AUTARQUIA ASSOCIADA À UNIVERSIDADE
DE SÃO PAULO

UM ESTUDO DE ARQUITETURAS DE HARDWARE PARA APLICAÇÃO EM SISTEMAS DIGITAIS DE PROTEÇÃO DE REATORES NUCLEARES - MÉTODOS DE ANÁLISE DE CONFIABILIDADE E SEGURANÇA

PEDRO LUIZ BENKO

Dissertação apresentada como parte dos requisitos para obtenção do Grau de Mestre em Ciências na Área de Reatores Nucleares de Potência e Tecnologia do Combustível Nuclear.

Orientador:
Dr. José Messias de Oliveira Neto

São Paulo

1997

INSTITUTO DE PESQUISAS ENERGÉTICAS E NUCLEARES

Autarquia associada à Universidade de São Paulo

"UM ESTUDO DE ARQUITETURAS DE HARDWARE PARA APLICAÇÃO EM SISTEMAS DIGITAIS DE PROTEÇÃO DE REATORES NUCLEARES - MÉTODOS DE ANALISE DE CONFIABILIDADE E SEGURANÇA"

PEDRO LUIZ BENKO

Dissertação apresentada como parte dos requisitos para obtenção do grau de Mestre em Ciências na Área de Reatores Nucleares de Potência e Tecnologia do Combustível Nuclear.

Orientador:

Dr. José Messias de Oliveira Neto

São Paulo

1997

"A criação do novo não é conquista do intelecto, mas do instinto de prazer agindo por uma necessidade interior. A mente criativa brinca com os objetos que ama"

Carl Gustav Jung.

Dedico este trabalho à Telma, minha mulher e companheira, pelo incentivo, compreensão, auxílio na revisão de textos e apoio demonstrado.

AGRADECIMENTOS

Ao meu Orientador, Prof. Dr. José Messias de Oliveira Neto, pela paciência, apoio e trabalho dedicado nas pesquisas, revisões e elaboração desta Dissertação.

Ao Prof. Dr. Benício José de Sousa, EPUSP-USP, pela grande ajuda na definição dos modelos e ferramentas de análise.

Ao amigo Prof. MSc. Renato Camargo Giacomini, pelas sugestões e valiosas discussões na fase de definição dos modelos.

Ao CF(EN) José Carlos Pires Ferreira, pelo incentivo e auxílio que tem dedicado a programas de Pós graduação, sem o que não seria possível a execução deste trabalho.

Aos Amigos que colaboraram com este trabalho de forma direta:

MSc Vadim Surkov

MSc Claude Emile Sthroll

Dr. Flávio Matsuyama

Ao Centro Tecnológico da Marinha em São Paulo (CTMSP), pelo apoio que recebi na realização deste trabalho.

"UM ESTUDO DE ARQUITETURAS DE HARDWARE PARA APLICAÇÃO EM SISTEMAS DIGITAIS DE PROTEÇÃO DE REATORES NUCLEARES - MÉTODOS DE ANALISE DE CONFIABILIDADE E SEGURANÇA"

Pedro Luiz Benko

Resumo

Um estudo de arquiteturas de *"hardware"* de sistemas digitais de proteção de reatores nucleares, é apresentado. Técnicas e topologias de circuitos componentes de sistemas digitais para aplicações críticas são sugeridas. Propõe-se um método para desenvolvimento de Sistemas de Proteção Digitais tendo como base índices extraídos dos requisitos de Confiabilidade e Segurança da planta. Apresenta-se diretrizes para avaliação desses dois fatores que são preponderantes na definição de arquiteturas para proteção e controle de plantas nucleares. São sugeridas técnicas e ferramentas para avaliação e modelagem de confiabilidade e segurança de arquiteturas de *"hardware"* digitais. Aplica-se modelagem por cadeias de Markov para avaliação da confiabilidade de arquiteturas redundantes. Para avaliação da qualidade do *"software"* sugere-se mecanismos de controle de projeto, especificação e procedimentos de verificação e validação (V&V). Uma arquitetura consagrada de sistema de proteção digital para reator nuclear é analisada como estudo de caso.

"A STUDY OF DIGITAL HARDWARE ARCHITECTURES FOR NUCLEAR REACTORS PROTECTION SYSTEMS APPLICATIONS - RELIABILITY AND SAFETY ANALYSIS METHODS."

Pedro Luiz Benko

Abstract

A study of digital hardware architectures, including experience in many countries, topologies and solutions to interface circuits for protection systems of nuclear reactors is presented. Methods for developing digital systems architectures based on fault tolerant and safety requirements is proposed. Directives for assessing such conditions are suggested. Techniques and the most common tools employed in reliability, safety evaluation and modeling of hardware architectures is also presented. Markov chain modeling is used to evaluate the reliability of redundant architectures. In order to estimate software quality, several mechanisms to be used in design, specification, and validation and verification (V&V) procedures are suggested. A digital protection system architecture has been analyzed as a case study.

Sumário

Índice de Figuras

1. INTRODUÇÃO.

1.1 Sistemas eletrônicos com requisitos críticos de segurança - uma visão geral

Os sistemas eletrônicos com requisitos críticos com relação a segurança, são sistemas que devem ser projetados segundo a ótica de equipamentos tipo falha segura. Portanto, devem ter todos os estados operativos e de falhas conhecidos e analisados, de modo que, a ocorrência de um ou mais desses estados não resulte em grande perda material e ou conseqüências indesejáveis para o homem e ao meio ambiente. O conceito de segurança está basicamente vinculado ao cumprimento desses objetivos, sobre os quais todo projeto deve ser conduzido.

Os requisitos variam de aplicação para aplicação, assim, cada sistema eletrônico com restrições de segurança, atende a determinados requisitos que são metas de projeto a serem cumpridas. É importante salientar que um sistema eletrônico crítico mantém a sua característica de segurança dentro do universo de sua aplicação. É incorreto adaptar sistemas críticos para outras aplicações sem uma análise adequada. Os requisitos críticos de um sistema de segurança são oriundos de uma determinada necessidade operativa da aplicação.

Podemos de uma forma macro, exemplificar : o requisito básico de segurança do sistema de proteção de um trem é parar em caso de falhas internas de seus componentes e ou de falhas operativas que violem o seu requisito principal; o de uma aeronave é manter-se voando sob quaisquer condições operativas e ou sob falha; o de uma planta nuclear é proteger o sistema no caso de falhas ou erros de operação desligando-se o reator. Cada subsistema componente do sistema global da aplicação deve ter requisitos próprios de modo a não violar o requisito principal.

1.2 Objetivo do trabalho

Este trabalho tem como escopo apresentar os resultados de um estudo de arquiteturas de *"hardware"* digitais, visando sua aplicação em plantas nucleares, por isto apresentará:

- Enfoque comparativo do problema entre sistemas convencionais e digitais com relação ao licenciamento;

- resultados sobre pesquisa da situação mundial no que se refere ao uso de sistemas digitais computadorizados aplicados em proteção de plantas nucleares;

- uma síntese e comentários de alternativas de arquiteturas aplicadas para este fim;

- soluções de topologias de circuitos eletrônicos para interfaces entre sistemas digitais e sensores e atuadores na planta controlada;

- proposta de método para análise de confiabilidade e segurança da arquitetura de sistema eletrônico digital com requisitos críticos de segurança apresentando as principais ferramentas de análise e diretrizes para desenvolvimento de um sistema para esta finalidade; e

- um estudo de caso de uma arquitetura de sistema de proteção consagrada, utilizada atualmente em plantas nucleares francesas, análise da arquitetura e discussão de resultados e incertezas.

O presente trabalho terá como objetivo principal o *"hardware"*, mas como em sistemas digitais o *"software"* é parte integrante, este será objeto de uma abordagem superficial.

1.3 Sistemas com requisitos críticos convencionais versus digitais.

Sistemas eletrônicos convencionais são baseados em técnicas de topologias de circuitos eletrônicos "*fail safe*", combinadas com intertravamentos baseados em relés

eletromecânicos que possuem modos de falhas conhecidos e estado permanente e definido em caso de falha (desligado). Estes sistemas operam em dezenas de aplicações em todo o mundo e embora a tecnologia de computadores seja a vanguarda, a substituição de sistemas convencionais por sistemas informatizados encontra grande resistência para aplicações críticas.

Verifica-se que a tecnologia de computadores pode superar facilmente algumas deficiências dos sistemas tradicionais, mas introduz novas incertezas. O problema principal associado à certificação de sistemas digitais está na avaliação de qualidade do *"software"*. Segundo [1] "*Enquanto a quantificação da qualidade do software para grandes sistemas não puder ser feita de maneira probabilística, a qualidade de produção, verificação e validação independente e testes dinâmicos são uma alternativa qualitativa para demonstrar que o objetivo foi atingido*". Atualmente é a alternativa adotada por todos os projetistas de sistemas digitais.

Os *"softwares"* para sistemas de proteção são: complexos, de grande porte, podem conter erros, e sua qualidade ainda não pode ser demonstrada por considerações probabilísticas. Para a utilização de todo o potencial de sistemas digitais, é necessário um *"software"* sem erros. A obtenção de tal meta compreende o projeto de um *"software"* segundo uma metodologia denominada "ciclo de vida do *"software"* a qual pode ser desenvolvida de várias formas (*"waterfalls, spiral models e phased models" etc)*. Entende-se como ciclo de vida do *"software"*, todo o conjunto de especificações, metodologias de análise e projeto, codificação, técnicas de verificação e validação, testes e operação. O objetivo é comprovar que a especificação é adequada e que o *"software"* desenvolvido atende essa especificação [27].

A complexidade na utilização de sistemas digitais pode ser ilustrada por um exemplo de controle de semáforos, fig.1 e fig.2. Observa-se em uma escala menor, os problemas que envolvem o desenvolvimento e comprovação da credibilidade operacional - em termos de segurança de um sistema digital - quando confrontado com um sistema analógico.

O exemplo apresentado tem cunho ilustrativo e não pretende detalhar com precisão os circuitos operacionais de um semáforo. Portanto, certos tipos de falhas críticas não foram consideradas nos esquemas apresentados.

A fig. 1 apresenta um semáforo convencional e detalha-se a sua operação. A fig. 2 representa um semáforo digital com todas as vantagens operacionais que o mesmo pode oferecer e também as suas limitações quanto à comprovação de operação segura.

Na análise dos requisitos para um semáforo, a condição de restrição de segurança é logicamente a sinalização "verde". Ou seja as indicações "vermelho" e "amarelo" significam parada e atenção, condições que não afetam a segurança, apenas a operacionalidade, mas o "verde" não pode ser acionado simultaneamente em ambos os sentidos pois o resultado seria um acidente. Portanto o requisito de segurança no caso do semáforo é: "*Não acionamento simultâneo dos sinaleiros verdes*". Este requisito deve ser claro e preciso por definição.

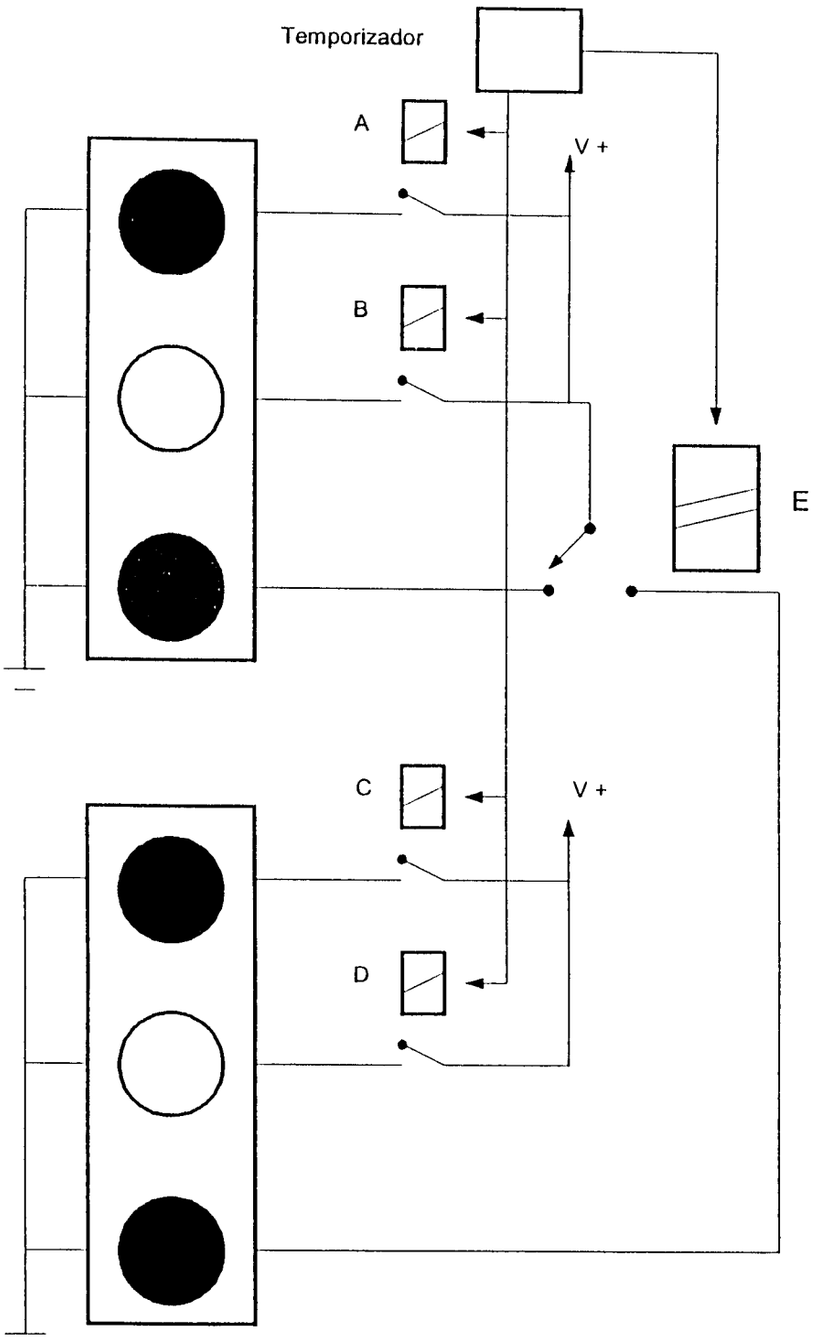


Fig. 1 - Semáforo analógico tradicional.

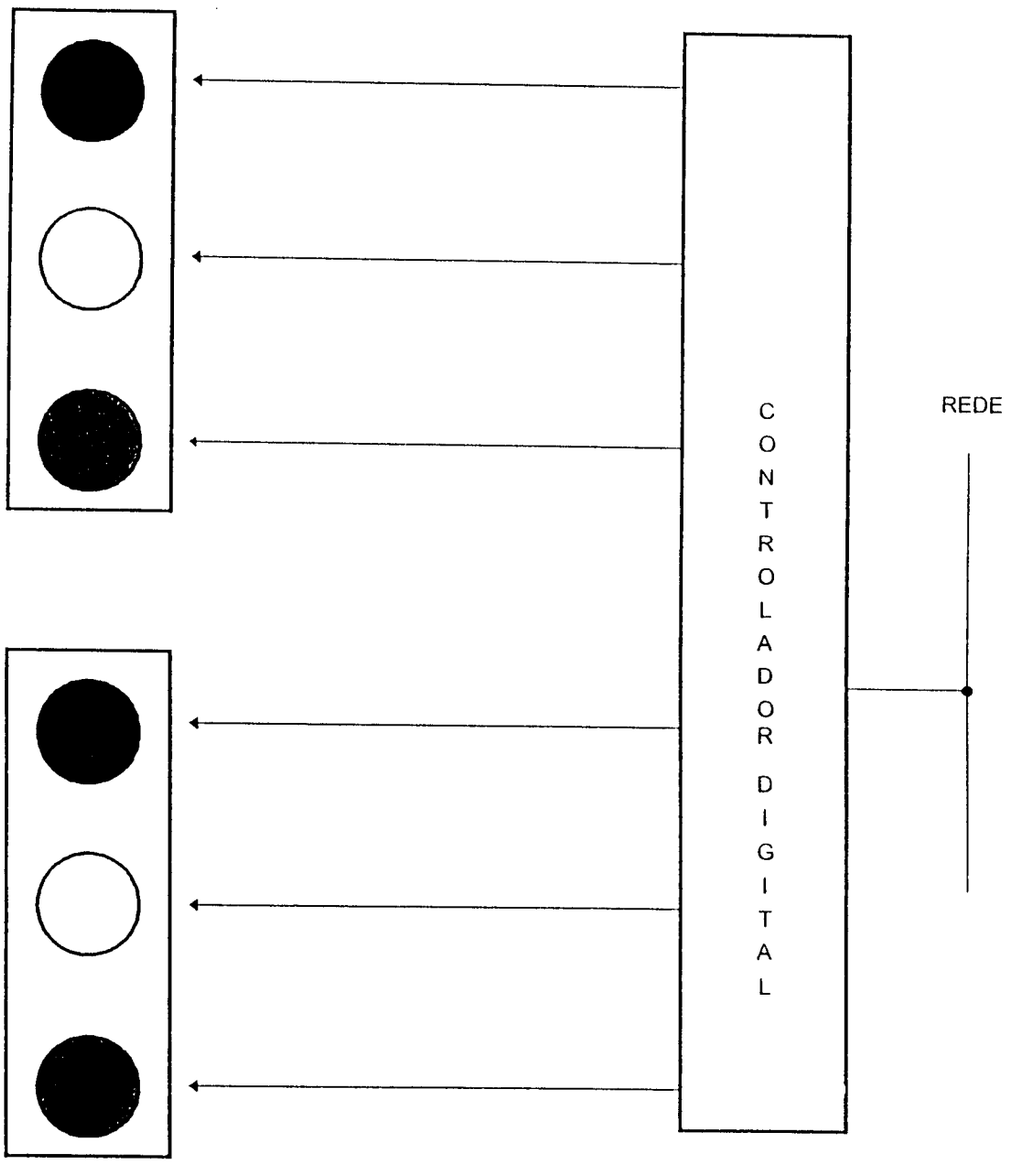


Fig. 2 - Semáforo computadorizado.

Tradicional.

Na fig. 1, os relés "A, B C, D e E" acionam determinados sinaleiros comandados por um temporizador. O relé "E", um equipamento robusto, pode garantir o não acionamento simultâneo do verde, isto é, a haste que aciona o verde de um sinaleiro não pode acionar o outro conjuntamente por restrição mecânica. Neste caso, o cumprimento do requisito é demonstrado por construção e é facilmente visualizado.

Digital computadorizado

Na fig. 2, um controlador setorial inteligente computadorizado exerce o controle do semáforo e possui inúmeras vantagens operacionais em relação ao controlador tradicional. Por exemplo:

- comunica-se com uma central enviando informações sobre o estado das lâmpadas;
- pode variar o tempo de abertura dos sinaleiros de acordo com a demanda de tráfego;
- executa autodiagnósticos e informa a central; e
- não utiliza um relé especial para acionamento dos sinaleiros verdes, utilizando acionamento independente para cada luz verde com sinal dinâmico via transformador com bobinas fisicamente separadas entre primário e secundário, isso garante o não acionamento por falha do tipo curto-circuito (técnica de interface "*fail safe*").

Para o atendimento do requisito de segurança, é necessário que o controlador digital "*não acione simultaneamente as duas saídas dos sinaleiros verdes*", a qual é a condição de falha crítica. Este requisito deve ser garantido pela arquitetura de "*hardware*" empregada e "*software*" desenvolvido para esta aplicação. Neste ponto, estabelece-se a polêmica do uso de computadores em sistemas de segurança, onde as assertivas, visibilidade e confiança, não apresentam as evidências necessárias:

- Visibilidade - o cumprimento do requisito não é facilmente visível ou comprovado.

- Confiança - o parâmetro grau de confiança deve ser demonstrado sem as ferramentas probabilísticas tradicionais, sendo que análises de modo de falhas de componentes e seus efeitos (FMEA), em sua totalidade não satisfazem, pois estas ferramentas não permitem avaliar a qualidade do *"software"* [1].

As técnicas atuais, empregadas para solução do problema, baseadas em verificação e validação de projeto de *"software"*, arquiteturas redundantes, etc, esbarram nessas incertezas e por isso na resistência ao uso, resultando em um processo de qualificação demorado e exaustivo.

Digital computadorizado + tradicional.

Adota-se em muitas aplicações, uma solução híbrida, no caso do semáforo usado como exemplo, as funções operacionais ficariam com o controlador digital o qual seria associado ao relé "E", para garantia da segurança. Portanto teríamos um sistema de controle digital associado a um sistema de proteção convencional.

2. EXPERIÊNCIA MUNDIAL NO USO DE SISTEMAS DIGITAIS EM PLANTAS NUCLEARES.

Sistemas digitais apresentam vantagens na implementação de funções complexas de controle, proteção e monitoração, sendo rápidos e precisos no seu processamento. A operação desses sistemas não está sujeita aos problemas encontrados nos sistemas analógicos, como por exemplo: *"drift"* de temperatura dos componentes e calibrações. Minimiza-se os períodos de tempo de manutenção e com isso reduz-se a incidência de erro humano.

No aspecto compactação, os equipamentos digitais em geral reduzem o número de cabos e o tamanho físico dos equipamentos. O aspecto mais atraente, entretanto, é o de compatibilidade com equipamentos padronizados, permitindo uma operacionalidade conjunta uma vez que podem ser configurados para executarem diferentes funções, utilizando-se *"softwares"* distintos. Dessa forma, padronizam-se barramentos e módulos eletrônicos (barramento VME é um exemplo).

Sistemas de proteção para Reatores (RPS), baseados em computadores, possuem muito de sua complexidade residente no *"software"* para o qual uma visão filosófica aponta que: *Software não falha, ele não atende uma especificação, ou a especificação é inadequada* [1]. Convém lembrar que qualquer falha em uma versão de *"software"* utilizada para proteção em arquitetura de *"hardware"* com canais redundantes, atinge todos os canais e tem potencial para falha simultânea de proteção. Aspectos funcionais ou mesmo equipamentos diferentes são recomendados de maneira a se procurar evitar falhas de modo comum. O uso de arquiteturas redundantes, com vários níveis de profundidade, visa atender aos requisitos de segurança (no caso também de confiabilidade) e procura resolver através de topologias de circuitos votadores, falhas tanto do *"software"* quanto do *"hardware"* que contrariem estes requisitos.

2.1 Situação mundial, quanto a Plantas Digitais.

A aplicação de sistemas computadorizados para aplicações críticas tem influenciado o programa nuclear em vários países. Existem variações devido a cultura, geografia e

aspectos industriais, mas há algumas similaridades na abordagem dessas questões. Os países responsáveis e atuantes no meio são:

•França.

Há muito tempo que a França vem desenvolvendo sistemas de proteção para reatores baseados em arquiteturas digitais microprocessadas. Em 20 unidades, série 1300 MWe a lógica convencional de relés eletromagnéticos utilizados para proteção, ações de segurança e sistemas de controle da planta, foram substituídos por sistemas microprocessados classe 1E, implementados pela CEGELEC (Controbloc), enquanto que o SPIN, desenvolvido pela *Merlin-Gerin,* garante e monitora as funções de segurança do reator.

Seguindo este conceito, teve início em 1984 um novo desenvolvimento de um sistema de controle Controbloc, junto com um sistema de proteção SPIN2 para as unidades de 1450MWe. Este novo sistema é baseado na utilização de técnicas programadas e sua sala de controle é totalmente computadorizada. A partir de dezembro de 1990 tornou-se aparente que tal desenvolvimento acarretaria anos de atrasos na sua conclusão e licenciamento das novas plantas, assim a EDF optou por substituir parte do sistema Controbloc pelo Hartmann and Braun Contronic E convencional.

•Japão

A primeira aplicação de controle digital na industria nuclear japonesa, é a usina *Kashiwazaki Kariwa* 2 5 *radwaste plant,* que entrou em operação comercial em 1990. Desde então, as aplicações que não envolvem segurança são executadas por sistemas digitais que vem evoluindo gradativamente. Atualmente a indústria Japonesa trabalha em um sistema de controle digital para reator do tipo ABWR (*Advanced Boiling Water Reactor) Kashiwazaki Kariwa 6/7,* englobando funções de segurança e controle. Essas funções serão realizadas por microprocessadores em substituição a relés eletromagnéticos e instrumentação analógica tradicional. O projeto obteve sua permissão de desenvolvimento em 1992 e possui perspectiva de entrada em operação em 1997. Neste sistema os dados

serão transmitidos via fibra ótica multiplexada utilizando-se uma lógica 2/4 e um sistema automático para diagnóstico de falhas.

•Estados Unidos

Nos Estados Unidos existe grande experiência no uso de sistema digitais para aplicações industriais, mas muito pouco uso em plantas nucleares, devido principalmente a estagnação em novos desenvolvimentos na área. Os EUA limitam-se a realizar modernizações em usinas em operação, utilizando controle digital microprocessado em partes dos seus sistemas analógicos convencionais. Isso é realizado devido ao problema de reposição dessas partes em sistemas antigos.

A NRC (*Nuclear Regulatory Commission*) [27], vem trabalhando no sentido de regulamentar o processo de certificação de sistemas digitais. Em particular sugere que, os aspectos de avaliação de falhas em modo comum, devido a erros de projeto do *"software"*, devem ser analisados. Trabalhos de pesquisas ainda continuam com o objetivo de desenvolver técnicas de avaliação de qualidade do *"software"*, visto que de fato não há ainda bases documentais certificadas para garantia dessa qualidade.

•Reino Unido.

No Reino Unido, a tecnologia digital vem sendo aplicada na indústria convencional, aeroespacial, militar e nuclear. No final da década de 1970, as especificações para a planta nuclear PWR (*Pressure Water Reactor) Sizewell B* [15] apontaram as vantagens de que um sistema digital traria para o seu sistema de controle e proteção. Devido ao estado da arte com relação a qualidade do *"software"*, isto não foi utilizado. O reator *Sizewell B*, portanto, está servindo como bancada de desenvolvimento da nova tecnologia emergente. Decidiu-se em 1992, após várias análises e trabalhos no campo de sistemas de proteção digitais, por dois sistemas de proteção: o PPS *(primary protection system)* usando tecnologia digital com meios para desligar o reator e iniciar o procedimento de emergência de ações de segurança, e o SSP (*secondary protection system*), concebido com circuitos tradicionais, que constitui no segundo nível de proteção da planta.

•Canadá

Desde o inicio da década de 1980, o Canadá vem utilizando sistemas digitais programados no reator CANDU 600 [7], para implementação das decisões de desligamento sem qualquer ocorrência de falhas não seguras. A tecnologia desenvolvida pela Ontario Hydro's para a Darlington Nuclear Generating Station, consiste de dois sistemas independentes de desligamento (*shut-down),* SDS1 e SDS2. Cada reator emprega 15 computadores, 7 para o SDS1, 7 para o SDS2 e 1 para monitoração que é compartilhado com outros reatores. O *"software"* para o desligamento do reator é armazenado em EPROMs (*erasable programmable read only memories)* e o *"software"* para monitoração em disco rígido.

O licenciamento junto a AECB *(Atomic Energy Control Board)* resultou em um considerável atraso, em razão da necessidade de critérios mais rígidos de verificação de requisitos. Os requisitos levam em consideração a verificação formal de código, formatação das funções matemáticas de *"software"* e testes de validação. Apesar dos resultados favoráveis a AECB decidiu que o sistema da Ontário Hydro deve ser reprojetado.

A experiência adquirida tem sido utilizada em padrões de documentação de *"software"* e distintamente de outros países, eles estão dispostos a abrir informações que normalmente não são divulgadas por outros países e a revelar suas falhas, sucessos e as lições aprendidas.

•Republica do Cazaquistão

A CEZ (*Ceske Energetick Zavody*), optou por continuar com o projeto Russo de reatores do tipo VVER, mas com uma modernização no sistema de instrumentação, controle e proteção.

Para a usina de Temelin [23], o sistema a ser fornecido pela Westinghouse, tem a arquitetura similar ao AP600, empregado em *Sizewell* B. Este incluirá sistemas de proteção, controle e monitoração do reator e sistemas da planta com informações de pós

acidente e alarmes. A proteção do reator, controle redundante da planta e sistemas de limitação, são implementados utilizando o *"Eagle family" de "hardware"*. Existem dois sistemas de proteção utilizando o mesmo *"hardware"* mas diferentes *"softwares"*. As autoridades de licenciamento do Cazaquistão terão a tarefa de licenciar a planta, mas em particular, estabelecer o requisito de grau de diversidade e métodos de validação de *"software* para o sistema de proteção,".

2.2 Dificuldades e resistências ao "Up date" dos sistemas de proteção e controle existentes.

Sistemas de proteção e controle de plantas nucleares são projetados para uma operação em torno de 20 anos em média, sendo que um dos fatores que contribui para uma atualização desses sistemas em um prazo menor é a obsolescência de componentes eletrônicos, dificultando a reposição. Como o trabalho de atualização é complexo por exigir um novo processo de certificação de segurança, é comum encontrar-se plantas nucleares operando com tecnologia ultrapassada.

Aproximadamente 80% das plantas nucleares nos Estados Unidos [2], estão operando com *"hardware"* que não mais possuem suporte do fornecedor e em muitos casos a velha tecnologia de *"hardware"* opera com componentes de 20 ou 30 anos de idade. Enquanto o desempenho dos módulos permanece bom, devido a manutenção apropriada, seus componentes aproximam-se do final de sua vida útil, e a tendência será o aumento da taxa de falhas nos equipamentos até que não seja mais possível o reparo. Com a degradação da estabilidade, atinge-se o ponto onde serão necessárias mudanças nos sistemas de segurança e, logicamente, adequá-los à nova realidade de licenciamento.

3. ARQUITETURAS DE SISTEMAS DE CONTROLE E PROTEÇÃO DE PLANTAS NUCLEARES.

3.1 Aspectos de Confiabilidade e segurança com redundância.

Dois fatores são preponderantes no uso de arquiteturas para proteção e controle de plantas nucleares: alta confiabilidade e segurança. O fator alta confiabilidade implica em alta disponibilidade operacional, que é alcançada com uso de sistemas tolerantes a falhas. Isso é alcançado com diagnósticos e reposição de partes com o sistema funcionando, tendo como objetivo a operação ininterrupta da planta. O fator segurança implica em que o sistema de controle e o sistema de proteção, devam garantir a operação segura, com risco aceitável, em qualquer condição operacional.

Em sistemas simplex, técnicas de detecção de falhas e circuitos intrinsecamente *"fail safe"*, garantem a operação segura de uma instalação, mas não incorporam tolerância a falhas. O uso de arquiteturas com duplicação "OU" aumentam a disponibilidade dos sistemas digitais, mas degradam os sistemas em termos de segurança, pois perde-se as características de comparação entre os canais redundantes.

De fato, a duplicação com comparação de saídas foi considerada uma técnica de detecção de falhas onde a segurança do sistema é aumentada em detrimento de sua disponibilidade. Alguns sistemas de proteção e controle empregam arquiteturas híbridas onde temos dois sistemas operando em *"hot e cold stand-by"*, e cada um deles possui subsistemas de proteção duplicados operando em "*And*" lógico e subsistema de controle em arquitetura simplex. O sistema ATC (*automatic train control*) de bordo dos trens metropolitanos da Companhia do Metropolitano de São Paulo (CMSP) é um exemplo dessa arquitetura.

3.2 Redundância TMR e NMR.

Se uma terceira cópia do canal funcional é adicionada, a informação redundante será disponível em três canais. A falha de um deles pode ser detectada por votação majoritária entre os resultados de saída (votação 2 em 3). O trabalho de base do TMR

(triple modular redundancy), foi proposto pela primeira vez em 1956, por von Neumann, conforme relata Siewiorek & Swarz [26]. Ele propôs uma configuração empregando cópias independentes de um sinal com restauração de integridade baseado em operações lógicas.

Este conceito foi estendido para incluir N copias de canais funcionais com votação majoritária de suas saídas. Esta técnica é chamada de *"N-modular redundancy"* ou NMR. Normalmente N é impar para evitar-se um empate na votação. O custo de NMR normalmente para o *"hardware"* é N vezes o custo do sistema simplex, adicionado ao custo dos votadores.

O atraso causado por votadores, devido a propagação de sinais, é fator limitante no desempenho de arquiteturas redundantes, dado que a ausência de sincronismo é necessária para caracterizar a independência dos canais redundantes.

Existem casos onde a votação par é aplicada a sistemas de proteção nuclear. Nesta situação utiliza-se técnicas de testes e verificações periódicas em um canal do sistema, enquanto os outros operam em votação impar. O sistema de proteção SPIN é um exemplo de arquitetura com votação par.

As topologias TMR, podem ser agrupadas em três configurações principais:

- Configuração básica simples, fig 3.
- Configuração cascata de módulos TMR, fig 4.
- Configuração com votadores triplicados para cascata de módulos TMR ,fig 5.

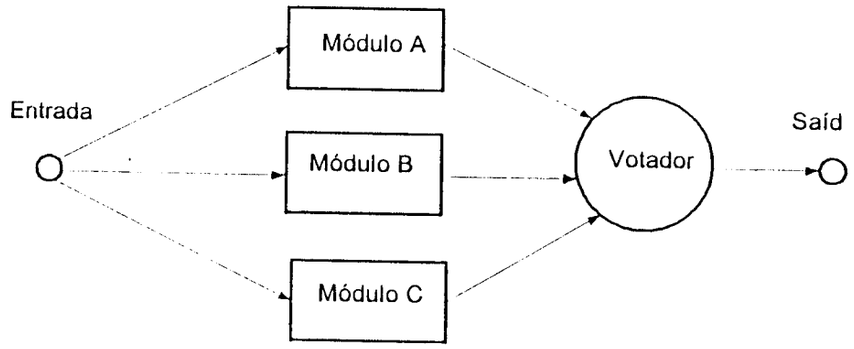


Fig. 3 - Configuração básica do TMR.

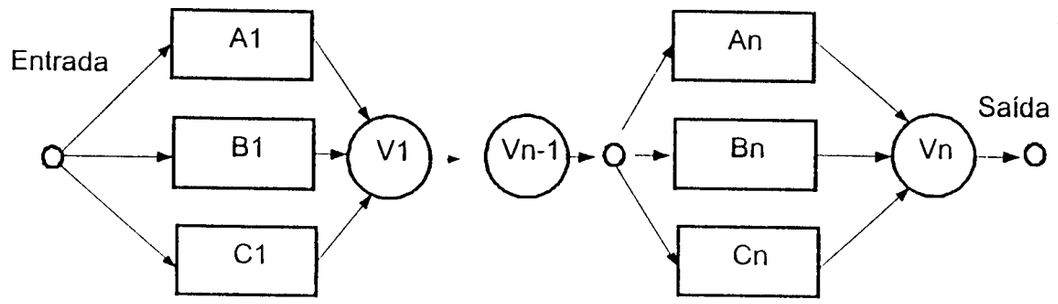


Fig. 4 - Módulos TMR em cascata

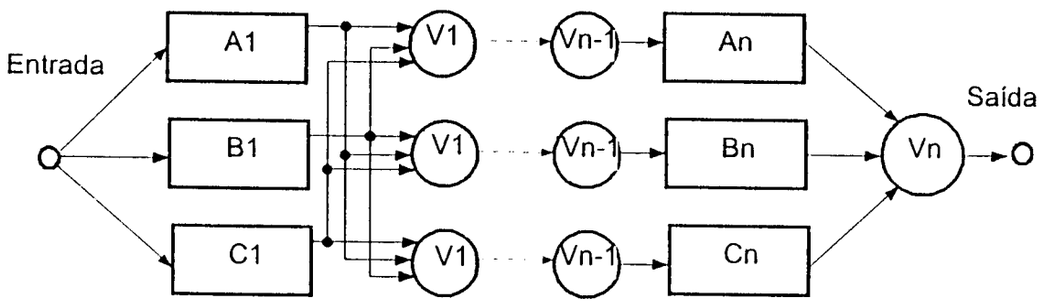


Fig. 5 - Votadores triplicados com módulos TMR em cascata

3.3 Arquiteturas aplicadas em sistemas de proteção para reatores nucleares, exemplos.

3.3.1 Arquitetura TMR

Arquiteturas do tipo TMR são comuns para aplicações em sistemas de proteção [3]. A fig 6 mostra uma configuração básica de sistema de controle TMR, onde três processadores são conectados às mesmas entradas e executam o mesmo aplicativo em *"software"*. Os resultados obtidos são comparados constantemente, através de votadores que podem ser implementados por *"hardware"* ou *"software"* e que normalmente votam maioria entre 2/3. Seu projeto é do tipo falha segura para as condições de restrição. Sistemas TMR assíncronos geralmente votam em *"software"* tolerante a falhas, e operam de modo a aguardar que todos os processadores tenham informações válidas antes de iniciar o processo de votação.

Os estados operativos normalmente se resumem em 3-2-0, onde por votação são detectadas falhas simples, para operação *"fail-safe"*. O estado "0" significa o desligamento (*shut-down*) do sistema. Estados operativos do tipo "3-2-1-0", são empregados em sistemas onde não existem requisitos de segurança, apenas os de confiabilidade e disponibilidade. Admite-se a operação de um processador apenas, com outros dois falhos. Devem existir diagnósticos de suas saídas tanto para os estados 3-2-0 como para os 3-2-1-0, e o projeto deve considerar que cada módulo processador possa ser substituído sem a necessidade de interrupção de operação (*replace in hot*).

A partir da aquisição dos sinais de campo, verifica-se dois níveis de votação 3/2, sendo que o primeiro é realizado no mesmo processador com a aquisição de sinais triplicada visando a sua integridade. O segundo, é relativo aos sinais dos três processadores e é realizado nos atuadores, para a integridade de atuação. O processo de aquisição de sinais é realizado por duas redes triplicadas, uma para sinais digitais e outra para sinais analógicos, sendo que ambas podem ser implementadas por fibra ótica ou cabos coaxiais.

A arquitetura apresentada utiliza módulos de entrada, tanto analógicos como digitais, com saídas triplicadas, sendo uma para cada processador, fig. 7, e possui características de substituição sem interromper a operação. Os módulos são distribuídos na

planta e, sendo similares, permitem fácil manutenção. Essa arquitetura consente que a aquisição de sinais críticos seja efetuada com redundância em módulos distintos. Não há limite para o número de redundâncias, o que permite o ajuste do sistema para o grau de confiança desejado.

Cada módulo de saída, fig 8, receberá sinais dos três processadores e executará a multiplexação. Assume-se que a votação também seja realizada pelos módulos. A saída votada em 2/3 acionará o atuador correspondente. Um ponto frágil desse sistema, são que falhas nos blocos transceptores podem deixar inoperante parte deste, apesar da redundância. Isso pode causar falha de sistema se não houver redundância em módulos de saída. A cobertura abrange falhas em um processador, sendo que a operação não será prejudicada se for diagnosticada e reparada a tempo.

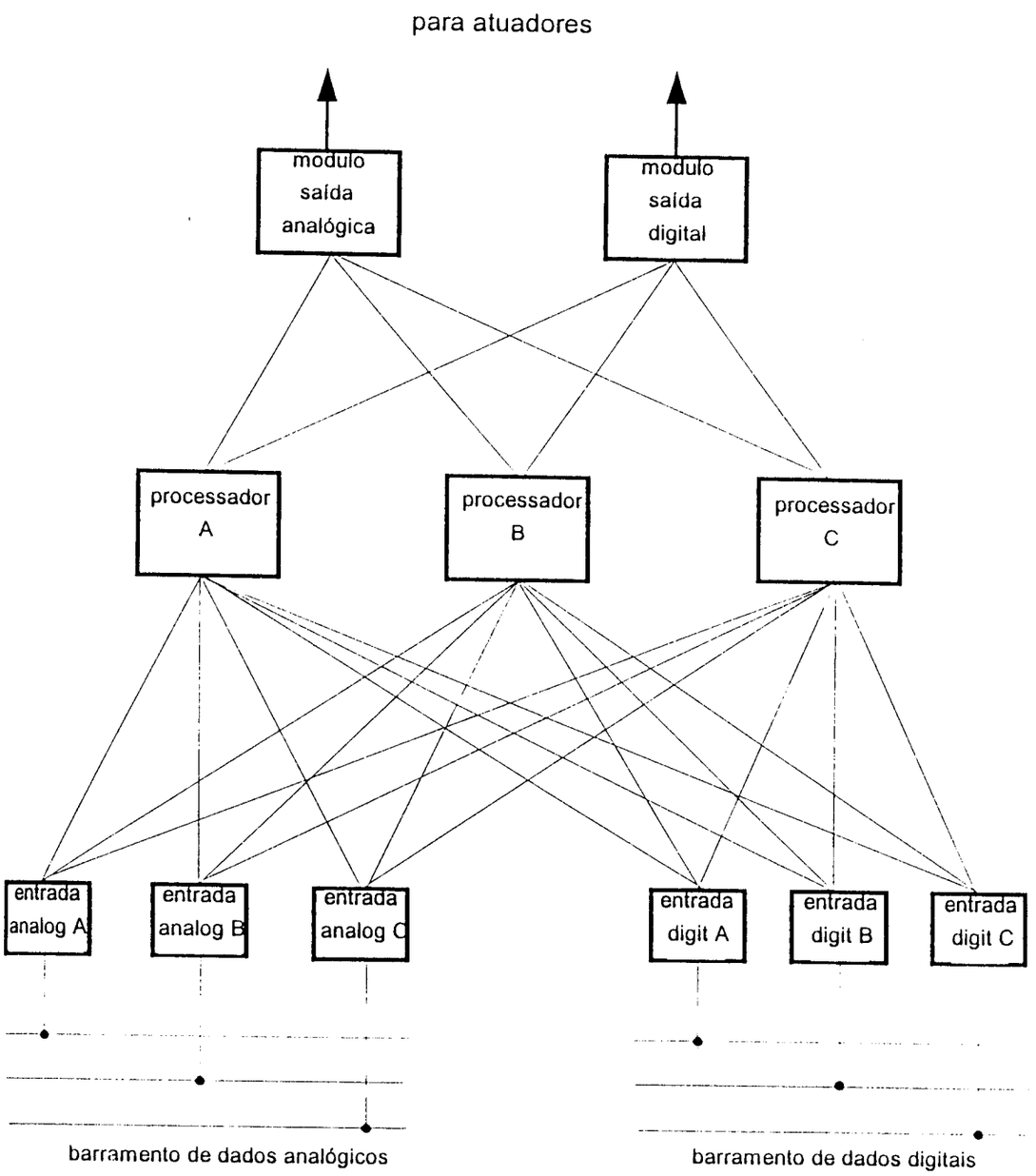


Fig. 6 - Sistema de controle e proteção em arquitetura TMR

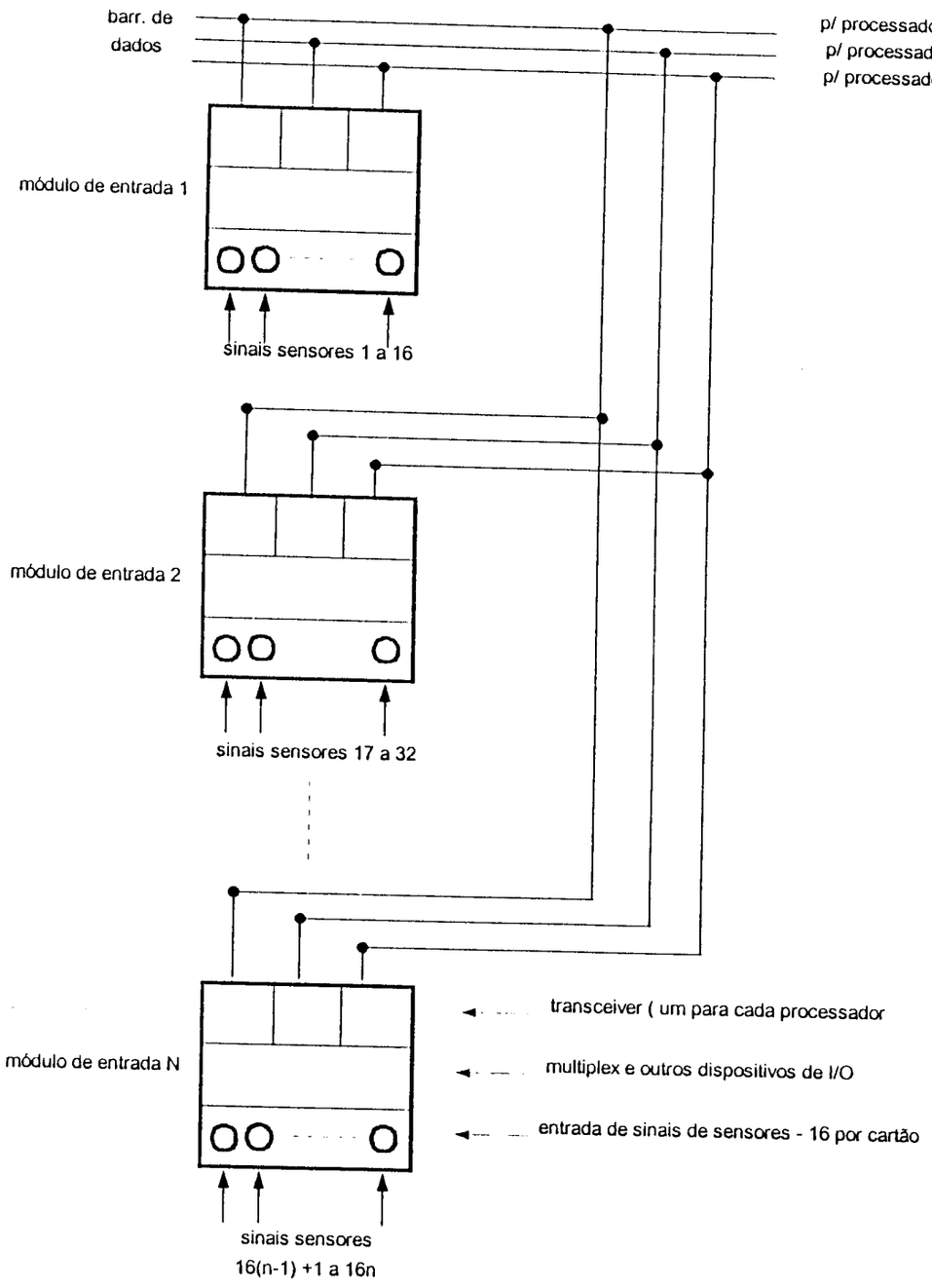


Fig. 7 - Módulos de entrada digital e analógica

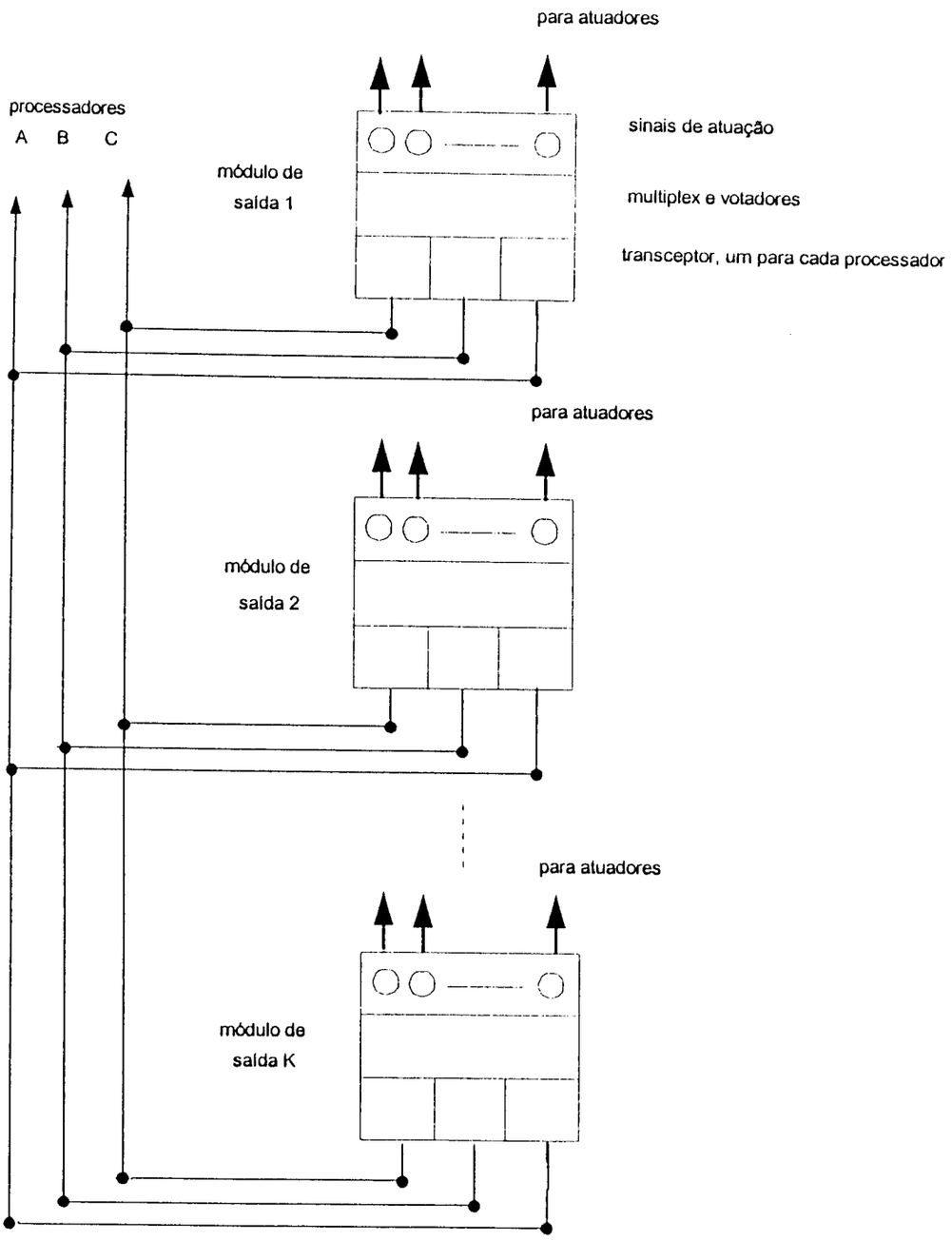


Fig. 8 - Módulos de saída.

Comentários sobre a arquitetura apresentada

Arquiteturas do tipo TMR, são classicamente empregadas em aplicações onde confiabilidade e segurança são indispensáveis. No caso, verifica-se que os módulos de entrada digitais e analógicas, do ponto de vista de *"hardware"*, possuem uma certa simplicidade de implementação. Já os módulos de saída devem ser implementados com submódulos independentes, com a restrição da existência de votadores independentes para cada saída de atuação. A perda de um poderia colocar em risco - caso não houvesse independência - a característica de tolerância à falha. Observa-se que o uso de módulos redundantes acionando o mesmo atuador não é recomendado, logo, admite-se que alguns módulos possam falhar e que eles possam ser reparados sem que o sistema sofra interrupção de operação.

3.4 Sistema de proteção baseado em arquitetura 2/4 redundante (NMR).

A fig. 9, mostra uma proposta de sistema de proteção desenvolvido pela Hitachi/Toshiba, para uma planta BWR (*Boiling Water Reactor*), baseada em arquitetura digital denominada "*digitalized safety system logic control*" (SSLC) [4]. Ela consiste de quatro canais separados incluindo transmissão de dados, comparador de "*setpoint*" chamado de DTM *(digital trip module)* e unidade lógica de desligamento TLU (*trip logic unit*) implementada pelo controlador digital. Os sinais dos sensores são enviados do campo quadruplicados, sendo um para cada canal através do RMU *(remote multiplexing unit)*.

As transmissões desses sinais de campo são realizadas através de cabos ópticos até o multiplexador de entrada de cada canal. O módulo DTM compara esses sinais com seu seu *"set point"* e determina o estado da planta; se mais de dois canais apontarem condição não segura, cada TLU procede com o envio do sinal de desligamento para a cadeia de desacionamento da válvula solenóide de desligamento do reator. O *"hardware"* do SSLC usa componentes e dispositivos normalmente aplicados em sistemas eletrônicos com restrição de segurança e há similaridade com modos de falhas.

O desenvolvimento do *"software"* contou com a formação de um grupo de trabalho para discutir a garantia de qualidade de *"software"*, incluindo verificação e validação

(V&V), e desenvolvimento para sistemas com requisitos de segurança. As diretrizes para a programação de sistemas digitais computadorizados com requisitos de segurança foram estabelecidas como JEAG-4609 [37].

3.4.1 Passos de Projeto/Manufatura e Verificação e Validação.

A sequência abaixo ilustra os passos usados pela Hitachi/Toshiba no desenvolvimento do sistema.

Fluxo de Projeto/Manufatura	**Fluxo de V&V**
1) Requisitos do projeto do sistema Especificações (Especificações das funções)	Verificação 1
2) Projeto de *"Hardware"* e *"Software"* Especificação de requisitos (Diagrama de blocos)	Verificação 2
3) Projeto de *"Software"* (Algoritmos e I/O)	Verificação 3
4) Manufatura do *"Software"*	Verificação 4
5) Integração *"Hardware" / "Software"*.	Verificação 5
6) Teste de Validação	Validação

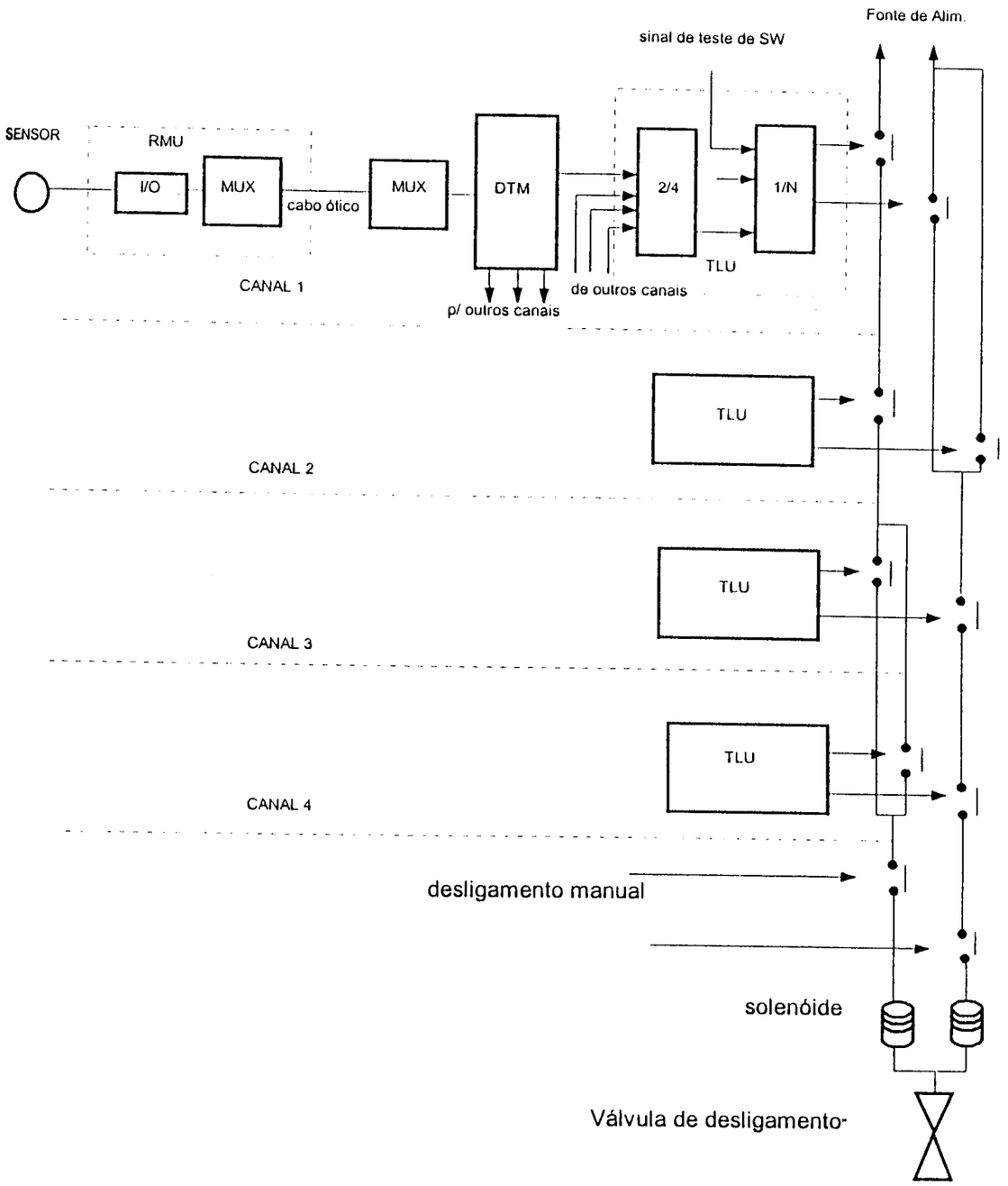


Fig. 9 - Exemplo do SSLC configurado como Sistema de Proteção de Reatores

Comentários sobre a arquitetura proposta pela Hitachi/Toshiba

A arquitetura apresentada tem uma configuração muito simples, de fácil entendimento e apresenta algo que seria um misto de sistema digital com tradicional, pois há uma lógica de votação 2/4 (NMR), realizada com dispositivos eletromagnéticos na cadeia de desligamento do Reator.

Verifica-se que o *"software"* é "policiado" por *"hardware"*, (TLU), através dos sinais de testes que supõem-se ser implementados com pulsos de *"watch-dog"* dinâmicos, utilizando-se a técnica do percurso controlado durante os *"loops"* de programa. Esta solução é empregada, inclusive no METRÔ de São Paulo, na linha Leste/Oeste. A unidade central de processamento é executada pelo DTM, onde seus resultados são distribuídos para os demais canais. O módulo TLU constitui um votador para cada canal que pode ser implementado por *"software"*, sendo que o resultado desta votação vai para a cadeia vital de "policiamento" do *"software"*.

O sistema da Hitachi/Toshiba possui quatro votadores digitais e um votador tradicional implementado com dispositivos eletromagnéticos. A presença de cabos óticos livra a comunicação de interferências eletromagnéticas e o sistema pode operar normalmente com 3 canais.

Um ponto que chama atenção neste sistema é que a votação entre os canais não deve violar o princípio da independência entre os mesmos, portanto é preciso assegurar que as falhas de um canal não possam desativar outros, prejudicando a disponibilidade do sistema.

De acordo com a referência [4], o sistema de proteção em questão foi projetado para a Kashiwasaki - Kariwa Nuclear Power Plant, unidade 6 e 7, a primeira do tipo ABWR (*Advanced Boiling Water Reactor*) existente no Japão, prevista para entrar em operação em 1997.

A arquitetura da Hitachi/Toshiba tem estrutura semelhante ao sistema SPIN, usado na proteção de reatores nucleares franceses.

3.5 *Topologias de circuitos digitais aplicados em sistemas de proteção.*

De um modo geral, qualquer sistema digital possui as seguintes características:

•Aquisição de sinais do campo ou processo, através de interfaces de entrada para sensores apropriados ou comandos.

•Conversão destes sinais em valores digitais.

•Processamento por meio de "*softwares*".

•Disposição de resultados por meio de interfaces de acionamentos, de apresentação ou de transmissão de dados.

Um esquema genérico de um canal simplex digital é apresentado na fig. 10:

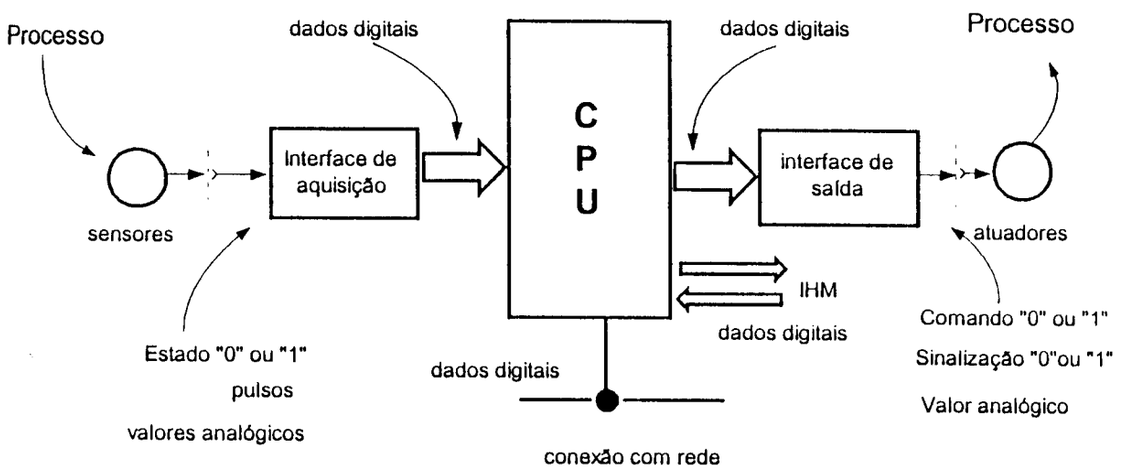


Fig. 10 - Esquema genérico de um canal digital

Os processos de conversão análogo/digital (A/D) e o de conversão digital/analógica (D/A), com circuitos discretos, podem ser suprimidos se a topologia contar com DSP's (*Digital Signals Process*). Neste caso o CI (circuito integrado) recebe em uma de suas entradas o sinal analógico diretamente e procede com a conversão internamente.

Para sistemas com restrições de segurança, estes circuitos de interface devem ter requisitos de falha segura, isto é, não permitem que falhas em seus componentes causem estados indesejáveis. O módulo digital deve receber os dados com garantia de sua integridade para o processamento e a topologia como um todo deve garantir o não mascaramento destes dados. Várias topologias de circuitos de interface são utilizadas para este fim e todas baseiam-se ou em topologias com estados intrinsecamente seguros, ou em diagnósticos e redundâncias que detectam a deterioração da informação.

Os circuitos intrinsecamente *"fail safe"* [5], baseiam-se em princípios físicos de armazenamento e transferência de energia, inversões de polaridade de tensões, sinais dinâmicos e isolações galvânicas entre blocos com separação física (separa-se adjacências se as mesmas podem causar inseguranças). Utilizam componentes de alta confiabilidade e não raro componentes especiais com modos de falha ou características de restrição definidas. Por exemplo: os capacitores com quatro terminais utilizados no meio ferroviário. Esses componentes são usados para garantir algum aspecto de restrição na configuração de circuito adotada. A técnica de FMEA (*failure mode and effects analysis*) é a principal ferramenta para análise dessas configurações, onde o requisito de segurança do circuito deve ser demonstrado por análise da topologia.

O uso de circuitos redundantes, com diagnósticos de falha representam outra opção para configurações de circuitos de interface de entrada. São utilizados em arquiteturas digitais que contam com diagnósticos por software e são empregados onde não é possível ou viável a implementação intrinsecamente *"fail safe"*. Devem ser construídos de forma que seja mantida a independência elétrica e mecânica dos canais redundantes e devem também basear-se no princípio de sinais dinâmicos para garantir a operação segura em caso de travamento de uma entrada em algum estado. Sua segurança está vinculada ao fluxo de sinais dinâmicos e aspectos funcionais do *"software"* e pode ser demonstrada por análise probabilística.

São apresentadas a seguir, exemplos de topologias de circuitos mais comuns empregados em: entradas digitais vitais, saídas digitais vitais, entradas de sinais analógicos vitais e saídas de atuação vitais.

Sinais de segurança nunca podem estar ligados a um estado fixo se o mesmo não for garantido em condição de falha, portanto a indicação de "ligado" ou "desligado" está associada a um sinal dinâmico para o estado de restrição. Nesse caso, a ausência deste sinal deve sempre representar a condição de segurança. As topologias podem variar em relação às apresentadas, mas o conceito embutido em sua filosofia permanece.

Entradas digitais vitais.

A topologia apresentada na fig.11 representa uma entrada digital vital, para um sistema de proteção computadorizado. Neste contexto, o sinal "0" ou ausência de tensão na entrada deve representar uma condição de segurança, um bloqueio, ou uma necessidade de desligamento. A presença do sinal "1" ou a presença de tensão, representa uma condição de restrição, uma liberação ou um sinal de OK para operação. Falhas simples de componentes não podem mascarar a condição de segurança e a leitura de um estado "1" no campo não ocorre por falha.

São exibidos dois acopladores óticos, separados fisicamente e isolados. Um sinal dinâmico de freqüência conhecida é aplicado ao primeiro e o processamento digital aguarda o retorno deste sinal com fase invertida pelo segundo. Verifica-se que este sinal só retornará quando existir a tensão que representa o "1" lógico no campo. Como estes componentes precisam de energia para propagar este sinal, enquanto não existir a tensão de campo não há retorno. Na configuração apresentada, falhas de curto-circuito ou circuito aberto não representam condição de restrição, apenas condição de segurança. São tomados cuidados no sentido de se avaliar o retorno desse sinal na freqüência enviada, na inversão de fase e até nos atrasos de tempo de retorno.

Como o *"software"* deve efetuar a leitura desta entrada, a responsabilidade pela integridade recai sobre o sistema digital, razão pela qual estas entradas costumam ser multiplicadas na razão da redundância empregada para sistema, como indica a fig.12. Assim sendo, o sinal da fonte sensora é distribuído para todos os canais redundantes onde posteriormente estes sinais serão confrontados via votação majoritária.

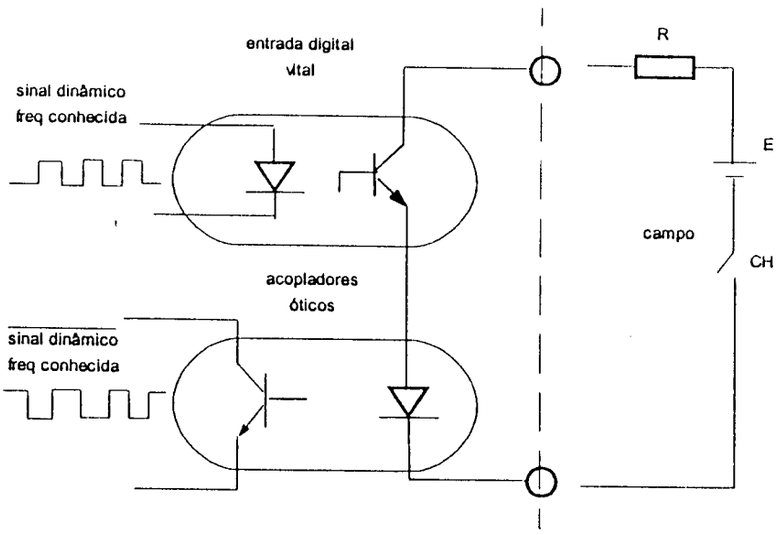


Fig. 11 - Topologia de uma entrada digital vital

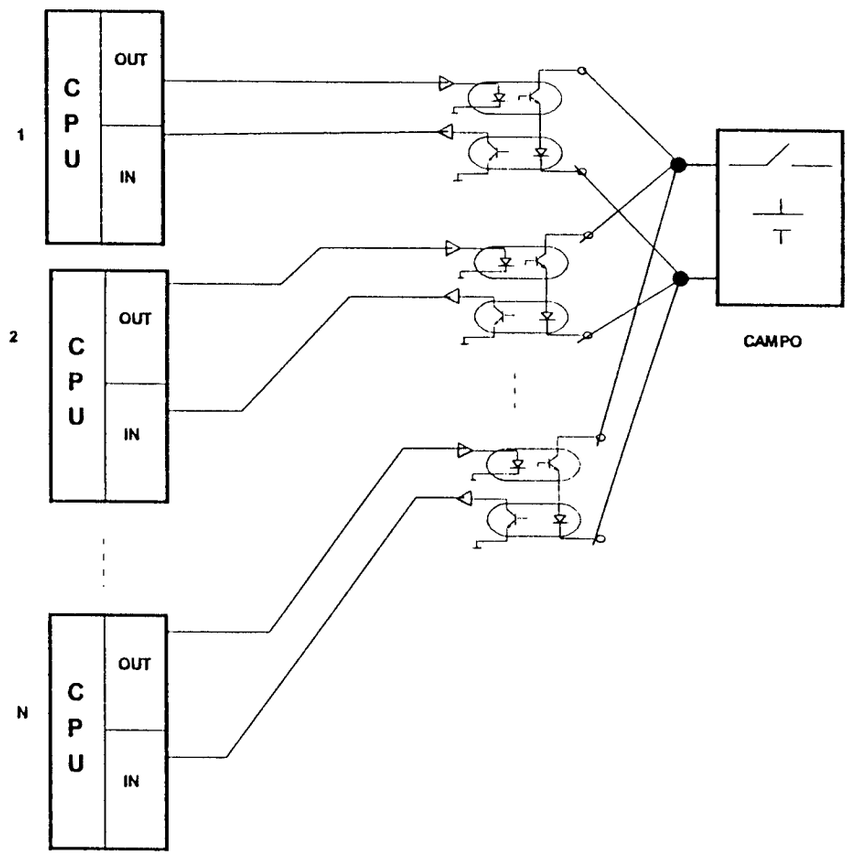


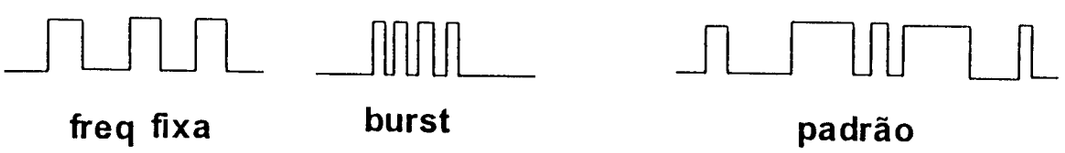
Fig. 12 - Arquitetura exibindo entradas digitais vitais

Saídas Digitais Vitais

As saídas digitais vitais em sistemas redundantes tendem a se concentrar em um circuito votador vital que converge as saídas redundantes para votação majoritária, fornecendo uma única saída de atuação. Características de isolação galvânica ou ótica são essenciais para garantir independência, pelo menos no que concerne ao aspecto físico. Este tipo de saída se aplicaria na saída da arquitetura TMR apresentada no itém 3.2.

Para a configuração "saída digital vital", pode ser utilizada a mesma configuração da "entrada digital vital" com diagnóstico realizado através de realimentação, ou sem diagnóstico, mais simplificada, mas sempre seguindo a característica de propagação de sinais dinâmicos.

Um aspecto importante dos sinais, tanto de entrada quanto de saída, é a freqüência de operação, onde para se evitar oscilações que geralmente ocorrem em freqüências elevadas, opta-se por sinais de baixa freqüência na faixa de dezenas de Hertz. Muitas vezes estes sinais seguem padrões preestabelecidos ou mais comuns, na forma de trens de pulsos (*burst*). Esta medida tende a garantir os aspectos de *"hardware"* de oscilação e alguns aspectos de falha de *"software"*, no que se refere ao programa ficar confinado em um *"loop"* fechado ativo. Obviamente os circuitos de atuação ou de votação devem se restringir a operar somente dentro das características destes sinais, sendo implementados com características *"fail-safe"*. A referência [5], apresenta um bloco denominado *"Pattern Recognition Logic"* que opera por reconhecimento e comparação de um padrão de referência com o sinal de saída digital vital e em caso de diferença, assume a condição de segurança.



A fig.13 apresenta duas topologias bastante comuns para aplicação em saídas digitais de sistemas de segurança. A primeira topologia, similar a uma entrada digital vital, apresenta um diagnóstico de retorno para detecção de falha, ou seja, o sinal aplicado retorna com atraso e inversão de fase, o módulo de atuação opera com sinais dinâmicos no padrão estabelecido. A segunda topologia não possui o diagnóstico de retorno, mas o módulo acoplado deve operar da mesma forma, a desvantagem é que não há detecção de falha do canal e pode haver prejuízo da disponibilidade do sistema.

A fig.14 apresenta um esquema de saída digital vital, de arquitetura redundante, com diagnóstico. O atuador de campo deve ser acoplado a um circuito votador para acionamento do dispositivo comandado.

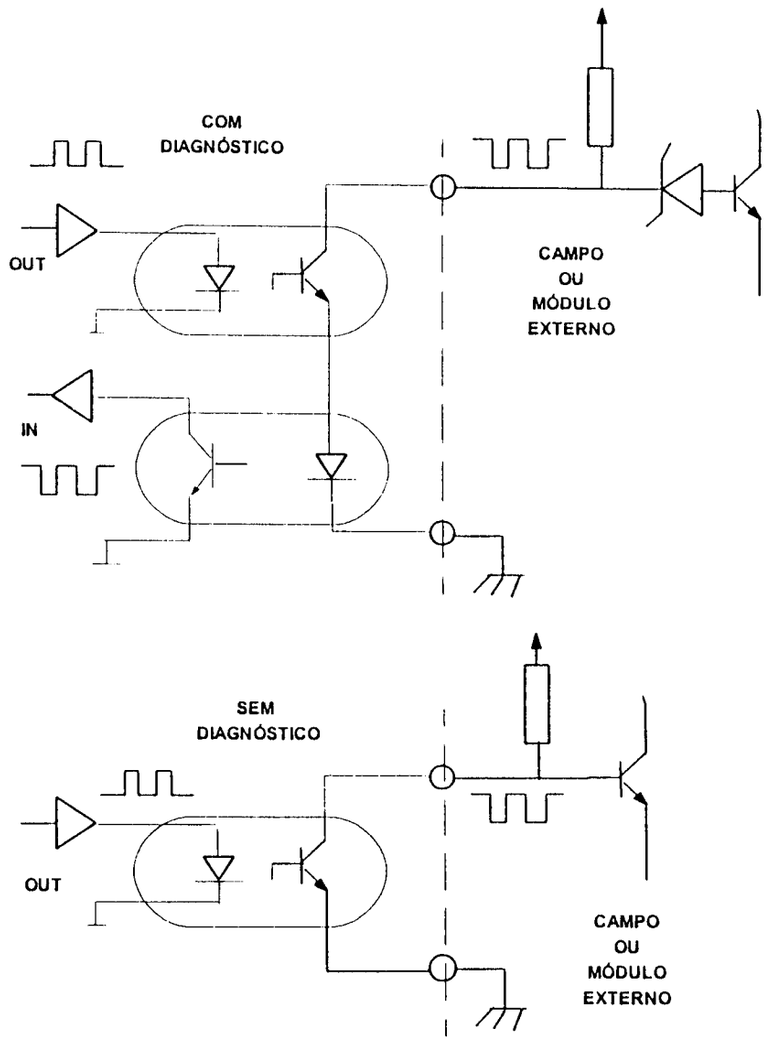


Fig. 13 - Topologias de saídas digitais vitais

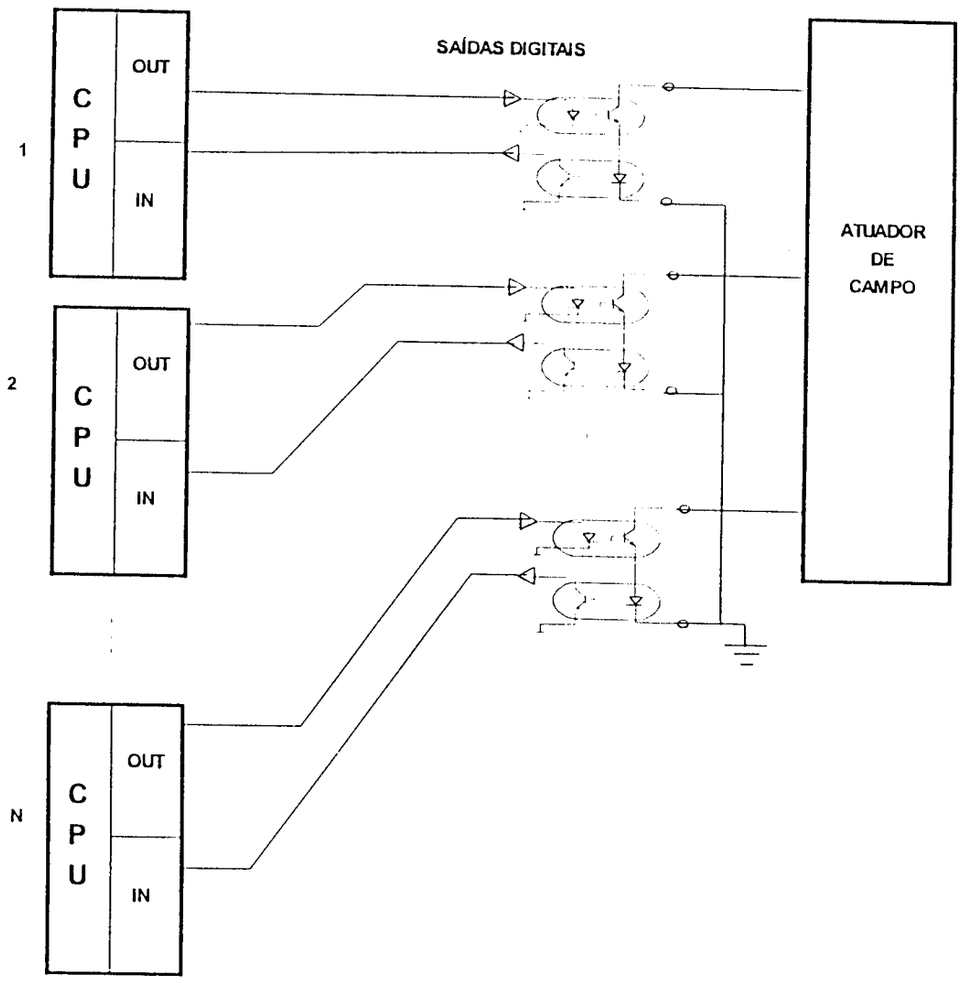


Fig. 14 - Arquitetura com saídas digitais vitais

Entradas analógicas vitais.

O objetivo da topologia apresentada para entradas analógicas vitais é garantir a integridade da aquisição dos sinais analógicos durante os processos de condicionamento e conversão análogo-digital. Neste caso, além de se detectar falhas dos tipos: presença de

oscilações, travado em "zero", travado em "um", é necessário detectar-se quaisquer variações de amplitude e mesmo de faixa de freqüência do sinal analógico. Logo, devem ser diagnosticadas falhas do tipo, aumento de ganho de amplificadores, resposta em freqüência alterada e conversão análogo digital incorreta [6].

Não existem topologias convencionais abrangentes para estes requisitos. Normalmente, utiliza-se técnicas de redundância com chaveamento de canais analógicos para valores padrões conhecidos com o objetivo de se garantir a integridade da conversão por igualdade de valores, conforme mostra a fig.15. Evidentemente, aspectos de segurança do *"software"* devem ser considerados, pois o processo depende da topologia de *"hardware"* e dos algoritmos de *"software"*. Procura-se evitar o uso de um único algoritmo de aquisição e testes, devido a probabilidade de ocorrência de falhas de modo comum. Assim, é indicado a utilização de algoritmos de *"software"*, diferentes e desenvolvidos por grupos distintos de programadores. Todos os mecanismo de verificação e validação de projeto deverão ser aplicados.

A configuração apresentada como exemplo, tem como princípio de funcionamento o diagnóstico de todos os canais de aquisição, através de padrões pré-estabelecidos, guardados na memória da CPU. Cíclicamente cada canal é exercitado através da aquisição de um sinal padrão. Isso é realizado enviado-se um sinal conhecido para um conversor D/A, o qual realiza a sua conversão e o emite ao canal de aquisição em teste, através de um demultiplex (DEMUX) e módulos compostos por chaves analógicas, responsáveis pela comutação de canais. O multiplex (MUX), transfere o sinal ao conversor A/D, e após aquisição, o sinal é processado, comparando-se seu valor original com o valor coletado. Em caso de discrepância, o processamento diagnosticará falha. Dessa forma, testa-se dinamicamente todo o conjunto de aquisição analógica em modo *"on line"*. Normalmente, as grandezas físicas são mensuradas por mais de um sensor com redundâncias, e suas saídas são aplicadas a CPU's redundantes que farão votação **m/n** dos sinais, de modo a garantir a integridade do conjunto, inclusive informações dos sensores, fig. 16. A referência [6], apresenta uma topologia semelhante à apresentada nesta seção.

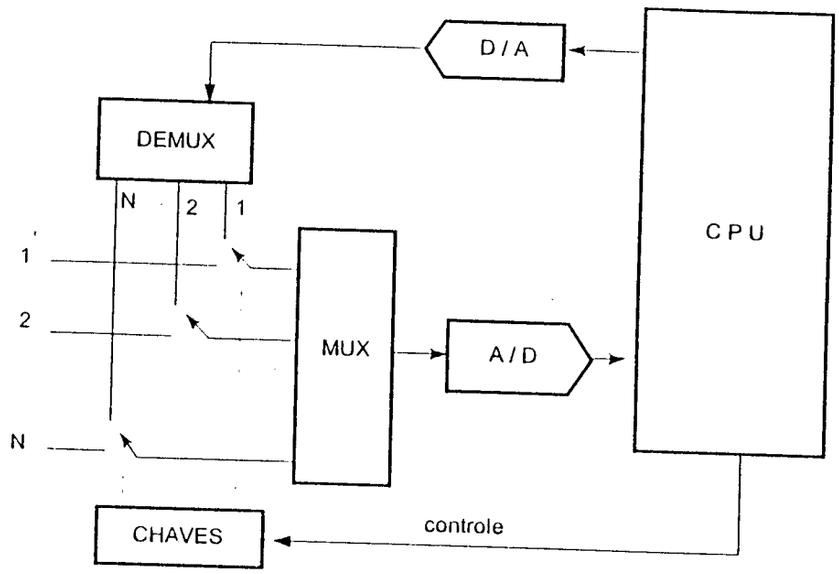


Fig. 15 - Exemplo de entrada analógica vital

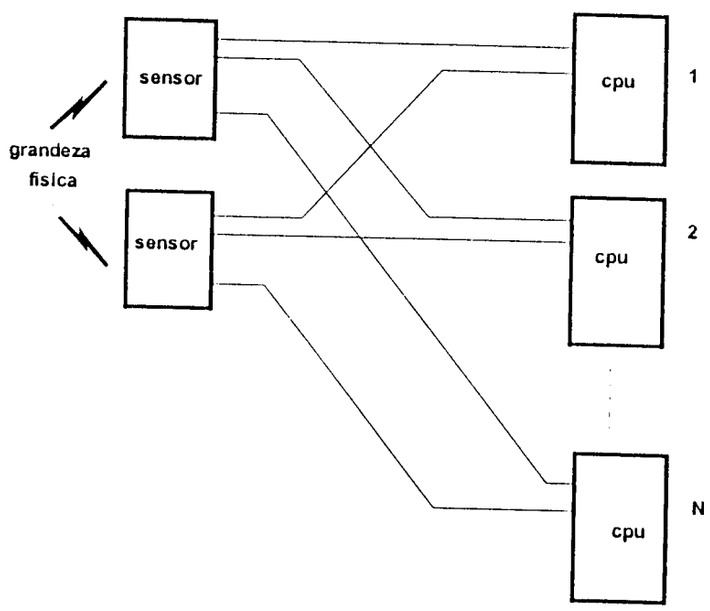


Fig. 16 - Topologia com entradas analógicas vitais

Saídas Analógicas vitais.

Não é possível garantir que um sinal analógico de saída não possa assumir valores espúrios na presença de falhas, mas pode-se diagnosticar quando um sinal não está dentro de suas características, através da monitoração do mesmo, pelo processo de realimentação, discutido no início do capítulo. Isto é feito de forma dual a uma entrada vital, conforme ilustra a fig. 17.

As saídas analógicas são testadas através da realimentação destes mesmos sinais. Dessa forma, pode-se comparar a integridade do sinal convertido, e em caso de diferença, apontar a falha e/ou bloquear o processamento através de circuitos apropriados (*watch-dog).* Assim, embora não seja possível garantir que um sinal analógico está sendo emitido com valor errôneo, pode-se detectar a ocorrência da falha e tomar as providências para que o sistema não sofra uma transição para um estado crítico.

Saídas de atuação vitais

As saídas de atuação vitais, baseiam-se na propagação de sinais dinâmicos com inversões de polaridade, amplificações, e acoplamentos finais realizados por dispositivos que garantam a isolação. O uso de transformadores com separação de enrolamentos garante isolação galvânica, de modo que, não existam por construção, possibilidades de curtos-circuitos entre suas bobinas. Essa é uma solução comum em sistemas para aplicações críticas.

O exemplo apresentado na fig.18, exibe uma topologia que deve garantir que em caso de qualquer modo de falha de componente, estados de entrada travados em "0" ou "1" e mesmo oscilações com freqüências erradas, não resultem em acionamento indevido de uma saída. Essas topologias, em geral, acabam acionando relés vitais para o desligamento de emergência de reatores nucleares.

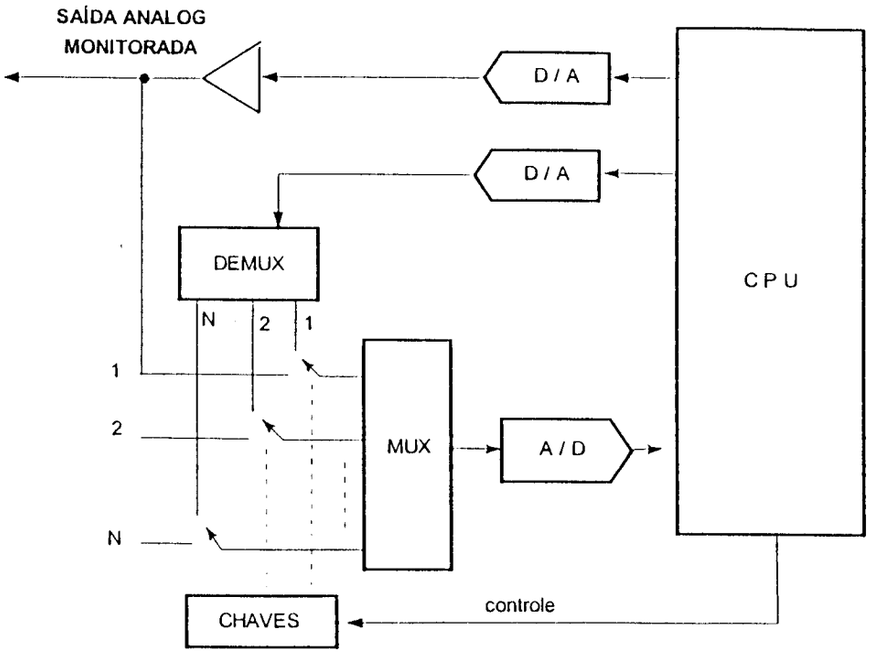


Fig. 17 - Topologia de uma saída analógica vital.

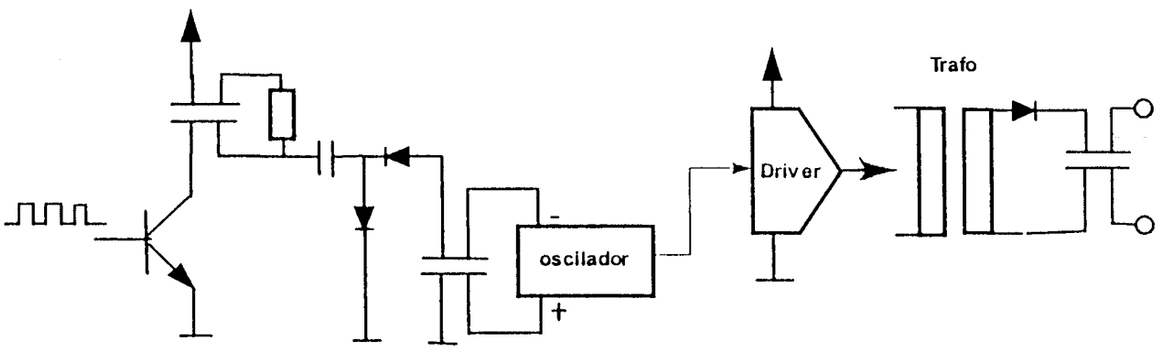


Fig. 18 - Inversor de polaridade

Na fig. 18, o acionamento é realizado por um sinal dinâmico de baixa freqüência oriundo de uma topologia de saída vital. Um filtro constituído por resistor e capacitor de quatro terminais, garante que na presença de freqüências elevadas, não haverá atuação de saída. A saída é acionada através de um transformador com isolação galvânica e separação física entre primário e secundário, excitado por um sinal de freqüência pulsada mais elevada, que transfere potência do primário para o secundário. Este sinal é gerado por um oscilador alimentado pelo inversor de polaridade.

Esta topologia garante que entradas indevidas não acionam a saída, bem como falhas simples de componentes e existência de freqüências elevadas. Dessa forma, restringe-se significativamente, a probabilidade de um acionamento inadequado por defeito de componentes ou sinal de excitação indevido. Uma aplicação típica para este tipo de topoiogia é uma votação de canais redundantes, que devem manter relés vitais acionados para completar uma cadeia de contatos que impede o desligamento do reator.

Relés vitais são dispositivos eletromecânicos que garantem por construção o desligamento quando desernegizados. Em geral, possuem contatos de uma liga prata/carbono - para se evitar a sua fusão - sendo a abertura garantida mecanicamente por ação da gravidade.

A fig.19, ilustra uma aplicação típica de cadeia de desligamento de reator composta por este tipo de dispositivo. Trata-se de uma lógica de votação 2/4 usada para esta finalidade. Os acionadores vitais devem garantir o desligamento, sendo que falhas em seus componentes não devem permitir a alimentação dos dispositivos eletromecânicos vitais. O acionamento só ocorrerá perante padrão de sinal com determinada frequência. As arquiteturas de sistemas de proteção de reatores que utilizam processo semelhante são o SPIN (Merlin Gerin) e SSLC (Hitachi/Toshiba).

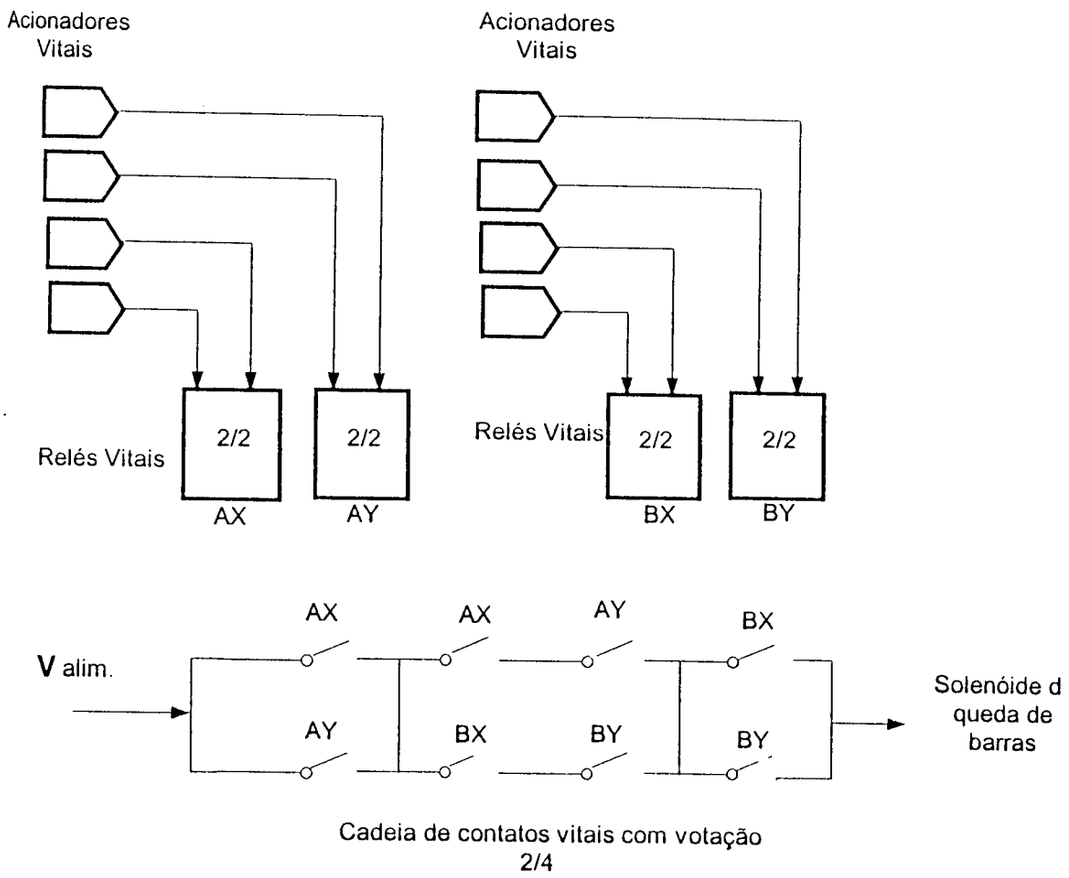


Fig. 19 - Esquema com acionadores vitais em cadeia de desligamento de reator

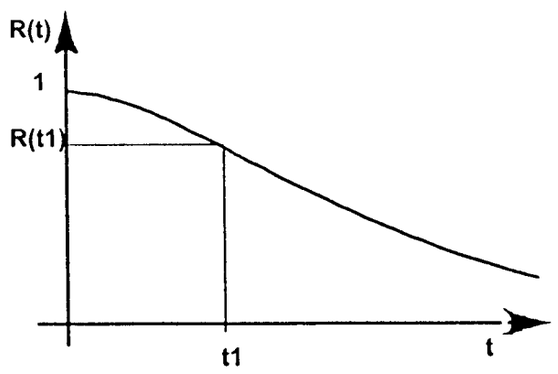
4. CONCEITOS BÁSICOS DE CONFIABILIDADE.

Apresenta-se neste capítulo, os conceitos básicos e as ferramentas que serão empregadas para o método de análise de confiabilidade e segurança, proposto nesta dissertação.

4.1 Índices de confiabilidade

4.1.1 Confiabilidade R(t)

Confiabilidade :- **R(t),** função que expressa a probabilidade de que um sistema funcione corretamente no intervalo de tempo (0, t), dado que esteja funcionando em t=0.

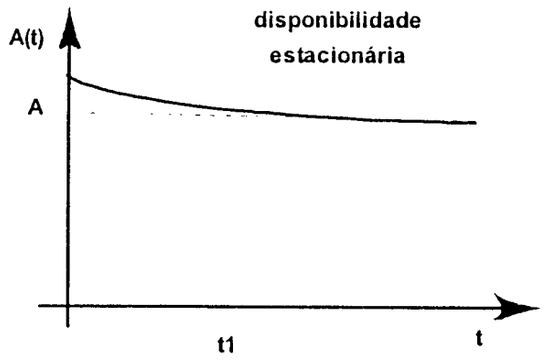


4.1.2 Disponibilidade A(t)

Disponibilidade:- A(t), função que expressa a probabilidade de que o sistema esteja funcionando normalmente no instante (t). Para um sistema com intervalos de reparo e operação, estabelecidas, define-se a disponibilidade estacionária "A" como sendo:

$$A = \lim_{t \to \infty} A(t)$$

Esse limite representa a disponibilidade assintótica e também a fração do tempo em que o sistema está disponível.



4.1.3 Segurança S(t)

Ou, confiabilidade segura S(t), é a função que expressa a probabilidade de que o sistema tenha sobrevivido no intervalo de tempo (0 a t) sem ter alcançado um estado inseguro, dado que o estado do sistema em t=0 é seguro. Este conceito é análogo a confiabilidade.

4.1.4 Manutenibilidade

A manutenibilidade M(t) é a probabilidade de que o sistema seja restaurado ao estado operacional no tempo t, dado que não estava funcionando em t=0. Manutenibilidade é normalmente apresentada em termos de taxa de reparos $\mu(t)$, ou MTTR *(mean time to repair),* se $\mu(t)$ = constante, então MTTR = $1/\mu$.

4.1.5 Dependabilidade.

Este termo não é do vernáculo, vem de "*Dependability*", que é definido em sistemas tolerantes a falhas como sendo a capacidade de que um sistema inicie e termine uma missão sem falhas que o tornem inoperante. É função da disponibilidade, confiabilidade e manutenibilidade.

4.1.6 Índices comuns de confiabilidade:

Probabilidade acumulada de falhas : - **F(t),** probabilidade de que tenha ocorrido pelo menos uma falha no sistema no intervalo (0, t). Expressa também a não confiabilidade de um sistema.

$$F(t) = 1 - R(t)$$

Densidade de probabilidade de falhas - f(t), probabilidade de ocorrência de uma ou mais falhas no intervalo (t,t+dt),

$$f(t) = \frac{dF(t)}{dt}$$

Taxa de falhas $\lambda(t)$ exprime a densidade de probabilidade de falhas no instante t, condicionada ao fato de não ocorrência de falhas no intervalo (0, t)

$$\lambda(t) = \frac{f(t)}{R(t)}$$

4.1.7 Definições de MTTF, MTTR, MTBF, MTTFc e MTTUF.

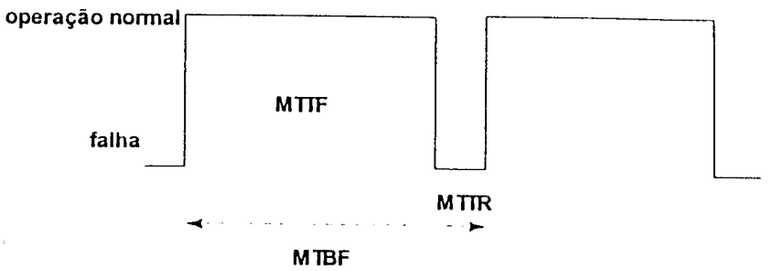
MTTF: - *Mean time to failure*, índice que expressa o tempo médio esperado para a ocorrência da primeira falha no equipamento. Esse índice é adequado para equipamentos não reparáveis. Em sistemas de segurança utiliza-se o **MTTFc**, "m*ean time to failure critical*" ou o sinônimo **MTTUF**, "m*ean time to unsafe failure*". onde o estado falho pode significar um acidente e portanto não há reparo.

$$MTTF = \int_{o}^{\infty} R(t)dt$$

MTTR: - *Mean time to repair*, expressa o tempo médio para a implementação do reparo do equipamento, associado a fatores humanos de substituição de módulos ou componentes.

MTBF: - *Mean time between failures*, índice que expressa o tempo médio de ocorrências de falhas, utilizado em contexto de aparelho reparável..

Admitindo-se que os sistemas possuam dois grandes estados (operacional e falho), de um modo geral é válida a seguinte aproximação:

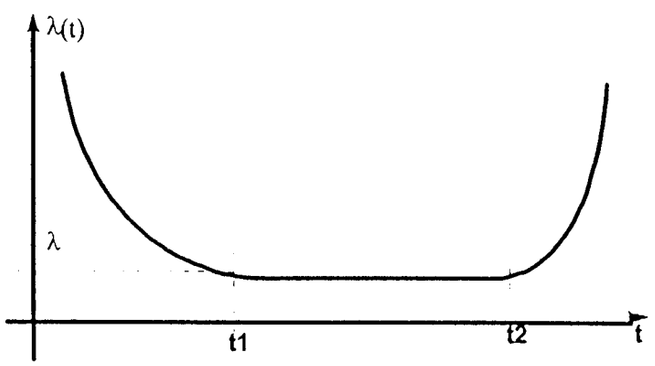


Uma aproximação para disponibilidade (A), para equipamentos com taxa de falhas $\lambda(t)$= constante e taxa de reparos $\mu(t)$=constante, é dada por

$$A = \frac{MTTF}{MTBF}$$

4.1.8 Aspectos da taxa de falhas $\lambda(t)$

Para equipamentos eletrônicos em operação, verifica-se que a taxa de falhas no início da vida útil possui um valor inicial que nos primeiros períodos diminui até um valor que permanece constante por um grande período até que a taxa de falhas começa a subir novamente, segundo o seguinte diagrama.



O intervalo (0, t1) é definido como região de mortalidade infantil, onde a taxa de falhas decresce até um valor constante, esse intervalo ocorre devido a defeitos de

fabricação e devido a falhas intrínsecas do próprio componente. Em geral acelera-se esse período através de processos denominados *"burn-in"* para componentes ou para equipamentos.

O intervalo (t1, t2) é definido como tempo de vida de operação normal do equipamento e para componentes eletrônicos em geral, a taxa de falhas permanece constante $\lambda(t)=\lambda$, pois componentes eletrônicos fabricados de acordo com processos tecnologicamente amadurecidos tendem a exibir essa característica para a taxa de falhas. Esse aspecto permite que a análise de confiabilidade possa ser modelada considerando-se taxa de falhas constante caracterizando-se uma distribuição exponencial para modelagem e cálculos de confiabilidade. O intervalo após t2 representa um crescimento da taxa de falhas caracterizado pelo envelhecimento e fim de vida do equipamento ou componente (*Wear-out*). Após t2 o equipamento necessita ser substituído ou sofrer reparos necessários de modo a continuar operando com a mesma confiabilidade.

A região de interesse para análise de confiabilidade é o intervalo (t1,t2).

4.2 Distribuição Exponencial.

Para $\lambda(t) = \lambda$ constante, então:

$$R(t)=e^{-\lambda t} \text{ para } t \geq 0$$

$$F(t) = 1 - e^{-\lambda t} \text{ para } t \geq 0$$

$$f(t) = \lambda e^{-\lambda t} \text{ para } t \geq 0$$

$$MTTF = \frac{1}{\lambda}$$

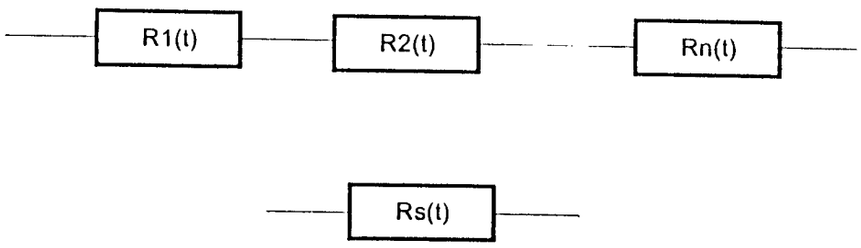
4.3 Confiabilidade de sistemas para arranjos série e paralelo.

Aplicável quando as falhas apresentadas por um sistema sejam aleatórias de modo que uma distribuição exponencial pode ser utilizada.

4.3.1 Arranjo série.

Dado um sistema Q composto de n subsistemas, define-se modelagem série quando a operação correta de Q depende da operação correta de todos os seus subsistemas. No caso o sistema é considerado não tolerante a falhas.

Considerando-se que Qi tenha confiabilidade Ri(t) (i=1,2,3.....n) e Rs(t) é a confiabilidade equivalente do arranjo, temos:



demonstra-se que: $Rs(t) = \prod_{i=1}^{n} Ri(t)$, e para distribuição exponencial, onde $\lambda(t)=\lambda i$ ou seja taxa de falhas constante, temos:

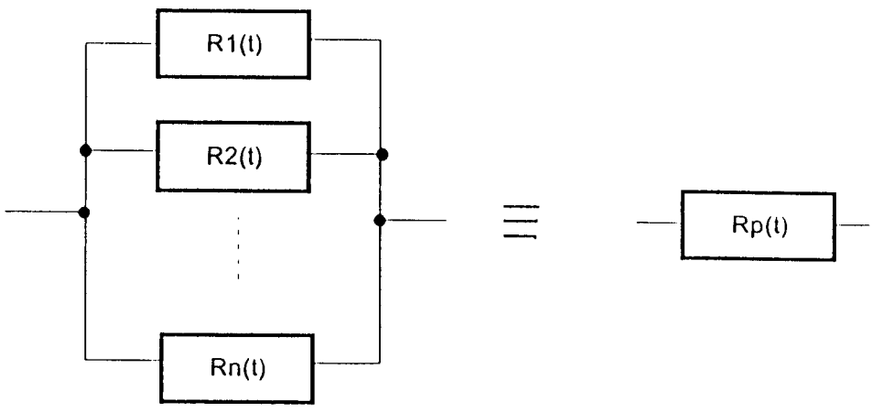
$$Rs(t) = e^{-\lambda st} \text{ para } \lambda s = \sum_{i=1}^{n} \lambda i \text{ e no caso o, } MTTF = \int_{0}^{+\infty} Rs(t)dt = \frac{1}{\lambda s}$$

Considerando-se, para uma placa de circuitos eletrônicos, que a falha de um componente causará a falha da placa, o calculo de confiabilidade pode ser realizado pela modelagem série de todos os seus componentes. Sugere-se utilizar a norma MIL HDBK 217F notice 2 [36], que estabelece métodos para determinação de taxas de falhas de componentes em função de parâmetros relacionados com o tipo de componente, classe de aplicação, ambiente, etc.

4.3.2 Arranjo paralelo.

Dado um sistema Q composto de n subsistemas, define-se arranjo paralelo se o mesmo puder ser decomposto em n subsistemas Q1, Q2,...Qn, onde a operação do sistema depende do funcionamento de apenas um dos subsistemas. Se os subsistemas forem idênticos, define-se um arranjo 1/n de redundância, se o funcionamento depender de m unidades corretas, o arranjo é caracterizado por m/n.

No caso Qi , tem confiabilidade Ri(t) (i=1,2,3.....n), e o esquema do arranjo fica.



demonstra-se que :

$$Rp(t) = 1 - \prod_{i=1}^{n} (1 - Ri(t))$$ e para λi=constante, $\Rightarrow$ $$Rp(t) = 1 - \prod_{i=0}^{n} (1 - e^{-\lambda i t})$$

Verifica-se que a taxa de falhas λp(t) do arranjo não é constante como havia ocorrido na confiabilidade série:

$$\lambda p(t) = -\frac{1}{Rp(t)} * \frac{dRp(t)}{dt}.$$

4.3.3 Arranjos não reparáveis.

Sistemas sem mecanismos de manutenção (reparo de falhas), podem ter sua confiabilidade avaliada segundo arranjos de modelagem de confiabilidade, série e paralelo. No caso de sistemas não redundantes, a primeira falha leva o sistema para o estado falho, com indisponibilidade de operação. A presença de redundâncias levam os sistemas a tolerarem uma seqüência finita de falhas até a sua inoperabilidade. Não são considerados reparos ou manutenção nestes sistemas, pelo menos durante o tempo de missão. As aplicações para este tipo de análise, podem ser ilustradas por equipamentos que operam dentro da contenção de uma planta nuclear, e que só podem sofrer reparos quando o acesso à contenção for permitido. A recarga de combustível, é um exemplo. Outro exemplo é o de satélites, onde qualquer possibilidade de manutenção é inexistente.

Um exemplo de arranjo não reparável pode ser uma arquitetura TMR 2/3, fig. 20, durante um tempo de missão, sem possibilidade de manutenção.

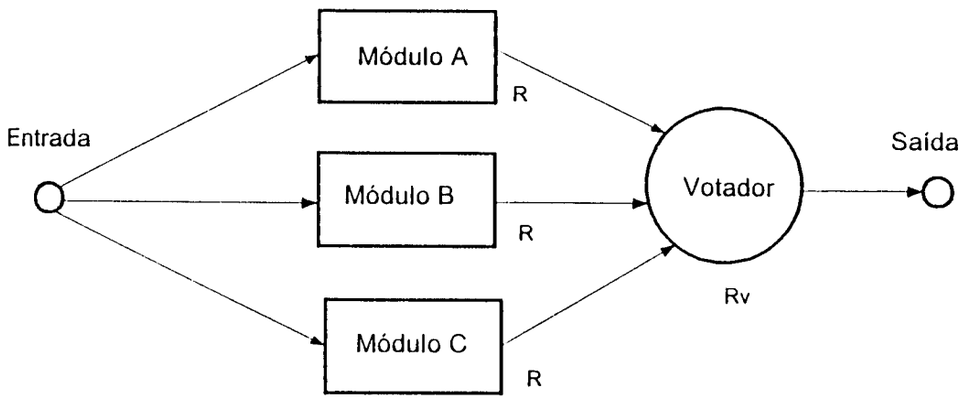


Fig. 20 - Arquitetura TMR

Na arquitetura mostrada na fig. 20, o votador é o gargalo do sistema, que não tolera falhas nesse módulo. Demonstra-se [26], que a confiabilidade é maximizada quando todos os módulos funcionais tem idênticos valores de confiabilidade "R".

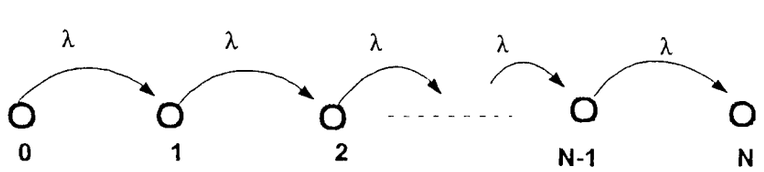
4.3.4 Arranjos reparáveis.

A análise de confiabilidade de arranjos reparáveis é mais complexa. Isso significa que a ocorrência de falha em um dos canais de um sistema redundante, tem a probabilidade de recuperação - segundo uma taxa de reparos - possibilitando o retorno do canal para operação plena. A introdução de reparos aumenta a confiabilidade e a disponibilidade do conjunto. Para a modelagem de análise do sistema é necessário introduzir uma probabilidade condicional $\mu(t)dt$ que dada uma ocorrência de falha em uma unidade no tempo t, ocorre o reparo no tempo dt de t. Então $\mu(t)$, (1/tempo), descreve a taxa instantânea de reparo tal como $\lambda(t)$ representa a taxa instantânea de falha. Se $\mu(t)=\mu$, então a taxa de reparo é constante e assume-se que o reparo somente é completado em um tempo aleatório após ter sido iniciado, e não que o reparo é iniciado a um tempo aleatório após a ocorrência de falha.

A modelagem proposta para avaliação de confiabilidade, segundo as condições estabelecidas, atende os requisitos de um processo de *cadeias de Markov.*

4.3.5 Modelagem de *Markov* - Resumo:

Dado N transições de estados de um sistema, seja Pn(t) definido como a probabilidade que o sistema esteja no estado n no tempo t, isto é ocorreram n transições, e seja $\lambda\Delta t$ a probabilidade de transição para outro estado no intervalo Δt, então:



$$Po(t+\Delta t) = (1-\lambda\Delta t)Po(t) \Rightarrow p/n = 0$$
$$Pn(t+\Delta t) = \lambda\Delta t P_{n-1}(t) + (1-\lambda\Delta t)P_n(t) \Rightarrow p/n = 1,2,3.....(N-1)$$
$$P_N(t+\Delta t) = \lambda\Delta t P_{N-1}(t) + P_N(t)$$

Dividindo-se por Δt e no limite Δt⇒0, temos um sistema de equações diferenciais (equações de Chapman-Kolmogorov):

$$\frac{dP_0(t)}{dt} = -\lambda P_0(t)$$
$$\frac{dP_n(t)}{dt} = \lambda P_{n-1}(t) - \lambda P_n(t)$$
$$\frac{dP_N(t)}{dt} = \lambda P_{n-1}(t)$$

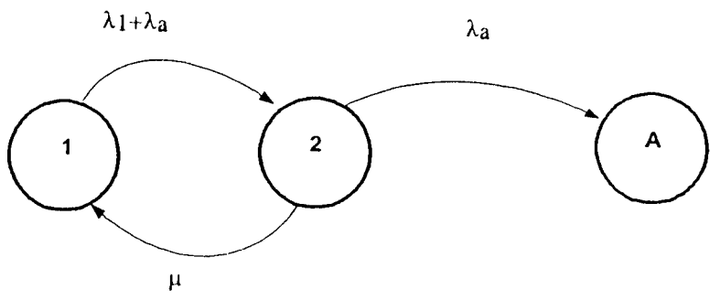
As condições iniciais deste sistema de equações diferenciais são:

$P_n(0)=1, \Rightarrow n=0$ e $P_n(0)=0, \Rightarrow n \geq 1$

4.3.6 Condições de Contorno

Algumas condições devem ser atendidas na utilização do modelo de *Markov* para avaliação de confiabilidade de sistemas. Consideremos que um sistema redundante, reparável, possa ter estados operacionais definidos em função de falhas; que a mudança de um estado para outro ocorra aleatoriamente no tempo; que a probabilidade de mudança de um estado para outro dependa somente do estado em que o sistema se encontre e para os estados que o sistema possa assumir, onde a probabilidade estacionária de ocupação de qualquer estado não depende do estado inicial; e que exista um estado absorvedor.

A título de exemplo, consideremos um sistema redundante 1/2 onde (1) corresponde a operação normal, (2) a operação com um canal falho e (A) o estado absorvedor. Seja λ1+λa a taxa de falhas para passagem do estado 1 para 2 e λa a taxa de falhas para a passagem do estado 2 para o estado absorvedor. Seja μ a taxa de reparos. Nessas condições, podemos representar a transição de estados do sistema por:



A cadeia possui um estado absorvedor e o processo é *Markoviano*.

Este exemplo pode ser representado pelo sistema de equações diferenciais:

$$\frac{dP_1(t)}{dt} = -(\lambda 1 + \lambda a)P_1(t) + \mu P_2(t)$$
$$\frac{dP_2(t)}{dt} = (\lambda 1 + \lambda a)P_1(t) - (\mu + \lambda a)P_2(t)$$
$$\frac{dP_A(t)}{dt} = (\lambda a)P_A(t)$$
$$P_1(t) + P_2(t) + P_A(t) = 1$$

Para t= 0 as condições iniciais são $P_1(0) = 1$, $P_2(0) = P_A(0) = 0$, admitindo-se que o sistema esteja funcionando no instante inicial.

Para $t \Rightarrow \infty$, teremos $P_1(\infty) = P_2(\infty) = 0$, *e* $P_A(\infty) = 1$, caracterizando que o ocupará o estado falho.

A confiabilidade deste sistema é dada pela probabilidade de ocupação dos estados operacionais, portanto:

$$R_s(t) = P_1(t) + P_2(t) \text{ e o } MTTF = \int_0^\infty R_s(t)dt$$

Quando o estado absorvente for caracterizado por um estado inseguro no modelo de transição de estados, o MTTF é o MTTUF.

Em geral, os modelos clássicos de *Markov* se resumem em :

•Modelos de confiabilidade⇒ R(t), MTTF, ⇒ análise transitória

•Modelos de disponibilidade⇒ A(t), A ⇒ análise permanente. *Cadeias de Markov* sem estados absovedores ⇒ disponibilidade estacionária.

Dado um sistema genérico, e Pi(t) = a probabilidade do sistema se encontrar no estado i no instante t, o espaço de ocupação de probabilidades tem o seguinte comportamento:

	t = 0	t1	t = ∞
Po(t) ...	1 ..	Po(t1) ..	0
P1(t) ...	0 ..	P1(t1) ..	0
:	0 ..	:	0
Pn(t) ...	0..	Pn(t1) ..	1

A confiabilidade R(t) do sistema genérico é a soma de probabilidades de ocupação dos estados em que o sistema está funcionado em função do tempo, portanto:

R(t) = Po(t) + P1(t) + ...Pn-1(t),

A disponibilidade A(t) do sistema genérico é a soma de probabilidades de ocupação de estados operacionais e não operacionais no instante k, portanto:

A(t) = Po(k) + P1(k) + ...Pn(k) ⇒ disponibilidade no instante t = k

A página 61 está com texto cortado e a página 62 não existe.

Em regime transitório, Po(0) = 1, caracteriza o instante inicial com

Em regime permanente, Po(n) = 0, caracteriza o instante

matriz

disponibilidade estacionária A

A = Po + P1 +.....Pn $\Rightarrow$ disponibilidade estacionária. Aplicável *Markov* sem estados absorvedores.

Formulação matricial.

operac

diferer

Na forma matricial [18], considera-se um modelo com N estados transição do estado ***i*** para ***j***, λij é constante para qualquer ***ij***. Seja Λ a m com elementos λij para $i \neq j$ temos:

$$\lambda_{ij} = -\sum_{k=1,k\neq i}^{N} \lambda_{ik}$$

absorv

Seja Pi(t) a probabilidade que o sistema esteja no estado i no instar

$$\rho = \left| P_1(t), \ldots\ldots, P_N(t) \right|$$

o vetor probabilidade de ocupação dos estados. Assim, podemos re

de eler

matrici

$$P_i(t+dt) = \sum_{k=1,k\neq i}^{N} P_k(t)\lambda_{ki}dt + P_i(t)[1 - \sum_{k=1,k\neq i}^{N} \lambda_{1k}]$$

e calculando-se o limite para dt$\rightarrow$0 resulta:

$$\lim_{dt\to 0} P_i(t+dt) \Rightarrow P_i'(t) = \sum_{k=1}^{N} P_k(t)\lambda_{ki}$$

e na forma matricial:

Estas equações serão utilizadas para resolução dos modelos no estudo de caso.

4.4 Árvore de falhas

A árvore de falhas [8] é uma ferramenta utilizada para representação gráfica de uma estrutura lógica que relaciona um evento indesejado de um sistema, denominado evento de topo, com eventos que combinados o provocam. Estes eventos são chamados de eventos primários e suas identificações são realizadas partindo-se do evento topo e das causas que poderiam levar a este evento topo indesejável. O mesmo procedimento é repetido para cada uma das causas que conduziram ao evento topo e assim recursivamente para a causa das causas, até identificar-se os eventos primários.

A análise de uma árvore de falhas pode assumir duas formas:

- **Análise qualitativa** - quando o objetivo é construir uma árvore de falhas logicamente equivalente em termos de combinações de eventos primários. São levantadas as causas que geram o evento topo crítico até se chegar aos eventos primários. Cada combinação será um "*cut-set*" mínimo de modos de falha constituindo um conjunto de eventos cuja ocorrência em seqüência causa o evento topo.

- **Análise quantitativa** - determina a probabilidade de ocorrência do evento topo em função das probabilidades de ocorrência dos eventos primários.

A representação gráfica de uma árvore de falhas é realizada através de símbolos lógicos, descritos na fig. 21. A fig. 22 ilustra uma árvore de falhas de um sistema genérico.

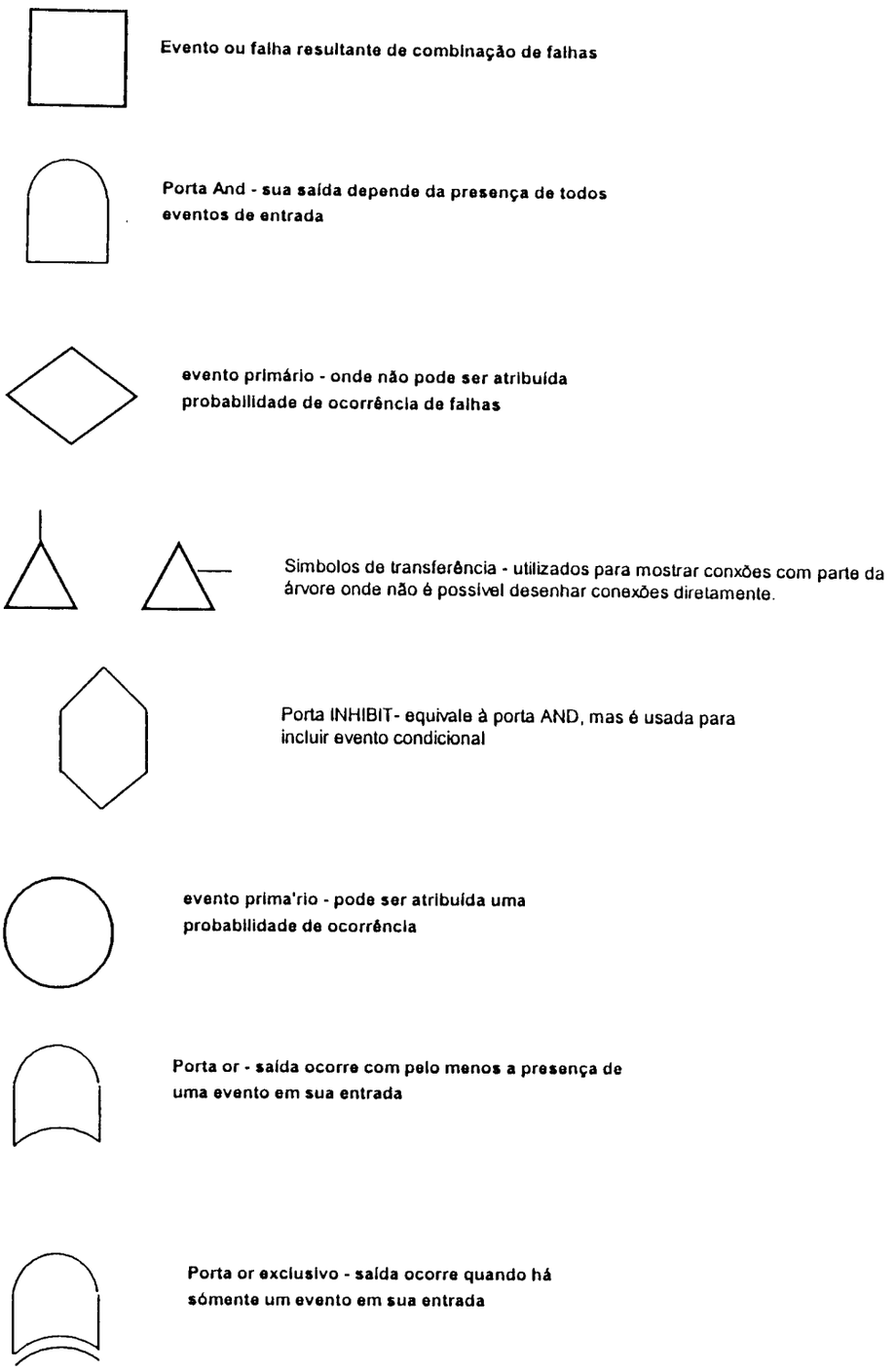


Fig. 21 - Simbologia para árvore de falhas

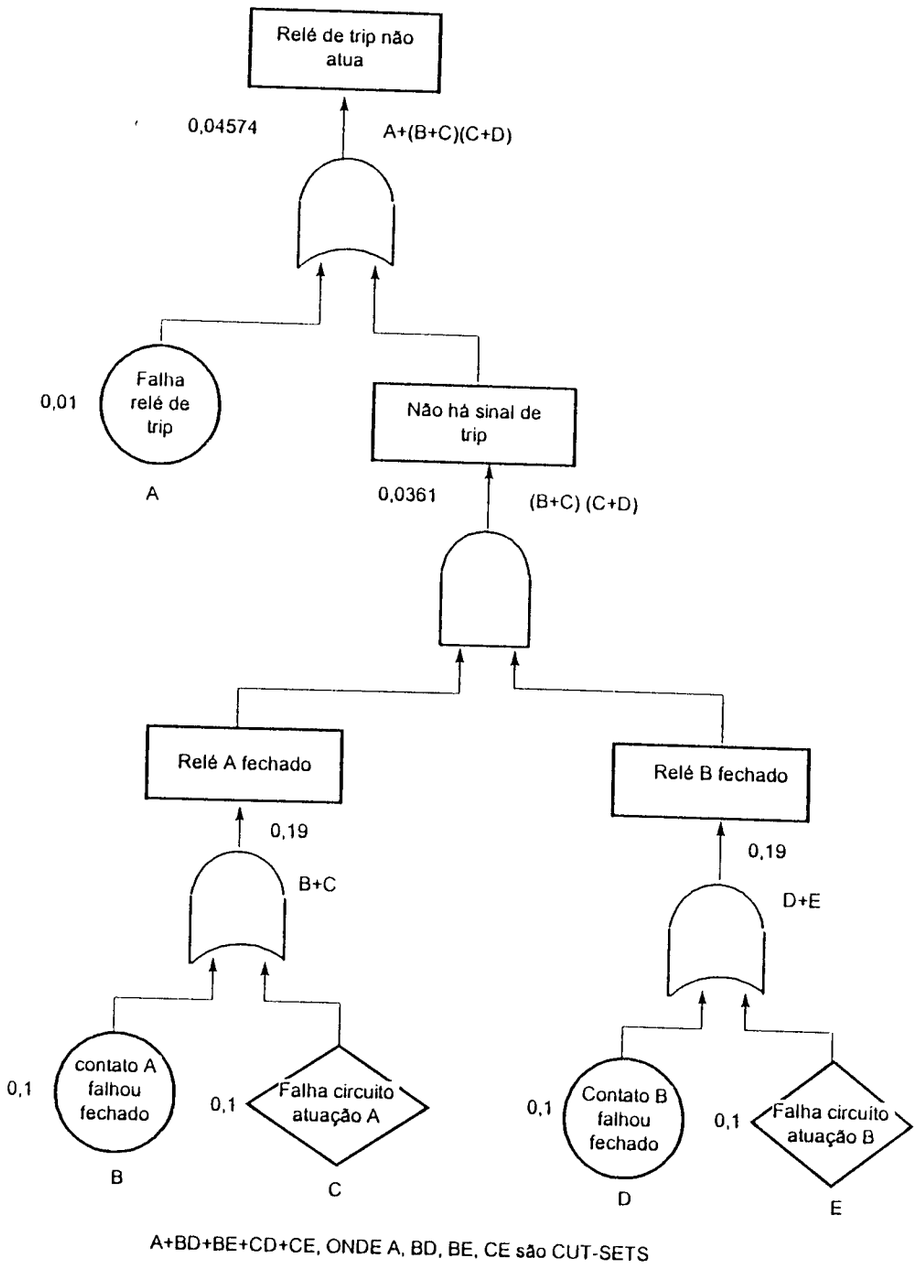


Fig. 22 - Exemplo de FTA: falha de atuação do relé de desligamento (*trip*).

4.5 Análise de Modos de Falhas e seus Efeitos (FMEA).

O objetivo da FMEA é a identificação dos pontos fracos do sistema no nível de componentes e topologias de circuitos. Para aplicações que envolvem segurança utiliza-se o termo FMECA *(failure mode effects and criticality analysis)* com o objetivo de identificar falhas que poderiam levar o sistema a um estado não seguro. Trata-se de uma avaliação funcional, verificando quais os efeitos que os modos de falhas de um componente, causam para o sistema, visando-se principalmente as condições de restrição. Esse tipo de análise procura determinar as causas relacionadas por falhas simples de componentes. isto é, sem combinação de falhas de outros componentes.

Definidos os estados de restrição de um determinado circuito ou módulo, analisa-se os modos de falhas possíveis de cada componente e seus efeitos para o sistema no aspecto global ou local.

As falhas são classificadas de acordo com o seu efeito e como o sistema reage em sua presença. Em geral definem-se quatro classes de falhas: monitoradas, detectáveis, não detectáveis e críticas.

- **monitoradas** - levam o sistema ao estado de intervenção quase de imediato. São verificadas por autotestes e independem do estado operacional.

- **detectáveis** - levam o sistema ao estado de intervenção dentro de um intervalo de tempo ou levam o sistema a um estado de degradação perceptível.

- **não detectáveis** - falhas que não são percebidas em condições normais, mas que deixam o sistema menos robusto, por exemplo, um supressor de transiente que ao se danificar em aberto, não afeta a operação do sistema, mas deixa-o sujeito a falhas.

- **críticas** - não possuem monitoração ou mecanismos de detecção e levam o sistema para a condição não segura. É o objeto da análise de segurança verificar a sua existência. Todas as falhas não seguras devem ser quantificadas para determinação da taxa de falhas críticas.

Do ponto de vista prático o FMEA faz uma abordagem de análise de modo *"botton-up"* e procura demonstrar que o equipamento apresenta comportamento seguro, quando submetido a falha simples. O trabalho também procura detectar todas as falhas simples não detectáveis que serão o ponto de partida para análise de falhas múltiplas. Recomenda-se o uso de bancos de dados, visando eficiência na verificação de falhas críticas, não detectáveis, etc.

Ilustra-se como exemplo, os modos de falha de um transistor: *Base aberta, coletor aberto, emissor aberto, curto de emissor com coletor, curto de emissor com base, curto coletor com base, aumento e diminuição de* β.

5. DIRETRIZES PARA O PROJETO DE SISTEMAS DE PROTEÇÃO.

As seguintes fases de projeto, fazem parte das atividades relacionadas com a confiabilidade e segurança no desenvolvimento de sistemas de proteção de reatores. A metodologia descrita é baseada nas referências [4], [5], [6], [8], [16], [27], [28], e na experiência adquirida em projetos de natureza semelhante desenvolvidos no Brasil. O projeto de um sistema de proteção pode ser dividido em três fases principais: Especificação de Sistema, Projeto Básico e Projeto de Detalhamento.

5.1 Especificação do sistema

Nesta fase são definidas as funções e restrições do Sistema de Proteção em relação as necessidades da planta.

As atividades relacionadas à confiabilidade e segurança devem:

1. Utilizar os valores de confiabilidade, disponibilidade e segurança necessários obtidos na análise de confiabilidade e segurança das instalações e considerando-se o sistema de proteção como um subsistema da planta. Podem ser utilizados como índices o MTTUF, MTBF, MTTR, requisitos de manutenibilidade e a disponibilidade estacionária em sistemas tolerantes a falhas.

2. Determinar os requisitos de segurança e confiabilidade, específicos do projeto. Limitar a velocidade máxima de retirada de barras de controle, por exemplo, é um requisito que deve constar da especificação do sistema de proteção.

3. Especificar todos os tempos envolvidos tais como, tempo de missão, intervalos entre manutenções preventivas, tempos médios para correção de falhas e etc.

4. Especificar todos os modos de operação e níveis de degradação aceitáveis.

Esses dados são imprescindíveis para o desenvolvimento das fases seguintes.

Observe-se que nesta fase do projeto, nenhum requisito específico de *"hardware"* ou *"software"* é apresentado. As especificações devem se limitar ao comportamento do sistema e a sua performance.

5.2 *Fase de Projeto Básico.*

Esta fase define a arquitetura e os módulos básicos do sistema de proteção. Para atender os requisitos, índices e modos de operação definidos na fase de especificação, as seguintes atividades deverão ser cumpridas:

a) Definição da arquitetura.

Para definição da arquitetura do sistema propõe-se:

- Avaliações de diferentes configurações de arquiteturas de sistema e plataformas de *"hardware"* e *"software"* visando determinar viabilidade, características e limitações.
- Definição da arquitetura de *"hardware"* do sistema de proteção com redundâncias se for o caso, e dos blocos funcionais que a compõem.
- Identificar as funções de segurança específicas para cada bloco funcional da arquitetura.
- Atribuir para cada modo de falha de cada bloco de *"hardware"* uma taxa de falhas ou uma função de confiabilidade, constante ou dependente do tempo, ou do modo de operação. Esses parâmetros devem ser estabelecidos a partir de experiência anterior com módulos semelhantes, de dados fornecidos por normas ou de referências confiáveis.

b) Modelagem do arranjo da arquitetura.

Este item tem por objetivo validar a arquitetura escolhida através da modelagem da confiabilidade e segurança do arranjo.

Os dados a serem considerados na determinação e análise do arranjo são os atribuídos aos módulos básicos que irão compor os blocos funcionais [4].

Dois tipos de modelagem são sugeridos nesta fase, de acordo com a aplicação:

- Arranjos não reparáveis.
- Arranjos reparáveis, com taxas de manutenção definidas.

Deverão ser considerados os intervalos de verificações periódicas e o índice de cobertura destas verificações.

O índice de segurança, MTTUF, deve ser comprovado na análise do arranjo de *"hardware"*. Os sinais trocados entre os blocos básicos, devem estar definidos, e estes sinais devem englobar variáveis de controle de processo, comunicação, alarmes e diagnósticos.

Pode ser realizada uma avaliação de FMECA em termos de blocos básicos, considerando-se topologias de circuitos adequados em termos de segurança.

Os blocos básicos são usualmente identificados como porções não redundantes para análise de confiabilidade. Esses blocos básicos devem ser unidades funcionais ou físicas bem definidas (memória, microcomputador, placa eletrônica, gaveta com cartões completa constituindo canal não redundante etc.).

Usualmente para os blocos caracterizados como não redundantes, qualquer modo de falha em cada um de seus componentes faz com que o bloco passe ao estado não operacional. Esta postura conservadora pode ser modificada, quando existir uma intenção explícita de introdução de redundância de componentes ou placas.

c) Qualidade do "*software*".

Os métodos tradicionais que avaliam a confiabilidade e a segurança de sistemas analógicos, reconhecidamente não são aplicáveis na avaliação da qualidade de sistemas digitais. O processo de engenharia de confiabilidade e segurança em sistemas computadorizados, requer o cumprimento de atividades (algumas das quais descritas a seguir), durante todo o seu ciclo de vida. Neste caso, as mesmas devem ser estruturadas com o objetivo de

obtenção de qualidade da especificação e qualidade do projeto. Por exemplo, as atividades que compreendem as fases iniciais do ciclo de vida do *"software"* [27]:

- Plano de gestão.
- Plano de desenvolvimento.
- Plano de instalação
- Plano de manutenção
- Plano de treinamento
- Plano de verificação e validação
- Especificação de requisitos de *"software"*
- Requisitos de análise de segurança.
- Requisitos de verificação e validação

5.3 Fase de detalhamento.

A fase de detalhamento caracteriza-se pelo projeto de implementação do sistema de proteção.

Assim, todos os módulos básicos de *"hardware"* devem ser obtidos através de desenvolvimento próprio e ou por aquisições no mercado. Todos os índices já foram atribuídos, as restrições conhecidas e o arranjo da arquitetura do sistema definido.

A implementação deve considerar: as configurações de circuitos; o arranjo físico dos componentes; a escolha dos componentes, arranjos de *"lay-out"* nas placas e nas gavetas, sendo que o projeto deve ser desenvolvido tendo-se em mente sempre as restrições de falha não segura.

Os projetistas devem ter a percepção sobre o que está sendo coberto em termos de detecção de falhas e o que estão deixando de cobrir com relação às restrições de segurança, particular de cada módulo básico. Isto se faz necessário para a determinação de índices de cobertura.

É necessário a figura de um gerente integrador, ou de uma ferramenta de integração entre os projetistas de "*hardware*" com projetistas de "*software*". O elemento integrador deve agir de modo que ambos os projetistas tenham o conhecimento completo dos diagnósticos, índices de cobertura e tratamento de falhas[5], [6].

São necessárias reuniões periódicas de "revisão de projeto" com grupos externos e projetistas, para o refinamento de idéias e identificação de problemas que possam ter passado despercebidos.

O mesmo procedimento se aplica quando forem adquiridas placas eletrônicas. O projeto deve ser conhecido, e os circuitos analisados pelo grupo responsável pela integração dos módulos básicos.

5.4 Análise de Confiabilidade e Segurança.

5.4.1 Avaliação de Confiabilidade do "*Hardware*".

Para se evitar erros sistemáticos de projeto, é necessária a criação de um grupo independente para análise de confiabilidade e segurança. Esse grupo terá acesso a todos os dados de projeto, e visará encontrar desvios que passaram despercebidos pelos projetistas e deverá também comprovar os valores-metas de projeto.

Para análise de confiabilidade, o ponto de partida são os módulos básicos. A análise deverá ser efetuada da seguinte forma:

Obter taxas de falha para todos os componentes de cada módulo básico, utilizando-se fontes reconhecidas. Sugere-se como referência a norma MIL-HDBK 217F Notice 2 [36]. Em geral considera-se o arranjo série de todos os componentes, onde a falha de um acarreta a indisponibilidade do módulo básico.

No caso de utilização da MIL HDBK 217F Notice 2, o método mais indicado para cada módulo de *"hardware"* é o cálculo dos índices de confiabilidade pelo método de análise de estressores, "*Stress Analysis*", que define de forma mais completa a taxa de falhas de cada componente, considerando a solicitação física a que o mesmo está sendo submetido na aplicação.

Calcula-se a taxa de falhas e o índice de confiabilidade de cada módulo básico obtendo-se os valores quantificados para o projeto.

Os índices determinados devem então substituir as taxas atribuídas para *"hardware"* na fase do projeto básico, e os índices globais do Sistema devem ser recalculados.

Caso os valores obtidos não atendam às especificações, serão necessários ajustes no projeto dos módulos ou da arquitetura.

5.4.2 Modelagem da arquitetura

A avaliação de confiabilidade do modelo da arquitetura, no caso de arranjo reparável, é efetuada por *cadeias de Markov*. O modelo de transição de estados de falha deve ser ajustado de acordo com as taxas de falhas λ obtidas no calculo de confiabilidade de cada módulo e taxas de reparos μ atribuídas segundo dados do projeto. Estas taxas serão correspondentes a probabilidades de transição de um determinado estado para outro no modelo. Os valores encontrados deverão atender a especificação.

Para arranjos sem reparo, a arquitetura deverá ser avaliada por combinações série e paralelo de funções confiabilidade dos blocos básicos.

Os valores determinados devem então substituir as taxas atribuídas para *"hardware"* na fase do projeto básico, e os valores globais de confiabilidade do sistema devem ser recalculados.

Caso os valores obtidos não atendam as especificações, serão necessários ajustes no projeto dos módulos ou da arquitetura.

Outras fontes podem ser utilizadas, para obtenção das taxas de falhas de componentes, uma fonte interessante é a "*Bellcore - Reliability Prediction Procedure for Electronic Equipment*" [38], que acrescenta um refinamento da existência de procedimentos de "*Burn-in*" na determinação das taxas de falhas de componentes.

O uso de *cadeias de Markov* para análise de arquiteturas possue restrições quanto ao número de estados de um sistema. Esta ferramenta permite contabilizar as probabilidades de ocupação de estados do sistema considerando falhas e reparos "on-line". Esta técnica permite a obtenção de parâmetros como confiabilidade R(t), disponibilidade A(t) e valores de MTTF e MTTUF entre outros. Para sistemas que apresentam muitos estados distintos, o uso de *cadeias de Markov* torna-se difícil devido ao número de equações diferenciais geradas, exigindo sofisticados programas computacionais para sua resolução. Procura-se, sempre que possível, simplificar arranjos de modo de viabilizar a utilização da técnica.

5.4.3 Avaliação de segurança da arquitetura.

Adota-se duas abordagens para análise de segurança da arquitetura de um sistema: uma visão "top-down", através de árvores de falhas e uma visão "botton-up" através de FMECA.

A análise de segurança de uma arquitetura de *"hardware"* deve ser iniciada sempre através da identificação dos eventos topos que causariam o estado inseguro para o sistema [5], [8],[28].

De posse dos requisitos básicos de segurança deverão ser identificados os eventos primários de falhas que combinados resultariam no evento topo de condição não segura.

O método propõe a realização de uma análise desta arquitetura por FTA onde são estabelecidos os eventos topos de falhas críticas e a partir desta verificação identificar os eventos primários e suas origens, que resultariam nestes eventos topos indesejáveis. Este procedimento pode ser realizado tanto no aspecto de arquitetura quanto ao de canal

redundante. Esta visão "top-down", identifica requisitos de projeto para módulos básicos, componentes da arquitetura.

Para os módulos básicos, quando dispõe-se de dados de projeto, recomenda-se uma exaustiva análise de FMECA para detecção de falhas simples de componentes que causariam situações de não seguras para o módulo básico, Estas falhas deverão ser classificadas conforme o seu grau de importância (monitoradas, detectáveis, não detectáveis e críticas). O objetivo é determinar a existência de falhas simples críticas e suas probabilidades de ocorrências. Recomenda-se também um FTA para falhas combinadas em componentes e circuitos comuns dependentes entre si, ou que possuem dependência de função sobre eventos topos que causariam situações não seguras. O objetivo será determinar os pontos fracos do módulo em termos de falhas não seguras e obter a contabilização de todas estas falhas para determinação da taxa de falhas não seguras total.

De posse dos dados de taxa de falha não segura de cada módulo do sistema deve-se calcular parâmetros de confiabilidade como o MTTUF e a confiabilidade segura S(t), para a arquitetura considerando-se todas as redundâncias e votações através de interpretações dos resultados obtidos da modelagem de *cadeias de Markov* para os estados operacionais do sistema. Considera-se as classes de falhas apontadas pelo FMECA, tempos médios de detecção através de diagnósticos, taxas de falhas, taxas de reparos, tempos de missão etc. A probabilidade de ocorrência do estado absorvedor e o caminho percorrido entre o estado operacional pleno sem falhas, caracterizam a chance de insegurança.

O valor obtido de MTTUF deve maior ou igual ao especificado no projeto de concepção.

É comum a utilização do conceito MTBUF, porém verifica-se que em sistemas de proteção de reatores este conceito não é adequado uma vez que a ocorrência de falha não segura pode resultar em um acidente onde o sistema e a planta não sobreviveriam. Logo o termo MTTUF expressa um índice da expectativa média de tempo para falhar, caracterizada por um estado sem volta, mais realista que o termo MTBUF.

5.4.4 Avaliação de Confiabilidade e Segurança do *Software*

Atualmente, não se dispõe de procedimentos ou ferramentas consagradas que possam mensurar níveis de qualidade e segurança de um *"software"* visando a qualificação.

Um *"software"* não apresenta falhas se estiver atendendo uma especificação adequada. Partindo-se deste princípio, verifica-se que um meio de garantir a qualidade do *"software"* é o desenvolvimento criterioso do projeto durante todo o seu ciclo de vida e um acompanhamento minucioso da operação do equipamento, durante o período de qualificação.

As técnicas orientadas ao objeto são consideradas como uma alternativa à técnica estruturada, apesar de serem mais trabalhosas e menos conhecidas para aplicação em sistemas de controle. Acredita-se que são mais fáceis de rastrear e corrigir erros devido ao encapsulamento de dados dentro dos objetos. Isso, em termos práticos significa restringir a ação da correção ou da modificação em apenas uma parte do *"software"*. Logo, a modificação geralmente não afeta outras partes.

A princípio, os seguintes itens devem ser considerados no desenvolvimento de *"software"* para aplicações críticas.

1) Projeto detalhado, documentado e acompanhado durante todas as fases de desenvolvimento.

2) Análise de segurança do código das partes de *"software"* relacionadas com segurança e uma análise de interferência dessas partes com outras não relacionadas com segurança, a qual deve prever:

- mapeamento dos requisitos nos módulos de *"software"* relacionando a especificação á implementação;

- separação das partes relacionadas com segurança das partes não relacionadas;

- inspeção das partes relacionadas à segurança segundo uma lista de verificação pré-estipulada, relativas ao fluxo de dados e ao fluxo de controle, segundo critérios funcionais e estruturais;

- inspeção de partes não relacionadas com a segurança, segundo uma lista de verificações pré-estipulada, visando identificar as interferências desses módulos sobre os módulos relacionados á segurança;

- realização de "*Walk Through*", segundo procedimento padronizado, das partes relacionadas entre si, mas identificadas como interferentes na inspeção.

Na fase de validação, instalação e operação, as principais atividades relacionadas à análise de confiabilidade e segurança são o acompanhamento de falhas de manutenção e o levantamento de erros de *"software"*.

Os dados coletados servirão para ajustes no índices de confiabilidade de *"hardware"* calculados e para qualificação do *"software"* por tempo de operação sem o aparecimento de erros.

Um aspecto importante é a qualidade de documentação gerada. Um dos processos para se avaliar a qualidade de um *"software"* é avaliar a qualidade de sua documentação de projeto, onde todos os requisitos podem ser verificados e todos os procedimentos validados. Porém qualidade não significa quantidade, pois conforme [7], conclusões importantes foram retiradas do processo de licenciamento de uma planta CANDU em Ontario Hydro no Canadá. O autor expõe que *"A produção massiva de documentação de "software" não deve tornar-se um fim em si próprio. Idealmente, a documentação deve ser axiomaticamente produzida como uma parte inerente do projeto e processo de verificação. Deve ser precisa e clara o bastante para habilitar revisões efetivas por todos diferentes grupos de interesse no sistema"*. Com isso conclui-se que os documentos devem ser criados somente se forem relevantes para o projeto.

Quanto ao aspecto quantitativo, existem vários modelos de crescimento de confiabilidade disponíveis que se propõem a avaliar a confiabilidade de um *"software"* em

várias fases de sua vida. Estão disponíveis modelos matemáticos para as fases de: desenvolvimento, validação, vida operacional e manutenção. Entretanto, para qualificação, não bastam ao órgão licenciador, servem apenas como modelos experimentais que auxiliam no seu ciclo de vida e buscam solidificar-se como ferramenta de projeto durante as atividades de testes [3].

Convém salientar, que em sistemas críticos, o "*hardware*" computacional deve ser considerado durante o cumprimento de requisitos de segurança pelo "*software*".

Duas fontes para balizar o desenvolvimento de "*software*" podem ser as normas IEC-880 de 1986 [33] e mais recentemente a IEEE 7-4.3.2 de 1993 [34] e como auxílio as referências [27] e [32].

5.4.5 Ilustração do método.

A fig. 23 ilustra o método proposto apresentando um esquema básico para a avaliação da confiabilidade e segurança de uma arquitetura genérica com redundância 1/2, considerando cada canal redundante como um módulo básico, assim qualquer falha de componente coloca este módulo em falha.

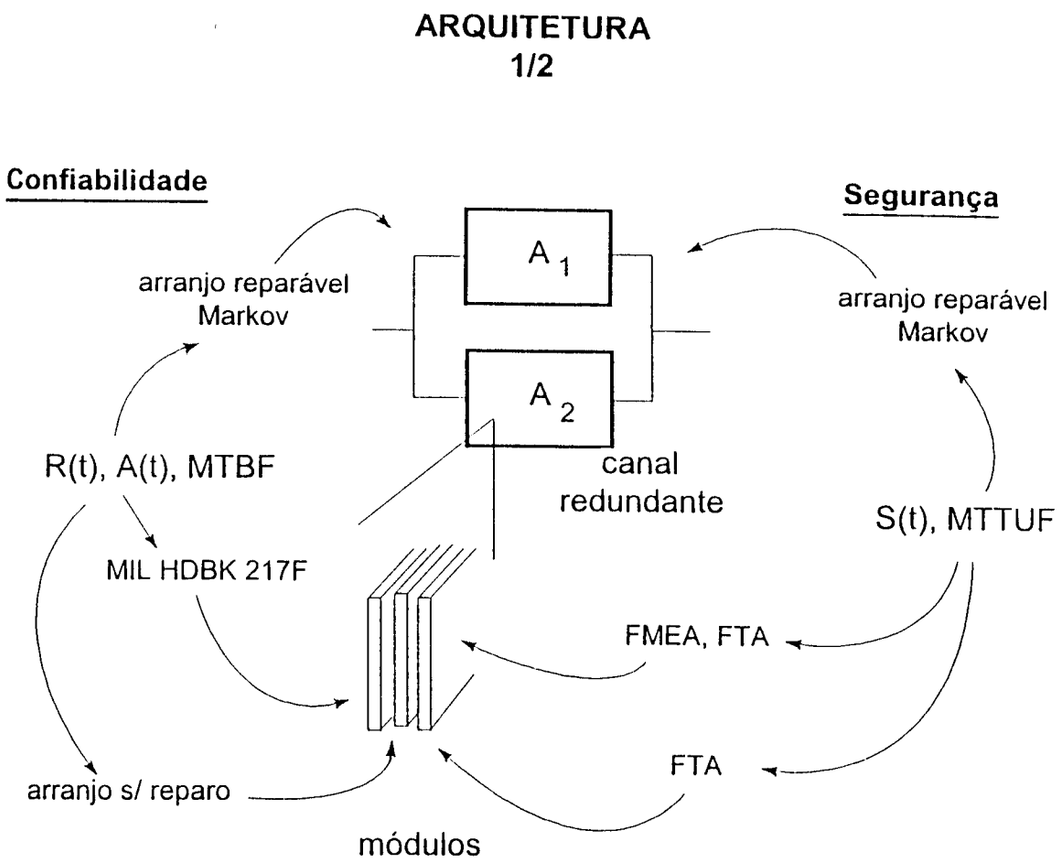


Fig. 23 - Ilustração do método para análise de confiabilidade e segurança

6. ESTUDO DE CASO.

Utilizando-se o método proposto e as ferramentas e técnicas apresentadas, foi realizada uma análise de confiabilidade e segurança da arquitetura de *"hardware"* de um sistema de proteção para reatores nucleares franceses. Trata-se do **SPIN** *(Digital Integrated Protection System)*, fig. 23, que executa as tarefas de proteção dos reatores PWR (*pressure water reactor*), classe 1300 MWe e 1500 MWe. O SPIN foi desenvolvido pela Merlin-Gerin [24] em conjunto com a *French Atomic Energy Commission* (CEA), Framatome e *French Electricity Board* (EDF). Devido a salvaguardas internacionais e por ser propriedade industrial, não foi possível se obter dados de projeto para a realização de uma análise realista. Portanto, através da informação de catálogos do fabricante e de artigos publicados, procurou-se analisar o SPIN até onde os dados obtidos permitiram.

Do ponto de vista de confiabilidade e segurança do *"software"*, assume-se que o mesmo é correto, porque não existem dados de projeto suficientes para se avaliar a sua qualidade.

6.1 Descrição Geral do SPIN

O SPIN é um sistema digital computadorizado, utilizado para execução de funções de desligamento de emergência de reatores nucleares de potência. O SPIN é associado a equipamentos de medição das grandezas físicas do processo para cumprimento de suas ações de proteção e segurança, tais como:

- Indicadores da posição de barras de controle e proteção do reator;
- sensores termodinâmicos da instrumentação de processo; e
- detectores de neutrons.

O SPIN executa também as seguintes funções de proteção e segurança: isolamento de circuitos, disparo de "*spray*" da contenção, acionamento de sistemas de água de resfriamento de emergência etc.

Toda filosofia de operação do SPIN é baseada no uso de técnicas de circuitos digitais de segurança com redundâncias e votação, acrescida da realização de testes periódicos de canais redundantes sem interrupção de operação. Sua configuração padrão está em redundância 2/4 para condições de desligamento, sendo que quando um dos canais está em teste periódico, o sistema opera em redundância 2/3. O mecanismo de verificação "on line" permite que cada canal seja isolado e testado sob várias condições operacionais, inclusive com simulação de condições de desligamento. Nessas condições, a arquitetura demonstra que não há degradação da capacidade de desligamento do reator.

O SPIN só atua na proteção do Reator, sendo que os sinais coletados por ele fazem parte do processo nuclear. O controle e ações de segurança de uma unidade de 1300 Mwe, que utiliza esse equipamento, é de responsabilidade do sistema CONTROBLOC, composto por controladores lógicos programáveis com funções Classe 1E {veja apêndice I}, e funções não ligadas a segurança. Os "*loops*" de controle dessa unidade, que não tem grau de importância de segurança na planta, são efetuados por controladores de "*loop*" fechado, de fornecimento Bailey. A fig. 24 mostra a arquitetura do controle e proteção das plantas 1300 Mwe.

A abordagem de segurança, é principalmente baseada no exame da natureza e aplicação de métodos e de requisitos associados com equipamentos e sistemas projetados e construídos mediante classificação 1E. No SPIN, os limites de MTTUF atendem a norma IEC 231-A, [39].

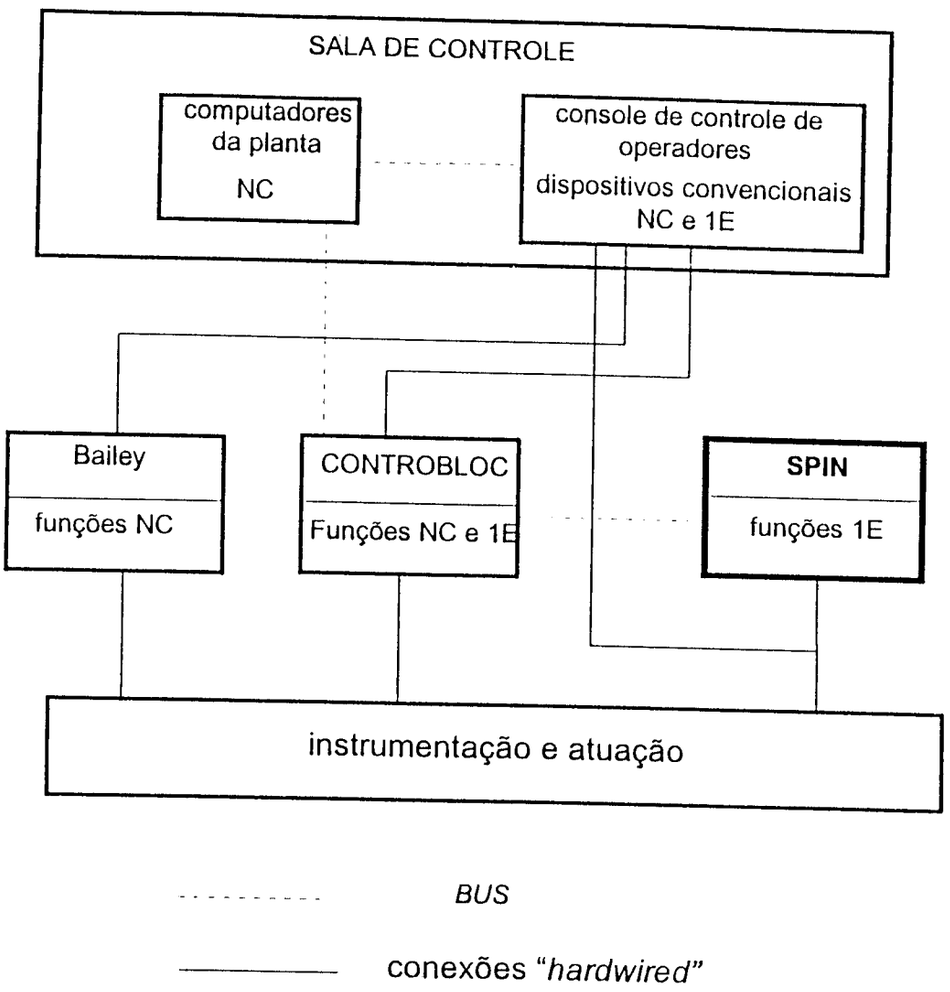


Fig. 24 - Diagrama do sistema de controle de planta nuclear

6.2 *Descrição da arquitetura de "hardware" do SPIN*

6.2.1 Subsistemas componentes do SPIN

O SPIN é composto dos seguintes subsistemas digitais computadorizados, esquematizados na fig. 25:

- UATP (*acquisition and processing unit for protection*), sendo cada módulo composto por cartões eletrônicos digitais de aquisição de dados de outros sistemas e de sensores. O SPIN possui 4 UATPs para operação em redundância 2/4 ou 2/3 quando uma estiver em teste.

- ULS (*logic safeguard unit*), subsistema que controla as ações de segurança e desligamento do reator. O SPIN possui redundância 2 em ações de segurança para este subsistema. Cada ULS é composta de quatro módulos UTP, conforme ilustra a fig. 27.

Associado ao SPIN, embora não faça parte de sua operação, estão os subsistemas de diagnósticos que executarão testes periódicos para verificação de integridade nas unidades UATP e ULS. Estas unidades de testes são as duas UTLP para o subsistema de aquisição UATP e as duas UTLS para o subsistema de ação de segurança ULS. Além disso, existem duas unidades de transferência de dados UTD, para a sala de controle e para as duas unidades de diagnósticos UD, que fazem a interface com o operador.

6.2.2 Redes de Proteção

Os subsistemas UATP e ULS são interligados por 2 (duas) redes locais de proteção, quadruplicadas, em fibra ótica e responsáveis pelo "link" principal de segurança. Estas redes são de fabricação Merlin Gerin, denominadas *Nervia,* com protocolo de acesso determinístico, com cada estação carregada com gerenciador de protocolo implementando camadas físicas, "*link*" de dados e aplicações do modelo OSI. Segundo informações do fornecedor, a rede *Nervia* obteve classificação de segurança e foi desenvolvida de acordo com métodos da norma IEC 880. Seu projeto considerou a máxima segurança em

transmissão de dados. Cada possível estado de falha é detectado sem causar distúrbios nas operações da rede, e não possuindo uma unidade mestre, a rede *Nervia* apresenta boa disponibilidade.

As figuras 25, 26 e 27, ilustram a conexão entre os subsistemas citados, mostrando em detalhes os aspectos de redundância.

Cada rede de proteção é também conectada às unidades de transferência de informações (UTD), para a sala de controle, conforme ilustra a fig. 25.

6.2.3 Redes de sinalização

Cada UTP é conectada a duas redes de sinalização, uma para a UTD-A e outra para o UTD-B, conforme mostra a fig. 27. Estas redes também habilitam a inibição do canal para testes de dois UTPs correspondentes a meio ULS. Isto resulta em verificar a atuação do canal simulando desligamento.

6.2.4 Geral

A caracterização da arquitetura de *"hardware"* do SPIN, demonstra claramente a preocupação com a segurança e disponibilidade da planta, devido a presença de várias redundâncias, tanto em processo, quanto a dispositivos de teste, também redundantes, de forma a minimizar erros de operação.

O sistema permite através de seus dispositivos testadores que seus módulos e subsistemas sejam exercitados durante a operação normal da planta, ou seja, não há interrupção de operação e não há diminuição do nível de proteção durante testes. É importante verificar que este procedimento é aplicado desde a aquisição de sinais, fig. 25, até a atuação nos módulos de acionamento de desligamento do reator.

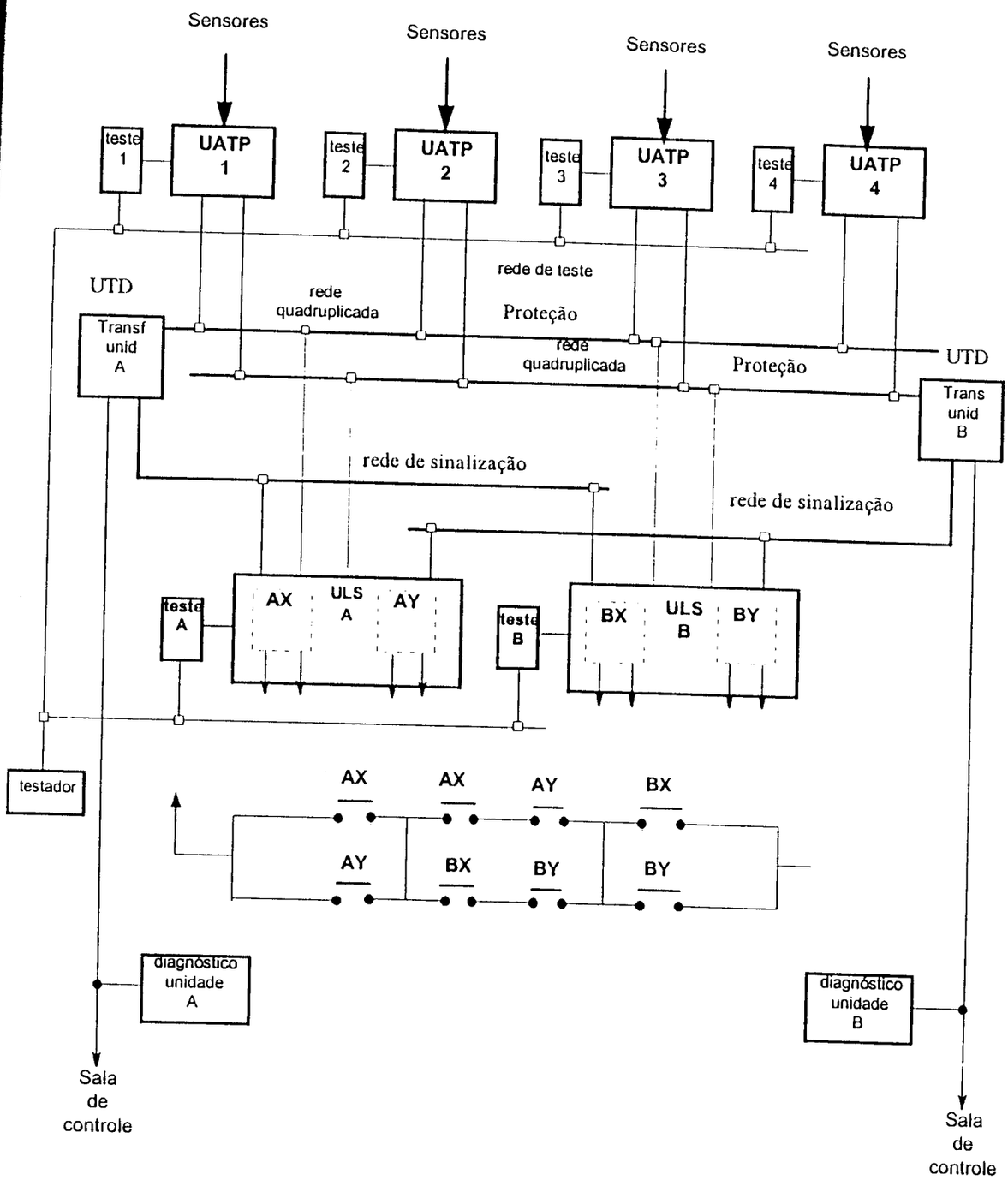


Fig. 25 - Arquitetura do SPIN

6.2.5 Descrição do UATP

Cada UATP, conforme ilustra a fig. 26, é composta dos módulos UA (2), unidade de aquisição de dados analógicos e digitais, e UF (5), unidade funcional.

Associado ao UATP existe a unidade UTLP que executa testes para diagnósticos de falhas.

Opcionalmente, a interface aceita uma entrada diretamente nas suas redes de transmissão de dados de proteção. O fabricante deixou esta possibilidade para a conexão com o sistema de indicação da posição das barras de controle e proteção do reator, de sua fabricação. Toda interface possui isolação galvânica e independência.

Todo o processo de aquisição de sinais digitais e analógicos são executados pelos módulos UA, sendo que esta aquisição é realizada de forma redundante, com isolação galvânica, e com conexões "fio a fio" (*wire by wire*). Esta informação é transmitida para as unidades de processamento UF, através da rede de proteção redundante.

Nota-se uma preocupação em reduzir a probabilidade de falha não segura da UATP. Isto é observado pela aquisição redundante de informações entre os dois módulos UA, sendo que isto permite, de acordo com o fabricante, realizar testes funcionais na UA em "*on-line*".

Os módulos UF são responsáveis pelo processamento das informações coletadas, realizando várias tarefas (filtros, comparações de valores de "*threshold*", algoritmos de proteção etc.). Todas as funções são realizadas por 5 (cinco) unidades de processamento UF. Segundo informações levantadas, estas unidades de processamento não realizam votação das informações, mas transmitem na rede os dados referentes a parâmetros do processo e resultados intermediários dos algoritmos de proteção.

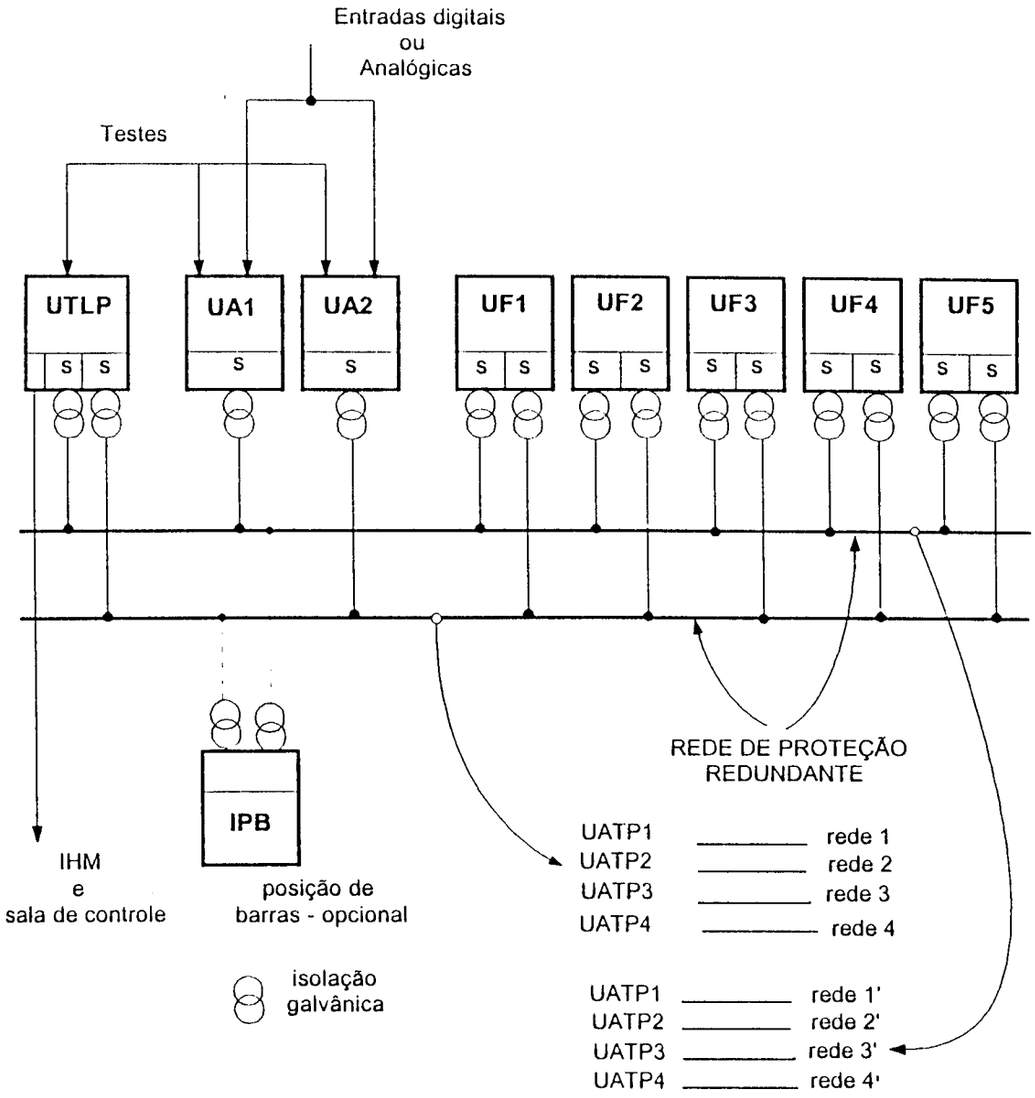


Fig. 26 - Arquitetura do subsistema UATP

6.2.6 Composição do subsistema UATP - módulos UA, UF e UTLP.

O módulo UA é composto de :

- "N" cartões eletrônicos de entradas analógicas com isolação galvânica (ANA)
- "N" cartões eletrônicos de entradas digitais isoladas galvânicamente (TOR)
- Cartão contador de pulsos "*ratemeter*".
- Um cartão de interface de comunicação com a rede com 16 bits no barramento paralelo de entrada e interface serial de saída com isolação galvânica e memória compartilhada.
- Uma fonte de alimentação.

O módulo UF é composto de:

- Um cartão CPU com dois cartões de interface com a rede de proteção
- Uma fonte de alimentação.

O módulo de teste UTLP é composto de :

- Um a dois cartões de saídas analógicas isoladas para testes de entradas do mesmo tipo (ANA).
- "N" cartões de saídas digitais isoladas para testes de entradas digitais (TOR).
- Um cartão de interface de comunicação com a rede com 16 bits no barramento paralelo de entrada e interface serial de saída com isolação galvânica e memória compartilhada.
- Um cartão de comunicação com a sala de controle e operação.

6.2.7 Descrição do ULS

Fazem parte do SPIN dois subsistemas denominados ULS, que executam as ações de segurança e de desligamento do reator. A fig. 27, exibe a arquitetura de uma ULS (existem 02). Verifica-se que sua composição consta de módulos UTPs (4), AS (2) e AU (2). Os módulos UTPs (unidades programadas de processamento de proteção), executam as ações de aquisição de dados das redes de proteção, efetuam o processamento das ações de desligamento requisitadas pelas UATPs, enviam comandos de desligamento para os módulos AU (desligamento de emergência) e comandos de atuação para os módulos AS (2) que atuam em ações de segurança. Além disso, transmitem informações para sala de controle e recebem ações de monitoração e testes através do módulo UTLS.

Observa-se que de acordo com a arquitetura, a falha de duas unidades UTP, não torna o sistema indisponível. Durante os testes periódicos, são simuladas condições de desligamento para verificação de integridade das unidades UTP; neste caso o sistema permanece ativo com sinalização de atuação dos sub-modulos UTPs em teste sem que haja desligamento do reator. Estes testes são importantes para garantia de segurança do equipamento e de certa forma a periodicidade é um dos parâmetros que garantem os valores de MTTUF.

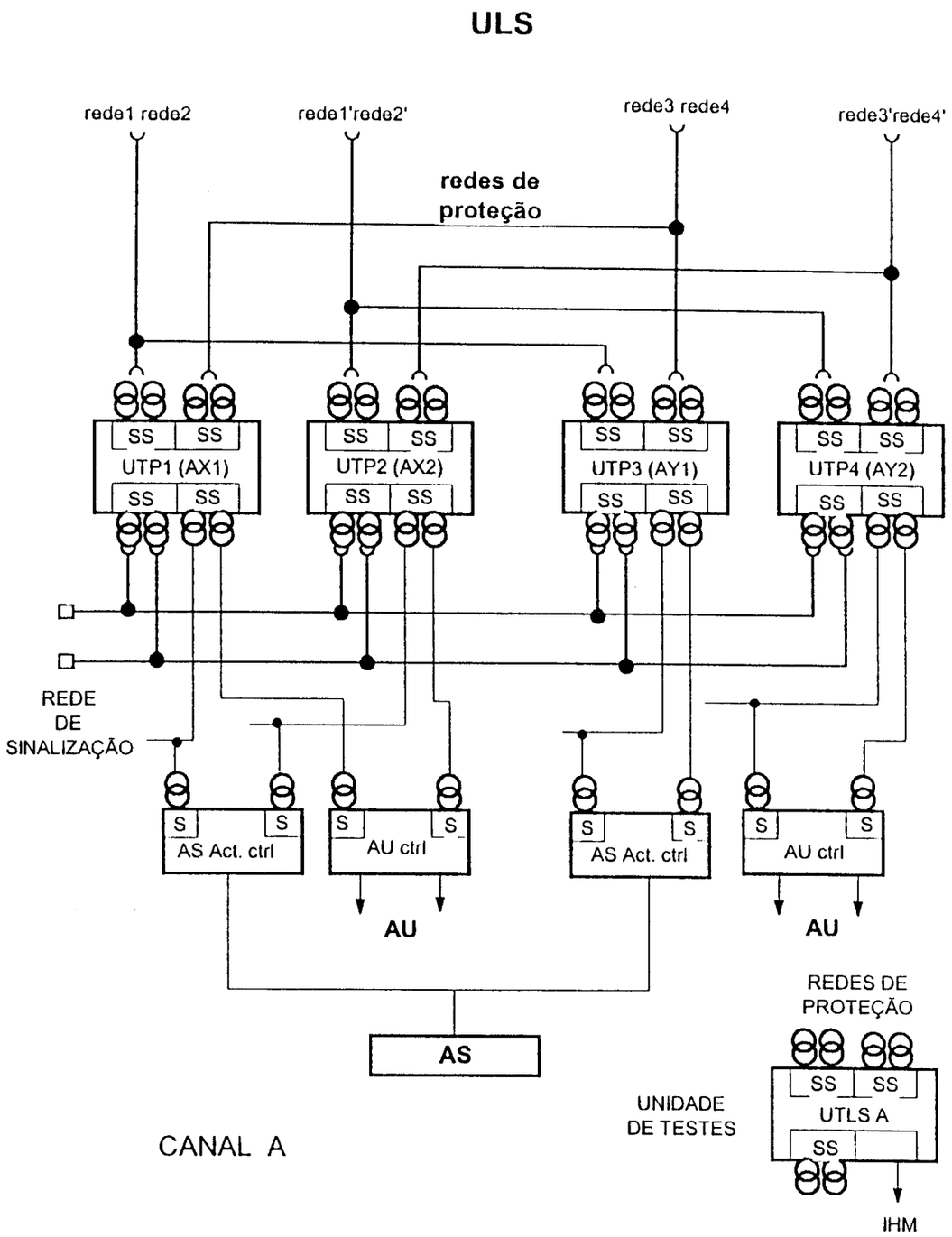


Fig. 27 - Arquitetura do subsistema ULS

6.2.8 Descrição dos módulos AU

Os módulos AU (desligamento de emergência) recebem comandos de desligamento de forma segura, ou seja, com topologia de circuitos que suportam modos de falha estáticos "0" ou "1", derivando sempre para o lado da segurança, onde atuam no desligamento do reator, em votação eletromecânica de 2/4.

Cada AU possui saídas em votação 2/2, e constituem em um total de 4 (quatro) módulos que geram duas saídas de atuação cada um, totalizando oito (8) saídas de atuação. A fig. 28, esquematiza a lógica de votação envolvida.

Uma característica importante é a disponibilidade que a topologia oferece, pois falhas simples nos AU são toleradas pelo sistema.

Os módulos AS, responsáveis pelas ações de segurança, recebem comandos de atuação pelas UATPs e executam comandos de acionamentos de dispositivos de segurança, através de relés auxiliares, podendo operar em votação 1/2. Portanto cada ULS transmite comandos de atuação de proteção de desligamento e atuação de segurança.

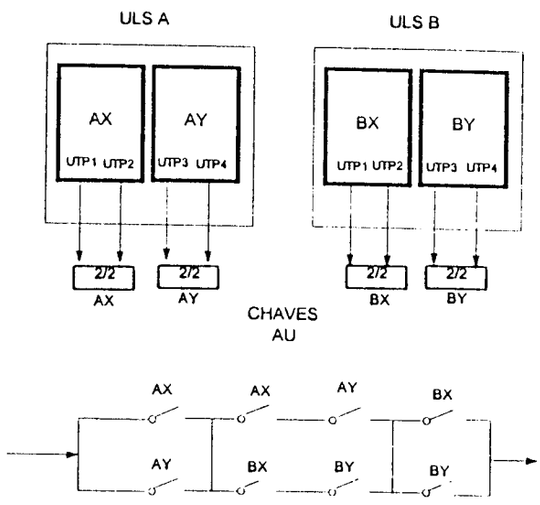


Fig. 28 - Desligamento de emergência AU.

6.3 Levantamento e determinação de requisitos de segurança da aplicação.

O SPIN possui requisito de restrição definido de modo que não exponha o reator à condição de falha não segura em quaisquer condições de operação. Este requisito constitui a meta de projeto a ser alcançada pelo sistema.

O requisito primário de segurança do SPIN é definido por:

"A probabilidade de falha de desligamento de emergência de um canal deve ser menor que 10^{-5} *falhas por ano" [24].*

Este dado foi obtido através do catálogo da MERLIN GERIN, e está de acordo com a norma IEC 231A. O fabricante considerou testes periódicos para que tal índice seja alcançado.

6.4 Determinação de eventos primários de falhas críticas através de FTA

Através de análise por árvore de falhas, determina-se qualitativamente quais os eventos primários que geram o evento topo de "*falha de desligamento de emergência*".

6.4.1 Considerações para análise FTA.

A análise é realizada na arquitetura ilustrada na fig. 25, e sua profundidade está limitada nos dados disponíveis do SPIN.

Dado que o estudo de caso tende a demonstrar mais a importância e eficácia das ferramentas, não é ponto imperativo a demonstração dos índices de segurança e confiabilidade do SPIN, e sim demonstrar que o equipamento foi projetado de acordo com esta ótica, e que sua arquitetura pode servir de exemplo para o desenvolvimento de um sistema para uso nacional, onde todos os dados de projeto estarão disponíveis para avaliação de seus parâmetros de *"dependability"*.

O objetivo desta FTA é identificar os possíveis focos de eventos primários que combinados poderiam em termos de arquitetura, gerar a condição crítica de não desligamento do reator. A combinação destes, através da lógica de árvore de falhas, resulta em uma expressão para probabilidade de ocorrência do evento topo.

A verificação visará localizar os focos de falhas críticas de forma qualitativa, e após, será realizada, através de quantificação literal, testes de hipóteses atribuindo-se valores probabilísticos para os eventos primários e verificando-se o comportamento da arquitetura, para o evento topo.

Considera-se que falhas críticas não são detectáveis por mecanismos de diagnósticos ou auto-testes, logo considera-se que não existe taxas de reparo.

Os intervalos de testes periódicos e sua duração estão distribuídos de acordo com os módulos componentes do SPIN, conforme [24]. A distribuição é a seguinte:

- Para os módulos de aquisição e processamento de sinais UATP:

UA - duração de 1/4 de hora e freqüência de 3 vezes ao ano. Neste caso a UATP não é inibida.

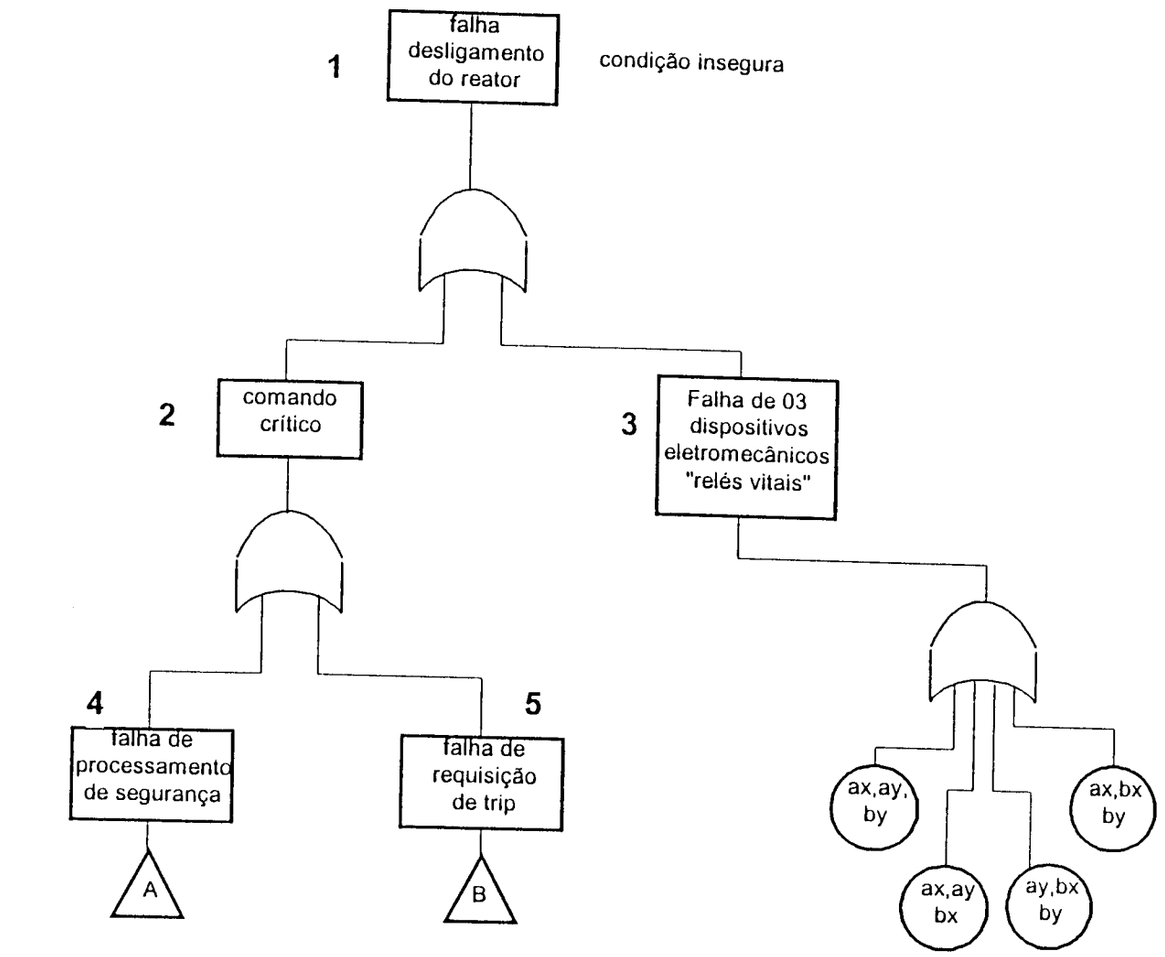
UF - duração variável com freqüência de uma vez a cada 12 a 18 meses. Nesse caso a UATP e uma rede de proteção são inibidas.

•Para os módulos de validação e atuação de proteção UTP.

UTP - duração variável com freqüência de uma vez a cada 12 a 18 meses. Para ação de desligamento AU a votação passa a ser de 2/3.

SPIN - Análise por Árvore de Falhas (folha 1)

Arquitetura redundante 2/4 // 2/3 (testes)

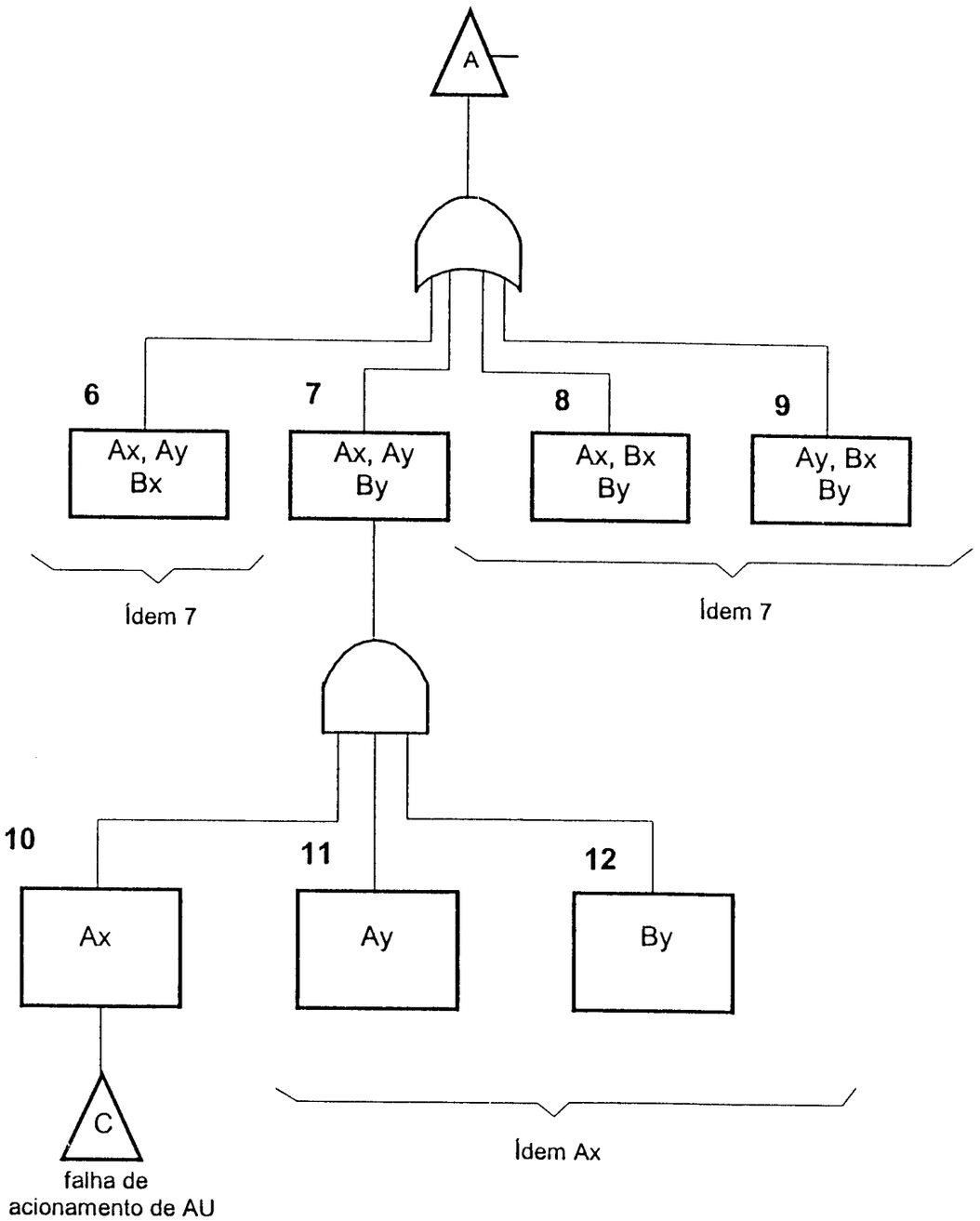


falha crítica devido eventos de falha independentes críticos e não detectáveis de módulos de processamento de segurança ULS

falha crítica causada por não requisição de trip devido a falhas de aquisição e ou processamento de sinais UATP

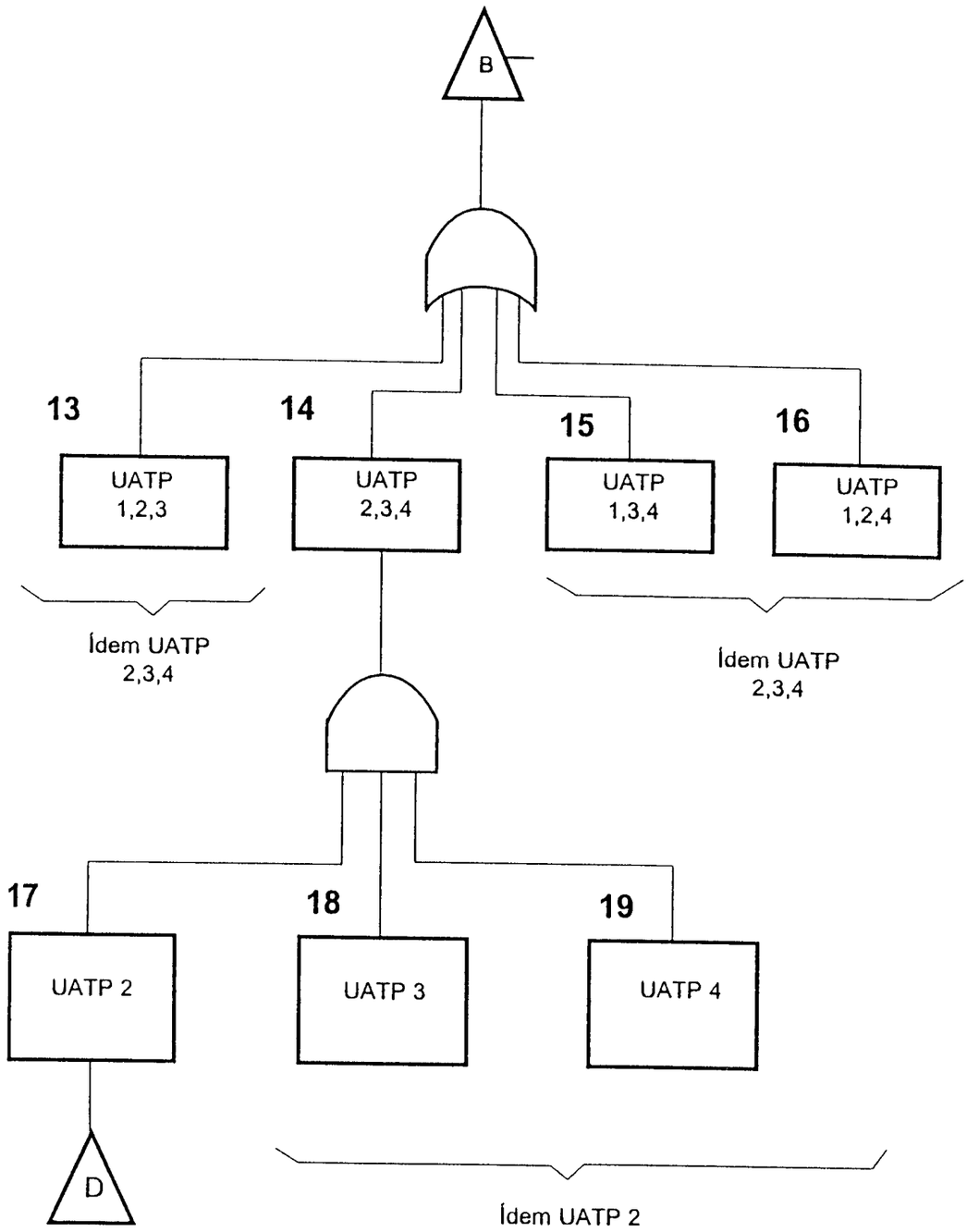
SPIN - Análise por árvore de falhas - (folha 2)

Combinações de falhas de UTP's que geram o evento topo.

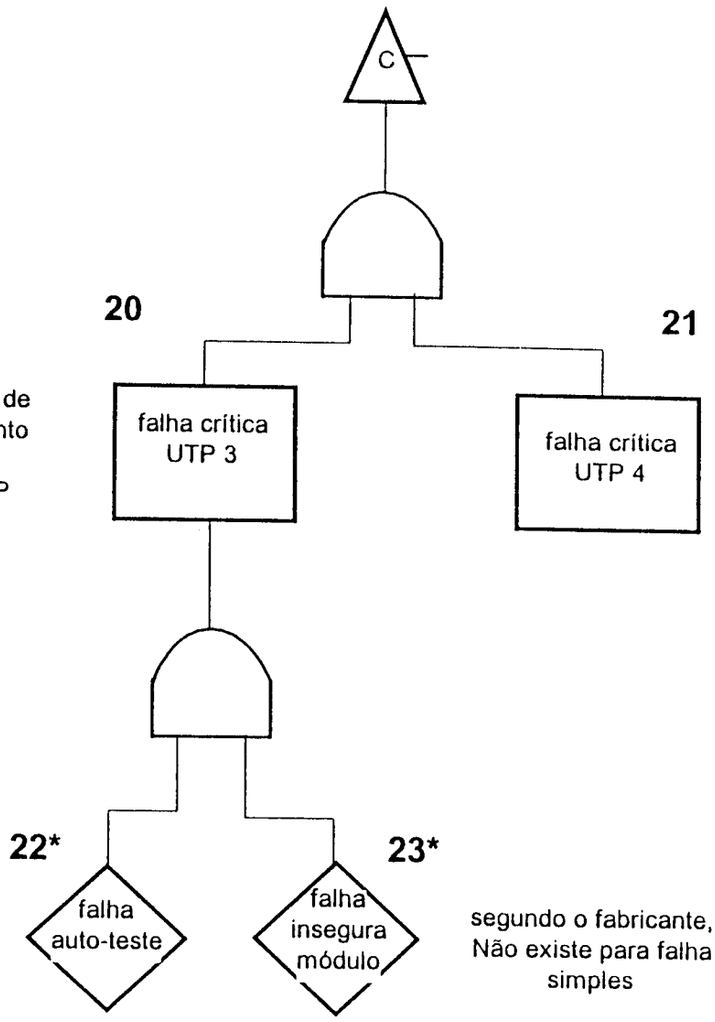


SPIN - Análise por árvore de falhas - (folha 3)

Combinações de falhas de UATP's que geram o evento topo.



SPIN - Análise por árvore de falhas - (folha 4)



Este ramo exibe a progressão de solicitação de um comando de travamento de barras causado por eventos de falha de UTP

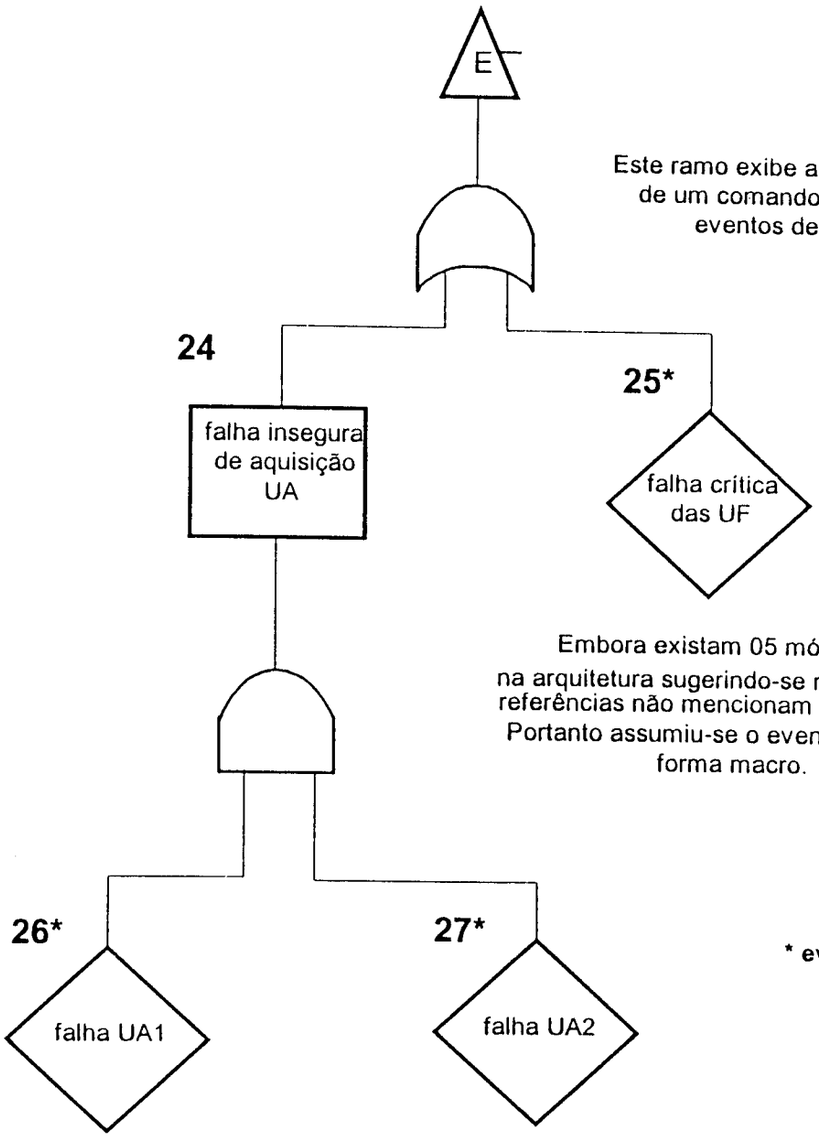
segundo o fabricante, Não existe para falha simples

evento primário de falha devido a erros de auto-teste. Pode ser causado por erros de software e/ou falha de hardware

* evento primário

SPIN - Análise por árvore de falhas - (folha 5)

Eventos críticos primários
devido a falhas não seguras nos módulos UATP



6.4.2 Identificação de eventos primários.

Os eventos primários são numerados conforme indicados na árvore, sendo:

{26},{27} = probabilidade de falha não segura do módulo UA - **Pa**

{25}= probabilidade de falha não segura de módulos UF. - **Pb**

{22} = probabilidade de falha não segura auto-testes do módulo UTP (considerando-se testes on-line). - **Pc**

{21} = probabilidade de falha não segura do módulo UTP (não existe para falha singular - dados do fabricante). - **Pd**

{3} = probabilidade de falha não segura de 3/4 dispositivos eletromecânicos - evento independente. - **Pr**

6.4.3 Determinação do evento topo.

A avaliação quantitativa será realizada sem considerar as intersecções dos arranjos paralelos da árvore de falhas. O erro de precisão é desprezível e o valor encontrado é mais conservativo.

Falha crítica devido a uma UATP, $\Rightarrow F_{uatp} = P_a^2 + P_b$

Falha crítica devido a uma UTP, $\Rightarrow F_{UTP} = P_c * P_d$

Falha crítica devido a uma AU, $\Rightarrow F_{AU} = P_R$

Falha de "shut-down", $\Rightarrow F_{spin} = 4\left[\left(P_c * P_d\right)^6 + \left(P_a{}^2 + P_b\right)^3 + P_r{}^3\right]$

Verifica-se a existência de três subsistemas distintos na arquitetura (UATP, UTP e AU), com funções independentes que podem por si só gerar as situações não seguras.

Não foram consideradas as falhas das redes de proteções, assumindo-se que, por construção, uma rede não pode bloquear os demais módulos, e que as falhas serão oriundas de módulos e não da rede.

Avaliação quantitativa da FTA do SPIN

Definição de variáveis correspondentes aos eventos primários da aplicação

Todos os eventos de falha são considerados independentes

$Pa = 0.01$ UATP

$Pb = 0.001$

As probabilidades de falhas críticas / ano (não detectável) foram atribuídas apenas para "o cálculo estimado" do valor da probabilidade de ocorrência do evento topo na arquitetura.

$Pc = 0.01$

$Pd = 0.01$ UTP

$Pr = 0$ Pax=Pay=Pbx=Pby=Pr

A avaliação quantitativa é realizada sem considerar as intersecções dos arranjos paralelos dos ramos da árvore de falhas (o erro de precisão é muito baixo e o valor simplificado é mais conservativo).

$Px = Pa^2 + Pb$ Px, corresponde a probabilidade de falha crítica devido a um UATP

$Py = 4 \cdot Px^3$ Py, requisição de comando não seguro - UATP's

$Pz = Pc \cdot Pd$ Pz, corresponde a probalidade de falha crítica devido a um UTP

$Pw = 4 \cdot Pz^6$ Pw, falha crítica devido a processamento de segurança - UTP's

$P = 4 \cdot Pr^3$ Pr, falha de "trip" causado por falha em dispositivos eletromecânicos

$Fspin = Py + Pw + P$ Fspin , probabilidade de falha de "trip"

$Fspin = 5.324 \cdot 10^{-9}$ $Pz = 1 \cdot 10^{-4}$ $Px = 0.001$ $P = 0$

$Pw = 0$ $Py = 5.324 \cdot 10^{-9}$

Identifica-se os subsistemas UATP e UTP/AU como vitais para a ação de desligamento do reator. Inferindo-se valores comuns de probabilidades de falhas para os

eventos primários, obtém-se um número aceitável para probabilidade de falha de desligamento comprovando a capacidade da arquitetura.

6.5 *Análise da Confiabilidade e Segurança da Arquitetura do SPIN.*

6.5.1 Introdução

As atividades executadas no estudo de caso, são:

- Desenvolvimento de modelos de estados representativos do sistema para análise de S(t) e MTTUF por *Cadeias de Markov* .

- Desenvolvimento de modelos de estados representativos do sistema para análise de R(t) e MTBF por *Cadeias de Markov* e *lógica combinatória*. São realizadas aproximações devido a existência de testes periódicos.

- Obtenção do sistema de equações diferenciais dos modelos.

- Solução do sistema de equações diferenciais e determinação de **R(t), MTBF, S(t),** e **MTTUF.**

- Discussão e comparação dos resultados obtidos entre os modelos e comentários.

De acordo com a metodologia proposta, será realizado a avaliação da Confiabilidade e Segurança da arquitetura através da modelagem de estados por cadeias de Markov e lógica combinatória.

A abordagem da arquitetura será realizada considerando-se o seguinte:

1.Destacam-se, baseados na árvore de falhas, 03 subsistemas distintos, com independência de função, conforme verificado na descrição do sistema e ilustrado na fig. 25.

2.Como a rede de proteção possui isolação galvânica, admite-se que uma falha física da rede não indisponibilizará os demais subsistemas.

3.Falhas da rede englobam *"software"* e o *"hardware"* envolvido. Considera-se que estas falhas estão incluídas nas taxas de falhas do *"hardware"* em análise.

4.Não são considerados diretamente na análise, os dispositivos de testes periódicos na modelagem de Markov, por não poderem ser aplicáveis no modelo, por serem determinísticos. É realizada, através de uma aproximação, uma modelagem da arquitetura para análise de falhas não seguras, baseada na existência de testes periódicos, impondo-se testes periódicos aleatórios segundo uma distribuição exponencial. Essa modelagem é mais conservativa que a arquitetura com testes periódicos determinísticos.

5.A avaliação da confiabilidade do SPIN é baseada em hipóteses assumidas de forma superficial. Não são considerados nos modelos, índices de cobertura de falhas e intervalos de tempo gastos na detecção de falhas por autotestes e votadores.

6.5.2 Definição dos modelos

A analise é concentrada nos subsistemas diretamente envolvidos nas ações de desligamento do reator. A fig. 29 ilustra a arquitetura composta destes subsistemas. A partir dela é implementada a seguinte estratégia para modelagem:

- Os subsistemas são analisados individualmente por modelos de Markov determinando-se os parâmetros R(t), S(t) e MTTUF. Através de uma aproximação com lógica combinatória será determinado os parâmetros do arranjo da arquitetura.

- Para o cálculo da confiabilidade são realizadas aproximações nos modelos, considerando-se que os estados ocupados por falhas não seguras não são significativos quando comparados com estados ocupados por falhas seguras. Esta aproximação é válida se as taxas de falhas não seguras forem desprezíveis em relação às taxas de falhas dos módulos dos subsistemas.

- Os valores de confiabilidade obtidos são associados em modelo de lógica combinatória, onde são determinados o MTTF, R(t), S(t) e MTTUF. Considerando os intervalos de manutenção periódica, previstos em [24], são introduzidas aproximações para determinação de taxas de falhas não seguras. Embora, estes intervalos para cada

subsistema sejam distintos, a análise faz o levantamento tendo por hipótese um valor comum a favor da condição mais conservativa. As aproximações de cálculo introduzem um erro tolerável nos resultados. A análise do sistema completo por Markov, recairia em um diagrama de estados de grande dimensão (maior que 100).

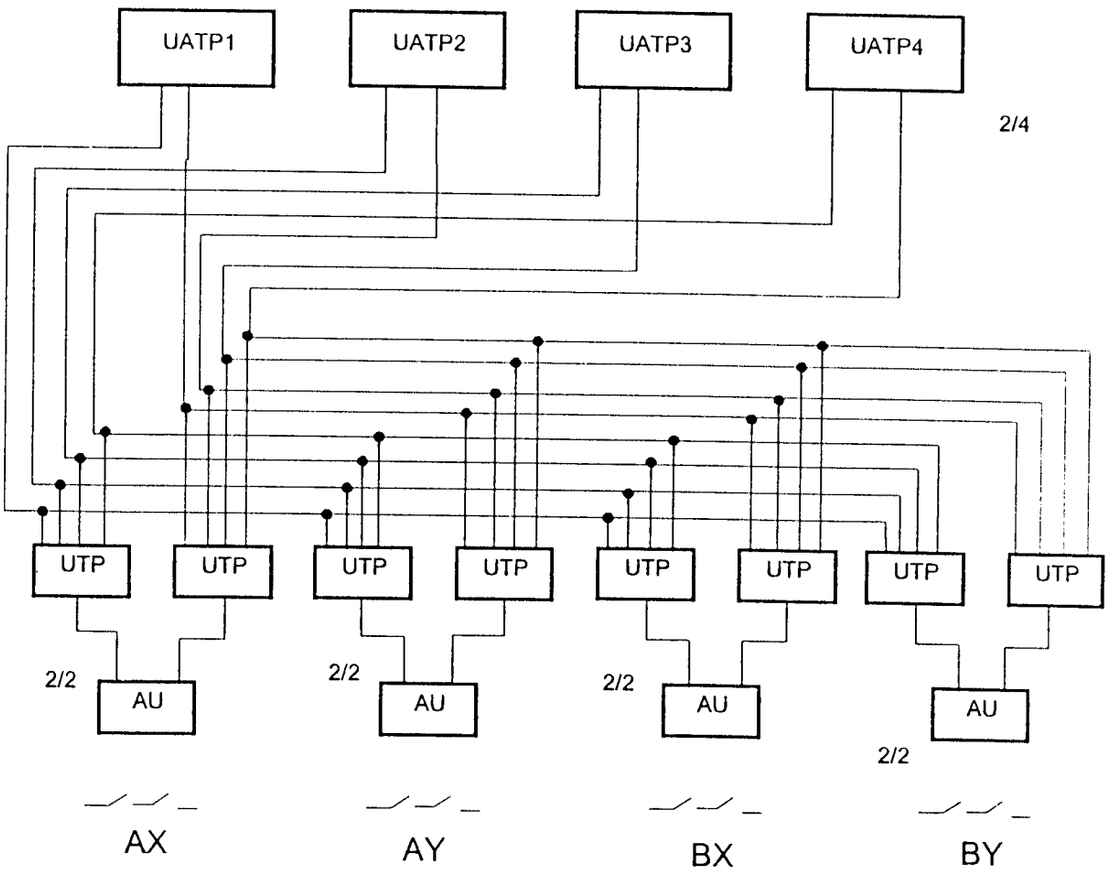


Fig. 29 - Modelo funcional do sistema para a cadeia de desligamento

A árvore de falhas mostrou três subsistemas distintos e em série em termos de segurança e confiabilidade. A fig. 29 ilustra os subsistemas, os quais são:

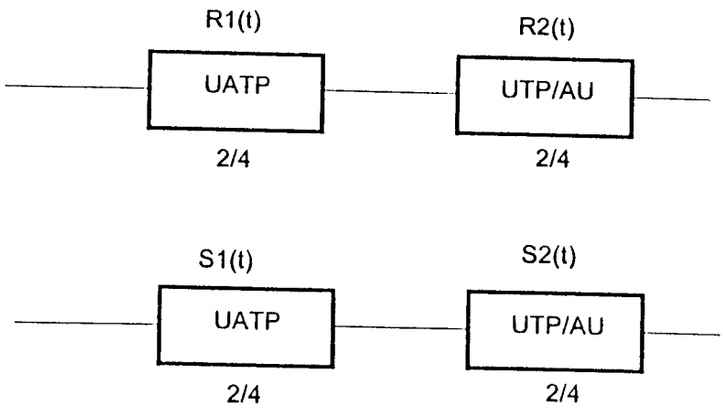
- subsistema de aquisição, processamento e requisição de desligamento composto por UATP's em redundância 2/4;

- subsistema de processamento de votação e atuações de ações de segurança composto por UTP's em redundância 2/2 por canal, em um total de 4 canais. Em conjunto opera em redundância 2/4;

- subsistema de atuação composto por dispositivos eletromecânicos AU de atuação em tecnologia "*fail safe*", em redundância 2/4.

Modelando-se o subsistema UTP associado ao subsistema AU, obtém-se duas arquiteturas semelhantes em redundância 2/4 composta por UATPs e UTP/AU em série, conforme ilustra a fig. 29.

A modelagem global do SPIN é feita de modo aproximado, por lógica combinatória, segundo associações de valores de confiabilidade operacional R(t) e confiabilidade segura S(t). A confiabilidade operacional fornece dados que permitem estimar a probabilidade de que o sistema esteja funcionando em um intervalo de tempo Δt. A confiabilidade segura permite estimar a probabilidade de que o sistema esteja em uma condição segura em um intervalo de tempo Δt. A modelagem global é feita segundo o esquema da fig. 30.



$$R(t) = R1(t) \times R2(t)$$

$$S(t) = S1(t) \times S2(t)$$

Fig. 30 - Modelagem de confiabilidade e segurança para a cadeia de desligamento

6.5.3 Estratégia de modelagem para UATP

Foram criados dois modelos de avaliação de segurança e um modelo para avaliação de confiabilidade na análise do subsistema UATP:

Segurança

A quantificação de segurança é obtida através do cálculo de MTTUF e confiabilidade segura S(t) considerando taxas de reparos μi e taxas de falhas não seguras λi. O processo é efetuado por *cadeias de Markov*, com um estado caracterizado como absorvedor dos subsistemas comuns na arquitetura. A probabilidade de ocupação de estados inseguros é caracterizada pela presença de falhas não seguras, que por definição não são detectáveis.

Foram realizados estudos por dois modelos distintos. O primeiro modelo, fig. 31, considera todos os estados falhos possíveis de ocupação pela arquitetura do subsistema. Esses estados são caracterizados por presença de falhas detectáveis, taxas de reparo para recuperação com relação a estas falhas, e falhas não seguras sem possibilidade de reparo porque não existe detecção. Admite-se que a probabilidade de ocorrência dos estados inseguros seja muito baixa visto que, taxas de falhas seguras e taxas de reparo devem ser muito maiores por projeto. Tem-se então, um modelo aproximado de comportamento onde determina-se o MTTUF da arquitetura do UATP. Foram avaliados também, o comportamento do MTTUF em relação a variação dos parâmetros de confiabilidade.

O segundo modelo para cálculo de S(t) é uma aproximação do comportamento dos estados do sistema, devido a existência de testes periódicos, os quais são realizados a cada 12 meses [24]. Um estado inseguro, por definição, só pode ser detectado e reparado com a realização destes testes. Dessa forma, o sistema retornaria à sua condição inicial após a realização dos mesmos.

O modelo aproximado propõe que, os intervalos entre os testes periódicos obedeçam um processo de Poisson com taxa média de ocorrência, exponencialmente

distribuída, de 12 meses. Assim, 12 meses corresponde a uma média de uma distribuição exponencial,

$G(t)=1-e^{-\lambda t}$, igual a $1/\lambda$ ou E[V].

O capítulo relativo ao "paradoxo de tempo residual" da referência [31], demonstra que um evento aleatório ocorrendo dentro desse intervalo sofre uma espera média de $2/\lambda$, para ser interceptado pelo evento "testes periódicos", ou seja, duas vezes o intervalo médio entre os testes periódicos.

No caso:

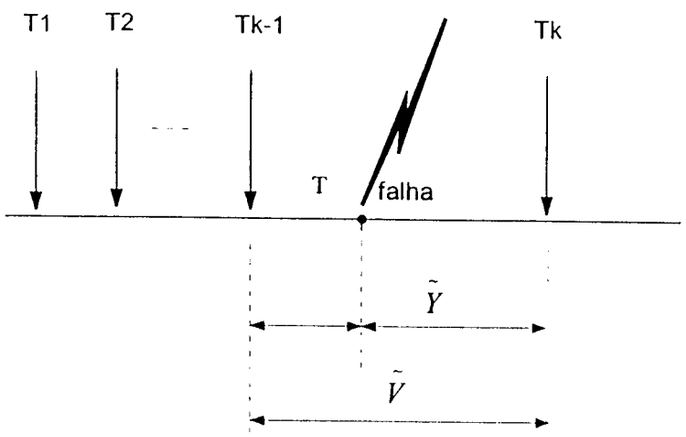
T_n indica o instante de execução de testes periódicos, para n=1,2,.....

T indica o instante de ocorrência do evento falha.

E[V] indica o intervalo médio entre os testes periódicos

$E[\tilde{V}]$ indica o intervalo médio de interceptação com tempo residual $\tilde{Y}$ "*observado*" pelo evento.

T_{k-1} e T_k indicam o intervalo onde ocorre o evento.



Demonstra-se nessas condições que $E[\tilde{V}]$=2E[V].

Caracterizando o evento como ocorrência de falha não segura no intervalo, o reparo ocorre segundo uma taxa média de reparos ou intervalo médio de espera de 24 meses. Para efeitos de modelagem, assume-se que não há espera e o reparo é iniciado logo após a ocorrência. O processo de *Markov* pode ser empregado para modelagem de segurança do sistema se a taxa de falhas não seguras for muito menor que a taxa média de reparos.

A aproximação adotada é mais conservativa que a existência real de períodos de testes determinísticos, pois nesse caso, o tempo médio seria a metade do intervalo, mas devido as condições de contorno, não poderíamos realizar a avaliação por *cadeias de Markov*. Esta observação serve para ilustrar um fato fundamental: Grandezas aleatórias sempre aumentam períodos de tempo de espera [31].

Este modelo corrige a deficiência do sistema, de que a existência de falhas detectáveis e taxas de reparo associadas, somente irão contribuir para que o sistema caminhe para a situação crítica. Isso ocorre porque assume-se que a falha critica não é percebida, e o módulo falho nunca é reparado se não existirem testes com índice de cobertura de falhas de 100%.

Deduz-se que a taxa de reparo de falhas detectáveis, portanto seguras, do módulo falho apenas o recupera, não tendo qualquer influência benéfica para o módulo em estado inseguro, pelo contrário, o prejudica conforme será demonstrado mais adiante, baseado na análise do primeiro modelo.

Assim, na análise dos modelos, considera-se que:

1.As falhas seguras estarão na classe monitoradas e detectadas e, as ocorrências resultam na ocupação de um estado que pode ser reparado segundo uma taxa média de reparos. Este tipo de falha aciona o desligamento no canal redundante.

2.As falhas não seguras situam-se na classe de falhas críticas, as ocorrências não são detectadas e causam o impedimento de acionamento de desligamento do reator. Tal situação somente ocorrerá se existirem 03 subsistemas UATPs falhos.

3.No caso de indisponibilidade do equipamento, supõe-se que o reator foi desligado, dado a ocupação desse estado. Assim, a recuperação do sistema se dará segundo uma taxa média de reparo global com índice de cobertura de 100%, recuperando todo o sistema de proteção.

4.No modelo nº 2, fig 32, assume-se que os testes periódicos obedecem a um processo de Poisson com taxa de ocorrência exponencialmente distribuída, com intervalo médio igual ao intervalo dos testes periódicos. Na ocorrência de testes periódicos, todas as falhas que ocorreram no intervalo são sanadas. Assim, aproximamos a taxa média de reparos como sendo o tempo de espera do teste periódico, uma vez que assume-se ser desprezível o tempo médio de reparos após o teste.

UATP's - Diagrama de transição de estados

Redundância 2/4

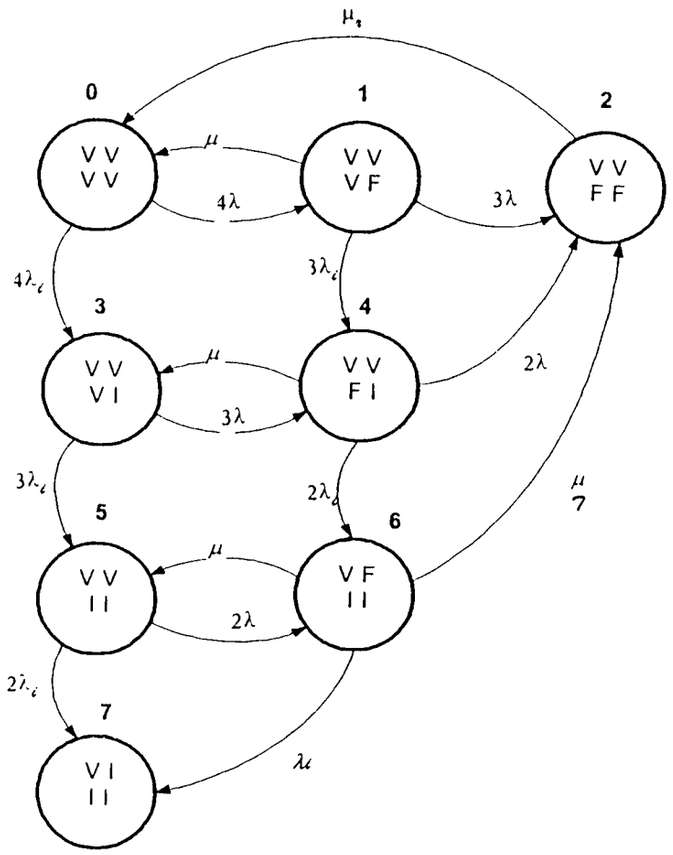
Modelo para avaliação de MTTUF

Processo de Markov-
caracterizado por
01 estado absovedor:
indisponibilidade crítica

V , sem falhas

I, falha insegura

F falha segura



O estado "7" constitue estado absorvedor

O estado "2" constitue queda do sistema e repara todo o sistema, retornando à condição de operação total sem falhas

legenda

μ_t , taxa de reparo total
μ taxa de reparo
λ taxa de falhas seguras (detectáveis)
λ_c taxa de falhas inseguras (não detectáveis)

Fig. 31 - Modelo completo englobando falhas seguras e não seguras

As equações diferenciais do modelo de estados do subsistema UATP para MTTUF ilustrado na fig 31, são:

$$\dot{P}_0(t) = -4(\lambda + \lambda i)P_0(t) + \mu r P_2(t) + 4\lambda P_1(t)$$

$$\dot{P}_1(t) = -(\mu + 3\lambda + 3\lambda i)P_1(t) + 3\lambda P_2 + 3\lambda i P_4(t) + \mu P_0(t)$$

$$\dot{P}_2(t) = -\mu r P_0(t) + 3\lambda P_1(t) + 2\lambda P_4(t) + \lambda P_6(t)$$

$$\dot{P}_3(t) = -3(\lambda + \lambda i)P_3(t) + 4\lambda i P_o(t) + \mu P_6(t)$$

$$\dot{P}_4(t) = -(2\lambda i + \mu + 2\lambda)P_4(t) + 3\lambda i P_1(t) + 3\lambda P_3(t)$$

$$\dot{P}_5(t) = -2(\lambda + \lambda i)P_5(t) + 3\lambda i P_3(t) + \mu P_6(t)$$

$$\dot{P}_6(t) = -(\mu + \lambda + \lambda i)P_6(t) + 2\lambda P_5(t) + 2\lambda i P_4(t)$$

$$\dot{P}_7(t) = 2\lambda i P_5(t) + \lambda i P_6(t)$$

onde $\dot{P}_i(t) = dP_i(t) / dt$

Considerando os estados operativos do sistema, a solução das equações $\dot{P}_i(t)$, as probabilidades destes estados permitem avaliar S(t).

$$S(t) = P_0(t) + P_1(t) + P_2(t) + P_3(t) + P_4(t) + P_5(t) + P_6(t)$$

e dessa forma: $P_0(t) + P_1(t) + P_2(t) + P_3(t) + P_4(t) + P_5(t) + P_6(t) + P_7(t) = 1$

No estado "7" o sistema está em falha crítica.

Assim sendo o MTTUF pode ser calculado pela equação:

$$MTTUF = \int_0^\infty (1 - P_7(t))dt \; ;$$

ou pelo método simplificado, mostrado na ref. [8], considerando apenas os estados em que o sistema está operando na matriz de transição M_a resultando na matriz de transição modificada M_u. Assim M_u é a submatriz formada das N_u+1 linhas e N_u+1 colunas da matriz de transição M_a.

A probabilidade de que o sistema esteja operando é $P_n^u(t)$. A confiabilidade é

$$R(t) = \sum_{n=0}^{Nu} P_n^u(t);$$

o sistema de equações de $P^u(t)$ pode ser escrito na forma;

$$dP^u(t)/dt = M_u P^u(t);$$

satisfazendo as condições iniciais $\Rightarrow P^u(0) = \begin{vmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{vmatrix}$ e $P^u(\infty)=0$, devido ao estado absorvedor;

o $MTTUF = \sum_{n=0}^{N_u} K_n$ onde $K_n = \int_0^\infty P_n^u(t)dt$ $n = 0$ a N_u .e;

K_n são os elementos do vetor K, portanto, resolvendo-se a integral obtém-se;

$$M_u K = -P^u(0);$$

satisfazendo as condições iniciais e finais, obtém-se como resultado ;

$$K_n = -\frac{(cof\,\mathrm{M}_u^{\mathrm{T}})n0}{|M_u|};$$

onde $cofM_u^T$ são os cofatores da matriz de transição transposta e $|M_u|$ o determinante, [8].

O segundo modelo para avaliação de S(t) e MTTUF é apresentado a seguir:

UATP's - Diagrama de transição de estados

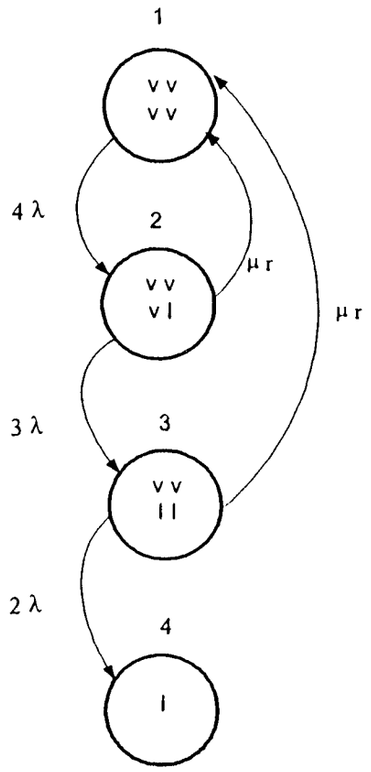
Redundância 2/4

Modelo para avaliação de S(t)

Processo de Markov
caracterizado por
01 estado absovedor:
indisponibilidade crítica

V , sem falhas

I, falha insegura



legenda

μ_t , taxa de reparo total.

λ taxa de falhas inseguras.

Fig. 32 - Modelo para avaliação de S(t) devido a falhas não seguras

As equações diferenciais que regem o modelo de estados ilustrado na fig. 32, são:

$$\dot{P}_1(t) = -4\lambda P_1(t) + \mu P_2(t) + \mu P_3(t)$$
$$\dot{P}_2(t) = 4\lambda P_1(t) - (3\lambda + \mu) P_2(t)$$
$$\dot{P}_3(t) = 3\lambda P_2(t) - (\mu + 2\lambda) P_3(t)$$
$$\dot{P}_4(t) = 2\lambda P_3(t)$$

A confiabilidade segura será dada pela seguinte expressão

$$S(t) = (1 - P_4(t))$$

E o valor de MTTUF por.

$$MTTUF = \int_0^{\infty} S\ (t)dt$$

O MTTUF também será avaliado pelo método simplificado descrito em [8] e os resultados serão comparados.

$$MTTUF = \sum_{n=0}^{Nu} K_n \text{ onde } K_n = -\frac{\left(cof\, \mathrm{M}_u^{\mathrm{T}}\right)n0}{|M_u|}$$

As soluções de MTTUF segundo os resultados das duas modelagens do subsistema UATP permitirão avaliar o grau de coerência entre os modelos.

A modelagem da função S(t) não permite uma solução totalmente literal, a qual seria importante para a associação com o subsistema UTP/AU para se obter a confiabilidade segura total de forma literal possibilitando o estudo de seu comportamento com variação de parâmetros.

A modelagem detalhada, sem considerar taxas médias de reparo para falhas não seguras, recai em um sistema de equações diferenciais de oito incógnitas e sua solução não reflete a realidade do sistema devido a não detecção de falhas não seguras e a existência de testes periódicos para detecção real da presença dessas falhas .

O modelo para confiabilidade R(t) com taxa de reparos μ e taxa de falhas λ é avaliado por *cadeias de Markov*, com um estado absorvedor, e desprezam-se os estados ocupados por elementos com falhas inseguras, por serem pouco significativos, fig. 33.

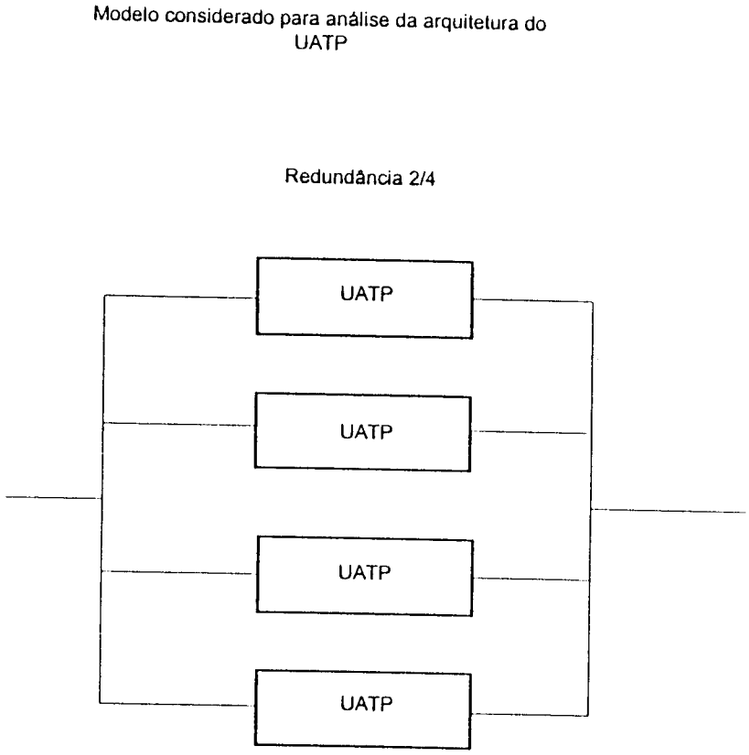


Fig. 33 - Modelagem de confiabilidade para UTAP

As falhas seguras são associadas a detecção e a uma taxa de reparos que recupera o módulo do subsistema. Uma falha segura ocasiona o desacionamento do canal de desligamento. Dois subsistemas UATPs em falha segura causa indisponibilidade do sistema.

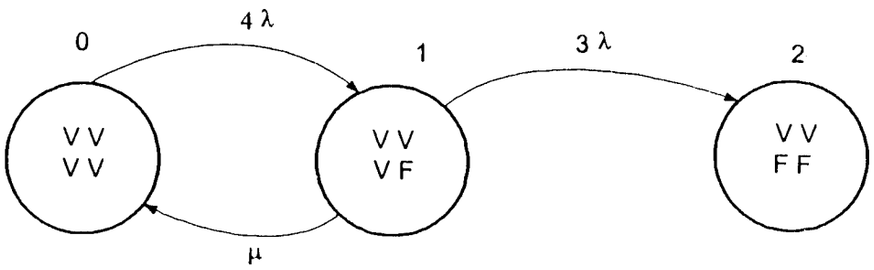
Para a modelagem de R(t) assume-se que a probabilidade de ocupação de um estado inseguro é muito menor que a ocupação de estado não operacional causado por uma falha simples, isso de acordo com a filosofia de projeto de sistema de segurança. Logo o erro causado pela aproximação não é significativo. Dessa forma, os estados que permanecerão maior tempo ocupados serão os considerados no modelo, dado que uma falha operacional é muito mais frequente que uma falha não segura. Assume-se então que os estados ocupados por falhas não seguras não serão significativos.

O modelo de estados com aproximações para análise de R(t) do subsistema UATP em redundância 2/4 está representado na fig. 34.

UATP's - Diagrama de transição de estados

Redundância 2/4

Modelo para avaliação de R(t)



legenda

O estado "2" constitue queda do sistema

μ taxa de reparo
λ taxa de falhas do módulo (detectáveis)

Processo de Markov- cadeia redutível-
caracterizada por 01 estado
absovedor:

Estados do sistema

V , sem falhas

F, falha

Fig. 34 - Modelo de Markov para confiabilidade UATP

As equações diferenciais que regem o modelo de estados do subsistema UATP para R(t) são:

$$\dot{P}_0(t) = -4\lambda P_0(t) + \mu P_1(t)$$

$$\dot{P}_1(t) = -(3\lambda + \mu) P_1(t) + 4\lambda P_0(t)$$

$$\dot{P}_2(t) = 3\lambda P_1(t)$$

$$R(t) = P_0(t) + P_1(t)$$

O MTBF pode ser avaliado de acordo com,

$$MTBF = \int_0^\infty R(t)\, dt$$

6.5.4 Estratégia de modelagem para UTP/AU

A modelagem dos canais UTP/AU é semelhante à modelagem do subsistema UATP. A estratégia adotada faz uma aproximação juntando canais de atuação UTP/AU e sendo estes canais idênticos e em número de quatro com redundância 2/4, será realizada uma simplificação dos modelos, fig 35.

É realizado o calculo de MTTUF do canal de atuação UTP/AU .A análise de MTTUF para este canal independente é realizada por Cadeias de Markov redutíveis, com um estado absorvedor. Este modelo visa verificar a aplicabilidade da arquitetura de canal de votação UTP/AU, os quais votam informações do subsistema UATP, com relação a segurança.

A simplificação na análise do arranjo 2/4, considerando o canal UTP/AU como um bloco único com taxa de falhas não seguras λi, é mais conservativa que a análise considerando o arranjo global dos módulos.

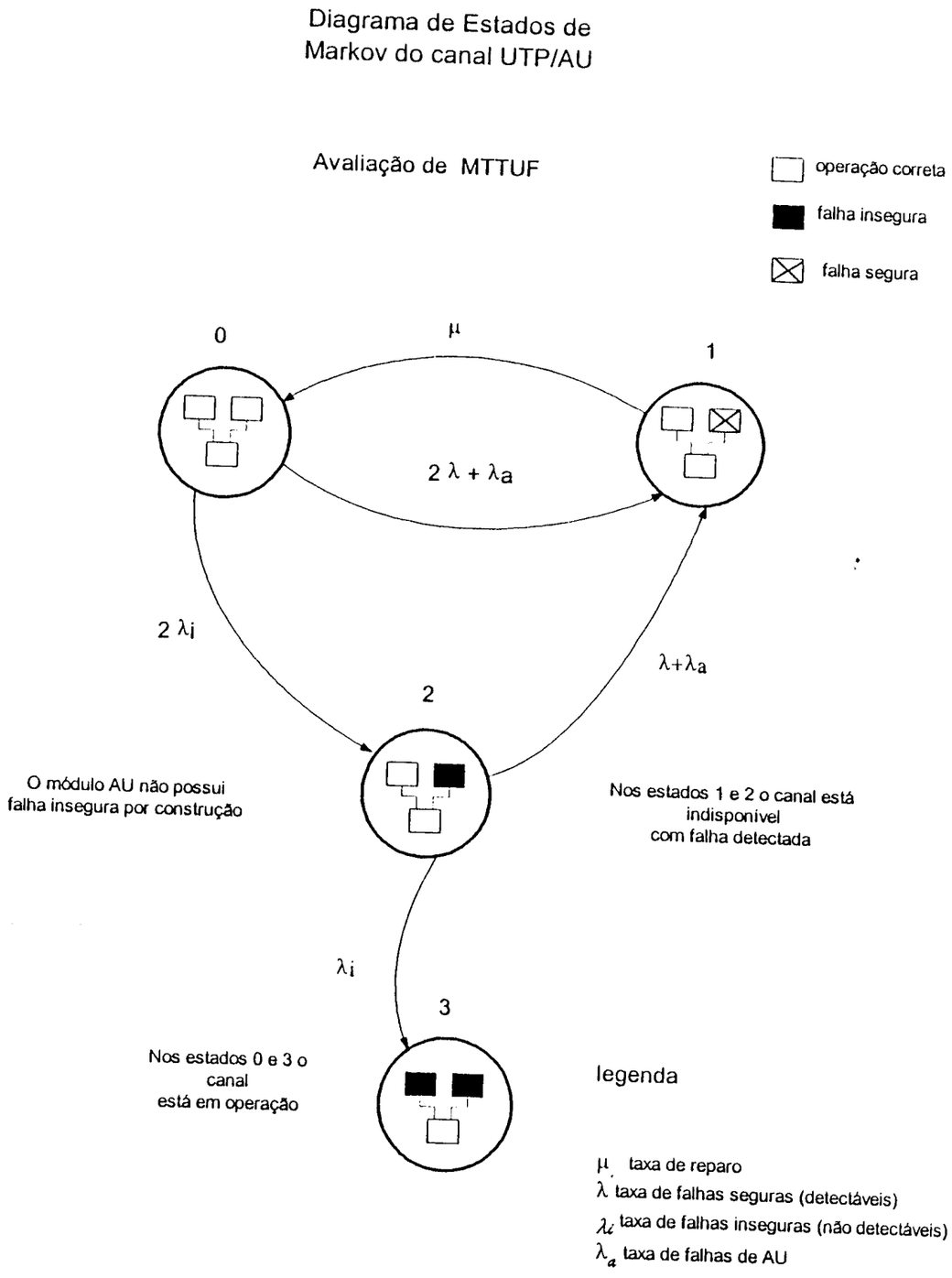


Fig. 35 - Modelo de Markov para R(t) e MTUF do subsistema UTP/AU

As equações diferenciais do modelo do subsistema UTP/AU para o MTTUF são:

$$\dot{P}_0(t) = -(2\lambda i + 2\lambda + \lambda a)P_0(t) + \mu P_1(t)$$
$$\dot{P}_1(t) = -\mu P_1(t) + (2\lambda + \lambda a)P_0(t) + (\lambda + \lambda a)P_2(t)$$
$$\dot{P}_2(t) = 2\lambda i P_0(t) - (\lambda i + \lambda + \lambda a)P_2(t)$$
$$\dot{P}_3(t) = \lambda i P_2(t)$$

e na forma matricial $MTTUF = \sum_{n=0}^{N_u} Kn$

$$K_n = -\frac{(\text{cof}\, M_u^T)no}{|M|}$$

O modelo de R(t) do canal UTP/AU é um arranjo série sem reparo dado que qualquer falha segura coloca o módulo indisponível. Isso é válido para a aproximação já mencionada na análise da UATP.

$$R(t) = e^{-(2\lambda_{utp} + \lambda_{au})t}$$

A análise de S(t), da arquitetura UTP/AU é um arranjo 2/4 e a solução adotada é similar a aproximação realizada para avaliação da S(t) do subsistema UATP.

A análise de R(t) da arquitetura UTP/AU recairá no modelo 2/4 de três estados com taxa de reparo μ e taxa de falhas λ com equacionamento idêntico ao UATP. Portanto:

As equações diferenciais do modelo do subsistema UTP/AU para R(t) são:

$$\dot{P}_0(t) = -4\lambda P_0(t) + \mu P_1(t)$$
$$\dot{P}_1(t) = -(3\lambda + \mu) P_1(t) + 4\lambda P_0(t)$$
$$\dot{P}_2(t) = 3\lambda P_1(t)$$

$$R(t) = P_0(t) + P_1(t)$$

Onde a taxa de falhas λ é dada por:

$$\lambda = 2\lambda_{UTP} + \lambda_{AU}$$

6.5.5 Confiabilidade do SPIN

Em termos de R(t) e S(t) do SPIN, ambos arranjos (UATP e UTP/AU) estão em série, então podemos aproximar por lógica combinatória que as confiabilidades operacionais e segura da arquitetura do SPIN será o arranjo série das confiabilidades correspondentes aos arranjos UATP e UTP/AU.

6.5.5.1 Arranjo UATP

- Modelo para MTTUF do UATP (mod 1).
- Modelo simplificado para análise de S(t) e MTTUF (mod 2).
- Modelo simplificado para R(t) e MTBF (mod 3).

6.5.5.2 Arranjo UTP/AU

- Modelo para análise de MTTUF e R(t) de um canal (mod 4).
- Modelo simplificado para análise de S(t) e MTTUF do arranjo.

•Modelo simplificado para análise de R(t) do arranjo.

6.5.5.3 Sistema SPIN completo

•Determinação de S(t), R(t), MTBF e MTTUF global.

Foi utilizado o programa **Mathcad 5.0 for Windows** [35], que dispõe de um processador literal para elaboração das operações com matrizes dos sistemas de equações diferenciais. Sempre que possível, procurou-se executar as operações dentro do programa e utilizar os recursos de "*Copy*" and "*Paste*" para evitar-se erros de digitação.

6.5.5.4 Valores de confiabilidade para os módulos básicos.

Para avaliação dos parâmetros de confiabilidade e segurança da arquitetura, as seguintes hipóteses são assumidas e valores atribuídos:

1. Qualquer falha detectável ou monitorada deixa o módulo básico inoperante. Os módulos básicos são as porções não redundantes da arquitetura. Neste caso, atribuiu-se o valor da taxa de falhas como sendo 1 falha / ano para cada módulo básico (valor dentro dos parâmetros de mercado para equipamentos de alta confiabilidade. No caso de projeto, este seria o valor a ser alcançado no módulo básico).

2. A taxa média de reparos de um módulo para colocação do canal redundante em operação teve seu valor atribuído em 12 horas. Este valor é muito conservativo se for considerado que após uma detecção de falha, o módulo deverá ter sua parte inoperante substituída e todos os testes realizados antes da sua entrada em serviço. Na prática este tempo pode ser diminuído, mas a postura assumida na análise é pessimista.

3. A taxa de falha não seguras teve seu valor atribuído em uma falha a cada 1000 anos por módulo básico. Sendo a ocorrência desta classe de falha muito rara para projetos dessa natureza, o valor assumido constitue um valor pessimista.

4. A taxa média de reparo global após desligamento será de 3 dias.

6.5.6 Solução dos modelos

Solução do modelo 1 para avaliação do MTTUF da arquitetura 2/4 UATP.

$\mu = 730$ taxa média de reparos $\Rightarrow$ um reparo / 12 horas

$\mu r = 180$ taxa média de reparos após desligamento do reator

$\lambda = 1$ taxa média de falhas $\Rightarrow$ 1 falha / ano

$\lambda i = 0.001$ taxa de falhas não seguras $\Rightarrow$ 0.001 falhas / ano

MTTUF = $3{,}479 \times 10^3$ anos

Verifica-se que o valor obtido de MTTUF é pior que o esperado,($> 10^5$ anos). Isso ocorre porque sem os testes periódicos em todo o sistema, é muito pouco provável que o mesmo retorne à condição inicial, existindo ocupação de estados devidos a módulos em falha não segura. As chances de detecção tornam-se escassas porque apenas módulos em falhas detectáveis e portanto seguras são reparados.

A única detecção provável ocorre em caso de indisponibilidade do sistema onde no caso assume-se uma verificação geral. Esta situação é prejudicada pela presença de taxas de reparo, implicando em uma probabilidade baixa de indisponibilidade do sistema.

Como verificação deste fato, assumindo uma taxa de reparos $\mu=0$;

MTTUF = 1.479×10^8 anos

Assim as falhas seguras, possuindo uma taxa de ocorrência muito maior que as falhas críticas, levariam o sistema a um estado de indisponibilidade e uma manutenção geral seria necessária. Logo o sistema ficaria muito seguro, mas pouco disponível.

Esta situação poderia ser modificada, caso ocorre-se uma manutenção geral cada vez que um módulo falha-se, mas isto é pouco prático.

Estas conclusões baseiam-se na hipótese de que as falhas não seguras consideradas causam a condição onde a requisição de desligamento não seria cumprida. Logo, tal ocorrência não é verificada até a atuação. Portanto a falha do módulo por hipótese não é percebida durante a operação normal.

Solução do modelo (2) para análise do MTTUF da arquitetura 2/4 UATP, considerando-se taxas de reparos para falhas não seguras em virtude da existência de testes periódicos. O calculo é efetuado pelo método simplificado [8] e pela definição:

$$MTTUF = \int_0^{\infty} S\ (t)dt$$

Resolvendo-se as equações diferenciais do modelo obtém-se:

•Solução do modelo 2 pelo método simplificado;

μ = 0.5 taxa média de reparos = um reparo em cada dois anos.

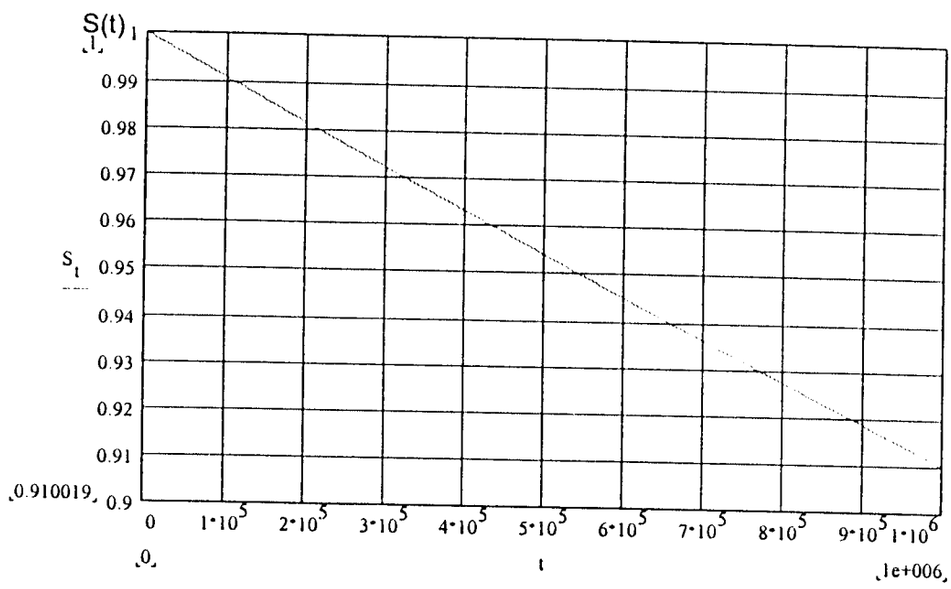
λ 0.001 taxa de falhas inseguras 0,001 falhas/ano

$$\text{MTTUF} = \left[\frac{1}{24}\cdot(3\cdot\lambda + \mu)\cdot\frac{(\mu + 2\cdot\lambda)}{\lambda^3}\right] + \left[\frac{1}{6}\cdot\frac{(\mu + 2\cdot\lambda)}{\lambda^2}\right] + \left[\frac{1}{(24\cdot\lambda^2)}\cdot(\mu \quad \lambda)\right]$$

$$\text{MTTUF} = 1.058\cdot 10^7 \quad \text{anos}$$

•Solução do modelo 2, pela definição;

$$S_t := (1.846\,10^{-7})\cdot\left(e^{0.504\cdot t}\cdot\cos(0.002)\cdot t - \frac{1}{0.004}\cdot e^{0.504\cdot t}\cdot\sin(0.002)\cdot t\right) + e^{9.429\cdot 10^{-8}\cdot t}$$



o MTTUF é calculado pela integral de S(t),

$$MTTUF = \int_{0}^{1000000000} (1.846\,10^{-7})\cdot\left(e^{0.504\cdot t}\cdot\cos(0.002)\cdot t - \frac{1}{0.004}\cdot e^{0.504\cdot t}\cdot\sin(0.002)\cdot t\right) + e^{9.429\cdot 10^{-8}\cdot t}\,dt$$

$MTTUF = 1.061\cdot 10^{7}$ anos

O modelo apresentou como resultado um MTTUF da ordem de 10 milhões de anos, valor dentro dos parâmetros de segurança para esta classe de equipamento.

Observou-se que o MTTUF obtido pelo método simplificado foi praticamente idêntico ao valor obtido a partir da função S(t).

Observou-se que o modelo apresentou na solução das equações, raízes complexas conjugadas, indicando a presença de oscilações. Foi verificado através da derivada da função S(t) se a mesma é monotônica decrescente, condição necessária para uma função confiabilidade, e comprovou-se tal fato.

O modelo analisado, com a aproximação introduzida, mostra a importância da existência de testes periódicos com 100% de grau de cobertura em sistemas de segurança, logicamente, o único meio de detecção de falhas não seguras residentes. A ref [24], afirma que o SPIN possui probabilidade de falha não segura inferior a 10^{-5} por ano se existirem testes periódicos segundo o intervalo mencionado.

Para o cálculo do MTTUF através da integração de S(t), o valor "∞", foi substituído por um número elevado (10^9 anos) devido a limitações do programa "*mathcad*", o erro introduzido é praticamente nulo.

Solução do modelo 3 para avaliação do comportamento de R(t) da arquitetura 2/4 UATP.

De acordo com taxas de reparo e falhas atribuídas, temos:

$\mu := 730$ um reparo em média a cada 12 horas.

$\lambda := 1$ taxa de falhas por módulo igual a uma falha por ano

$t := 0, 1 .. 100$

$k1 = 1$

$$a2 := \frac{7}{2}\cdot\lambda + \frac{1}{2}\cdot\mu - \frac{1}{2}\cdot\sqrt{\lambda^2 + 14\cdot\lambda\cdot\mu + \mu^2}$$

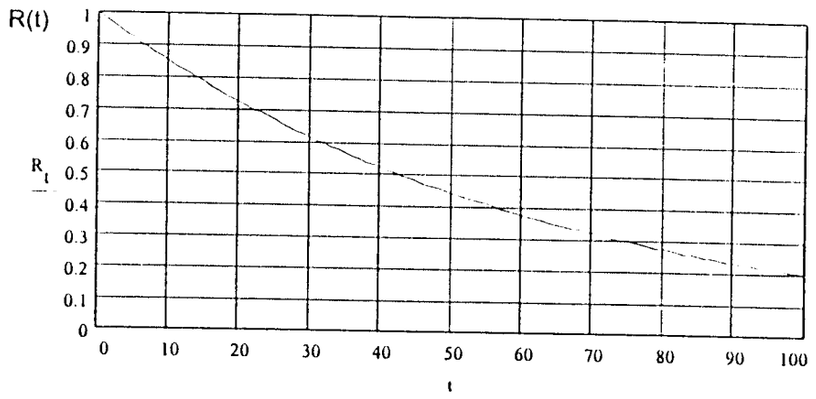
$$a3 := \frac{7}{2}\cdot\lambda + \frac{1}{2}\cdot\mu + \frac{1}{2}\cdot\sqrt{\lambda^2 + 14\cdot\lambda\cdot\mu + \mu^2}$$

$$k2 := \frac{12\cdot\lambda^2}{-a2\cdot(-a2 + a3)}$$

$$k3 := \frac{12\cdot\lambda^2}{-a3\cdot(-a3 + a2)}$$

$$R_t := -\left(k2 \cdot e^{-a2 \cdot t} + k3 \cdot e^{-a3 \cdot t}\right)$$

Análise de comportamento



Determinação do MTBF da arquitetura UATP

$$MTBF := \int_0^{10000} -k2 \cdot e^{-a2 \cdot t} - k3 \cdot e^{-a3 \cdot t}\, dt$$

MTBF = 61.417 anos

A resolução do modelo de confiabilidade nos fornece um valor de MTBF em torno de 67 anos para uma taxa de falhas de "1" falha por ano, de um canal redundante de UATP, valor dentro dos padrões de mercado para equipamentos de alta confiabilidade.

Supondo o sistema na condição de sem reparo "*on-line*", o MTBF da arquitetura seria em torno de 0,58 anos, ou seja em torno de meio ano, para redundância 2/4. Assim há um ganho de confiabilidade do sistema da ordem de 105 vezes.

Determinação do MTTUF do canal UTP/AU (mod 4)

Avaliação do MTTUF do canal UTP/AU , no caso a taxa de falhas do dispositivo eletromecânico AU é mais baixa que o dispositivo eletrônico UTP.

$\lambda := 1$ uma falha a cada ano

$\lambda a := 0.1$ uma falha a cada 10 anos

$\lambda i := 0.001$ uma falha insegura a cada 1000 anos

$\mu := 730$ taxa de reparo igual a um reparo em 12 horas

$$k0 := \frac{1}{2}\cdot\frac{(\lambda i + \lambda + \lambda a)}{\lambda i^2}$$

$$k1 := \frac{1}{2}\cdot\frac{4\cdot\lambda\cdot\lambda i + 2\cdot\lambda^2 + 3\cdot\lambda\cdot\lambda a + 3\cdot\lambda a\cdot\lambda i + \lambda a^2}{(\mu\cdot\lambda i^2)}$$

$$k2 := \frac{1}{\lambda i}$$

$MTTUF := k0 + k1 + k2$

$MTTUF = 5.531\cdot 10^5$ anos

O MTTUF de cada canal UTP/AU que vota informações dos UATPs, é da ordem de 500 mil anos de acordo com a arquitetura apresentada. Nesta modelagem não são considerados os testes periódicos, logo as falhas não seguras não possuem taxas de reparos, mas como foi assumido que a queda de um canal resulta no seu reparo completo, com índice de cobertura de falhas de 100%, a ocorrência de falhas detectáveis colaboram para aumentar o valor de MTTUF.

O modelo do subsistema UTP/AU para S(t), será o mesmo que foi utilizado para a arquitetura UATP na forma simplificada. Na realidade esta visão é mais realista devido a existência de verificações periódicas, e a modelagem considerando os canais UTP/AU em redundância 2/4 recairia em um diagrama de estados de Markov com um número muito grande de estados com somente solução por métodos numéricos. Logo será utilizado o

modelo do arranjo UATP com as aproximações introduzidas na modelagem para detecção de falhas não seguras.

Assim o modelo S(t) para UTP/AU é igual ao S(t) do arranjo UATP (mod-2)

$$S_t := \left(1.846\,10^{-7}\right)\cdot\left(e^{-0.504\cdot t}\cdot\cos(0.002)\cdot t - \frac{1}{0.004}\cdot e^{-0.504\cdot t}\cdot\sin(0.002)\cdot t\right) + e^{-9.429\cdot 10^{-8}\cdot t}$$

Modelo de confiabilidade para o arranjo UTP/AU (mod-5)

Determinação da confiabilidade R(t) para o arranjo 2/4 UTP/AU.

Utlizando-se aproximação semelhante à análise efetuada para o arranjo UATP, temos um modelo de 03 estados, com equações idênticas cuja solução será:

$\lambda u := 1$ taxa de falhas por módulo igual a uma falha por ano

$\lambda a := 0.1$ taxa de falhas do dispositivo eletromecânico uma falha a cada 10 anos

$\mu := 730$ um reparo em média a cada 12 horas.

$\lambda := 2\cdot\lambda u + \lambda a$

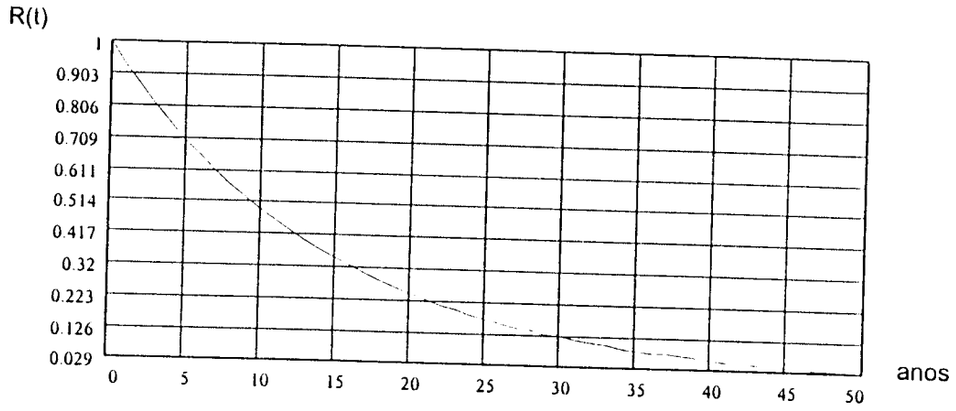
$t := 0, 1 .. 50$ anos

$$b2 := \frac{7}{2}\cdot\lambda + \frac{1}{2}\cdot\mu - \frac{1}{2}\cdot\sqrt{\lambda^2 + 14\cdot\lambda\cdot\mu + \mu^2} \qquad b3 := \frac{7}{2}\cdot\lambda + \frac{1}{2}\cdot\mu + \frac{1}{2}\cdot\sqrt{\lambda^2 + 14\cdot\lambda\cdot\mu + \mu^2}$$

$$p2 := \frac{12\cdot\lambda^2}{-b2\cdot(-b2 + b3)} \qquad p3 := \frac{12\cdot\lambda^2}{-b3\cdot(-b3 + b2)}$$

$$R_t := \left(p2\cdot e^{-b2\cdot t} + p3\cdot e^{-b3\cdot t}\right)$$

Análise de comportamento



E o MTBF do arranjo:

$$MTBF \int_{0}^{10000} p2 \cdot e^{b2 \cdot t} \; p3 \cdot e^{b3 \cdot t} \, dt$$

MTBF = 14.072 anos

Assumindo-se que existem módulos distintos para cada canal de votação de sinais de UATP para compor o votador eletromecânico, e que as taxas de falhas destes módulos possuem o mesmo valor (1 falha por ano) a arquitetura compreendida apresenta um valor baixo para o tipo de equipamento. Este fato, apontado pela análise de arquitetura pode ser corrigido, melhorando a confiabilidade no projeto dos módulos básicos do canal UTP/AU.

6.6 *Solução do modelo de R(t) e MTBF para a arquitetura do SPIN.*

Determinação de R(t) e MTBF do SPIN através de lógica combinatória entre os arranjos dos subsistemas UATP e UTP/AU

$t := 0, 1 .. 100$ anos

$\mu := 730$ taxa de reparos igual a um reparo em média a cada 12 horas.

$\lambda := 1$ taxa de falhas por módulo UATP igual a uma falha por ano

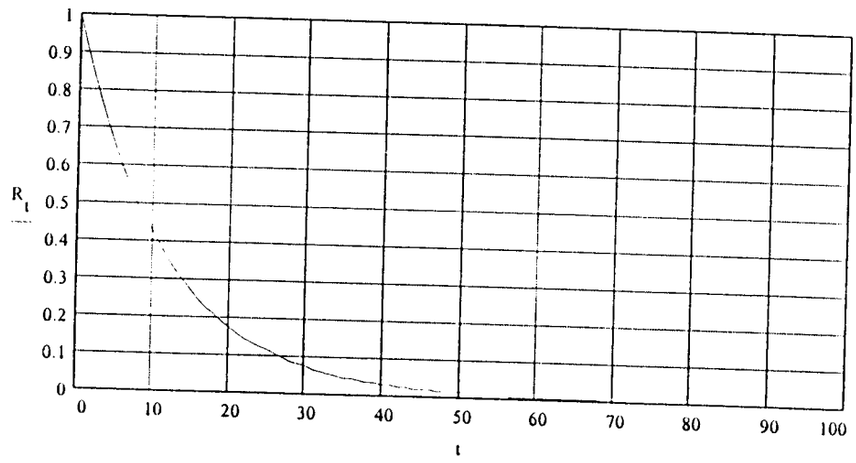
$\lambda u := 1$ taxa de falhas por módulo UTP igual a uma falha por ano

$\lambda a := 0.1$ taxa de falhas do dispositivo AU igual a uma falha a cada 10 anos

$\lambda utp := 2 \cdot \lambda u + \lambda a$

$$R_{SPIN}(t) = R_{UATP}(t) \times R_{UTP/AU}(t)$$

Confiabilidade R(t) do SPIN



$$MTBF := \int_0^{100} \left(k2 \cdot e^{-a2 \cdot t} + k3 \cdot e^{-a3 \cdot t}\right) \cdot \left(p2 \cdot e^{-b2 \cdot t} + p3 \cdot e^{-b3 \cdot t}\right) dt$$

MTBF = 11.447 anos

O valor encontrado é baixo, devido aos valores da arquitetura UTP/AU. Isto indica que para o SPIN, é necessário que os módulos básicos do UTP/AU possuam uma confiabilidade maior. Por exemplo, se a taxa de falhas λ dos módulos componentes da arquitetura UTP/AU fosse da ordem de 1 falha a cada 10 anos, teríamos o **MTBF** do **SPIN** igual a **56,3 anos**.

Por outro lado se a taxa média de reparos fosse de duas horas, mantendo-se a taxa de falhas original, o valor final de **MTBF** do **SPIN** seria de **67,2 anos.**

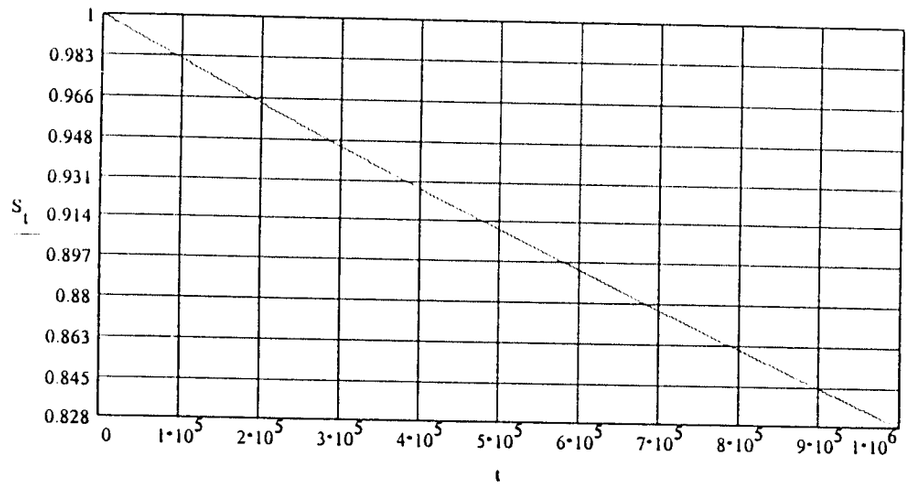
Logo a análise da arquitetura revela quantitativamente aspectos de disponibilidade do equipamento em função de projeto e manutenção. Ou seja, uma fragilidade de projeto pode ser compensada por uma estratégia de manutenção melhorando a disponibilidade do sistema de proteção.

Determinação de S(t) e MTTUF do SPIN por lógica combinacional

$$S(t)_{spin} = S(t)_{uatp} \times S(t)_{utp/au}$$

$t := 0, 10 .. 1000000$

$$S_t := \left[-\left(1.846\,10^{-7}\right) \cdot \left(e^{-0.504 \cdot t} \cdot \cos(0.002) \cdot t - \frac{1}{0.004} \cdot e^{-0.504 \cdot t} \cdot \sin(0.002) \cdot t \right) + e^{-9.429 \cdot 10^{-8} \cdot t} \right]^2$$



$$MTTUF := \int_0^{100000000} \left[-\left(1.846\,10^{-7}\right) \cdot \left(e^{-0.504 \cdot t} \cdot \cos(0.002) \cdot t - \frac{1}{0.004} \cdot e^{-0.504 \cdot t} \cdot \sin(0.002) \cdot t \right) + e^{-9.429 \cdot 10^{-8} \cdot t} \right]^2 dt$$

$MTTUF = 5.303 \cdot 10^6$ anos

O valor encontrado está coerente com equipamentos dessa classe, onde MTTUF superiores a 1 milhão de anos é o requisito mínimo. No caso o *"software"* foi considerado como correto e as falhas contabilizadas seriam pertentencentes aos módulos básicos. As aproximações realizadas sempre tiveram um aspecto pessimista, logo o MTTUF do sistema deve ser melhor que o apresentado.

7. CONCLUSÕES.

Este trabalho fez uma abordagem do ponto de vista de confiabilidade e segurança, em sistemas digitais computadorizados tolerantes a falhas para aplicações críticas. Abordou as principais incertezas que envolvem a qualificação de um sistema computadorizado, apontando inclusive, as dificuldades e resistências de sua utilização em plantas nucleares no mundo. Apresentou aspectos importantes em topologias de circuitos de interfaces de *"hardware"* de sistemas digitais, os quais são fundamentais em termos de filosofia de projeto, quando se desenvolve um sistema dessa natureza.

Apresentou um método de desenvolvimento de sistemas para essa finalidade, com enfoque principal em confiabilidade e segurança em aspectos de *"hardware"*. Mas, como em sistemas digitais computadorizados, não é possível separar-se o *"software"* do *"hardware"*, apresentou os principais aspectos que envolvem o seu desenvolvimento e sua obtenção.

O objetivo principal do trabalho foi sugerir um método para análise de arquiteturas de *"hardware"* digitais, mostrando suas potencialidades, limitações e emprego na análise de arquitetura de um sistema de proteção. De posse dos valores de projeto do SPIN, seria possível efetuar modelos baseados em outra realidade de hipóteses e determinar novos valores de confiabilidade para sua arquitetura.

Não foi objetivo deste trabalho, apresentar a análise de confiabilidade e segurança do sistema de proteção de reatores SPIN. Os valores utilizados como parâmetros de confiabilidade para análise de arquitetura, foram baseados em dados práticos. Estes valores não correspondem aos dados de projeto. Isto porque os dados são de propriedade do fabricante.

Um aspecto que chama a atenção, é a necessidade de testes periódicos. De acordo com enfoque colocado eles são a única alternativa para detecção de falhas não seguras.

O SPIN, de acordo com seu fabricante, foi projetado e implementado visando a execução destes testes, de maneira que o canal em teste seja exercitado sem perda de níveis de segurança durante a sua execução. A aproximação realizada para inclusão de taxas de reparo para falhas não seguras no modelo de *Markov* - devido a existência destes testes - baseou-se em processos de discretização no tempo [31], e procurou realizar uma aproximação para utilização de *Markov* para análise do problema.

Em um processo de análise de confiabilidade e segurança, as hipóteses definem o comportamento do modelo. Assim, a modelagem nada mais é, que o espelho dessas hipóteses. Isso significa que o bom senso deve ser utilizado na modelagem. O conhecimento do problema é fundamental. Várias topologias de modelos podem ser definidas de acordo com o enfoque adotado. A escolha dos mais adequados, devem refletir o comportamento do sistema, mas como estes valores são probabilísticos e normalmente os valores encontram-se na ordem de dezenas até milhares de anos, a adequação do modelo dificilmente é comprovada.

No estudo de caso, assumimos que o *"software"* era adequado e não continha erros. Isto não é verdade, é uma aproximação. Verificamos também, que vários aspectos de diagnósticos de falhas *"hardware"* dependem do *"software"* para cumprir seu papel. Em análises de sistemas computadorizados, pode-se computar efeitos de falhas de *"hardware"* decorrentes de erros no *"software"*. Estas falhas podem ser computadas quantitativamente na análise dos modelos.

Existem diversas linhas de pesquisa que podem dar seqüência ao trabalho enfocado nesta dissertação. Podemos citar dentre elas:

- Técnicas Orientadas ao Objeto para análise e desenvolvimento de softwares de segurança em sistemas críticos.

- Modelagem quantitativa de combinações de arquiteturas de sistemas digitais por processos de Semi-Markov.

- Modelagem de confiabilidade de *"software"* em sistemas digitais de proteção de reatores baseados em aspectos do erro humano.

- Modelagem de confiabilidade e segurança em redes locais de sistemas digitais de proteção.

8. APÊNDICE 1- Classe 1E.

Os sistemas, componentes e estruturas de instalações nucleares são classificadas de acordo com a sua importância para a segurança. Os sistemas elétricos com classificação de segurança são denominados *"Classe 1E"*. Este apêndice aponta os principais requisitos básicos e princípios de qualificação de equipamentos segundo esta classificação [30].

8.1.1 Definição de Equipamentos e Sistemas "Classe 1E".

"Classe 1E" é definida como classificação de segurança para equipamentos elétricos e sistemas que são essenciais para:

- *Desligamento de emergência do Reator.*
- *Isolamento da Contenção.*
- *Resfriamento do núcleo do Reator e Contenção.*
- *Remoção do calor do Reator*
- *Qualquer providência de segurança para prevenir vazamento de material radioativo ao ambiente.*

(IEEE-STD-323)[30].

Evidentemente para projeto e construção de equipamentos "classe 1E", todos os requisitos e ferramentas de análise de segurança devem ser empregados.

(IEEE-STD-323 item 3 e 4).

8.1.2 Vida útil e qualificação

O equipamento classe 1E deve ter uma previsão de vida operacional de 40 anos, com componentes substituídos periodicamente caso a vida útil destes componentes não atinjam este tempo.

(IEEE-STD-323 item 3)

Conclui-se que o conhecimento da expectativa de vida dos componentes é essencial, logo um cálculo de vida operacional de cada componente deve ser levantado através de dados apropriados e um programa de manutenção preventiva deve ser realizado para substituição de componentes em fim de vida operacional.

Pode-se utilizar meios teóricos como por sugestão a norma MIL-HDBK-217F - notice2, para avaliação teórica de índices de confiabilidade. A execução de ensaios de envelhecimento precoce de componentes determina sua expectativa de vida.

A manufatura e uso de equipamentos classe 1E garantem que tais equipamentos em uma planta, atenderão ou excederão seus requisitos durante a vida instalada. Isto é completado através de um programa disciplinado de qualidade assegurada que inclui, projeto, qualificação, controle de qualidade de produção, manutenção, instalação e testes periódicos.

(IEEE-STD-323-item 4).

A regra primária da qualificação assegura que para cada tipo de equipamento classe 1E, o seu projeto e o seu processo de manufatura são tais que há um grande grau de confiança que futuros equipamentos do mesmo tipo terão comportamento igual.

(IEEE-STD-323, item 4).

A qualificação pode ser completada de várias maneiras: testes de tipo, experiência operacional ou análises. Essa técnicas podem se utilizadas individualmente ou em qualquer combinação dependendo da situação particular.

(IEEE-STD-323, item 4).

Verifica-se que a norma não estabelece um procedimento padronizado de qualificação, mas sugere alguns métodos de trabalho de modo superficial. O teste de tipo sugerido é um ensaio que verifica o comportamento funcional do equipamento sob condições extremas e são particulares para cada aplicação.

8.1.3 Princípios de qualificação.

A qualidade de todo equipamento "classe 1E" deve ser demonstrada. É preferível que a demonstração seja feita por testes de tipo no equipamento. A experiência operacional e análises podem ser utilizadas para complementar testes de tipo.

Os princípios e procedimentos para qualificação "classe 1E" incluem:

- *Garantir que os vários métodos de qualificação igualam ou excedem os requisitos e condições de serviço antecipadamente.*
- *Garantir que quaisquer extrapolação ou conclusão seja justificada pela permissão do conhecimento de modos de falha em potencial e mecanismos direcionados a isto.*
- *Qualificação em operação que testa o equipamento instalado cuja vida qualificada é menor que a vida projetada.*
- *Documentação de qualificação.*
- *Qualificação de qualquer interface associada a equipamento "classe 1E".*

(IEEE-STD-323, item 5)

8.1.3.1 Testes de tipo

Os testes de tipo do equipamento com simulações das condições de serviço é o método preferencial. Este processo deve ser utilizado para qualificar grande parte do equipamento. Entretanto, um teste de tipo único, satisfaz a qualificação somente se o equipamento a ser testado é envelhecido, submetido a todas influências ambientais e operando sob condições extremas para garantia que todo equipamento semelhante estará habilitado a operar corretamente durante o tempo requerido.

(IEEE-STD-323, item 5.1).

Verifica-se que a norma aponta vários requisitos a serem cumpridos como objeto de qualificação. Aponta também o teste de tipo como método preferencial para qualificar "grande parte do equipamento", mas faz uma restrição da validade deste ensaio, que deve ser considerado se o equipamento em teste estiver "envelhecido" e submetido a extremas condições ambientais e operacionais. Verifica-se que a norma "IEEE-STD-323 item 6.3.3 - *aging*", aponta:

- *"O objetivo do envelhecimento é colocar as amostras em condições equivalentes à condição de fim de vida operacional".*

- *"Um curto período de envelhecimento térmico meramente simula a vida em serviço; entretanto produz deteriorações quando seguidas por vibrações podendo gerar modos de falha realísticos."*

Verifica-se que as ferramentas para tal ensaio não são sugeridas. Tais condições de simulação de vida são criticadas pela norma MIL-STD-785B, item 50.3.1.3.3. onde observamos:

Simulações precisas do perfil da vida operacional exporiam cada item e cada parte de cada item ao exato tipo de "stress" em nível e duração que sofrerão em serviço. Semelhante teste ideal é raramente praticável. Alguns tipos de "stress" não podem ser combinados em um mesmo teste com facilidade e alguns podem custar mais para serem

reproduzidos em laboratório que o prejuízo de falha em serviço. Note que sobre-stress (envelhecimento) é um caminho válido para acelerar a descoberta de deficiências e defeitos, mas não é um meio válido para comprimir o teste de vida quando a confiabilidade está sendo medida.[29].

Observa-se que o exposto pela norma IEEE-STD-323, se contradiz com os requisitos mais realísticos da norma MIL-STD-785B. Onde o objetivo de avaliação de confiabilidade quantificando-se falhas, não é recomendado através de ensaios de envelhecimento.

9. APÊNDICE 2 - Solução das equações.

A solução do modelo do MTTUF do canal UATP (mod 1) na forma matricial é apresentado a seguir

$$MTTF = k0 + k1 + k2 + k3 + k4 + k5 + k6 \qquad Kn = [\text{cofator } (M\ u)^T \text{ no}] / |Mu|$$

$$Ma = \begin{bmatrix} -4\cdot(\lambda+\lambda i) & \mu & \mu r & 0 & 0 & 0 & 0 & 0 \\ 4\cdot\lambda & -(\mu+3\cdot\lambda+3\cdot\lambda i) & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3\cdot\lambda & -\mu r & 0 & 2\cdot\lambda & 0 & \lambda & 0 \\ 4\cdot\lambda i & 0 & 0 & -3\cdot(\lambda+\lambda i) & \mu & 0 & 0 & 0 \\ 0 & 3\cdot\lambda i & 0 & 3\cdot\lambda & -(2\cdot\lambda i+\mu+2\cdot\lambda) & 0 & 0 & 0 \\ 0 & 0 & 0 & 3\cdot\lambda i & 0 & -2\cdot(\lambda+\lambda i) & \mu & 0 \\ 0 & 0 & 0 & 0 & 2\cdot\lambda i & 2\cdot\lambda & (\mu+\lambda+\lambda i) & 0 \\ 0 & 0 & 0 & 0 & 0 & 2\cdot\lambda i & \lambda i & 0 \end{bmatrix}$$

$$Mu = \begin{bmatrix} 4\cdot(\lambda+\lambda i) & \mu & \mu r & 0 & 0 & 0 & 0 \\ 4\cdot\lambda & (\mu+3\cdot\lambda+3\cdot\lambda i) & 0 & 0 & 0 & 0 & 0 \\ 0 & 3\cdot\lambda & -\mu r & 0 & 2\cdot\lambda & 0 & \lambda \\ 4\cdot\lambda i & 0 & 0 & -3\cdot(\lambda+\lambda i) & \mu & 0 & 0 \\ 0 & 3\cdot\lambda i & 0 & 3\cdot\lambda & -(2\cdot\lambda i+\mu+2\cdot\lambda) & 0 & 0 \\ 0 & 0 & 0 & 3\cdot\lambda i & 0 & -2\cdot(\lambda+\lambda i) & \mu \\ 0 & 0 & 0 & 0 & 2\cdot\lambda i & 2\cdot\lambda & (\mu+\lambda+\lambda i) \end{bmatrix}$$

$$(Mu)^T = \begin{bmatrix} -4\cdot\lambda-4\cdot\lambda i & 4\cdot\lambda & 0 & 4\cdot\lambda i & 0 & 0 & 0 \\ \mu & -\mu-3\cdot\lambda-3\cdot\lambda i & 3\cdot\lambda & 0 & 3\cdot\lambda i & 0 & 0 \\ \mu r & 0 & -\mu r & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -3\cdot\lambda-3\cdot\lambda i & 3\cdot\lambda & 3\cdot\lambda i & 0 \\ 0 & 0 & 2\cdot\lambda & \mu & -2\cdot\lambda i-\mu-2\cdot\lambda & 0 & 2\cdot\lambda i \\ 0 & 0 & 0 & 0 & 0 & 2\cdot\lambda-2\cdot\lambda i & 2\cdot\lambda \\ 0 & 0 & \lambda & 0 & 0 & \mu & -\mu-\lambda-\lambda i \end{bmatrix}$$

$$\text{cof k0} \quad \begin{vmatrix} -\mu - 3\cdot\lambda - 3\cdot\lambda i & 3\cdot\lambda & 0 & 3\cdot\lambda i & 0 & 0 \\ 0 & -\mu r & 0 & 0 & 0 & 0 \\ 0 & 0 & -3\cdot\lambda - 3\cdot\lambda i & 3\cdot\lambda & 3\cdot\lambda i & 0 \\ 0 & 2\cdot\lambda & \mu & -2\cdot\lambda i - \mu - 2\cdot\lambda & 0 & 2\cdot\lambda i \\ 0 & 0 & 0 & 0 & -2\cdot\lambda - 2\cdot\lambda i & 2\cdot\lambda \\ 0 & \lambda & 0 & 0 & \mu & -\mu - \lambda - \lambda i \end{vmatrix}$$

$$k0 \quad \frac{(\mu + 3\cdot\lambda + 3\cdot\lambda i)\cdot\left[\frac{1}{4}\cdot\left(\lambda i\cdot\mu + 2\cdot\lambda^2 + 4\cdot\lambda\cdot\lambda i + 2\cdot\lambda i^2\right)\cdot\left(\lambda i\cdot\mu + \lambda^2 + 2\cdot\lambda\cdot\lambda i + \lambda i^2\right)\right]}{\lambda i^3\cdot\left(24\cdot\lambda^3 + 54\cdot\lambda^2\cdot\lambda i + 36\cdot\lambda^2\cdot\mu + 36\cdot\lambda\cdot\lambda i^2 + 44\cdot\lambda\cdot\mu\cdot\lambda i + 12\cdot\lambda\cdot\mu^2 + 6\cdot\lambda i^3 + 11\cdot\mu\cdot\lambda i^2 + 6\cdot\mu^2\cdot\lambda i + \mu^3\right)}$$

$$\begin{vmatrix} 4\cdot\lambda & 0 & 4\cdot\lambda i & 0 & 0 & 0 \\ 0 & -\mu r & 0 & 0 & 0 & 0 \\ 0 & 0 & -3\cdot\lambda - 3\cdot\lambda i & 3\cdot\lambda & 3\cdot\lambda i & 0 \\ 0 & 2\cdot\lambda & \mu & -2\cdot\lambda i - \mu - 2\cdot\lambda & 0 & 2\cdot\lambda i \\ 0 & 0 & 0 & 0 & -2\cdot\lambda - 2\cdot\lambda i & 2\cdot\lambda \\ 0 & \lambda & 0 & 0 & \mu & -\mu - \lambda - \lambda i \end{vmatrix}$$

$$k1 = \frac{\left(\lambda i\cdot\mu + \lambda^2 + 2\cdot\lambda\cdot\lambda i + \lambda i^2\right)\cdot\left[\lambda\cdot\left(\lambda i\cdot\mu + 2\cdot\lambda^2 + 4\cdot\lambda\cdot\lambda i + 2\cdot\lambda i^2\right)\right]}{\lambda i^3\cdot\left(24\cdot\lambda^3 + 54\cdot\lambda i\cdot\lambda^2 + 36\cdot\mu\cdot\lambda^2 + 36\cdot\lambda\cdot\lambda i^2 + 44\cdot\lambda\cdot\lambda i\cdot\mu + 12\cdot\mu^2\cdot\lambda + 6\cdot\lambda i^3 + 11\cdot\lambda i^2\cdot\mu + 6\cdot\lambda i\cdot\mu^2 + \mu^3\right)}$$

$$\begin{vmatrix} 4\cdot\lambda & 0 & 4\cdot\lambda i & 0 & 0 & 0 \\ -\mu - 3\cdot\lambda - 3\cdot\lambda i & 3\cdot\lambda & 0 & 3\cdot\lambda i & 0 & 0 \\ 0 & 0 & -3\cdot\lambda - 3\cdot\lambda i & 3\cdot\lambda & 3\cdot\lambda i & 0 \\ 0 & 2\cdot\lambda & \mu & -2\cdot\lambda i - \mu - 2\cdot\lambda & 0 & 2\cdot\lambda i \\ 0 & 0 & 0 & 0 & -2\cdot\lambda - 2\cdot\lambda i & 2\cdot\lambda \\ 0 & \lambda & 0 & 0 & \mu & -\mu - \lambda - \lambda i \end{vmatrix}$$

$$k2 \quad \lambda^2\cdot\frac{\left(6\cdot\lambda^4 + 11\cdot\mu\cdot\lambda^2\cdot\lambda i + 6\cdot\mu^2\cdot\lambda i^2 + 36\cdot\lambda i^4 + 36\cdot\lambda^3\cdot\lambda i + 44\cdot\lambda i^2\cdot\lambda\cdot\mu + 30\cdot\mu\cdot\lambda i^3 + 90\cdot\lambda^2\cdot\lambda i^2 + 96\cdot\lambda i^3\cdot\lambda\right)}{\left[\mu r\cdot\left[\lambda i^3\cdot\left(24\cdot\lambda^3 + 54\cdot\lambda^2\cdot\lambda i + 36\cdot\lambda^2\cdot\mu + 36\cdot\lambda\cdot\lambda i^2 + 44\cdot\lambda\cdot\mu\cdot\lambda i + 12\cdot\lambda\cdot\mu^2 + 6\cdot\lambda i^3 + 11\cdot\mu\cdot\lambda i^2 + 6\cdot\mu^2\cdot\lambda i + \mu^3\right)\right]\right]}$$

$$\begin{bmatrix} 4\cdot\lambda & 0 & 4\cdot\lambda i & 0 & 0 & 0 \\ -\mu - 3\cdot\lambda - 3\cdot\lambda i & 3\cdot\lambda & 0 & 3\cdot\lambda i & 0 & 0 \\ 0 & -\mu r & 0 & 0 & 0 & 0 \\ 0 & 0 & -3\cdot\lambda - 3\cdot\lambda i & 3\cdot\lambda & 3\cdot\lambda i & 0 \\ 0 & 2\cdot\lambda & \mu & -2\cdot\lambda i - \mu - 2\cdot\lambda & 0 & 2\cdot\lambda i \\ 0 & \lambda & 0 & 0 & \mu & -\mu - \lambda - \lambda i \end{bmatrix}$$

$$k6 \quad \frac{\left(2\cdot\lambda^2 + 4\cdot\lambda\cdot\lambda i + 8\cdot\lambda\cdot\mu + 2\cdot\lambda i^2 + \mu^2 + 3\cdot\lambda i\cdot\mu\right)\cdot\left|\frac{1}{2}\cdot(3\cdot\lambda - 3\cdot\lambda i + \mu)\right|}{\lambda i\cdot\left(24\cdot\lambda^3 + 54\cdot\lambda^2\cdot\lambda i + 36\cdot\lambda^2\cdot\mu + 36\cdot\lambda\cdot\lambda i^2 + 44\cdot\lambda\cdot\mu\cdot\lambda i + 12\cdot\lambda\cdot\mu^2 + 6\cdot\lambda i^3 + 11\cdot\mu\cdot\lambda i^2 + 6\cdot\mu^2\cdot\lambda i + \mu^3\right)}$$

$$\begin{bmatrix} 4\cdot\lambda & 0 & 4\cdot\lambda i & 0 & 0 & 0 \\ -\mu - 3\cdot\lambda - 3\cdot\lambda i & 3\cdot\lambda & 0 & 3\cdot\lambda i & 0 & 0 \\ 0 & -\mu r & 0 & 0 & 0 & 0 \\ 0 & 0 & -3\cdot\lambda - 3\cdot\lambda i & 3\cdot\lambda & 3\cdot\lambda i & 0 \\ 0 & 2\cdot\lambda & \mu & -2\cdot\lambda i - \mu - 2\cdot\lambda & 0 & 2\cdot\lambda i \\ 0 & 0 & 0 & 0 & -2\cdot\lambda - 2\cdot\lambda i & 2\cdot\lambda \end{bmatrix}$$

$$k7 \quad \frac{\lambda}{\lambda i}\cdot\frac{\left(18\cdot\lambda^2 + 36\cdot\lambda\cdot\lambda i + 18\cdot\lambda i^2 + 7\cdot\lambda i\cdot\mu + 10\cdot\lambda\cdot\mu - \mu^2\right)}{\left(24\cdot\lambda^3 + 54\cdot\lambda^2\cdot\lambda i + 36\cdot\lambda^2\cdot\mu + 36\cdot\lambda\cdot\lambda i^2 + 44\cdot\lambda\cdot\mu\cdot\lambda i + 12\cdot\lambda\cdot\mu^2 + 6\cdot\lambda i^3 + 11\cdot\mu\cdot\lambda i^2 + 6\cdot\mu^2\cdot\lambda i + \mu^3\right)}$$

Determinação de MTTUF (mod 1)

$\mu = 720$ taxa de reparos = um reparo/12 horas

$\mu r = 180$ taxa de reparos após trip do reator

$\lambda = 1$ taxa de falhas = 1 falha/ano

$\lambda i = 0.001$ taxa de falhas inseguras = 0.001 falhas/ano

$$k1 = \frac{(\mu + 3\cdot\lambda + 3\cdot\lambda i)\cdot\left[\frac{1}{4}\cdot\left(\lambda i\cdot\mu + 2\cdot\lambda^2 + 4\cdot\lambda\cdot\lambda i + 2\cdot\lambda i^2\right)\cdot\left(\lambda i\cdot\mu + \lambda^2 + 2\cdot\lambda\cdot\lambda i + \lambda i^2\right)\right]}{\lambda i^3\cdot\left(24\cdot\lambda^3 + 54\cdot\lambda^2\cdot\lambda i + 36\cdot\lambda^2\cdot\mu + 36\cdot\lambda\cdot\lambda i^2 + 44\cdot\lambda\cdot\mu\cdot\lambda i + 12\cdot\lambda\cdot\mu^2 + 6\cdot\lambda i^3 + 11\cdot\mu\cdot\lambda i^2 + 6\cdot\mu^2\cdot\lambda i + \mu^3\right)}$$

$$k2 = \frac{\left(\lambda i\cdot\mu + 2\cdot\lambda^2 + 4\cdot\lambda\cdot\lambda i + 2\cdot\lambda i^2\right)\cdot\left[\lambda\cdot\left(\lambda i\cdot\mu + \lambda^2 + 2\cdot\lambda\cdot\lambda i + \lambda i^2\right)\right]}{\lambda i^3\cdot\left(24\cdot\lambda^3 + 54\cdot\lambda^2\cdot\lambda i + 36\cdot\lambda^2\cdot\mu + 36\cdot\lambda\cdot\lambda i^2 + 44\cdot\lambda\cdot\mu\cdot\lambda i + 12\cdot\lambda\cdot\mu^2 + 6\cdot\lambda i^3 + 11\cdot\mu\cdot\lambda i^2 + 6\cdot\mu^2\cdot\lambda i + \mu^3\right)}$$

$$k3 = \lambda^2\cdot\frac{\left(6\cdot\lambda^4 + 11\cdot\mu\cdot\lambda^2\cdot\lambda i + 6\cdot\mu^2\cdot\lambda i^2 + 36\cdot\lambda i^4 + 36\cdot\lambda^3\cdot\lambda i + 44\cdot\lambda i^2\cdot\lambda\cdot\mu + 30\cdot\mu\cdot\lambda i^3 + 90\cdot\lambda^2\cdot\lambda i^2 + 96\cdot\lambda i^3\cdot\lambda\right)}{\left[\mu r\cdot\left[\lambda i^3\cdot\left(24\cdot\lambda^3 + 54\cdot\lambda^2\cdot\lambda i + 36\cdot\lambda^2\cdot\mu + 36\cdot\lambda\cdot\lambda i^2 + 44\cdot\lambda\cdot\mu\cdot\lambda i + 12\cdot\lambda\cdot\mu^2 + 6\cdot\lambda i^3 + 11\cdot\mu\cdot\lambda i^2 + 6\cdot\mu^2\cdot\lambda i + \mu^3\right)\right]\right]}$$

$$k4 = \frac{\left(\mu^2 + 5\cdot\lambda i\cdot\mu + 6\cdot\lambda i^2 + 8\cdot\lambda\cdot\mu + 12\cdot\lambda\cdot\lambda i + 6\cdot\lambda^2\right)\cdot\left[\frac{1}{3}\cdot\left(\lambda i\cdot\mu + \lambda^2 + 2\cdot\lambda\cdot\lambda i + \lambda i^2\right)\right]}{\lambda i^2\cdot\left(24\cdot\lambda^3 + 54\cdot\lambda^2\cdot\lambda i + 36\cdot\lambda^2\cdot\mu + 36\cdot\lambda\cdot\lambda i^2 + 44\cdot\lambda\cdot\mu\cdot\lambda i + 12\cdot\lambda\cdot\mu^2 + 6\cdot\lambda i^3 + 11\cdot\mu\cdot\lambda i^2 + 6\cdot\mu^2\cdot\lambda i + \mu^3\right)}$$

$$k5 = \frac{\left(\lambda i\cdot\mu + \lambda^2 + 2\cdot\lambda\cdot\lambda i + \lambda i^2\right)\cdot(\lambda\cdot(\mu + 6\cdot\lambda i + 6\cdot\lambda))}{\lambda i^2\cdot\left(24\cdot\lambda^3 + 54\cdot\lambda^2\cdot\lambda i + 36\cdot\lambda^2\cdot\mu + 36\cdot\lambda\cdot\lambda i^2 + 44\cdot\lambda\cdot\mu\cdot\lambda i + 12\cdot\lambda\cdot\mu^2 + 6\cdot\lambda i^3 + 11\cdot\mu\cdot\lambda i^2 + 6\cdot\mu^2\cdot\lambda i + \mu^3\right)}$$

$$k6 = \frac{\left(2\cdot\lambda^2 + 4\cdot\lambda\cdot\lambda i + 8\cdot\lambda\cdot\mu + 2\cdot\lambda i^2 + \mu^2 + 3\cdot\lambda i\cdot\mu\right)\cdot\left[\frac{1}{2}\cdot(3\cdot\lambda + 3\cdot\lambda i + \mu)\right]}{\lambda i\cdot\left(24\cdot\lambda^3 + 54\cdot\lambda^2\cdot\lambda i + 36\cdot\lambda^2\cdot\mu + 36\cdot\lambda\cdot\lambda i^2 + 44\cdot\lambda\cdot\mu\cdot\lambda i + 12\cdot\lambda\cdot\mu^2 + 6\cdot\lambda i^3 + 11\cdot\mu\cdot\lambda i^2 + 6\cdot\mu^2\cdot\lambda i + \mu^3\right)}$$

$$k7 = \frac{\lambda}{\lambda i}\cdot\frac{\left(18\cdot\lambda^2 + 36\cdot\lambda\cdot\lambda i + 18\cdot\lambda i^2 + 7\cdot\lambda i\cdot\mu + 10\cdot\lambda\cdot\mu + \mu^2\right)}{\left(24\cdot\lambda^3 + 54\cdot\lambda^2\cdot\lambda i + 36\cdot\lambda^2\cdot\mu + 36\cdot\lambda\cdot\lambda i^2 + 44\cdot\lambda\cdot\mu\cdot\lambda i + 12\cdot\lambda\cdot\mu^2 + 6\cdot\lambda i^3 + 11\cdot\mu\cdot\lambda i^2 + 6\cdot\mu^2\cdot\lambda i + \mu^3\right)}$$

$MTTUF = (k1 + k2 + k3 + k4 + k5 + k6 + k7)$ $\quad MTTUF = 3.544\cdot10^3$ anos

Modelo simplificado de avaliação de MTTUF do UATP, (mod -2) considerando a existência de taxa de reparo para falhas inseguras.

Mu $\begin{bmatrix} 4\cdot\lambda & \mu & \mu \\ 4\cdot\lambda & -(3\cdot\lambda+\mu) & 0 \\ 0 & 3\cdot\lambda & -(\mu+2\cdot\lambda) \end{bmatrix}$ matriz de transposição

Mut $\begin{bmatrix} -4\cdot\lambda & 4\cdot\lambda & 0 \\ \mu & -3\cdot\lambda-\mu & 3\cdot\lambda \\ \mu & 0 & -\mu-2\cdot\lambda \end{bmatrix}$ $D = -24\cdot\lambda^3$

Determinação dos cofatores.

$\begin{pmatrix} -3\cdot\lambda-\mu & 3\cdot\lambda \\ 0 & -\mu-2\cdot\lambda \end{pmatrix}$ $\frac{1}{24}\cdot(3\cdot\lambda+\mu)\cdot\frac{(\mu+2\cdot\lambda)}{\lambda^3}$ k1

$\begin{pmatrix} 4\cdot\lambda & 0 \\ 0 & -\mu-2\cdot\lambda \end{pmatrix}$ $\frac{1}{6}\cdot\frac{(\mu+2\cdot\lambda)}{\lambda^2}$ k2

$\begin{pmatrix} 4\cdot\lambda & 3\cdot\lambda \\ -3\cdot\lambda-\mu & -\mu-2\cdot\lambda \end{pmatrix}$ $\frac{-1}{(24\cdot\lambda^2)}\cdot(\mu-\lambda)$ k3

Avaliação do modelo.

$\mu = 0.5$ taxa média de reparos = um reparo em cada dois anos.

$\lambda = 0.001$ taxa de falhas inseguras 0,001 falhas/ano

$$MTTUF = \left[\frac{1}{24}\cdot(3\cdot\lambda+\mu)\cdot\frac{(\mu+2\cdot\lambda)}{\lambda^3}\right] + \left[\frac{1}{6}\cdot\frac{(\mu+2\cdot\lambda)}{\lambda^2}\right] + \left[\frac{-1}{(24\cdot\lambda^2)}\cdot(\mu-\lambda)\right]$$

$MTTUF = 1.058\cdot10^7$ anos

Determinação de MTTUF e S(t) para o modelo simplificado do arranjo UATP, com taxa média de reparos para falhas inseguras igual a 0,5 reparo por ano.

$$M \quad \begin{bmatrix} -4\cdot\lambda & \mu & \mu & 0 \\ 4\cdot\lambda & -(3\cdot\lambda+\mu) & 0 & 0 \\ 0 & 3\cdot\lambda & (\mu-2\cdot\lambda) & 0 \\ 0 & 0 & 2\cdot\lambda & 0 \end{bmatrix}$$

$$Mt \quad \begin{bmatrix} -4\cdot\lambda & 4\cdot\lambda & 0 & 0 \\ \mu & -3\cdot\lambda-\mu & 3\cdot\lambda & 0 \\ \mu & 0 & -\mu-2\cdot\lambda & 2\cdot\lambda \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$sI\text{-}Mt \quad \begin{bmatrix} s & 0 & 0 & 0 \\ 0 & s & 0 & 0 \\ 0 & 0 & s & 0 \\ 0 & 0 & 0 & s \end{bmatrix} - \begin{bmatrix} -4\cdot\lambda & 4\cdot\lambda & 0 & 0 \\ \mu & -3\cdot\lambda-\mu & 3\cdot\lambda & 0 \\ \mu & 0 & -\mu-2\cdot\lambda & 2\cdot\lambda \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} s+4\cdot\lambda & 4\cdot\lambda & 0 & 0 \\ -\mu & s+3\cdot\lambda+\mu & -3\cdot\lambda & 0 \\ -\mu & 0 & s+\mu+2\cdot\lambda & -2\cdot\lambda \\ 0 & 0 & 0 & s \end{bmatrix} \qquad s^4+2\cdot s^3\cdot\mu+9\cdot s^3\cdot\lambda+9\cdot s^2\cdot\lambda\cdot\mu+26\cdot s^2\cdot\lambda^2+\mu^2\cdot s^2+24\cdot s\cdot\lambda^3$$

$$S(t) = 1 - P4(t)$$

$$\text{cofator}_{4,1}(A) \quad \begin{bmatrix} -4\cdot\lambda & 0 & 0 \\ s+3\cdot\lambda+\mu & 3\cdot\lambda & 0 \\ 0 & s+\mu+2\cdot\lambda & -2\cdot\lambda \end{bmatrix} = -24\cdot\lambda^3\cdot(1^5) = 24\cdot\lambda^3$$

$$P4(s) = \frac{24\cdot\lambda^3}{s^4+2\cdot s^3\cdot\mu+9\cdot s^3\cdot\lambda+9\cdot s^2\cdot\lambda\cdot\mu+26\cdot s^2\cdot\lambda^2+\mu^2\cdot s^2+24\cdot s\cdot\lambda^3}$$

$$a1 := 0$$

$$a2 := -x^{\left(\frac{1}{3}\right)} + \frac{y}{x^{\left(\frac{1}{3}\right)}} + \frac{2}{3}\cdot\mu + 3\cdot\lambda$$

$$a3 := \frac{1}{2}\cdot x^{\left(\frac{1}{3}\right)} - \frac{1}{2}\cdot\frac{y}{x^{\left(\frac{1}{3}\right)}} + \frac{2}{3}\cdot\mu + 3\cdot\lambda - \frac{1}{2}\cdot i\cdot\sqrt{3}\cdot\left[x^{\left(\frac{1}{3}\right)} + \frac{y}{x^{\left(\frac{1}{3}\right)}}\right]$$

$$a4 := \frac{1}{2}\cdot x^{\left(\frac{1}{3}\right)} - \frac{1}{2}\cdot\frac{y}{x^{\left(\frac{1}{3}\right)}} + \frac{2}{3}\cdot\mu + 3\cdot\lambda + \frac{1}{2}\cdot i\cdot\sqrt{3}\cdot\left[x^{\left(\frac{1}{3}\right)} + \frac{y}{x^{\left(\frac{1}{3}\right)}}\right]$$

S(t) = 1 - P4(t)

$$P4(s) = \frac{24\cdot\lambda^3}{s\cdot(s + a2)\cdot(s + a3)\cdot(s + a4)}$$

Determinação da antitransformada de Laplace

$$\alpha 2 - \alpha 1\cdot 0.504 = 9.429\,10^{-8}$$

$$\alpha 2 + \alpha 1\cdot 0.002 = 8.926\,10^{-10}$$

$$A := \begin{pmatrix} 1 & -0.504 \\ 1 & 0.002 \end{pmatrix} \qquad c := \begin{pmatrix} 9.429\,10^{-8} \\ 8.926\,10^{-10} \end{pmatrix}$$

$$h := \frac{24\cdot\lambda^3}{-a3\cdot(-a3 + a2)}$$

$$A^{-1} = \begin{pmatrix} 0.004 & 0.996 \\ -1.976 & 1.976 \end{pmatrix}$$

$$h = 9.429\,10^{-8} + 8.926\,10^{-10}\,i$$

$$X := A^{-1}\cdot c$$

$$X = \begin{pmatrix} 1.262\,10^{-9} \\ -1.846\,10^{-7} \end{pmatrix}$$

$$a3 = 0.504 - 0.002i$$

$$a4 = 0.504 + 0.002i$$

$$a2 = 9.429\,10^{-8}$$

$$\alpha 1 := -1.846\,10^{-7} \qquad a1 = 0$$

$$\alpha 2 := 1.262\,10^{-9}$$

$$\frac{24\cdot\lambda^3}{s\cdot(s + a2)\cdot(s + a3)\cdot(s + a4)}$$

$$k2 = \frac{24\cdot\lambda^3}{a2\cdot(-a2+a3)\cdot(-a2+a4)} \qquad \frac{24\cdot\lambda^3}{-a2\cdot(-a2+a3)\cdot(a2+a4)}$$

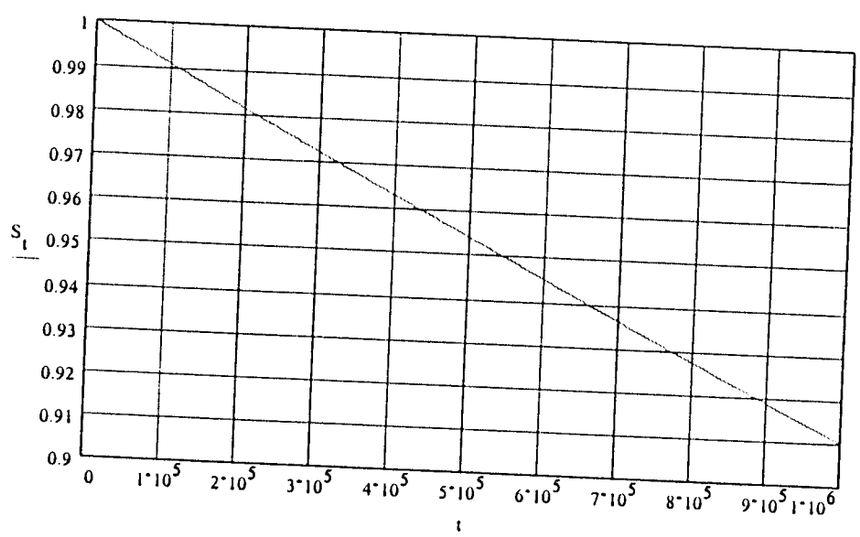
$k2 = -1$

$$k1 = \frac{24\cdot\lambda^3}{(0+a2)\cdot(0+a3)\cdot(0+a4)}$$

$k1 = 1$

$t := 0, 10 .. 1000000$

$$S_t := -\left(1.846\cdot10^{-7}\right)\cdot\left(e^{-0.504\cdot t}\cdot\cos(0.002)\cdot t - \frac{1}{0.004}\cdot e^{-0.504\cdot t}\cdot\sin(0.002)\cdot t\right) + e^{-9.429\cdot10^{-8}\cdot t}$$



$$MTTUF := \int_0^{1000000000} -\left(1.846\cdot10^{-7}\right)\cdot\left(e^{0.504\cdot t}\cdot\cos(0.002)\cdot t - \frac{1}{0.004}\cdot e^{0.504\cdot t}\cdot\sin(0.002)\cdot t\right) + e^{-9.429\cdot10^{-8}\cdot t}\,dt$$

$MTTUF = 1.061\cdot10^7$ anos

Solução do modelo 3, determinação de MTBF e R(t) do UATP

As equações diferenciais para a modelagem do MTBF e R(t) do canal UATP na forma matricial são:

$$P_0(s) = P_0(0)*[sI - A]^{-1} \qquad A = [sI - A]$$

$$P'o(t) = -4\lambda Po(t) + \mu P1(t)$$

$$P'1(t) = 4\lambda Po(t) - (3\lambda + \mu)P1(t)$$

$$P'2(t) = 0 + 3\lambda P1(t)$$

$$\begin{bmatrix} -4\cdot\lambda & \mu & 0 \\ 4\cdot\lambda & -(3\cdot\lambda+\mu) & 0 \\ 0 & 3\cdot\lambda & 0 \end{bmatrix} \qquad T \Rightarrow \begin{bmatrix} -4\cdot\lambda & 4\cdot\lambda & 0 \\ \mu & -3\cdot\lambda-\mu & 3\cdot\lambda \\ 0 & 0 & 0 \end{bmatrix}$$

$$\begin{pmatrix} s & 0 & 0 \\ 0 & s & 0 \\ 0 & 0 & s \end{pmatrix} - \begin{bmatrix} -4\cdot\lambda & 4\cdot\lambda & 0 \\ \mu & -3\cdot\lambda-\mu & 3\cdot\lambda \\ 0 & 0 & 0 \end{bmatrix} \qquad A = \begin{bmatrix} s+4\cdot\lambda & -4\cdot\lambda & 0 \\ -\mu & s+3\cdot\lambda+\mu & -3\cdot\lambda \\ 0 & 0 & s \end{bmatrix}$$

$$\Delta = s^3 + 7\cdot s^2\cdot\lambda + s^2\cdot\mu + 12\cdot s\cdot\lambda^2$$

mas $R(s) = 1 - P2(s)$

cofator $P_{13} = \begin{pmatrix} -4\cdot\lambda & 0 \\ s+3\cdot\lambda+\mu & -3\cdot\lambda \end{pmatrix}$ $\qquad \Delta P2(S) = 12\cdot\lambda^2$

$$P2(s) = \frac{12\cdot\lambda^2}{s^3 + 7\cdot s^2\cdot\lambda + s^2\cdot\mu + 12\cdot s\cdot\lambda^2}$$ e R(t) = 1 - P2(t) então ;

Resolvendo a equação do 3ª grau em "s" , temos:

$$s^3 + 7 \cdot s^2 \cdot \lambda + s^2 \cdot \mu + 12 \cdot s \cdot \lambda^2 = 0$$

$$\begin{matrix} a1 \\ a2 \\ a3 \end{matrix} \quad \begin{bmatrix} 0 \\ \frac{7}{2} \cdot \lambda + \frac{1}{2} \cdot \mu - \frac{1}{2} \cdot \sqrt{\lambda^2 + 14 \cdot \lambda \cdot \mu + \mu^2} \\ \frac{7}{2} \cdot \lambda + \frac{1}{2} \cdot \mu + \frac{1}{2} \cdot \sqrt{\lambda^2 + 14 \cdot \lambda \cdot \mu + \mu^2} \end{bmatrix}$$

raizes do polinômio

Executando a o inverso de Laplace

$$P2(s) = \frac{12 \cdot \lambda^2}{s \cdot (s + a2) \cdot (s + a3)} \qquad P2 = \frac{K1}{s} + \frac{K2}{s + a2} + \frac{K3}{s + a3}$$

$\mu := 730$ um reparo em média a cada 12 horas.

$\lambda := 1$ taxa de falhas por módulo igual a uma falha por ano

$t := 0, 1 .. 100$

$$a2 := \frac{7}{2} \cdot \lambda + \frac{1}{2} \cdot \mu - \frac{1}{2} \cdot \sqrt{\lambda^2 + 14 \cdot \lambda \cdot \mu + \mu^2}$$

k1 = 1

$$a3 := \frac{7}{2} \cdot \lambda + \frac{1}{2} \cdot \mu + \frac{1}{2} \cdot \sqrt{\lambda^2 + 14 \cdot \lambda \cdot \mu + \mu^2}$$

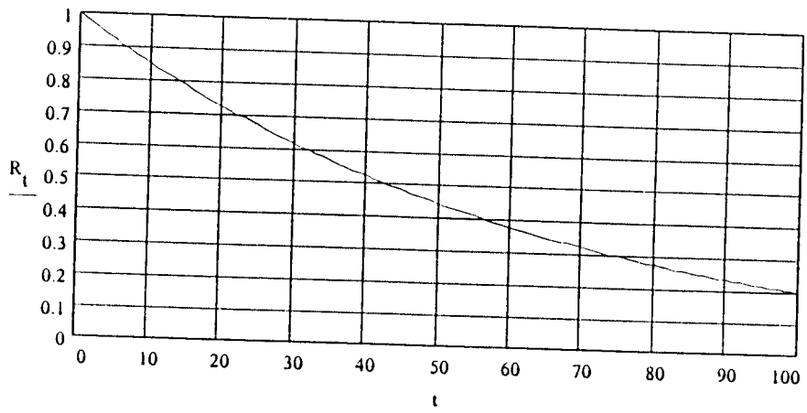
$$k2 := \frac{12 \cdot \lambda^2}{-a2 \cdot (-a2 + a3)}$$

$$k3 := \frac{12 \cdot \lambda^2}{-a3 \cdot (-a3 + a2)}$$

Invertendo a transformada de laplace temos:

$$R_t = -\left(k2 \cdot e^{-a2 \cdot t} + k3 \cdot e^{-a3 \cdot t}\right)$$

Análise de comportamento



Determinação do MTBF da arquitetura UATP

$$MTBF = \int_0^{10000} -k2 \cdot e^{-a2 \cdot t} - k3 \cdot e^{-a3 \cdot t}\, dt$$

$MTBF = 61.417$ anos

Solução do modelo 4, determinação de MTTUF canal UTP/AU pelo método simplificado.

A modelagem de MTTUF do canal UTP/UA na forma matricial será:

$MTTF = k0 + k1 + k2$ $\qquad$ $Kn = [\text{cofator } (M\,u)^T \text{ no}] / |Mu|$

$$Ma = \begin{bmatrix} -(2\cdot\lambda i + 2\cdot\lambda + \lambda a) & \mu & 0 & 0 \\ 2\cdot\lambda + \lambda a & -\mu & \lambda a + \lambda & 0 \\ 2\cdot\lambda i & 0 & -(\lambda i + \lambda + \lambda a) & 0 \\ 0 & 0 & \lambda i & 0 \end{bmatrix}$$

$$Mu = \begin{bmatrix} -(2\cdot\lambda i + 2\cdot\lambda + \lambda a) & \mu & 0 \\ 2\cdot\lambda + \lambda a & -\mu & \lambda a + \lambda \\ 2\cdot\lambda i & 0 & -(\lambda i + \lambda + \lambda a) \end{bmatrix} \qquad D = -2\cdot\mu\cdot\lambda i^2$$

$$Mu^T = \begin{bmatrix} -2\cdot\lambda i - 2\cdot\lambda - \lambda a & 2\cdot\lambda + \lambda a & 2\cdot\lambda i \\ \mu & -\mu & 0 \\ 0 & \lambda a + \lambda & -\lambda i - \lambda - \lambda a \end{bmatrix}$$

$$\begin{pmatrix} -\mu & 0 \\ \lambda a + \lambda & -\lambda i - \lambda - \lambda a \end{pmatrix} \qquad k0 = \frac{1}{2}\cdot\frac{(\lambda i + \lambda + \lambda a)}{\lambda i^2}$$

$$\begin{pmatrix} 2\cdot\lambda + \lambda a & 2\cdot\lambda i \\ \lambda a + \lambda & -\lambda i - \lambda - \lambda a \end{pmatrix} \qquad k1 = \frac{1}{2}\cdot\frac{\left(4\cdot\lambda\cdot\lambda i + 2\cdot\lambda^2 + 3\cdot\lambda\cdot\lambda a + 3\cdot\lambda a\cdot\lambda i + \lambda a^2\right)}{\left(\mu\cdot\lambda i^2\right)}$$

$$\begin{pmatrix} 2\cdot\lambda + \lambda a & 2\cdot\lambda i \\ \mu & 0 \end{pmatrix} \qquad k2 = \frac{1}{\lambda i}$$

Avaliação do MTTUF do canal UTP/AU , no caso a taxa de falhas do dispositivo eletromecânico AU é mais baixa que o dispositivo eletrônico UTP.

$\lambda := 1$ uma falha a cada ano

$\lambda a := 0.1$ uma falha a cada 10 anos

$\lambda i := 0.001$ uma falha insegura a cada 1000 anos

$\mu := 730$ taxa de reparo igual a um reparo em 12 horas

$$k0 := \frac{1}{2} \cdot \frac{(\lambda i + \lambda + \lambda a)}{\lambda i^2}$$

$$k1 := \frac{1}{2} \cdot \frac{\left(4 \cdot \lambda \cdot \lambda i + 2 \cdot \lambda^2 + 3 \cdot \lambda \cdot \lambda a + 3 \cdot \lambda a \cdot \lambda i + \lambda a^2\right)}{\left(\mu \cdot \lambda i^2\right)}$$

$$k2 := \frac{1}{\lambda i}$$

$$MTTUF := k0 + k1 + k2$$

$MTTUF = 5.531 \cdot 10^5$ anos

Determinação da confiabilidade R(t) para o arranjo 2/4 UTP/AU.

Utlizando-se aproximação semelhante à análise efetuada para o arranjo UATP, temos um modelo de 03 estados, com equações idênticas cuja solução será:

$\lambda u := 1$ taxa de falhas por módulo igual a uma falha por ano

$\lambda a := 0.1$ taxa de falhas do dispositivo eletromecânico uma falha a cada 10 anos

$\mu := 730$ um reparo em média a cada 12 horas.

$\lambda := 2 \cdot \lambda u + \lambda a$

$t := 0, 1 .. 50$

$$b2 := \frac{7}{2} \cdot \lambda + \frac{1}{2} \cdot \mu - \frac{1}{2} \cdot \sqrt{\lambda^2 + 14 \cdot \lambda \cdot \mu + \mu^2}$$

$$b3 := \frac{7}{2} \cdot \lambda + \frac{1}{2} \cdot \mu + \frac{1}{2} \cdot \sqrt{\lambda^2 + 14 \cdot \lambda \cdot \mu + \mu^2}$$

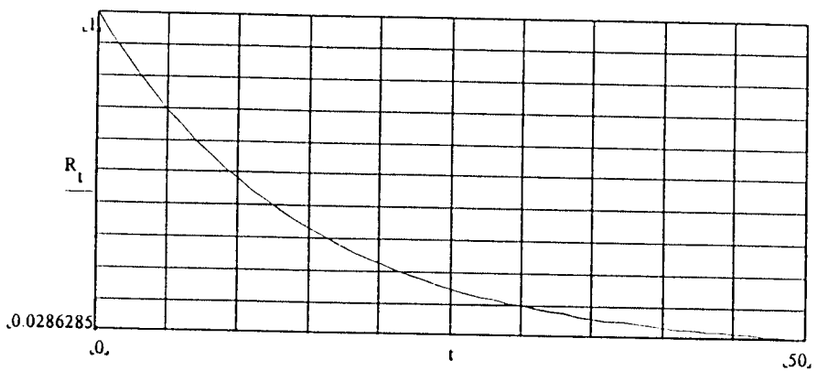
$$p2 := \frac{12 \cdot \lambda^2}{-b2 \cdot (-b2 + b3)}$$

$$p3 := \frac{12 \cdot \lambda^2}{-b3 \cdot (-b3 + b2)}$$

invertendo a transformada de laplace temos:

$$R_t := -\left(p2 \cdot e^{-b2 \cdot t} + p3 \cdot e^{-b3 \cdot t}\right)$$

Análise de comportamento



Determinação do MTBF da arquitetura UTP/AU

$$MTBF := \int_0^{10000} -p2 \cdot e^{-b2 \cdot t} - p3 \cdot e^{-b3 \cdot t}\, dt$$

MTBF = 14.072 anos

10. REFERÊNCIAS BIBLIOGRÁFICAS.

[1] IVES, G. Digital Systems - Review of Safety Applications. ***Nucl. Eng. Int.***, Instrumentation & Control. p 37-40. 1994

[2] KEIPER, J. T. Application of Digital Control Systems in Nuclear Power Plants. NUCLEAR ENGINEERING CONFERENCE ASME/JSME. v. 2. p 783-788. 1993.

[3] PAULA, H. M.; ROBERTS M W.; BATTLE, R. E. Reliability Performance of Fault-Tolerant Digital Control Systems. ***Plant/Oper. Prog.***, v 10. n 2. p 115-128. 1991.

[4] UTENA, S.; SUZUKI, T.; ASANO, H.; SAKAMOTO, H. Development of the BWR Safety Protection System with a new Digital Control System. INTERNATIONAL SYMPOSIUM OF NUCLEAR POWER PLANT INSTRUMENTATION AND CONTROL. Tokyo, Japan. 1992.

[5] DIAS, F J. O.; COELHO, M. M. Qualificação de equipamentos de segurança. EPUSP. São Paulo. 1989.

[6] KEATS, A.B. Failsafe design criteria for computer based reactor protection systems. ***Nucl. Energy***, vol 19. n. 6. p. 423-428. 1980.

[7] CHOU, Q.B.; ACCHIONE, P. N.; HOHENDORF, R. J. Digital Technology in Nuclear Power Plants - White Knight or Black Hole? TOPICAL MEETING ON NUCLEAR PLANT INSTRUMENTATION, CONTROL AND MAN-MACHINE INTERFACE TECHNOLOGIES. Oak-Ridge, Tenn. U.S.A. 1993. p. 366-373.

[8] MCCORMICK, N.J. ***Reliability and Risk Analysis***. New York, N. Y. Academic, 1981.

[9] SHITARA, N. Avaliação da Confiabilidade do Subsistema de Suprimento de Energia pelo Método de Ärvore de Falhas. INPE, S. J. Campos-SP. 1991.

[10] MELNIKOF, S.,S.,S; AVELINO,V.,F; GIACOMINI, R.,C. Software em Sistemas de Segurança de Plantas Nucleares. EPUSP SP. 1996.

[11] STAVRIANIDIS, P. Reliability and Uncertainty Analysis of Hardware Failures of an Electronic Programmable System. Factory Mutual Research Corporation, Norwood. Não paginado. 1991. (MA 02062).

[12] HUNNS, D. M; WAINWRIGHT, N. Software-based protection for Sizewell B: the regulator's perspective. ***Nucl. Eng. Int.,*** p. 38-40. Sept. 1991.

[13] HUNNS, D. M; WAINWRIGHT, N. The UK. Regulator's Approach to the Acceptance of a Software-Based Protection System for Sizeweel B. In: INTERNATIONAL SYMPOSIUM ON NUCLEAR POWER PLANT I&C. Tokyo. May 18-22, 1992.

[14] KAKEHI, A; OKUTAMI, T; SAKAMOTO, H. Microprocessor- Based Fault-Tolerant Reactor Control and Information System. IEEE ***Trans. Energy Convers.***, v. 5, n. 1, p. 52-57, 1990.

[15] WHITE, R. M; BOETTCHER, D. B. Putting Sisewell B digital protection in context ***Nucl. Eng. Int.,*** Instrumentation & Control. p. 41-42, April 1994

[16] MATRAS, J. R. Criteria for Computer Systems used in the design of Nuclear Generation Plant Safety Systems ,.TOPICAL MEETING ON NUCLEAR PLANT INSTRUMENTATION, CONTROL AND MAN-MACHINE INTERFACE TECHNOLOGIES. Oak Ridge, Tenn. 1993. p. 397-403.

[17] KORSAH, K; CLARK; R. L; ANTONESCU, C. Qualification Issues for Advanced Light Reactor Protection Systems. TOPICAL MEETING ON NUCLEAR PLANT INSTRUMENTATION, CONTROL AND MAN-MACHINE INTERFACE TECHNOLOGIES. Oak Ridge, Tenn. 1993. p. 415-423.

[18] SOUZA, J. M. de; MARTINI, M. R. B. Avaliação da Confiabilidade de Sistemas. 2° SIMPÓSIO EM SISTEMAS DE COMPUTADORES TOLERANTES A FALHAS. Campinas, SP. 1987, p. 5-44.

[19] BUSSAC, J. P; JOVER, P; CONFLANT, M. The Introduction of Computer Systems into Nuclear Power Plant Instrumentation and Control: The French Safety Approach. INTERNATIONAL SYMPOSIUM ON NUCLEAR POWER PLANT INSTRUMENTATION AND CONTROL. May, 18-22, 1992, Tokyo. Não paginado.

[20] KIM, S; JANG, I. H; LEE, Y. R; KOO, J. M; HAN, J. B. PLD Based Reactor Protection System. NUCLEAR POWER PLANT INSTRUMENTATION, CONTROL AND HUMAN-MACHINE INTERFACE TECHNOLOGIES. May, 6-9, 1996. Penn, p 179-182.

[21] BASTL, W; WACH, D. Qualification of an Advanced Digital Safety System. NUCLEAR POWER PLANT INSTRUMENTATION, CONTROL AND HUMAN-MACHINE INTERFACE TECHNOLOGIES. May, 6-9, 1996. Penn, p 505-512..

[22] KORSAH, K; ANTONESCU, C. A Survey of Issues Associated with Microprocessor-Based Reactor Protection System Hardware. ASME/ JSME Nuclear Engineering Conference - v.2, p. 751-755, ASME 1993.

[23] WERNER, C. L; WASSEL, W. W; NOVAK, V. Modernising the Temelin VVER Power Plant. Nuclear Power Progress. ***Mod. Power Syst.***, p. 34-37, July, 1993.

[24] MERLIN GERIN S. E. S. DEPARTMENT. SPIN, Nuclear Reactor Protection (catalogo), Franca, Grenoble [s.d.], p. 1-29.

[25] BRILL, R. W. High Integrity software guideline development for Nuclear Power Plants. NUCLEAR POWER PLANT INSTRUMENTATION, CONTROL AND

HUMAN-MACHINE INTERFACE TECHNOLOGIES. May, 6-9, 1996. Penn, p. 513-518.

[26] SIEWIOREK, D. P; SWARZ, ***R. S. Reliable Computer Systems: Design and Evaluation***. 2.ed. Digital. U.S.A. 1992.

[27] LAWRENCE, J. D. ***Software Reliability and Safety in Nuclear Protection Reactor***. U.S.A. Calif.: June, 1993, (Lawrence Livermore National Laboratory-Pub-UCRL-ID-114839).

[28] DIAS, F. J. da S. Confiabilidade e Segurança de Sistemas Eletrônicos. EPUSP, 1989.

[29] MILITARY STANDARD 785B - Reliability Program For Systems And Equipment Development And Production. 1980. (MIL-STD 785B)

[30] INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS. Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations. 1974. (IEEE std 323-1974).

[31] CASSANDRAS, C. G. ***Discrete Event Systems, Modelling and Performance Analysis***. Boston, Mass. Academic. 1993

[32] LAWRENCE, J. D. Software Safety Hazard Analysis. U.S.A. Calif. Oct. 1995. (Lawrence Livermore National Laboratory-Pub-UCRL-ID-122514).

[33], INTERNATIONAL ELECTROTECHNICAL COMMISSION. Software for Computers in the Safety Systems of Nuclear Power Stations. 1986. (IEC- 880)

[34] INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS, Standard Criteria for Digital Computers in Safety of Nuclear Power Generations, 1993. (IEEE 7-4.3.2).

[35] MathCad 5.0 for Windows, Mathsoft Inc. 1994.

[36] MILITARY HANDBOOK 217F Notice 2, "Reliability Prediction of Electronic Equipment", 1995. (MIL-HDBK-217F).

[37] JEAG4609, "Aplication Criteria for Programmable Digital Computer System in Safety-Related Systems of Nuclear Power Plants", Japan, 1989. (JEAG4609).

[38] BELL COMMUNICATIONS RESEARCH. ***"Reliability Prediction Procedure For Electronic Equipment"***. N.J. July 1988. (BELLCORE).

[39] INTERNATIONAL ELECTROTECHNICAL COMMISSION. "General Principles Of Nuclear Instrumentation". (supplement A). Genéve. Suisse, 1969. (IEC-231A).