APLICAÇÃO DA TÉCNICA DE ANÁLISE DE MODOS DE FALHA E EFEITOS AO SISTEMA DE RESFRIAMENTO DE EMERGÊNCIA DE UMA INSTALAÇÃO NUCLEAR EXPERIMENTAL

Osmar Conceição Júnior, Antonio Teixeira e Silva
Instituto de Pesquisas Energéticas e Nucleares
Av. Prof. Lineu Prestes, 2.242 - São Paulo – SP
CEP 05508-000
osmarjr@usp.br

RESUMO

Este estudo consiste em aplicar a técnica de identificação de perigos e análise de risco conhecida como Análise de Modos de Falha e Efeitos (AMFE) ao Sistema de Resfriamento de Emergência (SRE) de uma instalação nuclear experimental. Esse tipo de análise tem como objetivo encontrar possíveis vulnerabilidades nesse sistema e propor melhorias de modo a maximizar sua confiabilidade.

Descritores: *Análise de Risco, AMFE e SRE.*

ABSTRACT

This study consists on the application of the Failure Modes and Effects Analysis (FMEA), a hazard identification and a risk assessment technique, to the Emergency Cooling System (ECS), of an experimental nuclear power plant. Such analysis intends to identify possible weaknesses on the design of the system and propose some improvements in order to maximize its reliability.

Key words: *Risk Assessment, FMEA and ECCS.*

INTRODUÇÃO

A recente escalada dos preços do petróleo leva os analistas a acreditar que tenha ocorrido, no ano passado, o terceiro choque desta "commodity".

Ao contrário do ocorrido nos dois choques anteriores, quando houve basicamente um problema de restrição da oferta por motivos políticos, desta feita a crise se deveu a um desequilíbrio provocado pelos dois parâmetros da curva oferta e demanda.

Enquanto a procura pelo produto vinha crescendo significativamente ao longo dos últimos anos, impulsionada em sua maior parte pelos países em desenvolvimento; a capacidade de produção atingiu valores muito próximos ao seu limite, conforme demonstram DUNCAN e YOUNGQUIST [1], LAHERRERE [2] e IVANHOE [3].

Com os preços naqueles patamares, a tendência era (e, com o final da crise econômica atual, deve voltar a ser) a de restringir o uso deste recurso a suas aplicações mais nobres, procurando-se alternativas a sua utilização como combustível, inclusive como forma de minimizar seus efeitos em relação às emissões de CO_2 e, por conseguinte, ao aquecimento global.

Como conseqüência direta desses fatores, tem-se notado uma aceleração na busca por novas fontes de energia, capazes de substituir os combustíveis fósseis, diminuindo a dependência mundial em relação aos mesmos.

Neste ponto, é importante salientar que deve haver uma maior diversificação da matriz energética brasileira, de forma a que não seja simplesmente transferida a dependência de uma fonte de energia para outra.

Dentre as opções que se apresentam, a energia nuclear é particularmente interessante no caso brasileiro porque, além de não emitir gases causadores do efeito estufa e aquecimento global, apresenta vantagens competitivas em relação às demais. O Brasil é a 6ª maior reserva de Urânio do mundo, com apenas 25% do seu território prospectado (INB [4], dados

referentes ao ano de 2001); e domina as tecnologias de fabricação do combustível nuclear e de construção de reatores de pequeno e médio porte.

As grandes preocupações em relação a esta tecnologia resumem-se basicamente quanto à questão do rejeito radioativo e da segurança. Com relação à primeira, pode-se afirmar que, ao contrário do que acontece com os combustíveis fósseis, por exemplo, os produtos de fissão são armazenados em locais isolados e seguros e apresentam volume bastante reduzido.

A segunda questão é um pouco mais delicada, tendo-se em vista que, segundo FROSDICK [5], o ser humano por natureza tende a temer aquilo que julga não ter controle, ou que não lhe seja familiar ou ainda que possa afetar negativamente um grande número de pessoas de uma única vez.

A tecnologia nuclear, por ser relativamente nova (pouco mais de 60 anos) e em virtude do seu grande potencial de geração energética, encaixa-se em todos os fatores mencionados acima, sendo motivo de grande apreensão por parte de um número não desprezível de pessoas.

Para minimizar esses temores as regulamentações são extremamente rígidas e cerca de 90% dos custos de implementação desta tecnologia são relacionados à segurança (KUMAMOTO [6]).

Neste contexto, durante o projeto de centrais nucleares, aplicam-se várias técnicas de identificação de perigos e de análise de risco, a fim de se identificar os diversos eventos iniciadores de acidentes e verificar suas possíveis conseqüências. Dentre essas técnicas, há a Análise de Modos de Falha e Efeitos (AMFE), cuja aplicação é consagrada pela sua utilização em diversos campos da indústria como a aeronáutica, a automobilística e a nuclear.

O objetivo deste artigo é o de mostrar os principais resultados da aplicação dessa técnica ao Sistema de Resfriamento de Emergência (SRE) de uma instalação nuclear experimental.

O CONCEITO DE RISCO

Antes de apresentar a definição de risco é necessário conceituar o termo perigo. MACDONALD [7] afirma que este termo pode ser entendido como uma propriedade física ou química, inerente a um elemento, que tem potencial para causar danos às pessoas, propriedades ou ao ambiente. Em outras palavras, é uma condição necessária para ocorrência de um acidente.

De acordo com KUMAMOTO [6] e a BSI [8], risco é uma combinação de probabilidade com que se prevê a ocorrência de um evento adverso definido e a magnitude das conseqüências desta ocorrência.

Algumas características do risco são:

- traduz-se, necessariamente, por uma expectativa de perda;
- é sempre um elemento de incerteza;
- refere-se única e exclusivamente a eventos futuros.

O risco pode ser classificado em:

a) Negligenciável – quando a ocorrência do evento é muito improvável e suas conseqüências desprezíveis;

b) Baixo – os riscos são considerados administráveis através de medidas de mitigação apropriadas;

c) Intermediário – quando os riscos são maiores que o desejado e ações devem ser tomadas para reduzí-lo a um nível tão baixo quanto o economicamente praticável;

d) Alto – os riscos são considerados inaceitáveis e devem ser substancialmente reduzidos para níveis seguros ou o projeto deve ser descartado.

FISCHHOFF ET AL. [9] afirmam que o risco nunca é aceito incondicionalmente. Ele só é aceito caso traga algum benefício que o compense, em outras palavras é a decisão por uma alternativa, envolvendo risco, que é aceitável e não o risco por si só.

Neste ponto, é preciso fazer distinção entre risco individual e coletivo, em virtude das diferentes maneiras como são percebidos. O primeiro é definido pela HSE [10] como sendo o risco específico para um indivíduo, seja ele trabalhador ou membro do público em outras palavras, alguém que resida dentro de uma área delimitada, a uma certa distância da instalação, ou que siga um determinado padrão de comportamento. O segundo representa o risco para a sociedade como um todo e foi definido como a chance de ocorrer um grande acidente, causando um número de mortes pré-determinado.

Estes conceitos de risco não são compartilhados pelos cientistas sociais, para os quais há sérias dificuldades em enxergar o risco como um conceito unidimensional.

Como WARNER [11] salienta, os cientistas e os engenheiros utilizam estas definições porque elas fornecem a base com a qual eles podem desempenhar seu trabalho.

Uma das críticas às técnicas de análise de risco é que elas baseiam-se na experiência anterior para identificação dos riscos e esta dependência gera pelo menos três pontos fracos nessas técnicas:

- o primeiro, como acentua TOFT [12] é que, em muitas ocasiões, as organizações responsáveis têm falhado em transformar o conhecimento passivo, de acidentes ocorridos, em conhecimento ativo;
- outra questão a ser mencionada é que quando se transforma a experiência adquirida com estes eventos em conhecimento ativo geralmente isto acontece apenas naquele ramo de atividade ou se restringe apenas à indústria onde ocorreu o acidente;
- por fim, as experiências passadas, obviamente, não podem prever os riscos associados a novas tecnologias. KASPERSON E KASPERSON [13] discutem potenciais perigos da chuva ácida e do aquecimento global para a humanidade, uma vez que esses problemas apareceram como conseqüências indesejadas da atividade humana nos últimos anos. DOUGLAS E WILDAVSKY [14] concluem, a partir daí, que devem existir perigos substanciais à vida que ainda não são conhecidos.

Outros fatores que influenciam a percepção de risco são a influência cultural, a condição sócio-econômica, a experiência pessoal, o excesso de estímulos, a familiaridade com o problema, a voluntariedade ou imposição do risco por terceiros, a sensação de exercer ou não o controle sobre ele e se o mesmo deve-se a causas naturais ou provocadas pelo homem.

Devido a esta complexidade, mesmo entre as ciências comportamentais não há um consenso sobre o conceito de risco e não é objetivo deste trabalho aprofundar-se neste tema.

Um último fator a ser mencionado é a comunicação do risco ao público. HOOD ET AL. [15] asseveram que a confiança das gerações passadas na habilidade da ciência em prover respostas às questões transformou-se em desconfiança, em parte devido à ausência de consenso entre os cientistas, em determinados assuntos; também porque as respostas que a ciência fornece atualmente são muito mais complexas e contingentes e por fim, porque "eles" estão sempre mudando de opinião.

A confiança pode ser facilmente perdida, mas é dificilmente recuperada e, em certas situações, irrecuperável. Portanto é imprescindível que haja transparência e sinceridade no processo de comunicação do risco, por pior que seja o teor da informação.

TÉCNICAS DE IDENTIFICAÇÃO DE PERIGOS E DE ANÁLISE DE RISCO

A identificação de áreas de vulnerabilidade e de perigos específicos é de fundamental importância para a prevenção de acidentes.

Uma vez identificados grande parte do problema foi equacionada, entretanto esta tarefa não é trivial; geralmente quanto maior a tecnologia envolvida, mais complexo se torna o processo.

Segundo LEES [16], a prevenção de acidentes tende a depender cada vez mais do sistema de gerenciamento e nem sempre é uma tarefa simples descobrir pontos fracos nesse sistema. Os perigos físicos também, na maior parte das vezes, não estão evidentes de forma que possam ser identificados através de uma simples inspeção visual. Por outro lado, há à disposição, atualmente, uma ampla gama de técnicas de identificação de perigos e análise de risco que podem ser utilizadas para resolver este problema.

Diferentes métodos são indicados para as diversas fases do projeto e não há um procedimento único, ou ideal, para o processo de identificação de perigos e análise de risco.

A experiência anterior é sempre desejável e a obediência às normas e procedimentos certamente contribui para evitar perigos que poderiam passar despercebidos para a grande maioria das pessoas, mas é preciso estar atento ao fato de que a maioria das situações, nas quais serão empregadas as técnicas de identificação de

perigos, apresenta algum aspecto inovador.

As técnicas de identificação de perigos e análise de risco mais conhecidas são:

a) "Checklist"

É um dos instrumentos mais úteis no processo de identificação de perigos. O "checklist" é a garantia de que um determinado procedimento, que mostrou-se o mais adequado para aquela prática até o momento, está sendo seguido.

b) "What if?"

É uma técnica preliminar de identificação de perigos, que consiste na revisão de todo o projeto através de uma série de perguntas geralmente iniciadas com a expressão "o que aconteceria se ...."

A metodologia é executada por uma equipe de especialistas, freqüentemente com o auxílio de um checklist, e provavelmente seja, depois deste último, o mais antigo método de identificação de perigos.

c) "Preliminary Hazard Analysis"

PHA é uma técnica qualitativa de identificação de perigos a ser empregada na etapa inicial do projeto.

O primeiro passo no PHA é a identificação de componentes ou elementos perigosos existentes no sistema.

O segundo passo é a identificação dos eventos que podem transformar condições específicas de perigo em potenciais acidentes, a partir daí a gravidade destes potenciais acidentes é avaliada para determinar se há necessidade de medidas corretivas.

d) "Coarse Hazard Studies"

Outro método de identificação de perigos que deve ser utilizado preferencialmente na fase inicial do projeto é o "Coarse Hazard Studies" (CHS) ou "checklist" criativo, que é conduzido através de um exercício em equipe.

É uma técnica desenvolvida para ser utilizada como preparação para o "Hazard and Operability Study" (HAZOP).

Ele auxilia na identificação daqueles perigos e outros problemas que são básicos e que podem, em princípio, ser detectados neste estágio. O CHS revela deficiências nas informações do projeto e expõe perigos devido à interação entre a planta e o meio ambiente ou entre ela e outras plantas, nas quais o estudo de HAZOP não é tão eficaz, estas características contribuem para remover potenciais atrasos no caminho crítico do projeto.

e) HAZOP

Um método muito usado atualmente para identificação de perigos na etapa de confecção do fluxograma de processo é o "HAZOP". Esta técnica é executada através de um trabalho em equipe que envolve o exame da finalidade do projeto à luz de palavras-chave.

A técnica foi empregada pela primeira vez nos anos 60 na Imperial Chemical Industries (ICI) mas como muitas outras ferramentas de análise de risco há mais de uma fonte responsável pelo seu desenvolvimento como KLETZ [17] e KNOWLTON [18], através do Chemetics manual e ela tem sido objeto de numerosas variações.

O conceito básico do HAZOP é, a partir de uma descrição completa do processo, questionar todos os detalhes do mesmo para descobrir que desvios da concepção original podem ocorrer e quais as causas e as conseqüências destes possíveis desvios.

As características mais importantes para o estudo são:

- objetivo do projeto;
- desvios do objetivo;
- causas dos desvios;
- conseqüências.

O momento ideal para se aplicar a técnica HAZOP é uma decisão importante.

As desvantagens de um estudo prematuro são que as informações necessárias para sua eficácia podem, ainda, não estar disponíveis e há um risco maior de mudanças de projeto no decorrer do estudo.

As vantagens são as facilidades de incorporar ao projeto quaisquer mudanças provenientes do estudo, em particular, para alcançar uma concepção inerentemente mais segura.

Por outro lado, um estudo tardio apresenta as desvantagens de uma implementação mais cara e difícil das opções de melhoria, além disso, elas tendem a ser implementadas de forma conjunta, muitas vezes, sem o devido cuidado em verificar se há sobreposição ou interferência entre elas.

A técnica HAZOP possui, porém, suas limitações, que são basicamente de dois tipos:

- a primeira advém das hipóteses concernentes ao método e é uma limitação de escopo. Na sua forma original, o método assume que o projeto foi conduzido de acordo com as normas apropriadas; e

- a outra limitação é inerente ao método. O HAZOP não é indicado, por exemplo, para tratar com características espaciais associadas ao "layout" da planta.

f) Análise de Modos de Falha e Efeitos (AMFE).

É uma técnica indutiva que promove a revisão de todos os componentes de um dado sistema para descobrir seus modos de falha e seus respectivos efeitos.

A análise é orientada para os equipamentos, ao invés de parâmetros de processo, como é o caso do HAZOP.

O BS 5760 "Reliability of Systems, Equipment and Components, Part 5: 1991 Guide to Failure Modes, Effects and Criticality Analysis" trata dos propósitos, princípios, procedimentos e aplicações da AMFE, suas limitações e sua relação com outras técnicas de análise de risco.

Seu propósito é a identificação das falhas que conduzam a eventos indesejados na operação do sistema e seus objetivos incluem:

- identificação de cada modo de falha, da seqüência de eventos a ele associados e seus possíveis efeitos;

- uma classificação de cada modo de falha de acordo com características relevantes, incluindo capacidade de detecção, diagnóstico e teste, possibilidade de substituição, compensação e provisões operacionais; e

- a determinação da criticidade de cada modo de falha (no caso da AMFEC).

A informação básica de cada um dos itens analisados é: nome, função, identificação, modos de falha, causas da falha, efeitos da falha no sistema, métodos de detecção de falha, provisões para compensação, severidade dos efeitos e comentários.

A AMFE é uma metodologia eficaz de análise de elementos que podem provocar a falha de todo, ou grande parte de, um sistema, ela não é muito indicada quando uma lógica complexa é necessária para descrever a falha do sistema.

Uma técnica complementar a ela, de caráter dedutivo é a Árvore de Falhas, que é mais indicada nos casos em que a lógica da falha é mais complexa.

Passos para execução de uma análise do tipo AMFE:

1º) Definir o sistema e seus requisitos funcionais e operacionais:

- incluir as funções primárias e secundárias, o desempenho esperado, as restrições do sistema e as condições explícitas que constituam uma falha. A definição do sistema deve incluir a definição de cada modo de operação, bem como a sua duração;

- apontar quaisquer fatores ambientais relevantes como temperatura, umidade, radiação e pressão durante o período de operação e na parada da instalação; e

- considerar falhas que possam levar ao não cumprimento de requisitos mínimos exigidos pelas entidades reguladoras.

2º) Fazer o diagrama de blocos do sistema, de modo a mostrar as relações entre os elementos e eventuais interdependências.

3º) Identificar os modos de falha, suas causas e seus efeitos.

4º) Identificar métodos de detecção de falha e isolamento e verificar se outros modos de falha forneceriam a mesma indicação.

5º) Identificar características de projeto e provisões operacionais que previnam ou reduzam os efeitos do modo de falha.

6º) Identificar combinações específicas de falhas múltiplas a serem consideradas;

7º) Revisar o repetir a análise tipo AMFE toda vez que o projeto for modificado.

A AMFEC é uma complementação da AMFE, na qual é realizada uma análise de criticidade, que é uma função da severidade do efeito e da freqüência com a qual espera-se que ele ocorra.

g) Árvore de Eventos (AE)

A AE é um diagrama lógico que caracteriza a propagação de um evento iniciador de acidente em termos de falhas e/ou sucessos de funções ou sistemas, segundo uma determinada ordem lógica de prioridade (cronológica e/ou funcional), definindo as seqüências de acidentes.

Ela pode ter uma abordagem qualitativa ou quantitativa. Qualitativamente é utilizada para identificar as saídas do evento inicial, quantitativamente para estimar as freqüências ou probabilidades de cada saída.

Os principais elementos da árvore são as definições dos eventos e os vértices lógicos. O evento inicial é usualmente expresso como uma freqüência (eventos/ano) e as subdivisões seqüentes como probabilidades e, portanto, a saída final é expressa também como freqüência.

h) Árvore de Falhas (AF)

É um diagrama lógico destinado a apresentar as causas de um dado evento indesejável, freqüentemente um perigo. A possibilidade de ocorrência deste evento, chamado Evento Topo (ET), deve ser prevista antes da construção da árvore, através da utilização de outro método de identificação de perigos.

A AF é portanto uma técnica dedutiva e de natureza qualitativa e quantitativa, sendo largamente utilizada na avaliação de perigos mas de grande valor também na sua identificação.

O conceito original da AF foi desenvolvido pela Bell Telephone Laboratories no início dos anos 60.

Desenvolvimentos na metodologia aconteceram na essência do método, através de sua análise para descobrir os cortes mínimos para ocorrência do ET e na avaliação da freqüência ou probabilidade deste evento. O corte mínimo é um conjunto de eventos primários que podem causar o ET, o conjunto completo dos cortes mínimos constitui o grupo de modos de falha principais, causadores do ET.

Houve também progressos relacionados ao método em algumas características. Um importante avanço a ser mencionado nessa área é a teoria cinética da árvore, que foi desenvolvida por VESELY [19], permitindo a determinação de características tais como confiabilidade e disponibilidade de sistema ao longo do tempo.

Segundo FUSSEL [20], os maiores benefícios auferidos com uma AF são:

- direcionar o analista a enxergar a falha de modo dedutivo;
- apontar os aspectos importantes do sistema em relação às falhas de interesse para o estudo;
- proporcionar auxílio gráfico, dando visibilidade aos gerenciadores do sistema;
- prover opções de análise qualitativa ou quantitativa da confiabilidade do sistema em questão;
- permitir ao analista concentrar-se em uma determinada falha do sistema por vez;
- propiciar uma visão privilegiada do comportamento do sistema.

Fussel também cita algumas dificuldades no trabalho com a AF. Por ser uma forma sofisticada de análise de confiabilidade ela requer tempo e esforço considerável da parte de analistas bem treinados e, embora ela seja uma das melhores ferramentas para se analisar o sistema como um todo, ela não garante, por si só, a detecção de todas as falhas, especialmente as que possuam uma causa comum.

Geralmente os eventos são assumidos como estatisticamente independentes, mas, na prática, há várias situações em que isso não ocorre.

Na construção das Árvores de Falhas este problema ficou originalmente conhecido como "modo de falha comum", depois como "causa de falha comum" e mais recentemente como "falha dependente".

O problema é particularmente delicado em sistemas tais como os pertencentes ao reator nuclear, onde é exigido um alto grau de confiabilidade.

i) Diagrama Causa-Conseqüência

Uma outra técnica que incorpora características tanto da Árvore de Falhas quanto da Árvore de Eventos é o Diagrama Causa-Conseqüência, desenvolvido por NIELSEN [21] E TAYLOR [22].

Ele é construído através da definição de um evento crítico e da análise das possíveis causas e conseqüências deste evento, o desenvolvimento do diagrama para frente tem as características de uma AE e para trás de uma AF.

Algumas características importantes do Diagrama Causa-Conseqüência são a sua habilidade em tratar com caminhos que gerem conseqüências alternativas e com a cronologia dos eventos. O diagrama também pode ser utilizado para análise quantitativa.

j) Análise de Falhas Humanas

Uma fonte importante de danos e perigos é a operação incorreta de uma planta.

Há alguns métodos que estudam este problema, entre eles a Análise das Tarefas e a Análise dos Erros na Execução, o problema da falha humana é, contudo, muito complexo.

A Análise das Tarefas é uma técnica que foi originalmente desenvolvida como uma ferramenta de treinamento. Quando aplicada aos operadores da planta, ela procura desmembrar o procedimento operacional em sub-rotinas, com o objetivo de descobrir potenciais dificuldades (ou mesmo erros) na execução das tarefas ou do procedimento como um todo.

Outra técnica de identificação de erros operacionais é a Análise de Erros na Execução, desenvolvida por TAYLOR [23]. Este é o método de análise de procedimentos operacionais para descobrir possíveis erros na operação da planta, propriamente dita.

As ações a serem tomadas no processo são listadas, uma a uma, sendo cada qual seguida por seu efeito na planta, obtendo-se as seguintes seqüências: ação – efeito sobre a planta – ação – efeito sobre a planta.

As ações são intervenções na planta, tais como acionamento de botões, abertura de válvulas, etc.

A ESCOLHA DA TÉCNICA

A análise tipo AMFE foi a escolhida porque, conforme atesta KUMAMOTO [6], ela detalha sistematicamente, componente a componente, todos os possíveis modos de falha e identifica suas conseqüências na planta, possibilitando introdução de melhorias e/ou a correção dos defeitos, ainda na fase de projeto.

Prováveis deficiências em cada componente da planta são analisadas para determinar seus efeitos em outros componentes a ele relacionados.

De acordo com a MIL-STD-1629A [24], esta técnica pode ser orientada para o equipamento, concentrando-se nas potenciais falhas dos mesmos ou para os eventos, onde a ênfase é nas saídas funcionais e seus efeitos para o sistema em caso de falha.

A principal limitação deste método é considerar a progressão dos modos de falha individualmente, dificultando a avaliação dos efeitos para combinação de diversos modos de falha ocorrendo simultaneamente. Para minimizar essa deficiência foi introduzido o conceito de condição latente na análise, o que ocorre quando a falha de um componente não provoca maiores problemas mas cria condições para que, caso haja falha de outro componente a ele relacionado (física ou funcionalmente), aconteça um acidente.

Uma técnica complementar a AMFE, de caráter dedutivo é a Árvore de Falhas, que é mais indicada nos casos em que a lógica da falha é mais complexa.

Como já visto, algumas dificuldades no trabalho com a AF são que ela requer tempo e esforço considerável da parte de analistas bem treinados e, embora ela seja uma das melhores ferramentas para se analisar o sistema como um todo, ela não garante, por si só, a detecção de todas as falhas, especialmente as que possuam uma causa comum.

Esse problema é particularmente delicado em sistemas tais como os pertencentes ao reator nuclear, onde é exigido um alto grau de confiabilidade.

Teoricamente, as confiabilidades calculadas são extremamente altas, mas há uma certa preocupação quanto a um possível sub-dimensionamento desta proteção devido ao fenômeno da falha dependente, que pode estar "disfarçado" de muitas maneiras.

Já o HAZOP, além de ser uma técnica mais utilizada na análise de processos, apresenta basicamente dois tipos de limitações:

- a primeira advém das hipóteses concernentes ao método e são uma limitação de escopo. Na sua forma original, o método assume que o projeto foi conduzido de acordo com as normas apropriadas; e
- a outra limitação é inerente ao método. O HAZOP não é indicado, por exemplo, para tratar com características espaciais associadas ao "layout" da planta e os seus efeitos resultantes.

O SISTEMA DE RESFRIAMENTO DE EMERGÊNCIA

A escolha sobre o sistema a ser analisado recaiu sobre o SRE por ser ele o principal responsável pela mitigação de um

dos piores acidentes passíveis de ocorrência em uma planta nuclear, a perda de refrigerante no circuito primário.

Conforme TAKESHI [25], esse sistema é composto por equipamentos destinados a receber, estocar e injetar o refrigerante no reator, além de remover o calor residual do núcleo em condições normais e anormais de operação, ou ainda, durante os acidentes de perda de refrigerante.

O SRE é dividido em dois subsistemas:

a) Subsistema de Injeção de Emergência (SIE), que atua na reposição da água do circuito primário, quando houver um vazamento superior a 1,0 m^3/h, ou ainda de modo a garantir a integridade e a geometria do núcleo, através da inundação do vaso do reator, no caso de acidentes de perda de refrigerante por ruptura no circuito primário.

Este subsistema é composto por:

- dois tanques de compensação, situados na parte superior do compartimento do reator;
- dois acumuladores, instalados na contenção;
- dois tanques de inundação, localizados acima da contenção;
- duas bombas centrífugas para injeção à alta pressão (BIAP);
- duas bombas centrífugas para injeção à baixa pressão (BIBP).

b) Subsistema de Remoção de Calor Residual (SRCR), que é o responsável pelo resfriamento do reator após o desligamento nas diversas condições de operação da instalação, incluindo-se o caso de um acidente de perda de refrigerante.

Para isso, este subsistema dispõe de:

- dois trocadores de calor para remoção do calor residual;
- duas bombas centrífugas para a circulação de refrigerante do reator (ou do fluido presente no compartimento do reator após a sua inundação);
- duas bombas centrífugas para a circulação de água de resfriamento.

A localização exata e a interligação dos equipamentos do SRE, bem como a instrumentação e os controles associados, estão descritos em TAKESHI [26] e [27].

O Sistema de Resfriamento de Emergência é projetado para executar as seguintes funções básicas:

- resfriar o reator, após seu desligamento, com a remoção do calor residual do núcleo;
- garantir a integridade do núcleo do reator, em caso de acidente de perda de refrigerante;
- Assegurar o resfriamento do reator, por tempo indeterminado.

Um acidente de perda de refrigerante é constatado pelo SPP, através da ocorrência simultânea da queda de pressão no primário com o aumento de pressão e/ou radioatividade no interior da contenção, ou ainda com a queda do nível de água no pressurizador, abaixo do valor mínimo de desligamento do reator.

Ao constatar um acidente de perda de refrigerante, o SPP efetua inicialmente o desligamento do reator e o desligamento das bombas de circulação do primário gerando o Sinal de Injeção de Segurança (SIS) para atuação do SRE.

Em caso de grandes perdas de refrigerante do reator temos, além da atuação dos tanques de compensação e das BIAP, a injeção passiva, assegurada principalmente pelos dois acumuladores, que contribuem para o resfriamento do núcleo nos instantes iniciais do acidente.

Após a atuação dos acumuladores, quando seu nível atinge o valor mínimo, são fechadas as válvulas de bloqueio, isolando-os automaticamente e interrompendo a injeção através dos mesmos.

Neste mesmo instante, um sinal é emitido para o desligamento das BIAP, possibilitando assim uma vazão mais alta nas linhas de injeção.

Nesta fase entram em operação as BIBP, acionadas automaticamente pelo SIS quando a pressão do primário atingir 14 bar, injetando água borada, proveniente dos tanques de inundação, nas pernas fria e quente do reator.

Em caso de falha no funcionamento das BIBP, o sistema conta ainda com o recurso de injeção de água diretamente dos tanques de inundação, por gravidade, através das tubulações de descarga das bombas de injeção.

Parte da água injetada remolha o núcleo e deixa o SRR, através da tubulação

que sofreu ruptura, ficando retida no fundo do compartimento do reator.

Após o esgotamento dos tanques de inundação, o SRCR pode ser redirecionado pelo SPP para captar a água contida na parte inferior do compartimento do reator (água que escapou do circuito primário através da ruptura) e retorná-la ao vaso do reator, após ter sido resfriada nos trocadores de calor.

A FIG. 1 ilustra, de forma sintética, a seqüência de atuação dos equipamentos do SRE no caso de um acidente de perda de refrigerante do primário por grande ruptura (APRPGR).

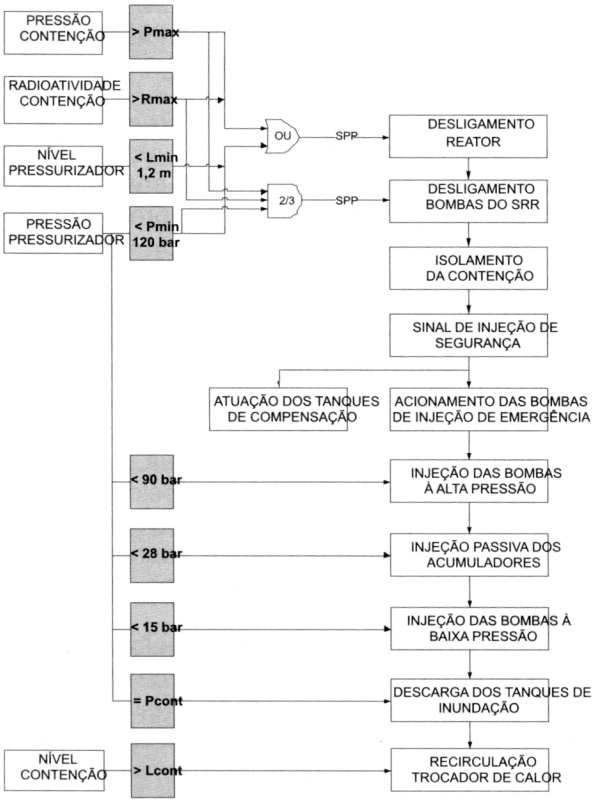

Figura 1 – Diagrama resumido da seqüência de atuação dos equipamentos do SRE, durante um APRPGR (obtido de TAKESHI).

ESCOPO DA ANÁLISE

Por ser empregada redundância de quatro nos instrumentos de medição de todas as variáveis existentes no SPP, para efeitos deste estudo, a análise destes componentes não será executada.

Com relação a falhas humanas, em virtude da atuação do SIE ser totalmente automatizada e, no caso do SRCR, a atuação mais crítica consistir em se realinhar o subsistema para o modo de recirculação de água contida no poço da contenção, partimos da hipótese que esta operação foi efetuada com sucesso e que, assim, não há ocorrência deste tipo de falha.

Outras formas de falha humana como erros de projeto, especificação inadequada de componentes e/ou erros em procedimentos de instalação e manutenção também não serão contempladas neste estudo.

RESULTADOS

Analisando-se o sistema pode-se observar que eventuais falhas nos tanques de compensação, nos acumuladores e nos componentes a eles interligados não apresentam maior gravidade, em função do reduzido volume de fluido refrigerante por eles armazenado e/ou do tempo de atuação dos mesmos em um APRPGR.

As únicas exceções ficam por conta de vazamentos nas válvulas de ligação desses componentes ao reator, que em operação normal, podem ocasionar o desligamento do reator em virtude de queda na pressão do circuito primário, provocando paradas desnecessárias e prejuízos com manutenções não programadas.

Pode-se verificar também que em um dos modos de falha mais graves do SRE é a perda de inventário de um dos tanques de inundação (seja ele por vazamento no tanque, na tubulação ou em seus componentes) mas, mesmo nesta circunstância, este tipo de acidente não implicaria em maior gravidade porque além da redundância da outra linha, temos o Subsistema de Remoção de Calor Residual, que recircula a água através do núcleo do reator até a temperatura de parada segura da instalação.

Sendo assim, podemos observar que um vazamento de grandes proporções da válvula, que possibilita a injeção por gravidade, teria o mesmo efeito da perda de um tanque de inundação, conforme visto acima.

As válvulas de retenção em série localizadas imediatamente após a válvula citada no parágrafo anterior, em caso de vazamento de grandes proporções, também

podem provocar a perda do inventário de um dos tanques mas, nesse caso, há a possibilidade de fechamento daquela válvula.

Passando para a análise da linha de injeção de alta pressão, pode-se observar que existe uma válvula de gaveta, normalmente aberta, na entrada da bomba cujo objetivo é isolá-la para manutenção.

Se houver um grande vazamento neste componente também poderá haver perda de inventário de um dos tanques de inundação.

Se o vazamento ocorrer na própria bomba de injeção de alta pressão ou na válvula de três vias, localizada imediatamente após aquela válvula, ou ainda na válvula globo e retenção no fim do circuito de injeção de alta pressão também pode acarretar a perda do conteúdo de um dos tanques de inundação, tendo-se como recurso para compensação, nesse caso, o fechamento da válvula de gaveta no início da linha.

A linha de injeção de baixa pressão apresenta exatamente os mesmos componentes da linha de alta e, portanto, com os mesmos modos de falha e conseqüências descritos acima. A única diferença é que a severidade em caso de perda desta linha é maior, visto que a atuação das bombas de baixa no APRPGR é mais efetiva que a das de bombas de alta.

A falha da tubulação, por grande vazamento, apresenta os mesmos efeitos que uma falha deste tipo no tanque de inundação, com a exceção que em alguns pontos da linha há recursos para compensação.

Prosseguindo-se com a análise, o próximo item é uma associação em paralelo de duas válvulas tipo gaveta, normalmente fechadas, cujo objetivo é vedar a contenção, durante a operação normal do sistema, e permitir a injeção de emergência e por gravidade, em caso de acidente.

Neste caso, elas também poderão falhar por vazamento, acarretando perda do inventário de um dos tanques e sem recurso para compensação (porque todo o fluido injetado na contenção, em caso de acidente, passa obrigatoriamente por uma destas duas válvulas).

A seguir temos uma válvula de retenção, cuja função é a mesma da associação em paralelo descrita anteriormente e que, em caso de vazamento num acidente, poderá acarretar a perda do inventário de um dos tanques de inundação, sem que haja recursos para compensação.

Finalmente, no trecho de injeção de emergência, temos uma associação em paralelo de um conjunto de uma válvula de gaveta em série com uma válvula de retenção, cujo objetivo é vedar o compartimento do reator, em operação normal, e possibilitar a injeção de emergência e por gravidade, em condição de acidente.

Em condição de acidente a falha na válvula de gaveta pode se dar por vazamento, permitindo a passagem de fluido para fora da linha e sem recurso para compensação neste circuito, podendo ocasionar a perda de inventário de um dos tanques.

A válvula de retenção, em operação normal, pode falhar por vazamento, permitindo a passagem de fluido para fora da linha, acarretando perda de pressão no primário e o desligamento do reator.

Em caso de acidente ela pode falhar por vazamento, ocasionando uma perda de refrigerante interna ao compartimento do reator, fazendo com que a água borada de um dos tanques não passe pelo seu núcleo antes de alagá-lo mas, se não houver falha conjunta do sistema de recirculação de água, o mesmo irá possibilitar a sua circulação pelo reator e seu resfriamento nos trocadores de calor.

A outra linha em paralelo apresenta os mesmos modos de falha e as mesmas conseqüências descritas.

Falhas na linha de equalização de pressão para injeção por gravidade, não apresentam maior gravidade, visto que a injeção pelas bombas de alta e baixa pressão é suficiente para alagar o vaso do reator e em caso de falha de um circuito, ainda há o outro em paralelo (além do SRCR).

Quanto ao Subsistema de Remoção de Calor Residual (SRCR), suas falhas somente apresentarão maior gravidade caso tenha ocorrido falha nos dois circuitos do SIE.

Se o núcleo do reator estiver, ao menos, parcialmente inundado a sua integridade estará preservada, independente da atuação do SRCR.

Assim, podemos inferir que as falhas no SRCR têm uma severidade menor que as do SIE e dentre as mais significativas podemos

citar o entupimento do coletor ou falha em dois componentes-chave (um em cada linha), como, por exemplo, um trocador de calor e uma bomba, vazamento ou fechamento espúrio de duas válvulas, que façam parte do caminho crítico, etc.

CONCLUSÕES

Podemos observar que o SRE é inerentemente seguro, uma vez que mesmo que ocorra um evento capaz de impedir a utilização de uma linha do SIE (probabilidades de ocorrência extremamente baixas, conforme mostram OLIVEIRA ET AL. [28]), há ainda o recurso da outra linha e do Subsistema de Remoção de Calor Residual.

As recomendações para melhorias no sistema são:

- Afastar fisicamente os dois tanques de inundação;
- Comunicar as duas linhas e instalar válvulas na saída dos tanques;
- Procurar, sempre que possível, utilizar componentes redundantes diferentes dos componentes da linha principal;
- Instalar um sistema de detecção de vazamentos ao longo de toda a linha;
- Realizar manutenção adequada e inspeções e testes regulares.

REFERÊNCIAS

[1] DUNCAN, R. C; YOUNGQUIST, W. The world petroleum life-cycle. In: THE PTTC WORKSHOP "OPEC OIL PRICING AND INDEPENDENT OIL PRODUCERS", Oct. 22, 1998, Los Angeles. Disponível em <http://www.dieoff.com/pg133.pdf>. Acesso em 16 jun. 2008.

[2] LAHERÈERE, J. H. Future sources of crude oil supply and quality considerations. Rueil-Malmaison, France: DRI/Mc Graw-Hill/French Petroleum Institute, 1997.

[3] IVANHOE, L. F. Get ready for another oil shock!. The Futurist, jan.- fev., p. 20-23, 1997.

[4] Indústrias Nucleares do Brasil, Reservas de Urânio no Brasil. Disponível em: <http://www.inb.com.br/reservasBrasil.asp>. Acesso em 16 jun. 2008.

[5] FROSDICK, S. The techniques of risk analysis are insufficient in themselves. Disaster prevention and management v.6, n. 3, p. 165 - 177, 1997.

[6] KUMAMOTO, H.; HENLEY, E.J. Probabilistic risk assessment and management for engineers and scientists. 2.ed. Nova York, N.Y.: IEEE Press, 1996.

[7] MACDONALD, D. Practical hazops, trips and alarms. Oxford, R.U..: Elsevier Inc., 2004.

[8] BRITISH STANDARDS INSTITUTION. Quality vocabulary. BS 4778, BSI, Londres, R.U., 1991.

[9] FISCHHOFF, B.; LICHTENSTEIN, S.; SLOVIC, P.; DERBY, S.L.; KEENEY, R.L. Acceptable risk. Cambridge, R.U.: Cambridge University Press, 1981.

[10] HEALTH AND SAFETY EXECUTIVE. The tolerability of risk from nuclear power stations. Londres, R.U.: HM Stationery Office, 1988.

[11] WARNER, F. Calculated risks. Science and Public Affairs, inverno de 92, p. 44 – 49, 1992.

[12] TOFT, B. The failure of hindsight. Disaster prevention and management v.1, n. 3, p. 48 - 59, 1992.

[13] KASPERSON, R; KASPERSON, J. Hidden hazards. Acceptable evidence: science and values in risk management, Oxford University Press, p. 9 - 28, 1991.

[14] DOUGLAS, M.; WILDAVSKY A. Risk and culture. Berkeley, CA: University of California Press, 1982.

[15] HOOD, C.; ROTHSTEIN, H.; BALDWIN, R. The government of risk: understanding risk regulation regimes. Oxford university Press, 2001.

[16] LEES, F. P. Loss prevention in the process industries: hazard identification, assessment and control. 2.ed. Oxford, R.U..: Butterworth-Heinemann, 1996.

[17] KLETZ T.A. Hazop and hazan. 2.ed. Rugby, R.U.: Institution of Chemical Engineers, 1986.

[18] KNOWLTON R.E. A manual of hazard and operability studies. Vancouver, B.C.: Chemetics International Company Ltd., 1992.

[19] VESELY, W.E. Analysis of fault trees by kinetic tree theory. Rep IN – 1330. Idaho Falls, ID: Idaho Nucl. Corp., 1969.

[20] FUSSEL, J.B. Generic techniques in systems reliability assessment - Fault tree analysis: concepts and techniques, Noordhoff International Pub., p. 133 - 162, 1976.

[21] NIELSEN D.S. The cause-consequence diagram method as a basis for quantitative accident analysis. Rep. Risö M – 1374. Risö, DM: Atom. Energy Comm., 1971.

[22] TAYLOR J.R. Cause-consequence diagrams. Urbino, Itália: Nato Advanced Study Inst. on Synthesis and Analysis Methods for Safety and Reliability Studies, 1978.

[23] TAYLOR J.R. A background to risk analysis v. 1 – 4. Risö, DM: Risö Nat. Lab., 1979.

[24] MILITARY STANDARD – 1629A. Procedures for performing a failure mode effects and criticality analysis. Washington, DC: DEPARTMENT OF DEFENSE, 1980.

[25] TAKESHI, R.V.R. Descrição do sistema de resfriamento de emergência (CONF.). São Paulo: CTMSP, 2004a.

[26] TAKESHI, R.V.R. Sistema de resfriamento de emergência – fluxograma de engenharia (CONF.). São Paulo: CTMSP, 2004b.

[27] TAKESHI, R.V.R. Sistema de resfriamento de emergência – fluxograma de processo (CONF.). São Paulo: CTMSP, 2004c.

[28] OLIVEIRA, P.S.P.; JAQUES SAUER, M.E.L.; VIEIRA NETO, A.S.. Análise de confiabilidade do sistema de resfriamento de emergência da INAP (CONF.). São Paulo: IPEN, 2000.