3cgen

3º Congresso Geral de Energia Nuclear

22 a 27 de abril de 1990

ANAIS - PROCEEDINGS

ANÁLISE PROBABILÍSTICA DE SEGURANÇA UTILIZANDO MICROCOMPUTADOR COMO FERRAMENTA

Fernando Luiz Futuro Filho
Jorge E. de Souza Mendes
Mário J. Pio dos Santos

NUCLEBRÁS ENGENHARIA S.A. - NUCLEN

SUMÁRIO

Este trabalho apresenta as principais etapas de execução de uma Análise Probabilística de Segurança (APS), ou seja, estudo da descrição dos sistemas, construção das árvores de eventos, estabelecimento das árvores de falhas e cálculo da indisponibilidade dos sistemas.

O artigo mostra também, a utilização de microcomputador para realização de algumas etapas, enfatizando as principais características que um "software" deve apresentar para realizar adequadamente esta função.

Um caso exemplo de construção de árvore de falha é apresentado, utilizando o pacote PSAPACK que foi distribuído pela Agência Internacional de Energia Atômica para treinamento.

ABSTRACT

The main steps of execution of a Probabilistic Safety Assessment (PSA) are presented in this report,as the study of the system description, construction of event trees and fault trees, and the calculation of overall unavailability of the systems.

It is also presented the use of microcomputer in performing some tasks,highlightning the main characteristics of a software to perform adequately the job.

A sample case of fault tree construction and calculation is presented, using the PSAPACK software, distributed by the IAEA (International Atomic Energy Agency) for training purpose.

1. INTRODUÇÃO

Desde a publicação do estudo WASH-1400 na metade da década passada (1975), a Análise Probabilística de Segurança (APS), foi introduzida como uma importante ferramenta de análise de segurança das usinas nucleares. Nos últimos anos, a maioria dos países que possuem programas nucleares vem tornando a APS uma exigência oficial de licenciamento.

A Análise Probabilística é um método que fornece informações (por exemplo, a análise detalhada da possibilidade de falhas) que não podem ser obtidas por outros meios, conseguindo-se desta forma uma melhora de segurança (sem que haja um superdimensionamento de projeto) e um aumento da disponbilidade de operação,inclusive dos sistemas não relacionados com a segurança.

Convencionou-se dividir as etapas de uma APS, de acordo com o objetivo final, em três níveis:

nível 1 - determinação de frequência de fusão do núcleo
nível 2 - determinação do termo fonte e frequência de liberação de radioatividade
nível 3 - determinação do risco.

Este trabalho apresenta no item 2 as principais etapas de execução da APS (nível 1): estudo da descrição dos sistemas, onde é feita uma análise funcional do problema identificando-se e agrupando-se os eventos iniciadores (acidentes), elaboração das árvores de eventos para cada categoria de iniciadores, determinando as sequências de eventos que serão analisados; construção das árvores de falhas dos sistemas envolvidos nas sequências de eventos de interesse; e cálculo da indisponibilidade dos sistemas para os quais foram construídas árvores de falhas.

No item 3, o artigo mostra a utilização do microcomputador para realização das etapas citadas no capítulo anterior,enfatizando os seguintes tópicos: principais características desejáveis em um "software", apresentação do pacote "PSAPACK", construção da árvore de falhas para um caso exemplo, resultados obtidos com o uso do "PSAPACK" e análise de resultados.

Para finalizar, no item 4 são feitas as conclusões do que foi desenvolvido no trabalho.

2. PRINCIPAIS ETAPAS DE EXECUÇÃO DE UMA APS

Antes da etapa de modelagem e cálculo que consome maior quantidade de homens-hora, algumas etapas devem ser executadas, pois delas depende toda a orientação e execução com sucesso de uma APS.

A definição clara dos objetivos da APS é o primeiro passo a ser dado, por que somente assim pode-se determinar exatamente como o trabalho vai se desenvolver; por exemplo, analisar uma planta para efeitos de licenciamento é muito diferente de avaliar as condições de segurança visando um melhor planejamento de manutenção e testes. Uma vez definido os objetivos da APS, pode-se então estabelecer o escopo de trabalho, os procedimentos de coordenação e pessoas (e companhias) envolvidas. É possível também, nessa sequência, a escolha da metodologia e ferramentas para execução do trabalho.

Com essas definições estabelecidas, parte-se para a formação da equipe de execução. Essa equipe tem formação variada dentro das áreas de Engenharia, Física e Matemática e Estatística e deve ter conhecimento da metodologia escolhida. Um treinamento preliminar com as ferramentas disponíveis é bastante desejável.

Além da equipe de execução, é imprescindível a participação dos engenheiros responsáveis pelo processo, pois eles possuem os conhecimentos detalhados sobre o funcionamento dos mesmos.

Para melhor desempenho do trabalho, deve ser estabelecido um cronograma que permita o acompanhamento das etapas e ainda defina os procedimentos de garantia da qualidade. Neste aspecto é importante notar que as etapas, cálculos e avaliações devem ser muito bem documentados com perfeita rastreabilidade para permitir uma revisão independente, que assegure a obtenção de resultados corretos e completos.

2.1 ESTUDO DA DESCRIÇÃO DOS SISTEMAS

O objetivo desta etapa é estudar a descrição dos sistemas para que possa ser feita a seguir uma análise funcional de toda a planta. Esta análise funcional é feita em duas fases: a primeira, mais geral, identificando os modos de operação da Usina e quais as fun-

ções que devem ser realizadas para o seu correto e seguro funcionamento, tendo como base o projeto determinístico; baseado nisso faz-se um levantamento e agrupamento dos eventos iniciadores (acidentes). A segunda fase da análise funcional, mais detalhada, é desenvolvida após a elaboração das árvores de eventos se concentrando nos sistemas nelas existentes.

Nesta etapa, é imprescindível que o trabalho seja realizado em conjunto, por no mínimo um especialista em funcionamento da planta e outro em APS.

2.2 ELABORAÇÃO DAS ÁRVORES DE EVENTOS

Como primeiro passo na elaboração das árvores de eventos, avalia-se dentre os eventos iniciadores levantados os que poderiam, sob certas circunstâncias, resultar em fusão do núcleo, classificando-os em categorias por características semelhantes de resposta dos sistemas de segurança da planta e por frequências de ocorrência. A análise em detalhe de todos os possíveis eventos iniciadores não é possível e nem se faz necessário, sendo suficiente a discussão de um número limitado deles que cubram todos os outros possíveis.

A partir de cada categoria de eventos iniciadores, podem resultar diferentes sequências de eventos, dependendo do sucesso ou da falha de sistemas de segurança específicos. Para se ter uma idéia das potenciais sequências de eventos resultantes, elaboram-se as árvores de eventos propriamente ditas.

As frequências de fusão do núcleo são determinadas a partir das frequências dos eventos iniciadores e das probabilidades de falhas dos sistemas necessários para mitigar o acidente.

2.3 CONSTRUÇÃO DAS ÁRVORES DE FALHAS

Um dos métodos usados para determinar a indisponibilidade ou probabilidade de falha dos sistemas necessários para mitigar o acidente é a análise por árvore de falhas, onde para cada sistema incluído nas árvores de eventos é construída uma árvore de falhas.

O primeiro passo para construção da árvore de falhas de um sistema é uma análise funcional detalhada do mesmo, sendo necessário para realizá-la a presença de um especialista no sistema, pois des-

ta forma consegue-se cobrir todas as possibilidades de falhas existentes. A seguir, constrói-se a árvore de falhas propriamente ditas, começando-se pelo evento topo que é formado pela falha da função requerida pela árvore de eventos.

Resultando neste evento indesejável são colocadas todas as combinações de falhas dos componentes considerados, interligadas por meio de operadores lógicos (portas "AND", "OR", "NOT").

2.4 CÁLCULO DA INDISPONIBILIDADE DOS SISTEMAS

O cálculo da indisponibilidade (probabilidade que um sistema falhe quando solicitado em um dado instante) ou da probabilidade de falha (taxa de falha de um sistema em um determinado intervalo de tempo) é determinada por meio do equacionamento lógico das árvores de falha. As causas da falha do sistema são determinadas até um nível hierárquico onde os dados de confiabilidade são suficientes ou precisos o bastante para que o cálculo possa ser realizado. Neste nível hierárquico mais baixo é que encontramos os chamados eventos básicos (dados de falhas resultantes da experiência operacional dos componentes).

O conjunto de dados referentes aos eventos básicos mais outros dados operacionais dos componentes é o que nós chamamos banco de dados. Este banco tem como dados de entrada: nome do componente, tipo de falha do componente, taxa de falha (λ), probabilidade de falha por demanda, intervalo entre testes, tempos de reparo, fatores de erro, etc. De posse destes dados de entrada, e assumindo uma distribuição de probabilidade de falhas (exponencial, por exemplo) pode-se fazer o cálculo de indisponibilidade ou da probabilidade de falha dos sistemas usando-se as equações de probabilidade de falha da distribuição escolhida para cada componente e inserindo estes resultados na equação lógica da árvore de falhas no sistema.

3. UTILIZAÇÃO DO MICRO COMPUTADOR EM ETAPAS DA APS

Programas de computador são ferramentas desenvolvidas para desempenhar tarefas complicadas e volumosas que seriam extremamente lentas se feitas manualmente.

Desde a execução do WASH 1400, vários programas foram desenvolvidos para computadores de grande porte, assim como para micros. Várias são as tarefas de uma APS; em algumas o uso do computador é considerado indispensável (ex.: modelagem da sequência de eventos , quantificação da sequência de acidentes, análise de incertezas,etc), enquanto que para outras, podemos dizer que é desejável (ex.: documentação, análise qualitativa de dependência...), ou ainda apenas possível (ex.: probabilidade de falha humana, análise de causa comum, etc.).

Acompanhando a evolução da informática, também a APS viu nos microcomputadores uma ferramente versátil de grande potencial. Assim, diversos softwares estão sendo (ou foram) adaptados ou desenvolvidos para funcionar em ambientes micro. Outra opção adotada é o uso de instalações que utilizam microcomputadores para determinadas tarefas e os mantêm conectados a computadores maiores que se encarregam dos cálculos mais extensos.

3.1 PRINCIPAIS CARACTERÍSTICAS DESEJÁVEIS EM UM SOFTWARE

No processo de desenvolvimento da APS, como diversas etapas devem ou podem ser executadas por computador, apareceram no mercado softwares integrados que têm rotinas para resolver diferentes tarefas. Esses pacotes de programas têm se desenvolvido basicamente em ambientes de microcomputador, notadamente os "IBM-PC compatível".

A principal característica deste conjunto de rotinas integradas é a compatibilidade de dados entre elas, o que facilita o usuário no decorrer das etapas do trabalho.

De uma maneira geral, deve ser observado que

a) O software tem suporte adequado (manuais e especialistas);
b) O software foi feito para a utilização desejada;
c) O software faz o que se propõe fazer (homologação e histórico);
d) Um software mais acessível ao usuário poupa tempo de treinamento;
e) Um software que tenha módulo gráfico integrado permite maior visualização das árvores elaboradas;
f) A maneira de entrar os dados deve ser adequada e clara. A entrada de dados deve ser possível de ser corrigida sem ter que ser

totalmente redigitada;

g) Os resultados devem ser apresentados de maneira clara e com todas as informações necessárias para análise do problema listadas;

h) A velocidade do código deve ser levada em consideração para trabalhos muito grandes;

i) O software escolhido é adequado ao hardware disponível.

É bom se ter em mente também que os programas de computador, ao contrário dos computadores (hardware), quando falham podem continuar produzindo resultados; porém resultados errados. Assim, cada vez que for instalado um software é interessante que seja produzido um teste, de resultados já conhecidos para se poder avaliar a qualidade da operação e garantir os resultados posteriores de cálculo.

3.2 APRESENTAÇÃO DO PACOTE PSAPACK

O pacote PSAPACK (Probabilistic Safety Analysis Package) consiste de vários programas de computador integrados para a análise de árvores de eventos e de falhas. O pacote foi desenvolvido pela Agência Internacional de Energia Atômica para APS nível 1 utilizando computadores pessoais compatíveis com o padrão IBM-PC.

O pacote é um sistema interativo que opera através de menus, os quais permitem a utilização dos diversos módulos, conforme o objetivo da análise.

O pacote é constituído dos seguintes módulos:

- Árvore de Eventos
- Árvore de Falhas
- Banco de dados de Confiabilidade
- Cortes mínimos
- Utilitários

3.2.1 ÁRVORE DE EVENTOS

O módulo de árvore de eventos avalia as sequências lógicas do acidente indicando as sequências de sucesso e de dano ao núcleo do reator baseado nos dados fornecidos pelo usuário. Este módulo associa os cortes mínimos da árvore de falha dos sistemas e consulta o banco de dados de confiabilidade para avaliar as sequências do aci

dente.

3.2.2 ÁRVORE DE FALHAS

O módulo de árvore de falhas é constituído de duas partes:

- Editor de texto para a elaboração da árvore de falhas (dados de entrada para o código FTAP)
- Código FTAP para a redução da árvore de falhas e para a determinação dos cortes mínimos que são armazenados na biblioteca de cortes mínimos.

3.2.3 BANCOS DE DADOS DE CONFIABILIDADE

O módulo do banco de dados de confiabilidade permite o manuseio de dados sobre os componentes do sistema (bombas, válvulas, instrumentação, etc.). Os dados podem ser v'stos e modificados pelo usuário.

O banco de dados fornecido pela Agência Internacional de Energia Atômica contém aproximadamente 1000 registros de 21 fontes diferentes (IEEE, NUREG, EPRI, etc.). A construção de bancos de dados internos particularizados para cada caso em estudo é possível através deste módulo.

Todos os componentes e modos de falha normalmente considerados em APS estão incluídos neste banco de dados.

3.2.4 CORTES MÍNIMOS

O módulo de cortes mínimos permite a visualização e quantificação dos cortes mínimos, obtendo-se a partir desta quantificação a indisponibilidade do sistema. O módulo inclui também o código SAMPLE, que é usado para a análise de incerteza desta indisponibilidade.

3.2.5 UTILITÁRIOS

O módulo de utilitários inclui todas as ferramentas necessárias para o manuseio dos arquivos do pacote.

3.3 CONSTRUÇÃO DA ÁRVORE DE FALHAS DE UM SISTEMA DE SEGURANÇA

O sistema de segurança escolhido para caso exemplo é o Sistema de Água de Alimentação de Emergência. Este sistema realiza a seguinte função: alimentação de emergência dos geradores de vapor em caso de eventos externos, como terremoto.

O sistema é composto dos seguintes componentes principais: bomba de água de alimentação de emergência (o eixo da bomba está acoplada mecanicamente ao eixo do motor Diesel do gerador elétrico de emergência), tanque de água desmineralizada, válvulas especiais e uma linha secundária de arrefecimento do motor Diesel com uma bomba e trocadores de calor. (fig. 1)

O evento topo escolhido para a nossa árvore de falhas foi a falha de alimentação de emergência dos geradores de vapor, ou mais precisamente a falha de uma das quatro redundâncias existentes no sistema.

Uma análise detalhada foi realizada em conjunto com o especialista responsável pelo sistema em estudo, visando descobrir todas as possibilidades de falha que devem ser consideradas na árvore de falhas. O resultado desta análise é a árvore de falhas do Sistema de água de alimentação de emergência apresentado na Tabela 1.

3.4 RESULTADOS OBTIDOS COM O USO DO PSAPACK PARA O CÁLCULO DA ÁRVORE DE FALHAS DE UM SISTEMA DE SEGURANÇA

Antes de apresentar os resultados propriamente ditos, é importante mencionar as premissas utilizadas quando da elaboração do banco de dados e no cálculo da indisponibilidade do sistema: a obtenção das probabilidades de falhas de componentes foi conseguida no banco de dados de confiabilidade genérico da IAEA ou de dados operacionais de usinas alemãs aceitos pelo órgão licanciador alemão. Para a maioria dos casos foi encontrado no conjunto de dados, componentes cujas características se aproximavam daquelas apresentadas pelos componentes do caso exemplo. Onde isto não foi possível utilizou-se dados aproximados conservativos (taxas de falha mais altas).

As falhas de componentes no banco de dados foram classificados em 4 tipos:

- Falhas de componentes "STAND BY" testados
- Falhas de componentes não reparáveis durante a operação
- Falhas por demanda
- Falhas de componentes "STAND BY" testados e não reparáveis durante a operação

Na obtenção das probabilidades de falha de componentes e classificação das falhas dos componentes foram considerados as características e o funcionamento do sistema para uma missão de 10 horas.

Para o nosso caso exemplo, o resultado do cálculo da probabilidade de falha de uma redundância do Sistema de Água de Alimentação de Emergência na realização da função de alimentação de emergência dos geradores de vapor foi 2,74 E - 02. O componente cuja falha mais influiu no resultado final foi a bomba de água de alimentação.

O programa distribuído pela IAEA utilizado neste caso exemplo forneceu resultados compatíveis com outros códigos. Estes resultados porém não podem ser usados para outros fins e a IAEA se exime de qualquer responsabilidade decorrentes da utilização do PSAPACK.

4. CONCLUSÃO

Uma das maiores dificuldades a ser enfrentada na execução de uma APS é o tratamento dos dados de falhas de componentes, muitas vezes de difícil interpretação e necessitando tratamento estatístico específico. A literatura sobre o assunto é grande, mas os valores numéricos são imprecisos e às vezes contraditórios. O levantamento de dados diretamente na planta analisada tem sido a solução adotada pelos concesssionários, mas não é possível para o caso de usinas em fase de construção.

No desenvolvimento de uma APS completa há necessidade de formação de um grupo de técnicos com vasto conhecimento na planta e/ ou nas técnicas de análise aplicada, além de ser preciso dispor das ferramentas adequadas.

A quantidade de horas para execução do serviço é bastante grande e requer uma organização minuciosa com claras definições de objetivos.

TABELA 1

B1	B1A	B1B					
B1A	R2	B3	B5	B7	B9	LA001EL	
	LA002EL						
B1B	R10	B14	B21	B25			
B2	LA003FD	LA003EL					
B3	B4	LA004EL	LA004FD				
B4	JR7B	LA004CC	LA004CF				
B5	B6	LA005EL	LA005FR				
B6	LA005CC	LA005CF	JR75				
B7	R8	LA006EL	LA006FR				
B8	LA006CC	LA006CF					
B9	LA007FD	LA007IL	LA007EL				
B10	B11	LA008CH	LA008B8				
B11	B12	R13					
B12	JR74	LA008FB					
B13	LA008FR	LA008CC					
B14	B15	R18	LA009IL				
B15	B16	LA013IL					
B16	B17	LA012IL					
B17	LA010IL	LA011IL					
B18	B19	LA014IL					
B19	R20	LA015IL	LA015EL				
B20	LA015CC	LA015EE					
B21	R22	R23	B24	LA016EL			
B22	LA017IL	LA018IL					
B23	LA019IL	LA020IL					
B24	LA021IL	LA022IL					
B25	R26	R27	LA024EL	LA025FD			
B26	LA026IL	LA027IL	LA028IL	LA029IL	LA030IL		
B27	LA031CF	LA031CC	LA031FB				

ENDIREE
PUNCH
*REB

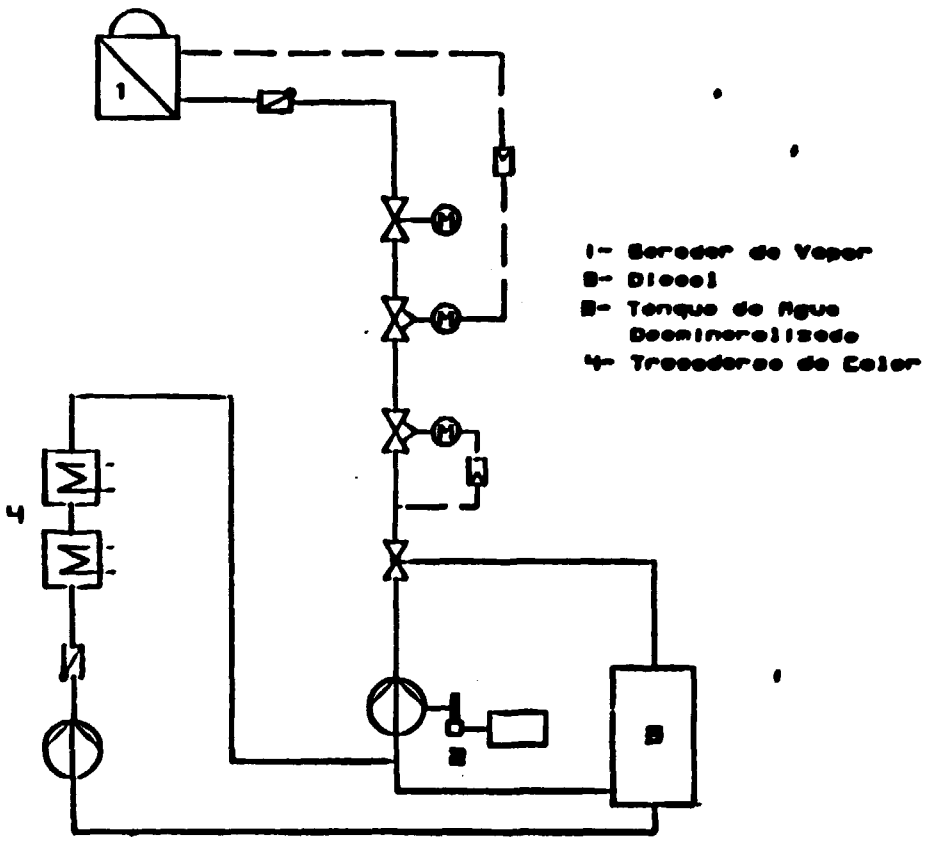

Figura 1 - Diagrama Simplificado do Sistema de Água de Alimentação de Emergencia