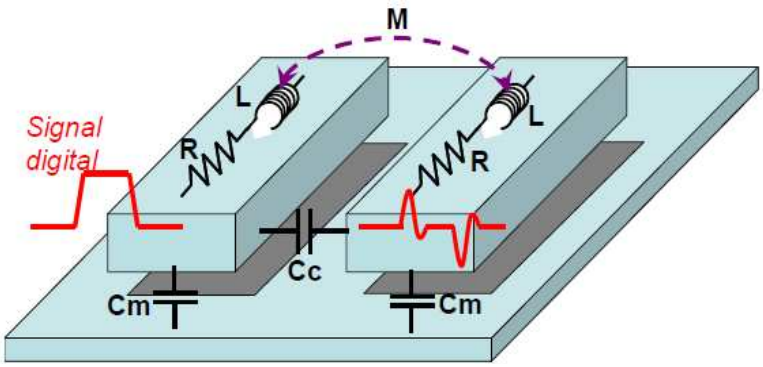


Figure I-9 : Couplage en mode conduit inductif et capacitif entre deux interconnexions.

A l'intérieur des circuits intégrés, puisque les interconnexions sont très peu inductives et très rapprochées, le couplage est de nature capacitive, contrairement aux boîtiers où le couplage est plutôt de nature inductive. Celui-ci joue un rôle prépondérant dans la génération de couplages diaphoniques et peut être responsable de fluctuations de niveaux de tension internes. Le couplage entre interconnexions prend une importance cruciale dès que les fréquences des signaux des entrées/sorties augmentent. En effet, l'amplitude de tensions induites par la diaphonie dépend du temps de montée des signaux. De plus, plus les signaux sont rapides, plus ils sont sensibles à toute forme de dégradation de leur intégrité.
A l'intérieur des circuits, un autre couplage est aussi à l'œuvre. L'ensemble des blocs d'un même circuit partage le même substrat. Du fait de son faible dopage, celui-ci présente une résistivité élevée offrant une bonne isolation entre les différents blocs. Cependant, les blocs bruyants tels que les blocs digitaux peuvent injecter du bruit dans le substrat, qui va se propager vers des blocs sensibles tels que les blocs analogiques et éventuellement les perturber. Ce phénomène appelé couplage substrat est un des principaux freins au développement de l'intégration de systèmes sur puce (SoC ou System on Chip) mixant des blocs analogiques et numériques. Différents mécanismes d'injection sont détaillés sur la figure I-10 :

- Par les contacts de polarisation du substrat ; si une alimentation bruitée vient polariser le substrat, alors le bruit est directement injecté dans le substrat à travers la résistance formée par le contact.

- Le couplage capacitif entre le substrat et les différents éléments d'un circuit, tels que les jonctions PN au niveau des drains et des sources, les interconnexions des niveaux de métaux inférieurs, et les caissons d'isolation. Ce mode est particulièrement important pour les blocs digitaux rapides.
- Le courant d'ionisation par impact, dû à la création de porteurs chauds formés entre le drain et la source des transistors mis en saturation et qui sont injectés dans le substrat. Ce phénomène est prépondérant jusqu'à quelques dizaines de mégahertz et prend de l'importance avec la réduction de la taille des circuits.

Les phénomènes liés à la réception de ce bruit sont assez similaires et sont les suivants :

- l'interaction du bruit substrat avec les transistors MOS peut se faire au niveau des capacités de jonction, ou à cause du body effect. A cause de la variation de la tension de polarisation du substrat due au bruit, le seuil de commutation, la tension drain source et le courant de drain sont modifiés.
- Couplages capacitifs au niveau des résistances de diffusion et des capacités on chip, puisqu'elles présentent une surface en regard importante avec le substrat.
- les alimentations analogiques peuvent aussi être affectées par le couplage substrat à travers les contacts de polarisation.

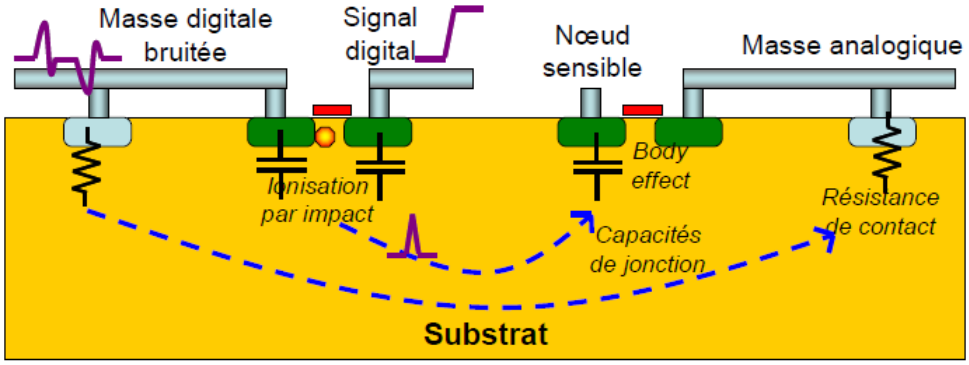


Figure I-10 : Mécanismes d'injection et de réception de bruit par couplage substrat.

c) Mécanismes de couplage rayonné :

Toute interconnexion peut jouer le rôle d'antenne, de manière plus ou moins efficace à une fréquence donnée. Ainsi, dès que la longueur L d'une interconnexion s'approche de $L \approx \frac{\lambda}{4}$ celle-ci joue un rôle d'antenne et les courants qui les traversent ou les tensions à leurs bornes peuvent engendrer la création d'un champ électromagnétique. Le tableau de la figure I-2 [2] donne une idée des structures pouvant jouer le rôle d'antenne en fonction de la fréquence.

Fréquence	10 MHz	100 MHz	1 GHz	10GHz
Longueur d'onde λ	30 m	3 m	30 cm	3 cm
λ/4	7.5 m	75 cm	7.5 cm	7.5 mm
Antenne physique	Long câble	Câble	Piste PCB	Lead boîtier

Tableau I-2 : Dimension d'antenne en fonction de la fréquence et identification des parties susceptibles de jouer ce rôle.

La circulation d'un courant à l'intérieur d'une boucle (formée par exemple par un conducteur et son retour à la masse) constitue une source efficace de champ magnétique, alors que la variation de potentiel d'une interconnexion (par exemple la commutation d'une broche d'un port de microcontrôleur) constitue une source efficace de champ électrique. La figure I-11 illustre les mécanismes de génération des champs électrique et magnétique à proximité des broches d'un boîtier.

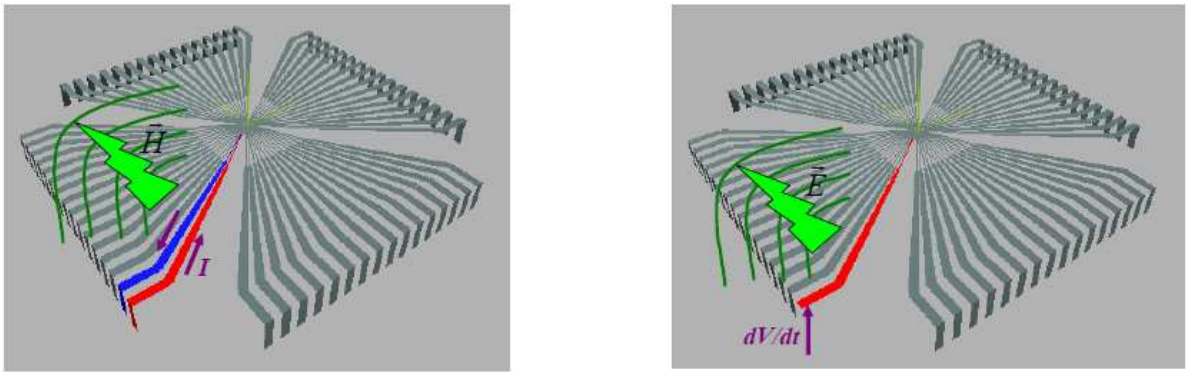


Figure I-11 : Mécanismes de génération des champs magnétique (à gauche) et champ électrique (à droite).

Le rayonnement produit par n'importe quelle antenne peut se séparer en trois zones, détaillées sur la figure I-12.

On distingue les zones suivantes :

- la zone de rayonnement en champ proche, qui se situe à proximité de l'antenne. A l'intérieur de cette zone, l'onde plane ne s'est pas encore formée et la distribution des composantes du champ dépend de la distance à l'antenne. L'amplitude des, 28 composantes du champ se met à décroître très rapidement à mesure qu'on s'éloigne de l'antenne.
- La zone de Fresnel, qui est une zone intermédiaire.
- La zone de champ lointain, où l'onde plane est localement formée. Celle-ci est qualifiée d'onde transverse électromagnétique ou TEM.

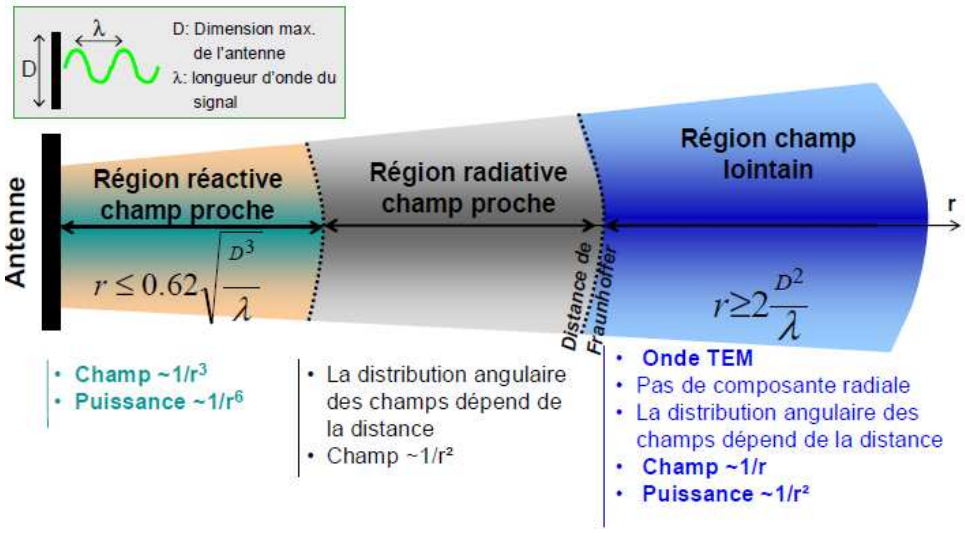


Figure I-12 : Régions électromagnétiques d'une antenne.

4) La susceptibilité des circuits intégrés :

La susceptibilité d'un circuit intégré signifie la sensibilité ou le degré de fragilisation de son fonctionnement correct par des émissions extérieures. Ces émissions ont plusieurs origines, c'est justement ces sources qui seront citées dans le paragraphe suivant.

4-1) Principales sources de perturbation extérieures :

Comme nous l'avons déjà fait remarquer, les circuits intégrés sont une source de rayonnement, certes, elle ne doit pas être négligée, mais il existe des sources plus nuisibles qui peuvent causer des accidents dramatiques. Un exemple serait la foudre qui peut causer des accidents d'avions qui a, à juste titre, une attention particulière de l'industrie aéronautique. Il existe de nombreuses autres sources (voir la figure I-13) qui peuvent fragiliser et rendre plus susceptibles les circuits intégrés, et induire des dysfonctionnements parfois graves. La liste de ces sources n'est pas exhaustive car leur nombre tend à augmenter avec l'évolution technologique ; cependant, nous allons citer dans la suite les principales sources de perturbations actuelles.

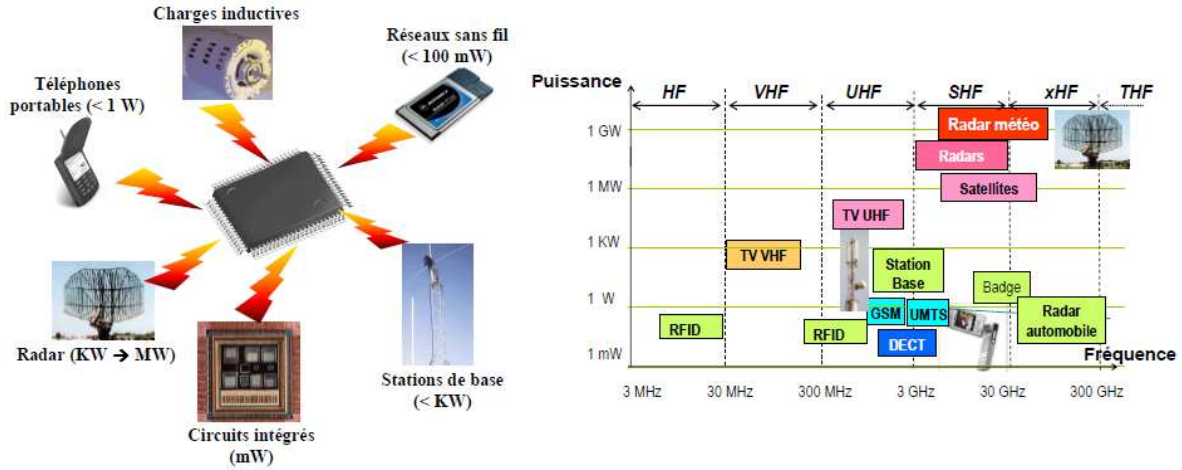


Figure I-13 : Exemple de sources de perturbation électromagnétique.

a) Les décharges électrostatiques ou les ESD (ElectroStatic Discharges) :

Il existe deux grandes familles de décharges électrostatiques (ESD) dans l'air. La foudre qui se propage sur plusieurs centaines de mètres, et met en jeu des tensions de plusieurs centaines de kilovolts, et les plus petites décharges qui sont générées sur moins d'un centimètre (contact humain avec un circuit intégré par exemple) avec des tensions de l'ordre du kilovolt. Ce sont ces dernières qui intéressent la plus grande majorité des concepteurs de circuits intégrés et de systèmes électroniques, la foudre étant plus spécifiquement traitée dans le domaine aéronautique.

Une décharge électrostatique est la remise à l'équilibre des charges d'un système initialement déséquilibré. Il existe deux processus pour créer le déséquilibre de charges : la triboélectricité et l'induction. Appliqué au circuit intégré, cela revient généralement à deux types de

configurations. Dans le premier cas, le circuit intégré se trouve dans le chemin de décharge, entre un générateur externe et un plan de masse. Dans le second cas, le composant initialement isolé, subit un champ électrique et se charge, pour ensuite se décharger dès qu'il a un contact externe.

Une décharge électrostatique peut avoir deux effets néfastes sur un circuit intégré. Elle génère un courant important qui, au passage dans le circuit, peut élever sa température jusqu'à atteindre sa destruction thermique. Elle provoque aussi dans le circuit une surtension qui peut mener à la rupture d'un diélectrique ou la mise en conduction par avalanche d'une jonction dans le silicium. Les défaillances peuvent intervenir à plusieurs endroits dans le circuit intégré. Dans le semi-conducteur, sous l'effet d'un fort courant et d'un champ électrique important, les jonctions peuvent atteindre localement la température de fusion du silicium, ce qui entraîne une diffusion des dopants, et une modification des caractéristiques. Une jonction qui, avant d'être exposée à une décharge électrostatique, était bloquée à la tension d'alimentation du circuit, devient maintenant passante, entraînant un dysfonctionnement du circuit. Les oxydes de grille des technologies MOS sont aussi menacés par la décharge sous l'effet d'un champ électrique élevé. Enfin le courant de décharge qui circule dans un métal peut provoquer sa fusion. La métallisation peut s'évaporer et créer un circuit ouvert. Ou alors, au cours du refroidissement du métal, un court-circuit peut se former entre des lignes adjacentes. Un contact métallique peut aussi diffuser dans le silicium et atteindre une jonction. Il y a alors court-circuit de cette dernière.

Historiquement, ce sont les technologies MOS qui étaient les plus susceptibles aux décharges électrostatiques, de par la grande sensibilité de leurs oxydes de grille. Cette tendance s'est ensuite généralisée aux autres technologies avec la réduction de leurs dimensions. Les jonctions moins profondes, les oxydes plus fins et les métallisations et vias (connexions métalliques entre deux étages voisins d'interconnexions) moins larges, sont autant de progrès technologiques qui rendent les circuits intégrés de plus en plus sensibles aux décharges électrostatiques.

b) Les charges inductives :

Les charges inductives sont essentiellement constituées par des appareils mettant en jeu des moteurs (Figure I-14 partie de gauche). Le nombre de moteurs ne cesse de croître dans les équipements d'une automobile moderne : essuie-vitre, lève-vitre, rétroviseur, ventilateur, etc. On peut également dans certaines conditions y ajouter les interrupteurs ou les relais, lorsqu'ils véhiculent des courants de fortes intensités.

La partie de droite de la figure I-14 [15] présente une forme d'onde transitoire représentative de ce phénomène. A l'origine de ces perturbations conduites, se trouvent de forts appels de courant, comme lors de la mise en marche d'un moteur, ou de forts courants induits, lors de son arrêt. La puissance et la forme d'onde de tels phénomènes varient en fonction des caractéristiques intrinsèques de l'élément perturbateur.

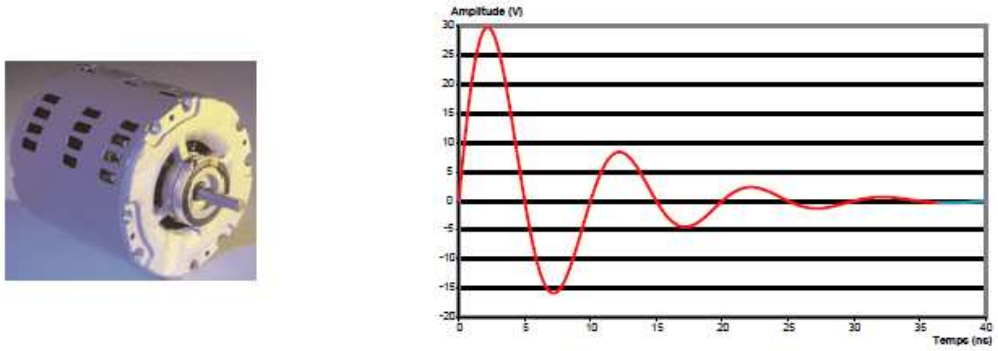


Figure I-14 : Exemple de charge inductive (gauche) et d'un signal transitoire généré par celui-ci (droite).

c) Les circuits intégrés :

Du fait de leur activité interne toujours plus grande, les circuits intégrés actifs (Figure I-15 partie de gauche), tels que les microcontrôleurs ou microprocesseurs, sont à l'origine d'une émission électromagnétique non négligeable. Un exemple de spectre d'émission est fourni par la partie de droite de la Figure I-15 [15]. Cette forme de pollution électromagnétique est aussi bien conduite que rayonnée. En effet, les interconnexions les plus longues, telles que l'arbre d'horloge ou le réseau d'alimentation, ainsi que les bondings (connexion métallique entre la puce et son boîtier) de connexion au boîtier sont des chemins privilégiés pour transmettre les parasites vers l'extérieur.

Les niveaux de perturbations émis sont généralement de l'ordre du milliwatt. Mais du fait de la diversité des composants et l'augmentation de leur fréquence d'horloge, la bande de fréquence qu'ils couvrent est très large et s'agrandit au fil des générations.

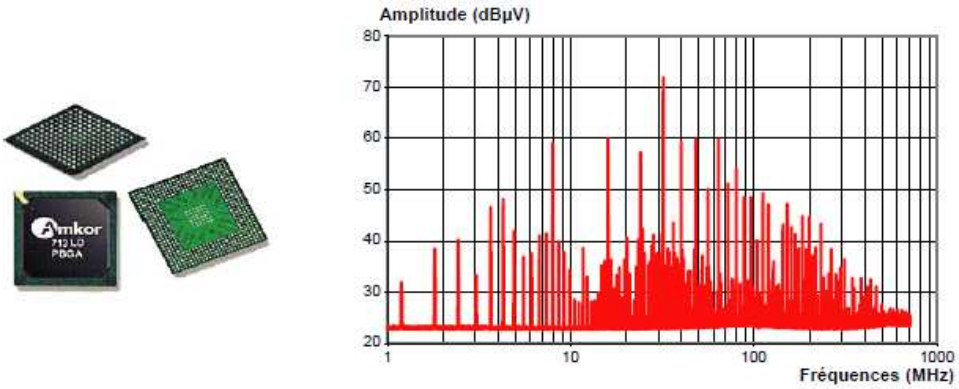


Figure I-15 : Exemple de circuits intégrés bruyants et de spectre d'émission d'un circuit intégré.

d) Les réseaux de communication de données sans fil :

Avec l'essor des systèmes embarqués et portables, les protocoles de communication sans fil ont vu le jour. Ils mettent en jeux des liens de type transpondeur (inférieur à 10 cm) pour les très courtes distances, infrarouge pour de courtes distances (inférieures à quelques mètres), et

hertzien de faible puissance pour les distances inférieures à quelques centaines de mètres. Ce sont bien évidemment les communications hertziennes de faible puissance telles que Bluetooth, WiFi, RFHome ou HiperLAN2 qui font l'objet de toutes nos attentions (Figure I-16).

Ces communications, de plus en plus nombreuses, mettent en jeux des puissances de l'ordre de quelques dizaines de milliwatts à des fréquences situées actuellement aux alentours de 2.5 GHz, mais qui devraient monter jusqu'à 5 GHz (WiFi3, HiperLAN2) dans les années à venir. De plus, le fait de créer des réseaux locaux mobiles (Bluetooth), rend difficile un contrôle précis des paramètres de puissance émise, et par conséquent les niveaux de pollution électromagnétiques engendrés.

La figure I-16 illustre quelques exemples matériels utilisés par les communications sans fils moyennant le Bluetooth ou le WiFi.

Figure I-16 : Exemples d'équipements de réseaux de données sans fil.

e) Les téléphones mobiles et les stations relais associées :

Si l'on se réfère aux nombres de portables et de relais téléphoniques existant dans le monde, la téléphonie mobile (Figure I-17) est incontestablement la source de perturbation électromagnétique la plus dense. Concernant les caractéristiques fréquentielles, que l'on considère un téléphone mobile ou une antenne relais, elles sont identiques et situées dans trois bandes principales centrées autour de 900 MHz (GSM), 1,8 (DCS) et 1,9 GHz (UMTS).

Figure I-17 : Téléphone mobile (à gauche) et antenne-relais (à droite) de type GSM.

Les signaux sont transmis en modulation de phase mais leur puissance et leur gestion diffèrent selon que l'on a affaire à une station relais ou un téléphone cellulaire. En effet, la puissance, transmise par un téléphone portable en communication peut atteindre un watt, tandis que celle d'une antenne-relais peut atteindre la centaine de watts. Il est bon de noter que dans les deux cas, la puissance émise est susceptible de fluctuer en fonction de la distance et de l'environnement qui sépare la station de base du téléphone mobile.

Pour les standards GSM [15], les signaux sont transmis en modulation de phase (partie centrale de la Figure I-18). Par contre, leur gestion est différente. Le portable a une forme d'onde de type

burst (Figure I-18 partie de droite), c'est-à-dire qu'il émet son signal pendant une durée relativement courte (577 µs) comparée à la période de répétition (4,61 ms). La station relais a une transmission plus aléatoire du fait qu'une même station peut gérer jusqu'à 8 communications "simultanément". Dans les périodes creuses, elle se comporte pratiquement comme un téléphone mobile, et en périodes de forte affluence, elle transmet quasiment en continu (Figure I-18 partie de gauche).

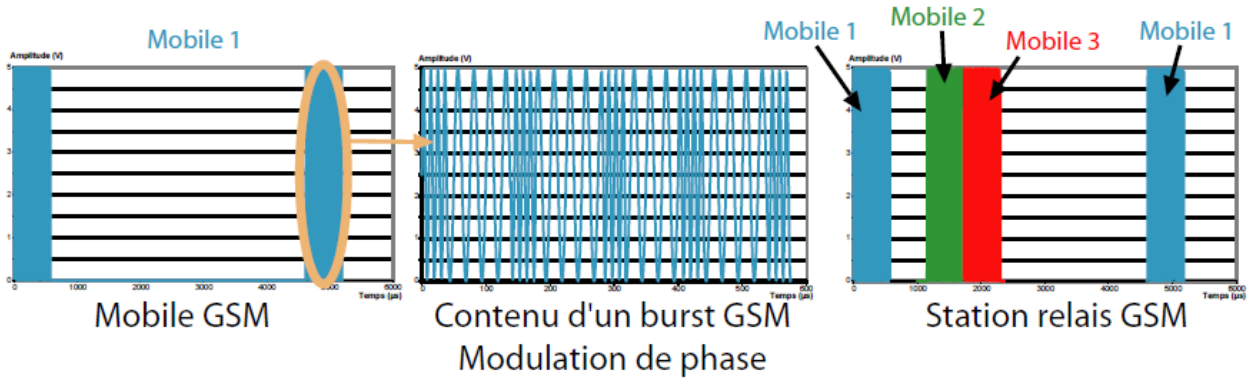


Figure I-18 : Formes d'onde par un téléphone mobile (parties centrale et de gauche) et une antenne-relais en communication avec trois téléphones portables.

f) Les relais de radiodiffusion ou de télédiffusion :

Bien que moins nombreux en comparaison des relais de téléphonie mobile [15], les antennes-relais de radiodiffusion ou télédiffusion (Figure I-19 partie de gauche) n'en sont pas moins des perturbateurs électromagnétiques importants. En effet, ils transmettent en continu des signaux modulés en fréquences (Figure I-19 partie de droite) dont l'énergie peut atteindre quelques kilowatts. Une telle puissance est susceptible de perturber le fonctionnement d'un système embarqué, tels que ceux équipant une voiture, qui se situerait dans son environnement proche.

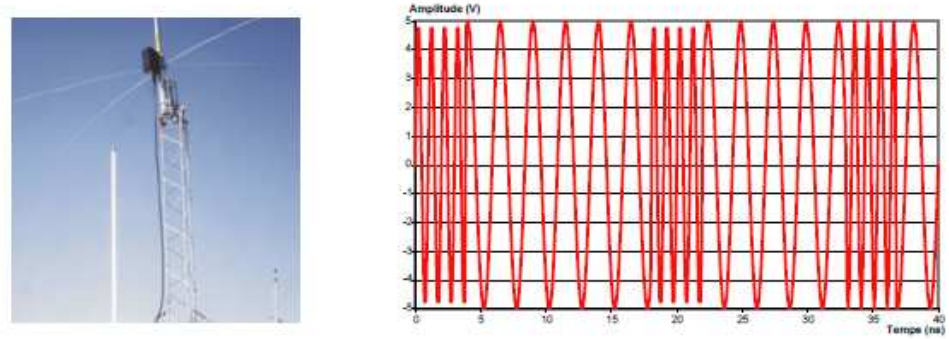


Figure I-19 : Antenne-relais de radiodiffusion (à gauche) et la forme d'onde qui lui assignée (à droite).

g) Les radars :

Que ce soit dans l'aviation ou la marine civile, militaire ou dans le domaine de la météorologie (Figure I-20 partie de gauche), les radars font partie des sources de perturbations électromagnétiques parmi les plus énergétiques. De quelques kilowatts pour les radars "classiques", ils peuvent émettre jusqu'à 10 GW pour les radars de forte puissance. La plupart d'entre eux fonctionnent dans des gammes de fréquences supérieures au gigahertz [15].

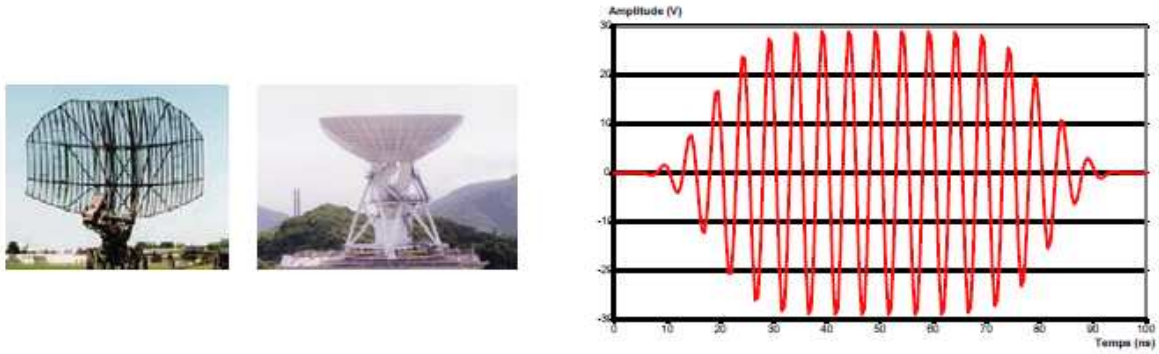
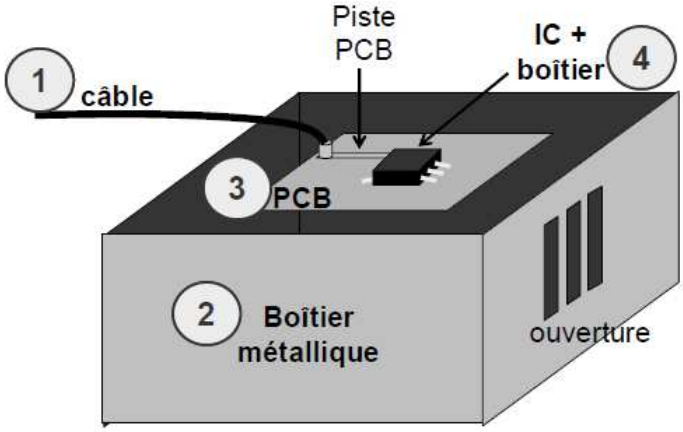


Figure I-20 : Radars (à gauche) et exemple de frome d'onde générée par un radar (à droite).

4-2) Couplage des perturbations externes :

Avant de perturber un circuit, la perturbation doit se coupler à celui-ci, soit de manière rayonnée, soit de manière conduite. Dans la partie précédente (émission parasite des circuits intégrés), nous avons vu comment se couplait le bruit émis par un circuit intégré. Nous n'allons considérer ici que le bruit provenant d'une source extérieure. Tout l'environnement du circuit intégré peut coupler une partie de l'énergie d'une perturbation incidente par effet d'antenne et ainsi influencer la susceptibilité du système électronique. En effet, les structures de couplage vont être à l'origine de résonances dont les fréquences sont liées à leurs dimensions. En outre, chacune de ces structures est constituée d'éléments électriques parasites qui vont modifier la pénétration de l'onde à l'intérieur du circuit en fonction de la fréquence.

Prenons comme modèle le schéma, de la figure I-21, représentant un système électronique classique. Nous allons décrire les différents niveaux de ce système et leur influence sur la susceptibilité du système.



D'abord, les câbles constituent des antennes très efficaces et il s'agit du mode de couplage principal en dessous de 1 GHz. Ce couplage va ensuite permettre aux perturbations de venir se propager de manière conduite aux différents circuits composant le système.
Ensuite, à une échelle inférieure, on trouve la carte ou le PCB. Les pistes peuvent former des antennes à partir de quelques centaines de mégahertz et peuvent être considérées comme des lignes de transmission miniatures. Le PCB (le circuit imprimé) a aussi une influence sur la susceptibilité du circuit, qui varie suivant la nature du substrat (le diélectrique, les pertes, le nombre de couches). On peut aussi citer l'influence de structures telles que des radiateurs placés sur le capot de circuits dans le couplage du champ électrique incident. En effet, un radiateur peut former avec le plan de masse du PCB (circuit imprimé) une cavité électromagnétique ou une antenne patch, qui couplera de manière efficace le champ incident à ses fréquences de résonance.

Le boîtier du circuit constitue le dernier étage de couplage avant le circuit. Il constitue certes une antenne moins efficace que les câbles et les pistes de PCB, mais il s'agit d'une partie inévitable du chemin de couplage et de propagation du bruit vers le circuit. Les broches des circuits intégrés représentant des résistances et des inductances parasites, elles présentent des bandes passantes limitées, dont les fréquences de coupure varient de quelques centaines de mégahertz à plusieurs gigahertz suivant le type de boîtier.

4-3) Effets des perturbations sur le comportement des circuits intégrés :

Après avoir abordé la génération, la propagation et les modes de couplage d'un champ électromagnétique, nous allons nous intéresser aux effets que les perturbations peuvent avoir sur les systèmes électroniques. Pour cela, nous distinguerons les composants analogiques des composants numériques puisque leurs réactions sont sensiblement différentes.

4-3-1) Les circuits analogiques :

Tous les circuits ont un domaine de fréquence dans lequel leur fonctionnement est normal. Donc, pour les perturbations électromagnétiques deux cas de figure peuvent se présenter : elles peuvent tomber dans l'intervalle de fonctionnement nominal du circuit ou en dehors de celui-ci.

a) Hors-bande de fréquence du composant :

Il faut distinguer le mode de fonctionnement dans la bande de fréquence du composant analogique de celui hors bande. En effet, considérons une perturbation électromagnétique dans la bande de fréquence du composant susceptible de générer un dysfonctionnement. Pour que la même perturbation soit capable de provoquer un dysfonctionnement comparable hors bande, il lui faudra avoir des caractéristiques énergétiques bien supérieures. Ce phénomène est directement lié aux caractéristiques intrinsèques des circuits intégrés, qui se comportent de manière générale comme un filtre passe-bas. Ce phénomène est d'autant plus vrai avec les composants analogiques.

b) <u>Dans la bande de fréquence du composant :</u>

Une faible variation de tension ou de courant en entrée est susceptible de créer un dysfonctionnement sur un capteur de pression, de température ou tout autre composant analogique (Figure I-22 partie de gauche). La perturbation va venir se superposer au signal utile et a pour principal effet de créer une tension d'offset comme l'illustre la partie de droite de la Figure I-22. Cet offset est ensuite transmis au système de contrôle qui va traiter des valeurs en entrée erronées avec toutes les conséquences qui en découlent.

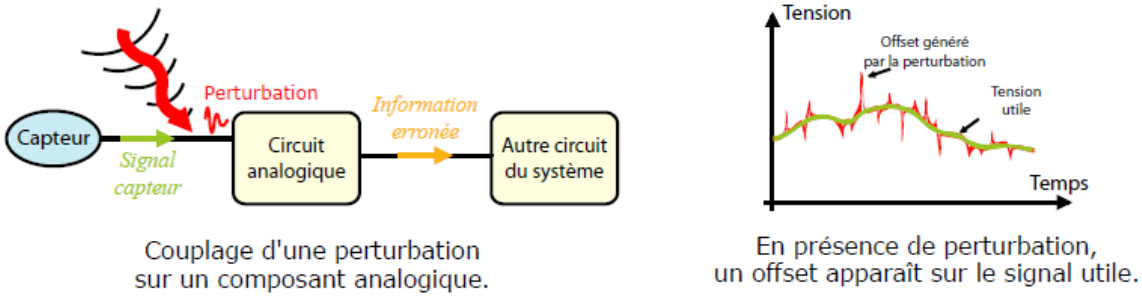


Figure I-22 : Couplage (à gauche) et génération d'offset (à droite) due à une perturbation électromagnétique sur un composant analogique.

D'autres effets existent, et parmi eux nous pouvons retenir la fluctuation de tension d'alimentation. En effet, certains composants analogiques, tels que les convertisseurs analogique/numérique ou numérique/analogique, ou les amplificateurs de précision, y sont particulièrement sensibles. La susceptibilité des convertisseurs est liée au fait que l'alimentation leur sert également de référence et que les données délivrées sont directement en rapport avec les références basse et haute. De surcroît, plus la résolution porte sur un nombre important de bits, et plus la susceptibilité du composant est forte. Quant à la susceptibilité des amplificateurs, elle vient principalement du fait qu'ils tirent leur puissance de l'alimentation. Des fluctuations du niveau d'amplification sont alors perceptibles, d'autant plus aisément lorsqu'il s'agit de signaux audio. De plus, il a été montré que l'étage différentiel des amplificateurs est un élément critique de par le fait qu'il conduit simultanément les bruits de mode commun et différentiel.

Enfin, les effets des perturbations électromagnétiques sur les composants analogiques revêtent un caractère généralement temporaire voire éphémère. Une fois la perturbation disparue, le comportement du composant redevient souvent nominal. Ce qui n'est pas forcément le cas pour les composants numériques qui font l'objet des paragraphes suivants.

4-3-2) Les circuits numériques :

a) Le phénomène de latchup :

Le phénomène de latchup [2] est dû à la mise en conduction involontaire (suite à une perturbation électromagnétique par exemple), d'une succession de jonctions PNPN formant un thyristor parasite entre l'alimentation et la masse (Figure I-23). Le déclenchement de thyristor parasite provoque un court-circuit entre l'alimentation et la masse du circuit intégré qui peut être destructif.

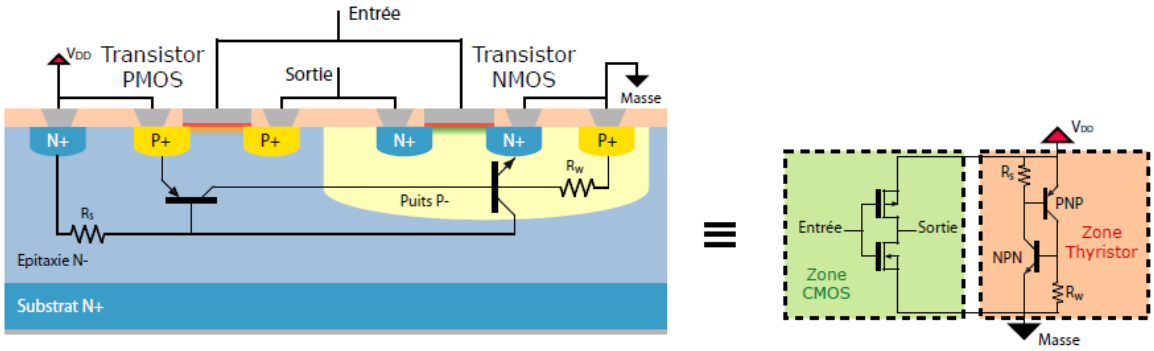


Figure I-23 : Phénomène du latchup dans les circuits intégrés numériques.

b) Effet sur les sorties :

Un autre élément des composants numériques peut s'avérer susceptible : la sortie d'un composant élémentaire. Du fait de sa faible impédance, une sortie numérique peut être perturbée par l'injection d'un courant parasite d'amplitude relativement faible (de l'ordre de la dizaine de milliampère). L'effet d'une telle perturbation se traduit généralement par un changement d'état de la sortie.

c) Effet sur les entrées :

Bien que leur impédance soit relativement élevée en comparaison de celles des sorties, les entrées numériques peuvent également être perturbées. En effet, la réduction des tensions d'alimentation s'accompagne d'une réduction des seuils de commutation et par conséquent d'une diminution des marges de bruits en entrée. De ce fait, les entrées sont toutes aussi susceptibles. Et cette susceptibilité se traduit, comme pour les sorties, par une inversion du niveau de l'information d'entrée.

Conclusion :

Dans ce chapitre, nous avons défini en premier ce qu'est la compatibilité électromagnétique, puis quelques notions de base indispensables pour pouvoir aborder les différents problèmes rencontrés en compatibilité électromagnétique des circuits intégrés. Nous avons abordé les deux sous-domaines de la compatibilité électromagnétique des circuits intégrés, c'est-à-dire, leur émission parasite et leur susceptibilité.

Dans l'émission parasite des circuits intégrés, nous avons abordés le problème du bruit de commutation simultanée ou SSN, qui est le principal mécanisme par lequel certains blocs de circuits intégré émettent du bruit. Ensuite, nous avons explicité comment ce bruit venait se coupler et gêner ainsi le fonctionnement de circuits extérieurs ou de blocs du même circuit.

Dans la partie susceptibilité des circuits intégrés aux rayonnements extérieurs, nous avons cité les sources de bruit les plus étudiées et les plus problématiques, du point de vue CEM. Puis, nous avons expliqué comment ces perturbations se couplaient aux différentes composantes d'un système électronique (Circuit intégré, câbles, pistes du circuit imprimé…). Enfin, nous avons succinctement discuté les conséquences de tels couplages sur les circuits intégrés analogiques et numériques.

Chapitre II :

Evolution historique de la CEM des circuits intégrés et de leur conception

1) Premiers pas de la CEM des circuits intégrés :

L'évolution des circuits intégrés a connu une allure extraordinairement rapide, fait prédit par le grand visionnaire Gordon Moore co-fondateur de Intel Corporation dans sa publication en 1965 qui affirmait que la densité des circuits réalisés sur une même puce doublerait chaque année, et en 1975 la loi dite de Moore a été revue et corrigée à une densité qui doublerait tous les 18 mois. Cette affirmation est toujours vérifiée ce qui donne une idée de la vitesse du progrès en microélectronique et la figure II-1 [2] en donne un bon aperçu.

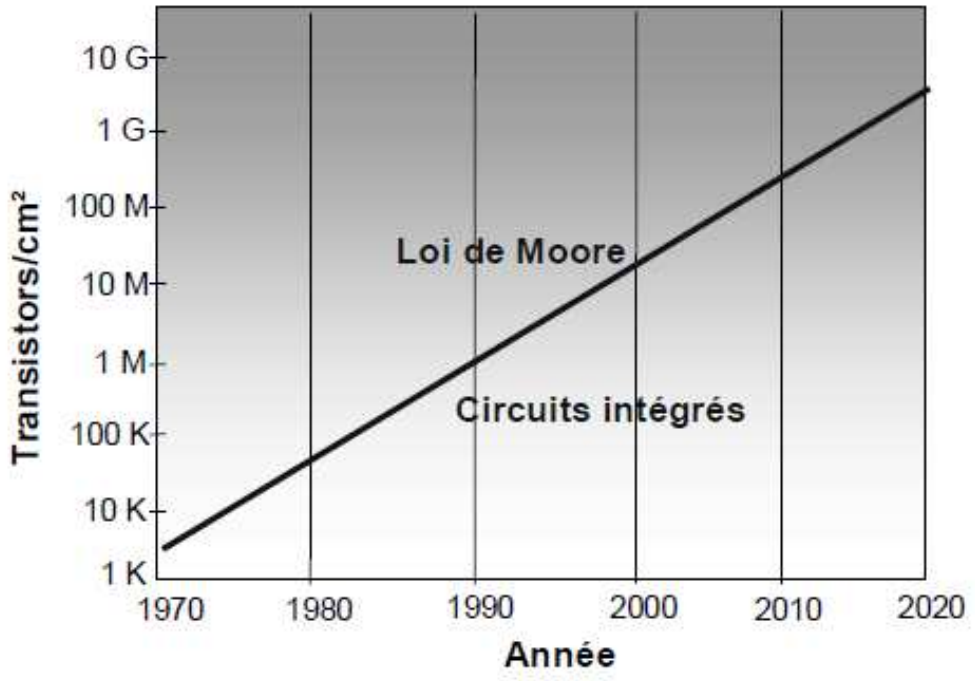


Figure II-1 : Représentation de l'évolution dans la fabrication des circuits intégrés selon la loi de Moore.

Les premiers travaux traitant le problème de compatibilité électromagnétique datent de 1965 et ils ont été conduits par l'armée américaine qui s'est focalisée sur l'étude de l'effet des champs électromagnétiques créés lors d'une explosion nucléaire sur les dispositifs électroniques utilisés sur des sites de lancement de missiles. IBM prît le relais en développant le logiciel de simulation SPECTRE en 1967 qui visait à reproduire les effets d'une explosion nucléaire sur les composants électroniques.

Des techniques se développèrent pour la protection des équipements électroniques du couplage avec les émetteurs de radio et de télévision, les radars ou encore les explosions nucléaires. Plusieurs normes militaires ont été publiées aux Etats-Unis telles que la BE Mil-STD (Military Standard) 461 qui a fixé les limites d'interférence à ne pas dépasser pour les équipements électroniques, et la Mil-STD 462 qui a détaillé les méthodes de mesure des interférences.

Une des premières publications académiques (et donc dans le cadre civil) traitait l'amplificateur opérationnel intégré 741. C'est Wooley qui, en 1971, simula avec succès les différents étages de ce circuit intégré en utilisant le logiciel CANCER.

James J. Whalen, professeur à l'université de l'état de New York, était un pionnier dans le domaine de la compatibilité électromagnétique des circuits intégrés. En 1975, il publia des études sur la susceptibilité de transistors discrets aux impulsions en fréquence radio. Dans un article, Whalen a parlé de l'intérêt de l'étude sur le risque d'interférences entre des sources d'ondes électromagnétiques utilisant la bande VHF (30 MHz – 300 MHz), la bande UHF (300 MHz – 3 GHz) ou encore dans la bande EHF avec les radars travaillant dans la bande XHF (3 GHz – 30 GHz).

L'IEEE posa le problème des effets éventuellement néfastes des rayonnements en fréquence radio sur les circuits intégrés et la prédiction de leur comportement par le moyen d'outils de simulation. Ainsi, le besoin de modifier les modèles des dispositifs à semi-conducteurs en tenant compte de ces conditions exceptionnelles (exposition aux rayonnements électromagnétiques en fréquence radio) fut exprimé par C. E. Larson en 1979, qui a proposé alors une modification du modèle du transistor bipolaire.

Un an plus tard, Chen et Whalen proposèrent un macro-modèle afin d'accélérer les simulations, une idée qui fut utilisée par beaucoup d'autres ingénieurs et scientifiques, car elle permettait un temps de simulation acceptable tout en traitant des circuits assez complexes.

Des méthodes de mesure de l'immunité aux fréquences radio ont été définies en 1981 par Bersier de Swiss Telecom, peu après, une méthode, peu coûteuse, pour tester l'immunité aux fréquences radio des produits audio et vidéo fut développée.

La première analyse de susceptibilité des composants MOS fut publiée en 1980, où J.N. Roach a pu caractériser la sensibilité de mémoires NMOS de 1 ko. Quelques années plus tard, une étude fut publiée par Tront traitant le comportement du processeur 8085 d'Intel en présence d'ondes électromagnétiques de fréquences comprises entre 100 et 200 MHz. Il utilisa le logiciel SPICE pour reproduire un nombre de phénomènes observés pendant la mesure. La figure II-2 [1] en montre un exemple.

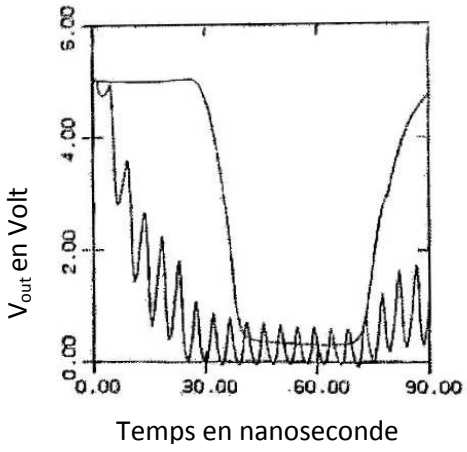


Figure II-2 : Simulation à 200 MHz d'une sortie perturbée et une sortie non perturbée du processeur Intel 8085

Des circuits Watchdog ont été ajoutés aux microprocesseurs dès 1982 qui se sont avérés très efficaces. Ils récupèrent des erreurs et en effectuant des remises à zéro (redémarrage ou encore reset en anglais) des données et en réexécutant les programmes depuis le début. Ainsi, vu la rapidité d'exécution de tels circuits, les erreurs passeraient inaperçues.

2) Recherches sur la CEM des circuits intégrés effectuées entre 1990 et 1995 :

En 1990, Bakoglu rassembla une importante compilation sur les effets parasites à l'intérieur des circuits intégrés, l'effet des boîtiers et les effets sur les circuits imprimés. Il dériva plusieurs problèmes liés aux courants transitoires présentés aux fronts montants et descendants de l'horloge tout en détaillant les mécanismes de résonance dans les circuits intégrés. Des modèles sur les boîtiers ont été décrits pour les boîtiers DIL (Dual In Line), QFP (Quad Flat Pack) et les familles PGA (Pin Grid Array).

Simultanément (en 1990), Kenneally présenta des résultats de mesure pour des circuits intégrés simples réalisés en technologie CMOS et TTL. Des différences significatives ont été remarquées, du point de vue CEM, pour les technologies CMOS et TTL : dans tous les cas (en comparant le même circuit réalisé avec les deux technologies) les circuits CMOS avaient tendance à être moins résistants que les circuits TTL. En tant qu'étudiant en Ph.D. à l'université de Toronto, Laurin publia, en 1991, une étude sur les effets des perturbations radioélectriques sur les circuits oscillateurs utilisés dans le processeur Motorola 6809. En plaçant une boucle de courant très près de l'oscillateur, il observa des fluctuations du signal horloge, des dysfonctionnements dans certaines des fonctions du microprocesseur ainsi que des pertes de données transmises en série dans le bus de données.

En 1993, Tang, de l'université de Singapour, montra que les interférences électromagnétiques pouvaient causer des erreurs de calcul dans les microprocesseurs. Il effectua des mesures sur leur susceptibilité aux émissions conduites et rayonnées. Finalement, Il put illustrer un problème de permutation de bits dans l'octet dont le poids est le plus fort d'un compteur, induisant ainsi à des erreurs de calculs graves. Des solutions logicielles ainsi qu'un tracé du circuit imprimé et une disposition des composants plus judicieuse furent proposés. L'auteur fit remarquer que les systèmes à faible vitesse étaient aussi vulnérables aux interférences électromagnétiques que les systèmes à grande vitesse.

Beaucoup d'ouvrages sur la CEM des circuits imprimés furent publiés au début des années 1990, la majorité des livres publiés avaient un aperçu rapide sur les problèmes de CEM des circuits intégrés. Dans le chapitre 3 de son livre « Principles and application of EMC » publié en 1990, Weston compara les différentes caractéristiques de commutation de plusieurs familles de circuits intégrés ainsi que l'incidence de ces commutations sur les émissions conduites et rayonnées .Une étude fut publiée par Graffi, en 1991, sur le comportement de l'amplificateur opérationnel 741 en présence d'interférences de fréquences variant de 200 KHz à 50 MHz. Ainsi, des résultats très corrélés à ceux de la mesure ont été obtenus avec une simulation à l'aide d'un macro-modèle simplifié.

Le bruit de commutation simultanée est l'une des plus grandes préoccupations des ingénieurs de compatibilité électromagnétique. L'une des toutes premières publications sur le sujet

remonte à 1993, qui traitait la caractérisation des effets des capacités de découplage à l'intérieur de la puce et au voisinage du circuit intégré.

3) Etudes publiées à partir de 1995 sur la susceptibilité des circuits intégrés :

Les effets d'une onde électromagnétique couplée à un circuit imprimé et les conséquences de ce couplage sur de simples circuits, furent analysés par Laurin en 1995. Il ne remarqua aucune anomalie dans le fonctionnement des composants exposés à des champs allant jusqu'à 200 V/m. Cependant, l'ajout d'un fil long d'une moitié de longueur d'onde (la référence est l'onde responsable des interférences) causait des dysfonctionnements graves pour des champs d'intensités ne dépassant pas 2 V/m.

En 1997, Chappel discuta la possibilité de « durcir » les circuits intégrés. Il s'agit de les rendre résistants aux interférences électromagnétiques en utilisant des techniques spécifiques pouvant augmenter le niveau d'immunité de certains circuits intégrés, de 1,5 V à plus de 5 V, dans un domaine de fréquence allant de 1 à 10 MHz.

En 1998, Hattori démontra les avantages des simulations dans le domaine fréquentiel sur celles effectuées dans le domaine temporel. Cette approche s'avéra très efficace pour l'obtention de la réponse des circuits analogiques très rapidement.

En 2000, une version mise à jour de « Integrated Circuit Electromagnetic Immunity Handbook » fut publiée par la NASA donnant ainsi des informations de grande valeur sur les niveaux d'immunité de circuits intégrés simples pour des fréquences allant jusqu'à 10 GHz.

Avec l'expérience acquise dans divers microprocesseurs et microcontrôleurs, quelques ingénieurs ont commencé à développer des stratégies visant à « durcir » les systèmes à base de microprocesseurs. En 1997, Coulson identifia les points vulnérables de circuits spécifiques tels le contrôleur d'alimentation ou le Watchdog, et proposa également quelques techniques logicielles telles que la vérification de l'intégrité des mémoires et le codage redondant. En 1998, Campbell prétendit que par de simples techniques de programmation logicielle défensive, l'immunité d'un microcontrôleur pouvait être augmentée significativement.

Une étude publiée par Ong, en 2001, traitant l'efficacité des techniques logicielles sur la CEM a montré que certains des logiciels dits défensifs (defensive softwares) se sont avérés inefficaces et leur utilisation reste limitée à certains cas particuliers seulement. Par contre, l'utilisation de la commande NOP (No OPeration) pour combler l'espace mémoire programme inutilsé, semblait avoir un impact positif sur le fonctionnement général de n'importe quel système à microprocesseur ou à microncontrôleur.

4) Etudes publiées à partir de 1995 sur les émissions parasites des circuits intégrés :

En 1995, Goodman publia des résultats d'une comparaison entre les mesures et les simulations de la propagation du signal dans les PGA (Pin Grid Arrays). Il montra que les effets non désirables dépendaient du type des pins du boîtier. Il utilisa pour cela dans sa modélisation, de simples éléments R, L et C mais pour des fréquences assez importantes.

A côté des éléments R, L et C discrets utilisés pour modéliser les pins du boîtier, il y a les bondings (représentés dans la figure II-3) et les structures entrée/sortie intégrées. Il utilisa les lignes de transmission pour représenter les pistes du circuit imprimé ce qui a valu à son modèle d'être validé jusqu'à 4 GHz.

Figure II-3 : Représentation au microscope électronique d'un bonding.

La complexification continuelle des circuits intégrés impose l'utilisation de boîtiers dont la densité des pins et la bande passante sont en croissance inévitable. Ainsi à titre d'exemple, en 1996, McCredie a modélisé avec succès le bruit de commutation d'un ASIC (Application Specific integrated Circuit), monté sur un BGA (Ball Gate Array) compact dont le nombre de pins d'entrée/sortie est d'environ 1000, en utilisant les modèles des sources de courant distribuées, des capacités de découplage tant au niveau de la puce qu'au niveau du boîtier ainsi que le modèle des inductances de connexion séries. La même année, T. Williams publia un livre très pratique sur les contraintes de la CEM avec un chapitre dédié aux circuits intégrés. Aux États-Unis, la SAE (Society for Automotive Engineering) a proposé une méthode de mesure des émissions rayonnées des circuits intégrés en utilisant la cellule TEM.

D'intéressantes études comparatives furent publiées par Slattery, en 1997, portant sur les microcontrôleurs de 8 et 16 bits en caractérisant l'impact des technologies de fabrication (des circuits intégrés), des boîtiers et de la température sur le spectre d'émission.

En 1998, Robinson compara les émissions rayonnées de plusieurs familles de circuits logiques et des résultats furent obtenus pour des inverseurs et des NAND appartenant à des familles telles que : ACT (Advanced CMOS-TTL), FCT (Fast speed CMOS), HC (High speed CMOS) et HCT (High speed TTL-CMOS).

En 1998, Jonghoon présenta des mesures avec une cellule TEM d'un microprocesseur complexe avec et sans capacité de découplage locale, ainsi on a pu observer l'avantage de la capacité de découplage au niveau de la puce sur la réduction des perturbations.

Plusieurs travaux publiés confirmaient que la réalisation de grandes capacités, à l'intérieur des circuits intégrés, de valeurs de 1 à 50 nF en fonction de la technologie et de la taille de la puce, était un moyen très efficace de réduire les émissions.

En 2000, Van Wershoven a montré également qu'en agissant sur le temps de montée (ou de descente) on pouvait réduire les émissions. En 2000, Une autre approche a été suggérée par Kim Soo-Hyung qui a analysé l'impact des matériaux absorbants et a observé une réduction du niveau des harmoniques de 3 dB à 20 dB pour des fréquences dépassant 300 MHz.

Le scanneur de champ (Near-Field Scanner) proche fut adapté au problème de la CEM des circuits intégrés, en 1995, par K. Slattery de Chrysler Corporation. En 1999, il réussît à fabriquer un scanneur de champ proche avec une sensibilité remarquable pouvant ainsi faire une représentation assez précise du champ au dessus du boîtier d'un circuit intégré. En effet, beaucoup de laboratoires de recherche impliqués dans l'étude la CEM au niveau puce, utilisent des scanneurs de champ proche basés sur le modèle conçu par Slattery.

❖ **Quelques idées proposées pour la réduction des émissions des circuits intégrés :**

Hardin et ses collègues, de Lexmark Corporation, ont été probablement les premiers à proposer l'idée de réduire les pics d'émission des harmoniques de la fréquence d'horloge en variant la période du signal d'horloge de façon contrôlée. Des résultats expérimentaux confirmant la pertinence de cette idée ont été publiés par Slattery, en 2001, qui montraient clairement une réduction sensible des rayonnements avec la méthode décrite précédemment.

Une seconde idée visant à réduire les émissions des circuits intégrés, est l'utilisation des systèmes asynchrones. En effet, une étude publiée par Furber, en 1999, a montré une réduction significative des pics des harmoniques (autour de 180 MHz), même pour des fréquences relativement élevées pour la version asynchrone du processeur ARM60.

5) Standardisation de la CEM des circuits intégrés :

Un nombre important de règles furent légiférées par la Communauté Européenne en 1996, ce qui a probablement redonné de l'élan aux chercheurs et aux ingénieurs concernés par la CEM, surtout en Europe. Les lois européennes fixaient des limites au-delà desquelles il faut éviter des émissions parasites, d'autre part, des bornes, cette fois-ci, minimales devant être respectées en termes d'immunité pour la plupart des produits électroniques.

Au niveau composant, les standards les plus importants ont été développés sous la supervision de l'IEC (International Electrotechnical Commission) qui se charge de contrôler une importante activité de standardisation via plus de 100 comités techniques. Un de ces comités, nommé Technical Commitee 47A, s'est focalisé sur la CEM des circuits intégrés dès 1990. Le rôle de ce comité était de préparer des standards sur les circuits logiques, les mémoires, les convertisseurs et les modules hybrides.

❖ **Standardisation des méthodes de mesure pour l'évaluation de la CEM :**

Plusieurs méthodes de mesure des émissions et de l'immunité électromagnétiques furent développées par plusieurs pays, principalement en France, Allemagne, Italie, Pays-Bas, aux Etats-Unis et au Japon. La création de ces méthodes de mesure a été conduite par l'industrie automobile, qui souffrait notamment des interférences électromagnétiques dues au nombre croissant des dispositifs électroniques embarqués dans les voitures.

La SAE (Society of Automotive Engineers) a proposé une méthode utilisant une cellule TEM (un exemple d'une cellule TEM est illustré ci-dessous en figure II-4) pour mesurer les émissions rayonnées.

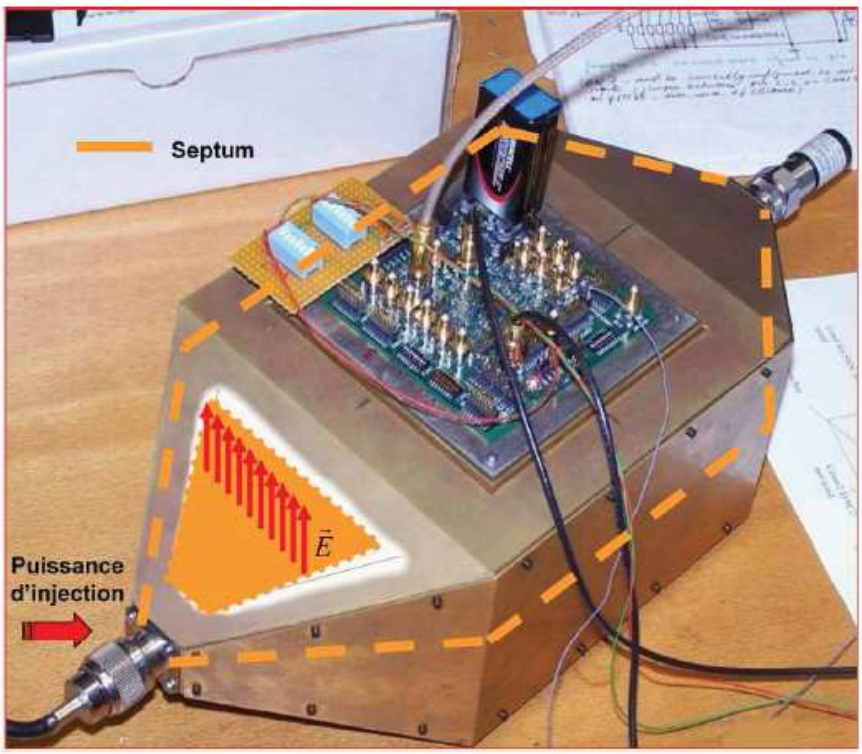


Figure II-4 : Illustration d'une cellule TEM.

Un groupe néerlandais a proposé une méthode basée sur le WBFC (Workbench Faraday Cage –voir figure II-5–) et un groupe allemand de standardisation a proposé une méthode de mesure des perturbations conduites en utilisant une résistance de 1 Ω en série le composant (à tester) reliés à la masse.

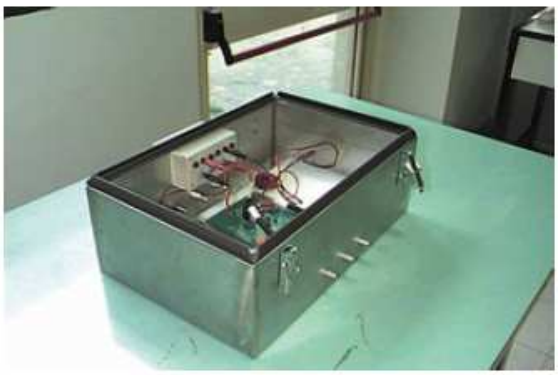


Figure II-5: Photo du Workbench Faraday Cage.

En octobre 1997, le sous-comité 47A de l'IEC a décidé de créer un groupe de travail (Working Group WG9) pour analyser les méthodes de mesure suggérées pour les circuits intégrés. Après une discussion approfondie, il a été décidé de créer une « boîte à outils » (tool box) de cinq méthodes pour évaluer la CEM des circuits intégrés : La mesure par une cellule TEM, la technique de scan surfacique, la méthode 1Ω/150Ω, la technique de mesure utilisant la WBFC (Workbench Fraday Cage) et la méthode utilisant une sonde magnétique.

6) Evolution des circuits intégrés et état de l'art de leur fabrication:

La lithographie a connu des avancées extraordinaires au cours des ces dernières années rendant possible la construction de circuits intégrés travaillant dans le domaine du GHz. Les progrès essentiels ont eu lieu notamment dans la réduction de la taille du canal du dispositif MOS, ainsi que dans la multiplication des couches d'interconnexion. Ceci est illustré par la figure II-6 [1] où on voit une portion d'un layout (disposition et façon dont les composants sont connectés à l'intérieur du circuit intégré) réalisé selon la technologie 0,8 µm de 1990 (à gauche) et une portion d'un layout réalisé en miniaturisation 90 nm réalisé en 2005.

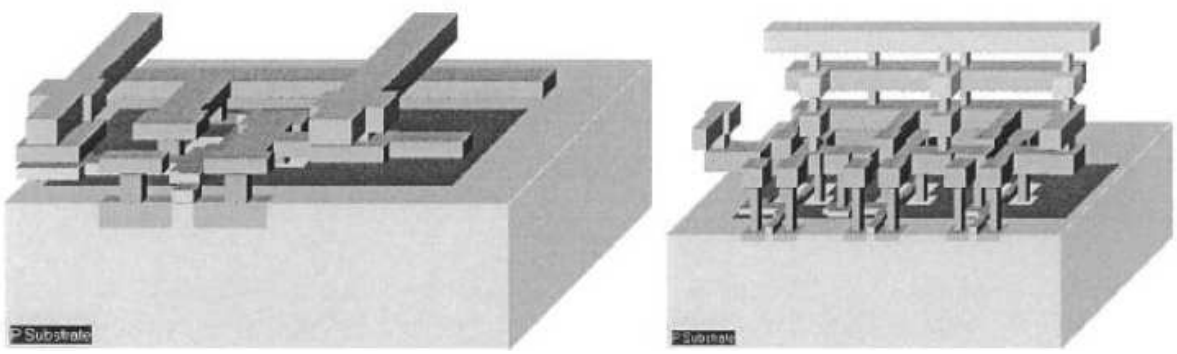


Figure II-6 : Evolution des technologies de fabrication des circuits intégrés CMOS de 0,8µm avec deux couches d'interconnexions en 1990 à 90 nm avec huit couches d'interconnexions en 2005.

Les besoins croissants d'une miniaturisation poussée, de la réduction de la consommation des circuits intégrés et de l'amélioration des services proposés par les industriels ont induit à des avancées « sans limites » et une intégration de plus en plus importante.

Un circuit intégré se compose d'une puce (die en anglais) en silicium dont la surface est, en générale, autour de 1 cm^2 dans le cas des microprocesseurs et des mémoires. Le circuit intégré est monté sur un boîtier (voir figure II-7) qui est placé sur un circuit imprimé (PCB en anglais). La partie dite active du circuit intégré est une portion de la puce dont l'épaisseur est très fine.

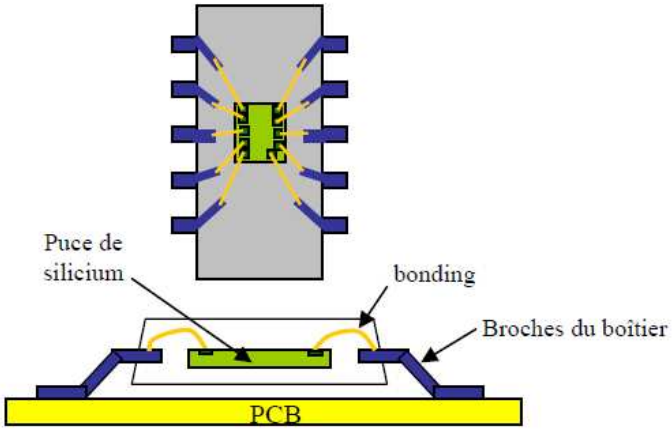


Figure II-7 : Blocs constitutifs d'un circuit intégré standard.

La figure II-8 [15] décrit l'évolution de la complexification des microprocesseurs Intel en termes du nombre de transistors. Le processeur Pentium IV tel qu'il est produit en 2003 comporte environ 50 millions de transistors MOS intégrés dans une seule pièce de silicium de surface ne dépassant pas 4 cm^2.

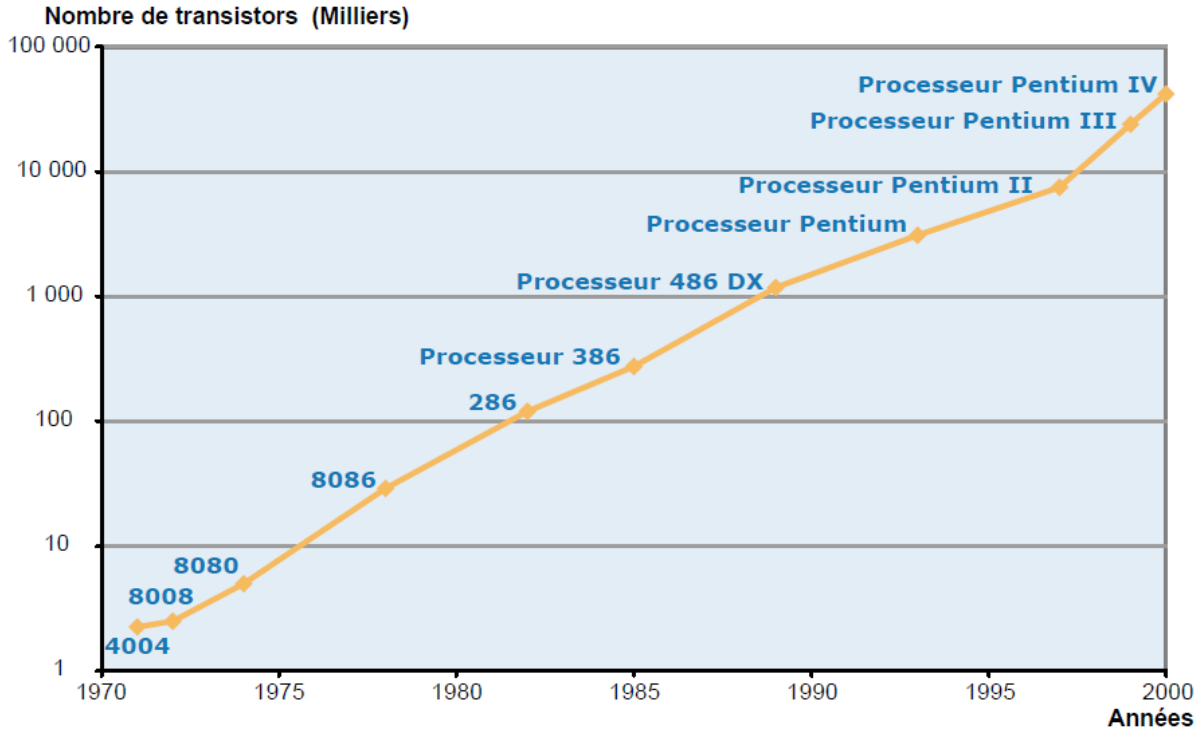


Figure II-8 : Evolution au cours des années du nombre de transistors intégrés dans les microprocesseurs Intel.

La fabrication des ordinateurs (personnels) requiert l'utilisation de microprocesseurs cadencés à des fréquences élevées ce qui induit à une consommation plus importante (30 Watts pour la

génération du Pentium IV). L'industrie automobile requiert également des contrôleurs embarqués de plus en plus sophistiqués en termes de fonctionnalités, les mémoires exigées ont des capacités de plus en plus grandes et les fréquences de travail sont en augmentation également constante.

Il y a quatre générations importantes de circuits intégrés (du point de vue taille), ce sont les technologies micrométriques (micron), sous-micrométriques (submicron), sous-micrométriques profondes (deep submicron) et sous-micrométriques ultra profondes (deep submicron). L'ère sous-micrométrique a débuté en 1990 avec la technologie 0,8 µm, quant à la technologie sous-micrométrique profonde (deep submicron technology), elle a vu le jour en 1995, elle concernait notamment les circuits intégrés fabriqués en dessous des 0,1 µm. Les nanotechnologies sont apparues en 2004 avec la technologie CMOS 90 nm, suivi de 65 nm. Les technologies nanométriques profondes (deep nano-scale technologies) devraient inclure les tailles allant jusqu'à 32 nm ou encore 22 nm à partir de 2010 (entre 2010 et 2013 probablement).

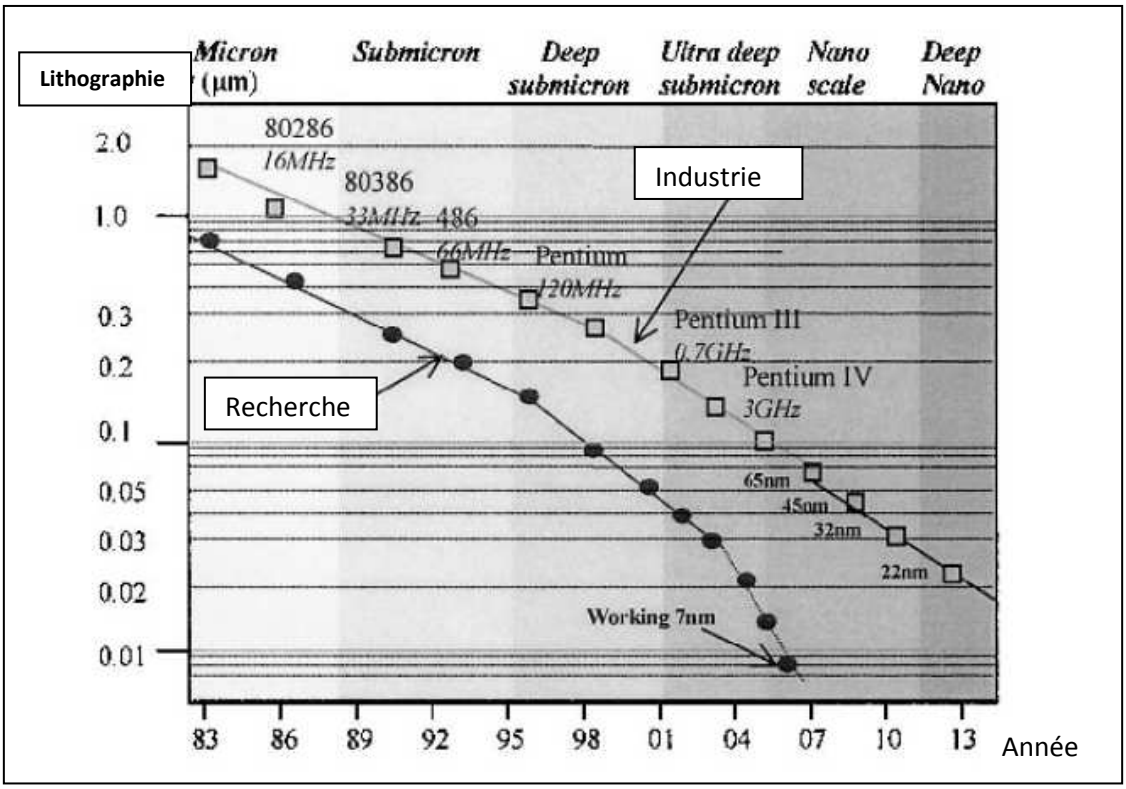


Figure II-9 : L'évolution de la lithographie.

Dans la figure II-9 [1] on remarque que la recherche a toujours eu au moins cinq ans d'avance sur la production industrielle, on peut également mettre l'accent sur la tendance vers une miniaturisation de plus en plus poussée, une tendance qui s'est accélérée depuis 1996.

La lithographie est exprimée en µm et correspond au plus petit modèle qui puisse être réalisé sur la surface d'un circuit intégré. La conséquence évidente du progrès de la lithographie est la possibilité de réaliser des fonctions identiques sur des surfaces de plus en plus petites. De surcroît, le nombre de couches métalliques utilisées comme interconnexions a augmenté constamment au cours des dix dernières années. Plus de couches pour le routage signifie une utilisation plus efficace de la surface de silicium à travailler. Les surfaces actives, i.e. les composants MOS, peuvent être juxtaposées et rapprochées s'il y a plusieurs couches de routage.

Une densité plus importante induit à deux améliorations notables : La réduction de la surface du silicium qui va avec une diminution de la capacité parasite des jonctions et des interconnexions, ainsi on peut augmenter la vitesse de commutation des cellules. En deuxième lieu, plus les dimensions des dispositifs sont petites, plus on peut augmenter la fréquence de travail (fréquence d'horloge plus importante).

D'autre part, quand une porte (logique) commute, une petite impulsion de courant se crée principalement sur les lignes d'alimentation. La superposition de ces petites impulsions élémentaires de courant donne naissance a des courants d'amplitude pouvant atteindre 100 A dans le cas des microprocesseurs de haute performance !

L'augmentation de la fréquence, de la complexité des circuits et du nombre d'entrées/sorties aggrave le problème d'interférence et des émissions parasites conduites et rayonnées.

Quant aux wafers (fines disques de silicium sur lesquels sont fabriqués les transistors en masse) de silicium, leurs dimensions ont constamment augmenté grâce aux avancées technologiques. Un diamètre plus grand signifie la fabrication simultanée d'un nombre plus important de puces mais d'un autre côté ces technologies requièrent des équipements extrêmement chers.

7) Evolution technologique des boîtiers:

Les boîtiers contenant les circuits intégrés ont connu également des progrès considérables afin d'augmenter le nombre d'entrées/sorties. Du tout premier DIL (Dual-In-Line) au Chip-Scale Packaging, le tableau de la figure II-10 donne un aperçu comparatif des différents boîtiers ; et à titre d'exemple, on cite les boîtiers les plus utilisés pour les microprocesseurs qui sont les technologies BGA (Ball-Gate-Array) et FBGA (Fine pitch Ball Gate Array technology).

Le circuit intégré est en général connecté au boîtier par l'intermédiaire d'un bonding en or ou de « boules de soudure » (solder balls) qui est une technologie très utilisée dans les microprocesseurs cadencés à de grandes vitesses , les figures II-11 et II-12 en donnent une bonne illustration.

Comme la complexité des circuits intégrés est en augmentation, un nouveau type de liaison (entre la puce et le boîtier) a été inventé rendant possible la création de toutes les connexions entre la puce et le boîtier en une seule étape. Cette technologie, appelée Ball Grid Array, a été introduite il y a quelques années et maintenant, elle est couramment utilisée pour la fabrication des circuits intégrés de plus de 200 broches.

Le boîtier est utilisé comme une matrice de routage des pads (voir le figure II-11) des circuits intégrés (pas de 100 µm environ) aux boules de liaisons (Ball Gate Array de pas compris entre 500 µm à 2 mm). Ce boîtier est un réseau complexe de conducteurs très fins en cuivre à l'intérieur d'un isolant. Le substrat du BGA (Ball Gate Array) peut comporter 2 à 6 couches de métal servant de routeurs pour différents signaux ainsi que pour l'alimentation de tout le circuit. La tendance vers un rétrécissement des leads réduit « l'effet antenne » du boîtier, donc minimise les émissions parasites ; et d'un autre côté, elle contribue à la réduction des couplages avec des ondes incidentes ce qui améliore l'immunité du dispositif aux interférences.

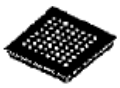
Boîtier	Désignation	Nombre d'entrées/sorties
	Dual In Line (DIL)	40
	Shrink Dual In Line (SDIL)	100
	Small Outline Package (SOP)	100
	Quad Flat Pack (QFP)	250
	Ball Gate Array (BGA)	1000
	Fine Pitch Ball Gate Array (FBGA)	3000
	Chip Scale Package (CSP)	>5000

Figure II-10 : Nombre d'entrées/sorties des boîtiers les plus courants.

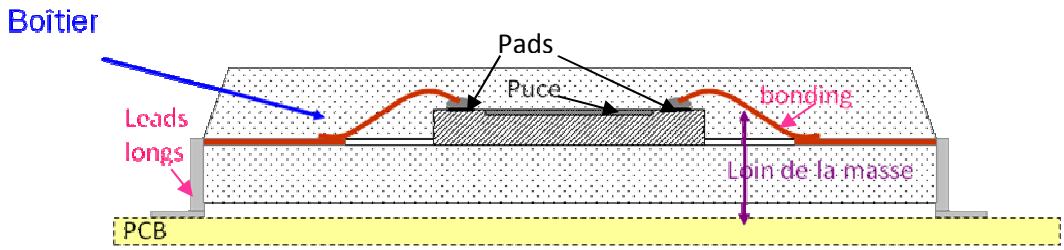


Figure II-11 : Différentes parties d'un circuit intégré protégé par un boîtier.

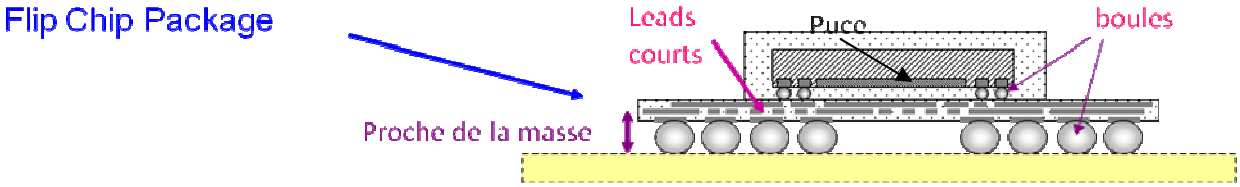


Figure II-12 : Illustration d'un boîtier lié à la puce par des boules de soudure (solder balls), technologie couramment utilisée dans les microprocesseurs.

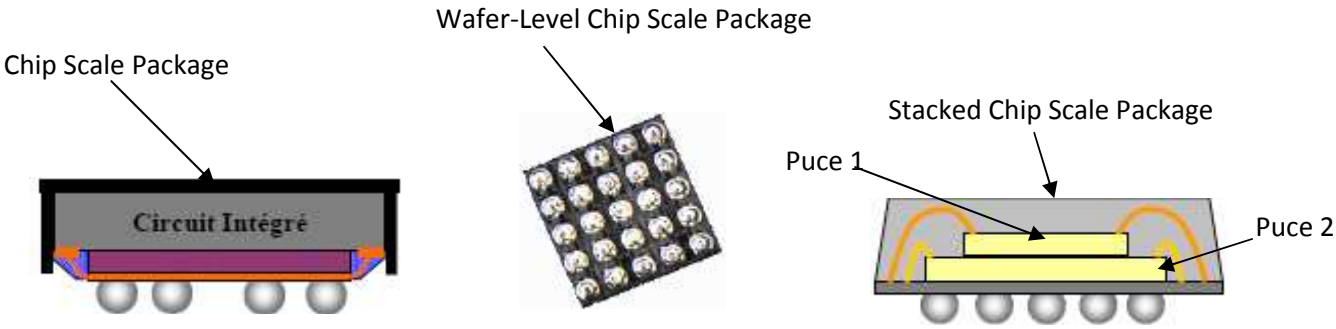


Figure II-13 : Quelques types de boîtiers CSP (Chip Scale Package).

Les boîtiers CSP (voir la figure ci-dessus) permettent de relier directement la puce au circuit imprimé sans passer par le substrat du boîtier. La puce est montée en sens inverse (vers le bas au lieu du haut comme dans d'autres types de boîtiers) et est électriquement connectée au circuit imprimé par le moyen de « boules de soudure » (solder balls). Cette technologie permet d'éliminer significativement l'effet antenne, donc les émissions et la susceptibilité de tels circuits intégrés se trouvent relativement diminués. Cependant, la puce elle-même, se comporte comme une antenne pour des fréquences bien au-delà du GHz.

Pour réduire encore la surface des systèmes électroniques, on recourt à l'empilement (stacking) des circuits intégrés à l'intérieur d'un seul et unique boîtier (voir Stacked CSP dans la figure ci-dessus). L'objectif d'une telle technique est de compacter davantage les systèmes

électroniques, mais d'un autre côté, elle impose des techniques d'assemblage plus complexes et crée des problèmes de fiabilités et de dissipation thermique plus importants.

8) Evolution des problèmes de la CEM des circuits intégrés :

Le besoin de caractériser la CEM des circuits intégrés a été accentué par les exigences, d'une part, des fabricants des circuits à semi-conducteurs et les consommateurs, et d'autre part, de la tendance affichée par l'évolution technologique.

La miniaturisation des applications électroniques portables contraint à réduire les espaces et à rapprocher les circuits les uns des autres, augmentant ainsi le risque d'interférences électromagnétiques entre les circuits. Parallèlement à cette miniaturisation des circuits intégrés, le développement croissant d'applications sans fils émettant principalement dans les bandes VHF (30MHz – 300MHz) et UHF (300MHz – 3000MHz) ont rendu l'environnement électromagnétique des circuits intégrés de plus en plus pollué. La figure II-14 décrit l'occupation du spectre radiofréquence. Les sources de pollution électromagnétique sont nombreuses et leur niveau d'émission peut être suffisant pour induire des comportements anormaux ou des défaillances dans les circuits intégrés environnants.

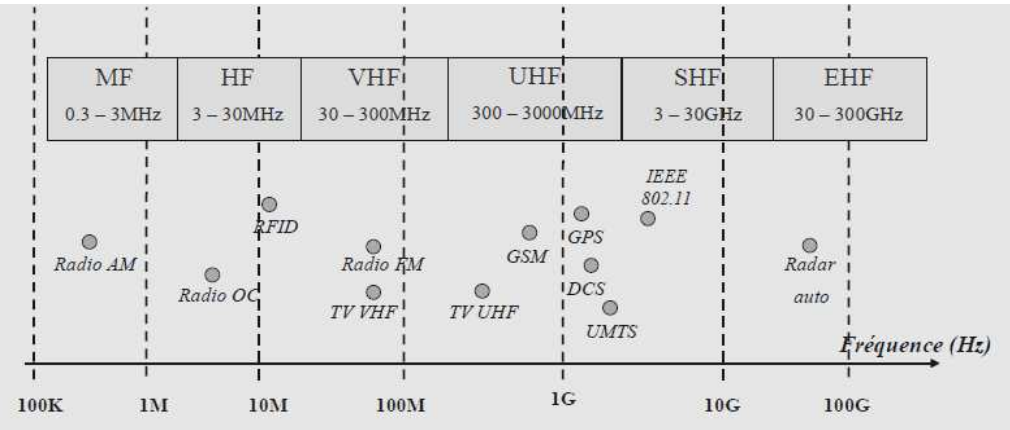


Figure II-14 : Occupation du spectre de fréquence.

En outre, la tendance actuelle dans le domaine des systèmes embarqués est la plus électrique, notamment dans l'aéronautique. Il s'agit de remplacer par exemple des systèmes pneumatiques et hydrauliques par des systèmes électriques, permettant ainsi des économies de poids et d'énergie. Cependant, un des problèmes de cette nouvelle tendance est d'assurer une haute compatibilité électromagnétique des systèmes électroniques.

Toutes ces raisons obligent les fabricants de circuits intégrés et de systèmes électroniques à réduire l'émission et la susceptibilité de leurs produits et à être en mesure d'apporter des solutions efficaces visant à les rendre robustes dans des environnements de plus en plus sévères.

Conclusion :

Dans ce chapitre, nous avons évoqué les débuts de la compatibilité électromagnétique, domaine, comme nous l'avons vu, initialement exploré par l'armée américaine. Nous avons également cité quelques points résumant l'évolution de la compatibilité électromagnétique au cours des années 1990. En effet, les contraintes et enjeux devenaient de plus en plus importants, ce qui a valu à la compatibilité électromagnétique des circuits intégrés de s'être dotée de normes. Enfin, nous avons évoqué l'évolution de la miniaturisation des circuits intégrés, des techniques de leur fabrication et de leurs boîtiers.

Les problèmes de la compatibilité électromagnétiques deviennent de plus en plus délicats, et leur résolution est une condition nécessaire pour qu'un système électronique ait un fonctionnement normal. Les chapitres suivants donneront une idée des précautions et des techniques employées pour résoudre les problèmes rencontrés en CEM des circuits intégrés.

Chapitre III :

Solutions générales pour améliorer la CEM des circuits intégrés

Introduction :

Avant de concevoir des circuits intégrés, il faut penser à leurs émissions et à leur capacité à résister aux attaques électromagnétiques extérieures. Il existe des techniques qui permettent, si elles sont prises en considération à la conception des circuits intégrés, d'améliorer leur compatibilité électromagnétique. Dans ce chapitre, ces techniques seront abordées et elles devront répondre aux deux questions fondamentales posées aux ingénieurs de compatibilité électromagnétique :

- Comment construire un circuit intégré qui rayonne le moins possible ?
- Comment concevoir un circuit intégré qui résiste le mieux aux perturbations externes ?

Ce chapitre va tenter d'apporter des réponses à ces deux questions et devra permettre de construire des systèmes plus robustes et moins bruyants.

1) Solutions pour affaiblir les émissions électromagnétiques des circuits intégrés :

Les émissions d'un circuit intégré sont liées à trois sources indépendantes : le courant d'alimentation du cœur du circuit intégré, le bruit du substrat et les courants d'entrée(s)/sortie(s). En agissant sur ces sources, en réduisant ces pics de courant, on arrivera à réduire les émissions des circuits intégrés.
Les solutions qui seront présentées concerneront :

- ✓ Le bruit d'alimentation (du cœur du circuit intégré).
- ✓ Les bruits liés aux boîtiers.
- ✓ Les capacités de découplage.
- ✓ Le bruit des entrées/sorties.

1-1) Solutions relatives au bruit d'alimentation (du cœur) :

Dans le domaine temporel, le courant d'alimentation observé dans les mesures est constitué de pics instantanés dont l'amplitude est beaucoup plus importante que la valeur moyenne du courant. Le bruit d'alimentation peut être minimisé soit en réduisant les pics de courant, soit en diminuant la fréquence de travail.

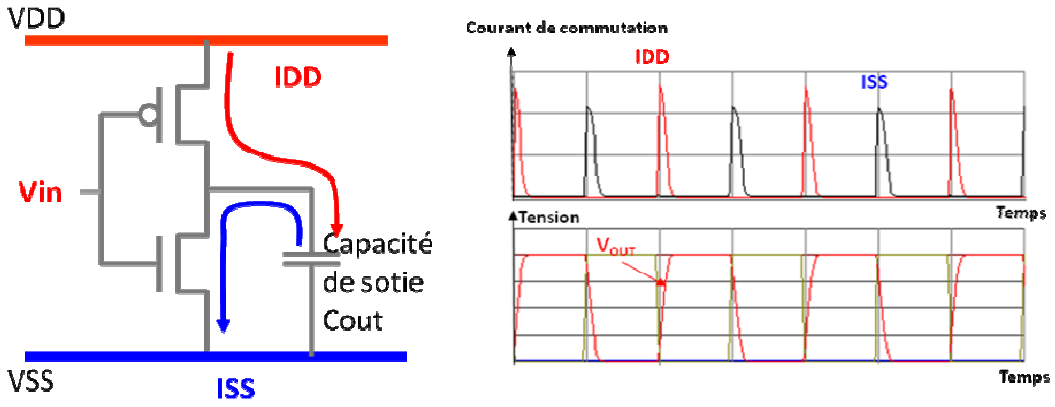


Figure III-1 : Représentation des pics de courant présents dans les pins d'alimentation.

1-1-1) Remèdes aux pics de courant dans les circuits numériques synchrones :

❖ **Distribution du signal d'horloge :**

Il est évident que, en se rapportant aux équations de Maxwell, les pics de courants, une fois véhiculés à l'extérieur du circuit intégré, ont un impact direct sur les émissions conduites et rayonnées. A l'intérieur un circuit intégré, toute horloge, buffer ou oscillateur inutilisés doivent être transparents, i.e., arrêter leur alimentation. Dans les circuits synchrones, le signal d'horloge peut être réparti à travers des « arbres d'horloges » (clock trees en anglais). Cette appellation d'arbres d'horloge est justifiée, puisque comme à l'instar d'un arbre, le signal est ramifié et subdivisé (figure III-2).

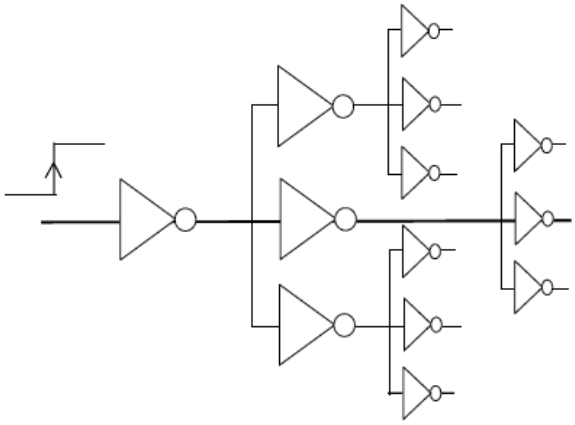


Figure III-2 : Distribution du signal d'horloge.

La réduction du rapport di/dt est assurée en subdivisant le signal d'horloge sur un réseau de buffers (voir la figure ci-dessus). D'autre part, il faut veiller à satisfaire les exigences en termes de vitesse et de puissance requise par les buffers.

Pour les oscillateurs embraqués (dans un circuit intégré), on peut réduire leur bruit en transformant leur sortie dont les changements sont brusques en tension en changements lents et sinusoïdaux. Le circuit obtenu générerait la même fonction et son signal sera dénué d'harmoniques. Une autre recommandation serait la réduction de la consommation de la circuiterie à la valeur la plus basse possible. Cependant, des courants forts doivent être utilisés, puisque c'est nécessaire, pour faire démarrer l'oscillation rapidement ; d'un autre coté, l'intensité du courant peut être diminuée afin d'assurer juste le minimum nécessaire pour maintenir l'oscillation.

❖ **Modulation du signal d'horloge :**

En modulant en fréquence le signal d'horloge, on élargit son spectre de fréquence mais l'amplitude de certains pics de courants, relativement gênants, sont réduits (Figure III-3 [7]). Cela vient du fait que la période de l'horloge varie, donc les occurrences des commutations simultanées augmentent ou diminuent. Cela signifie que les appels de forts courants sont également étalés dans le temps, donc dans le spectre fréquentiel.

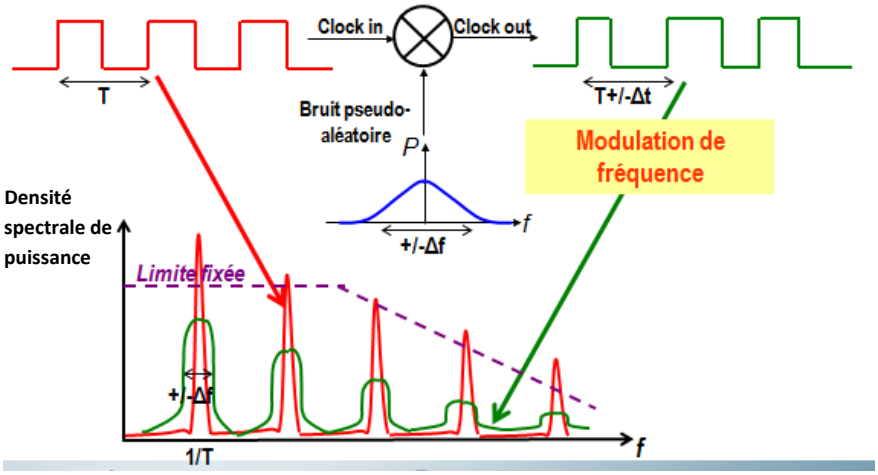


Figure III-3 : Modulation en fréquence du signal d'horloge et ses effets bénéfiques sur les émissions électromagnétiques des circuits numériques synchrones.

1-1-2) Fréquence de travail des circuits numériques synchrones :

La fréquence de travail doit être fixée au minimum qui assurerait l'application à laquelle le circuit intégré conçu est dédié. Par exemple, en cadençant un microcontrôleur à 1 MHz au lieu de 100 MHz permet d'avoir une réduction significative des pics d'émission dans un domaine de fréquence assez large. Ceci est illustré par la figure III-4 [1].

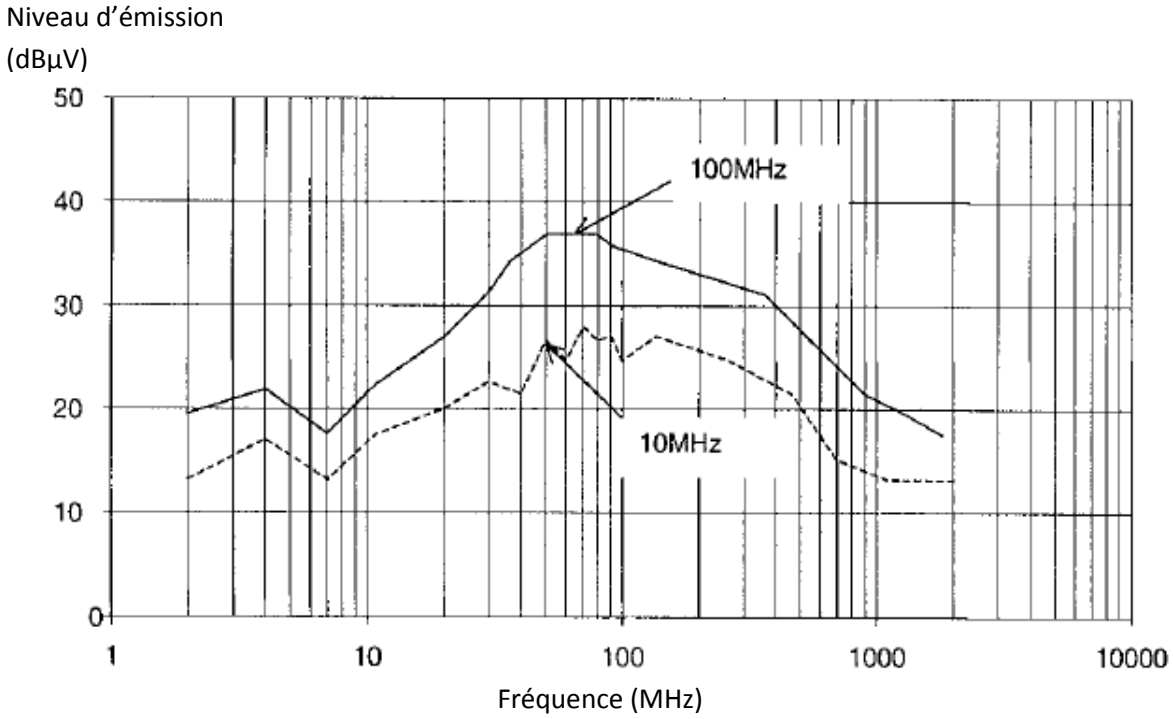


Figure III-4 : Réduction des pics d'émission en réduisant la fréquence de travail d'un microcontrôleur.

1-1-3) Conception de davantage de circuits intégrés numériques asynchrones :

L'étude des circuits asynchrone sera faite en détail dans le chapitre V, cependant nous préférons les aborder, de façon abrégée, afin d'en donner l'idée de base.

Contrairement aux circuits synchrones dont la fonction est organisée par un seul signal, les blocs des circuits asynchrones ne fonctionnent pas simultanément. En effet, tous les blocs envoient un signal (requête) pour indiquer à celui en aval que des données sont disponibles ; et ce dernier l'informe (acquittement) s'il peut « accueillir » les nouvelles données. Ceci réduit le nombre de transistors commutant en même temps, et permet de mettre hors tension tout bloc passif. Par conséquent, leurs émissions électromagnétiques de tels circuits intégrés sont amoindries.

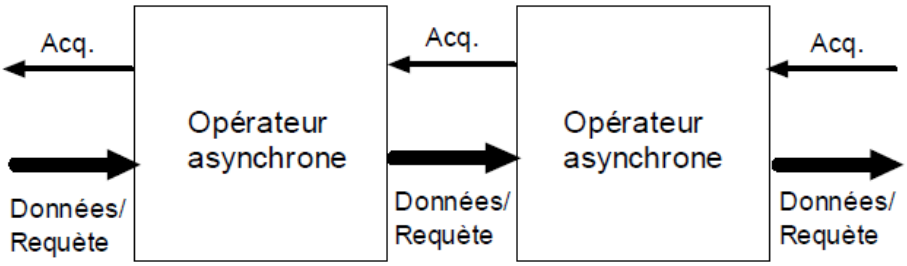


Figure III-5 : Communications entre blocs (opérateurs) asynchrones.

Cependant, des techniques de développement de tels circuits ne sont pas opérationnelles. Donc on peut penser à utiliser les outils de fabrication des circuits synchrones et puis les « asynchroniser » (figure III-6). Cette méthode est également évoquée au chapitre V avec beaucoup plus de détails.

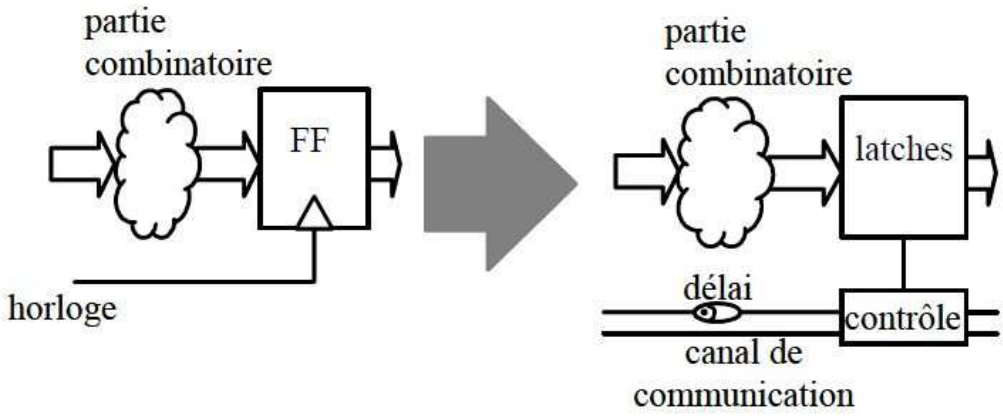


Figure III-6 : Principe général de l'asynchronisation.

Cette méthode consiste à remplacer les blocs synchrones par des blocs équivalents asynchrones, c'est-à-dire, sans signal de commande global mais assurant la même fonction. Comme il sera également expliqué au chapitre V avec plus de détail, on peut toujours diminuer les émissions de ces circuits en répartissant, de façon calculée, les courants consommés.

1-2) Capacité de découplage :

On peut créer une capacité à l'intérieur d'une puce par un couplage capacitif entre les lignes d'alimentation. Ce couplage est favorisé en élargissant les lignes d'alimentation et les rapprochant au maximum. La capacité ainsi créée, permet de réduire considérablement les courants créés lors de la commutation (surtout simultanée) des éléments du cœur du circuit intégré. Dans le cas d'une petite capacité [1], une partie importante du courant circule à l'extérieur du circuit intégré ce qui engendre des émissions conduites et rayonnées importantes (Figure III-7 [1], partie gauche). Par contre, quand une capacité de valeur relativement importante est ajoutée à l'intérieur du circuit intégré (Figure III-7 [1], partie droite), la partie la plus importante du courant circule dans le circuit intégré ; ce qui réduit significativement le bruit créé par la fluctuation de di/dt sur les leads.

Une technique efficace de réaliser une capacité intégrée (à la puce) consiste à l'utilisation de lignes VDD et VSS larges, disposées l'une au dessus de l'autre, pour un effet capacitif maximal. Des valeurs de capacités assez importantes (plusieurs nF) peuvent être réalisées à partir de jonctions métal-isolant-métal (the thin-oxide gate capacitor).

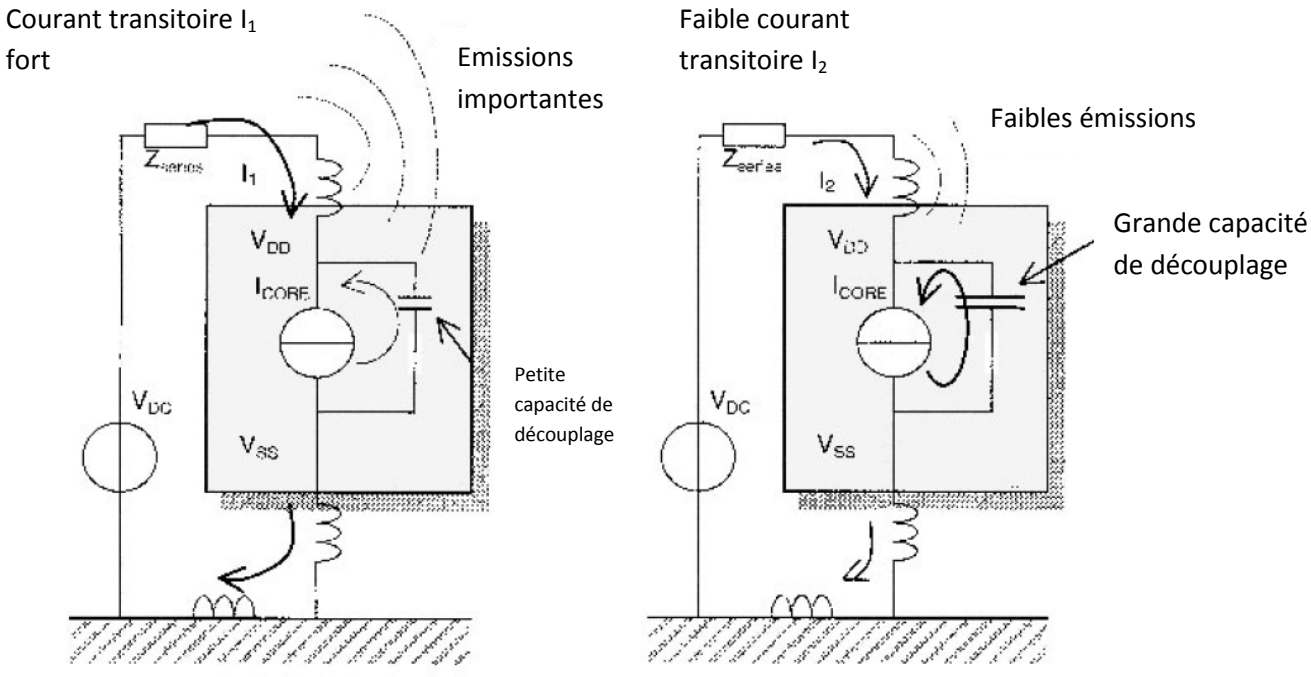


Figure III-7 : Le rôle d'une capacité de découplage (intégrée) dans la réduction des émissions parasites.

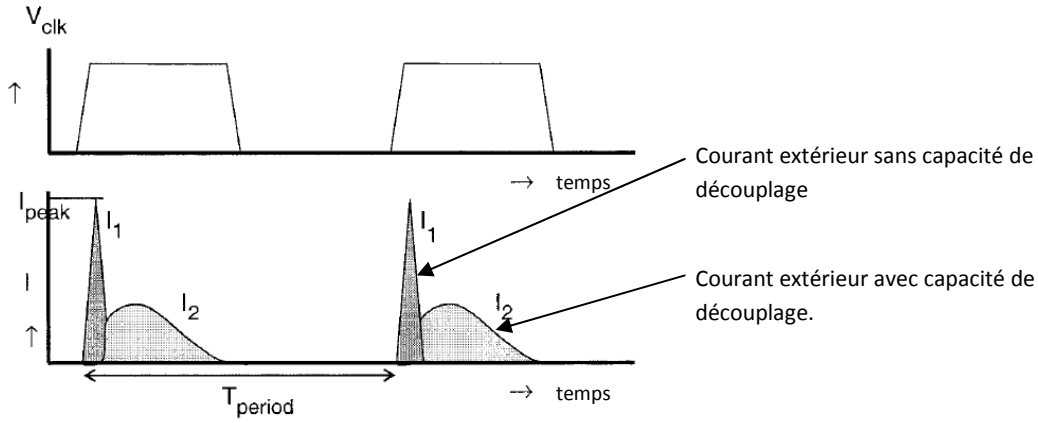


Figure III-8 : Courants extérieurs des circuits intégrés (de la figure ci-dessus) avec et sans capacité de découplage qui leur est interne.

Un détail important à noter serait la distance à laquelle il faut placer la capacité de découplage par rapport aux lignes d'alimentation. Si la capacité est placée loin des lignes d'alimentation, le circuit équivalent serait un modèle LC (car les connexions se comportent comme des inductances) en haute fréquence. Par conséquent, la capacité de découplage doit obligatoirement être située à la plus petite distance possibles des lignes d'alimentation. La figure III-9 [10] résume ce qui vient d'être expliqué.

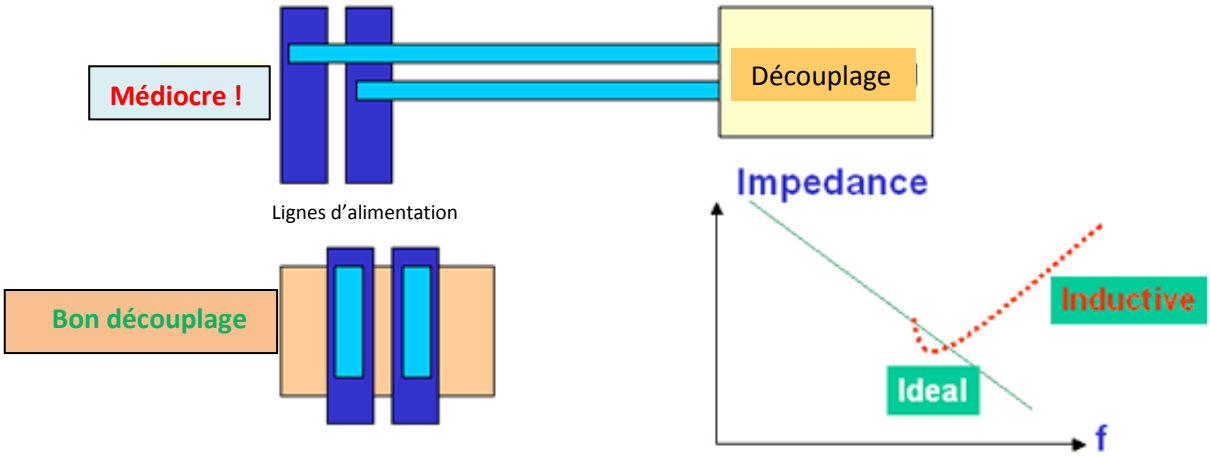


Figure III-9 : Nécessité du rapprochement entre la capacité de découplage et les lignes d'alimentation.

La valeur de la capacité de découplage intrinsèque est intimement liée au nombre de dispositifs (transistors) réalisés sur la même puce. Elle est également liée à la technologie adoptée pour la fabrication. Ces deux corrélations sont représentées par la figure III-10 [7]. Par exemple, un circuit intégré réalisé en technologie 90nm contenant 100 millions de transistors possède une capacité intrinsèque d'environ 10nF (voir la figure III-10). L'ajout d'une capacité interne pourrait augmenter ce chiffre à 50nF.

Enfin, il faut noter que l'ajout d'une résistance (choke resistor) à la capacité de découplage permet d'améliorer l'efficacité de celle-ci, en réduisant encore davantage les courants sortants.

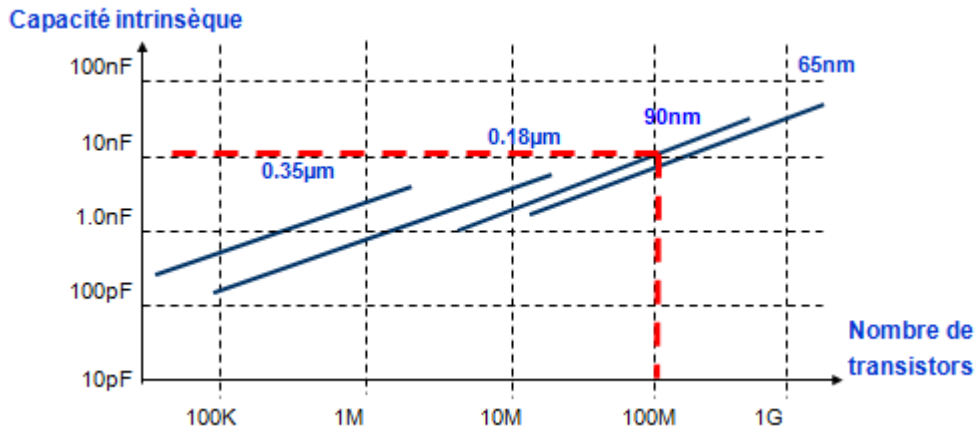


Figure III-10 : La capacité intrinsèque des circuits intégrés en fonction de leur complexité et la technologie de leur fabrication.

1-3) Solutions liées aux boîtiers et à la disposition des éléments du circuit intégré :

Les fils des bondings (voir les figures III-11 et III-12) liant le circuit intégré avec son boîtier sont essentiellement à caractère inductif. Ils contribuent donc à l'augmentation de la valeur de l'inductance totale sur le chemin de l'alimentation. Une cavité judicieusement usinée afin qu'elle corresponde exactement à la taille de la puce permet de réduire la longueur des bondings, ce qui réduit leur inductance parasite. De plus, l'attribution des fils transportant les courants les plus faibles aux leads (voir les figures III-11 et III-12) les plus longs est recommandée. Il faut également faire attention à ce que les lignes d'alimentation suivent toujours les trajets les plus courts possibles.

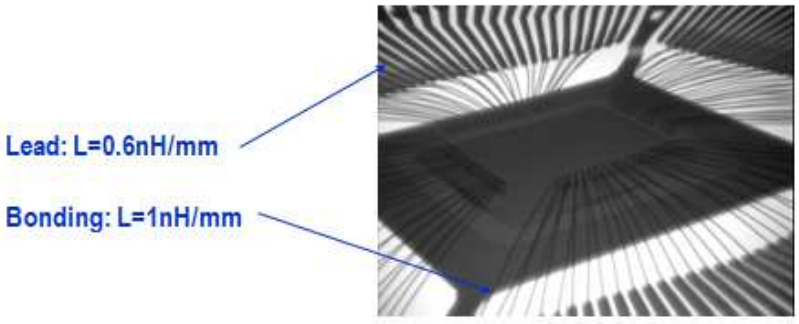


Figure III-11 : Illustration d'un bonding, d'un lead et de la valeur de leur inductance par unité de longueur.

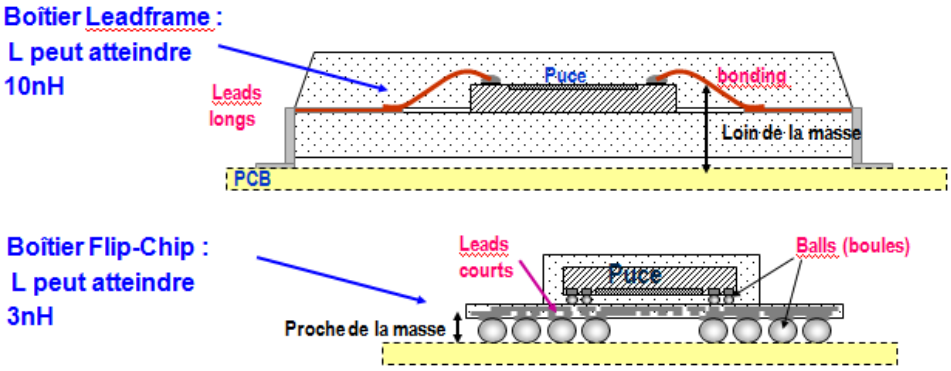


Figure III-12 : Réduction de l'induction des leads et des bondings en réduisant leurs tailles.

La conception systématique de lignes VDD et VSS adjacentes minimisent la boucle que parcoure le courant pour revenir à la masse (voir les figures III-13 et III-14). Par conséquent, le champ magnétique rayonné par de tels circuits intégrés est réduit. De surcroît, si les formes des courants des lignes VDD et VSS se ressemblent (ils ont la même allure quand on les représente graphiquement) dans le domaine temporel, les champs magnétiques qu'ils engendrent se compensent (car les courants suivent des trajectoires opposées en VDD et en VSS) ; ceci permet donc de réduire grandement les rayonnements de tels circuits intégrés. La figure III-15 illustre ce phénomène.

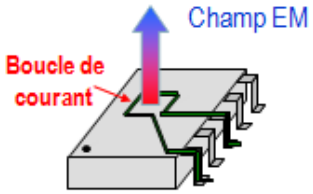
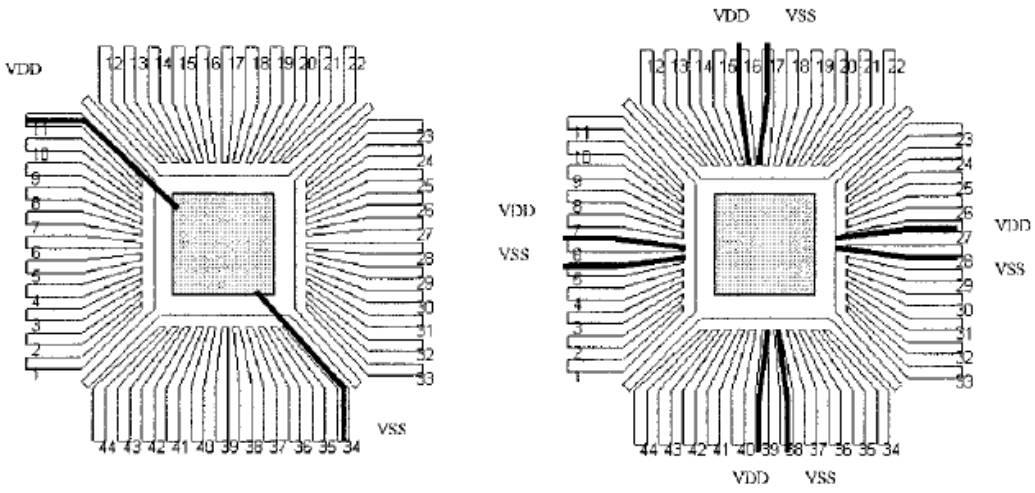


Figure III-13 : Création de champs électromagnétiques à partir de boucles de courant.



Mauvaise disposition des leads VDD et VSS

Bonne disposition des leads VDD et VSS

Figure III-14 : Exemple d'une mauvaise et d'une bonne disposition des leads VDD et VSS.

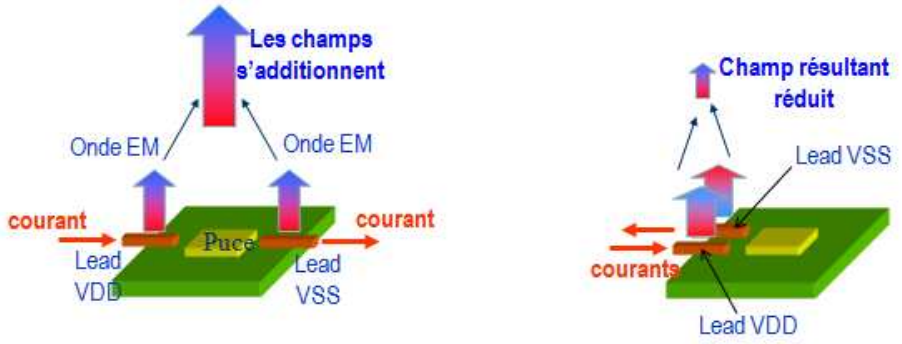


Figure III-15 : Phénomènes d'addition et de compensation des champs issus des leads transportant les courants VDD et VSS.

Des chemins multiples pour l'alimentation du circuit intégré permettent de subdiviser leur inductance équivalente ce qui réduit les fluctuations du courant d'alimentation de façon linéaire. Un exemple d'une disposition à chemins d'alimentation multiples pour un microcontrôleur 16 bits est décrit par la figure III-16. 22 couples de lignes VDD et VSS ont été distribués uniformément dans le boîtier. Certaines de ces alimentations sont connectées au cœur logique du microcontrôleur, d'autres sont connectées aux oscillateurs, aux parties analogiques et aux entrées/sorties.

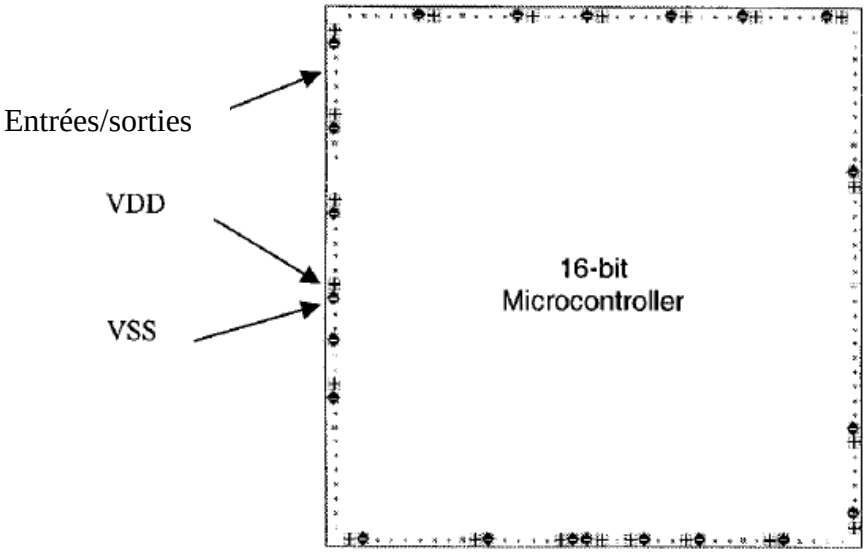


Figure III-16 : Disposition des couples VDD et VSS autour du boîtier du microcontrôleur.

Une autre façon de disposer les alimentations est celle illustrée par la figure III-17 [1]. Elle diffère complètement de la première méthode qui n'utilise que des leads à la périphérie du boîtier. Cette nouvelle distribution concerne le circuit programmable « Virtex ». Il utilise des broches VDD et VSS à accès multiples au centre du boîtier. Il divise ainsi le courant en plus de 60 chemins différents, ce qui réduit l'inductance parasite équivalente. En réalisant des pads

(la partie assurant le contact entre les connexions venant du boîtier –les bondings– et la puce) pour VDD et VSS voisins, on facilitera le découplage externe et ceci augmentera également la valeur de la capacité entre les deux conducteurs transportant les signaux de VDD et de VSS.

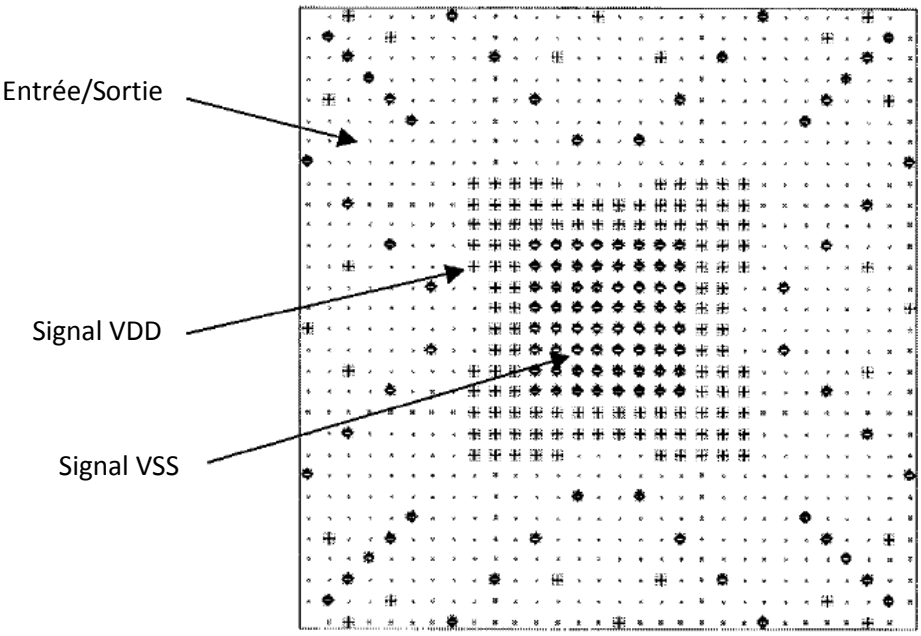


Figure III-17 : Disposition des signaux d'alimentation VDD et VSS dans le circuit programmable VIRTEX.

1-4) Buffers des entrées/sorties :

Une source importante de bruit trouve son origine dans les buffers des sorties. Les buffers sont d'habitude conçus pour satisfaire des contraintes de rapidité extrême. La commutation synchronisée des canaux N ou P de dispositifs MOS implique des pics de courants de courts-circuits. Ces pics peuvent être réduits en ajoutant un petit retard entre les transitions de niveaux entre les différents dispositifs. La plupart des microcontrôleurs et des circuits programmables possèdent des drivers qui peuvent s'accommoder avec plusieurs types de charges, des grandes charges capacitives rencontrées dans les interfaces de câbles, par exemple, aux plus petites telles que les interfaces de mémoires externes.

Un autre élément à prendre en considération dans la réduction des émissions parasites, serait le temps de montée/descente du buffer. On peut alors ralentir une commutation d'un buffer en rallongeant ce temps, tout en faisant attention aux limites des retards à ne pas dépasser pour assurer un fonctionnement correct de l'application visée. Le gain en termes d'émissions parasites est significatif dans le domaine de fréquence allant de 100 MHz à 1 GHz. Ceci est illustré par la figure III-18 [7].

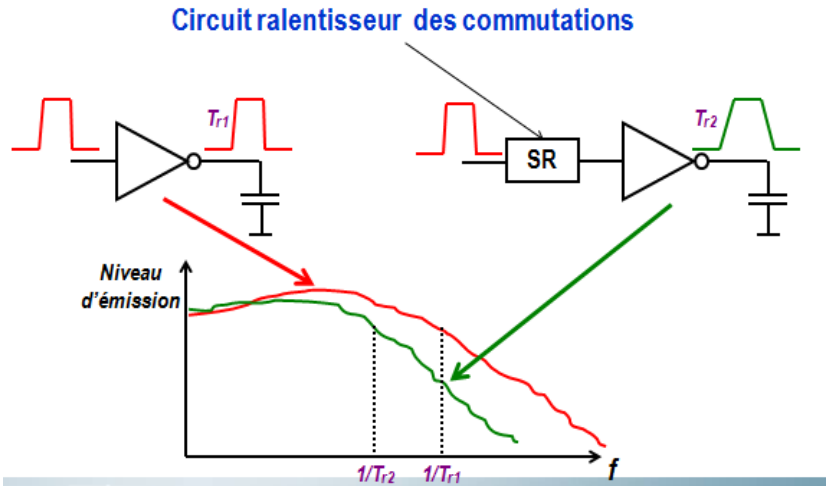


Figure III-18 : L'allongement des temps de commutation et son effet sur la réduction des émissions parasites.

Les bus (busses) des entrées/sorties peuvent devenir un fardeau à l'ensemble du système comme ils assurent les communications entre plusieurs blocs à l'intérieur d'une puce ou entre plusieurs circuits intégrés. Il y a plusieurs options afin de s'assurer que le courant global transporté par le bus est continu, et ce, quelque soit son contenu en termes de données. Une solution simple serait l'adoption d'un bus différentiel (comme l'USB, le RS-442, LVDS ou PC1 Express) où la somme des courants échangés à chaque instant est idéalement constante. Cela signifie malheureusement que le nombre de pads requis pour assurer une telle condition sur le courant devra doubler (100% en plus), ce qui signifie également que des circuits d'interfaçage plus complexes doivent être prévus.

Une autre façon de procéder, serait de préférer l'usage de codages sur de simples signaux différentiels. En adoptant un codage ternaire, en utilisant 4 fils pour transporter les données, le nombre de combinaisons possibles sont, dans ce cas, de 81 (3^4 = 81) à partir desquels 19 combinaisons vont être retenues car leurs signaux vont représenter des courants simultanés dont la somme est constante.

La figure III-19 [1] illustre un exemple d'implémentation d'un codage ternaire.

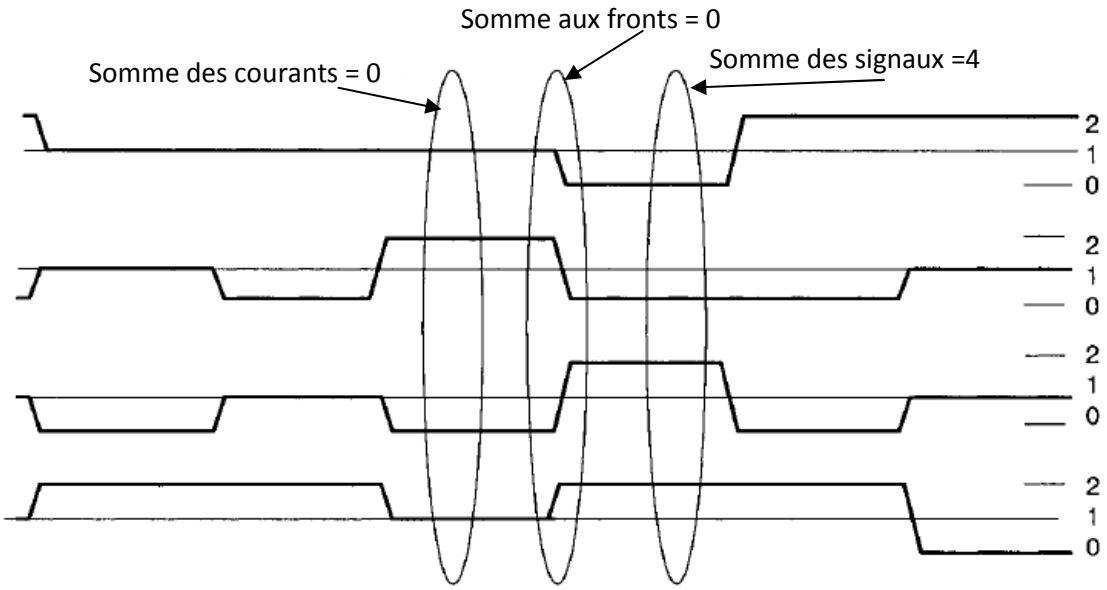


Figure III-19 : Exemple d'implémentation d'un codage ternaire.

2) Solutions pour augmenter l'immunité des circuits intégrés :

2-1) Introduction :

Des approches traditionnelles pour améliorer l'immunité d'un système en général (intégré ou pas) existent. On peut citer des techniques connues telles que le filtrage du bruit ou le blindage qui visent à protéger les systèmes électroniques des interférences électromagnétiques extérieures. Ces techniques similaires sont également applicables aux circuits intégrés, mais ces derniers étant plus fragiles, imposent qu'on fasse preuve de plus d'imagination et de trouver d'autres méthodes. Le but des paragraphes suivants est de citer, justement, ces techniques spécifiques visant à augmenter, plus efficacement, l'immunité des circuits intégrés.

2-2) Capacité de découplage :

Une capacité de découplage formée à l'intérieur d'une puce a ses effets bénéfiques sur la diminution des niveaux des émissions émanant de la puce. En termes d'immunité, elle joue un rôle également significatif. La capacité étant un composant symétrique, elle diminue aussi bien les perturbations sortantes du circuit intégré que celles qui essaient d'y pénétrer. La figure III-20 [1] illustre des résultats de mesure, où un circuit intégré subit une injection de bruit volontaire, pour mettre en évidence l'effet de l'ajout d'une capacité de découplage sur l'immunité d'un circuit intégré. On voit dans la figure III-20 que la capacité (à l'intérieur de la puce) a un impact réel et considérable sur le gain en transfert d'énergie de la source de perturbation à la partie interne du circuit intégré.

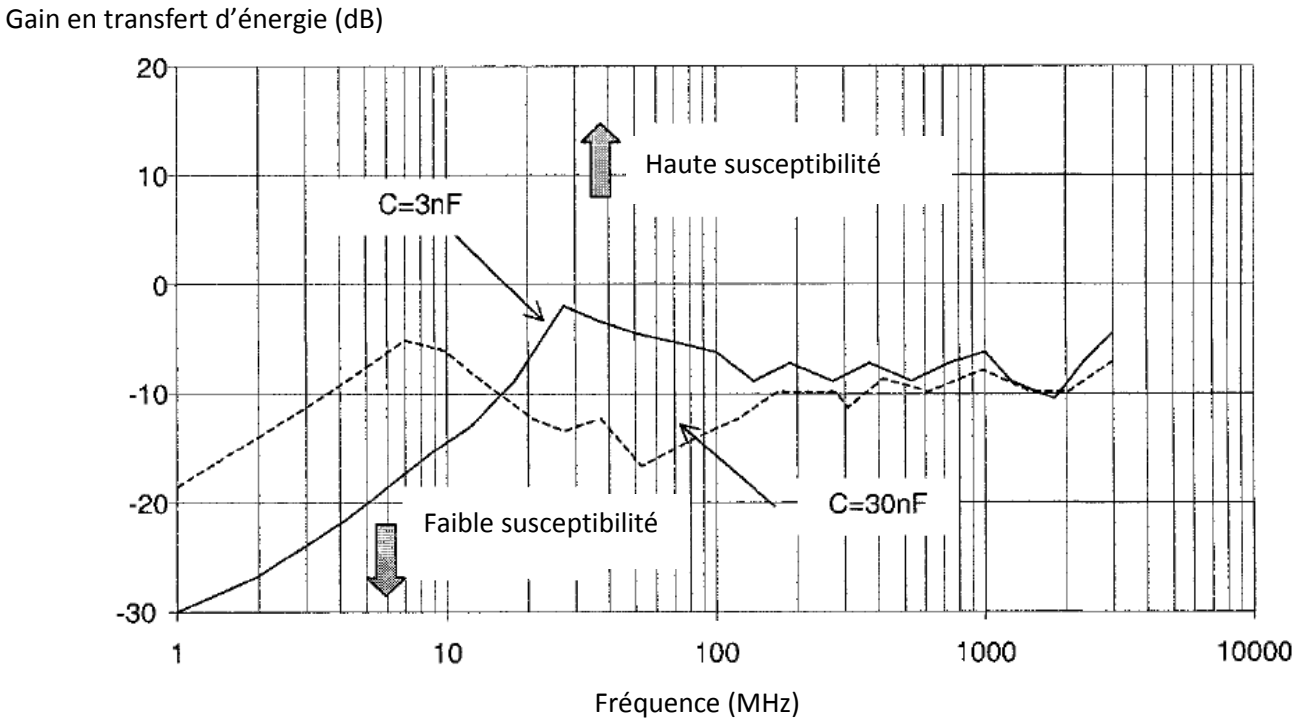


Figure III-20 : Effet d'une capacité de découplage interne à la puce sur le gain de transfert de la source de perturbation RF au circuit intégré.

2-3) Blindages :

Le blindage est une des solutions des plus connues pour améliorer l'immunité de tout système, en l'occurrence, dans notre cas celle d'un circuit intégré. Tous les dispositifs électroniques rapides utilisent une forme de blindage. Les ordinateurs, les téléphones cellulaires ou les jeux vidéo sont emballés dans un boîtier métallisé. Tous les systèmes électroniques, en fait, utilisent au moins un blindage sur certains composants sensibles.

Les blindages proprement conçus et installés représentent un moyen très efficace pour atténuer, à la fois, les émissions rayonnées et les rayonnements issus de sources externes. En effet, une enclave métallique sans aucune ouverture que ce soit peut réduire les émissions et améliorer l'immunité aux radiations de 40 dB ou plus [11]. En d'autres termes, un blindage rend la satisfaction des normes de compatibilité électromagnétiques imposées facilement atteignable.

Le blindage fonctionne en réfléchissant, absorbant ou redirigeant les champs électrique ou magnétique. Il n'est pas toujours nécessaire d'envelopper complètement un produit par un blindage, pour que ce dernier soit efficace. Par exemple, des blindages partiels placés sur un circuit source (de perturbations), sont souvent utilisés afin de rediriger les champs électrique

et magnétique. Ceci permet de l'isoler de certains circuits, jugés sensibles. Cela permet également d'éviter un couplage avec des antennes non intentionnelles.

Le choix de la bonne place, de la bonne orientation et du bon matériau pour un blindage requiert une connaissance du type du champ (à orienter, isoler ou absorber) et des objectifs précis attendus du blindage.

2-4) Protection contre les décharges électrostatiques (ESD) :

2-4-1) Introduction :

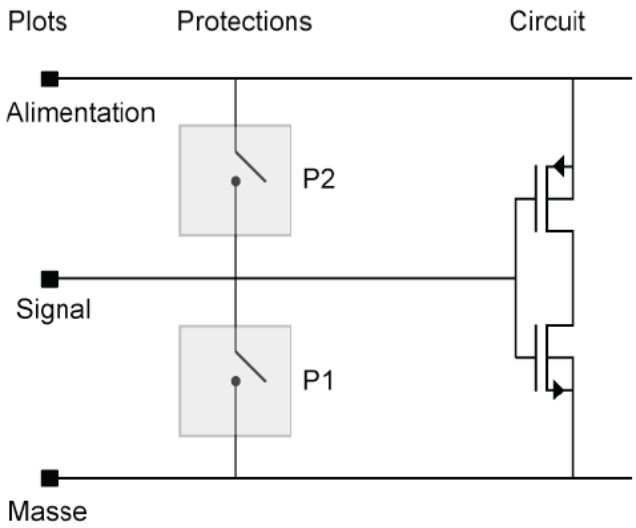
On appelle protections ESD l'ensemble des protections électriques présentes sur un circuit intégré pour le protéger des décharges électrostatiques. Sans ces protections, le circuit serait extrêmement sensible et risquerait d'être détruit par la moindre surtension à ses bornes. Ces protections sont présentes sur les entrées, les sorties et les alimentations du circuit. Elles s'articulent autour d'éléments non linéaires sensibles aux surtensions et aux fortes variations de tension. Ces éléments interviennent lors d'une décharge électrostatique mais peuvent aussi réagir en cas d'agression RF lors de fortes variations de signal, par exemple.

Des protections rapportées au niveau de la carte électronique sont généralement utilisées pour compléter les protections internes aux circuits intégrés et permettre d'absorber ce type de stress. Pour notre part, notre étude ne se focalisera que sur les seules protections internes.

2-4-2) Dispositifs intégrés de protection :

a) Concepts de base des protections ESD :

Une décharge électrostatique peut engendrer deux types de dommages dans un circuit intégré: une destruction thermique à cause du fort courant de la décharge, et le claquage des diélectriques qui sont dus aux surtensions. La fonction électrique d'une protection ESD est idéalement celle d'un interrupteur commandé. A la détection du stress ESD, la structure doit conduire tout le courant et présenter à ses bornes une faible tension. Par contre en utilisation normale, la structure doit être transparente pour l'application, en présentant alors une forte impédance.



La figure III-21 [5] montre un exemple d'implantation de structures de protection sur une entrée de type CMOS. L'application d'un stress ESD entre le plot de signal et le plot de masse, déclenche la structure P1 qui absorbe la décharge. La structure P2 sera active pour un stress appliqué entre le plot de signal et le plot d'alimentation. Les structures de protection doivent fonctionner pour les deux polarités de stress, et elles sont localisées au plus près des plots afin d'éviter la destruction des connexions métalliques internes au circuit.

Les structures de protection ESD présentent généralement deux types différents de caractéristiques dynamiques courant/tension. Ces caractéristiques sont expérimentalement obtenues avec un équipement de test dédié : TLP (Transmission Line Pulsing). La première caractéristique de la figure III-22 [5] (partie gauche) possède un régime de forte impédance pour des faibles niveaux de courant, et un régime de faible impédance pour des tensions supérieures à la tension de déclenchement V_{T1}. Le couple courant/tension (I_{T2}, V_{T2}) correspond au point de défaillance de la structure. La seconde caractéristique (figure III-22 partie droite) est singulière des structures à retournement. A son déclenchement, la protection entre dans son régime de conduction et soutient une tension plus faible que la tension de déclenchement. Cette tension de maintien V_H est intéressante pour la protection car elle permet de supporter, à puissance équivalente, un plus fort niveau de courant par rapport à un comportement sans retournement.

Les paramètres des caractéristiques dynamiques que nous venons d'expliciter doivent rentrer dans une fenêtre de conception afin de garantir l'efficacité de la protection. La tension de déclenchement V_{T1} doit avoir une valeur plus grande que la tension d'alimentation du circuit afin d'éviter le déclenchement intempestif de la structure en utilisation normale. Par contre, cette tension doit, bien sûr, être plus faible que la tension maximum V_{MAX} que peut supporter le circuit sans destruction. La tension V_{T2} doit aussi être plus faible que V_{MAX}, ce paramètre est fortement dépendant de la résistance à l'état passant du composant. Pour le cas des structures à retournement, la tension V_H est généralement prise supérieure à la tension d'alimentation. Cette précaution garantit au concepteur que la structure ne puisse pas rester verrouillée en cours d'utilisation par un déclenchement intempestif de la protection ou une décharge électrostatique. Dans certains cas, la tension V_H peut être prise inférieure à la tension d'alimentation, mais alors le courant de maintien I_H devra être supérieur au courant maximum que peut fournir l'alimentation.

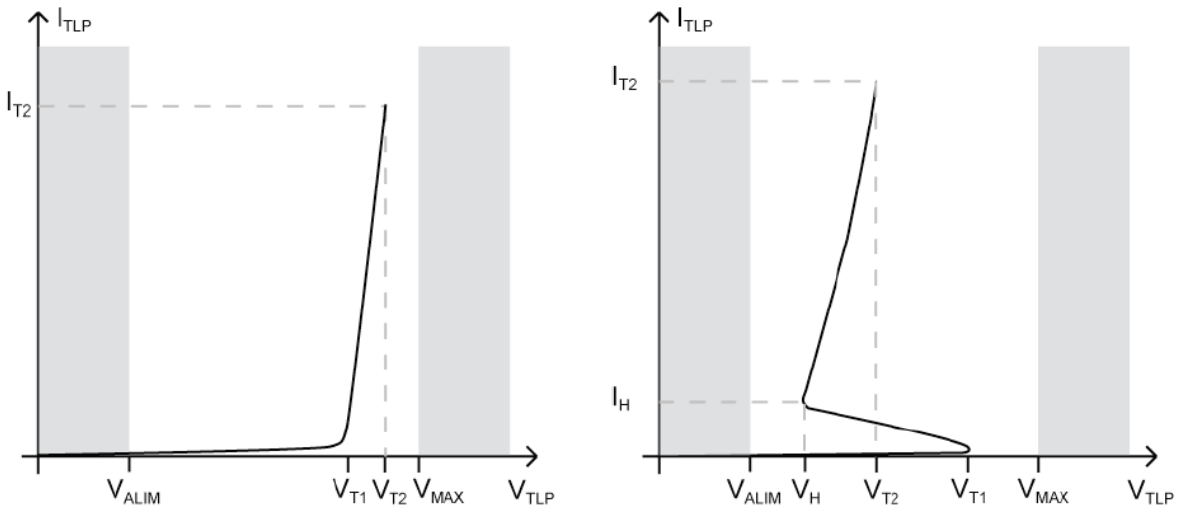


Figure III-22 : Caractéristiques typiques dynamiques de protection ESD sans et avec retournement.

b) Dispositifs intégrés utilisés comme protection ESD :

Après avoir donné un aperçu sur les concepts théoriques concernant les protections ESD, nous allons présenter les différentes structures élémentaires concrètement utilisées comme protections ESD.

❖ La diode :

La diode a été longtemps utilisée comme unique protection ESD. La Figure III-23 montre un exemple d'implantation entre deux plots. En utilisation normale, le signal voit des tensions positives par rapport à la masse. En mode ESD, la décharge est appliquée sur la broche de signal. Deux polarités sont possibles. Dans le cas d'une polarité négative, la diode est polarisée en direct et elle évacue facilement la décharge. Pour une polarité positive, la diode conduit quand elle atteint sa tension d'avalanche. La résistance à l'état passant dans ce mode est plus élevée. La diode doit avoir une surface suffisante pour atteindre le niveau de robustesse désiré.

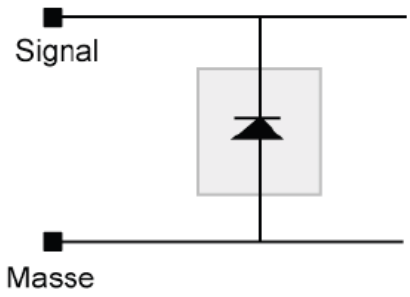


Figure III-23 : Protection ESD à base de diode.

Il est possible d'utiliser plusieurs diodes en série afin d'augmenter les tensions de déclenchement au détriment de la place occupée.

Une diode Zener peut aussi être utilisée. A surface comparable, elle présente une résistance à l'état passant plus faible que la diode à avalanche, mais son courant de fuite élevé limite souvent son utilisation.

Les diodes restent à ce jour les protections privilégiées du domaine des hautes fréquences. Elles ont une capacité parasite plus faible que les autres composants, ce qui est un facteur déterminant pour satisfaire aux contraintes fréquentielles de ces applications.

❖ **Le transistor bipolaire :**

Le transistor bipolaire utilisé comme protection ESD voit sa jonction base-émetteur court-circuitée (Figure III-24). Lors d'une décharge négative par rapport à la masse, la jonction collecteur-base est polarisée en direct, et comme la tension de mise en conduction est très basse, la structure est généralement robuste. Pour une décharge positive, ce transistor bipolaire autopolarisé (TBA) possède une caractéristique dynamique courant/tension à repliement (Figure III-25 [5]). Le composant est bloqué jusqu'à atteindre la tension d'avalanche de la jonction collecteur-base. Le courant de trous dans la base augmente alors localement le potentiel de cette dernière. Pour un courant d'avalanche suffisant, la jonction base-émetteur est polarisée en direct, et le transistor se déclenche, entraînant un repliement de la tension.

La faible résistance à l'état passant du transistor, et le repliement de la tension, font de cette structure une protection plus robuste que la diode. Les tensions de déclenchement sont habituellement dans la gamme des moyennes aux fortes tensions (10 à 80V). Une résistance externe peut être ajoutée entre la base et l'émetteur pour réduire la tension de déclenchement.

Ce sont classiquement des transistors NPN qui sont utilisés. Les transistors PNP ont un gain plus faible, ce qui se traduit par un retournement beaucoup plus faible.

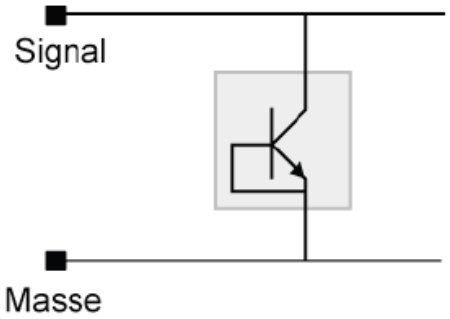


Figure III-24 : Protection ESD à base de transistor bipolaire NPN.

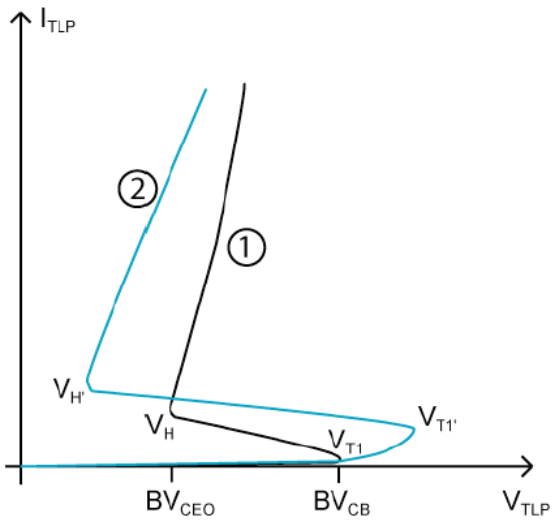


Figure III-25 : Exemple de courbes de caractéristiques courant/tension de structures TBA (Transistor Bipolaire Autopolarisé).

❖ **Le transistor MOS :**

Le GGNMOS (Gate-Grounded NMOS) est un transistor NMOS dont la grille, la source et le substrat sont connectés à la masse (Gate-Grounded). Dans cette configuration, le transistor bipolaire parasite, formé par le drain, le substrat et la source, est exploité comme un TBA. La protection (la jonction drain-substrat) présente une caractéristique courant/tension à retournement sur un stress positif, et un comportement de diode polarisée en direct pour une décharge négative.

La deuxième configuration rajoute une résistance entre la grille et la source pour former un GCNMOS (Gate-Coupled NMOS). La valeur de cette résistance est choisie en fonction de la tension de seuil du transistor, et de la valeur de sa capacité drain-grille. Une capacité externe entre le drain et la grille peut aussi être ajoutée. Au début d'un stress positif sur le drain du composant, la capacité drain-grille conduit le courant transitoire qui traverse la résistance. La tension sur la grille augmente jusqu'à mettre en conduction le transistor MOS. En fonction de la configuration de la structure deux comportements sont alors possibles. Soit le transistor est suffisamment dimensionné pour évacuer toute la décharge par conduction MOS. Soit son canal conduit une partie du stress avant que le transistor bipolaire parasite ne se déclenche et évacue le reste de la décharge. Le couplage capacitif permet alors de diminuer la tension de déclenchement de la protection.

Figure III-26 : Protections ESD à base de transistors NMOS.

Les surtensions sur la grille durant le stress doivent être limitées afin d'éviter sa destruction. Même si le principe de fonctionnement est identique, à surface égale, la robustesse d'un GGNMOS est souvent inférieure à celle d'un TBA. En effet, le GGNMOS exploite un transistor bipolaire parasite latéral qui dissipe moins facilement la température qu'un TBA vertical.

Les figures III-27 et III-28 montrent des exemples d'application concrets pour protéger le plus élémentaire des circuits numériques : l'inverseur CMOS.

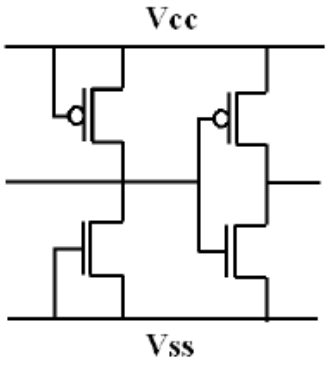
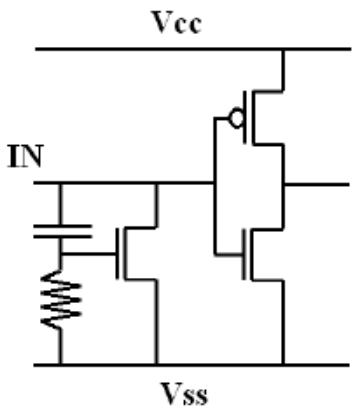


Figure III-27 : Exemple de protection ESD symétrique à GGMOS pour un inverseur CMOS.



❖ Le thyristor :

Le thyristor, appelé aussi SCR (Silicon-Controlled Rectifier), est utilisé comme élément de commutation pour les applications de forte puissance. Ce composant est formé de l'association d'un transistor PNP imbriqué dans un transistor NPN, voir Figure III-29. Il possède une commande de déclenchement, ou gâchette, sur laquelle une impulsion de contrôle déclenche la conduction des deux transistors qui se verrouillent. La structure présente alors une très faible résistance à l'état passant. Elle repasse à l'état bloqué quand le courant qui la traverse devient inférieur à son courant de maintien.

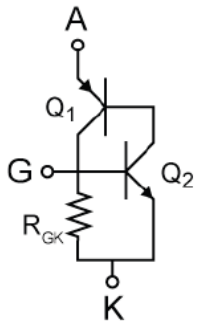


Figure III-29 : Structure interne d'un thyristor.

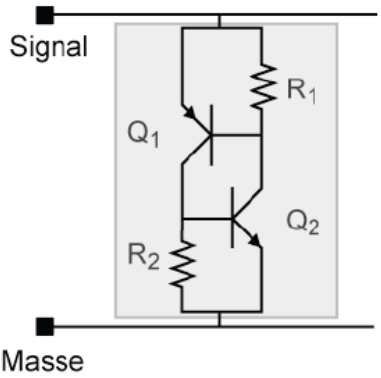


Figure III-30 : Protection ESD utilisant une structure de thyristor.

Le concept est repris pour former la protection ESD de la Figure III-30. La commande de gâchette sur la base du transistor NPN Q2 est supprimée, et une résistance R1 est ajoutée entre la base et l'émetteur du transistor PNP Q1. Dans le schéma de la figure III-30, il y a des masques de la structure : les deux transistors ont en fait leurs contacts de base et d'émetteur court-circuités, et les résistances R1 et R2 sont en fait les résistances intrinsèques de leurs bases. Le déclenchement de Q2 se fait par le claquage de la jonction collecteur-base et la polarisation de la jonction base-émetteur. Le transistor Q1 se déclenche à son tour et le système se verrouille.

Les tensions de déclenchement sont généralement importantes. Des solutions technologiques permettent de les réduire, comme l'ajout d'une implantation localisée de type N fortement dopée sur la jonction collecteur-base du transistor NPN. Les protections ainsi modifiées sont appelées MLSCR (Modified Lateral Silicon-Controlled Rectifier).
Les thyristors ne sont pas employés comme protections sur les plots d'alimentation. Cette précaution permet d'éviter, en cas de déclenchement intempestif de la structure, le verrouillage de la protection sur le courant d'alimentation qui conduirait à la destruction inévitable du circuit. Sur des plots d'entrées/sorties, les thyristors permettent d'obtenir des structures très robustes et compactes. Ces protections présentent en principe les meilleures performances contre les décharges électrostatiques.

2-5) Identification des blocs les plus bruyants et leur isolation :

Une solution qu'on aurait pu citer aussi parmi les recommandations énoncées pour la réduction des émissions des circuits intégrés, est l'identification des blocs les plus bruyants et leur isolation du reste du circuit. On entend par isolation, l'isolation de leurs alimentations, l'éloignement des circuits les plus bruyants des circuits les plus sensibles et même, dans la mesure du possible, l'isolation de leurs substrats respectifs (isolation de leurs bruits de substrat). Ceci permet d'améliorer l'auto-compatibilité d'un circuit intégré, par conséquent, cela accroît sa résistance aux agressions externes.

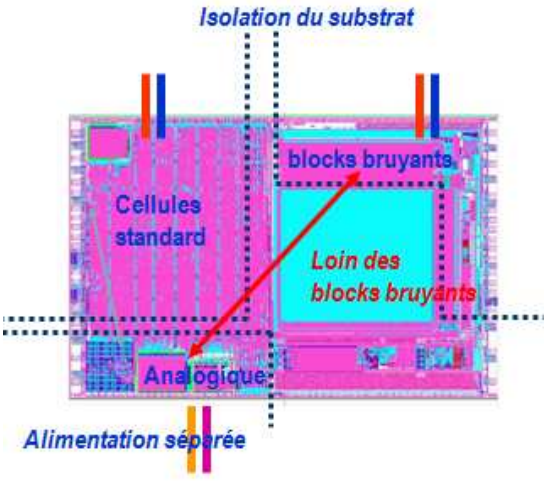


Figure III-31 : Isolation des blocs les plus bruyants.

L'identification des sources de bruit n'est pas une tâche aisée, il faut d'abord pouvoir identifier les blocs avec des commutations rapides, et des courants forts. Les circuits les plus critiques, du point de vue compatibilité électromagnétique, sont les entrées/sorties rapides, les oscillateurs, les circuits des cœurs et les bus (busses en anglais) de données. Des entrées/sorties lentes peuvent également produire du bruit, quoique moins important que celui créé par les circuits déjà cités. Les lignes d'alimentation des parties analogiques d'un circuit intégré sont moins bruyantes que celles qui alimentent le cœur de celui-ci. Les lignes transportant les signaux de contrôle, rarement en commutation, crée un faible bruit. Les lignes

transportant les signaux de Reset ou d'interruption(s) ne commutent presque pas, ce sont donc les parties les moins perturbatrices.
A partir de ce qui vient d'être dit, nous pouvons dresser un tableau récapitulatif résumant un classement des circuits, des plus bruyants (ceux qui ont le plus d'étoiles ****) aux plus calmes (sans étoiles) :

Signaux	Importance du bruit
Entrées/sorties rapides	****
Oscillateurs	***
Alimentation du cœur	**
Bus de données	**
Entrées/sorties lentes	**
Alimentation des circuits analogiques	**
Signaux de contrôle	*
Signaux de Reset et d'interruption(s)	

Tableau III-1 : Classement des circuits selon l'importance du bruit qu'ils émettent.

2-6) Ajout de triggers de Schmitt aux entrées :

Les entrées d'un circuit intégré numérique comme un microprocesseur ou un microcontrôleur sont très importantes. En fonction des données qu'elles lui transmettent, il effectue des calculs et « prend des décisions ». Cependant ces entrées sont exposées aux hostilités de l'environnement extérieur. Les données se trouvent donc mélangées au bruit. Un trigger de Schmitt, possédant une marge de sécurité (tensions de seuil inférieure et supérieure), ne prend pas en compte toutes les variations brusques d'un signal appliqué à son entrée. En l'ajoutant comme protection pour les entrées, il permettra de « lisser » l'allure des signaux entrants, cela réduit donc le bruit accédant par ces entrées au circuit intégré (microprocesseur ou microcontrôleur).

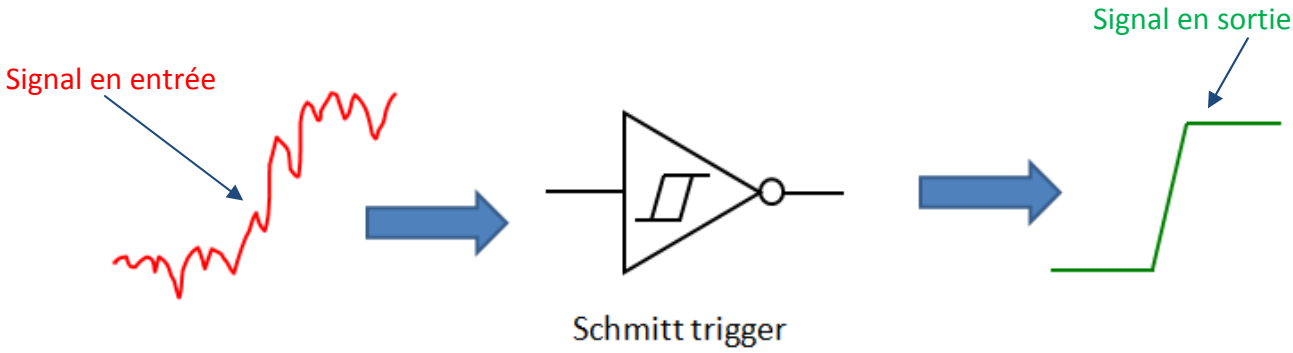


Figure III-32 : Lissage du signal d'entrée d'un circuit intégré par un Trigger de Schmitt.

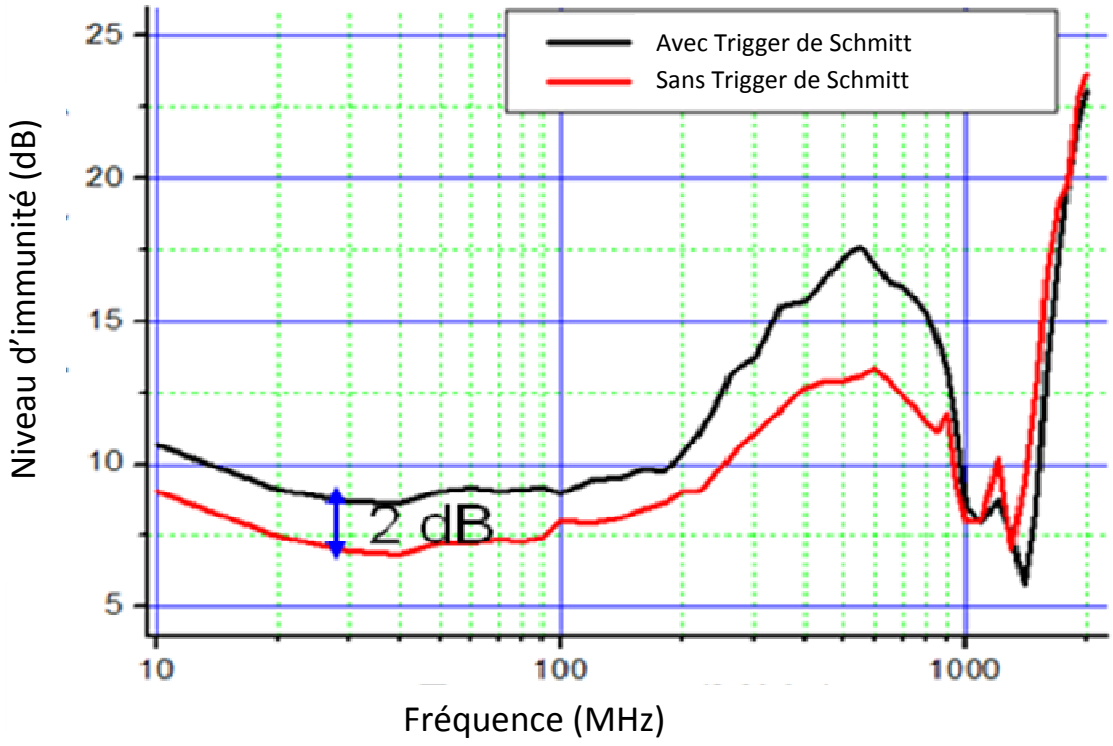


Figure III-33 : Amélioration des niveaux d'immunité en ajoutant un trigger de Schmitt aux entrées.

2-7) Amélioration de l'immunité des systèmes à microprocesseurs par des logiciels :

La programmation judicieuse qui prend en considération certains paramètres CEM peut améliorer significativement l'immunité de systèmes à microprocesseurs. Ces concepts sont très détaillés dans le chapitre IV, cependant nous tenons à ce que nous abordions l'idée de base de ces méthodes.

Ces techniques logicielles visent certaines voies stratégiques pour détecter les erreurs. Leur tâche est d'empêcher de déclencher des décisions erronées, des comportements imprévisibles ou un dysfonctionnement pur et simple de l'application visée.

Ces logiciels contrôlent les points les plus vulnérables, du point de vue sensibilité et exposition aux rayonnements électromagnétiques : Les entrées (du microcontrôleur ou du microprocesseur), la RAM, le registre contrôlant le flot d'exécution.

Les entrées sont très exposées aux agressions électromagnétiques extérieures, c'est la raison pour laquelle il faut vérifier l'authenticité des données qu'elles transmettent au microprocesseur. Bien sûr, ces données sont primordiales pour les calculs et « la prise des bonne décision » par le microprocesseur. L'idée de base de la détection d'une erreur réside dans la nature des données et de ce qu'elles représentent comme phénomènes physiques. Il est évident que lorsqu'on connaît la vitesse de variation des données, si une variation nous parait anormale nous la considérerions comme n'étant pas due au phénomène physique mesuré, il s'agit donc d'une erreur. Il est évident également que, si un capteur ne peut fournir une valeur

de tension qu'on retrouve à l'entrée, il s'agit d'une erreur (qui peut être due aux perturbations électromagnétiques).
Cela dit, après avoir vérifié que les données entrantes sont correctes, il faut veiller à ce qu'elles soient protégées là où elles seront stockées pour effectuer des calculs, c'est-à-dire la RAM. Il faut donc veiller régulièrement à ce que les données que contient la RAM ne sont pas corrompues par des agressions électromagnétiques de l'environnement.

Enfin et en dernier lieu, après s'être assuré que les données sont correctes lors de leur extraction de la RAM, il faut vérifier les séquences d'exécution du programme. Il s'agit de s'assurer que le programme suive les étapes spécifiées par le programmeur. Il faut également s'assurer que toute la mémoire programme ait été utilisée, au cas où le programme tombe, par accident, sur cet espace qui, inutilisé, contiendrait une valeur aléatoire ; et dans le cas d'applications critiques cela représenterait un très grand risque.

2-8) Exemple d'amélioration de l'immunité d'un circuit intégré par conception :

Les amplificateurs opérationnels, comme la plupart des circuits intégrés, sont extrêmement susceptibles aux interférences électromagnétiques. Ces perturbations sont transportées, à l'intérieur des circuits intégrés, par des fils, des pistes des circuits imprimés et des connexions entre la puce et son boîtier (des bondings).

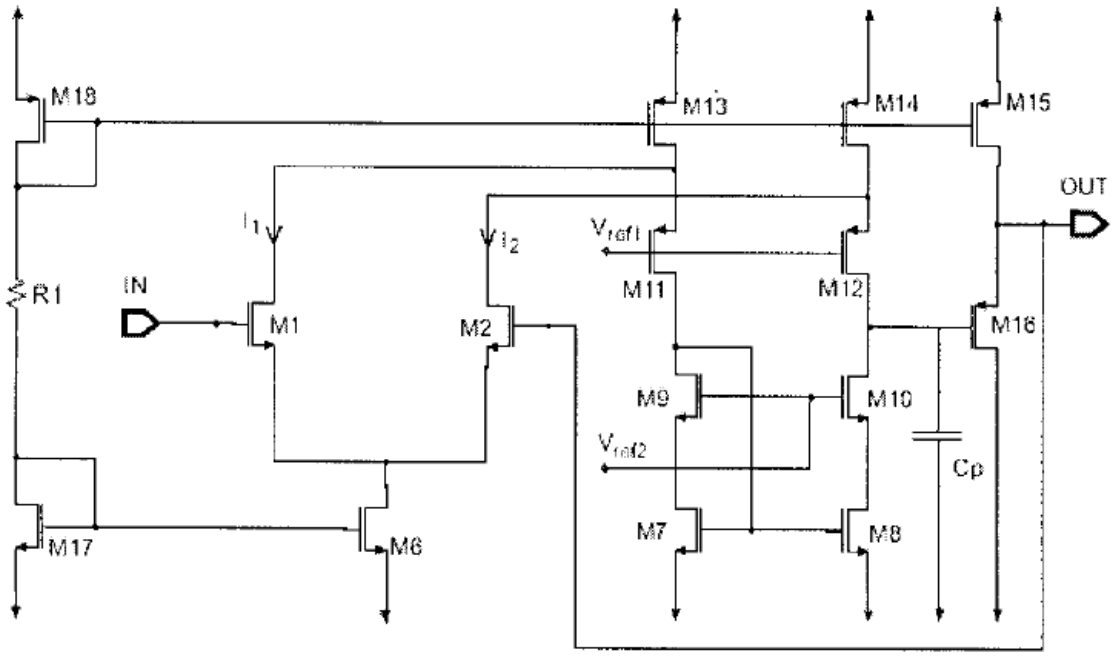


Figure III-34 : Schéma de base d'un amplificateur opérationnel conventionnel.

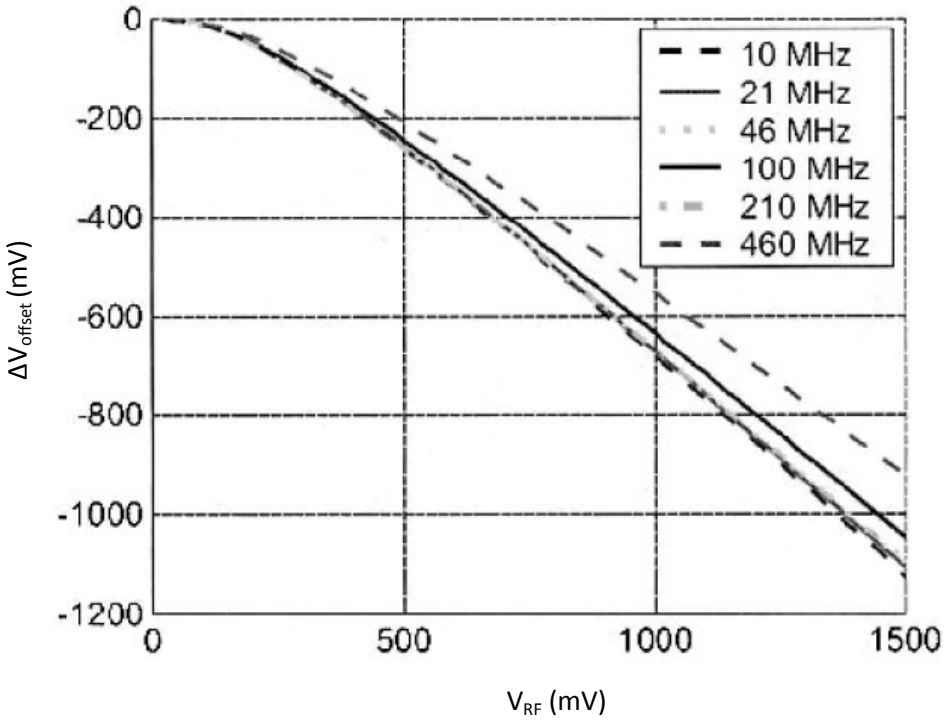


Figure III-35 : Dérive (offset) de la tension de sortie de l'amplificateur opérationnel en fonction de l'amplitude de l'interférence.

Une fois superposées aux signaux utilisés, les interférences RF se propagent sur tout le circuit intégré (interconnexions métalliques et substrat) atteignant ainsi les composants actifs comme les transistors bipolaires et MOS. Les parties non linéaires de ces composants sont excitées par ces interférences. Et comme ces interférences peuvent tomber (et c'est le cas souvent) dans des fréquences faisant partie de la bande passante du système, les signaux utilisés (par le système) ne peuvent être recouvrés ; ceci induit donc des dysfonctionnements non négligeables.

Par exemple, si une interférence RF est ajoutée à une entrée de tension constante (considérons que c'est ce signal qui est exploité par le système) de l'amplificateur opérationnel de la figure III-34 [1], il y aurait un décalage de la tension de sortie. L'amplitude de ce décalage dépend de l'amplitude et de la fréquence du signal interférent, comme le montre la figure III-35 [1].

Même si tous les transistors d'un amplificateur opérationnel sont excités par une interférence RF, il n'y a que ceux qui font partie de l'étage différentiel d'entrée qui contribuent à la tension de sortie. En effet, les signaux générés au premier étage se trouvent fortement amplifiés dans les étages qui suivent. Par conséquent, les solutions CEM se focalisent, surtout, sur la réduction des phénomènes de distorsion dans les paires différentielles induits par des signaux radioélectriques.

La susceptibilité aux interférences électromagnétiques de l'amplificateur opérationnel, de la figure III-34, peut être significativement réduite par une sélection particulièrement attentionnée de la méthode de conception de la paire différentielle et de l'amplitude du courant de polarisation. La figure III-36 [1] montre clairement que si l'on augmente la valeur du courant de polarisation, le décalage sur la tension d'entrée dû à une interférence électromagnétique diminue.

Enfin, il a été montré que l'immunité des amplificateurs opérationnels aux interférences RF, pourrait être augmentée en choisissant les topologies appropriées du circuit de la paire différentielle d'entrée [1]. La topologie adéquate est schématisée sur la figure III-37 [1]. On voit qu'une double paire différentielle remplace la paire cascode croisée de l'amplificateur opérationnel. La sortie de la paire M3-M4 est uniquement modulée par des signaux d'entrée dont la fréquence est supérieure à la fréquence de coupure du filtre passe haut CR.

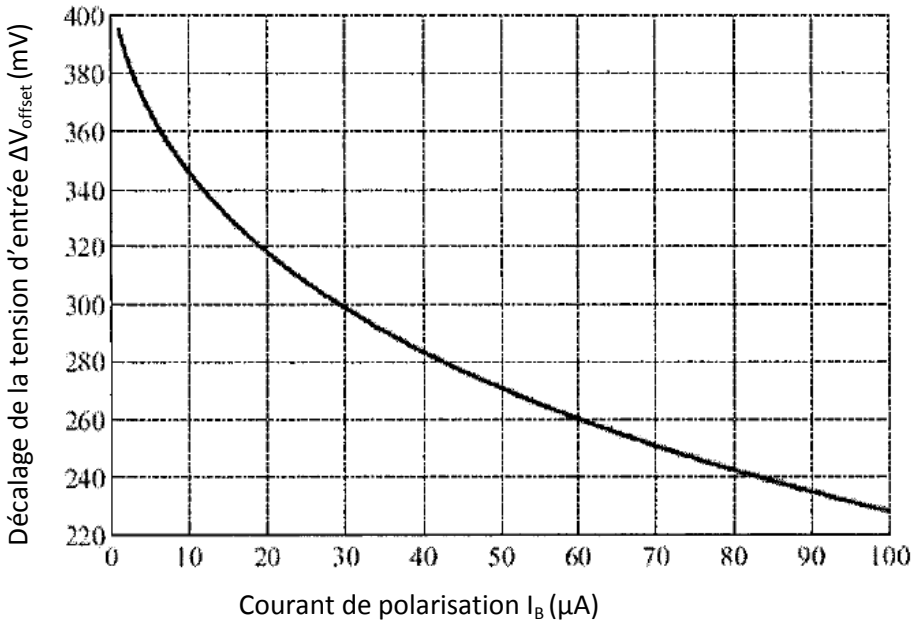


Figure III-36 : Dérive de la tension d'entrée en fonction du courant de polarisation.

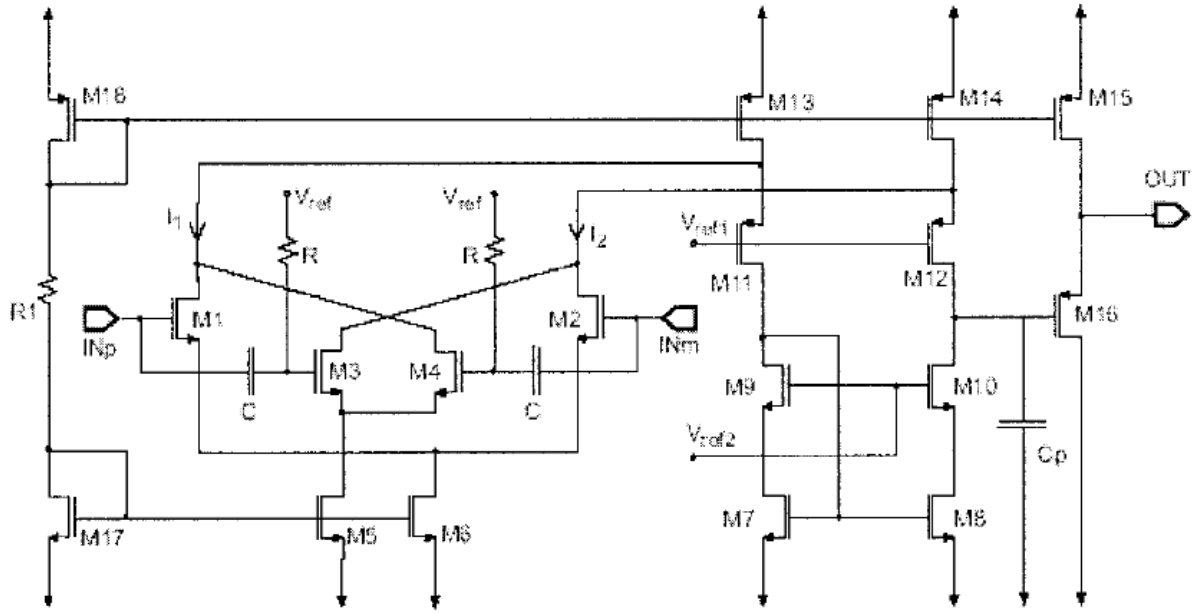


Figure III-37 : Amplificateur opérationnel avec, à l'entrée, une double paire différentielle.

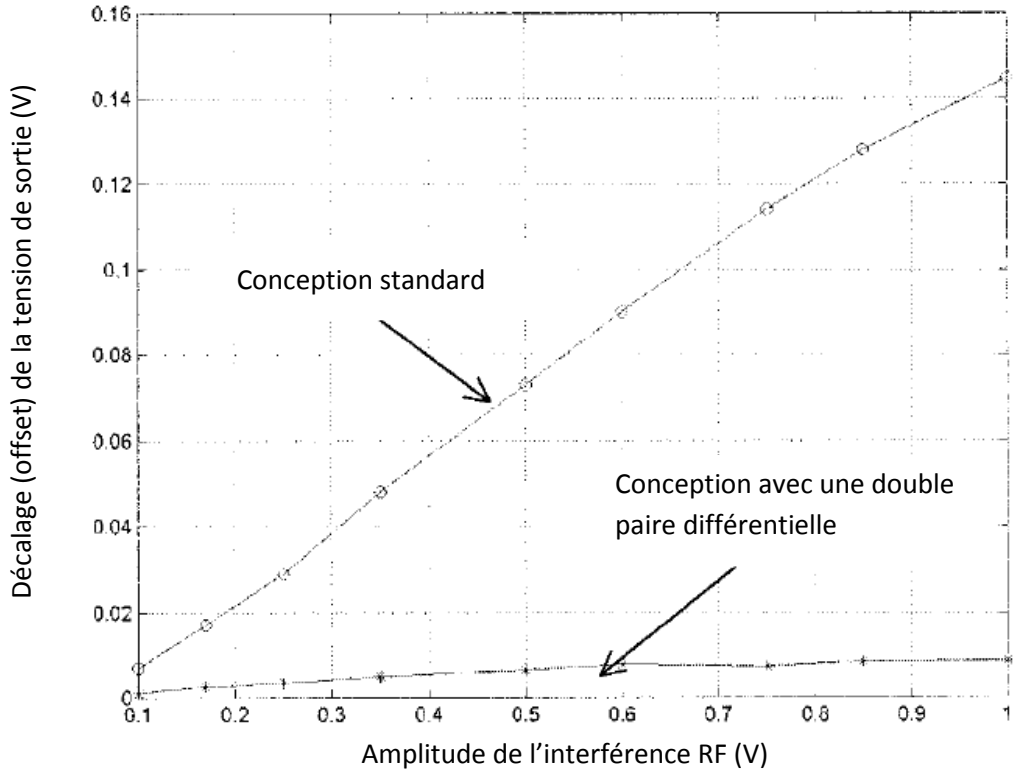


Figure III-38 : Le décalage de la tension de sortie de l'amplificateur opérationnel en fonction de l'amplitude de l'interférence RF de fréquence 100 MHz.

Ainsi, le courant différentiel général de sortie est formé par la différence entre les courants produits par M1-M2 et ceux produits par M3-M4. Par conséquent, tous les courants de

fréquence élevée (supérieure à la fréquence de coupure du filtre passe-haut CR) se trouvent diminués. La figure III-38 [1] montre que la dernière technique de conception de l'étage d'entrée induit à une diminution des décalages de la tension de sortie, dus aux interférences électromagnétiques, d'un facteur de dix.

Conclusion:

Dans ce chapitre, nous avons présenté des techniques et un ensemble de procédures pouvant améliorer la compatibilité électromagnétique d'un circuit intégré. Pour ce faire, il faut agir sur deux fronts : réduire les émissions électromagnétiques d'un circuit intégré et augmenter son immunité.

Pour réduire les émissions électromagnétiques des circuits intégrés, on a proposé plusieurs plans d'action. Pour les circuits numériques, on a vu qu'il était recommandé de répartir le signal d'horloge en plusieurs branches (arbres d'horloges). On a vu également qu'on pouvait moduler en fréquence le signal d'horloge, et que ceci permettrait de répartir son spectre de fréquence et de diminuer l'amplitude de ces composantes critiques. La diminution de la fréquence était une option également dans notre étude, cela dit, il ne faut pas ralentir excessivement le système afin qu'il puisse remplir correctement sa tâche. Enfin, toujours pour les circuits intégrés numériques, la conception de circuits asynchrone est préférable sur les circuits synchrone, du point de vue compatibilité électromagnétique, car elle évite les commutions simultanées des transistors. En ce qui concerne les circuits intégrés en général (numériques ou analogiques), on a constaté que la disposition des lignes d'alimentation VDD avec VSS de sortes qu'elles soient les plus proches possibles les unes des autres, l'augmentation des temps de montée et de descente des buffers d'entrée et la construction des bondings et des leads les plus courts possibles permettaient de réduire leurs émissions électromagnétiques.

Nous nous sommes également penchés sur plusieurs méthodes visant à augmenter l'immunité des circuits intégrés face aux agressions extérieures. Nous avons évoqué les blindages et les systèmes de protection contre les décharges électrostatiques ; nous avons également recommandé l'isolation des blocs les plus bruyants des parties les plus sensibles d'un circuit intégré. Nous avons évoqué le principe des logiciels défensifs, repris en détail dans le chapitre suivant. Nous avons également proposé d'ajouter un trigger de Schmitt aux entrées d'un circuit numérique afin que les signaux soient lissés ou, d'un autre point de vue, filtrés. Enfin, il a été montré que l'adoption de certaines méthodes de conception de certains circuits intégrés, tenant compte des problèmes CEM (dernier paragraphe), permettait d'améliorer leur immunité aux interférences électromagnétiques.

Nous avons également cité les capacités de découplage qui permettaient, à la fois, de réduire les émissions électromagnétiques et d'augmenter l'immunité d'un circuit intégré aux interférences électromagnétiques.

Bien sûr, l'évolution de l'électronique peut rendre caduques certaines de ces techniques parce que la miniaturisation sera de plus en plus poussée et le problème de la pollution de l'environnement en ondes électromagnétiques s'accentuera. Il faut donc veiller à faire évoluer

les techniques améliorant la compatibilité électromagnétique d'un système, intégré notamment, pour éviter les graves dysfonctionnements qui ont eu lieu dans le passé.

Chapitre IV :

Amélioration de l'immunité des circuits intégrés par des logiciels défensifs

Introduction :

Certaines applications où des dommages graves peuvent avoir lieu exigent une robustesse accrue face aux interférences électromagnétiques, ceci est souvent atteint en ajoutant des blindages matériels en guise de protection. Cependant, pour réaliser des fonctions électroniques complexes on recourt toujours à l'utilisation d'éléments « intelligents » tels que les microcontrôleurs qui exécutent des logiciels. On voit bien alors le bien-fondé d'utiliser ces logiciels en synergie avec les techniques matérielles afin d'améliorer la résistance des systèmes électroniques ainsi réalisés. A cause de l'efficacité (qui sera démontrée) de ces logiciels et du faible coût de leur implémentation, nous avons opté pour détailler ces techniques logicielles dites défensives, pour enfin conclure par un exemple de leur utilisation pour une application spécifique (mesure de la température d'un moteur d'une voiture).

Parmi les avantages apportés par ces logiciels, nous pouvons citer en premier une bonne complémentarité avec les solutions matérielles. En effet, dans certains cas, la modification du logiciel embarqué dans un microcontrôleur peut permettre au système de passer au-delà de certaines contraintes CEM sans avoir à intervenir sur le circuit électronique. De ce fait, le coût financier qui aurait pu être engendré par rapport à la conception d'une nouvelle carte est moindre. De plus, le temps de modification du logiciel est généralement plus court comparé à celui nécessaire pour modifier une carte électronique.

D'un autre côté, il faut prendre en considération l'impact de l'ajout des instructions constituant ces logiciels défensifs sur le temps d'exécution de l'application et sur l'espace mémoire supplémentaire nécessaire. Ces contraintes sont accentuées lorsqu'on est amené à réaliser des applications embraquées en temps réel.

Enfin, il est important de se rappeler que ces protections ne se substituent pas aux solutions matérielles, mais qu'elles sont complémentaires. Leur principal objectif est de détecter un dysfonctionnement afin de le traiter (quand c'est nécessaire) le plus rapidement possible, et dans les meilleures conditions afin que le système conserve un fonctionnement sûr. Cependant, il ne faut pas oublier que cette approche a des limites, par exemple, si une agression met hors fonctionnement le microcontrôleur, celle-ci ne peut être traitée par une méthode logicielle. Ces méthodes que nous préconisons restent néanmoins efficaces quand il s'agit de concevoir des systèmes de criticité moyenne ou pour lesquels le fabricant désirent augmenter la qualité du service ou la fiabilité face aux interférences électromagnétiques à des coûts raisonnables.

Dans les paragraphes qui vont suivre, nous distinguerons quatre catégories de logiciels défensifs selon leur domaine de "prédilection" : les logiciels défensifs destinés à gérer les entrées/sorties, ceux qui s'occupent de la gestion de la mémoire volatile, ceux dont le rôle est de surveiller le flot de contrôle et enfin les logiciels spécifiques à certaines applications. Toutes les techniques logicielles présentées ci-après sont focalisées sur des applications embarquées.

1) Gestion des entrées/sorties :

Les ports d'entrées/sorties sont le moyen de communication du microcontrôleur avec son environnement. Cependant, ils peuvent représenter l'accès par excellence aux différentes perturbations électromagnétiques. On sait également que le programme qui traite les données issues de l'extérieur (via les ports d'entrées) dépend de la qualité et de l'authenticité de ces informations. Ces agressions peuvent perturber le protocole des communications, la valeur des registres de contrôle de direction des ports, ou plus simplement leur gestion. Nous allons aborder successivement les moyens proposés pour améliorer la robustesse de ces trois points.

1-1) Les protocoles des communications :

Les perturbations imprévues des champs électromagnétiques ont toujours souillé les messages transmis via les canaux. Dès les balbutiements des communications numériques la question d'ajouter des bits supplémentaires pouvant indiquer la présence d'une erreur dans une séquence binaire transmise, ou encore mieux, pouvoir la corriger ont induit à la création de ces codes uniformisés et standardisés qu'on appelle communément : Les protocoles. Un exemple des plus simples est celui des bits de parité. C'est un bit supplémentaire ajouté aux bits représentant une information de sorte que si on effectue la somme (modulo 2) on obtienne un « 0 » ou un « 1 » selon une convention qui sera définie par l'émetteur et le récepteur. On prendra un exemple (figure IV-1) où la convention impose qu'il faille trouver un « 0 » comme résultat de la somme binaire de la séquence 101.

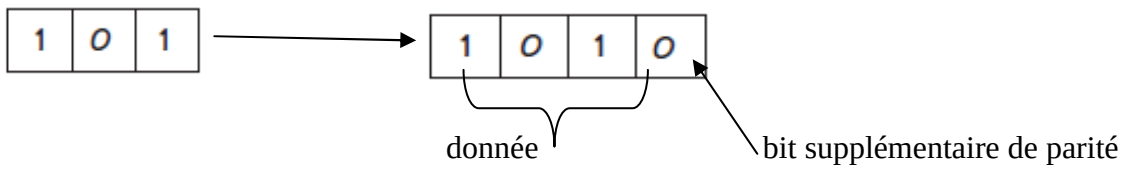


Figure IV-1 : Illustration de l'utilisation du bit de parité.

Malheureusement, cette méthode ne permet de détecter qu'un nombre impair d'erreurs dans une séquence binaire (donnée), ceci est illustré dans les exemples de la page suivante.

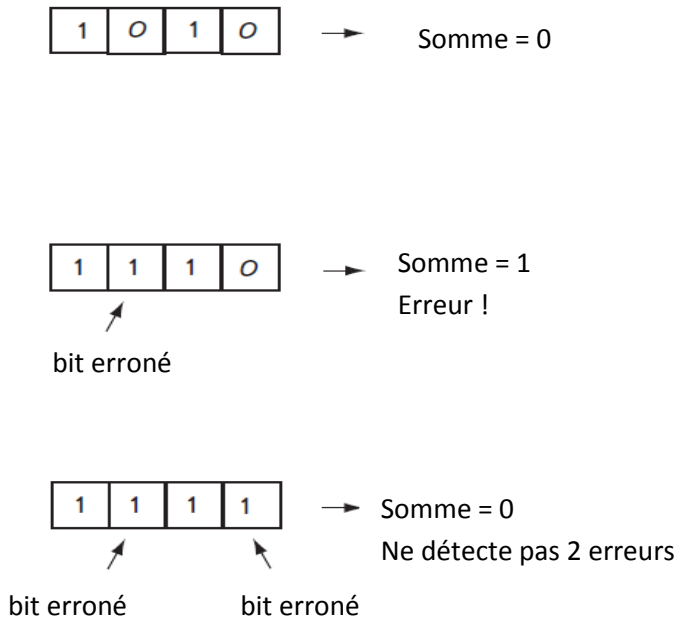


Figure IV-2 : Illustration de l'incapacité du bit de parité à corriger deux erreurs simultanées

Une variante de cette technique consiste à prendre les données sous forme matricielle (sous forme de tableaux) et effectuer les sommes modulo 2 suivant les lignes et les colonnes. Bien sûr, il n'y a détection d'erreur(s) que si le nombre d'erreurs simultanées est impair mais cette méthode présente l'avantage supplémentaire de corriger une erreur (une seule et unique). La figure IV-3 en illustre le principe.

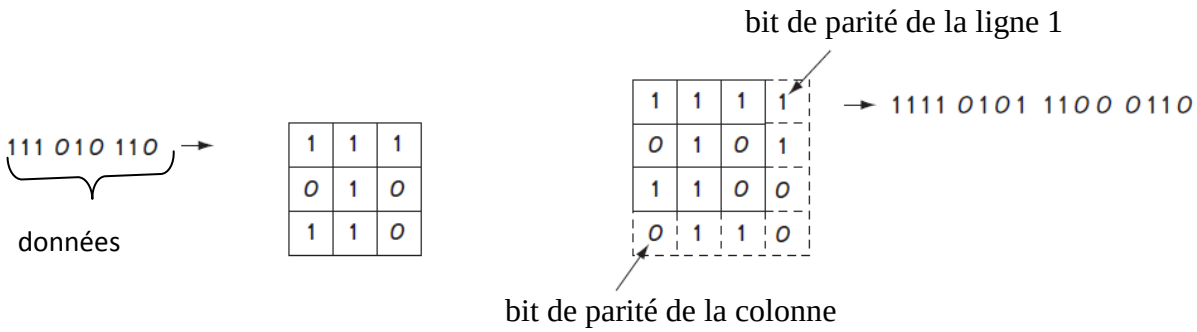


Figure IV-3 : Illustration de la méthode matricielle d'ajout des bits de parité.

Vu l'insuffisance de ces méthodes, de nombreux scientifiques se sont penchés sur la création de nouveaux protocoles qui soient capables de détecter et de corriger un nombre important d'erreurs. Ils devaient également prendre en considération les problèmes des rayonnements électromagnétiques et des couplages éventuels pouvant avoir lieu sur le support qui contient évidemment (s'il est filaire) un nombre important de conducteurs. Ainsi, dans certains protocoles non seulement on essaie de corriger les erreurs mais on choisit une forme de signal transportant la donnée de sorte à éviter de créer des erreurs éventuelles par diaphonie.

Pour résumer, un bon protocole est celui qui crée le moins d'erreurs par les différents couplages essentiellement magnétiques (en choisissant des formes de courant sur les différents conducteurs se compensant mutuellement), tout en transportant des bits pouvant indiquer et corriger un nombre important d'erreurs par les méthodes mathématiques et les algorithmes adéquats.

1-2) Les registres de contrôle de direction des ports :

Tous les microcontrôleurs actuels disposent de nombreux ports pouvant émettre des signaux avec lesquels des « organes » extérieurs tels un moteur ou un afficheur sont coordonnés. Ces signaux représentent des données dans le cas d'un afficheur et ils sont issus des ports appelés des sorties. Réciproquement, certains ports reçoivent des signaux représentant des données de l'extérieur qui seront exploitées dans le programme afin de faire fonctionner le système ainsi construit. Ces ports sont appelés des entrées. En fait, c'est les même ports qui servent d'entrées et de sorties et la décision appartient à l'utilisateur de choisir de les configurer en entrée ou en sortie, suivant l'application, par l'intermédiaire d'un registre de contrôle de direction (émission ou réception). Ces registres sont généralement situés à proximité des ports comme le montre la figure IV-4 [15], et cette position (proche de l'extérieur) pose le problème de les rendre vulnérables et donc facilement corruptibles par des éventuelles interférences électromagnétiques.

Pour prévenir toute corruption des valeurs du registre de direction qui serait catastrophique, une solution logicielle consiste les actualiser (les rafraîchir) régulièrement. Généralement, les programmes utilisent une fonction principale exécutée en boucle d'où la facilité évidente de la réinitialisation de la valeur du registre de contrôle (il suffit d'inclure l'initialisation dans la fonction principale qui s'exécute sans arrêt). Cette méthode n'est pas coûteuse en termes de temps et d'espace mémoire pour une vérification assez fiable tout de même.

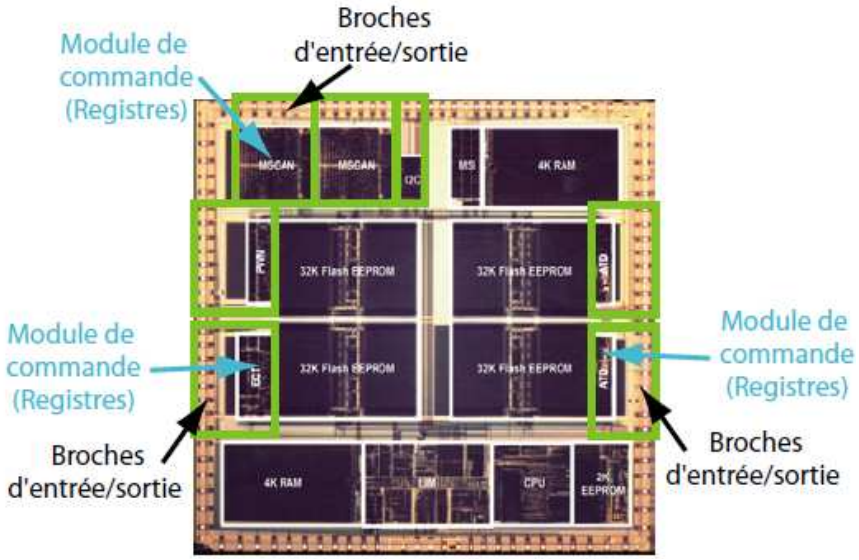


Figure IV-4 : Exemple d'un layout (disposition) d'entrée/sortie de microcontrôleur.

1-3) Gestion des données d'entrée :

Le traitement des données dépend de leur caractère qui peut être, soit analogique ou numérique. Par conséquent, nous détaillerons la démarche suivant les deux cas cités.

a) Les données analogiques :

Tous les phénomènes physiques sont des grandeurs continues et variables dans le temps, donc les transducteurs les interprétant en grandeur électrique en font ressortir un signal forcément analogique. Les techniques logicielles qui peuvent remédier à la vulnérabilité de ces données sont multiples, cependant, il existe des solutions génériques qui peuvent être appliquées à un grand nombre de cas sans avoir à changer le programme assurant la défense.

Une des techniques génériques pouvant être appliquée à un capteur interprétant des grandeurs physiques quelconques est la définition d'un domaine de validité. En effet, à partir de la connaissance des propriétés du phénomène physique et des caractéristiques du capteur (tension minimale et maximale pouvant être fournies à sa sortie), on peut définir facilement un domaine de validité de ces données. Cela signifie qu'on peut rejeter les valeurs qui sont à l'extérieur de ce domaine de validité. Le rejet de valeur prend ainsi en compte l'existence de perturbations électromagnétiques pouvant modifier temporairement les valeurs d'entrée.

D'autre part, quand la loi de variation de la réponse du capteur est connue avec précision, on peut écarter toute variation excessive entre deux mesures et l'interpréter comme résultant d'une valeur erronée. La figure IV-5 [15] illustre ces deux cas : dans la partie gauche, c'est le domaine de validité qui est connu ; et dans la partie droite, c'est la loi de variation de la réponse en sortie du capteur qui est connue.

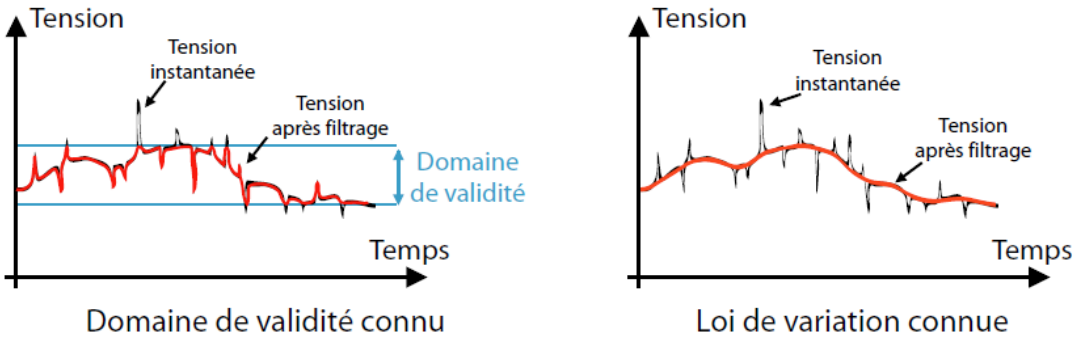


Figure IV-5 : Détection des données analogiques erronées.

Une autre solution, proposée par William, consiste à prendre un ensemble de valeurs et à effectuer une moyenne plutôt que d'utiliser la valeur brute de l'échantillon. Cette solution présente cependant quelques inconvénients, principalement dans le cas de systèmes temps réel. En effet, attendre plusieurs échantillons avant de traiter l'information, génère irrémédiablement un délai qui peut s'avérer être un handicap pour l'application. En contrepartie, plus le nombre d'échantillons est faible, plus le retard est court, mais plus l'incertitude sur la moyenne est grande.

Pour conclure sur le traitement logiciel des données analogiques, nous pouvons apparenter ceci à du traitement de signal et du filtrage numérique « traditionnels ». Mais la mise en forme du programme, surtout dans le cas de systèmes embarqués, peut revêtir une apparence bien différente dans le but de limiter la taille du code et le temps d'exécution.

b) Les données numériques :

Un processus de vérification similaire au traitement des données analogiques peut être mis en œuvre pour celui des données numérique. Ceci est vrai à condition que le signal d'entrée soit suffisamment lent au regard de la fréquence d'horloge du microcontrôleur, ce qui est bien souvent le cas. Ainsi, avant de traiter la valeur en entrée, on prélève plusieurs échantillons puis, suivant la criticité de l'application, on optera pour une des solutions présentées par la Figure IV-6 [15]. La partie de gauche correspond à la version de base sans protection et donc avec un traitement immédiat de l'information.

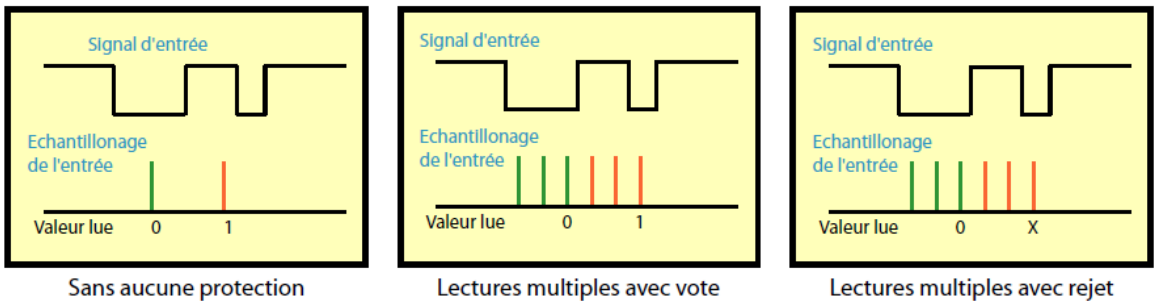


Figure IV-6 : Détection de données numériques erronées.

La partie centrale de la figure précédente, correspond à une lecture multiple avec vote pour fixer la valeur à considérer. Cette solution suppose obligatoirement l'existence d'un nombre d'échantillons impair pour pouvoir considérer une valeur majoritaire. Dans l'exemple pris, le nombre d'échantillons est de 3. On remarque que le premier tirage ne pose pas de problèmes puisque les trois échantillons ont tous la même valeur, à savoir 0. Par contre dans le second groupe, les deux premières valeurs sont à 1, tandis que la troisième est à 0. En conséquence, le 1 étant majoritaire, c'est cette valeur qui sera considérée comme étant exacte. Cette option présente notamment le grand avantage de ne pas avoir à effectuer des calculs, ce qui amenuise considérablement le temps d'exécution de cette routine. Un double compteur est suffisant : le premier pour compter le nombre d'échantillons, et le second, initialement nul, que l'on incrémente pour les valeurs 1 lues et qu'on décrémente pour les valeurs 0 lues. Le résultat du vote correspond au signe du compteur final : un nombre négatif correspond à un 0 et un signe positif à un 1. La partie de droite de la figure IV-6 suit un principe similaire à celle du centre, si ce n'est qu'il n'y a pas de vote. En effet, une valeur est considérée comme valide dans le cas où tous les échantillons (pris périodiquement, dans notre cas 3 par 3) sont identiques. Dans le cas contraire, le système rejette la valeur, il la considère comme indéterminée, et procède à un nouvel échantillonnage. Le principal avantage d'une telle solution est de traiter des valeurs avec un taux d'erreur faible si le nombre d'échantillons est suffisamment grand tout en ne demandant pas un temps d'exécution important puisqu'il n'y a pas de calcul.

En contrepartie, si l'entrée est instable pour une quelconque raison, le traitement sera d'autant plus retardé que cette instabilité perdure.

2) La gestion de la mémoire volatile (Random Access Memory) :

La RAM est un élément des plus importants dans un système à microprocesseur, elle permet le transite des données et leur circulation de façon accélérée. Il y a un nombre non négligeable de solutions qui ont été proposées dans le passé pour remédier aux corruptions, de données dans les RAM, éventuellement induites par des interférences électromagnétiques.

Une solution pour améliorer l'immunité de la RAM, consiste à dupliquer les données et puis effectuer le même traitement (une addition par exemple) pour les données originales et les copies. Si on aboutit au même résultat, bien sûr, on considérera les données traitées comme étant saines. Dans le cas contraire, on déclencherait une routine de traitement d'erreurs. Ce principe présente plusieurs inconvénients puisqu'il ralentit considérablement l'exécution d'un programme. De plus, cette méthode ne permet pas de corriger les erreurs éventuelles de façon à repartir avec des données saines.

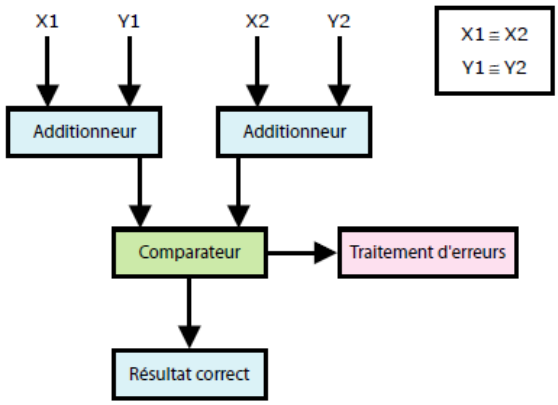


Figure IV-7 : Duplication des données et leur traitement par une simple addition.

Une autre solution, proposée par Coulson, consiste à stocker, cette fois-ci, les données dans un tableau et puis ajouter une variable qui contient la somme (somme de contrôle) de toutes les valeurs contenues dans le tableau. Avant chaque lecture, la somme de contrôle est recalculée et si sa valeur est restée inchangée, on considérera que toutes les valeurs contenues dans le tableau sont correctes. Bien sûr, dans le cas contraire il y aurait erreur. Par Ailleurs, toute nouvelle écriture **volontaire** est suivie d'une mise à jour de la somme de contrôle.

Cette technique présente les avantages d'être peu consommatrice en espace mémoire, tout en offrant la possibilité de recouvrir les données corrompues, ce qui est en bon accord avec les contraintes des systèmes embarqués. D'un autre point de vue, elle peut s'avérer relativement coûteuse en temps d'exécution si le nombre de variables est important. Dans ce dernier cas, il est fortement recommandé de scinder l'ensemble des variables en plusieurs tableaux de taille moindre, chacun ayant sa propre somme de contrôle et fonctionnant sur le principe

préalablement énoncé. En outre, pour alléger encore plus le code, on peut appliquer la technique uniquement aux variables considérées comme étant critiques.

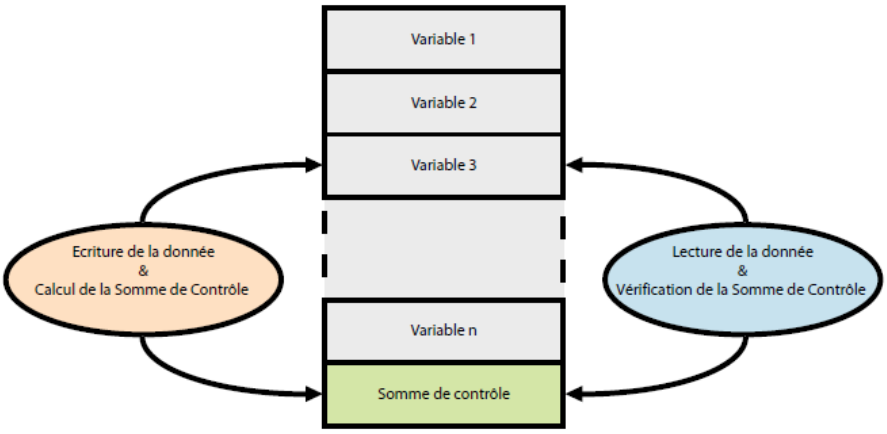


Figure IV-8 : Exemple de protection d'une RAM par le calcul multiple de la somme de contrôle.

L'emploi de l'une des méthodes citées nécessite une étude préalable des ressources nécessaires. De plus, quand on est amené à sélectionner les variables critiques, les critères de leur choix et même leur choix (avec des critères déjà définis) poseront parfois problème.

3) Gestion du flot de contrôle :

Le flot de contrôle correspond à l'ordre d'exécution des instructions d'un programme. Il est clair que si le programme s'exécute dans l'ordre imposé par le programmeur, et que s'il ne contient pas d'erreurs, il aboutira forcément au bon résultat.

L'ordre de toutes les séquences (une par une) à exécuter est contrôlé par un registre qui a pour contenu l'adresse de la prochaine instruction à s'être exécutée. Cependant, la perturbation du contenu de ce registre par une interférence électromagnétique peut induire à des erreurs très graves. C'est la raison pour laquelle, dans notre démarche, nous aborderons les techniques employées pour pallier à ce problème.

3-1) Vérification du flot de contrôle par signatures logicielles :

L'emploi de cette méthode présuppose que le programme soit composé d'un ensemble de fonctions et de procédures (blocs indépendants effectuant des tâches qui, en les combinant, constitue le programme). De plus, il ne faut pas qu'il y ait d'instructions de saut ou de branchement à l'intérieur de chaque bloc (bien sûr, le saut après la fin de l'exécution d'une fonction est autorisé). Enfin, à chaque bloc s'attribuera, lors de la compilation, une signature, notée s_i, et une différence de signature, notée d_i, qui lui sont propres.

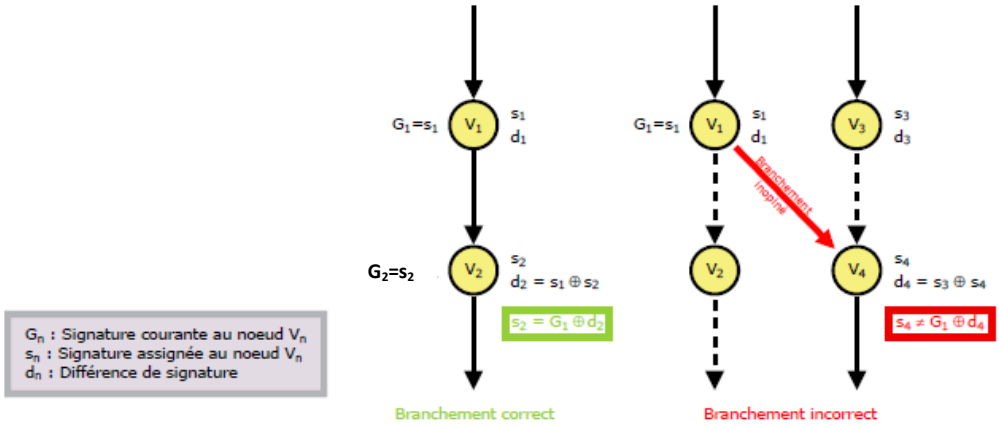


Figure IV-9 : Principe de vérification du flot de contrôle par signatures logicielles.

Durant l'exécution du programme (qui est composé de plusieurs fonctions), on utilisera un registre d'utilisation générale, noté G_n, pour stocker la signature du bloc (fonction ou procédure) en cours d'exécution. La figure IV-9 [15] illustre bien la méthode des signatures. Dans la partie gauche on suppose que le bloc V_1 est en train de s'exécuter. On lui assigne une signature (une valeur, un code…) s_1 qui est stockée dans le registre G_1. A la fin de l'exécution du bloc V_1, en supposant que c'est le bloc V_2 qui doive s'exécuter, on effectue une différence entre la signature précédente (s_1 dans notre cas) et la signature du bloc courant (s_2 qui est stockée dans le registre G_2). Cette différence est tout simplement calculée en utilisant un OU-Exclusif (XOR). Le résultat de la différence sera mémorisé dans un registre qu'on notera d_2. Cela dit, avant de procéder à l'exécution du bloc V_2, il faut veiller à vérifier que le résultat de la différence entre G_1 et d_2 est bien égal à s_2. Car il est évident que :

$$G_1 - d_2 = G_1 - (s_1 - s_2) = G_1 - s_1 + s_2$$

Or : $G_1 = s_1$. Il est clair qu'on doit retomber sur s_2 comme résultat si le branchement est correct, c'est-à-dire que le registre de contrôle contient la bonne adresse et n'a pas été corrompu. Dans le cas contraire, on se brancherait sur une routine de traitement d'erreurs d'exécution.

Cette technique présente de nombreux avantages puisqu'elle peut être implémentée directement dans un compilateur et donc être indépendante du programmeur. De plus, si la taille des blocs n'est pas trop petite, le temps de calcul ne pénalise alors pas trop le déroulement de l'exécution. En contrepartie, le fait de réserver un registre spécifiquement pour cette fonction, réduit son utilisation aux processeurs d'architectures RISC, dont le nombre de registres est déjà assez réduit. Dans le cas d'un processeur CISC, l'exécution risque d'être très fortement pénalisée en termes de temps, vu le nombre d'instructions (important) dont ils disposent et dont le décodage est forcément plus lent que les processeurs RISC.

3-2) Les marqueurs de passage :

Le principe des marqueurs de passage (figure IV-10 [15]) est relativement similaire à celui de la vérification du flot de contrôle par des signatures logicielles. En effet, chaque fonction ou procédure est affectée d'un identificateur ou marqueur qui lui est propre. Par contre, il n'y a pas de contrainte concernant les instructions de branchement ou de saut dans un bloc, c'est-à-dire : des branchements ou des sauts peuvent être utilisés sans aucun problème même si l'exécution de la fonction en cours n'est pas complètement terminée.

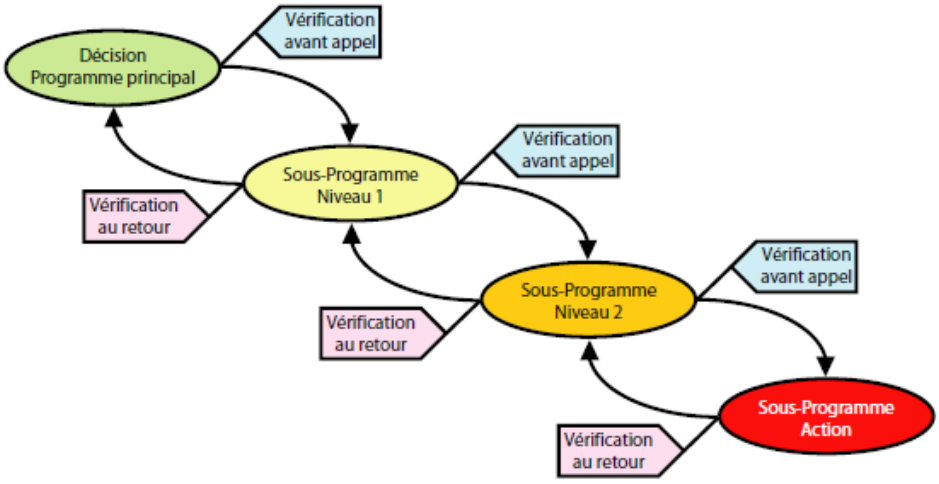


Figure IV-10 : Principe de fonctionnement des marqueurs de passage.

Durant l'exécution, lorsqu'un changement de procédure est nécessaire, le bloc appelant vérifie que le marqueur courant correspond bien au bloc dans lequel il se situe. Puis, il modifie la valeur du marqueur courant pour prendre la valeur du bloc appelé. Une fois le saut effectué, le nouveau sous-programme regarde la validité du marqueur. Si sa valeur correspond à celle du bloc, les instructions sont exécutées. Dans le cas contraire, le programme est dérouté vers un sous-programme de traitement d'erreurs. Lors du retour au programme initial, des vérifications semblables sont également effectuées.

Enfin, si un bloc est relativement long avant d'effectuer un appel à un sous-bloc, il est possible d'insérer un contrôle de marqueur intermédiaire, de façon à vérifier que le flot de contrôle n'a pas été perturbé.

3-3) Remplissage de la mémoire programme non utilisée :

Il est très rare que la totalité de la mémoire programme soit occupée par une application logicielle, c'est la raison pour laquelle il faut songer à l'occuper même si cela semble, *a priori*, inutile et absurde. En effet, si le registre qui contient l'adresse de la prochaine instruction à exécuter a été corrompu par une éventuelle interférence électromagnétique, et que de surcroît, l'adresse pointée (corrompue) se situe en dehors de la zone mémoire allouée au programme ; si, malencontreusement, la case mémoire pointée contient une valeur

(en général une valeur de la forme hexadécimale FFFF) qui décrit une instruction valide, le microcontrôleur exécutera cette instruction rendant ainsi son comportement imprévisible.

Afin de remédier à ce problème d'errance incontrôlée, diverses solutions sont envisageables. La première consiste à mettre dans toute la mémoire inutilisée l'instruction STOP qui met un terme à l'exécution du programme et place le microcontrôleur dans un état de latence. Afin que cet état ne perdure pas indéfiniment, un chien de garde externe est nécessaire. Son rôle est de contrôler en permanence la présence d'activité du microcontrôleur. Son compteur s'incrémente à chaque cycle d'horloge, et si celui-ci n'est pas remis à zéro, régulièrement, (avant d'arriver à une valeur qui sera fixée par l'utilisateur) il générera un reset. Cette réexécution du programme rend finalement quasi-inaperçue la présence d'éventuelles dérives.

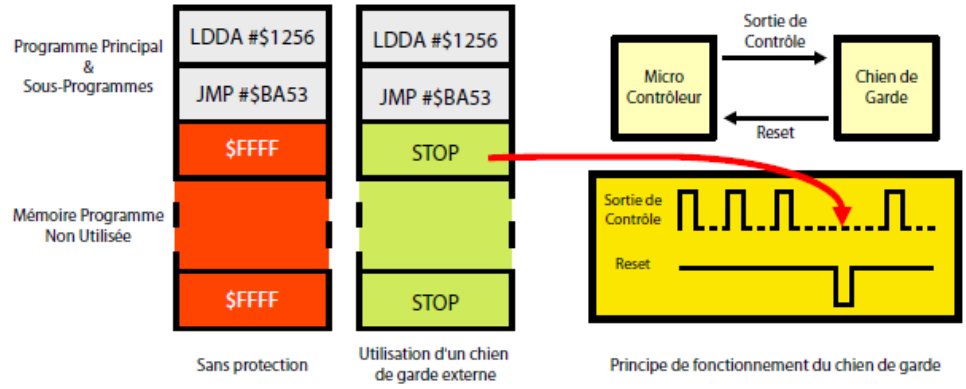


Figure IV-11 : Remplissage de la mémoire morte par des instructions STOP.

Le principal inconvénient de cette méthode est le recours à un circuit externe. En effet, cela signifie la présence d'une liaison électrique et donc la possibilité qu'une perturbation électromagnétique vienne s'y coupler et générer un reset impromptu. Le chien de garde existe dans la plupart des microcontrôleurs récents, ce qui donne l'assurance d'un redémarrage propre. Cela dit, dans l'absence d'un circuit chien de garde interne, le problème des interférences peut être contourné en n'ayant plus recours au circuit chien de garde mais à une série d'instructions NOP (NO Operation) terminée par un saut à l'adresse de reset. D'un autre côté, si la taille de la mémoire morte (inutilisée) est importante, le temps de latence augmentera, et pourrait bien ainsi porter préjudice au comportement du système conçu.

Afin de limiter au maximum ce temps d'improductivité, il est préférable de remplacer la série d'instructions NOP par des instructions de saut JMP à l'adresse de reset. Les conditions requises pour une mise en place satisfaisante sont :

- La connaissance du code de l'instruction de saut.
- La possibilité de définir l'adresse de reset, ce qui est très souvent le cas avec les microcontrôleurs modernes, et surtout, que cette adresse soit identique au code de l'instruction de saut tout en étant en zone de mémoire programme, ce qui n'est pas toujours compatible.

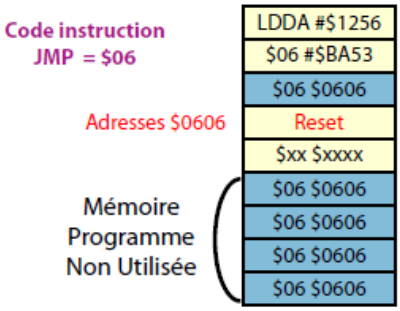


Figure IV-12 : Remplissage de la mémoire morte avec des instructions JMP (JuMP).

Parmi toutes les techniques existantes, c'est la seule qui ne nécessite aucun surcoût que ce soit au niveau du temps d'exécution ou de l'espace mémoire utilisé, puisqu'elle ne nécessite aucun calcul et elle n'utilise comme espace mémoire que celui qui, normalement, ne devrait pas être utilisé par l'application.

4) Les techniques de détection d'erreurs spécifiques à certaines applications :

Nous venons de citer une panoplie de méthodes qui sont génériques, mais comme vous l'imaginez bien, les solutions qui ne sont applicables qu'à une application particulière sont beaucoup plus nombreuses. C'est la raison pour laquelle nous n'en ferons pas une citation exhaustive mais nous nous limiterons à donner quelques exemples donnant une idée basique sur les techniques employées.

Pour prendre un premier exemple, supposons que nous ayons un programme utilisant deux variables Min et Max contenant les valeurs minimales et maximales d'une grandeur physique quelconque, convertie en électricité par un capteur. Alors, il est clair que si la valeur de Min dépasse celle contenue dans Max, nous avons bien une erreur qui pourrait être induite par des interférences électromagnétiques.

L'exemple précédent concernait les données, la détection d'une éventuelle erreur se basait sur l'idée de trouver une contradiction entre deux valeurs (valeurs dont l'ordre est connu) contenues dans deux variables. Et si on appliquait la même idée (trouver une contradiction évidente dans l'ordre) au flot de contrôle. Supposant qu'on ait dans un programme gérant les communications. Supposons également que le sous-programme transmettant la première donnée qui s'exécute avant le sous-programme établissant la connexion avec le récepteur. Il est évident qu'on a là aussi une erreur d'ordre chronologique évidente qu'on peut facilement détecter.

En fait, l'implémentation de ces techniques n'est pas spécifique à la détection des erreurs survenant sur une plateforme matérielle, sujet qui nous concerne; elles sont, en fait, développées pour détecter des fautes de conception dans les programmes.

Même si ces techniques de détection d'erreurs ont été introduites pour une toute autre raison, il serait néanmoins intéressant de juger l'efficacité de leur capacité à détecter les dysfonctionnements dus aux agressions électromagnétiques.

5) Exemple d'utilisation de logiciels défensifs et degré de leur efficacité :

Nous allons à présent exposer les bienfaits de deux techniques logicielles (l'une assez élémentaire et l'autre légèrement plus élaborée) sur une application à la base d'un microcontrôleur Motorola HC12. Les logiciels qui seront décrits ont été implémentés en langage C. Le système décrit dans la figure IV-13 [15] est un thermomètre chargé de contrôler la température du moteur d'une voiture. Une alarme sera déclenchée dans le cas d'une température jugée critique (au-delà ou en-deçà d'un certain seuil). Le système est constitué de :

- Un capteur de température qui « traduit » les variations de la température en variations électriques.
- Un convertisseur analogique-numérique (embarqué au microcontrôleur) qui transforme le signal analogique, décrivant la grandeur continue qu'est la température, en grandeurs discrètes (donnés numériques) pouvant être traitées par un microcontrôleur.
- Une alarme qui est peut être déclenchée par le microcontrôleur et qui peut être un simple voyant (une simple LED) qui s'allume pour indiquer que l'alarme est déclenchée.

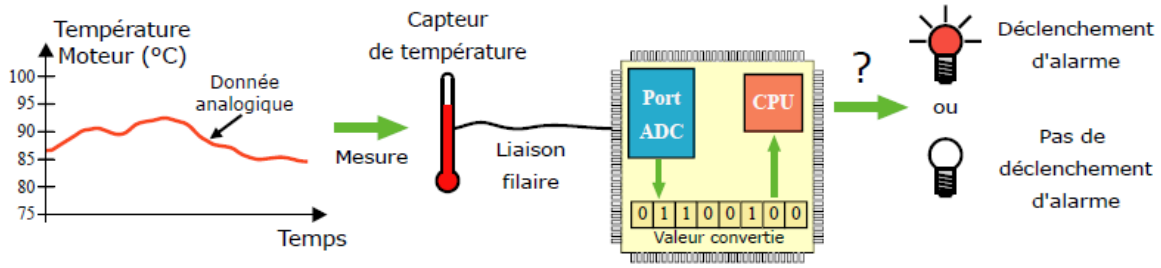


Figure IV-13 : Schéma de principe d'un système de mesure d'une température avec alarme.

Ceci étant, puisque notre but est de tester l'efficacité de la capacité des solutions logicielles à lutter contre les problèmes dus aux interférences électromagnétiques, nous allons « agresser » volontairement notre microcontrôleur en superposant au signal utile un signal perturbateur comme le montre la figure IV-14 [15].

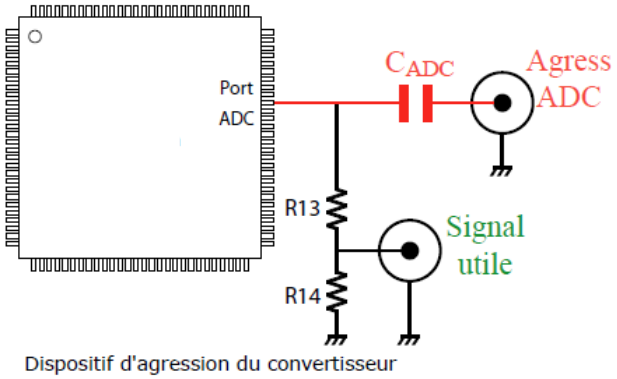


Figure IV-14 : Dispositif de test soumis à des agressions.

Dans un but de commodité, puisque le but recherché n'est pas la mesure d'une température, au lieu d'utiliser un capteur de température mesurant la température (du moteur) dans une voiture, un générateur suffira. Son signal doit varier lentement (comme une température) auquel on superpose un signal perturbateur dont la puissance est, bien sûr, connue à tout instant. Le pont résistif constitué par R13 et R14 (voir la figure IV-14) a pour vocation de limiter la propagation du signal d'agression vers le générateur de signaux. Il favorise ainsi la superposition du signal agresseur au signal utile **à l'entrée du convertisseur**. Enfin pour l'alarme, il suffit d'ajouter une LED qui s'allumera pour indiquer qu'une alarme est déclenchée.

5-1) Considérations préliminaires :

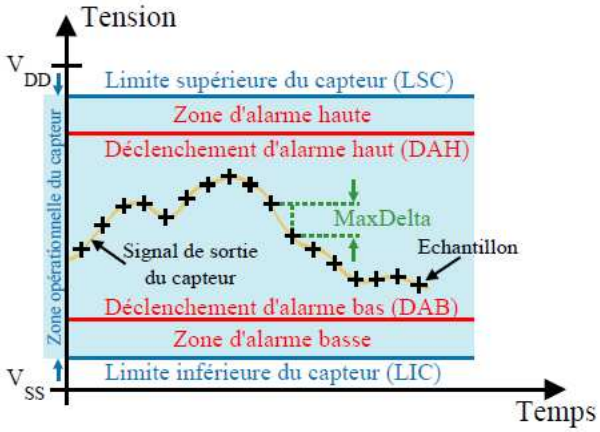


Figure IV-15 : Définition de certains paramètres génériques propres aux capteurs.

La figure ci-dessus [15] illustre certains paramètres que nous aurons à utiliser dans notre démarche. Il est vrai que les capteurs dépendent de la technologie dans laquelle ils sont fabriqués, ils possèdent une zone de tension dans laquelle ils sont opérationnels. Cette zone est délimitée par deux paramètres :

- Une limite supérieure du capteur (LSC) qui correspond à la tension maximale que peut fournir sa sortie.
- Une limite inférieure du capteur (LIC) qui représente le niveau minimum de tension que peut atteindre sa sortie. Généralement ce niveau est celui de la masse.

De plus, de tels composants analogiques sont caractérisés par leur temps de réponse. C'est la raison pour laquelle chaque capteur possède une variation maximale entre deux échantillons notée MaxDelta.

Ajoutons deux autres niveaux indépendants des caractéristiques physiques du capteur, qui sont nécessaires à l'application choisie qui sont bien sûr:

- Le niveau de déclenchement d'alarme haut (DAH) qui délimite la partie basse de la zone d'alarme haute. Autrement dit, une tension de sortie de capteur au-delà de ce niveau de tension est génératrice d'alerte. C'est typiquement ce niveau que l'on considère pour signaler au conducteur ou à d'autres systèmes une température moteur excessive.
- Le niveau de déclenchement d'alarme bas (DAB) qui représente le niveau minimum que le signal du capteur peut avoir avant de pénétrer dans la zone d'alarme basse. De façon similaire au DAH, une tension de sortie de capteur en-deçà de ce niveau génère une alerte. Par exemple, ce paramètre permet d'avertir le conducteur de l'éventuelle présence de verglas sur la chaussée.

La fréquence d'échantillonnage est fixée à 35 kHz [15], soit une période légèrement supérieure à 28 µs. Ce temps entre deux conversions a été déterminé pour être en accord avec plusieurs paramètres. Le premier correspond à l'échantillonnage d'une température : les variations étant relativement lentes, quelques points de mesure suffisent. Par ailleurs, le convertisseur (du microcontrôleur considéré) ne peut être utilisé avec des fréquences d'échantillonnage inférieures à 20 kHz. Enfin, le dernier paramètre est lié au temps nécessaire pour exécuter les instructions de traitement de la valeur convertie. L'objectif étant d'avoir un échantillonnage périodique constant, il est nécessaire de finir le traitement de la valeur courante avant l'arrivée de la suivante. Ce temps est dépendant du logiciel de test embarqué. Par conséquent, nous avons considéré le pire cas, c'est-à-dire celui qui requiert le temps d'exécution maximum (Figure IV-16 [15]).

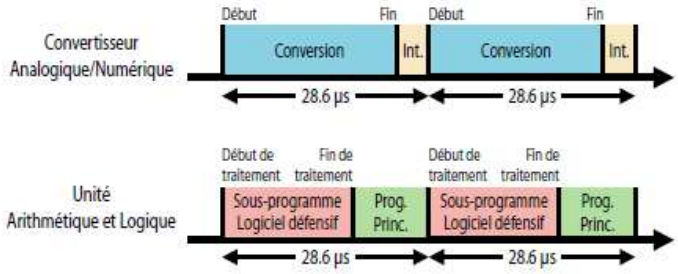


Figure IV-16 : Répartition du temps dans l'application.

Revenons à présent au signal qui simule celui du capteur, bien entendu, celui-ci doit être en parfait accord avec la nature du phénomène physique (la température) et son caractère lent. Le signal triangulaire périodique est tout à fait adapté pour remplacer de vraies mesures de températures qui sont absolument facultatives. L'allure et les caractéristiques du signal choisi sont illustrées par la figure IV-17 [15].

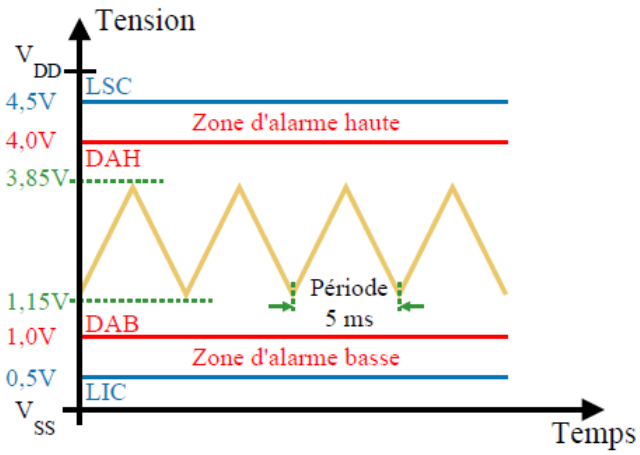


Figure IV-17 : Signal simulé de la sortie du capteur de température.

Enfin, le choix d'un signal triangulaire périodique n'est pas anodin. En effet, même si dans le cas de l'évolution de la température d'un moteur, les pentes ascendantes et descendantes n'ont pas des valeurs identiques, on peut facilement en donner une approximation linéaire.

Avant de passer aux logiciels défensifs proposés, une dernière discussion s'impose sur le signal d'alarme. Il paraît, *a priori*, que le choix du signal d'alarme est évident et aussi simple qu'un état haut à la bonne broche du microcontrôleur déclencherait l'alarme, et un état bas voudrait dire que la température est normale. Mais, un problème se posera dès que le microcontrôleur vient à sortir du flot de contrôle de l'application à cause d'une interférence électromagnétique par exemple. En plus, il est fort probable que la sortie ne soit pas rafraîchie et par conséquent le système de contrôle ne pourra détecter le dysfonctionnement résultant. En conséquence, le signal d'alarme doit présenter trois états. Deux états qui reflètent l'absence d'alarme et le bon fonctionnement du microcontrôleur, ce qui peut être réalisé par un signal carré périodique. Un troisième état qui indique le déclenchement d'une alarme, pour effectuer ceci, il faut interrompre la régularité du précédant signal. Pour plus de facilité, le signal sera synchronisé (de façon logicielle) à celui du convertisseur analogique-numérique. Le signal choisi respectant toutes les contraintes précédemment citées est illustré par la figure IV-18 [15].

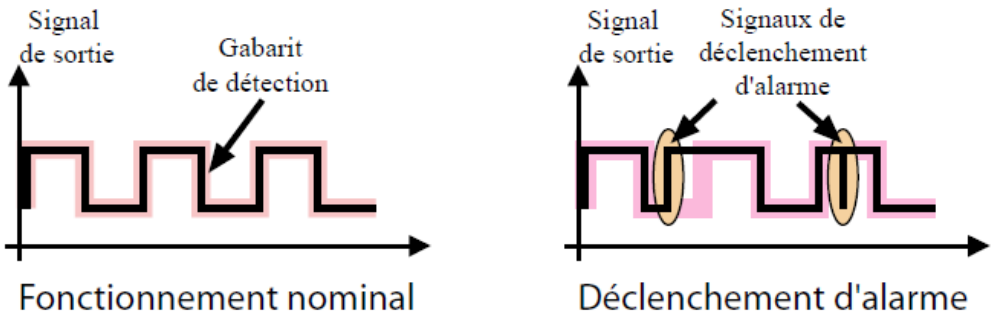


Figure IV-18 : Caractéristiques du signal d'alarme.

La génération de tels signaux est relativement simple à mettre en œuvre. En effet, nous partons du principe que la conversion qui vient d'être effectuée ne déclenche pas d'alarme. Donc dans un premier temps, le signal de sortie est juste complémenté par rapport à l'état de la sortie précédente. Ceci nous permet d'obtenir ainsi un signal périodique puisqu'il repose sur la fréquence d'échantillonnage du convertisseur analogique numérique. Dans un second temps, on regarde si le signal dépasse l'un des seuils de déclenchement. Si tel est le cas, nous forçons la sortie une fois à l'état bas puis une fois à l'état haut réalisant ainsi une sortie de gabarit. Il y aura donc une rupture de la régularité quelque soit l'état logique courant. Ceci est illustré en détail par l'organigramme de la figure IV-19 [15]. Ce programme nous servira, en fait, de référence pour confirmer ou infirmer l'efficacité des solutions logicielles qui seront ultérieurement proposées.

Le signal qui est utilisé à l'entrée du microcontrôleur et qui est composé du signal auquel on superpose un signal nuisible simulant les perturbations électromagnétiques environnantes est représenté sur la figure IV-20 [15].

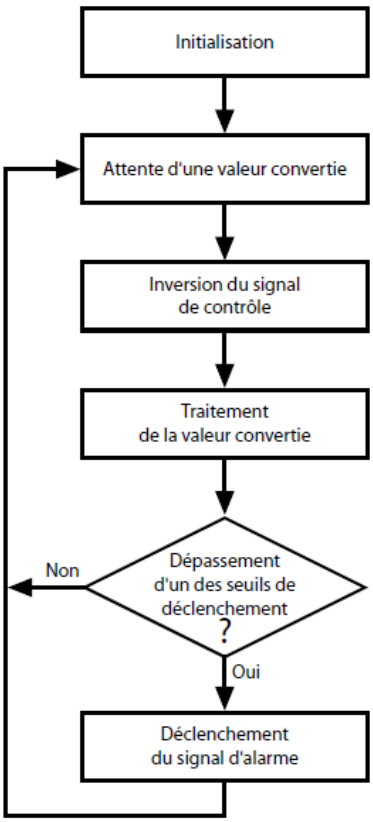


Figure IV-19 : Organigramme du logiciel embraqué de base (sans protection).

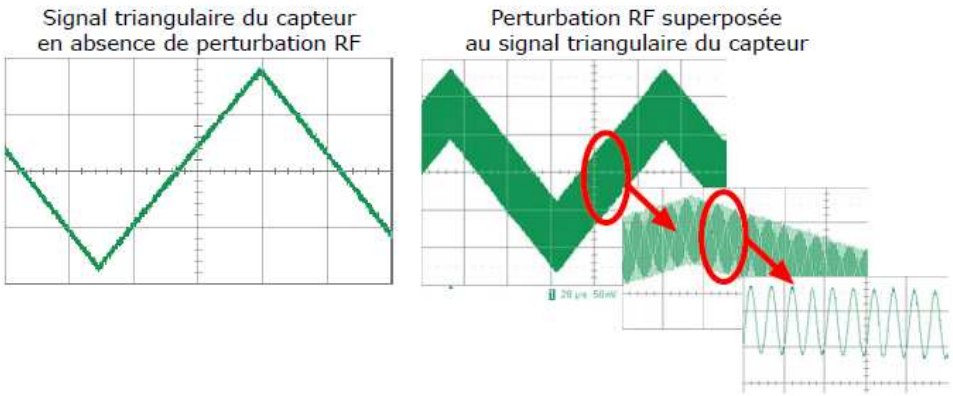


Figure IV-20 : Superposition du signal d'agression au signal utile.

5-2) Logiciels défensifs ajoutés à l'application de base :

Maintenant que nous avons décrit l'application ainsi que le logiciel conventionnel (de base), nous allons pouvoir nous focaliser sur les logiciels embarqués à caractère défensif. Les paragraphes suivants présentent les deux versions testées et dont le niveau de complexité est différent. Bien que différentes dans leur réalisation, l'approche n'en reste pas moins semblable et constituée de deux étapes. La première repose sur la détection d'erreur selon des critères que nous préciserons. La seconde consiste à prendre la ou les décisions en fonction de la situation rencontrée.

a) Logiciel défensif de bas niveau (low defensive software) :

Cette première version de logiciel défensif est basée sur une seule et unique caractéristique du capteur, en l'occurrence, le domaine de validité en tension. En effet, comme l'illustre la figure IV-21 [15], l'application définit cinq zones qui peuvent, par leur nature, être regroupées en trois sections :

- Une section de fonctionnement nominal.
- Une section de déclenchement de l'alarme.
- Une section impossible.

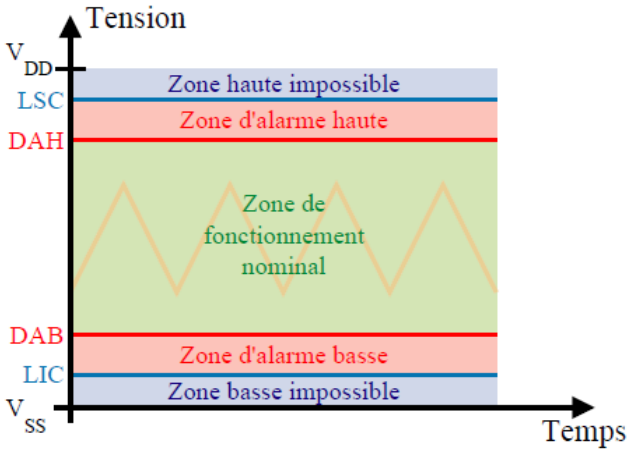


Figure IV-21 : Différentes zones que peut prendre le signal de l'application.

Les zones impossibles peuvent être exploitées pour détecter une erreur, du fait qu'elles constituent des valeurs de tension que le capteur ne peut fournir. Ainsi, un échantillon qui aurait une valeur comprise dans ces zones n'aurait pas de signification pour l'application. La définition de ces zones permet donc de déterminer une première protection logicielle qui sera incluse dans le logiciel défensif de bas niveau (low defensive software). On peut également penser à ajouter un second critère relatif à la prise de décision. Contrairement au logiciel conventionnel, une alarme sera considérée comme telle qu'à partir du moment où plusieurs échantillons auront été successivement mesurés dans une même zone d'alarme. Cela vient du fait que de fausses alarmes peuvent survenir à cause d'une perturbation quelconque, donc il serait intéressant de contrer ce problème. La variable AlarmNbr reflète le nombre d'échantillons successifs qui ont été prélevés en zone d'alarme. Et la constante MaxAlarm correspond au nombre maximum « d'alarmes » que l'on considère avant de déclencher le signal d'alarme. L'organigramme ainsi obtenu est présenté à la figure IV-22 [15]. A chaque fois qu'une nouvelle valeur est convertie, on regarde sa zone d'appartenance. Dans le cas où la valeur appartient à l'une des zones d'alarme, un test conditionnel supplémentaire est effectué pour savoir si l'on a dépassé MaxAlarm détections successives. Si tel est le cas, il y a déclenchement d'alarme, sinon le compteur courant est incrémenté. Dans tous les autres cas, le compteur courant est réinitialisé à zéro.

Il est à noter que l'ordre des tests conditionnels est relativement important, d'autant plus lorsqu'il s'agit d'une application temps-réel. En effet, de cet ordre dépendra la longueur du traitement et, par conséquent, le coût supplémentaire en temps d'exécution généré par l'utilisation d'un logiciel défensif.

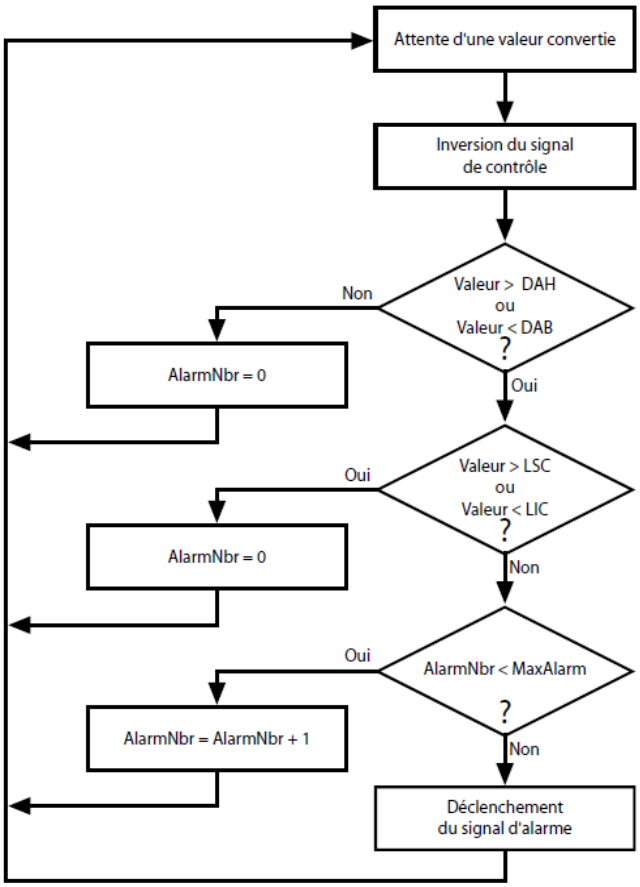


Figure IV-22 : Organigramme du logiciel défensif de bas niveau (low defensive

b) Logiciel défensif de niveau moyen (medium defensive software) :

La mise en œuvre de ce logiciel est relativement simple, puis qu'il s'agit d'une amélioration de la version de bas niveau en ajoutant un test supplémentaire portant sur la variation du signal échantillonné. On suppose que la variation entre deux échantillons ne peut excéder une variation maximale MaxDelta, fixée en accord avec la réponse du capteur. La variable ValeurPrec correspond à la valeur précédente de l'échantillon dont la valeur a été considérée comme correcte. Enfin, la variable Delta correspond à la valeur absolue calculée de la variation entre deux échantillons et qui, bien sûr, ne doit absolument pas dépasser la valeur contenue dans MaxDelta.

La figure IV-23 [15] présente l'organigramme ainsi obtenu. Les parties supérieure et inférieure sont similaires à celle de l'algorithme du low defensive software (logiciel défensif de bas niveau), avec l'ajout d'une mise à jour de la variable ValeurPrec. La partie intermédiaire correspond au test conditionnel spécifique au medium defensive software (logiciel défensif de niveau moyen) que nous venons juste d'expliciter.

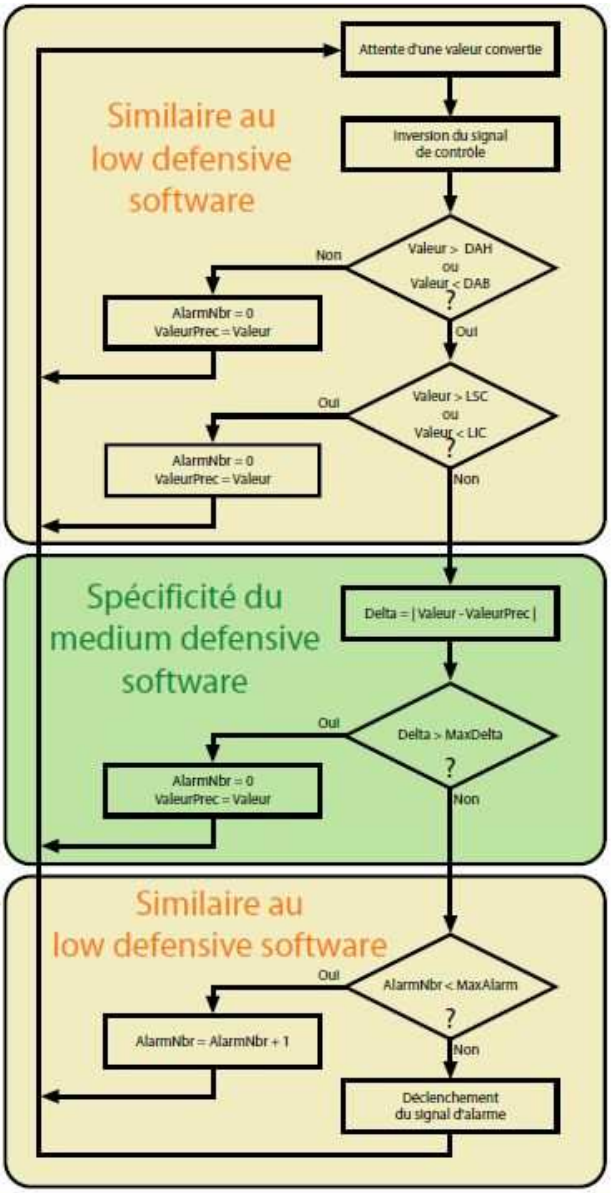


Figure IV-23 : Organigramme du logiciel défensif de niveau moyen (medium defensive software)

5-3) Confrontation entre les résultats des mesures pour chaque version logicielle :

Avant de passer aux résultats qui montrent l'efficacité des logiciels défensifs cités précédemment, il est d'abord nécessaire de définir, au préalable, certains paramètres utilisés dans la suite. Pour l'instant, les valeurs par défaut qui seront prises en considération dans les résultats empiriques sont incluses dans le tableau IV-1 [15] :

Paramètres	Valeur par défaut	Logiciels
MaxAlarm	3	*Low* et *Medium defensive softwares*
MaxDelta	100%	*Medium defensise software*

Tableau IV-1 : Valeurs par défauts des paramètres des logiciels défensifs testés.

Avant de passer à la suite, il est nécessaire de lever l'ambiguïté sur le paramètre MaxDelta. En effet, l'expression d'une donnée en pourcentage peut s'avérer peu explicite. La figure IV-24 [15] présente la définition que nous avons donnée à MaxDelta.

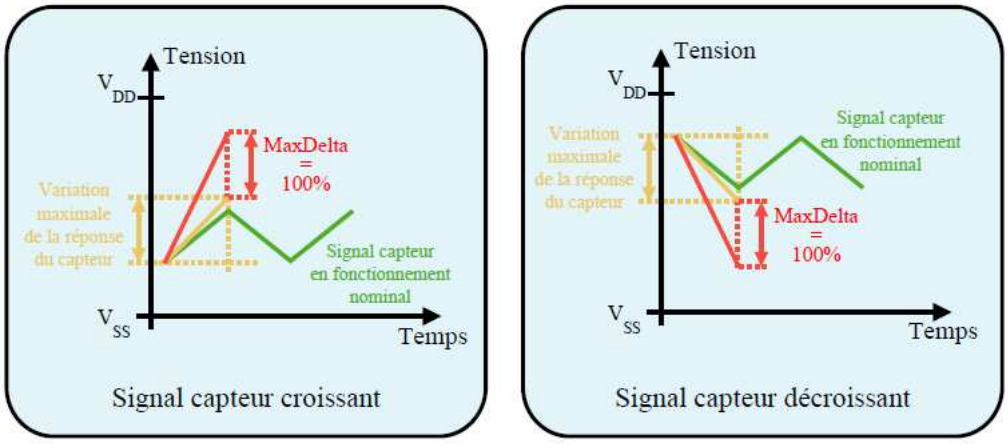


Figure IV-24 : Définition de la valeur en pourcentage de la variable MaxDelta.

Précisons cette définition pour le cas d'un signal capteur croissant, celle d'un signal décroissant se déduisant de manière analogue. Considérons la variation maximale de la réponse du capteur, c'est-à-dire la caractéristique indiquée par le fabricant. L'échantillonnage s'effectuant à fréquence constante, seule la variation de tension nous importe. MaxDelta correspond au pourcentage de tension que l'on ajoute à la variation maximale de la réponse du capteur. Si l'on considère un MaxDelta de 100%, cela signifie que tant que la variation entre deux échantillons ne sera pas supérieure au double de la variation maximale capteur, on considèrera la variation comme valide. Dans le cas contraire, elle sera considérée comme étant due à un dysfonctionnement du capteur ou à une perturbation électromagnétique.

Toutes les variables étant initialisées, nous pouvons à présent donner les résultats qu'ont apportés les solutions logicielles (implémentées avec les valeurs par défaut définies ci-dessus) déjà décrites.
Dans la figure ci-dessous [15], l'axe des abscisses définit les fréquences des agressions RF sur le microcontrôleur, et l'axe des ordonnées mesure la puissance minimale pouvant induire des perturbations dans l'application réalisée.

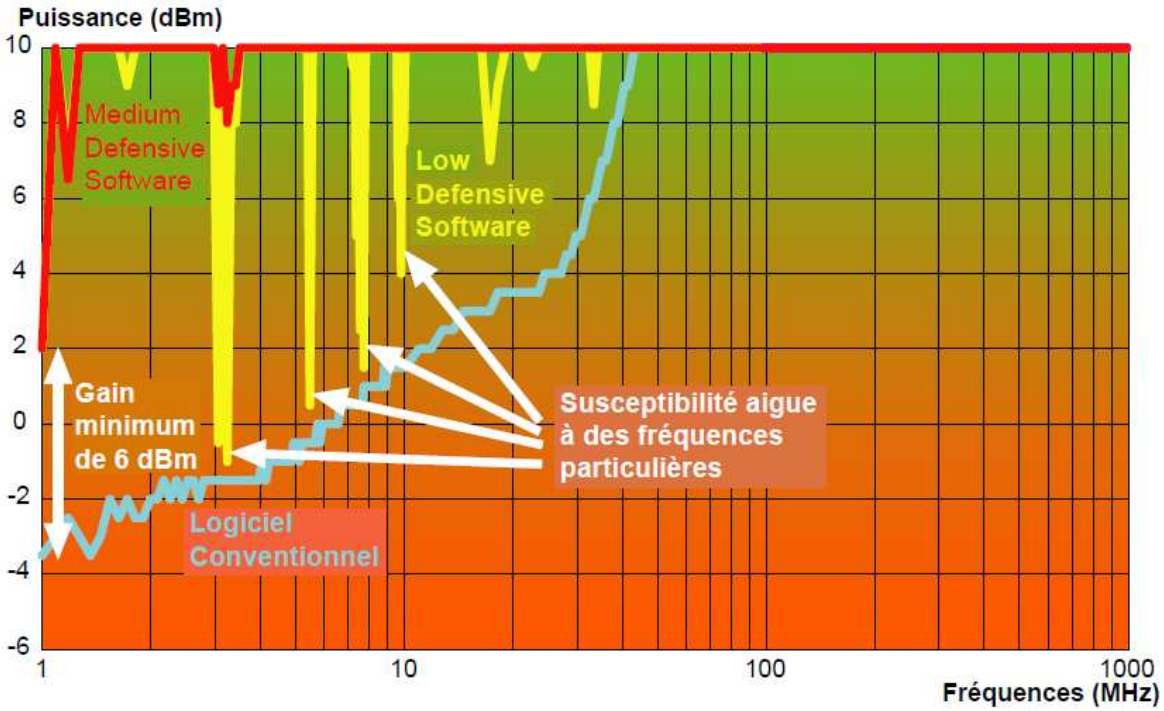


Figure IV-25 : Comparaison des logiciels implémentés avec les paramètres par défaut.

D'après la figure ci-dessus, le low defensive software s'avère être d'une assez bonne efficacité sur l'ensemble de la plage de fréquences. Cependant pour certaines fréquences, le déclenchement d'alarme a lieu pour un niveau de perturbation identique à celui du logiciel conventionnel. Ces fréquences semblent être des multiples et des sous-multiples de la fréquence d'horloge du microcontrôleur utilisé. Ce qui se conçoit relativement bien puisque l'horloge du convertisseur analogique-numérique est directement dérivée de l'horloge principale.

En ce qui concerne le medium defensive software, les résultats obtenus sont bien plus encourageants, puisque l'on obtient au minimum un gain d'immunité de 6 dBm sur l'ensemble de la plage de fréquence testée. Ce gain est même porté à 10 dBm si l'on fait abstraction de la mesure faite à 1 MHz.

Quelque soit le logiciel défensif utilisé, il est intéressant de remarquer que la susceptibilité du composant analogique n'est plus uniforme sur l'ensemble de la bande de fonctionnement. De plus, la forte dépendance du convertisseur de l'horloge interne fait que l'on peut rendre prédictible une baisse d'immunité à certaines fréquences.

Maintenant que nous avons vu l'efficacité de ces logiciels et la supériorité notable du medium defensive software sur sa version la plus basique, on peut également tester le bien-fondé de faire varier certains paramètres, afin de mettre en évidence l'éventuelle influence que cela pourrait engendrer.

On se propose de reprendre le logiciel défensif de niveau bas (low level defensive software), mais cette fois-ci, en faisant varier le paramètre MaxAlarm. La figure IV-26 [15] montre les résultats obtenus pour MaxAlarm = 3 (valeur par défaut prise comme référence) et MaxAlarm = 10.

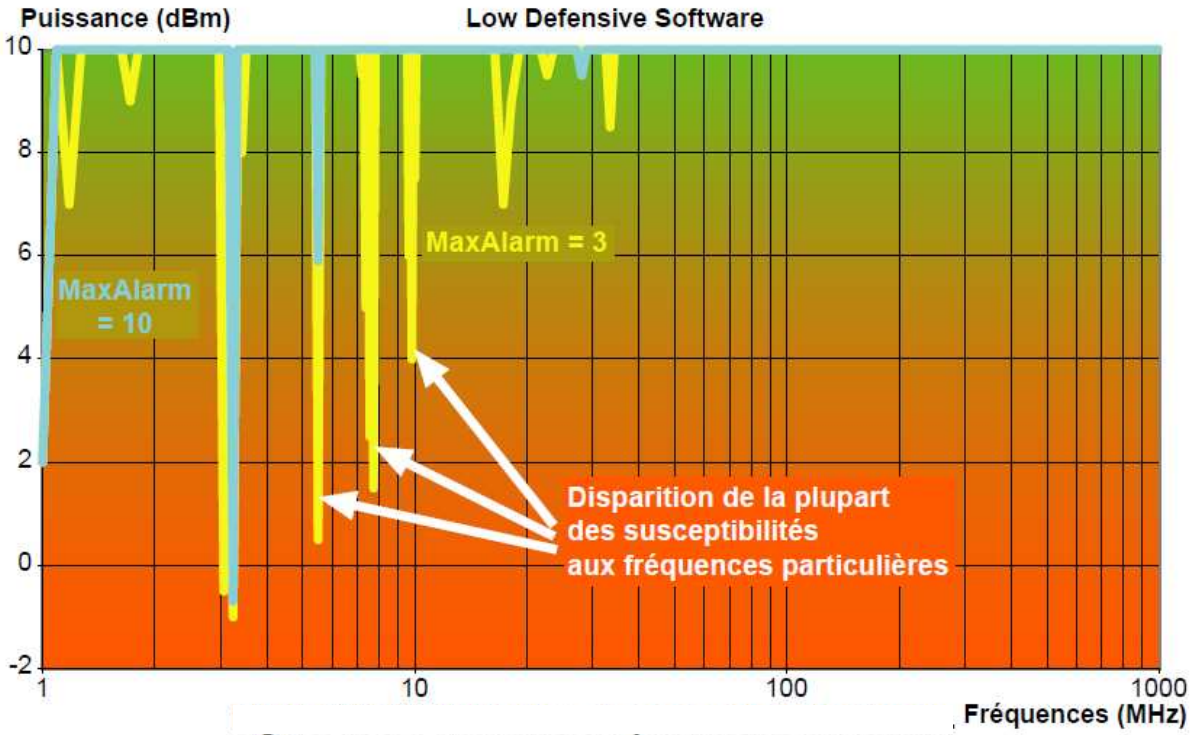


Figure IV-26 : Influence de la variation du paramètre MaxAlarm.

On voit bien l'influence qu'exerce ce paramètre, apparemment capital, puisque l'augmentation de la valeur de MaxAlarm évitera de nombreuses fausses alarmes. Par conséquent, cela augmente donc grandement l'immunité du système.

Enfin, on peut également faire le même test pour le medium defensive software, en variant le paramètre (qui lui est propre) MaxDelta. La figure IV-27 [15] montre des courbes tracées pour MaxDelta = 100% et MaxDelta = 50%.

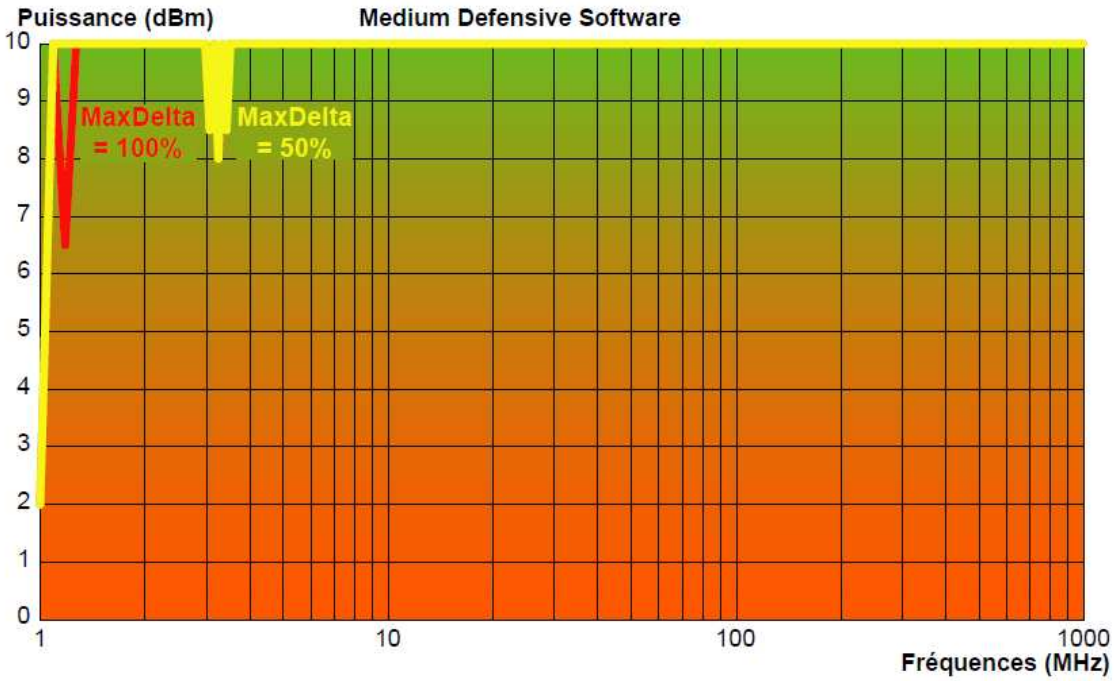


Figure IV-27 : Influence de la variation du paramètre MaxDelta.

On constate que l'influence de la valeur de ce paramètre est moindre, puisque le fait de réduire la tolérance sur la variation entre deux échantillons ne permet que d'éliminer une susceptibilité locale. Nous sommes forcés de remarquer que les résultats obtenus avec la valeur par défaut sont déjà de bonne qualité. Donc, il semble relativement naturel que l'on n'obtienne pas une très forte amélioration de l'immunité de l'application.

Conclusion :

Ce chapitre a été consacré aux techniques logicielles visant à augmenter l'immunité des circuits intégrés numériques programmables. Ces techniques, comme nous les avons décrites, visent à détecter des anomalies et les corriger sans induire un comportement catastrophique. Pour ce faire, elles vérifient l'intégrité de trois points sensibles aux perturbations de l'environnement : les entrées/sorties, la mémoire volatile (la RAM) et le registre de contrôle du flot d'exécution. Cette procédure a pour buts d'acheminer des donner saines à l'intérieur du circuit (en vérifiant l'intégrité des données en entrée), puis de s'assurer que les données stockées ne sont pas corrompues (à l'intérieur de la RAM) et enfin de rendre l'exécution du programme sécurisée.

Comme cela a été évoqué dans ce chapitre, les logiciels défensifs peuvent être génériques, c'est-à-dire à caractère général, ou spécifiques à quelques applications seulement.

Nous avons enfin étayé le bien-fondé d'utiliser de tels logiciels en citant quelques résultats empiriques.

Ces logiciels défensifs sont d'une utilité telle et d'un prix si bas que leur utilisation s'impose pour la consolidation de systèmes à microprocesseurs. Ils sont utilisés dans tous les systèmes

électroniques de criticité suffisante. Ils présentent l'avantage d'être facilement modifiables sans avoir à intervenir sur le circuit lui-même.

Chapitre V :

Réduction des émissions des circuits intégrés numériques en utilisant la version asynchrone

Introduction :

L'origine des circuits asynchrones remonte aux premiers ordinateurs, en particulier le fameux ENIAC élaboré vers 1945 par Eckert et Mauchly. Depuis, les architectures des ordinateurs ont évolué et des fonctions de calcul sans cesse croissantes en complexité sont intégrées sur une puce dont la surface s'amenuise. Dans la course à l'intégration, les circuits asynchrones n'ont pas « su » s'imposer car les méthodes de conception qui leur étaient dédiées ont rapidement montré leur lourdeur face à la gestion des évènements aléatoires. En effet dans un circuit asynchrone, tout évènement de ce type peut être interprété comme une donnée à traiter et déclencher, donc, un fonctionnement erroné. C'est ainsi que la méthode suivante, plus simple, a été largement employée : cadencer les traitements dans le circuit par un signal globale de période régulière (horloge) afin d'assurer la validité des données.

Depuis, malgré l'omniprésence des circuits synchrones, des recherches sur les circuits asynchrones ont tout de même été menées.

Aujourd'hui, avec l'évolution technologique qui suit les prévisions de Moore, les circuits synchrones montrent leurs faiblesses et les circuits asynchrones apparaissent comme une alternative intéressante. En l'occurrence dans notre cas, les circuits synchrones rayonnent plus que les circuits asynchrones puisque toutes les commutations des transistors sont simultanées ce qui n'est pas le cas des derniers. Ces courant s'accumulent et se rejoignent finalement pour rayonner et perturber les circuits environnants, c'est pour cela que nous considérons que l'étude des circuits asynchrones est primordiale. Cette étude est intéressante également puisque, dans la plupart des pays du monde, les ingénieurs concepteurs des circuits digitaux sont principalement formés pour fabriquer des circuits synchrones. De surcroît, la répartition judicieuse des courants, que nous aborderons, permettra une diminution plus poussée des pics de courant aux pins de masses (qui permettent leur retour) et limitera ainsi les agressions électromagnétiques sur les circuits extérieurs.

1) Définitions préliminaires :

Avant de passer aux définitions qui nous intéressent, en l'occurrence celles qui concernent les circuits numériques synchrones et asynchrones, nous avons préféré de définir au préalable des blocs constitutifs de tout circuit synchrone ou asynchrone.

1-1) Bloc combinatoire :

Tout circuit numérique comporte des blocs combinatoires, ceux-ci sont constitués de portes logiques et réalisent des fonctions différentes afin d'assurer le traitement des données. Les circuits combinatoires sont caractérisés par le fait que l'état de leur sortie ne dépend que de l'état de leurs entrées.

1-2) Bloc de mémorisation :

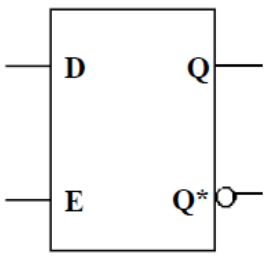
A titre égal en importance aux blocs combinatoires, aucun circuit ne peut se passer des éléments de mémorisation. Ces éléments de mémorisation suivent une logique dite séquentielle et comme son nom le suggère, la sortie dépend des entrées mais aussi du moment de l'application de ces entrées, c'est-à-dire, du temps.

L'horloge est un signal de commande (des circuits synchrones) carré périodique, dont la fréquence détermine la vitesse du système. Le signal carré de l'horloge est souvent positif ou nul. On adoptera la nomenclature de niveau haut pour désigner la partie positive du signal, et de niveau bas pour désigner la partie nulle du signal.

On appelle front d'horloge (edge en anglais), tout basculement du signal carré d'un niveau haut à niveau bas ou l'inverse. Dans le cas d'un basculement d'un niveau bas à un niveau haut, le front engendré est appelé front montant (positive edge en anglais). Dans l'autre cas, le front décrit est appelé front descendant (negative edge en anglais).

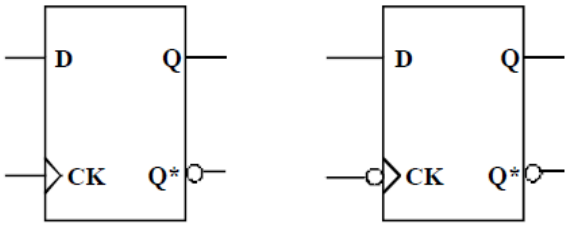
Les mémoires sont construites à partir d'éléments élémentaires séquentiels appelés bascules. Il y a deux types de bascules, en prenant comme critère la nature du signal qui les commande :

- Les bascules à verrouillage appelées aussi latch(es) qui comportent une entrée asynchrone (voir la figure V-1) qui, selon son niveau, « autorise » l'activation de ces bascules (au niveau haut par exemple), ou au contraire, les rend inactives (au niveau bas par exemple).
- Les bascules à déclenchement sur front ou flip-flop(s) (voir les figures V-2) qui sont synchrones, i.e., suivent un signal d'horloge. Elles sont actives quand elles « perçoivent » un front montant ou descendant (selon la construction), et dans tous les autres cas, elles deviennent complètement bloquées (leurs sorties ne changent pas).



E	D	Q^+	Q^{*+}
0	0	Q	$\overline{Q}$
0	1	Q	$\overline{Q}$
1	0	0	1
1	1	1	0

Figure V-1 : Schéma-bloc d'une bascule D latch (à gauche) et sa table de vérité (à doite).



CK	D	Q^{+}	Q^{*+}
0	X	Q	$\overline{Q}$
1	X	Q	$\overline{Q}$
↓	0	0	1
↓	1	1	0

Figure V-2 : Schémas-blocs d'une bascule D à déclenchement sur un front montant (à gauche) et d'une bascule D à déclenchement sur front descendant (au centre), et table de vérité d'une bascule D à déclenchement sur front montant (à gauche).

1-3) Circuits logiques synchrones complexes :

Un circuit numérique est dit synchrone si tous les traitements des données sont simultanés. Cela signifie que tous les blocs travaillent en synergie et attendent un « ordre » bien précis émanant d'un signal d'horloge globale. Tout système synchrone comporte une alternance de blocs de mémorisation et de traitement (combinatoire) disposés en cascade (voir la figure V-3).

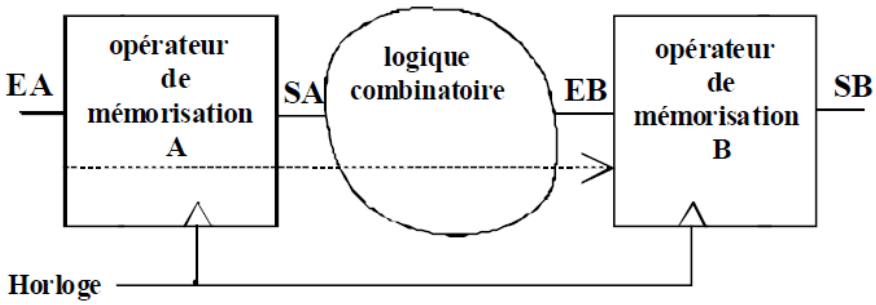


Figure V-3 : Structure d'un système synchrone complexe.

Pour détailler le fonctionnement de ce circuit, on suppose la présence d'une donnée à l'entrée EA de l'opérateur de mémorisation A (on suppose qu'il est construit à base de bascules D à déclenchement sur front montant). Dès que l'horloge présente un front montant, la donnée est copiée à la sortie SA. Cette donnée étant également « ressentie » par l'entrée du système combinatoire, elle est traitée et à sa sortie on obtient le résultat. Cette sortie bien que connectée à l'entrée de l'opérateur de mémorisation EB, ses donnée ne sont mémorisées par l'opérateur B qu'au prochain front montant de l'horloge. Simultanément, si une nouvelle donnée est présente à l'entrée de l'opérateur A, celle-ci n'est mémorisée qu'au front montant de l'horloge. Ce fonctionnement en chaîne continue d'un bloc à l'autre, à chaque front d'horloge, jusqu'à ce que les données finalisées et traitées arrivent à la sortie finale. En

général, si un système synchrone est constitué de N opérateurs de mémorisation, il faudra attendre N périodes d'horloge pour qu'une donnée finalisée arrive à la sortie de l'opérateur N.

Dans les systèmes synchrones aussi bien que dans les systèmes asynchrones, on parle parfois d'aléas (hazard(s) en anglais). Il s'agit de dysfonctionnements dus à l'apparition d'états d'entrées trop brefs, soient volontaires et qui sont de durée trop courte, soient involontaires et donc imprévues. Ces états « fugitifs » ont des conséquences parfois bénignes, mais parfois, ils faussent carrément le fonctionnement du système. Pour illustrer ce phénomène on prend l'exemple du compteur asynchrone modulo 5 à cycle incomplet illustré par la figure V-4 [16].

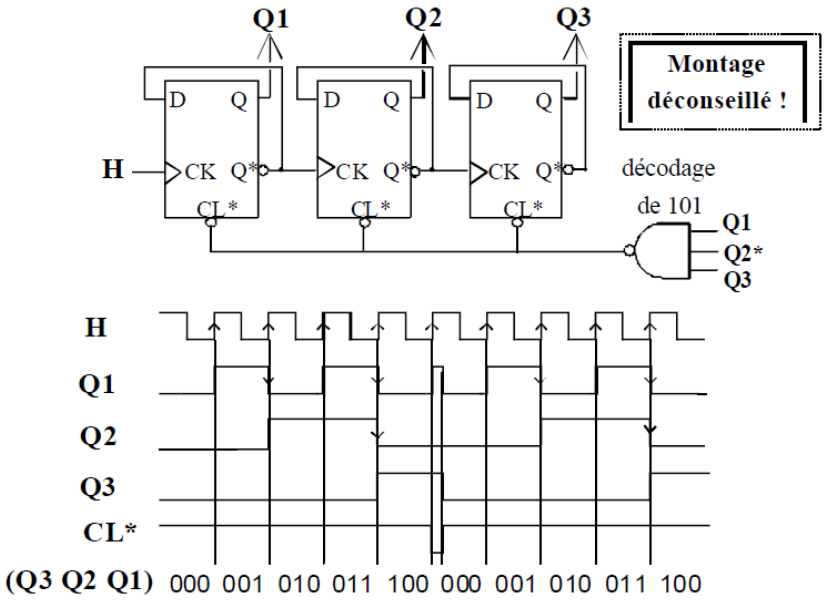


Figure V-4 : Montage théorique assurant une fonction de comptage modulo 5 et son chronogramme.

En théorie, le comptage débute normalement et lorsque le compteur passe à l'état 5, cette configuration est détectée (passage à 0 de la sortie de la porte NAND), le reset des bascules est activé, et les sorties *Q* des bascules sont forcées à 0. Dès que la configuration 101 n'est plus présente en entrée de la porte NAND, l'entrée de remise à zéro des bascules repasse à 1, et le compteur retourne dans un état de comptage normal.

En pratique, cette méthode présente, surtout, des **risques d'aléas**. En particulier, si les bascules présentent des dispersions importantes sur les temps de réaction à l'activation du reset, il se peut que l'entrée *CL** des bascules repasse à 1 avant que toutes les sorties ne soient forcées à 0. De plus, pour certains montages, le décalage des sorties les unes par rapport aux autres peut entraîner l'apparition indésirable de la configuration de remise à zéro.

1-4) Définition préliminaire des circuits logiques asynchrones :

Dans un circuit asynchrone (figure V-5), le traitement des données n'est pas régi par un signal global mais par des communications locales entre les différents éléments du circuit.

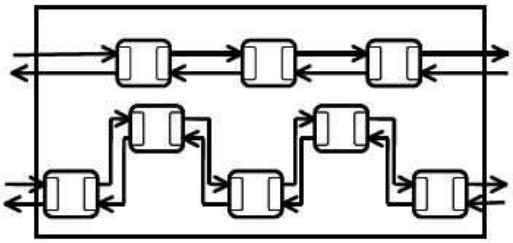


Figure V-5 : Structure modulaire d'un circuit asynchrone.

Ces communications assurent la séquence des traitements dans le circuit par les protocoles de types poignée de main (handshake en anglais). Elles sont synchronisées par le biais de canaux qui permettent à deux opérateurs d'échanger des données par une connexion point à point gérée par le protocole de communication. Chaque canal est composé de signaux de contrôle (requête et acquittement) qui permettent d'assurer le protocole et du chemin des données (voir la figure V-6).

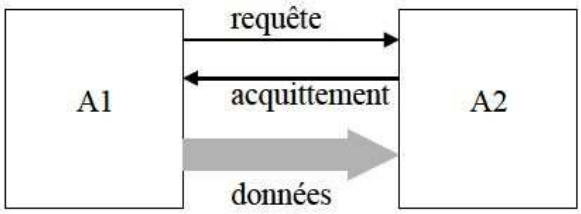


Figure V-6 : Communication de type poignée de main (handshaking communication).

2) Propriétés avantageuses des circuits asynchrones :

Les circuits asynchrones, en plus d''éviter en partie les problèmes liés à l'utilisation d'une horloge globale, possèdent d'autres propriétés avantageuses :

- Haute performance : Grâce à la synchronisation locale, chaque étape de calcul dans un circuit asynchrone démarre dès que l''etape précédente est terminée. Et ceci, sans devoir attendre un signal d'horloge et indépendamment du pire des cas (bloc le plus lent). Cela se traduit par une vitesse de traitement accrue, car les circuits asynchrones calculent en temps moyen et non en temps de pire des cas.
- Faible consommation : Contrairement aux circuits synchrones où à chaque cycle d'horloge, tous les éléments logiques du circuit évaluent leurs entrées, et donc consomment ; dans un circuit asynchrone chaque élément non sollicité se placera en attente d'un jeu d'entrées valides, réduisant l'activité au minimum.
- Robustesse vis-à-vis des conditions environnementales : Alors qu'en synchrone on est obligé d'introduire dans le délai (retard) des marges de sécurité pour pallier aux éventuelles variations des conditions environnementales, en asynchrone aucune hypothèse n'est faite sur le délai de l'opérateur. Un circuit asynchrone est capable

grâce à la synchronisation locale de calculer au maximum de sa capacité même en présence de perturbations, telles que les variations de la température ou encore la variation de la tension d'alimentation étant donné que celui-ci est conçu en prenant déjà comme hypothèse que ces paramètres-là varient, puisque son activité varie en intensité.

- Meilleure composabilité et modularité : La synchronisation locale permet de considérer les éléments d'un circuit comme des boites noires faciles à déplacer et à réutiliser puisque aucune assertion n'est faite sur le délai et les conditions environnementales de fonctionnement.
- Plus de problèmes de génération, de distribution d'horloge et de course critique : Il n'y a plus de signal à distribuer simultanément dans tout le circuit, ce qui est l'un des plus gros problèmes des processeurs synchrones.
- Faibles émissions électromagnétiques : Les opérations locales s'effectuent généralement de façon aléatoire dans le temps, répartissant les impulsions électromagnétiques créées par l'alimentation d'un composant et lissant le spectre électromagnétique du circuit ; alors que l'alimentation ponctuée par l'horloge de l'ensemble d'un circuit synchrone génère un spectre particulier et sévère en quelques endroits bien précis du spectre électromagnétique. La figure V-7 [4] illustre l'activité du courant (lié aux émissions électromagnétiques) dans un CAN (Convertisseur Analogique-Numérique) synchrone et asynchrone.

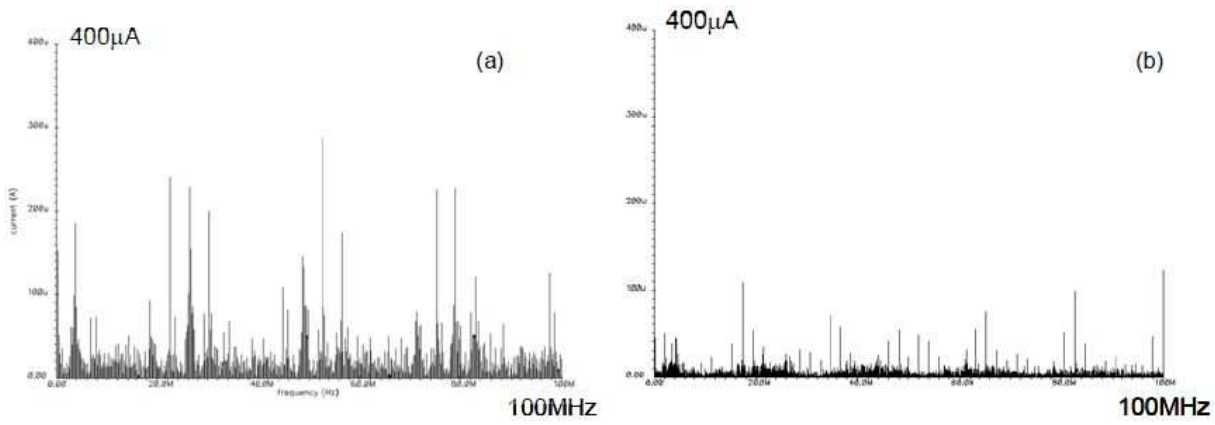


Figure V-7 : Spectre de l'activité du courant dans un CAN synchrone (figure a) et asynchrone (figure b).

3) Principe de fonctionnement des circuits asynchrones :

3-1) Mode de fonctionnement asynchrone :

Le terme «asynchrone » signifie qu'il n'existe pas de relation temporelle entre les objets qu'il qualifie. Dans le contexte de la conception de systèmes intégrés, ces objets sont des événements au sens large (contrôle ou données) implémentés par des signaux électriques.

La différence entre les systèmes synchrones et les systèmes asynchrones la plus éloquente, quoiqu'ils comportent tous les deux des opérateurs de mémorisation disposés en cascade et en

alternance avec des fonctions combinatoires, est la présence d'un signal d'horloge jouant le rôle d'un actionneur global dans les premiers. Ainsi, tous les éléments du système évoluent lors de l'occurrence d'un évènement horloge (un front montant par exemple), l'exécution de tous les éléments est donc synchronisée. D'un autre côté, cela signifie qu'il y a commutation simultanée de tous les transistors, qui engendre d'énormes courants dans les pins de masse. Ces courants induisent inévitablement à des rayonnements, parfois, assez importants pour nuire au bon fonctionnement du système.

A l'opposé, les systèmes asynchrones évoluent de façon localement synchronisée et le déclenchement des actions dépend uniquement de la présence des données à traiter. Il y a en fait une véritable communication entre chaque pair de blocs successifs. En effet, les données ne sont envoyées que si l'opérateur en aval qui les recevra a un espace mémoire suffisant (car il a communiqué à son tour ses données à l'opérateur qui le succède en aval). Il faut remarquer que tout ceci est effectué de façon indépendante des autres blocs et des autres processus concurrents, c'est la raison pour laquelle ces systèmes sont qualifiés d'asynchrones. Dans les systèmes asynchrones, tous les blocs qui n'ont pas de données à traiter ou mémoriser sont inactifs, c'est-à-dire, ne consomment pas de courant. De plus, les commutations des transistors sont indépendantes et aléatoires (donc elles ne sont pas forcément simultanées) ce qui réduit grandement les rayonnements de tels systèmes.

3-2) Caractéristiques d'un opérateur asynchrone :

D'un point de vue externe, un opérateur asynchrone peut être considéré comme une cellule, réalisant une certaine fonction (partie combinatoire), communiquant avec son environnement à travers des canaux de communication. Ces canaux de communication servent à échanger, avec l'environnement, aussi bien des données que des informations de synchronisation. La figure V-8 illustre deux opérateurs asynchrones (dans cette représentation la partie combinatoire et la partie mémoire sont confondues) et la notion de canal illustrée par un couple de flèches : Une sortante qui transmet les données et la requête à l'opérateur en aval, et l'autre entrante qui transmet le signal d'acquittement à l'opérateur en amont.

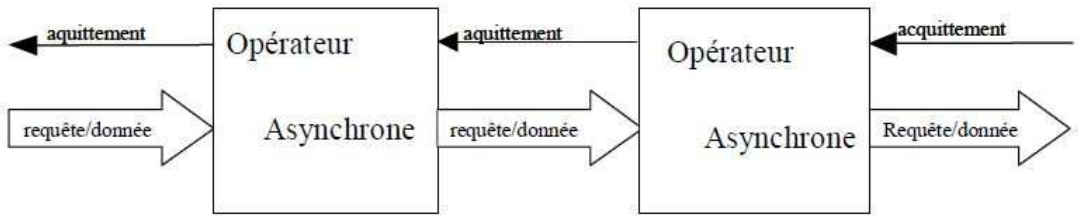


Figure V-8 : Opérateurs asynchrones synchronisés par un canal (les flèches entrante et sortante).

Ces opérateurs sont caractérisés par quatre paramètres :

- Le temps de latence : Ce temps correspond au temps nécessaire à une sortie de réagir à la donnée présente à l'entrée. Il est égal au temps de calcul de la chaîne combinatoire.
- Le temps de cycle : Il caractérise le temps qui sépare la validation de deux entrées successives.
- La profondeur du pipeline : Il définit le nombre maximum de données que l'opérateur peut mémoriser.
- Le protocole de communication : Il détermine la façon dont des opérateurs asynchrones échangent des informations. Il assure la détection des informations en entrée ainsi que la génération d'une signalisation indiquant, d'une part, qu'une information est valide en entrée (de l'opérateur), et d'autre part qu'une information est disponible en sortie (de l'opérateur).

3-3) Protocoles de communications :

Il existe deux principaux protocoles, le protocole 2 phases (NRZ pour Non Retour à Zéro) et le protocole 4 phases (RZ pour retour à zéro).

Le fonctionnement d'un protocole 2 phases est décrit par la figure V-9 et se déroule en 2 phases comme l'indique son nom :

- Phase 1 : C'est la phase active du récepteur qui détecte la présence de nouvelles données, effectue le traitement et génère le signal d'acquittement.
- Phase 2 : C'est la phase active de l'émetteur qui détecte le signal d'acquittement et émet les nouvelles données si elles sont disponibles.

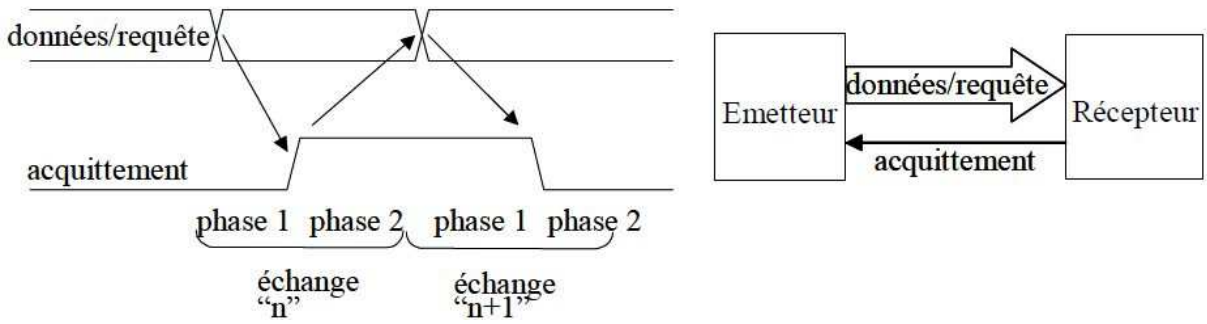


Figure V-9 : Protocole 2 phases.

Le fonctionnement d'un protocole 4 phases (figure V-10) se déroule comme suit :

- Phase 1 : C'est la première phase active du récepteur qui détecte la présence de nouvelles données, effectue le traitement et génère le signal d'acquittement.
- Phase 2 : C'est la première phase active de l'émetteur qui détecte le signal d'acquittement et émet des données invalides (retour à zéro).

- Phase 3 : C'est la deuxième phase active du récepteur qui détecte le passage des données dans l'état invalide et place le signal d'acquittement dans l'état initial (retour à zéro).
- Phase 4 : C'est la deuxième phase active de l'émetteur, qui détecte le retour à zéro de l'acquittement. Il est alors près à émettre de nouvelles données.

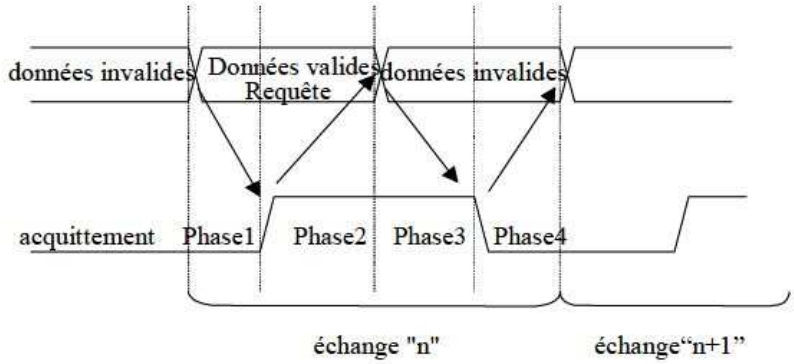


Figure V-10 : Protocole 4 phases.

3-4) Codage des données :

A ce niveau, une question légitime se pose : Comment peut-on reconnaître la présence d'une donnée valide ou invalide, ou encore la fin d'un traitement ?

La solution consiste en l'attribution de signaux bien particuliers à chaque opération (ou évènement), de sorte à distinguer de façon unique tous les évènements possibles. Il faut, de surcroît, utiliser un codage bien précis pour les données. En effet, l'utilisation d'un seul fil par bit de donnée ne permet pas de détecter que la nouvelle donnée prend un état identique à la précédente (par exemple deux 1 qui se succèdent).

Une première solution à ce problème consiste à adopter un codage bifilaire ou double rail pour chaque bit de donnée. Cela double donc le nombre de fils par rapport aux réalisations synchrones. Une seconde solution consiste à ajouter un signal de requête aux données, c'est-à-dire, que c'est justement ce nouveau signal qui indique au bloc en aval qu'un nouveau bit est disponible. Donc, même si deux bits successifs sur un fils sont identiques, c'est le signal de requête qui distinguera le nouveau bit du précédent.

Avec deux fils par bit de donnée, quatre états sont utilisables (combinaison de deux bits) pour exprimer les valeurs logiques (« 0 », « 1 »). Deux codages sont communément adoptés : l'un utilisant trois états seulement, et l'autre utilisant quatre états (voir figure V-11).

Pour le codage trois états, un fil prend la valeur 1 pour coder une donnée à 1, et l'autre fil prend la valeur 1 pour coder la valeur 0. L'état 11 (c'est-à-dire, les deux fils sont à 1 simultanément) est interdit alors que l'état 00 (les deux fils sont à 0) représente l'invalidité d'une donnée (utile pour le protocole 4 phases). Ainsi, passer d'une valeur valide à une autre

implique toujours un passage préalable par l'état invalide (figure V-11). Ce codage garantit que le passage d'un état à un autre se fait toujours par un changement de l'état d'un seul bit, ce qui immunise ce passage contre les aléas. Le signal de fin de calcul d'un opérateur peut facilement être généré en détectant qu'un des bits de sortie est passé à 1.

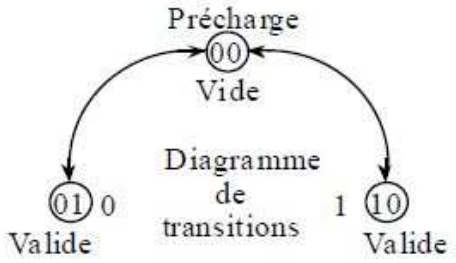


Figure V-11 : Codage à trois états d'un bit donnée.

La convention adoptée dans le cas du codage quatre états, est de coder les valeurs 0 ou 1 d'un bit avec deux combinaisons possibles, l'une paire et l'autre impaire. Ce codage consiste à fixer une valeur d'un fil, par exemple 1 indique la présence d'un 1 et **sur le même fil**, la présence d'un 0 signifie la disponibilité d'un 0. L'autre fil contient le bit de parité, il change de valeur de sorte qu'à chaque fois qu'un nouveau bit est émis, la somme modulo 2 des deux bits présents sur les deux fils change (voir la figure V-12). Ceci permet donc au bloc en aval de « savoir » si un nouveau bit est présent ou pas. Ce type de codage est adapté pour l'implémentation du protocole 2 phases. Il assure comme le codage trois états un changement d'état sur un fil ce qui est efficace, comme nous l'avons déjà fait remarquer, pour contrer tout aléa.

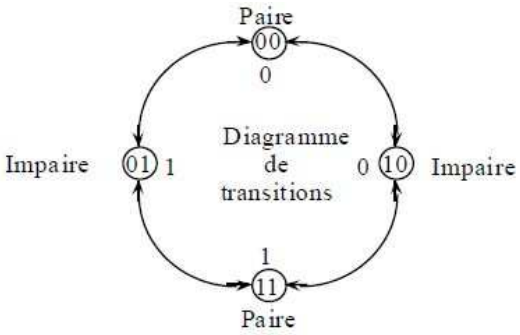


Figure V-12 : Codage à quatre états d'un bit donnée.

4) Asynchronisation de circuits synchrones :

4-1) Introduction :

Le style de conception synchrone s'est imposé depuis l'apparition des circuits intégrés, car pour assurer la séquence des traitements et la validité des données, le choix le plus simple était l'utilisation d'un de contrôle global : l'horloge. Les outils pour la conception synchrone

se sont alors développés depuis plus de dix ans suivant l'évolution des méthodes de conception dédiées à ce type de circuits. Mais avec les problèmes d'émissions importantes des ondes électromagnétiques inhérents aux circuits synchrones, la tendance asynchrone a regagné du terrain. Cependant, vu l'immaturité des outils de développement de tels circuits nous avons opté pour transformer un circuit synchrone en un circuit équivalent asynchrone.

Avant d'aller plus loin, nous devons au préalable fixer le niveau d'abstraction, c'est-à-dire, à quel niveau de la réalité vont se situer nos symboles ? Au niveau portes ou registres ?

Vu la complexité des circuits qui nous intéressent, un schéma se basant sur des portes logiques searit trop encombrant. Par contre, une description au niveau registres est plus judicieuse et fait apparaître tous les détails dont nous avons besoin. Cette description est également connue sous le sigle RTL (Register Transfer Level).

4-2) Principe de l'asynchronisation :

Afin d'asynchroniser un système synchrone, il faut supprimer le signal d'horloge et le remplacer par des communications locales de type poignée de main (handshaking communications). La séquence des traitements des ressources étant gérée par les communications locales, l'activité du courant est répartie dans le circuit : les pics courants sont réduits par rapport aux circuits synchrones. Les émissions électromagnétiques dues à l'horloge sont ainsi diminuées.

4-3) Introduction de l'étape d'asynchronisation dans le flot de conception :

La synthèse comportementale est une étape où l'ensemble des fonctions sont définies ainsi que les séquences suivies par les différents processus. Cette étape permet d'avoir un aperçu sur le fonctionnement du circuit qui sera conçu, à partir d'une description graphique simple qui décrit comment fonctionne celui-ci. Ensuite, vient la synthèse RTL où les différents opérateurs requis sont définis. Enfin, vient la synthèse logique où les différentes fonctions sont définies par des circuits logique, de niveau d'abstraction inférieur (portes logiques).

Les étapes citées ci-dessus décrivent globalement les étapes à suivre lors de la conception d'un circuit synchrone. Comme nous l'avons déjà cité, des méthodes pour fabriquer des circuits asynchrones ne sont pas encore matures. Pour contourner ce problème, il suffit d'intercaler une étape d'«asynchronisation » qui fera produire finalement des circuits asynchrones opérationnels sans avoir à attendre de nouvelles techniques de conception [4].

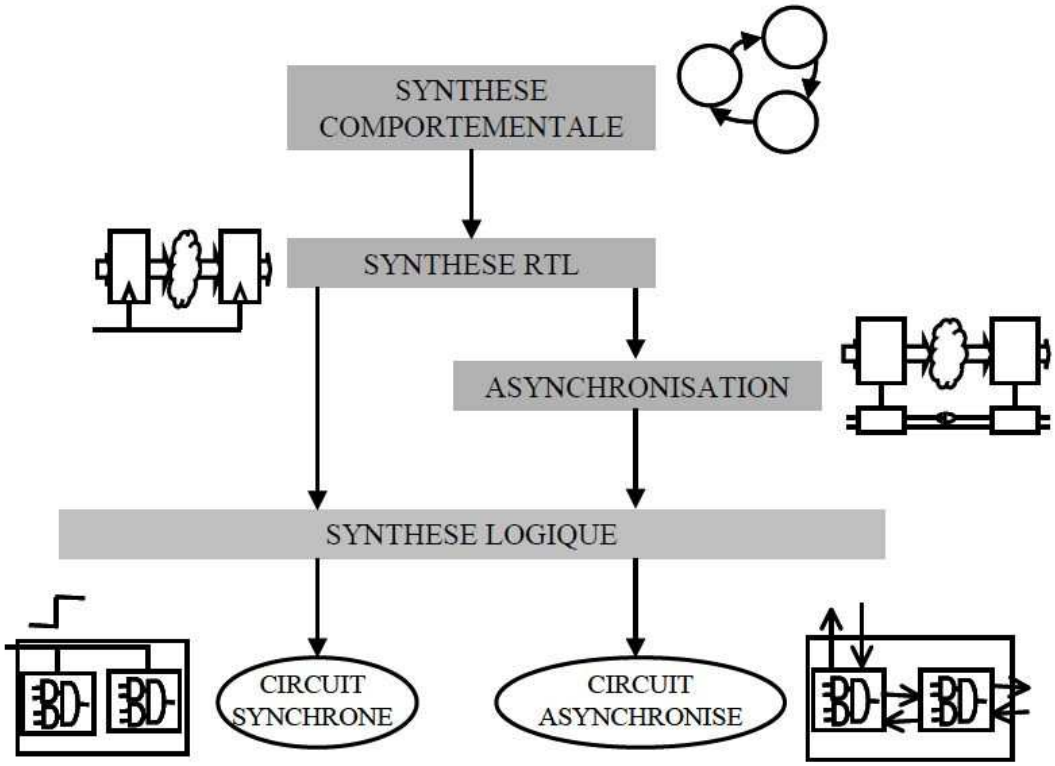


Figure V-13 : Etape de l'asynchronisation dans le flot de conception.

4-4) Elaboration d'une méthode d'asynchronisation :

L'idée de cette élaboration consiste à remplacer toutes les briques synchrones dans la description RTL du circuit, pour les remplacer par des briques asynchrones dont le comportement est identique.

Cette élaboration se fait en deux étapes :

- Comprendre les concepts du fonctionnement pour identifier des analogies entre les circuits synchrones et leurs équivalents asynchrones.
- Proposer une procédure d'asynchronisation.

4-5) Concepts du fonctionnement synchrone :

Ce paragraphe tente de réunir les concepts du fonctionnement synchrone afin de trouver les structures asynchrones équivalentes. Les signaux d'entrée et de sortie du circuit sont synchronisés.

a) Bloc combinatoire :

Les sorties d'un bloc combinatoire dépendent uniquement des données en entrée. Les données en sorties sont calculées dès qu'il y a un changement sur son/ses entrée(s).

La condition du bon fonctionnement d'un bloc combinatoire est la suivante : les entrées doivent se présenter suffisamment espacées dans le temps pour lui laisser le temps d'effectuer

son calcul. Si une erreur arrive à l'entrée d'un bloc combinatoire, alors elle provoque une sortie erronée et une consommation inutile de courant pour sont traitement.

b) Bloc mémoire :

Les sorties du bloc mémoire dépendent de ses données en entrées et du temps (logique séquentielle). Deux types peuvent être rencontrés : la logique sensible à un front de l'horloge (Flip-flop(s)) et la logique sensible au niveau de l'horloge (Latch(es)).

La condition du bon fonctionnement d'un bloc mémoire sensible au front d'un signal est la suivante : les entrées doivent changer suffisamment à l'avance afin de respecter le temps d'établissement du régime (setup time) et doivent rester stables assez longtemps pour respecter le temps de maintien (hold time).

Les conditions de bon fonctionnement d'un bloc mémoire sensible au niveau d'un signal sont les suivantes :

- Les données en entrée doivent être stables suffisamment à l'avance avant que les signaux *enable* ne soient actifs.
- Les données en entrée doivent être stables assez longtemps pour respecter la latence de la partie combinatoire.

Dans un circuit synchrone, le flot de données est régulé par un signal d'horloge. A chaque front montant ou descendant de celui-ci, les données entrantes ou sortantes des blocs combinatoires sont garanties valides. Un bloc mémoire sensible au front d'horloge est utilisé en amont ou en aval d'un bloc combinatoire. Il mémorise ses sorties lorsqu'il reçoit le signal d'horloge approprié et permet ainsi la gestion du flux des données. C'est donc ce type de bloc qu'on cherche à remplacer.

4-6) Architecture générale utilisée pour l'asynchronisation :

Le principe de l'asynchronisation est de remplacer un circuit ou une partie de circuit par son équivalent asynchrone. L'horloge qui gère les parties mémoire est remplacée par un contrôle local composé d'un contrôleur, de latches et des canaux de communication. Le signal qui orchestre les échanges respecte des protocoles bien définis. Les parties mémoires sensibles au front de l'horloge (Flip-flops) sont remplacées par des latches. Ce sont les parties mémoires sensibles au niveau du signal local injecté à l'entrée *enable* géré par les protocoles des communications.

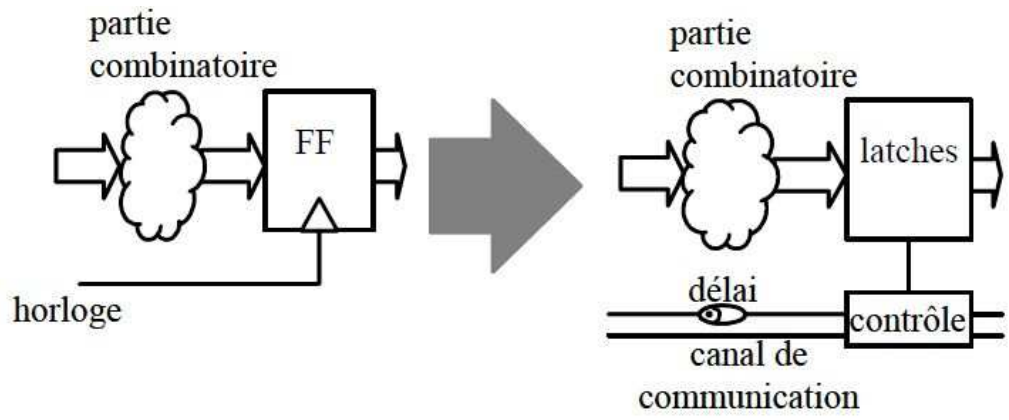


Figure V-14 : Principe général de l'asynchronisation.

Chaque bloc sensible à l'horloge est équivalent, après asynchronisation, à une partie contrôle et une partie donnée. La partie contrôle du circuit a pour rôle de gérer les communications entre les blocs asynchronisés. La partie donnée représentera le traitement effectué à l'intérieur du bloc combinatoire activé et des latches commandées par la partie contrôle.

5) Mise en forme du courant (current-shaping methodology) :

5-1) Introduction :

Les circuits asynchrones sont attractifs pour leur qualité de faibles émissions électromagnétiques. Cependant, de forts pics de courant peuvent subsister lors de leur fonctionnement. A certaines fréquences, et selon leur amplitude, ces pics s'avèrent être plus ou moins nuisibles. Néanmoins, une distribution judicieuse des courants permet de diminuer davantage ces pics de courant et donc, leurs émissions électromagnétiques.

5-2) Principe général de la mise en forme du courant :

Les composantes élevées (en termes d'amplitude) d'un spectre de courant parcourant un circuit asynchrone proviennent principalement des appels de courant simultanés dans le circuit. Dès la conception du circuit, la concurrence des appels de courant dans le circuit peut être diminuée afin de minimiser ces pics. Les paramètres structurels sur lesquels il est possible d'agir sont, au niveau architectural, les délais caractéristiques des temps de calcul des blocs d'architecture, et, au niveau portes logiques, les délais caractéristiques de chacune des portes. Contrôler ces délais permet de « mettre en forme » le courant consommé. En effet, en introduisant des retards différents dans des blocs concurrents, on évitera la coïncidence des commutations. Cette gestion intelligente des retards permettra de réduire les courants sur le chemin de retour (les masses), et du coup, il y a moins émissions électromagnétiques.

5-3) Activité du courant :

a) Activité du courant pour un opérateur :

Pour chaque élément d'un circuit, un modèle i(t) (t allant de 0 à dmax – latence maximum de l'élément) de l'activité du courant peut être obtenu. L'allure de la consommation du courant par un opérateur peut être approximée par une expression analytique, ou par un choix de points considérés significatifs (voir la figure V-15 [4]).

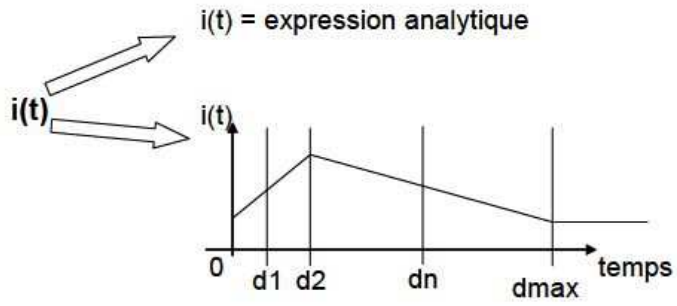


Figure V-15 : Activité du courant dans un opérateur.

b) Activité globale du courant :

Dans un circuit où des traitements concurrents s'effectuent, l'activité globale du courant peut être estimée à l'instant t.

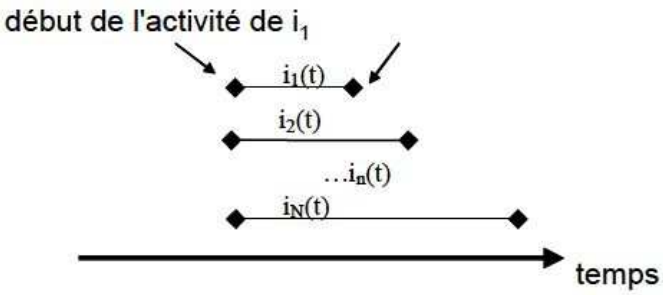


Figure V-16 : Activité de N opérateurs effectuant leur traitement en parallèle.

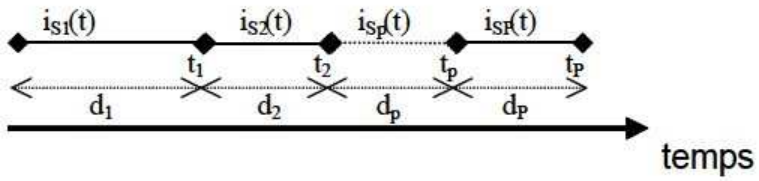


Figure V-17 : Représentation de l'activité d'un opérateur composé de plusieurs opérateurs en série.

La figure V-16 [4] représente le cas où N éléments fonctionnent en parallèle. Les latences maximums des traitements des différents opérateurs sont modélisées par des segments. Chaque opérateur j possède sa propre latence maximum $d_j max$.
$d_1 max < d_2 max < \ldots < d_n max < \ldots < d_N max$

Chaque opérateur possède également sa propre activité en courant $i_j(t)$. La représentation figure V-16 donne une idée sur la valeur du courant à tout instant, ainsi que le retard maximal que peut faire chaque opérateur. Par ailleurs, un opérateur peut lui-même être une composition en série de P « sous-opérateurs » (figure V-17 [4]). Sont activité devient alors :

$$i_j(t) = \begin{cases} i_{s1}(t) \ pour \ t \in [0, t_1] \\ i_{s2}(t) \ pour \ t \in [t_1, t_2] \\ i_{sP}(t) \ pour \ t \in [t_{P-1}, t_P] \end{cases}$$

Et sa latence maximum : $d_j \max = \sum_{i=0}^{P} d_i$ (avec d_P : temps de latence maximum de l'élément p) [4].

L'activité globale du courant à l'instant t du système représenté dans la figure V-16 est égale à la somme des activités du courant de tous les opérateurs (opérateurs en parallèle) à l'instant t :

$$Itot(t) = i_1(t) + i_2(t) + \ldots + i_n(t) = \sum_{i=0}^{N} i_j(t) \qquad [4]$$

Dans le système de la figure V-16, si le déclenchement du traitement d'un opérateur j est décalé $D_j t$, le modèle en courant de l'élément j devient :

$I_{Dj}(t) = i_j(t - D_j t)$ [4]

$avec : si \ t < Dt \ alors \ I_{Dj}(t) = i_j(t - D_j t) = 0$ [4]

Si le traitement de l'opérateur 1 est décalé de $D_1 t$, alors l'activité globale du courant dans le circuit est la suivante :

$Itot_{D1}(t) = I_{D1}(t) + I_2(t) + \ldots + I_n(t) + \ldots + i_N(t) \ avec \ I_{D1}(t) = i_1(t - D_1 t)$ [4]

$Avec \ i_{D1}(t) = 0 \ si \ t < D_1(t)$

$$Itot_{D1}(t) = \sum_{j=0}^{N} i_j(t) - i_1(t) + i_{D1}(t)$$

D'une façon générale, lorsque le traitement de l'opérateur k est retardé de $D_k t$, avec $D_k t < d_N max - d_k max$:

$Itot_{Dk}(t) = i_1(t) + i_2(t) + \ldots + I_{Dk}(t) + \ldots + i_n(t) + \ldots + i_N(t)$

$avec \ I_{Dk}(t) = i_k(t - D_k t) ; I_{Dk}(t) = 0 \ si \ t < D_k t(t)$ [4]

$$Itot_{Dk}(t) = \sum_{j=0}^{N} i_j(t) - i_k(t) + I_{Dk}(t)$$

D'une manière plus générale, si tous les traitements des opérateurs dans le circuit sont retardés, l'activité du courant global dans le circuit devient :

$$I_{tot}(t) = I_{D1}(t) + I_{D2}(t) + ... + I_{Dn}(t) + ... + I_{DN}(t)$$

$$avec\ I_{D_j}(t) = i_j(t - D_j t)\ ;\ I_{D_j}(t) = 0\ si\ t < I_{D_j}(t)\ et\ I_{D_j}(t) = i_j(t)\ si\ j \le N \qquad [4]$$

$$Itot(t) = \sum_{j=0}^{N} I_{\Delta j}(t)\ ;\ avec\ j \in [0, N-1]$$

Ainsi, pour optimiser l'activité du courant en réduisant au maximum les pics de courant, il faut déterminer l'ensemble des retards [Δ1t, Δ2t,…, Δ(N−1)t].

5-4) Approche sur les étapes à suivre pour une bonne répartition du courant :

Le problème d'optimisation nécessite d'aborder quatre points fondamentaux :

- La modélisation structurelle de l'architecture qui est nécessaire pour identifier des processus/opérateurs/ressources concurrents et pour leur traitement.
- L'estimation du temps de calcul des blocs de l'architecture : les retards à l'intérieur du circuit permettent d'estimer le profil du courant.
- La modélisation des profils de courant des blocs de l'architecture : l'activité du courant de chaque opérateur est étudiée pour évaluer le profil du courant global.
- L'optimisation du profil du courant global par répartition des traitements des ressources afin de modeler le courant global et de distribuer la consommation en courant.

5-4-1) Modélisation structurelle de l'architecture :

Les forts pics de courant qui subsistent lors du fonctionnement des circuits asynchrones résultent de la concurrence des traitements des opérateurs dans le circuit. Ce parallélisme peut être identifié en analysant le fonctionnement du circuit. Pour cela, un graphe (un modèle graphique) de représentation de l'architecture du circuit doit être utilisé.

❖ **CDFG :**

Le CDFG (Control Data Flow Graph) est un graphe qui représente le fonctionnement du circuit. Un exemple d'un tel graphe est représenté par la figure V-18 [4].

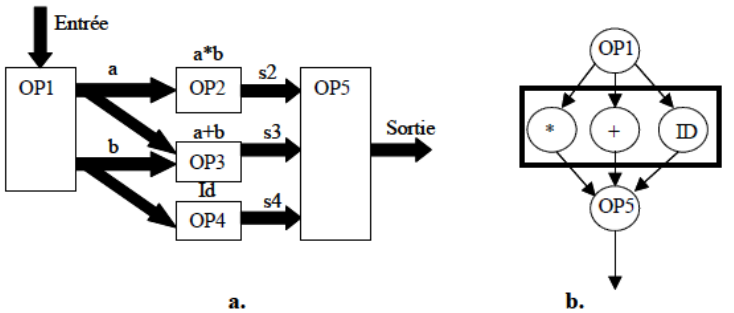
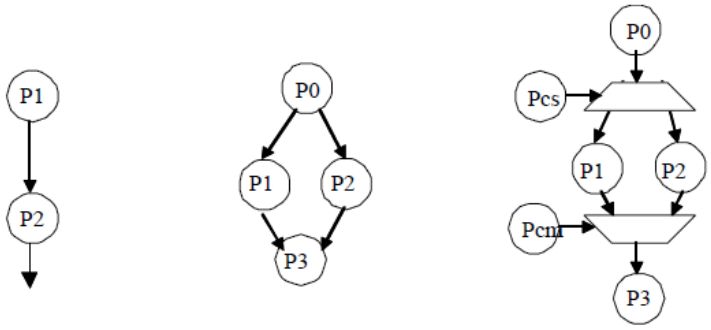


Figure V-18 : Un circuit (a) et la représentation de son CDFG (b).

Dans ce graphe, chaque cercle, également appelée nœud, est marquée par une opération (fonction assurée par la partie combinatoire) et chaque arc représente une liaison entre les ressources.

Les motifs qui peuvent être rencontrés dans le CDFG qui représente l'architecture du circuit :

- La séquence (figure V-19 a [4]).
- Le parallélisme (figure V-19 b [4]).
- Le choix (figure V-19 c [4]).



a)Séquence : P2 est traité après P1.

b) Parallélisme : P1 et P2 sont traités concurremment.

Choix : P1 ou P2 est traité.

Figure V-19 : Motifs d'un CDFG.

Les concurrences (parallélismes) des traitements sont les principales cibles de ce travail et sont facilement identifiables (motifs de parallélisme) dans la représentation du circuit. Cependant, il faut noter que d'autres concurrences moins explicites existent et sont rencontrées dans d'autres motifs. Par exemple, il existe une concurrence des activités dans les canaux de communication. En effet, lorsqu'un protocole de communication est en exécution, les portes constituant le contrôle peuvent être activées en parallèle.

5-4-2) Modélisation des profils des courants des opérateurs :

a) Analyse du protocole (phases de l'activité en courant) :

L'activité du courant d'un opérateur dépend du protocole de transmission utilisé, puisque c'est celui-ci qui gère la les communications entre les blocs. Son activité peut être décomposée en différentes phases.

Un protocole 4 phases WCHB (Weak Condition Half Buffer), par exemple, peut être décomposé en 3 phases [4]. Chaque phase correspond à une action principale d'un étage : arrivée des données, ouverture du latch et fermeture du latch.

L'analyse du comportement de l'opérateur B de la figure V-20 [4] justifie cette décomposition :

- Phase 1 : Les données arrivent de l'étage précédant A, qui envoie le signal de requête (ReqA). La logique combinatoire de l'opérateur A traite des données reçues. La fin du calcul marque la fin de la phase.
- Phase 2 : Le signal *enable* commute et laisse les données passer à travers les latches de B. L'étage B envoie une requête (ReqB) à l'étage C et un acquittement (AckB) à l'étage A.
- Phase 3 : L'étage B attend le signal d'acquittement (AckC) de l'étage C et la remise à zéro du signal de requête (ReqA) de l'étage A. Ensuite, le signal *enable* passe à zéro : les latches de B sont bloqués. Puis l'étage B cesse d'envoyer le signal de requête (ReqB) à l'étage C et le signal d'acquittement (AckB) à l'étage A.

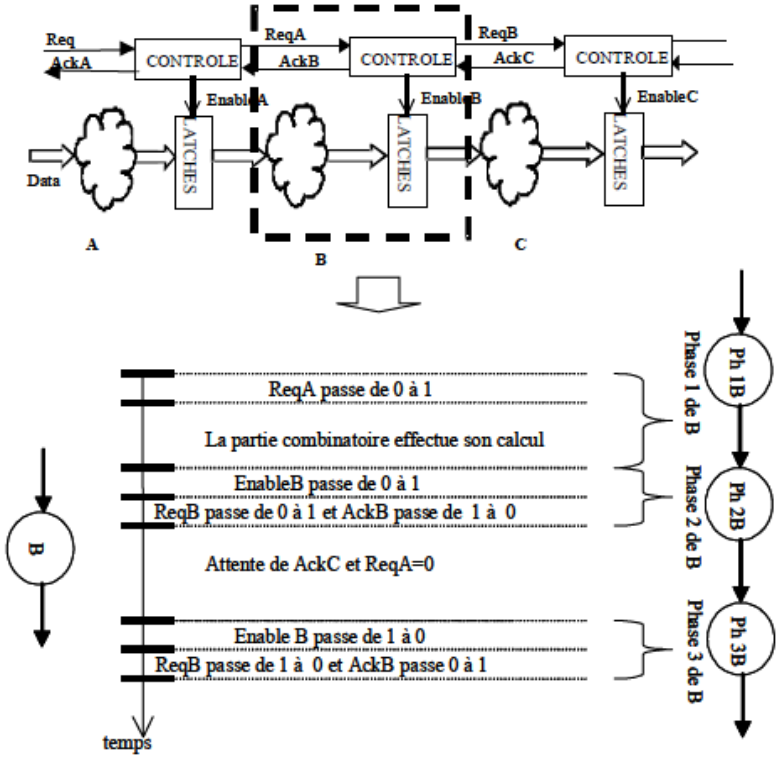


Figure V-20 : Activité du courant dans l'opérateur B (régi par le protocole WCHB).

b) Modèle de courant dans une phase :

Le courant consommé à chaque phase peut être représenté par un triangle (figure V-21 [4]) qui illustre une forte consommation au début de la phase, suivie d'une diminution graduelle de celle-ci.

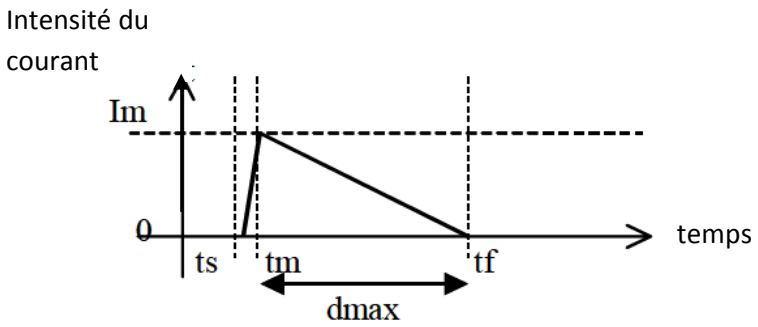


Figure V-21 : Modélisation de l'activité du courant d'une phase d'un protocole.

Les caractéristiques du triangle sont les suivantes :

- ts : Instant où le courant croît et atteint 1% de sa valeur maximale.
- tf : Instant où le courant décroît et descend en dessous de 1% de sa valeur maximale.
- Im : Valeur maximale du courant.
- tm : Instant où le courant atteint sa valeur maximale Im.

Cette représentation permet de déterminer approximativement la position des pics de courant. Soit le triangle $\Delta_i^{phase1}(t)$ la représentation de l'activité du courant de la première phase de l'opérateur i. Elle inclut essentiellement l'activité de la fonction combinatoire (voir le paragraphe 5-4-2-a). Les triangles, représentant la deuxième phase $\Delta_i^{phase2}(t)$ et la troisième phase $\Delta_i^{phase3}(t)$ incluent essentiellement les profils des courants dus au protocole de communication.

c) Allure du courant global :

Après avoir représenté le CDFG représentant le circuit avec les modèles des courants des opérations et des phases de communication, le profil global du courant peut être estimé à :

$$Itot(t) = \sum_{i=0}^{N} \Delta_i^{phase1}(t) + \sum_{i=0}^{N} \Delta_i^{phase2}(t) + \sum_{i=0}^{N} \Delta_i^{phase3}(t) \qquad [4]$$

Et en insérant des retards, l'expression précédente devient comme suit:

$$Itot(t) = \sum_{i=0}^{N} \Delta_i^{phase1}(t, D_i) + \sum_{i=0}^{N} \Delta_i^{phase2}(t, D_i) + \sum_{i=0}^{N} \Delta_i^{phase3}(t, D_i) \qquad [4]$$

Cependant, certains chemins ne doivent pas subir de retard au risque de faire perdre au circuit son fonctionnement normal. Donc, il faut veiller à identifier ces chemins dits critiques et ne pas les perturber.

5-5) Exemple illustrant la mise en forme du courant d'un circuit asynchrone :

Pour illustrer la méthode de répartition des courants, reprenons l'exemple de la figure V-18.

5-5-1) Analyse du modèle de l'architecture :

L'architecture est modélisée selon les priorités des opérations et leur ordre d'exécution, d'un point de vue chronologique. Le modèle obtenu permet de mettre en évidence la liaison entre les opérations. On voit bien dans la figure V-22 [4] que la multiplication, l'addition et l'identité fonctionnent en parallèle. Il est à noter que le fonctionnement récurrent de la structure n'est pas pris en compte : pour des raisons de simplification, le circuit traite une donnée en entrée lorsqu'il délivre sa sortie. On suppose également que l'architecture du circuit et les portes qui le composent sont connues.

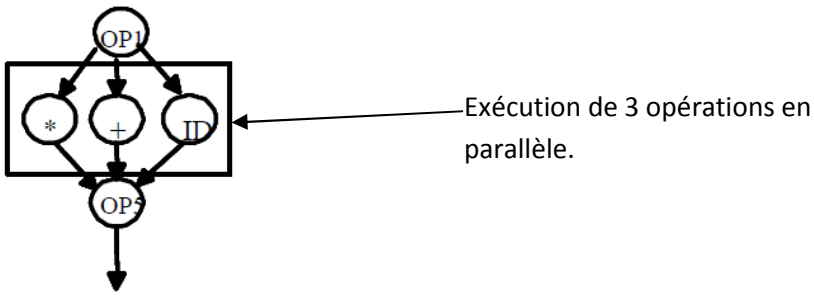


Figure V-22 : Mise en évidence de la concurrence de la multiplication, de l'addition et de l'identification.

5-5-2) Utilisation des modèles de courant :

Tous les opérateurs peuvent être modélisés par les phases de leur activité en courant. Dans notre cas, les opérateurs sont régis par le protocole WCHB (décrit dans le paragraphe 5-4-2-a) dont les phases 2 et 3 sont fusionnées en une seule, dans les représentations qui suivent. Les latences des différents opérateurs peuvent être estimées après leur synthèse. Les latences des différentes phases d'activité du courant dans les opérateurs ainsi que la forme du courant (qui va permettre de définir les triangles) sont déterminées par le moyen d'une simulation électrique.

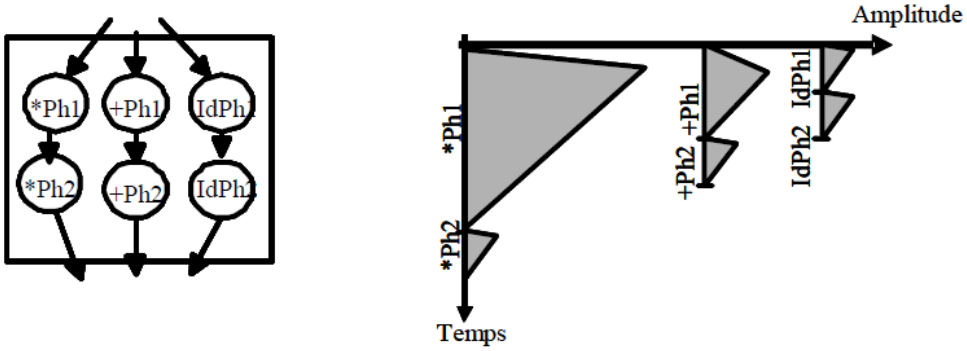


Figure V-23 : Utilisation des modèles de courant pour représenter l'activité des différents opérateurs

La représentation du côté droit de la figure V-23 [4] met l'accent sur l'activité en courant des différents blocs et leurs phases d'activité.

5-5-3) Définition des pas de temps:

De façon analogue à celle d'une discrétisation des signaux utilisée dans les systèmes de communications numériques, il faut définir une fréquence d'échantillonnage. Cette fréquence, dans le domaine temporel est une période (inversée), elle définira à quel temps il faut prendre un échantillon. Ce temps sera défini comme une référence telle qu'à tous ces multiples entiers un échantillon soit enregistré. On appellera cette unité de temps : un pas de temps.

Les pas de temps sont définis en fonction de la latence des différents opérateurs, prendre la petite valeur de latence d'un bloc semble une solution satisfaisante.

Soient les latences suivantes [4] :
La latence de la multiplication au cours de la phase 1 : *Ph1 = 8ns
La latence de la multiplication au cours de la phase 2 : *Ph2 = 2ns
La latence de l'addition au cours de la phase 1 : +Ph1 = 4ns
La latence de l'addition au cours de la phase 2 : +Ph2 = 2ns
La latence de l'identification au cours de la phase 1 : IdPh1 = 2ns
La latence de l'identification au cours de la phase 2 : IdPh2 = 2ns

Le pas qui sera pris (la plus petite valeur) : Tstep = 2ns. Le pas étant fixé, on procède à la discrétisation des triangles pour qu'ils puissent être utilisés par un processeur. Les calculs appropriés seront effectués (par un processeur) pour bien répartir les courants [4] :

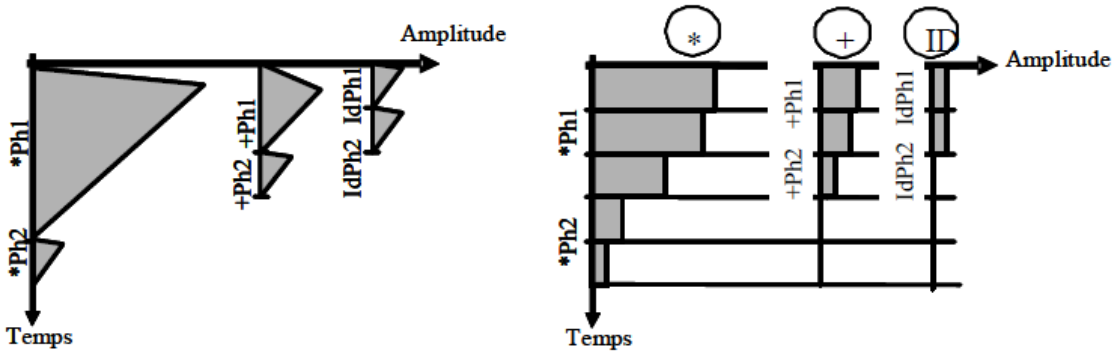


Figure V-24 : Discrétisation des modèles en courant.

5-5-4) Répartition des courants :

Pour répartir les courants, un ordinateur effectuera des calculs de sorte que ceux-ci soient distribués de la façon la plus équitable possible. Un exemple d'un résultat optimal est représenté dans la figure V-25 [4].

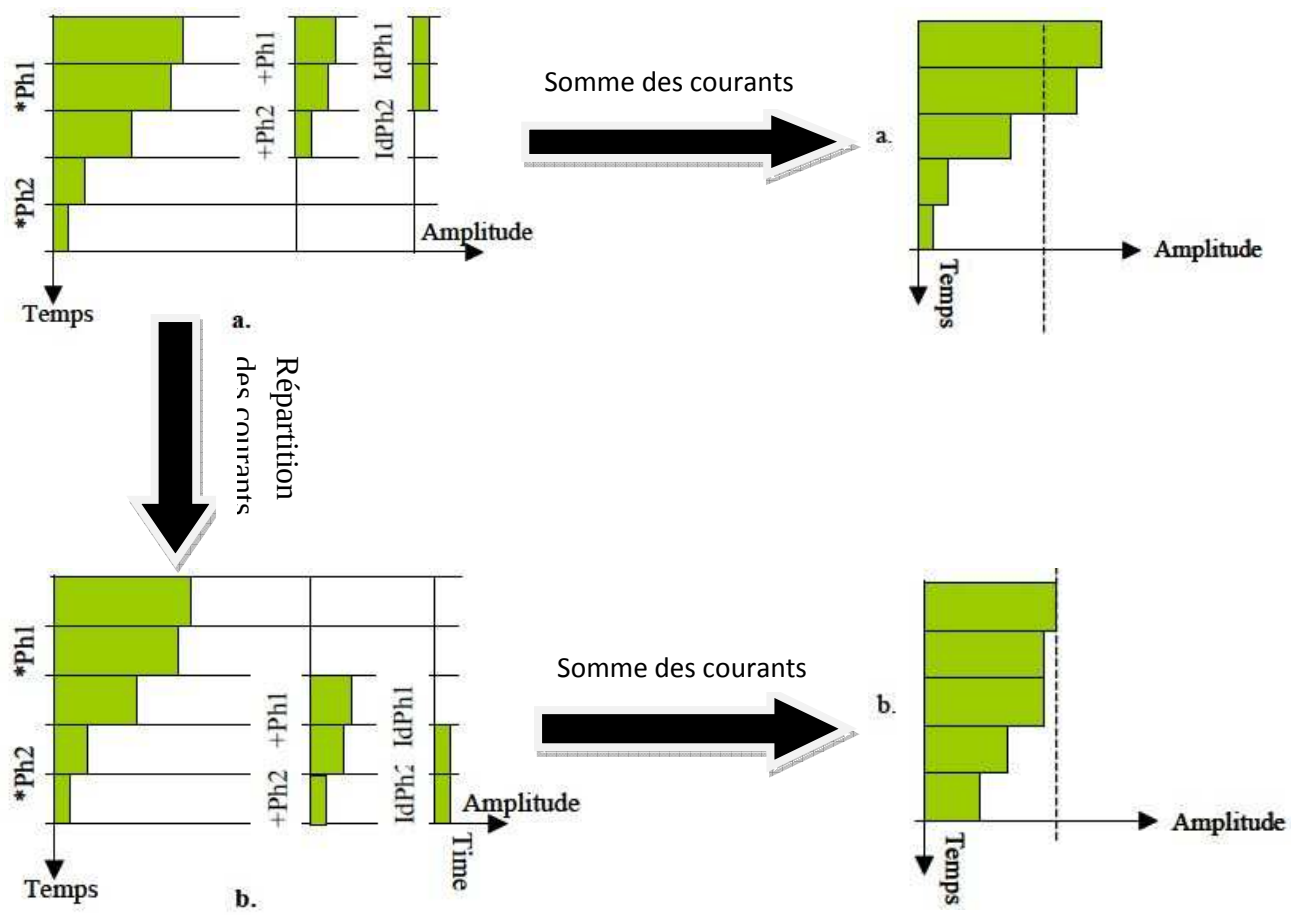


Figure V-25 : Représentation de l'activité des courants et de leurs sommes avant d'être répartis (partie a) et après avoir été répartis (partie b).

La figure ci-dessus fait comparer la consommation en courant dans le circuit pris comme exemple. Elle met en évidence ce qu'il aurait consommé sans une étude de répartition préalable, et avec une étude préalable de répartition des courants. Il semble évident que les courants consommés sont bien moins importants dans le dernier cas.

5-6) Application de la méthode à un circuit réalisant une fonction concrète :

Enfin, nous exposons dans la figure comparative V-26 [4] l'effet de l'application de cette méthode sur un filtre numérique FIR.

La figure V-26 montre le spectre en fréquence de l'activité du courant dans deux filtres asynchrones :

- Un filtre (partie a de la figure) dont la répartition des courants est aléatoire.
- Un filtre (partie b de la figure) dont la répartition des courants est étudiée, et donc bien distribués.

Il est évident que le deuxième filtre consomme moins de courant et donc rayonne moins, ce qui confirme l'efficacité de la méthode de la répartition des courants.

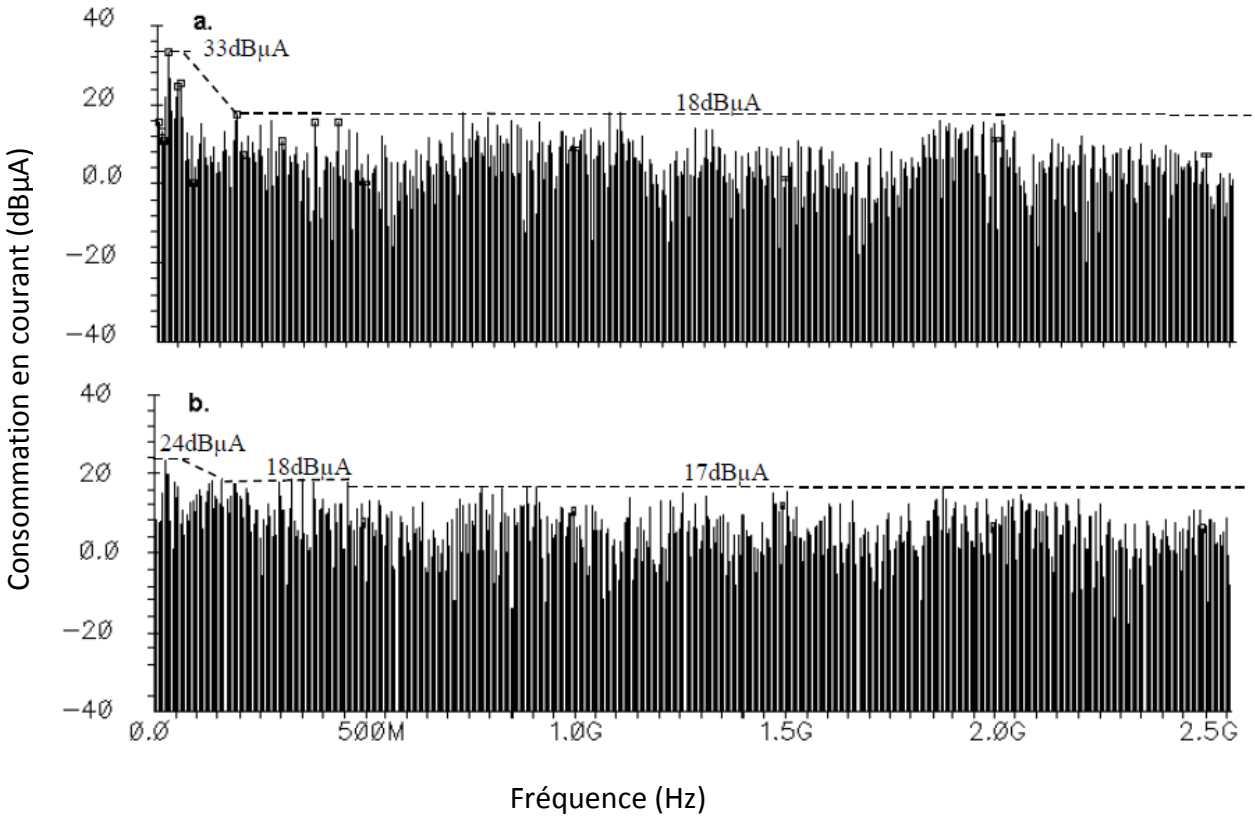


Figure V-26 : Spectres en fréquence du courant dans le filtre RIF sans application de la méthode de la mise en forme du courant (en haut) et avec l'application de celle-ci (en bas).

Conclusion :

Dans ce chapitre, nous avons définis les circuits synchrones et leurs homologues asynchrones, qui sont moins connus. Nous avons justifié notre préférence pour l'utilisation et la fabrication des circuits asynchrones en énumérant leurs avantages sur les circuits synchrones. Un avantage considérable à citer, est une consommation moindre de courant car les blocs inactifs sont désactivés contrairement à leurs équivalents synchrones. De plus, le déclenchement décalé (asynchrone) des commutations transistors favorisent la diminution des courants sur les pins de masses ce qui induit à un rayonnement amoindri.

Nous avons présenté la méthode d'asynchronisation des circuits déjà synchrones. En effet cela est nécessaire, puisque des méthodes de fabrication de masse automatisées n'ont pas atteint le degré de maturité des méthodes utilisées pour fabriquer des circuits synchrones. C'est la raison pour laquelle des méthodes de fabrication provisoires comme celles-ci ont été introduites. Nous avons donné les conditions (de bon fonctionnement) qu'un circuit asynchrone devait respecter pour remplir, sans problème, la fonction de son équivalent synchrone. Bien sûr, un exemple de chaque bloc élémentaire d'un circuit asynchrone

équivalent à un circuit synchrone a été également donné : les latches remplacent les flip-flops et le signal d'horloge est remplacé par un contrôleur et une liaison transportant les signaux de communication (requête/acquittement) et les données.

Puis, la méthode de la répartition des courants a été présentée pour diminuer davantage les émissions des circuits asynchrones. En effet, outre le caractère aléatoire avantageux de la répartition des courants dans un circuit asynchrone, une distribution intelligente et équitable des courants diminuera des pics de courants indésirables. Une méthode graphique a été présentée (CDFG) pour mettre en évidence les blocs fonctionnant en parallèle. C'est la répartition des courants de ces blocs qui est décisive. Enfin, des résultats de mesure confirment l'efficacité de cette méthode sur un circuit effectuant une fonction complexe : un filtre FIR.

La dernière méthode peut encore être améliorée en étudiant les concurrences dans la partie contrôle qui gère le protocole de communication.

Conclusion générale :

L'étude de la compatibilité électromagnétique des circuits intégrés est primordiale, du fait de leur omniprésence dans tous les systèmes automatisés modernes. Notre étude s'est justement intéressée à l'optimisation de la compatibilité électromagnétique des circuits intégrés, en présentant des techniques réduisant leur émission et diminuant leur susceptibilité aux perturbations externes au maximum. Dans le chapitre trois, nous avons évoqué plusieurs techniques permettant l'amélioration de la compatibilité électromagnétique des circuits intégrés. Certaines visaient à réduire leur émission parasite, telles que la réduction de la taille des bondings et des leads. D'autres visaient à augmenter leur immunité aux agressions extérieures telles que l'ajout d'un trigger de Schmitt aux entrées d'un circuit numérique afin de lisser les signaux. Enfin, l'ajout des capacités de découplage permet de réduire les émissions parasites et d'augmenter l'immunité d'un circuit intégré à la fois.

Nous avons détaillé, ensuite, des techniques de programmation pouvant améliorer davantage l'immunité de circuits intégrés numériques programmables (microcontrôleurs ou microprocesseur).

Une étude sur les circuits asynchrones, du fait de leurs faibles émissions, a été faite. Elle a exposé leur architecture et a mis en évidence son efficacité, du point de vue compatibilité électromagnétique. Cette logique de conception des circuits numériques permet, en évitant les commutations simultanées des transistors, d'éviter la consommation de forts courants. Cela se traduit par un bruit émis plus faible comparativement à un circuit équivalent synchrone.

Toutes les techniques citées dans ce mémoire, doivent évoluer afin de satisfaire des contraintes de plus en plus sévères. Il n'est pas possible d'imaginer ou de dissocier la microélectronique de la compatibilité électromagnétique des circuits intégrés. Les deux domaines, dépendants l'un de l'autre, doivent évoluer au même rythme. Par ailleurs, le contexte de fonctionnement des systèmes électronique est de plus en plus sévère, ce qui rend les exigences fixées par les normes CEM de plus en plus difficiles à respecter. Cela présuppose qu'il faille encore explorer ce domaine, toujours fertile, et trouver de nouvelles techniques tenant compte des exigences futures.

GLOSSAIRE

ASIC : Application-Specific Integrated Circuit. Circuit intégré conçu à assurer le fonctionnement d'une application spécifique, par opposition aux circuits intégrés d'utilisation générale tels que les microcontrôleurs.

Bonding : Connexion métallique qui lie la puce aux connexions extérieurs du boîtier.

Circuit numérique asynchrone : Circuit dont les séquences des traitements sont assurées par des communications de type poignée de (handshake) entre les opérateurs.

Circuits synchrones : Circuit dont la séquence des traitements est régie par un signal global appelé couramment horloge. A chaque front de ce signal, des données sont libérées par des registres à l'intérieur du circuit.

CEM : Compatibilité électromagnétique. Aptitude d'un système électrique à fonctionner dans un environnement donné sans perturber son environnement ni être lui-même perturbé.

CI : Circuit Intégré.

(C)DFG : (Control) Data Flow Graph. Graphe permettant de décrire le flot de données d'un système. Les nœuds représentent les opérations dans le système. Les arcs représentent les dépendances entre les opérations.

di/dt : Variation du courant qui est la principale cause des émissions électromagnétiques du circuit lors de son passage dans les éléments inductifs et capacitifs. Plus les variations du courant sont brusques, plus le circuit génère des émissions électromagnétiques.

Discrétisation : Action de découper, en échantillons réguliers, un signal soit en temps soit en amplitude. Cette opération est très utile en particulier pour que le signal puisse être traitée par un microprocesseur.

ESD : ElectroStatic Discharge. Décharge électrostatique.

IEM : Interférences électromagnétiques. Elles sont dues aux émissions électromagnétiques des systèmes. Elles peuvent survenir suite à des phénomènes de couplages ou une interprétation des ondes électromagnétiques parasites comme un signal utile par des circuits récepteurs.

Lead : Connexion métallique extérieure du boîtier. Elle est appelé également broche.

Micropipeline : Catégorie de circuits asynchrones où la partie de contrôle est distincte de la partie chemin de donnée. Des délais sont utilisés dans les canaux de communication pour assurer la validité des données dans le circuit.

Ordonnancement : Action de répartir et d'ordonner dans le temps les traitements de différents opérateurs. L'ordonnancement s'effectue sous différentes contraintes (temps, nombre de ressources…). Cette action est généralement effectuée à la synthèse comportementale du circuit.

PCB : Printed Circuit Board. Circuit imprimé.

RTL : Register Transfer Level. Description d'un circuit intégré numérique au niveau registre d'un circuit, c'est-à-dire, les briques de construction utilisées pour former le circuit est le registre.

TLP : Transmission Line Pulsing : méthode de génération d'un signal impulsionnel utilisant une ligne de transmission. Par extension, caractéristique courant/tension quasi-statique d'un composant ESD.

Via : Connexion métallique qui lie deux étages successifs de réseaux de connexions métalliques. C'est une sorte d'ascenseur qui fait la liaison entre deux étages dans certains points uniquement.

WCHB : Weak Condition Half Buffer. Protocole de communication utilisé dans les circuits asynchrones, appelé aussi protocole standard.

Bibliographie

[1] Sonia Ben Dhia, Mohamed Ramdani, Etienne Sicard, "Electromagnetic compatibility of integrated circuits, Techniques for low emission and suscpetibility", Springer Edition, ISBN : 0-387-26600-3, 2006.

[2] Alexandre Boyer, "Méthode de prédiction de la compatibilité électromagnétique des systèmes en boîtier", Thèse de Doctorat présentée à l'Institut National des Sciences Appliquées de Toulouse, 2007.

[3] Nicolas Guitard, "Caractérisation de défauts latents dans les circuits intégrés soumis à des décharges électrostatiques", Thèse de Doctorat présentée à l'Université Paul Sabatier Toulouse III, 2007.

[4] Dhanistha Panyasak, "Réduction de l'émission électromagnétique des circuits intégrés : l'alternative asynchrone", Thèse de Doctorat présentée à l'Institut National Polytechnique de Grenoble, 14 juin 2004.

[5] Nicolas Nolhier, "Méthodologie de conception des protections des circuits intégrés contre les décharges électrostatiques", Synthèse de travaux en vue de l'obtention de l'Habilitation à Diriger des Recherches de l'Université Paul Sabatier Toulouse III, 30 novembre 2005.

[6] JY Fourniols, "Compatibilité électromagnétique des circuits intégrés, caractérisation des interconnexions", Cours de 2ème année Master Recherche Spécialité Microélectronique du Pôle de Formation en Microélectronique de l'Institut National des Sciences Appliquées de Toulouse.

[7] Etienne Sicard, "Compatibilité électromagnétique des circuits intégrés", Cours de l'Institut National des Sciences Appliquées de Toulouse, 2009.

[8] www.lesia.insa-toulouse.fr

[9] www.lattis.univ-toulouse.fr

[10] http://www.lesia.insa-toulouse.fr/~bendhia/

[11] http://www.cvel.clemson.edu/emc/

[12] Hans Jacobson, "Asynchronous circuit design, a study of a framework called ACK", Thèse de Master of Science soumise à l'Université de Technologie de Lulea (Lulea University of Technology), Mai 2006.

[13] Bertrand Folco, "Contribution à la synthèse de circuits asynchrones quasi-insensibles aux délais, application aux systèmes sécurisés", Thèse de Doctorat présentée à l'Institut National Polytechnique de Grenoble, 4 octobre 2007.

[14] Vivian Brégier, "Synthèse automatisée de circuits asynchrones optimisés prouvés quasi-insensibles aux délais", Thèse de Doctorat présentée à l'Institut National Polytechnique de Grenoble, 14 septembre 2007.

[15] Stéphane Baffreau, "Susceptibilité des micro-contrôleurs aux agressions électromagnétiques", Thèse de Doctorat présentée à l'Institut National des Sciences Appliquées de Toulouse.

[16] Catherine Douillard, Gérald Ouvradou, Michel Jézéquel, "Logique séquentielle, techniques d'intégration", Cours de 3ème année Licence d'électronique numérique de l'Ecole Nationale Supérieure des Télécommunications de Bretagne, Septembre 2006.

[17] J.G. Sketoe, "Integrated circuit electromagnetic immunity handbook", NASA (Boeing Information, Space and Defense, Seattle, Washington), Août 2000.
[18] C.R. Paul, "Introduction to electromagnetic compatibility", Wiley-Interscience, ISBN 0-471-54927-4, 1992.
[19] Christos Christopoulos, "Principles and techniques of electromagnetic compatibility", Second edition, CRC Press, ISBN : 0-8493-7035-3, 2007.
[20] Tim Williams, "EMC for product designers", Third edition, Newnes, ISBN : 07506 4930 5, 2001.
[21] Carl Nassar, "Telecommunications demystified, a streamlined course in digital communications (and some analog) for EE students and practicing engineers", LLH Technology Publishing, ISBN : 1-878707-55-8 ,2001.
[22] Chris J. Myers, "Asynchronus Circuit Design", Wiley-Interscience, ISBN : 0-471-22414-6, 2001.
[23] Enrique Lamoureux, "Etude de la susceptibilité des circuits intégrés numériques aux agressions hyper-fréquences", Thèse de Doctorat présentée à l'Institut National des Sciences Appliquées de Toulouse, 25 janvier 2006.