CONCEPÇÃO CELULAR DE CONTROLADORES AUTOTESTÁVEIS BASEADA EM HIPÓTESES DE FALHAS FÍSICAS

I. JANSCH*

SUMÁRIO

Os controladores de código são usados em sistemas autotestáveis, visando a detecção de falhas durante o funcionamento normal - eles têm propriedades particulares e devem ser concebidos sob condições especiais. A partir deste pressuposto e das definições básicas desses circuitos, aborda-se os procedimentos de concepção dos controladores "de código fortemente disjunto" de estrutura celular, considerando-se modelos de falhas reais. As considerações tecnológicas são baseadas em NMOS.

ABSTRACT

Checkers are used in self-checking systems in order to detect failures during normal operation. They have particular properties and are designed under special conditions. From these ideas and giving the basic definitions of these circuits, we study the "strongly code disjoint" checkers design procedure, these chechers having a cellular structure. The fault model is based on physical fault hypotheses. The technological considerations are based on NMOS.

- Pesquisa realizada mormente no INPG - Instituto Nacional Politécnico de Grenoble, França.

* Eng. Eletrônica (UFRGS, 1979), Mestre em Ciência da Computação (UFRGS, 1982), Doutora-Engenheira em Microeletrônica (INPG, 1985). Endereço: Departamento de Informática/PGCC - Caixa Postal 1501 - 90.000 - Porto Alegre - RS.

I. INTRODUÇÃO

Desde que Galiay et al. /GAL 80/ mostraram os problemas decorrentes do modelamento de falhas através de "colagens" (do inglês "stuck-at"), o diagrama lógico revelou-se inadequado como representação de um circuito. Ao nível da concepção de um circuito e da geração de padrões de teste, é necessário usar modelos de falhas representando defeitos reais que podem ocorrer nos circuitos integrados. Estes modelos são referidos como "hipóteses de falhas físicas". O procedimento baseado no conhecimento da topologia real do circuito permite a detecção de circuitos abertos e curtos os quais, na prática, constituem-se na grande maioria das falhas físicas. Os sistemas autotestáveis aqui considerados são compostos de um circuito funcional e um controlador para os quais são requeridas propriedades bem definidas, como será visto resumidamente a seguir. Inicialmente definidos por Carter e Schneider /CAR 68/ e estudados por Anderson /AND 71/, os controladores eram definidos como "Totalmente Autotestáveis" (TAT) e "de Código Disjunto" (CD). Associados a um circuito funcional TAT (o qual é "Seguro a Falhas" (SF) e "Autotestável" (AT)), eles compõem um sistema completo que atinge o objetivo TAT, i.e., a primeira saída errada da rede é uma palavra não codificada. Os controladores de "código fortemente disjunto" (CFD) constituem a maior classe de controladores quando são considerados circuitos combinacionais. Eles são os companheiros naturais dos circuitos "Fortemente Seguros a Falhas" (FSF), definidos por Smith & Metze /SMI 78/.

Tais circuitos FSF formam a maior classe de circuitos funcionais, e admitem a ocorrência de falhas com relação as quais eles são redundantes. O conceito de redundância relacionado aos circuitos funcionais significa que seu comportamento para o espaço de código de entrada não é modificado em presença da falha. A "redundância forte" é uma extensão deste conceito para os casos em que ocorrem sequências de falhas. Então, os circuitos SFS mantêm-se seguros a falhas mesmo em presença dessas falhas.

Os controladores CFD são definidos /NIC 84/ com base em propriedades semelhantes: eles mapeiam entradas codificadas em saídas codificadas e entradas não codificadas em saídas não codificadas, mesmo existindo falhas internas.

Nicolaidis & Courtois /NIC 83/ analisaram a concepção de circuitos FSF baseada em hipóteses de falhas físicas. O objetivo deste artigo é o projeto de controladores com base nas mesmas hipóteses de falhas, as quais são englobadas sob a denominação da Classe I, segundo a definição de Courtois /COU 82/. Essa classe inclui defeitos como circuitos abertos, transistor MOS permanentemente aberto ou conduzindo, contatos ou pré-contatos falhados, curtos entre duas linhas de alumínio (respectivamente, duas de difusão) próximas geograficamente. Um único defeito físico é considerado, e as implementações físicas (ou regras dependentes da tecnologia) são baseadas na tecnologia NMOS.

Para todos os testadores aqui tratados, a indicação geral de erro é dada por um par de linhas de saída com valores complementares (código double-rail).

II. CONSIDERAÇÕES E DEFINIÇÕES BÁSICAS

Neste artigo só estão incluídas as definições diretamente relacionadas aos controladores CFD, tendo sido omitidas algumas intermediárias e outras referentes à teoria clássica e aos demais blocos componentes do sistema autotestável. Para entendimento desta estrutura global e análise dessas definições, sugerimos reportar-se às referências /COU 82/, /JAN 83/ e /JAN 85b/.

Consideramos os controladores como 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 codificado de entrada B e produz um subconjunto de Y denominado espaço codificado de saída C. Elementos que pertencem ao espaço codificado são ditos "palavras codificadas" (ou de código). Palavras não codificadas podem ser geradas sob a ocorrência de falhas.

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

O controlador de código fortemente disjunto é definido como se segue:

Definição: Um controlador é de código fortemente disjunto (CFD) para uma classe C_f de hipóteses de falhas se ele é de código disjunto e, se para todas as sequências de falhas f_i pertencentes a C_f que podem ocorrer, ou existe k tal que:

* o controlador é fortemente redundante com relação à sequência de falhas $\langle f_1, f_2, f_3, \ldots, f_{k-1}\rangle$ e
* $b \in B \mid G(b, \langle f_1, f_2, \ldots, f_k\rangle) \notin C$, ou
* o controlador é fortemente redundante com relação às sequências de falhas.

Lembramos que no caso dos controladores, a redundância com relação a uma falha dada pressupõe o mapeamento de entradas codificadas em saídas codificadas e de entradas não codificadas em saídas do mesmo tipo. O conceito de "fortemente redundante" é uma extensão do primeiro para o caso de ocorrência de uma sequência de falhas: o controlador deve ser redundante com relação a cada uma das subsequências $\langle f_1\rangle$, $\langle f_1,f_2\rangle$, $\langle f_1,f_2,f_3\rangle$, ...

Embora a Classe I considere apenas defeitos simples, a ocorrência sequencial de falhas individuais pertencentes a essa classe resulta em um grupo dessas, podendo ser visto como um defeito múltiplo. Essas falhas serão $\langle f_1\rangle$, $\langle f_1,f_2\rangle$, ... Cabe observar também que a sequência ... $f_i f_j$... não é igual a ... $f_j f_i$ ...

A seguir, passamos a analisar a concepção propriamente dita desses controladores CFD.

III. CONCEPÇÃO: OPÇÃO CELULAR

A concepção de um controlador de código fortemente disjunto não se constitui em uma atividade comum de projeto. O circuito e topologia resultantes devem assegurar a manutenção das propriedades dadas pela definição. Em /JAN 83/, mostrou-se um exemplo de topologia onde ocorre uma falha que não é detectada com a aplicação dos vetores de código, mas com relação a qual o circuito não é redundante. O resultado de uma situação destas é que, esta falha não sendo percebida, não é sinalizada. Mais tarde, ocorrendo uma outra falha no bloco funcional, (cujas saídas constituem-se em entradas do controlador) vai resultar em entradas não codificadas ao controlador. O controlador afetado pela falha não consegue mais garantir a propriedade de código disjunto, i.e., o fornecimento de saídas não codificadas, para este caso.

A complexidade da concepção desses controladores CFD está associada ao fato de que é necessário analisar o comportamento das propriedades desses diante de cada uma das falhas potenciais. Portanto, é evidente o aumento desta complexidade com o aumento do tamanho do circuito - a inclusão de cada nova linha exige estudo.

Como consequência desta constatação pensou-se na possibilidade de fazer o projeto baseado em células, nos casos em que é viável a estrutura celular regular do controlador. Uma vez concebida e verificada a célula de base, resta a examinar apenas as falhas que podem resultar da montagem destas, o que reduz enormemente o número de casos a serem estudados.

Não existem regras que garantam as propriedades CFD de células. Mas algumas delas podem servir como guias ao projetista do circuito, a fim de que ele possa conceber células novas para os casos ainda não disponíveis. O grau de dificuldade da montagem posterior pode ser diminuido pelo planejamento adequado das unidades.

IV. CASCATEAMENTO DE CÉLULAS DE CONTROLADORES CFD

A concepção de controladores de código fortemente disjunto pode ser feita a partir de células CFD, desde que essas sejam montadas de forma a preservar a propriedade CFD. Vimos que essas propriedades são definidas para:

* um conjunto ou classe de hipóteses de falhas;
* um conjunto de palavras codificadas (geralmente todas as palavras de código pertencem a um espaço de código de entrada;
* alguma hipótese de ocorrência de falhas com relação ao circuito funcional FSF e ao controlador CFD, assegurando que o objetivo TAT será atingido.

Essas propriedades devem ser definidas para um controlador concebido a partir de células CFD.

IV.A. Hipóteses de falhas

Ao realizar-se a montagem de células para compor um controlador, as falhas podem se relacionar às células e/ou às linhas usadas para interligar células. Isto é, essas falhas podem ser:

F1. falhas dentro de células;
F2. falhas afetando uma interconexão;
F3. curtos entre células;
F4. curtos entre interconexões;
F5. curtos entre células e interconexões.

As falhas possíveis que podem ocorrer dentro da célula são estudadas durante a sua concepção. A detecção dessas nas saídas da célula é assegurada a este nível e não é necessário revisá-las durante a montagem das células.

As falhas que afetam uma linha de interconexão dependem da classe de hipóteses de falhas. Sendo considerada a classe I, tem-se basicamente circuitos abertos. Estas falhas resultam em condições representáveis por "colagens", que podem ser facilmente detectadas com a aplicação de todas entradas pertencentes ao espaço de código de entrada, uma vez que estas linhas assumem os dois valores possíveis em condições normais. Portanto, devido a essa condição de colagem, uma palavra não codificada será rapidamente produzida nas saídas do controlador. Os circuitos abertos nas interconexões também podem ser vistos como transportados logicamente às entradas da próximo célula e esta condição também é estudada durante a concepção da célula.

Sendo considerada a Classe I, também os curtos entre células devem ser analisados. Esta verificação baseia-se na redundância do controlador com relação à falha resultante: se o controlador é redundante com relação ao curto, ou a falha pode ser detectada com a aplicação do espaço de código de entrada, esta não causará problemas. A maior dificuldade se refere aos curtos com relação aos quais o controlador não é redundante somente quando são aplicadas palavras não codificadas - assim eles não são detectados durante a operação normal do bloco funcional, e a sua possibilidade de ocorrência deve ser eliminada. Isto será visto mais tarde.

A detecção de curtos entre interconexões pode ser assegurada se cada par de linhas internas é ativado com os diferentes valores possíveis, assumindo a tecnologia NMOS. Particularizando esta situação para a classe I, e considerando somente os casos nos quais os curtos ocorrem entre linhas do mesmo nível (na estrutura em árvore), a detecção é assegurada se cada par de linhas internas vizinhas é ativada com os valores 01 ou 10. Outras situações como curtos envolvendo linhas de níveis diferentes na árvore, ou se o circuito não recebe um espaço de código de entrada completo, devem ser estudados como casos particulares.

No caso de curtos entre células e interconexões, nós consideramos linhas internas às células e não linhas conduzindo sinais de entrada e saída, uma vez que essas já haviam

sido consideradas no caso precedente. Se com a aplicação das palavras do espaço codificado de entrada ao circuito estas linhas recebem valores diferentes, esta falha será detectada, em geral. O mesmo problema de não-detectabilidade apesar de não ser redundante apontado no caso de curtos envolvendo linhas de células diferentes, também pode ocorrer no caso presente.

A situação ilustrada na figura 1 é a de um curto entre saídas intermediárias de um controlador de paridade par, ambos assumindo valores idênticos em operação normal, o que impede a detecção da falha. Tal curto impede o controlador de ser CFD. O problema pode ser evitado com a modificação do circuito de base ou com uma concepção cuidadosa (implementação física).

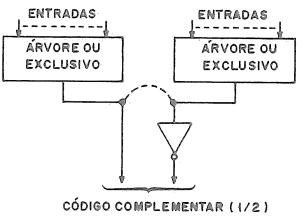

Figura 1: Curto-circuito não detectável em controlador de paridade

Outros exemplos serão dados com base em controladores "double-rail" (de código complementar). O circuito lógico /CAR 68/ e a versão elétrica correspondente, com número reduzido de transistores /NIC 84/, são mostrados pela figura 2. Se for feita a montagem de células "double-rail" cuja topologia corresponda ao da representação elétrica da figura 3, há o risco de ocorrer um curto entre o ponto P e a saída intermediária f_2, mesmo se separadamente estas células são CFD. Lembramos que o espaço de entrada do código double-rail se compõe de pares complementares, dois por célula (p.ex. X_1 e X_2, que podem assumir valores em 4 combinações possíveis). A falha assinalada não é detectável pelas entradas de código, e a concepção da célula deverá assegurar que o curto não será fisicamente possível.

IV.B. Palavras codificadas de entrada

Em geral, todas as palavras de código são necessárias para testar todas as falhas que podem ocorrer na célula CFD. Mas este pressuposto não implica que todas as palavras de código devam ser aplicadas ao controlador construído de células independentes, a fim de assegurar a detecção de todas as falhas passíveis de ocorrer.

Na seção precedente nós verificamos que há basicamente cinco grupos de falhas. Cada um destes tipos de falhas é testado por um conjunto de palavras de código, segundo descrição a seguir:

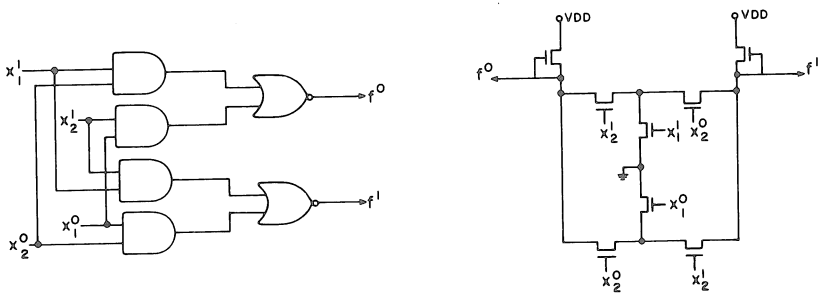

Figura 2: Controlador double-rail: circuito lógico e elétrico

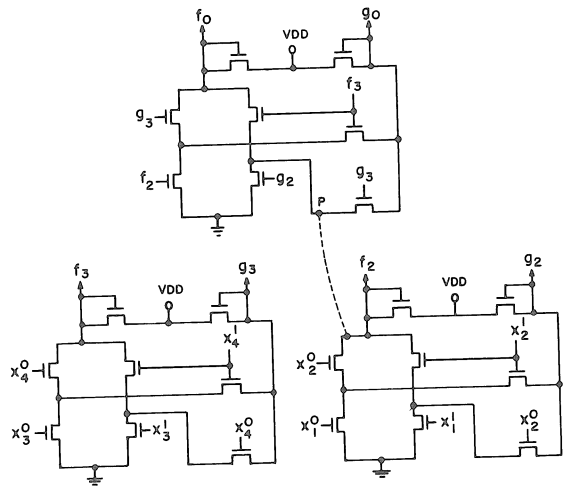

Figura 3: Curto não detectável em controlador celular double-rail

* as falhas detectáveis dentro das células são testadas com a aplicação do conjunto de palavras de código de entrada da célula;
* as falhas afetando uma interconexão são testadas pela aplicação dos dois valores lógicos diversos a cada uma destas linhas;
* os curtos entre células são testados com os valores de entrada do controlador que forçam uma das regiões afetadas a induzir um erro nas saídas da célula respectiva. Sendo esta condição atingida apenas com a aplicação de entradas não codificadas, o curto deve ser evitado por modificações topológicas;
* os curtos entre interconexões são testados com a aplicação das diferentes combinações de entrada a cada par dessas linhas (01 ou 10);
* os curtos entre célula e interconexão são testados à semelhança dos curtos entre células.

Assim, a fim de testar todos os tipos de falhas mencionadas, precisaremos, como palavras de código de entrada, o conjunto composto por aquelas descritas em todos os itens acima, que se constitui em um subconjunto do espaço de código de entrada (esse subconjunto e o espaço de código de entrada podem ser iguais ou não).

IV.C. Hipóteses de ocorrência de falhas

Faz-se necessário também considerar uma hipótese de falhas para o sistema - circuito funcional e controlador. A hipótese usual, com a qual pode-se atingir o objetivo TAT usando um sistema composto por circuito FSF e controlador CFD, prevê a ocorrência de falhas ou no circuito funcional ou no controlador, mas não em ambos em um mesmo intervalo de tempo. Isto nos garante que as situações de falha interna ao controlador são avaliadas independentemente das de erro em suas entradas. Ainda, concernente ao controlador, teremos apenas uma falha interna e outra não ocorre antes que todo o espaço de código de entrada seja aplicado. Esta hipótese está enunciada sob o nome de H2, em /JAN 83/.

Em certas proposições celulares, hipóteses menos restritivas podem ser consideradas. Estas possibilidades, entretanto, devem ser analisadas com referência a casos particulares de controladores e suas estruturas internas.

V. Procedimentos para a concepção e montagem de células

Regras para a concepção de células de controladores podem ser muito restritivas e não necessárias para todos os tipos de controladores. Mas elas podem auxiliar no projeto de novas células para diferentes códigos ou com outra forma e dimensões melhor adaptadas para aplicações específicas. A concepção ótima de uma célula pode facilitar o processo de montagem. Se as restrições não são dadas explicitamente com o projeto da célula, o usuário de uma biblioteca CFD pode necessitar de tempo e esforço não negligenciáveis para testar todas as falhas possíveis introduzidas pela reunião destas células e

assegurar a propriedade CFD do controlador resultante.

As regras apresentadas a seguir referem-se à topologia das células e interconexões e têm como maior objetivo evitar a ocorrência de falhas detectáveis unicamente pelas entradas não codificadas, causadas por uma dentre os três tipos possíveis de curtos descritos na seção IV.A.

A classe I de hipóteses de falhas não inclui curtos entre duas linhas de polisilício. Considera-se que tal defeito pode ocorrer apenas durante o processo de fabricação /COU 81/. Então, pode-se usar esta característica a fim de reduzir os defeitos possíveis - esta é a origem da regra R1.

Regra 1: Todas as interconexões entre células são efetuadas com linhas de polisilício. Essas interconexões aqui referidas são os sinais de entrada e saída de cada célula e não incluem linhas de alimentação.

A montagem de células CFD efetuada respeitando-se a regra R1, elimina as possibilidades de falhas envolvendo os curtos entre linhas de interconexão (ítens F4 e F5 da seção IV-A).

A possibilidade de curto-circuito entre duas linhas internas de células diferentes causando falhas não detectáveis pelo código de entrada (mas com relação às quais o circuito não é redundante) pode ser eliminada por modificações na topologia da célula, como sugerido a seguir.

Regra 2: As regiões limítrofes de cada célula que são concebidas em difusão devem corresponder a linhas de alimentação, V_{SS} OU V_{DD}. As linhas de metalização localizadas próximo aos limites da célula devem ser isoladas pela inserção de uma linha de alimentação em metal entre essas outras linhas e o limite da célula, se observa-se que um curto poderia ocorrer com uma metalização de outra célula que não seja linha de alimentação (ver figura 4).

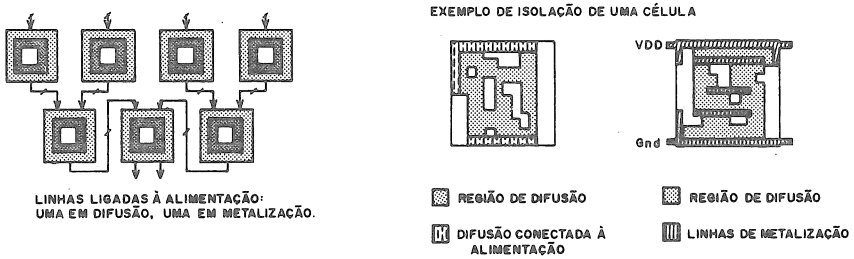

Figura 4: Restrições de isolação (regra 2)

A montagem de células CFD cujo projeto respeita a regra 2, interconectadas de acordo com a regra 1, e sendo assegurado que cada célula recebe seu espaço de código de entrada resulta um circuito controlador CFD, com relação à Classe I de hipóteses de falhas (sendo excetuados destas hipóteses os cortes nas linhas de alimentação).

O uso das regras 1 e 2 elimina tipos inaceitáveis de curtos descritos pelos ítens F_3, F_4 e F_5 (da seção IV.A), sendo considerada a classe I. Uma vez que os defeitos do tipo F_1 e F_2 são cobertos pelo uso de células CFD, o controlador completo é CFD.

A regra 2 é excessivamente restrita para alguns casos, mas ela pode ser particularizada para os diferentes códigos e estruturas de arranjo celular. Assim, para bordas de células situadas uma em frente à outra, apenas uma delas precisa respeitar a regra 2. Cumpre observar, entretanto, a associação implícita, neste caso, com restrições de lay-out - elas não podem ser, uma vez concebidas, associadas de qualquer maneira. As consequências sobre as propriedades CFD do circuito que resulta de operações de montagem não pré-definidas executadas com a célula - como rotações, translações, simetrias, etc... - devem ser analisadas previamente.

A restrição nas hipóteses de falhas mencionada na regra 2, pode ser eliminada se a regra 3 também for considerada.

Regra 3: Cada nível da estrutura em árvore deve ser alimentada por uma de suas extremidades, todas as linhas de alimentação do mesmo tipo tendo sua origem no mesmo lado. As linhas de alimentação dos diversos níveis devem ser separadas por outra de tipo diferente.

O uso da regra 3 resultará em uma organização esquemática semelhante a da figura 5. Isto significa que uma organização como a da figura 6 não é admitida. A sequência de defeitos ilustrada por $\langle f_1, f_2, f_3 \rangle$ resultará em um erro não detectável (mas não redundante) nas saídas. Logo, precisa ser eliminado.

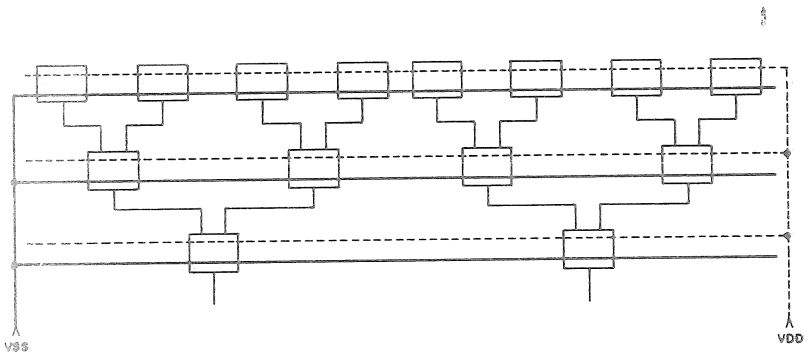

Figura 5: Linhas de alimentação organizadas de acordo com a regra 3

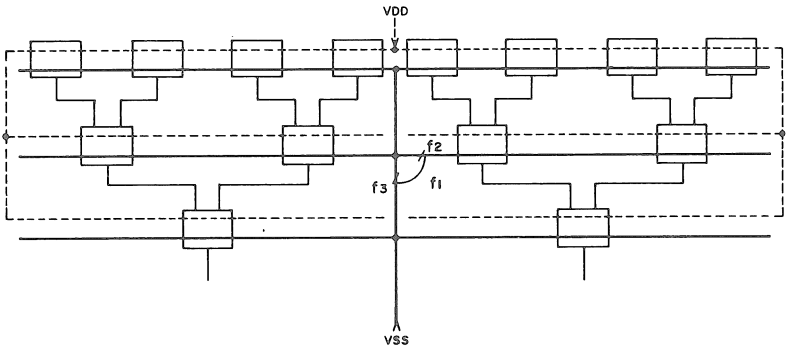

Figura 6: Sequência de falhas perigosas em linhas de alimentação

Uma montagem de células cuja organização e concepção respeita as regras R2 e R3, e cujas interconexões são feitas de acordo com a regra 1, assegurando que cada célula recebe seu espaço de código de entrada, resulta em um controlador CFD com relação à Classe I de hipóteses de falhas.

Conforme foi explicado no início, as regras aqui apresentadas são suficientes mas não necessárias. Outras menos estritas podem ser dadas, referindo-se a casos específicos de controladores. Elas encontram-se enunciadas e ilustradas em /JAN 85a/.

VI. CONCLUSÃO

Neste artigo, os controladores CFD são usados como componentes em sistemas autotestáveis - esses sistemas atingem o objetivo TAT, sob determinadas hipóteses de falhas.

Os principais problemas relacionados à concepção desses controladores, no que se refere ao caso de uma célula e à montagem da célula resultante, são discutidos. São dadas normas gerais para o projeto de uma célula, a fim de obter elementos convenientes à montagem, que possam compor uma biblioteca de células de controlador. Assim, o projeto de novos controladores pode ser facilmente obtido com o auxílio de ferramentas de PAC associadas.

REFERÊNCIAS

/AND 71/ ANDERSON, D. Design of self-checking networks using coding techniques. Univ. de Illinois, Urbana, Setembro 1971. 133p. (Relatório R527)

/CAR 68/ CARTER, W. & SCHNEIDER, P. Design of dinamically checked computers. Inf. Processing 68. Amsterdam, North Holland, 1969. v.2., p.878-83.

/COU 81/ COURTOIS, B. Failure mechanisms, fault hypotheses and analytical testing in LSI NMOS (HMOS) circuits" VLSI 81, Univ. de Edinburgh, Academic Press, 1981.

/COU 82/ COURTOIS, B. Analytical testing of regular circuits. In: IIº SIMPÓSIO BRASILEIRO DE MICROELETRÔNICA, São Paulo, 27-29 de julho de 1982. Anais. São Paulo, USP, 1982. (v.1). p.32-47.

/GAL 80/ GALIAY, J.; CROUZET, Y. & VERGNIAULT, M. Physical versus logical fault models MOS LSI circuits. IEEE Trans. on Computers, 29(6):527-31, Junho de 1980.

/JAN 83/ JANSCH, I. & COURTOIS, B. On the design of checkers based on analytical fault hypotheses. In: IIIº SIMPÓSIO BRASILEIRO DE MICROELETRÔNICA, São Paulo, 25-27 de julho de 1983. Anais. São Paulo, USP, 1983. (v.1, 1ª parte). p.41-56.

/JAN 85a/ JANSCH, I. Conception de contrôleurs autotestables pour des hypothèses de pannes analytiques. INPG, Grenoble, janeiro de 1985. (Tese de Doutor-Engenheiro).

/JAN 85b/ JANSCH, I. Circuitos autotestáveis: opção de projeto de circuitos visando o teste implícito ou concorrente. (proposto ao V Congresso da Sociedade Brasileira de Computação/SEMISH).

/NIC 84/ NICOLAIDIS, M.; JANSCH, I. & COURTOIS, B. Strongly code disjoint checkers. THE FOURTEENTH INTERNATIONAL CONFERENCE ON FAULT-TOLERANT COMPUTING. Kissimmee, 19-21 de junho de 1984. Anais. New York, IEEE, 1984. p.16-21.

/SMI 78/ SMITH, J. & METZE, G. Strongly fault secure logic networks. IEEE Trans. on Computers, 27(6):491-9, Junho de 1978.