MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO
INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS

sid.inpe.br/mtc-m21b/2014/02.28.17.33-TDI

ESTUDO DE UM PROCESSO DE GARANTIA DA CONFIABILIDADE DE SISTEMAS ELETRÔNICOS EMBARCADOS A SINGLE EVENT UPSETS CAUSADOS POR PARTÍCULAS IONIZANTES

Sérgio Roberto Ferreira Machado

Dissertação de Mestrado do Curso de Pós-Graduação em Engenharia e Tecnologia Espaciais/Engenharia e Gerenciamento de Sistemas Espaciais, orientada pelo Dr. Marcelo Lopes de Oliveira e Souza, aprovada em 14 de maio de 2014.

URL do documento original:
<http://urlib.net/8JMKD3MGP5W34M/3FRBRB2>

INPE
São José dos Campos
2014

PUBLICADO POR:

Instituto Nacional de Pesquisas Espaciais - INPE
Gabinete do Diretor (GB)
Serviço de Informação e Documentação (SID)
Caixa Postal 515 - CEP 12.245-970
São José dos Campos - SP - Brasil
Tel.:(012) 3208-6923/6921
Fax: (012) 3208-6919
E-mail: pubtc@sid.inpe.br

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO
INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS

sid.inpe.br/mtc-m21b/2014/02.28.17.33-TDI

ESTUDO DE UM PROCESSO DE GARANTIA DA CONFIABILIDADE DE SISTEMAS ELETRÔNICOS EMBARCADOS A SINGLE EVENT UPSETS CAUSADOS POR PARTÍCULAS IONIZANTES

Sérgio Roberto Ferreira Machado

Dissertação de Mestrado do Curso de Pós-Graduação em Engenharia e Tecnologia Espaciais/Engenharia e Gerenciamento de Sistemas Espaciais, orientada pelo Dr. Marcelo Lopes de Oliveira e Souza, aprovada em 14 de maio de 2014.

URL do documento original:
<http://urlib.net/8JMKD3MGP5W34M/3FRBRB2>

INPE
São José dos Campos
2014

Dados Internacionais de Catalogação na Publicação (CIP)

Machado, Sérgio Roberto Ferreira.

M131e Estudo de um processo de garantia da confiabilidade de sistemas eletrônicos embarcados a single event upsets causados por partículas ionizantes / Sérgio Roberto Ferreira Machado. – São José dos Campos : INPE, 2014.

xxviii + 192 p. ; (sid.inpe.br/mtc-m21b/2014/02.28.17.33-TDI)

Dissertação (Mestrado em Engenharia e Tecnologia Espaciais/Gerenciamento de Sistemas Espaciais) – Instituto Nacional de Pesquisas Espaciais, São José dos Campos, 2014.

Orientador : Dr. Marcelo Lopes de Oliveira e Souza.

1. Efeitos de radiações ionizantes. 2. SEU-Single Event Upset. 3. Sistemas tolerantes à falha. 4. Engenharia de sistemas. I.Título.

CDU 620.1.004:519.2

Aprovado (a) pela Banca Examinadora em cumprimento ao requisito exigido para obtenção do Título de ***Mestre*** em

Engenharia e Tecnologia Espaciais/Gerenciamento de Sistemas Espaciais

Dr. Walter Abrahão dos Santos

Presidente / INPE / São José dos Campos - SP

Dr. Marcelo Lopes de Oliveira e Souza

Orientador(a) / INPE / SJCampos - SP

Dr. Paulo Giácomo Milani

Membro da Banca / INPE / SJCampos - SP

Dr. Silvio Manea

Membro da Banca / INPE / São José dos Campos - SP

Dr. Claudio Antonio Federico

Convidado(a) / IEAv/CTA / São José dos Campos - SP

Este trabalho foi aprovado por:

( ) maioria simples

(X) unanimidade

Aluno (a): ***Sérgio Roberto Ferreira Machado***

São José dos Campos, 14 de Maio de 2014

NOTA DE ESCLARECIMENTO

O presente trabalho não representa posição oficial da Agência Nacional de Aviação Civil (ANAC). O Autor é servidor desta Agência e procurou elaborar este trabalho de forma consistente com as políticas da ANAC aplicadas à Certificação de Produtos Aeronáuticos, porém o conteúdo deste trabalho não foi discutido no âmbito interno da Agência e representa apenas o ponto de vista do Autor.

O que sabemos é uma gota; o que ignoramos é um oceano.

Isaac Newton

A Deus, pelo dom da vida

AGRADECIMENTOS

Ao INPE, pela oportunidade oferecida, por meio do Curso de Pós-Graduação em ETE/CSE, de formar cidadãos mais qualificados e capacitados para a sociedade brasileira.

Ao Prof. Dr. Marcelo Lopes de Oliveira e Souza, pelo incentivo constante, conhecimentos compartilhados, orientação positiva e exigente, e pelo exemplo de professor competente que busca extrair o melhor dos alunos.

Aos membros da Banca Examinadora, Prof. Dr. Walter Abrahão dos Santos, Prof. Dr. Claudio Antonio Federico, Prof. Dr. Odair Lelis Gonçalez, Dr. Paulo Giácomo Milani, Dr. Silvio Manea, pela valiosa dedicação em avaliar este trabalho e assim contribuir para sua melhoria e evolução.

Ao Dr. Silvio Manea, pelo tempo, auxílio e conhecimento compartilhados em nível de um verdadeiro co-orientador, contribuindo de maneira fundamental para este trabalho.

Aos Drs. Claudio Federico e Odair Gonçales Lélis, do Instituto de Estudos Avançados – IEAV, por todo o auxílio no esclarecimento de dúvidas fundamentais para minha evolução nos estudos e realização deste trabalho.

Aos professores do INPE do curso ETE/CSE, pelo conhecimento, orientação e paciência ao longo do Curso de Mestrado em Engenharia e Tecnologia Espaciais/Engenharia e Gerenciamento de Sistemas Espaciais, e a todos os demais profissionais do INPE que, direta ou indiretamente, colaboraram para a realização deste trabalho.

À Agência Nacional de Aviação Civil, pelo apoio e disponibilização do tempo necessário para a realização das matérias e estudos ao longo do curso de Mestrado.

A minha família, em especial os meus pais João e Neusa, pelo apoio constante a minha formação como profissional e ser humano, e os meus irmãos João, Ademilson e Edilson, pelo companheirismo e amizade.

A minha esposa Maria Fernanda, pelo constante companheirismo e incentivo, pela paciência e compreensão ao longo das inúmeras noites de trabalho durante todo o curso.

A meu filho Rafael, que chegou bem próximo do fim deste Mestrado, me trazendo muita alegria e me incentivando a seguir em frente.

A todas as pessoas que, direta ou indiretamente, contribuíram para a realização desta Dissertação.

O meu muito obrigado.

Resumo

Os sistemas aeroespaciais estão se tornando cada vez mais complexos e/ou altamente integrados, conforme definido pela ARP 4754A, fazendo uso extensivo de microeletrônica e memórias digitais que, por sua vez, operam em freqüências cada vez mais altas e tensões cada vez menores. Além disso, as aeronaves estão voando a altitudes cada vez maiores e em rotas polares com freqüências cada vez maiores. Tais fatores aumentam a probabilidade de ocorrência de efeitos prejudiciais causados por partículas e radiações ionizantes gerando efeitos do tipo *Single Event Upsets* - SEUs sobre os seus sistemas eletrônicos embarcados. Estes devem ser projetados de forma a serem robustos aos SEUs baseando-se em critérios como confiabilidade, disponibilidade e criticalidade. A presente dissertação apresenta uma proposta de recomendações para garantia da robustez de sistemas eletrônicos embarcados aeroespaciais a SEUs causados por partículas e radiações ionizantes. A proposta visa auxiliar o setor aeroespacial (especialmente, o INPE e a ANAC) na captura e estruturação das principais considerações para o desenvolvimento e especificação de sistemas aeroespaciais robustos a falhas causadas pelo ambiente de partículas e radiações ionizantes. Para isto, o trabalho: 1) faz uma revisão bibliográfica dos principais conceitos envolvidos no problema da ocorrência de SEUs em sistemas eletrônicos embarcados aeroespaciais; 2) estuda os aspectos ligados à garantia de robustez à SEUs causados por radiações ionizantes em sistemas aeroespaciais; 3) estuda algumas das normas e recomendações mais utilizadas pela indústria espacial (normas da ESA e NASA) e aeronáutica (normas da SAE, RTCA, etc.) ligadas aos processo de garantia de robustez à partículas e radiações ionizantes; 4) discute as normas ESA, NASA, SAE, IEC, RTCA, etc. e recomendações para garantia de robustez a SEU em sistemas eletrônicos embarcados aeroespaciais; 5) propõe recomendações para garantia de robustez de sistemas eletrônicos embarcados a SEUs causados por partículas e radiações ionizantes (a grande experiência do setor espacial em lidar com o fenômeno SEU contribuiu para a definição de recomendações para sistemas aeronáuticos); 6) aplica estas recomendações a casos de estudo da literatura. Os resultados destas aplicações sugerem que as recomendações propostas são adequadas para a utilização no setor aeroespacial (especialmente no INPE e na ANAC). O detalhamento de um processo de garantia de robustez a SEUs e a extensão das recomendações para garantia de robustez a outros efeitos de partículas e radiações ionizantes são sugestões para trabalhos futuros.

STUDY OF AN ASSURANCE PROCESS OF RELIABILITY OF EMBEDDED ELECTRONIC SYSTEMS TO SINGLE EVENT UPSETS CAUSED BY IONIZING PARTICLES

ABSTRACT

The aerospace electronic systems are getting more complex and/or highly integrated, as defined by ARP 4754A, making extensive use of microelectronics and digital memories which, in turn, operate in higher frequencies and lower voltages. In addition, the aircraft are flying in higher altitudes, and polar routes are getting more frequent. These factors raise the probability of occurrence of hazardous effects caused by ionizing radiation like the Single Event Upsets - SEUs in their embedded electronic systems. These must be designed in a way to be robust to Single Event Upsets, based upon criteria such as reliability, availability and criticality. This dissertation presents a proposal of guidelines for the assurance of the robustness of aerospace embedded electronic systems to SEUs caused by ionizing particles and radiations. The proposal aims to assist the aerospace sector (especially INPE and ANAC) in capturing and structuring of the main considerations for the development and specification of aerospace systems robust to failures caused by the ionizing particles and radiations environment. To accomplish this objective, this work: 1) performs a bibliographic review of the main concepts related to the issue of SEUs occurrence in aerospace embedded electronic systems; 2) studies the aspects related to the assurance of robustness to SEUs caused by ionizing particles and radiations in aerospace systems; 3) studies some of the main standards and guidelines from the space (ESA and NASA standards) and aeronautics (SAE, RTCA, etc. standards) industry, related to the issue considered in this work; 4) discuss the standards from ESA, NASA, SAE, RTCA, etc. and guidelines to assurance the robustness of aerospace embedded electronic systems to SEUs caused by ionizing particles and radiations; 5) proposes guidelines to assure the robustness of embedded electronic systems to SEUs caused by ionizing particles and radiations (the great background of the space sector in dealing with the phenomena contributed to the definition of the guidelines for the aeronautics systems); 6) applies the guidelines to case studies of the literature. The results of this application suggest that the proposed guidelines are adequate to be used in the aerospace sector (especially at INPE and ANAC). The detailing of a process of assurance of robustness to SEUs and the extension of the guidelines to assure the robustness to other ionizing particles and radiation effects are suggestions to future works

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS E ABREVIATURAS

AC – *Advisory Circular*

ACE – *Actuator Control Electronics*

ADEOS - *Advanced Earth Observing Satellite*

ADIRU - *Air Data Inertial Reference Unit*

ADS – *Air Data System* (Sistema de Dados do Ar)

ANAC – Agência Nacional de Aviação Civil

ARINC - *Aeronautical Radio, Incorporated*

ARGOS - *Advanced Research and Global Observation Satellite*

ARP – *Aerospace Recommended Practice*

CBERS - *China-Brazil Earth Resources Satellite* (Satélite Sino-Brasileiro de Recursos Terrestres)

CFR – *Code of Federal Regulations*

CME – *Coronal Mass Ejections*

CM – *Certification Memorandum*

COTS - *Commercial Off The Shelf*

CRC - *Cyclic Redundancy Check*

DAL - *Development Assurance Level*

DO - *Directive Ordnance*

DRAM- *Dynamic Random Access Memory*

DSE - *Device Single Event*

DWC-CED - *Duplication With Comparison – Concurrent Error Detection*

EASA - *European Aviation Safety Agency*

ECSS - *European Cooperation for Space Standardization*

EDAC - *Error Detection And Correction*

EDDI - *Error Detection by Duplicated Instructions*

ESA - *European Space Agency*

FAA - *Federal Aviation Administration*

FDAL - *Function Development Assurance Level*

FHA – *Functional Hazard Assessment*

FMEA - *Failure Mode and Effects Analysis*

FMECA - *Failure Modes, Effects and Criticality Analysis*

FMES - *Failure Modes and Effects Summary*

FTA - *Fault Tree Analysis*

HF – *High Frequency*

ICAO - *International Civil Aviation Organization*

IDAL - *Item Development Assurance Level*

IEC - *International Electrotechnical Commission*

IMA – *Integrated Modular Avionics*

INCOSE - *International Council on Systems Engineering*

IS – Instrução Suplementar

ISS – *International Space Station*

ITAR - *International Traffic in Arms Regulations*

JEDEC - *Joint Electron Device Engineering Council*

LEO – *Low Earth Orbit* (Órbita Baixa da Terra)

LET – *Linear Energy Transfer*

LET_{th} – *Linear Energy Transfer threshold*

LRU – *Line Replaceable Unit*

MECB - Missão Espacial Completa Brasileira

MBU – *Multiple Bit Upset*

MCU – *Multiple Cell Upset*

MOE – *Measures of Effectiveness* (Medidas de Efetividade)

MSAFE - *Marshall Solar Activity Future Estimates Model*

MTBF - *Mean Time Between Failures* (Tempo Médio entre Falhas)

NASA - *National Aeronautics and Space Administration*

nMOS – *n-type Metal Oxide Semiconductor* (Semicondutor Metal Óxido tipo n)

PFC – *Primary Flight Computer*

PSSA - *Preliminary System Safety Assessment*

RBAC – Regulamentos Brasileiros de Aviação Civil

RBD – *Reliability Block Diagram*

RDM – *Radiation Design Margin*

RHA – *Radiation Hardness Assurance*

RTCA - *Radio Technical Commitee for Aeronautics*

SAA - Anomalia do Atlântico Sul

SAE - *Society of Automotive Engineers*

SAFO – *Safety Alert For Operators*

SEB - *Single Event Burnout*

SEC-DEC - *Single-Error Correcting Double-Error Detecting*

SEECA - *Single Event Effects Criticality Analysis*

SEE – *Single Event Effect*

SEL - *Single Event Latchup*

SEP – *System Engineering Plan*

SEPE – *Solar Energetic Particle Event*

SET - *Single Effect Transient*

SEU – *Single Event Upset*

SIB – *Safety Information Bulletin*

SMU – *Single Word Multiple Bit Upset*

SRD – *System Requirements Document*

SSA – *System Safety Assessment*

TS – *Technical Specification*

VHF – *Very High Frequency*

SUMÁRIO

1. INTRODUÇÃO

1.1. Contexto deste Trabalho

O clima espacial oferece diversos desafios para o projeto, desenvolvimento e operação de sistemas aeroespaciais. É preciso compreender este ambiente e seus efeitos nos sistemas aeroespaciais para se obter um projeto otimizado, minimizando os custos e os riscos e maximizando a confiabilidade e a qualidade.

Para se ter uma idéia dos efeitos dramáticos que o clima espacial oferece aos diversos sistemas desenvolvidos pelo ser humano, durante um período de intensa atividade solar entre outubro e novembro de 2003, foram registrados diversos eventos de partículas solares de alta energia, gerando tempestades geomagnéticas. Estes eventos ficaram popularmente conhecidos como as Tempestades do *Haloween* de 2003. Algumas das conseqüências destes eventos foram: correntes geomagneticamente induzidas em transformadores de energia elétrica com o seu subsequente desligamento, necessidade de proteção adicional dos astronautas da ISS e o desvio de rotas de aviões para evitar as regiões de alta latitude, gerando custos para as companhias aéreas na faixa de 10 mil a 100 mil dólares por voo. O setor espacial aparentemente foi o mais atingido, onde se estima que aproximadamente 59% das missões espaciais foram impactadas. Por exemplo, suspeita-se que tais eventos causaram a perda do satélite de 640 milhões de dólares ADEOS-2. E, mesmo que estes efeitos tenham sido observados durante períodos de atividade solar mais intensa, estes não foram os maiores eventos já registrados, sugerindo que, embora sejam eventos raros, são prováveis de ocorrer futuramente. O evento de atividade solar mais intenso documentado até hoje ocorreu de 28 de agosto a 4 de setembro de 1859, quando foram observadas auroras em latitudes onde geralmente não são visíveis, como no Caribe, Havaí e Santiago, no Chile. Observatórios magnéticos registraram perturbações no campo magnético da Terra tão extremas que os medidores atingiram o fundo de

escala, e as redes de telégrafos registraram inúmeros distúrbios (NATIONAL, 2008).

Atualmente, os componentes eletrônicos utilizados no ambiente aeroespacial estão gradativamente ficando mais integrados e realizando funções de maior complexidade, demandando maior uso de memórias, tanto no setor espacial como no setor aeronáutico.

Além disto, os aviões estão voando a altitudes cada vez maiores, devido a restrições de eficiência e custo, e voos em rotas por regiões polares são cada vez mais frequentes. A companhia aérea United Airlines, por exemplo, começou a utilizar rotas de Chicago a Hong Kong passando pelo Pólo Norte, em 1999 com 12 voos de demonstração. Já em 2007, a United havia realizado mais de 1800 voos no ano e realizou seu voo de número 8000 em abril de 2008. Outras treze companhias aéreas voaram rotas polares em 2007 totalizando quase 7300 voos, o que mostra o acréscimo dramático no tráfego aéreo nesta região do globo (CARLSON, 2011).

Esses fatores contribuem para o aumento da exposição dos sistemas às características do ambiente aeroespacial e para o aumento dos diversos efeitos destas características sobre os sistemas embarcados. Assim, tais características e efeitos acarretam a necessidade de se conhecê-los melhor e de se tomar ações no sentido de minimizar os riscos à missão inerentes a tais efeitos.

Em particular, as radiações ionizantes presentes nesse ambiente são uma ameaça aos subsistemas eletroeletrônicos, gerando efeitos como o *Total Ionization Dose* (TID) e *Single Event Effects* (SEEs). Este último é um grupo de efeitos causados pela interação de uma única partícula ionizante ao passar por um dispositivo eletrônico, gerando a mudança de estado do dispositivo, podendo ser divididos em: efeitos transitórios, que podem alterar um nível de sinal ou bit; e efeitos permanentes, que podem levar à perda de um componente. Dentre os efeitos transitórios, o mais estudado é o *Single Event Upset* (SEU), que gera uma mudança no estado ou um transiente em um

componente, induzido por uma partícula carregada como, por exemplo, próton ou átomo ionizado, sendo considerado responsável por diversas anomalias e falhas em espaçonaves (NASA RP 1390, 1996).

Especialmente, sobre o sul do território brasileiro, deve-se esperar um ambiente ainda mais severo para os satélites de órbita baixa e para as aeronaves que voam em grandes altitudes por conta de uma relativamente maior incidência de partículas carregadas devidas a chamada Anomalia do Atlântico Sul (SAA). Esta região de baixa intensidade de campo magnético que abrange grande parte do sul do Brasil permite uma maior incidência de partículas carregadas vindas do espaço, e consequentemente, uma maior probabilidade de ocorrência de *Single Event Upsets* (HARTMANN, 2005).

O INPE tem um histórico de projeto e operação de satélites de órbita baixa, que se iniciou em 1979, com a aprovação da MECB (Missão Espacial Completa Brasileira), onde ficou estabelecido que o INPE desenvolveria satélites de coleta de dados e de sensoriamento remoto.

Como produto deste trabalho, em 1993 foi lançado o Satélite de Coleta de Dados SCD-1, de órbita circular de 787 km de apogeu e 722 km de perigeu e 25 graus de inclinação, sendo o primeiro satélite brasileiro de coleta de dados totalmente desenvolvido pelo INPE. Na sequência, em 1998, foi lançado o SCD-2, de órbita de inclinação 25 graus, apogeu de 769 km e perigeu de 743 km.

Em 1988, Brasil e China assinaram o acordo de cooperação para o desenvolvimento dos satélites sino-brasileiro de recursos terrestres CBERS. Este programa contemplou, num primeiro momento, apenas dois satélites de sensoriamento remoto, CBERS-1 e 2, e foi expandido para incluir outros três satélites da mesma categoria, os satélites CBERS-2B e os CBERS-3 e 4 como uma segunda etapa da parceria Sino-Brasileira. A sequência de lançamentos até o presente é a seguinte:

- 1999: Lançamento do Satélite CBERS-1 - Satélite Sino-Brasileiro de Recursos Terrestres, com órbita de inclinação de 98,3º, apogeu de 745 km e perigeu 733 km.
- 2003: Lançamento do Satélite CBERS-2, com órbita de inclinação 98,5º, apogeu de 750 km e perigeu de 731 km.
- 2007: Lançamento do Satélite CBERS-2B, com órbita de inclinação 98,6º, apogeu de 774 km e perigeu 773 km.

O INPE atualmente trabalha nos projetos do satélite Amazônia-1, com lançamento previsto para 2015, e o programa de satélite Lattes-1, ambos baseados na Plataforma Multimissão (PMM). Como os satélites anteriores, a órbita planejada será baixa.

No setor aeronáutico, o controle e a limitação da exposição da tripulação à radiação ionizante são de grande preocupação. Em diversos países europeus e nos Estados Unidos e Canadá, por exemplo, os profissionais de voo são considerados como ocupacionalmente expostos a radiações e, por isso, possuidores de um risco adicional de desenvolver câncer em relação à população em geral. Estudos recentes realizados no território brasileiro (FEDERICO, 2011) mostram que grande parte das tripulações de aeronaves é exposta a níveis acima dos recomendados para o público em geral.

Há uma grande probabilidade de que SEUs já tenham causado graves incidentes devido aos efeitos em sistemas aeronáuticos embarcados. Em 7 de outubro de 2008, um avião, voando em cruzeiro a 37 Kft, alterou sua altitude de modo brusco e não comandado, devido a um dado incorreto enviado por uma de suas três unidades inerciais de referência (ADIRU). Dos 303 passageiros, ao menos 110 sofreram ferimentos, sendo 12 graves, e 9 dos 12 tripulantes foram feridos. Embora o relatório de investigação não tenha sido conclusivo, a ocorrência de um SEU foi a única hipótese não descartada como causa deste incidente grave (ATSB, 2011). Outro caso digno de nota é o das falhas reportadas no sistema de piloto automático do Boeing 777, que foram

consideradas como sendo devidas a SEUs, levando à necessidade de alterações neste sistema para acomodar e tolerar tais falhas (COOPER, 2012). Em face de tais ocorrências, tais características e efeitos acarretam a necessidade de conhecê-los melhor e tomar ações no sentido de minimizar os riscos à missão inerentes a tais efeitos. Muitos fabricantes de sistemas aeronáuticos já consideram os efeitos de SEEs no desenvolvimento de sistemas aeronáuticos embarcados.

1.2. Motivação deste Trabalho

Uma vez considerado o contexto exposto, o projeto de um sistema aeroespacial embarcado deve, portanto, operar no ambiente de radiações ionizantes durante o máximo de tempo possível, dentro de restrições de custo e recursos.

A definição de recomendações que possibilitem auxiliar a especificação de sistemas eletrônicos embarcados aeroespaciais, garantindo um nível de robustez adequada, baseado em critérios de criticalidade e confiabilidade, desde as etapas iniciais, traz um projeto otimizado como benefício. Ou seja, as medidas necessárias para que os sistemas eletrônicos embarcados sejam tolerantes a falhas induzidas por *Single Event Upsets* serão aplicadas em uma medida adequada.

As normas e recomendações utilizadas na área aeroespacial cumprem um papel fundamental para estabelecimento: 1) dos requisitos sobre os sistemas pelo uso da Engenharia de Requisitos; e 2) dos processos, medidas de efetividade e especificações dos sistemas, pelo uso da Engenharia de Sistemas, considerando todo o ciclo de vida do produto. Estes processos podem exigir um nível mínimo de desempenho, confiabilidade e segurança do sistema operando no ambiente aeroespacial, tendo um papel fundamental para garantir a robustez destes a SEUs. Por conta disso, as normas e recomendações serviram de base para este estudo.

1.3. Objetivo deste Trabalho

Este trabalho tem por objetivo o estudo de um processo de garantia da confiabilidade de sistemas eletrônicos embarcados a *Single Event Upsets* causados por partículas ionizantes.

1.4. Organização deste Trabalho

Para atingir os objetivos propostos, o presente trabalho é organizado da seguinte maneira:

O Capítulo 2 (Conceitos Básicos e Revisão Bibliográfica) apresenta a terminologia, os conceitos e algumas das normas e recomendações aplicáveis ao contexto do trabalho.

O Capítulo 3 (Formulação do Problema e Abordagens para a Sua Solução) descreve o problema considerado neste trabalho, possíveis abordagens para sua solução e a abordagem escolhida.

O Capítulo 4 (Efeitos da Radiação Ionizante em Sistemas Eletrônicos Embarcados Aeroespaciais) discute brevemente alguns dos principais aspectos que devem ser considerados no desenvolvimento de sistemas eletrônicos embarcados aeroespaciais tolerantes a SEUs e que portanto devem ser considerados para as recomendações propostas por este trabalho.

O Capítulo 5 (Normas e Recomendações Aeroespaciais Aplicadas a SEUs) descreve os principais pontos abordados nas normas e recomendações, no que se referirem aos SEUs e ao objeto de estudo deste trabalho, de modo a se ter subsídios para a discussão das recomendações para garantia de robustez a SEUs em sistemas eletrônicos embarcados aeroespaciais.

O Capítulo 6 (Discussão das Normas e Recomendações Aeroespaciais e Proposta de Recomendações) discute as normas e recomendações para garantia de robustez a SEUs em sistemas eletrônicos embarcados aeroespaciais descritos no capítulo 5, à luz dos aspectos expostos e discutidos no capítulo 4, e propõe recomendações para garantia da confiabilidade de

sistemas eletrônicos embarcados aeroespaciais a SEUs causados por radiações ionizantes.

O Capítulo 7 (Conclusões, Recomendações e Sugestões para Trabalhos Futuros) se dedica às conclusões, considerações finais e sugestões para trabalhos futuros.

2. CONCEITOS BÁSICOS E REVISÃO BIBLIOGRÁFICA

Este capítulo apresenta alguns conceitos básicos e uma revisão bibliográfica com o intuito de uniformizar a terminologia usada, além de descrever brevemente algumas das normas e recomendações aplicáveis ao escopo deste trabalho.

2.1. Ambiente de Radiações Ionizantes

O espaço é permeado por um fluxo de partículas como prótons e átomos ionizados, com diferentes níveis de energia, que variam da faixa de 30 keV a 10^{15} MeV (FEDERICO, 2011). Na faixa considerada de alta energia, ou seja, com níveis de energia da ordem de milhões de elétrons-volt, as partículas são capazes de ionizar os átomos em materiais como os semicondutores em componentes eletrônicos, causando efeitos como os *Single Event Effects*.

Estes fluxos de partículas energéticas, cujas fontes podem ser separadas em fluxos de partículas de origem Solar e fluxos de “radiação” galáctica originada de fora do Sistema Solar, interagem com a atmosfera terrestre e com o campo magnético da Terra. As partículas solares são compostas majoritariamente de elétrons e prótons. A “radiação” galáctica é composta de 98% de núcleos de átomos, sendo que destes, aproximadamente 87% são prótons (núcleos de hidrogênio), 12% de núcleos de hélio e 1% de íons pesados; o restante, cerca de 2% é composto basicamente de elétrons e pósitrons (FEDERICO, 2011). A Figura 2.1 abaixo mostra uma representação gráfica da interação das radiações Solar e galáctica com a magnetosfera e a ionosfera terrestres.

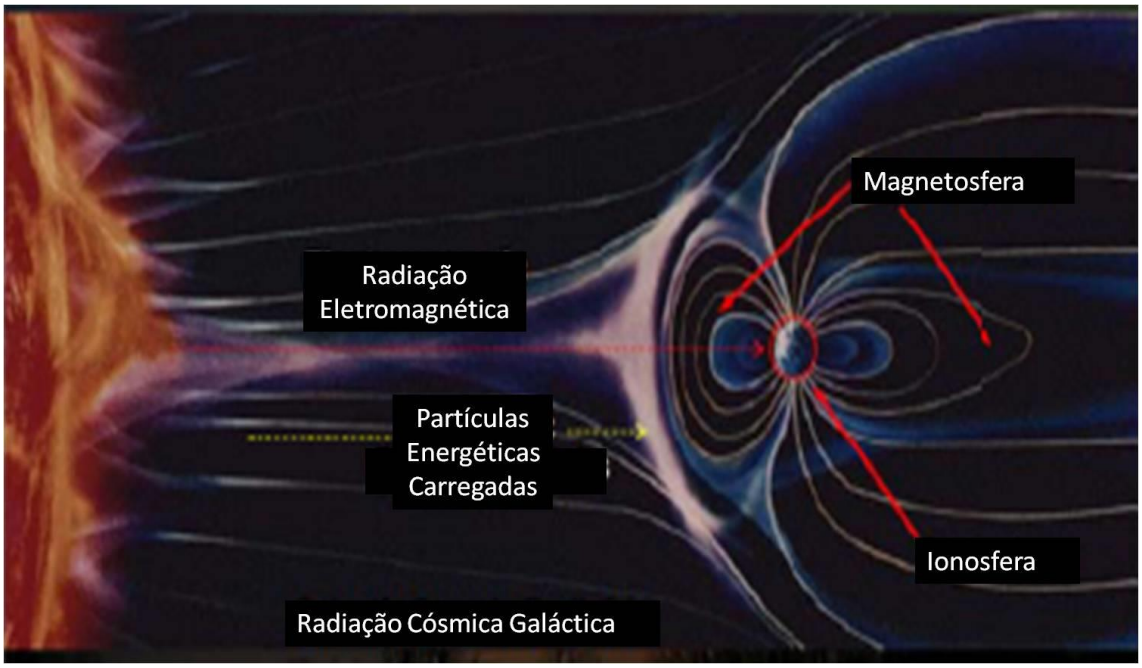

Figura 2.1 - Interação das radiações solar e galáctica com a magnetosfera e a ionosfera terrestres
Fonte: adaptado de EASA SIB 2012-09 (2012).

De acordo com (MORO, 2011), a magnetosfera terrestre é uma região em que o campo magnético domina o movimento do plasma, que é constituído principalmente de prótons e elétrons. A forma das linhas do campo magnético é deformada pela ação do vento solar, sendo achatadas de frente para o Sol e alongadas do lado oposto (Figura 2.1).

Grupos de partículas ionizadas são aprisionados em regiões conhecidas como cinturões de radiação de Van Allen. Tais partículas, sob a ação do campo magnético terrestre, executam um complexo movimento em espiral ao longo das linhas de campo magnético, formando basicamente dois cinturões: o mais interno composto majoritariamente de prótons e o mais externo composto majoritariamente de elétrons, como mostra a Figura 2.2. O cinturão interno está situado acima de 400 quilômetros da superfície terrestre, enquanto que o externo está a aproximadamente 12000 quilômetros; outros cinturões podem surgir temporariamente devidos principalmente à ação do Sol (MAZUR, 2003).

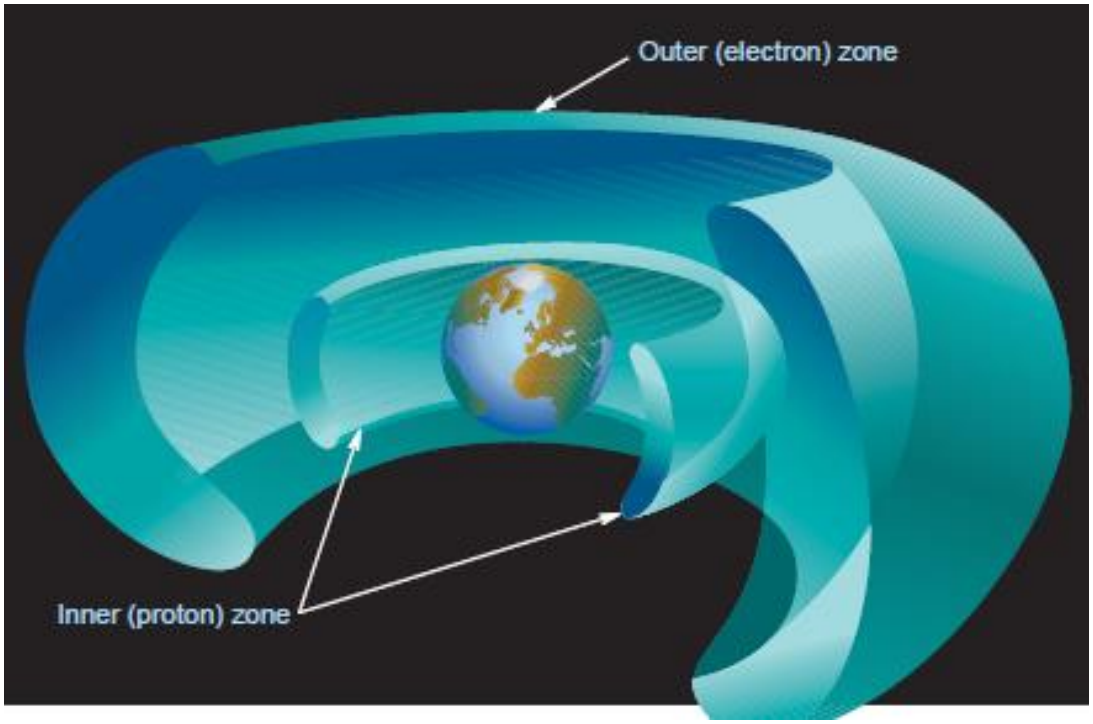

Figura 2.2 - Diagrama dos cinturões de radiação de Van Allen
Fonte: extraído de MAZUR (2003).

O campo magnético da Terra e a atmosfera proporcionam um nível de proteção que varia conforme a latitude e altitude do local, e a intensidade e direção do campo magnético terrestre no local. As regiões polares são as mais suscetíveis a essas partículas, pois as linhas de campo magnético nestas regiões se estendem verticalmente, permitindo que ao realizar seu movimento em espiral ao longo das linhas de campo magnético, as partículas cheguem a altitudes relativamente menores (MORO, 2011; FEDERICO, 2011).

De acordo com (HARTMANN, 2005), a baixa intensidade de campo magnético na região da Anomalia do Atlântico Sul (SAA) faz com que haja menor resistência ao fluxo de partículas ionizantes nesta região. Em consequência disso, há uma deformação no cinturão de Van Allen mais interno que, nesta região, tem em média menor altitude em relação à superfície terrestre, além de outros fenômenos que causam problemas em equipamentos e satélites que orbitam a Terra e passam por essa região.

A atividade Solar segue um ciclo de aproximadamente 11 anos (entre 9,5 a 12,5 anos), e é a maior responsável pela variação do clima espacial e consequentemente do fluxo de partículas energéticas que atingem a Terra. Ainda, eventos de curto prazo com duração de dias, como grandes explosões solares chamadas de Eventos de Partículas Solares Energéticas (*Solar Energetic Particle Events* - SEPEs), podem ocorrer (FEDERICO, 2011).

De acordo com (EASA SIB 2012-09, 2012), algumas causas desta atividade e suas consequências são descritas a seguir:

- Tempestade geomagnética: Ejeções Coronais de Massa (*Coronal Mass Ejections* – CMEs) são geralmente os agentes causadores, levando o campo geomagnético a um estado perturbado por dias. As Ejeções Coronais de Massa (CMEs) são erupções de plasma e campo magnético vindos do Sol, contendo até 10^{16} gramas de matéria e viajam a velocidades em média de 300 km/s com energia cinética de até 10^{32} ergs (1 erg=100 nJ). Ocorrem mais frequentemente durante o período de máxima atividade solar e são resultado da liberação de energia armazenada no campo magnético do Sol. Para gerar uma tempestade magnética, a CME deve ter uma trajetória tal que irá impactar o campo magnético da Terra, ser rápida e massiva (>= 1000 km/s), ou seja, com alta energia cinética e ter um forte campo magnético cuja orientação seja oposta ao da Terra. A topologia do campo magnético da Terra muda no curso da tempestade, causando problemas a vários sistemas tecnológicos.
- Tempestades de radiação solar: ocorrem quando grandes quantidades de partículas carregadas, principalmente prótons, são acelerados por processos na vizinhança do Sol, sendo que a Terra é atingida por tais partículas. Isto, por sua vez, causa um aumento na dose de radiação recebida por humanos e aumenta a probabilidade de ocorrência de SEUs em componentes eletrônicos.

- *Radio blackout*: afetam primariamente as faixas de HF (3-30 MHz), sendo observados efeitos de diminuição na habilidade de recepção nas faixas de freqüências superiores, como VHF (30-300 MHz). É conseqüência da maior densidade de elétrons causada pela emissão de partículas do Sol (SEPE), que ionizam o lado iluminado da Terra. Por exemplo, um evento em novembro de 2003 causou a perda ou comunicação degradada em comunicações via HF por várias horas.
- Tempestades ionosféricas: surgem pelo grande afluxo de partículas solares e radiação eletromagnética, dando início a tempestades geomagnéticas. Há um forte acoplamento entre a ionosfera e a magnetosfera, fazendo com que em geral, ambas sejam perturbadas.

Na atmosfera terrestre, os fluxos de partículas solares e fluxos de radiação galáctica, ao colidirem com núcleos de átomos da atmosfera terrestre, produzem chuveiros de partículas secundárias como nêutrons, píons, elétrons, fótons e prótons. As partículas solares e de origem galáctica, de acordo com sua energia ou massa, interagem de diversas formas com as moléculas da atmosfera terrestre, perdendo energia até serem finalmente freadas ou absorvidas na atmosfera ou na crosta terrestre (FEDERICO, 2011).

A intensidade do fluxo das partículas secundárias atinge seu máximo em torno de 18,3 km de altitude em relação ao nível do mar, chamado de máximo de Pfotzer. Na altitude de interesse para a aviação, os fluxos de partículas chegam a ser centenas de vezes maiores que ao nível do mar, e o principal componente causador de efeitos de SEUs em componentes eletrônicos embarcados são os nêutrons. Há, também, uma forte dependência do fluxo de partículas em relação à latitude, por conta principalmente da deflexão destas partículas pelo campo magnético terrestre, sendo que a incidência de raios cósmicos próximo aos polos chega a ser duas a três vezes maior do que nas regiões equatoriais (DYER, 2001).

A interação das partículas ionizantes com os diversos sistemas eletrônicos embarcados, tanto em satélites quanto em aeronaves, é extremamente

complexa, variando basicamente de acordo com o tipo de partícula, seu nível de energia e fluxo, que podem variar consideravelmente de intensidade ao longo do tempo por causa de diversos fenômenos que ocorrem no espaço e na atmosfera terrestre.

Uma forma comum de se descrever essa interação é por meio da energia absorvida pelo material o qual a partícula incide por unidade de massa. A unidade de medida de energia comumente usada é o elétron volt (eV), que é a energia cinética adquirida por um elétron que passa por uma diferença de potencial de 1V no vácuo (aproximadamente, 1 eV = $1{,}602.10^{-19}$ J). O fluxo de partículas pode ser definido como o número de partículas que atravessam uma área transversal de 1 cm^2 durante 1 segundo. A quantidade de energia absorvida, ou dose de radiação, deve ser medida na unidade especial do Sistema Internacional de Unidades, gray (Gy), que vale 1 J/kg, mas ainda é comum a utilização da unidade antiga rad (*radiation absorbed dose*), onde 1 rad = 10^{-2} J/kg. (ARRUDA, 2006).

2.2. Efeitos da Radiação em Componentes Eletrônicos

Os efeitos das interações da radiação de partículas em componentes eletrônicos são diversos, e podemos classificá-los de diversas maneiras. Ao se considerar o efeito final, podemos distinguir entre efeitos transitórios e efeitos permanentes.

Os efeitos permanentes estão ligados a modificações estruturais no material do componente eletrônico, não sendo reversível tanto ao se retirar a fonte de partículas quanto ao se efetuar uma ciclagem de energia do componente. Ao se considerar os aspectos físicos do componente, os efeitos podem ser classificados em danos por deslocamento e danos por ionização (ARRUDA, 2006). Na sequência, são descritos os conjuntos mais comuns de efeitos.

2.2.1. *Total Ionization Dose* (TID)

As partículas ionizantes, ao atingirem os componentes eletrônicos com energia suficiente, interagem com os materiais que ao receberem energia da partícula, liberam elétrons, gerando pares de elétrons-lacuna (um elétron livre e uma lacuna do átomo original). Durante o funcionamento do circuito, muitas cargas são recombinadas e estes pares são eliminados. No entanto, algumas cargas podem persistir, acumulando-se no componente e modificando seu desempenho, de acordo com esta energia ionizante total absorvida (ARRUDA, 2006).

No caso do óxido de silício (SiO_2), comumente usado como material isolante em componentes eletrônicos, as lacunas, por se difundirem lentamente, têm maior probabilidade de se acumularem no volume do óxido, ou na interface do óxido-silício, tornando-se assim uma carga positiva. Como consequência, temos a criação de um campo elétrico parasita que, de acordo com seu efeito acumulado, modifica e prejudica o funcionamento do componente. Assim, a Dose Total de Ionização - TID, que pode ser considerado um dano por ionização, pode ser entendida como uma medida da dose total da energia acumulada no material do componente eletrônico por radiação (ARRUDA, 2006).

A dose é usada para quantificar os efeitos da liberação de carga por ionização, é definida como a energia depositada pela unidade de massa do material (que deve ser especificado), e pode ser medida em termos de J/kg ou rad, onde 1 rad = 100 ergs/g (DYER, 2001)

2.2.2. *Displacement Damage* (DD)

Os átomos dos componentes eletrônicos semicondutores são dispostos em uma rede cristalina, que caracteriza seu funcionamento. Ao serem atingidos por partículas de alta energia, pode haver um deslocamento do núcleo de um ou mais átomos da rede, o que altera as características eletrônicas do componente. Este fenômeno é também chamado de Dose Total Não Ionizante

(Total Non Ionization Dose), de forma a distinguir este fenômeno do TID (ECSS E-HB-10-12A, 2010).

A energia e o momento linear transferido pela partícula variam principalmente de acordo com a massa e a energia que a partícula incidente detém. Alguns exemplos de efeitos em componentes eletrônicos são: redução no ganho de transistores bipolares, redução na eficiência de células solares e fotodetectoras, ineficiência na transferência de carga em dispositivos CCD (*Charge Coupled Devices*) e degradação na resolução de sensores de estado sólido. Assim, podemos definir os Danos por Deslocamento – DD, como danos na estrutura cristalina de um material causados pela colisão, elástica ou não, de uma partícula de alta energia (ARRUDA, 2006).

2.2.3. *Single Event Effects* (SEEs)

Os *Single Event Effects* (SEEs), ou Efeitos de Evento Único, são um grupo de fenômenos em que os componentes microeletrônicos alteram um sinal ou podem ser permanentemente danificados pelo resultado de uma deposição altamente localizada de energia por meio de uma única partícula ionizante. São causados tanto por ionização direta devida a uma partícula ionizante atravessando um componente (Figura 2.3a), como por ionização indireta devida a emissão de um núcleo que interage com uma partícula (Figura 2.3b).

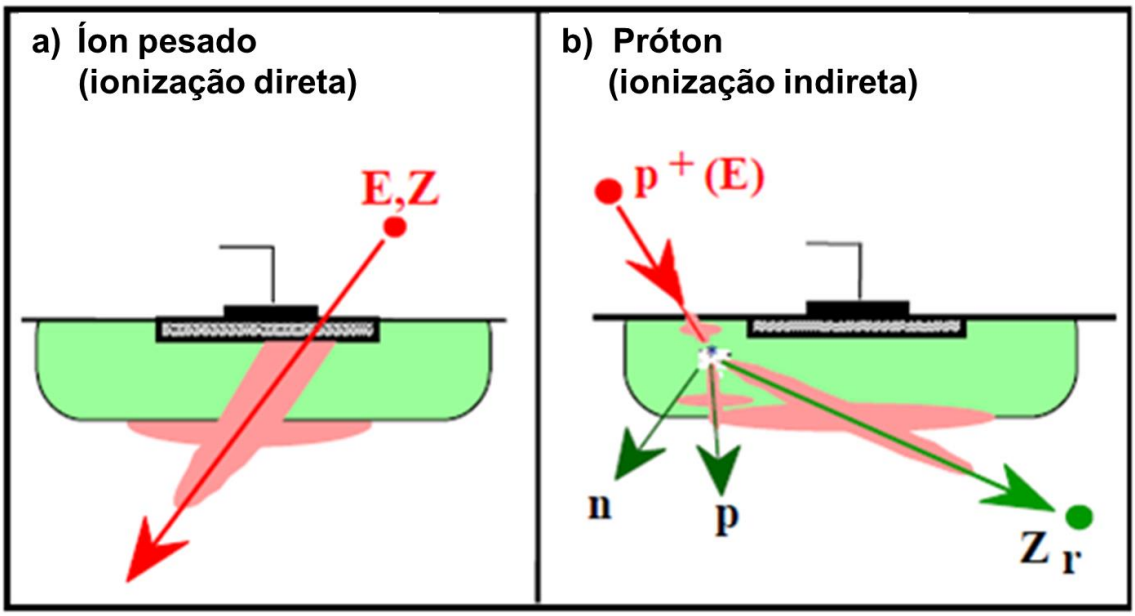

Figura 2.3 - Mecanismos de geração de SEEs: a) por ionização direta (partículas ionizantes: íons pesados); e b) por interações nucleares (partículas ionizantes: prótons e nêutrons)
Fonte: adaptado de ECSS-E-ST-10-12C (2008).

De acordo com (ARRUDA, 2006), em geral, o funcionamento dos componentes eletrônicos pode ser baseado no controle de fluxo de portadores de carga através da variação do potencial elétrico; e as partículas ionizantes agem de modo a gerar pares de lacunas e elétrons iguais, comprometendo o desempenho do componente.

Na Figura 2.3a, o íon pesado (Z) atravessa o componente, transferindo energia suficiente (E) para a geração de pares de portadores de carga (ilustrado em vermelho). Na Figura 2.3b, o impacto de um próton (p^+) com alta energia (E) em um núcleo do componente gera partículas secundárias de alta energia, que no caso da Figura 2.3b, é o íon pesado Z_r, que por sua vez causa a geração dos pares de elétrons e lacunas.

Os parâmetros usados para expressar essa interação entre a partícula ionizante e os circuitos eletrônicos são complexos e variam de acordo com diversos fatores. Baseado em (ECSS-E-HB-10-12C, 2010) temos como principais parâmetros:

A **Transferência Linear de Energia (*Linear Energy Transfer* - LET)**, definida como a quantidade de energia depositada no caminho percorrido pela partícula ionizante, medida tipicamente em MeV.cm^2/mg. A LET é expressa em função do tipo de partícula e pode ser aproximada por:

$$\begin{cases} LET\ (x) \cong \dfrac{1}{\rho}\dfrac{dE}{dx}(x), & 0 \le x \le r \\ LET\ (x) = 0, & demais\quad casos \end{cases}$$

(2.1)

Onde r é o alcance da partícula e ρ a densidade do material no qual a partícula está depositando a energia (2,32g/cm^3 para o silício, por exemplo), e dE/dx é a é a energia perdida pela partícula (dE) ao percorrer uma distância (dx).

A **seção de choque (*cross section*)** é uma medida da probabilidade de ocorrência de SEEs e é medida experimentalmente como o número de eventos registrados (SEUs, por exemplo) de acordo com a fluência de partículas. A seção de choque de partículas como íons pesados, é geralmente medida em função do LET, e em função da energia da partícula para nêutrons e prótons:

$$\sigma_{íon}\ (LET\ ) = \frac{número\ \_\ de\ \_\ eventos}{fluência\ \_\ do\ \_\ íon}, \qquad ou$$

$$\sigma(E)_{nêutron\ \_\ ou\ \_\ próton} = \frac{número\ \_\ de\ \_\ eventos}{fluência\ \_\ do\ \_\ próton\ \_\ ou\ \_\ nêutron}$$

(2.2)

As unidades típicas são geralmente cm^2/dispositivo ou cm^2/bit.

A **carga crítica, Q_c**, é a quantidade mínima de carga coletada por uma região sensível do componente eletrônico, pela passagem de uma partícula ionizante, que resulta em um SEE.

O **volume sensível** é geralmente modelado como um paralelepípedo retangular onde é possível haver a coleta de carga de maneira a resultar em um SEE no componente eletrônico. Há diversas simplificações nesta abordagem e, em geral, assume-se que a dimensão deste volume pode ser

dada pela seção de choque (a superfície sensível em cm^2/bit, por exemplo) multiplicada pela sua espessura; e, baseado em estudos dos SEUs, assume-se uma espessura de 2μm.

Há diversos tipos de SEEs descritos na literatura. Basicamente, os SEEs podem ser subdivididos em: destrutivos, também chamados de *hard errors*, que podem causar danos permanentes na operação do componente eletrônico; e não destrutivos, também chamados de *soft errors*, em que uma operação de ciclagem do componente (reescrita de um bit de memória ou retirada da alimentação de energia, por exemplo) o traz de volta à condição não perturbada. Baseado em (ECSS-E-HB-10-12A, 2010), pode-se dividir os SEEs da maneira a seguir:

2.2.3.1. Single Event Latchup (SEL)

Single Event Latchup (SEL) é uma condição potencialmente destrutiva envolvendo correntes parasitas as quais podem exceder o valor máximo suportado pelo componente, levando à perda do componente quando não há limitação de corrente. É geralmente referido a circuitos CMOS, em que o efeito criando tiristores parasitas PNPN.

2.2.3.2. *Single Event Snapback* (SESB)

Single Event Snapback (SESB) é similar ao SEL, ocorrendo geralmente em transistores N-MOS, onde uma partícula ao atingir a região do dreno, cria um caminho de alta corrente.

2.2.3.3. *Single Event Gate Rupture* (SEGR)

Single Event Gate Rupture (SEGR) é a formação de um caminho condutor disparado por uma partícula ionizante que atinge uma região de alto campo elétrico no óxido da porta de um transistor.

2.2.3.4. *Single Event Dielectric Rupture* (SEDR)

Single Event Dielectric Rupture (SEDR) é a ruptura destrutiva de um dielétrico causada por uma particular ionizante na região de alto campo elétrico do dielétrico de componentes como FPGAs e dispositivos lineares.

2.2.3.5. *Single Event Burnout* (SEB)

Single Event Burnout (SEB) é o disparo de um dispositivo semicondutor de potência, geralmente operando em altas tensões, gerando altas correntes e perda do componente.

2.2.3.6. *Multiple Bit Upset* (MBU)

Multiple BIT Upset (MBU) é a interação de uma partícula que causa a mudança de estado de mais de um bit de um componente digital, em geral, memórias e registradores.

Esta definição é aplicável a todos os casos de alteração de mais de um bit causado por uma partícula, e engloba as definições de: *Single Word Multiple Bit Upset* – (SMU), que é a mudança de estado de mais de um bit de um componente digital no mesmo bloco de dados (única palavra, ou *word*); e o Multiple Cell Upset (MCU), que é a mudança de estado de um ou mais bits em mais de uma célula.

2.2.3.7. *Single Event Functional Interrupt* (SEFI)

Single Event Functional Interrupt (SEFI): mudança de um sinal de controle de um circuito ou em processadores, causado por uma partícula ionizante, tendo como conseqüência a interrupção do funcionamento normal do circuito ou dispositivo.

2.2.3.8. *Single Effect Transient* (SET)

Single Effect Transient (SET): efeito que gera um sinal espúrio na forma de uma excursão no valor da tensão em um semicondutor (*voltage spike*), que pode ser propagado e capturado como um valor lógico errado.

2.2.3.9. *Single Event Upset* (SEU)

Single Event Upset (SEU): é uma mudança de estado lógico ou tensão causada por uma partícula energizada que colide com o nodo sensível de um circuito, tal como uma célula de memória.

A norma ECSS-E-ST-10-04C define SEU como uma mudança de estado de um bit em um elemento digital que foi causado tanto por uma partícula ionizante atravessando um componente, como por emissão de um núcleo que interage com uma partícula. De acordo com (NICOLAIDS, 2011), a literatura por vezes utiliza o termo SEU como sendo o conjunto dos SEEs não destrutivos. Embora seja o tipo mais comum de SEE não destrutivo, para o presente trabalho o SEU deve ser entendido em seu sentido mais restrito.

O SEU ocorre em circuitos digitais quando uma partícula com alta energia (partícula ionizante) faz com que um elemento de eletrônica digital mude de estado. Isto pode ocorrer em micro circuitos, como por exemplo, chips de memória, dispositivos de comunicação, circuitos de potência ou microprocessadores. Esta mudança de valor pode levar a comportamentos observáveis em nível de sistema, como o travamento de um subsistema ou um comando inesperado do mesmo.

Para fins de organização, a Figura 2.4 abaixo ilustra uma possível classificação dos efeitos causados pelas partículas ionizantes:

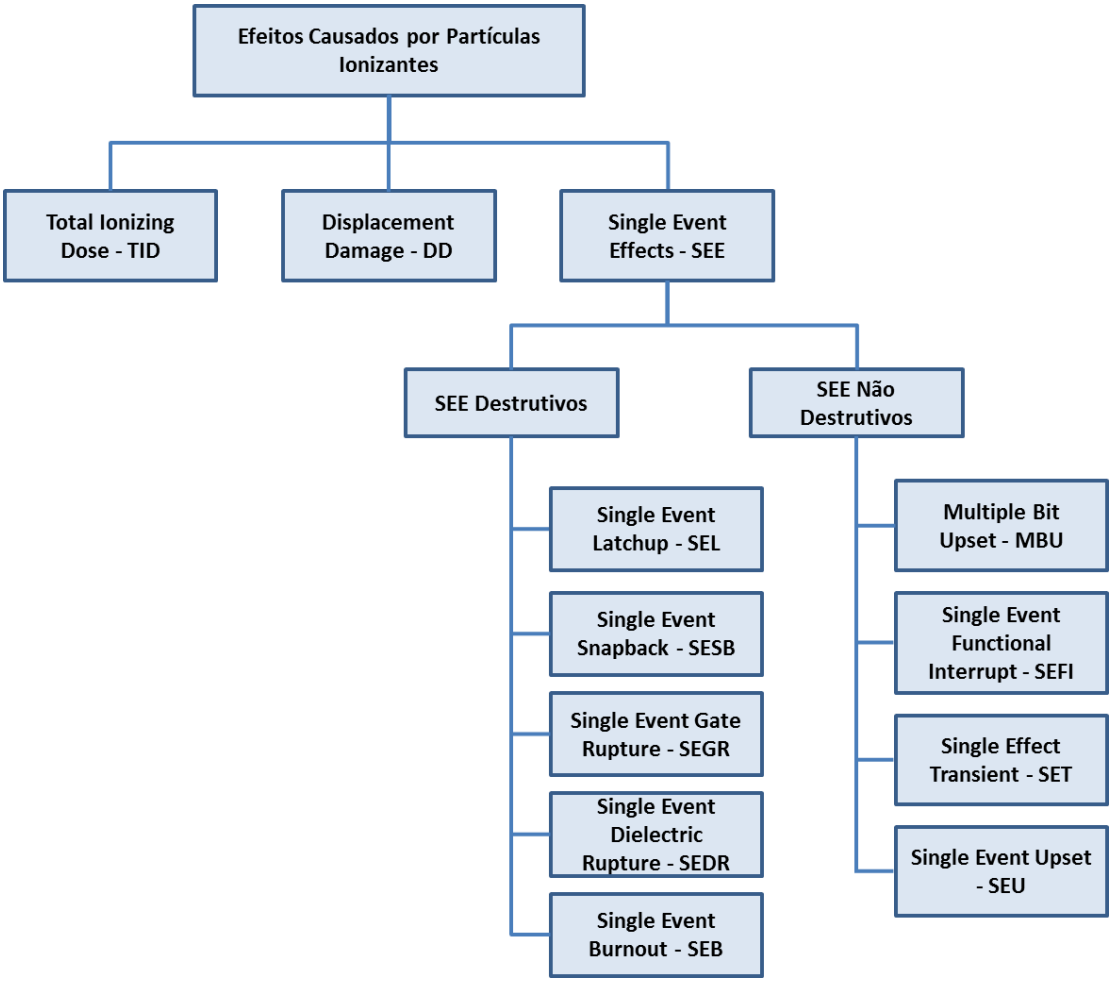

Figura 2.4 - Principais efeitos em componentes eletrônicos causados por partículas ionizantes de acordo com ECSS-E-HB-10-12A

2.2.3.10. Exemplo dos Efeitos do Ambiente Espacial de Radiações Ionizantes

O experimento MOPITT (*Measurements Of Pollution In The Troposphere*), lançado em 1999 a bordo do satélite Terra, mediu de março de 2000 a janeiro de 2003 vários Eventos Únicos em Dispositivos (DSEs - *Device Single Events*). Do total, cerca de 54% dos DSEs ocorreram na região da SAA, enquanto que 26% ocorreram nas regiões polares (HARTMANN, 2005), mostrando o impacto do ambiente mais severo da SAA. Uma vez que a medição destes eventos não foi em circuitos eletrônicos digitais, mas em um acelerômetro piezelétrico, não

foi utilizado o termo *Single Event Upset* e sim *Device Single Event* (NICHITIU et al., 2004). A Figura 2.5 mostra a distribuição dos DSEs.

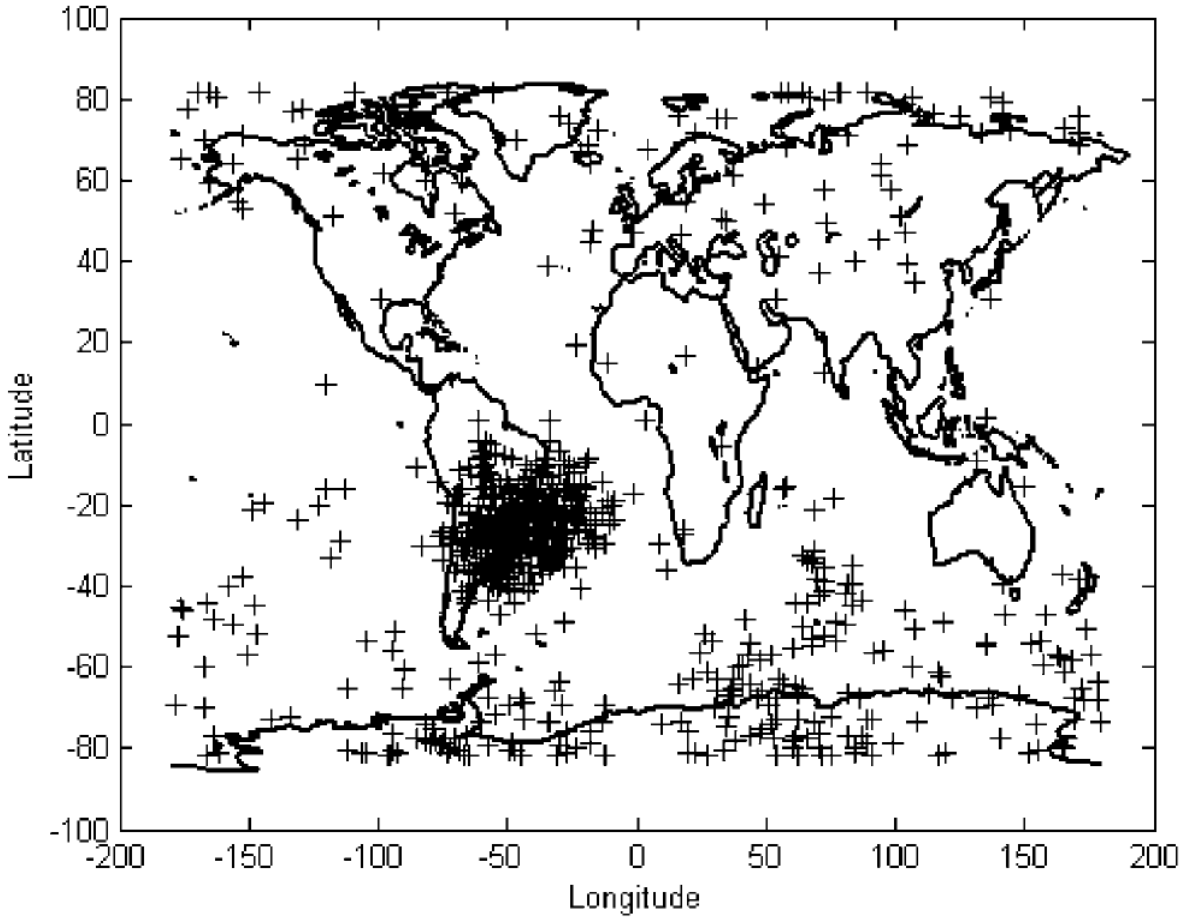

Figura 2.5: Distribuição geográfica de *Device Single Events* (DSEs). A Anomalia do Atlântico sul pode ser identificada pela densidade de pontos medidos. Fonte: extraído de HARTMANN (2005).

2.3. Engenharia de Sistemas no Contexto de Sistemas Eletrônicos Embarcados

Os diversos sistemas utilizados nos projetos aeroespaciais são o que podemos considerar complexos. Segundo (LOUREIRO, 2012), esta complexidade é resultante do número de conexões e das interações entre as partes ou elementos de um conjunto. Para se desenvolver tais sistemas, é preciso uma abordagem capaz de lidar com todas as variáveis de projeto de modo a se obter um resultado otimizado.

A Engenharia de Sistemas trabalha no projeto do sistema como um todo, diferentemente das engenharias de componentes/tradicionais/especializadas que trabalham focadas nas partes do sistema. Isso faz com que o projeto ou modificação de uma parte ou subsistema gere um resultado mais completo e consistente, tornando fundamental o uso do Processo da Engenharia de Sistemas.

De acordo com (INCOSE, 2006), a Engenharia de Sistemas é uma profissão, um processo e uma perspectiva, tendo diversas definições. Utilizaremos a definição de (LOUREIRO, 2012):

> *Engenharia de Sistemas é uma abordagem inter e multidisciplinar colaborativa de engenharia para derivar, evoluir e verificar uma solução-sistema balanceada ao longo do ciclo de vida que satisfaça às expectativas dos interessados (stakeholders) e a aceitação pública.*

Nesta definição, a satisfação dos interessados tem papel central. Segundo (LOUREIRO, 2012), os interessados são indivíduos ou grupos que têm um interesse, podem afetar ou ser afetados por um sistema ao longo de seu ciclo de vida.

De acordo com essa visão, as atividades de Engenharia de Sistemas começam pela **Definição dos Requisitos dos Interessados** e prosseguem com a **Análise dos Requisitos** (INCOSE, 2006). A partir desses processos, requisitos e atributos são capturados e as organizações envolvidas no seu ciclo de vida são identificadas. Desta forma, desde os estágios iniciais da definição dos sistemas já é possível ter visibilidade de conexões de impactos, rastreabilidade e hierarquia, diminuindo o risco de se necessitar efetuar mudanças tardias, que possuam impacto muito maior em termos de custo e tempo (LARSON et al., 1999).

As atividades de Definição dos Requisitos dos Interessados englobam desde a elicitação de interessados e das capacidades do sistema, até o arquivamento e

manutenção dos requisitos dos interessados ao longo do ciclo de vida do produto (INCOSE, 2006).

A Análise dos Requisitos busca obter uma descrição técnica das características que o sistema deverá ter para atender aos requisitos dos interessados. Como parte do processo de análise, os requisitos entre as partes interessadas, funções, desempenho, condições, restrições, premissas e objetivos são identificados e são transformados em um conjunto completo e consistente de requisitos técnicos (INCOSE, 2006).

A Engenharia de Sistemas propõe e seleciona soluções baseada nos atributos de um sistema. Estes são medidos e comparados por Medidas de Efetividade (*Measures of Effectiveness* - MOEs), que são as métricas que os interessados utilizarão para medir sua satisfação com relação à solução proposta e selecionada para o sistema(LARSON et al., 1999).

2.4. Engenharia de Requisitos no Contexto de Sistemas Eletrônicos Embarcados

De acordo com (HALLIGAN, 1993), a Engenharia de Requisitos lida com a criação, captura, validação, especificação e rastreabilidade de requisitos. Começa com a declaração de uma necessidade, que seguirá até a definição de uma solução (sistema), chegando aos níveis relacionados à especificação de elementos que fazem parte do sistema.

A elaboração de um bom conjunto de requisitos é uma tarefa crítica para o sucesso de um projeto, pois é nele onde as necessidades e problemas estarão claramente definidos e registrados. Os requisitos são a linha vital de comunicação entre os desenvolvedores do projeto e os interessados (DOORS, 2008).

Dentre as várias definições da Engenharia de Requisitos e de termos encontrados na literatura, destacamos alguns que são considerados fundamentais para o presente trabalho:

- **Requisito:** um elemento identificável de uma especificação de função que pode ser validada e contra o qual uma implementação pode ser verificada (ARP 4754, 2010).
- **Rastreabilidade de Requisitos:** atributo do requisito que liga cada requisito ao seu requisito de mais alto nível, dentro do conjunto dos requisitos. Isto possibilita a derivação de uma Árvore de Requisitos, a qual demonstra a coerência dos requisitos (ECSS-E-ST-10-06C, 2009).
- **Validação de requisitos:** a determinação de que os requisitos para um produto estão adequados e completos (resposta à pergunta: estamos construindo o sistema / função / item adequado?) (ARP 4754, 2010).
- **Verificação de requisitos:** a avaliação de uma implementação de requisitos para determinar que os requisitos foram atendidos (resposta à pergunta: construímos o sistema / função / item correto?) (ARP 4754, 2010).

De acordo com (LOUREIRO, 2012) os requisitos dos interessados podem ser classificados como **capacidades e restrições**. As **capacidades** são as funções que o sistema realiza, quando é solicitado por um usuário ou outro sistema, ou seja, em termos de requisitos, é algo que os interessados querem ser capazes de realizar. As **restrições** modificam um requisito ou conjunto de requisitos, limitando as possíveis soluções, sendo geralmente ligadas a aspectos de segurança e desempenho, por exemplo, a Confiabilidade.

2.5. Confiabilidade

Uma das maneiras de se definir confiabilidade (*Reliability*), como descrito na ARP 4754A, é a probabilidade de um item desempenhar a sua função, dentro de condições previamente especificadas, por um determinado intervalo de tempo.

Algumas definições e conceitos são importantes para o estudo da confiabilidade, tais como Manutenabilidade (*Maintainability*), Disponibilidade

(*Availability*), Redundância (*Redundancy*) e Tempo Médio entre Falhas (*Mean Time Between Failures*- MTBF).

(SOUZA et al., 2005) apresenta as seguintes definições:

- **Manutenabilidade:** A probabilidade de um sistema ou dispositivo ser retido na ou restaurado para a condição operacional em um intervalo de tempo específico com recursos e procedimentos prescritos.
- **Disponibilidade:** A probabilidade de um sistema ser capaz de exercer a sua função requerida em um determinado instante de tempo.
- **Redundância:** A propriedade de um dispositivo ou sistema ter mais de um meio de executar sua função.
- **Tempo Médio Entre Falhas (*Mean Time Between Failures* – MTBF):** Tempo esperado durante o qual o componente operará corretamente entre falhas.

A (IEC TS 62396-1, 2012) apresenta ainda a definição de MTBUR:

- **Tempo Médio Entre Remoções não Programadas (*Mean Time Between Unscheduled Removals* – MTBUR):** tempo médio entre as remoções não programadas de um equipamento ou sistema.

A análise da confiabilidade de determinado sistema pode ser tanto qualitativa quanto quantitativa. No segundo caso, a mais importante característica do sistema é a chamada “Taxa de Falhas”. Considerando a natureza probabilística da análise, pode-se entender esse parâmetro como uma descrição estatística de quando o sistema ou componente irá falhar.

2.5.1. Confiabilidade no Contexto do Ambiente de Radiações Ionizantes

Para se obter um sistema aeroespacial que opere em um ambiente de radiações ionizantes de maneira confiável, podemos escolher basicamente dois tipos de abordagem: 1) uma abordagem de prevenção a radiação, que consiste na aquisição de componentes chamados de robustecidos ou resistentes à

radiação, de modo a se minimizar ou até evitar a ocorrência de SEUs, ou 2) uma abordagem de robustez a radiação, utilizando técnicas de mitigação via hardware ou software para que o sistema mantenha seu funcionamento mesmo com a ocorrência de SEUs.

Prevenção a Radiação

A prevenção a radiação é um método de projeto, construção e teste de componentes eletrônicos com o objetivo de torná-los resistentes aos danos e mau funcionamento causados pela radiação. Este método está englobado na abordagem para aumento de confiabilidade chamada de *fault avoidance*, que no contexto deste trabalho tratam de reduzir ou evitar a ocorrência das falhas por meio da diminuição da susceptibilidade do componente ou resposta do mesmo ao ser atravessado por partículas ionizantes (SOUZA et al., 2005; HEIDERGOTT, 1995). Entretanto, há diversas restrições no uso de tais componentes envolvendo parâmetros como disponibilidade, potência requerida, volume, obsolescência, desempenho, prazo de entrega e custo (MURAOKA, 2010).

Robustez a Radiação

A abordagem de robustez a radiação busca mitigar os efeitos da ocorrência de SEUs no sistema por meio de técnicas implementadas via hardware e/ou software. Este conceito está englobado na abordagem para aumento de confiabilidade chamada de *fault tolerance*, que é o projeto de sistemas que possam tolerar as falhas de componentes e assim manter sua funcionalidade (SOUZA et al., 2005). No caso do presente trabalho, a falha ou erro é a manifestação do SEU induzido por radiação ionizante, de modo a não exibir uma falha funcional (HEIDERGOTT, 2005).

Há vários tipos de esquema de robustez aplicáveis aos SEUs, como os esquemas de detecção e correção de erros (*Error Detection And Correction* - EDAC), Watchdog Timers e redundância. No entanto, Efeito a (HEIDERGOTT, 2005).

2.5.2.Métodos e Técnicas de Análise de Confiabilidade

Diversas ferramentas são usadas para realizar uma análise sistemática e completa da confiabilidade de sistemas complexos, como é o caso de sistemas eletrônicos embarcados aeroespaciais. Algumas destas ferramentas são descritas a seguir.

2.5.2.1. FMEA/FMECA

A Análise de Modos de Falha e seus Efeitos (*Failure Mode and Effects Analysis*– FMEA) e a Análise de Modos de Falha, seus Efeitos e sua Criticalidade (*Failure Modes, Effects and Criticality Analysis*- FMECA), são metodologias destinadas a identificar os modos de falha potenciais para um produto ou processo, analisar o risco associado a estes modos de falha, ordenar os modos em termos de importância e identificar e tomar medidas corretivas para tratar os itens mais críticos. O propósito, terminologia e detalhes podem variar de acordo com o tipo (FMEA de processo, de item ou de sistema, por exemplo), mas a metodologia básica é similar para todas (ECSS-Q-ST-30-02C, 2009).

De acordo com a norma ECSS-Q-ST-30-02C, a FMECA é semelhante à FMEA, com o adicional de ser uma análise de criticalidade. Os modos de falha são identificados na FMEA, sendo que a FMECA adicionalmente considera a criticalidade envolvida.

A FMEA/FMECA é organizada de modo a conter diversos dados, como por exemplo, (ARP 4761, 1996):

- Identificação do componente, sinal e/ou função;
- Modos de falha e taxas de falha associadas ao hardware em questão;
- Efeitos da falha (para o nível acima, por exemplo, uma FMEA de item descreve o efeito da falha no sistema);
- Detectabilidade e meios de detecção;
- Ações compensatórias;

- Fase de operação/voo em que acontece o modo de falha;
- Severidade dos efeitos da falha;

A FMEA/FMECA consiste basicamente em uma análise "*bottom-up"* considerando cada modo de falha simples e analisando seus efeitos no produto, sistema ou processo sob análise. A análise se aplica para o nível de onde os efeitos da falha são observados (componente, item ou sistema) (ARP 4761, 1996; ECSS-Q-ST-30-02C, 2009).

2.5.2.2. FMES

Os resultados de uma FMEA podem ser usados para geração de um Sumário de Modos de Falha e seus Efeitos (*Failure Modes and Effects Summary* - FMES). Este por sua vez suporta outras técnicas de análise, dentro do processo de Apreciação de Segurança do Sistema (*System Safety Assessment* – SSA) em aeronaves, como a Análise de Árvore de Falhas (*Fault Tree Analysis*– FTA) (ARP 4761, 1996).

O FMES é um agrupamento dos modos de falhas simples que produzem o mesmo efeito (ou seja, cada efeito de falha contém um agrupamento separado de modos de falhas simples). Pode ser realizado pelo fabricante de uma aeronave, integrador do sistema ou fornecedor do equipamento. Deve haver uma coordenação com o usuário do sistema para que a FMES trate adequadamente a necessidade de entradas para as análises em um nível acima via FMEA/FMECA ou FTA (ARP 4761, 1996).

2.5.2.3. FTA

A Análise de Árvore de Falhas (*Fault Tree Analysis*– FTA) é um método que usa lógica booleana para evidenciar a relação entre os modos de falha e os efeitos das falhas. As portas lógicas usadas mais comumente são a porta "E" e a "OU". Uma porta "E" representa uma condição na qual todas as condições de entrada devem ocorrer para que a saída seja considerada um evento para o próximo nível da árvore. A porta "OU", por sua vez, representa que, se

qualquer um dos eventos de entrada ocorrer, haverá uma saída a ser considerada no nível mais alto (ARP 4761, 1996). É uma análise lógica que pode se tornar probabilística, uma vez que as entradas da árvore, que são os eventos que representam os modos de falha, têm uma probabilidade de ocorrência. Assim, o evento topo, terá uma probabilidade de ocorrência associada a estas probabilidades e o tempo de operação; este resultado em geral está associado ao cumprimento ou não de um requisito.

2.5.2.4. RBD

O Diagrama de Blocos de Confiabilidade (*Reliability Block Diagram*– RBD) é um método que usa lógica booleana para ilustrar a configuração de um sistema onde é possível ver o caminho onde há dependência de certos elementos que compõem o sistema, dispostos em série, paralelo, ou configurações mistas, responsáveis pela execução de uma função. É uma análise lógica que pode se tornar probabilística através do estabelecimento de uma probabilidade de sucesso de cada componente responsável pela função, e seus correspondentes efeitos na probabilidade geral de sucesso na execução daquela função (RELIASOFT, 2012).

A diferença fundamental entre as FTA e RBD é que o foco da RBD é nas combinações de sucesso dos blocos (probabilidade de funcionamento) enquanto que as FTA focam nas combinações de falha (probabilidade de falha de cada evento). Ambas são consideradas análises estáticas, ou seja, tradicionalmente as taxas de falhas têm probabilidades fixas ou dependentes do tempo, mas sem dinâmica. De um modo geral, uma metodologia pode ser convertida na outra.

2.6. Normas e Recomendações do Setor Espacial e Aeronáutico

As normas do setor espacial e aeronáutico são usadas como instrumento para o projeto de sistemas embarcados de modo a se ter uma abordagem uniformizada e focada em parâmetros como confiabilidade e qualidade. Sua

correta utilização proporciona altos níveis de confiabilidade e segurança em um projeto espacial e aeronáutico. Algumas das normas lidam com o problema de robustez à radiação e, portanto, são aplicáveis ao escopo do presente trabalho e são mencionadas a seguir.

2.6.1.Normas da ECSS

As normas da ECSS - *European Cooperation for Space Standardization* são publicadas com o intuito de manter uma padronização dos processos de gerenciamento, engenharia e garantia de produto de projetos e aplicações da ESA – *European Space Agency* e da indústria espacial européia. Como premissa, as normas devem sempre que possível descrever a necessidade a ser satisfeita, sem prescrever as características do produto. Estão organizadas nos seguintes níveis:

- Nível 0 (ECSS-P-00) – descreve a política e os objetivos do sistema de normas ECSS e sua arquitetura junto com as regras para criação, validação e manutenção dos documentos.
- Nível 1 (ECSS-M-00, ECSS-Q-00, ECSS-E-00) – descreve a estratégia no domínio específico, dando uma visão geral dos requisitos e interface entre os documentos e elementos no nível 2.
- Nível 2 (ECSS-M-10, ECSS-Q-10, etc.) – descreve os objetivos e funções requeridas para os aspectos do domínio em questão (organização do projeto, garantia da qualidade, engenharia de sistemas, etc.).
- Nível 3 – descreve métodos, procedimentos e ferramentas recomendadas para cumprir com os requisitos dos documentos do nível 2. Adicionalmente, definem as restrições e requisitos para interfaces e desempenho do produto ou atividade especifica.

Como exemplo de normas deste conjunto aplicáveis ao presente trabalho, temos:

- **ECSS-E-ST-10C** *System Engineering General Requirements* (Requisitos Gerais para a Engenharia de Sistemas), especifica os requisitos de implementação da Engenharia de Sistemas para o desenvolvimento de produtos e sistemas espaciais. Destacam-se dentre seus objetivos principais: implementar os requisitos para a Engenharia de Sistemas para assegurar uma base técnica robusta e minimizar o risco técnico e o custo do projeto de sistemas e produtos espaciais; especificar as tarefas essenciais de Engenharia de Sistemas, seus objetivos e saídas; implementar a integração e o controle de disciplinas de engenharia.
- **ECSS-E-ST-10-04C** *Space Environment* (Ambiente Espacial), define o ambiente natural do espaço e modelos gerais para caracterizar tais ambientes para um projeto.
- **ECSS-E-ST-10-12C** *Methods for the Calculation of Radiation Received and its Effects, and a Policy for Design Margins* (Métodos para Cálculo da Radiação recebida e seus Efeitos, e uma Política para Margens de Projeto), cobre os métodos para o cálculo da radiação recebida e seus efeitos, e uma política para margens de projeto. Considera todos os efeitos do ambiente natural do espaço, como Dose Total de Ionização e Danos por Deslocamento.
- **ECSS-Q-60-15C** *Radiation Hardness Assurance - EEE Components* (Garantia de Resistência à Radiação – Componentes EEE (Elétricos Eletrônicos e Eletromecânicos)), especifica os requisitos para assegurar a Garantia de Resistência à Radiação (RHA) de projetos espaciais, abrangendo TID, DD e SEEs.

2.6.2. Normas da NASA

As normas da NASA – *National Aeronautics and Space Administration* têm como objetivo aumentar as capacidades de engenharia da NASA provendo padrões técnicos para atender às necessidades da agência. Os documentos

têm caráter de melhores práticas e recomendações aplicáveis ao escopo deste trabalho:

O guia **NASA *Reference Publication* 1350** *The Natural Space Environment: Effects on Spacecraft* (O Ambiente Natural do Espaço - Efeitos sobre Espaçonaves) provê uma visão geral do ambiente natural do espaço e seus efeitos em projetos de sistemas espaciais. Seu objetivo principal é contribuir para um melhor entendimento do ambiente espacial para se minimizar riscos e custos, auxiliando na definição do ambiente de radiação de partículas.

O guia **NASA *Reference Publication* 1390** *Spacecraft System Failures and Anomalies Attributed to the Natural Space Environment* (Falhas em Sistemas de Espaçonaves e Anomalias Atribuídas ao Ambiente Natural do Espaço) provê uma visão geral dos efeitos em vários subsistemas de espaçonaves, apresentando mais de 100 casos de falhas em espaçonaves e anomalias documentadas de 1974 a 1994 que foram atribuídas ao ambiente natural do espaço. O documento é um valioso registro dos efeitos de radiação por partículas em sistemas espaciais embarcados que causaram SEEs, além dos efeitos causados por outros fenômenos do ambiente espacial.

O documento emitido pela **NASA 431-REF-000273 *Single Event Effect Criticality Analysis*** (Análise de Criticalidade de Efeitos de Evento Único) é um documento cujo objetivo é ser um guia para a análise dos efeitos dos SEEs baseado em critérios de criticalidade, desempenho, disponibilidade e custo. Como mencionado em seu prefácio, o documento pretende ser uma ferramenta para projeto de sistemas tolerantes à radiação, geração de requisitos de robustez à SEEs, verificação de projeto, e validação de requisitos.

2.6.3.Normas e Recomendações Aeronáuticas

A indústria aeronáutica, por tratar com sistemas complexos e/ou altamente integrados, utiliza uma série de normas e padrões para desenvolvimento de sistemas, software e hardware. Antes de apresentar algumas das normas que contêm conceitos e ferramentas que são aplicáveis às recomendações para

garantia da robustez de sistemas eletrônicos embarcados a SEUs causados por partículas ionizantes, é interessante contextualizá-las no processo de certificação aeronáutica civil, que reconhece legalmente o uso de diversas das normas mencionadas a seguir.

2.6.3.1. Normas no Contexto da Certificação Aeronáutica Civil

A certificação do projeto de aeronaves civis é uma obrigação legal, prevista na Lei 7.565, de 19 de dezembro de 1986 (Código Brasileiro de Aeronáutica), mais especificamente em seu Capítulo IV – Do Sistema de Segurança de Vôo, artigo 68. O projeto de aeronaves civis que operam no transporte de passageiros deve ser certificado por meio de um processo estabelecido pela Agência Nacional de Aviação Civil – ANAC, de maneira a atender aos Regulamentos Brasileiros de Aviação Civil – RBAC aplicáveis ao projeto em questão. O objetivo da certificação na área de aviação civil é estabelecer um nível mínimo de segurança apropriado a cada produto aeronáutico por meio de requisitos e confirmar técnica e legalmente por meio de testes, análises, ensaios em voo, simulações, etc. que o projeto atende aos níveis mínimos de segurança estabelecidos pelos requisitos.

Os requisitos de certificação do projeto de produtos aeronáuticos são divididos conforme tipo e categoria do produto, como por exemplo, o RBAC 33 que trata dos requisitos para certificação de motores aeronáuticos, e o RBAC 27 que contém requisitos para a certificação do projeto de aeronaves de asas rotativas.

O RBAC 25 é o conjunto que demanda o maior rigor para o projeto, pois é aplicável aos aviões de grande porte, classificados como aeronaves Categoria Transporte (com configuração acima de 19 passageiros e peso máximo de decolagem acima de 8620 kg, de acordo com o RBAC 23.3). Este regulamento por sua vez adota o texto integral do *14 Code of Federal Regulations* (CFR) Part 25 da *Federal Aviation Administration* (FAA). Para a aviação civil, as aeronaves de Categoria Transporte são as que operam nas rotas mais longas, em quase todas as regiões do globo, nas maiores altitudes e transportam o

maior número de passageiros. Estes são fatores que aumentam a criticalidade dos sistemas aeronáuticos que fazem parte destes aviões, daí a necessidade de requisitos mais rigorosos.

A ANAC emite Instruções Suplementares – IS e reconhece as *Advisory Circulars* – ACs, emitidas pela FAA, para auxiliar e guiar os requerentes à certificação dos projetos no cumprimento dos requisitos estabelecidos nos RBACs. Estes documentos descrevem os meios aceitáveis e estabelecidos pela autoridade aeronáutica para cumprimento com os requisitos de certificação. Cabe ressaltar que o requerente à certificação pode, alternativamente, propor outros meios de cumprimento.

As autoridades aeronáuticas emitem também outros documentos que têm caráter informativo e de alerta a comunidade aeronáutica, como por exemplo os SIB (*Safety Information Bulletin*) da EASA e os SAFOs (*Safety Alert For Operators*) da FAA.

As normas da indústria aeronáutica estão inseridas neste contexto como meios aceitáveis para demonstração de cumprimento com os requisitos de certificação a serem adotados pelos requerentes. Neste caso, os documentos emitidos pelas autoridades, como as ACs e IS, reconhecem formalmente tais normas.

2.6.3.2. Normas da Indústria Aeronáutica

A *Aerospace Recommended Practice* **ARP-4761** *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment* (Diretrizes e Métodos para Conduzir o Processo de Análise da Segurança em Sistemas e Equipamentos Aeroembarcados Civis) é uma norma internacional publicado pela SAE (*Society of Automotive Engineers*), reconhecida pela AC 25.1309. Seu objetivo é ser um guia para o processo de Apreciação de Segurança (*Safety Assessment*), o qual consiste de uma análise sistemática e abrangente com intuito de demonstrar que um projeto é seguro quanto a falhas (*fail-safe design*).

A **ARP-4754A** *Recomendações for Development of Civil Aircraft and Systems* (Diretrizes para o Desenvolvimento de Aviões e Sistemas Civis) é uma norma da SAE com o objetivo de ser um guia para autoridades certificadoras e para as empresas requerentes à certificação, reconhecida pela AC 20-174. Estabelece os controles de garantia do processo (*process assurance*), que variam de rigor conforme o Nível de Garantia de Desenvolvimento (*Development Assurance Level* - DAL). O rigor é de acordo com a severidade da condição de falha funcional, que é definido através do uso de ferramentas como a Análise Funcional de Perigos (*Functional Hazard Assessment* - FHA), definido na ARP 4761.

A **DO-178C** *Software Considerations in Airborne Systems and Equipment Certification* (Considerações de Software sobre a Certificação de Sistemas e Equipamentos Aeroembarcados) é uma norma publicada pela Comissão Rádio-Técnica para a Aeronáutica (*Radio Technical Comission for Aeronautics*-RTCA), e reconhecida pela AC 20-115C. Contém diretrizes de desenvolvimento e produção de software embarcado que exerce suas funções com um nível de confiança compatível com os requisitos de aeronavegabilidade.

A **DO-254** *Design Assurance Guidance for Airborne Electronic Hardware* (Diretrizes de Garantia de Projeto para Hardware Eletrônico Aeroembarcado), reconhecida pela AC 20-152, contém diretrizes de desenvolvimento e produção de hardware eletrônico aeroembarcado para que o mesmo execute sua função de forma segura, em um ambiente especificado.

A **IEC Technical Specification 62396-1** *Accommodation of Atmospheric Radiation Effects Via Single Event Effects within Avionics Electronic Equipment* (Acomodação dos Efeitos de Radiação Atmosférica por Efeitos de Evento Único em Equipamentos Eletrônicos Aviônicos) é uma norma publicada pela IEC (*International Electrotechnical Comission*). Seu com objetivo é ser um guia para os efeitos de radiação atmosférica para sistemas eletrônicos embarcados operando em altitudes até 18,3 km. Define o ambiente de radiação, os efeitos

deste ambiente na eletrônica e considerações de projeto para acomodar e tolerar tais efeitos nos sistemas eletrônicos embarcados.

Estas normas serão usadas a seguir

3. FORMULAÇÃO DO PROBLEMA E ABORDAGENS PARA A SUA SOLUÇÃO

3.1. Formulação do Problema

Dentre os diversos efeitos da radiação ionizante em sistemas eletrônicos embarcados descritos no capítulo 2 (TID, DD, e os tipos de SEE), o SEU será objeto deste trabalho.

A potencial susceptibilidade de sistemas eletrônicos embarcados aeroespaciais à SEU gera riscos de falhas com consequências catastróficas para aeronaves ou ainda a perda de missão de satélites. Estas falhas são geradas por radiações ionizantes nos circuitos eletrônicos de satélites e aeronaves.

De acordo com (NASA RP 1390, 1996), os efeitos não destrutivos, como é o caso dos SEUs, são mais comuns, e podem levar à perda de um sistema ou ainda à perda da missão, se não forem evitados ou ações mitigatórias não forem tomadas.

Fatores como: 1) a integração por exemplo, a Aviônica Modular Integrada, ou *Integrated Modular Avionics* – IMA; 2) a complexidade; e 3) a criticalidade das funções realizadas por sistemas eletrônicos embarcados aeroespaciais, podem aumentar a susceptibilidade e ainda a gravidade dos efeitos de SEUs. Na sua implementação, tais sistemas fazem uso cada vez maior de memórias, que por sua vez trabalham em frequências maiores e tensões menores, potencialmente diminuindo a carga crítica necessária para ocorrência de SEUs nestes dispositivos.

Os aviões estão voando a altitudes cada vez maiores, devido a restrições de eficiência e custo, e vôos em rotas por regiões polares são cada vez mais frequentes. (NATIONAL, 2008). Sobre o sul do território brasileiro, é esperado um ambiente ainda mais severo para os satélites de órbita baixa, e potencialmente severo para as aeronaves que voam em grandes altitudes, por conta de uma potencial maior incidência de partículas ionizantes devido à SAA (FEDERICO, 2011).

Em face do exposto acima, o projeto de um sistema aeroespacial embarcado deve considerar que este estará operando em um ambiente de radiações ionizantes com potencial de causar SEUs com consequências graves. Sendo assim, esta ameaça deve ser tratada por meio de uma abordagem uniformizada e focada em garantir um sistema com confiabilidade adequada, mantendo a integridade de suas funções críticas.

3.2. Abordagens para a sua Solução

As possíveis abordagens para a solução do problema de se garantir a prevenção ou robustez à SEUs no projeto de sistemas eletrônicos embarcados aeroespaciais exposto acima podem envolver:

- Modelamento e realização de experimentos (testes), realizados por meio de equipamentos.
- Simulações e Modelamento e simulações computacionais, realizadas por meio de softwares.
- Modelamento e análise teórica, realizadas por meio de equações.
- Pesquisa e análise da bibliografia existente, propondo o uso de documentos, o uso com adaptações, alterações ou complementações.

3.3. Abordagem Escolhida

A abordagem escolhida é a pesquisa e análise da bibliografia existente, com relação ao tópico prevenção ou robustez à ocorrência de SEUs causados por radiação ionizante, visando propor adaptações, alterações e/ou complementações.

Para o estudo da garantia da robustez à ocorrência de SEUs nos sistemas embarcados, foi realizada pesquisa na bibliografia e nos documentos emitidos pelas principais instituições do setor espacial (NASA, ESA, etc.) e aeronáutico (FAA, EASA, RTCA, etc.).

A documentação consultada, normas e recomendações dos setores espacial e aeronáutico são discutidas, com o objetivo de identificar os pontos onde sao recomendadas a adoção das normas e recomendações e os pontos onde foram identificadas melhorias. Na seqüência, são propostas recomendações de projeto para garantia de prevenção ou robustez à SEUs causados por partículas ionizantes em sistemas eletrônicos embarcados, que podem contribuir para a melhoria dos processos de engenharia de sistemas no INPE relacionados ao fenômeno.

O próximo capitulo traz uma breve discussão de alguns dos principais aspectos envolvidos na solução do problema abordado e que, portanto, devem ser considerados na elaboração das recomendações de projeto para garantia de robustez a SEUs causados por partículas ionizantes em sistemas eletrônicos embarcados.

4. EFEITOS DAS RADIAÇÕES IONIZANTES EM SISTEMAS ELETRÔNICOS EMBARCADOS AEROESPACIAIS

Para compreensão dos efeitos de SEUs em sistemas eletrônicos embarcados, é necessário abordar diversos aspectos e disciplinas, com o objetivo final de se obter um nível de robustez ao efeito que seja aceitável.

Este capítulo discute brevemente alguns dos principais aspectos que devem ser considerados no desenvolvimento de sistemas eletrônicos embarcados aeroespaciais preventivos ou robustos a SEUs e que, portanto, devem ser considerados para as recomendações propostas por este trabalho. São abordados os aspectos de ambiente de radiação ionizante, a prevenção ou robustez de sistemas eletrônicos embarcados aeroespaciais a SEUs e o impacto na confiabilidade e as estratégias de mitigação de SEUs mais usadas.

Uma vez que o ambiente de radiações ionizantes para sistemas eletrônicos embarcados espaciais difere significantemente do ambiente para sistemas eletrônicos embarcados aeronáuticos, serão abordados separadamente.

4.1. Considerações Sobre o Ambiente de Radiações Ionizantes Para Sistemas Eletrônicos Embarcados Espaciais

Dada a experiência do INPE em projeto de satélites de órbitas baixas e os seus projetos atuais de satélite serem esperados de operar neste ambiente, as recomendações para garantia de prevenção ou robustez a SEUs causados por partículas ionizantes deste trabalho são focadas aos sistemas eletrônicos embarcados espaciais instalados em satélites que operarão em ambiente de órbitas baixas.

De acordo com (IADC, 2007) a região de órbitas baixas terrestres (*Low Earth Orbit* ou LEO) se estende da superfície terrestre até uma altitude de 2.000 km.

As partículas ionizantes que são potencialmente causadoras de SEUs em sistemas eletrônicos embarcados nestas órbitas são: partículas de radiação galáctica, prótons do cinturão de radiação de Van Allen interno e prótons de

Eventos de Partículas Solares Energéticas (SEPE) (LABEL et al., 1996; BARTH et al., 2003).

A blindagem de uma espaçonave interage com as partículas das fontes descritas a seguir, sendo, portanto, um elemento a se considerar na definição do espectro de partículas ionizantes. Em geral, as blindagens são de alumínio, e, de modo a simplificar o modelamento dos espectros, assume-se uma espessura padrão para todas as regiões da espaçonave (ECSS-E-HB-10-12C, 2010).

4.1.1. Radiação Galáctica

O campo magnético terrestre reduz o fluxo de partículas de radiação galáctica, no entanto a blindagem é apenas parcial. O fluxo destas partículas, composto de prótons e íons pesados de numero atômico 1 até 92, pode ser considerado pequeno, porém a faixa de energia (de dezenas de MeV chegando a até TeV) de elementos pesados como o ferro fazem com que estas partículas produzam intensa ionização ao longo do seu caminho através dos componentes eletrônicos (LABEL et al., 1996; BARTH et al., 2003).

Diversos fatores influenciam o ambiente de radiação galáctica para sistemas eletrônicos embarcados em satélites de órbita baixa. O ciclo solar influencia o fluxo de maneira inversa, ou seja, no mínimo do ciclo solar elas atingem o fluxo máximo e no máximo do ciclo solar o fluxo é mínimo. A altitude e inclinação da órbita são fatores que influenciam seu fluxo, sendo que a inclinação é o fator primário nesta variação (LABEL et al., 1996).

4.1.2. Prótons e Íons Pesados de Eventos de Partículas Solares Energéticas - SEPEs

Os prótons e íons pesados de SEPEs poderão atingir os satélites, dependendo da posição do SEPE no Sol. Os eventos podem durar dias e as partículas são aceleradas com energias tipicamente alcançando centenas de MeV, e terão maior influência em satélites com grandes altitudes e inclinações (DYER, 2001; BARTH et al., 2003).

Para os SEPEs, a proteção que o campo magnético da Terra vai proporcionar contra partículas solares também dependerá da inclinação da órbita e, em menor escala, da altitude. Conforme a altitude aumenta, a exposição de partículas solares aumenta gradualmente. Entretanto, o efeito que a inclinação tem na exposição destas partículas é muito mais importante. Conforme a inclinação aumenta, aumenta também o tempo em que o satélite estará exposto a regiões em que estas partículas têm maior acesso pois, conforme a inclinação atinge regiões polares, estas estão fora das linhas de campo magnético fechadas da Terra, expondo o satélite. Em condições magnéticas normais, os satélites com inclinação abaixo de 45 graus serão blindados de prótons de partículas solares. Em situações perturbadas de eventos solares, a pressão na magnetosfera fará com que as linhas de campo magnético da Terra se comprimam, conseqüentemente as partículas solares e cósmicas alcançam altitudes e regiões não normalmente atingíveis. O mesmo pode ocorrer para situações de grandes tempestades geomagnéticas (LABEL et al., 1996; BARTH et al., 2003).

4.1.3.Prótons dos Cinturões de Radiação de Van Allen

Os satélites de órbita baixa encontram as porções interiores do cinturão de radiação de Van Allen, sendo que os prótons de alta energia do cinturão interior são predominantes nesta órbita (BARTH et al., 2003). Os satélites de órbita baixa geralmente passam várias vezes por dia por estas regiões (LABEL et al., 1996). Os satélites de órbita baixa de grande inclinação (acima de 60º) irão atingir também o cinturão de radiação mais externo, no entanto este é composto majoritariamente de elétrons, e a quantidade de prótons em comparação ao cinturão interno é pequena (DYER, 2001).

O fluxo de prótons na região de órbitas baixas pode variar de acordo com o ciclo solar e os SEPEs, atingindo energias de até 600 MeV. Em alguns casos, SEPEs podem gerar aumento do fluxo de partículas e, embora os SEPEs em geral durem até dias, este fluxo aumentado pode durar até um ano (DYER, 2001). Tempestades geomagnéticas e Solares, a altitude e inclinação da órbita

também influenciam grandemente nestes fluxos (BARTH et al., 1996), além da influência da região da Anomalia do Atlântico Sul.

As partículas aprisionadas no cinturão de radiação de Van Allen interno, ao realizarem seu complexo movimento ao longo das linhas de campo magnético terrestre, podem chegar a até 100 km de altitude na região da Anomalia do Atlântico Sul. Por comparação, a mesma partícula no hemisfério norte alcançaria altitudes em torno de 1000 km (MORO, 2011).

O impacto do fluxo intenso de partículas ionizantes nos sistemas eletrônicos espaciais pode ser constatado pelos casos ilustrados a seguir, onde a região da SAA é evidenciada pelo registro de ocorrência de SEUs.

4.1.4.Exemplos de Ocorrências em Satélites

O satélite UoSAT-2, lançado em 1984, com órbita polar a 700 km da superfície terrestre, registrou 7995 SEUs de setembro de 1988 a maio de 1992 em memórias nMOS, modelo TMS4416 da Texas Instruments conforme mostrado na Figura 4.1 (DYER, 2001).

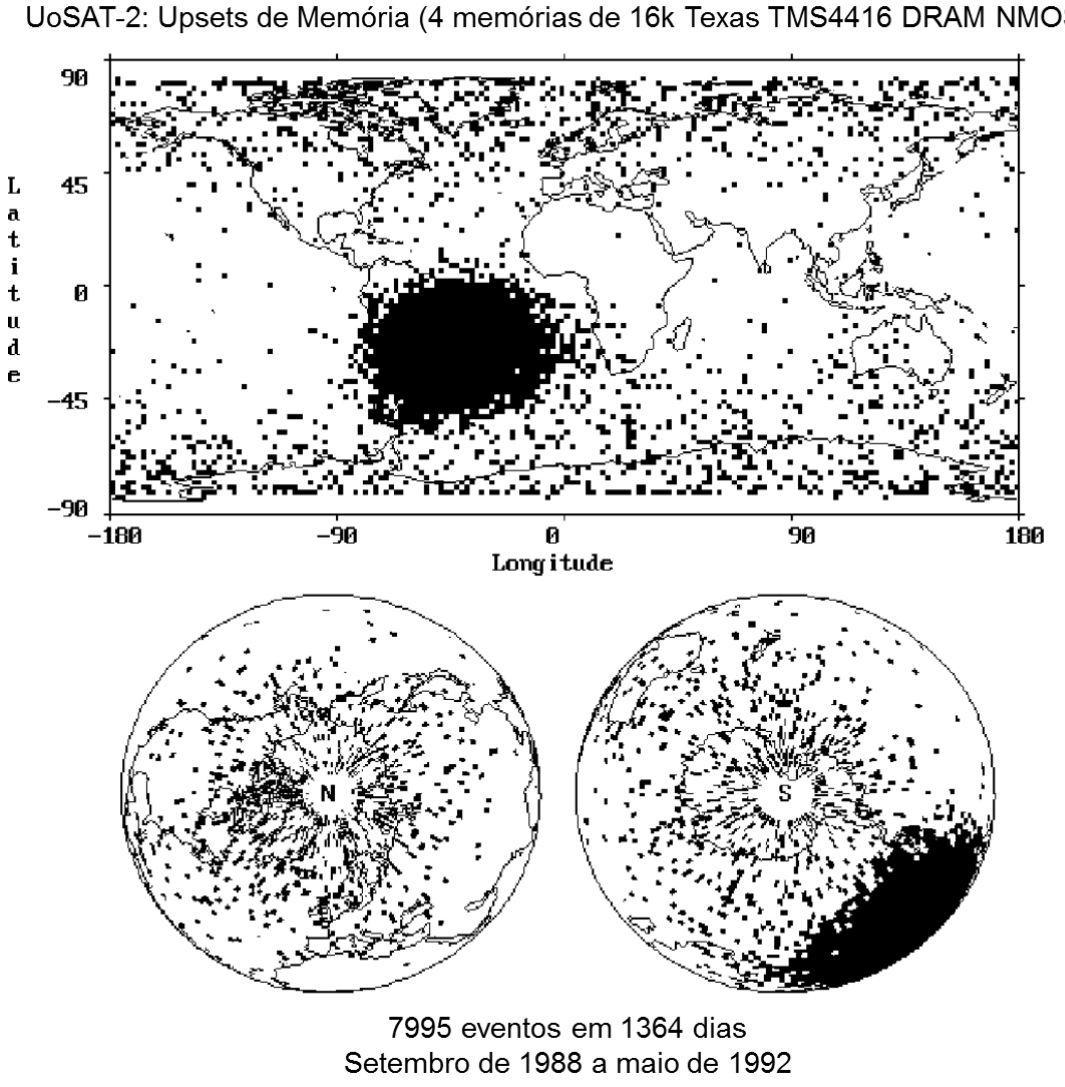

Figura 4.1: Distribuição geográfica de SEUs em memórias do satélite UoSAT-2
Fonte: Adaptado de DYER (2001).

O satélite ARGOS - *Advanced Research and Global Observation Satellite* continha o experimento chamado *Advanced Space Computing and Autonomy Testbed*, com o intuito de comparar as abordagens de confiabilidade baseadas em componentes robustecidos contra radiação (*radiation hardened*) e em componentes comerciais com arquitetura de software tolerante à falhas (*fault tolerant*). A Figura 4.2 mostra os resultados das abordagens: à esquerda, as ocorrências de SEU na placa RH3000 robustecida contra radiação e à direita,

as ocorrências na placa R3081 com software visando tolerar as falhas (LOVELLETTE et al., 2001).

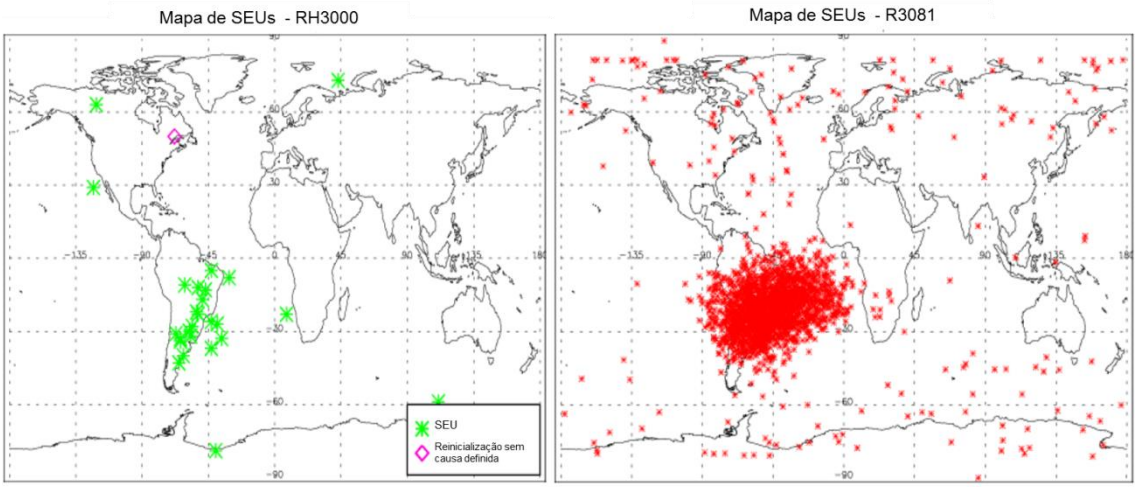

Figura 4.2: Distribuição geográfica de SEUs registrados nas placas do experimento *Advanced Space Computing and Autonomy Testbed* do satélite ARGOS
Fonte: adaptado de LOVELLETTE et al. (2001).

Este último será usado como caso de estudo de um sistema espacial, mostrado no capítulo 6.

4.2. Considerações Sobre o Ambiente de Radiações Ionizantes Para Sistemas Eletrônicos Embarcados Aeronáuticos

A altitude e a latitude de operação são parâmetros fundamentais para o ambiente de radiações ionizantes, pois conforme mencionado no capítulo 2, o fluxo das partículas ionizantes na atmosfera terrestre varia consideravelmente por conta destes parâmetros.

A máxima altitude operacional dos projetos de aviões de Categoria Transporte é em torno de 13,1 km (43 kft), como é o caso, por exemplo, do Boeing 787 (13,137 km, ou 43,1 kft) e o Airbus A380 (13 km ou 43 kft). Os aviões chamados comercialmente de executivos, embora não transportem grande número de passageiros comparativamente aos aviões supramencionados, são considerados aviões de Categoria Transporte principalmente devido ao peso

máximo de decolagem e propulsão a jato. Em geral, são capazes de voar em altitudes um pouco maiores, em torno de 15,5 km (51 kft), como por exemplo, o Gulfstream GV (15,5 km) e o Falcon 7X (15,5 km) (FAA, 2013). Estes se aproximam do máximo de Pfotzer (18288 m ou 60 kft), onde o fluxo de partículas secundárias com potencial de causar SEUs atinge seu valor máximo.

As rotas polares, realizadas pelos aviões de Categoria Transporte, são cada vez mais freqüentes, o que aumenta a exposição dos sistemas eletrônicos aos fluxos mais intensos de partículas secundárias. No fim da década de 1990, as companhias aéreas começaram a voar por rotas polares entre a América do Norte e Ásia, de modo a se obter tempos menores de viagem, menor consumo de combustível e consequente maior capacidade de transporte de passageiros e carga (CARLSON, 2011). A Tabela 4-1 mostra o acréscimo dramático no trafego pelas rotas polares de 2003 a 2011:

Tabela 4-1 – Número de voos realizados em rotas polares entre 2003 e 2011

Ano	Quantidade de voos realizados em rotas polares
2003	884
2004	2053
2005	3731
2006	5308
2007	6930
2008	8017
2009	8549
2010	9683
2011	Acima de 10000

Fonte: CARLSON (2011).

As operações de aeronaves nas regiões mais ao sul do território brasileiro passam pela região da Anomalia do Atlântico Sul, onde são esperados fluxos de partículas mais intensos em grande altitudes. As medições realizadas por (FEDERICO, 2011) tiveram o intuito de medir a dose de radiação recebida por tripulações, e estudos dedicados à caracterização dos fluxos de partículas ionizantes secundárias para avaliação em sistemas aeronáuticos embarcados devem ser realizados futuramente.

As aeronaves militares podem operar em ambientes de radiação ionizante ainda mais severos que as aeronaves civis, por conta da altitude operacional em geral maior, notadamente para as aeronaves utilizadas para missões combate e de alerta antecipados. Por exemplo, a aeronave Northrop F-5 tem máxima altitude operacional de 15,8 km (51,8 kft) e o Dassault Mirage 2000 tem máxima altitude operacional de 17 km (aproximadamente 59 kft), ou seja, este último pode operar em uma altitude muito próxima da considerada de maior fluxo de partículas secundárias.

Para entender a variação do fluxo de partículas e assim, entender a variação nas taxas de SEUs, é importante considerar os parâmetros como altitude, latitude e energia, além da variação no ciclo solar e eventos solares de curto prazo (SEPEs) (BARTH et al., 2012).

4.2.1.Nêutrons

Os nêutrons são as partículas ionizantes secundárias que tem se mostrado as principais causadoras de SEUs em sistemas eletrônicos aeronáuticos embarcados. Este fato é baseado nas seguintes correlações, de acordo com (NORMAND et al., 1995; HUBERT et al., 2013):

- entre a variação de fluxos de nêutrons conforme latitude e altitude e a ocorrência de SEUs registrados em memórias;
- os cálculos de taxas de SEUs baseadas em medidas em laboratório de seção de choque de SEUs e as medições de SEUs em voo e;

- taxas de SEUs a nível de solo serem proporcionais às taxas registradas em altitudes de aeronaves.

A variação de energia dos nêutrons atmosféricos é geralmente apresentada plotando o chamado fluxo diferencial (fluxo da partícula) como função da energia, o qual é frequentemente chamado de espectro. A Figura 4.3 mostra quatro espectros medidos de diversas fontes e reunidos na IEC TS 62396-1, de nêutrons a uma altitude de aproximadamente 12,2 km (40 kft).

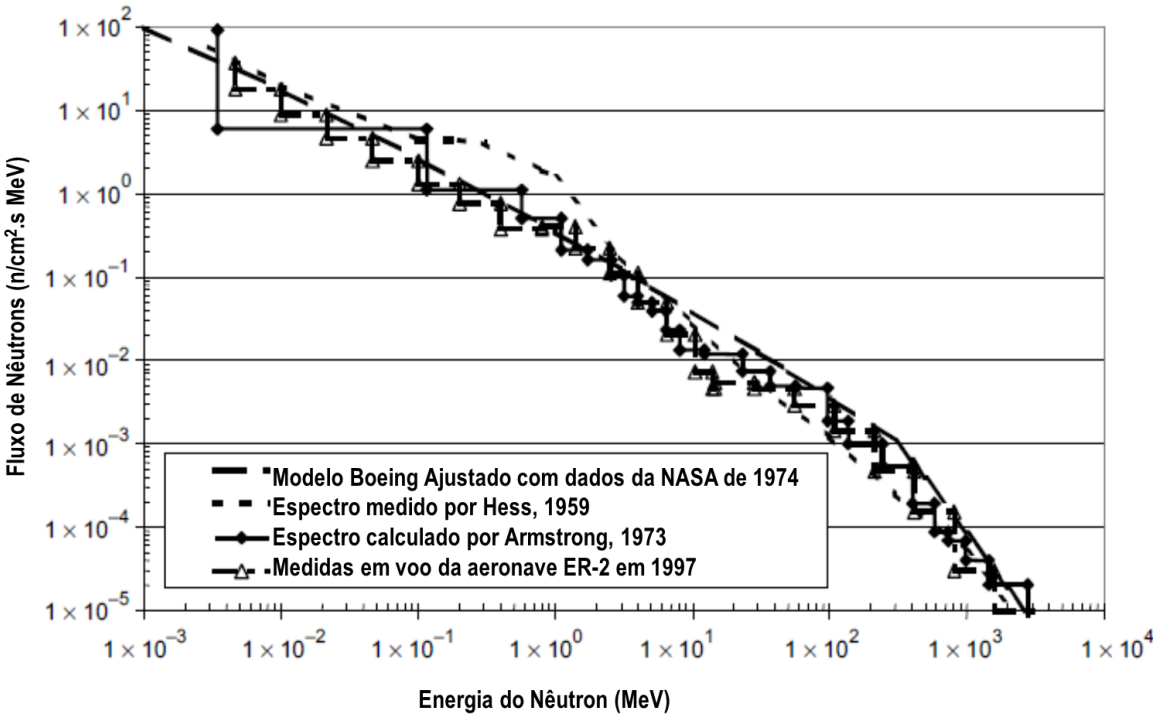

Figura 4.3: Espectro de energia dos nêutrons atmosféricos a 40 kft (12,16 km) e latitude de 45º.
Fonte: adaptado de IEC TS 62396-1 (2012).

4.2.1.1. Variação do Fluxo Conforme Altitude

A variação de fluxo de nêutrons atmosféricos em relação à altitude deriva da competição entre os vários processos de produção e remoção que afetam como os nêutrons e as partículas de raios cósmicos primários interagem com as partículas da atmosfera (FEDERICO, 2011). O resultado é um fluxo máximo em aproximadamente 18,3 km (60 kft), chamado de **máximo de Pfotzer**, que

pode ser visto no gráfico da Figura 4.4. Este gráfico foi desenvolvido utilizando-se dois conjuntos de medidas de fluxo de nêutrons na faixa de 1 a 10 MeV por meio de balões, e é baseada em uma latitude de 45º (NORMAND et al., 1995), sendo chamado de **modelo simplificado da Boeing**.

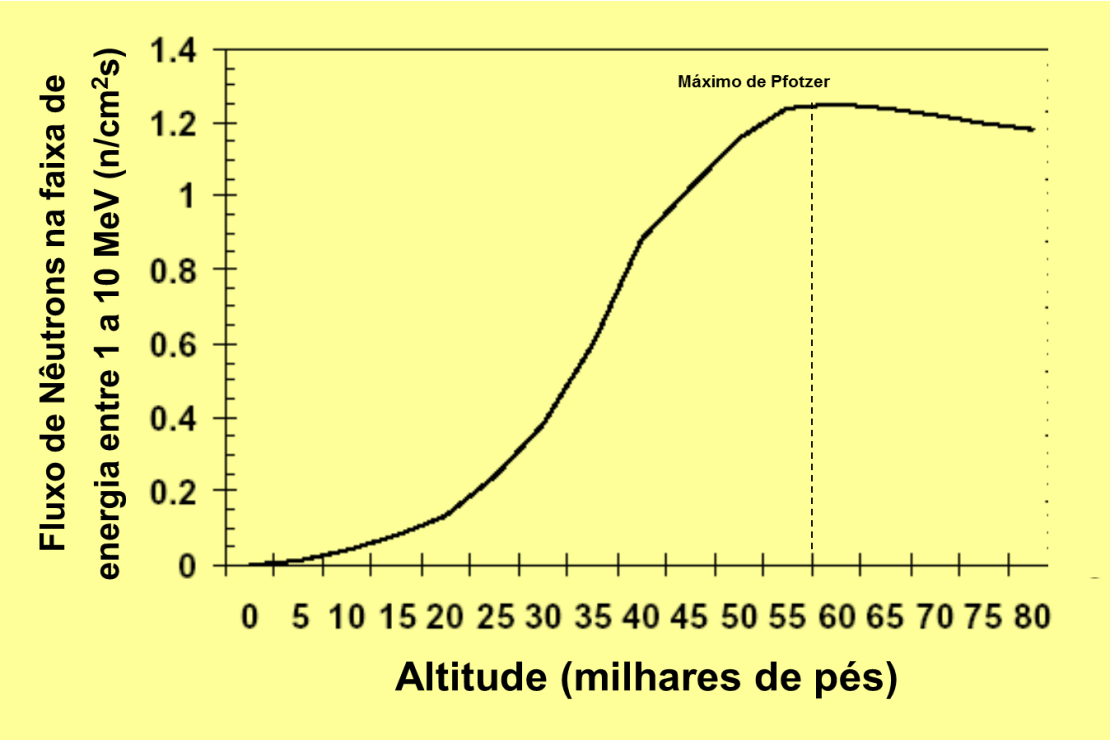

Figura 4.4: Fluxo de nêutrons na faixa de 1 a 10 MeV em relação à altitude
Fonte: adaptado de NORMAND et al. (1995).

4.2.1.2. Variação do Fluxo Conforme Latitude

A variação do fluxo de nêutrons em função da latitude é mostrada na Figura 4.5, evidenciando a ação do campo magnético terrestre, defletindo parte das partículas incidentes (NORMAND et al., 1995).

Esta variação de fluxo conforme latitude é aproximada. No entanto, podemos simplificar o campo magnético, considerando-o como um dipolo, sendo que a deflexão de partículas é máxima na região do equador magnético e mínima nos pólos magnéticos, resultando em um fluxo de nêutrons de até seis vezes maior próximo aos pólos do que nas regiões equatoriais. É possível observar também

que, para latitudes acima de 60 graus, o fluxo é aproximadamente constante (NORMAND et al., 1995).

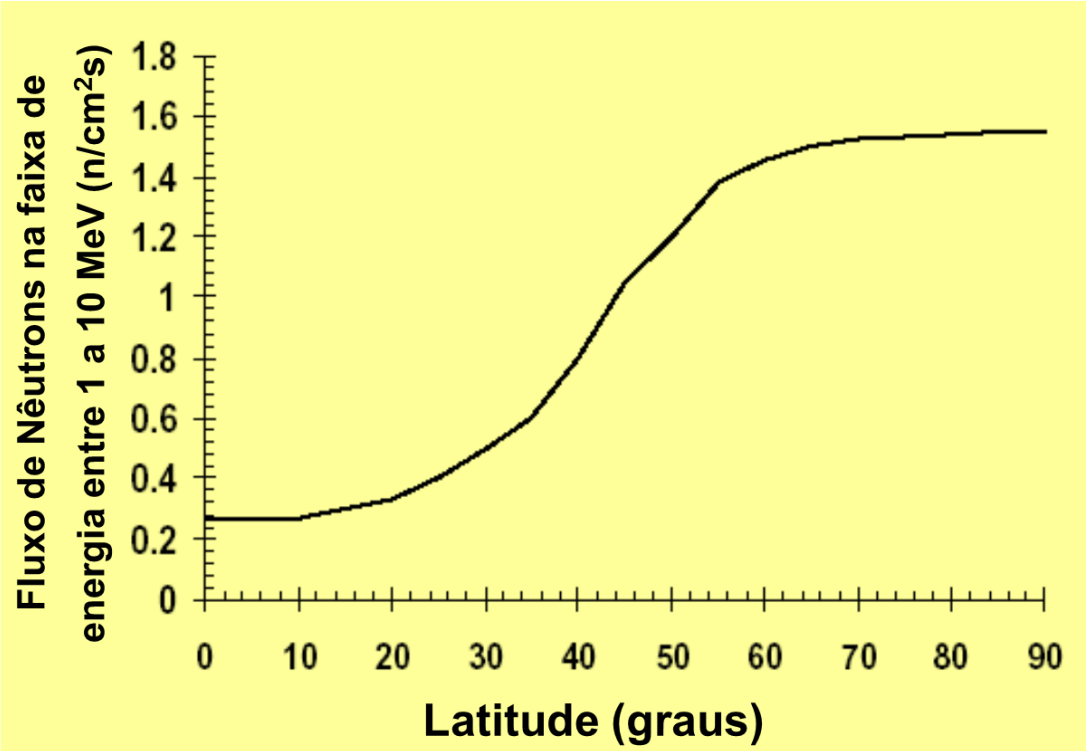

Figura 4.5: Fluxo de nêutrons na faixa de 1 a 10 MeV em relação à latitude.
Fonte: adaptado de NORMAND et al. (1995).

4.2.2.Outras Partículas

Os prótons advindos das interações das partículas galácticas, chamados prótons secundários, também podem causar SEUs de modo semelhante aos nêutrons, ou seja, por interações nos núcleos dos átomos dos semicondutores. A distribuição de fluxos segue uma proporção semelhante ao descrito para os nêutrons, principalmente nos parâmetros de altitude e energia. A proporção estimada do fluxo de prótons na atmosfera é de aproximadamente 20 a 30% para energias até 500 MeV, e de mesmo nível para energias acima de 500 MeV (IEC TS 62396-1, 2012).

Outra partícula que pode induzir SEUs nos sistemas aviônicos é o píon. Para altitudes das aeronaves consideradas, o fluxo de píons é apenas uma pequena

fração comparada aos fluxos de prótons e nêutrons. Para energias menores ou iguais a 1 GeV, a relação píon/próton é de aproximadamente 0,1 para aproximadamente 6,1 km (20 kft) até o nível do mar, e de 1/30 para 12,2 km (40 kft). O fluxo de píons é de comparativamente 1 % em relação ao fluxo de nêutrons. (IEC TS 62396-1, 2012)

Uma pequena quantidade de íons pesados, ou seja, radiação galáctica primária, é capaz de atravessar a atmosfera terrestre. Embora o fluxo de tais partículas seja pequeno para as altitudes de voos comerciais, acima de 18,3 km a radiação galáctica primária não pode ser desconsiderada (IEC TS 62396-1, 2012).

Nêutrons na faixa de baixa energia, em torno de 25 meV a 20ºC, chamados de nêutrons térmicos, são gerados pela interação dos nêutrons de maior energia com o material da aeronave, principalmente o combustível. Estes nêutrons de muito baixa energia cinética podem interagir com os átomos de Boro (B_{10}), por meio de uma reação em que primariamente o nêutron é absorvido pelo núcleo e posteriormente uma reação de fissão é criada, gerando partículas de lítio, radiação alfa e gama, alcançando energias de até 2,8 MeV. Estas partículas podem ser capazes de gerar SEUs. Os processos atuais de fabricação de semicondutores procuram substituir o boro como elemento dielétrico, como por exemplo, com o uso de Háfnio. Este, ao absorver o nêutron térmico, mantém-se como núcleo estável, portanto sem liberar partículas (GAILLARD et al., 2010).

4.2.3. Impacto da Atividade Solar no Fluxo de Partículas Ionizantes na Atmosfera

A atividade solar tem grande impacto no fluxo das partículas galácticas que atingem a atmosfera terrestre. Conseqüentemente, o fluxo das partículas secundárias é afetado. A variação nesta atividade pode ser descrita em termos da variação ciclo solar, de duração aproximada de 11 anos, e os SEPEs, de duração aproximada de horas a dias.

A Figura 4.6 mostra uma representação do ciclo solar e a taxa de contagem de nêutrons, evidenciando uma anti-correlação entre a atividade solar intensa (maior número de manchas) com um fluxo reduzido de nêutrons atmosféricos (diminuição na contagem de nêutrons), e vice versa. Isto se deve principalmente pelo fato da atividade solar intensa (vento solar) e seus efeitos no sistema solar gerarem uma espécie de “escudo”, que diminui a intensidade do fluxo de partículas de radiação galáctica (FEDERICO, 2011).

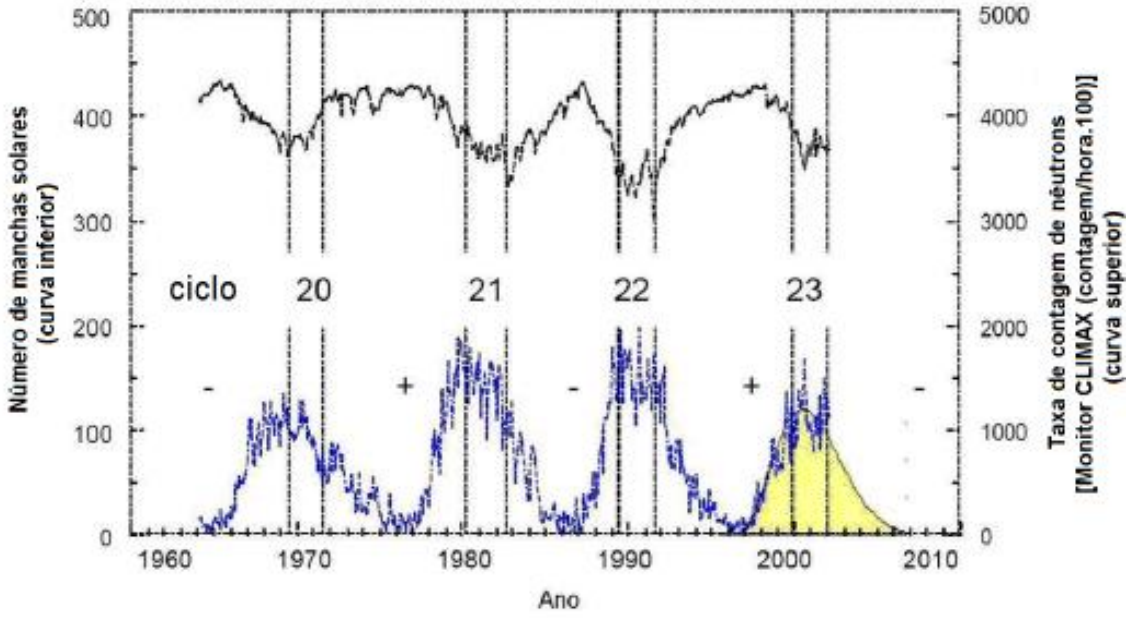

Figura 4.6: Taxa de contagem de nêutrons e do número de manchas solares em função do tempo.
Fonte: extraído de FEDERICO (2011).

O estudo de (INCEOGLU et. al., 2013), considerou a anti-correlação entre a atividade solar e a intensidade dos raios cósmicos galácticos que chegam à atmosfera terrestre como fora de fase, o que cria um atraso temporal entre o ciclo solar e a intensidade dos raios cósmicos galácticos, chamado de **efeito histerese**. Assim, ele modelou a relação entre a contagem de nêutrons na atmosfera e o número de manchas solares, no período que cobriu os ciclos solares 20, 21, 22 e 23. Os dados utilizados foram dos monitores de nêutrons das localidades de McMurdo, Swarthmore, Pólo Sul e Thule. Os resultados do

estudo atingiram ótimos coeficientes de correlação (por exemplo, 0.97, 0.97, 0.92, e 0.97 para respectivamente McMurdo, Swarthmore, Pólo Sul e Thule), demonstrando quantitativamente a anti-correlação entre a atividade solar e a intensidade dos raios cósmicos galácticos.

A aeronave Concorde G-BOAB realizou 412 voos (entre Londres e Nova York ou Washington DC) de novembro de 1988 a dezembro de 1992, medindo o fluxo de nêutrons na atmosfera entre 16,5 e 16,8 km, onde foi possível evidenciar a anticorrelação entre o ciclo Solar e o fluxo dos nêutrons atmosféricos (DYER, 2001).

Os SEPEs podem aumentar dramaticamente o fluxo de partículas de alta energia vindas do Sol, que também interagem com os átomos da atmosfera. As grandes explosões que geralmente são acompanhadas por ejeção de massa coronal solar, liberam grandes quantidades de partículas na maioria prótons de altas energias, além de elétrons, núcleos de hélio, podendo chegar até centenas de MeV ou eventualmente unidades de GeV (BARTH et al., 2003; FEDERICO, 2011).

As medições realizadas no Concorde G-BOAB também foram capazes de evidenciar o grande impacto dos SEPEs no fluxo de nêutrons atmosféricos, durante o período de intensa atividade Solar entre setembro e outubro de 1989. Foram registrados acréscimos instantâneos de um fator de até 10 vezes, e média de 6 vezes no fluxo de nêutrons durante os dias de ocorrências de SEPEs (DYER, 2001).

4.2.4. Exemplos de Ocorrências em Aeronaves

Além das ocorrências medidas na aeronave Concorde G-BOAB, mencionadas anteriormente, outros relatos de ocorrências em aeronaves podem ser mencionados.

Por exemplo, foram medidos diversos erros em um computador comercial embarcado que utilizava memórias de 256 kB SRAM CMOS. Após testes em laboratórios, a taxa observada na altitude de 10,7 km, que foi em torno de

$4{,}8x10^{-8}$ falhas por bit por dia, pode ser correlacionada em termos do fluxo de nêutrons secundários na atmosfera (DYER, 2001).

Uma extensa investigação dos SEUs em equipamentos aviônicos foi realizada por (NORMAND et al., 1995) utilizando conjuntos de memória do tipo CMOS SRAM de 64 kB modelo IMS1601. Diversos voos foram realizados com duas aeronaves: um Boeing E-3 Sentry em altitudes de voo comercial (aproximadamente 30 kft), e um avião da NASA ER-2 em altas altitudes (em torno de 18,3 km). As medições variaram entre $1{,}2x10^{-7}$ SEUs por bit por dia a 9,1 km e 40^{o} de latitude até $5{,}4x10^{-7}$ SEUs por bit por dia em altas latitudes e altitudes. Foi possível estabelecer uma correlação entre as medidas de SEUs registradas e as previsões baseadas em fluxo de nêutrons atmosféricos.

O sistema de piloto automático do Boeing 777 registrou diversos erros que foram atribuídos a SEUs, e estes erros foram também correlacionados com os fluxos de nêutrons atmosféricos. O sistema contém aproximadamente $1{,}5x10^{6}$ bits de SRAM, continuamente checados por um esquema de redundância tripla. A quantidade registrada foi de aproximadamente 1 erro por 200 horas, e mais de 1000 erros foram registrados entre 1997 e 1999 (DYER, 2001).

4.3. Alguns Softwares Utilizados para Modelar os Ambientes de Radiações Ionizantes

Para se caracterizar o ambiente de partículas ionizantes exposto nos itens anteriores, são utilizados softwares que modelam o fluxo de partículas e seus respectivos níveis de energia esperados. A seguir são mencionados alguns dos softwares que podem ser usados. Cabe ressaltar que não é objetivo do presente trabalho discutir os parâmetros, representatividade e precisão dos mesmos, mas sim relacionar os softwares que usam os modelos recomendados por normas e literatura para referência:

- O pacote de ferramentas de software CRÈME disponível para usuários cadastrados em https://creme.isde.vanderbilt.edu/CREME-MC tem, em seu conjunto softwares de diversas capacidades. O CREME96 - *Cosmic*

Ray Effects on Microeletronics (Efeitos de Raios Cósmicos na Microeletrônica) é um conjunto de programas para, dentre outras funções, criar modelos numéricos para o ambiente de radiação em órbitas próximas da Terra e avaliar os efeitos da radiação em sistemas eletrônicos embarcados em espaçonaves e aeronaves de altas altitudes. O CREME foi primeiramente desenvolvido em 1981, e foi atualizado em 1986. A versão mais atual disponível é o CREME96 e é a recomendada pelo site. Na parte de avaliação dos efeitos da radiação em componentes eletrônicos, há uma ressalva de que a aplicação do software para novas tecnologias CMOS e SiGe, por exemplo, pode não representar o comportamento esperado de tais componentes e, portanto, recomenda o uso do software GEANT4.

- GEANT4 - *GEometry ANd Tracking* (Geometria e Rastreamento), disponível em http://geant4.web.cern.ch/geant4/support/download.shtml, é uma ferramenta para simulação da passagem de partículas pela matéria, sendo o sucessor da série de softwares GEANT desenvolvida pelo CERN - *European Organization for Nuclear Research* (Organização Europeia para Pesquisa Nuclear). Seu desenvolvimento, manutenção e suporte ao usuário são mantidos por um grupo de colaboradores internacional (http://www.geant4.org/geant4/). Suas áreas de aplicação incluem Física de Aceleradores, Física Nuclear e de Alta Energia, assim como estudos em Ciência Espacial e Ciência Médica.

- FLUKA - *FLUktuierende KAskade* (Flutuação de Cascatas - este nome foi dado por razoes históricas, uma vez que o programa surgiu pelo estudo das variações das chamadas cascatas de hádrons), disponível em http://www.fluka.org/fluka.php, é um pacote de simulação para a interação e transporte de partículas nos materiais. Tem diversas aplicações como, por exemplo, em física de partículas, física e engenharia experimental de altas energias, estudos de raios cósmicos, dosimetria, etc. O programa é mantido pelo CERN.

- SPENVIS – *Space ENVironment Information System* (Sistema de Informações do Ambiente Espacial), é uma interface via internet, acessível em https://www.SPENVIS.oma.be/intro.php, para modelar o ambiente especial e seus efeitos, incluindo raios cósmicos, cinturões de radiação de Van Allen, partículas energéticas solares, plasmas, gases, etc. O programa, mantido pela ESA, é capaz de calcular coordenadas geomagnéticas, fluxo de prótons, aprisionados e fluxo de elétrons e prótons solares, doses de radiação (ionizantes e não ionizantes) para geometrias simples, espectro de LET para íons e taxas de SEUs, além de diversas outras funcionalidades.
- EXPACS - *EXcel-based Program for calculating Atmospheric Cosmic-ray Spectrum* (Programa Baseado em Excel para calcular o Espectro de Raios Cósmicos Atmosféricos), disponível em http://phits.jaea.go.jp/EXPACS/, é um programa para estimar o espectro de raios cósmicos atmosféricos (partículas secundárias). É capaz de calcular não somente os nêutrons, mas também prótons, núcleos de hélio, elétrons pósitrons e múons para qualquer região da atmosfera em altitudes abaixo de 20 km. Permite também estimar a dose equivalente e a dose efetiva em seres humanos devido à exposição aos raios cósmicos, que também pode ser visualizada nos mapas do Google Earth™ pelo software EXPACS-V.
- RADBELT – RADiation BELT, disponível em http://ccmc.gsfc.nasa.gov/modelweb/models/trap.php, é um programa para estimar os fluxos de prótons e elétrons dos cinturões de radiação terrestres. O programa permite ao usuário especificar online parâmetros de entrada e opções e gerar tabelas de fluxo que podem ser armazenadas para uso posterior.
- SOLPRO – SOLar PROton, disponível em ftp://hanna.ccmc.gsfc.nasa.gov/pub/modelweb/solar/proton_flux/solpro/ é um programa que calcula a fluência de prótons de origem solar, usando

parâmetros como a duração da missão em meses, e limiar de energia a ser considerado, em MeV.

4.4. Uso de Cenários Para Caracterização do Ambiente de Radiações Ionizantes

A atividade solar é um fator que influencia enormemente a caracterização do ambiente de radiações ionizantes no espaço e na atmosfera terrestre. Para se definir o ambiente de radiações ionizantes, é importante prever esta atividade e seu impacto.

No caso de sistemas eletrônicos embarcados espaciais, ao se ter em mãos as datas e duração da missão, é possível estimar em que etapas do ciclo solar a missão estará em operação.

O estudo da NASA desenvolvido por (SUGGS, 2013) prevê a atividade cíclica solar entre 2014 e 2030 (o que corresponde aproximadamente aos ciclos 24 e 25), baseando-se nos dados da atividade solar dos ciclos 1 a 23. O modelo utilizado, chamado de *Marshall Solar Activity Future Estimates Model* (MSAFE), foi desenvolvido para ter a capacidade de estimar índices como o número médio de manchas solares R, um importante indicador da atividade solar, de acordo com percentil sobre os dados dos ciclos anteriores de, por exemplo, 5, 50 e 95. Estes percentis podem ser interpretados como previsões de atividade cíclica solar respectivamente de intensidade baixa, média e alta. A duração prevista do período dos ciclos solares 24 e 25 foi estimada em 11 anos (132 meses), baseado nos ciclos anteriores.

O estudo tem como objetivo prover dados de entrada para os modelos que caracterizam o ambiente espacial. Por exemplo, para caracterizar o fluxo de raios cósmicos, alguns modelos utilizam o número médio de manchas solares (R) como dado de entrada (SUGGS, 2013). A Figura 4.7 abaixo ilustra o registro de manchas solares do período entre 1999 e 2013 em vermelho, e o gráfico correspondente à aplicação da técnica de estimação estatística

chamada de *13-month Zurich smoothing technique*, em preto realizado por (SUGGS, 2013).

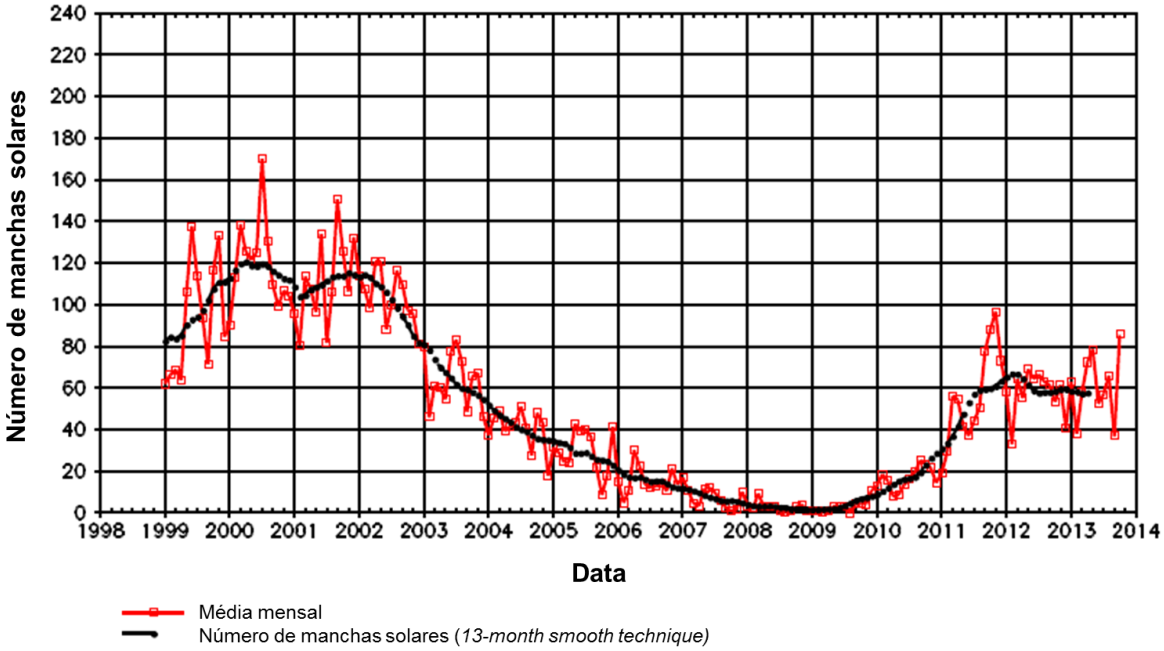

Figura 4.7: Gráfico da média mensal e do número de manchas solares entre 1999 e 2013.
Fonte: adaptado de SUGGS (2013).

A Figura 4.8 representa o resultado do trabalho de (SUGGS, 2013), com a estimação da atividade solar futura até 2030, prevista para o período dos ciclos solares 24 e 25, de acordo com cenários de ciclo solar com atividade intensa (em azul, percentil de 95%), média (verde, percentil de 50%) e baixa (em vermelho, percentil de 5%).

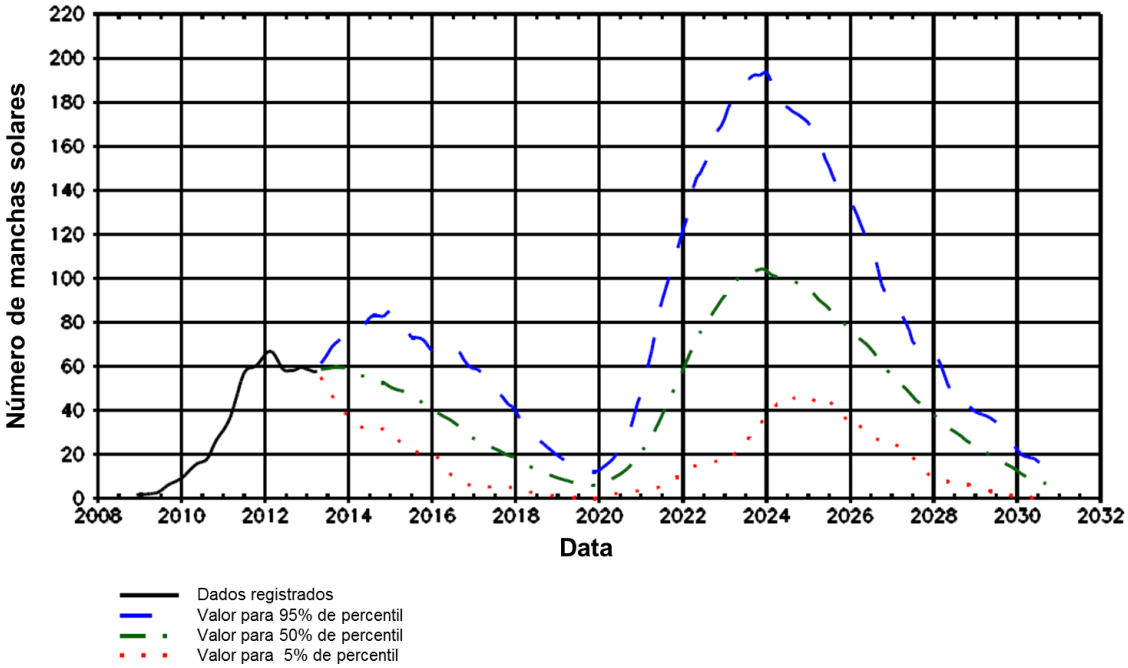

Figura 4.8: Gráfico da média mensal do número de manchas solares prevista para o período dos ciclos solares 24 e 25.
Fonte: adaptado de SUGGS (2013).

O cenário que considera a ocorrência de um evento de SEPE, onde haveria um acréscimo dramático no fluxo de partículas potencialmente causadoras de SEU, é muito importante para caracterizar um ambiente extremo, onde o fluxo de partículas ionizantes pode aumentar significantemente em relação aos 3 ambientes considerados acima.

4.5. Robustez de Sistemas Eletrônicos Embarcados Aeroespaciais a SEUs e o Impacto na Confiabilidade

Para que os SEUs sejam inseridos adequadamente no contexto das análises de confiabilidade, o correto estabelecimento das taxas de SEUs atribuídos ao componente, LRU ou sistema, é fundamental. As taxas são geralmente expressas em falhas por componente ou bit por um determinado tempo (por exemplo, número de SEUs / bit / hora, número de SEUs / LRU/ hora, etc.).

4.5.1.Estimação das Taxas de Ocorrências de SEUs

As taxas de ocorrência de SEUs em um dispositivo eletrônico dependem de fatores como a susceptibilidade, da quantidade de bits afetados e do fluxo de partículas ionizantes (NICOLAIDIS, 2011). As taxas de SEUs não são avaliadas em termos de uma dose ou tempo até a falha, onde o cronômetro se inicia no lançamento da missão, mas por uma probabilidade que um SEU ocorrerá dentro de um determinado intervalo de tempo (LABEL et al., 1996).

As taxas de SEUs nos dispositivos são baseadas em parâmetros obtidos por testes, sendo que alguns dos parâmetros foram expostos no capítulo 2 (seção de choque, LET_{th}, espectro das partículas conforme energia ou LET, etc.). A abordagem é de expor um componente, dispositivo ou LRU a um feixe conhecido de partículas e observar a resposta (número de eventos, no caso de SEUs).

Os ambientes expostos em 4.1 e 4.2 são variáveis e complexos em níveis de energia e composição Os testes devem ser realizados, portanto com aceleradores que possam ser operados com uma variedade de tipos de partículas e energias. Para se obter as taxas de ocorrências de SEUs, é realizada a combinação das curvas de susceptibilidade obtidas experimentalmente com os parâmetros apropriados do ambiente (ECSS-E-HB-10-12A, 2010).

Os testes devem ser realizados de preferência nas etapas iniciais do projeto. Para se obter uma estimativa mais precisa das taxas de SEUs, é preciso que o dispositivo seja testado funcionando da forma mais próxima possível da real. Parâmetros como tensão, velocidade de *clocks*, freqüência de amostragem de sinais, etc., podem alterar significantemente os valores estimados (ECSS-E-HB-10-12A, 2010). Em casos onde ainda não for possível determinar tais parâmetros nas etapas iniciais do projeto, uma abordagem de pior caso pode ser uma solução viável (LABEL et al., 1996; NICOLAIDIS, 2011).

4.5.2. Análise de Confiabilidade de Sistemas Eletrônicos Embarcados Aeroespaciais e SEUs

No contexto de desenvolvimento de sistemas eletrônicos aeroespaciais, a determinação da taxa de SEUs e a avaliação da severidade do risco de SEU envolve conhecimentos de diversos campos técnicos como física da radiação, engenharia de componentes, física do estado solido, engenharia elétrica, análise de confiabilidade e engenharia de sistemas. A aplicação direta das ferramentas de análise, que por si só é uma tarefa complexa, não é tão simples, principalmente por conta das abordagens do ambiente, mecanismos, efeitos e mitigação.

Uma premissa fundamental na abordagem de robustez à falha é admitir o fato de que as mesmas nunca poderão ser totalmente eliminadas, mas sua probabilidade de ocorrência e consequências podem ser gerenciadas de modo a se obter um nível aceitável (ATSB, 2011). Este nível aceitável é traduzido quantitativamente em uma probabilidade de perda da função, definida de acordo com a criticalidade da função executada pelo sistema/componente. Ou seja, quanto mais crítica for a função, menor é a probabilidade aceitável de falha daquela função.

As análises a seguir estão ligadas às analises de confiabilidade que são realizadas durante o processo de desenvolvimento de sistemas.

Dentre as ferramentas que podem ser usadas na abordagem de robustez à SEUs relacionadas à análise de confiabilidade, podemos usar as *Failure Mode and Effects Analysis* (FMEA) e *Failure Modes, Effects and Criticality Analysis* (FMECA).

De acordo com (SOUZA et al., 2005), a FMEA é uma ferramenta útil para se examinar a integridade de um sistema utilizando-se uma abordagem *bottom-up,* com foco nos pontos de falha simples, o que é característico dos SEUs.

Para se cumprir com os requisitos de segurança dentro do processo de desenvolvimento e certificação de sistemas aeronáuticos, as FMEA são

realizadas para se alimentar as árvores de falha (ou diagrama de dependência, ou cadeias de Markov). A FMEA de item é sumarizada na FMES (Failure Mode and Effects Summary), que reúne as taxas de falhas a serem consideradas nas árvores de falha do item. No nível sistema, o processo é semelhante, ou seja, é realizada a FMEA do sistema e respectiva FMES, alimentando as árvores de falha do sistema. Ao se chegar ao nível da aeronave, ocorrerá a integração dos itens em sistemas e sistemas para a aeronave, onde os efeitos das falhas serão comparados com as condições de falha identificadas na FHA (isto acontece também para o nível sistema, onde será usado a FHA nível sistema). independentemente do nível da FMEA, os principais passos para sua execução incluem preparação, análise e documentação.

A FMEA deve levar em consideração todos os efeitos relacionados à segurança e outros identificados por requisitos, onde se deve abordar o pior caso se não for possível identificar a natureza específica do modo de falha. Os SEUs se inserem neste contexto como um dos efeitos relacionados à segurança.

As análises realizadas com base na FMEA/FMECA podem identificar necessidades de alterações no projeto para atender aos requisitos para SEU. Diversas técnicas de mitigação, incluindo de hardware e software, podem ser implementadas para tanto. De acordo com (NICOLAIDIS, 2011), para se obter um sistema que atenda os requisitos de robustez a SEU, diversas abordagens são disponíveis e necessárias, de modo a evitar penalidades na complexidade e custo do sistema:

- Abordagens de mitigação de SEU a nível de hardware, que podem incluir códigos de detecção e correção de erros (*Error Detection And Correction* – EDAC), abordagens de duplicação de amostragem de sinal, etc.
- Abordagens de mitigação de SEU a nível de software, como duplicação de instruções, *rollback recovery*, etc.

O item a seguir descreve algumas estratégias de mitigação e exemplos de implementação de tais técnicas em sistemas aeroespaciais com potencial para garantir a robustez às falhas induzidas por SEUs.

4.6. Estratégias de Mitigação para Robustez a SEU de Sistemas Eletrônicos

Em geral, para se atingir os níveis de confiabilidade e segurança necessários a projetos aeroespaciais, algum esquema de Robustez à SEUs será adotado. A seleção e aplicação criteriosa, além da execução dos testes necessários para verificação destas medidas, levarão a um projeto otimizado e que atinja os requisitos de segurança.

A abordagem de *prevenção a falha* envolve prevenir a falha em primeiro lugar, ao contrário de recuperar o sistema uma vez que ela ocorre (NORMAND et al., 1995). Envolve o projeto de sistemas e componentes para longos períodos de uso, com controle de manufatura rígido, e manutenção e testes com foco na confiabilidade do produto em sua operação (SOUZA et al., 2005).

Para o caso da radiação ionizante, diversos esforços para proteger os componentes eletrônicos resultaram em diversas técnicas, incluindo (SOUZA et al., 2005; NORMAND et al., 1995):

- **Margens de projeto e *derating*:** prevenção da falha do componente devido aos estresses e outros desvios das condições nominais de operação acima do esperado (mais aplicado em circuitos lineares analógicos e componentes discretos);
- **Redução da coleta de carga:** aumenta-se assim a carga crítica do componente e, portanto diminui sua susceptibilidade a SEEs;
- **Seleção de partes e *screening*:** o *screeening* (seleção de partes por testes por teste) é um processo que elimina unidades que tem uma alta probabilidade de falha em serviço que outras unidades do lote;

Muitas destas técnicas podem reduzir ou até eliminar os SEUs, mas o custo e disponibilidade de componentes robustecidos podem inviabilizar o projeto. E, mesmo com a aplicação de técnicas de *fault avoidance*, elas podem não ser suficientes para atender alguns requisitos de confiabilidade e segurança, portanto há um interesse cada vez maior na abordagem de *fault tolerance* (SOUZA et al., 2005).

As divisões das técnicas de mitigação para garantia de robustez a SEUs a seguir tem caráter apenas de organização, não sendo objetivo deste trabalho classificá-las de modo definitivo, e sim destacar a característica preponderante da técnica (pois, por exemplo, uma técnica de redundância pode envolver o uso de códigos de detecção de erros).

4.6.1. Códigos de Detecção e Correção de Erros

Os códigos de Detecção E Correção de Erros (*Error Detection And Correction* – EDAC) são um conjunto de soluções usadas para reduzir as taxas de erros, principalmente em memórias, que representam atualmente as maiores porções de componentes de projetos de sistemas eletrônicos modernos e as mais sensíveis a SEU (NICOLAIDIS, 2011). Em geral, as técnicas consistem em adicionar bits nas palavras de informação de modo a se detectar e corrigir valores errôneos. Assim as medidas podem demandar grandes acréscimos de potência e velocidade.

O método mais elementar de mitigar erros em fluxos de dados e memória é utilizando cheques de paridade, que na verdade é um código de apenas detecção, e não há tentativa de correção do erro ocorrido, portanto deve estar associada a outros mecanismos de recuperação. Este método conta o numero de estados lógicos “1” em uma estrutura de dado (uma palavra de 16 bits, um byte de 8 bits, etc.). A paridade geralmente usa um único bit adicionado no fim da estrutura de dado, indicando se há uma quantidade par ou impar de “1” na estrutura. Este método detecta um erro se um número impar de bits está com erro, entretanto se um número par de erros ocorrer, a paridade será correta (ou

seja, a paridade será a mesma se 0 ou 2 erros ocorrem) (NORMAND et al., 1995)

Outro código EDAC é o chamado código de Hamming, capaz de corrigir um bit errôneo e detectar dois bits errôneos (*Single-Error Correcting Double-Error Detecting,* SEC-DEC). Para codificar um conjunto de bits, o código usa bits de checagem. Para tanto, os bits de checagem são colocados nas posições de potência de 2 na estrutura da palavra. Por exemplo, para 8 bits de informação (D_7, D_6, D_5, D_4, D_3, D_2, D_1, D_0), teremos 4 bits de checagem (C_3, C_2, C_1, C_0), a palavra, portanto ficará assim disposta: D_7, D_6, D_5, D_4, C_3, D_3, D_2, D_1, C_2, D_0 C_1,C_0. Por exemplo, para 8 bits de informação, precisamos de 4 bits de checagem, para 16 de informação, 5 de checagem, para 32 de informação, 6 de checagem, e assim por diante. O código é capaz de localizar a posição do erro por meio de uma síndrome que codifica a posição do erro. A checagem é realizada pela decodificação da palavra, que é capaz de identificar a posição de um e a ocorrência de dois erros na palavra, ao se inserir um bit de paridade. A detecção de dois erros é dada pela paridade, pois conforme visto anteriormente, ao se cruzar o erro com a paridade, é possível concluir se houve um erro (decodificação com erro mais paridade errada) ou dois erros (decodificação com erro e paridade correta) (NICOLAIDS, 2011).

Os códigos de Cheque de Redundância Cíclica (*Cyclic Redundancy Check* – CRC) são esquemas de EDAC onde o emissor e o receptor da informação concordam com um polinômio gerador G(x), em que quanto maior for o seu grau maior será a capacidade de detecção de erros, e o polinômio p(x), composto pelos bits de informação e paridade, deve ser divisível por G(x); se houver resto ≠0, houve um erro de transmissão. De acordo com (NICOLAIDIS, 2011) são códigos com propriedades matemáticas que permitem uma arquitetura eficiente e com grande capacidade de detecção de erros. Outra característica importante é que requerem circuitos relativamente simples para codificação e decodificação. Os códigos CRC podem ser usados também para a correção de um erro.

Por exemplo, a placa R3081 (com componentes COTS e abordagem tolerante a falhas) do projeto ARGOS implementou um código de detecção e correção de erros (EDAC) via software, provendo detecção de mais de um bit e correção de um bit. Os SEUs ocorridos nos segmentos de código de programa são corrigidos e um reporte enviado via telemetria, informando o endereço, numero do bit e posição do satélite (LOVELLETTE et al., 2002).

4.6.2. Watchdog Timers

Watchdog Timers podem ser implementados em hardware ou software ou ainda uma combinação dos dois. Tipicamente, os *Watchdogs* são um método de detecção de erro via informação do status. Ou seja, uma mensagem indicando a saúde do dispositivo ou sistema é enviada de um local para outro. Se a mensagem não é recebida pela segunda localização dentro de um período estipulado, o sistema deve ter uma ação no dispositivo, caixa, subsistema que é a potencial fonte de mau funcionamento. Os *Watchdog timers* são, portanto um esquema de monitoramento do comportamento de um componente, podendo ser implementados em diversos níveis como entre dispositivos, entre caixas, etc. Os *Watchdog Timers* podem ser ainda classificados como ativos ou passivos (HEIDERGOTT, 2005; NORMAND et al., 1995).

Considere, por exemplo, um *Watchdog* ativo, onde o dispositivo A deve enviar um pulso indicando que está ok a cada segundo, para um dispositivo B. B pode ser um controlador de interrupção de um microprocessador. Se A falhar em enviar o pulso dentro do tempo estipulado, B entende que o tempo está esgotado e inicia uma ação de recuperação como o envio de um sinal de reset, remoção de energia, envio de uma mensagem de telemetria para terra, colocar o sistema em modo seguro, etc. A ação de B será bem específica para cada cenário e modo de operação (HEIDERGOTT, 2005).

Considere, por exemplo, um *Watchdog* passivo, implementado entre um satélite e uma estação em terra. Em um cenário de operação normal, este

poderia receber mensagens de *uplink* (comandos, trechos de códigos, tabelas de dados, etc.) da estação em terra a cada 12 horas. Há um timer embarcado que indica se o tempo foi esgotado se não houve nenhum *uplink* dentro das 12 horas (ou dependendo, 24 horas). O satélite então inicia uma ação, por exemplo, de chavear para uma antena redundante ou interface de uplink, uma ciclagem de energia da interface de uplink, etc. A classificação deste *watchdog* como passivo é por conta de não haver uma mensagem indicando o status ok entre pares, mas apenas um monitoramento da condição de operação normal (HEIDERGOTT, 2005).

De acordo com (HEIDERGOTT, 2005), muitos processadores utilizam *watchdog timers*, geralmente na forma de um co-processador, para detectar paradas na execução do processador ou erros no fluxo de programa, que são detectados por meio da falha na execução do programa em zerar o timer do *watchdog* em um tempo esperado. O co-processador estende a noção do uso de um timer simples para um processador capaz de processar vários elementos do processador principal. Por exemplo, o *watchdog* pode executar um programa no mesmo tempo que o processador, ou operar em separado e computar previamente os resultados como forma de teste de aceitação dos valores processados, assumindo que em caso de discordância houve uma ruptura no fluxo do programa, dados corrompidos, ou dados numéricos incorretos.

4.6.3. Redundância

O uso de redundância permite um sistema continuar funcionando durante ou após a ocorrência de um SEU, uma vez que é esperado um segundo SEU ocorra em uma localização diferente do circuito (redundância física) ou, caso a operação seja repetida (redundância no tempo), o segundo SEU não ocorrerá da mesma maneira (NORMAND et al., 2005). A redundância entre circuitos, caixas, subsistemas, circuitos, etc. são um meio potencial de se recuperar de um SEU.

(SOUZA et al., 2005) provê um sumário com a aplicabilidade e limitações de técnicas de redundância, que podem ser aplicadas para tolerar falhas, mostrados na Tabela 4-2 e descritos na sequência.

Tabela 4-2 – Técnicas de Redundância, aplicabilidade e limitações

Técnica	**Proteção Contra**	**Limitações**
Redundância com mesma implementação	Falhas aleatórias	Alto custo de produção, acréscimo de peso e potência
Redundância com implementação(ões) diversa(s)	Falhas aleatórias e falhas de projeto	Mesmo que anterior, mais custos de desenvolvimento e logística
Redundância de K entre N	Falhas aleatórias	Aplicável somente quando várias cópias do artigo estão presentes
Redundância funcional	Falhas aleatórias e falhas de projeto	Necessário ter disponibilidade de métodos diferentes de se realizar a função
Redundância temporal	Falhas intermitentes e transitórios	Tempo necessário para recuperação

Fonte: adaptado de SOUZA et al. (2005).

- A redundância com mesma implementação consiste na instalação de dois ou mais componentes idênticos em conjunto com sistema de chaveamento para a unidade ativa.
- A redundância com implementação(ões) diversa(s) consiste no uso de dois ou mais componentes de projeto diferente para realizar uma mesma função.

- A redundância de K entre N elementos consiste no uso de N > K elementos, de modo que a função é mantida quando ao menos K elementos estão operacionais.
- A redundância funcional consiste em realizar uma mesma função de modos diferentes.
- A redundância temporal é a repetição de uma operação ou função de um componente defasada no tempo, de modo a se obter redundância por duplicação (ou triplicação, etc.) pelo mesmo componente.

Um exemplo de esquema com redundância de mesma implementação é o chamado de *lockstep*. Consiste em operar dois circuitos idênticos com *clocks* sincronizados. A detecção do erro é realizada pela verificação da saída dos circuitos, ou seja, se há discordância, provavelmente um SEU ocorreu. O sistema então tem opções de entrar em modo de segurança, reiniciar, etc. No entanto, para sistemas espaciais com missões longas, esta medida deve ser evitada, pois outros efeitos como degradação por TID podem levar a efeitos como defasagem de *clock* entre os circuitos (*clock skew*), causando falsa detecção de erro, se cada dispositivo de um circuito responder de maneira diferente ao TID.

Um exemplo de redundância com implementações diversas é o caso do sistema de comando de voo do Boeing 777, composto de três *Primary Flight Computers* (PFCs), cada um com três canais similares, hardware dissimilar e mesmo software. São usadas técnicas de votação com diferentes comparações para cada tipo de dado de forma a detectar discrepâncias ou discordâncias. Para atuar nas superfícies de voo (ailerons, profundor, leme, etc.) o *Actuator Control Electronics* (ACEs) recebe dados de diversos barramentos ARINC 629 e atua diretamente nas superfícies (MOIR, 2008).

Um exemplo de redundância implementada por software é o caso da placa R3081 (com componentes COTS e abordagem tolerante a falhas) do projeto ARGOS, que implementou um esquema chamado de EDDI -. *Error Detection*

by Duplicated Instructions (Detecção de Erros Por Duplicação de Instruções). Basicamente, consiste em duplicar um bloco de instruções ou instruções específicas, em geral operações de cálculo, e comparar os resultados antes de escrevê-los na memória. Caso os valores não sejam iguais, o programa realiza um salto para uma rotina de tratamento de erro que irá fazer o programa reiniciar. As diversas técnicas implementadas no projeto tolerante à falha tiveram bons resultados, pois embora tenham sido detectados mais de 2000 SEUs, e foram registradas mais de 50 execuções das rotinas de erro e 5 reinicializações, em geral a funcionalidade e integridade da placa foi mantida, e foi possível correlacionar os ambientes mais severos com o maior número de das ocorrências. Em 543 dias, a placa RH3000, embora robustecida à radiação, teve 25 erros registrados em 543 dias de operação; além de uma operação de reinicialização (esta última sem uma causa raiz definida); a Figura 4.2 mostra a correlação entre os SEUs e as regiões esperadas de alto fluxo de partículas, como a SAA e os cinturões de radiação de Van Allen. (LOVELLETTE et al., 2001)

Um sistema de comando de voo adaptado, chamado de *Rollback Rapid-Recovery Computer* foi testado com sucesso por (BELCASTRO et al., 2006). Este teste foi realizado com nêutrons, como um teste acelerado (alto fluxo de nêutrons). Neste esquema, uma unidade de hardware compara os comandos críticos enviados por duas CPUs em cada ciclo de clock, bit por bit. Quando dois comandos forem diferentes, estes são descartados e o valor anterior, que foi armazenado, é usado, ou seja, uma rápida recuperação resgatando o valor anterior (*rollback*, ou para trás) é realizada.

(KASTENSMIDT, 2003) testou o uso de redundância tripla implementada em circuitos programáveis FPGA, destacando a eficácia do esquema e as limitações de uso por conta do aumento em consumo e área do componente. De modo a otimizar os custos e melhorar a confiabilidade desta implementação, propôs o uso de uma arquitetura chamada DWC-CED (*Duplication With Comparison – Concurrent Error Detection*, Duplicação Com

Comparação – Detecção de Erro Simultânea) que envolve o uso de redundância dupla (DWC) e temporal (CED), com ganhos na redução da quantidade pinos, área usada e consumo de energia.

O sistema de comando de voo do A330, assim como em outros projetos de sistemas críticos para a segurança de voo de aviões (caso, por exemplo, do Boeing 777, onde neste trabalho foram mencionadas apenas algumas estratégias de mitigação), Categoria Transporte, contém diversas técnicas de mitigação, visando obter um sistema robusto a falhas. O sistema de comando de voo Airbus A330 e 340 contêm cinco computadores, dispostos da seguinte forma: três computadores de comando de voo primário (FCPC, chamados também de PRIM), que geram comandos e controlam algumas superfícies de voo, e dois computadores de comando de voo secundários (FCSC, chamados também de SEC), que comandam algumas superfícies de voo. Um os três FCPC atua como mestre, que computa os comandos para todas as superfícies de voo e as envia para os demais computadores para execução; os demais computadores, por sua vez, monitoram a operação do mestre e podem tomar o lugar de mestre em caso de detecção de uma falha. Os diversos esquemas de mitigação de falhas incluem (ATSB, 2011):

- **Redundância:** o uso de cinco computadores diferentes prove redundância no caso de falha em um ou mais computadores. Na presença de certos tipos de falhas ou problemas de processamento, o papel de mestre é chaveado de um FCPC para outro. O controlador dos atuadores para uma superfície de voo também pode ser mudado de um FCPC para outro ou um FCSC
- **Pares de Auto verificação (Redundância):** cada computador tem dois canais fisicamente independentes. O canal de comando (COM) computa as ordens de controle e ou sinais de atuadores e o monitor (MON) realiza as mesmas operações e compara os resultados. Os dois canais têm seu próprio processador, fonte de alimentação, memórias e circuitos

de entrada/saída. O uso de dois canais auxilia a identificação de problemas de hardware ou processamento.

- **Monitoramento (*Watchdog*):** cada computador tem testes internos para monitorar seu próprio desempenho e o dos demais computadores, assim como para monitorar outros elementos do sistema como atuadores e sensores. O FCPC também monitora sistemas externos que provem dados para o sistema de comando de voo, para verificar a validade e consistência dos dados.
- **Diversidade de dados (Redundância):** os *clocks* dos computadores não são sincronizados, e os *clocks* dos canais COM e MON não são sincronizados. Assim, os canais e computadores usam dados amostrados de sensores e sistemas externos em tempos diferentes, o que aumenta a robustez aos processos de monitoramento.
- **Dissimilaridade de equipamentos (Redundância):** o hardware e software dos FCPCs e FCSCs são diferentes. Ainda, o software dos canais COM e MON foram desenvolvidos por times diferentes usando a mesma especificação. O uso de implementações de projeto separadas reduziu a influencia em potencial de falhas de modo comum ou erros de códigos de software.
- **Reconfiguração das leis de controle:** se são constatados certos tipos de falhas ou problemas de processamento, o sistema de comando de voo altera para uma lei de controle de mais baixo nível, pois conclui que o sistema não é mais capaz de prover as proteções de envelope de voo com os níveis de confiabilidade necessários.
- **Segregação física:** os computadores foram instalados em localizações diferentes na aeronave, que auxiliam na prevenção de uma perda total na funcionalidade no caso de alguns tipos de eventos. O roteamento de linhas hidráulicas e elétricas também foi segregado.

5. NORMAS E RECOMENDAÇÕES AEROESPACIAIS APLICADAS A SEUs

No setor espacial, encontramos normas e recomendações que contém abordagens para a realização de atividades que visam a garantia de robustez de sistemas eletrônicos embarcados a SEEs, sendo que algumas foram brevemente descritas no capítulo 2.

O setor aeronáutico não tem em sua literatura a mesma riqueza de informações e experiência em lidar com os SEEs, considerando-se que se trata de um efeito com estudos mais recentes e os impactos do ambiente de radiação ionizante em sistemas eletrônicos embarcados aeronáuticos serem menores comparativamente aos sistemas eletrônicos embarcados espaciais.

Neste capítulo, procuram-se identificar e descrever os principais pontos abordados na nas normas e recomendações, no que se referirem aos SEUs e ao objeto de estudo deste trabalho, de modo a se ter subsídios para a discussão das recomendações para garantia de robustez a SEU em sistemas eletrônicos embarcados aeroespaciais do capítulo seguinte.

5.1. Normas da ECSS

5.1.1. ECSS-E-ST-10C

A norma intitulada "*System Engineering General Requirements"* (Requisitos Gerais para Engenharia de Sistemas), especifica os requisitos de implementação da Engenharia de Sistemas para o desenvolvimento de produtos e sistemas espaciais. Destaca-se dentre seus objetivos principais: implementar os requisitos de engenharia de sistemas para assegurar uma base técnica robusta e minimizar o risco técnico e custo de projeto de sistemas e produtos espaciais; especificar as tarefas essenciais de Engenharia de Sistemas, seus objetivos e saídas; implementar a integração e controle de disciplinas de engenharia.

A Figura 5.1, extraída da norma, mostra as funções e fronteiras da Engenharia de Sistemas.

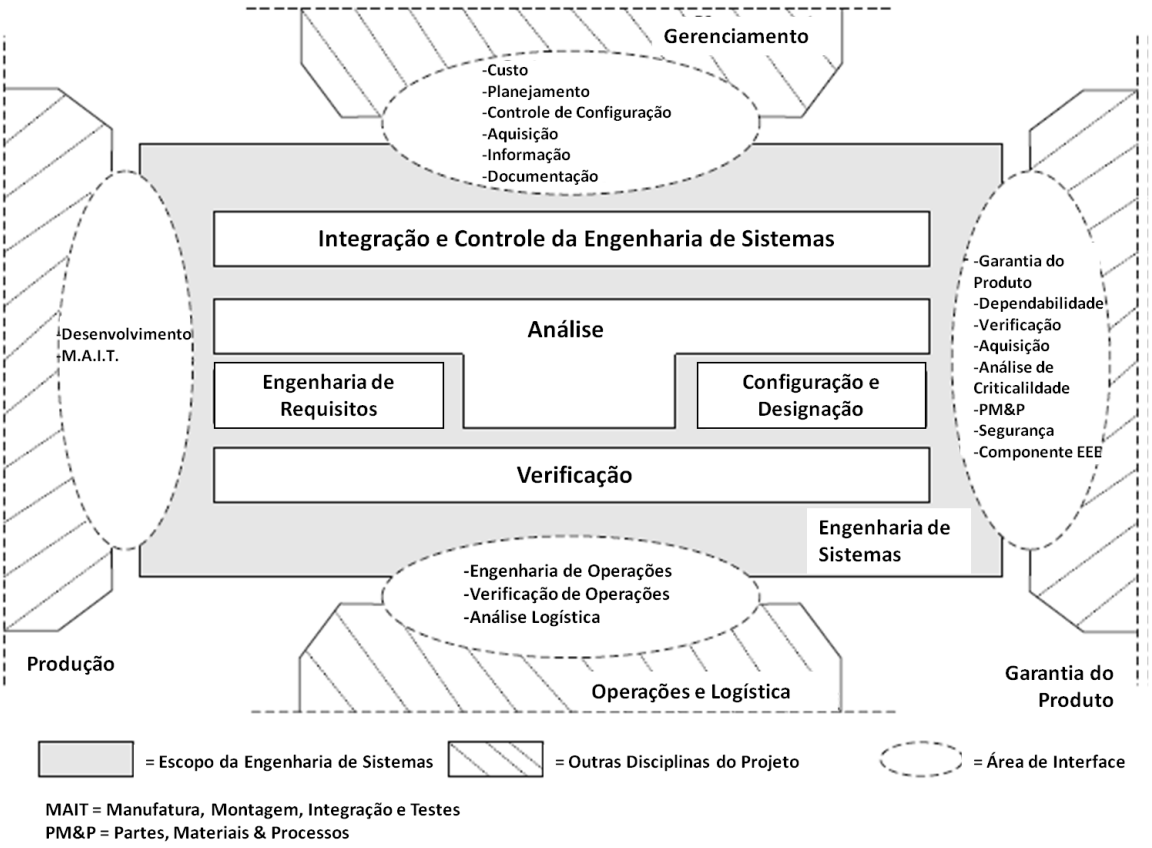

Figura 5.1 – Funções e Fronteiras da Engenharia de Sistemas
Fonte: adaptado de ECSS-E-ST-10C (2009).

O documento mostra quais são as atividades de Engenharia de Sistemas que devem ser desenvolvidas para cada uma das seguintes fases de projeto:

- **Fase 0:** Análise da missão – Identificação das necessidades
- **Fase A:** Viabilidade
- **Fase B:** Definição Preliminar
- **Fase C:** Definição Detalhada
- **Fase D:** Qualificação e Produção
- **Fase E:** Operação/Utilização

- **Fase F:** Descarte

A norma contém requisitos que exigem o estabelecimento e a análise da influência de todos os tipos de ambiente durante todo o ciclo de vida do produto, considerando condições normais e extremas, além das incertezas que possam advir da análise destes ambientes. A norma ECSS-E-ST-10-04C, descrita na sequência desta proposta, é explicitamente referenciada para uso como suporte na definição e estabelecimento de processo de garantia da robustez a efeitos de partículas e radiações ionizantes no ambiente espacial. Especificamente o item 5.3.2 (Ambientes do Sistema e fatores de projeto e teste) requer que a influência de todos os tipos de ambientes para todos os perfis de operação seja estabelecida, em termos de condições nominais e extremas, além dos critérios de qualificação e aceitação, testes e margens aplicáveis para o projeto.

No item 5.3.4 (métodos de análise, ferramentas e modelos), é requerido que a precisão e limitações dos testes sejam consideradas quando se estabelecer os desempenhos e as condições ambientais para a verificação do produto. Na etapa de verificação (5.5), as condições de configuração e condições ambientais para verificação do produto e critérios para qualificação e aceitação devem ser estabelecidas.

Outro ponto de destaque é a parte relativa à confecção do Plano de Engenharia de Sistema (*System Engineering Plan* - SEP), que segundo a norma define as abordagens métodos, procedimentos, recursos e organização para coordenar e gerenciar todas as atividades necessárias para especificar, projetar, verificar, operar e manter um sistema ou produto de acordo com os requisitos do cliente. Este plano deve definir o processo e controle para atingir os requisitos para especificar o ambiente natural para todos os regimes no espaço. Estes requisitos estão na norma ECSS-E-ST-10-04.

5.1.2.ECSS-E-ST-10-04

A norma ECSS-E-ST-10-04C intitulada "*Space Environment*" (Ambiente Espacial), define o ambiente natural do espaço e modelos gerais para alguns ambientes induzidos. Na norma há a definição de alguns termos de relevância para o trabalho, como a seguir:

- **Partícula energética**: partículas as quais, no contexto dos efeitos de radiação em sistemas espaciais, podem penetrar as camadas externas da espaçonave. Para elétrons, é tipicamente acima de 100 keV, enquanto que para prótons e outros íons é acima de 1 MeV. Nêutrons, raios gama e raios X também são considerados partículas energéticas.
- ***Single-Event Upset* (SEU), *Single-Event Effect* (SEE), *Single-Event Latch-up* (SEL):** efeitos resultantes de deposição de energia por partículas únicas e quando a deposição de energia é suficiente para causar efeitos observáveis.

O Capítulo 9 da norma – Radiação de Partículas Energéticas provê uma visão geral do ambiente de radiação por partículas energéticas e seus efeitos, os requisitos para definição de ambiente de radiação de partículas energéticas e preparação de uma especificação de ambiente de radiação. Na introdução do capítulo, identifica que os ambientes de radiação são elementos para se considerar antes da Fase A na seleção da órbita, ao se considerar tanto o efeito na carga paga quanto na plataforma do satélite. Considera também que a especificação de ambiente de radiação para uma missão é estabelecido quando todos os tipos de radiação são considerados, refletindo-se em potenciais susceptibilidades específicas para aquela missão, sendo assim usada para seleção de componentes.

O item 9.2 (Requisitos para Ambientes de Radiação de Partículas Energéticas) estabelece os modelos para estimar o fluxo de cada tipo de partícula e fontes de radiação ionizantes (fluxos de radiação dos cinturões de radiação, dos eventos de partículas solares e raios cósmicos, etc.). Define os modelos para

os fluxos de radiação dos cinturões de radiação (Modelos AE8 (elétrons) e AP8 (prótons), levando em consideração o ciclo solar e respectiva atividade (Solar MAX ou Solar MIN). O Anexo I deve ser usado para SEUs, pois os modelos são mais adequados para efeitos acumulativos e as variações estatísticas de fluxo são importantes para este efeito. Há ainda um requisito que leva em conta a deriva da SAA, que devido ao campo geomagnético deve ser considerada aproximadamente 0,3º a cada ano a partir de 1960. Para os SEPEs são considerados adequados o modelo CREME 96 ou as tabelas do Anexo B. Para as partículas de raios cósmicos, indica o modelo ISO 15390.

O item 9.3 (Preparação de uma Especificação de Ambiente de Radiação) define que uma especificação do ambiente de radiação para o sistema espacial deve ser estabelecida, e ainda o que deve ser incluído nesta especificação. Para SEUs, basicamente requer os espectros de energia para as partículas que foram consideradas pelos modelos definidos no item anterior, a variação orbital dos fluxos das fontes de radiação (cinturões de radiação, Solar e raios cósmicos) e eventuais contribuições de fontes radiativas a bordo. Por fim, indica que as incertezas nos resultados devem ser consideradas nas análises de risco e na especificação de margens de projeto.

5.1.3.ECSS-E-ST-10-12

A norma ECSS-E-ST-10-12C intitulada *“Methods for the Calculation of Radiation Received and its Effects, and a Policy for Design Margins”* (Métodos para Cálculo de Radiação Recebida e seus Efeitos, e uma Política para Margens de Projeto), cobre os métodos para o cálculo de radiação recebida e seus efeitos, e uma política para margens de projeto. Considera todos os efeitos do ambiente natural e induzidos, como TID e DD. No escopo do trabalho, são aplicáveis os métodos para efeitos de SEUs nos sistemas eletrônicos embarcados. A norma ainda pode ser complementada pela ECSS-E-HB-10-12 *”Radiation Received and Its Effects and Margin Policy Handbook”* (Manual para Radiação Recebida e seus Efeitos, e uma Política para Margens de Projeto).

Algumas definições importantes extraídas da norma são repetidas a seguir:

- **Carga crítica:** menor quantidade de carga recebida em um componente por um impacto de uma partícula carregada que resulta em um SEE.
- **Seção de Choque *(Cross-Section)*:** probabilidade de ocorrência de SEE por unidade de partícula incidente. Medido experimentalmente como o número de SEEs registrado considerando um fluxo de partículas.
- **Fluência:** integral no tempo do fluxo de partículas.
- **Fluxo:** número de partículas atravessando uma superfície por unidade de área por unidade de tempo. É frequentemente expressado pela quantidade de partículas acima de um dado valor de energia que atravessam uma unidade de área por unidade de tempo (e.g. elétrons $cm^{2}s^{-1}$).
- **Radiação ionizante:** transferência de energia por meio de partículas onde a mesma tem energia suficiente para remover elétrons ou realizar interações elásticas ou inelásticas com núcleos (incluindo o deslocamento de átomos), incluindo fótons e na faixa de energia de raios-X e acima.
- **Transferência Linear de Energia (*Linear Energy Transfer* - LET):** energia transferida pela radiação ionizante para um material. É normalmente usada para descrever o rastro de ionização causado pela passagem de um íon, sendo dependente do material o qual a partícula transfere energia, da massa da partícula energética e também sendo função da energia da partícula.
- **Limiar da Transferência Linear de Energia (*Linear Energy Transfer threshold - LET_{th}*):** LET mínimo para causar um SEE quando a partícula atravessa o volume sensível em um circuito.

- **Margem:** fator ou diferença entre a especificação de projeto de ambiente para um produto ou dispositivo e o ambiente no qual o comportamento inaceitável ocorre.
- **Volume Sensível:** região de coleta de carga de um componente.

A norma tem quatro definições diferentes para o termo “Margem de Projeto para Radiação” (*Radiation Design Margin* – RDM). Para o presente trabalho é importante a definição para SEEs não destrutivos, que é a razão entre a robustez de projeto para SEE e a taxa de ocorrência de SEE no ambiente previsto. Neste caso, a robustez de projeto para SEE é a taxa de ocorrência de SEE aceitável que o equipamento ou missão pode experimentar e ainda atender os requisitos de confiabilidade e disponibilidade do equipamento.

O principal objetivo da norma é prover uma abordagem para aplicar tais margens de projeto na medida correta, levando em conta as incertezas em procedimentos de testes, variações entre lotes de componentes e incertezas no ambiente de radiação. De acordo com a norma, esta aplicação correta tem efeitos importantes na engenharia de sistemas, pois um nível muito alto, que levaria a considerar um ambiente muito severo, implicaria em acréscimos de custos e/ou degradação de desempenho desnecessário. Por outro lado, uma margem muito baixa pode resultar em desempenho comprometido ou falhas prematuras.

O capítulo 4 discute alguns dos princípios para a correta avaliação e tratamento dos efeitos de radiação no projeto de um sistema espacial. A Tabela 5-1 abaixo resume as atividades que devem ser realizadas durante o projeto.

Tabela 5-1 – Estágios de um projeto e as análises de efeitos de radiação realizadas

Fase	Atividade
Pré fase A	Especificação do ambiente para cada opção de missão; Análise preliminar das susceptibilidades e disponibilidades dos componentes.
Fase A	Especificação de ambiente para o *baseline* da missão e opções que forem retidas para consideração; Análise preliminar das susceptibilidades e disponibilidade dos componentes.
Fase B	Atualização da especificação de ambiente, requisitos de garantia de robustez incluindo análise detalhada dos requisitos de componentes e identificação da disponibilidade de dados de susceptibilidade; Estabelecimento e execução de planos de testes para componentes.
Fase C e D	Análises precisas de efeitos de radiação (incluindo análise específica de componentes)*; Consolidação de resultados de testes; testes mais precisos.
Fase E	Investigação dos efeitos de radiação; consideração dos efeitos de radiação na investigação de anomalias; retorno para os grupos de engenharia das lições aprendidas incluindo, por exemplo, as anomalias relacionadas à radiação.
* Se as premissas da missão mudarem nesta fase, como por exemplo, a órbita proposta, uma reavaliação completa da especificação de ambiente deve ser realizada.	

Fonte: Adaptado da ECSS-E-ST-10-12C (2008).

O capítulo 5 (Margens de Projeto para Radiação) especifica os requisitos para tratar e estabelecer as RDM. O item 5.1 provê as justificativas para geração das RDM e os critérios usados para tal, enquanto que os itens posteriores (5.2 a 5.6) estabelecem os requisitos a serem cumpridos.

O capítulo 9 descreve os SEEs, identifica algumas tecnologias e componentes suscetíveis a SEEs e especifica os métodos a serem usados para calcular as taxas de SEEs para um sistema espacial. O item 9.2 estabelece os requisitos para os ambientes relevantes (cinturões de radiação, radiação solar e raios cósmicos, por exemplo). O item 9.3 identifica tecnologias susceptíveis a SEE, na Tabela 9-1. A Tabela 5-2 abaixo é um extrato desta tabela, para as tecnologias consideradas susceptíveis a SEUs:

Tabela 5-2 – SEEs em potencial como função da tecnologia do componente e família

Tipo de componente	Tecnologia	Família	Função
Circuitos integrados	CMOS BiCMOS SOI	Digital	SRAM
			DRAM/SDRAM
			FPGA
			Micro controlador
		Sinal Misto	ADC
			DAC
	Bipolar	Digital	Não definido
		Linear	

Fonte : adaptado da ECSS-E-ST-10-12C (2008).

O item 9.4 define requisitos para definição dos parâmetros e taxas de ocorrências de SEEs. Os subitens 9.4.1.1, 9.4.1.2, 9.4.1.3 e 9.4.2 são aplicáveis para SEUs.

5.1.4.ECSS-Q-ST-60-15

A norma ECSS-Q-ST-60-15C intitulada *"Radiation Hardness Assurance - EEE components"* (Garantia de Robustez à Radiação – Componentes EEE), especifica os requisitos para assegurar a garantia de robustez à radiação (RHA) de projetos espaciais. Estes requisitos formam a base para estabelecimento do intitulado programa de Garantia de Robustez à Radiação (*Radiation Hardness Assurance* – RHA) para um projeto espacial, tratando de TID, DD e SEEs. Para esta norma, os componentes EEE são entendidos como elétricos mecânicos e eletrônicos, não englobando nesta definição, componentes como células solares e outros materiais.

O capítulo 4 descreve em alto nível o processo de RHA e as principais atividades deste programa em cada fase do projeto de um sistema espacial. A Figura 5.2 abaixo ilustra uma visão geral do processo:

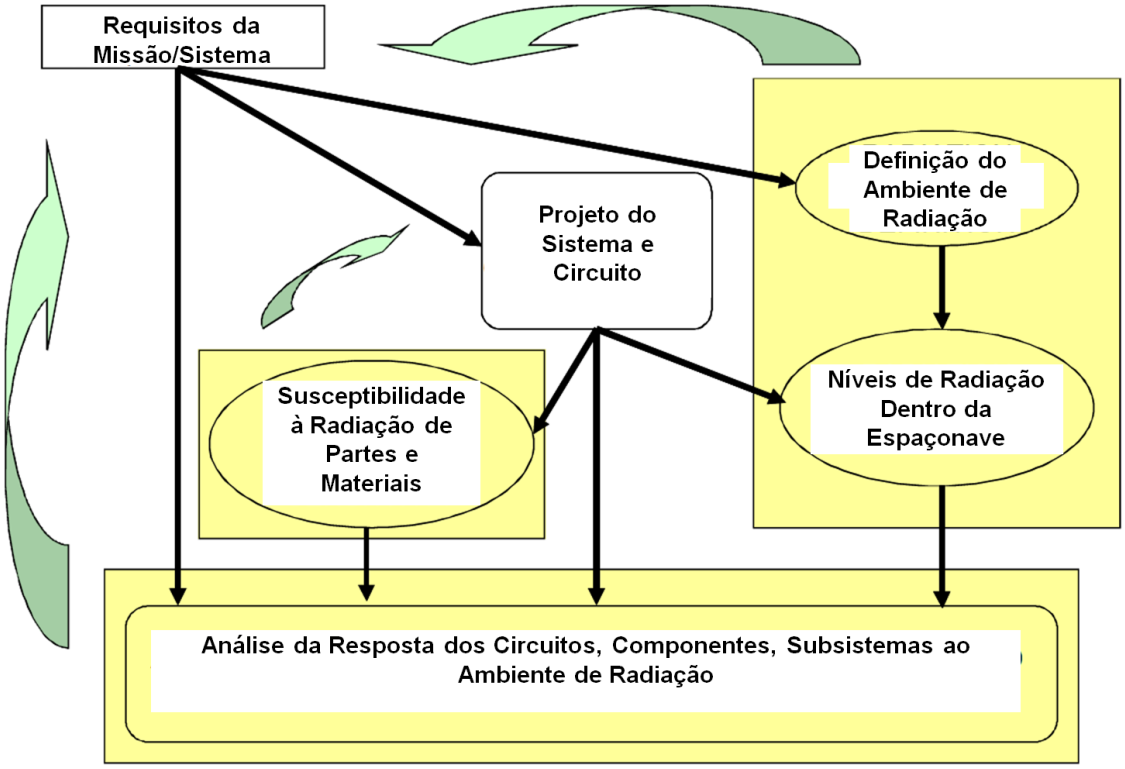

Figura 5.2 – Visão Geral do Processo de RHA
Fonte: adaptado da ECSS-Q-ST-60-15C (2012).

Este processo segue uma abordagem iterativa e *top-down*, em que o ambiente de radiação da missão é especificado atendendo os requisitos da missão e os modelos de ambiente de radiação e regras definidas na ECSS-E-ST-10-04. Os requisitos de alto nível derivados desta especificação são empregados como ponto de partida. Na sequência, quando necessário, o ambiente de radiação é levado para o nível de componente, de acordo com os métodos descritos na ECSS-E-ST-10-12. A análise de radiação é realizada no nível do equipamento. A susceptibilidade à radiação de cada componente é definida e seu impacto no desempenho do equipamento é analisado. Um projeto eletrônico do equipamento é validado quando o equipamento é capaz de atender aos requisitos aplicáveis ao serem expostos ao ambiente de radiação do espaço com uma RDM suficiente.

A norma indica que a análise de SEEs é realizada geralmente durante a FMECA conforme a norma ECSS-Q-ST-30-02, item 6.4.2.2. O impacto operacional do SEE de cada componente é analisado e sua criticalidade verificada baseada na taxa de ocorrência de SEE com uma RDM apropriada.

O capitulo 5 descreve os requisitos para o programa de RHA, sendo que o item 5.3 é específico para SEEs.

5.1.5.ECSS-Q-ST-30-02

A norma ECSS-Q-ST-30-02C intitulada *“ Failure Modes, Effects (and Criticality) Analysis (FMEA/FMECA)”* (Análise de Modos de Falha, Efeitos (e Criticalidade (FMEA/FMECA)), define os procedimentos e requisitos relacionados à realização de FMEA/FMECA nos elementos do projeto espacial de modo a se atender os requisitos da missão assim como os objetivos de dependabilidade e segurança, levando em conta as condições ambientais do projeto.

O Capítulo 4 da norma define os requisitos para a FMEA, estabelecendo as categorias de severidade de falhas funcionais conforme a Tabela 5-3 abaixo:

Tabela 5-3 – Severidade das consequências das falhas funcionais

Categoria de severidade	Nível de severi-dade	Efeitos de dependabilidade (conforme especificado na ECSS-Q-ST-30)	Efeitos na segurança (conforme ECSS-Q-ST-40)
Catastrófico	1	Propagação de falhas	Perda de vidas, ameaça à vida ou ferimentos permanentemente desabilitantes ou doenças ocupacionais.
			Efeitos ambientais negativos severos.
			Perda de estações de lançamento.
			Perda de sistema.
Crítico	2	Perda da missão	Ferimentos temporariamente desabilitantes, mas não ameaçando a vida, ou doença ocupacional temporária.
			Grandes efeitos ambientais negativos.
			Grandes danos a propriedades públicas ou privadas.
			Grandes danos a sistema de voo de interface.
			Grandes danos a estações em terra.
Maior	3	Grande degradação da missão	*
Menor ou insignificante	4	Pequena degradação da missão ou qualquer outro efeito	*

* não especificado pela norma

Fonte: Adaptado da ECSS-Q-ST-30-02C (2009).

O capítulo 5 estabelece os requisitos para realização da FMECA, considerando que a mesma é uma extensão da FMEA do capítulo 4, pois se atribui adicionalmente um valor numérico (*criticality number* - CN) para o modo de falha funcional. Este valor é obtido de acordo com o índice de severidade (*severity number* – SN, de 1 a 4, sendo que 1 é o menos severo e 4 o mais severo) e o de probabilidade da falha (*probability number* – PN, de 1 a 4, sendo que 1 é o menos provável e 4 o mais provável), de maneira que CN = SN x PN. A Tabela 5-4 abaixo mostra a relação entre estes índices; em laranja, estão indicados os valores de CN considerados críticos, e em verde os considerados aceitáveis. A probabilidade de ocorrência de uma falha está correlacionada com o índice PN na parte superior direita da tabela. A norma não deixa clara qual a base de tempo para o valor (por missão, ano, etc.).

Tabela 5-4 – Severidade, Probabilidade de Ocorrência e Índice de criticalidade associados

Categoria de severidade	SN	Probabilidade de ocorrência			
		10^{-5}	10^{-3}	10^{-1}	1
		PN			
		1	2	3	4
Catastrófico	4	4	8	12	16
Crítico	3	3	6	9	12
Maior	2	2	4	6	8
Menor/Insignificante	1	1	2	3	4

Fonte: Adaptado da ECSS-Q-ST-30-02C (2012).

O capítulo 6 define os requisitos de implementação da FMEA/FMECA conforme as fases de desenvolvimento do projeto do sistema espacial.

O Anexo G indica alguns modos de falha para componentes ao se considerar o ambiente espacial. Por exemplo, para micro circuitos, devem ser considerados

os modos de falha por SEEs, indicado na norma como *Single Event Phenomena* - SEP.

5.2. Normas da NASA

A seguir são descritos os pontos de algumas normas e recomendações da NASA que estão relacionados aos efeitos de SEUs causados por radiação ionizante no espaço.

5.2.1.NASA RP 1350

O guia *NASA Reference Publication 1350,* intitulado "*The Natural Space Environment: Effects on Spacecraft*" (O Ambiente Natural do Espaço - Efeitos sobre Espaçonaves) provê uma visão geral do ambiente natural do espaço e seus efeitos em projetos de sistemas espaciais, descrevendo diversos ambientes além do de radiação ionizante. Seu objetivo principal é contribuir para um melhor entendimento do ambiente espacial para se minimizar riscos e custos.

As partes relacionadas a SEUs estão nas paginas 18 e 19 onde é descrito o que é denominado de Ambiente Solar, enquanto que nas páginas 20 e 21 são discutidos alguns pontos importantes sobre o ambiente de radiação ionizante no espaço

5.2.2.NASA RP 1390

O guia *NASA Reference Publication 1390,* intitulado "*Spacecraft System Failures and Anomalies Attributed to the Natural Space Environment*" (Falhas em Sistemas de Espaçonaves e Anomalias Atribuídas ao Ambiente Natural do Espaço) provê uma visão geral dos efeitos em vários subsistemas de espaçonaves, apresentando mais de 100 casos de falhas em espaçonaves e anomalias documentadas de 1974 a 1994 que foram atribuídas ao ambiente natural do espaço.

A figura 1 do guia reúne os ambientes, as principais preocupações dentro de um programa espacial e trabalho em relação a cada ambiente, e os modelos

sugeridos para caracterização dos ambientes. Assim, o ambiente de radiação ionizante no espaço é formando por Radiação de prótons/elétrons dos cinturões de radiação, raios cósmicos galácticos e eventos de partículas solares, sendo que as preocupações típicas no projeto de sistemas eletrônicos espaciais embarcados são SEUs, e os modelos/base de dados sugeridos são CRÈME, AE–8MIN, AE–8MAX, AP–8MIN, AP–8MAX, RadBelt e Solpro.

A figura 2 da norma resume os efeitos do ambiente espacial nos diversos subsistemas indicando o ambiente responsável por causar tais efeitos. Para sistemas eletrônicos espaciais embarcados, a radiação ionizante é responsável por causar degradação por SEUs causando erros de bits e mudança de bits.

O documento contém registro de diversos casos de efeitos da radiação ionizante em sistemas espaciais embarcados que causaram SEEs. A seguir são reproduzidos alguns dos registros:

- ***Hipparcos:*** Após mais de 3 anos de operações eficientes e com sucesso, as comunicações com o satélite astronômico Hipparcos da ESA foram encerradas em 15 de agosto de 1993. Em junho de 1993, o satélite encontrou dificuldades em comunicações entre o computador embarcado e a estação em terra. As causas do problema foram atribuídas ao dano por radiação em alguns componentes. Após tentativas de reiniciar as operações terem se mostrado sem sucesso, as operações da missão foram encerradas.
- ***GOES-5:*** A unidade de telemetria central deste satélite geoestacionário sofreu 10 SEUs durante 1989, seis dos quais foram associados com eventos de partículas solares. Também, um grande evento de partículas solares em 19 de outubro de 1989 danificou a eletrônica de um conjunto de painéis solares e diminuiu a corrente de saída do conjunto em 0,5A.
- ***HST(STS-31):*** Em 7 de maio de 1990, alterações de bit (*bit flips,* ou seja, SEUs) ocorreram na memória RAM de uma eletrônica de guiagem e por conseqüência afetou o sistema de guiagem do HST enquanto passava

pela SAA. O software embarcado foi modificado para compensar as mudanças de bit. Em julho de 1990, a SAA também causou alterações no sistema de guiagem. Isto resultou em falhas na aquisição de dados de posicionamento de estrelas. Na seqüência, o uso do sistema de guiagem foi suspendido enquanto na região da SAA. Ambos os incidentes são suspeitos de serem ocasionados por efeitos do ambiente de radiação ionizante intensa na região da SAA.

5.2.3.NASA 431-REF-000273

O documento 431-REF-000273 emitido pela NASA intitulado "*Single Event Effect Criticality Analysis*" (Análise de Criticalidade de Efeitos de Partícula Única) é um guia cujo objetivo é ser um guia para a análise dos efeitos dos eventos de partícula única (SEEs) baseado em critérios de criticalidade, desempenho, disponibilidade e custo.

O documento SEECA é específico para tratamento dos SEEs, expondo as preocupações sobre o ambiente de radiação ionizante, os efeitos em componentes eletrônicos e taxas de ocorrência de SEEs, análise de propagação e métodos para reduzir o impacto de SEEs.

Na parte 1, Introdução, expõe os argumentos para uma abordagem de se projetar um sistema espacial embarcado tolerante à radiação em contraste a um imune a radiação. Seu principal argumento é que o projeto de sistemas imunes à radiação não é possível e nem efetivo em custo, e as decisões que deverão ser tomadas dentro do processo de engenharia de sistemas ao se considerar os SEEs levarão em conta disponibilidade, desempenho, prazos e custo, o que inviabilizaria uma solução puramente imune à radiação.

A parte 2 descreve alguns dos principais pontos da análise de SEEs, focada nas funções executadas pelos sistemas e suas respectivas criticalidades, e propõe duas ferramentas para serem usadas nesta análise.

Para a primeira ferramenta, define um índice de criticalidade para as funções executadas pelos sistemas dividindo-as em três grupos de criticalidade: *error-*

functional, *error-vulnerable*, e *error-critical*. As funções do grupo *error-functional* podem ser afetadas por SEEs, e uma alta probabilidade de SEEs pode ser aceita. As funções *error-vulnerable* podem ser afetadas por SEEs com um baixo grau de probabilidade. As funções *error-critical* não podem ser afetadas por SEEs. A Figura 5.3 abaixo ilustra esta primeira ferramenta, que é uma árvore de decisão para avaliação dos riscos de SEEs em relação à criticalidade das funções executadas pelo sistema em questão:

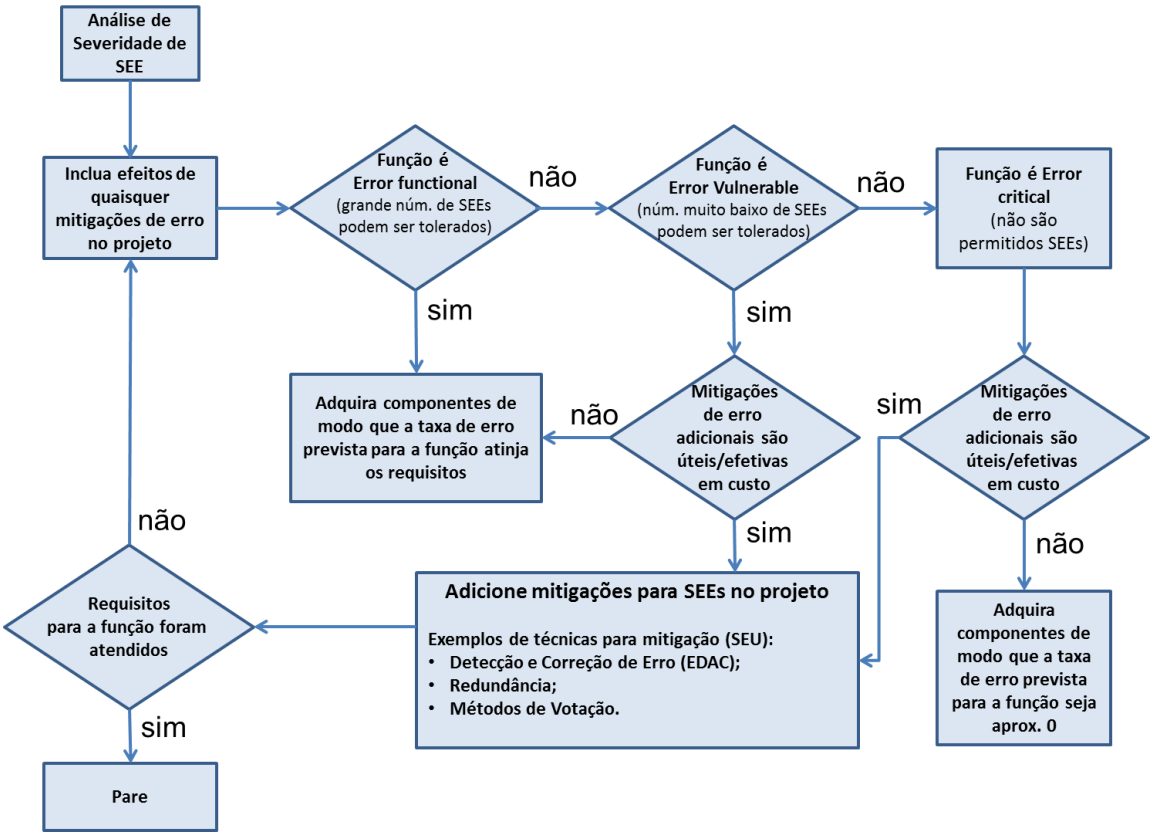

Figura 5.3 – Árvore de decisão dos riscos de SEEs em relação à criticalidade da função realizada pelo sistema
Fonte: Adaptado de NASA 431-REF-000273 (1996).

O item 2.5 discute a criação de requisitos de projeto para SEEs, do nível de requisitos funcionais descendo até o nível de requisitos de componentes, e define a segunda ferramenta para analise de criticalidade. Na árvore de decisão da Figura 5.3, os requisitos para probabilidade de ocorrência de SEUs para os três grupos de criticalidade são diretamente ligados ao risco aceitável.

Quanto mais crítico for um SEE para um desempenho operacional, tanto mais restrito o requisito de SEE deve ser. Os requisitos são especificados para cada grupo funcional determinando-se a máxima probabilidade aceitável de ocorrência de SEE para cada categoria. Cada tipo de SEE (*latchup, gate rupture*, SEU, etc.) pode gerar um valor diferente de probabilidade aceitável de ocorrência. Estes requisitos são especificados para o nível funcional, e são cumpridos por meio de diversos recursos incluindo mitigação por hardware, esquemas via software, robustez de dispositivos, redundância, etc.

A Figura 5.4 mostra a segunda ferramenta, que consiste em um fluxograma para geração de requisitos de SEEs para um dispositivo, onde um requisito funcional não necessariamente se traduz em um requisito para o dispositivo, pois dependerá da criticalidade da função e o requisito funcional associado.

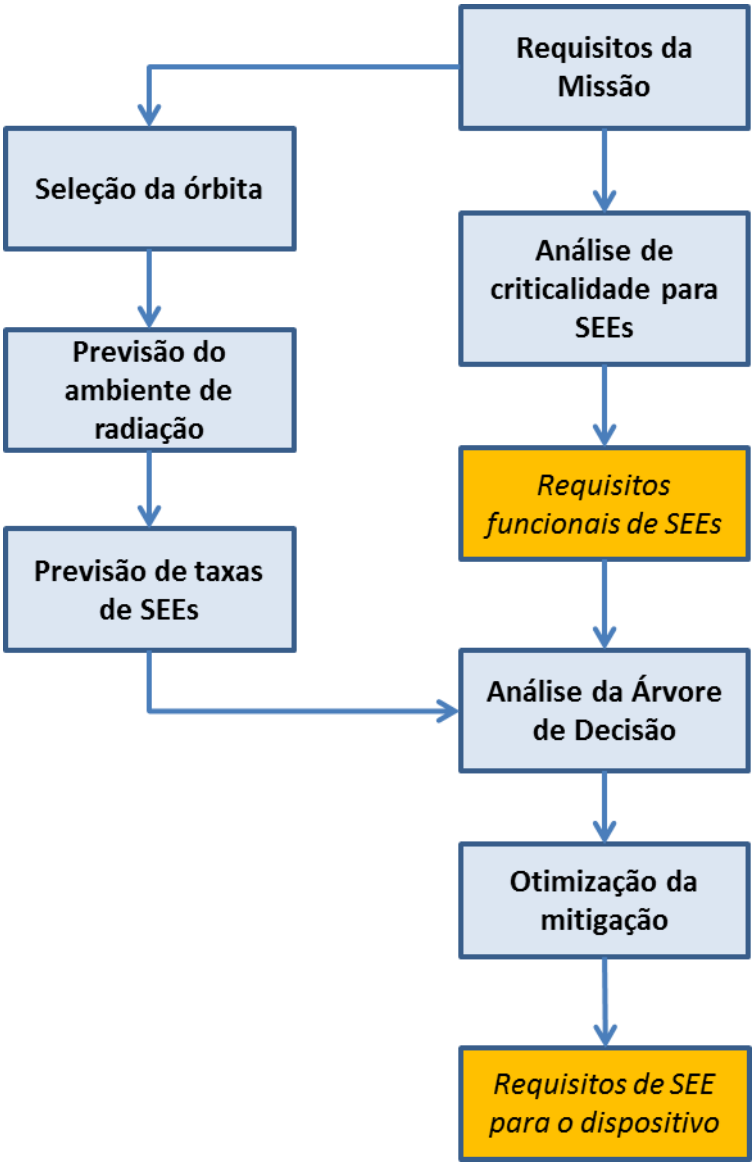

Figura 5.4 – Fluxograma para geração de requisitos de SEEs para dispositivo
Fonte: Adaptado de NASA 431-REF-000273 (1996).

O item 3 discute a definição de ambiente de radiação ionizante e características deste para órbitas de satélites. Este ambiente deve ser definido considerando dois cenários: um “normal”, em que o sistema irá operar em fluxos médios das fontes de radiação e se deve analisar o sistema na operação normal, e outro “pior caso”, que considerando os picos de fluxo das fontes (cinturões de radiação ou um SEPE) deve-se analisar o sistema para falhas catastróficas (perda de dados essenciais, danos permanentes em partes do

sistema, etc.). A Tabela 5-5 abaixo é um sumário das fontes de radiação no espaço, resumindo as fontes, os modelos sugeridos, o efeito do ciclo solar na fonte, e variações, considerando um satélite operando em órbita baixa.

Tabela 5-5 – Sumário das fontes de radiação

Fonte de Radiação	Modelos	Efeitos do Ciclo Solar	Variações
Prótons aprisionados	AP8-MIN AP8-MAX	Mínimo Solar – maior Máximo Solar - menor	Campo geomagnético SEPEs Tempestades geomagnéticas
Íons de raios cósmicos galácticos	CREME CHIME Badhwar & O'Neill	Mínimo Solar – maior Máximo Solar - menor	Níveis de ionização (da partícula)
Prótons de SEPEs	SOLPRO JPL92	Grande número (de SEPEs) durante o máximo Solar Pouco durante o mínimo Solar	Atenuação da órbita Localização do SEPE no Sol
Íons pesados de SEPEs	CREME JPL92 CHIME	Grande número (de SEPEs) durante o máximo Solar Poucos durante o mínimo Solar	Atenuação da órbita Localização do SEPE no Sol

Fonte: Adaptado de NASA 431-REF-000273 (1996).

O item 4 discute e explica os efeitos da radiação ionizante na eletrônica embarcada, algumas formas de se testar esta eletrônica para SEEs e ainda como estimar as taxas de ocorrências de SEEs.

O item 5 discute sobre como analisar a propagação dos SEEs e seu impacto a nível de sistema. Propõe uma metodologia, ilustrada na Figura 5.5, para a análise no nível de componente:

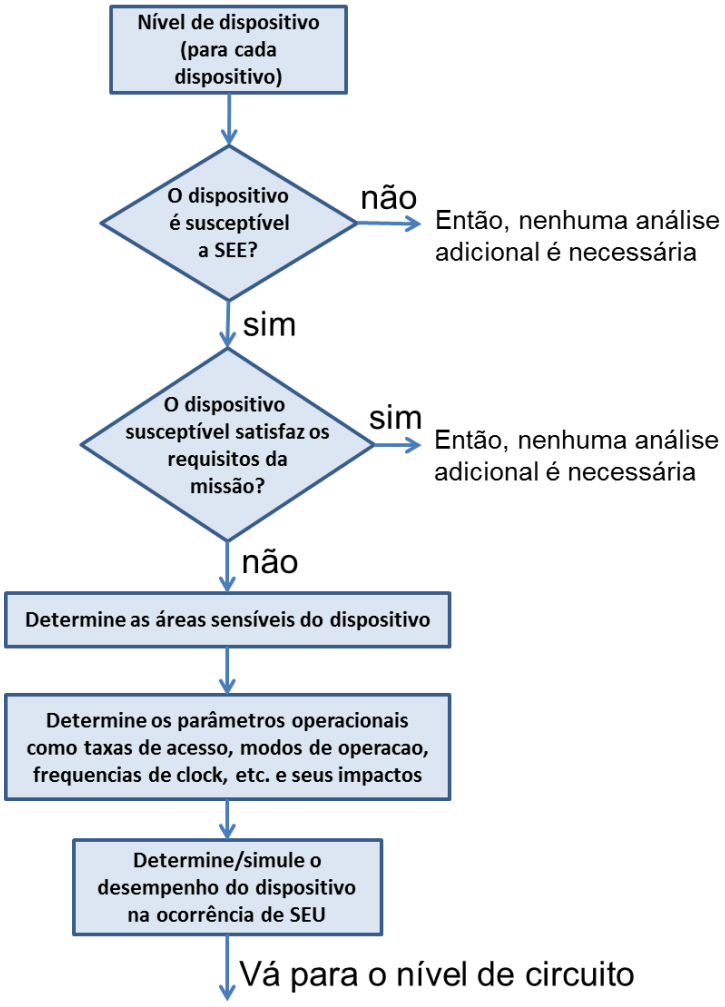

Figura 5.5 – Metodologia para análise de propagação de SEUs
Fonte: Adaptado de NASA 431-REF-000273 (1996).

A primeira pergunta, “O dispositivo é suscetível a SEU?” é direta: se não, não é preciso continuar a análise; se sim, é feita a pergunta seguinte, “O dispositivo atende aos requisitos da missão?”, pois um dispositivo que tem uma

susceptibilidade conhecida a SEU pode ainda cumprir os requisitos da missão. Na sequência, devem-se determinar as áreas do dispositivo susceptíveis a SEU, para saber onde e quais tipos de SEUs podem ocorrer. Sugere o uso da Tabela 5-6, reproduzida na sequência, dividindo os SEUs em dois tipos: *bit flip* (mudança de estado) que tipicamente ocorrem em células de memórias ou *flip flops*, e transitórios, que podem se manifestam em lógica combinatória ou se manifestam como “pulso de ruído de tensão” tanto em áreas digitais e analógicas do CI, alertando para o fato de que a tabela não é uma lista exaustiva, mas uma amostra dos tipos de dispositivos a se considerar em um projeto:

Tabela 5-6 – Áreas Susceptíveis de Dispositivos a SEUs

Tipo de Dispositivo	Áreas Susceptíveis	Tipos de SEU
Memórias	Células de memória	*Bit flips*
	Lógica de controle	*Bit flips* se sequencial, transitórios se combinatória
Lógica combinatória	Lógica combinatória	Transitórios
Lógica sequencial	Lógica sequencial	*Bit flips*
FPGAs	Lógica combinatória	Transitórios
	Lógica sequencial	*Bit flips*
Microprocessadores	Registradores, cache, lógica de controle sequencial	*Bit flips*
	Lógica de controle combinatória	Transitórios
ADCs, DACs	Porção analógica	Transitórios
	Porção digital	*Bit flips* ou transitórios dependendo do projeto
CIs lineares	Área analógica	Transitórios
Fotodiodos	Fotodiodo	Transitórios

Fonte: Adaptado de NASA 431-REF-000273 (1996).

Na sequencia, determinam-se os parâmetros operacionais. Parâmetros como taxas de amostragem, modos operacionais, frequências de *clock*, tensão da fonte de alimentação, etc. podem impactar não na ocorrência, mas nos efeitos observáveis de um SEU. Por fim, deve-se explorar a determinação de quais efeitos aparentes o SEU terá no desempenho do dispositivo, como por

exemplo, operação indevida, saída incorreta, erros em estruturas de memórias que serão acessadas externamente, etc.

Na análise a nível de circuito, sugere o fluxograma da Figura 5.5 adaptado e sem as etapas de decisão (uma vez que a susceptibilidade já foi determinada no nível anterior), com foco na operação e desempenho do circuito, embora não ilustre nem detalhe os fluxogramas. O mesmo é sugerido para os níveis superiores (subsistema, sistema, espaçonave).

O item 7 descreve em alto nível algumas das tarefas dentro do desenvolvimento de sistemas embarcados no que se referem a SEEs. Em resumo, são as seguintes:

- Previsão do ambiente de radiação/partículas ionizantes;
- Requisitos funcionais de alto nível para SEE;
- Requisitos em nível de *part number* para SEE;
- Testes de SEE e verificação de projeto.

5.3. Normas e Recomendações da Indústria Aeronáutica

A seguir são descritas algumas das normas e recomendações da indústria aeronáutica que estão relacionadas às recomendações para garantia da robustez de sistemas eletrônicos embarcados a SEUs causados por radiações ionizantes.

5.3.1. ARP-4754

A ARP-4754A (*Aerospace Recommended Practice*) intitulada *Guidelines for Development of Civil Aircraft and Systems* (Recomendações para o Desenvolvimento de Aviões e Sistemas Civis) tem como escopo os sistemas considerados complexos ou altamente integrados. O termo "**complexo**" refere-se a sistemas cujo atendimento aos requisitos de segurança não é explicitado somente por testes e cuja lógica é difícil de compreender sem o auxílio de ferramentas analíticas. O termo "**altamente integrado**" refere-se a sistemas que executam ou contribuem para múltiplas funções na aeronave.

A ARP 4754A tem um papel central no conjunto de normas que auxiliam no processo de desenvolvimento de sistemas aeronáuticos embarcados, que pode ser mais bem entendido na Figura 5.6, que ilustra a relação entre normas usadas na aviação para desenvolvimento de sistemas eletrônicos embarcados considerados complexos ou altamente integrados:

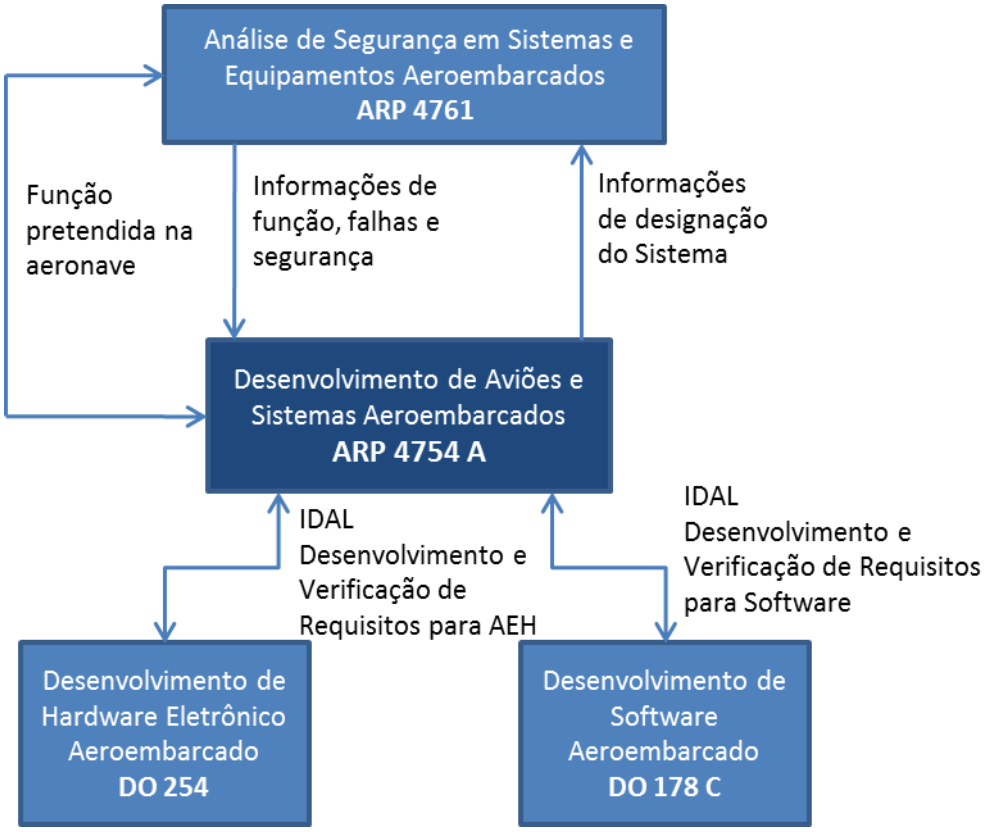

Figura 5.6 – Principais documentos que cobrem as fases de desenvolvimento de projetos aeronáuticos
Fonte: adaptado da ARP 4754A (2010).

Neste processo, as funções executadas por uma aeronave são alocadas para sistemas que irão implementar estas funções. De modo a analisar a criticalidade destas funções, são realizadas as Análises Funcionais de Perigos (FHA). Em um primeiro momento, as funções nível aeronave são analisadas quanto à criticalidade da consequência de suas falhas funcionais (perda da função, mau funcionamento, operação inadvertida, etc.). As funções executadas pelo sistema passam por uma FHA nível sistema, de modo a identificar a criticalidade das funções e subfunções que o mesmo realiza (ARP 4761, 1996).

As condições de falha funcional são classificadas de acordo com sua severidade, conforme a Tabela 5-7. Esta classificação é um dos pontos chave do processo de desenvolvimento do sistema, pois o rigor no seu

desenvolvimento será conforme esta classificação, que varia do nível A, cuja consequência pode ser a perda da aeronave e vidas humanas, até E, em que não haveria efeitos na segurança operacional da aeronave e pessoas, mostrado na Tabela 5-7.

Tabela 5-7 – Classificação da Severidade das Condições de Falha Funcional

Classificação da Severidade das Condições de Falha Funcional	**Nível de Garantia de Desenvolvimento (*Development Assurance Level* – DAL) Atribuído à Função**
Catastrófico	A
Perigoso/ Maior Severo	B
Maior	C
Menor	D
Sem efeito na Segurança	E

Fonte: Adaptado da ARP 4754A (2010).

Os níveis de criticalidade são traduzidos em Níveis de Garantia de Desenvolvimento (*Development Assurance Levels* – DAL). A versão A da ARP 4754 introduziu o conceito de Nível de Garantia de Desenvolvimento da Função (*Function Development Assurance Level* - FDAL) e Nível de Garantia de Desenvolvimento do Item (*Item Development Assurance Level* - IDAL). Basicamente, o FDAL é atribuído diretamente da análise funcional, e está ligado à criticalidade da função executada pelo sistema, enquanto que o IDAL está ligado ao item (LRU, software, AEH, etc.) do sistema que implementa a função. O IDAL é atribuído também de acordo com a criticalidade da função implementada, entretanto pode ser menor que o FDAL, desde que atenda a critérios de independência funcional e redundância, definidos pela norma em

seu item 5.2. O rigor e disciplina exigidos para o desenvolvimento do sistema e item serão exigidos conforme estas classificações.

Durante o desenvolvimento do sistema e alocação das funções para os itens, é realizada uma análise preliminar de segurança, chamada de *Preliminar System Safety Assessment* – PSSA, que avalia a arquitetura proposta, buscando avaliar e determinar se o sistema atende aos requisitos atribuídos ao mesmo. Os modos de falhas dos componentes do sistema são avaliados conforme as conseqüências de falhas funcionais identificadas na FHA.

A natureza iterativa da dinâmica do desenvolvimento dos sistemas ou aeronave é mais bem traduzida pela norma ao se definir os chamados Processos Integrais (*Integral Processess*). Estes são chamados assim porque que são usados durante todas as etapas do ciclo de desenvolvimento (desenvolvimento das funções da aeronave, alocação das funções da aeronave para sistemas, desenvolvimento da arquitetura do sistema, alocação dos requisitos dos sistemas aos itens e implementação do sistema), e são os seguintes:

- Análise de Segurança (*Safety Assessment*);
- Definição dos Níveis de Garantia de Desenvolvimento (DALs);
- Captura de Requisitos;
- Validação de Requisitos;
- Gerenciamento de Configuração;
- Garantia de Processo;
- Coordenação com as Autoridades de Certificação e Regulação;
- Verificação da Implementação.

5.3.2. ARP-4761

A ARP-4761, intitulada Guidelines *and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment* (Diretrizes e Métodos para Conduzir o Processo de Análise da Segurança em Sistemas e

Equipamentos Aeroembarcados Civis), descreve diversas ferramentas para condução do processo de Análise da Segurança (*Safety Assessment*). Algumas dessas ferramentas foram descritas no item 2.5.2.

5.3.3.DO-178C

A DO-178C, intitulada "*Software Considerations in Airborne Systems and Equipment Certification*" (Considerações de Software sobre a Certificação de Sistemas e Equipamentos Aeroembarcados). Esta revisão foi emitida em dezembro de 2011 em substituição à revisão B, com o objetivo de melhorar as recomendações tendo em vista os avanços nas metodologias de desenvolvimento de softwares embarcados e outros pontos explicitados em seu Anexo A. É importante destacar que a revisão foi coordenada com a ARP 4754A, emitida em dezembro de 2010.

A DO-178C explicita os processos de Planejamento, Desenvolvimento, Verificação, Controle de Configuração e Garantia da Qualidade.

5.3.4.DO-254

A DO-254, intitulada "*Design Assurance Guidance for Airborne Electronic Hardware*" (Diretrizes de Garantia de Projeto para Hardware Eletrônico Aeroembarcado) é um documento publicado pela Comissão Rádio-Técnica para a Aeronáutica (*Radio Technical Comission for Aeronautics*- RTCA).

O processo da DO-254 gera requisitos para hardware eletrônico de acordo com o Nível de Garantia de Desenvolvimento (DAL), semelhantes aos utilizados na ARP 4754A. Descreve cinco processos principais para o projeto de hardware: Captura de Requisitos, Projeto Conceitual, Projeto Detalhado, Implementação, e Transição para Produção. Tais processos podem ser aplicados aos componentes de uso aeroespacial, como *Programmable Logic Devices* (PLDs) e *Field Programmable Gate Arrays* (FPGAs).

Assim como na DO-178C, os requisitos de hardware devem se originar de requisitos de sistema e a definição dos Níveis de Garantia de Desenvolvimento de sistema associados.

5.3.5.CM – SWCEH - 001

O documento CM – SWCEH – 001 – "*Development Assurance of Airborne Electronic Hardware"* (Garantia de Desenvolvimento de Hardware Eletrônico Embarcado), é um *Certification Memorandum* (Memorando de Certificação - CM) emitido pela EASA. Os CM esclarecem o curso de ação da EASA para itens específicos de certificação, não estabelecendo novos requisitos e não sendo de cumprimento obrigatório. Sua intenção é fornecer recomendações adicionais em um assunto para demonstrar cumprimento com requisitos ou normas vigentes. O propósito deste CM é fornecer material para guiar nos aspectos de certificação associados ao uso de hardware eletrônico em sistemas eletrônicos aeroembarcados, dentro do escopo das normas relacionadas e organizadas na Figura 5.6, mais especificamente aos aspectos ligados à RTCA DO-254.

O item 6 - *Guidelines for Single Event Effects* (Recomendações para SEEs), recomenda duas abordagens complementares para tratar os SEEs em hardware eletrônico embarcado:

- Uma abordagem ***top-down*** (geralmente realizada pelo requerente à certificação):
    - Uma vez que um SEE pode ter um impacto no nível aeronave/motor uma análise de SEE deve ser realizada naquele nível, para examinar a susceptibilidade dos componentes de hardware aos SEEs. Por exemplo, a probabilidade de um SEE pode ser definida baseada na altitude de cruzeiro de uma aeronave. O objetivo é que o fabricante da aeronave ou motor defina as regras de projeto relacionadas à SEE aplicáveis a todos

os fornecedores. Estas regras são definidas com respeito à arquitetura do sistema e seu DAL/FDAL designado.

- Uma abordagem ***bottom-up*** (geralmente realizada pelo fornecedor do equipamento/sistema):
    - Uma vez que alguns componentes são mais susceptíveis a SEE que outros, há uma necessidade de: 1) identificar as falhas que podem ocorrer em cada um dos componentes de hardware devido a SEEs e 2) demonstrar como estas falhas devido a SEEs são contidas e/ou mitigadas no nível do componente, placa, equipamento, sistema ou aeronave/motor (o requerente é envolvido na etapa final).

Conclui o item informando que qualquer abordagem alternativa, que forneça o mesmo nível de confiança, pode ser aceito, se justificado adequadamente.

5.3.6.SIB 2012-09

O documento EASA *Safety Information Bulletin* 2012-09, "*Effects of Space Weather on Aviation"* (Efeitos do Clima Espacial na Aviação), emitido em maio de 2012, é de caráter informativo para a comunidade aeronáutica, incluindo projetistas de aeronaves, sobre os efeitos do clima espacial em componentes eletrônicos, serviços de navegação e comunicação e em seres humanos.

O documento faz uma lista dos sistemas e serviços que são afetados pela radiação Solar e galáctica, relacionando os eventos com a consequência nos sistemas. Os sistemas aviônicos são afetados principalmente por prótons dos SEPEs e o fluxo de partículas de radiação cósmica modulado pelo ciclo Solar. Dentre as considerações de risco, o documento cita como fatores, além do aumento das rotas e voos polares, os vôos a altas altitudes e a integração dos sistemas aviônicos.

Recomenda que os fabricantes de aeronaves, projetistas de sistemas aviônicos e fabricantes de componentes eletrônicos embarcados trabalhem

conjuntamente para avaliar os potenciais efeitos da radiação Solar e galáctica nos níveis de componente, sistema e avião, de modo a conceberem sistemas que sejam tolerantes às falhas causadas por tais fenômenos.

5.3.7.SIB 2012-10

O documento da EASA *Safety Information Bulletin* 2012-10, "*Single Event Effects (SEE) on Aircraft System caused by Cosmic Rays"* (SEEs em Sistemas de Aeronaves causados por Raios Cósmicos), emitido em maio 2012, é um informativo que se aplica aos sistemas aviônicos de aeronaves críticos, considerando falhas que podem ser atribuídas aos SEEs.

Informa que os efeitos de SEEs nos sistemas aviônicos, como por exemplo, displays, comando de voo *fly-by-wire* e FADEC (*Full Authority Digital Engine Control*), podem variar desde uma falha de hardware até um efeito não observado no nível de sistema (apenas localmente). Considera que os diversos casos de mau funcionamento de sistemas em campo, em que ao se testar este sistema novamente, resulta no chamado *no fault found* (sem falha encontrada), são provavelmente causados por SEEs. Ainda, pela característica do fenômeno, não considera que todos os sistemas sejam afetados simultaneamente.

Assim como o SIB 2012-09, recomenda que os fabricantes de aeronaves, projetistas de sistemas aviônicos e fabricantes de componentes eletrônicos embarcados trabalhem conjuntamente para avaliar os potenciais efeitos da radiação solar e galáctica nos níveis de componente, sistema e avião, de modo a conceberem sistemas que sejam tolerantes às falhas causadas por tais fenômenos.

5.3.8.IEC TS 62396-1

A IEC Technical Specification 62396-1, intitulada "*Accommodation of Atmospheric Radiation Effects Via Single Event Effects within Avionics Electronic Equipment*" (Acomodação dos Efeitos de Radiação Atmosférica por

Efeitos de Partícula Única em Equipamentos Eletrônicos Aviônicos) é uma norma específica para tratar os SEEs em sistemas aeronáuticos.

Em seu item *5 – Radiation Environment of the Atmosphere* (Ambiente de Radiação na Atmosfera), são descritas as principais fontes de radiação ionizante na atmosfera (radiação Solar e raios cósmicos galácticos) e a geração das chamadas partículas secundárias como nêutrons, prótons, píons e múons que resultam das colisões das partículas das fontes de radiação com os átomos da atmosfera. O foco maior é dado aos principais parâmetros que afetam o fluxo e níveis de energia de nêutrons secundários (altitude, latitude, variações no ciclo Solar e SEPEs). Os nêutrons são considerados pela norma como os principais causadores de SEEs e, portanto, as partículas a serem consideradas nos testes e análises de SEEs para sistemas aviônicos. Os nêutrons térmicos são também considerados, e são tratados separadamente no Anexo A da norma, que recomenda o uso da IEC TS 62396-5.

O item 6 - *Effects of Atmospheric Radiation on Avionics* (Efeitos da Radiação Atmosférica nos Aviônicos) descreve os principais efeitos da radiação ionizante em sistemas aviônicos e o impacto nas tecnologias atualmente usadas nestes sistemas. Por exemplo, apresenta os argumentos que justificam descartar efeitos como TID e DD como efeitos relevantes na eletrônica embarcada em aeronaves, e alerta para a tendência a aumentos significativos da susceptibilidade das tecnologias futuras à MBUs.

O item 7 – *Guidance for System Designs* (Recomendações para Projetos de Sistemas), recomenda uma abordagem que é ilustrada na Figura 5.7. A norma informa que esta abordagem é consistente com as normas utilizadas em sistemas aeronáuticos para desenvolvimento de sistemas complexos (ARP 4754) e realização da análise de segurança (ARP 4761) da Figura 5.6:

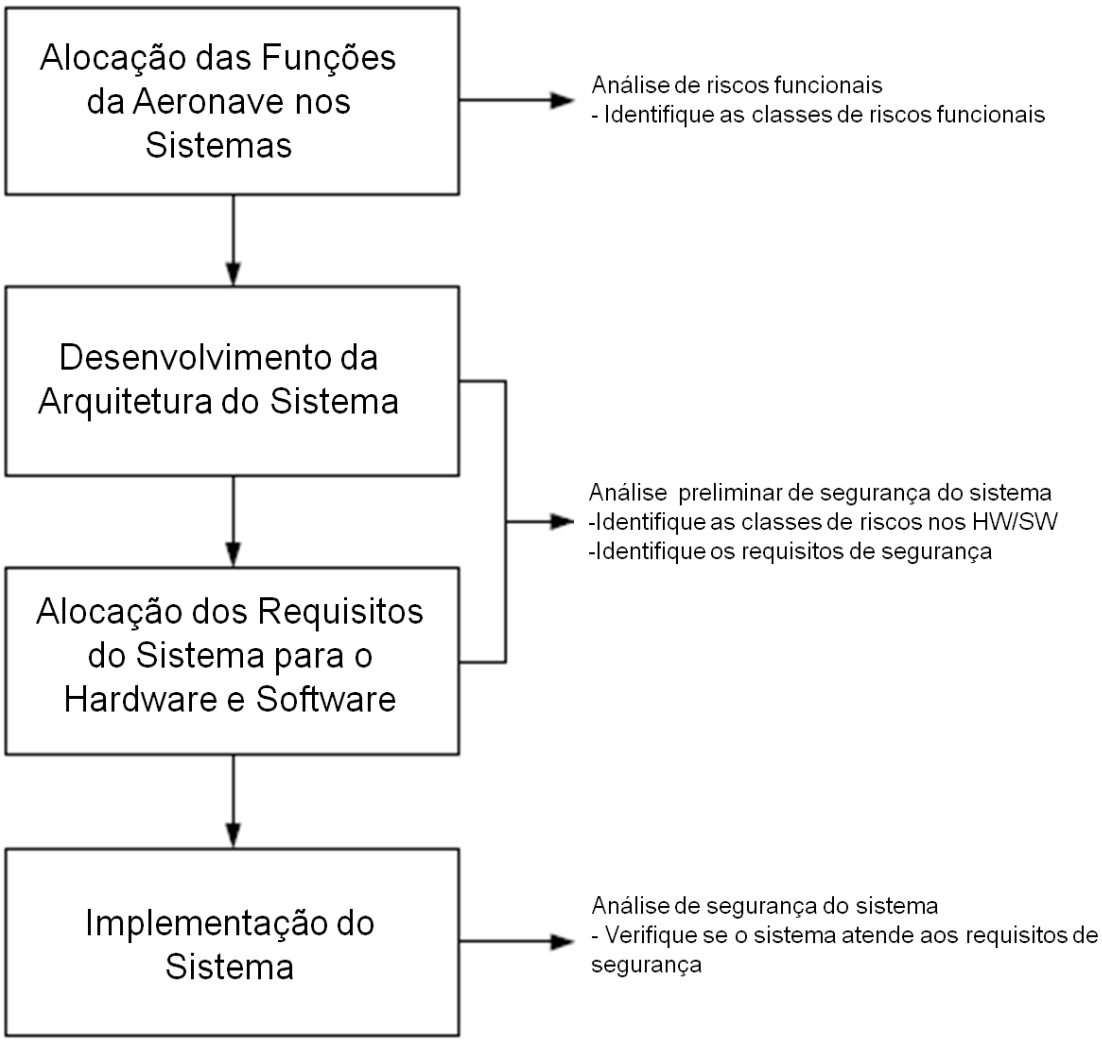

Figura 5.7 – Processo de análise de segurança de sistemas segundo IEC TS 62396-1
Fonte: adaptado da IEC TS 62396-1 (2012).

O processo é descrito pela norma da seguinte maneira: o primeiro passo no processo de desenvolvimento é a alocação das funções no nível avião para os sistemas que irão implementar estas funções, e o uso da FHA identifica os riscos e os classifica de acordo com a consequência da falha funcional (a classificação dos DALs, que será a principal referência no rigor do desenvolvimento do sistema). Em geral os SEEs não causam uma condição de falha em particular e adicional a outros já considerados na análise tradicional de FHA, portanto não precisa ser incluído como um risco em separado na FHA.

Os Níveis de Garantia de Desenvolvimento (DAL), que são gerados de acordo com a consequência da falha funcional, associada à função no nível da aeronave implementada no sistema, irão guiar o rigor e disciplina desenvolvimento do sistema.

Durante o desenvolvimento da arquitetura, e alocação dos requisitos do sistema em software e hardware, uma PSSA é realizada, já considerando a arquitetura a ser implementada à luz do atendimento dos requisitos de segurança. Uma vez que os SEEs não induzirão novos modos de falha este fenômeno deve ser incluído. Conforme os efeitos de SEEs, o PSSA irá considerar aqueles que causam falhas permanentes e não permanentes separadamente. O impacto da fase de voo deverá ser considerado, uma vez que a probabilidade de SEE é maior em cruzeiro do que em outras fases, como decolagem ou pouso. Os resultados do PSSA irão demandar ações de mitigação, identificando quaisquer mitigações na arquitetura que sejam necessárias. Durante a implementação, a designação é completada e verificada. O SSA é realizado para verificar e documentar que o sistema, conforme designado e construído, atende os requisitos de segurança. Assim, todas as taxas de SEE serão incluídas no SSA. A Figura 5.8 abaixo mostra a relação dos SEEs com os efeitos no nível de LRUs e sistema:

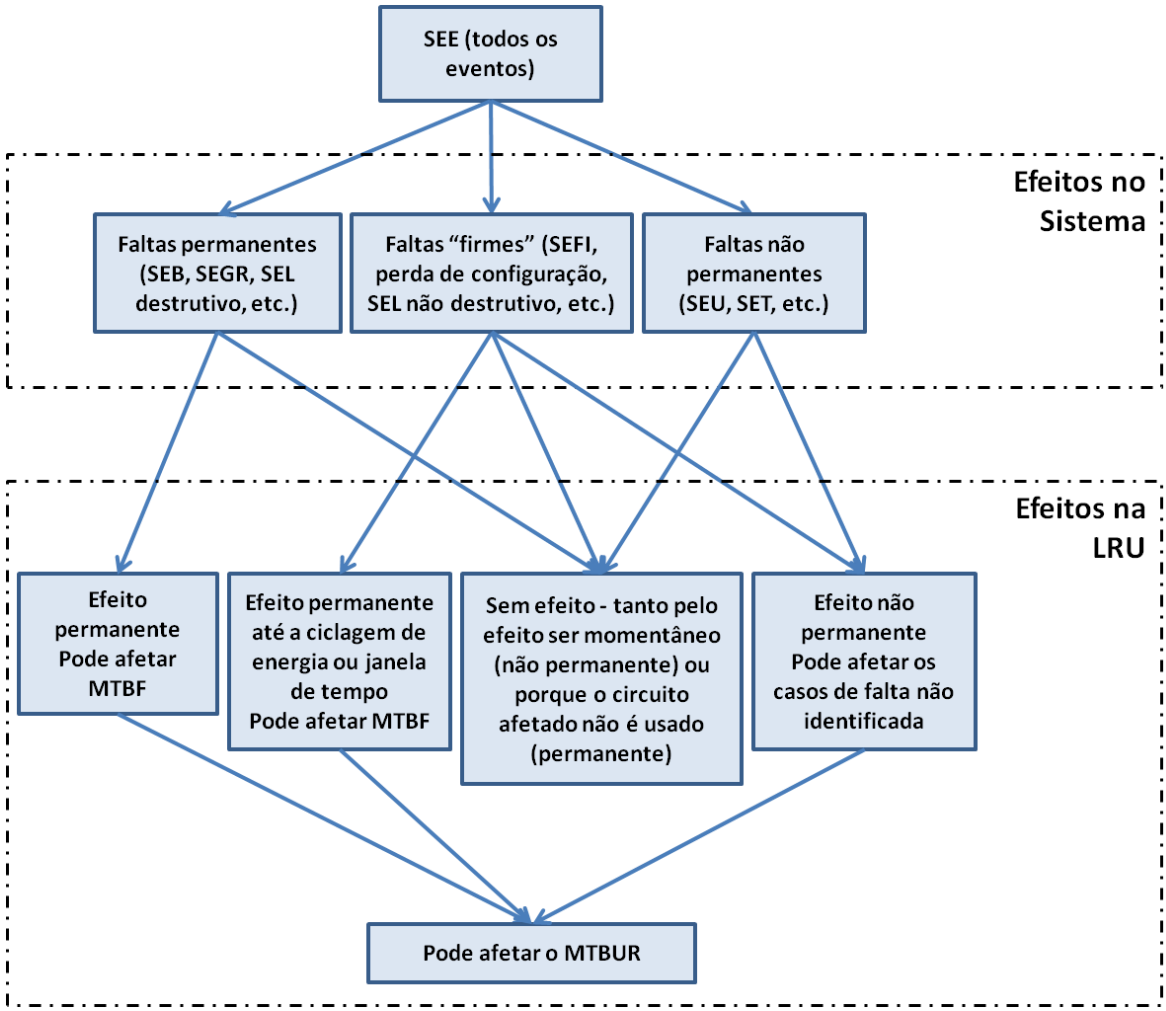

Figura 5.8 – SEEs em relação ao efeito no sistema aeronáutico e LRU
Fonte: adaptado da IEC TS 62396-1 (2012).

A norma considera que os SEEs são eventos aleatórios e atualmente raros o suficiente para demandar ações para sistemas e partes que implementam funções com níveis de criticalidade acima de DAL C. Considera também que as falhas permanentes de SEEs (SEL destrutivo, SHE, SEB, etc.) tem taxas de falhas muito pequenas para os sistemas aviônicos, na faixa de 1.10^{-6} a 1.10^{-7} falha/dispositivo X hora, embora devam ser consideradas no desenvolvimento do sistema.

De acordo com a norma, a base para se tratar adequadamente os riscos de SEEs é a taxa de falha do efeito. A disciplina e rigor associados à

determinação da taxa de SEE podem variar, desde a determinação de taxa de um dispositivo pela caracterização real (teste com nêutrons), até a similaridade com uma classe de dispositivos com uma taxa estimada de SEEs. Este rigor e disciplina na caracterização da taxa de SEE são derivados da criticalidade da função desempenhada pelo sistema/LRU. Esta caracterização é descrita a seguir:

Sistemas Nível A:

Os sistemas nível A são caracterizados em dois grupos: Nível A Tipo I e Nível A Tipo II. O Tipo I envolve sistemas onde a função critica é executada sem o piloto estar diretamente no fluxo de execução/troca de informações como, por exemplo, um sistema de comando de voo *fly-by-wire*. O Tipo II se refere a sistemas onde a função critica é executada com o piloto inserido no fluxo de execução/troca de informações como, por exemplo, um sistema de displays que forneça informações críticas de altitude, atitude e velocidade da aeronave. Esta divisão se dá porque as falhas e maus funcionamentos de um sistema Tipo I podem contribuir mais diretamente e abruptamente para uma falha catastrófica que um sistema Tipo II. Assim, a caracterização das taxas de SEEs para sistemas nível A deve ser feita da seguinte maneira:

Nível A Tipo I:

Um dos métodos a seguir deve ser empregado:

- Taxas de SEEs em componentes eletrônicos podem ser derivados de testes com nêutrons em partes específicas usadas no projeto, expondo-as em um laboratório adequado, como por exemplo, o Los Alamos WNR. A precisão deste método é de um fator de aproximadamente 2 na taxa de eventos.
- Taxas de SEEs em componentes eletrônicos podem ser derivadas também de testes com prótons em partes específicas usadas no projeto expondo-as a feixes de prótons de alta energia (< 100 MeV). A precisão deste método é de um fator de aproximadamente 3 na taxa de eventos.

- Pode ser realizado um teste de SEE em equipamento ou sistema aviônico *"in-the-loop"* no nível de sistema, como descrito no Anexo B.1 da norma. A precisão deste método é de um fator de aproximadamente 2 a 3 na taxa de eventos dependendo da partícula a ser usada.
- Quando não houver dados de nenhum dos testes acima ou tais testes forem inviáveis, então os métodos para Nível A Tipo II podem ser usados, entretanto um fator mínimo na taxa de eventos, que seja considerado razoável, deve ser aplicado sobre os valores calculados por tais métodos.

Estes tipos de sistemas requerem os controles mais robustos de desempenho e tecnologia dos dispositivos. Os controles de tecnologia devem ser estabelecidos para monitorar as mudanças do fornecedor no dispositivo que possam impactar as taxas de falhas de SEEs.

Nível A Tipo II

As taxas de SEE devem ser baseadas em:

- O rigor/disciplina estabelecido para nível A tipo I ou
- Uma abordagem menos rigorosa/disciplinada usando um dos seguintes métodos:
    - Uso de informação proprietária e dados aplicáveis a SEEs, por exemplo, silício em isolante (SOI) e determinada camada epitaxial tolerante à radiação para impedir *latchup* e memórias não contiguas para evitar MBU. A precisão deste método é de um fator de aproximadamente 2 na taxa de eventos.
    - Irradiação de itens de um equipamento aviônico individual contendo uma variedade de partes potencialmente susceptíveis como descritas no Anexo B.2 da norma.
    - Quaisquer das seguintes ferramentas de engenharia que possam ser aplicadas por especialistas em efeitos de radiação de SEEs:

        - Uso de dados processados de SEE de íons pesados usando uma abordagem analítica para obter dados de SEEs por nêutrons (ver Anexo B.3). A precisão deste método é de um fator de aproximadamente 10 na taxa de eventos.
        - Uso de dados de SEE de nêutrons/prótons em tipos de componentes específicos (ver Anexo B.3). A precisão deste método é de um fator de aproximadamente 10 na taxa de eventos.
    - Uso de dados genéricos de SEE baseados na tecnologia básica do componente e tipo (por exemplo, CMOS SRAM) (ver Anexo B.4); pode ser usado quando não há dados relevantes de SEE para o componente. A precisão é de um fator de aproximadamente 10 na taxa de eventos, pois é um método inerentemente conservativo.
    - Uso de testes de SEEs de componentes por simulação a laser, usando um laser que foi calibrado usando um dispositivo de referência do mesmo tipo funcional (por exemplo, SRAM), e tamanho e tecnologia similares (veja B.5). A precisão deste método é de um fator de aproximadamente 10 na taxa de eventos.

Estes tipos de sistemas requerem os controles mais robustos de desempenho e tecnologia dos dispositivos. Os controles de tecnologia devem ser estabelecidos para monitorar as mudanças do fornecedor no dispositivo que possam impactar as taxas de falhas de SEES.

Nível B

As taxas de SEE devem ser baseadas em:

- O rigor/disciplina estabelecido para nível A ou

- Taxas de falhas de SEE rastreáveis aos testes de SEE em componentes similares usando resultados de testes em laboratórios que não usaram nêutrons, ver Anexos B.3, B.4 e B.5 da norma.

Estes tipos de sistemas requerem controles moderados de desempenho e tecnologia dos dispositivos com garantias periódicas de que nenhuma mudança do fornecedor no dispositivo impacte as taxas de falhas de SEEs.

Nível C

As taxas de SEE devem ser baseadas em:

- O rigor/disciplina estabelecido para nível B ou
- Taxas de falhas de SEE rastreáveis aos testes de SEE via um modelo de taxas de falhas de SEE (uso de uma taxa de erros de SEE média para todos os componentes potencialmente susceptíveis – nestes casos, a taxa de erros de SEE pode ser alta para alguns componentes e baixa para outros, mas é esperado que a taxa total do equipamento seja aceitável).

Estes tipos de sistemas usam as praticas normais de controle e notificação de mudança dos dispositivos. As mudanças devem ser analisadas quanto ao impacto nas taxas de falhas de SEEs. O impacto de mudança de um dispositivo será rastreado por produto (identificar as tendências indicando grandes acréscimos nas taxas de falhas).

O item 8 da norma contém recomendações e abordagens sugeridas para se determinar as taxas de SEEs nos equipamentos aviônicos, e algumas considerações sobre a potencial susceptibilidade de tipos de semicondutores como SRAM, DRAM, etc. A metodologia simplificada para se calcular as taxas de SEE considera dois fatores:

- O primeiro é a seção de choque, definido pela norma como a relação entre a área sensível do dispositivo e a probabilidade de interação de uma partícula que depositaria uma carga crítica suficiente para ocorrer um SEE. Em outras palavras, o valor obtido ao se medir o número de

SEEs dividido pela fluência de partículas que o dispositivo foi exposto, o que resulta em uma medida de cm^2 por dispositivo ou por bit.

- O segundo é um fluxo nominal de 6000 nêutrons/cm^2 por hora, que é um fluxo estimado de acordo com o item 5 para altitude de 12,2km (40 kft) e latitude de 45º, ao se considerar os nêutrons com energia acima de 10 MeV. Este fluxo pode ser ajustado para outras altitudes e latitudes conforme Anexo D. Ainda, esta revisão da norma considera que as tecnologias de semicondutores com canal de 150 nm e abaixo são potencialmente susceptíveis aos nêutrons com energias acima de 1 MeV, sendo necessário corrigir o valor de fluxo para 9200 nêutrons/cm^2 por hora, (também para uma altitude de 40 kft (12,2 km) e latitude de 45º, ou seja, deve ser corrigido conforme Anexo D conforme necessário).

O item 9 sugere os passos a serem seguidos para se cumprir com os requisitos de segurança e lidar com os SEEs em sistemas aviônicos, descrito a seguir:

- Confirme o ambiente de radiação para a aplicação aviônica: recomendações são descritas no item 5.3, e o grau de acomodação das variações da atividade solar deve ser definida pelo usuário (5.6).
- Identifique o nível de garantia de desenvolvimento do sistema (DAL): o nível de garantia de desenvolvimento vai determinar o rigor e disciplina associado à acomodação dos SEEs.
- Análise do projeto eletrônico preliminar para SEE:
    - Identifique os componentes susceptíveis a SEE de acordo com os itens 6 e 8 da norma.
    - Quantifique as taxas de SEE de acordo com o item 7 e a abordagem de cálculo conforme 8.4.
    - Verifique que os requisitos para o nível de garantia de desenvolvimento do sistema são cumpridos para SEE.

- Combine as taxas de SEE para o sistema inteiro: o acumulo de faltas permanentes pode impactar o MTBF do sistema; faltas não permanentes podem impactar o MTBF e MTBUR. As faltas induzidas por SEEs não destrutivos podem ser toleradas por medidas via software e hardware conforme item 7. Enquanto o equipamento se recupera de erros não permanentes induzidos por radiação, alguns elementos de redundância não estarão disponíveis, e o tempo de recuperação deve ser demonstrado que é aceitável no nível do sistema.
- Gerencie a configuração de partes, pois mudanças de componentes eletrônicos podem afetar suas taxas de SEE.

5.3.9.IEC TS 62396-5

A IEC *Technical Specification* 62396-5, intitulada *"Guidelines for Acessing Thermal Neutron Fluxes and Effects in Avionics Systems"* (Recomendações para Analisar os Efeitos de Fluxos de Nêutrons Térmicos em Sistemas Aviônicos) é uma norma específica para tratar os nêutrons térmicos em sistemas aeronáuticos.

Com base em testes e literatura existente sobre o assunto, recomenda a aplicação da seguinte fórmula, para os componentes os quais contém boro em sua fabricação, e, portanto são susceptíveis a nêutrons térmicos:

Taxa de SEU = Taxa de SEU de nêutrons de alta energia X Razão 1 X Razão 2

(5.1)

Onde:

$Razão\_1 = \frac{\Phi_{termico}}{\Phi_{alta\_energia}}$, razão entre o fluxo de nêutrons térmicos e de alta energia

(5.2)

$Razão\ \_2 = \frac{\sigma_{termico}}{\sigma_{alta\ \_energia}}$, razão entre a seção de choque para nêutrons térmicos e de alta energia

(5.3)

$\Phi_{termico}$ = fluxo de nêutrons térmicos

$\Phi_{alta\ \_energia}$ = fluxo de nêutrons de alta energia

$\sigma_{alta\ \_energia}$ = seção de choque para nêutrons de alta energia

$\sigma_{termico}$ = seção de choque do componente para nêutrons térmicos

Estas fórmulas se aplicam para os componentes que não tem dados de seção de choque e fluxo para nêutrons térmicos. A norma, baseada em dados da literatura de componentes com valores das variáveis acima conhecidas, sugere que se use o valor de 1,1 para a razão 1, ou seja, sugere que o fluxo de nêutrons térmicos é 1,1 vezes o fluxo de nêutrons de alta energia dentro de uma aeronave.

Para a razão 2, sugere um valor de 2,8, ou seja, de que a seção de choque a ser considerada para componentes eletrônicos que usam boro e não se tem dados de teste com nêutrons térmicos, seja 2,8 vezes a seção de choque para nêutrons de alta energia.

6. DISCUSSÃO DAS NORMAS E RECOMENDAÇÕES AEROESPACIAIS E PROPOSTA DE RECOMENDAÇÕES

Este capítulo está dividido em duas partes. A primeira discute as normas e recomendações para garantia de robustez a SEU em sistemas eletrônicos embarcados aeroespaciais descritos no capítulo 5, à luz dos aspectos expostos e discutidos no capítulo 4. A segunda propõe recomendações para garantia de robustez de sistemas eletrônicos embarcados aeroespaciais à SEUs causados por radiações ionizantes.

6.1. Discussão das Normas e Recomendações Aeroespaciais

Algumas características gerais foram identificadas nas normas e recomendações abordadas no capítulo 5 que valem a pena mencionar neste item.

Normas ECSS X normas da NASA: as normas da ECSS em geral são mais prescritivas, definindo de maneira mais objetiva o que deve ser feito em termos de requisitos, enquanto que as normas da NASA tem características mais discursivas, em especial a NASA 431-REF-000273, que aborda praticamente todos os aspectos relacionados a SEUs, recomendando abordagens e dando exemplos de aplicação.

A norma aeronáutica mais diretamente ligada ao escopo deste trabalho, a IEC 62396-1, é mais discursiva e informativa no que se refere à definição do ambiente de radiações ionizantes (item 5 da norma) de demais itens, e mais prescritiva na abordagem de atribuição de valores de taxas de ocorrência de SEUs (item 7 da norma). No geral, sua aplicação é dificultada pela falta de clareza em estabelecer critérios objetivos na definição de ambiente e cálculo de taxas de falhas por SEEs.

Embora tenham sido abordadas diversas normas e recomendações aeronáuticas no capítulo 5, a norma IEC 62396-1, a IEC 62396-5 e o memorando CM – SWCEH – 001 são os únicos documentos que diretamente prescrevem e recomendam abordagens para tratar os SEUs nos projetos de

sistemas aviônicos. Os SIB 2012-09 e 2012-10, embora sejam documentos que tratam especificamente dos efeitos do clima espacial, contém recomendações no sentido de se avaliar e buscar conceber sistemas tolerantes à falhas causadas pela radiação ionizante, portanto em um estágio anterior aos objetivos do presente trabalho.

Fases do projeto de sistemas espaciais: o contexto das normas nos processos de desenvolvimento de sistemas eletrônicos embarcados espaciais está bem definido nas normas da ESA, como é possível ver na Tabela 6-1 abaixo, adaptado da ECSS-E-ST-10-12C. A ECSS-E-ST-10-04C, por exemplo, destaca que a especificação do ambiente de radiação deve ser realizada na Pré-fase A, em acordo com a ECSS-E-ST-10-12C, de modo a ser um importante parâmetro para escolha da órbita da missão.

O documento da NASA 431-REF-000273 permite inferir pela discussão dos diversos itens que a organização das atividades e as correspondentes fases do projeto são semelhantes ao conjunto de normas da ESA.

Tabela 6-1 – Estágios de um projeto e normas da ESA envolvidas nas análises de efeitos de radiação

Fase	Atividade	Normas Envolvidas
Pré-fase A	Especificação do ambiente para cada opção de missão; Análise preliminar das susceptibilidades e disponibilidades dos componentes.	ECSS-E-ST-10-04C ECSS-E-ST-10-12C ECSS-Q-ST-60-15C
Fase A	Especificação de ambiente para o *baseline* da missão e opções que forem retidas para consideração; Análise preliminar das susceptibilidades e disponibilidade dos componentes.	ECSS-E-ST-10-04C ECSS-E-ST-10-12C ECSS-Q-ST-30-02C ECSS-Q-ST-60-15C
Fase B	Atualização da especificação de ambiente, requisitos de garantia de robustez incluindo análise detalhada dos requisitos de componentes e identificação da disponibilidade de dados de susceptibilidade; Estabelecimento e execução de planos de testes para componentes.	ECSS-E-ST-10-04C ECSS-E-ST-10-12C ECSS-Q-ST-30-02C ECSS-Q-ST-60-15C
Fase C e D	Análises precisas de efeitos de radiação (incluindo análise específica de componentes)*; Consolidação de resultados de testes; testes mais precisos.	ECSS-E-ST-10-12C ECSS-Q-ST-30-02C ECSS-Q-ST-60-15C
Fase E	Investigação dos efeitos de radiação; consideração dos efeitos de radiação na investigação de anomalias; retorno para os grupos de engenharia das lições aprendidas incluindo, por exemplo, as anomalias relacionadas à radiação.	ECSS-Q-ST-30-02C

Projeto de sistemas aeronáuticos: As IEC 62396-1 e 62396-5 se inserem no contexto da Figura 5.6 como suporte para os processos de análise de segurança de sistemas da ARP 4761, ilustrado na Figura 5.7, adaptada da IEC 62396-1. Mais especificamente, a norma se insere como processo para definir taxas de falha dos componentes eletrônicos susceptíveis aos SEUs ilustrado na Figura 6.1 abaixo. Cabe ressaltar, no entanto, que até o presente as IEC 62396-1 e 62396-5 não são normas reconhecidas formalmente pelas autoridades aeronáuticas para uso nos processos de desenvolvimento de sistemas aeronáuticos.

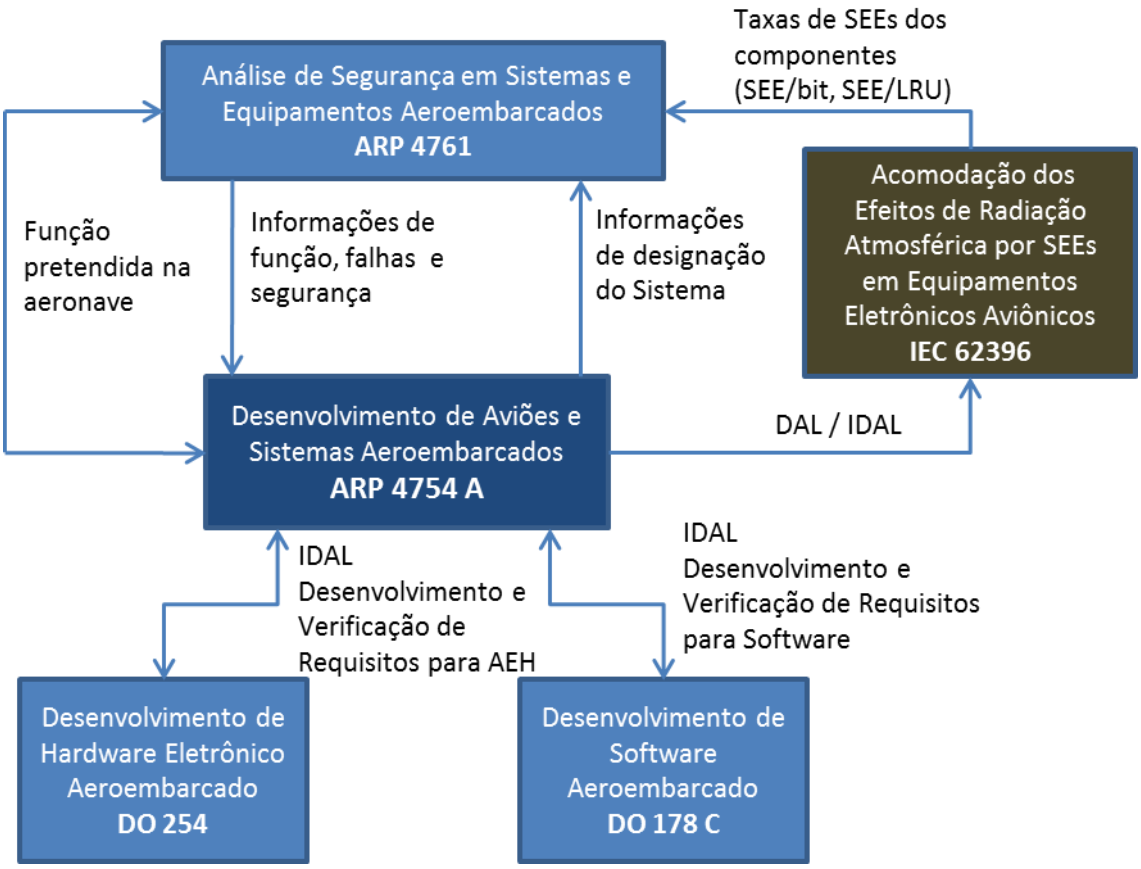

Figura 6.1 – Principais documentos que cobrem as fases de desenvolvimento de projetos aeronáuticos e a relação com a IEC 62396-1 e 5.

Cada conjunto de normas e recomendações abordados (NASA, ESA e aeronáutico) busca usar margens de projeto para acomodar incertezas e

variações do fenômeno nos sistemas eletrônicos embarcados. Tais margens podem ser aplicadas em diversas etapas dentro do processo de garantia de robustez a SEUs no projeto, como por exemplo: na modelagem do ambiente de radiação ionizante, no uso de fatores para acomodar a incerteza nas taxas de falhas determinadas por testes em componentes similares ou operando em condições não representativas da operação real do sistema, e nas análises de confiabilidade qualitativas que podem assumir uma falha devido a um SEU independente da probabilidade de ocorrência. Estes aspectos serão abordados em maiores detalhes nos próximos itens.

6.1.1. Normas e Recomendações e a Especificação do Ambiente de Radiações Ionizantes Espacial

(NASA RP 1350, 1994) aborda os ambientes de maneira a alertar e informar sobre os ambientes, não sendo possível, portanto extrair informações em detalhes suficientes.

O item 3 de (NASA 431-REF-000273) prove uma discussão que está de acordo com o discutido em 4.1, e reconhece a dificuldade em se estimar um ambiente tão complexo e sujeito a inúmeras variações. Por exemplo, (LABEL et al., 1996) e (NASA 431-REF-000273, 1996) provêem tabelas semelhantes para sumarizar as fontes de radiações (ver Tabela 5-5) que devem ser consideradas na estimativa do ambiente potencialmente causador de SEUs em sistemas eletrônicos embarcados e os modelos recomendados.

A norma ECSS-E-ST-10-04C estabelece no capítulo 9 requisitos, mais objetivos e quantitativos, para definição dos ambientes de radiações ionizantes que também cobrem os aspectos discutidos em 4.1, indicando os modelos a serem usados para caracterização. Embora o presente trabalho não tenha explorado os modelos que podem ser utilizados para caracterizar o ambiente de radiações ionizantes, é possível inferir que os modelos definidos por esta norma são mais atuais e, portanto, representativos (além do fato de que uma norma é de 1996 e a outra de 2008). Por exemplo, conforme descrito em 4.3, o

modelo CREME evoluiu para o CREME96, não sendo mais recomendado o uso do anterior. Portanto, a Tabela 5-5 está desatualizada.

A norma ECSS-E-ST-10-04C reconhece que pode haver incertezas nos resultados dos modelos usados para caracterizar os ambientes de radiações ionizantes, indicando um fator de multiplicação para cada modelo a ser usado. O requisito 9.3 c, deixa a cargo do gerente da missão especificar as margens de projeto.

Os requisitos para especificar os ambientes de radiação desta norma também são mais completos e objetivos. Por exemplo, o item 9.3 demanda que as possíveis variações de órbita (como uma manobra de mudança de órbita que seja prevista na operação de um satélite) sejam consideradas. Outro ponto a destacar é que a norma também leva em conta na especificação do ambiente as fontes de radiações ionizantes que possam ser embarcadas na espaçonave, ou seja, as fontes que não são do ambiente natural do espaço.

6.1.2. Normas e Recomendações e a Especificação do Ambiente de Radiações Ionizantes Aeronáutico

A IEC 62396-1, em seu capítulo 5, provê uma discussão que está de acordo com o item 4.2. Ao se consultar a bibliografia utilizada pela norma, nota-se que ela coincide na maioria dos casos com a consultada pelo presente trabalho, uma vez que o assunto é relativamente novo para o setor aeronáutico e a norma é atual (2012).

Os nêutrons são considerados pela norma os principais responsáveis pela ocorrência de SEEs em sistemas aviônicos. Pelo exposto em 4.2.1, e no item 5 da norma, há evidências que suportam este entendimento. O item 5.3 da IEC 62396-1 discute a correlação entre fluxo de nêutrons na atmosfera e a ocorrência de SEUs em sistemas aviônicos, e o item 6.2.1 e 6.2.2 relata os efeitos de SEEs causados por estas partículas.

É importante notar, entretanto, que de acordo com 4.2.2, outras partículas são capazes de causar SEUs em sistemas aviônicos. A contribuição de partículas

como píons pode ser desprezada do ponto de vista de engenharia (apenas 1% do fluxo de nêutrons), e o fluxo de raios cósmicos é considerado muito pequeno, no entanto os prótons tem uma proporção em torno de 20 a 30% dos nêutrons, o que não pode ser desprezado.

A IEC 62396-1 sugere uma abordagem conservativa para cálculo do fluxo de nêutrons no item 5.3.2, que acomodaria este fluxo de prótons, descrito no item 5.4. Assim, o fluxo de prótons na atmosfera com potencial de causar SEUs pode ser considerado como incluído no fluxo de nêutrons.

O fluxo recomendado é de 6000 n/cm^2 por hora para energias acima de 10 MeV, para uma altitude de 40 kft e latitude de 45 graus, ajustável para outras altitudes e latitudes conforme o Anexo D, o que era considerado como padrão pela revisão original da norma e conservativo, pois o valor calculado seria de 5600 n/cm^2 por hora. A revisão de 2012 já leva em consideração que as tecnologias atuais sejam potencialmente susceptíveis a nêutrons com energias acima de 1 MeV. Assim, o fluxo calculado para energias acima de 1 MeV seria de 9200 n/cm^2 por hora.

A IEC 62396-1 não determina um modelo ou padrão a ser usado para modelar ambiente, apenas recomenda. O capítulo 9, que contém as considerações gerais da norma, deixa a cargo do usuário definir qual modelo deve ser usado com base no discutido no capítulo 5 (item 9.2). Não considera, também, a variação do ciclo solar médio de 11 anos como significativo nos fluxos, apenas para os casos descritos no Anexo E, que é informativo e aplicável apenas para aeronaves voando acima de 60 kft.

Com relação à variação do fluxo de radiações ionizantes devido à atividade solar, o item 5.6 da IEC 62396-1 provê uma discussão e reconhece que os SEPEs podem aumentar drasticamente tais fluxos, baseando-se em estudos como os mencionados no capítulo 4 do presente trabalho. A norma sugere que os fatores de multiplicação em relação ao fluxo nominal de 6000 n/cm^2/h historicamente variaram de 1,6 a 263. Este histórico sugere também que sejam esperados 7 eventos de SEPEs que atinjam os sistemas terrestres em 67 anos,

com um acréscimo de 25 vezes na taxa de ocorrência de SEU se comparado aos fluxos médios em períodos de mínimo solar. No entanto, no capítulo 9, deixa a cargo do usuário definir um fator de multiplicação em relação ao ambiente normal de nêutrons, para usar no caso dos SEPEs, o que pode ser passível de questionamentos dentro de um processo de certificação aeronáutica.

Para tratar dos nêutrons térmicos, a norma sugerida é a IEC 62396-5. Apesar da fórmula e valores sugeridos pela norma, mencionados em 5.3.9 serem objetivos, a discussão sobre tais valores na norma inferem que estes são passiveis de discussão e argumentação acerca da validade ou precisão dos mesmos, o que também compromete a aplicação da norma dentro de um processo de certificação aeronáutica. Por outro lado, sendo um assunto novo na aviação, o presente trabalho não encontrou melhores abordagens que não sejam a adoção da fórmula e valores sugeridos pela IEC 62396-5.

Outros documentos, como os EASA SIB 2012-09 e SIB 2012-10 são apenas informativos, e podem ser usados para conhecimento do assunto dos SEEs no setor aeronáutico.

6.1.3. Normas e Recomendações e Uso de Cenários na Especificação do Ambiente de Radiações Ionizantes

NASA 431-REF-000276 (1996) reconhece que cenários devem ser considerados, pois as estimativas que levam em consideração somente o pior caso levam a um sobre-projeto (*overdesign*) e devem ser usadas somente na fase conceitual e quando não se tem certeza sobre as datas e duração da missão. Cenários puramente otimistas teriam, por outro lado, o efeito inverso, levando a falhas prematuras e comprometimento de uma missão espacial / aeronave.

As normas aeronáuticas não consideram o uso de cenários para caracterizar o ambiente de radiação ionizante. De acordo com o capítulo 5 da IEC 62396-1, as aproximações sobre o espectro de nêutrons ilustrado na Figura 4.3 são

conservadoras e, portanto, acomodam as incertezas e variações do ambiente. No caso dos SEPEs, a discussão no item 5.6 da norma leva à conclusão de que o usuário pode caracterizar um ambiente muito menos severo do que o esperado, como é o discutido no relatório emitido por (NATIONAL, 2008).

A norma ECSS-E-ST-10-04C não estabelece cenários diferentes no que se refere a variações no ambiente espacial (impacto das variações no mínimo ou máximo solar no ambiente (SUGGS, 2013), por exemplo) em si. No entanto, leva em consideração a variação do ambiente para cenários de operação diferentes. Um dos requisitos para a preparação da especificação de ambiente de radiação (item 9.3) é de que a especificação inclua a evolução da órbita, seja esta causada por motivos naturais ou por manobras previstas, pois pode, por exemplo, afetar a exposição da missão aos cinturões de radiação.

6.1.4. Normas e Recomendações para Robustez de Sistemas Eletrônicos Embarcados Aeroespaciais a SEUS e o Impacto na Confiabilidade

Taxas de ocorrências de SEUs

O documento NASA 431-REF-000273 traz uma interessante discussão sobre a determinação das taxas de ocorrências de SEUs em seu item 4, reconhecendo a complexidade do assunto, descrevendo alguns dos principais parâmetros para se estimar a ocorrência de SEUs e discutindo alguns dos aspectos sobre testes, estando de acordo com o discutido em 4.5.1. No entanto, o conjunto de normas da ESA, em especial a ECSS-E-ST-10-12C, prove uma abordagem mais estruturada e detalhada neste aspecto.

A ECSS-E-ST-10-12C estabelece que os dados de testes em geral contêm imprecisões com relação às taxas reais de ocorrências de SEEs devido a fatores como variações de susceptibilidade do componente por conta de lotes diferentes, variações de susceptibilidade do componente devido a mudanças em processos de manufatura ou encapsulamento e ainda a correlação entre as medições feitas em laboratório com as ocorrências registradas em voo de

missões passadas ou em operação. Para se acomodar tais imprecisões, são definidas as RDM para a missão.

A aplicação de margens de projeto é uma decisão tomada, em última instância, pela gestão do projeto, e baseada na consideração de incertezas como as mencionadas anteriormente. A ECSS-E-ST-10-12C discute tais aspectos para estabelecimento das RDMs, no entanto, devido à complexidade, dados os fatores envolvidos, e à outros fatores ligados à missão que são específicas para cada projeto (custo, prazo, cronograma de execução, componentes disponíveis, etc.), a norma, em geral, não prescreve valores para serem aplicados como base. O guia ECSS-E-HB-10-12A reconhece o problema de se estabelecer margens adequadas sem haver, nas palavras da norma, uma base sólida para tal. Ainda assim, a ECSS-Q-ST-60-15C estabelece uma RDM de 10x para o caso das taxas de falhas devido a prótons ter sido baseada em simulações de dados de íons pesados.

Especificamente para testes de componentes de uso espacial, as recomendações do capítulo 4 do guia ECSS-E-HB-10-12A são mais específicas no que se refere à representatividade de ensaios e uso de margens de acordo com os fatores que afetam tal representatividade, como encapsulamento, feixe de partículas usado, níveis de energia, etc.

Na IEC 62396-1, as margens de projeto para sistemas eletrônicos embarcados aeronáuticos, aplicáveis às incertezas dos testes realizados em componentes eletrônicos, estão definidas no capítulo 7 e são de acordo com a criticalidade e dado de teste usado. O Anexo B da norma deve ser usado em conjunto com o capítulo 7 para definição das taxas de ocorrências de SEUs.

Os fatores de multiplicação podem atingir um fator de até 10 na taxa de erros. Este valor coincide com a norma ECSS-E-ST-10-12C que indica em 5.5.3.1 que as incertezas na previsão das taxas de erro podem atingir um fator de até 10 em algumas circunstâncias. Uma vez que atualmente há poucos dados de testes de componentes e sistemas usados em aeronaves, essa abordagem

pode ser útil, mas também levar a valores muito altos de taxas de falhas devido a SEUs em um sistema como um todo.

Análise da Confiabilidade de Sistemas Eletrônicos Embarcados Aeroespaciais e SEUs

As funções dos sistemas aeroespaciais são classificadas pelas normas e recomendações de acordo com sua criticalidade, ou seja, de acordo com a consequência da falha funcional. Cada conjunto de normas e recomendações abordado (ESA, NASA e aeronáutico) tem um sistema de classificação próprio, com uma máxima probabilidade de ocorrência associada a cada uma das categorias, evidenciando qual é taxa de falha aceitável. No entanto, apesar de serem diferentes, todas seguem uma classificação por nível coerente com a criticalidade da função executada pelo componente.

Para os sistemas embarcados espaciais, (NASA 431-REF-000273, 1996) define três níveis de criticalidade (*error-functional, error-vulnerable, e error-critical*) das funções executadas pelos sistemas de modo a auxiliar as análises de severidade de SEEs como a ilustrada pela Figura 5.3.

Uma vez que o INPE usa as normas ESA, é coerente utilizar a classificação das normas deste conjunto, ilustrada na Tabela 5-3. Assim, os componentes eletrônicos potencialmente susceptíveis devem ser identificados conforme as correspondentes categorias de severidade.

A IEC 62396-1 busca seguir as definições de criticalidade realizados dentro dos processos descritos na ARP 4754 e ilustrados nas Figura 5.6 e Figura 5.7. De acordo com norma, somente os componentes eletrônicos embarcados cuja falha tem consequências até Maior devem ser considerados para SEEs. Os itens classificados como Menor e abaixo tem consequências de não reduzirem significantemente a segurança da aeronave e, portanto a ocorrência de um SEU poderia ser tolerada. Esta ponderação é razoável, pois está baseada em critérios bem estabelecidos de criticalidade para os projetos de sistemas aeronáuticos embarcados.

No entanto, a IEC 62396-1, ao definir a abordagem para caracterização das taxas de falhas por SEEs, não considera o IDAL. O rigor no dado de teste e correspondente aplicação de fatores levam em conta os componentes que fazem parte de sistemas classificados por nível de criticalidade da função (DAL), como era realizado na primeira revisão da ARP 4754. Na revisão A, entro do processo de designação dos elementos que irão realizar a função nível A, é aceito que o sistema tenha redundâncias com IDAL menores que A (dois IDAL B para realizar a função A, por exemplo). Sendo assim, a aplicação direta da IEC pode levar a um excesso de rigor e até inviabilizar o uso de dados de taxas de ocorrências em componentes conforme o Anexo B da norma, para determinados sistemas com IDAL B dentro de um sistema nível A, por exemplo.

O conjunto de normas da ESA trata dos aspectos levantados pelo item 4.5.2 do presente trabalho de maneira adequada. A análise da resposta dos circuitos, componentes, subsistemas ao ambiente de radiação, ilustrada na Figura 5.2, é realizada em geral por meio de ferramentas como FMEA/FMECA, descritas na ECSS-Q-ST-30-02C Cada tipo de SEE é analisado e a criticalidade verificada com base na taxa de ocorrência do SEE. A taxa de ocorrência de SEUs deve ser definida para componentes que realizam funções críticas ou potencialmente críticas, de acordo com a classificação da Tabela 5-3 e Tabela 5-4. O programa de RHA estabelecido na norma ECSS-Q-ST-60-15C estabelece que, para SEUs, a criticalidade de um componente em sua aplicação deve ser definida incluindo os impactos nos níveis acima, ou seja, subsistema e sistema.

O documento da NASA 432-REF-000273 é mais especifico no que se refere às análises de criticalidade de SEEs em sistemas. O próprio documento se autodenomina “um tipo de FMECA especializada”. A Figura 5.5, por exemplo, usada em conjunto com a Tabela 5-6, pode ser considerada em conjunto com o uso de uma FMEA/FMECA tradicional como forma de refinamento e especialização da análise com foco nos SEUs. No entanto, mesmo sendo um

documento específico, este não prescreve abordagens, e sim sugere algumas abordagens que podem auxiliar a análise.

Para o caso aeronáutico, os processos de análise de confiabilidade da norma ARP 4761 não mencionam os SEUs como uma das fontes de falhas em componentes eletrônicos. O ambiente de radiações ionizantes não está entre os fatores ambientais mencionados pela norma em que a aeronave irá operar. A IEC 62396-1 considera que a as taxas de ocorrências de SEEs serão incluídas nas análises como FMEA e FTA, mas ainda falta um elemento de ligação entre as normas.

O documento CM – SWCEH – 001 que está inserido no contexto da norma RTCA DO-254, recomenda duas abordagens (top-down e botton-up), mas não sugere ferramentas e considera que qualquer abordagem que forneça o mesmo nível de confiança pode ser aceito.

6.1.5. Normas e Recomendações e Estratégias de Mitigação para Robustez a SEUs

O item 4.6 descreveu brevemente algumas das estratégias de mitigação para tolerar os SEUs em sistemas eletrônicos embarcados, que conforme já mencionado, deve ser aplicada considerando as limitações de projeto e criticalidade das funções executadas pelo dispositivo.

Uma vez que o assunto envolve o conhecimento aprofundado dos detalhes de cada projeto e as mitigações são inúmeras e aplicáveis de acordo com o caso analisado, as normas e recomendações em geral não especificam uma técnica a ser usada.

(NORMAND et al, 1996) recomenda a estratégia de mitigação de implementação de EDAC para SEUs, como uma das conclusões do seu estudo. A norma IEC 62396-1 embora não aborde o tópico de estratégias de mitigação para SEUS, considera o uso de EDAC como o mais comum e aplicável a SEUs, em seus itens 8.3.1 e Anexo B.

No caso de sistemas embarcados aeronáuticos, a IEC 62396-1 considera que as mitigações necessárias para acomodar os SEEs serão identificadas majoritariamente no processo de PSSA. No entanto, cabe a ressalva de que se a ARP 4761 não considerar os efeitos do ambiente de radiações ionizantes, tais mitigações provavelmente não serão identificadas.

AS normas da ESA deixam claro que técnicas de mitigação devem ser usadas sempre que for necessário. A ECSS-Q-ST-60-15C explicita nos requisitos para implantação do programa de RHA que as taxas de eventos (SEEs) devem ser tais que atendam os requisitos de desempenho, disponibilidade e confiabilidade. Caso contrário, mitigações devem ser implementadas para eliminar a possibilidade de dano ou degradação do desempenho dos sistemas. Ainda, informa que a mitigação deve ser verificada por testes ou análises.

O documento da NASA 431-REF-000273 considera o uso de mitigações de erro causado por SEEs já nas fases iniciais do projeto, como é ilustrado na árvore de decisão da Figura 5.3. Isso é uma vantagem, pois se as alternativas são selecionadas baseadas em critérios como a utilidade e efetividade em custo, o projeto potencialmente será mais robusto e confiável sem impor grandes custos adicionais.

6.2. Proposta de Recomendações para Garantia de Robustez de Sistemas Eletrônicos Embarcados a SEUs Causados por Radiações Ionizantes

Este item apresenta recomendações de projeto visando garantir a robustez de sistemas eletrônicos embarcados aeroespaciais a SEUs causados por radiações ionizantes com base na literatura (normas e recomendações aeroespaciais e bibliografia) analisada.

As recomendações podem ser divididas em três tipos: 1) recomendação de uso de norma ou recomendação existente, sem adaptações, 2) recomendação de uso de norma ou recomendação com adaptações e 3) recomendar um processo ou procedimento novo.

6.2.1. Recomendações para Sistemas Eletrônicos Embarcados Espaciais

Para sistemas eletrônicos embarcados espaciais, ao se considerar os satélites de órbita baixa lançados pelo INPE, basicamente recomenda-se o uso do conjunto de normas da ESA identificado na Tabela 6-1, com adaptações descritas a seguir.

A abaixo ilustra a relação entre os resultados dos processos descritos pelas normas da ESA e os estágios de um projeto espacial, no que relacionam com os processos de garantia de robustez a SEU de sistemas eletrônicos embarcado espaciais.

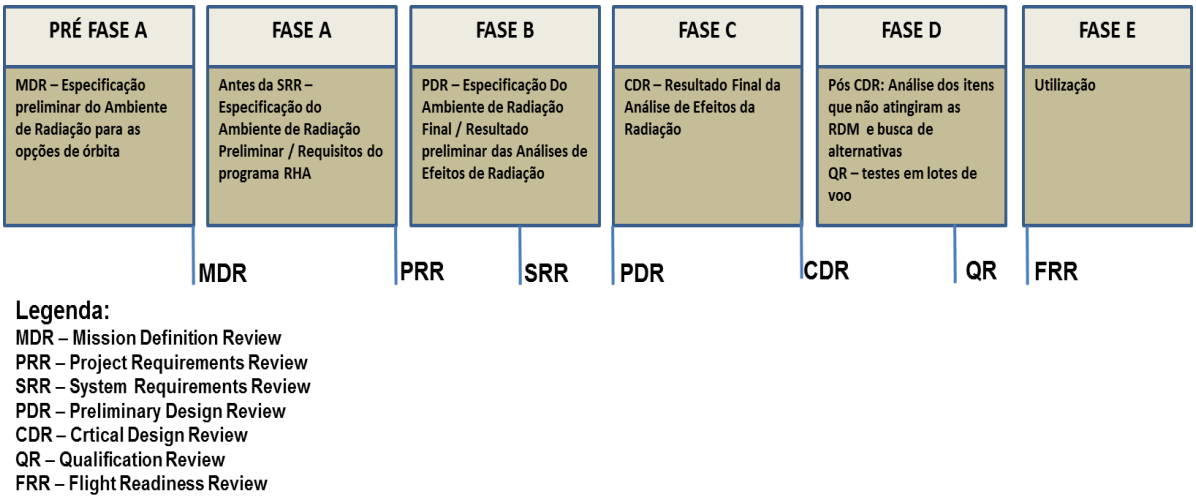

Figura 6.2 – Fases de um projeto e os resultados dos processos de garantia de robustez a SEUs em sistemas

Na Pré-Fase A, são realizadas especificações preliminares de ambiente de radiação para cada opção de órbita, de modo a ser um insumo que auxilie na escolha final da órbita da missão.

Na Fase A, a especificação de ambiente é detalhada para a opção de órbita, podendo ainda ser preliminar. Os requisitos de robustez à radiação são definidos, de acordo com a ECSS-Q-ST-60-15C antes do SRR.

Na Fase B o ambiente de radiação é especificado e as análises de efeitos de radiação realizadas. Na PDR, o resultado preliminar e a especificação do ambiente de radiação final são documentados.

Ao final da Fase C, na CDR, a análise de efeitos de radiação é finalizada. Neste caso, itens pendentes podem ser identificados que não atingiram as margens de projeto e requisitos de confiabilidade, por exemplo.

Na Fase D, até a QR, os testes de verificação de radiação, também chamados de testes de radiação para aceitação de lotes são realizados. Nesta fase os itens pendentes identificados na análise de efeitos de radiação devem ser solucionados por meio de análises detalhadas, uso de técnicas de mitigação, troca de componentes, etc.

De acordo com o conjunto de normas da ESA e o apresentado no capítulo 4, é possível dividir as recomendações de acordo com etapas consideradas fundamentais para garantia da robustez dos sistemas eletrônicos embarcados aeronáuticos, destacados a seguir.

6.2.1.1. Especificação do Ambiente de Radiações Ionizantes

Recomenda-se o uso da ECSS-E-ST-10-04C com as seguintes adaptações:

- Na parte de especificação de ambiente de radiação, recomenda-se adaptar o item B.1 da ECSS-E-ST-10-04, que estabelece que as datas de começo dos períodos de máximo e mínimo solar para os ciclos futuros sejam definidas de acordo com a equação:

  Ano de máximo solar = 2000,3 + 11 * (i - 23)

  (6.1)

  Onde:

  i = número do Ciclo Solar

Estudos como o de (SUGGS, 2013) contém estimativas mais atuais sobre a variação do ciclo solar. A norma, sendo de 2008, não considera também os dados mais atuais da evolução do ciclo solar atual.

Recomenda-se o uso de cenários que envolvam a variação da atividade solar, como discutido em 4.4, ou outros parâmetros que influenciam o fluxo das partículas potencialmente causadoras de SEUs.

- Isto pode ser feito de maneira a se recolher subsídios para o estabelecimento de margens mais precisas na especificação do ambiente de radiação, diminuindo incertezas por conta da variação do clima espacial e melhorando as estimativas para a missão. Deste modo, a aplicação de margens de projeto não levará a excessos que onerem desnecessariamente a missão e nem a previsões otimistas que possam comprometer a missão ou subsistemas.

6.2.1.2. Análise dos Efeitos de SEUs

Recomenda-se um estudo sobre o uso das margens de projeto de radiação (RDM) para sua correta aplicação.

- Um ponto importante no conjunto de normas da ESA é o estabelecimento de margens de projeto (RDM) discutidas na ECSS-E-ST-10-12C. A norma define que o gerente de projeto tem a responsabilidade final sobre a definição de margens, mas para isso é preciso um parecer técnico que suporte esta decisão. Os diversos fatores mencionados na norma requerem uma compreensão mais profunda de especialistas de diversas áreas para uma correta aplicação das margens de projeto. Por exemplo, em 5.5.1, é requerido que a RDM atingida inclua as incertezas advindas dos dados de susceptibilidade do programa de RHA da ECSS-Q-ST-60 incluindo diferenças entre circuitos de testes (o que requer especialistas na área de eletrônica), incerteza nos resultados por conta dos possíveis efeitos do uso de feixes de

prótons de baixa energia (< 30 MeV) (o que requer um especialista em testes/radiação).

Recomenda-se realizar as análises dos efeitos de SEUs durante um SEPE de modo separado e somente para falhas que levem a condições críticas.

- Durante um evento de SEPE, os fluxos de partículas potencialmente causadoras de SEEs podem ter acréscimos muito grandes se comparado com os fluxos normais. Uma análise dedicada para este caso seria recomendável, considerando que estes eventos ocorrem em uma periodicidade pequena em comparação com o período de uma missão, que as falhas não destrutivas como o SEU poderia afetar outras funções sem comprometer a missão neste cenário e que se pode prever uma ação mitigatória alternativa nestes casos. Por exemplo, se a análise concluir que taxa de SEUs leva a uma condição catastrófica neste caso, a ação de mitigação não necessariamente seria modificação do sistema; poderia se optar pelo desligamento do subsistema susceptível ou a colocação em um modo de operação menos susceptível.

6.2.2. Estudo de Caso de Aplicação das Recomendações para Sistemas Eletrônicos Embarcados Espaciais nos Satélites ARGOS e PakSat 1R

A aplicabilidade das recomendações para a garantia de robustez de sistemas eletrônicos embarcados espaciais a SEUs causados por radiações ionizantes é discutida a seguir, por meio da análise dos dados disponíveis na literatura do experimento *Advanced Space Computing and Autonomy Testbed* do satélite ARGOS, mencionado no item 4.1.4, de acordo com o discutido por (LOVELLETTE et al., 2002); e do satélite PakSat, de acordo com o discutido por (MURTAZA, 2011).

Satélite ARGOS

O satélite ARGOS é um satélite de órbita baixa, polar, de 850 km de altitude e inclinação de 98,7º, com duração de missão prevista de 3 anos. Foi lançado

em 23 de fevereiro de 1999 e, em 31 de julho de 2003, as operações do satélite foram encerradas, após aproximadamente 4 anos e meio de operação.

Para esta órbita, a ECSS-E-ST-10-04C considera que o satélite atravessa os cinturões de radiação de Van Allen interno e externo e a região da SAA, além de ser exposto à radiação galáctica.

Desta forma, as seguintes partículas devem ser consideradas: prótons aprisionados do cinturão de radiação interno especialmente na região da SAA, íons de raios cósmicos galácticos, prótons e íons pesados de SEPEs.

O período da missão estava inteiramente dentro do Ciclo Solar Mínimo. Desta forma, é esperado que as fontes de radiação dos prótons aprisionados do cinturão de radiação interno e íons de raios cósmicos tenham seus fluxos aumentados, enquanto que, dada a atividade solar diminuída, os eventos de SEPEs que geram os prótons e íons pesados são menos freqüentes. A blindagem do satélite é de 2,5mm de alumínio.

Os dados disponíveis na literatura (LOVELLETTE et al., 2002) não possibilitam concluir sobre os passos definidos em 6.2.1. Isto se deve provavelmente ao fato de que os objetivos da missão eram de comparar abordagens de confiabilidade e o foco foi dado em testar os componentes no ambiente real. (LOVELLETTE et al., 2002) informa também que as análises de efeitos de radiação foram realizadas por meio de injeção de falhas, e não informa se foram realizados testes de radiação da placa tolerante à falhas com uso de componentes COTS (placa IDT-3000).

Antes da implementação das medidas de mitigação via software, a placa IDT-3000 levou em média dois dias até o travamento e necessidade de *reset*. Após a implementação, houve uma melhora de uma ordem de grandeza, ou seja, em média levava vinte dias para seu travamento. A literatura consultada não informa se os projetistas tinham previsto estes tempos com precisão. É provável que a aplicação das recomendações do presente trabalho levariam a aplicação de medidas adicionais de mitigação que reduziriam a ocorrência de

SEUs, ilustrados na Figura 4.2, mas cabe ressaltar que os objetivos do experimento *Advanced Space Computing and Autonomy Testbed* eram *a*plicar medidas de mitigação a SEUs em um ambiente real e concluir sobre sua suficiência.

Satélite PakSat 1R

O satélite PAKSAT é um satélite geoestacionário lançado em 11 de agosto de 2011 e tem órbita a 38º leste. O projeto foi especificado para uma vida operacional 15 anos, provendo serviços como acesso à internet e transmissão de sinal de televisão digital.

Para especificar o ambiente de radiação, a norma ECSS-E-ST-10-04C estabelece nos itens 9.2.1.1 e 9.2.1.2 o uso dos modelos AP-8 e AE-8 para prótons e elétrons, respectivamente, de acordo com o período do Ciclo Solar (máximo ou mínimo), para as partículas dos cinturões de radiação de Van Allen. Para os SEPEs, a norma estabelece no item 9.2.2 o uso do modelo ESP, e o modelo ISSO 15390 para as partículas de raios cósmicos galácticos, conforme o item 9.2.4. De acordo com (MURTAZA, 2011), o programa SPENVIS e os modelos acima foram usados para estimar os ambientes de radiações ionizantes. Foi considerado que o satélite passará 11 anos de atividade no Máximo de Ciclo Solar e apenas 4 no Mínimo de Ciclo Solar.

Os prótons dos cinturões de radiação foram considerados não serem capazes de causar SEUs nos componentes eletrônicos embarcados, considerando que o satélite é geoestacionário. Para comprovar isto, foram realizadas simulações de ambiente por meio dos modelos AP-8 MAX e AP-8 MIN. Assim, as partículas de raios cósmicos galácticos e prótons de SEPEs fora consideradas as fontes potenciais de SEUs.

Para estimar a ocorrência de SEUs, o software SPENVIS também foi utilizado, provendo estimativas para componentes que, potencialmente, poderiam ser usados no satélite. Os dados de taxas de SEUs estimadas para prótons são reproduzidos na

Tabela 6-2 abaixo, onde, de acordo com (MURTAZA, 2011) foi possível concluir que a memória RAM CMOS de 16k é a melhor escolha.

Tabela 6-2 – Taxas de SEUs para diversos componentes considerados para o satélite PakSat

Dispositivo	Seção de choque (cm^2/bit)	SEU/bit/dia
4044	3.31×10^{-13}	1.08×10^{-7}
MM 5280	5.83×10^{-12}	1.92×10^{-6}
C2107B	4.56×10^{-11}	1.52×10^{-5}
MK4116J-2	1.60×10^{-12}	5.21×10^{-7}
8X350	8.29×10^{-10}	2.79×10^{-4}
93422	4.81×10^{-11}	1.60×10^{-5}
7164 nMOS SRAM	4.72×10^{-14}	1.52×10^{-8}
CMOS 16k RAM	2.33×10^{-15}	7.4×10^{-10}

Fonte: Adaptado de MURTAZA, (2011).

Os dados disponíveis em (MURTAZA, 2011) não permitem concluir sobre todos os passos e resultados dos processos de garantia de robustez a SEUs ilustrados na Tabela 6-1 e Figura 6.2 para o satélite PakSat. No entanto, é possível ver que atividades como a Análise Preliminar das Susceptibilidades e Disponibilidades dos Componentes (Pré-Fase A e Fase A) e Atualização da Especificação de Ambiente (Fase B) foram realizadas e são adequadas para o projeto de sistemas eletrônicos espaciais embarcados.

6.2.3. Recomendações para Sistemas Eletrônicos Embarcados Aeronáuticos

O setor aeronáutico não tem a mesma experiência em lidar com o fenômeno das radiações ionizantes e seu impacto nos sistemas eletrônicos embarcados que o setor espacial. Sendo assim, era esperado que o presente trabalho

identificasse mais recomendações para sistemas eletrônicos embarcados aeronáuticos que para os espaciais.

As normas mais ligadas à garantia de robustez de SEUs no setor aeronáutico são a IEC 62396-1 e a IEC 62396-5. As demais normas mencionadas neste trabalho estão inseridas em um contexto maior do desenvolvimento de aeronaves, e já são utilizadas em outros processos. Neste sentido, as recomendações para sistemas eletrônicos embarcados aeronáuticos não pretendem alterar nenhum processo das normas ARP 4754a, 4761, DO-254 e DO-178 (os demais documentos, CM-SWCEH-001, SIB 2012-09 e SIB 2012-10 tem caráter de recomendação), embora haja a recomendação geral de se incluir o ambiente de radiação como parte dos ambientes considerados na ARP 4761. As recomendações têm basicamente objetivo de substituir, alterar ou complementar alguns dos pontos da IEC 62396-1.

De acordo com o conjunto de normas da ESA e o apresentado no capítulo 4, é possível dividir as recomendações de acordo com etapas consideradas fundamentais para garantia da robustez dos sistemas eletrônicos embarcados aeronáuticos, destacados a seguir.

6.2.3.1. Especificação do Ambiente de Radiações Ionizantes

Recomenda-se que, para definição do ambiente de partículas ionizantes na atmosfera, os nêutrons devem ser considerados os principais responsáveis por causarem SEUs na eletrônica embarcada. No entanto, uma vez que os prótons contribuem significantemente para as taxas de ocorrência de SEUs, um fator de ajuste deve ser incluído no modelo a ser usado. Este fator pode ser de 1,3 , uma vez que, em geral, o fluxo de prótons é em torno de 20 a 30% do fluxo de nêutrons. Alguns modelos que podem ser usados para especificar o ambiente estão descritos no capitulo 5 da IEC 62396-1.

É recomendado que o ambiente seja definido considerando-se a maior altitude de voo esperada para a aeronave. De acordo com o exposto no item 4.2.1.1 e ilustrado na Figura 4.4, uma aeronave vai ser exposta ao fluxo de partículas

mais crítico na maior altitude de voo que esta atingir, portanto o fluxo deve ser definido na máxima altitude operacional da aeronave. Embora a IEC 62396-1 destaque a influência da altitude nas taxas de ocorrências de SEUs, não estabelece que o valor usado seja a máxima altitude do voo da aeronave, mas sim altitude de voo. Isto pode ser interpretado como uma altitude típica de voo, e não o teto de voo do projeto da aeronave.

Caso esta máxima altitude operacional não esteja definida para o projeto, é razoável considerar preliminarmente, baseado no item 4.2, uma máxima altitude operacional de 15,2 km (50 kft) para aeronaves civis e 18,3 km (60 kft) (onde o fluxo atinge seu pico) para as militares, para estimativa dos fluxos.

O ambiente deve ser definido também, considerando-se a maior latitude de voo esperada para a aeronave. De acordo com 4.2.1.2 e Figura 4.5, o fluxo é mais intenso nas regiões dos Polos, ou seja, em maiores latitudes. É esperado que as aeronaves militares e as aeronaves civis Categoria Transporte não sejam limitadas em latitude, portanto deve-se definir o ambiente para a máxima latitude (90 graus). Mais uma vez, a IEC 62396-1 não impõe que seja usada a maior latitude, apenas infere que o usuário tomará este valor como parâmetro.

Segundo as recomendações acima, os seguintes ambientes devem ser considerados:

- **Um ambiente normal**, ou seja, não perturbado por um SEPE, especificado em um período de mínimo solar. Pelo exposto em 4.2.3, uma vez que o ciclo de vida de uma aeronave militar e uma aeronave civil Categoria Transporte é maior que o ciclo Solar de 11 anos, o fluxo esperado de nêutrons deve considerar a modulação do Sol. Ou seja, ao se definir o ambiente normal, o ciclo solar em seu mínimo terá como impacto o maior fluxo de raios cósmicos atingindo a atmosfera e, por sua vez, a maior geração de nêutrons secundários. Assim, este fator deve ser considerado para definir o fluxo de nêutrons para o ambiente normal.

- **Um ambiente de pior caso**, ou seja, considerando um evento de SEPE extremo. Os eventos de SEPEs descritos em 2.1 e 4.2.3 podem gerar acréscimos dramáticos no fluxo de nêutrons secundários na atmosfera. Assim, um ambiente de pior caso, baseado em eventos já registrados de SEPEs, deve ser especificado. O item 5.6 da IEC 62396-1 discute os SEPEs e seu impacto no fluxo de nêutrons, considerando fatores de multiplicação para o fluxo padrão de 6000 n/cm^2/h que variam entre 1,6 e 263, baseados em estudos como os mencionados em 4.2.3. No entanto, não é aceitável deixar a cargo do usuário, em seu item 9.2, a definição de um fator de multiplicação do fluxo em relação ao valor calculado para um ambiente normal. Assim, considerando a discussão realizada na IEC 62396-1, e (DYER, 2001), recomenda-se ou usar um fator de 25 vezes o fluxo definido para o ambiente normal, ou se definir um fluxo baseado em dados de estudos mais recentes.

Recomenda-se usar cenários para prever os fluxos de radiações ionizantes potencialmente causadoras de SEUs em que a aeronave estará sujeita em seu ciclo de vida, para diminuir as incertezas na previsão dos ambientes de radiações ionizantes.

Recomenda-se também considerar os nêutrons térmicos de acordo com a abordagem proposta pela IEC 62396-5 e descrita no item 5.3.9. As Razões 1 e 2 foram definidas com base em estudos sobre a caracterização de ambiente de nêutrons térmicos internos às aeronaves e dados de componentes, sendo uma alternativa viável para analisar os componentes que não tem dados de seção de choque para nêutrons térmicos.

6.2.3.2. Listagem de componentes potencialmente susceptíveis a SEUs de acordo com a criticalidade

Recomenda-se, como mínimo, que os seguintes componentes eletrônicos devam ser considerados como potencialmente susceptíveis a SEUs:

Tabela 6-3 – Susceptibilidade de Dispositivos a SEUs

Tecnologia	**Função**	**Áreas Susceptíveis**	**Tipos de SEU**
CMOS BiCMOS	Memórias SRAM, DRAM, SDRAM	Células de memória	*Bit flips*
		Lógica de controle	*Bit flips* se sequencial, transitórios se combinatória
SOI	FPGAs	Lógica combinatória	Transitórios
		Lógica sequencial	*Bit flips*
	Microprocessadores	Registradores, cache, lógica de controle sequencial	*Bit flips*
		Lógica de controle combinatória	Transitórios
	ADCs, DACs	Parte analógica	Transitórios
		Parte digital	*Bit flips* ou transitórios dependendo do projeto
	CIs lineares	Área analógica	Transitórios
	Fotodiodos	Fotodiodo	Transitórios

A Tabela 6-3 não deve ser considerada exaustiva. As tecnologias podem evoluir aumentando ou diminuindo sua susceptibilidade e outras novas podem surgir.

Esta Tabela 6-3 é uma compilação da Tabela 5-2 e da Tabela 5-6, respectivamente extraídas das normas ECSS-E-ST-10-12C e NASA 431-REF-000273. As normas demonstram estar em acordo com os tipos de dispositivos e tecnologias potencialmente susceptíveis a SEUs. Ambas contém informações relevantes sobre a susceptibilidade, e, mesmo sendo menos atual, a norma NASA 431-REF-000273 contém informações mais detalhadas.

Embora a Tabela 6-3 tenha sido compilada com dados de normas espaciais, os itens 6.2.2 e 8.3.4 da norma IEC 62396-1 permitem concluir que a Tabela 6-3 é aplicável também a sistemas eletrônicos embarcados aviônicos. Adicionalmente, o item 8.3.5 da norma discute alguns aspectos e tendências de tecnologias futuras que podem auxiliar nas análises de componentes potencialmente susceptíveis a SEUs.

A listagem deve conter componentes cujas falhas devidas a um SEU podem ter consequências até Maior. Esta classificação não é exclusiva dos processos de garantia de robustez à radiação, pois é derivada dos processos de desenvolvimento de sistemas embarcados descritos na ARP 4754a. De acordo com o objetivo deste trabalho, que é desenvolver recomendações para tolerar os efeitos dos SEUs, não é recomendado se listar os componentes com classificação Menor ou insignificante, uma vez que a consequência seria uma pequena degradação da missão ou qualquer outro efeito.

Esta listagem pode ainda ser um indicativo da necessidade de se implementar técnicas de mitigação durante as fases preliminares do processo de desenvolvimento do sistema, por exemplo, nas análises da PSSA.

6.2.3.3. Determinação da susceptibilidade dos componentes eletrônicos a SEUs

Uma vez que o setor aeronáutico não tem a mesma riqueza de dados e os testes com nêutrons que representem os ambientes a serem definidos em 6.2.3.1 por hora não sejam comuns, recomenda-se usar como base o capítulo 7 da IEC 62396-1, adaptado da seguinte maneira:

- Aplicar o critério definido no capítulo 7 da IEC 62396-1, descrito em 5.3.8, para os componentes/LRUs com **IDAL** correspondente ao nível exigido pela norma. A norma pede para que o rigor no dado de teste e correspondentes fatores de imprecisão nos dados sejam aplicados nos componentes do sistema conforme nível (DAL) de criticalidade do sistema. Isso pode levar à aplicação do critério de maneira excessiva. A ARP 4754a, dentro do processo de atribuição de IDAL, permite que sistemas nível A tenham componentes com IDAL inferiores a A, dentro de critérios bem estabelecidos.
- Uniformizar o critério do capítulo 7 da IEC 62396-1 para nível A, unificando Tipos I e II, e desconsiderando um fator adicional para a abordagem para Tipo II, mencionado no item 7.4.2.2 (d). Não é claro qual o valor deste fator a se usar em adição, quando não houver dados de nenhum dos testes necessários para nível A Tipo I. A norma indica que um fator mínimo na taxa de eventos, que seja considerado razoável, deve ser aplicado sobre os valores calculados pelos métodos do nível A Tipo II. As abordagens de Tipo II já contêm fatores para cada caso, o que torna a aplicação da norma confusa e sem um critério uniforme.
- Aplicar o critério do capitulo 7 da IEC 62396-1, levando em consideração as adaptações acima, gerando dois conjuntos de taxas de ocorrências de SEUs: um para o ambiente não perturbado por um SEPE e no mínimo solar e um para o ambiente de pior caso durante o evento de um SEPE extremo. Neste último, as taxas devem ser calculadas somente para componentes mais críticos de nível IDAL A.

6.2.3.4. Análise da Ocorrência de SEUs no Sistema

Análises qualitativas podem ser realizadas de forma a apoiar a decisão sobre as medidas de mitigação que eventualmente sejam necessárias durante o processo de PSSA. Deste modo, as medidas de mitigação serão identificadas nas etapas iniciais do projeto ao se considerar uma falha causada por um SEU.

É importante notar que a ARP 4761 não considera explicitamente os SEUs como uma das falhas possíveis dentro dos processos de PSSA e SSA. Desta forma, é recomendável que a norma seja revisada para inclusão de considerações sobre a inclusão do fenômeno no contexto das análises de segurança.

Para realização das análises quantitativas previstas na ARP 4761, como por exemplo, FMEA e FTA, recomenda-se que as taxas de SEUs dos componentes devam ser inseridas nas análises de confiabilidade para:

- Compor a taxa de falhas do dispositivo ao se considerar as demais fontes de falhas, nas FMEA e FTA dos sistemas nível A, B e C quando aplicável nos processos de SSA.
- Analisar a propagação da falha devido a um SEU no nível de análise correspondente (placa/LRU/sistema/etc.).

Do mesmo modo, recomenda-se que as taxas de falhas por SEUs para o ambiente de radiação de um evento extremo (SEPE), sejam incluídas em uma análise dedicada, realizada somente para os sistemas com funções cuja falha teriam consequências catastróficas (nível A). Isto se deve a dois fatores:

- A consideração do cenário para ocorrência de SEUs em um ambiente de radiação caracterizado por um evento extremo (SEPE), conforme definido em 6.2.3.1, poderia causar uma sobre-designação (*overdesign*) para sistemas cuja falha não comprometeriam o voo e pouso seguro de uma aeronave;

- Mesmo que durante a vida operacional da aeronave a probabilidade desta estar voando durante um pico de um evento de SEPE não seja grande, as falhas catastróficas envolvem consequências como a perda da aeronave e de vidas. Portanto, estas falhas devem ser evitadas durante o evento.

6.2.3.5. Medidas Adicionais de Mitigação a SEUs

As medidas de mitigação identificadas durante o processo de PSSA eventualmente podem não ser suficientes para tolerar a ocorrência dos SEUs no sistema.

Deste modo, recomenda-se que, quando as análises de confiabilidade indicarem uma probabilidade de falha mais alta que o tolerável para a classificação da falha funcional do componente e cuja contribuição devido aos SEUs é significativa, as seguintes opções devem ser consideradas:

- Uma modificação (*redesign*) do componente ou o uso de um componente com uma taxa de ocorrência de SEUs aceitável para a classificação da falha funcional;
- Testes com nêutrons nos componentes onde os fatores de precisão definidos no item 7 (adaptado) da IEC 62396-1 foram aplicados e a acomodação das incertezas pode ter levado a taxas de SEUs acima do esperado.
- Alterações no projeto implementando uma estratégia de mitigação que tolere a ocorrência de SEUs em um nível aceitável para a classificação da falha funcional.

Estratégias como as descritas em 4.4 podem ser usadas para tolerar a ocorrência de SEUs em sistemas eletrônicos embarcados de modo que a falha induzida pelo fenômeno não se propague ao nível do sistema/função no qual o componente estiver envolvido.

6.2.4. Sumário das Recomendações para Garantia de Robustez de Sistemas Eletrônicos Embarcados a SEUs Causados por Radiações Ionizantes

A Figura 6.3 abaixo sumariza as recomendações para garantia de robustez de sistemas eletrônicos embarcados aeronáuticos a SEUs causados por radiações ionizantes, de forma a organizar e resumir o discutido no item anterior. Na seqüência da Figura 6.3, as recomendações são descritas de forma sucinta para servir de apoio.

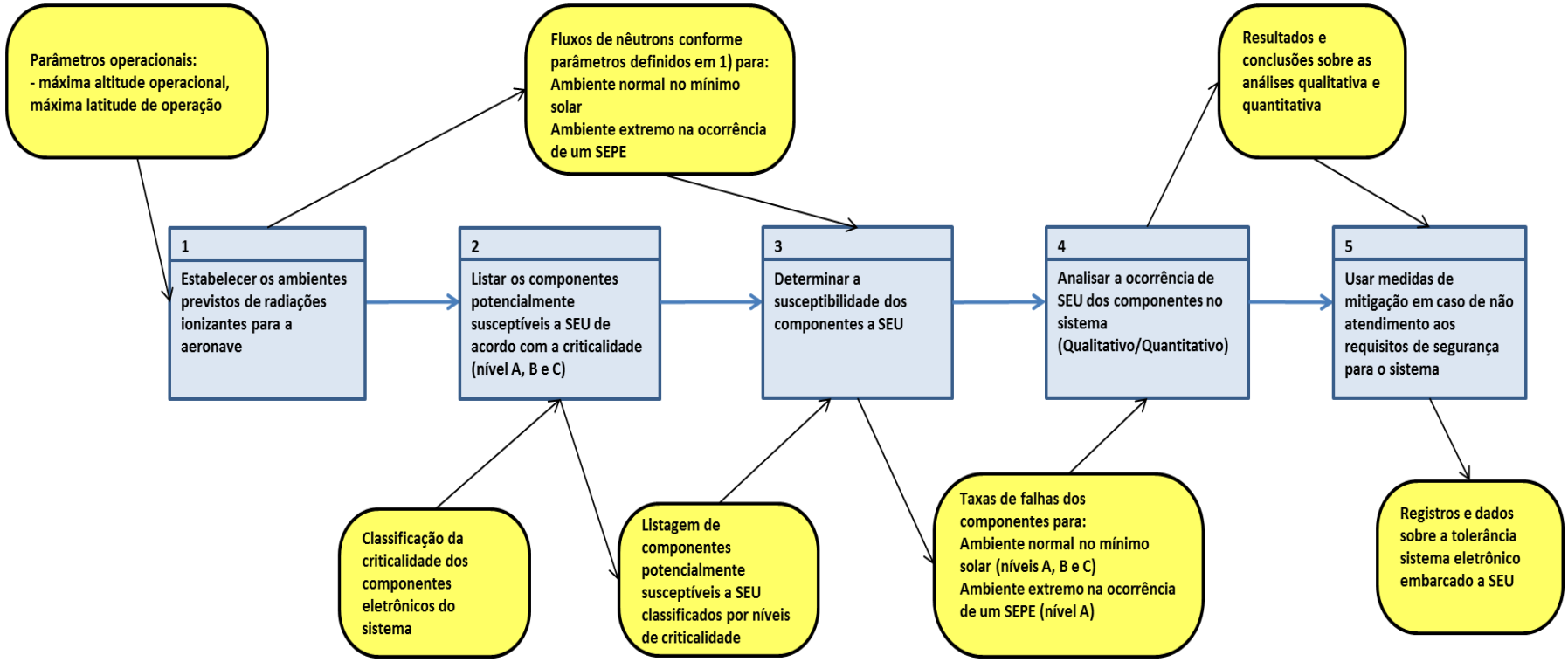

Figura 6.3 - Sumário das Recomendações para Garantia da Confiabilidade de Sistemas Eletrônicos Embarcados a SEUs Causados por Radiações Ionizantes.

Sumário das Recomendações:

1. Estabeleça os ambientes previstos de radiações ionizantes (espectro de nêutrons em função da energia) para a aeronave da seguinte maneira:

    a) Aplicar um fator de 1,3 para acomodar o fluxo de prótons;
    b) A especificação do ambiente deve ser realizada para a máxima altitude operacional da aeronave e para a máxima latitude de operação. Caso estes dados não estejam disponíveis no momento, considerar uma máxima altitude operacional de 15,2 km (50 kft) e latitude de 90 graus.
    c) Dois ambientes devem ser especificados: 1) Um ambiente normal, ou seja, não perturbado por um SEPE, especificado em um período de ciclo solar de 11 anos mínimo e 2) Um ambiente de pior caso, considerando um evento de SEPE extremo, com fluxo 25 acima do calculado para o ambiente normal, ou um fluxo baseado em estudos de SEPEs mais recentes .
    d) Considere cenários de acordo com a variação do ciclo solar (variações do mínimo solar, por exemplo) para diminuir as incertezas na especificação dos ambientes.

2. Fazer uma listagem dos componentes potencialmente susceptíveis a SEU de acordo com o indicado abaixo:

    a) Usar a Tabela 6-3 como referência para listar os componentes potencialmente susceptíveis a SEUs.
    b) Fazer a listagem de acordo com a classificação da criticalidade dos componentes eletrônicos do sistema (IDAL A, B e C). Esta classificação é um elemento externo e é resultado de processos da ARP 4754A.

3. Estimar a susceptibilidade dos componentes a SEUs da seguinte maneira:

    a) Tendo em mãos a listagem dos componentes potencialmente susceptíveis a SEUs, e os espectros de nêutrons conforme parâmetros definidos em (1) para: ambiente normal no mínimo solar e ambiente extremo na ocorrência de um SEPE:

        i. Aplicar o critério definido no capítulo 7 da IEC 62396-1, para os componentes com IDAL correspondente ao nível exigido pela norma (sistema nível A = IDAL nível A, e assim por diante).
        ii. Uniformizar o critério do capítulo 7 da IEC 62396-1 para nível A, unificando os Tipos I e II, e desconsiderando um fator adicional para a abordagem para Tipo II, caso necessário.

iii. Aplicar o critério do capitulo 7 da IEC 62396-1, levando em consideração as adaptações acima, gerando dois conjuntos de taxas de ocorrências de SEUs para os componentes listados:

- Um para o ambiente não perturbado por um SEPE e no mínimo solar; e
- Um para o ambiente de pior caso durante o evento de um SEPE extremo. Neste último, as taxas devem ser calculadas somente para componentes mais críticos de nível IDAL A.

iv. Aplicar a fórmula da IEC 62396-5 para cálculo da taxa de SEUs devido a nêutrons térmicos, descrita em 5.3.9, para o conjunto de componentes listados e para os casos de ambiente não perturbado (IDAL A, B e C) e perturbado por um SEPE (IDAL A). Caso se tenha informações mais precisas sobre taxas de fluências de nêutrons para a aeronave, estes dados devem ser usados

v. Compor os dados de taxas de ocorrências de SEUs devidos a nêutrons de alta energia e térmicos dos itens iii e iv.

4. Analisar a ocorrência de SEUs dos componentes no sistema (Qualitativo/Quantitativo)

a) As taxas de SEUs dos componentes obtidas em (3) para o ambiente normal devem ser inseridas nas análises de confiabilidade para:

i. Compor a taxa de falhas do dispositivo ao se considerar as demais fontes de falhas, nas FMEA e FTA dos sistemas nível A, B e C quando aplicável nos processos de SSA.

ii. Analisar a propagação da falha devido a um SEU no nível de analise correspondente (placa/LRU/sistema/etc.).

a) As taxas de falhas por SEUs para o ambiente de radiação de um evento extremo (SEPE) devem ser incluídas em uma análise dedicada, realizada somente para os sistemas com funções cuja falha teriam consequências catastróficas (nível A).

5. Usar medidas de mitigação em caso de não atendimento aos requisitos de segurança para o sistema, com base nos resultados das análises da ocorrência de SEUs no sistema.

6.2.5. Estudo de Caso de Aplicação das Recomendações para Sistemas Eletrônicos Embarcados Aeronáuticos

O estudo de caso a seguir visa demonstrar a aplicabilidade das recomendações para garantia de robustez de sistemas eletrônicos embarcados aeronáuticos à SEUs causados por radiações ionizantes, com base em dados disponíveis na literatura

Para este estudo, os seguintes dados foram estabelecidos, buscando representar um caso condizente ao de aeronaves atualmente em operação:

- Uma aeronave típica de Categoria Transporte (RBAC 25), com máxima altitude operacional típica de 13,1 km (43 kft) e sem limite de operação em altas latitudes.
- Um sistema eletrônico embarcado que executa uma função cuja falha tem conseqüências catastróficas para a aeronave, portanto classificado como FDAL A.

Um sistema com tais características é, por exemplo, um Sistema de Dados do Ar. O Sistema de Dados do Ar (*Air Data System* - ADS) calcula parâmetros críticos para o vôo por meio da medida da temperatura e pressão da massa de ar ao redor de uma aeronave, como por exemplo:

- Velocidade (Mach, indicada, verdadeira, etc.);
- Altitude;
- Taxa de subida ou descida (variação da altitude);

As medidas de temperatura do ar podem ser obtidas por sensores que, em geral, obtêm a temperatura total do ar, que é a temperatura do ar externo à aeronave quando o mesmo é levado ao repouso adiabaticamente, ou seja, considerando que a energia cinética do ar será absorvida pelo sensor. Esta medida é usada para calcular a temperatura estática do ar, que é a temperatura do ar não perturbado pela aeronave, e a velocidade da aeronave.

As medidas de pressão são obtidas por meio de sensores, sendo basicamente medidas de pressão estática e total. A pressão estática é a pressão atmosférica do ar que circunda a aeronave, sem considerar as perturbações causadas pela aeronave. A pressão total é a soma da pressão estática com a pressão de impacto. Esta, chamada também de pressão dinâmica, é causada pela força do fluxo de ar sobre a aeronave em deslocamento.

Um Sistema de Dados do Ar típico é composto de elementos sensores, elementos transdutores também chamados de computadores de dados do ar, e meios de transmissão de dados. Os sensores de pressão são, tipicamente, tomadas estáticas colocadas na parte externa da aeronave, como por exemplo, tubos de Pitot ou Pitot-estático. E os sensores de temperatura são elementos sensores que, posicionados externamente à aeronave, geram um valor de resistência elétrica correspondente a uma temperatura. Os transdutores recebem entradas pneumáticas (das medidas de pressão) ou resistivas (das medidas de temperatura) e as convertem em parâmetros críticos para o vôo, como os mencionados anteriormente, que serão utilizados por outros sistemas como, por exemplo, comandos de vôo, piloto automático, telas para os pilotos, etc.. A saída de um transdutor é, tipicamente, um sinal digital, que utiliza barramentos digitais com protocolo e velocidade padronizados, como, por exemplo, ARINC 429, que é um protocolo ponto a multiponto. A Figura 6.4 mostra uma arquitetura de um sistema de dados do ar genérico, utilizando sensores de pressão do tipo Pitot-estático e redundância de componentes:

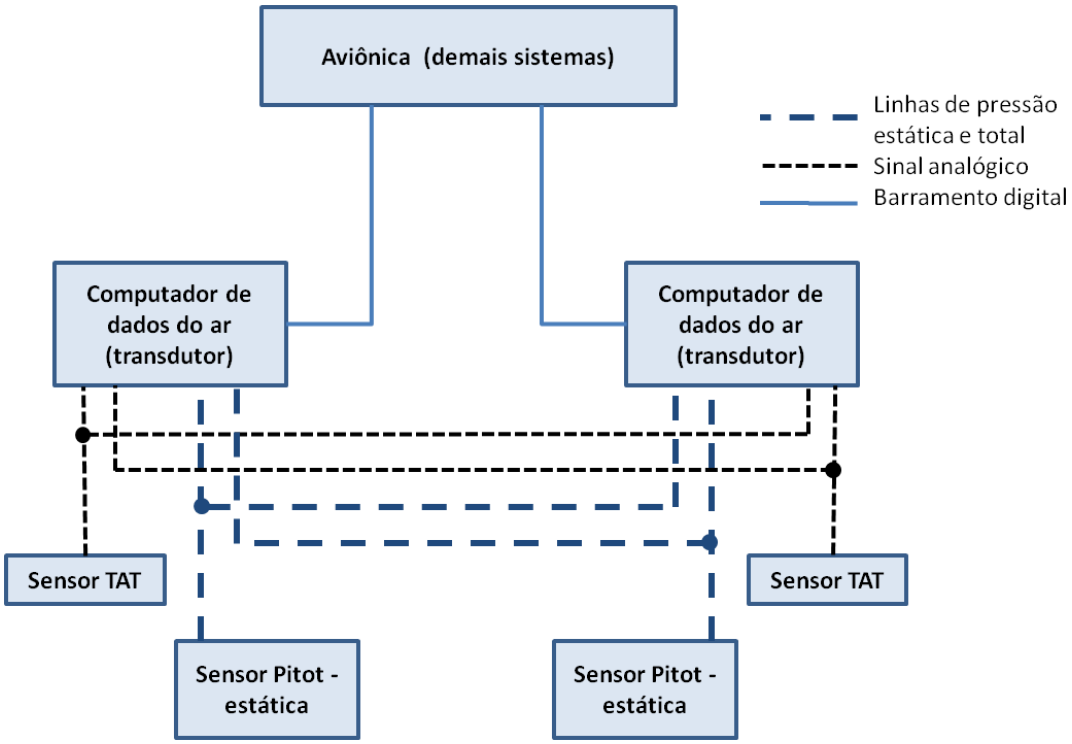

Figura 6.4 – Sistema de dados do ar genérico.

Os modernos computadores de dados do ar utilizam componentes eletrônicos digitais como memórias e microprocessadores, que podem ser susceptíveis a partículas ionizantes que causariam SEUs neste sistema.

6.2.5.1. Estabelecimento dos ambientes previstos de radiações ionizantes para a aeronave

Para exemplificar a aplicação dos cenários e o impacto da atividade solar no fluxo de partículas potencialmente causadoras de SEUs, o estudo de (SUGGS será usado em conjunto com (INCEOGLU et al., 2013) para estimação dos cenários futuros para sistemas eletrônicos embarcados aeronáuticos. O objetivo aqui tem caráter apenas qualitativo e não pretende definir um ambiente a ser usado, mas sim ilustrar a possibilidade do uso das diversas fontes de dados disponíveis na literatura no auxílio a projetos e operação de sistemas eletrônicos embarcados.

Cenário 1: Ambiente de Radiações Ionizantes Durante um Ciclo Solar de Alta Intensidade

O primeiro cenário considerado é um ciclo solar futuro de alta intensidade. A Figura 6.5 é um gráfico com os dados de (SUGGS, 2013), com as estimativas mês a mês do numero médio de manchas solares para um percentil de 95%, ou seja, considerando uma atividade solar intensa para os ciclos 24 e 25.

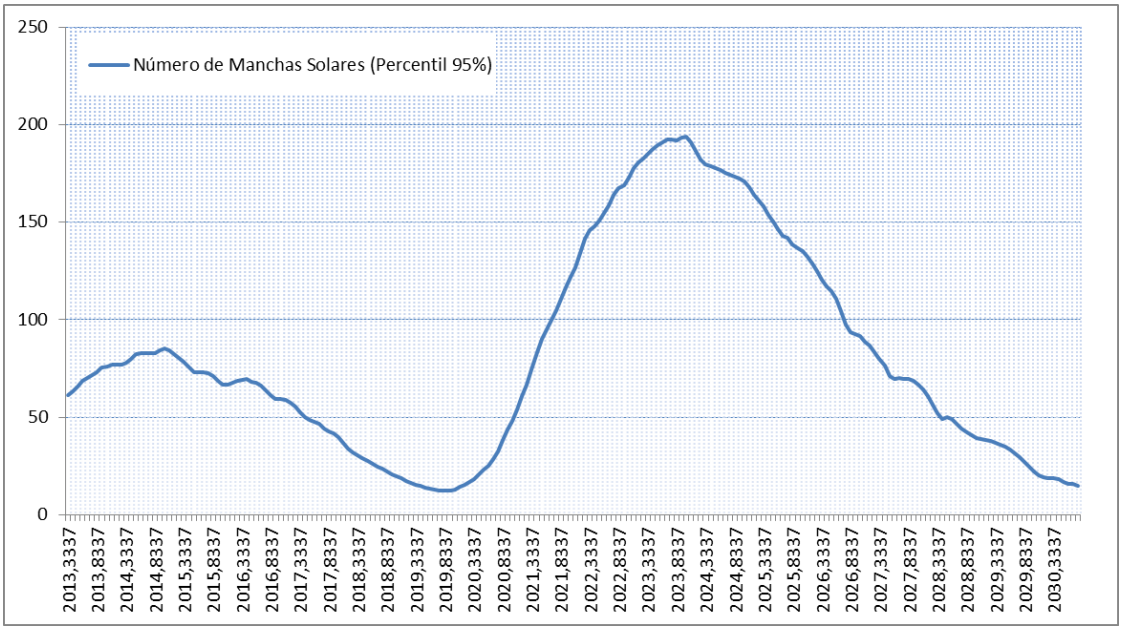

Figura 6.5: Número médio de manchas solares estimado entre 2013 e 2030
Fonte: dados extraídos de SUGGS (2013).

Inceouglu et al. (2013) considerou em seu estudo a seguinte equação de regressão linear como uma possível aproximação da anti-correlação entre manchas solares e contagem de nêutrons na atmosfera:

$$NCR = \beta SSN + \alpha \quad (1)$$

(6.2)

Onde:

NCR = número de nêutrons por hora;

SSN = número de manchas solares;

β = parâmetro linear.

α = parâmetro angular;

Os valores dos parâmetros α e β são definidos de acordo com a estação de monitoramento de nêutrons (McMurdo, Swarthmore, Pólo Sul e Thule). Considerando-se a estação de Thule, por exemplo, temos os seguintes parâmetros calculados por (INCEOGLU et. al., 2013) para o ciclo 22: β = 4622 e α = -5,3. Aplicando-se a fórmula (1) para os dados de (SUGGS, 2013) e os valores de β e α acima, obtemos a Figura 6.6, que indica uma anti-correlação entre a atividade solar prevista intensa (número de manchas solares médio mensal em azul, curva inferior) e o fluxo de nêutrons na atmosfera (contagem de nêutrons por hora média mensal da estação de Thule em vermelho, curva superior) coerente com a Figura 4.6.

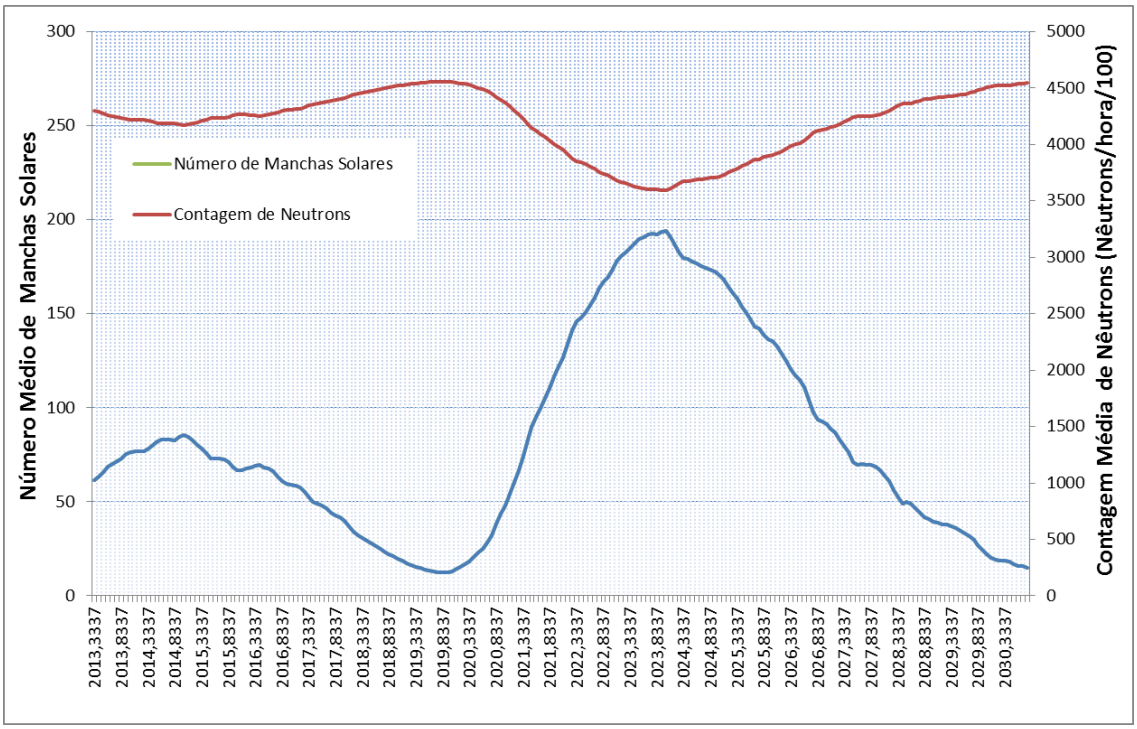

Figura 6.6: Contagem média de nêutrons estimada para um ciclo solar de alta intensidade.

Os valores máximo e mínimo de contagem de nêutrons por hora atingidos para o período abrangido pela Figura 6.6 são respectivamente 4557 e 3594

nêutrons/hora/100. Os valores correspondem aos períodos esperados de mínimo solar (4557 nêutrons/hora/100) e máximo solar (3594 nêutrons/hora/100).

A partir destes valores, procurou-se identificar os registros do medidor de Thule que correspondessem a dois critérios de representatividade:

- um registro de contagem de nêutrons com o valor máximo igual ou próximo a 4557 nêutrons/hora/100 e que tenha ocorrido durante um período de mínimo solar;
- um registro de contagem de nêutrons com o valor mínimo igual ou próximo a 3594 nêutrons/hora/100 e que tenha ocorrido durante um período de máximo solar;

Tais registros estão disponíveis no site http://neutronm.bartol.udel.edu/~pyle/bri_table.html, onde é possível resgatar os registros de contagem de diversas estações de contagem de nêutrons ao redor do globo, de 1960 até a data atual.

Desta forma, para o caso de mínimo solar, foi escolhido o dia de 21 de maio de 2007, que atingiu valores próximos a 4557 nêutrons/hora/100 e, para o caso de máximo solar, foi escolhido o dia de 22 de março de 1990, que atingiu valores próximos a 3595 nêutrons/hora/100.

Estas datas foram buscadas com o objetivo de inseri-las como parâmetros para estimar o espectro de nêutrons através do software EXPACS, ilustrando o ambiente de nêutrons esperado para este cenário.

De acordo com o discutido anteriormente, os parâmetros que devem ser considerados para estimar este ambiente são a máxima altitude operacional da aeronave e a máxima latitude operacional que, para o estudo de caso em questão, serão 43 kft e 90º, respectivamente.

As Figuras 6-7 e 6-8 abaixo mostram o resultado da simulação do espectro de nêutrons por meio do software EXPACS (SATO, 2010), para o cenário de ciclo solar de alta intensidade, considerando uma altitude de 43 kft (13,1 km) e 90

graus de latitude. É possível distinguir os períodos de menor atividade de nêutrons (22 de março de 1990, Figura 6-7), e de maior atividade (dia de 21 de maio de 2007, Figura 6-8).

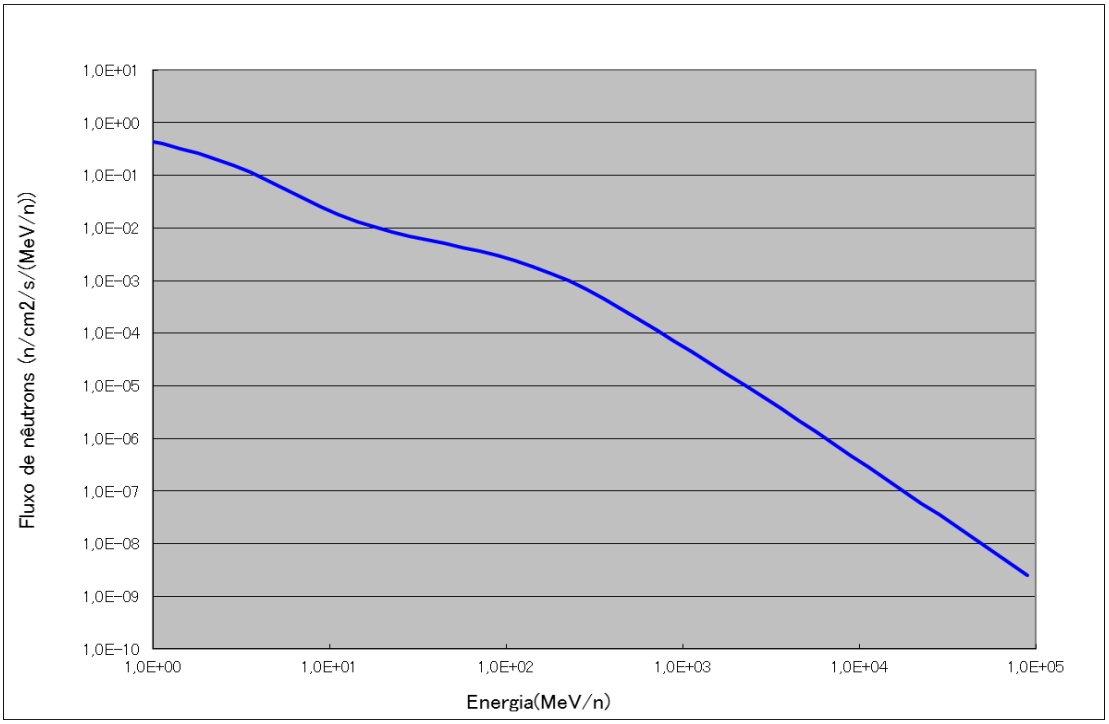

Figura 6.7: Espectro de nêutrons para o cenário de ciclo solar de alta intensidade, altitude de 43 kft (13,1 km), 90 graus de latitude e máximo solar.

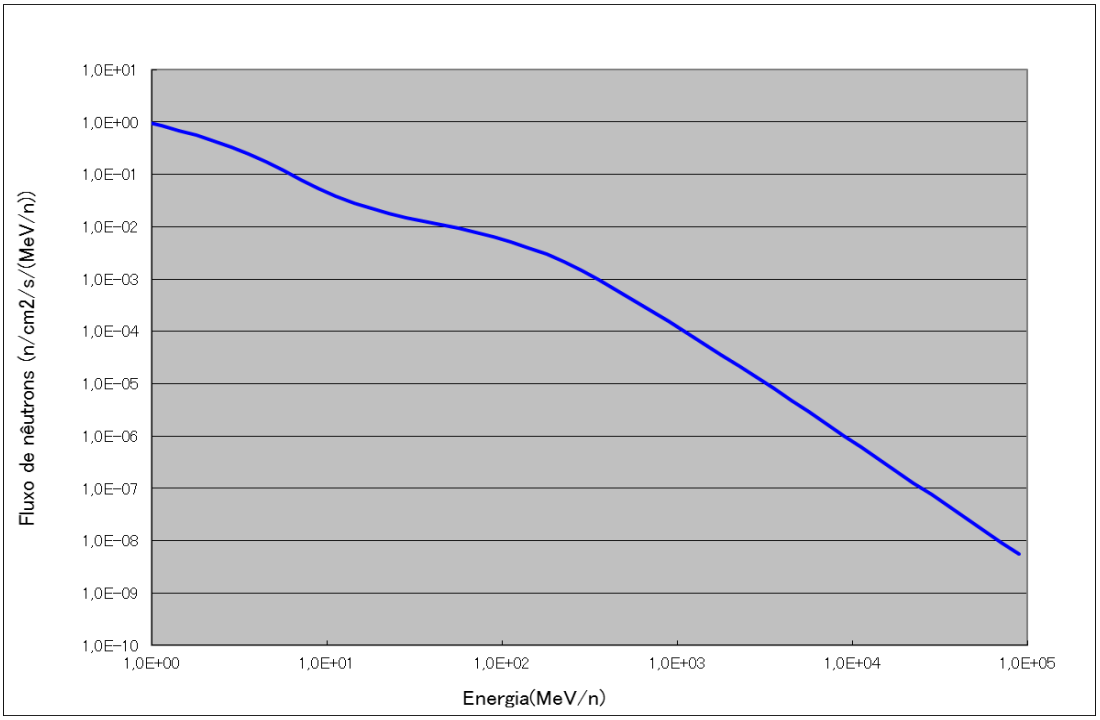

Figura 6.8: Espectro de nêutrons para o cenário de ciclo solar de alta intensidade, altitude de 43 kft (13,1 km), 90 graus de latitude e mínimo solar.

Fazendo-se uma integração numérica do fluxo de nêutrons para energias acima de 10 MeV, encontramos os valores aproximados de 4059 e de 8698 nêutrons/cm^2/hora, respectivamente para os casos da Figura 6.7 e Figura 6.8.

Cenário 2: Ambiente de Radiações Ionizantes Durante um Ciclo Solar de Média Intensidade

O segundo cenário a ser considerado é um ciclo solar futuro de média intensidade. A Figura 6.9 é um gráfico com os dados de (SUGGS, 2013) com as estimativas mês a mês do numero médio de manchas solares para um percentil de 50%, ou seja, considerando uma atividade solar média para os ciclos 24 e 25.

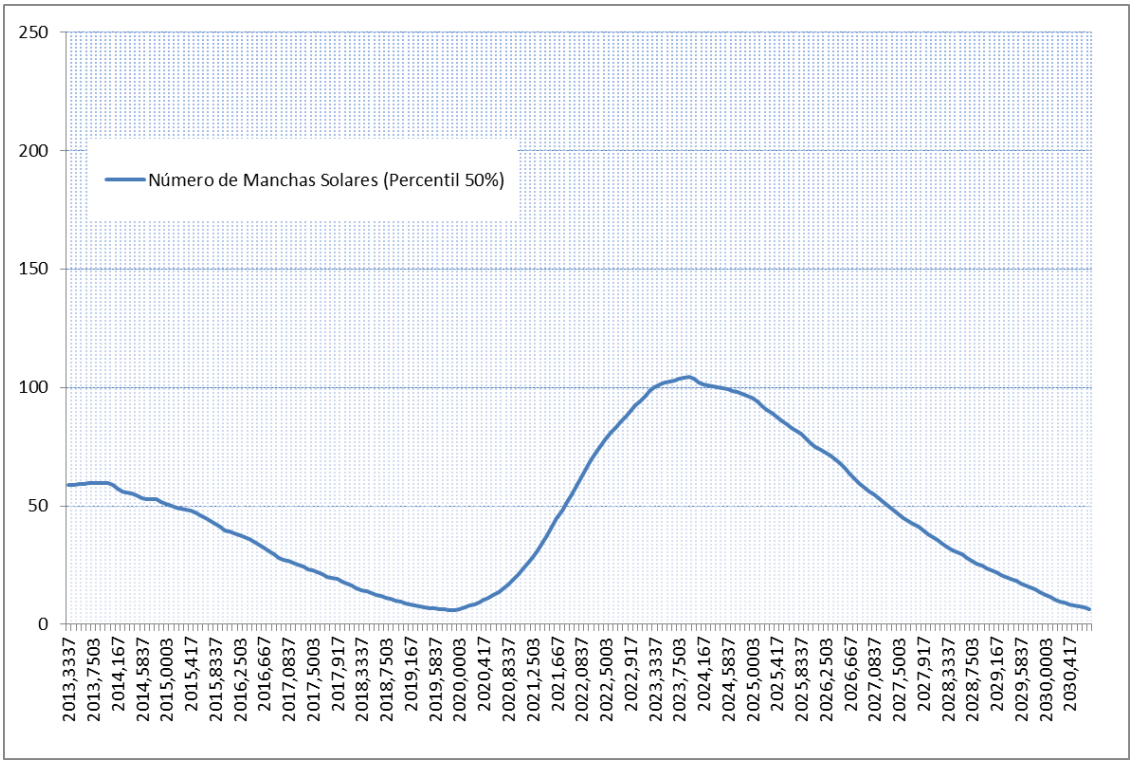

Figura 6.9: Número médio de manchas solares estimado entre 2013 e 2030
Fonte: dados extraídos de SUGGS (2013).

A mesma metodologia do item anterior foi usada para estimar a contagem média de nêutrons da estação de Thule, e o resultado é ilustrado na Figura 6.10, que indica uma anti-correlação entre a atividade solar prevista intensa (número de manchas solares médio mensal em azul, curva inferior) e o fluxo de nêutrons na atmosfera (contagem de nêutrons por hora média mensal da estação de Thule em vermelho, curva superior) coerente com a Figura 4.6.

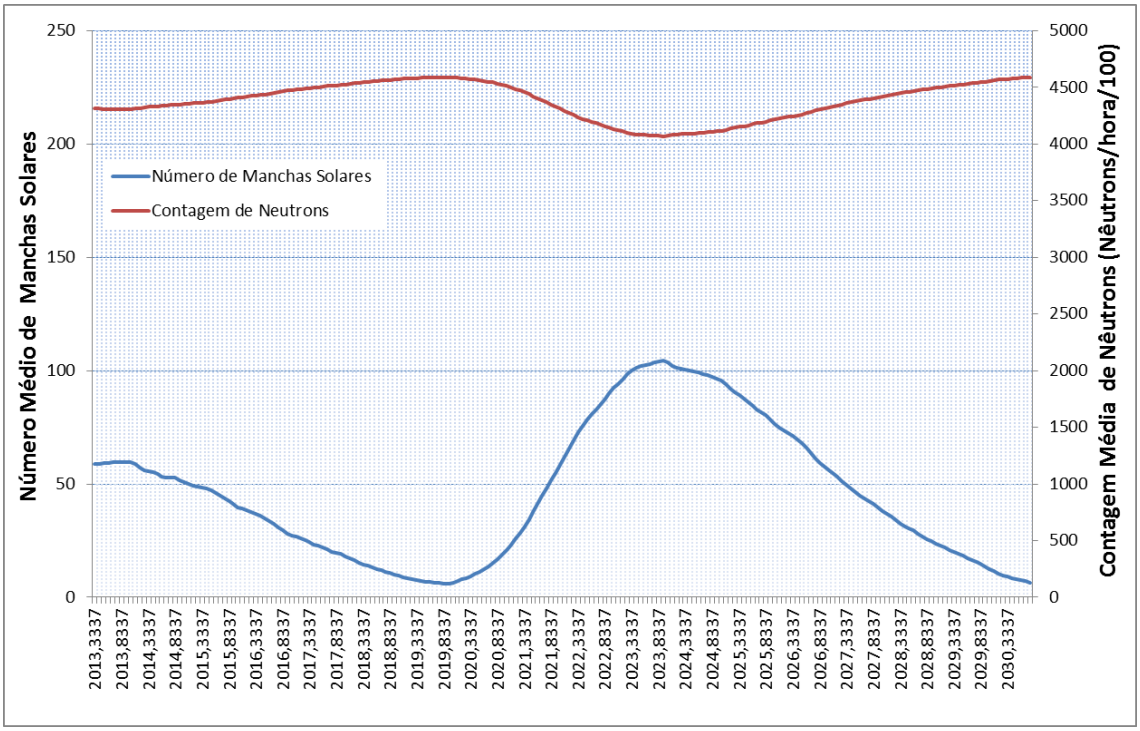

Figura 6.10: Contagem média de nêutrons estimada para um ciclo solar de média intensidade.

Os valores máximo e mínimo de contagem de nêutrons por hora atingidos para o período abrangido pela Figura 6.10 são respectivamente 4590 e 4068 nêutrons/hora/100. Os valores correspondem aos períodos esperados de mínimo solar (4590 nêutrons/hora/100) e máximo solar (4068 nêutrons/hora/100). Para os registros do medidor de Thule que correspondem ao caso de mínimo solar, foram escolhidos o dia de 08 de dezembro de 2007, e para o caso de máximo solar, foi escolhido o dia de 25 de dezembro de 1991. Estes registros estão disponíveis para consulta na internet em http://neutronm.bartol.udel.edu/~pyle/bri_table.html.

Estas datas foram inseridas como parâmetros para estimar o espectro de nêutrons através do software EXPACS, ilustrando o ambiente de nêutrons esperado para este cenário, considerando mais uma vez uma máxima altitude operacional de 13,1 km (43 kft) e sem limitação operacional de voos em latitudes altas.

As figuras abaixo mostram o resultado da simulação do espectro de nêutrons por meio do software EXPACS, para o cenário de ciclo solar de média intensidade, considerando uma altitude de 13,1 km (43 kft) e 90 graus de latitude. É possível distinguir os períodos de menor atividade de nêutrons (25 de dezembro de 1991) e de maior atividade (08 de dezembro de 2007).

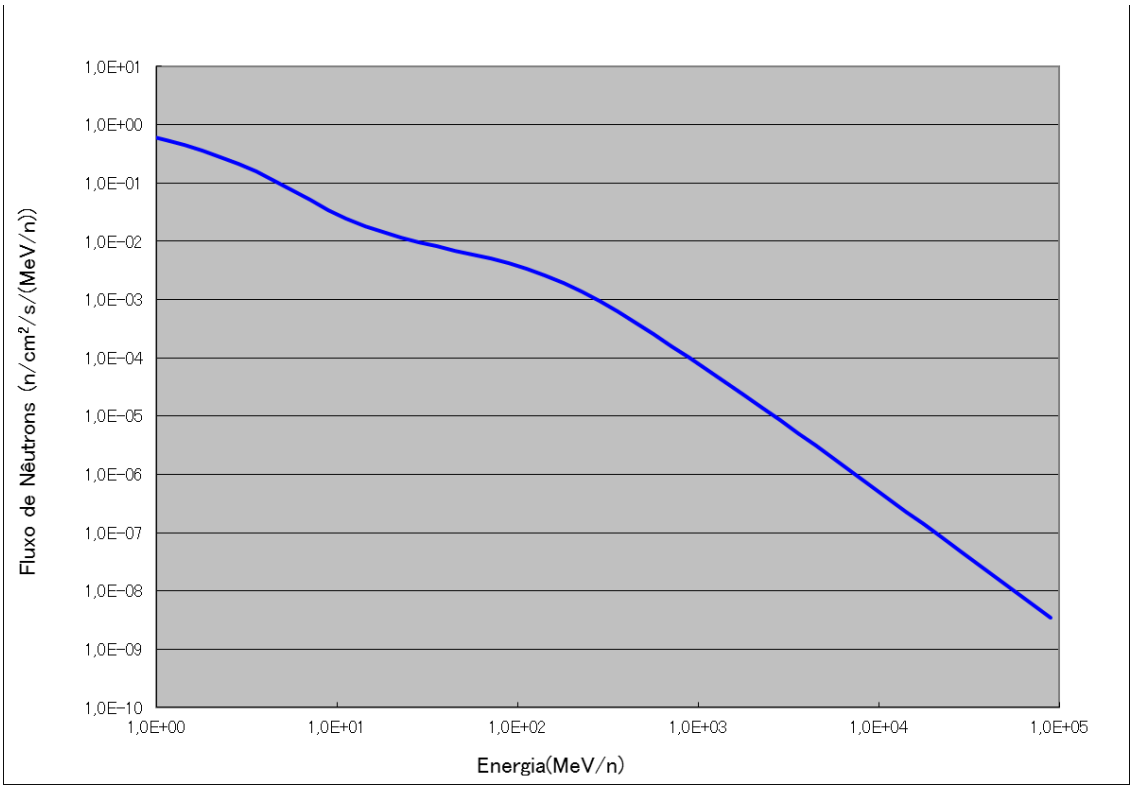

Figura 6.11: Espectro de nêutrons para o cenário de ciclo solar de média intensidade, altitude de 43 kft (13,1 km), 90 graus de latitude e máximo solar.

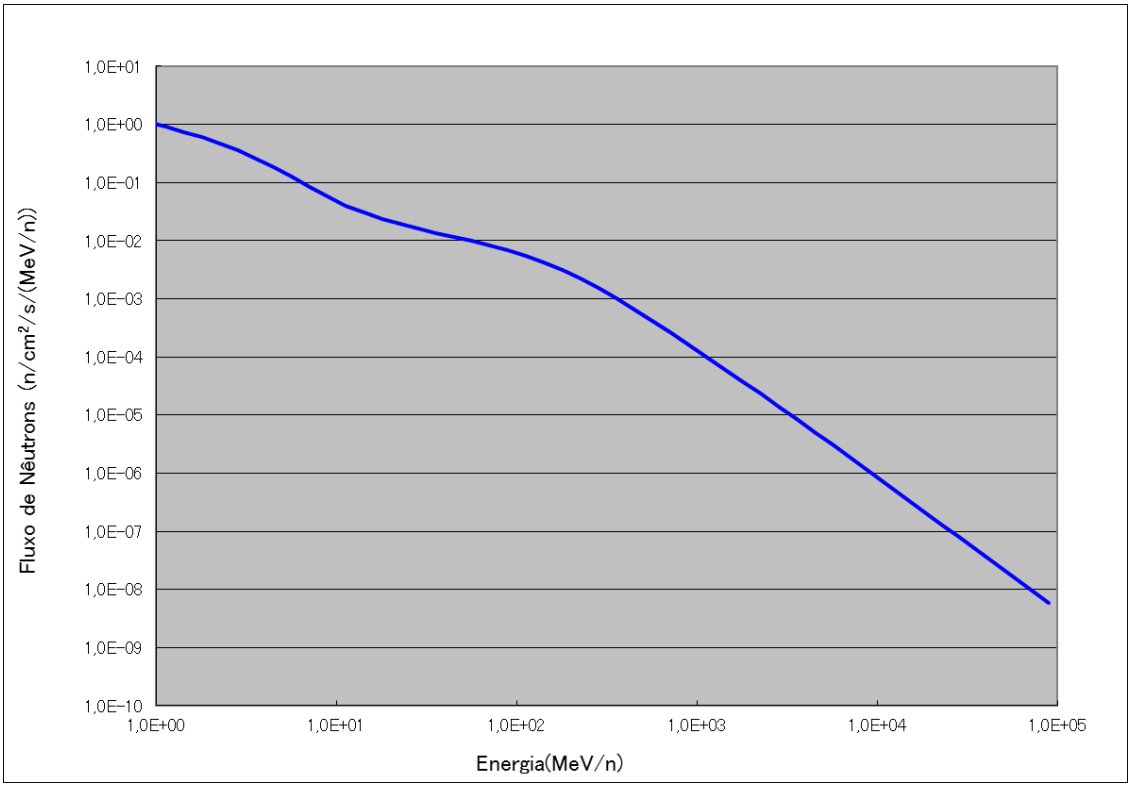

Figura 6.12: Espectro de nêutrons para o cenário de ciclo solar de média intensidade, altitude de 43 kft (13,1 km), 90 graus de latitude e mínimo solar.

Fazendo-se uma integração numérica do fluxo de nêutrons para energia acima de 10 MeV, encontramos os valores aproximados de 5577 e de 9245 nêutrons/cm^2/hora, respectivamente para os casos da Figura 6.11 e Figura 6.12.

Cenário 3: Ambiente de Radiações Ionizantes Durante um Ciclo Solar de Baixa Intensidade

O terceiro cenário considerado é um ciclo solar futuro de baixa intensidade. A Figura 6.13 é um gráfico com os dados de (SUGGS, 2013) com as estimativas mês a mês do numero médio de manchas solares para um percentil de 5%, ou seja, considerando uma atividade solar baixa para os ciclos 24 e 25.

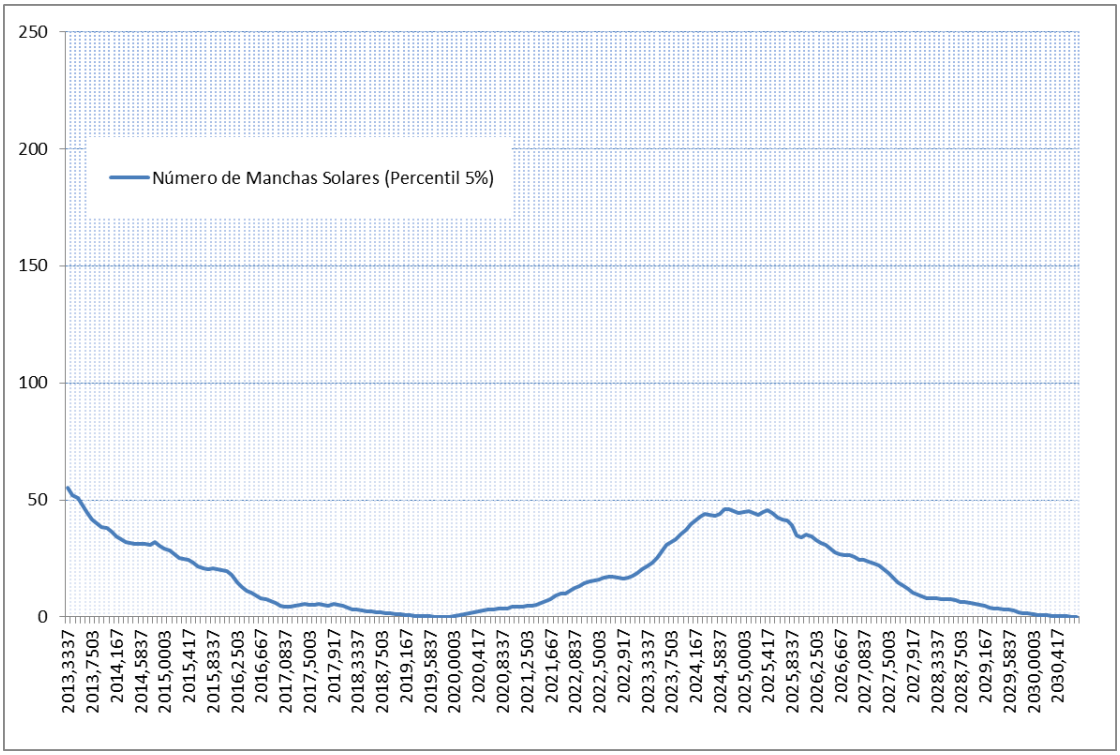

Figura 6.13: Número médio de manchas solares estimado entre 2013 e 2030
Fonte: dados extraídos de SUGGS (2013).

Mais uma vez, a mesma metodologia do item anterior foi usada para estimar a contagem média de nêutrons da estação de Thule,e o resultado é ilustrado na Figura 6.14, que indica uma anti-correlação entre a atividade solar prevista intensa (número de manchas solares médio mensal em azul, curva inferior) e o fluxo de nêutrons na atmosfera (contagem de nêutrons por hora média mensal da estação de Thule em vermelho, curva superior).

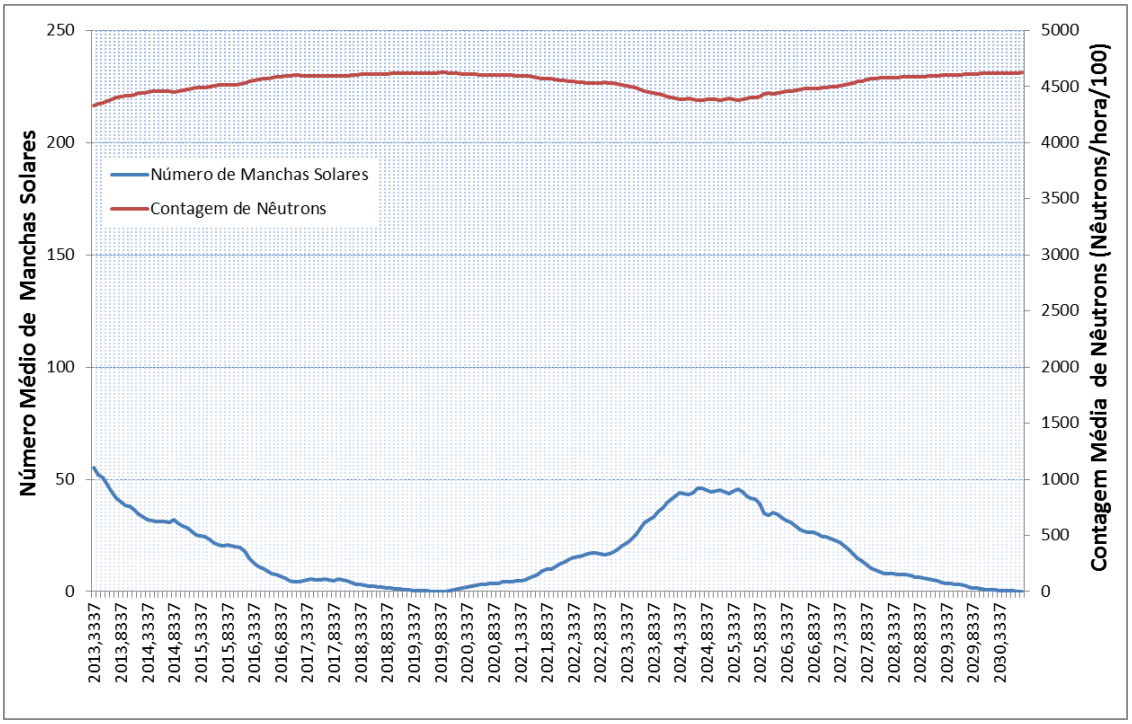

Figura 6.14: Contagem média de nêutrons estimada para um ciclo solar de baixa intensidade.

O valor máximo e mínimo de contagem de nêutrons por hora atingidos para o período abrangido pela Figura 6.14 são respectivamente 4622 e 4329 nêutrons/hora/100. Os valores correspondem aos períodos esperados de mínimo solar (4622 nêutrons/hora/100) e máximo solar (4329 nêutrons/hora/100). Para os registros do medidor de Thule que correspondem ao caso de mínimo solar, foram escolhidos o dia de 11 de outubro de 2007, e para o caso de máximo solar, foi escolhido o dia de 15 de janeiro de 1971.

Estas datas foram inseridas como parâmetros para estimar o espectro de nêutrons através do software EXPACS, ilustrando o ambiente de nêutrons esperado para este cenário, considerando mais uma vez uma máxima altitude operacional de 43 kft e sem limitação operacional de voos em latitudes altas.

As figuras abaixo mostram o resultado da simulação do espectro de nêutrons por meio do software EXPACS, para o cenário de ciclo solar de média intensidade, considerando uma altitude de 43 kft (13,1 km) e 90 graus de

latitude. É possível distinguir os períodos de menor atividade de nêutrons (15 de janeiro de 1971) e de maior atividade (11 de outubro de 2007).

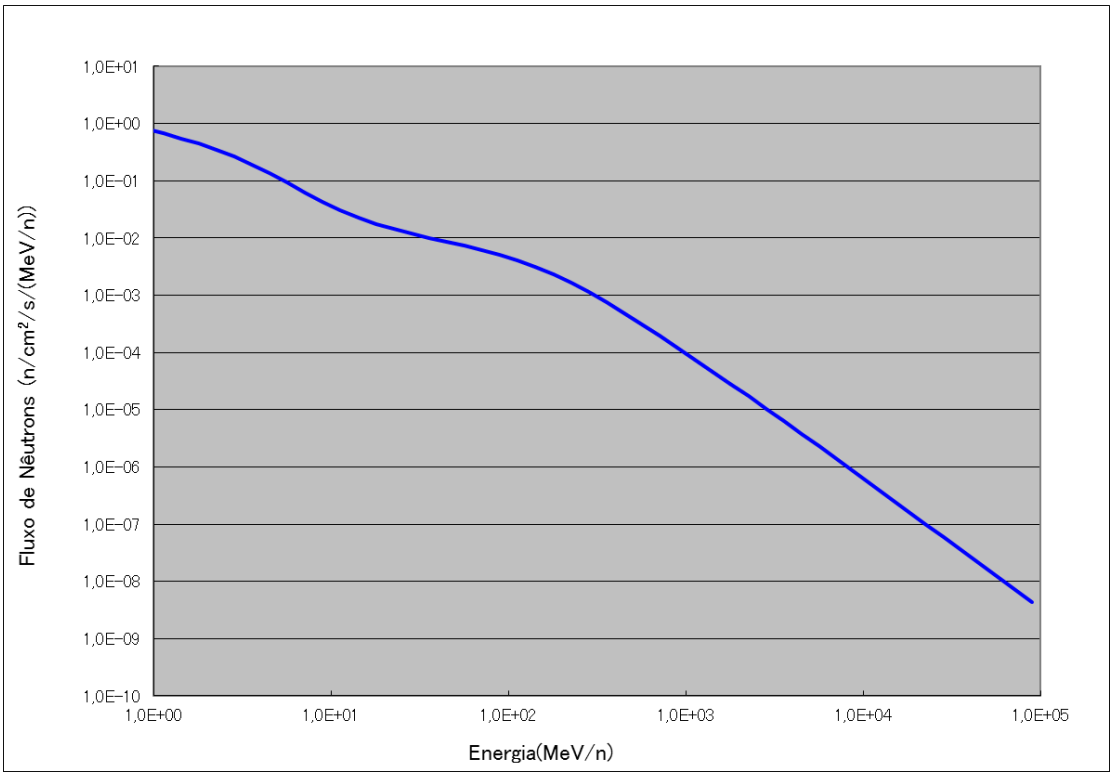

Figura 6.15: Espectro de nêutrons para o cenário de ciclo solar de média intensidade, altitude de 43 kft (13,1 km), 90 graus de latitude e máximo solar.

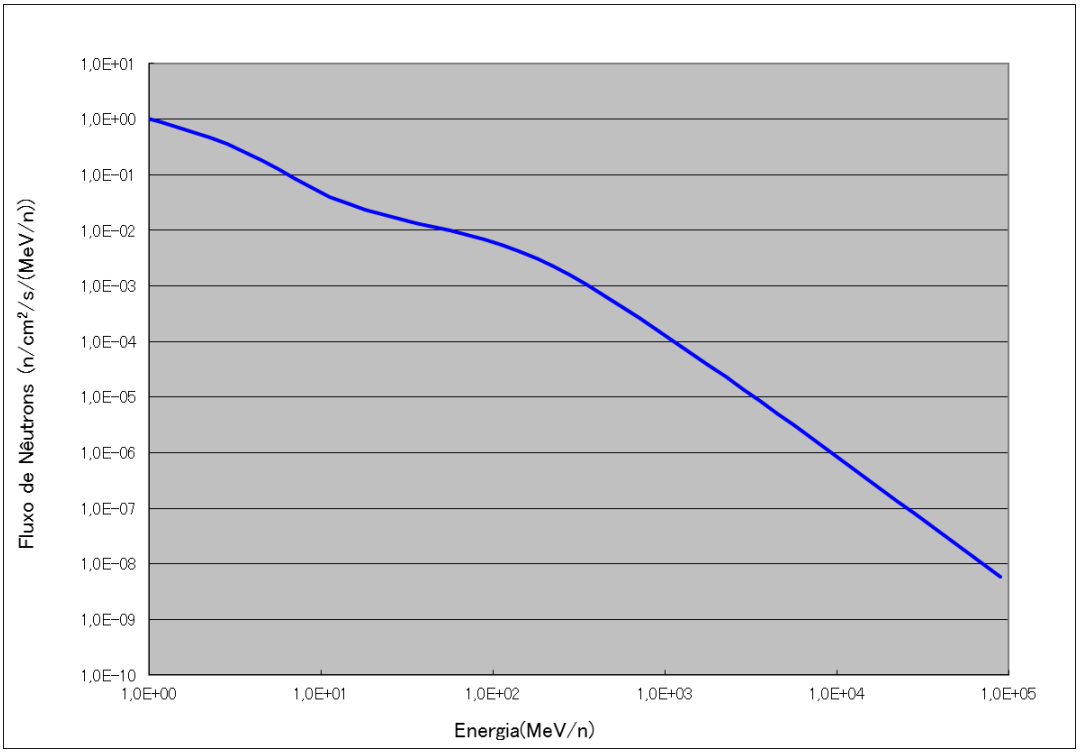

Figura 6.16: Espectro de nêutrons para o cenário de ciclo solar de média intensidade, altitude de 43 kft (13,1 km), 90 graus de latitude e mínimo solar.

Fazendo-se uma integração numérica do fluxo de nêutrons para energia acima de 10 MeV, encontramos os valores aproximados de 6870 e de 9230 nêutrons/cm^2/hora, respectivamente para os casos da Figura 6.15 e Figura 6.16.

Os três cenários que foram ilustrados acima demonstram quantitativamente a variação do ambiente de nêutrons na atmosfera em função da previsão da atividade solar futura.

A Figura 6.17 abaixo mostra a composição dos três cenários analisados, para fins de comparação:

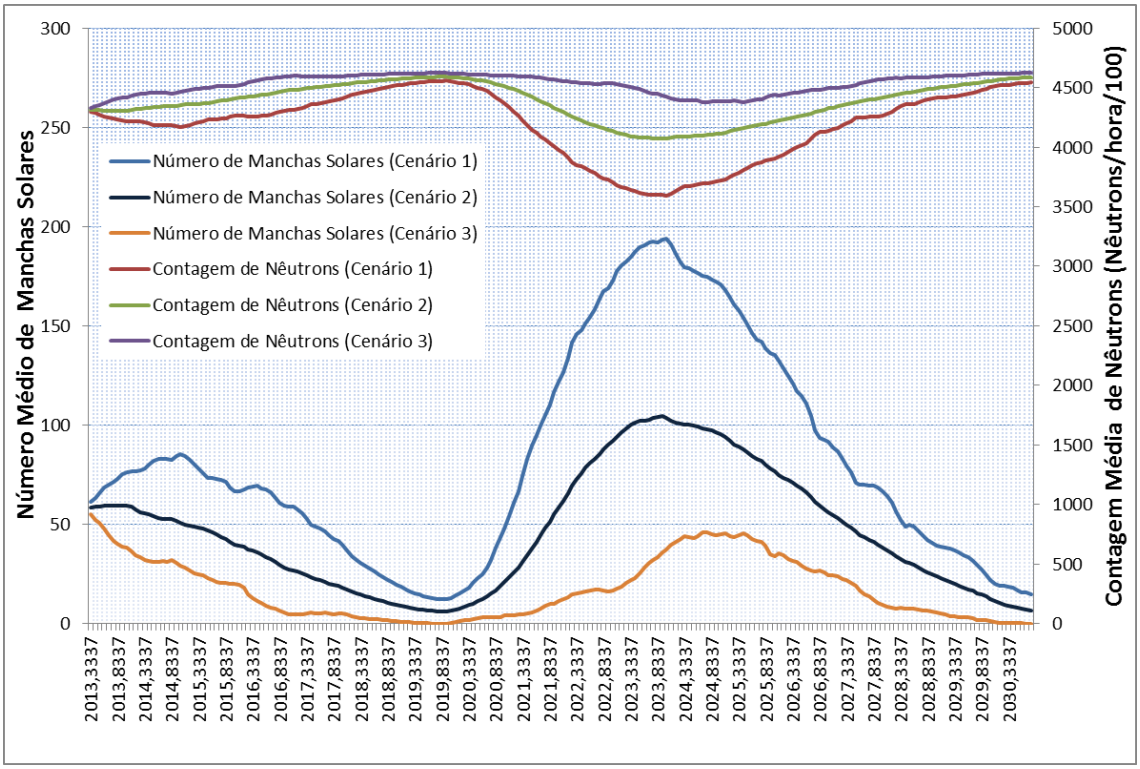

Figura 6.17: Composição dos resultados para os cenários futuros de ciclo solar de baixa, média e alta intensidade, altitude de 43 kft (13,1 km) e 90 graus de latitude.

A tabela abaixo reúne os valores de fluxo de nêutrons para energias acima de 10 MeV estimados para os três cenários, considerando um altitude de 43 kft e 90 graus de latitude.

Tabela 6-4 – Valores de fluxo de nêutrons acima de 10 MeV encontrados para cada cenário

	Fluxo de nêutrons para Cenário 1 (n/cm^2/h)	**Fluxo de nêutrons para Cenário 2 (n/cm^2/h)**	**Fluxo de nêutrons para Cenário 3 (n/cm^2/h)**
Mínimo Solar	8698	9245	9230
Máximo Solar	4059	5577	6870

Dadas as incertezas e imprecisões nos cálculos, modelos e abordagens, era de se esperar que houvessem inconsistências nos valores encontrados, como foi no caso entre o mínimo solar do cenário 2 em relação ao cenário 3 (esperava-

se que o cenário 3 encontrasse um fluxo de nêutrons maior que o cenário 2). Por outro lado, nota-se uma boa concordância com o discutido em itens anteriores, além da evidência quantitativa da anti-correlação entre a atividade solar e os nêutrons secundários potencialmente causadores de SEUs. A aplicação das recomendações para definição do ambiente de radiação ionizante também é mais precisa e representativa do ambiente real que a aeronave vai operar em comparação ao fluxo padrão de 6000 n/cm^2 estabelecido na IEC 62396-1.

Aplicando-se o fator de acomodação de 1,3 para o fluxo de prótons, temos como resultado final os fluxos em p/cm^2/h (onde p é o fluxo total nêutrons + prótons), para os cenários conforme tabela abaixo.

Tabela 6-5 – Valores de fluxo para o estudo de caso de aplicação das recomendações para sistemas eletrônicos embarcados aeronáuticos

	Fluxo para Cenário 1 (p/cm^2/h)	**Fluxo para Cenário 2 (p/cm^2/h)**	**Fluxo para Cenário 3 (p/cm^2/h)**
Mínimo Solar	11307	12019	11999
Máximo Solar	5277	7250	8931

6.2.5.2. Listagem dos componentes potencialmente susceptíveis a SEU

Para o sistema eletrônico embarcado deste estudo de caso, consideraremos 2 componentes internos ao computador de dados do ar como potencialmente susceptíveis a SEUs, de acordo com a Tabela 6-3, envolvidos no armazenamento de dados de velocidade, classificados pela metodologia da ARP 4754 como tendo IDAL A:

- Uma memória SRAM Samsung K6X4016C3F, de 256 k x 16 bit (4 Mbit), com seção de choque de 5.10^{-15} cm^2/bit para testes com nêutrons de alta energia e de 1,0.10^{-14} cm^2/bit para testes com nêutrons térmicos.

• Uma memória de 10 Mbit, de tecnologia SRAM, sem dados de seção de choque disponível e uso de boro na fabricação.

A classificação do IDAL, conforme definido nas recomendações reflete as normas mais atuais de desenvolvimento de aeronaves e seus sistemas (ARP 4754 revisão A).

6.2.5.3. Susceptibilidade dos componentes a SEUs

Os componentes listados em 6.2.5.2 têm classificação IDAL A. Para estimar a susceptibilidade dos componentes a SEUs, o critério do capítulo 7 da IEC 62396-1 foi aplicado com os ajustes do item 6.2.3.3.

A memória K6X4016C3F, de 256 k x 16 bit (4Mbit), tem seção de choque definida de 5.10^{-15} cm^2/bit.

De acordo com o Anexo B.4 da IEC 62396-1, devemos considerar para a memória de 10 Mbit, de tecnologia SRAM, uma seção de choque de 5.10^{-13} cm^2/bit, de modo conservativo, baseado em dados de memórias semelhantes.

Os valores de fluxo estimados no item 6.2.5.1 e os valores de seção de choque são usados na seguinte fórmula, de acordo com o item 8 da IEC 62396-1:

$$\textit{Taxa de SEUs} = \textit{fluxo (partículas/cm}^2\textit{.h}^{-1}\textit{) x seção de choque (cm}^2\textit{/bit)} \quad (6.3)$$

Os valores máximos obtidos de taxa de SEUs, de acordo com os fluxos estimados na Tabela 6-5 são:

- Memórias K6X4016C3F = $6{,}0.10^{-11}$ SEU/bit/hora
- Memórias de 10 Mbit SRAM = $6{,}0.10^{-9}$ SEU/bit/hora

Para nêutrons térmicos, ao aplicar a IEC 62396-5, teremos a seguinte fórmula:

$$\textit{Taxa de SEUs} = \textit{Taxa de SEU de nêutrons de alta energia X Razão1 X Razão2} \quad (6.4)$$

Os valores máximos obtidos de taxa de SEUs para nêutrons térmicos, de acordo com os fluxos estimados na Tabela 6-5 são:

- Memórias K6X4016C3F = $1{,}3.10^{-10}$ SEU/bit/hora
- Memórias de 10 Mbit SRAM = $1{,}8.10^{-8}$ SEU/bit/hora

Para as memórias em questão, teremos como valor de taxa de ocorrência de SEUs para o componentes de $7{,}6.10^{-4}$ SEU/componente/hora e $2{,}4.10^{-1}$ SEU/componente/hora, respectivamente para a memória K6X4016C3F e memória de 10 Mbit SRAM. É possível concluir que a maior precisão de dados de testes da memória K6X4016C3F gera taxas de SEUs de menos que duas ordens de grandeza inferior à memória de 10 Mbit, que não tem dados de testes disponíveis. Embora as memórias sejam fabricadas com o mesmo tipo de tecnologia (SRAM), a incerteza nos dados da memória de 10 Mbit leva a números consideravelmente maiores.

Para o computador de dados do ar, portanto, teremos uma taxa final de ocorrência de SEUs de $2{,}407.10^{-1}$ SEU/computador/hora.

Para o caso de ocorrência de um SEPE, de acordo com as recomendações, teremos uma taxa 25 vezes maior, ou seja, de 6 SEU/computador/hora, ou seja, a cada hora é esperado ao menos 6 SEUs em um evento de partículas solares.

6.2.5.4. Análise de ocorrência de SEUs dos componentes no sistema

A análise da ocorrência dos SEUs nos componentes do sistema envolve diversas técnicas e considerações que, dadas as limitações deste estudo de caso, não serão exploradas. No entanto, alguns pontos podem ser discutidos à luz das taxas de SEUs obtidas em 6.2.5.3.

A taxa final de SEUs deve levar em consideração o tempo de voo típico da aeronave, ou seja, qual é o tempo médio de voo, em horas, a ser considerado nas análises de segurança durante os processos de desenvolvimento e certificação do projeto ou, ainda, a duração da fase de voo especifica onde a

condição de falha catastrófica ocorre. No caso de estudo, se tivermos um tempo médio de 4 horas, a taxa de ocorrência em um voo será de $2{,}4.10^{-1}$ SEU/computador/voo.

As análises de falha devem considerar também quais os bits efetivamente usados pelo sistema, ou seja, quais os SEUs que causariam uma falha funcional no sistema. Este fator pode reduzir consideravelmente as taxas estimadas acima.

Muitas das memórias atualmente em uso na aviação possuem técnicas de EDAC embutidas. Assim, os bits que estão protegidos por esta técnica poderiam ser excluídos do cálculo das taxas de ocorrência.

Em geral, as taxas de falha são inseridas em análises com o uso de ferramentas como as FTA. Desta forma, os SEUs são inseridos no contexto de outras falhas que o sistema estará sujeito. O resultado final desta análise pode levar a taxas de falhas inaceitáveis de acordo com os requisitos de segurança, como, por exemplo, o RBAC 25.1309. Para uma falha funcional do sistema de dados do ar que leve a uma condição catastrófica, a taxa de falhas deve ser inferior a 1.10^{-9}.

O uso das recomendações do presente trabalho gera dados quantitativos que viabilizam a identificação das susceptibilidades dos componentes a SEUs dentro do contexto do sistema. Isto facilita a identificação dos pontos fracos na arquitetura do sistema e que necessitam de medidas de mitigação adicionais.

6.2.5.5. Uso de medidas de mitigação

O estudo de caso não pretende explorar o uso de medidas de mitigação, pois a aplicação destas técnicas envolve o conhecimento detalhado da arquitetura do sistema em diversos níveis, de modo que se obtenha a melhor opção de mitigação levando em conta critérios como custo, efetividade e prazos.

Um fator a se considerar para o caso de SEUs é o uso de redundâncias no nível do sistema. Para o estudo de caso, foi considerado que os componentes

têm um taxa de falhas sem considerações se os dados armazenados são providos por outro computador de dados do ar, mostrado na Figura 6.4.

Outro fator a se considerar é a incerteza nos dados de testes dos componentes, evidenciando a necessidade de se testar os componentes a serem instalados nos sistemas aviônicos embarcados quanto à susceptibilidade aos SEUs.

6.2.6.Geração de Requisitos para SEUs

Este item é uma discussão complementar às recomendações expostas acima. Tais recomendações devem evoluir para a criação de um processo de garantia de robustez a SEUs em sistemas eletrônicos embarcados, e um dos aspectos que devem ser abordados por tal processo é a criação de requisitos para robustez a SEUs.

Requisitos para SEUs no contexto da certificação aeronáutica

No conjunto de requisitos do RBAC 25, alguns tratam especificamente de condições ambientais adversas as quais os aviões estão sujeitos durante sua operação. Por exemplo, os sistemas eletrônicos embarcados, de acordo com a criticalidade das funções executadas, devem atender ao requisito RBAC 25.1316, que trata da proteção contra descargas atmosféricas para sistemas.

Outras condições de instalação e operação do sistema em um determinado ambiente do avião estão cobertas por requisitos como o RBAC 25.1309, que é um requisito mais abrangente e aplicado para equipamentos, sistemas e instalações da aeronave. Este demanda que, levando em consideração as condições esperadas de operação, o sistema não contenha uma falha simples que leve a uma condição catastrófica (perda do avião e de vidas humanas). Além disso, deve ser demonstrado que há uma relação inversa (de modo qualitativo e quantitativo) entre a criticalidade da função executada pelo sistema e a probabilidade de falha desta. O objetivo final é se obter um projeto livre de falhas. Este conceito é conhecido como *fail safe*. É a partir deste requisito que as atividades para demonstração de tal conceito, como o SSA,

que consiste em testes e avaliações sistemáticas e abrangentes do sistema com o objetivo de se demonstrar que o projeto atende ao conceito *fail safe*, são demandadas.

Para auxiliar no processo de demonstração de cumprimento com os requisitos de certificação, são emitidos documentos chamados de *policies*, como é o caso da Advisory Circular (AC) 25.1309-1A, que é um guia contendo um meio aceitável, mas não o único, para se atender ao requisito 25.1309. No detalhamento das ferramentas e métodos para demonstração de cumprimento com o requisito, são reconhecidos outros documentos de apoio, como é o caso da ARP 4761, que auxilia no detalhamento do processo de *safety assessment*, e a ARP 4754, que trata do processo de desenvolvimento de sistemas aeronáuticos embarcados.

A DO 160, reconhecida pela FAA através da AC 21-16, é o padrão mais usado para procedimentos de testes e condições ambientais (vibração, temperatura, fogo, interferência eletromagnética, etc.) para equipamentos embarcados, contendo qualificações ambientais aceitáveis para demonstrar cumprimento com vários requisitos de aeronavegabilidade, incluindo aspectos cobertos pelo RBAC 25.1309. É dividida em diversos capítulos descrevendo procedimentos de testes. No entanto, não havendo ainda nenhum que cubra os aspectos relacionados às partículas ionizantes presentes na atmosfera, que podem causar os SEEs.

A IEC 62396-1 não tem caráter de "*policy*", ou seja, não está ligada a um requisito do RBAC 25 por meio de um documento emitido pela ANAC ou FAA, até a data do presente trabalho.

Por outro lado, dentro do processo de desenvolvimento e produção de hardware eletrônico aeroembarcado da DO-254, o *Certification Memorandum* EASA CM-SWCEH-001 *Development Assurance of Airborne Electronic Hardware* (Garantia de Desenvolvimento de Hardware Eletrônico Aeroembarcado) emitido pela EASA, embora sem caráter obrigatório, é usado para complementar e auxiliar nas atividades de demonstração de requisitos

como o RBAC 25.1309 aplicado aos hardwares eletrônicos. Em seu capitulo 6, o documento provê alguns recomendações para lidar com SEEs, basicamente recomendando duas análises para verificar a susceptibilidade dos componentes à SEEs: uma *top-down* e outra *botton-up*.

Os dois SIBs da EASA (SIB 2012-09 e SIB 2012-10) têm caráter apenas informativo e de recomendação, sobre o assunto. Recomenda que os fabricantes de aeronaves, projetistas de sistemas aviônicos e fabricantes de componentes eletrônicos embarcados trabalhem conjuntamente para avaliar os potenciais efeitos da radiação solar e galáctica nos níveis de componente, sistema e avião, de modo a conceberem sistemas que sejam tolerantes às faltas causadas por tais fenômenos.

Pelo exposto acima, é possível ver que há a preocupação com o fenômeno dos SEEs na certificação aeronáutica, mesmo que ainda não tenham sido emitidos requisitos específicos para SEEs.

Geração de Requisitos de Robustez a SEUs em Sistemas

Tanto no setor espacial quanto no aeronáutico, os processos de engenharia de sistemas buscam, por meio de uma abordagem interdisciplinar, transformar requisitos em uma solução, ou seja, um sistema que atenda aos requisitos

Conforme exposto no capítulo 2, a geração de requisitos é uma tarefa crítica e fundamental para o desenvolvimento de um sistema e, em última análise, para se obter o nível adequado de robustez à SEUs. Os requisitos de robustez a SEUs estarão inseridos nos processos de **Definição dos Requisitos dos Interessados** e **Análise dos Requisitos** , conforme descritos em 2.3.

Os requisitos são capturados começando pela elicitação dos requisitos dos interessados e definindo os requisitos de mais alto nível. Em geral, os requisitos do sistema são derivados, gerados e validados em relação aos requisitos do nível acima. A mesma abordagem é realizada para os itens do sistema e validada para o nível acima e assim por diante (aeronave/satélite, sistema, item, etc.). Esta atividade é crucial para definição e desenvolvimento

do sistema, pois identificam e quantificam as informações necessárias para um sistema completo e confiável.

Dentro deste contexto, para se obter um nível adequado de robustez de sistemas eletrônicos embarcados a SEUs causados por partículas ionizantes, deve-se buscar definir requisitos baseados na criticalidade das funções realizadas pelo sistema. O impacto funcional e a probabilidade de ocorrência do SEU em um sistema são os fundamentos para estabelecer um requisito de projeto. Quanto mais crítico for o SEU para o desempenho do sistema, mais restritivo deve ser o requisito. Os requisitos para SEU podem ser definidos então para cada grupo funcional, especificando a máxima probabilidade de ocorrência de SEU permitida de acordo com a categoria.

Para o aspecto de criticalidade, por exemplo, os requisitos de robustez a SEU podem ser derivados do requisito de mais alto nível ligado a confiabilidade e relacionado a pontos de falha simples. O sentido mais amplo destes requisitos é que os sistemas aeroespaciais não devem ter um ponto de falha simples (que para o problema abordado por este trabalho é gerado por um SEU) que leve a uma conseqüência catastrófica, ou seja, a perda do satélite ou aeronave.

Abaixo, temos um exemplo de um requisito de alto nível para SEU, baseado nas discussões dos itens anteriores do presente capítulo. Este poderia ser definido para o projeto de uma aeronave ou espaçonave:

Todo sistema eletrônico embarcado deve ser projetado de modo que:

- *Nenhum SEU isoladamente possa resultar em uma condição de falha catastrófica*
- *Falhas classificadas como catastróficas, causadas pela combinação de falhas causadas por SEE com a falha de medidas de mitigação devem ser extremamente improváveis*
- *As falhas classificadas como perigosas, causadas por SEUs ou pela combinação de falhas causadas por SEE com a falha de medidas de mitigação devem ser extremamente remotas.*

- *As falhas classificadas como maior, causadas por SEUs ou pela combinação de falhas causadas por SEE com a falha de medidas de mitigação devem ser remotas.*

O objetivo do requisito é traduzir os níveis de robustez à ocorrência de SEUs aceitáveis para uma aeronave/espaçonave, de acordo com a criticalidade das funções executadas pelos sistemas eletrônicos. Está traduzida neste requisito a filosofia de que nenhuma falha simples pode causar a perda de uma função critica, ou seja, a perda de uma missão espacial / aeronave. Ainda, os termos “extremamente improváveis”, “extremamente remotas” e “remotas”, podem ser traduzidos em termos de máximas probabilidades aceitáveis de ocorrência de acordo com a criticalidade da função. Por exemplo, no caso aeronáutico para aeronaves categoria transporte, isso se traduziria em máximas probabilidades aceitáveis de respectivamente até 1.10^{-9}, 1.10^{-7} e 1.10^{-5}.

No caso do ambiente de radiações ionizantes durante um evento de um SEPE, foi destacado que é importante garantir as funções mais críticas. O requisito acima seria aplicável em um contexto de um ambiente não perturbado por um SEPE, deste modo seria interessante termos também um requisito dedicado para este caso:

Todo sistema eletrônico embarcado deve ser projetado de modo que no evento de um SEPE:

- *Nenhum SEU isoladamente possa resultar em uma condição de falha catastrófica*
- *Falhas classificadas como catastróficas, causadas pela combinação de falhas causadas por SEE com a falha de medidas de mitigação devem ser extremamente improváveis*

O fator de multiplicação de 25 vezes acima do valor de fluxo para o ambiente normal, definido nas recomendações do presente trabalho, deve ser considerado com cautela, pois mais estudos são necessários para compreender e definir melhor este fenômeno. Ou seja, para que este requisito

possa ser claro e objetivo, é necessário definir uma magnitude padrão ou uma metodologia para estimar um SEPE e assim derivar o espectro de partículas potencialmente causadoras de SEUs.

7. CONCLUSÕES, RECOMENDAÇÕES E SUGESTÕES PARA TRABALHOS FUTUROS

7.1. Conclusões

Este trabalho se propôs a estudar as normas e padrões da indústria espacial e aeronáutica relativos à *Single Event Upsets* causados por radiações ionizantes, a fim de permitir a discussão dos principais aspectos relativos ao impacto do fenômeno no projeto de sistemas embarcados aeroespaciais. Em particular, o objetivo foi elaborar um conjunto de recomendações para possibilitar a garantia de robustez dos sistemas ao fenômeno que sejam adequados à realidade do INPE e do setor aeronáutico nacional.

As normas e recomendações aeroespaciais contém diversos aspectos a serem explorados, e as recomendações propostas pelo presente trabalho são um passo inicial dado em um campo vasto de estudo rumo à evolução das mesmas para um processo de garantia de robustez a SEUs em sistemas eletrônicos embarcados aeroespaciais. Dentro deste contexto, é importante destacar a necessidade da participação de especialistas do INPE e ANAC nos grupos de discussão das normas e recomendações internacionais. Tais fóruns possibilitam o aprofundamento, compreensão e influência sobre os detalhes técnicos das normas e recomendações que são determinantes para o sucesso e segurança de projetos aeroespaciais.

O trabalho explicitou a importância de se considerar o impacto do ambiente de radiações ionizantes e seus efeitos desde as etapas iniciais do desenvolvimento de sistemas aeroespaciais embarcados. O estudo das normas e recomendações do setor espacial e aeronáutico mostrou que o setor espacial tem experiência maior em lidar com o fenômeno, se comparado com o setor aeronáutico. Isto se deve principalmente ao fato do ambiente de radiação ionizante no espaço ser mais severo que o ambiente na atmosfera terrestre, gerando a necessidade de se discutir e estabelecer recomendações para o ambiente diferentes para o setor espacial e aeronáutico, explicitado nos itens 6.2.1 e 6.2.3. Por outro lado, os níveis de confiabilidade exigidos pelas normas

e recomendações do setor aeronáutico são grandes, o que demanda uma ponderação sobre o rigor na tratativa do fenômeno em sistemas aeronáuticos.

Em relação às recomendações propostas, o foco inicial foi abranger os principais aspectos relacionados à garantia de robustez a SEUs no projeto de sistemas embarcados aeroespaciais. Por se tratar de um assunto complexo, abrangente e multidisciplinar, as recomendações foram estabelecidas em um nível elevado e sem entrar em detalhes sobre cada aspecto, porém contendo informações suficientes para que sejam aplicáveis e úteis ao INPE e ao setor aeronáutico. Na discussão do ambiente de radiações ionizantes espacial, foram recomendados que sejam consideradas as fontes de partículas dos cinturões de radiação, galáctica e Solar, moduladas pelo ciclo Solar, além de considerar os eventos extremos de SEPEs. Na discussão do ambiente de radiações ionizantes aeronáutico, foram recomendadas que fossem considerados os nêutrons secundários como principais causadores de SEUs modulados pelo ciclo Solar na máxima altitude e latitude de operação da aeronave, além de considerar os eventos extremos de SEPEs e o efeito dos nêutrons térmicos.

A aplicação das recomendações para o estudo de caso aeronáutico evidenciaram que as taxas de SEUs em componentes devem ser obtidas por testes de acordo com o ambiente de radiações ionizantes e a criticalidade da função executada pelo componente; esta taxa deve ser considerada nas análises de confiabilidade do sistema e, caso estas não atinjam os requisitos de confiabilidade definidos, algum esquema de robustez a falhas induzidas pelos SEUs deve ser implementada. Foi possível notar que as taxas de SEUs devido aos nêutrons térmicos foram comparativamente maiores que as taxas para nêutrons de alta energia, principalmente quando não há dados de testes disponíveis. Por outro lado, a tendência da indústria é de eliminar o uso de boro nos componentes eletrônicos, eliminando ou diminuindo consideravelmente as taxas devido a este fenômeno.

Utilizando um estudo de caso de um sistema aeronáutico embarcado genérico, o trabalho apresentou um exemplo da aplicação das recomendações

propostas, considerando a operação normal, em que o ambiente de radiações ionizantes na atmosfera está correlacionado com o ciclo de atividade Solar previsto para até 2030, e um cenário de um SEPE, onde é esperado um ambiente de radiações ionizantes extremo. Deste modo, foi possível demonstrar a aplicabilidade prática das recomendações e a importância de se considerar previsões de ambiente futuras.

7.2. Sugestões para Trabalhos Futuros

Ao longo do estudo da bibliografia e durante a discussão das recomendações, por várias vezes foi necessário abandonar a discussão de um determinado tema por conta de sua grande extensão e em favor dos objetivos do presente trabalho.

A compreensão e tratamento dos riscos gerados pelas radiações ionizantes em projetos de sistemas eletrônicos embarcados é um campo vasto e em constante evolução, gerando inúmeras possibilidades de temas a serem desenvolvidos por trabalhos futuros. Alguns dos seguintes temas podem ser destacados:

a) Proposta de um processo de garantia de robustez a SEUs causados por radiações ionizantes em sistemas eletrônicos embarcados, estendendo e detalhando os temas abordados por este trabalho.

b) Proposta de recomendações para garantia de robustez de sistemas eletrônicos embarcados a outros fenômenos gerados pelas radiações ionizantes, como por exemplo SEB, TID e DD.

c) Proposta de definição de requisitos para garantia de robustez a SEUs causados por radiações ionizantes em sistemas eletrônicos embarcados.

d) Caracterização do ambiente de radiações ionizantes no espaço e na atmosfera terrestre na região da SAA.

e) Estudo e detalhamento das técnicas de mitigação de SEEs em sistemas eletrônicos embarcados aeroespaciais.

Para o futuro, é esperado que os componentes eletrônicos embarcados aeroespaciais aumentem a susceptibilidade destes às partículas como os nêutrons atmosféricos. Assim, as estratégias de robustez a radiação deverão ser mais robustas e usadas em todas as camadas do projeto de sistemas, desde o software de aplicação e sistema operacional até a arquitetura dos componentes individuais dos circuitos.

REFERÊNCIAS BIBLIOGRÁFICAS

AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL (ANAC). **Procedimentos e normas gerais para a elaboração de regras e emendas aos regulamentos brasileiros da aviação civil.** Brasília, 2009. Emenda nº 00, publicada no diário oficial da união N° 36, de 20/02/2009. Regulamento Brasileiro da Aviação Civil - RBAC 11.

AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL (ANAC). **Certificação de produto aeronáutico**. Brasília, 2011. Emenda nº 01, publicada no diário oficial da união N° 230, de 01/12/2011. Regulamento Brasileiro da Aviação Civil - RBAC 21.

AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL (ANAC). **Requisitos de aeronavegabilidade:** aviões categoria normal, utilidade, acrobática e transporte regional. Brasília, 2013. Emenda nº 61, publicada no diário oficial da união N° 112, de 13/06/2013. Regulamento Brasileiro da Aviação Civil - RBAC 23.

AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL (ANAC). **Procedimentos e normas gerais para a elaboração de regras e emendas aos regulamentos brasileiros da aviação civil**. Brasília, 2013. Emenda nº 134, publicada no diário oficial da união N° 12, de 13/06/2013. Regulamento Brasileiro da Aviação Civil - RBAC 25.

ARRUDA, T. M. **A Influência da radiação em circuitos eletrônicos**. 212f. 2006. Dissertação (Mestrado em Engenharia Aeronáutica e Mecânica e Área de Sistemas Aeroespaciais e Mecatrônica) – Instituto Tecnológico da Aeronáutica, São José dos Campos – SP, 2006.

AUSTRALIAN TRANSPORT SAFETY BUREAU (ATSB) - **Aviation occurrence investigation AO-2008-070 final -** In-flight upset 154 km west of Learmonth, WA 7 October 2008 VH-QPA Airbus A330-303. Canberra, 2011. Commonwealth of Australia.

BARTH, J. L.; DYER, C. S.; STASSINOPOULOS E. G. Space, atmospheric, and terrestrial radiation environments. **IEEE Transactions on Nuclear Science**, v. 50, n. 3, June 2003.

BELCASTRO, C. M.; EURE, K., HESS, R. Testing a flight control system for neutron induced disturbances. **Los Alamos Science**, n. 30, p. 104-111, 2006.

CARLSON, B. Polar routes-past, present and future. **Direct Route**, Fall 2011, v. 6, n. 2, NAV CANADA, Ottawa, ON, 2011.

COOPER, N. G. The invisible neutron threat, **National Security Science**, n. n.1 2012, Los Alamos National Laboratory, Los Alamos, NM, EUA, 2012. <http://www.lanl.gov/science/NSS/issue1_2012/story4full.s html>. Acesso em: 09/11/2012

DYER, C. Radiation effects on spacecraft & aircraft. In: SOLAR CYCLE AND SPACE WEATHER EUROCONFERENCE, 2., 2001, 24 – 29, Vico Equense, Italy. **Proceedings…** Vico Equence, 2001.

EUROPEAN AVIATION SAFETY AGENCY (EASA). **CM-SWCEH-001**. EASA Certification Memorandum - SWCEH – 001, Development Assurance of Airborne Electronic Hardware, Germany, 2011.

EUROPEAN AVIATION SAFETY AGENCY (EASA). **EASA SIB 2012-09**. Safety Information Bulletin 2012-09, Effects of Space Weather on Aviation, France, 2012.

EUROPEAN AVIATION SAFETY AGENCY (EASA). **EASA SIB 2012-10**. Safety Information Bulletin 2012-10, Single Event Effects (SEE) on Aircraft System caused by Cosmic Rays, France, 2012.

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (ECSS). **ECSS-E-ST-10C space engineering –** system engineering general requirements. Noordwijk, The Netherlands, 2009.

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (ECSS). **ECSS-E-ST-10-06 space engineering –** technical requirements specification, Noordwijk. The Netherlands, 2009.

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (ECSS). **ECSS-E-ST-10-04C space engineering** - space environment. Noordwijk, The Netherlands, 2008.

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (ECSS). **ECSS-E-ST-10-12C space engineering -** methods for the calculation of radiation received and its effects, and a policy for design margins. Noordwijk, The Netherlands, 2008.

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (ECSS). **ECSS-E-HB-10-12A space engineering -** calculation of radiation and its effects and margin policy handbook. Noordwijk, The Netherlands, 2010.

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (ECSS). **ECSS-Q-ST-30-02C space product assurance -** failure modes, effects (and criticality) analysis (FMEA/FMECA). Noordwijk, The Netherlands, 2009.

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (ECSS). **ECSS-Q-ST-60-15C space product assurance -** radiation hardness assurance - EEE components. Noordwijk, The Netherlands, 2012.

FEDERAL AVIATION ADMINISTRATION (FAA). **Type certificate data sheets database.** Disponível em: http://rgl.faa.gov/Regulatory_and_Guidance_Library/rgMakeModel.nsf/MainFrame?OpenFrameSet . Acesso em: 10/08/2013.

FEDERAL AVIATION ADMINISTRATION (FAA). Advisory Circular **AC 25.1309:** system design and analysis, ANM-112 - Transport Airplane Directorate, Renton, WA, 1988.

FEDERICO, C. A. **Dosimetria da radiação cósmica no interior de aeronaves no espaço aéreo brasileiro**. 2011. Tese (Doutorado em Tecnologia Nuclear –

Aplicações) - Instituto de Pesquisas Energéticas e Nucleares – IPEN/USP, São Paulo, SP, Brasil, 2011.

GAILLARD, R.; LAUZERAL, O. **Thermal neutron vs. low energy neutrons:** their fundamental differences concerning SER. Grenoble, France: IROC Technologies Technical Note, 2010.

HALLIGAN, R. J. **Requirements quality metrics:** the basis of informed requirements engineering management. In: COMPLEX SYSTEMS ENGINEERING SYNTHESIS AND ASSESSMENT TECHNOLOGY WORKSHOP (CSESAW '93), 1993, Calvados, MD, USA. **Proceedings...** Calvados, 1993.

HARTMANN, G. A. **A anomalia magnética do atlântico sul:** causas e consequências. 153 p. 2005. Dissertação Mestrado em Ciências Geofísicas - Departamento de Geofísica, Instituto de Astronomia, Geofísica e Ciências Atmosféricas, Universidade de São Paulo, São Paulo, SP, Brasil, 2005.

HEIDERGOTT, W. **SEU tolerant device, circuit and processor design**. Scottsdale, AZ, USA: General Dynamics C4 Systems, 2005.

HUBERT, G.; VELAZCO, R.; FEDERICO, C.; CHEMINET, A.; SILVA-CARDENAS, C.; CALDAS, L.V.E.; PANCHER, F.; LACOSTE, V.; PALUMBO, F.; MANSOUR, W.; ARTOLA, L.; PINEDA, F.; DUZELLIER, S. **Continuous high-altitude measurements of cosmic ray neutrons and SEU/MCU at various locations: correlation and analyses based-on MUSCA SEP**., IEEE Transactions on Nuclear Science, v. 60, n. 4, Aug. 2013.

INCEOGLU, F., KNUDSEN, M. F., KAROFF, C., OLSEN, J. Modeling the relationship between neutron counting rates and sunspot numbers using the hysteresis effect. **Solar Physics**, v. 289, n. 4, p.1387-1402, Sept. 2013..

INTER-AGENCY SPACE DEBRIS COORDINATION COMMITTEE (IADC). **Space debris mitigation guidelines**, 2007. (IADC-02-01 Revision 1).

INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC). **IEC 62396-1 -** accommodation of atmospheric radiation effects via single event effects within

avionics electronic equipment. Edition 1.0. 2012-05. Geneva, Switzerland, 2012.

INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC). **IEC 62396-5 –** guidelines for assessing thermal neutron fluxes and effects in avionics systems. Edition 1.0. 2008-08. Geneva, Switzerland, 2008.

INTERNATIONAL COUNCIL ON SYSTEM ENGINEERING (INCOSE). **Systems engineering handbook -** a guide for system life cycle processes and activities version 3. London, UK: INCOSE Systems Engineering Handbook, June 2006.

LABEL, K. A.; GATES, M. M.; MORAN, A. K.; MARSHALL, P. W.; STASSINOPOULOS, E. G.; BARTH, J.; SEIDLECK, C. M.; DALE, C. J. **Commercial microelectronics technologies for applications in the satellite radiation environment.** Greenbelt, MD: NASA Goddard Space Flight Center, EUA, 1996.

LARSON, W. J., WERTZ, J. R. **Space mission analysis and design**3. ed. Space Technology Library, 1999.

KASTENSMIDT, F. G. L. **Designing single event upset mitigation techniques for large SRAM-Based FPGA components.**157 f. 2003. Tese (Doutorado em ciência da Computação) PPGC da UFRGS, Porto Alegre, RS, 2003. Disponível em: http://hdl.handle.net/10183/4181. Acesso em: 02 abr. 2014.

LOUREIRO, G. **Engenharia de sistemas -** aulas 1 e 2 - conceitos básicos. INPE, São José dos Campos, SP, Brasil, 2012.

MAZUR, J. E. An overview of the space radiation environment**. Crosslink Summer**, v. 4, n. 2, p. 10-14, 2003. The Aerospace Corporation, El Segundo, CA, EUA, 2003.

MORO, J. **Absorção ionosférica do ruído cósmico utilizando dados de riômetros da rede SARINET**. 2011. 159 p. (sid.inpe.br/mtc-m19/2011/01.27.18.33-TDI). Dissertação (Mestrado em Geofísica

Espacial/Ciências do Ambiente Solar - Terrestre) - Instituto Nacional de Pesquisas Espaciais, São José dos Campos, 2011. Disponível em: <http://urlib.net/8JMKD3MGP7W/393UJCB>. Acesso em: 02 abr. 2014.

MOIR, I.; SEABRIDGE, A.; **Aircraft systems:** mechanical, electrical and avionics subsystem integration. 3. ed. [S.l]: John Wiley & Sons Ltd, 2008.

MURTAZA, H. Prediction of the space radiation environment of PakSat, a geostationary communication satellite. **Journal of Space Technology**, v. 1, n.. 1, June 2011.

LOVELLETTE, M.N.;Wood, K.S.;Wood, D.L.;Beall, J.H.;Shirvani, P.P.;McCluskey, E.J. **Strategies for fault-tolerant, space-based computing:** lessons learned from the ARGOS testbed. Washington, DC.: Naval Research Lab., 2002.

MURAOKA, I. Development on electronic components for Brazilian satellite program. In: INTERNATIONAL SCHOOL ON THE EFFECTS OF RADIATION ON EMBEDDED SYSTEMS FOR SPACE APPLICATION (SERESSA 2010), 6., 2010, São José dos Campos – SP. **Anais…** São José dos Campos: DCTA.IEAv, 2010.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION REFERENCE PUBLICATION. **NASA RP 1350 the natural space environment:** effects in spacecraft. Alabama, EUA: Marshall Space Flight Center - MSFC, 1994.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION REFERENCE PUBLICATION. **NASA RP 1390 spacecraft system failures and anomalies attributed to the natural space environment**. Alabama, EUA: Marshall Space Flight Center - MSFC, 1996.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION. **431-REF-000273 -** single event effect criticality analysis. Maryland, EUA: Goddard Space Flight Center – GSFC, 1996.

NATIONAL RESEARCH COUNCIL. **Severe space weather events -** understanding societal and economic impacts workshop report, Washington, DC: The National Academies Press, 2008.

NICHITIU, F.; DRUMMOND, J. R.; ZOU, J.; DESCHAMBAULT, R. Solar Particle Events Seen by the MOPITT Instrument. **Journal of Atmospheric and Solar-Terrestrial Physics**, v. 66, p. 1797–1803, 2004. Elsevier Ltd, The Netherlands.

NICOLAIDIS, M. **Soft errors in modern electronic systems** . New York: Springer Science and Business Media, LLC 2011. ISBN 978-1-4419-6992-7.

NORMAND, E.; TABER, A. H. **Investigation and characterization of SEU effects and hardening strategies in avionics**. Alexandria, VA: Defense Nuclear Agency, 1995.

RELIASOFT, INC, **System analysis reference:** reliabiliy, availability and optimization. Tucson, EUA: Reliasoft Inc., 2012. Disponível em http://reliawiki.com/index.php/System_Analysis_Reference

RTCA INC. **DO-160G environmental conditions and test procedures for airborne equipment**. Washington, D.C., EUA, 2010.

RTCA INC. **DO-178C software considerations in airborne systems and equipment certification**. Washington, D.C., EUA, 2011.

RTCA INC. **DO-254 design assurance guidance for airborne electronic hardware**. Washington, D.C., EUA, 2000.

SAE INTERNATIONAL. **SAE ARP 4754 Rev. A -** Guidelines for development of civil aircraft and systems. Warrendale, PA, EUA, 2010. Aerospace Recommended Practice.

SAE INTERNATIONAL. **SAE ARP 4761 -** guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment. Warrendale, PA, EUA, 1996. Aerospace Recommended Practice.

SATO, T **EXPACS:** excel-based program for calculating atmospheric cosmic-ray spectrum user's manual. Tokai, Japan: Japan Atomic Energy Agency, 2010.

SOUZA, M. L. O.; CARVALHO, T. R. **The fault avoidance and the fault tolerance approaches for increasing the reliability of aerospace and automotive systems.** São Paulo: SAE, 2005. SAE Technical Paper 2005-01-4157. doi: 10.4271/2005-01-4157.

SUGGS, R. J. **Future solar activity estimates for use in prediction of space environmental effects on spacecraft orbital lifetime and performance**. Huntsville, AL, EUA: NASA George C. Marshall Space Flight Center, Nov. 2013

TELELOGIC DOORS® Manual **Get it right the first time:** writing better requirements. New York, NY, EUA: IBM® Corporation, 2008.