# ARQUITETURA DE HARDWARE DO COMPUTADOR DE BORDO PARA O SATÉLITE UNIVERSITÁRIO ITASAT E CONFIABILIDADE

**Edson Vinci, edsonvinci@gmail.com**
**Osamu Saotome, osaotome@ita.br**
ITA – Instituto Tecnológico de Aeronáutica. Pça. Mal. Eduardo Gomes, 50, Vila das Acácias, CEP 12.228-900, São José dos Campos, SP, Brasil.

***Resumo.*** *Este artigo apresenta um estudo de caso que visa o desenvolvimento de uma arquitetura de hardware para o computador de bordo do satélite universitário ITASAT, baseado em arquitetura tolerante a falha e resultados de cálculos de confiabilidade. O computador de bordo de um satélite, inserido no subsistema de supervisão de bordo, tem funções de recepção, processamento e distribuição de comandos para os subsistemas e carga útil do satélite; e de aquisição, formatação, armazenamento e transmissão de telemetrias dos subsistemas e carga útil. Os principais requisitos de um computador de bordo é a alta confiabilidade, a capacidade de processamento em tempo real, a resistência à radiação, e minimização de potência, volume e massa. O aumento de confiabilidade pode ser alcançado pela técnica de tolerância a falhas, que tem como base a adição de redundâncias ao sistema. As redundâncias podem estar presentes no hardware, software, tempo ou informação. Neste estudo de caso, são considerados técnicas de implementação de redundância em hardware. Uma arquitetura sem redundância, na sua concepção simplificada, foi projetada e sua confiabilidade calculada para uma missão de vinte e quatro meses. A partir dos resultados, são propostas mais duas arquiteturas redundantes, tolerantes a falha, com suas respectivas confiabilidades calculadas para o mesmo período de missão. Os resultados finais demonstram a evolução positiva da confiabilidade por intermédio das arquiteturas tolerantes a falha. Isto traz sustentação na escolha mais eficaz da arquitetura do computador de bordo para o satélite universitário ITASAT, podendo ser estendido a outras aplicações espaciais.*

***Palavras-chave****: Satélite, Computador de bordo, Tolerância a falha, Redundância de hardware, Confiabilidade.*

## 1. INTRODUÇÃO

O sistema brasileiro de coleta de dados via satélite é constituído pelos satélites SCD1, SCD2 e CBERS2, no segmento espacial, pelas diversas redes de plataformas de coleta de dados espalhadas pelo território nacional, pelas estações de recepção de Cuiabá e de Alcântara, e pelo Centro de Missão de Coleta de Dados em Cachoeira Paulista (Plataformas, 2009). No segmento espacial, o SCD-1 foi o primeiro satélite projetado, fabricado, testado e operado pelo Brasil, lançado em 9 de fevereiro de 1993 (SCD-1, 2009). Com o objetivo de atualização do SCD-1, a Agência Espacial Brasileira – AEB, o Instituto Nacional de Pesquisas Espaciais – INPE e o Instituto Tecnológico de Aeronáutica – ITA constituíram uma parceria dando início ao projeto do satélite universitário ITASAT (ITASAT, 2009).

Um satélite, na visão de subsistemas, pode ser dividido em: estrutura, suprimento de energia, controle de órbita e atitude, propulsão, comunicação e serviço, gestão de bordo, controle térmico e carga útil (Satélite, 2009). O computador de bordo, presente no subsistema de Gestão de Bordo, é um dos pontos vitais de um satélite. Ele possui funções como: recepção, processamento e distribuição de comandos para os subsistemas e para a carga útil; e aquisição, formatação, armazenamento e transmissão de telemetrias dos subsistemas e da carga útil. Os principais requisitos de um computador de bordo é a alta confiabilidade, a capacidade de processamento em tempo real, a resistência a radiação, o consumo baixo de potência, e fisicamente, massa e volume reduzidos.

Durante o ciclo de vida do satélite, é atribuído um valor de confiabilidade a cada subsistema. Este valor não pode ser inferior ao estipulado durante o período de vida útil da missão. A confiabilidade é importante para o sucesso de missões espaciais, pelo motivo dos elevados custos numa possível manutenção. Para obter um equipamento com alta confiabilidade, basicamente pode ser investido em dois quesitos: em componente com alta confiabilidade individual ou na técnica de tolerância a falha, que consiste na adição de redundância ao sistema. As redundâncias podem estar presentes no sistema de hardware, software, tempo ou informação. Decisões em quando e como aplicar redundância em hardware depende da criticidade do sistema ou função e sempre deve estar equilibrado com a necessidade de minimizar complexidade e custo. É freqüentemente possível melhorar a confiabilidade usando elementos de circuitos redundantes, devido ao baixo custo da maioria dos dispositivos modernos (O'Connor, 1991).

Pelas razões apresentadas, este artigo propõe três tipos de arquitetura de hardware, sustentado-as por cálculos de confiabilidade. Os componentes das arquiteturas em questão tiveram suas taxas de falhas estimadas pelo método da contagem de partes (MIL-HDBK-217F, 1991), através de uma ferramenta dedicada para tal finalidade (Relex, 2008). A primeira arquitetura, na topologia centralizada e numa concepção simplificada, possui um computador de bordo sem redundância. A segunda arquitetura, também na topologia centralizada, apresenta à técnica de tolerância a falha, ou seja, redundância no computador de bordo. A gerência desta redundância é executada por uma unidade denominada supervisora. A terceira e última arquitetura é uma evolução da segunda, e apresenta além do computador de bordo

redundante, a unidade supervisora também redundante, para evitar que essa unidade seja um ponto simples de falha dentro do subsistema. As arquiteturas propostas são comparadas pelas suas respectivas confiabilidade, proporcionando sustentabilidade na escolha mais adequada para o computador de bordo do satélite universitário ITASAT. Além disto, este estudo de caso pode ser um ponto base para definições de arquiteturas aplicadas em sistemas espaciais.

Este artigo está estruturado da seguinte forma: na Seção 2, são apresentados conceitos e definições de confiabilidade; na Seção 3, são revistos conceitos fundamentais de redundância de hardware e suas principais topologias; na Seção 4, são apresentadas as arquiteturas propostas juntamente com suas respectivas confiabilidades; e na Seção 5, são apresentadas as conclusões sobre os resultados obtidos.

## 2. CONFIABILIDADE

A confiabilidade é um termo que define a capacidade de um componente, um subsistema ou sistema, exercer sua função sob determinada condição, num dado intervalo de tempo (NBR 5462, 1994). A estimativa da confiabilidade de um item pode ser feita de forma direta, através da relação entre o valor da confiabilidade e o valor da função taxa instantânea de falha (Azevedo, 2008). Em resumo, a expressão geral da confiabilidade é dada na Eq. (1):

$$R(t) = exp\left[ - \int_0^t h(t)dt \right] \qquad t \geq 0 \tag{1}$$

Considerando um sistema com distribuição exponencial, a expressão pode ser reescrita na Eq. (2):

$$R(t) = \int_t^\infty \lambda . e^{-\lambda t} dt = e^{-\lambda t} \qquad t \geq 0 \tag{2}$$

Conclui, portanto, que para um a taxa de falha $\lambda$ constante, a confiabilidade de um sistema é uma curva decrescente em função do tempo, como mostra a Fig. 1.

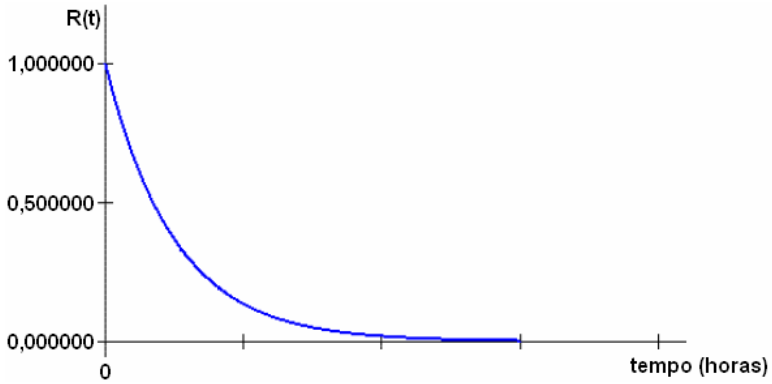


Figura 1. Curva característica da confiabilidade.

Outros termos importantes definidos dentro do contexto da confiabilidade são: a disponibilidade, que é a capacidade de um item de estar em condição de executar sua função; e a mantenabilidade, que é a capacidade de um item de ser mantido ou recolocado em condições de executar suas funções (Azevedo, 2008).

Portanto, a dependabilidade é o termo que descreve a disponibilidade e seus fatores de influência, como a confiabilidade e a mantenabilidade (NBR 5462, 1994).

## 3. REDUNDÂNCIA DE HARDWARE

A redundância de hardware tem por objetivo utilizar artefatos extras ou duplicados, que através da implementação de técnicas de tolerância a falhas, permita contornar falhas (Kozenieski, 2006) e simultaneamente aumentar a confiabilidade do sistema.

A redundância é geralmente classificada em ativa e de prontidão, ou *standby* (Azevedo, 2008). Na redundância ativa, todos os artefatos extras ou duplicados estão em operação simultânea. Na redundância *standby*, os artefatos extras ou duplicados operam um por vez. Esta última é subclassificada de acordo com a alimentação dos artefatos: *cold*, *warm* ou *hot* (Azevedo, 2008). Em *cold* os artefatos não estão energizados, em *warm* eles se encontram parcialmente energizados, e em *hot* eles estão completamente energizados.

Num hardware eletrônico, os componentes podem ser dispostos de tal forma que, na falha de qualquer um deles, uma condição de falha de todo o conjunto é estabelecida. Nesta circunstância o sistema possui redundância nula. A confiabilidade do sistema será então expressa pela Eq. (3):

$$Rs(t) = \prod_{i}^{n} Ri(t) \tag{3}$$

Quando os artefatos estão dispostos de tal forma que na presença de falha em um componente, outro componente contorna esta condição, permitindo que o sistema como todo não falhe, há, portanto, um sistema com redundância paralela ativa. A confiabilidade do sistema será então expressa pela Eq. (4):

$$Rp(t) = 1 - \prod_{i}^{n} [1 - Ri(t)] \tag{4}$$

Na redundância em *standby*, a confiabilidade pode ser determinada pelo método da árvore de eventos, o qual consiste em determinar todas as combinações de eventos potenciais que levariam o sistema a falhar. A redundância em *standby* também pode ser calculada pelos primeiros n termos da expressão de Poisson (Lafraia, 2001), dada pela Eq. (5):

$$R(t) = exp(-N\lambda t).\left(1 + N\lambda t + \frac{N^2\lambda^2 t^2}{2!} + ... + \frac{N^{(n-1)}\lambda^{(n-1)}t^{(n-1)}}{(n-1)!}\right) \tag{5}$$

onde, N é o número de unidade operando e n é o número de unidades em prontidão.

## 4. ARQUITETURA

Um satélite, na composição de subsistemas, pode ser dividido conforme Fig. 2:

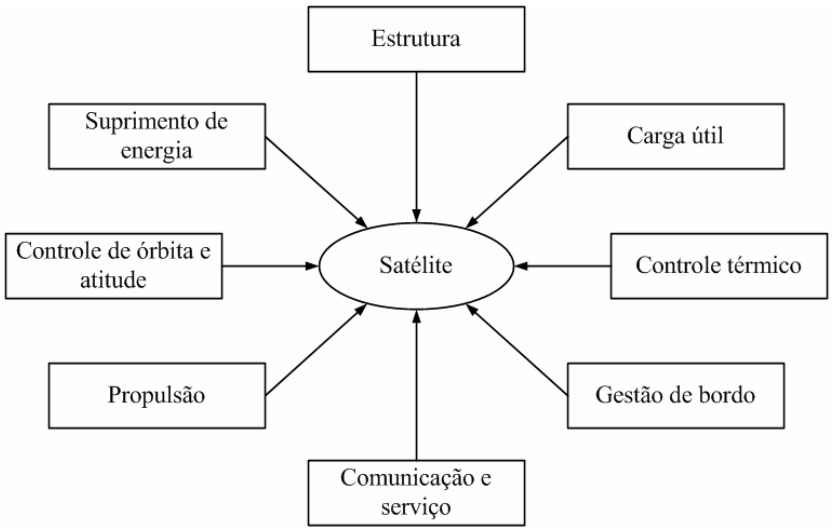


Figura 2. Subsistemas de um satélite.

Em diagramas de blocos de confiabilidade, os subsistemas podem ser representados em série, levando em consideração que, na falha de qualquer subsistema, uma condição de falha de todo o conjunto é estabelecida. Portanto, a confiabilidade do satélite pode ser calculada pela Eq. (6):

$$Confiabilidade\ do\ satélite(t) = \prod^{n} [Confiabilidade\ do\ subsistema(t)] \tag{6}$$

onde, n é o número de subsistemas.

A confiabilidade do satélite é determinada alocando um valor de confiabilidade para cada subsistema. Este valor não pode ser inferior ao estipulado durante o período de vida útil da missão.

O subsistema Gestão de Bordo possui genericamente três grupos de funções principais: controle do satélite, comunicação interna e processamento dos dados (Satélite, 2009). Neste subsistema está presente o computador de bordo, que é o responsável por essas funções vitais. Devido a sua importância, este estudo de caso aborda três propostas de computador de bordo para o satélite universitário ITASAT.

Uma arquitetura centralizada do hardware do computador de bordo pode ser especificada, na sua concepção simplificada, com os componentes descritos na Tab. 1.

Tabela 1. Lista de componentes do computador com as respectivas predições de taxas de falha.

| Part Number | Component | Failure Rate, Predicted [Failures / hour] |
|---|---|---|
| PCB | Printed circuit board | 1,10500E-08 |
| CON | Connector | 5,03304E-08 |
| ERC32 | Low-Voltage Rad-Hard 32-bit SPARC Embedded Processor | 2,08333E-06 |
| 74LV00 | Quad 2-Input NAND Gate | 1,96232E-09 |
| 74LV04 | Hex Inverter | 1,96232E-09 |
| 74LV244 | Octal Buffer/Line Driver | 3,92464E-09 |
| 74LV245 | Octal Bus Transceiver | 4,90580E-09 |
| AT49BV040B | 4 Megabit Flash Memory | 1,75068E-08 |
| K6R4008V1D | 512K x 8 Bit High-Speed CMOS Static RAM | 9,91817E-09 |
| Resistor | RES XX OHM 1/8W 1% 0805 SMD | 1,09741E-09 |
| Capacitor | Solid Tantalum Chip Surface Mount Capacitor | 2,72207E-10 |
| Capacitor | Surface Mount Capacitor | 4,04290E-09 |
| Inductor | Inductor | 1,20740E-11 |
| Oscillator | Oscillator | 1,96232E-09 |
| Power | Integrated Switching Regulators | 1,78571E-07 |
| RS-422 | 3V RS-422 DIFF DRV/RCV | 1,81550E-09 |

A Tabela 1 apresenta uma lista de componentes, da arquitetura de um computador, com as respectivas predições de taxas de falha (Relex, 2008). As taxas de falha foram estimadas utilizando o método de *Parts Count* (MIL-HDBK-217F, 1991). Em diagramas de blocos de confiabilidade, a arquitetura do computador de bordo sem redundância é representada pela Fig. 3:

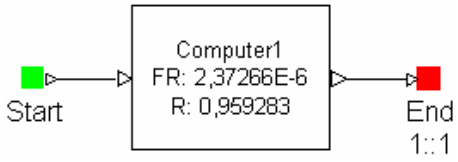


Figura 3. Diagrama em blocos do computador de bordo sem redundância.

Por intermédio da taxa de falha e vida útil de vinte e quatro meses, a confiabilidade do computador de bordo é dada por *R(24 meses) = 0,959283*, sendo o *MTTF = 421467 horas*. O valor de confiabilidade obtido, do computador de bordo sem redundância, está abaixo do valor especificado de 0,960000 (Amazonia-1, 2008).

Utilizando técnica de tolerância a falha, como a redundância de hardware, é possível avaliar o aumento de confiabilidade da arquitetura do computador de bordo. Levando em consideração que os requisitos de um satélite exigem um consumo baixo de potência, a redundância *cold standby* é mais adequada. A duplicação do computador pressupõe uma unidade de gerenciamento da redundância, ou seja, uma unidade que analise o comportamento dos computadores e direcione o comando para aquele que não apresentar falha. Uma arquitetura para esta unidade supervisora pode ser projetada, na sua concepção simplificada, com os componentes descritos na Tab. 2.

A unidade supervisora, na sua concepção, tem a função de gerenciar a redundância dos computadores em redundância *cold standby*. No entanto, para o satélite universitário ITASAT, ela poderá também assumir o comando do satélite numa condição degradada, quando ambos os computadores apresentarem falhas ao mesmo tempo.

A Tabela 2 apresenta uma lista de componentes, da arquitetura de uma unidade supervisora, com as respectivas predições de taxas de falha (Relex, 2008). As taxas de falha foram estimadas utilizando o método de *Parts Count* (MIL-HDBK-217F, 1991). Em diagramas de blocos de confiabilidade, a unidade supervisora é representada pela Fig. 4:

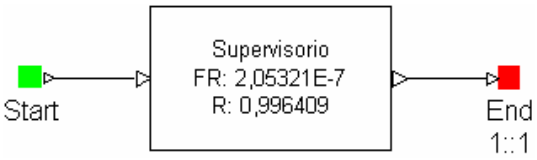


Figura 4. Diagrama em blocos da unidade supervisora.

Levando-se em consideração a taxa de falha e a vida útil de vinte e quatro meses, a confiabilidade da unidade supervisora é dada por *R(24 meses) = 0,996409*, sendo o *MTTF = 4870417 horas*.

Tabela 2. Lista de componentes da unidade supervisora com as respectivas predições de taxas de falha.

| Part Number | Component | Failure Rate, Predicted [Failures / hour] |
|---|---|---|
| PCB | Printed circuit board | 1,10500E-08 |
| CONN1 | Connector | 5,03304E-08 |
| 74HCT373 | Octal D-Type Latch | 9,81160E-10 |
| 80C32 | 8-Bit Microcontroller | 6,88903E-09 |
| AT28HC256 | High-speed Parallel EEPROM | 1,21282E-09 |
| BC327 | Small Signal Transistor (PNP) | 1,17724E-09 |
| BC337 | Small Signal Transistor (NPN) | 1,17724E-09 |
| Capacitor | Surface Mount Capacitor | 7,77481E-10 |
| Capacitor | Surface Mount Capacitor | 2,09390E-11 |
| Capacitor | Solid Tantalum Chip Surface Mount Capacitor | 1,46573E-10 |
| Oscillator | Oscillator | 9,81160E-10 |
| CY62128E | Static RAM | 1,07363E-08 |
| Inductor | Low Profile Power Inductors | 8,04900E-12 |
| LM317 | Voltage Regulator | 2,37859E-09 |
| MAX3070E | Dual Driver/Receiver | 9,81160E-10 |
| Power | Integrated Switching Regulators | 1,12360E-07 |
| Resistor | RES XX OHM 1/8W 1% 0805 SMD | 1,31689E-09 |
| UCC3946 | Watchdog Time | 9,81160E-10 |
| RS-422 | 3V RS-422 DIFF DRV/RCV | 1,81550E-09 |

A arquitetura do computador de bordo em redundância *cold standby*, contendo a unidade supervisora, é arranjada em diagramas de blocos de confiabilidade representada pela Fig. 5.

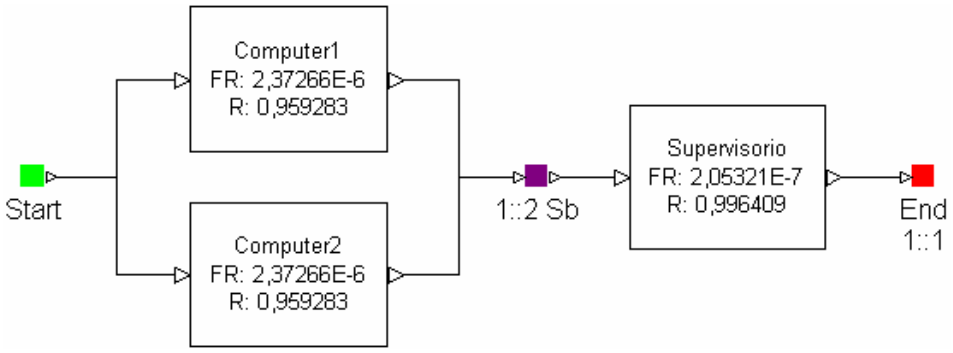


Figura 5. Diagrama em blocos do computador de bordo com redundância *cold standby*.

Por intermédio da taxa de falha e vida útil de vinte e quatro meses, a confiabilidade do computador de bordo com redundância *cold standby* é dada por *R(24 meses) = 0,995572*, sendo o *MTTF = 744905 horas*. O valor de confiabilidade obtido, do computador de bordo com redundância *cold standby*, está acima do valor do especificado de 0,960000 (Amazonia-1, 2008).

A unidade supervisora do computador de bordo com redundância *cold standby*, numa visão geral, pode ser um ponto de falha (ECSS-E-ST-20C, 2008) dentro do subsistema Gestão de Bordo. Para eliminar este ponto de falha, pode-se optar por aplicar redundância na unidade supervisora. Esta redundância, estando na configuração ativa, permite que as unidades sejam as próprias responsáveis pelo gerenciamento desta redundância, descartando assim uma terceira unidade para executar esta atividade.

A arquitetura do computador de bordo em redundância *cold standby*, contendo a unidade supervisora em redundância paralela ativa, é arranjada em diagramas de blocos de confiabilidade representada pela Fig. 6.

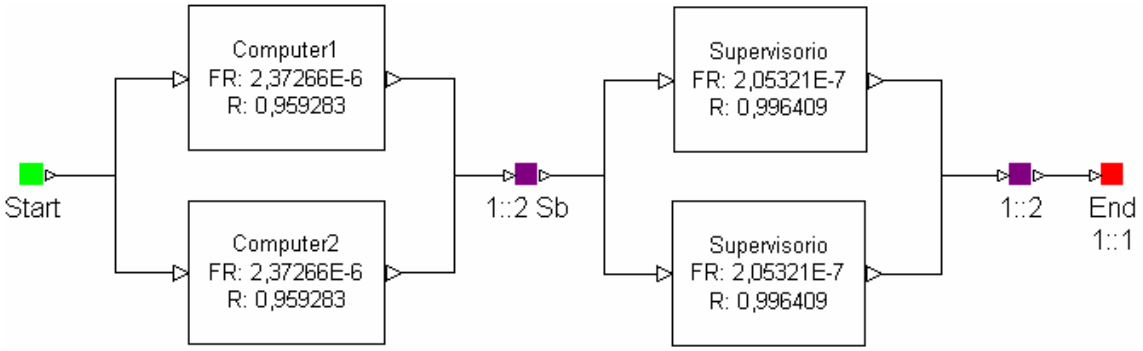


Figura 6. Diagrama em blocos do computador com redundância *cold standy* e unidade supervisora com redundância paralela ativa.

Por intermédio da taxa de falha e vida útil de vinte e quatro meses, a confiabilidade do computador com redundância *cold standby* e unidade supervisora com redundância paralela ativa é dada por *R(24 meses) = 0,999147*, sendo o *MTTF = 824249 horas*. O valor de confiabilidade obtido do computador com redundância *cold standby* e unidade supervisora com redundância paralela ativa, está acima do valor especificado de 0,960000 (Amazonia-1, 2008). Além de cumprir a especificação de confiabilidade, esta arquitetura também elimina o ponto de falha presente na unidade supervisora.

## 5. CONCLUSÃO

Num projeto de alta complexidade e multidisciplinar, em especial nos sistemas aeroespaciais, a confiabilidade deve ser abordada como ponto chave do sucesso da operação ao longo de sua da vida útil. O computador de bordo, como parte integrante do subsistema Gestão de Bordo, deve apresentar altos valores de confiabilidade, devido a sua importância dentro do sistema. Como relatado, a confiabilidade pode ser aumentada com a injeção da técnica de tolerância a falha, como a redundância de hardware, ou pela utilização de componentes com alto valor de confiabilidade individual. A Tabela 3 sintetiza os dados obtidos das arquiteturas propostas em três cenários: o primeiro se refere ao computador de bordo sem redundância; o segundo, ao computador com redundância *cold standby* e unidade supervisora sem redundância; e o terceiro, ao computador com redundância *cold standby* e unidade supervisora com redundância paralela ativa.

Tabela 3. Síntese da confiabilidade das arquiteturas propostas para o computador de bordo.

| | Cenário 1 | Cenário 2 | Cenário 3 |
|---|---|---|---|
| R(24 meses) | 0,959283 | 0,995572 | 0,999147 |
| MTTF (horas) | 421467 | 744905 | 824249 |

Pela Tabela 3, observa-se um aumento da confiabilidade à medida que se avançam ente os cenários 1, 2 e 3. O aumento maior é observado entre o cenário 1 e 2, porém, neste último há um ponto simples de falha. No cenário 3, o ponto simples de falha foi eliminado, no entanto, o acréscimo de confiabilidade foi relativamente menor. É importante salientar a utilização de uma unidade supervisora com maior confiabilidade, se comparada ao computador. Para isto, foi projetada uma arquitetura extremamente simplificada e com componentes que apresentam baixas taxas de falha, ou seja, alta confiabilidade, como comprova a Tab. 2.

O cenário 1, sem a redundância no computador de bordo, não atende a especificação de confiabilidade de 0,960000 (Amazonia-1, 2008). Pela utilização da técnica de tolerância a falha, a especificação é satisfeita nos cenários 2 e 3.

Estendendo a vida útil do sistema para um período superior aos vinte e quatro meses, é possível observar a influência positiva do cenário 3 no subsistema Gestão de Bordo. A Figura 7 mostra esta tendência quando a missão apresentar um período aproximadamente dez vezes maior a utilizada para a determinação da confiabilidade das arquiteturas propostas.

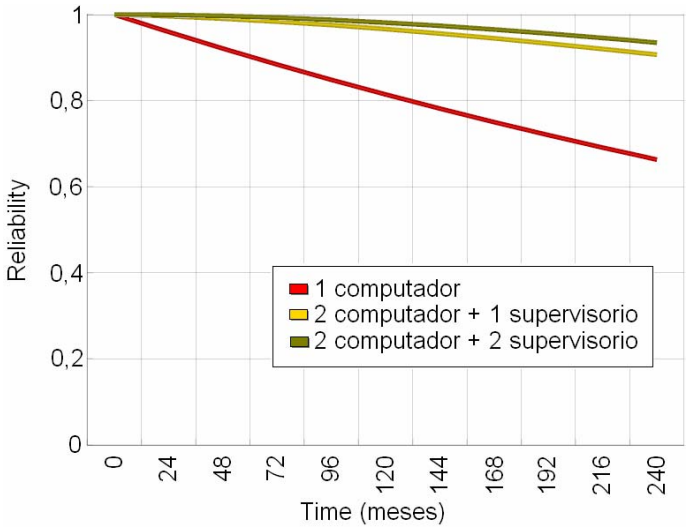


Figura 7. Confiabilidade do cenário 1, 2 e 3, para 240 meses.

Além da redundância de hardware, abordada neste artigo, outras técnicas poderiam contribuir para o aumento da confiabilidade do computador de bordo. Por exemplo, a redundância no software embarcado, presente em alguns trechos do programa ou até mesmo na sua totalidade; ou pela redundância de tempo, repetindo processo de computação do qual o tempo não seja fator determinante.

## 6. AGRADECIMENTOS

Agradecemos o apoio da Agência Espacial Brasileira, o Instituto Nacional de Pesquisas Espaciais e ao Instituto Tecnológico de Aeronáutica pela oportunidade e apoio financeiro para execução do projeto.

## 7. REFERÊNCIAS

Amazonia-1 Satellite Attitude Control and Data Handling (ACDH) Subsystem Specification – A12700-SPC-01, 2008, rev. 1, 26 p.

Azevedo, I. A., 2008, Apostila EA-160, Confiabilidade de componentes e sistemas, São José dos Campos: Instituto Tecnológico de Aeronáutica.

ECSS-E-ST-20C – European Cooperation For Space Standardization, Space Engineering, 2008, Electrical and Electronic, 21 p.

ITASAT – Programa de Satélites Universitários [Online], Acessado em Março 2009, http://www.itasat.ita.br/portuguese/index.htm.

Kozenieski, N. J., Saotome, O., Oliveira, N., Sistema de controle e processamento embarcado com arquitetura redundante tolerante a falhas de software e hardware, 2006.

Lafraia, J. R. B., 2001, Manual de Confiabilidade, Mantenabilidade e Disponibilidade, Qualitymark Editora Ltda, vol.1, pp. 98-100.

MIL-HDBK-217F, Reability Prediction of Eletronic Equipment. U.S. Department of Defense. Washington D.C. 1991.

NBR 5462 – Confiabilidade e mantenabilidade. Novembro de 1994.

O'Connor, P. D. T., 1991, Practical Reliability Engineering, 3º edition, 221 p.

Plataformas de Coleta de Dados, INPE/CPTEC/DSA [Online], Acessado em Março de 2009, http://satelite.cptec.inpe.br/PCD/sistema.jsp.

Relex Software Corp. Relex Reliability Studio 2008, setembro 2008 Update.

Satélite e seus subsistemas [Online], Acessado em Março de 2009, http://www6.cptec.inpe.br/~grupoweb/Educacional/MACA_SSS/.

SCD-1 – 1º Satélite de Coleta de Dados [Online], Acessado em Março de 2009, http://www.inpe.br/scd1/site_scd/historico.htm.

## 8. NOTA DE RESPONSABILIDADE

Os autores são os únicos responsáveis pelo material incluído neste artigo.