UMA MODELAGEM DAS INCERTEZAS ASSOCIADAS A FALHAS DE CAUSA COMUM CONSIDERANDO DIVERSIDADE E ENVELHECIMENTO

Mauricio Correia Sant'Ana

TESE SUBMETIDA AO CORPO DOCENTE DA COORDENAÇÃO DOS PROGRAMAS DE PÓS-GRADUAÇÃO DE ENGENHARIA DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE DOUTOR EM CIÊNCIAS EM ENGENHARIA NUCLEAR.

Aprovada por:

Prof. Paulo Fernando Ferreira Frutuoso e Melo, D.Sc.

Prof. Antônio Carlos Marques Alvim, Ph.D.

Prof. Cláudio Márcio do Nascimento Abreu Pereira, D.Sc.

Prof. Júlio César Silva Neves, D.Sc.

Prof. Celso Marcelo Franklin Lapa, D.Sc.

RIO DE JANEIRO, RJ - BRASIL
FEVEREIRO DE 2006

SANT'ANA, MAURICIO CORREIA

Uma Modelagem das Incertezas Associadas a Falhas de Causa Comum considerando Diversidade e Envelhecimento [Rio de Janeiro] 2006

XII, 95 p. 29,7 cm (COPPE/UFRJ, D.Sc., Engenharia Nuclear, 2006)

Tese – Universidade Federal do Rio de Janeiro, COPPE

1. Falhas de Causa Comum
2. Diversidade
3. Envelhecimento

I. COPPE/UFRJ II. Título (série)

A Deus, princípio, meio e fim.

Aos meus pais, por acreditarem que tudo isto seria possível e investirem em mim.

Ao meu filho Bruno, motivação para meu trabalho e minha alegria.

AGRADECIMENTOS

Ao Prof. Paulo Fernando F. Frutuoso e Melo, por sua prestatividade, dedicação e críticas construtivas, sempre visando o aprimoramento do texto final e, especialmente, por sua aceitação em me orientar mais uma vez.

Aos Profs. Antônio Carlos Marques Alvim, Celso Marcelo Franklin Lapa, Cláudio Márcio do Nascimento Abreu Pereira e Júlio César Silva Neves, por aceitarem participar da minha banca e terem dedicado parte do seu tempo à leitura de meu trabalho.

Ao doutor Pedro Luiz da Cruz Saldanha, da Comissão Nacional de Energia Nuclear, incansável e sempre solícito, pelo incentivo, pelas dicas e pela cessão de literatura fundamental para a elaboração desta tese.

Aos funcionários do Programa de Engenharia Nuclear, Tânia, Reginaldo, Josevalda e Ana, por toda a paciência e apoio ao longo de todo esse tempo.

Ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), pelo apoio financeiro, fundamental, especialmente nos casos de aquisição de material didático.

A todos os amigos com os quais tive o prazer de conviver ao longo de toda este tempo, com menção especial a Pauli e Vanessa Garcia, Laís Alencar, Vinícius Damaso e Patrícia Crossetti, pelo apoio, dicas, cessão de material didático, e pelo bom humor, sempre presente em todos.

Resumo da Tese apresentada à COPPE/UFRJ como parte dos requisitos necessários para a obtenção do grau de Doutor em Ciências (D.Sc.)

UMA MODELAGEM DAS INCERTEZAS ASSOCIADAS A FALHAS DE CAUSA COMUM CONSIDERANDO DIVERSIDADE E ENVELHECIMENTO

Mauricio Correia Sant'Ana

Fevereiro/2006

Orientador: Paulo Fernando Ferreira Frutuoso e Melo

Programa: Engenharia Nuclear

Muitos sistemas são projetados com o uso de equipamentos redundantes. Como resultado, tem-se que a maioria dos registros de falha em tais plantas referem-se a falhas de componentes múltiplos, que podem ser resultado de falhas independentes de cada componente ou serem provenientes de um único evento que torna os múltiplos componentes indisponíveis (um evento de falha dependente). Os eventos de falhas dependentes conhecidos como falhas de causa comum são, usualmente, os maiores contribuintes para o risco apresentado por operações de plantas de potência nucleares.

Entre as estratégias de defesa mais utilizadas para inibir ou, pelo menos, diminuir as conseqüências das falhas de causa comum, está o uso da diversidade, que busca diminuir os fatores de acoplamento existentes entre os componentes redundantes.

Além disso, a incorporação do envelhecimento na descrição da confiabilidade de um componente e dos processos de manutenção é importante, dado que o envelhecimento pode ter impacto significativo tanto na confiabilidade quanto na indisponibilidade dos componentes.

Com isto, este trabalho busca estudar a influência da diversidade e do envelhecimento na probabilidade de falha de sistemas, e apresentar um novo modelo que leve estes fatores em consideração e procura modelá-los explicitamente. Um enfoque especial é dado à avaliação das incertezas inerentes ao processo de quantificação.

Abstract of Thesis presented to COPPE/UFRJ as a partial fulfillment of the requirements for the degree of Doctor of Science (D. Sc.)

A MODELING OF THE UNCERTAINTIES ASSOCIATED TO COMMON CAUSE FAILURES CONSIDERING DIVERSITY AND AGEING

Mauricio Correia Sant'Ana

February/2006

Advisor: Paulo Fernando Ferreira Frutuoso e Melo

Department: Nuclear Engineering

Many systems are designed with redundant equipment. As a consequence, it can be seen that most of the registered failure data in such plants are related to multiple component failures, which result from independent failures of each component or stem from unique events, so that multiple components may become unavailable (a dependent failure event). Those dependent failure events known as common cause failures usually are the major contributors to the risk associated with the operation of nuclear power plants.

One of the defense strategies commonly used to inhibit or, at least, to decrease the consequences of common cause failures is the use of diversity, which is applied to decrease the existing coupling factors between redundant components.

Moreover, the incorporation of aging in the reliability modeling of a component and the maintenance processes is important, since aging significantly impacts on the component reliability and unavailability.

Therefore, this work presents a study of the influence of diversity and aging in the probability of system failures, and also a new model which takes these factors into consideration by explicitly modeling them. A special approach has been devised to consider the inherent uncertainties in the quantification of these values.

SUMÁRIO

Pág.

1. Introdução.....1

2. Metodologia para Análise de Eventos de Causa Comum.....10

2.1. Introdução.....10

2.1.1. A Mecânica da Falha.....10

2.1.2. Fatores de Acoplamento.....11

2.1.3. Táticas Defensivas.....11

2.2. Elementos-chave do sistema.....12

2.3. Estágio 1: Desenvolvimento do Modelo Lógico.....12

2.4. Estágio 2 : Identificação dos Grupos de Componentes de Causa Comum...13

2.5. Estágio 3: Modelo de Causa Comum e Análise dos Dados.....14

2.5.1. Definição dos Eventos Básicos de Causa Comum.....14

2.5.2. Seleção para os Modelos de Probabilidade para os Eventos Básicos de Causa Comum.....15

2.5.3. Classificação e Exame dos Dados.....15

2.5.4. Estimação dos Parâmetros.....17

2.5.5. Avaliação de Incertezas nas Estimativas dos Parâmetros.....18

2.6. Estágio 4: Quantificação do Sistema e Interpretação de Resultados.....19

3. O Impacto da Diversidade em FCC.....21

3.1.Introdução.....21

3.2. Uso de Meios (Recursos) Redundantes e Diversos.....22

3.3. O efeito da variabilidade ambiental entre as FCC.....26

3.4. O Modelo de Hughes Generalizado.... 28

3.4.1. Cálculo da confiabilidade do sistema com uso de Diversidade Falha.....30

4. Avaliação e Modelagem de Dependência Temporal.....33

4.1. Avaliação de Tendência ao Envelhecimento.....33

4.1.1. Introdução.....33
4.1.2. Testando Tendências.....34
4.2. Modelagem de Taxas de Falha Dependentes do Tempo.....39
4.2.1. Introdução.....39
4.2.2. Definição de Conceitos Inerentes à Estimação de Taxas de Falha.....41
4.2.3. Estimação Paramétrica de Taxas de Falha.....43

5. Modelagem de Incertezas em Análises de Risco.....46
5.1. Introdução.....46
5.2. Modelos Aplicados à Análise de Risco.....47
5.2.1. Introdução.....47
5.2.2. Critérios para aceitação de um Modelo.....48
5.2.3. Incertezas em Modelos.....49
5.3. Análise de Incerteza do Modelo, considerando Diversidade.....51
5.4. Análise de Incerteza do Modelo Selecionado, considerando Envelhecimento.....52
5.4.1. Intervalo de Confiança para $\lambda(t)$, baseado na Aproximação Assintótica de Normalidade.....54
5.5. Modelagem de Incertezas considerando Diversidade e Envelhecimento.....54

6. Exemplos Práticos.....59
6.1. Introdução.....59
6.2. 1º. Exemplo: Geradores Diesel em uma Usina Nuclear.....59
6.3. 2º. Exemplo: Sistema de Motores Diesel.....62
6.4. 3º. Exemplo: Geradores Diesel em uma Usina Nuclear.....67

7. Conclusões e Recomendações.....74

Referências Bibliográficas.....77

Apêndice A: Glossário.....84

Apêndice B: Dados de Falha dos Componentes.....92

NOMENCLATURA

- **APS** – Avaliação Probabilística de Segurança.
- **C. C.** – Causa Comum.
- $E(\pi_A(E))$ - Valor esperado da probabilidade de falha do componente *A*, quando este se encontra em um ambiente *E*.
- **EMV** – Estimador de Máxima Verossimilhança.
- **FCC** - Falhas de causa comum.
- ***IC*** – Intervalo de Confiança.
- ***IF* –** Intensidade de falhas.
- ***PP* –** Processo de Poisson.
- ***PPH* –** Processo de Poisson Homogêneo.
- ***PPNH* –** Processo de Poisson não Homogêneo.
- ***PR* –** Processo de Renovação.

LISTA DE FIGURAS

Figura 1.1 – Curva típica mostrando a evolução da taxa de falha de componentes mecânicos com o tempo.....8
Figura 6.1 – Gráfico da evolução da taxa de falha do sistema GD-1A / GD-1B com o tempo.....62
Figura 6.2 – Gráfico da evolução da taxa de falha do componente DG3 com o tempo..65
Figura 6.3 – Gráfico da evolução da taxa de falha do componente DG4 com o tempo..65
Figura 6.4 – Gráfico da evolução da taxa de falha do sistema DG3 / DG4 com o tempo.....66
Figura 6.5 – Gráfico da evolução da probabilidade de falha do sistema DG3 / DG4 com o tempo.....66
Figura 6.6 – Gráfico da evolução da probabilidade de falha do sistema DG3 / DG4 com o tempo, mostrando a convergência das probabilidades com o tempo.....67
Figura 6.7 – Gráfico da evolução da taxa de falha do componente GD-A com o tempo.....70
Figura 6.8 – Gráfico da evolução da taxa de falha do componente GD-C com o tempo.....70
Figura 6.9 – Gráfico da evolução da taxa de falha do sistema GD-A/ GD-C com o tempo.....71
Figura 6.10 – Gráficos da evolução da probabilidade de falha do sistema GD-A/GD-C com o tempo.....71
Figura 6.11 – Gráfico da variação percentual entre as probabilidades de falha, quando consideradas taxas de falhas variáveis no tempo e constantes, e para dois casos-exemplo (Tempo < 14.000h).....72
Figura 6.12 – Gráfico da variação percentual entre as probabilidades de falha, quando consideradas taxas de falhas variáveis no tempo e constantes, e para dois casos-exemplo (Tempo < 100.000h). 73
Figura A.1 – Interações entre o Processo de Poisson e o Processo de Renovação dão origem ao Processo de Poisson Homogêneo.....88

LISTA DE TABELAS

Tabela 4.1: Tipo de tendência apresentada pelos dados em função dos valores calculados para os testes.....38
Tabela 6.1: Resultado calculado de teste para tendência para o sistema composto por GD-1 e GD-2 e respectiva estatística correspondente ao valor obtido.....60
Tabela 6.2: Resultados calculados de testes para tendências para o GD-1 e respectivas estatísticas correspondentes aos valores obtidos.....60
Tabela 6.3: Resultados calculados de testes para tendências para o GD-2 e respectivas estatísticas correspondentes aos valores obtidos. 61
Tabela 6.4: Resultado calculado de teste para tendência para o sistema composto por DG3 e DG4 e respectiva estatística correspondente ao valor obtido.....63
Tabela 6.5: Resultados calculados de testes para tendências para o DG3 e respectivas estatísticas correspondentes aos valores obtidos. 63
Tabela 6.6: Resultados calculados de testes para tendências para o DG4 e respectivas estatísticas correspondentes aos valores obtidos. 64
Tabela 6.7: Resultado calculado de teste para tendência para o sistema composto por GD-A e GD-C e respectiva estatística correspondente ao valor obtido. 68
Tabela 6.8: Resultados calculados de testes para tendências para o GD-A e respectivas estatísticas correspondentes aos valores obtidos. 68
Tabela 6.9: Resultados calculados de testes para tendências para o GD-C e respectivas estatísticas correspondentes aos valores obtidos. 69
Tabela A.1: Propriedades dos Processos de Poisson, de Poisson Homogêneo e de Renovação.....89

Capítulo 1 - Introdução

Redundância é uma técnica usada para aumentar a confiabilidade de sistemas, sem nenhuma mudança na confiabilidade das unidades individuais que o formam. Tal técnica consiste no uso de um ou mais componentes adicionais, similares ou não, de modo a se efetuar a mesma função do componente inicialmente existente. Há diferentes tipos de redundância: ativa, reserva ou *k*-de-*n* unidades, uniforme ou diversa, etc. (DHILLON & YANG, 1997). Cada qual tem suas vantagens e desvantagens. O uso de redundância tem como objetivo aumentar a confiabilidade do sistema como um todo. Uma atenção cuidadosa é dada à escolha do tipo de redundância a ser usada, de modo a melhorar a confiabilidade global do sistema pela consideração de vários fatores (DHILLON & YANG, 1997).

Sistemas de engenharia, em especial sistemas de proteção, são, freqüentemente, projetados com o uso de redundância e técnicas de lógica de votação (lógica de votação *k*-de-*n*: são necessários pelo menos *k* componentes falhos, de um total de *n*, para que um sistema falhe), de modo a se conseguir uma alta confiabilidade. Estas técnicas são, usualmente, aplicadas em nível de subsistema, ou componente mais importante, do que em nível de componente básico. O critério importante na decisão de aplicação de redundância é a confiabilidade relativa do subsistema e a exigida para o sistema.

Conforme FLEMING (1975) e DHILLON & YANG (1997), na realização da análise de confiabilidade de sistemas de engenharia redundantes, geralmente, é considerada a suposição de falhas independentes. Isto pode ou não ser uma situação real, visto que o sistema redundante pode estar sujeito a FCC. No passado, a ocorrência de FCC, nas análises de confiabilidade, era negligenciada. Atualmente, atenção crescente vem sendo dada à ocorrência de FCC durante a análise de redundância de sistemas de engenharia.

Segundo WATSON & EDWARDS (1979), "Uma FCC é o resultado de um evento, ocorrido em um tempo aleatório, o qual, em função das dependências, causa uma coincidência de estados de falha de componentes em dois ou mais canais separados de um sistema redundante, podendo levar à falha do sistema, em realizar sua função pretendida". Por exemplo (KVAM, 1996), em uma instalação nuclear, as chances de dano ao núcleo podem ser diminuídas por meio da incorporação de dois ou mais geradores diesel em reserva à linha de fornecimento de potência, em um evento em que

a potência externa da planta é interrompida. Porém, tal aumento de confiabilidade produzido pelo acréscimo do segundo gerador em reserva pode ser comprometida se um único evento externo, como, por exemplo, inundação, bloqueio de ventilação ou erros humanos recorrentes de manutenção, causar a falha de ambos os geradores.

Há muitas razões para a ocorrência de FCC. Citam-se, por exemplo (DHILLON & YANG, 1997):

- Erros de manutenção;
- Ambiente desfavorável (poeira, umidade, vibração, temperatura, etc.);
- Deficiência de projeto;
- Erro de operador;
- Catástrofe externa (fogo, enchente, terremoto, tornado, etc.).

Há, basicamente, dois tipos de FCC (KULKARNI, 1994):

1. A primeira categoria de FCC são aquelas resultantes de acoplamento estocástico, o qual pode ser conhecido ou não. As probabilidades ou taxas de falhas (geralmente, indisponibilidades) dos equipamentos de um sistema que compartilham um ambiente adverso comum (temperatura, umidade ou práticas insuficientes – de qualidade inferior – de manutenção) tendem a ser, consistentemente, maiores do que aquelas na ausência de um ambiente adverso;
2. A segunda categoria de FCC são aquelas resultantes de acoplamento determinístico. Devido a algumas causas comuns, todos os equipamentos do sistema podem estar indisponíveis simultaneamente. Tipicamente, tais falhas catastróficas podem ocorrer devido a, por exemplo, um grande incêndio ou terremoto.

Segundo RASMUSON (1991), uma investigação qualitativa deve incluir a identificação de atributos, tais como projeto, localização, modos de operação e história operacional para vários grupos de componentes de um sistema, de modo a identificar fatores que podem determinar as interdependências entre os mesmos e, assim, avaliar adequadamente as FCC que, porventura, possam ser identificadas.

Em geral, o evento de causa comum é aquele que causa a falha de dois ou mais canais de um sistema redundante, na mesma categoria de modo de falha. Esta categoria pode ser ou perigosa (como, por exemplo, um alarme ter que disparar na ocorrência de determinado evento de falha e não o faz), ou segura (por exemplo, alarme dispara sem a

ocorrência de nenhum evento de falha) ou neutra (isto é, desprezível) (WATSON & EDWARDS, 1979). Uma falha perigosa é aquela que impede a operação exigida de um sistema ou de seus componentes, como quando algum risco externo ao sistema é causado ou quando o mesmo não pode ser prevenido. Falhas perigosas que são não reveladas, ou permanentemente ou até o próximo teste, têm a maior significância na análise de confiabilidade de sistemas de proteção. Para alguns sistemas, somente alguns modos de falha podem ser considerados perigosos, por exemplo, em alguns sistemas aeronáuticos (para mais detalhes, consulte-se WATSON & EDWARDS, 1979). Tipos particulares de eventos de FCC são as falhas de componentes idênticos, ou diferentes, em canais separados, devido a uma causa comum. Em cada caso, as falhas podem ocorrer no mesmo instante, em tempos diferentes, ou uma falha pode iniciar outra. Contudo, em algum instante, haverá coincidência de estados de falha dos canais. Outro tipo de evento pode ser a falha de algum serviço que é comum a dois ou mais canais.

Tais eventos têm papel crucial quando do estabelecimento de altos padrões de confiabilidade de plantas nucleares. Como as FCC ocorrem raramente em uma instalação nuclear, dados de falhas simultâneas são escassos e difíceis de serem quantificados em uma avaliação probabilística de segurança (APS). Isto pode ter sérias conseqüências em determinadas plantas, cujas altas confiabilidades são conseguidas por meio de redundância no sistema. Por exemplo, pode-se pensar em aumentar a confiabilidade de um determinado sistema adicionando-se uma unidade redundante ao mesmo; porém, caso o sistema redundante seja suscetível a FCC a melhoria potencial pode ser completamente perdida.

Segundo JAIN (1998), podem ocorrer também situações onde a falha de um componente cria um fenômeno dinâmico que gera tensões que desafiam a resistência dos componentes operacionais restantes; tais situações são bastante comuns em sistema elétricos/mecânicos. Por exemplo, a falha de um sistema de emergência de fornecimento de potência pode degradar a eficiência das unidades operacionais restantes. Caso um dos geradores falhe, as taxas de falha e reparo do(s) outro(s) gerador(es) modificam-se.

Na análise de confiabilidade de um sistema de engenharia complexo, as FCC podem ser um aspecto significativo e difícil de quantificar. A análise de FCC pode ser difícil em função de várias considerações a serem feitas, tais como (WATSON & EDWARDS, 1979):

1. Reconhecimento das muitas causas possíveis de uma FCC e os meios de identificação;
2. Definição dos modelos a serem utilizados na quantificação da confiabilidade de sistema;
3. Análise e/ou reinterpretação dos dados surgidos de FCC relatadas (descritas);
4. A comparativa raridade de FCC influencia tanto na sua identificação quanto na sua quantificação.

Exames de eventos apresentados em PAULA *et al*. (1991) e de muitos outros eventos de FCC já ocorridos indicam que a razão de uma causa particular afetar diversos componentes está freqüentemente associada a uma ou mais condições (ou fatores de acoplamento) que eram os mesmos para todos os componentes que falharam; ou seja, as causas das falhas de causa comum geralmente não diferem das causas das falhas simples, independentes; o acoplamento é o fator real que separa os eventos de falha simples e múltiplos.

Exemplos de fatores de acoplamento incluem (PAULA *et al*., 1991):

- Projeto;
- *Hardware*;
- Pessoal de instalação, manutenção ou operação;
- Procedimento;
- Ambiente;
- Localização.

Portanto, a busca por fatores de acoplamento é, primariamente, a busca por similaridades em projeto, fabricação, construção, instalação, comissionamento, manutenção, operação, ambiência e localização de componentes redundantes. A busca por defesas contra o acoplamento, por outro lado, é, primariamente, a busca por diferenças entre os próprios componentes, na maneira como eles são instalados, operados e na maneira de se fazer manutenção, além de diferenças nos seus ambientes e localizações. Ou seja, é a busca pela diversidade.

Defesas tipicamente empregadas contra as causas raízes incluem controle de projetos, uso de equipamentos ambientalmente qualificados, programas de teste e manutenção preventiva, treinamento de pessoal, controle de qualidade e muitos outros.

Defesas empregadas para reduzir o acoplamento entre falhas de equipamentos incluem diversidade (funcional, de equipamentos e de pessoal), redundâncias adicionais, barreiras e alternância de testes e manutenção.

PAULA *et al*. (1991) ilustram também que defesas contra as falhas simples de componentes também podem impactar as FCC. O contrário ocorre apenas quando os mecanismos de defesa agem sobre as causas raízes das falhas; defesas empregadas contra fatores de acoplamento somente geram impactos contra as FCC.

Muitos trabalhos (por exemplo, HUGHES, 1987, LITTLEWOOD, 1996 e FISCHER & PIEL, 1999) consideram que uma das estratégias mais eficientes de defesa ante a ocorrência de FCC é o uso da diversidade, que seria o uso de equipamentos de modos de operação, fabricantes, ambientes operacionais ou em condições ambientais diferentes daqueles constantes no sistema, de modo que a causa comum que ataca os componentes pré-existentes no sistema não tenha efeito nestes novos componentes.

Para se tratar as FCC, o primeiro passo é identificar as possíveis FCC. Se a lógica de causa-efeito é clara, pode-se incorporar, diretamente, as FCC ao modelo lógico do sistema (MATSUOKA & KOBAYASHI, 1997). Para FCC que não são modeladas explicitamente, aplicam-se, geralmente, modelos paramétricos de causa comum (FLEMING *et al*., 1986, MOSLEH *et al.*, 1988/1989, MOSLEH, 1991, LAPA, 1996, SANT'ANA, 1996, entre outros). Neste caso, as árvores de falhas devem incorporar todos os possíveis eventos básicos de causa comum. Como se pode obter um número de cortes mínimos muitas vezes impraticável, deve-se fazer uma análise de importância de cortes mínimos, ou, então, tentar-se uma redução do nível de detalhamento da análise do sistema.

Tal redução leva a uma perda de precisão do resultado final, via eliminação de eventos (e, conseqüentemente, de suas probabilidades ou freqüências de falha), considerados de menor chance de ocorrência, levando ao surgimento de incertezas com relação à acurácia dos resultados intermediários e final. Além disso, conforme citado em AMENDOLA (1986), devido à natureza intrínseca de qualquer modelagem e predição de probabilidade, introduz-se um grau significativo de subjetividade em alguma fase da análise.

Os efeitos que, em geral, mais contribuem para a incerteza global nos resultados são os seguintes (AMENDOLA, 1986):

- <u>Aspectos gerais:</u>
  - Processo de tomada de decisão mal definido;

- Procedimentos implicitamente assumidos;

- Dados
  - Registro dos dados de falha (especialmente a não distinção entre FCC e falhas independentes e coincidentes);
  - Uso de dados;
  - Limites dos componentes;
  - Grau de acoplamento nas taxas de falha;
  - Fontes de dados;

- Modelagem
  - Interpretação de documentação;
  - Suposições quando a documentação não está completa;
  - Definição e interpretação do evento topo;
  - Definição e interpretação dos limites do sistema;
  - Análise incompleta;
  - Escolha do tempo adequado para a intervenção do operador.

Além disso, dados usados em análise de confiabilidade são, usualmente, dados observacionais, os quais podem se desviar de seus valores verdadeiros devido a algumas razões, tais como: ruído aleatório, falta de precisão do dispositivo de medida e erros na coleta e avaliação de dados. A relação entre os valores observados e seus valores verdadeiros é caracterizada pela incerteza, significando que a relação não pode ser descrita de uma forma determinística. Análises dos dados que não considerem tais incertezas podem produzir resultados tendenciosos (ZHIBIN & WEI, 2003).

Na análise de incertezas dos dados, associam-se distribuições de probabilidades adequadas às indisponibilidades dos componentes, de modo a representar a incerteza surgida da variabilidade entre subsistemas, de fabricação, local de instalação e tempo.

Outra fonte de incerteza pouco documentada diz respeito à falta de precisão do número de eventos coletados e/ou do tempo total de operação a ser considerado. Um método que pode ser usado para se quantificar o efeito de incertezas no tempo de operação, t, e/ou no número de ocorrência de eventos, x, quando se estimando a taxa de ocorrência de evento em um modelo amostral de Poisson pode ser encontrado em MARTZ & HAMADA (2003).

Tratar incertezas é um aspecto importante e difícil da análise de sistemas, com especial ênfase em sistemas complexos. Tais sistemas envolvem muitas incertezas (como, por exemplo, dificuldades de se levantar dados de falha para tais sistemas e em se decompor o sistema em unidades mais facilmente entendíveis e administráveis, fazendo-se avaliações, separadamente, destas partes, ao invés de se avaliar diretamente o problema como um todo – WINKLER, 1996) e a avaliação de probabilidades utilizada para representar tais incertezas é, por si só, uma tarefa complicada, em virtude do uso de uma variedade de fontes de informações, relacionadas com a estrutura do modelo, avaliação probabilística, coleta de informações e análise de sensibilidade.

Para que se possa modelar as incertezas referentes à ocorrência de FCC em sistemas complexos redundantes, geralmente consideram-se os componentes em seu período de vida útil (com o uso de taxas de falha constantes). Tal modelagem já foi objeto de estudo de diversos autores durante os últimos anos (MOSLEH *et al.*, 1988/1989, MOSLEH, 1991, FLEMING *et al.*, 1993, SANT'ANA, 1999, CASTILLO *et al.*, 1999, VAURIO, 2002, entre outros). Porém, devido ao envelhecimento natural dos componentes e os desgastes devido à demanda exigida dos mesmos, os equipamentos estão sujeitos a deterioração, influindo, assim, em sua confiabilidade, fazendo-a diminuir com o passar do tempo, aumentando, com isto, a probabilidade de ocorrência de falhas. O envelhecimento é uma propriedade inerente a produtos e sistemas. Ele tem um impacto significativo no efeito da estratégia de manutenção (por exemplo, consulte-se JIANG *et al.*, 2003) e seus efeitos devem ser explicitamente tratados.

Para corroborar a afirmação acima é apresentado na Figura 1.1 o gráfico da evolução da taxa de falha de sistemas mecânicos (que correspondem a uma gama importante de componentes analisados nas instalações industriais, como nas áreas nuclear, química, etc. Como exemplos, podem ser citados, entre outros componentes, bombas, válvulas e motores):

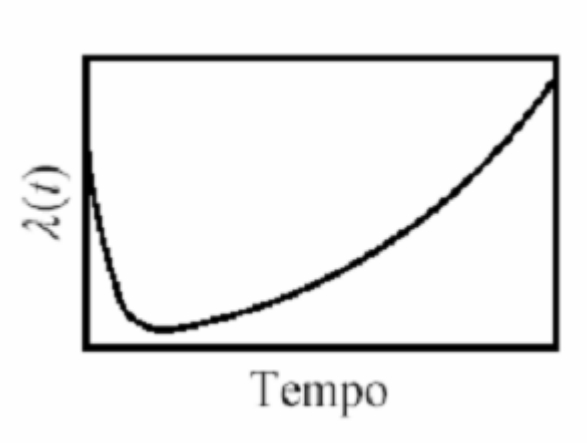

Figura 1.1 – Curva típica mostrando a evolução da taxa de falha de componentes mecânicos com o tempo (LEWIS, 1994)

A análise do gráfico da Figura 1.1 mostra que o período de vida útil é bem curto seguido de um gradual e prolongado período de envelhecimento. Tal fato demonstra a importância de se considerar o envelhecimento no estudo do comportamento tanto de um sistema quanto de seus componentes.

Além disso, falhas de sistemas reparáveis podem ocorrer não somente devido a deficiências de projeto, fragilidade de materiais, imperfeições na fabricação e desgaste normal, mas também em função de condições ambientais dinâmicas, interação entre componentes e interferências por parte do pessoal de operação e manutenção.

Portanto, este trabalho tem como objetivo a ampliação de muitos conceitos aplicados, visto que a modelagem de sistemas com aplicação de diversidade, considerando componentes e sistemas em seu período de vida útil já foi desenvolvido anteriormente em HUGHES (1987) e LITTLEWOOD (1996), a modelagem de componentes envelhecidos foi apresentado por COX & LEWIS (1966) assim como de sistemas envelhecidos, por ATWOOD (1992), enquanto que uma modelagem não paramétrica de taxas de falha de sistemas envelhecidos foi desenvolvida por KIRCHSTEIGER (1994). Portanto, este trabalho desenvolve um novo conceito, o qual seria apresentar uma nova modelagem paramétrica que considere os efeitos da diversidade aplicada a sistemas, e do envelhecimento tanto do sistema quanto de seus componentes, em especial avaliando-se as incertezas provenientes da consideração destes dois efeitos, como tais efeitos podem afetar o valor da probabilidade de falha do sistema e como esta pode ser modelada explicitamente, considerando a ocorrência, além das falhas independentes, de FCC. Para tal, este estudo está organizado da maneira descrita a seguir.

No Capítulo 2, será apresentada uma metodologia geral para a análise de eventos de causa comum, baseada no trabalho descrito em MOSLEH (1991), destacando os pontos principais para o estudo a ser desenvolvido.

Em seguida, no Capítulo 3, serão mostradas as vantagens e desvantagens do uso da diversidade, os tipos de diversidade existentes e como se inserir a diversidade no modelo de confiabilidade a ser aplicado.

O Capítulo 4 é dedicado à apresentação de testes estatísticos utilizados para verificar se os dados de falha coletados apresentam algum tipo de tendência em seu comportamento (ou seja, se os dados provêm de um sistema envelhecido e/ou com componentes envelhecidos). A seguir, serão destacados os efeitos principais do envelhecimento sobre a taxa de falha do componente e do sistema redundante, além de uma forma de se modelar explicitamente o problema.

O Capítulo 5 é reservado a considerações a respeito de análise de incertezas em modelos de análise de risco e como tais considerações são aplicáveis aos casos de ocorrência de diversidade e envelhecimento. A seguir, é apresentado um novo modelo para representar explicitamente tanto os efeitos de diversidade quanto os de envelhecimento, baseado nos conceitos destacados nos capítulos anteriores.

O Capítulo 6 é dedicado à apresentação de exemplos práticos da utilização da nova metodologia apresentada.

Ao final, no Capítulo 7, serão apresentadas conclusões e feitas recomendações visando o prosseguimento das pesquisas na área de análise de FCC considerando sistemas envelhecidos e com aplicação de diversidade.

2 – Metodologia para a Análise de Eventos de Causa Comum

2.1 – Introdução

Para entender como surge uma FCC, é importante, primeiro, reconhecer como uma falha ocorre, e como esta pode ocorrer simultaneamente em diversos componentes. O significado de simultâneo neste contexto é que as falhas ocorrem dentro do tempo de missão requerido. Há três questões separadas a serem discutidas com relação a eventos de FCC: causas, fatores de acoplamento e defesas.

2.1.1 – A Mecânica de Falha

KURIEN (1993) cita que se deve definir o termo "falha" cuidadosamente, dado que ele pode significar desde a ocorrência de um evento que necessita tão somente de um pequeno ajuste *on-line*, até um defeito sério, que necessita de uma investigação detalhada e de reparos extensivos.

A descrição de uma falha em termos de uma causa-raiz única é, de acordo com alguns autores (por exemplo PARRY, 1991), muito simplista. Para algumas finalidades, pode ser muito adequado identificar que, por exemplo, uma bomba falhou em função de grande quantidade de umidade no ambiente. Contudo, para entender de maneira detalhada o potencial para falhas múltiplas, ou como impedir falhas adicionais, faz-se necessário identificar porque o nível de umidade estava alto e porque este afeta a planta.

De modo a auxiliar a investigação com relação aos mecanismos de falha, os seguintes conceitos são úteis:

- Uma causa imediata associada a um evento de falha é uma caracterização da condição que é prontamente identificável como aquela que conduz à falha, porém, ela não fornece, em si própria, um entendimento completo do que leva àquelas condições. No exemplo acima, a umidade pode ser identificada como a causa imediata da falha. A causa imediata pode ser considerada como um sintoma da causa da falha;
- Um evento condicionador é um evento que predispõe o componente à falha ou aumenta a sua susceptibilidade à falha, porém o mesmo não causa a falha. Por exemplo, uma situação em que tem-se dois componentes localizados em um ambiente com alto grau de umidade aumenta sobremaneira as chances de ocorrência de FCC;

- Um evento gatilho é um evento que ativa uma falha ou inicia a transição para o estado falho, estando ou não o estado falho revelado àquele tempo. Um evento gatilho, particularmente no caso de eventos de falhas de causa comum, é, usualmente, um evento externo aos componentes em questão. Um evento que resulta em nível alto de umidade e subseqüente falha de equipamento seria um evento gatilho. Nem sempre é necessário, nem mesmo possível, definir unicamente um evento condicionador e um evento gatilho para cada tipo de falha.

PARRY (1991) apresenta alguns exemplos de como o uso destes conceitos podem ser aplicados.

2.1.2 – Fatores de Acoplamento

Para que as falhas se tornem múltiplas, as condições que levaram à ocorrência dos eventos gatilho e dos eventos condicionadores devem afetar todos os componentes simultaneamente. Um fator de acoplamento é uma propriedade de um grupo de componentes, ou de parte destes, que os identifica como suscetíveis ao mesmo mecanismo de falha.

Alguns autores (por exemplo, PARRY, 1991) consideram questionável a necessidade de se falar sobre mecanismo de acoplamento como uma entidade separada do mecanismo de falha. O importante, neste caso, seria identificar as características específicas dos fatores de acoplamento que resultam em impactos simultâneos em componentes em um grupo.

2.1.3 – Táticas Defensivas

As FCC podem ser evitadas por meio de uma variedade de defesas. Uma defesa pode operar de modo a impedir a ocorrência de mecanismos de falha. Outro método seria desacoplar falhas por meio de um efetivo decréscimo da similaridade entre os componentes e seus ambientes, de algum modo que impeça um tipo particular de causa raiz afetar todos os componentes simultaneamente, e permita mais oportunidades de detectar falhas antes que elas apareçam em todos os componentes do grupo.

A chave para uma mitigação bem sucedida e prevenção de FCC é se entender como as defesas primárias falharam.

Um conjunto geral de táticas defensivas pode ser definido:

- Barreiras;
- Treinamento de pessoal;
- Controle de qualidade;
- Redundância;
- Manutenção preventiva;
- Monitoramento, teste de observação e inspeção;
- Revisão de procedimento;
- Diversidade.

A definição de cada uma destas táticas pode ser encontrada em PARRY (1991).

2.2 – Elementos-chave da Estrutura de Modelagem

MOSLEH *et al.* (1991) consideram que uma análise de FCC pode ser realizada por meio de um processo envolvendo quatro estágios, a saber:

- Desenvolvimento do modelo lógico do sistema;
- Identificação do grupo de componentes de causa comum;
- Modelagem de causa comum e análise de dados;
- Quantificação do sistema e interpretação de resultados.

Cada um destes estágios será destacado brevemente, ressaltando-se que uma análise mais detalhada destes passos pode ser encontrada, entre outras referências, em FLEMING *et al.* (1986), MOSLEH *et al.* (1988/1989), MOSLEH (1991) e SANT'ANA (1996). Deve-se mencionar que o número de estágios e a ordem devem ser vistos no contexto de um guia genérico, pois há, em geral, interações e intercambialidade entre os passos que compõem a metodologia.

2.3 – Estágio 1: Desenvolvimento do Modelo Lógico

Os três passos básicos deste estágio são:

1. Familiarização com o sistema;
2. Definição do problema;
3. Desenvolvimento do modelo lógico.

Tais passos envolvem o entendimento da função do sistema, de quais componentes tal sistema é composto e os procedimentos de operação, teste e manutenção, de modo a se determinar as condições-limite (limites físicos e funcionais do sistema), suas dependências funcionais e os critérios de sucesso do sistema. Com isso, pode-se desenvolver um modelo lógico que relaciona um estado do sistema (como, por exemplo, a sua indisponibilidade) com uma combinação de um ou mais eventos elementares, tais como estado dos componentes que compõem o sistema. Entre as técnicas para a representação lógica do sistema, incluem-se árvores de falhas, de eventos e diagramas de blocos.

2.4 – Estágio 2: Identificação dos Grupos de Componentes de Causa Comum

Os objetivos deste estágio incluem:

- Identificação de grupos de componentes do sistema a serem incluídos (ou eliminados) da análise de FCC;
- Priorização de determinados grupos de componentes, com relação à alocação de recursos e disponibilização de tempo para a análise das FCC.

Tais processos resultam na identificação dos componentes e modos de falha a serem considerados (ou não) na análise, em função das condições-limite, nível de detalhamento, etc. identificados no estágio anterior. O resultado final deste estágio é a definição dos componentes para os quais suas FCC serão incluídas no modelo e a determinação de quais causas raízes e mecanismos de acoplamento devem ser incluídos em um evento de causa comum para propósitos de quantificação.

Neste estágio, há dois tipos de exame a serem considerados:

1. Análise qualitativa: neste passo, uma pesquisa é feita sobre os atributos comuns e mecanismos de falha que podem conduzir a FCC potenciais. Alguns dos principais atributos, destacados por MOSLEH (1991) são: tipo, uso, fabricante e limites dos componentes e suas interfaces, procedimentos de teste e manutenção, etc.
2. Análise quantitativa: serve para reduzir a lista de grupos de causa comum essenciais para a ocorrência do evento topo (falha do sistema). É, normalmente, realizada pela análise da árvore de falhas do sistema, em busca dos cortes mínimos para a seqüência de ocorrência de falhas do sistema. Com isto, ao final do processo, tem-se uma lista de grupos de FCC que têm maiores chances de contribuir para a indisponibilidade do sistema.

2.5 – Estágio 3: Modelo de Causa Comum e Análise dos Dados

O objetivo deste estágio é completar a quantificação do sistema pela incorporação dos efeitos dos eventos de causa comum para os grupos de componentes selecionados no estágio anterior. Isto pode ser feito por meio de quatro passos:

1. Definição dos eventos básicos de causa comum;
2. Seleção dos modelos de probabilidade para eventos básicos de causa comum;
3. Classificação e exame dos dados;
4. Estimação dos parâmetros.

2.5.1 – Definição dos Eventos Básicos de Causa Comum

Eventos básicos de causa comum são eventos que representam falhas de componentes específicos de um grupo de componentes em função de causa comum. A definição dos mesmos é essencial para a estimação dos parâmetros do modelo selecionado.

É óbvio que um sistema falha porque (alguns dos) seus componentes falham. Assim, se dados completos, detalhados e precisos dos componentes são conhecidos, então estes dados conterão toda a informação exigida para a predição da confiabilidade do sistema, dado o projeto do mesmo. Segundo HUGHES (1987), o que constitui dados completos e detalhados para os componentes são dados de falha que contêm informações detalhadas sobre a história e a causa raiz das falhas. Com efeito, tal informação descreve o ambiente no qual o componente falhou. Portanto, o ambiente não representa somente os detalhes das condições ambientais da instalação do componente, mas também detalhes com relação à sua história, manutenção, etc., que levaram à falha do componente. Note-se que pode haver variação do ambiente de um componente particular com relação ao tempo (isto é, um componente desgastado tem um ambiente diferente de um novo, mesmo que as condições ambientais dos dois componentes sejam as mesmas). Detalhes sobre quais componentes falharam e quais não, em um determinado ambiente, medem a probabilidade de que um componente particular falhe neste ambiente. E, por definição, esta medida conterá toda a informação necessária à predição dos efeitos das FCC no sistema.

Isto é feito escrevendo-se os eventos básicos de causa comum em termos de combinações particulares de eventos afetados (MOSLEH, 1991). Ao final, obtém-se uma representação booleana reduzida dos sistemas, em termos dos cortes mínimos considerados, fazendo-se uso de simplificações, de modo a impedir a proliferação de

termos na equação booleana. Meios de se fazer esta simplificação podem ser encontrados em FLEMING (1986), MOSLEH (1991) e LAPA (1996).

2.5.2 – Seleção dos Modelos de Probabilidade para os Eventos Básicos de Causa Comum

O objetivo principal deste passo é a seleção do modelo de causa comum a ser usado na quantificação dos eventos básicos de causa comum selecionados. Primeiro, transforma-se a equação booleana, encontrada no passo anterior, em uma equação de probabilidades, de modo que as probabilidades dos eventos básicos possam ser substituídas diretamente na expressão algébrica resultante desta transformação. Para facilitar os cálculos, faz-se uso da suposição de simetria entre componentes de tipos similares.

A partir daí, define-se a probabilidade de um evento básico envolvendo k ($1 \leq k \leq m$, onde m é o número de componentes em um grupo de componentes de causa comum) componentes específicos, a partir dos dados que se tem à disposição (ou na ausência de precisão dos dados ou em função de dados escassos, faz-se uso de suposições adicionais ou consulta-se a opinião de especialistas), selecionando-se o modelo paramétrico adequado à situação vigente, de modo a se calcular a probabilidade de evento básico de causa comum.

2.5.3 – Classificação e Exame dos Dados

- *Classificação dos Dados*

As fontes de dados disponíveis situam-se nas seguintes categorias globais:

1. Compilação de dados brutos genéricos;
2. Registros de dados brutos específicos para a planta;
3. Estimativas de parâmetros de dados de eventos classificados genericamente (fontes de dados especialmente desenvolvidos para a análise de falhas dependentes).

Exemplos de cada uma destas fontes de dados podem ser encontrados em MOSLEH (1991). Devido à escassez de eventos de causa comum para as plantas industriais (muitas vezes devido ao pouco tempo de operação), com a conseqüente pequena quantidade de dados específicos para a planta para a análise de causa comum, recorre-se, na maioria das vezes, a fontes de dados genéricos e à experiência

operacional acumulada para se fazer inferências com relação às freqüências dos eventos de FCC da planta em estudo.

A seguir, deve-se encontrar um conjunto completo de eventos para cada um dos grupos de componentes de causa comum no modelo do sistema (isto é, identificar os registros de eventos de falha). As descrições dos eventos devem incluir as seguintes informações:

- Causa raiz;
- Fator de acoplamento;
- Tamanho do grupo de componentes;
- Eventos básicos de causa comum observados;
- Modo de falha.

A definição de cada um destes termos pode ser encontrada em FLEMING *et al.* (1986), MOSLEH *et al.* (1988/1989) e MOSLEH (1991). Um exemplo prático de como cada um destes fatores influencia a confiabilidade do sistema pode ser encontrado em LAPA (1996).

- *Avaliação do Impacto do Evento*

Um evento pode ser classificado, matematicamente, sob a forma de um vetor de impacto. Um vetor de impacto para um dado evento em um grupo de componentes de causa comum de tamanho m tem m+1 elementos, onde cada elemento representa o número de componentes falhos no evento. Se k elementos falham, então o k-ésimo elemento do vetor de impacto vale 1 (um) e os restantes, 0 (zero) (MOSLEH, 1991, FLEMING *et al.*, 1993, SANT'ANA, 1999).

Da experiência operacional, porém, verifica-se a pouca clareza na descrição do evento de falha, o que leva o evento de falha a ser representado por um vetor de impacto médio, onde cada elemento do vetor representa a incerteza com relação ao número de componentes falhos no evento.

Um problema sempre recorrente quando se está trabalhando com vetores de impacto é o caso da diferença entre os tamanhos do sistema em estudo e o do qual os dados são provenientes (quando do uso de fontes de dados genéricos). O tamanho do sistema sob estudo (isto é, o número de componentes no sistema) pode afetar as probabilidades de FCC por várias razões; portanto, há problemas se o sistema em estudo

tem tamanho diferente dos grupos representados nos dados de FCC disponíveis. Se tal diferença existe, deve-se traduzir os dados de FCC de forma a adequar o tamanho do sistema representado nos dados ao sistema em estudo. Segundo KVAM & MILLER (2002), em uma APS, tal procedimento, chamado mapeamento, não é incomum nos estudos de confiabilidade para plantas nucleares.

Os procedimentos de mapeamento permitem aos analistas combinar diferentes fontes de dados sem a necessidade de fazer numerosas suposições sobre os mecanismos de falha e suas correspondentes distribuições de probabilidade.

No caso onde os dados originam-se de grupos de causa comum maiores do que o grupo na APS, o mapeamento tem a forma de uma função de distribuição hipergeométrica. Este procedimento é conhecido como *mapping down*. Caso contrário, para a realização do procedimento de mapeamento são necessárias mais informações para se fazer uma transferência coerente. Este procedimento é chamado de *mapping up*. Claro está que ambos os procedimentos (*mapping up* e *mapping down*) inserem incertezas na modelagem de falhas de causa comum, pois além de se fazer uso de dados genéricos, são feitas transposições baseadas em análises subjetivas.

Há diversas formas de se construir vetores de impacto (com transferência do tempo de missão, da freqüência de falhas ou de ambos). Tais métodos, contudo, apresentam resultados similares. Critérios para a escolha do método mais adequado a cada situação, e a forma precisa de se trabalhar com cada um destes, podem ser encontrados em MOSLEH *et al.* (1988/1989), KVAM (1996), KVAM & MILLER (2002) e VAURIO (2002).

- *Criação da Base de Dados Específicos para a Planta*

Uma vez desenvolvidos os vetores de impacto para um evento na planta onde o mesmo ocorreu, este deve ser transportado para a planta em estudo. Isto é feito verificando-se a aplicabilidade do evento na planta de destino, via associação de um fator de aplicabilidade do evento, p, $(0 \leq p \leq 1)$ (uma descrição da utilização de tal técnica pode ser encontrada em MOSLEH *et al.*, 1988/1989, e SANT'ANA, 1999).

2.5.4 – Estimação dos Parâmetros

O propósito deste passo é usar os "pseudo-dados" (vetores de impacto), gerados no passo anterior para estimar ou a probabilidade de eventos básicos diretamente ou os

parâmetros dos modelos de FCC (valores pontuais). A informação contida no conjunto de vetores de impacto é o número de eventos nos quais 1, 2, ..., *n* componentes falharam (onde *n* é o grau de redundância) ou o tempo de falha de tais componentes, dependendo da técnica de mapeamento utilizada. Procedimentos para a escolha do modelo, em função dos dados disponíveis, além de informações e suposições adicionais necessárias para a realização dos cálculos dos parâmetros necessários à computação do valor de interesse (por exemplo, a indisponibilidade do sistema), podem ser encontradas em diversas referências, entre elas, FLEMING *et al.* (1986), MOSLEH *et al.* (1988/1989), MOSLEH (1991) e SANT'ANA (1996).

2.5.5 – Avaliação de Incertezas nas Estimativas dos Parâmetros

Geralmente, uma Avaliação Probabilística de Segurança (APS) para um sistema em uma Instalação Nuclear visa responder às seguintes questões:

- Quais eventos, em particular, são possíveis?
- Qual é a probabilidade de tais eventos?
- Quais são as conseqüências de tais eventos para o sistema e/ou ambiente?

Tenta-se encontrar respostas para estas questões por meio da construção de um modelo do sistema, no qual algumas partes deste podem ser descritas como um processo determinístico e algumas outras como um estocástico. É uma característica natural destes tipos de modelos, e de todos os dados envolvidos, de que eles são, em geral, imperfeitos (KAFKA & POLKE, 1986). As incertezas nestes modelos surgem, principalmente, por duas razões:

1. Há uma transferência imperfeita do sistema real para um modelo que o descreve, tanto por processos determinísticos quanto estocásticos;
2. Inerentemente, todos os dados usados nos modelo contêm uma faixa de incertezas e erros.

No primeiro caso, tais imperfeições provêm do fato de que o entendimento físico do sistema pode não ser desenvolvido o suficiente, ou as fórmulas ou códigos computacionais serem aproximações para facilitar a computação. Para lidar com este grupo de incertezas, considera-se principalmente a experiência operacional, experimentação e exercício de *benchmark* para expandir-se o grau de conhecimento de modo a aperfeiçoar os modelos.

Em relação ao segundo grupo de incertezas, usualmente, um estudo de incerteza irá mostrar as fontes, tipos e medidas de propagação nos resultados de APS, que são itens importantes para usuários e tomadores de decisão. Para lidar com este grupo, consideram-se, principalmente, métodos matemáticos adequados para propagação de incerteza, assim como para a coleta e atualização da experiência operacional de modo a gerar uma base de dados representativa e suplantar os problemas surgidos de julgamentos subjetivos.

Existe um grande número de incertezas que devem ser consideradas quando se deseja apresentar uma descrição realista do que o analista conhece em relação ao valor dos parâmetros do modelo. Em geral, em uma análise de incertezas, são desenvolvidas distribuições dos contribuintes mais importantes para a indisponibilidade do sistema (tais contribuintes são identificados em função da classificação dos contribuintes por intermédio dos valores de suas estimativas pontuais).

Geralmente, as incertezas em uma análise advêm de:

- Classificação dos dados e avaliação dos vetores de impacto;
- Estimação dos dados de sucesso ou fontes de dados de eventos de falha incompletos, como, por exemplo, eventos independentes não relatados de maneira precisa;
- Inferência estatística, ditada pelo tamanho da amostra de dados;
- Variação entre plantas em equipamentos, projetos de sistema e operações.

Uma descrição detalhada de cada uma destas fontes e técnicas para incorporar estes elementos de incerteza na avaliação da distribuição dos parâmetros é apresentada em MOSLEH *et al.* (1988/1989), MOSLEH (1991) e SANT'ANA (1999). Cabe ressaltar que o trabalho aqui desenvolvido é baseado neste estágio da análise.

2.6 – Estágio 4: Quantificação do Sistema e Interpretação de Resultados

O estágio final da análise envolve a quantificação da indisponibilidade do sistema, realizando-se análises de incerteza e sensibilidade, interpretação dos resultados e documentação. Os objetivos deste estágio são obtidos através dos seguintes passos:

1. Quantificação;
2. Avaliação de resultados e análise de sensibilidade;
3. Geração de relatório.

A descrição completa de cada um destes passos pode ser encontrada em MOSLEH (1991).

3 - O Impacto da Diversidade em FCC

3.1 – Introdução

Independência do comportamento de falha dos componentes em um sistema redundante ou diverso é uma situação desejada, porque isto permitiria a realização de cálculos bastante simples para se determinar a confiabilidade do sistema. Caso não se possa exigir independência, então se necessita estimar o grau de dependência entre os componentes de um sistema em particular sob exame, de modo a se calcular a sua confiabilidade.

Na análise de uma APS, uma questão importante é até que extensão as interações entre os componentes devem ser modeladas, de modo a produzir uma descrição de risco mais próxima da realidade. Neste campo, falhas dependentes de componentes representam um papel significativo, se não dominante, na determinação das características de confiabilidade e disponibilidade de um sistema de segurança e devem, portanto, ser consideradas.

Infelizmente, meios de se usar a informação sobre o projeto do sistema, de modo a se estimar esta dependência são muito escassos em função da raridade de evidência (dados de falhas).

Com este objetivo, diversos modelos para quantificar falhas dependentes foram apresentados (MOSLEH *et al*., 1988/1989, MOSLEH, 1991, LAPA, 1996, SANT'ANA, 1996, entre outros). Enquanto, no geral, estes modelos meramente reconhecem a existência da multiplicidade das falhas potenciais, não há a identificação de nenhuma estrutura causal.

Os modelos causais são baseados na idéia de que as falhas de componentes podem ser originárias de variações no nível de tensão (*stress*) do ambiente operacional e descrevem esta variabilidade probabilisticamente.

As dependências entre componentes podem ser de dois tipos (MARSEGUERRA *et al*., 1999):

- Aquela que surge quando há uma ligação física entre os modos de operação dos componentes em um grupo redundante. Esta dependência é tratada explicitamente pela introdução de um fator de conexão que justifica a variação na probabilidade de falha dos componentes causada pela modificação na configuração do sistema (isto é, no modo de operação de alguns componentes no sistema);

- O segundo tipo de dependência é algo mais sutil, visto que ele está oculta no ambiente no qual o componente está instalado, mas contém detalhes de sua historia, manutenção, etc. Este tipo de dependência pode ser tratada probabilisticamente por meio de uma metodologia formal simples, baseada em probabilidades condicionais de falhas, sendo a condição fornecida pelo ambiente.

Antes de se demonstrar teorias e modelos, que permitirão a predição da confiabilidade de sistemas na presença de FCC, deve-se ter um entendimento básico destes conceitos fundamentais e de suas relações. Portanto, inicialmente, faz-se necessário responder a questões tais como: o que é diversidade? Quão diversos são dois projetos? Que nível de diversidade pode-se esperar com o uso de dois projetistas, trabalhando livremente, porém, com a proibição de comunicação entre eles? Nos últimos anos, modelos causais formais foram propostos para começar a responder a algumas destas questões (HUGHES, 1987, LITTLEWOOD, 1996 e FISCHER & PIEL, 1999).

3.2 – Uso de Meios (Recursos) Redundantes e Diversos

Falhas dependentes podem se originar tanto de comportamento errôneo (imperfeito) de natureza idêntica nos trens, quanto de mecanismos de propagação de falhas com conseqüências comuns. Neste caso, não é mais válida a suposição de independência entre os trens individuais.

Devem ser tomadas todas as providências necessárias para se evitar falhas dependentes, ou, pelo menos, reduzi-las a um determinado patamar aceitável. Uma série de medidas que poderiam ser consideradas pode ser encontrada em FISCHER & PIEL (1999). Porém, algumas vezes, as medidas que poderiam ser adotadas não são possíveis, ou do ponto de vista técnico ou econômico (por exemplo, dados de observações insuficientes de determinados componentes do sistema, rotina de teste muito cara, ou se deseja quantificar falhas extremamente raras ou de causa desconhecida). Portanto, nestes casos, deve ser considerado o uso da diversidade.

Diversidade é um conceito no qual unidades diferentes (do ponto de vista operacional, de procedimentos de teste e manutenção, de fabricantes diferentes, situados em ambientes diferentes, etc.) são usadas juntas em um sistema redundante. Baseia-se

no fato de que unidades diferentes respondem de maneira diferente a uma tensão comum, em função da diminuição do acoplamento entre as várias unidades.

Diversidade é uma defesa robusta contra falhas acopladas. Por exemplo, equipamentos diferentes deveriam ser separados fisicamente, em salas diferentes, para defesa contra o acoplamento proveniente de, por exemplo, temperatura alta em uma determinada sala.

Uma das fontes de falhas dependentes são os impactos externos. Geralmente, a solução empregada, nestes casos, é o isolamento adequado dos trens, colocando-os em salas, ou até mesmo em prédios apropriadamente protegidos. Porém, caso se assuma a ocorrência de dependência funcional, então a probabilidade de uma falha dependente pode, ou ser reduzida suficientemente, ou até mesmo ser evitada completamente, caso sejam escolhidos elementos funcionais diferentes, ou em projeto ou em modo de operação.

Há, basicamente, duas formas de diversidade:

- Modos de operação diferentes são conhecidos como diversidade funcional;
- Projetos diferentes são conhecidos como diversidade física.

Elementos diversos são usados para se tentar obter independência entre todos os trens, os quais iniciam uma certa ação protetora contra as falhas dependentes postuladas. Meios ou medidas apropriados à aplicação da diversidade são as seguintes:

- Ter elementos funcionais tecnicamente diferentes, pelo uso de produtos de diferentes fabricantes;
- Usar elementos funcionais diferentes, os quais implementam a mesma função;
- Ter elementos funcionais tecnologicamente diferentes, os quais recebem e processam dados de entrada diferentes, porém dão início à mesma ação protetora.

Componentes redundantes usando diferentes tecnologias podem fazer aumentar a resistência a eventos de C.C., caso os projetos respondam diferentemente a uma tensão comum. Por exemplo, uma unidade mecânica em *standby* a uma unidade elétrica é um bom exemplo de uso da diversidade. O uso de diferentes fabricantes de um mesmo componente pode fornecer algum benefício, pois reduz a possibilidade de defeitos por

fabricação comum; porém, não são alcançados grandes benefícios caso ambas as unidades respondam a uma mesma tensão.

Os seguintes itens são exigidos para que seja possível o uso da diversidade (FISCHER & PIEL, 1999):

- As operações dos elementos diversos são independentes; somente assumindo-se isto, o uso da diversidade se torna efetiva (evitando-se, assim, os mecanismos de acoplamento entre os elementos diversos do sistema);
- Não há a criação de nenhuma outra nova fonte de falhas, originária das diferentes exigências de manutenção, ou de compatibilidade insuficiente, dos elementos diversos do sistema;
- Os gastos em projeto, verificação e operação, causados pela aplicação de elementos diversos não podem exceder os limites aceitáveis do ponto de vista econômico.

Após isto, de acordo com FISCHER & PIEL (1999), a aplicação de elementos diversos deve promover uma melhoria significativa na confiabilidade do sistema.

Por tudo isto, deve-se ponderar cuidadosamente o que é melhor, em relação ao uso da redundância:

- Compensar a falta de disponibilidade de trens individuais ou de partes destes;
- Criar uma medida adicional contra falhas raras ou de causa desconhecida, em geral.

Como exemplo adicional (extraído de PAULA *et al*., 1991), pode ser citado o caso de um gerador diesel. A diversidade de equipamento não seria defesa contra o acoplamento "alinhamento impróprio de válvulas de água de refrigeração" porque geradores diesel de diferentes fabricantes ainda assim usariam água de serviço do mesmo sistema. Se a diversidade de equipamento fosse estendida (por exemplo, um gerador diesel refrigerado a água e outro a ar), então a diversidade de equipamento teria um impacto poderoso no acoplamento associado a este mecanismo de falha. Diversidade de equipe (pessoal diferente realizando teste e manutenção de cada gerador, incluindo o alinhamento das válvulas de água de refrigeração) seria uma defesa poderosa. Separação espacial forneceria alguma defesa porque o pessoal de manutenção poderia não ser capaz de confiar nas posições da válvula em um sistema de

refrigeração, o qual pode estar incorreto, enquanto estivesse testando uma outra válvula do mesmo sistema redundante. Teste e manutenção alternados seriam defesas robustas e estes seriam realçados (acentuados) pela separação espacial (a diversidade de pessoal também seria realçada pela separação espacial).

É reconhecido que componentes iguais apresentam algumas dependências no seu comportamento de falhas, embora não exista ligação física evidente entre seus modos de operação. Nestes casos, a dependência pode ser interpretada como causada pelo ambiente. De acordo com esta interpretação, componentes aparentemente iguais, operando em plantas diferentes, têm probabilidades de falhas diferentes, de acordo com o ambiente no qual elas operam. Em outras palavras, os ambientes resumem todas as causas raízes das falhas dependentes.

A existência de um efeito ambiental é vista pela comparação da variância externa com aquelas computadas para as duas situações (efeito ambiental existe e efeito ambiental não existe), para os casos de igualdade dos valores da média.

A variância da distribuição de probabilidade do número de componentes falhos, em um dado tempo *t*, para o caso de um ambiente fixo λ_e, é dada por (MARSEGUERRA *et al*., 1999):

$$Var_{\delta}[m(t)] = Np(\lambda_e, t)[1 - p(\lambda_e, t)] \tag{3.1}$$

onde: *N*: número total de componentes que constituem um determinado sistema;

$m(t)$: número de componentes falhos em *t*;

$p(\lambda_e, t)$: probabilidade de que um componente falhe antes de *t*, quando operando em um dado ambiente λ_e.

No caso de variação ambiental estocástica, a variância da distribuição de probabilidade do número de componentes falhos, em um dado tempo *t*, é dada por (MARSEGUERRA *et al*., 1999):

$$Var_{ext}[m(t)] = Var_{\pi}[m(t)] = Var_{\delta}[m(t)] + N(N-1)Var_{\pi}[p(\lambda_e, t)] \tag{3.2}$$

Compara-se $Var_{\delta}[m(t)]$ com a variância externa $Var_{ext}[m(t)]$. Se as duas estão próximas, pode-se concluir que não existe efeito ambiental. Caso contrario, Var_{ext} é maior do que Var_{δ} e esta diferença é uma indicação da existência de efeito ambiental nas falhas.

MARSEGUERRA *et al*. (1999) demonstram que a presença de um ambiente estocástico pode ser detectada pelo aumento na variância na distribuição do número de componentes falhos. Esta detecção pode ser de suprema importância, dado que o impacto de um ambiente operacional não observado pode resultar em uma mudança drástica das características de uma confiabilidade redundante.

Uma questão crítica é como o projetista pode obter informação suficiente para avaliar a distribuição de variação ambiental. Note-se que o projeto é altamente sensível à variação ambiental. Isto sugere que um projeto conservativo deveria, em algum caso, considerar tal variabilidade.

3.3 - O efeito da variabilidade ambiental entre as FCC

A noção-chave aqui é a variabilidade. Em alguns modelos (veja-se HUGHES, 1987, e LITTLEWOOD, 1996), há a variabilidade na probabilidade de falha de um tipo particular de componente, com a mudança do ambiente operacional. Por ambiente operacional, tem-se em mente uma formulação muito geral que inclui, por exemplo, políticas de manutenção (HUGHES, 1987). Caso se colocasse mais de um componente similar em uma arquitetura redundante, de modo a tentar melhorar a confiabilidade sobre o que se esperaria para um único componente, é a natureza da distribuição desta variabilidade de probabilidade de falha que determina o quão bem sucedido se seria. Muito informalmente, a idéia aqui é a seguinte: imagine-se que se construiu um sistema a partir de dois componentes similares e o sistema funciona com sucesso se, pelo menos, um dos componentes funciona. Como exemplo, considere-se um sistema de resfriamento de emergência compreendendo duas bombas similares: uma demanda sobre o sistema é satisfeita se, pelo menos, uma das bombas dá a partida com sucesso quando a demanda ocorre. Agora, observa-se que uma das bombas, na realidade, falhou: o que se pode pensar sobre as chances da outra bomba também falhar? Sob uma suposição simples de independência de comportamento de falhas entre os dois componentes, a probabilidade de que a segunda bomba falhará é meramente a probabilidade marginal de falha de uma bomba (LITTLEWOOD, 1996). Se esta suposição de independência estivesse correta, então esperar-se-ia uma confiabilidade significativamente maior para um sistema 1-de-2 do que para um único componente sozinho: na realidade, uma probabilidade de falha p^2 ao invés da probabilidade de falha de um componente simples, p.

No modelo de Hughes (HUGHES, 1987), o raciocínio é que, dado que a primeira bomba falhou, este é, provavelmente, um ambiente estressante para todas as bombas deste tipo e, assim, será mais provável a falha da segunda. Na pior das hipóteses, neste modelo, cada ambiente poderia ter a propriedade de que ou todos os componentes falham, ou todos os componentes funcionam – neste caso, o conhecimento de que o primeiro componente falhou significaria a certeza de que o segundo componente também falhou, em um sistema 1-de-2.

Em geral, sempre que há variação de nível de *stress* entre ambientes (e parece difícil de imaginar circunstâncias onde este não é o caso), o sistema 1-de-2 terá uma confiabilidade menor do que aquela dada pela suposição de independência: a probabilidade de falha do sistema situar-se-á em algum lugar entre p e p^2.

Para ser um pouco mais formal em relação ao modelo, necessita-se estabelecer cuidadosamente a natureza da incerteza nas várias afirmações em relação às probabilidades. Por exemplo, para o modelo de Hughes, seja-se $P(falha \mid e)$, a probabilidade de que um tipo particular de componente falhe em um ambiente particular, e. Como há muitos (talvez infinitos) ambientes operacionais, a seleção de um ambiente é, ela mesma, um processo aleatório. Caso se tenha um mecanismo que selecione ambientes, isto induz a uma distribuição de probabilidades para $P(falha \mid e)$, isto é, $F(p) \equiv P(falha \mid e) < p$ (LITTLEWOOD, 1996). É a forma desta distribuição e, em particular, sua variância, que determina o grau de sucesso que advém da construção do sistema redundante a partir de tais componentes.

Quando se fala da probabilidade $P(falha \mid e)$ está-se referindo à incerteza de comportamento de falha entre componentes diferentes de um mesmo tipo, e no mesmo ambiente. A distribuição $F(p)$, por outro lado, trata-se da variação desta probabilidade para diferentes ambientes selecionados. É a variância desta distribuição que desempenha papel importante; quanto maior a variância, maior o desvio do tipo de comportamento de falha que seria esperado se as falhas dos diferentes componentes ocorressem independentemente.

Uma questão que não é discutida no modelo de Hughes (HUGHES, 1987) diz respeito à possibilidade de variação no comportamento de falhas entre componentes, dentro de um mesmo ambiente operacional. Parece claro que um componente não irá, em geral, se comportar sempre da mesma maneira quando exposto repetidamente ao mesmo ambiente: por exemplo, ele pode falhar hoje em um ambiente no qual ele

funcionou perfeitamente ontem. Isto significa que a "probabilidade de falha" é um conceito significativo não somente em termos de proporções de todos os componentes que podem falhar quando cada um deles é exposto sozinho (individualmente) a um ambiente particular, como considerado por HUGHES (1987), mas também por um único componente quando exposto repetidamente a um mesmo ambiente. Assim, por exemplo, pode-se usar uma distribuição geométrica para a probabilidade de que um componente usado repetida e independentemente, no mesmo ambiente, terá sucesso *n* vezes, e falha na (*n*+1)-ésima tentativa (LITTLEWOOD, 1996). Mais importante, é sensato perguntar se, para um ambiente em particular, todos os componentes terão a mesma probabilidade de falha: de acordo como o exposto em HUGHES (1987) e LITTLEWOOD (1996), este não será o caso quando se estiver tratando de aplicações práticas.

3.4 – O Modelo de Hughes Generalizado

LITTLEWOOD (1996) apresenta um modelo de Hughes generalizado, de modo a se compensar as deficiências apresentadas pelo modelo de Hughes (HUGHES, 1987) original (no modelo original, por exemplo, não há possibilidade de variação entre componentes, ou seja, tal modelo trabalha com componentes redundantes idênticos, sem a aplicação de diversidade). Ele descreve tanto populações de componentes quanto de ambientes e as probabilidades de que um determinado componente/ambiente seja selecionado de tais populações, além da probabilidade de que um particular componente falhe em um ambiente em particular.

Antes da apresentação da estrutura do modelo, devem ser definidos os seguintes conceitos:

- Para um determinado componente, em um ambiente particular, a probabilidade de que o componente falhe ao ser submetido a uma demanda neste ambiente é dada por:

$$f(c,e) = P(\textit{falha do componente c no ambiente e}) \tag{3.3}$$

- A probabilidade de falha de um componente, aleatoriamente escolhido, em um ambiente particular *e* é dado por:

$$\pi(e) \equiv P(\textit{falha} \mid E = e) = \sum_{C} f(c,e)S(c) = E_S(f(c,e)) \tag{3.4}$$

onde $C = \{c_1, c_2, \ldots\}$ é a população de todos os componentes possíveis;

$S(c) = P(C = c) \equiv$ probabilidade de seleção do componente *c*.

- A probabilidade de que um componente aleatoriamente escolhido falhe em um ambiente, também aleatoriamente escolhido é:

$$E(\pi(E)) = E_{S,Q}(f(C,E)) = \sum_C \sum_E f(c,e) S(c) Q(e) \tag{3.5}$$

onde $E = \{e_1, e_2, \ldots\}$ é a população de todos os ambientes possíveis;

$Q(e) = P(E = e) \equiv$ probabilidade de seleção do ambiente *e*.

A idéia por trás deste novo modelo (LITTLEWOOD, 1996) é a seguinte: têm-se disponíveis dois ou mais tipos de componentes diferentes (*A*, *B*, ...). Sem perda de generalidade, serão considerados componentes de apenas dois tipos, *A* e *B*; porém o processo pode ser estendido para sistemas de *n* componentes. Componentes do tipo *A* podem diferir daqueles do tipo *B*, porque eles representam dois projetos diferentes; porém, todos os componentes do tipo *A* têm o mesmo projeto, assim como os do tipo *B*.

Este tipo de diversidade introduz outra forma de variação, além das já discutidas. Em particular, além da variação entre as confiabilidades dos componentes do tipo *A*, e entre as confiabilidades dos componentes do tipo *B*, ao longo dos mais diferentes ambientes, o novo modelo leva em consideração a variação entre os *A*'s e *B*'s, isto é, a distribuição de probabilidade de falha, para os diferentes ambientes, é uma distribuição bivariada.

Considere-se um sistema 1-de-*n*. A confiabilidade deste sistema depende não somente do grau de dependência entre os comportamentos de falha dos componentes, mas também das confiabilidades individuais dos componentes. Para se fazer algumas afirmações gerais sobre a eficácia deste tipo de diversidade forçada, LITTLEWOOD (1996) faz diversas simplificações em relação à indiferença entre tipos de componentes e chega a importantes resultados:

- Caso se saiba que os componentes *A* e *B* são diferentes, porém se é indiferente entre uma escolha aleatória de um sistema *AA* ou *BB* (sistemas 1-de-2 homogêneos), por exemplo, então se deve construir, ao invés disso, sistemas aleatoriamente escolhidos *AB*. Ou seja, um sistema misto aleatório escolhido será mais confiável do que qualquer um dos sistemas homogêneos aleatórios escolhidos;

- No caso em que se deseja construir um sistema 1-de-*n*, porém têm-se apenas $m < n$ tipos diferentes de componentes, pode ser mostrado (LITTLEWOOD, 1996) que o melhor projeto é aquele que usa todos os tipos de componentes disponíveis, porém usa de cada tipo a menor quantidade possível. Por exemplo, é preferível um sistema *AABBC* a um sistema *AAABC*.

Deve-se enfatizar que todos estes resultados são baseados em médias e dizem respeito ao que é considerado o "melhor projeto de sistema" quando nada se sabe a respeito das confiabilidades de componentes particulares, em ambientes específicos. Caso se tenha mais informações, as coisas podem mudar drasticamente. Para mais detalhes, consulte-se LITTLEWOOD (1996).

É importante destacar que o uso de sistemas diversos implica em considerações logísticas importantes e um custo logístico maior, visto que há uma necessidade maior de pesquisa, de modo a encontrar componentes que desempenham funções semelhantes, porém apresentam algumas das diferenças destacadas na Seção 3.2 (serem elementos funcional ou fisicamente diferentes), custos diferentes na aquisição destes diferentes equipamentos e de material sobressalente e/ou de reposição e custos associados de armazenamento, custos adicionais no treinamento para a operação e manutenção de componentes diferentes, entre outros custos.

LITTLEWOOD (1994) mostra que um sistema utilizando diversidade forçada é preferível ao sistema de Hughes (HUGHES, 1987), pois com seu uso consegue-se uma probabilidade de falha do sistema menor.

3.4.1 - Cálculo da confiabilidade do sistema com uso de Diversidade

Foi visto anteriormente que há algumas idéias gerais que se pode demonstrar sobre as vantagens do uso de diversidade forçada ao invés do simples uso de redundância como no modelo de Hughes. Na prática, no entanto, deseja-se ter estimativas da confiabilidade real de sistemas construídos desta maneira. Uma vantagem tanto do método de Hughes quanto de sua generalização, é que tudo depende das distribuições, tais como a distribuição bivariada para (π_A, π_B), dada por

$$F(\pi_A, \pi_B) = P[\pi_A(E) \leq \pi_A, \pi_B(E) \leq \pi_B] \tag{3.6}$$

[$\pi_A(E)$ representa a probabilidade de que um componente do tipo *A*, aleatoriamente escolhido, falhará em um ambiente *E*, também aleatoriamente escolhido].

Pode-se estimar estas distribuições a partir dos dados coletados sobre os comportamentos operacionais de sistemas anteriores diferentes que contêm os componentes *A* e *B* (não se exige similaridade entre sistemas, apenas que as informações nos sistemas tenham conexão com relação aos comportamentos de falha, tipos de componente e ambiente).

Assume-se que há, no total, *m* ambientes nos quais um componente possa estar. Para um determinado ambiente e_j, assume-se que foram observadas n_{Aj} demandas para componentes do tipo *A*, das quais r_{Aj} resultaram em falhas, e n_{Bj} demandas para componentes do tipo *B*, das quais r_{Bj} resultaram em falhas.

Assume-se, também, que o mecanismo de seleção de ambientes é tal que haja uma probabilidade p_j de seleção do ambiente e_j (uma simplificação básica é que estas probabilidades permanecem as mesmas para todas as seleções de ambientes). Assuma-se, também, que observou-se que e_j foi selecionado q_j vezes $(j = 1,2,\ldots,m)$.

Uma forma não refinada de proceder é usar os dados para estimar as probabilidades (condicionais) de falhas dos tipos de componentes em ambientes diferentes e, então, combiná-las com as probabilidades de seleção dos ambientes, de modo a obter uma estimativa da distribuição incondicional,

$$F(\pi_A, \pi_B) = P[\pi_A(E) \le \pi_A, \pi_B(E) \le \pi_B], \tag{3.7}$$

para a probabilidade de falha conjunta dos componentes do tipo *A* e do tipo *B*. Pode ser mostrado (LITTLEWOOD, 1996) que uma estimativa para $\pi_A(e_j)$ (probabilidade de falha de um componente tipo *A* em um ambiente e_j) é dada por:

$$\hat{\pi}_A(e_j) = \frac{r_{A_j} + 1}{n_{A_j} + 2} \tag{3.8}$$

Uma expressão para $\hat{\pi}_B(e_j)$ pode ser deduzida de maneira similar [note-se que estes componentes falham (condicionalmente), independentemente em seu ambiente].

Uma estimativa para p_j é dada por:

$$\hat{p}_j = \frac{q_j + 1}{\sum_k q_k + m} \tag{3.9}$$

Então, por exemplo, a probabilidade de falhas para um sistema *AB* diverso 1-de-2 seria:

$$P_{SD} = \sum_j \left(\frac{r_{A_j} + 1}{n_{A_j} + 2} \right) \left(\frac{r_{B_j} + 1}{n_{B_j} + 2} \right) \frac{q_j + 1}{\sum_k q_k + m} \tag{3.10}$$

A probabilidade de falha do mesmo sistema supondo independência é dada por::

$$P_{SI} = \left(\sum_j \left(\frac{r_{A_j} + 1}{n_{A_j} + 2} \right) \frac{q_j + 1}{\sum_k q_k + m} \right) \left(\sum_j \left(\frac{r_{B_j} + 1}{n_{B_j} + 2} \right) \frac{q_j + 1}{\sum_k q_k + m} \right) \tag{3.11}$$

Sob o modelo de Hughes, a probabilidade de falha de um sistema redundante (sem aplicação de diversidade), com componentes somente do tipo *A* (resultado similar seria conseguido com componentes do tipo *B* – LITTLEWOOD, 1996) é igual a:

$$P_{SR} = \sum_j \left(\frac{r_{A_j} + 1}{n_{A_j} + 2} \right)^2 \frac{q_j + 1}{\sum_k q_k + m} \tag{3.12}$$

Com isso, segundo LITTLEWOOD (1996), pode-se conseguir, a princípio, que a probabilidade de falha do sistema dado pela Equação (3.10) seja menor do que as dadas pelas Equações (3.11) e (3.12). Na prática, o grau de confiabilidade extra em relação ao sistema, para ser conseguido, a partir deste método, dependerá criticamente da natureza da correlação entre o comportamento de falha dos diferentes tipos de componentes, dada pela diferença entre as expressões nas Equações (3.10) e (3.11).

Capítulo 4 – Análise e Modelagem de Dependência Temporal

4.1 – Análise de Tendência ao Envelhecimento

4.1.1 – Introdução

O envelhecimento de componentes pode ser identificado por meio de monitoração de mecanismos de degradação física e pela detecção de tendências crescentes dos dados armazenados em sistemas de coleta de falhas.

Enquanto análises qualitativas de experiência operacional auxiliam a identificar as causas e os mecanismos de envelhecimento, modelos estatísticos são necessários para revelar tendências crescentes na probabilidade de falha e para avaliar a significância estatística de possíveis mudanças.

O estado de degradação de um componente é afetado pelas tensões (*stresses*) ambientais e a taxa de falha é, freqüentemente, dependente da história operacional do componente. Conclui-se, daí, que modelos de envelhecimento de taxas de falha de componentes requerem a introdução de taxas e probabilidades de falhas dependentes do tempo.

Existem alguns testes destinados a caracterizar o envelhecimento de um componente e/ou sistema. Por exemplo, em JIANG *et al*. (2003) foi apresentada uma metodologia para a análise de tendências ao envelhecimento, que pode ser definida como a razão entre a taxa de falha instantânea e uma taxa de falha base; neste caso, é comumente utilizada a taxa de falha média, dada por:

$$\frac{M(t)}{t} = \frac{1}{t}\int_0^t \lambda(t')dt' \tag{4.1}$$

onde $M(t)$ é a função de falhas acumulada (ou função de risco) e $\lambda(t)$ é a taxa de falha instantânea. Assim, a função intensidade de envelhecimento $L(t)$ é dada por:

$$L(t) = \frac{\lambda(t)}{M(t)/t} = \frac{t\lambda(t)}{M(t)} = \frac{tf(t)}{-R(t)\ln[R(t)]}, \qquad t > 0 \tag{4.2}$$

A intensidade de envelhecimento $L(t) = 1$ indica uma taxa de falha constante, $L(t) > 1$, uma taxa de falha crescente e $L(t) < 1$, uma taxa de falha decrescente. Quanto maior o valor de $L(t)$, mais forte a tendência ao envelhecimento.

Contudo, neste trabalho, para se testar se os dados apresentam algum tipo de tendência, serão usados os testes apresentados por VAURIO (1999). As razões para tal escolha devem-se a:

- Facilidade de cálculo do valor numérico dos testes, a partir dos registros de dados de falha;
- Os testes apresentados permitem a detecção dos mais variados tipos de tendência.

4.1.2 – Testando Tendências

Serão apresentadas técnicas para teste de tendência, dentre as quais podem ser citadas:

(a) Técnicas gráficas simples;

(b) Testes que têm como base os valores dos tempos de falha

Diz-se que um teste apresenta tendência monotônica se $F_{X_i}(x) \leq F_{X_j}(x)$ ou $F_{X_i}(x) \geq F_{X_j}(x)$, para cada $i \geq 1,\ j > i,\ x > 0$, onde X_i e X_j são variáveis aleatórias independentes, $i \neq j$. Pode ser demonstrado (ASCHER & FEINGOLD, 1984) que todo modelo que apresenta tendência possui incrementos não estacionários, apesar do inverso não ser verdadeiro (incrementos estacionários => $N(t) - N(s)$ e $N(t+\Delta) - N(s+\Delta)$ são identicamente distribuídos). Caso os testes demonstrem a existência de tendência, os X_i's não são identicamente distribuídos, de modo que se deve ajustar aos dados um modelo não estacionário.

(a) Técnicas Gráficas

Há alguns procedimentos gráficos simples, os quais têm o intuito de ajudar a determinar se um sistema esta melhorando ou se deteriorando. Tais técnicas são particularmente úteis para se buscar uma determinada característica dos dados e para se verificar as suposições feitas no ajuste de modelos formais aos dados. Porém, conforme destacado em ASCHER & FEINGOLD (1984), a natureza monotonicamente crescente do gráfico do número acumulado de falhas faz com que variações locais tendam a ser mascaradas, até mesmo quando o tamanho amostral é relativamente grande. Na mesma referência, é proposto um procedimento alternativo, baseado na divisão do intervalo total de observações em vários intervalos e na observação das variações locais das taxas de falha por subintervalo. Porém, tal técnica é muito dependente do número de intervalos adotados e da amplitude dos mesmos. Com isso, conclui-se que os

procedimentos gráficos não são muito adequados para a detecção precisa de tendências nos dados, a não ser que a tendência apresentada seja muito evidente.

(b) Testes para a Detecção de Tendências Monótonas e não Monótonas

Para se melhorar e otimizar a eficiência de programas de manutenção para sistemas, faz-se necessária a detecção de possíveis correlações e padrões de tempo em uma seqüência de falhas. Isto também é um pré-requisito para suposições de modelagens corretas e estimação de parâmetros de uma modelagem. A seguir, serão apresentados testes estatísticos que tentam estabelecer se os tempos entre falhas são sistematicamente crescentes ou decrescentes.

Considere-se uma unidade, observada a partir de $t = 0$, quando a unidade é nova ou foi recentemente reparada. Seus tempos de falha sucessivos são $T_1 < T_2 < \ldots T_n < T_{n+1} = \hat{T}$ e os seus tempos entre falhas são dados por $X_i = T_i - T_{i-1}$, $i = 1, 2, \ldots, n+1$ $\left(T_0 = 0 < T_1\right)$. Assume-se que os tempos de reparo ou substituição são desprezíveis. Ao invés de apenas considerar as falhas, um evento também poderia ser definido como algum grau de deterioração que leva a uma ação de manutenção. A seqüência é truncada em falhas: ela é observada até que um número pré-especificado, $n+1$, de eventos ocorra e o tamanho do período total observado total $\hat{T} = T_{n+1}$ é aleatório. Seqüências truncadas no tempo são discutidas em VAURIO (1999).

- ***Teste para detecção de Tendências em Sistemas***

Para testar tendências em sistemas, em COX & LEWIS (1966) é apresentado o seguinte teste: suponha que séries de tempos de falha, independentes, estejam disponíveis (uma para cada componente do sistema), com tempos finais de falhas $\hat{T}', \hat{T}'', \ldots$. O número de eventos de falhas em cada série seria denotado por $m', m'', \ldots$, onde $m = n+1$. Para testar se o sistema, como um todo, apresenta tendência (ou seja, está envelhecendo), faz-se uso da estatística de teste:

$$z_0 = \frac{\left(\sum T_i' + \sum T_i'' + \ldots\right) - \frac{1}{2}\left(m'\hat{T}' + m''\hat{T}'' + \ldots\right)}{\left\{\frac{1}{12}\left(m'\hat{T}'^2 + m''\hat{T}''^2 + \ldots\right)\right\}^{1/2}} \tag{4.3}$$

que, sob a hipótese nula (o sistema esta em seu período de vida útil) tem distribuição, aproximadamente, normal padrão.

- ***Testes Gerais para Componentes***

  Estimativas do valor médio, μ, e o desvio-padrão, σ, de X_i são dados por:

$$\overline{X} = \frac{\sum_{i=1}^{n+1} X_i}{n+1} \tag{4.4}$$

$$s^2 = \frac{\sum_{i=1}^{n+1} \left(X_i - \overline{X}\right)^2}{n} \tag{4.5}$$

Um dos testes padrões atribuídos a Laplace (VAURIO, 1999, COX & LEWIS, 1966) é baseado na estatística $L = \frac{\sum T_i}{\hat{T}}, i = 1,2,\ldots,n$. Sob a condição (hipótese nula H_0) de que os valores $\frac{T_i}{\hat{T}}$ são uniformemente distribuídos em $(0,1)$, tem-se que L é, aproximadamente, normalmente distribuída com média $\frac{n}{2}$ e desvio-padrão $\sqrt{\frac{n}{12}}$. Assim, sob H_0:

$$U = \frac{\sum_{i=1}^{n} T_i - \frac{n\hat{T}}{2}}{\hat{T}\sqrt{\frac{n}{12}}} \sim N(0,1) \tag{4.6}$$

tem distribuição, aproximadamente, normal padrão. Sob a mesma condição:

$$Z = 2\sum_{i=1}^{n} \log\left(\frac{\hat{T}}{T_i}\right) \sim \chi^2(2n) \tag{4.7}$$

tem, exatamente, distribuição χ^2 com $2n$ graus de liberdade. Rejeita-se H_0 se U ou Z são valores maiores, em módulo, do que os valores correspondentes a um nível α previamente especificado das distribuições indicadas. Valores $U > 0$ e Z pequenos implicam em unidades se deteriorando enquanto que valores $U < 0$ e Z grandes implicam em unidades melhoradas (valores-p pequenos indicam tendência).

Pode ser mostrado (VAURIO, 1999) que *U* e *Z* são efetivos na detecção de tendências monotônicas, com eficiência melhor, ou aproximadamente igual a muitos outros testes que são matematicamente mais complexos. Isto acontece em função das propriedades descritas na mesma referência acima citada.

Contudo, *U* e *Z* não são efetivos na detecção de desvios da exponencialidade se não há uma tendência monotônica, por exemplo, se o processo é:

(a) um *PP* com taxa de risco na forma de uma curva da banheira simétrica ou invertida;

(b) um *PR* com tempos entre falhas não exponenciais.

Caso se saiba por antecipação que o processo é um *PP*, *U* e *Z* podem ser usados para testar a exponencialidade. Algumas questões que podem ser destacadas com relação a estes testes são as seguintes (VAURIO, 1999):

1) *U* e *Z* não são efetivos na detecção de desvios na exponencialidade (*PPH*) se não há uma tendência monotônica na *IF;*
2) *U* e *Z* não são efetivos na detecção de pequenas tendências quando $s << \overline{X}$;
3) *U* e *Z* podem ser muito sensíveis (indicando falsas tendências) quando $s >> \overline{X}$;
4) *U* e *Z* (e muitos outros testes) são ineficientes para detectar tendências não monotônicas;
5) Nenhum método parece estar disponível ou sendo usado para testes gerais, se o processo com tendência é um *PPNH*.

- ***Teste Alternativo para Detecção de Tendências Monotônicas***

  Sob a condição de que o processo é *PR* (VAURIO, 1999):

$$J = \frac{\sum_{i=1}^{n} T_i - \frac{n\hat{T}}{2}}{s\left[\frac{n(n+1)(n+2)}{12}\right]^{1/2}} \sim t(n) \qquad (4.8)$$

obedece a uma distribuição aproximadamente *t* de Student com *n* graus de liberdade. Em casos em que $s << \overline{X} = \frac{\hat{T}}{n+1}$, *J* é mais efetivo do que *U* e *Z* para a detecção de tendência monotônica verdadeira e, em casos em que $s >> \overline{X}$, ele é menos provável de indicar falsa tendência.

- ***Testes para Tendências não Monotônicas***

Para testar tendências não monotônicas (como comportamento tipo curva da banheira), VAURIO (1999) sugere três testes estatísticos:

$$V_1 = \frac{\sum_{i=1}^{n}\left|T_i - \frac{\hat{T}}{2}\right| - \frac{n\hat{T}}{4}}{\hat{T}\sqrt{\frac{n}{48}}} \sim N(0,1) \tag{4.9}$$

$$V_2 = \frac{\sum_{i=1}^{n}\left|T_i - \frac{\hat{T}}{2}\right|^2 - \frac{n\hat{T}^2}{12}}{\hat{T}^2\sqrt{\frac{n}{180}}} \sim N(0,1) \tag{4.10}$$

$$V_3 = 2\sum_{i=1}^{n}\log\left(\frac{\hat{T}}{\left|2T_i - \hat{T}\right|}\right) \sim \chi^2(2n) \tag{4.11}$$

Enquanto U e J medem o desvio com relação ao valor médio de T_i e $\hat{T}/2$, V_1 e V_2 medem a distribuição média dos valores observados T_i com relação ao seu ponto médio VAURIO (1999). V_3 apresenta alguma semelhança com Z. V_1, V_2 e V_3 têm algum poder para detectar também tendências monotônicas.

Dos resultados apresentados por VAURIO (1999), conclui-se o seguinte:

- valores-p pequenos (abaixo dos correspondentes ao nível α estabelecido) para U, Z e J claramente indicam uma tendência monotônica (deterioração);
- valores-p pequenos para V_1, V_2 e V_3 indicam uma *IF* não monótona, do tipo curva da banheira.

Os indicativos, com relação aos dados estão apresentados na Tabela 4.1.

Tabela 4.1: Tipo de tendência apresentada pelos dados em função dos valores calculados para os testes ($2n$-0,66 é o valor aproximado da mediana de uma distribuição χ^2, com n graus de liberdade)

Valores das Estatísticas calculadas			Tipo de Tendência
$U > 0$	$J > 0$	$Z < 2n - 0{,}66$	Crescente
$U < 0$	$J < 0$	$Z > 2n - 0{,}66$	Decrescente
$V_1 > 0$	$V_2 > 0$	$V_3 < 2n - 0{,}66$	Curva-da-Banheira
$V_1 < 0$	$V_2 < 0$	$V_3 > 2n - 0{,}66$	Curva-da-Banheira invertida

4.2 – Modelagem de Taxas de Falha Dependentes do Tempo

4.2.1 – Introdução

Diversos tipos de sistemas e componentes (mecânicos, elétricos e estruturais) estão sujeitos, durante seu período de vida, à ocorrência de um fenômeno conhecido como envelhecimento. Tal fenômeno leva a mudanças nas propriedades de engenharia dos componentes, com o decorrer do tempo, fazendo com que os mesmos tenham diminuídas as suas capacidades de suportar as demandas normais de operação, as condições ambientais e as conseqüências de acidentes que, porventura, ocorram.

HILSMEIER *et al*. (1995) ressaltam a importância da incorporação dos efeitos de envelhecimento na descrição da confiabilidade e de processos de manutenção, visto que os componentes estão sujeitos a envelhecimento, e isto pode resultar em impactos significativos tanto na confiabilidade quanto na disponibilidade dos componentes em consideração.

Devido à deterioração, a confiabilidade de um sistema, estimada no momento de projeto e monitorada durante e ao fim da construção é, portanto, dependente do tempo e esta pode decrescer com o passar do tempo, causando o aumento da probabilidade de ocorrência de falhas. Com isto, de acordo com CIAMPOLI (1998), a confiabilidade de um sistema em deterioração deve ser determinada em função de seu tempo de vida em serviço, definido como o período durante o qual os componentes estão aptos a suportar, com segurança, todas as demandas e cargas exigidas.

A deterioração de sistemas identifica-se, especialmente, com a degradação de suas propriedades mecânicas. Tal deterioração, devido a efeitos de desgaste durante seu serviço ordinário, de uso impróprio e de manutenção, assim como de eventos ambientais e de ocorrência de acidentes, é grandemente acelerada por exposição a um ambiente agressivo. Conforme CIAMPOLI (1999), a taxa de deterioração depende de vários

fatores, tais como: projeto do componente, seleção de matérias-primas, qualidade de fabricação e agressividade do ambiente ao qual o componente está exposto.

Segundo CIAMPOLI (1998), na avaliação de efeitos dos mecanismos de degradação, deve-se levar em consideração que as causas da degradação podem interagir entre si, levando a uma diminuição ainda mais acentuada da resistência do componente.

A maior parte das pesquisas em relação ao impacto do envelhecimento e da deterioração dos componentes e sistemas em uma planta nuclear é com relação a equipamentos mecânicos e elétricos. Estes representam um papel importante com relação à mitigação das conseqüências das seqüências de acidentes postulados ocorridos (ELLINGWOOD, 1998).

De acordo com MARTORELL *et al.* (1999), mecanismos ambientais e operacionais condicionam o processo de envelhecimento de um componente: para componentes em condições de trabalho normais (tanto condições ambientais quanto operacionais), sua idade coincide com o tempo transcorrido desde a sua instalação; caso contrário (isto é, componente submetido a condições ambientais adversas) sua idade evolui mais depressa que seu tempo cronológico desde a instalação.

As condições operacionais representam os modos de operação de um determinado componente: se seu funcionamento é contínuo ou não; se opera com carga máxima ou parcial, etc., além de também estarem relacionadas às condições de *stress* ao qual o componente é submetido. Geralmente, segundo MARTORELL *et al.* (1999), expressam-se tais condições operacionais como uma função do número e duração de demandas para operar (para componentes em reserva), ou através do tempo operacional (para componentes em operação contínua). Contudo, conforme MARTORELL *et al.* (1999), pode-se falar em condições operacionais ruins, normais ou boas.

Condições ambientais representam os parâmetros ambientais sob os quais um componente opera, como por exemplo, temperatura, umidade, dose de radiação no ambiente, nível de corrosão, etc. De acordo com MARTORELL *et al.* (1999), da mesma forma que as condições operacionais, as condições ambientais também podem ser qualificadas em ruins, normais ou boas.

Sabe-se que os componentes instalados em uma planta de potência nuclear trabalham sob condições operacionais as mais diversas, isto é, enquanto alguns componentes passam a maior parte do tempo em reserva (em especial, equipamentos de sistemas de segurança), outros funcionam continuamente. Além disso, tais

componentes estão sujeitos a variadas condições ambientais, ou seja, alguns ficam instalados em ambientes muito rigorosos, sujeitos a altas temperaturas e liberação de doses de radiação (como, por exemplo, componentes situados na contenção), enquanto outros estão em ambientes mais confortáveis. De tudo isto, é óbvio que as características de confiabilidade de um componente são afetadas, influenciando no seu tempo de vida, e corroborando a importância de se estudar a variação da taxa de falha dos componentes com o decorrer do tempo.

Alguns dos modelos, descritos na literatura, que levam em consideração a idade do componente são: linear, exponencial, Weibull e lognormal. Cada um destes modelos tem parâmetros característicos, geralmente definidos pelo usuário, em função dos dados de falhas disponíveis. Deve-se, portanto, identificar e analisar, apropriadamente, as fontes de dados, de modo que o modelo selecionado seja utilizado adequadamente. Segundo DUTHIE *et al.* (1998), normalmente, os dados são provenientes de duas fontes, dependendo do tipo de componente: os componentes ativos (por exemplo, bombas e válvulas) e os passivos (por exemplo, tubulações e vasos de pressão).

4.2.2 – Definição de Conceitos Inerentes à Estimação de Taxas de Falha

Normalmente, em uma APS, assume-se que as taxas de falha de todos os componentes são constantes. Contudo, há situações em que as mesmas não podem ser assim consideradas, principalmente em função do envelhecimento e do desgaste do componente. Com isso, devem ser consideradas taxas de falha dependentes do tempo, de modo a avaliar a probabilidade de falha em um determinado tempo.

Assume-se que os componentes falham de acordo com um processo de Poisson dependente do tempo, com taxa de falha $\lambda(t)$ [ou seja, ocorrências futuras de um evento independem de sua ocorrência no passado, há a ocorrência de somente um evento em um intervalo de tempo Δt e a probabilidade de falha em um período curto $(t, t+\Delta t)$ é dado por $\lambda(t)\Delta t$; informações mais detalhadas sobre o Processo de Poisson podem ser encontradas em MANN *et al.* (1974), LEWIS (1994), RAMAKUMAR (1993), entre outros].

Os dados a serem considerados ou são censurados no tempo ou censurados em falhas. Conforme ATWOOD (1992), os dados são chamados censurados no tempo (*time-censored data*) se há um período fixo de tempo durante o qual os componentes são observados e seus dados de falha registrados. Durante este tempo, um componente

falho é restaurado e recolocado em serviço; neste caso, o número total de falhas é aleatório. Dados são chamados censurados em falhas (*failure-censored data*) se um componente é reparado até a ocorrência de um número pré-determinado de falhas, depois do qual o componente é removido e substituído por um componente novo. Neste caso, o final do período de observação é um tempo aleatório.

Na descrição que se segue, os componentes são indexados por *j* enquanto que os tempos de falha de um componente são indexados por *i*. Portanto, T_{ij} é o tempo da *i*-ésima falha do componente *j*. O número de falhas (sem contar nenhuma falha que resulte em substituição) é representado por *n*, enquanto que o total de falhas, com substituição, sera denotado por *m*. Portanto, $n = m$ no caso de componentes censurados no tempo e $n = m$-1 no caso de componentes censurados em falhas.

ATWOOD (1992) descreve que a taxa de falha de um componente pode ser descrita da seguinte forma:

$$\lambda(t) = \lambda_0 g(t;\beta) \tag{4.12}$$

onde λ_0 é uma constante multiplicativa e $g(t;\beta)$ é a parte da expressão que determina a forma de $\lambda(t)$. ATWOOD (1992) apresenta três modelos para representar a taxa de falha, os quais seriam:

$\lambda(t) = \lambda_0 \exp[\beta(t - t_0)]$ (modelo de taxa de falha exponencial ou log-linear) (4.13a)

$\lambda(t) = \lambda_0[1 + \beta(t - t_0)]$ (modelo de taxa de falha linear) (4.13b)

$\lambda(t) = \lambda_0(t/t_0)^{\beta}$ (modelo de taxa de falha de Weibull para a 1ª. falha) (4.13c)

É facilmente verificável que λ_0 é o valor de $\lambda(t)$ quando $t = t_0$; aqui, β é chamado parâmetro de envelhecimento. Neste caso, t_0 é um valor selecionado pelo analista [geralmente zero nos dois primeiros casos ou um valor que normaliza as escalas de medidas de tempo, no terceiro (ATWOOD, 1992)]. Os resultados apresentados por estes três modelos, quando representando uma estimativa pontual para a taxa de falha de um componente, são similares. Contudo, o modelo selecionado para representar as taxa de falhas de um componente neste trabalho será o exponencial em função de duas vantagens importantes que este apresenta (ATWOOD, 1992):

1. Não há restrições com relação aos valores que o parâmetro β pode assumir (no caso do modelo de taxa de falhas linear, tem-se a restrição $\beta > \frac{-1}{\max_{s_{1j}>t_0}\left(s_{1j}-t_0\right)}$ e no caso do modelo de taxa de falha de Weibull para a 1ª. falha, há a restrição $\beta > -1$);
2. As aproximações assintóticas usadas para quantificar incertezas e representar os intervalos de confiança são mais bem representadas por este modelo, ou seja, os intervalos de confiança criados a partir deste modelo são mais fidedignos.

4.2.3 – Estimação Paramétrica de Taxas de Falha

ATWOOD (1992) apresenta as fórmulas de se estimar os valor de λ_0 e β para os três modelos considerados no seu trabalho. No caso do modelo de taxa de falha exponencial, COX & LEWIS (1966) definem como EMV para β, para um determinado componente, o valor que satisfaz $L'\left(\hat{\beta}\right)=0$, onde:

$$L'\left(\hat{\beta}\right)=\begin{cases}\sum_j\left[\frac{n_j}{\beta}-\frac{n_j s_{1j}}{1-e^{-\beta s_{1j}}}+\sum t_{ij}\right] & \left(\beta\neq 0\right)\\ \sum_j\left[-\frac{1}{2}n_j s_{1j}+\sum t_{ij}\right] & \left(\beta=0\right)\end{cases} \tag{4.14}$$

onde t_{ij} : tempos (ordenados) da *i*-ésima falha do *j*-ésimo componente;

s_{1j} : tempo final de observação do componente *j*;

n_j : número de falhas observadas para o componente *j*, não contando a falha final, em caso de dados censurados em falhas.

Tal valor é facilmente determinado a partir dos dados amostrais, constantes nos registros de falha ou nas fontes de dados genéricas (COX & LEWIS, 1966, utilizam-se de um método de interpolações gráficas para determinar uma estimativa para β com bastante precisão).

Um EMV para λ_0, considerando-se o modelo de taxa de falha exponencial, e assumindo-se conhecido o valor da estimativa de β, é dado por:

$$\hat{\lambda}_0 = \begin{cases} \dfrac{n}{\nu} & \left(\textit{para dados censurados em tempo}\right) \\ \dfrac{m}{\nu} & \left(\textit{para dados censurados em falhas}\right) \end{cases} \tag{4.15}$$

onde $\nu_j = \dfrac{\exp\left(\beta s_{0j}^*\right)\left[\exp\left(\beta r_j\right)-1\right]}{\beta}$ e $\nu = \sum_j \nu_j$

onde:

$s_{0j}^* = s_{0j}$ $\left(\textit{quando } t_0 = 0\right)$: tempo inicial de observação do componente j (em geral, $s_{0j} = 0$);

$r_j = s_{1j} - s_{0j}$: amplitude de tempo observacional (o j-ésimo componente é observado no tempo entre s_{0j} e s_{1j}).

A partir destas duas estimativas e com a estrutura do modelo de taxa de falha exponencial, definida pela Equação (4.13a), obtém-se um estimativa pontual para $\lambda(t)$. Por meio deste método pode ser obtida uma região de confiança bidimensional. Tal intervalo de confiança tem algumas desvantagens:

- É conservativo;
- O intervalo de confiança não é proveniente de nenhuma distribuição que possa ser usada como a priori conjugada em um método de Bayes. A possibilidade de uso desta priori conjugada facilitaria sobremaneira os cálculos.

De modo a se eliminar estas desvantagens, ATWOOD (1992) apresenta um meio de obter os EMV de $\left(\hat{\beta}, \hat{\lambda}_0\right)$, para dados censurados em falhas, por meio de uma função de log-verossimilhança completa:

$$\sum_j \sum_{i=1}^{m_j} \log\left\{\exp\left[\beta\left(t - t_0\right)\right]\right\} + m\log\lambda_0 - \lambda_0 \nu(\beta) \tag{4.16}$$

onde $m = \sum m_j$ e $\nu = \sum \nu_j$.

Para um dado valor de β (obtido via EMV condicional, veja-se ATWOOD, 1992), verifica-se que a função de log-verossimilhança é maximizada em:

$$\hat{\lambda}_0 = \frac{m}{\nu(\beta)} \tag{4.17}$$

A partir daí, obtém-se uma estimativa para β, por meio da seguinte equação:

$$\sum_j \sum_{i=1}^{m_j} (t - t_0) - \frac{m[\nu'(\beta)]}{\nu(\beta)} = 0 \tag{4.18}$$

onde $\nu'_j(\beta) = \dfrac{\exp(\beta s_0^*)\left[\beta\left(s_1^* e^{\beta r_j} - s_0^*\right) - \left(e^{\beta r_j} - 1\right)\right]}{\beta^2}$, $\qquad \nu'(\beta) = \sum_j \nu'_j(\beta)$

e $s_{1j}^* = s_{1j} - t_0$

Conforme pode ser visto em COX & LEWIS (1966), tal resultado é facilmente obtido via iteração numérica e interpolação.

Tais estimadores fazem com que sejam obtidos intervalos de confiança mais fidedignos, a despeito de algum conservadorismo ainda existente com relação ao valor de β.

Uma adaptação deste método, apresentada em COX & LEWIS (1966) e em ATWOOD (1992), pode ser usada para testar a escolha de uma distribuição normal bivariada para representar $(\hat{\beta}, \log\hat{\lambda}_0)$ (suposição esta adotada a priori, visto que o modelo de taxa de falha exponencial se adequa a esta suposição muito bem; para mais detalhes, veja-se ATWOOD, 1992).

5 – Modelagem de Incertezas em Análise de Risco

5.1 – Introdução

Nas análises padrões de risco/segurança, os parâmetros do modelo são considerados constantes. Porém, em muitas ocasiões, tais parâmetros são difíceis de avaliar ou, então, são estimados. Assim, sua característica determinística, considerada de início, não é adequada e os parâmetros são considerados variáveis aleatórias. Quando isto acontece e o objetivo da análise é monitorar os efeitos de tal aleatoriedade na variável destino, diz-se que se está tratando com análise de incertezas. Incertezas em modelos têm sido objeto de estudo em muitos trabalhos (CHATFIELD, 1995, ZIO & APOSTOLAKIS, 1996, DEWOOGHT, 1998, entre outros).

Alguns autores (HORA, 1996, CASTILLO *et al*., 1999, entre outros) fazem a distinção das incertezas em aleatórias e epistêmicas. Incertezas aleatórias provêm de variações naturais, imprevisíveis na performance do sistema. Não se espera que haja uma redução na incerteza aleatória por meio de conhecimento de especialistas, embora seus conhecimentos possam ser úteis na quantificação das incertezas. Assim, algumas vezes, refere-se a este tipo de incertezas como sendo incerteza irredutível. Ao contrário disso, a incerteza epistêmica é devida à falta de conhecimento com relação ao comportamento do sistema, que é conceitualmente determinável. A incerteza epistêmica pode, a principio, ser eliminada com suficiente estudo e, portanto, julgamentos de especialistas podem ser úteis nesta redução.

Quando tanto incertezas aleatórias quanto epistêmicas estão presentes, dependências ou correlações podem ser introduzidas no processo.

Julgamentos de especialistas são freqüentemente usados am APS. Uma razão para se fazer isto, segundo CHHIBBER *et al.* (1992), é porque os eventos de interesse do analista de segurança são raros e informações estatísticas ou experimentais não estão facilmente disponíveis. Freqüentemente, estes julgamentos estão implicitamente entendidos e, portanto, não ficam explicitamente especificados.

Dependências introduzidas por incertezas epistêmicas são, algumas vezes, ignoradas ou não reconhecidas na modelagem de sistemas complexos. Componentes de um mesmo tipo, por exemplo, podem ser assumidos que falham independentemente na presença de incertezas aleatórias somente. Contudo, caso existam incertezas epistêmicas sobre a probabilidade de falha para os componentes, as falhas resultantes não podem ser consideradas como independentes.

Que fontes de incertezas, variáveis, ou probabilidades podem ser rotuladas como epistêmicas e quais serão rotuladas como aleatórias? Esta é uma importante consideração porque uma vez combinadas, será muito difícil se desenvolver distribuições de probabilidade que reflitam corretamente as várias incertezas. Pode-se fazer uma distinção entre incertezas aleatórias e epistêmicas puramente através de propriedades físicas e julgamentos de especialistas. A mesma quantidade pode ser tratada em um estudo como tendo incertezas aleatórias enquanto que em outro a incerteza pode ser tratada como epistêmica. Um exemplo de como isto acontece pode ser encontrado em HORA (1996).

Uma hipótese deste trabalho é que a distinção exata e natural entre estes dois tipos de incerteza usualmente não existe. A distinção surge em função do modelo específico a ser quantificado e dos propósitos para o qual o modelo será calculado.

Segundo APELAND *et al*. (2002), há três elementos básicos no processo de quantificação de incertezas, os quais, na prática, estão intimamente relacionados: julgamentos das probabilidades por parte dos especialistas, uso de dados históricos e aplicação dos modelos.

5.2 – Modelos Aplicados à Análise de Risco

5.2.1 – Introdução

Em análise de risco, a extensão de quais conseqüências indesejáveis potenciais ameaçam a performance de uma dada atividade é quantificada pela construção e análise de um modelo. De acordo com DUTHIE *et al*. (1998), o modelo constitui uma representação simplificada de um sistema real, refletindo as relações causais que produzem os eventos focados pelos analistas. A complexidade do modelo é influenciada por diversos fatores, tais como a complexidade do sistema, o conhecimento em relação ao sistema que está disponível para os analistas, a quantidade de informação que é considerada como base suficiente para se tomar a decisão em questão e os recursos disponíveis para os analistas. O fundamento principal da análise é se descrever a incerteza relacionada a quantidades que ocorrem em modelos e deduzir a probabilidade da conseqüência indesejável em questão, através da estrutura do modelo, pela aplicação das leis de cálculo de probabilidades.

Freqüentemente, os tipos exatos de leis aleatórias e seus parâmetros de distribuições, assim como a relevância do fenômeno, as informações do modelo, os valores dos parâmetros e os dados de entrada da aplicação do modelo não são

precisamente conhecidos e, portanto, sujeitos a incertezas epistêmicas (de "falta de conhecimento"). Tais incertezas são representadas por meio de probabilidades subjetivas, as quais quantificam os respectivos estados de conhecimento. Conseqüentemente, as variáveis do processo de um modelo estão sujeitas tanto a incertezas aleatórias quanto epistêmicas.

Um tratamento adequado para ambos os tipos de incerteza, neste caso, seria quantificar a influência das mesmas nas estimativas estatísticas das probabilidades de estado do processo. Um procedimento, fazendo-se uso de métodos de Monte Carlo, pode ser encontrado em HOFER *et al.* (2002).

5.2.2. – Critérios para aceitação de um Modelo

Causas associadas a muitos eventos de falhas de múltiplos componentes em plantas de potência nucleares incluem: projeto inadequado, deficiências de fabricação e instalação, erros de comissionamento, erros relacionados à manutenção, tensões (*stresses*) ambientais, (por exemplo, umidade excessiva, corrosão ou contaminação).

Um ponto importante considerando dados de FCC é que usualmente não há eventos de FCC específicos suficientes para a planta, de modo a dar suporte a uma análise de FCC ou para estimar a probabilidade de um determinado evento de FCC; devem ser usados dados genéricos para este propósito. Contudo, fazer uso de informação requer:

1. uma interpretação das ocorrências de falhas anteriores, de modo a identificar os mecanismos envolvidos nestes eventos;
2. reinterpretação destes eventos, à luz das características de projeto e operação de uma planta específica.

Ambos os fatores apresentados acima levam ao surgimento de incertezas.

O processo de avaliação é complexo e envolve muitas incertezas (visto que estes processos são subjetivos), especialmente quando considerando as defesas específicas da planta que podem ser postas em prática, de modo a evitar ou mitigar FCC. Portanto, é difícil assegurar (e defender) a completeza das avaliações, com respeito às causas e defesas consideradas pelo analista. Tais avaliações também são muito dependentes da formação e do entendimento técnico do analista das plantas e dos componentes levados em consideração. Assim, a profundidade e a qualidade das avaliações dependem

substancialmente da perícia do analista. Também é, comumente, muito difícil, se não impossível, assegurar consistência entre analistas diferentes.

As incertezas em análise de engenharia provêm de três tipos de fonte (MOSLEH *et al.*, 1988/1989):

1. Incerteza física ou variabilidade inerente, que é quantificada, de maneira geral, pela distribuição de probabilidade estimada dos dados;
2. Incerteza estatística, que se refere à incerteza nos parâmetros da distribuição estatística das variáveis aleatórias identificadas na primeira fonte, devido à escassez nos dados;
3. Incerteza na modelagem, que inclui incerteza nos modelos probabilísticos e de análise de sistema.

5.2.3 – Incertezas em Modelos

A idéia de incertezas em modelo está, comumente, relacionada com desvios entre o mundo real e sua representação simplificada em modelos. Quando se está analisando sistemas complexos na vida real, não é possível se conseguir conformidade entre as suposições do modelo e as propriedades do sistema que está sendo analisado. Na maioria dos casos, a questão é se o modelo pode ser aceito apesar de infringir uma ou mais das condições que dão suporte (corroboram) o modelo.

Claro está que algumas incertezas são mais fáceis de serem avaliadas do que outras. Portanto, pode ser útil se pensar com relação a certos tipos de distinção entre incertezas. Modos de se distinguir incertezas podem ser vistos a seguir:

1. Uma distinção importante é entre incerteza com relação a eventos ou variáveis que são observáveis, pelo menos em princípio, e incertezas com relação a eventos e variáveis que não o são. Por exemplo, suponha que se queira prever a temperatura máxima em um determinado dia, em uma localidade específica. Este é, claramente um evento observável.

   Quando especialistas são perguntados a respeito de probabilidades subjetivas é mais fácil para eles pensarem com relação a probabilidades para eventos observáveis (como a temperatura) do que em relação a valores não observáveis (tal qual o parâmetro, em um modelo físico ou estatístico, usado no auxílio à previsão de temperatura).
2. Quando se limita um modelo, é importante que se dê atenção a alguma incerteza que possa ser suprimida por esta limitação e que se ajuste à análise, de modo a

levar em conta tal incerteza (embora ajustes específicos sejam, freqüentemente, difíceis de justificar);

3. A informação surge de formas variadas, e das mais diversas fontes. Isto pode envolver, por exemplo, dados, modelos ou julgamentos de especialistas. Em problemas complexos utilizam-se todas as formas de informação. O analista deve estar habilitado a combinar informações das mais variadas fontes. Isto pode ser feito por meio de procedimentos inferenciais bayesianos.

Intuitivamente, uma distinção pode ser feita entre duas fontes de discrepâncias em modelos (NILSEN & AVEN, 2003):

1. limitações no conhecimento do fenômeno pelo analista;
2. simplificações deliberadas introduzidas pelo analista.

A fonte 1 diz respeito à capacidade de se capturar propriedades de sistemas do mundo real e o conhecimento do analista dos fenômenos físicos determinantes para o sistema que está sendo investigado. Fatores associados a esta falta de entendimento são, tipicamente (NILSEN & AVEN, 2003):

- sistemas e fenômenos altamente complexos;
- interação entre seres humanos e equipamentos técnicos;
- sistemas e fenômenos novos, para os quais ou existem poucos ou não existem modelos para representar adequadamente tais sistemas/fenômenos.

Métodos mais formais e estruturados, tais como métodos bayesianos têm sido usados para combinar o julgamento de especialistas. A opinião de um especialista pode vir de muitas maneiras (MOSLEH, 1992): um especialista pode fornecer uma estimativa pontual, parâmetros de uma distribuição de incertezas, ou seu melhor palpite com limites superior e inferior, e assim por diante.

A fonte 2 contribui para disparidades adicionais entre o modelo e o mundo, quando o analista, deliberadamente, usa modelos fora de sua área de aplicação, isto é, quando modelos são, propositadamente, selecionados para representar sistemas reais com as quais as suposições do modelo concordam somente parcialmente. Motivações para tal prática de modelagem podem ser (NILSEN & AVEN, 2003):

- Escolha entre a economia de projeto e o nível de detalhamento da modelagem;

- O modelo serve a seu propósito suficientemente bem, a despeito de algumas imprecisões;
- Conveniente redução dos esforços da análise.

Formas de se referenciar estes dois tipos de fontes de discrepâncias podem ser encontradas em NILSEN & AVEN (2003).

5.3 – Análise de Incerteza do Modelo, considerando Diversidade

Os resultados apresentados pelo modelo de LITTLEWOOD (1996) mostram a importância que a variabilidade representa em diversas áreas, e quão enganoso pode ser o caso de simplesmente calcular a média desta variação, quando se estão estudando as FCC. Mais importante, o comportamento médio de um componente médio não é suficiente para se conhecer a confiabilidade de um sistema redundante.

Um método mais refinado do que o apresentado no Capítulo 3, seguindo a mesma estrutura do modelo de Hughes (HUGHES, 1987), é apresentado a seguir. Neste método, as estimativas pontuais das probabilidades de falha dos diversos tipos de componentes [Eq. (3.8)] são substituídas pela distribuição a posteriori bayesiana, a partir dos quais elas são deduzidas. Com distribuições a priori independentes uniformes, tem-se, condicionalmente, a função de densidade (LITTLEWOOD, 1996):

$$f\left(\pi_A, \pi_B \mid e_j\right) = C\pi_A^{r_{Aj}} \left(1-\pi_A\right)^{n_{Aj}-r_{Aj}} .\pi_B^{r_{Bj}} \left(1-\pi_B\right)^{n_{Bj}-r_{Bj}} , \tag{5.1}$$

onde C é uma constante de normalização (HUGHES, 1987, descreve formas de se encontrar esta constante)[1]. Então, de acordo com LITTLEWOOD (1996), a distribuição conjunta incondicional das probabilidades de falha tem função de densidade:

$$f\left(\pi_A, \pi_B\right) = \sum_j f\left(\pi_A, \pi_B \mid e_j\right) \frac{q_j + 1}{\sum_k q_k + m} \tag{5.2}$$

Então, por exemplo, a probabilidade de falhas de um sistema AB 1-de-2 é:

$$E\left(\pi_A(E), \pi_B(E)\right) = \int_0^1 \int_0^1 \pi_A \pi_B f\left(\pi_A, \pi_B\right) d\pi_A d\pi_B \tag{5.3}$$

Estes resultados podem ser fácil e naturalmente estendidos para mais do que dois tipos de componentes. Assim, a probabilidade de falha de um sistema 2-de-3 é:

[1] A adoção da distribuição binomial advém do fato de que, em uma dada demanda ao sistema, os componentes do mesmo podem apresentar sucesso ou falha na resposta essa demanda.

$$E(\pi_A(E),\pi_B(E))+E(\pi_A(E),\pi_C(E))+E(\pi_B(E),\pi_C(E))-2E(\pi_A(E),\pi_B(E),\pi_C(E)) \tag{5.4}$$

Uma vantagem destes meios de se computar as confiabilidades do sistema é que eles decompõem em fatores os dois tipos diferentes de evidências necessárias – em relação ao comportamento do componente em um ambiente em particular, e em relação ao mecanismo de seleção dos ambientes.

5.4 – Análise de Incerteza do Modelo Selecionado, considerando Envelhecimento

Considere-se, novamente, que o modelo de taxa de falhas selecionado é da forma:

$$\lambda(t)=\lambda_0\exp[\beta(t-t_0)] \tag{5.5}$$

Intervalos de confiança para os parâmetros deste modelo, que levam em consideração as incertezas associadas ao processo, são obtidas da forma que se segue (de acordo com o apresentado em COX & LEWIS, 1966, e ATWOOD, 1992).

Uma região de confiança (aproximada) para β é o conjunto de todos os β_0 tais que:

$$t=\frac{L'(\beta_0)}{\sqrt{I(\beta_0)}} \tag{5.6}$$

é menor do que um valor z_α (em valor absoluto), onde z_α é um valor da tabela da distribuição normal [ou seja, dado que $\beta=\beta_0$, $t\sim N(0,1)$].

Na Equação (6.6), $L'(\beta)$ está definido na Equação (5.3) enquanto $I(\beta)$ é dado por:

$$I(\beta)=E\{-L''(\beta)\}=\begin{cases}\displaystyle\sum_j\left\{n_j\left[\frac{1}{\beta^2}-\frac{s_{1j}^2e^{-\beta s_{1j}}}{\left(1-e^{-\beta s_{1j}}\right)^2}\right]\right\} & (\beta\neq 0)\\ \\ \displaystyle\sum_j\frac{n_j s_{1j}^2}{12} & (\beta=0)\end{cases} \tag{5.7}$$

Considerando os valores observados dos dados amostrais disponíveis, obtém-se facilmente um intervalo de confiança para β.

Intervalos de confiança bilaterais para $\hat{\lambda}_0$, considerando-se dados censurados no tempo, com nível de confiança $100(1-\alpha)\%$ são dados por (JOHNSON & KOTZ, 1969):

$$\left[\frac{\chi^2_{2n,\frac{\alpha}{2}}}{2\nu},\ \frac{\chi^2_{2(n+1),1-\frac{\alpha}{2}}}{2\nu}\right], \tag{5.8}$$

onde $\nu = \sum \nu_j$,

$$\nu_j = \frac{\exp(\beta s^*_{0j})[\exp(\beta r_j)-1]}{\beta},$$

$n = \sum n_j$ e

s^*_{0j}, s_{1j} e r_j foram anteriormente definidos no Capítulo 5.

Em caso de dados censurados em falhas, defina-se $m = \sum m_j$ o número total de falhas, incluindo a falha final ao final do período de observação. Neste caso, os intervalos de confiança bilaterais, com nível de confiança $100(1-\alpha)\%$, para dados censurados em tempo e falhas são correspondentes, diferindo nos graus de liberdade ($2m$ ao invés de $2n$).

ATWOOD (1992) apresenta um processo gráfico para a obtenção da região de confiança bidimensional para (β, λ_0). A partir daí, um intervalo de confiança para $\lambda(t)$ consiste dos valores mínimos e máximos obtidos para $\lambda(t)$, à medida que os parâmetros β e λ_0 variam ao longo da região de confiança bidimensional. Tal intervalo de confiança, apesar de válido, tem algumas desvantagens:

- É conservativo;
- Requer uma busca numérica ao longo dos limites de confiança;
- O intervalo de confiança não é proveniente de nenhuma distribuição que possa ser usada como a priori conjugada em um método de Bayes. A possibilidade de uso desta priori conjugada facilitaria sobremaneira os cálculos.

5.4.1 – Intervalo de Confiança para $\lambda(t)$, baseado na Aproximação Assintótica de Normalidade

Tomando-se o logaritmo da Equação (4.13a), tem-se:

$$\log \lambda(t) = \log \lambda_0 + \beta(t - t_0) \tag{5.9}$$

A partir daí, assumindo-se que $(\hat{\beta}, \log \hat{\lambda}_0)$ tem distribuição aproximadamente normal bivariada (suposição esta válida para o modelo de taxa de falha exponencial – veja-se ATWOOD, 1992), então $\log \hat{\lambda}(t)$ também é, aproximadamente, normal. Com isto, intervalos de confiança para $\log \lambda(t)$ e, conseqüentemente, para $\lambda(t)$ podem ser obtidos.

Um intervalo de confiança $\lambda(t)$ com nível de confiança $100(1-\alpha)\%$, para um dado *t*, é dado por (DeGROOT, 1986):

$$\log \hat{\lambda}(t) \pm z_{1-\frac{\alpha}{2}} \left[\log \left(\frac{n}{\nu} \right) \right] \tag{5.10}$$

onde $z_{1-\frac{\alpha}{2}}$ é o $\left(1-\frac{\alpha}{2}\right)$-ésimo quantil da distribuição normal.

Limites de confiança válidos, simultaneamente, para todos os *t*, são dados por:

$$\log \hat{\lambda}(t) \pm \left[\chi^2_{1-\alpha}(2) \right]^{1/2} \left[\log \left(\frac{n}{\nu} \right) \right] \tag{5.11}$$

onde $\chi^2_{1-\alpha}(2)$ é o $(1-\alpha)$-ésimo quantil da distribuição qui-quadrado com dois graus de liberdade.

5.5 - Modelagem de Incertezas considerando Diversidade e Envelhecimento

De tudo o que foi apresentado anteriormente, verificou-se que o modelo apresentado por LITTLEWOOD (1996), apesar de considerar todos os efeitos inerentes à variabilidade ambiental, ignora os efeitos de envelhecimento, ao supor que seus componentes estão em seu período de vida útil. Ou seja, neste modelo, a despeito de haver dependência entre os componentes (ocorrência de falhas dependentes e de eventos de FCC), não há dependência temporal (com a suposição de taxas de falha constantes).

Para que tais efeitos sejam levados em consideração, este trabalho propõe uma modificação no modelo de LITTLEWOOD (1996), de modo a englobar os efeitos de

deterioração do componente com o passar do tempo. Como foi escolhido o modelo de taxa de falha exponencial para agregar os efeitos de envelhecimento (em função do que foi destacado no Capítulo 4, ou seja, não há restrições com relação aos valores que o parâmetro β pode assumir e os intervalos de confiança criados a partir deste modelo são mais fidedignos), então, na nova formulação, a probabilidade de falha para um componente específico, em um ambiente particular, será:

$$\pi(e) \equiv P(falha \mid E = e) = \sum_{C} f(c,e)S(c) \tag{5.12}$$

onde $f(c,e) = \lambda(t)\exp[\lambda(t)t], \qquad (t \geq 0)$

$\lambda(t) = \lambda_0 \exp[\beta(t - t_0)]$

As formas de se encontrar tanto uma estimativa pontual para a taxa de falhas, $\lambda(t)$, quanto intervalos de confiança representando toda a incerteza inerente à estimação de tal parâmetro foram descritas no Capítulo 4 e na Seção 5.4.

A probabilidade de seleção de um determinado componente (ou ambiente) será modelada por meio de uma distribuição multinomial. Uma estimativa da probabilidade de seleção de um determinado ambiente (p_j) será dada por:

$$\hat{p}_j = \frac{q_j + 1}{\sum_k q_k + m} \tag{5.13}$$

onde m é o número total de ambientes possíveis de serem selecionados.

As probabilidades p_j de seleção dos ambientes e_j serão consideradas imutáveis durante o tempo de observação considerado, e da primeira até a última demanda ao sistema.

O valor de p_j deve ser estimado da mesma maneira que é feita a estimação de $\pi(e_j)$, para cada ambiente, e ele será distribuído de acordo com os dados disponíveis. Contudo, quando da construção da distribuição completa de $f(\pi(E))$ somente é necessário o valor da estimativa da probabilidade média de seleção de um ambiente particular. Isto deve-se ao fato de que, em um dado ambiente, a variação da probabilidade de falha do sistema depende somente da variação de $\pi(e_j)$ e não da variação de p_j [veja-se a Eq. (4) de HUGHES, 1987]. Portanto, podem ser usados os valores esperados dos p_j [Eq. (5.13)] na expressão do cálculo da probabilidade de falha do sistema.

Sem perda de generalidade, considere-se um sistema *AB* (ou seja, um sistema diverso, composto de dois componentes). Estes dois componentes são selecionados aleatoriamente (via distribuição multinomial) de duas subpopulações, uma com todos os componentes do tipo *A* (subpopulação *C*1) e outra com os do tipo *B* (subpopulação *C*2). Assume-se que as probabilidades de falha dos componentes *A* e *B*, em um ambiente específico *E*=*e*, são independentemente distribuídas, com funções de densidade:

$$\pi_A(e) \equiv P(A\ falha \mid E=e) = 1 - e^{\int_0^{t'} -\lambda_A(t).t\,dt'} \tag{5.14}$$

$$\pi_B(e) \equiv P(B\ falha \mid E=e) = 1 - e^{\int_0^{t'} -\lambda_B(t).t\,dt'} \tag{5.15}$$

onde $t \geq 0$.

Com isso, a função de densidade, condicionada em um determinado ambiente selecionado, será, então, semelhante àquela descrita na Eq. (5.1), ou seja,

$$f(\pi_A, \pi_B \mid e_j) = C\pi_A^{r_{A_j}} (1-\pi_A)^{n_{A_j}-r_{A_j}} .\pi_B^{r_{B_j}} (1-\pi_B)^{n_{B_j}-r_{B_j}} \tag{5.16}$$

Em função de dificuldades de se determinar a constante de normalização *C*, e em função de se ter, explicitamente, as *f.d.p.* de $\pi_A(e_j)$ e de $\pi_B(e_j)$, adotar-se-á, ao invés do modelo binomial, um modelo de Poisson para a *f.d.p.*, condicionada em um determinado ambiente selecionado, ou seja:

$$f(t_A, t_B \mid e_j) = \frac{e^{-\tau_{A_j}} .\tau_{A_j}{}^{r_{A_j}}}{r_{A_j}!} . \frac{e^{-\tau_{B_j}} .\tau_{B_j}{}^{r_{B_j}}}{r_{B_j}!} \tag{5.17}$$

onde $\tau_{i_j} = n_{ij}.\pi_{i_j}(e_j)$

$$\pi_{i_j}(e_j) = 1 - e^{\int_0^{t'} -\lambda_i(t).t_i\,dt'}$$

$i = A, B$

Esta nova formulação é uma evolução do modelo inicialmente apresentado por SANT'ANA & FRUTUOSO e MELO (2005). Evidentemente, a adoção do modelo de Poisson é uma simplificação do modelo original, sujeito a restrições que devem ser obedecidas, de modo a se ter boas aproximações. Tais restrições são:

1. O tamanho amostral n_{ij} $(i = A, B)$ deve ser maior ou igual a 15;
2. A probabilidade de falha dos componentes, em um determinado ambiente, $\pi_{i_j}(e_j)$, deve ser menor ou igual a 0,07.

Então, a distribuição conjunta incondicional das probabilidades de falha tem função de densidade:

$$f(t_A, t_B) = \sum_j f(t_A, t_B \mid e_j) \frac{q_j + 1}{\sum_k q_k + m}$$

$$f(t_A, t_B) = \sum_j \frac{e^{-\tau_{A_j}} . \tau_{A_j}{}^{r_{A_j}}}{r_{A_j}!} \cdot \frac{e^{-\tau_{B_j}} . \tau_{B_j}{}^{r_{B_j}}}{r_{B_j}!} \cdot \frac{q_j + 1}{\sum_k q_k + m} \tag{5.18}$$

Então, por exemplo, o valor esperado da probabilidade de falha obtido a partir da distribuição de probabilidade de falhas de um sistema *AB* 1-de-2, considerando agora tanto os efeitos de diversidade e da seleção de ambientes, para todos os ambientes, quanto os efeitos de envelhecimento, é:

$$f(t_A, t_B) = \int_0^\infty \int_0^\infty \sum_j \left(1 - e^{\int_0^{t'} -\lambda_A(t).t_A dt'}\right)\left(1 - e^{\int_0^{t''} -\lambda_B(t).t_B dt''}\right) \frac{e^{-\tau_{A_j}} . \tau_{A_j}{}^{r_{A_j}}}{r_{A_j}!} \cdot \frac{e^{-\tau_{B_j}} . \tau_{B_j}{}^{r_{B_j}}}{r_{B_j}!} \cdot \frac{q_j + 1}{\sum_k q_k + m} dt_A dt_B \tag{5.19}$$

Assim, para este mesmo exemplo, o valor esperado da probabilidade de falha da distribuição bivariada proposta que englobe todos os efeitos de incerteza com relação aos mecanismos de seleção de componentes e ambientes, os efeitos de diversidade e incerteza, será da forma:

$$E\left[f\left(t_A, t_B\right)\right] = \int_0^{\infty}\int_0^{\infty}\sum_j \left(1 - e^{\int_0^{t'} -\lambda_A(t).t_A\,dt'}\right)\left(1 - e^{\int_0^{t''} -\lambda_B(t).t_B dt''}\right) \frac{e^{-n_{A_j}\cdot\left(1-e^{\int_0^{t'} -\lambda_A(t).t_A\,dt'}\right)}\cdot\left[n_{A_j}\left(1 - e^{\int_0^{t'} -\lambda_A(t).t_A\,dt'}\right)\right]^{r_{A_j}}}{r_{A_j}!}\cdot$$

$$\frac{e^{-n_{B_j}\left(1-e^{\int_0^{t''} -\lambda_B(t).t_B dt''}\right)}\cdot\left[n_{B_j}\left(1 - e^{\int_0^{t''} -\lambda_B(t).t_B dt''}\right)\right]^{r_{B_j}}}{r_{B_j}!}\cdot\frac{q_j + 1}{\sum_k q_k + m}\,dt_A dt_B \tag{5.20}$$

Convém ressaltar que o resultado aqui obtido para um sistema 1-de-2 pode ser facilmente generalizado para sistemas com mais de dois tipos de componentes diferentes, da mesma maneira como foi apresentado na Seção 5.3. Ou seja, por exemplo, a probabilidade de falha de um sistema 2-de-3 seria:

$$E\left[f\left(t_A, t_B\right)\right] + E\left[f\left(t_A, t_C\right)\right] + E\left[f\left(t_B, t_C\right)\right] - 2E\left[f\left(t_A, t_B, t_C\right)\right] \tag{5.21}$$

No Capítulo 6, são apresentados exemplos que demonstram a aplicabilidade dos testes descritos no Capítulo 4, são calculadas as taxas de falha dos componentes considerados e comparadas as evoluções tanto das taxas quanto das probabilidades de falha, quando consideradas taxas de falha tanto constantes quanto dependentes do tempo.

Capítulo 6 – Exemplos Práticos

6.1 – Introdução

Neste capítulo, serão apresentados exemplos que demonstram a aplicabilidade do modelo proposto, ao analisar casos envolvendo diferentes tipos de equipamentos, em diferentes situações.

Aqui, assume-se a mesma estratégia adotada por Hughes (HUGHES, 1987) no qual todas as falhas em uma dada demanda são devidas a uma mesma causa, isto é, causas comuns diferentes ou uma causa comum e uma falha independente não ocorrem simultaneamente – tal simplificação não é necessária, porém facilita a explanação dos princípios. Em outras palavras, o ambiente no qual as falhas ocorrem é o mesmo, e este fato acontece para todas as demandas de sistemas. Note-se que, em função disso, todas as falhas independentes poderiam ser classificadas juntas, representando um ambiente no qual nenhuma falha de causa comum esteja presente. HUGHES (1987) demonstra que há pouca variabilidade entre os resultados obtidos quando do agrupamento ou não de ambientes no qual as falhas ocorrem.

Por exemplo, demandas produzidas pelo mesmo par de números para falhas de componentes dos tipos *A* e *B* correspondem a ambientes únicos; isto não é, evidentemente, realista e foi adotado simplesmente para propósitos ilustrativos. Por exemplo, todas as falhas que produzem o par (1,1) (falha do componente *A* e falha do componente *B*) estão no mesmo ambiente, o que nem sempre é verdade, pois pode haver dois ambientes hostis aos componentes e que podem levar à falha de ambos.

6.2 – 1º. Exemplo: Geradores Diesel em uma Usina Nuclear

Neste exemplo (adaptado de LOFGREN & GREGORY, 1991), tem-se um sistema composto de dois geradores diesel, com lógica de votação 1-de-2, cuja operação foi observada durante 8.760 horas (1 ano). Os tempos de falha de cada um dos geradores estão descritos no Apêndice B. A partir destes dados, são apresentadas tabelas com os valores numéricos obtidos para todos os testes apresentados no Capítulo 4, os valores das estatísticas referentes a estes valores calculados e a conclusão que se pode obter a partir da comparação entre o valor obtido e o valor da estatística considerado (utilizando-se como nível de significância α=0,05, para testes bilaterais, o que nos fornece, na cauda inferior, $\frac{\alpha}{2} = 0{,}025$, e na cauda superior, $1 - \frac{\alpha}{2} = 0{,}975$):

- **Teste para detecção de tendência no sistema:**

O valor da Eq. (4.3), em função dos dados disponíveis, e juntamente com o valor da estatística associada a tal valor e a conclusão referente à análise de ambos, é apresentada na Tabela 6.1.

Tabela 6.1: Resultado calculado de teste para tendência para o sistema composto por GD-1 e GD-2 e respectiva estatística correspondente ao valor obtido.

Teste de envelhecimento para os sistemas	Valor Calculado (Eq. 4.3)	Valor da Estatística (α/2 = 0,025 e 1-α/2 = 0,975)		Interpretação
Sistema GD :	-0,5871	Φ(-0,59)	0,2786	Dados não apresentam tendência

- **Testes para detecção de tendência em cada um dos componentes do sistema:**

Os valores das Eq. (4.6-11), calculados a partir dos dados, os valores das estatísticas associadas a cada valor calculado e as conclusões tiradas com relação à análise dos resultados obtidos, são apresentados na Tabela 6.2 (para o GD-1) e na Tabela 6.3 (para o GD-2).

Tabela 6.2: Resultados calculados de testes para tendências para o GD-1 e respectivas estatísticas correspondentes aos valores obtidos.

Testes para tendência monotônica	Valores Calculados (Eq. 4.6-11)	Valores das Estatísticas (α/2 = 0,025 e 1-α/2 = 0,975)		Interpretação
U	0,1341	Φ(0,13)	0,5533	Dados não apresentam tendência
Z	16,5253	χ^2 (16,52; 40)	0,0004	Dados apresentam tendência
Teste alternativo para tendência monotônica				
J	0,1370	*t* (0,14; 20)	0,5538	Dados não apresentam tendência
Testes para tendência não monotônica				
V1	0,4715	Φ(0,47)	0,6814	Dados não apresentam tendência
V2	0,2936	Φ(0,29)	0,6155	Dados não apresentam tendência
V3	14,9698	χ^2 (14,97; 40)	0,0001	Dados apresentam tendência

Tabela 6.3: Resultados calculados de testes para tendências para o GD-2 e respectivas estatísticas correspondentes aos valores obtidos.

Testes para tendência monotônica	Valores Calculados (Eq. 4.6-11)	Valores das Estatísticas (α/2 = 0,025 e 1-α/2 = 0,975)		Interpretação
U	-0,4373	Φ(-0,44)	0,3309	Dados não apresentam tendência
Z	11,5952	χ^2 (11,60; 28)	0,0027	Dados apresentam tendência
Teste alternativo para tendência monotônica				
J	-0,5263	*t* (-0,53; 14)	0,3035	Dados não apresentam tendência
Testes para tendência não monotônica				
V1	-0,2411	Φ(-0,24)	0,4047	Dados não apresentam tendência
V2	-0,3841	Φ(-0,38)	0,3504	Dados não apresentam tendência
V3	12,9822	χ^2 (12,98; 28)	0,0070	Dados apresentam tendência

A partir dos resultados obtidos nestes testes, pode-se observar que nem o sistema nem seus componentes apresentam tendências que os caracterizariam como envelhecidos. Portanto, estes são considerados em seu período de vida útil e, conseqüentemente, apresentam taxas de falha aproximadamente constantes, cujos valores são:

- GD-1 : $\lambda(t) = 1{,}41x10^{-3} \exp\left[3{,}37x10^{-5}.t\right]/h$;
- GD-2 : $\lambda(t) = 1{,}10x10^{-3} \exp\left[-1{,}37x10^{-4}.t\right]/h$.

Verifica-se, das equações para as taxas de falha apresentadas acima, que as interdependências entre os componentes influenciam decisivamente o comportamento da taxa de falha do sistema, considerada constante, visto que a taxa de falha do GD-1 é ligeiramente crescente enquanto que a do GD-2 é ligeiramente decrescente. Porém, as taxas de falha dos componentes GD-1 e GD-2 apresentam tendências que, do ponto de vista estatístico, são considerada não significativas.

O gráfico da evolução da taxa de falhas do sistema é apresentado na Figura 6.1.

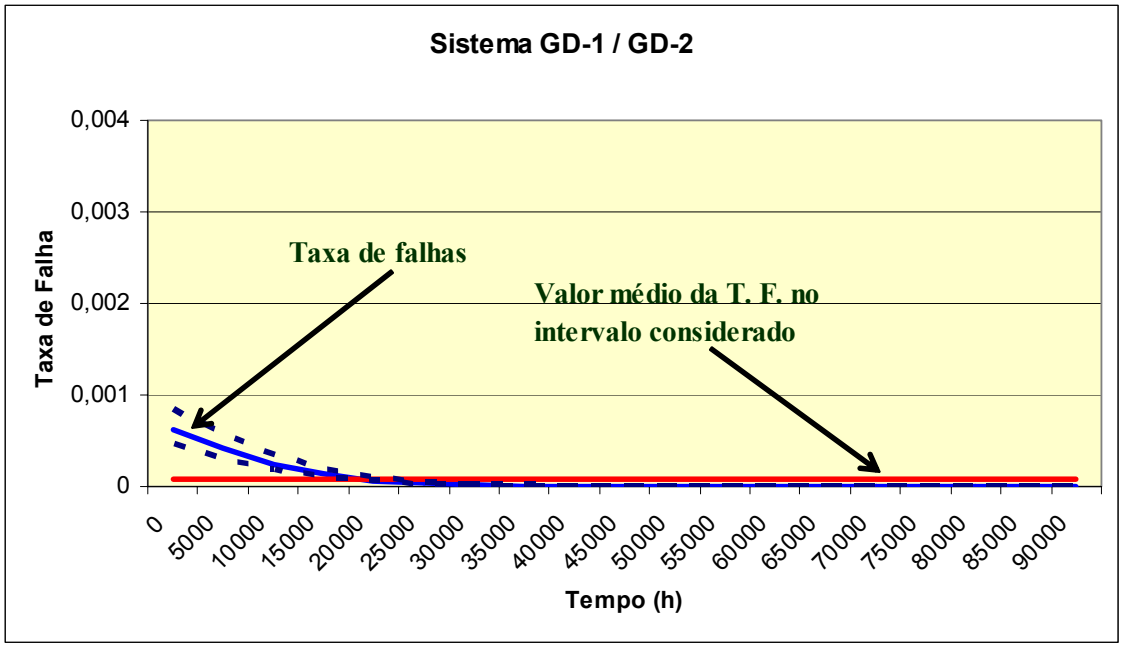

Figura 6.1 – Gráfico da evolução da taxa de falha do sistema GD-1A / GD-1B com o tempo.

Verifica-se, pela Figura 6.1, que há uma tendência à convergência dos limites inferior e superior do intervalo de confiança para a taxa de falha do sistema; veja-se, também que a taxa de falhas converge para um valor-limite (aproximadamente $9{,}42x10^{-6}$/h). Tais fatos corroboram os resultados dos testes apresentados nas Tabelas 6.1, 6.2 e 6.3, as quais indicam uma ausência de tendência para a taxa de falha.

8.3 – 2º. Exemplo: Sistema de Motores Diesel

Neste exemplo (adaptado de ASCHER & FEINGOLD, 1984), têm-se dois motores diesel, cujo período de observação foi de 27.000 horas (aproximadamente 3 anos). Os dados de falha levantados são apresentados no Apêndice B. Os valores numéricos dos testes, os valores das estatísticas referentes a estes valores calculados e a conclusão que se pode obter a partir da comparação entre o valor obtido e o valor da estatística considerado (utilizando-se como nível de significância α=0,05, para testes de hipóteses bilaterais, o que nos fornece, na cauda inferior, $\frac{\alpha}{2} = 0{,}025$, e na cauda superior, $1 - \frac{\alpha}{2} = 0{,}975$) são apresentados a seguir.

- **Teste para detecção de tendência no sistema:**

O valor da Eq. (4.3), em função dos dados disponíveis, e juntamente com o valor da estatística associada a tal valor e a conclusão referente à análise de ambos, é apresentada na Tabela 6.4.

Tabela 6.4: Resultado calculado de teste para tendência para o sistema composto por DG3 e DG4 e respectiva estatística correspondente ao valor obtido.

Teste de envelhecimento para os sistemas	Valor Calculado (Eq. 4.3)	Valor da Estatística (α/2 = 0,025 e 1-α/2 = 0,975)		Interpretação
Sistema A&F :	12,6438	Φ (12,64)	1	Dados apresentam tendência

- **Teste para detecção de tendência em cada um dos componentes do sistema:**

Os valores das Eq. (4.6-11), calculados a partir dos dados, os valores das estatísticas associadas a cada valor calculado e as conclusões tiradas com relação à análise dos resultados obtidos, são apresentados na Tabela 6.5 (para o DG3) e na Tabela 6.6 (para o DG4).

Tabela 6.5: Resultados calculados de testes para tendências para o DG3 e respectivas estatísticas correspondentes aos valores obtidos.

Testes para tendência monotônica	Valores Calculados (Eq. 4.6-11)	Valores das Estatísticas (α/2 = 0,025 e 1-α/2 = 0,975)		Interpretação
U	7,4832	Φ(7,48)	1	Dados apresentam tendência
Z	25,4202	χ^2 (25,42; 154)	0	Dados apresentam tendência
Teste alternativo para tendência monotônica				
J	4,5819	*t*(4,58; 77)	0,9999	Dados apresentam tendência
Testes para tendência não monotônica				
V1	3,7824	Φ(3,78)	0,9999	Dados apresentam tendência
V2	3,4602	Φ(3,46)	0,9997	Dados apresentam tendência
V3	41,2809	χ^2 (41,28; 154)	0	Dados apresentam tendência

Tabela 6.6: Resultados calculados de testes para tendências para o DG4 e respectivas estatísticas correspondentes aos valores obtidos.

Testes para tendência monotônica	Valores Calculados (Eq. 4.6-11)	Valores das Estatísticas (α/2 = 0,025 e 1-α/2 = 0,975)		Interpretação
U	0,1497	Φ(0.15)	0,5595	Dados não apresentam tendência
Z	28,2548	χ^2 (28.25, 76)	1,1E-07	Dados apresentam tendência
Teste alternativo para tendência monotônica				
J	0,1793	*t*(0.18, 38)	0,4293	Dados não apresentam tendência
Testes para tendência não monotônica				
V1	-1,2342	Φ(-1.23)	0,1086	Dados não apresentam tendência
V2	-1,2089	Φ(-1.21)	0,1133	Dados não apresentam tendência
V3	39,6553	χ^2 (39.66, 76)	0,0002	Dados apresentam tendência

A partir dos resultados obtidos nestes testes, conclui-se que o sistema apresenta uma tendência, a despeito de apenas um dos dois componentes presentes no sistema apresentar este comportamento, ou seja, tem-se um dos componentes envelhecido e o outro em seu período de vida útil (para o nível de significância α determinado). A interdependência entre os dois componentes do sistema pode ser a causa desta tendência apresentada pelo sistema. Tais interdependências podem ser provenientes de muitas causas, como ambiente físico comum, mesma política de teste e manutenção, entre outros fatores.

As taxas de falha para os componentes do sistema têm como valores:

- DG3 : $\lambda(t) = 3{,}25x10^{-4} \exp\left[1{,}38x10^{-4}.t\right]/h$;
- DG4 : $\lambda(t) = 3{,}69x10^{-3} \exp\left[8{,}52x10^{-6}.t\right]/h$.

Os gráficos da evolução da taxa de falha de cada um dos componentes do sistema são dados nas Figuras 6.2 e 6.3.

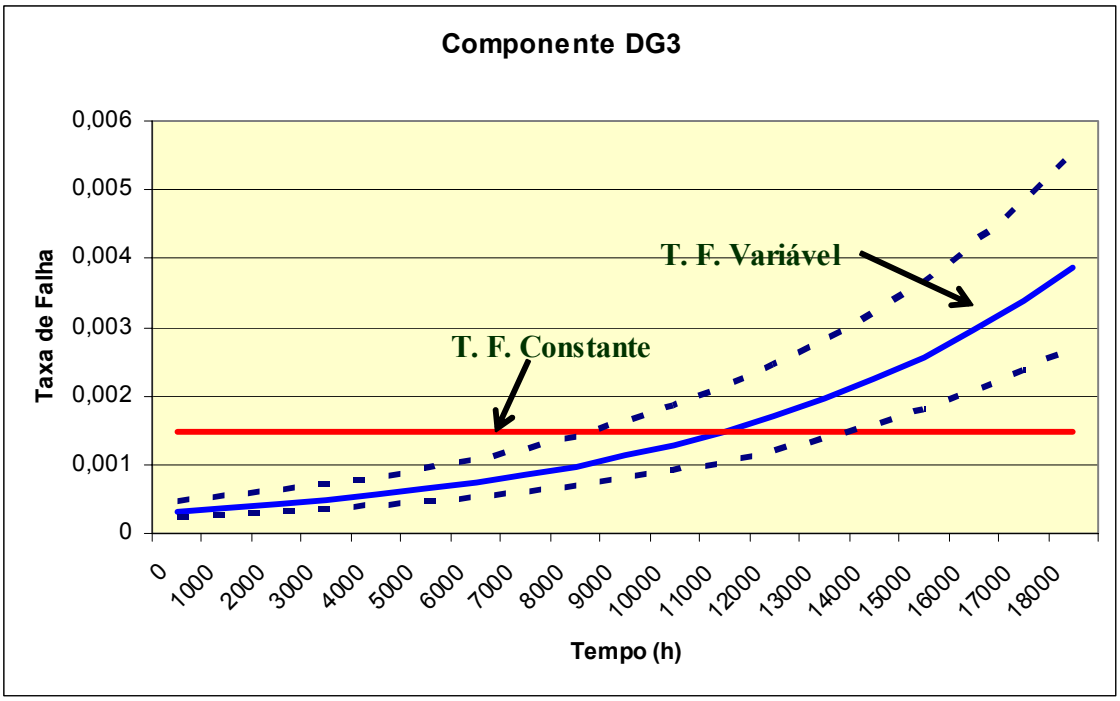

Figura 6.2 – Gráfico da evolução da taxa de falha do componente DG3 com o tempo.

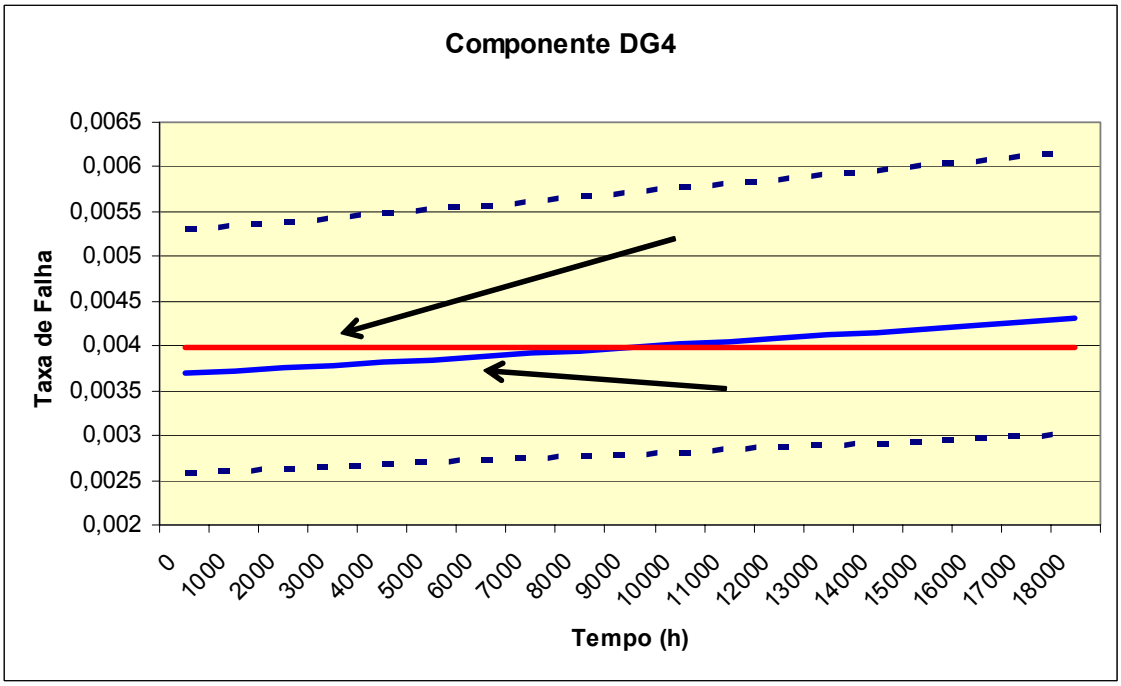

Figura 6.3 – Gráfico da evolução da taxa de falha do componente DG4 com o tempo.

Verifica-se, da Figura 6.3, que a taxa de falha do componente DG4 encontrar-se-ia dentro do intervalo de confiança, caso esta fosse considerada constante (no caso deste exemplo, esta taxa de falha constante somente fica menor que o limite inferior de tal intervalo de confiança após um tempo maior do que 55.000 horas).

A partir daí, podem ser gerados gráficos que mostram a evolução tanto da taxa quanto da probabilidade de falha do sistema em questão, com os respectivos intervalos de confiança. Tais gráficos são apresentados nas Figuras 6.4 e 6.5.

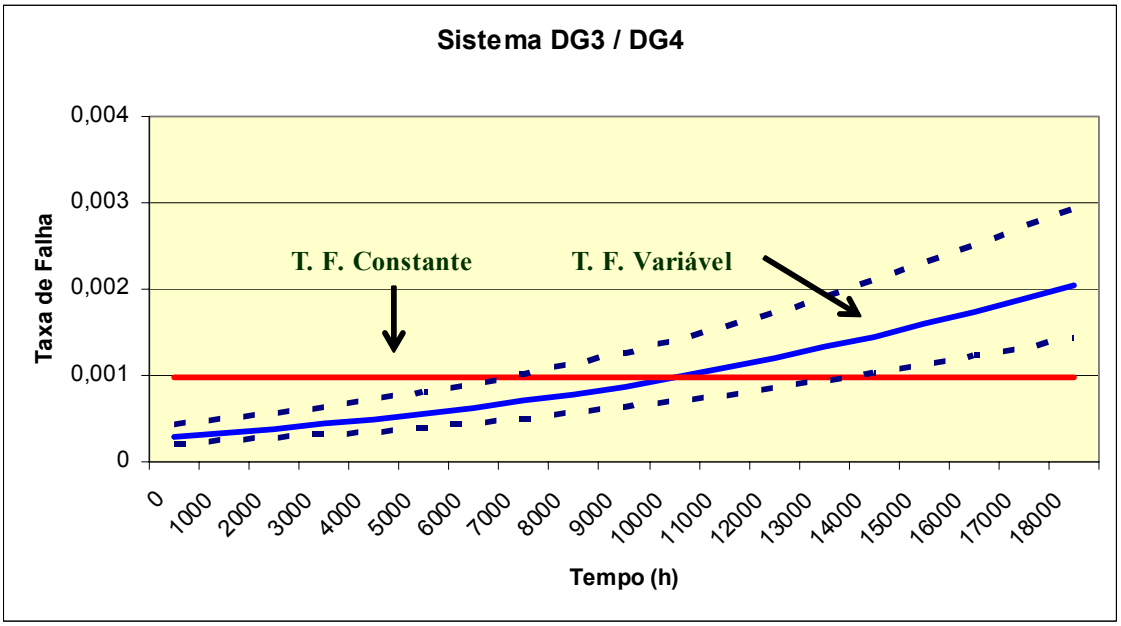

Figura 6.4 – Gráfico da evolução da taxa de falha do sistema DG3 / DG4 com o tempo.

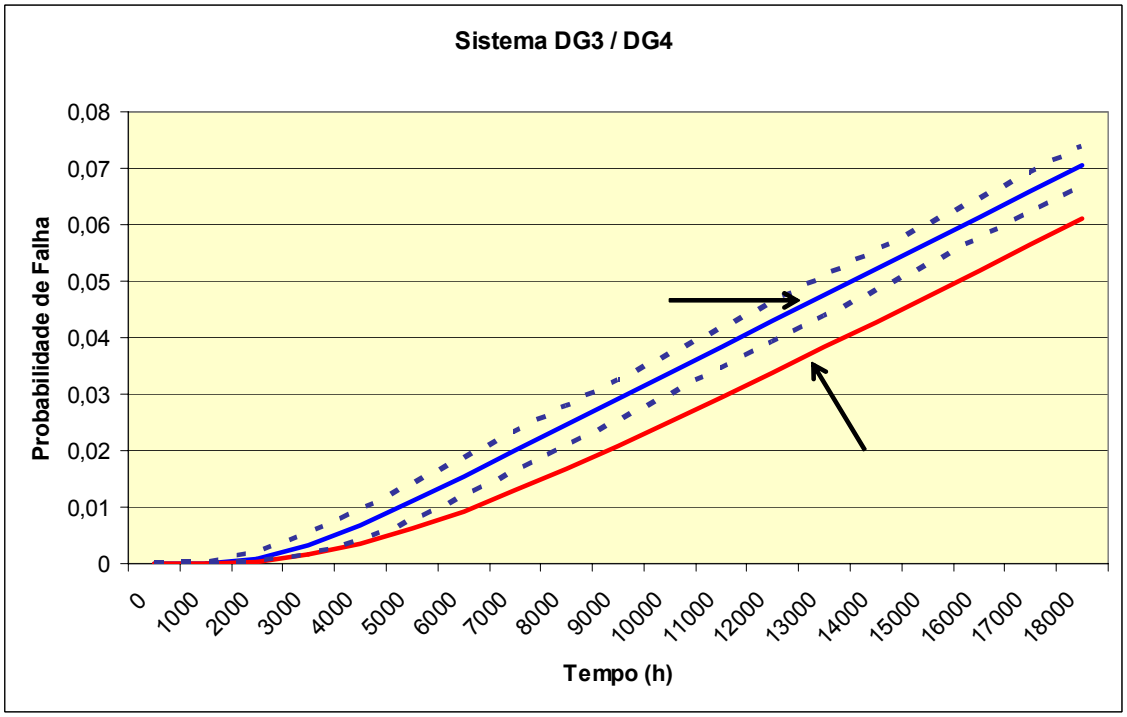

Figura 6.5 – Gráfico da evolução da probabilidade de falha do sistema DG3 / DG4 com o tempo.

Conforme esperado, a probabilidade de falha do sistema quando consideradas taxas de falha variáveis é maior do que quando as mesmas são consideradas constantes

(visto que a taxa de falhas é maior), tendendo à convergência para um valor comum para ambas à medida que o tempo aumenta, conforme mostrado na Figura 6.6.

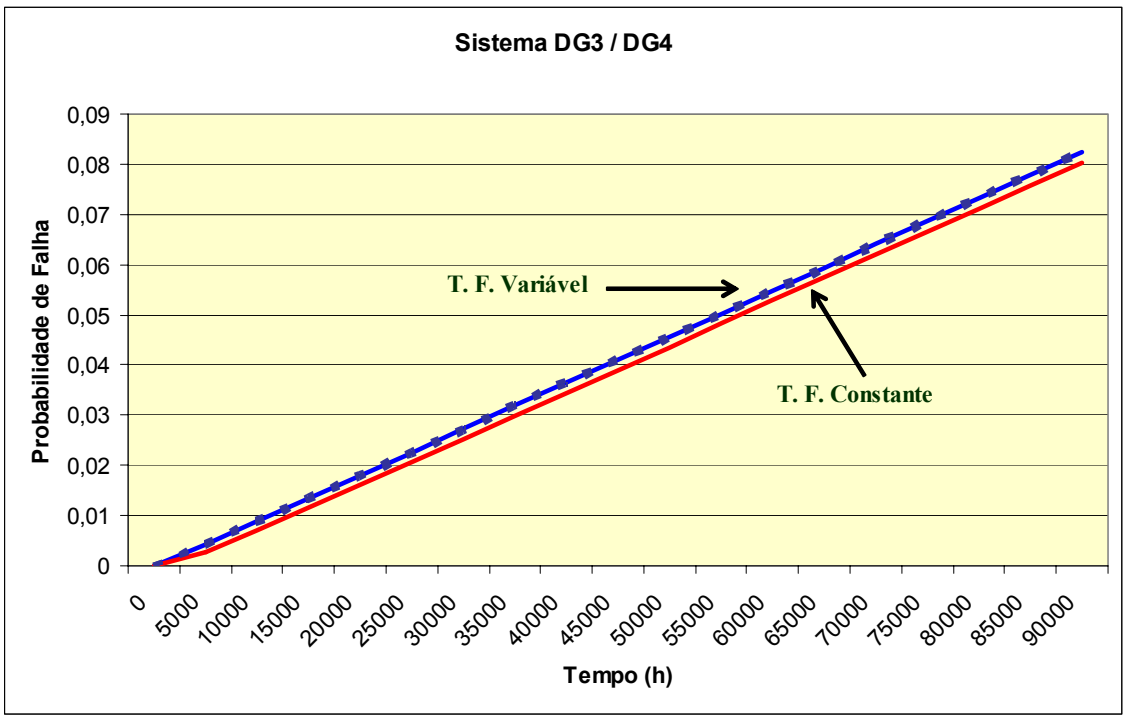

Figura 6.6 – Gráfico da evolução da probabilidade de falha do sistema DG3 / DG4 com o tempo, mostrando a convergência das probabilidades com o tempo.

Veja-se também que à medida que o valor do limite inferior do intervalo de confiança para a taxa de falhas variável do sistema afasta-se do valor da taxa de falhas constante, tem-se que a diferença entre os valores das probabilidades de falha para o sistema considerando-se taxas de falha variáveis e constantes aumenta (até o ponto em que se inicia a convergência entre ambas).

8.4 – 3º. Exemplo: Geradores Diesel em uma Usina Nuclear

Neste exemplo (adaptado de LOFGREN & GREGORY, 1991), tem-se um sistema composto de dois geradores diesel, com lógica de votação 1-de-2, cuja operação foi observada durante 87.600 horas (10 anos). Os tempos de falha de cada um dos geradores estão descritos no Apêndice B. A partir destes dados, são apresentadas tabelas com os valores numéricos obtidos para todos os testes apresentados no Capítulo 4, os valores das estatísticas referentes a estes valores calculados e a conclusão que se pode obter a partir da comparação entre o valor obtido e o valor da estatística

considerado (utilizando-se como nível de significância α=0,05, para testes bilaterais, o que nos fornece, na cauda inferior, $\frac{\alpha}{2} = 0{,}025$, e na cauda superior, $1 - \frac{\alpha}{2} = 0{,}975$):

- **Teste para detecção de tendência no sistema:**

O valor da Eq. (4.3), em função dos dados disponíveis, e juntamente com o valor da estatística associada a tal valor e a conclusão referente à análise de ambos, é apresentada na Tabela 6.7.

Tabela 6.7: Resultado calculado de teste para tendência para o sistema composto por GD-A e GD-C e respectiva estatística correspondente ao valor obtido.

Teste de envelhecimento para os sistemas	Valor Calculado (Eq. 4.3)	Valor da Estatística (α/2 = 0,025 e 1-α/2 = 0,975)		Interpretação
Sistema GD :	13,6993	Φ (13,70)	1	Dados apresentam tendência

- **Teste para detecção de tendência em cada um dos componentes do sistema:**

Os valores das Eq. (4.6-11), calculados a partir dos dados, os valores das estatísticas associadas a cada valor calculado e as conclusões tiradas com relação à análise dos resultados obtidos, são apresentados na Tabela 6.8 (para o GD-A) e na Tabela 6.9 (para o GD-C).

Tabela 6.8: Resultados calculados de testes para tendências para o GD-A e respectivas estatísticas correspondentes aos valores obtidos.

Testes para tendência monotônica	Valores Calculados (Eq. 4.6-11)	Valores das Estatísticas (α/2 = 0,025 e 1-α/2 = 0,975)		Interpretação
U	2,8030	Φ(2.80)	0,9975	Dados apresentam tendência
Z	14,6329	χ^2 (14.63, 68)	6,9E-13	Dados apresentam tendência
Teste alternativo para tendência monotônica				
J	1,3861	*t*(1.39, 34)	0,9126	Dados não apresentam tendência
Testes para tendência não monotônica				
V1	-2,7068	Φ(-2.71)	0,0034	Dados apresentam tendência
V2	-2,0490	Φ(-2.05)	0,0202	Dados apresentam tendência
V3	44,5020	χ^2 (44.50, 68)	0,0122	Dados apresentam tendência

Tabela 6.9: Resultados calculados de testes para tendências para o GD-C e respectivas estatísticas correspondentes aos valores obtidos.

Testes para tendência monotônica	Valores Calculados (Eq. 4.6-11)	Valores das Estatísticas (α/2 = 0,025 e 1-α/2 = 0,975)		Interpretação
U	2,8661	Φ(2.87)	0,9979	Dados apresentam tendência
Z	5,0219	χ^2 (5.02, 32)	1,1E-08	Dados apresentam tendência
Teste alternativo para tendência monotônica				
J	1,8264	*t*(1.83, 16)	0,9567	Dados não apresentam tendência
Testes para tendência não monotônica				
V1	2,4995	Φ(2.50)	0,9938	Dados apresentam tendência
V2	2,3105	Φ(2.31)	0,9896	Dados apresentam tendência
V3	6,0677	χ^2 (6.07, 32)	1,4E-07	Dados apresentam tendência

A partir dos resultados obtidos nestes testes, conclui-se que o sistema apresenta uma tendência, além dos componentes também apresentarem tendência (para o nível de significância α determinado).

As taxas de falha para os componentes do sistema têm como valores:

- GD-A : $\lambda(t) = 1{,}60x10^{-4} \exp\left[2{,}22x10^{-5}.t\right]/h$;
- GD-C : $\lambda(t) = 3{,}63x10^{-5} \exp\left[3{,}27x10^{-5}.t\right]/h$.

Os gráficos da evolução da taxa de falha de cada um dos componentes do sistema são dados nas Figuras 6.6 e 6.7.

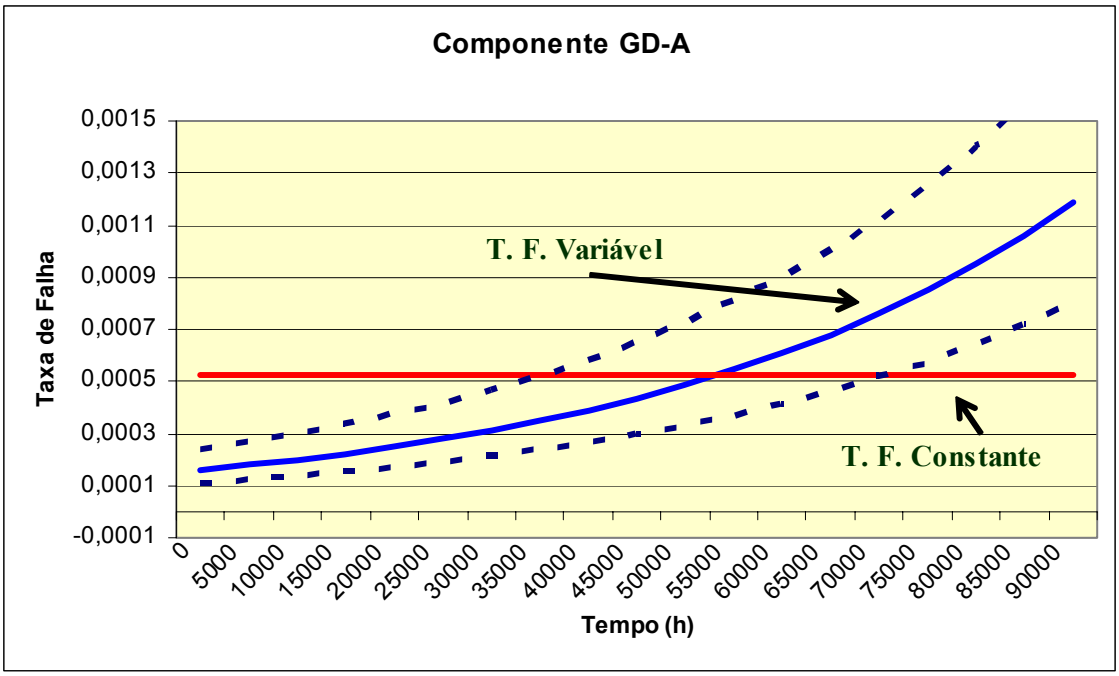

Figura 6.7 – Gráfico da evolução da taxa de falha do componente GD-A com o tempo.

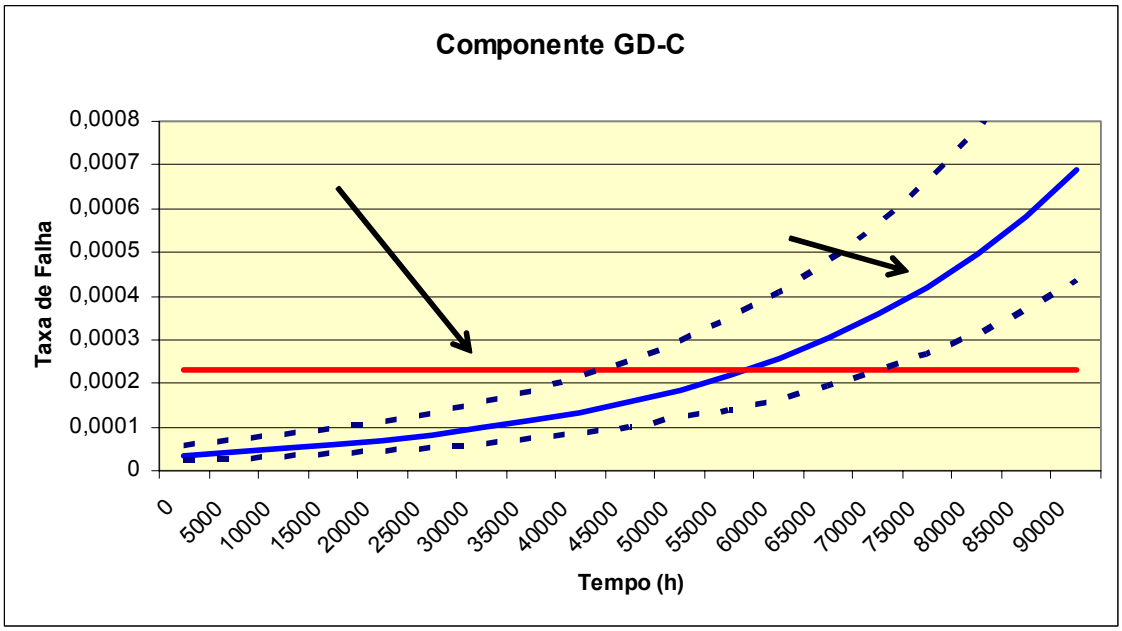

Figura 6.8 – Gráfico da evolução da taxa de falha do componente GD-C com o tempo.

Com isso, podem ser gerados gráficos que mostram a evolução tanto da taxa quanto da probabilidade de falha do sistema em questão, com os respectivos intervalos de confiança. Tais gráficos são apresentados nas Figuras 6.9 e 6.10.

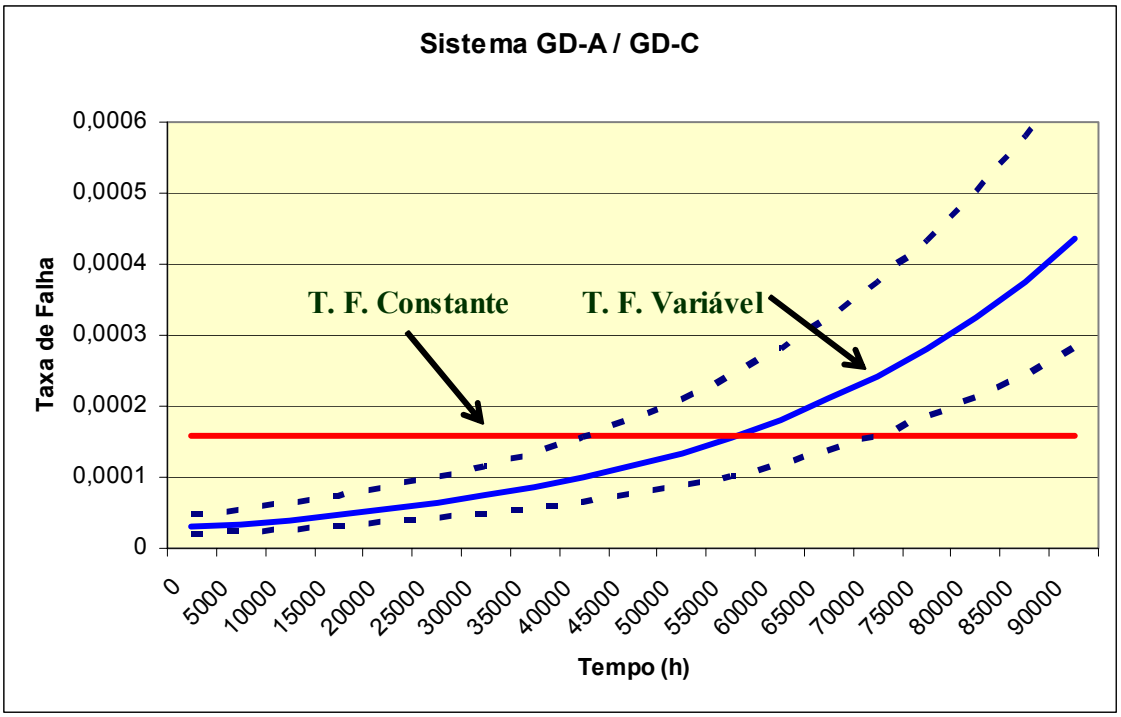

Figura 6.9 – Gráfico da evolução da taxa de falha do sistema GD-A/ GD-C com o tempo.

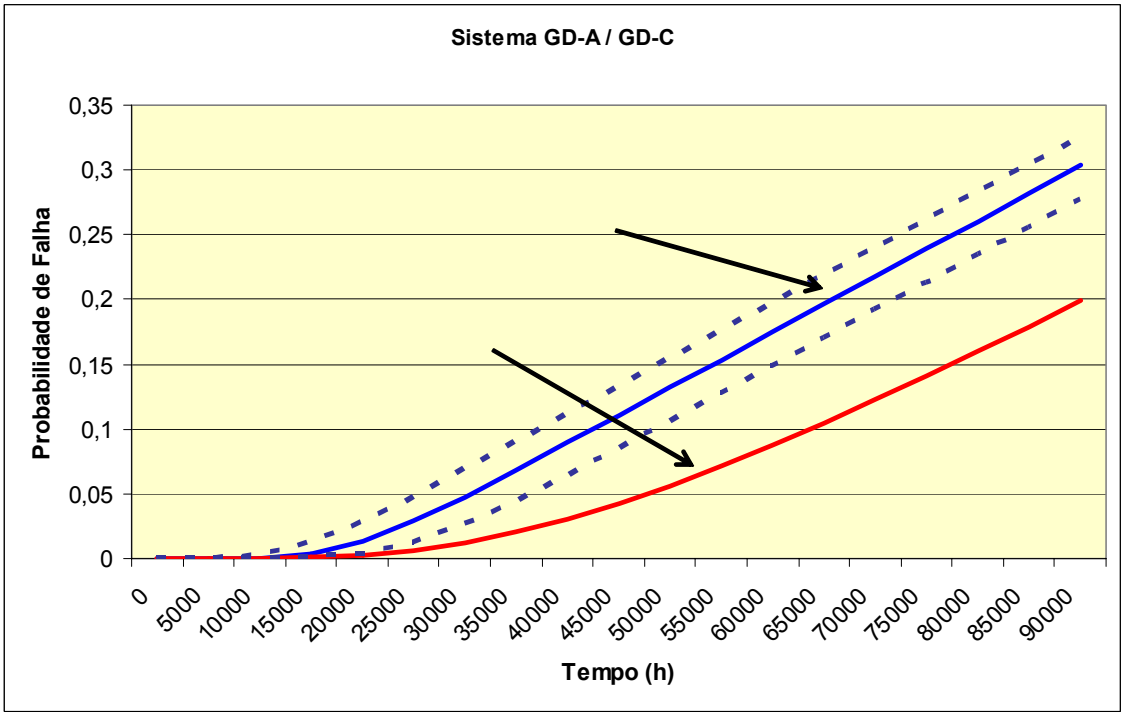

Figura 6.10 – Gráficos da evolução da probabilidade de falha do sistema GD-A/GD-C com o tempo.

As mesmas conclusões apresentadas no Exemplo 2 podem ser estendidas a este caso, ou seja, o uso de taxas de falha constantes subdimensiona o valor final da probabilidade de falha, tanto dos componentes quanto do sistema considerado, com o

enfoque de que quando os componentes do sistema estão todos envelhecidos este subdimensionamento é ainda mais evidente. Isto pode ser visto nas Figuras 6.11 e 6.12, que apresenta a variação percentual entre as probabilidades de falha, quando consideradas taxas de falha variáveis e constantes, para dois casos-exemplo (2º. e 3º. exemplos). Verifica-se, também, claramente, que, à medida que o tempo aumenta, a diferença percentual entre as probabilidades de falha, considerando taxas de falha variáveis e constantes, aumenta, em função do aumento da diferença entre as taxas de falha, até um determinado patamar (Figura 6.11); a partir daí, tal diferença diminui, o que corrobora a afirmação de convergência de ambas para um único valor (Figura 6.12).

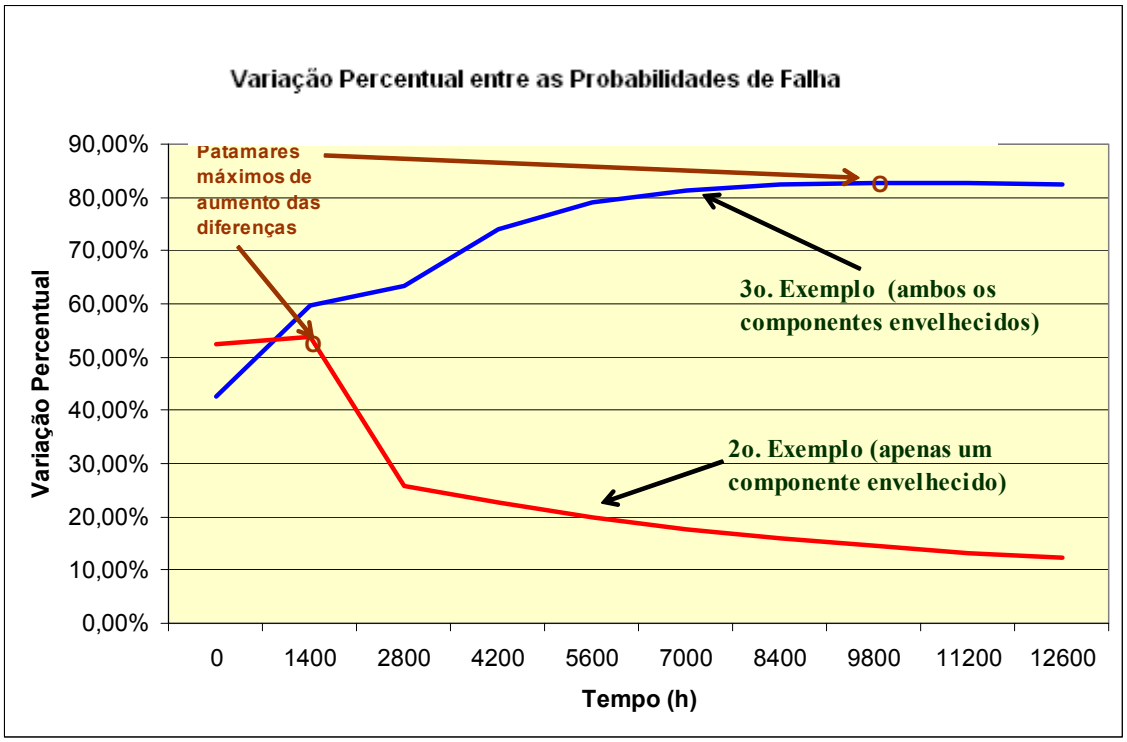

Figura 6.11 – Gráfico da variação percentual entre as probabilidades de falha do sistema, quando consideradas taxas de falhas variáveis no tempo e constantes, e para dois casos-exemplo (Tempo<14.000h).

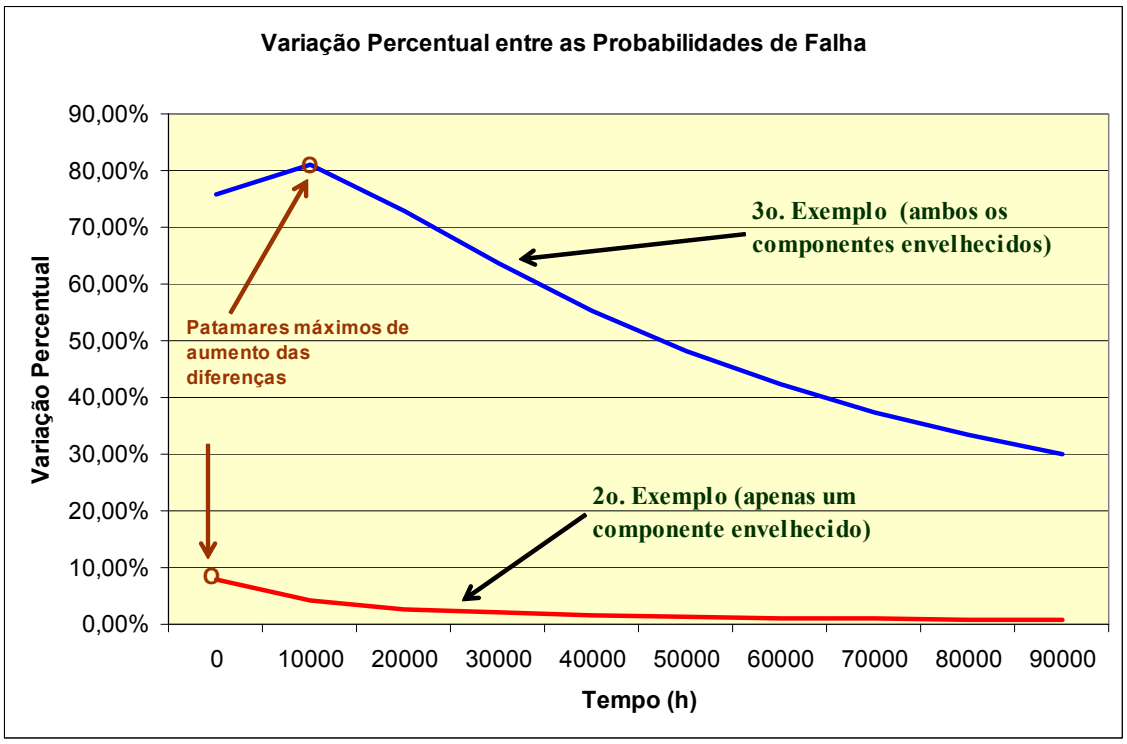

Figura 6.12 – Gráfico da variação percentual entre as probabilidades de falha do sistema, quando consideradas taxas de falhas variáveis no tempo e constantes, e para dois casos-exemplo (Tempo<100.000h).

Veja-se que, no caso do 3º Exemplo da Figura 6.12, a adoção de um valor constante para a taxa de falha dos componentes pode resultar em um valor para a probabilidade de falha do sistema que difere percentualmente acima de 80% com relação ao valor da mesma probabilidade de falha do sistema, quando se adota a hipótese de taxas de falha dependentes do tempo para os componentes.

7 - Conclusões e Recomendações

Neste trabalho, tratou-se da questão de se modelar dependências nas falhas de sistemas redundantes. Modelos recentes demonstram que um tipo de falha dependente pode ser explicado em termos da variabilidade das probabilidades de falha dos componentes com relação aos ambientes operacionais. Conforme demonstrado no trabalho, a definição de ambiente é mais ampla, não englobando apenas as condições ambientais da instalação dos componentes, mas também detalhes com relação à sua história, manutenção, etc. Este tipo de dependência pode ser tratada probabilisticamente por meio de uma metodologia formal simples, conforme apresentada por HUGHES (1987) e LITTLEWOOD (1996); porém, tais trabalhos não consideraram determinados fatores, em especial o envelhecimento do componentes do sistema, e do envelhecimento do sistema em si.

Foram apresentados testes estatísticos (Capítulo 4) que analisam a situação de um sistema e de seus componentes e, por intermédio deles, pode ser verificado (vide Capítulo 6) que há situações em que um sistema envelhece, mesmo que algum(ns) de seus componentes não apresentem tal tendência.

Em função disso, buscou-se formular um novo modelo para se quantificar ao mesmo tempo tanto a influência do uso de equipamentos diversos quanto do envelhecimento na confiabilidade dos componentes e do sistema. Também foi destacada a importância de serem considerados ambos os fatores no desenvolvimento do modelo.

Além disso, o novo modelo formulado apresenta facilidades na definição das taxas de falha para os componentes do sistema, o que não está presente nos modelos descritos em HUGHES (1987) e LITTLEWOOD (1996), visto que as definições das probabilidades condicionais de falha em um determinado ambiente são muito dependentes da opinião de especialistas, aumentando a subjetividade e, conseqüentemente o nível de incerteza do resultado final. Deve ser destacado também que os métodos diretos de HUGHES (1987) e LITTLEWOOD (1996) são baseados sempre em distribuições a priori uniformes, ou seja, desconsidera-se toda a história anterior do sistema e/ou de seus componentes, além de dados de falha de sistemas e/ou componentes similares àqueles que estão sendo analisados (é descartada a possibilidade de uso de dados genéricos para definir a distribuição a priori); tal fato, de acordo com MARSEGUERRA (1999), faz aumentar a variância dos intervalos de confiança obtidos.

Claro está que o modelo sugerido apresenta determinadas condições a serem observadas para a sua adoção, porém, em linhas gerais, os analistas não devem encontrar dificuldades em atendê-las, tanto no que se refere ao tamanho amostral mínimo necessário (com o uso de dados de falha específicos, dados genéricos e julgamentos de especialistas) quanto com relação à probabilidade de falha de um componente de um determinado tipo em um certo ambiente.

Do que foi apresentado nos casos exemplos, verifica-se claramente a influência que o tempo exerce sobre componentes em período de envelhecimento e, a partir daí, podem ser mensuradas as conseqüências de se desprezar esta variável, pela adoção de um modelo de taxa de falhas constante. Conforme destacado no 3º caso exemplo do Capítulo 6, a adoção de taxas de falha constantes para componentes e sistemas envelhecidos conduz a um subdimensionamento na probabilidade de falha do sistema que pode ultrapassar os 80%, fazendo com que as estimativas pontuais obtidas sejam completamente destoantes da realidade do sistema que está sendo estudado.

O uso do modelo sugerido neste trabalho é especialmente útil no ajuste de políticas e procedimentos de teste e manutenção, que podem estar em não conformidade com a realidade apresentada pelo comportamento do sistema.

Como recomendações para a continuação deste trabalho de pesquisa podem ser destacados os seguintes pontos:

- Modelos, como o apresentado em ATWOOD (1992), se baseiam na suposição de uma forma funcional fixa para a taxa de falha. Os modelos com taxa de falhas estocástica não são comuns. Tais modelos se baseiam na suposição de que a taxa e/ou a probabilidade de falha apresentam formas variáveis, ou seja, estas podem mudar estocasticamente com o tempo. PULKKINEN & SIMOLA (2000) citam dois modelos que fazem uso desta suposição: o modelo logit-binomial, aplicados a componentes em reserva testados periodicamente, e o modelo lognormal-Poisson, aplicado a componentes que operam continuamente. Aconselha-se fazer um estudo no qual a forma funcional da taxa de falha seja mutável, especialmente em dois casos: mudança de forma com o aumento do tempo operacional e com mudança do ambiente dos componentes do sistema.
- Além disso, deve-se fazer um estudo que leve em consideração as influências de erros humanos, em todas as fases, ou seja, no projeto, instalação, comissionamento, operação, manutenção, coleta de dados, etc.

- Devem ser testadas novas combinações de componentes, como, por exemplo, dois componentes, um com taxa de falha crescente e outro com taxa de falha decrescente, ou então dados que apresentem um outro tipo de tendência, que não somente monotônica, para verificar o comportamento do sistema como um todo.
- Deve-se fazer um estudo comparativo mais extensivo entre os modelos paramétricos e não paramétricos utilizados para a obtenção de taxas de falha. Na comparação entre resultados paramétricos e não paramétricos obtidos, KIRCHSTEIGER (1994) mostrou que os intervalos de confiança para os modelos paramétricos apresentam menor variância do que aqueles fornecidos pelos modelos não paramétricos. Deve-se analisar se o aumento na subjetividade provocado pelo uso de julgamentos de especialistas influencia decisivamente no aumento da variância de modelos paramétricos.

REFERÊNCIAS BIBLIOGRÁFICAS

AMENDOLA, A., 1986, "Uncertainties in Systems Reliability Modeling: Insight Gained Through European Benchmark Exercises", *Nuclear Engineering and Design*, n. 93, pp. 215-225.

APELAND, S., AVEN, T. e NILSEN, T., 2002, "Quantifying Uncertainty under a Predictive, Epistemic Approach to Risk Analysis", *Reliability Engineering and System Safety*, n. 75, pp. 93-102.

ASCHER, H. e FEINGOLD, H., 1984, *Repairable System Reliability: Modeling, Inference, Misconceptions and their Cause*, 1 ed., New York, Marcel Dekker, Inc.

ATWOOD, C. L., 1992, "Parametric Estimation of Time-Dependent Failure Rates for Probabilistic Risk Assessment", *Reliability Engineering and System Safety*, n.37, pp. 181-194.

BUKOWSKI, J. V. e GOBLE, W.M., 2001, "Verifying Common Cause Reduction Rules for Fault Tolerant Systems via Simulation Using a Stress-Strength Failure Model", *ISA Transactions*, n. 40, pp. 183-190.

CASTILLO, E., SARABIA, J. M., SOLARES, C. *et al.*, 1999, "Uncertainty Analyses in Fault Trees and Bayesian Networks using FORM/SORM Methods", *Reliability Engineering and System Safety*, n.65, pp. 29-40.

CHATFIELD, C., 1995, "Model Uncertainty, Data Mining and Statistical Inference", *Journal of Royal Statistical Society*, n. 158, v. 3, pp. 419-466.

CHHIBBER, S., APOSTOLAKIS, G. e OKRENT, D., 1992, "A Taxonomy of Issues Related to the Use of Experts Judgments in Probabilistic Safety Studies", *Reliability Engineering and System Safety*, n. 38, pp. 27-45.

CIAMPOLI, M., 1998, “Time Dependent Reliability of Structures Systems subject to Deterioration”, *Computers and Structures*, n. 67, pp. 29-35.

CIAMPOLI, M., 1999, “A Probabilistic Methodology to Assess the Reliability of Deteriorating Structural Elements”, *Computers Methods in Applied Mechanics and Engineering*, n. 168, pp. 207-220.

COX, D. R. e LEWIS, P. A. W., 1966, *The Statistical Analysis of Series of Events*, 1 ed., New York, John Wiley and Sons.

DeGROOT, M. H., 1986, *Probability and Statistics*, 2 ed., Reading, MA, Addison-Wesley Publishing Company.

DEWOOGHT, J., 1998, “Model Uncertainty and Model Accuracy”, *Reliability Engineering and System Safety*, n. 59, pp. 171-185.

DHILLON, B. S. e YANG, N., 1997, “Stochastic Analysis of an Active-Stand By Redundant Network with Two Types of Common-Cause Failures”, *Stochastic Analysis and Applications*, n. 15 (3), pp. 313-325.

DUTHIE, J. C. *et al*, 1998, “Risk-based Approaches to Ageing and Maintenance Management”, *Nuclear Engineering and Design*, n. 184, pp. 27-38.

ELLINGWOOD, B. R., 1998, “Issues Related to Structural Aging in Probabilistic Risk Assessment of Nuclear Power Plants”, *Reliability Engineering and system Safety*, n.62, pp. 171-183.

FISCHER, H. D. e PIEL, L., 1999, “Diversity in computerized reactor protection systems”, *Reliability Engineering and System Safety*, n. 63, Issue 1, pp. 91-97.

FLEMING, K. N., 1975, “A Reliability Model for Common Mode Failure in Redundant Safety Systems”, In: *Proceedings of the Sixth Annual Pittsburgh Conference on Modeling and Simulation*, General Atomic Report GA-A13284, April 23-25.

FLEMING, K. R., MOSLEH, A. e DEREMER, R. K., 1986, “A Systematic Procedure for the Incorporation of Common Cause Events into Risk and Reliability Models”, *Nuclear Engineering and Design*, n. 93, pp. 245-273.

HILSMEIER, T. A., ALDEMIR, T. e VESELY, W. E., 1995, “Time-Dependent Unavailability of Aging Standby Components Based on Nuclear Plant Data”, *Reliability Engineering and system Safety*, n. 47, pp. 199-205.

HOFER, E., KLOSS, M., KRZYKACZ-HAUSMANN, B., PESCHKE, J. e WOLTERECK, M., 2002, “An Approximate Epistemic Uncertainty Analysis in the Presence of Epistemic and Aleatory Uncertainties”, *Reliability Engineering and System Safety*, n. 77, pp. 229-238.

HORA, S. C., 1996, “Aleatory and Epistemic Uncertainty in Probabilistic Elicitation with an Example from Hazardous Waste Management”, *Reliability Engineering and System Safety*, n. 54, pp. 217-223.

HUGHES, R. P., 1987, “A New Approach to Common Cause Failures”, *Reliability Engineering and System Safety*, n. 17, pp. 211-236.

JAIN, M., 1998, “Reliability Analysis of a Two Unit System with Common Cause Shock Failures”, *Indian Journal of Pure and Applied Mathematics*, n. 29 (12), pp. 1281-1289.

JIANG, R., JI, P. e XIAO, X., 2003, “Aging Properties of Unimodal Failure Rate Models”, *Reliability Engineering and System Safety*, n. 79, pp. 113-116.

JOHNSON, N. L. e KOTZ, S., 1969, *Distributions in Statistics – Discrete Distributions*, 1 ed., New York, John Wiley & Sons.

KAFKA, P. e POLKE, H., 1986, “Treatment of Uncertainties in Reliability Models”, *Nuclear Engineering and Design*, n. 93, pp. 203-214.

KIRCHSTEIGER, C., 1994, "Nonparametric Estimation of Time-dependent Failure Rates for Probabilistic Risk Assessment", *Reliability Engineering and System Safety*, n. 44, pp. 1-9.

KULKARNI, R. N., 1994, "Modeling Common Cause Failures under Data Uncertainty of System Unavailability", *Microelectronics Reliability*, vol. 34, n. 10, pp. 1615-1622.

KURIEN, K. C., SEKHON, G. S. e CHAWLA, O. P., 1993, "Reliability and Ageing of Repairable Systems", *Microelectronics Reliability*, vol. 33, n. 3, pp. 1095-1100.

KVAM, P. H., 1996, "Estimation Techniques for Common Cause Failure Data with Different System Sizes", *Technometrics*, vol. 38, n. 4, pp. 382-388.

KVAM, P. H. e MILLER, J. G., 2002, "Common Cause Failure Prediction Using Data Mapping", *Reliability Engineering and System Safety*, n.76, pp. 273-278.

LAPA, C. M. F., 1996, *Análise da Confiabilidade do Sistema de Alimentação de Angra I considerando FCC pelo Modelo das Letras Gregas Múltiplas*, Tese M.Sc., COPPE/UFRJ, Rio de Janeiro, RJ, Brasil.

LEWIS, E. E., 1994, *Introduction to Reliability Engineering*, 2 ed., New York, John Wiley & Sons.

LITTLEWOOD, B., 1996, "The Impact of Diversity upon Common Mode Failures", *Reliability Engineering and System Safety*, n. 51, pp. 101-113.

LOFGREN, E. V. e GREGORY, S. H., 1990, *Issues and Approaches for Using Equipment Reliability Alerts Levels*, NUREG/CR-5611, BNL-NUREG-52251, RX, June.

MANN, N. R., SCHAFER, R. E. e SINGPURWALLA, N. D., 1974, *Methods for Statistical Analysis of Reliability and Life Data*, 1 ed., New York, John Wiley & Sons.

MARSEGUERRA, M., PADOVANI, E. e ZIO, E., 1999, "The Impact of Operating Environment on the Design of Redundant Configurations", *Reliability Engineering and System Safety*, n. 63, pp. 155-160.

MARTORELL, S., SANCHEZ, A. e SERRADELL, V., 1999, "Age-dependent Reliability Model Considering Effects of Maintenance and Working Conditions", *Reliability Engineering and System Safety*, n. 64, pp. 19-31.

MARTZ, H.F. e HAMADA, M.S., 2003, "Uncertainty in Counts and Operating Time in Estimating Poisson Occurrence Rates", *Reliability Engineering and System Safety*, n. 80, pp. 75-79.

MATSUOKA, T. e KOBAYASHI, M., 1997, "The GO-FLOW Reliability Analysis Methodology – Analysis of Common Cause Failures with Uncertainty", *Nuclear Engineering and Design*, n. 175, pp. 205-214.

MOSLEH, A., FLEMING, K. N., PARRY, G. W. *et al.*, 1988/1989, *Procedures for Treating Common Cause Failures in Safety and Reliability Studies*, NUREG/CR-4780. Nuclear Regulatory Commission, EPRI NP-5613 (Vol 1, January 1988, Vol. 2., January 1989).

MOSLEH, A., 1991, "Common Cause Failures: An Analysis Methodology and Examples", *Reliability Engineering and System Safety*, n.34, pp. 249-292.

MOSLEH, A., 1992, "Bayesian Modeling of Expert-to-Expert Variability and Dependence in Estimating Rare Events Frequencies", *Reliability Engineering and System Safety*, n.38, pp. 45-57.

NILSEN, T. e AVEN, T., 2003, "Models and Model Uncertainty in the Context of Risk Analysis", *Reliability Engineering and System Safety*, n. 79, pp. 309-317.

PARRY G. W., 1991, "Common Cause Failures Analysis: A Critique and Some Suggestions", *Reliability Engineering and System Safety*, n. 34, pp. 309-326.

PAULA, H. M., CAMPBELL, D. J. e RASMUSON, D. M., 1991, "Qualitative Cause-Defense Matrices: Engineering Tools to Support the Analysis and Prevention of Common Cause Failures", *Reliability Engineering and System Safety*, n. 34, pp. 389-415.

PULKKINEN, U. e SIMOLA, K., 2000, "Bayesian Models and Ageing Indicators for Analyzing Random Changes in Failure Occurrence", *Reliability Engineering and System Safety*, n. 68, pp. 255-268.

RAMAKUMAR, R., 1993, *Engineering Reliability: Fundamentals and Applications*, 1 ed., New Jersey, Prentice-Hall International, Inc.

RASMUSON, D. M., 1991, "Practical Considerations in Treating Dependencies in PRAs", *Reliability Engineering and System Safety*, n. 34, pp. 327-343.

SANT'ANA, M. C., 1996, "Análise Estatística de Alguns Modelos Paramétricos para a Incorporação de Falhas de Causa Comum na Avaliação da Confiabilidade de Sistemas", Projeto Final de Curso de Graduação, DME/IM/UFRJ, Rio de Janeiro, RJ, Brasil.

SANT'ANA, M. C., 1999, "Avaliação de Incertezas em Modelos Paramétricos de Falha de Causa Comum", Tese M.Sc., COPPE/UFRJ, Rio de Janeiro, RJ, Brasil.

SANT'ANA, M. C. e FRUTUOSO e MELO, P. F. F., 2005, "Avaliação da Indisponibilidade de Sistemas associada a Falhas de Causa Comum considerando Diversidade e Envelhecimento", *2005 International Nuclear Atomic Conference – INAC 2005*, Santos, São Paulo, Brasil, 28 de Agosto a 2 de Setembro.

VAURIO, J. K., 1994, "The Theory and Quantification of Common Cause Shock Events for Redundant Standby Systems", *Reliability Engineering and System Safety*, n. 43, pp. 289-305.

VAURIO, J. K., 1999, "Identification of Process and Distribution Characteristics by Testing Monotonic and Non-Monotonic Trends in Failure Intensities and Hazard Rates", *Reliability Engineering and System Safety*, n. 64, pp. 345-357.

VAURIO, J. K., 2002, “Extensions of the Uncertainty Quantification of Common Cause Failure Rates”, *Reliability Engineering and System Safety*, n. 78, pp. 63-69.

WATSON, I.A. e EDWARDS, G.T., 1979, “Common-Mode Failures in Redundancy Systems”, *Nuclear Technology*, vol. 46, pp. 183-191.

WINKLER, R. L., 1996, “Uncertainty in Probabilistic Safety Assessment”, *Reliability Engineering and System Safety*, n. 54, pp. 127-132.

ZHIBIN, T. e WEI, X., 2003, “Bayesian Analysis with Concentration of Data Uncertainty in a Specific Scenario”, *Reliability Engineering and System Safety*, n. 79, pp. 17-31.

ZIO, E. e APOSTOLAKIS, G. E., 1996, “Two Methods for the Structured Assessment of Model Uncertainty by Experts in Performance Assessments of Radioactive Waste Repositories”, *Reliability Engineering and System Safety*, n.54, pp. 225-241.

Apêndice A: Glossário

- **Causa Raiz** - Razão original ou primitiva que proporcionou, ou contribuiu definitivamente, para a ocorrência de determinado evento em um certo (na maioria das vezes, desconhecido) instante de tempo; tal razão, se corrigida, evitaria a recorrência de tal falha. Há quatro tipos de causas raízes a serem consideradas:
    - ♦ Equipamento / Material : Falhas aleatórias em equipamentos isolados devido a causas inerentes ao componente afetado.
    - ♦ Humano : Erros ocorridos durante a operação da instalação (isto é, interação dinâmica com a instalação), durante teste e manutenção do equipamento, e durante projeto e fabricação do componente e construção da instalação.
    - ♦ Ambiental : Eventos externos ao equipamento em questão, porém internos em relação à instalação onde os mesmos ocorreram e que resultam em condições ambientais perturbadoras aplicadas ao equipamento.
    - ♦ Externo : Eventos externos à instalação e que também resultam em condições ambientais perturbadoras aplicadas ao equipamento.

- **Choque** - É um evento que ocorre em um determinado instante de tempo e que atua sobre alguns ou todos os componentes do sistema. Pode ser letal (todos os componentes no sistema falham) ou não letal (choque em que cada componente no sistema tem uma chance, independente, de falhar, dada a ocorrência do choque).

- **Componente** - É todo e qualquer elemento de uma instalação, projetado para desempenhar uma determinada função. Seu limite depende do nível de detalhamento da análise a ser feita. Neste trabalho, um componente será o nível mais baixo de detalhamento escolhido pelo analista para se modelar o impacto de um evento no sistema (isto é, não serão analisadas separadamente partes de componentes).

- **Corte Mínimo** - Combinação mínima de eventos (falhas de componentes do sistema) que, caso ocorram simultaneamente, levam à falha do sistema. Os cortes mínimos são classificados da seguinte maneira: um corte mínimo com uma falha primária é dito de 1ª. ordem, com duas, é dito de 2ª ordem e assim por diante. Cortes mínimos controversos referem-se a duas ou mais falhas de causa comum que

atingem um mesmo componente de um dado grupo de componentes redundantes (por exemplo, uma falha tripla que atinge os componentes 1, 2 e 3 seguida de uma falha dupla que atinge os componentes 1 e 4).

- **Defesa –** as características de projeto que protegem os equipamentos das causas de falhas (ou indisponibilidades) e/ou seu acoplamento.

- **Demanda** – Um sistema é demandado quando é posto em operação, de modo que possa executar a função para o qual foi projetado.

- **Diversidade** - Técnica que consiste no uso de equipamentos ou componentes de outros fabricantes ou de tipos diferentes do pré-existente (por exemplo, uso de dois tipos de motores, um movido a eletricidade e outro a óleo diesel) que faz com que os mesmos não estejam sujeitos a problemas que impactam componentes similares (por exemplo, erro de projeto ou de fabricação de um componente).

- **Estado de um Componente** - O estado de um componente define o seu *status* em relação ao desempenho da função para o qual foi projetado. Serão considerados três tipos de estado:
    1. Disponível : Um componente é dito disponível se é capaz de realizar sua função, de acordo com o critério de sucesso previamente estabelecido.
    2. Indisponível : O componente é incapaz de realizar suas funções, de acordo com o critério de sucesso definido. Deve ser citado que um componente pode ser diferentemente classificado em instalações diversas, dependendo do critério de sucesso a ser estabelecido. Os estados indisponíveis podem ser divididos em duas categorias, a saber:

        $\Rightarrow$ Falho : O componente é incapaz de realizar suas funções e para que o mesmo volte a funcionar, algum tipo de reparo ou substituição faz-se necessário. Também pode ser considerado como falha um componente realizar sua função quando não demandado e vice-versa, não realizando sua função quando requerido.

⇒ Funcionalmente Indisponível : O componente é capaz de operar, porém a função desempenhada pelo mesmo está indisponível devido a algum outro fator, como falta de energia elétrica, estar em teste ou manutenção, etc.

3. Potencialmente Indisponível : O componente é capaz de realizar suas funções, porém existe uma condição degradada ou incipiente incidindo sobre ele.

⇒ Degradada : Um componente está em estado degradado quando exibe redução em sua performance, porém esta degradação não é suficiente para que se declare o mesmo indisponível.

⇒ Incipiente : Um componente está em estado incipiente quando apresenta um pequeno problema que, caso não sanado, conduzirá o mesmo a um estado degradado ou indisponível.

- **Evento** - Qualquer ocorrência que promova alteração no estado normal de funcionamento ou de disponibilidade de um componente (ou grupo de componentes) do sistema (falha, manutenção, degradação, etc.)

- **Evento Básico de Causa Comum** - É um evento que envolve a falha de causa comum de um subconjunto específico de componentes de um grupo de componentes de causa comum.

- **Falha** - Evento que atinge um determinado componente, em função de um procedimento ou ocorrência não programados, fazendo com que este seja incapaz de realizar, plenamente, a função para a qual foi projetado, de acordo com o critério de sucesso estabelecido.

- **Falhas de Causa Comum -** São falhas que impactam mais de um componente de um mesmo grupo de componentes redundantes em decorrência de uma mesma causa raiz.

- **Indisponibilidade** - Probabilidade de que o sistema, ou alguns de seus componentes, torne-se indisponível em um determinado instante de tempo.

- **Mecanismos de Acoplamento (*Coupling Mechanisms*)** - Um mecanismo de acoplamento é a maneira de se explicar como a causa de um evento se propaga até o ponto de envolver múltiplos equipamentos. Tais mecanismos podem ser categorizados como se segue:
    - ♦ Funcionais :
        - ⇒ Equipamentos Conectados : Englobam projetos de instalações as quais envolvem equipamentos compartilhados, linhas de entrada comuns, etc. além de situações onde um mesmo componente executa múltiplas funções.
        - ⇒ Equipamentos Não Conectados : Inclui critérios de sucesso interrelacionados tais como o relacionamento entre um sistema de reserva e o sistema que este está apoiando. Formas mais sutis de acoplamento de componentes não conectados são "condutores ambientes" como, por exemplo, sistemas de aquecimento, ventilação e ar-condicionado.
    - ♦ Espaciais :
        - ⇒ Proximidade Espacial : Refere-se a equipamentos que podem ser encontrados dentro de uma mesma sala, barreiras anti-incêndio e anti-inundação comuns, etc.
        - ⇒ Equipamentos Ligados : Equipamentos em locais diferentes que, embora não relacionados funcionalmente, são afetados de modo semelhante por uma condição ambiental externa, possivelmente devido ao rompimento de alguma barreira.
    - ♦ Acoplamentos Humanos : Refere-se a atividades tais como projeto, fabricação, construção, instalação, controle de qualidade, controle de instalações, testes, manutenções, etc.

- **Modos de Falha** - Maneiras pelas quais um componente pode falhar. Serão considerados dois tipos de modo de falha: a falha na partida, quando um componente ou não consegue iniciar seu funcionamento, ou dá a partida e logo após um período de tempo falha; ou falha em operação, ou seja, um componente deixa de obedecer aos critérios de sucesso estabelecidos após entrar em funcionamento.

Processo de Renovação (PR) – Processo onde a probabilidade de falha depende apenas do tempo desde o último reparo. Os tempos entre falhas (X_i) são mutuamente independentes e identicamente distribuídos (porém, com distribuição arbitrária). Sabe-se que a intensidade de falhas (*IF*), $w(t)$, de um *PR* é um valor constante igual ao inverso do valor médio de X_i, com tempo crescente. *IF* é a probabilidade incondicional de falha, por unidade de tempo, igual ao numero esperado de falhas, por unidade de tempo, no tempo *t*.

- **Processo de Poisson (PP) –** Processo onde cada reparo é mínimo (o componente retorna à condição imediatamente anterior à falha), fazendo da unidade "tão boa quanto velha, porém não falha".

Então, a probabilidade de falha durante $(t, t+dt]$, dado que a unidade está boa em *t*, é independente de eventos ocorridos antes de *t*. É o mesmo caso como se a unidade nunca tivesse falhado, ou seja, $\lambda(t) = -\dfrac{dR(t)}{R(t)}$, onde $\lambda(t)$ é a taxa de falhas e $R(t)$ é a probabilidade de não ter ocorrido falha até *t* (ou seja, a confiabilidade),

$$R(t) = e^{-\Lambda(t)}, \qquad \Lambda(t) = \int_0^t \lambda(t')dt'$$

e $\Lambda(t)$ é a densidade acumulada de falhas. Desprezando-se os tempos de reparo, a *IF* é $w(t) = \lambda(t)$ e $W(t) = \Lambda(t)$ é o número esperado de falhas entre $(0, t]$.

Quando $\lambda(t)$ depende, na realidade, do tempo *t*, o processo é chamado de Processo de Poisson não Homogêneo (*PPNH*), deteriorando-se quando $\lambda(t)$ é crescente e melhorando quando $\lambda(t)$ é decrescente com o passar do tempo. Se $\lambda(t)$ assume o valor de uma constante λ, o processo é chamado Processo de Poisson Homogêneo (*PPH*), no qual os X_i's são exponencialmente distribuídos. Algumas propriedades dos *PR* e dos *PP* podem ser vistas na Figura A.1 e na Tabela A.1:

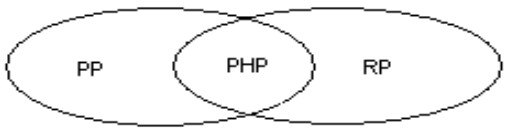

Figura A.1: Interações entre o Processo de Poisson e o Processo de Renovação dão origem ao Processo de Poisson Homogêneo

Tabela A.1: Propriedades dos Processos de Poisson, de Poisson Homogêneo e de Renovação.

Processo de Poisson (*PP*)	**Processo de Poisson Homogêneo (*PPH*)**	**Processo de Renovação (*PR*)**
intensidade de falhas $w(t) \equiv$ taxa de falhas $\lambda(t)$	$w(t) = \lambda(t) = cte$	$T_i - T_{i-1}$ independente e identicamente distribuído
$w(t)$ pode apresentar tendência	$T_i - T_{i-1}$ independente e exponencialmente distribuído	$\lambda(t)$ pode apresentar tendência
$\Lambda(T_i) - \Lambda(T_{i-1})$ independente e identicamente distribuído		$w(t) \approx cte$, para *t* grande

- **Processo de Poisson Homogêneo (*PPH*) -** Processo onde cada reparo é completo, fazendo da unidade "tão boa quanto nova". A maneira mais direta de se definir um *PPH* é como uma seqüência de X_i's variáveis aleatórias independentes e exponencialmente distribuídas. De maneira mais formal, diz-se que um processo de contagem $\{N(t), t \geq 0\}$ é um *PPH* se:

(a) $N(0) = 0$;

(b) $\{N(t), t \geq 0\}$ possui incrementos independentes;

(c) O número de eventos (que neste contexto, são falhas) em qualquer intervalo de comprimento $t_2 - t_1$ segue uma distribuição de Poisson com média $\rho(t_2 - t_1)$:

$$P[N(t_2) - N(t_1) = j] = \frac{e^{-\rho(t_2 - t_1)} \{\rho(t_2 - t_1)\}^j}{j!}$$

Para $j \geq 0$. De (c), segue que:

$$E[N(t_2 - t_1)] = \rho(t_2 - t_1)$$

onde a constante ρ é a taxa de ocorrência de falhas (ROCOF). Desta definição, tem-se que a função confiabilidade é:

$$R(t_1, t_2) = e^{-\rho(t_2 - t_1)}$$

- **Processo de Poisson não Homogêneo (*PPNH*) :** o *PPNH* difere do *PPH* somente pelo fato de que a taxa de ocorrência de falhas varia com o tempo ao invés de ser

considerada constante. Ou seja, as condições (a) e (b) são mantidas, enquanto a condição (c) é modificada para:

$$\text{(c')}\ P\left[N(t_2)-N(t_1)=j\right]=\frac{e^{-\int_{t_1}^{t_2}\rho(t)dt}\left\{\int_{t_1}^{t_2}\rho(t)dt\right\}^{j}}{j!}$$

Para $j \geq 0$. De (c'), segue que:

$$E\left[N(t_2-t_1)\right]=\int_{t_1}^{t_2}\rho(t)dt$$

Da condição (c'), decorre que a função confiabilidade de um *PPNH* é:

$$R(t_1,t_2)=e^{-\int_{t_1}^{t_2}\rho(t)dt}$$

Esta pequena mudança na definição leva a uma grande diferença entre os modelos *PPH* e *PPNH*. Em um *PPNH*, os X_i's não são nem independentes nem identicamente distribuídos (independente de sua distribuição).

- **Quantil** – Dada uma variável aleatória *X*, define-se quantil de ordem q $(0 \leq q \leq 1)$ desta variável aleatória como o menor valor x_q tal que $F_X(x_q) \geq q$.

- **Risco -** Probabilidade de que uma situação física com potencial de causar danos (PERIGO) possa acontecer, em qualquer nível, em decorrência da exposição durante um determinado espaço de tempo a essa situação.

- **Simetria** - Suposição feita quando se trabalha com modelos paramétricos de causa comum nos quais a freqüência de eventos básicos depende unicamente do número de componentes envolvidos e não de quais componentes estão envolvidos (isto é, as probabilidades de eventos similares envolvendo tipos de componentes similares são as mesmas).

- **Taxa de Risco –** A taxa de risco é a taxa de falhas instantânea em um certo tempo *t*, para um determinado componente, dado que este componente está funcionando em *t*. Define-se a taxa de risco por meio da seguinte equação:

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

onde $f(t)$: função densidade de probabilidade do componente em *t*;

$R(t)$: confiabilidade do componente em *t*.

- **Vetor de Impacto** - Técnica que consiste no uso de um vetor para se medir o nível de impacto de um evento sobre um grupo de componentes redundantes. Neste vetor, por exemplo, $V = (v_1, \ldots, v_k)$, cada elemento v_i, $i = 1, \ldots, k$, representa a probabilidade de o evento ter afetado *i*-1 componentes do sistema. Em um vetor de impacto binário um dos elementos do vetor, por exemplo, v_i, vale 1 e os restantes 0, caso o evento envolva a falha de *i* componentes.

Apêndice B: Dados de Falha dos Componentes

B.1 – Gerador Diesel em uma Usina Nuclear

Dados de Falha do Gerador Diesel em uma Usina Nuclear

Tempos de falha do Gerador (em horas de operação)	
GD-1	**GD-2**
161	384
283	501
298	604
511	640
563	755
644	767
1169	1029
1265	1506
1299	1623
1317	1646
1593	2071
2053	2266
2104	2624
2247	2932
2445	2964
2514	
2522	
2668	
2722	
3006	
3085	

B.2 – Sistema de Motores Diesel

Dados de Falha do Sistema de Motores Diesel

Tempos de falha do Grupo de Válvulas (em horas de operação)	
DG3	**DG4**
1382	860
2990	1203
4124	1258
6827	1317
7472	1442
7567	1897
8845	2011
9450	2122
9453	2439
9794	3197
10848	3203
11528	3298
11933	3902
11993	3910
12300	4000
15058	4247
15413	4411
16497	4456
17315	4517
17352	4899
17632	4910
18122	5414
19067	5676
19172	5755
19299	6137
19360	6221
19686	6311
19940	6613
19944	6975
20121	7335
20132	7723
20431	8158
20525	8498
21057	8690
21061	9042
21309	9330
21310	9394
21378	9426
21391	9872
21456	
21461	
21603	

21658	
21688	
21750	
21815	
21820	
21822	
21888	
21930	
21943	
21946	
22181	
22311	
22634	
22635	
22669	
22691	
22846	
22947	
23149	
23305	
23491	
23526	
23774	
23791	
23822	
24006	
24006	
24286	
25000	
25000	
25010	
25048	
25268	
25400	
25500	
25518	

B.3 – Gerador Diesel em uma Usina Nuclear

Dados de Falha do Gerador Diesel em uma Usina Nuclear

Tempos de falha do Gerador (em horas de operação)	
GD-A	**GD-C**
25584	10632
26352	20640
27696	23232
32784	23592
34248	55032
34368	61344
34560	65112
39168	65472
41184	70080
41472	72816
41472	76272
41760	78336
44016	79176
44040	80592
44280	81336
44328	82800
44328	83688
45960	
46632	
47016	
53016	
54480	
55680	
59088	
59208	
61992	
63048	
63168	
70416	
74784	
74976	
76464	
77568	
78264	
78432	