CIRCUITOS AUTOTESTAVEIS: OPÇAO DE PROJETO DE CIRCUITOS VISANDO O TESTE IMPLICITO OU CONCORRENTE.

I. JANSCH *

SUMARIO

A partir de uma abordagem genérica inicial sobre a testabilidade dos circuitos, estuda-se em detalhe as propriedades de autoteste desses, com vista à detecção de falhas em funcionamento. A evolução da teoria clássica à moderna é analisada e vislumbra-se a conveniência da inclusão dessas propriedades nos circuitos a serem concebidos. Somente as principais definições de base são formuladas - o enfoque predominante é conceitual.

ABSTRACT

Initially, a generic approach introduces the idea of testability. From this one, we study in detail the self-checking properties of the circuits, in view of on-line faults detection. The evolution from the classic theory to the modern one is analyzed, conducting us to see that these properties may be conviniently included in circuits during their design. Only the basic definitions are formulated - this paper is mainly conceptual.

* Engenheira Eletrônica (UFRGS, 1979), Mestre em Ciência da Computação (UFRGS, 1982), Doutora-Engenheira em Microeletrônica (INP de Grenoble, 1985). Endereço: PGCC/UFRGS - Caixa Postal 1501 - 90.000 PORTO ALEGRE - RS.

I. Introdução

Os avanços atingidos pela tecnologia de circuitos integrados têm tornado possível a realização de dispositivos muito complexos em um único "chip" (circuito integrado). Isto provocou uma consequência indesejável: o aumento do tempo de geração de teste. Achar em pouco tempo um conjunto de testes de comprimento razoável que assegure uma cobertura satisfatória de falhas tornou-se um problema de dificuldade crescente à medida que a complexidade do circuito aumenta. Sabe-se que o tempo necessário para a geração automática de testes e a simulação de falhas em um circuito combinacional aumenta com o cubo do seu número de portas lógicas; já em circuitos sequenciais, o tempo de geração de teste pode ser muito maior do que o anterior, dependendo do seu número de estados. Por outro lado, uma baixa cobertura de falhas no teste do chip leva ao decréscimo do rendimento a nível de placa ou sistema.

O custo de localização e reparação de uma falha cresce em um fator da ordem de 10 à medida que se evolui de um chip a uma placa e de uma placa ao nível do sistema - portanto, o teste do chip com alta cobertura de falhas se torna necessária. Mas, referindo-se a um circuito VLSI, isto pode ser impossível de ser obtido em um tempo razoável. E a solução para este problema é incluir testabilidade como restrição de projeto. O resultado desta decisão é a geração de metodologias de projeto visando o aprimoramento das técnicas de teste dos circuitos.

II. Alguns conceitos de "Concepção visando a Testabilidade".

Sob o nome de "Concepção visando a Testabilidade", CVT (do inglês "Design for Testability"), várias técnicas são reunidas, cujos objetivos e campos de aplicação diferenciam-se totalmente.

Uma classificação inicial pode ser feita de acordo com o tipo de capacidade de teste que o método CVT fornece ao circuito: autoteste em funcionamento, autoteste fora de funcionamento,ou técnicas não relacionadas com autoteste.

Os testes em funcionamento são concorrentes com a operação normal do circuito (do inglês, "on-line") e os testes fora de funcionamento são aqueles cuja execução necessita suspender a operação normal do circuito (do inglês, "off-line").

Os métodos usados para atingir a capacidade de teste em funcionamento são completamente diferentes daqueles usados para o teste fora de funcionamento. Os primeiros baseiam-se em informação redundante (codificação), redundância do circuito (duplicação) ou redundância de tempo (auto-

comparação), enquanto que os últimos baseiam-se na reconfiguração funcional da arquitetura do chip.

Fora de funcionamento, o circuito é: facilmente testável, se o seu procedimento de teste deve ser executado por um monitor externo; e autotestável, se ele executa o seu próprio teste sem necessitar nenhuma supervisão externa.

Os circuitos facilmente testáveis contêm uma lógica extra usada para gerar padrões de teste e executar os testes facilmente. Entretanto, necessitam de dispositivo externo para gerar os estímulos de entrada e verificar a correção da resposta. Outros, mais complexos, são capazes de gerar, internamente, parte ou todo o estímulo de teste, mas necessitam de avaliação externa da resposta; ou, se podem realizar auto-avaliação das saídas de teste, necessitam da aplicação externa de padrões de teste.

Os circuitos autotestáveis possuem internamente toda a lógica necessária à geração dos estímulos de entrada, a coletar respostas e avaliá-las. O testador externo só é usado para iniciar o procedimento de teste, esperar por sua realização e então controlar o resultado (dado, em geral, por uma indicação externa do tipo "prosseguir" ou não).

As metodologias de concepção associadas a testes executados em períodos intercalados à operação do circuito, visam a detecção de falhas de fabricação ou daquelas surgidas como consequência do esgotamento da vida útil do componente ou da má-utilização de equipamentos ou componentes. Mas em sistemas críticos, onde a ocorrência de uma falha pode resultar em consequências graves, não podemos admitir que resultados errados sejam gerados e reutilizados dentro dos circuitos. Se este é o caso, é imprescindível o emprego de técnicas de autoteste em funcionamento, as quais permitem a detecção e sinalização de falhas, antes que essas resultem em erros perigosos. Exemplos desses tipos de sistemas podem ser: complexos de transporte de contrôle eletrônico (trens, metrôs, etc...), aviação, aplicações espaciais e militares, etc... Na maior parte delas, erros podem trazer como consequência a perda de vidas humanas.

Nas seções que se seguem, abordaremos conceitos relacionados aos sistemas autotestáveis que detectam falhas durante o funcionamento, sinalizando-as. O objetivo básico é a "tomada de consciência da falha". A reconfiguração do sistema, a entrada em operação de uma unidade suplementar, ou outras providências, são deixadas à área de "Tolerância a Falhas".

III. Hipóteses de falhas

Durante um longo tempo, o modelo de falhas mais frequentemente considerado em técnicas de teste era baseado na suposição de falhas lógicas representáveis por valores fixos nos níveis lógicos 0 ou 1 (em inglês, "stuck-at-0" "stuck-at-1"), associados ao diagrama lógico do circuito a ser testado. Mas existem alguns tipos de falhas não modeláveis por "colagens" ("stuck-at"). Na figura 1 é mostrado um exemplo, através do qual Galiay et al. [Gal 79] mostrou um caso não modelável por colagem - a falha implica na modificação da função executada pela porta lógica. O curto circuito 1 e o circuito aberto 2 não podem ser representados sobre o circuito lógico correspondente.

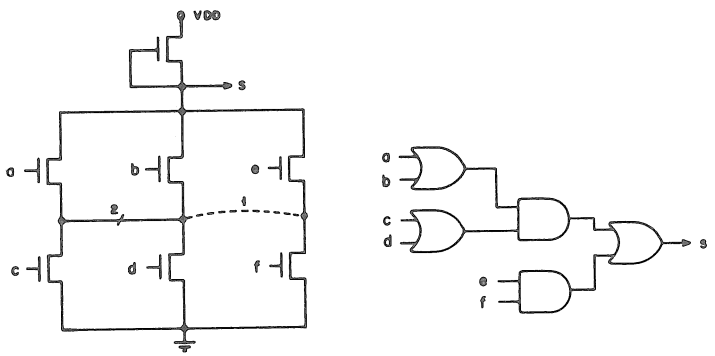

Figura 1: Falhas não representáveis por colagens.

Na prática, aparentemente a maior parte das falhas físicas são curtos circuitos e circuitos abertos (cortes nas linhas). Para esses, a representação do circuito por diagramas lógicos não é mais adequada. O estudo dos tipos de falhas deve ser embasado na topologia real do circuito, i.e., no modelo real do circuito físico. E os modelos de falhas devem representar falhas reais que ocorrem nos circuitos integrados, o que é referido como "hipóteses de falhas físicas" (ou "reais", ou "de baixo nível").

Para o projeto do circuito propriamente dito, outras considerações adicionais devem ser feitas, como: somente uma falha física ocorre em cada momento; há um certo espaçamento temporal entre a ocorrência de duas falhas físicas, etc...

IV. O sistema autotestável-teoria clássica

Conforme abordamos anteriormente, a metodologia de concepção autotestável emprega redundância de informação e material. Faz-se necessário

codificar informações internas para que "irregularidades" sejam detectadas, e incluir circuitos que atuarão nesta detecção. Assim a função básica inicial do circuito é executada por um circuito funcional construído sob determinadas regras e fornece um conjunto de saídas codificadas - estas serão decodificadas ou usadas diretamente por outros circuitos. O conjunto codificado é analisado por um controlador, o qual produz uma sinalização de erro, se for o caso. O sistema assim composto é representado pelo esquema da figura 2. Para que o mesmo tenha capacidade de detecção de 100% das falhas perigosas (que causam modificações da função executada), é necessário que este tipo de falhas cause modificação no código de saída do circuito funcional e/ou que o controlador garanta a indicação de erro, mesmo em presença de falha.

Com esse propósito são definidos os sistemas totalmente autotestáveis [AND 71]. São consideradas redes lógicas combinacionais G de múltiplas entradas e múltiplas saídas. O espaço de entrada X é composto de 2^r vetores binários de comprimento r, para r linhas de entrada. O espaço de saída Y é composto de 2^q vetores binários de comprimento q, para q linhas de saída. Não ocorrendo falha, a rede G recebe somente um subconjunto de X denominado espaço de código de entrada A e produz um subconjunto de Y denominado espaço de código de saída B. Elementos pertencentes ao espaço de código são referidos como palavras codificadas. Palavras não codificadas podem ser geradas sob a ocorrência de uma falha.

A saída de G sob uma entrada x é representada por: G(x,f), para uma falha f presente na rede G e G(x,∅), se não há falha na rede G.

Definição 1: G é segura a falhas com relação a F se para todas falhas em F e todas entradas de código, a saída ou é correta ou é uma palavra não codificada; i.e., para todas f ε F e para todas a ε A,

$$G(a,f) = G(a,\emptyset) \text{ ou } G(a,f) \notin B.$$

Definição 2: G é autotestável com relação a F se para cada falha em F há ao menos uma entrada de código que produz uma saída não codificada; i.e., para todos fεF, há uma entrada aεA, tal que G(a,f)∉B.

Definição 3: G é totalmente autotestável (TAT) com relação a F se ela é segura a falhas e autotestável com relação a F.

Portanto, de acordo com as definições acima, uma saída errada provocada por uma falha em um circuito seguro a falhas é sempre um vetor não codificado. E um circuito autotestável é diagnosticável com apenas suas entradas de código, e ao menos uma entrada de código resulta em uma saída não codificada para qualquer falha. Assim, em circuitos que são simultaneamente autotestáveis e seguros a falhas (circuitos TAT), todas as falhas

causam saídas errôneas detectáveis durante sua operação normal.

Definição 4:Uma rede G é de código disjunto se ela sempre mapeia entradas codificadas em saídas codificadas, e entradas não codificadas em saídas não codificadas, i.e., se:

$\forall a \in A,\ G(a,\emptyset) \in B$

$\forall a \notin A,\ G(a,\emptyset) \notin B.$

Definição 5: Uma rede é um controlador TAT se ela é TAT e de código disjunto.

O objetivo dos sistemas construídos com as características definidas acima é de assegurar que a primeira saída incorreta obtida, não é uma palavra do espaço de código de saída B. Esta propriedade é referida como objetivo TAT.

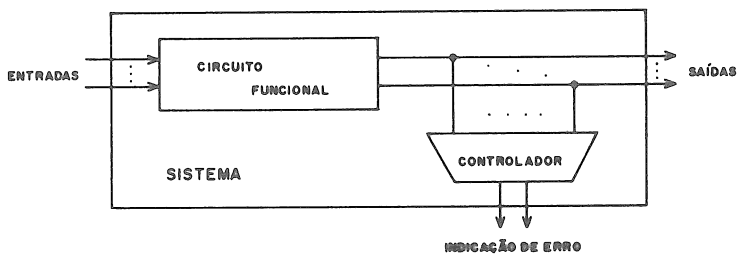

Figura 2: Estrutura de um Sistema autotestável.

V. O caso real (teoria moderna)

Quando são consideradas hipóteses de falhas físicas, sabe-se que podem ocorrer determinadas falhas que não causam erros na saída, como certos tipos de curtos circuitos entre linhas de mesmo tipo, cortes em uma linha redundante, etc... Entretanto estes casos não são previstos pela teoria clássica (redundância com relação a determinadas falhas).

Da mesma maneira, a teoria clássica, calcada sobre portas lógicas como elemento base, podia considerar a utilização de circuitos integrados comerciais como elementos de implementação, cujas entradas e/ou saídas estariam com valores fixos em 0 ou 1, dependendo da falha ocorrida. Atualmente sabe-se que o emprego de portas complexas internas a um mesmo chip cuja estrutura interna não se conhece,pode resultar em modificações de função não representáveis através dos parâmetros e variáveis disponíveis como entradas e saídas deste circuito.

A partir dessas considerações foram definidos os circuitos funcionais "fortemente seguros a falhas" (do inglês, "strongly fault secure",

[SMI 78]), e os controladores "de código fortemente disjunto" (do inglês, "strongly code disjoint", [NIC 84b]). Esses circuitos são definidos a partir de hipóteses de falhas físicas, e são concebidos sob determinadas restrições (regras). A principal diferença, com relação à teoria clássica, refere-se a possibilidade de ocorrerem falhas com relação as quais o circuito é redundante, como definido a seguir.

Definição 6: Uma rede que realiza a função $G(a,\emptyset)$ é redundante com relação a falha f se $G(a,f) = G(a,\emptyset)$, $\forall a \in A$.

Pode-se observar que uma rede redundante com relação a uma falha f não mantém a propriedade autotestável. Mas o maior problema é a possibilidade de ocorrência de uma segunda falha a qual, associada à primeira não detectada, pode provocar palavras de saída erradas. Lembramos que a segunda falha pode ser vista como não mais afetando a rede G, mas uma rede G modificada pela primeira falha. Ou podemos considerar G como sendo afetada por uma falha dupla. Assim, o conceito de circuitos TAT não é mais aplicável: ele deve ser substituído por outro que, admitindo a ocorrência de falhas redundantes, ainda permita ao sistema atingir o objetivo TAT.

Definição 7: Para uma sequência de falhas $<f1, f2, \ldots, fn>$, seja k o menor inteiro para o qual existe $a \in A$ tal que

$$G(a, \bigcup_{j=1}^{k} fj) \neq G(a,\emptyset).$$

Se não existe tal k, seja k=n. Então G é fortemente seguro a falhas (FSF) com relação à sequência de falhas se, para todas as palavras de código $a \in A$,

$$\text{ou } G(a, \bigcup_{j=1}^{k} fj) = G(a,\emptyset) \text{ ou } G(a, \bigcup_{j=1}^{k} fj) \notin B.$$

No caso dos controladores, para que o circuito seja redundante com relação a determinada falha, ele deve manter sua propriedade de "código disjunto". No caso do controlador denominamos B o seu espaço de código de entrada (é o espaço de código de saída do circuito funcional) e C, o seu espaço de código de saída.

Definição 8: Um controlador G é redundante com relação a uma falha f e com relação a um espaço de código de entrada B e com relação a um espaço de código de saída C se:

$\forall b \in B$, $G(b,f) \in C$ e

$\forall b \notin B$, $G(b,f) \notin C$.

Definição 9: Antes que ocorram falhas, o circuito G é de código disjunto. Para uma sequência de falhas $<f1, f2, \ldots, fn>$, seja k o menor inteiro para o qual existe um vetor $b \in B$ tal que:

$$G(b, \bigcup_{j=1}^{k} fj) \notin C.$$

Se não existe tal k, façamos k=n. Assim, o circuito G é "de código fortemente disjunto"(CFD) para a sequência <f1,f2,..., fn> se:

$$\forall b \in B, \forall m \in \{1,2,\ldots,k-1\}, G(b, \bigcup_{j=1}^{m} fj) \notin C.$$

Um circuito funcional FSF é seguro a falhas mesmo em presença de falhas com relação às quais ele é redundante. Um controlador CFD mantém a propriedade de código disjunto também em presença de falhas com relação as quais ele é redundante. Sob a suposição de que não ocorrem falhas ao mesmo tempo no circuito funcional e no controlador, isto é,que após a ocorrência de uma falha no circuito funcional ou no controlador, decorre um espaço de tempo suficiente para a aplicação das entradas de código do respectivo bloco, e que não ocorre nenhuma outra falha, pode-se verificar que o objetivo TAT é atingido pelo sistema assim composto.

VI. Aplicação e conclusões

Os circuitos funcionais FSF são construídos sob determinadas regras que lhes conferem propriedades de detecção de erros simples, unidirecionais ou múltiplos [NIC 84a]. A codificação interna deve ser também coerente com a capacidade de detecção desejada. As estruturas internas de blocos diversos como memória, PLA, unidade logica-aritmética, decodificadores dão margem à ocorrência de diferentes tipos de erros. Assim, se o tipo de erros produzidos é simples, usa-se um código de paridade; para erros unidirecionais produzidos, usa-se códigos m-entre-n, Berger ou Berger modificado; onde erros múltiplos podem ser gerados, um código double-rail garante a detecção.

Na saída dessas unidades, o controle da codificação correta é executada por controladores CFD. Para esses controladores, não existem regras específicas de construção - eles devem ser analisados individualmente em sua topologia interna. O emprego de células de base em sua construção é uma possibilidade que auxilia enormemente a agilização dessa atividade [JAN 84].

A redundância introduzida pela nova concepção dos circuitos ou pela inclusão de outros é variável conforme o tipo de unidades funcionais especificadas. Em média, não ultrapassa 60% da superfície inicial. Um estudo executado sobre o MC 68000 [NIC 84a], um circuito processador geral, resultou em um aumento de superfície em 48%, assegurando a detecção de 100% das falhas simples - inclui corte de linhas, grade flutuante, falha em contato ou pré-contato, e curto-circuito entre duas linhas de alumínio ou duas de difusão. Estes são defeitos reais passíveis de ocorrer em circuitos cuja tecnologia de construção é NMOS.

De acordo com os métodos clássicos, esta proteção só seria atingida através da duplicação integral do circuito, o que implicaria 100% de aumento da superfície e um controlador de saída para executar a comparação.

Referências

[AND 71] ANDERSON, D.A. Design of self-checking digital networks using coding techniques. Urbana, CSL/Univ. Illinois, Set.1971. (Report 527). 133p.

[GAL 79] GALIAY, J.; CROUZET, Y.; VERGNIAULT, M. Physical versus logical fault models in MOS LSI circuits. Impact on their testability. FTCS-9, Madison, 20-22/junho/79. New York, IEEE, 1979. p.189-192.

[JAN 84] JANSCH, I. & COURTOIS,B. Design of SCD checkers based on analytical fault hypothèses. ESSCIRC'84, Edinburgh, 19-21 /setembro/84. Edinburgh, CEP Consultants Ltd., 1984. p. 109-12.

[NIC 84a] NICOLAIDIS, M. Conception de circuits integrés autotestables pour des hypothèses de pannes analytiques. Grenoble, INPG, Jan. 1984 (Tese).

[NIC 84b] NICOLAIDIS, M.; JANSCH, I.; COURTOIS, B., Strongly code disjoint checkers. FTCS-14, Kissimmee, 20-22/junho/84. New York, IEEE, 1984. p. 16-21.

[SMI 78] SMITH, J.E.; METZE, G. Strongly fault secure logic networks. IEEE Transactions on Computers. New York, IEEE, 27(6): 491-9, Junho/1984.