ASPECTOS DE TOLERÂNCIA A FALHAS DO SISTEMA DE COMPUTAÇÃO DO SATÉLITE DE SENSORIAMENTO REMOTO DA MECB

Autor: Alderico R. de Paula Jr. (1)

RESUMO

Este trabalho apresenta o sistema de computação, ora em desenvolvimento no Instituto Nacional de Atividades Espaciais (INPE), a ser utilizado para supervisão e controle do Satélite de Sensoriamento Remoto (SSR) do Programa Espacial Completo Brasileiro (MECB).

O sistema de computação é constituído de dois computadores com redundância interna que se comunicam entre si através de um barramento serial. As técnicas de tolerância a falhas que estão sendo projetadas para o sistema de computação foram organizadas em três fases: detecção de erros, diagnose e recuperação. Algumas destas técnicas são implementadas em hardware, outras em software, contudo a maioria delas utiliza uma combinação de hardware e software.

ABSTRACT

This paper presents the computer system that has been developed at the Instituto Nacional de Atividades Espaciais (INPE) to supervise and control the Remote Sensing Satellite (SSR) of the Brazilian Complete Spatial Mission (MECB).

The computer system is composed of two computers having internal redundancy that are connected through a serial bus. The fault tolerant techniques that have been designed are organized in three phases: error detection, diagnosis and recovery. Some of these techniques are implemented in hardware, others in software, however most of them uses a combination of hardware and software.

(1) PhD em Ciência da Computação - UCLA 1982; Engenheiro de Desenvolvimento Tecnológico Sênior no Instituto Nacional de Atividades Espaciais (INPE).

Áreas de interesse: Arquitetura de Computadores, Sistemas de Computação Tolerantes a Falhas, Redes de Computadores.

Endereço: Caixa Postal 515
12201-970 São José dos Campos, SP

se tornam necessárias à medida que as características de projeto vão sendo delineadas de forma mais precisa. Com os resultados destas novas avaliações torna-se possível realizar revisões formais de projeto com base na verificação do atendimento aos requisitos especificados.

Como comentário final, é importante ressaltar que as estimativas obtidas dizem respeito a falhas hardware, e, na verdade, as falhas software e operacionais também podem conduzir a situações de sobrecarga. Em função do tipo de sistema, cada tipo de falha pode ter maior ou menor influência sobre o comportamento operacional do mesmo, dependendo, é claro, do grau de complexidade do sistema, do processo de projeto/desenvolvimento, das características particulares de funcionamento, etc. Apesar desta influência, estes dois tipos de falha não são abordados nesta análise e, consequentemente, não entram no cômputo das estimativas apresentadas, uma vez que não existem padrões definidos que permitam estimar as taxas de falha software e operacional, enquanto o sistema se encontra em sua fase de concepção/desenvolvimento.

Referências

[1] CCITT, Blue Book Vol. II.3. Geneva, 1989.

[2] A.S.Morais, M.P.Cavaletti & V.A.Valenzuela Diaz," CLAD - Concentrador de Linha de Assinante Distribuído". *Anais X SBT/V SBMO*, Brasília - DF, Julho de 92, p.55-60.

[3] M.Claudia et al.," Arquitetura do Protótipo do CLAD". *Relatório Técnico* - CPqD-TELEBRÁS, Março de 92, 11 p.

[4] 0.I. Szentsi, "Reliability of Optical Fibers, Cables and Splices". *IEEE Journal on Selec. Areas in Communic.*, Vol. SAC-4, No.9, Dec. 1986, pp.1502-1508.

[5] MIL-HDBK-217 E *Military Standardization Handbook: Reliability Prediction of Electronic Equipment*, 1986.

[6] *Electronic Switching Systems: Operating and Working Standards.* Vol.1, Telecommunications-France.

1) INTRODUÇÃO

O Satélite de Sensoriamento Remoto (SSR) é o primeiro da segunda série de satélites da Missão Espacial Completa Brasileira (MECB). O SSR tem como função principal a aquisição de imagem de média resolução da Terra, nas bandas espectrais do visível e do infravermelho próximo. A cobertura total do território Brasileiro é realizada a cada quatro dias.

Devido à alta repetição da aquisição dos dados de uma mesma área, o SSR terá aplicações no estudo de fenômenos dinâmicos, tais como o estudo da evolução das plantações visando a previsão de safras, o estudo do desmatamento de florestas, queimadas, enchentes, estiagem e, na área de oceanografia, o estudo das correntes marinhas próximo a costa brasileira.

As principais características do satélite são:

Órbita: Heliossíncrona com altitude de 640 Km, inclinação de 98 graus, excentricidade próxima a zero e período de aproximadamente 100 min.

Sistema de controle: Estabilizado nos três eixos.

Massa: 170 Kg.

Potência elétrica: 140 W (após 2 anos)

Resolução da câmera CCD: 214 m

Vida Útil: 2 anos

Confiabilidade: 0,6 (2 anos)

O satélite SSR é constituído dos seguintes subsistemas:

a) **Transponder de Serviço** - tem a função de receber e demodular os sinais provenientes das estações terrenas, gerar os pulsos de comandos diretos e as mensagens de telecomando para o Computador de Supervisão de Bordo. Adicionalmente, o transponder modula e transmite as mensagens de telemetria fornecidas por este computador.

b) **Computador de Supervisão de Bordo** - tem a função de adquirir os sinais de telemetria dos diversos subsistemas, processá-los, formatá-los em mensagens e enviá-las para o Transponder de Serviço. Tem ainda a função de receber as mensagens de telecomando, decodificá-las e gerar os comandos para os diversos subsistemas.

c) **Controle de Atitude e Órbita** - é constituído do Computador de Controle de Atitude, dos sensores de

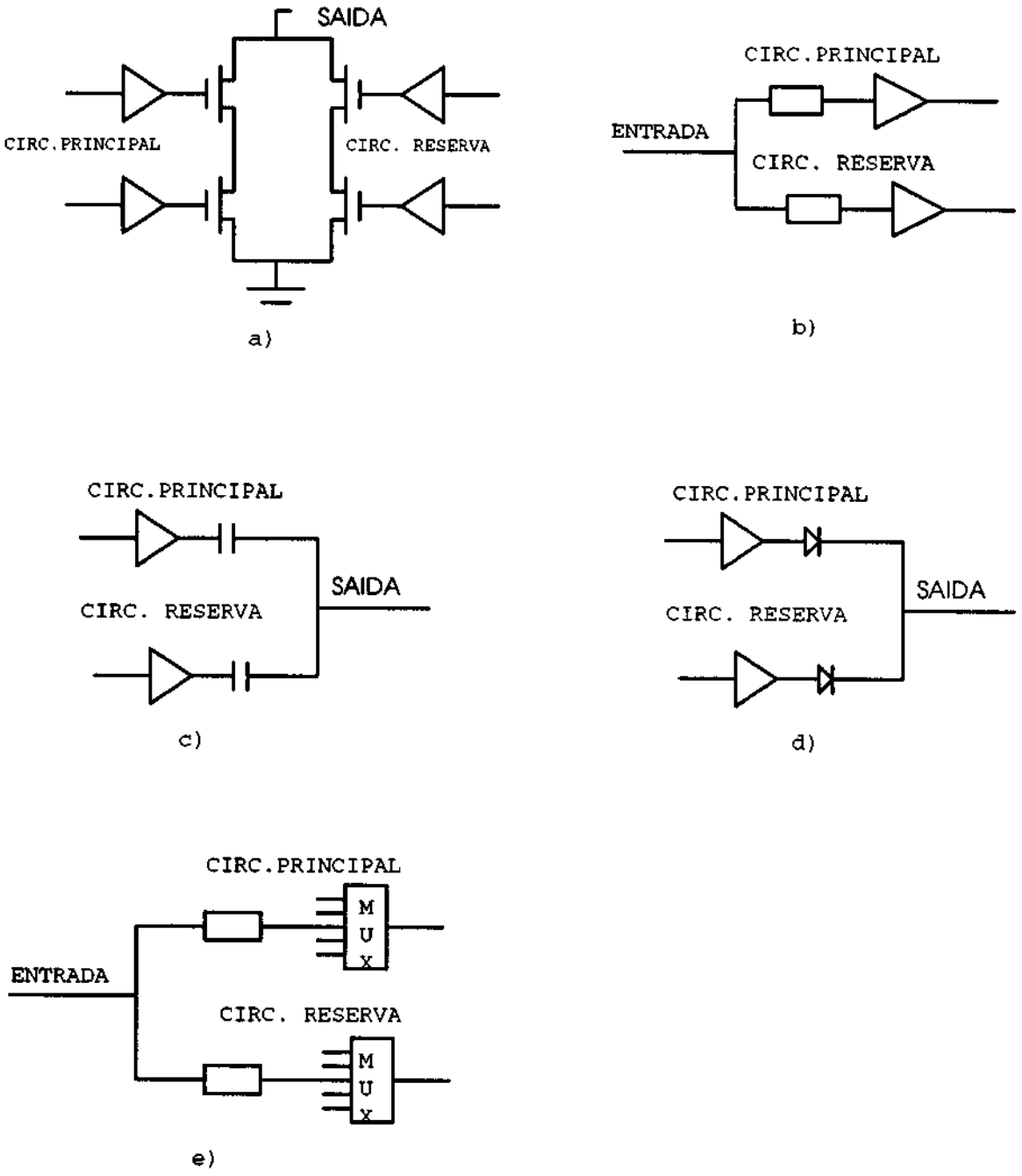

Fig 3 Circuitos de Entrada e Saida

Cada circuito do Módulo de Telecomando e Telemetria é constituído de dois canais de recepção de mensagens de telecomando. Cada canal ativo é isolado do canal reserva através de dois resistores como é mostrado na Figura 3-b. Adicionalmente, esta unidade contém o circuito para gerar as mensagens de telemetria. O canal ativo é isolado do reserva por dois capacitores como mostrado na Figura 3-c.

O Módulo de Pulsos Liga/Desliga contém os circuitos para gerar até 16 pulsos utilizados para ligar ou desligar equipamentos a bordo. Os canais ativos são isolados dos canais reservas através de dois diodos como mostrado na Figura 3-d.

Cada Módulo de Aquisição de Dados tem a capacidade de adquirir até 60 sinais de telemetria. Os sinais analógicos são convertidos para palavras digitais. Os canais ativos são isolados dos canais reservas através de resistores como mostrado na Figura 4-e.

2.2) COMPUTADOR DE CONTROLE DE ATITUDE E ÓRBITA (CCA)

O CCA tem a função de adquirir os sinais dos diversos sensores de atitude, processá-los segundo as leis de controle pré-estabelecidas e ativar os atuadores para realizarem as correções necessárias na atitude do satélite. Além desta função o CCA realiza, baseado nos comandos recebidos do Centro de Controle, as manobras necessárias para corrigir a órbita do satélite.

A arquitetura do CCA é bastante similar ao do CSB. Apenas alguns módulos de entrada e saída do CSB são substituídos por outros módulos. O CCA é formado dos seguintes módulos:

- Um Módulo de Potência e Chaveamento (MPC);
- Dois Módulos Centrais de Processamento (UCP);
- Dois Módulos de Memória Principal (MMP);
- Um Módulo de Pulsos Liga/Desliga (MPL);
- Um Módulo de Entrada e Saída de Dados Seriais (MES);
- Um Módulo de Controle dos Micropropulsores (MCM);
- Um Módulo de Emergência (MEM).

O Módulo de Entrada e Saída de Dados Seriais envia os comandos seriais para os atuadores e recebe as telemetrias seriais dos sensores de atitude. Os circuitos de entrada são similares aos da Figura 3-a, e os de saída similares aos da Figura 3-b.

O Módulo de Controle dos Micropropulsores gera os pulsos para controlar o tempo de atuação dos micropropulsores. O circuito de saída é similar ao da Figura 3-a.

O Módulo de Emergência, quando ativado, aponta os painéis solares do satélite em direção ao sol. Esta unidade só é ativada quando a unidade principal for desligada devido a um

D) Módulo de Telemetria e Telecomando

Os telecomandos provenientes do Segmento Solo são recebidos através de dois canais independentes. Estes canais podem ser testados pela rotina de recepção de telecomando verificando a palavra de "checksum" da mensagem.

O circuito de transmissão de telemetria armazena, em um registro de deslocamento, a última palavra de telemetria transmitida que é lida pela rotina de transmissão de telemetria. Esta rotina compara a palavra lida com a transmitida. Adicionalmente, as mensagens enviadas para o segmento solo recebem uma palavra de "checksum" que é verificada em solo.

E) Módulo de Entrada e Saída Serial

Os diversos comandos seriais transmitidos para os diversos subsistemas do satélite são também lidos pelo circuito de entrada serial, e a rotina de entrada e saída compara as palavras lidas com as transmitidas.

3.1.3) Detecção de Erro a Nível de Programa Aplicativo

Os programas aplicativos estão ainda em fase de desenvolvimento, contudo alguns mecanismos de detecção de erro que deverão ser usados são:

a) Verificação da consistência dos dados calculados ou lidos dos subsistemas do satélite.

b) Verificação da palavra de "checksum" das mensagens recebidas e sua origem.

c) Verificação de tempo de recebimento das mensagens.

d) Execução do Programa de Testes.

O Programa de Testes está sendo projetado para ser executado periodicamente. Sua principal função será testar a memória principal e a UCP.

O teste da UCP consiste em executar uma rotina que exercita, ao máximo, os circuitos da UCP, principalmente o microprocessador. Esta rotina deverá ser executada a cada 18 horas.

A primeira parte do teste da RAM consiste em ler todos os endereços da memória a cada quatro horas. Caso exista algum erro gerado por algum fenômeno transitório, ele será corrigido automaticamente pelo circuito EDC. Ao se detectar um erro simples o Programa de Teste lê novamente o endereço da memória onde foi localizado o erro. Caso o erro se repita este é considerado permanente, e o programa de diagnose gera um relato de erro.

A segunda parte do teste da RAM consiste em escrever e em seguida ler palavras que exercitam todos os seu bits em todas as posições da RAM. Esta rotina tem a função de detectar erros permanentes na RAM e deve ser executada a cada 18 horas.

As palavras de "checksum" da memória PROM também são verificadas a cada 18 horas através do Programa de Testes.

3.2) Diagnose

A fase de diagnose tem a função de localizar o defeito que ocasionou o erro e avaliar os danos causados na estrutura de dados. Muitas vezes os mecanismos de detecção de erro localizam o defeito, como é o caso do erro duplo na memória que armazena em um registro o endereço da RAM onde ocorreu o erro.

Os erros podem ter sido causados por fenômenos físicos transitórios como, por exemplo, radiações cósmicas de alta energia, ou por defeitos nos circuitos eletrônicos, ou ainda por defeito no projeto do hardware ou software do computador. Devido à complexidade dos circuitos e à diversidade dos possíveis defeitos, o Programa de Diagnose deverá se limitar somente a algumas classes de erros.

O Programa de Diagnose é constituído por um conjunto de rotinas, uma para cada classe de erro. Algumas destas rotinas são chamadas através de interrupção, como por exemplo, as seguintes:

- Erro duplo na memória,
- Tentativa de escrita em área protegida,
- Cão-de-Guarda.

Outras rotinas são chamadas pelas rotinas de entrada e saída do Sistema Operacional quando verificam que o dado ou comando transmitido é diferente do gerado. Estas rotinas já indicam o circuito com defeito.

As rotinas do Sistema Operacional e os programas aplicativos, quando detectam um parâmetro fora do limite, não informam as possíveis causas do erro ao Programa de Diagnose. Nestes casos as rotinas de diagnose ativam o Programa de Testes visando localizar um possível defeito no hardware.

Dependendo do procedimento pré-estabelecido para cada classe de erro, o Programa de Diagnose realiza uma das seguintes ações:

a) Gera um relato de erro e retorna à operação normal;

b) Gera um relato de erro e repete a última operação;

c) Escreve um relato de erro na área da RAM que não é zerada pelo Programa de Iniciação. Em seguida, envia um relato de erro para o outro computador de bordo e deixa de zerar o Cão-de-Guarda. Após três BTs no máximo o Cão-de-Guarda

gera um pulso que leva o sistema para a fase de iniciação;

d) Envia um relato de erro para o outro computador de bordo, ativa o biestável de auto teste e deixa de zerar o Cão-de-Guarda. Após três BTs o Cão-de-Guarda ativa o biestável de sinalização de erro o que provoca o chaveamento para a unidade reserva ou a ativação do Módulo de Emergência.

3.3) RECUPERAÇÃO

A rotina de recuperação é acionada logo após a conclusão da fase de iniciação, quando o sistema entra na fase operacional. A principal função desta rotina é levar o sistema para a fase operacional correta, de forma autônoma, baseada nas informações armazenadas no outro computador de bordo e na sua própria memória, sem trocar mensagens com o Centro de Controle de Satélite.

Durante a operação normal, cada computador de bordo envia para o outro uma mensagem de status contendo os principais parâmetros operacionais. Nos casos em que o Programa de Diagnose decide reiniciar a unidade ativa, ou comutar para a unidade reserva, esta envia uma mensagem para o outro computador contendo o relato do erro. Este relato é também armazenado na sua própria memória, na área que não é zerada pelo Programa de Iniciação.

O Cão-de-Guarda, ao zerar a unidade, ativa o biestável de autoteste. Este biestável não é zerado pelo Programa de Iniciação e é utilizado para indicar ao Programa de Recuperação se a unidade foi ativada devido a energização do sistema ou devido a atuação do Cão-de Guarda.

A Rotina de Recuperação da unidade principal difere ligeiramente da rotina da unidade reserva.

Na unidade principal, a rotina de recuperação ao ser ativada verifica inicialmente o estado do biestável de autoteste. Caso ele não esteja zerado, indicando que o programa de iniciação foi ativado pela energização do sistema, a rotina de recuperação leva o sistema para operação normal na fase inicial.

Estando o biestável de autoteste ativado, a rotina de recuperação lê os relatos de erro da área não zerada da memória. Com base no número e tipo de erros já ocorridos, o Programa de Recuperação decide retornar a fase operacional antes da atuação do Cão-de-Guarda ou comutar para a unidade reserva . Para retornar a fase operacional correta, a rotina de recuperação envia para o outro computador uma mensagem solicitando a última palavra de status enviada antes de ir para a fase de iniciação.

Caso os dados recebidos estejam consistentes, a rotina de recuperação atualiza os parâmetros operacionais e retorna o sistema para a operação normal. Quando for detectada inconsistência nos dados recebidos, ou quando não for possível comunicar com o outro computador de bordo, o Programa de Recuperação leva o sistema para a operações normal na fase inicial. Após contacto com o Centro de Controle, este envia os comandos operacionais para levar o sistema para fase operacional correta.

4) CONCLUSÕES

Atualmente os protótipos de laboratório do CSB e do CCA estão sendo montados e testados. O Sistema Operacional para estes sistemas será uma adaptação daquele desenvolvido para os satélites da série Coleta de Dados da MECB, e está atualmente na fase do projeto detalhado. Estima-se que, no prazo de um ano, os protótipos juntamente com o sistema operacional estejam testados e validados.

Os programas aplicativos deverão ser validados em computadores pessoais antes de serem implantados nos protótipos dos computadores de bordo. A fase final dos testes integrados deverá durar pelo menos um ano, pois, como o sistema de computação está sendo projetado para executar tarefas críticas, tais como mudanças de órbitas, um defeito no software de bordo poderá causar a perda do satélite.

5) BIBLIOGRAFIA

(1) Santana, C. E.; Kono, J., "SSR Spacecraft Specification" MECB-SSR-A-ETC-1001, abril de 1988.

(2) Kono, J.; De Paula Jr., A. R., "On-Board Computer Specification", MECB-SSR-A-ETC-1029, abril de 1992.