AVALIAÇÃO DA METODOLOGIA ATHEANA PARA SUA UTILIZAÇÃO NA ANÁLISE DA CONFIABILIDADE HUMANA EM USINAS NUCLEARES

Paulo Cabrera Ambros

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 MESTRE EM CIÊNCIAS EM ENGENHARIA NUCLEAR.

Aprovada por:

_____
Prof. Roberto Schirru, D.Sc.

_____
Prof. Aquilino Senra Martinez, D. Sc.

_____
Dr. Ronaldo Célem Borges, D. Sc.

_____
Dr. Marco Antonio Bayout Alvarenga, D.Sc.

RIO DE JANEIRO, RJ – BRASIL
ABRIL DE 2005

AMBROS, PAULO CABRERA

Avaliação da Metodologia ATHEANA Para sua Utilização na Análise da Confiabilidade Humana em Usinas Nucleares. [Rio de Janeiro] 2005

XVIII, 162 p. 29,7 cm (COPPE/UFRJ, M.Sc., Engenharia Nuclear, 2005)

Tese – Universidade Federal do Rio de Janeiro, COPPE

1. ATHEANA
2. Análise de Confiabilidade Humana

I. COPPE/UFRJ II. Título (série)

"*As melhores pessoas podem cometer os piores erros*".

Dr. James Reason.

AGRADECIMENTOS

Ao Prof. Roberto Schirru, pela orientação e ajuda no desenvolvimento deste trabalho.

Ao Dr. Marco Antonio Bayout Alvarenga por ter mostrado o início do caminho que resultou neste trabalho.

Ao amigo John Wreathall pelo incentivo e suporte recebido.

Aos amigos da US-Nuclear Regulatory Commission, Susan E. Cooper, Deny Ross e John V. Kauffman pelo suporte recebido.

Ao amigo Oliver Sträter, do GRS, pela ajuda recebida.

Aos amigos e colegas de COPPE e de trabalho Alexandre, Herculano e Jefferson, pelas longas discussões e conversas sobre o tema.

Aos funcionários do Programa de Engenharia Nuclear pelo carinho e atenção dispensados.

À minha irmã Adalgiza pelo incentivo e apoio recebidos.

Às minhas filhas, Tatiana e Vanessa, pela esperança da chegada deste dia.

Aos meus pais pelo conforto espiritual.

À minha mulher, Izaura, pela compreensão das ausências e pelo incentivo sempre recebido.

A Deus, por tudo.

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

AVALIAÇÃO DA METODOLOGIA ATHEANA PARA SUA UTILIZAÇÃO NA ANÁLISE DA CONFIABILIDADE HUMANA EM USINAS NUCLEARES

Paulo Cabrera Ambros

Abril/2005

Orientador: Roberto Schirru

Programa: Engenharia Nuclear

Esta tese tem por objetivo apresentar uma avaliação qualitativa da metodologia ATHEANA (*A Technique for Human Error Analysis*) de Análise da Confiabilidade Humana (ACH) de segunda geração, apresentando as suas bases técnicas e as principais características que a diferenciam dos métodos tradicionais de ACH, bem como, uma avaliação de sua utilização na análise da confiabilidade humana nas usinas nucleares da Central Nuclear Almirante Álvaro Alberto, em Angra dos Reis, pois se trata de uma nova técnica que está, ainda, em desenvolvimento. ATHEANA é uma metodologia multidisciplinar que alterou os conceitos de falha humana baseada em eventos operacionais. Ela considera os contextos não usuais criados em situações de acidentes em usinas nucleares de potência, associados com fatores centrados no homem, relativos a estes contextos, os quais predispõem o operador a executar uma ação inadequada (erro de comissão) que degrada as condições de segurança da planta. Esta nova interpretação também modifica a representação do risco relativo à ação humana a qual não está, devidamente, representada nas análises probabilísticas de segurança.

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

EVALUATION OF ATHEANA METHODOLOGY FOR ITS USE IN HUMAN RELIABILITY ANALYSIS IN NUCLEAR POWER PLANTS

Paulo Cabrera Ambros

April/2005

Advisor: Roberto Schirru

Department: Nuclear Engineering

This work presents a qualitative evaluation of ATHEANA (A Technique for Human Error Analysis), a second-generation Human Reliability Analysis (HRA), its technical basis and the main differences from current HRA, as well as, an evaluation of its use in HRA at Angra 1 and Angra 2 Nuclear Power Plants, in Angra dos Reis, Brazil, as a new HRA technique, which is still under development. ATHEANA is a multidisciplinary methodology that has changed the human failure concepts based on operational events. It considers the abnormal context created by the accident scenarios at nuclear power plant, associated with human-centered factors related to these contexts, which set up the operator to take an inappropriate action (error of commission) that aggravates the plant condition. This new interpretation also modifies the human risk representativeness that is not adequately considered in current probabilistic risk analysis.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

LISTA DE ABREVIATURAS

AAE/AAA	Água de alimentação de Emergência/Água de alimentação auxiliar
AC	Corrente alternada (Alternative Current)
ACH	Análise de confiabilidade humana
ACRS	Advisory Committee on Reactor Safeguards
AEOD	Departamento de análise e avaliação de dados operacionais da NRC (Office of Analysis and Evaluation of Operational Data)
APS	Análise Probabilística de Segurança (Probabilistic Risk Assessment)
ASEP	Programa de Avaliação da Seqüência de Acidente (Accident Sequence Evaluation Program)
ATHEANA	Uma Técnica para Análise de Eventos Causados pelo Homem (A Technique for Human Event Analysis)
ATWS	Transiente previsto sem o desligamento do reator (Antecipated Transient Without Scram)
CAHR	Avaliação Conexionista da Confiabilidade Humana (Connectionism Assessment of Human Reliability)
CCF	Falha de modo comum (commom-cause failure)
CD	Dano ao núcleo (core damage)
CDF	Frequência de dano ao núcleo (Core Damage Frequency)
CREAM	Método de Análise de Confiabilidade e Erros Cognitivos (Cognitive Reliability and Error Analysis Method)
DC	Corrente contínua (Direct Current)
EFC	Contexto que força ao erro (Error-forcing context)
EFW/AFW	Água de alimentação de emergência (Emergency feed water/ Auxiliary feed water).
EI	Evento inicial
EOC	Erro de comissão (Error of commission)
EOO	Erro de omissão (Error of Omission)

EPRI	Instituto de Pesquisa de Potência Elétrica (Electric Power Research Institute)
ESF	Dispositivos de engenharia relacionados a segurança (Engineered Safety Features)
ERV	Válvula de alívio do pressurizador (Emergency relief valve) (outra denominação para a PORV)
F & B	Enchimento e esvaziamento (Feed and Bleed)
HAZOP	Estudo de Perigos e Operabilidade (Hazard and Operability Study)
HCR	Confiabilidade cognitiva humana (Human Cognitive Reliability)
HEART	Um Método de Banco de Dados para Acessar e Reduzir o Erro Humano (A Data-base Method for Assessing and Reducing Human Error)
HEP	Probabilidade de Erro Humano (Human Error Probability)
HERMES	Métodos de Confiabilidade de Erro Humano para Seqüências de Eventos (Human Error Reliability Methods for Event Sequences)
HFE	Evento de falha humana (Human failure event)
HPI	Injeção de alta pressão (Hi-pressure injection)
HRA	Análise de confiabilidade humana (Human Reliability Assessment)
HSECS	Esquema de classificação de evento de sistema humano (Human System Event Classification Scheme)
HVAC	Sistema de aquecimento, ventilação e ar condicionado (Heat, Ventilation and Air Conditioning).
IDA	Método do Diagrama de Influência (The Influence Diagram Approach)
IHM	Interface homem-máquina (Human-system interface)
IPE	Análise Individual da Planta (Individual Plant Examination)
LOCA	Acidente de perda de refrigerante do primário (Loss of coolant accident)
MERMOS	Métodos de Avaliação da Realização de Missões dos Operadores para Segurança (Méthode d'Evaluation de la Réalisation des Missions Opérateurs pour la Sûreté)
MFW	Água de alimentação principal (Main feed water)

MSIV	Válvula de isolamento de vapor principal (Main Steam Isolation Valve)
NPP	Usina Nuclear de Potência (Nuclear Power Plant)
NRC	Órgão Regulatório Americano (Nuclear Regulatory Commission)
OAT	Árvore de Ação dos Operadores (Operator Action Trees)
ORE	Experiência de confiabilidade do operador (Operator Reliability Experiment)
PIF	Fatores de influência no desempenho (Performance Influencing Factors).
POE	Procedimento de Operação de Emergência
PORV	Válvula de alívio do pressurizador operada a potência (Power Operated Relief Valve) (Outra denominação para a ERV)
PSF	Fatores que formatam o desempenho (Performance shaping factors)
PZER	Pressurizador (Pressurizer)
RFAS	Relatório Final de Análise de Segurança
SHARP	Procedimento de Confiabilidade da Ação Humana Sistematizada (Systematic Human Action Reliability Procedure)
SLIM	Metodologia do Índice da Probabilidade de Sucesso (Success Likelihood Index Methodology)
SLIM-SAM	Módulo de Avaliação do SLIM (SLIM Assessment Module)
SLIM-SARAH	Análise de sensibilidade do SLIM para a análise de confiabilidade de humanos (SLIM Sensitivity Analysis for Reliability Assessment of Humans)
SPR	Sistema de Proteção do Reator
SRR	Sistema de Refrigeração do Reator (RCS, Reactor Coolant System)
SWS	Sistema de água de serviço (Service Water System)
TESEO	Técnica Empírica para Estimar Erros dos Operadores (Técnica Empirica Stima Errori Operatori)
THERP	Técnica para Previsão de Taxa de Erro Humano (Technique for Human Error Rate Prediction)

TMFW	Desarme do sistema de água de alimentação principal (Trip Main Feed Water)
TMI-2	Usina Nuclear de Three Mile Island Unidade 2 (Three Mile Island NPP Unit 2)
UA	Ação insegura (unsafe action)

Capítulo 1

INTRODUÇÃO

1.1 Considerações

Eventos operacionais em usinas nucleares de potência (NPP, Nuclear Power Plant) foram e sempre serão consideradas ocorrências indesejáveis, danosas e altamente prejudiciais à continuidade da política de produção de energia elétrica a partir da energia nuclear liberada pela fissão do núcleo do urânio.

Neste contexto, o fator humano destaca-se como o maior contribuidor para as falhas que levaram a ocorrência de eventos de sérias proporções. Acidentes nucleares, mundialmente, conhecidos e analisados (NUREG/CR-6265, 1995, NUREG-1624, Rev.1, 2000) como o de Three Mile Island NPP, Unidade 2 (TMI-2), nos Estados Unidos, em 1979 e Chernobyl, Unidade 4, na Ucrânia, União Soviética, em 1986, mostraram deficiências na área de fatores humanos, que concorreram decisivamente para o agravamento do evento.

Acidentes por falha humana não são prerrogativas da área nuclear. Eventos nas áreas de petroquímica (REASON, 1990) (Bhopal, Índia, 1987: vazamento de gás venenoso matou certa de 2000 pessoas), de aviação (COLAS, 1997) (Tenerife, 1977: colisão de 2 boings 747, na pista, devido à falha de comunicação entre a torre e a equipe de terra onde morreram 570 pessoas) e de outras indústrias de alta tecnologia foram sempre uma grande preocupação. Todos eles enfrentam as mesmas dificuldades: como fazer o ser humano não errar ou errar menos.

Ao contrário da evolução tecnológica, onde a melhoria dos materiais e processos obedece a um aperfeiçoamento relativamente gradual e crescente e que pode ser avaliado e melhorado, o comportamento e o aperfeiçoamento do ser humano apresentam dificuldades e complexidades variadas porque o mesmo é único e sofre

influências adversas e imprevisíveis do meio em que vive, as quais tem influência direta no seu comportamento.

Sendo assim, a partir de TMI-2, além das melhorias nas áreas de interface homem-máquina, ergonomia, avaliação da experiência operacional, estruturação dos procedimentos operacionais de emergência, métodos de treinamento e processos de ajuda aos operadores, todas estas centradas no homem, para aprimorar e facilitar as decisões dos operadores, o ser humano passou a ser motivo de um profundo estudo para se conhecer suas condições psicológicas que o levam a cometer estas ações inadequadas. Várias disciplinas (NUREG 1624, Rev. 1, 2000), a princípio, de forma independente, e, posteriormente, de uma maneira integrada, intensificaram suas pesquisas para determinar e tentar eliminar ou diminuir, os motivos que levam o ser humano a cometer ações inadequadas levando a eventos indesejados.

Vários pesquisadores contribuíram para identificar e analisar a natureza do erro humano. Jens Rasmussen publicou vários estudos sobre o comportamento humano no período de 1974 a 1987, que foram utilizados por James Reason para descrever um amplo aspecto deste comportamento. O próprio James Reason publicou, desde 1974, estudos sobre o erro humano e que foram intensificados a partir de 1979. Seu livro, "*Human Error*" (REASON, 1990) tem sido uma referência básica importante para quem se inicia no estudo do erro humano, o qual é citado por vários autores e pesquisadores.

Paralelamente ao estudo das causas dos erros humanos, a análise da confiabilidade humana utilizada na avaliação probabilística de risco, também chamada de avaliação probabilística de segurança (APS), teve um impulso muito importante. Era preciso considerar adequadamente a confiabilidade humana para poder quantificar, mais realisticamente, o risco associado com a operação das usinas nucleares para determinar se o mesmo seria aceitável e, também, onde colocar melhoramentos para reduzí-lo a valores tão baixo quanto possível.

Neste sentido (REASON, 1990), numerosas técnicas (mais de 30) aparecerem até o início da década de 1990. Todas elas apresentavam elementos comuns, mas não eram exatamente iguais. Entretanto, um número, relativamente, pequeno destas técnicas foram aplicadas nas avaliações de risco. As mais conhecidas e, de certa maneira, mais utilizadas e estudadas são: THERP (Technique for Human Error Rate Prediction) (SWAIN & GUTTMANNN, 1983), ASEP (Accident Sequence Evaluation Program) (SWAIN, 1987), SLIM (Success Likelihood Index Methodology) (EMBREY *et al.*, 1984), SHARP (Systematic Human Action Reliability Procedure) (EPRI TR-100259, 1992), OAT (Operator Action Trees) (NUREG/CR-3010, 1982, WREATHALL, 1982), TESEO (Tecnica Empirica Stima Errori Operatori) (BELLO, 1980), Confusion Matrix (POTASH *et al.*, 1981), IDA (The Influence Diagram Approach, também conhecida como A Sociotechnical Approach to Assessing Human Reliability) (PHILLIP *et al.*, 1990), HEART (A data-based method for assessing and reducing human error to improve operational performance) (WILLIAMS, 1988). Entretanto, nenhuma delas considerava, adequadamente, um tipo de erro humano, denominado *erro de comissão*, o qual altera, significativamente, a sequência do acidente e que foi observado em vários eventos importantes.

1.2 Experiência Operacional

Uma das várias lições aprendidas do acidente de TMI-2, foi a análise e utilização da experiência operacional como elemento de realimentação de melhorias para evitar recorrências dos eventos indesejados.

Neste contexto, tanto a análise deste evento (TMI-2) como as de outros eventos importantes para a segurança revelaram (NUREG 1624, Rev. 1, 2000) uma substancial diferença no desempenho humano em relação àqueles representados pelos modelos atuais de Avaliação Probabilística de Segurança (APS) . Este último, quase sempre considera falhas em executar determinados itens de um procedimento,

denominados *erros de omissão*, ao passo que, as análises dos eventos operacionais reais têm mostrado que os problemas de desempenho humano envolvem os operadores executando ações, não requeridas pelos procedimentos de resposta ao acidente, e que pioraram as condições da planta. Estes erros são denominados *erros de comissão*, ou seja, ações inadequadas realizadas conscientemente pelo operador porém baseadas em avaliações erradas das condições da planta.

As análises iniciais do acidente de TMI-2 e de Chernobyl (NUREG 1624, Rev. 1, 2000) desconsideraram estes tipos de erros, pois os mesmos davam a impressão de serem ações ilógicas e incabíveis e trataram como uma deficiência operacional específica da planta, ao invés de reconhecer como uma deficiência de preocupação geral para todas as usinas.

Esta deficiência foi constatada mais tarde (NUREG 1624, Rev. 1, 2000) quando, apesar de todas as melhorias, relativas ao fator humano, introduzidas a partir de TMI-2, verificou-se que o mesmo tipo de erro continuava ocorrendo. Em 1995, um estudo (AEOD/E95-01, 1995) do órgão regulador americano (NRC, Nuclear Regulatory Commission), identificou que esta deficiência (ver Anexo A) também ocorreu em vários outros eventos (14 eventos ocorridos num período de 41 meses), onde o operador, intencionalmente, executou a ação de desligar ou impedir o funcionamento de um equipamento que perfaz uma função segurança, baseada numa avaliação incorreta das condições da usina. Em TMI-2 (NUREG 1624, Rev. 1, 2000), os operadores desligaram, indevidamente, as bombas de injeção de segurança de alta pressão, para evitar que o pressurizador tornasse-se sólido (totalmente cheio de água) resultando em uma drástica redução do resfriamento e causando sério dano ao núcleo do reator (fusão parcial).

A NRC concluiu, em seu relatório (AEOD/E95-01, 1995), que estes eventos e outros similares mostravam que este tipo de intervenção do operador (erro de

comissão) pode ser um importante modo de falha humana e que os mesmos são precursores de eventos mais sérios.

A partir desta constatação, a NRC (NUREG 1624, Rev. 1, 2000) passou a desenvolver uma metodologia de análise de confiabilidade humana de segunda geração denominada ATHEANA*, A Technique for Human Event Analysis*, *(Uma técnica para análise de eventos causados pelo homem)*, que procura identificar e quantificar estas situações, para que as APS's possam representar, mais realisticamente, o risco introduzido pelo homem.

Diversos outros especialistas, em diferentes países, também realizaram estudos semelhantes e desenvolveram metodologias para a sua análise, como por exemplo na França, EDF (MERMOS- Méthode d'Evaluation de la Réalisation des Missions Opérateurs pour la Sûreté) (BIEDER *et al.*, 1998), na Alemanha, Sträter and Bubb (CAHR- Connectionism Assessment of Human Reliability) (STRÄTER, *et al.*, 1998), na Itália, Cacciabue *et al.* (HERMES- Human Error Reliability Methods for Event Sequences) (CACCIABUE *et al.*, 1996) e na Dinamarca, Erik Hollnagel (CREAM- Cognitive Reliability and Error Analysis Method) (HOLLNAGEL, 1988) e outros. Todos estes métodos procuram, de alguma maneira, modelar aspectos específicos do processo cognitivo do operador ou da equipe de operadores e o contexto em que os mesmos estão inseridos. No desenvolvimento da ATHEANA foram utilizados vários conceitos e desenvolvimentos dos métodos acima, assim como uma participação, mesmo que parcial, de seus autores.

1.3 Objetivo e motivação

O objetivo deste trabalho é apresentar um estudo detalhado e uma análise da metodologia ATHEANA, sob o ponto de vista qualitativo, para avaliar as suas vantagens e desvantagens, tentar identificar suas fraquezas e destacar seus pontos fortes; apresentar uma análise global do método, para identificar suas lacunas e

vantagens. Verificar se é uma tecnologia que agrega segurança e se deve ter seu uso recomendado, e, finalmente, avaliar a aplicabilidade desta metodologia nas usinas nucleares de Angra dos Reis, Brasil.

O elemento motivador é a extrema relevância do assunto para a segurança operacional das usinas nucleares e o interesse despertado pela participação, inequívoca, do ser humano nos eventos operacionais e as consequências para o estudo da confiabilidade humana.

Eventos ocorreram e sempre ocorrerão. A máquina humana não é infalível. Não importa o quanto de automatismo pode ser colocado em uma usina, porque o elemento que a projetará, que fará a sua manutenção e que fará o seu uso, é o elemento humano.

É sabida e, de uma certa maneira, temida, a posição da opinião pública (não técnica e infundada) sobre usinas nucleares. Na hipótese de qualquer evento de proporções que vier a afetar o público ou o meio ambiente, não importa o lugar onde isto acontecer, será altamente maléfico e colocará em sério questionamento a continuação da geração de energia elétrica por usinas nucleares. Portanto, quanto mais próximo da realidade estiverem as estimativas dos riscos associados e as consequentes melhorias para a sua redução, mais segura estará a operação destas usinas.

1.4 Estrutura da tese

A descrição da tese foi estruturada da seguinte maneira:

O capítulo 2 faz considerações sobre os modelos atuais de APS, destacando as suas partes básicas, e sobre a contribuição humana para o risco.

O capítulo 3 apresenta uma revisão metodológica dos principais processos, atualmente existentes, de análise de confiabilidade humana.

O capítulo 4 apresenta as bases, características e os processos da metodologia ATHEANA, conforme descrito no NUREG-1624, Rev. 1 (2000), incluindo os processos de análise retrospectiva e prospectiva.

O capítulo 5 apresenta uma avaliação qualitativa da metodologia ATHEANA, onde é analisada a utilidade da mesma, apresentando as suas vantagens e desvantagens, dificuldades de aplicação e uma análise de outros trabalhos apresentados sobre o assunto.

O capítulo 6 apresenta as conclusões e faz uma abordagem da aplicação desta metodologia nas usinas nucleares Angra 1 e Angra 2.

O Anexo A apresenta alguns eventos operacionais importantes, resultado do estudo especial (AEOD/E95-01, 1995), onde foram identificados erros de comissão que foram considerados importantes modos de falha e precursores de acidentes sérios.

O Anexo B apresenta uma ilustração dos princípios da ATHEANA identificados nas análises de eventos ocorridos.

O Anexo C apresenta o resultado da análise retrospectiva do acidente de TMI-2, ilustrando toda a documentação gerada por este tipo de análise.

Capítulo 2

AVALIAÇÃO PROBABILÍSTICA DE SEGURANÇA

2.1 Introdução

O NUREG/CR-6823 (2003) cita, na página 1-1, que a avaliação probabilística de risco, também chamada de análise probabilística de segurança (APS), é uma tecnologia que já se encontra bem amadurecida e que pode fornecer uma avaliação quantitativa do risco de acidentes em usinas nucleares de potência. A mesma envolve o desenvolvimento de modelos que delineiam a resposta dos sistemas e dos operadores ao evento iniciador do acidente.

Segundo REASON (1990), a estrutura geral da APS foi estabelecida em 1975 (NUREG-75/014, 1975) com a publicação de um estudo de segurança de reatores, nos Estados Unidos, constituído por cerca de 10 quilos de documentos, denominado WASH-1400, com o seguinte título: *"An Assessment of Accident Risk in U.S. Commercial Nuclear Power Plants"*. Entretanto, a partir de TMI, as APS's tiveram um notável desenvolvimento.

A revisão do modelo de APS descrita a seguir, está baseada no NUREG-1624, Rev. 1 (2000), a qual tem a intenção de servir como base para o entendimento de como o modelo atual de APS precisa ser modificado para incorporar as inovações da metodologia ATHEANA.

Atualmente, existe uma considerável variedade nos detalhes de como os diferentes analistas constroem um modelo de APS para representar os acidentes severos nas usinas nucleares de potência. Entretanto, as APS's, comumente, usam um modelo lógico indutivo denominado "*árvore de eventos*", em combinação com um modelo dedutivo, denominado "*árvore de falhas*".

A "*árvore de eventos*" (fig. 2.1) é uma representação gráfica de uma possível sequência de eventos que pode acontecer após a ocorrência de algum desafio inicial à planta, denominado "*evento iniciador*". Estas sequências são representadas por dois estados: sucesso ou falha das funções ou sistemas que são importantes em mitigar as consequências do evento iniciador, normalmente, consideradas como dano ao núcleo (CD, core damage). Ela responde à seguinte pergunta: ***"O que pode acontecer se ocorrer uma determinada falha ou evento?"*** (por exemplo, a perda da função de água de alimentação de emergência).

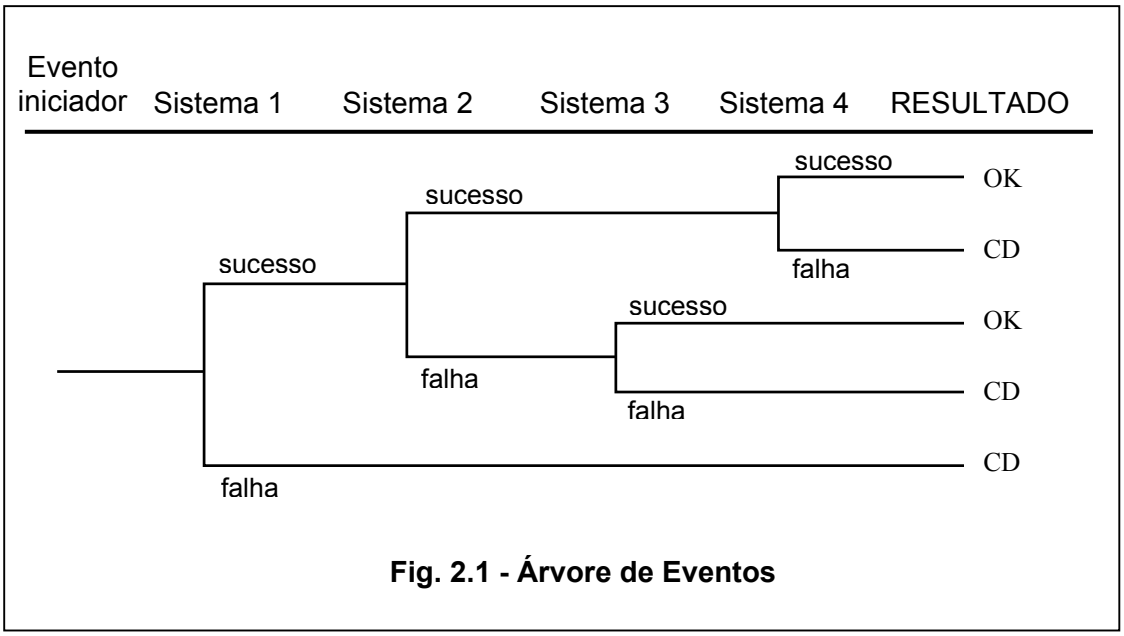


Fig. 2.1 - Árvore de Eventos

As *"árvores de falhas"* (fig. 2.2) são representações gráficas, comumente, utilizadas para modelar a resposta da planta a nível de componentes. São modelos dedutivos que representam as combinações de falhas de equipamentos que precisam ocorrer para falhar a função ou sistema de interesse da árvore de eventos. Ela responde à seguinte pergunta: ***"Como pode ocorrer um determinado tipo de falha?"*** (por exemplo, como a função de água de alimentação de emergência pode falhar?).

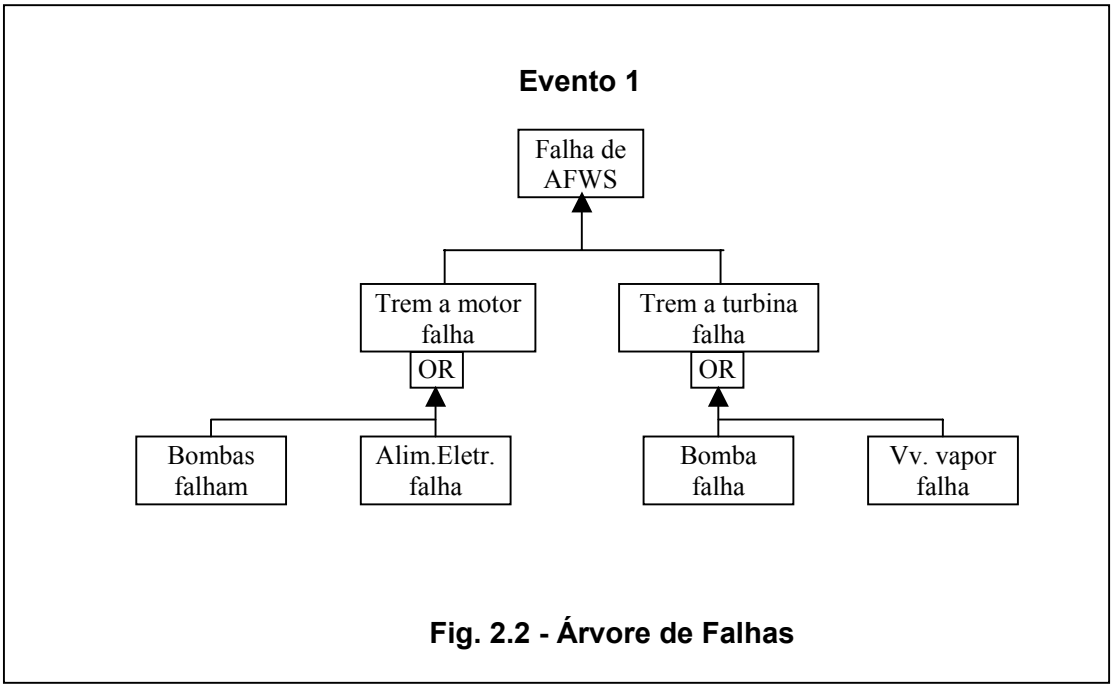


Fig. 2.2 - Árvore de Falhas

As APS's possuem dois objetivos: primeiro, identificar áreas de riscos potenciais significativos e indicar como podem ser feitas melhorias; segundo, quantificar o risco global de um perigo potencial na planta.

Quantificar a APS significa calcular a freqüência da sequência dos eventos que leva a dano ao núcleo. Inicialmente, são determinadas as probabilidades de falha das funções ou dos sistemas do modelo. As combinações destas probabilidades com a frequência esperada do evento iniciador determinam as frequências das sequências

indesejadas que levam a dano ao núcleo. A falha de cada função ou sistema pode ser por diversas causas, designados eventos básicos. O resultado do processo de cálculo fornece uma série de expressões, cada uma feita pelo produto da frequência do evento iniciador pela probabilidade dos vários eventos básicos de cada sequência de falhas, que juntas levam a dano ao núcleo. Cada expressão é chamada de corte (cut set) e cada corte tem uma freqüência associada. Combinando as frequências de cada corte relacionado com uma determinada sequência obtém-se a frequência global para aquela sequência. Combinando as frequências de todas as sequências obtém-se a taxa global esperada, usualmente expressa como uma probabilidade de ocorrência por ano, de dano ao núcleo.

2.2 Tratamento da falha humana nas APS's atuais

As APS's atuais podem, tipicamente, incorporar os eventos de falha humana em quatro lugares diferentes: nos eventos iniciadores, árvores de eventos, árvores de falhas e na recuperação da ação inadequada. Estes estão mostrados na figura 2.4 onde estão destacadas as interfaces da modelagem humana com o modelo básico da APS. A figura 2.3 destaca o modelo básico da APS antes desta inclusão.

2.2.1 Falha humana nos eventos iniciadores

O primeiro lugar, na estrutura da APS, onde os eventos de falha humana podem ser incluídos, é na identificação dos eventos iniciadores e de suas respectivas frequências. Os eventos iniciadores incluem desafios à planta tais como desarmes da turbina, perda de água de alimentação principal, ruptura de tubos dos geradores de vapor, perda de refrigerante do reator (LOCA, loss of coolant accident), terremotos,

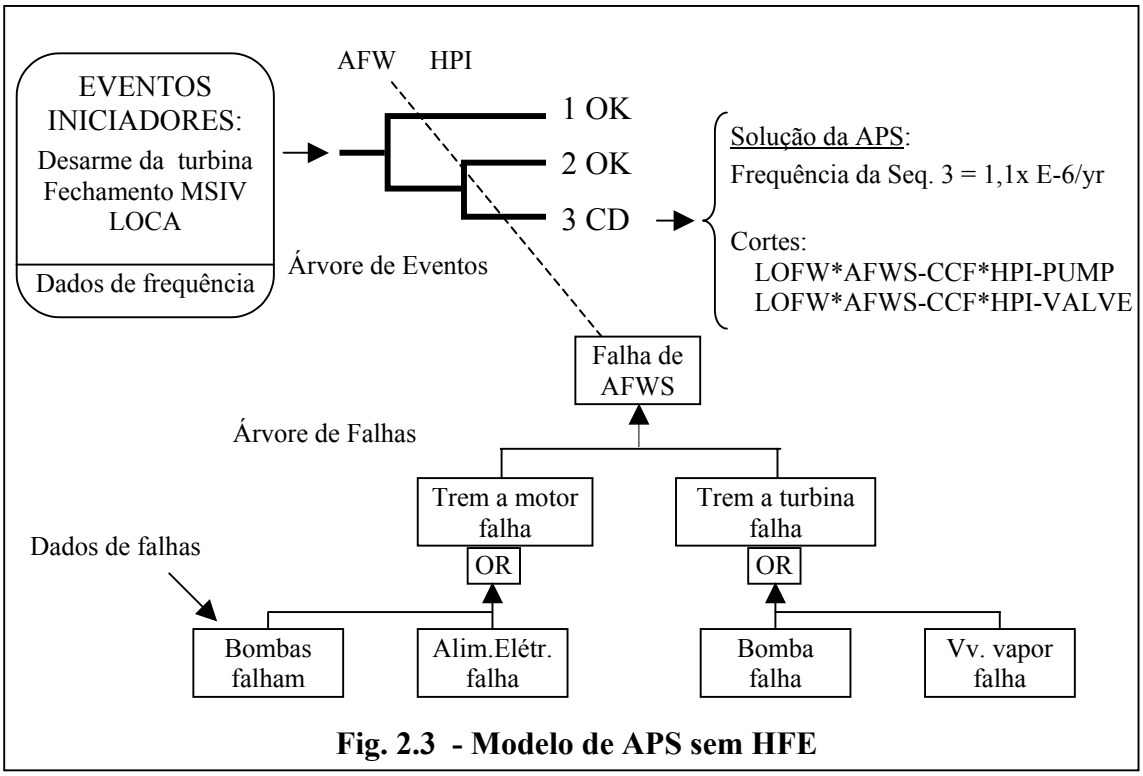


Fig. 2.3 - Modelo de APS sem HFE

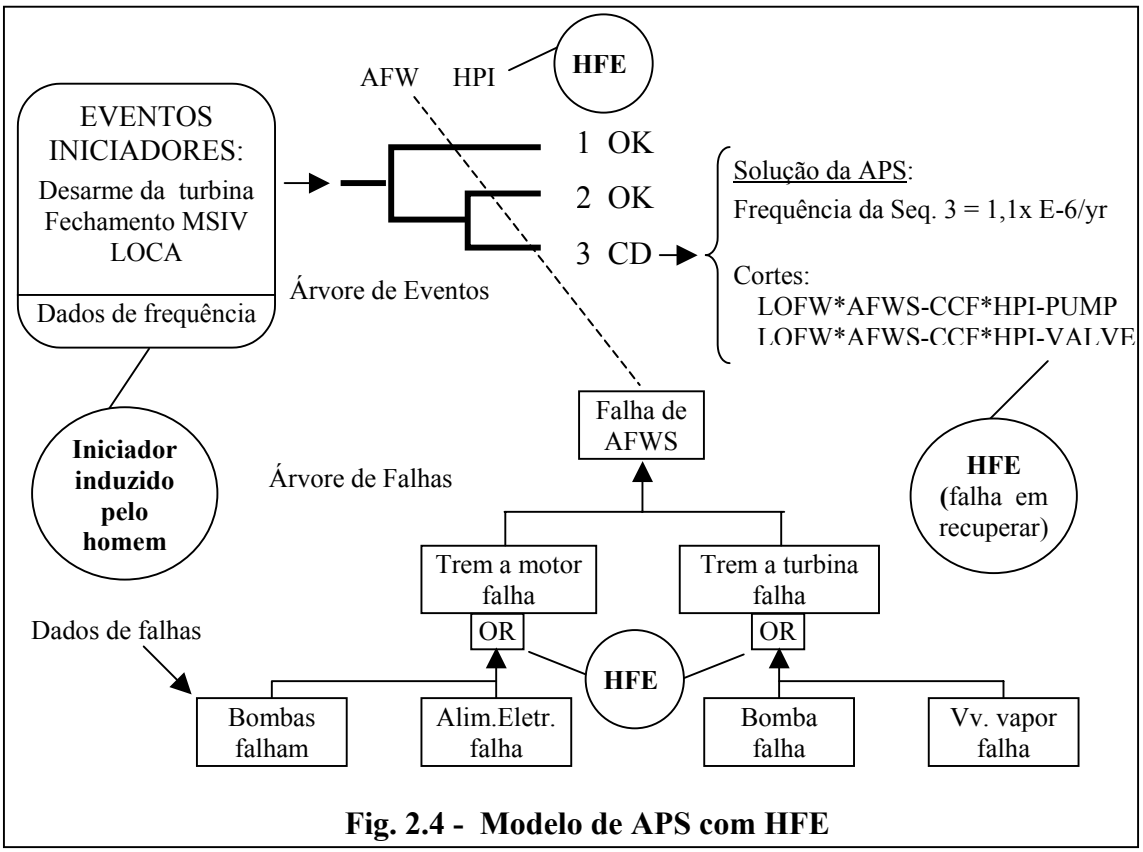


Fig. 2.4 - Modelo de APS com HFE

etc. Muitos destes podem ser induzidos por falhas humanas. Entretanto, como as frequências de tais eventos iniciadores, induzidos por falha humana, são considerados na frequência de cada classe de possíveis iniciadores, muitas das vezes estes eventos não são, especificamente, modelados nas APS's. Isto é devido, basicamente, a três motivos:

1) é assumido (mesmo implicitamente) que existe pequena ou nenhuma dependência entre a causa do evento iniciador e como os operadores da planta responderam aos eventos subsequentes;
2) dependendo do escopo e do objetivo da análise, usualmente, o analista de APS requer, somente, a frequência do evento iniciador, não precisando saber "porque" ou "como" o evento iniciou; e
3) nas APS's de usinas em potência, a contribuição humana para os iniciadores é, frequentemente, considerada ser pequena, se comparada com falhas de equipamentos.

2.2.2 Falha humana nas árvores de eventos

Muitas vezes, as árvores de eventos das APS's, explicitamente, indicam os eventos de falha humana (representando ações dos procedimentos) (fig. 2.5). Porém, não existe nenhuma regra ou padrão aceito pela indústria, de quando incluir tais eventos na estrutura das árvores de eventos. Entretanto, isto é feito, usualmente, quando a ação humana de interesse é uma parte chave das numerosas sequências da árvore de eventos e a ação não está, particularmente, associada com um sistema ou equipamento específico, mas, ao invés, tem uma repercussão funcional em relação se existe uma recuperação com sucesso ou se ocorre dano ao núcleo. Algumas vezes, tais eventos devem ser incluídos nas árvores de eventos para destacar o evento de falha humana como uma parte, potencialmente, importante na sequência completa dos eventos que podem ocorrer. Nas APS's atuais, estes eventos de falha humana quase

sempre envolvem erros de omissão, onde uma ação simples tem um efeito direto na progressão do acidente tais como na despressurização do sistema primário para permitir resfriamento por enchimento e drenagem (feed and bleed) ou quando ocorrer ruptura de tubos dos geradores de vapor, etc.

2.2.3 Falha humana nas árvores de falhas

Tais eventos de falha humana podem ser modelados (bem parecidos com falhas de componentes dentro de sistemas), adequadamente, nas árvores de falhas, se a ação de interesse está facilmente associada com um sistema ou equipamento específico da planta e a falha desta ação pode contribuir para a falha do sistema ou do equipamento em realizar a sua função (fig.2.6). Aqui, o analista tenta definir todos os modos, nos quais as falhas humanas podem contribuir para a falha do sistema ou do equipamento de interesse e estimar a probabilidade desta falha, eventualmente, no contexto de cada sequência na qual a falha deste sistema ou equipamento participa. Os eventos de falhas humanas, nas árvores de falhas, tendem a incluir o seguinte:

- O chamado erro ou evento pré-iniciador que envolve omissões em atividades de manutenção, teste ou calibrações que deixam o equipamento em um estado de falha não detetada (*falha latente*), de maneira que o equipamento não pode responder adequadamente quando o evento iniciador ocorrer.
- Eventos pós-iniciador tais como mostrados na fig. 2.6 envolvendo omissões em responder à sequência de eventos após a ocorrência do evento iniciador.

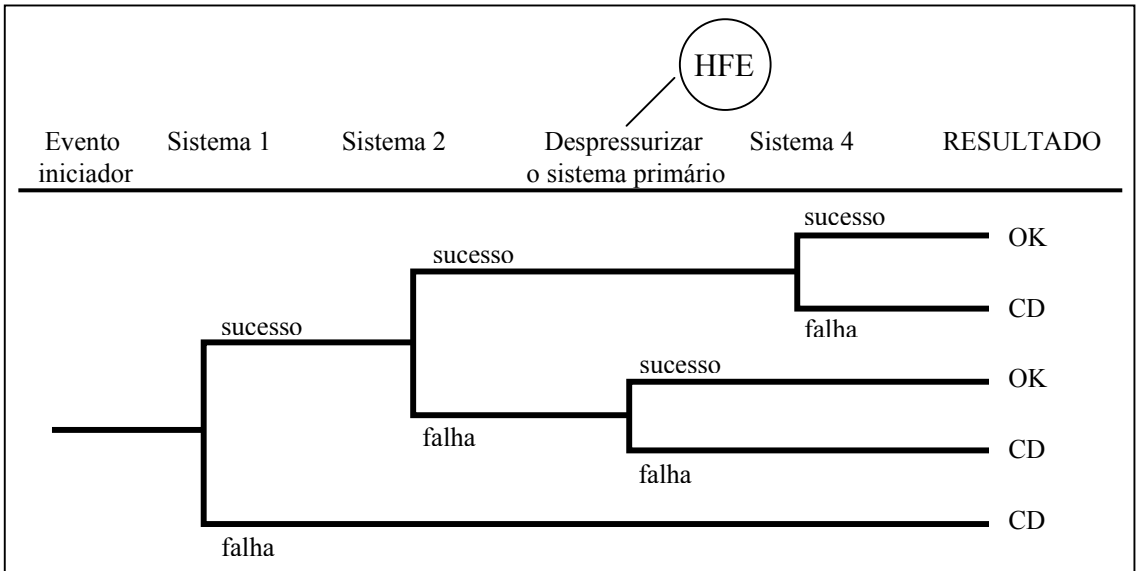


Fig. 2.5 – Ilustração de HFE nas Árvores de Eventos

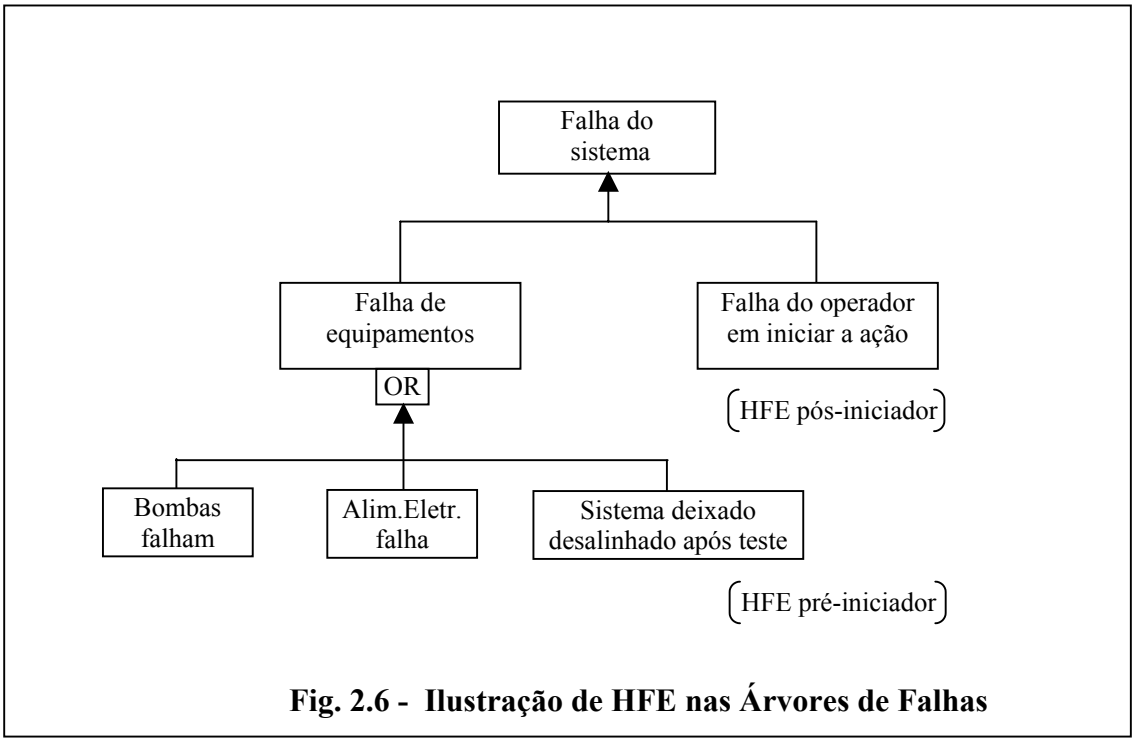


Fig. 2.6 - Ilustração de HFE nas Árvores de Falhas

2.2.4 Falha humana em realizar ações de recuperação

Ações de recuperação podem ser ou não estabelecidas nos procedimentos de operação de emergência. Estas ações são tomadas em resposta a uma falha de uma função requerida. Exemplos destes tipos de ações incluem recuperação do suprimento elétrico, partida manual de bomba que deveria ter partido automaticamente e re-enchimento do tanque de água de recarregamento, no evento de falha de recirculação do sistema de resfriamento de emergência do núcleo.

Nem todas as combinações de falhas de equipamentos que levam a dano ao núcleo podem ser predeterminados antes da solução do modelo. Por motivos de cálculos e de eficiência da modelagem, uma variedade de eventos com falhas na recuperação é incluída nos modelos de APS durante os estágios finais de quantificação. Isto envolve o exame, pelo analista, das sequências de cortes, derivadas das soluções do modelo da APS e, conforme a combinação de falhas em cada corte que leve a dano ao núcleo, o analista pode postular ações razoáveis de recuperação que podem ser tomadas pelos operadores, para mudar o resultado da sequência que leva a dano ao núcleo para o sucesso na mitigação do acidente. Falhas em realizar as ações de recuperação são incluídas nas APS's. Isto é feito pela inclusão de eventos representando tais falhas, nas sequências de cortes e desta maneira, considerando a probabilidade de que os operadores não serão capazes de achar uma maneira de evitar o resultado de dano ao núcleo pela execução de uma ação não, explicitamente, incluída no modelo original. Exemplo de falhas de recuperação de eventos e como elas são incluídas nos modelos de corte estão mostrados na fig. 2.7.

Sequência de corte sem considerar ações de recuperação:

TMFW * AFWS-CCF * HPI-CCF

TMFW * AFWS-CCF * SWS-CCF

TMFW * AFWS-HVAC * HPI-CCF

Sequência de corte considerando ações de recuperação:

TMFW * AFWS-CCF * HPI-CCF * OPER-DEP-COND

TMFW * AFWS-CCF * SWS-CCF (sem ação de recuperação)

TMFW * AFWS-HVAC * HPI-CCF * OPER-DOOR

Onde:

TMFW = iniciador; perda de água de alimentação principal

AFWS-CCF = falha de modo comum do AFWS

AFWS-HVAC = falha do AFWS devido a falha do HVAC

HPI-CCF= falha de modo comum de feed and bleed de alta pressão

SWS-CCF= falha de modo comum de água de serviço

OPER-DEP-COND = falha do operador em despressurizar e usar o condensador para alimentar os geradores de vapor

OPER-DOOR = falha do operador em abrir as portas da sala das bombas AFWS para ventilação.

MFW- água de alimentação principal (Main FeedWater)

AFWS- sistema de água de alimentação auxiliar (Auxiliary FeedWater System)

HPI- injeção de alta pressão (Hi Pressure Injection)

SWS- sistema de água de serviço (Service Water System)

HVAC- aquecimento, ventilação e ar condicionado (Heat, Ventilation and Air Conditioner).

Figura 2.7 - Ilustração de falha em recuperar de um corte (cut set)

Capítulo 3

ANÁLISE DA CONFIABILIDADE HUMANA - ACH

3.1 Perspectivas das ações humanas

O NUREG-1150 (1990), que sumariza as análises de risco de 5 usinas nos Estados Unidos, cita que o desempenho humano tem sido visto como um fator dominante nos principais acidentes relacionados com a segurança em usinas nucleares de potência, tanto nos Estados Unidos quanto em outros lugares. Exemplos incluem eventos tais como Three Mile Island Unit 2, Davis-Besse e Oyster Creek, nos Estados Unidos e Chernobyl, na União Soviética. Em cada um destes, uma interação complexa entre o operador e os equipamentos levaram a eventos, significativamente, perigosos e, em dois casos, a liberação de radioatividade para a atmosfera. Deficiências no desempenho humano ocorreram tanto antes do início do evento, em áreas tais como manutenção, treinamento e planejamento, quanto em resposta ao evento.

Igualmente, o NUREG-1560 (1996), que revisou 75 relatórios de Análise Individual de Plantas (IPE, Individual Plant Examination) de 108 usinas norte-americanas identificou que, devido ao papel realizado pelos operadores em manter e operar usinas nucleares de potência e de reconhecer e responder a eventos que podem levar a dano ao núcleo e riscos para o meio-ambiente, um aspecto importante da avaliação da segurança operacional de usinas nucleares é a identificação das ações humanas importantes na prevenção e mitigação de acidentes severos.

O objetivo da análise da confiabilidade humana (ACH), segundo o NUREG-1560 (1966) é identificar e avaliar aquelas ações humanas relevantes para o acidente em análise. Dado o alto grau de confiabilidade dos equipamentos e das redundâncias, a interface humana tornou-se um aspecto crítico em causar, prevenir e mitigar

acidentes. Neste contexto, a análise da confiabilidade humana é esperada ser um dos componentes importantes da avaliação probabilística de risco. A incorporação das ações humanas nos modelos de árvores de eventos e árvores de falhas e a quantificação de suas probabilidades de falhas podem ter um impacto importante nos resultados estimados da frequência de dano ao núcleo (CDF, Core Damage Frequency). Análises realizadas indicaram que, não somente os erros humanos podem significar importantes contribuidores para a CDF, mas que a ação humana correta pode reduzir, substancialmente, o CDF total. A finalidade deste capítulo é dar uma revisão dos métodos de ACH mais conhecidos.

3.2 Caracterização das ações humanas

Na avaliação do desempenho humano apresentada no NUREG-1150 (1990), diferentes tipos de erros humanos foram identificados. O primeiro é, geralmente, um erro onde uma ação intencional não é realizada, devido, usualmente, à falta de atenção, denominado de deslize (slip), ou a um lapso de memória ou esquecimento, (lapse). Exemplos deste tipo de erros envolvem o esquecimento (lapse), pelo operador, de executar um passo do procedimento ou, acidentalmente, acionar uma chave errada (slip). O segundo tipo de erro humano (mistake), caracterizado por um engano, é, geralmente, uma ação realizada, de acordo com um plano que é inadequado para a situação. O plano pode ser inadequado porque houve um erro em diagnosticar o tipo de evento ou porque o tipo de evento não foi considerado na preparação do plano e não é parte da experiência e treinamento do operador. O terceiro tipo de erro humano é o desvio deliberado, violação (violation), das práticas supostas necessárias para manter a segurança. Erros deste tipo podem ser rotineiros (como fazendo um atalho) ou excepcionais (como no caso de Chernobyl). Como descrito por REASON (1990), em Chernobyl, os operadores, deliberadamente,

infringiram rigorosos procedimentos de segurança e permaneceram operando a planta, com a potência do reator abaixo do valor mínimo permitido, de 20%. Esta e outras violações subsequentes dos procedimentos de segurança resultaram em duas explosões dentro do núcleo do reator as quais destruíram o prédio de contenção, liberando uma grande quantidade de material radioativo para o meio ambiente.

Os erros acima (slip, lapse e mistake) são classificados em erros de omissão (EOO, errors of omission) e em erros de comissão (EOC, errors of comission). Erro de omissão é quando não é feita a ação pretendida ou planejada e erros de comissão é quando é feita uma ação intencional que não deveria ter sido feita. Erros de omissão são, geralmente, deslizes e lapsos, e erros de comissão, podem ser deslizes e lapsos, mas os mais importantes são os enganos (mistakes). .

No capítulo anterior, Seção 2.2, foi mostrado que os eventos de falha humana são incorporados às APS's em quatro lugares diferentes. De uma maneira mais global, a abordagem tradicional das ACH's (NUREG-1560, 1996) separa as ações humanas em duas categorias básicas: ações pré-iniciador e ações pós-iniciador. As ações pós-iniciador são também, usualmente, sub-categorizadas em "ações de resposta" e "ações de recuperação".

A ações humanas pré-iniciador são aquelas que, se realizadas incorretamente ou no tempo indevido, podem tornar os sistemas ou a instrumentação indisponíveis para quando eles forem demandados para responder a um acidente (erros de omissão). Estas ações incluem, tipicamente, falhas em calibrar instrumentos e falhas em restabelecer, corretamente, a operabilidade dos sistemas, após manutenções e/ou testes.

As ações humanas pós-iniciador são aquelas requeridas em resposta a eventos iniciadores ou em recuperar falhas dos sistemas em responder a estes eventos. As ações pós-iniciador de resposta são geralmente distinguidas das ações pós-iniciador de recuperação, em que as ações de resposta são usualmente

direcionadas por procedimentos de operação de emergência. As ações humanas de resposta que são incluídas nas APS's são aquelas ações requeridas para, manualmente, iniciar, operar, controlar ou terminar a operação daqueles sistemas e/ou componentes necessários para prevenir e/ou mitigar o dano ao núcleo. As ações de resposta modeladas incluem, somente, aquelas ações necessárias para assegurar que os sistemas ou componentes satisfaçam os requisitos dos critérios de sucesso definidos para aqueles sistemas ou componentes nas análises de segurança. Por outro lado, as ações pós-iniciador de recuperação podem incluir a recuperação de sistemas falhados ou indisponíveis, a tempo de evitar consequências indesejáveis, usando os sistemas de maneira relativamente usual, ou, em alguns casos, indo além das ações prescritas nos procedimentos existentes. As ações de recuperação também podem incluir a utilização dos sistemas de forma relativamente diferente da usual. Entretanto, créditos para ações de recuperação não são realizados a não ser que, pelo menos alguma orientação, através de procedimentos, seja fornecida ou os operadores recebam, regularmente, treinamento que podem levá-los a executar as ações requeridas. Ações de recuperação também podem incluir o restabelecimento ou reparo de equipamentos falhados (falhas de hardware). Exemplos destes tipos de ações incluem recuperação do suprimento elétrico, partida manual de bomba que deveria ter partido automaticamente e re-enchimento do tanque de água de recarregamento no evento de falha de recirculação do sistema de resfriamento de emergência do núcleo.

3.3 Revisão da análise de confiabilidade humana

Devido ao fato de que muitos dos esforços de pesquisa no domínio da confiabilidade humana foram dirigidos para a quantificação da probabilidade de erros, um grande número (mais de 30) de técnicas foi criado (EMBREY, 1994a). Entretanto, somente um número relativamente pequeno destas foram de fato, aplicadas nas

avaliações de risco. Por esta razão serão apresentadas, resumidamente, como informação, somente cinco destas técnicas.

Deve-se destacar que o processo de quantificação deve ser precedido por uma rigorosa análise qualitativa, para assegurar que todos os possíveis erros, com consequências significativas para a segurança, sejam identificados. Se a análise qualitativa for incompleta, então a quantificação será incorreta. Também é preciso estar atento para a limitação da precisão dos dados, geralmente, disponíveis para a quantificação da confiabilidade humana.

3.4 O processo de quantificação

Segundo EMBREY (1994a), praticamente todas as técnicas de quantificação seguem os mesmos quatro estágios, descritos a seguir:

- Modelagem da tarefa;
- Representação do modelo de falha;
- Dedução da probabilidade de erro para os passos da tarefa;
- Combinação das probabilidades das tarefas elementares para obter a probabilidade global da tarefa.

3.4.1 Modelagem da tarefa

Envolve analisar a tarefa de interesse e identificar quais aspectos devem ser quantificados. Em alguns casos, o analista pode estar interessado na probabilidade de uma ação humana simples, como por exemplo "*qual é a probabilidade de que o operador da sala de controle fechará a válvula de suprimento de água dentro de 30 segundos após a atuação do alarme?"*

Em outros casos, o interesse é quantificar a tarefa como um todo. Por exemplo "*qual é a probabilidade de que a função de injeção de alta pressão operará como requerida?"* Neste caso, a quantificação pode ser conduzida em um nível global da

tarefa, como um todo ou então, a mesma pode ser desdobrada em tarefas elementares, onde cada uma é quantificada. A probabilidade global do sucesso ou insucesso da tarefa será a combinação das probabilidades das tarefas elementares.

Existem argumentos contra e a favor, tanto para a abordagem global como para abordagem da decomposição em tarefas elementares. As principais vantagens da abordagem da decomposição são:

- Pode-se utilizar bancos de dados existentes de probabilidades das tarefas elementares;
- Recuperações de erros dos passos das tarefas individuais podem ser modeladas;
- Consequências para outros sistemas advindas de falhas nos passos das tarefas individuais (por exemplo, os resultados de uma ação alternativa em oposição a, simplesmente, omissão de uma ação) pode ser modelada e incluída na avaliação;
- Efeitos de dependências entre os passos da tarefa podem ser modelados.

Defensores da abordagem global argumentam que as atividades humanas são, essencialmente, direcionadas para o objetivo (goal-directed, isto é, considerações cognitivas) e que isto não pode ser capturado por uma simples decomposição da tarefa em seus elementos. Eles também afirmam que, se a intenção está correta (baseado no diagnóstico da situação) então os erros de omissão das ações baseadas na habilidade (skill-based actions) serão improváveis porque o retorno da informação fornecerá, constantemente, uma comparação entre o esperado e os resultados reais obtidos. Deste ponto de vista, o foco seria na confiabilidade da ação cognitiva (planejamento da resposta) ao invés dos elementos da ação da tarefa.

Na grande maioria, muitas das quantificações empregam a abordagem da decomposição, por um lado, porque a maioria dos engenheiros se sente mais confortável com a abordagem da análise e a síntese e, por outro lado, porque o

modelo mecanicista do desempenho humano foi a base para muitos dos trabalhos de avaliação da confiabilidade humana.

3.4.2 Representação do modelo de falha

Se o modelo da decomposição for usado, é necessário representar uma maneira pela qual, as várias atividades elementares e outras falhas possíveis são combinadas para dar a probabilidade de falha da tarefa como um todo. Geralmente, a forma mais comum de representação é a árvore de eventos. Isto é a base para a metodologia THERP (SWAIN & GUTTMANN, 1983), que será descrita a seguir. Árvores de falhas são usadas, somente, quando as probabilidades discretas de erro humano são combinadas com as probabilidades de falhas de equipamentos (hardware) em aplicações tais como avaliações quantitativas de risco.

3.4.3 Probabilidade de erro para os passos da tarefa

Probabilidades de erros que são usadas na abordagem da decomposição são todas obtidas, basicamente, da mesma maneira. Uma classificação de tarefas, de forma explícita ou implícita, é utilizada para criar categorias de tarefas no domínio utilizado pela técnica empregada. Por exemplo, categorias típicas do THERP são a seleção de chaves do painel de controle, inspeções de campo, resposta à alarmes e operação de válvulas.

A probabilidade de erro básico é então atribuída para as tarefas em cada categoria ou subcategoria. Esta probabilidade pode ser proveniente de julgamento de especialistas ou dados empíricos e representa, usualmente, a probabilidade de erro em condições normais. Esta probabilidade é então modificada pela especificação de um grupo de fatores os quais moldam a probabilidade da referência básica para as características específicas da situação sendo analisada. Então, a probabilidade da referência básica de, por exemplo 10^{-3}, para a probabilidade da operação correta de

uma válvula sob condições normais, pode ser degradada até 10^{-1} sob efeito de alto estresse.

3.4.4 Probabilidades das tarefas elementares para obter a probabilidade global da tarefa.

Durante o estágio final da abordagem da decomposição, a probabilidade dos elementos da tarefa, na árvore de falhas, são combinadas, usando regras pré-estabelecidas, para fornecer a probabilidade global de falha da tarefa. Neste estágio, várias correções de dependências entre os elementos das tarefas podem ser aplicadas.

3.5 Técnicas de quantificação

Para ilustrar algumas das abordagens existentes para a quantificação, as seguintes técnicas serão descritas:

- THERP - Técnica para o Prognóstico da Taxa de Erro Humano. (Taxa, no sentido de valor, probabilidade) (Technique for Human Error Rate Prediction);
- TÉCNICA DE TEMPO-DISPONIBILIDADE;
- MATRIZ CONFUSÃO – Confusion Matrix;
- SLIM - Método do Índice da Probabilidade de Sucesso (Success Likelihood Index Method);
- ASEP - Programa de Avaliação da Sequência de Acidente (Accident Sequence Evaluation Program); e
- SHARP – Procedimento Sistemático da Confiabilidade da Ação Humana (Systematic Human Action Reliablity Procedure).

3.5.1 THERP - Técnica para o Prognóstico da Taxa de Erro Humano (Taxa, no sentido de valor, probabilidade) (Technique for Human Error Rate Prediction)

A descrição geral da metodologia THERP encontra-se no NUREG/CR-1278 , Rev. 1 (SWAIN & GUTTMANN, 1983). A descrição a seguir, está baseada em EMBREY (1994a).

THERP é a técnica mais antiga dos métodos estabelecidos, para quantificar a confiabilidade humana. Foi desenvolvida por Alan. D. Swain, na década de 1960, originalmente, para aplicações no contexto militar. Posteriormente, foi desenvolvida para a indústria nuclear. Mais tarde (SWAIN, 1987), após passar por novos desenvolvimentos, originou a técnica de análise de confiabilidade humana denominada Accident Sequence Evaluation Program Human Reliability Analysis, (ASEP). THERP é, provavelmente, a técnica de quantificação de erro humano mais conhecida e mais utilizada pelos especialistas. Isto é devido ao fato de que ela fornece sua própria base de dados e métodos de uso, tais como árvores de eventos, as quais são, prontamente, familiares ao analista de engenharia de risco.

O objetivo do THERP, segundo REASON (1990) é “estimar a probabilidade de erro humano e avaliar a degradação do sistema homem-máquina provável de ser causada por erro humano sozinho ou em conjunto com o funcionamento de equipamentos, procedimentos e práticas operacionais, outros sistemas e características humanas que influenciam o comportamento dos sistemas”.

O nível básico da análise THERP (EMBREY, 1994a) é a tarefa, a qual é feita de passos elementares tais como o fechamento de válvulas, operação de chaves, leitura de instrumentos, etc. A ação do operador pode ser considerada do mesmo modo como o sucesso ou falha de uma dada bomba ou válvula em operar. O THERP, predominantemente, endereça ações de erro numa bem estruturada linha de tarefas que podem ser reduzidas ao nível dos dados contidos no manual do THERP. Erros

cognitivos, tais como erros de diagnóstico são avaliados por meio de uma curva tempo-confiabilidade, a qual relaciona o tempo permitido para o diagnóstico versus a probabilidade de erro do diagnóstico.

A aplicação do THERP envolve os seguintes estágios:

a- Definição do problema: é obtida pela visita à planta e discussões com os analistas de risco. Em aplicações usuais do THERP, os cenários de interesse são definidos pelos analistas de risco, os quais podem especificar tarefas críticas (tais como as realizadas durante emergências) em cenários tais como fogo de grandes proporções ou liberação de gases. O encaminhamento da análise é, usualmente, ditado pelas necessidades de avaliar o equipamento para considerar o erro humano específico em cenários pré-definidos e, potencialmente, de alto risco (por exemplo, a bomba vai funcionar? Qual é a probabilidade de falha da bomba devido ao erro humano?)

b- Prognóstico qualitativo do erro: o primeiro passo da quantificação é a análise da tarefa. O THERP é aplicado, usualmente, ao nível de tarefas específicas e de passos dentro destas tarefas. O formato utilizado nas análises de tarefas é focado na operação, a qual pode ser de mais baixo nível em uma hierarquia de análise de tarefas, como a sequência passo a passo de um procedimento. Os tipos principais de erros considerados, para cada ação, são os seguintes:

- Erros de omissão (omitir um passo ou a tarefa inteira);
- Erros de comissão;
- Seleção dos erros (selecionar um controlador errado, confundir a posição dos controladores ou dar uma ordem errada);
- Erros de sequência (ação executada numa ordem errada);
- Erros no tempo (muito cedo/muito tarde);
- Erros quantitativos (muito pouco/demais).

O analista também registra oportunidades para a recuperação dos erros e dos vários fatores que afetam o desempenho do operador (PSF - Performance Shaping Factors) os quais serão, posteriormente, necessários como parte do processo de quantificação

c- Representação: os erros identificados no item anterior que podem ocorrer durante a execução da tarefa são representados no formato de árvore de falhas (fig. 3.1). Os ramos para o lado esquerdo da árvore representam sucessos e os para o lado direito, falhas. Apesar do exemplo da figura ser relativamente simples, tarefas complexas podem gerar árvores de eventos muito elaboradas. Recuperações de erros são representadas por linhas tracejadas, normalmente, incluídas nas árvores de ações do operador (fig. 3.2), similar à árvores de eventos da APS. Nesta, quando uma falha (erro) de uma ação esperada do operador, for identificada e corrigida, a sequência de eventos retorna para a sequência de sucesso da árvore de ações do operador.

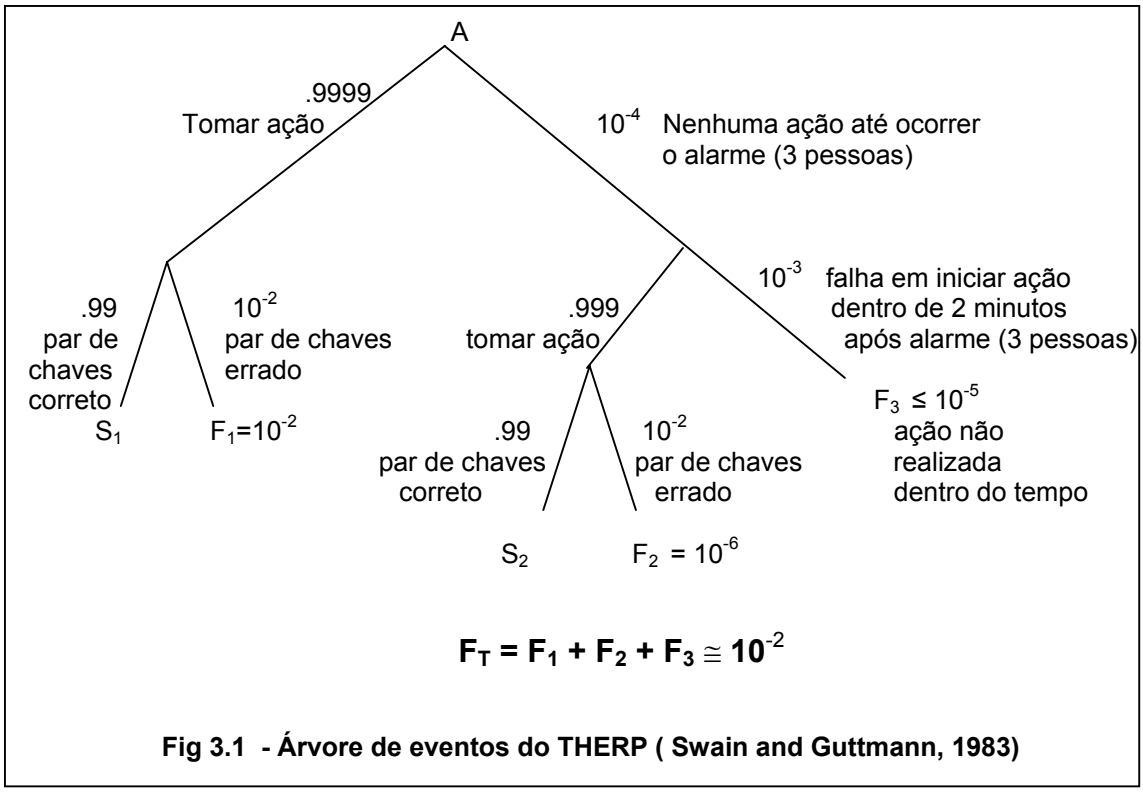


Fig 3.1 - Árvore de eventos do THERP (Swain and Guttmann, 1983)

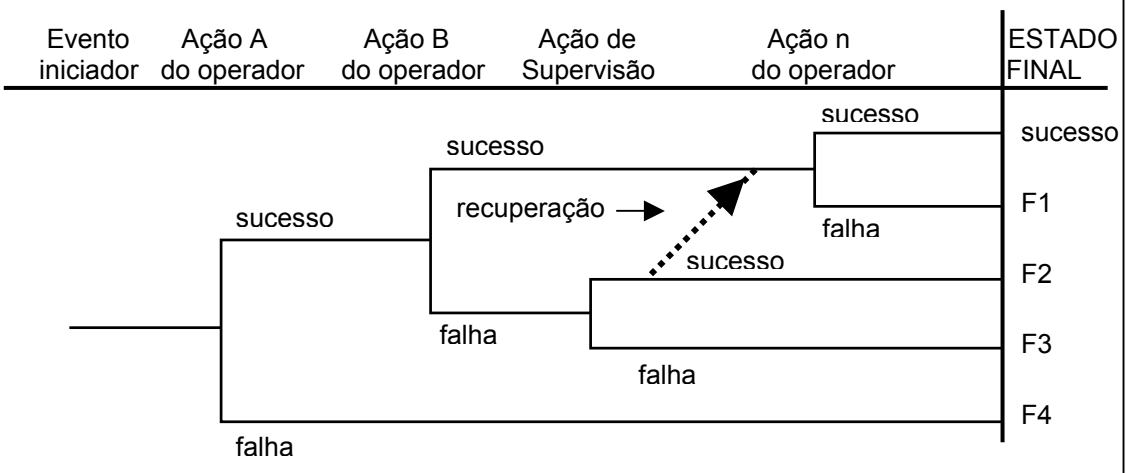


Fig. 3.2 – Árvore de Ação do Operador - Ilustração de ação de recuperação

d- Quantificação: a quantificação é feita de acordo com a árvore de falhas do THERP, como a seguir:

- Definir os erros na árvore de falhas para os quais os dados são requeridos. Na figura 3.1, estes erros são:
  - Nenhuma ação tomada até ocorrer o alarme (ação omitida);
  - Falhar em iniciar a ação dentro de 2 minutos após o alarme; e/ou
  - Escolher o par de chaves errado.
- Selecionar a tabela de dados aplicável no manual do THERP (SWAIN & GUTTMANN, 1983). O manual contém um grande número de tabelas (27 tabelas) de probabilidade de erros de operações mais comumente encontradas na sala de controle. Por exemplo, a seleção de uma determinada chave dentre várias chaves similares. A fonte destes dados não foi revelada em detalhes pelos autores, apesar de parecer estar, parcialmente, baseada no banco de dados de erro humano do American Institute for Research (MUNGER *et al.*, 1962), juntos com dados de plantas, extrapolados e modificados pelas experiências dos autores.
- Modificar os dados básicos obtidos de acordo com as orientações fornecidas pelo manual, para refletir as diferenças das condições nominais assumidas para as condições específicas da tarefa sendo avaliada. O fator mais importante levado em consideração é o nível de estresse sentido pelo operador quando executa a tarefa.
- Modificar o valor obtido no estágio anterior para refletir possíveis dependências entre as probabilidades de erros atribuídas nos passos individuais da tarefa sendo avaliada. Um modelo de dependência é fornecido, permitindo modelar níveis de dependência, desde dependência completa até total independência. Dependências podem ocorrer se um erro

afetar a probabilidade dos erros subsequentes, por exemplo, se o tempo total disponível para executar a tarefa for reduzido.

- Combinar as probabilidades modificadas para obter a probabilidade total da tarefa. A regra de combinação para obter a probabilidade total segue o mesmo processo de adição e multiplicação de árvores de falhas padrões.

e- Integração com a análise dos equipamentos (software): as probabilidades de erros obtidas no processo de quantificação são incorporadas ao sistema global de árvores de eventos e árvores de falhas.

f- Estratégia de redução de risco: se a probabilidade de erro calculada pelo procedimento acima levar a um valor inaceitável de probabilidade de falha para o sistema ou função, então o analista deverá examinar as árvores de eventos para determinar se alguns dos fatores que influenciam o desempenho podem ser modificados ou se a estrutura das tarefas pode ser modificada, para reduzir a probabilidade de erro para um nível aceitável.

Segundo REASON (1990), o manual da metodologia THERP transferiu uma experiência de mais de 30 anos de seu principal arquiteto, Alan Swain, para as novas gerações de analistas de confiabilidade humana (ACH) e, provavelmente, devido aos resultados de seu extensivo uso e a efetividade de sua disseminação, o mesmo, também, esteve sujeito às maiores críticas do que qualquer outro método de ACH. Foi julgado por alguns especialistas (SENDERS *et al.*, 1985) “como, provavelmente, a melhor técnica disponível”.

A suposição básica do método, é de que a ação do operador pode ser considerada da mesma maneira que o sucesso ou falha de uma bomba ou válvula e desta maneira ser analisado como um item de equipamento. O objetivo do THERP, segundo SWAIN & GUTTMANN (1983), é “diagnosticar a probabilidade do erro

humano e avaliar o grau de degradação do sistema homem-máquina provável de ser causado pelo erro humano, sozinho ou em conjunto com equipamentos que estão operando, procedimentos e práticas operacionais ou outras características humanas que influenciam o comportamento dos sistemas".

Os fatores que afetam o desempenho (PSF) foram a maior contribuição que o THERP fez para a comunidade dos operadores. Eles são usados para modificar a probabilidade nominal de erro humano (HEP, Human Error Probability), de acordo com o julgamento dos analistas de tais fatores (como as condições ambientais de trabalho, a qualidade da interface homem-máquina, a habilidade, a experiência, a motivação e as expectativas do operador e o grau e tipos de estresse prováveis de estarem presentes em situações operacionais variadas).

A essência do THERP está contida nas 27 tabelas de probabilidade de erro humano citadas anteriormente. Estas probabilidades são valores genéricos, baseados na opinião de especialistas ou dados tomados de atividades análogas às dos operadores de NPP. Cada uma destas tabelas está referenciada a um determinado tipo de erro associado com uma atividade específica. Por exemplo, erros de omissão em ler e registrar informações quantitativas mostradas nos indicadores, erros em operar controles manuais ou válvulas operadas localmente, etc. Cada tabela é desmembrada em atividades componentes menores e, para cada componente, é atribuído, usualmente, dois valores: o *valor nominal da HEP* e, ou o *fator de erro* (raiz quadrada da razão entre os limites de incerteza superior e inferior) ou os próprios *limites de incerteza* (os limites superior e inferior da uma dada HEP, refletindo a incerteza das estimativas). Os limites de incerteza superior e inferior correspondem aos percentis de noventa e cinco e cinco, respectivamente, em uma escala lognormal de HEPs. Como já dito, é requerido ao analista ajustar o valor da probabilidade de erro nominal, de acordo com o seu julgamento dos efeitos dos fatores locais que afetam o desempenho

As versões mais antigas do THERP foram largamente criticadas por ter o seu foco, exclusivamente, nas formas de erros comportamentais e por omitir os enganos (mistakes) tais como erros de diagnóstico ou a seleção de uma estratégia corretiva inadequada, exatamente, do tipo de erro (erro de comissão) que contribuiu, extensivamente, para o agravamento do acidente de TMI. Posteriormente, Swain e seu colaborador (SWAIN & WESTON, 1988) pensaram em revisar o método original de maneira a considerar erros de diagnóstico e outros “enganos” de alto nível cognitivo.

Segundo REASON (1990), estas versões mais recentes foram importantes por duas razões: primeiro, marcaram a separação das probabilidades nominais de erro, obtidas do julgamento de especialistas, as quais apresentavam resultados altamente variados (COMER *et al.*, 1984). Swain considerou a freqüência de erro dependente do tempo baseada em dados de simulador, onde equipes de operadores foram submetidas a diferentes tipos de eventos anormais. Estes dados mostram o tempo necessário para cada diagnóstico correto e o número de equipes de controle que falharam em atingir este diagnóstico. Segundo, forneceram uma base para estimar a probabilidade de erro de diagnóstico de diferentes tipos de eventos ocorridos após o início do acidente.

Apesar destas mudanças (de uma consideração exclusivamente comportamental para outra que começou a considerar elementos cognitivos), o método permaneceu, ainda, insuficiente para identificar e quantificar, de uma maneira realística, todas as situações em que o operador pode interferir negativamente no risco global da operação da planta.

3.5.2 Técnica de tempo-confiabilidade

Trata de técnicas relacionadas com a quantificação de erros pós-acidentes, baseada em curvas de tempo-confiabilidade. A primeira delas foi o modelo denominado árvores de ação dos operadores (OAT's, Operator Action Trees).

Segundo REASON (1990), quando as OAT's foram, inicialmente desenvolvidas, no início da década de 1980 (NUREG/CR-3010, 1982; WREATHALL, 1982), THERP era a única técnica que tinha sido utilizada para quantificar o risco, causado por erro humano, contribuidor para acidentes em NPP. O método THERP original tratava, basicamente, dos erros de procedimento (p.ex., deixar uma válvula na posição errada), os quais eram realizados antes (pré-acidente) de ocorrer o desarme do reator e que poderiam causar ou o desenvolvimento de um evento ou uma indisponibilidade de um sistema de segurança. Os arquitetos da técnica de OAT entendiam que esta consideração desprezava outros tipos importantes de erros humanos: aqueles que ocorrem após a sequência de acidente ter começado (pós-acidente). Estes foram chamados de erros cognitivos porque eles têm, para a maior parte envolvida, processos de falhas (mistakes) em alto nível cognitivo, tais como raciocínio, diagnoses e seleção de estratégia. Erros comportamentais e cognitivos requerem uma técnica analítica diferente, tanto para modelagem quanto para quantificação. A técnica OAT foi planejada para tratar erros de operador realizados durante acidentes e situações anormais e é projetado para fornecer tipos de erros e probabilidades associadas para serem usadas nas APS's.

O detalhamento do método é dado pelo NUREG/CR-3010 (1982) e por WREATHALL (1982). Basicamente o método emprega uma árvore lógica, a árvore de ação básica do operador (OAT, Operator Action Tree), que identifica os modos de falhas pós-acidente do operador. Três tipos de erros cognitivos são identificados:

(a) Falha em perceber que um evento iniciou;

(b) Falha em diagnosticar a natureza do evento e de identificar as necessárias ações corretivas; e

(c) Falha em implementar, corretamente, as respostas e no tempo requerido.

Estes erros são quantificados pela aplicação de uma ferramenta analítica chamada curva de tempo-confiabilidade, a qual descreve a probabilidade da falha, como uma função do intervalo de tempo transcorrido desde o momento no qual um sinal relevante ocorreu e o tempo em que a ação deveria ter sido tomada, para alcançar uma recuperação com sucesso. Por exemplo, segundo o IAEA-TECDOC-592 (1991), no caso de perda de água de alimentação principal com falha do desligamento automático do reator (ATWS), o operador tem 79 segundos para desligar, manualmente, o reator, antes que ocorra sobrepressurização do circuito primário e abertura das válvulas de alívio. Este período inclui o tempo para o operador diagnosticar a falha, através de alarmes, planejar e executar a ação de desligamento.

Algumas modificações podem ser feitas nestas curvas quando o analista julgar que o operador poderia estar relutante para tomar certas ações. A probabilidade derivada do relacionamento destas curvas representa a probabilidade do sucesso da ação pela equipe de operadores. A maior informação para a curva de quantificação é o tempo disponível para pensar, dado por: $t_T = T_0 - t_I - t_A$, onde t_T é o intervalo para pensar, T_0 é o tempo total transcorrido desde o início da seqüência do acidente até o ponto no qual as ações devem ser completadas, t_I é o tempo após o início no qual indicações apropriadas são dadas e t_A é o tempo tomado para realizar as ações planejadas. As bases para estes parâmetros são dadas por WREATHALL (1982). No caso de ausência de dados de campo adequados, elas dividem com THERP o problema fundamental de serem as melhores estimativas, provenientes de especialistas ou de extrapolações de estudos de laboratório.

REASON (1990) cita os seguintes comentários, feitos por especialistas, sobre a técnica OAT. HANNAMAN *et al.* (1984a) destacam um ponto alto da técnica:

“fornece uma estrutura definida para avaliar os modos de falhas do operador a qual é independente de procedimentos, é simples para usar com dependências definidas, tem um guia de aplicação e dados definidos”. SENDERS *et al.* (1985) comentam que “as OAT’s não foram formalmente validadas mas tem sido relacionadas com dados empíricos, de uma maneira particularmente interessante, pelo uso de curvas genéricas de tempo para conclusão. Como resultado, as OATS podem prognosticar a probabilidade de que nenhuma resposta será dada ao anúncio de um incidente, como uma função do tempo transcorrido desde que o incidente ocorreu ”.

REASON (1990) também comenta que, na descrição original da técnica OATs (NUREG/CR-3010, 1982) seus autores sugeriram que, curvas diferentes de tempo versus confiabilidade poderiam ser produzidas para desempenhos baseados em habilidade, regras e conhecimento, tendo como referência a correlação tempo-confiabilidade desenvolvida por Joe Fragola. Esta idéia foi desenvolvida por Hannaman e seus colaboradores (HANNAMAN *et al.*,1984a) na forma de modelos de confiabilidade cognitiva humana (HCR, Human Cognitive Reliability).

HCR está fundamentada na suposição de que diferentes tipos de atividades cognitivas podem ter tempos diferentes de execução. Seus resultados são as probabilidades de falta de resposta dos operadores de NPP, em relação ao tempo, quando confrontados com situações anormais da planta. Enquanto as OATs envolvem somente uma relação simples de tempo-confiabilidade, HCR fornece um conjunto de curvas, cada uma relativa a um tipo diferente de processamento cognitivo (habilidade, regras ou conhecimento), para modelar uma dada situação específica (por exemplo, ruptura de tubos dos geradores de vapor). Assim sendo, ela fornece uma avaliação da persistência do erro em função ao tempo.

Revisores da técnica de HCR (SENDERS *et al.*, 1985, EMBREY & LUCAS, 1989), comentaram várias de suas vantagens:

(a) É uma técnica rápida e, relativamente, conveniente para aplicar;

(b) Considera a natureza das ações dos operadores dependentes do tempo;

(c) Foram encontradas semelhanças adequadas entre o modelo e o tempo real para finalizar as ações, em estudos de simuladores;

(d) Cobre comportamento baseado em conhecimento assim como os modelos mais usuais de níveis de desempenho baseados em habilidade e em regras;

(e) As informações de entrada (tempo disponível desde o estabelecimento da emergência) são as mesmas utilizadas nas técnicas de avaliação de confiabilidade de equipamentos.

O modelo HCR diagnostica o tempo para a conclusão da tarefa, porém não constitui um modelo de erro. “O método usa modelos ou dados de erros como entrada (input) ao invés de produzir tais dados como saída (output). Especificamente, a ocorrência de erros aumenta o tempo para conclusão, mas o modelo não prevê quando ou quão freqüente tais erros irão ocorrer.” (SENDERS *et al.*, 1985).

De acordo com EMBREY & LUCAS (1989), o maior benefício da correlação HCR é seu foco concentrado na probabilidade de falta de resposta. Muitos dos erros críticos cometidos pelos operadores durante emergências em NPP envolvem erros de comissão assim como de omissão. Por exemplo, a rápida escolha de uma ação errada ou a violação deliberada de procedimentos. EMBREY & LUCAS (1989) também destacaram que as regras para designar tarefas para os vários níveis de desempenho (habilidade, regras e conhecimento), não consideram o chaveamento rápido entre estes níveis aparentes durante o curso de eventos reais. Da mesma maneira, não é fácil determinar se a probabilidade de falta de resposta (obtida das curvas do HCR) é devida ao processamento lento da informação ou à falha em detetar o estabelecimento da emergência. Estes são processos, psicologicamente, diferentes e não parecem prováveis que eles podem ser descritos pelas mesmas curvas de tempo disponível/falta de resposta.

3.5.3 Matriz Confusão (Confusion Matrix)

Conforme descrito por REASON (1990), a Matriz Confusão foi um legado deixado por POTASH *et al.* (1981) como um meio de avaliar os erros dos operadores quando respondendo às condições anormais na planta. Foi utilizado, para esta finalidade, em duas APS's de usinas nucleares americanas: OCONEE (1984), e Seabrook (PICKARD *et al.*, 1983).

O método se baseia no julgamento de especialistas (usualmente, do pessoal da área de treinamento da planta em questão) e considera a probabilidade de diferentes erros de diagnose de situações críticas específicas da planta. Estes julgamentos são colocados em uma distribuição estruturada e sistemática, permitindo a evolução da probabilidade em tempos diferentes durante uma dada sequência de acidente. A sua resposta representa a probabilidade de que o operador irá falhar em responder, corretamente, aos eventos A, B, C, etc., nos tempos t_1, t_2, ... t_n após o início da sequência de eventos. Ao dar seus julgamentos, os especialistas são encorajados a considerar outros fatores tais como a sobreposição de sintomas entre eventos diferentes, a expectativa do operador baseada na sua experiência prévia, o efeito do estresse e a qualidade da ergonomia geral da sala de controle.

Segundo REASON (1990), a principal vantagem desta técnica é que ela fornece uma estrutura simples para ajudar os analistas a identificar situações não facilmente modeladas por outros métodos de ACH. Ela parece ter mais valor como uma ferramenta de análise qualitativa do que quantitativa. Diferenças consideráveis aparecem entre as probabilidades estimadas por diferentes especialistas. Ela também divide com outras técnicas, a fraqueza de ser baseada em manipulações simplistas de dados subjetivos que, neste caso, são de probabilidade absoluta de valores baixos.

3.5.4 SLIM - Método do Índice da probabilidade de sucesso (Success Likelihood Index Methodology)

Conforme descrito por REASON (1990), a metodologia SLIM criada por Embrey, Humphreys, Rosa, Kirwan & Rea (EMBREY *et al.*, 1984), assim como a Matriz Confusão (POTASH *et al.*, 1981) foi desenvolvida para fornecer um meio de deduzir e estruturar o julgamento de especialistas. O programa de computador que suporta esta metodologia permite aos especialistas gerar modelos que conectam as probabilidades de erro de uma situação específica com os fatores que influenciam estas probabilidades. A razão básica é que a probabilidade de ocorrer um erro em uma determinada situação é função dos efeitos combinados de um número, relativamente, pequeno de fatores que influenciam o desempenho (PIF, Performance Influencing Factors). Estes são pequenas variantes, alguma coisa menos comportamental dos que os utilizados pelo THERP (PSF- Performance Shaping Factors). O índice da probabilidade de sucesso (SLI, success likelihood index) é derivado de considerações de variáveis típicas que são sabidas influenciar a taxa de erro (isto é, a qualidade do treinamento, procedimentos e tempo disponível para a ação). Também é assumido que os especialistas podem graduar, numericamente, o quão bom ou ruim são estes PIFs em uma dada situação. Os pesos e os valores das importâncias relativas para cada PIF são multiplicados juntos e os produtos são somados para dar um índice da probabilidade de sucesso. Este índice é pressuposto relacionar a probabilidade de sucesso que poderia ser observado num longo período de ação de uma situação particular de interesse.

A metodologia SLIM tem vários dispositivos atraentes. Ela está disponível na forma de dois pacotes de programa de computador, completos e interativos: SLIM-SAM (SLIM Assessment Module), o qual gera o índice da probabilidade de sucesso e o SLIM-SARAH (SLIM Sensitivity Analysis for Reliability Assessment of Humans), o qual permite executar análises adicionais de sensibilidade e custo-benefício. Para

estabelecer as independências dos PIFs (um suposição importante do modelo base), o pacote SLIM-SAM verifica a variação do grau de compartilhamento entre as graduações geradas pelos analistas e informa ao usuário se a taxa de dois PIFs estão correlacionadas. Adicionalmente, até 10 tarefas podem ser avaliadas em uma única sessão de SLIM. Isto reduz, substancialmente, o tempo de dedicação do especialista.

Até o presente, existem algumas dificuldades com a calibração do SLIM. Uma suposição básica é que o SLIM pode ser calibrado com referencia à seguinte equação linear: $log\ HEP = a\ SLI + b$, onde HEP é a probabilidade de erro humano (human error probability). Na teoria, as probabilidades de erros podem ser obtidas por referência a duas tarefas calibradas, cujas probabilidades de erro são, objetivamente, conhecidas. Entretanto, ela torna crítica a escolha destas tarefas de referência e a equação base da função linear da calibração não foi largamente aceita. Adicionalmente, como será discutido mais tarde, SLIM não foi bem cobrada, particularmente, em estudos de validações independentes. Mas isto, como será visto, não é exclusividade do SLIM.

A descrição, a seguir, está baseada em EMBREY (1994a) e a técnica está descrita, em detalhes, em EMBREY *et al.* (1984) e KIRWAN (1990). Esta técnica foi, originalmente, desenvolvida para apoiar o órgão regulatório americano, (United States-Nuclear Regulatory Commission - US-NRC), e igualmente, como o THERP, seu uso foi estendido para outras indústrias como a petroquímica, transporte, etc. A técnica é aplicada em tarefas em qualquer nível de detalhes.

Como sabido, os erros podem ser quantificados nos diversos níveis de atividades, como em uma tarefa total, em sub-tarefas, passos da tarefa e mesmo em erros individuais associados com os passos da tarefa.

A premissa básica da técnica SLIM é que a probabilidade de erro associada com a tarefa, sub-tarefa, passo da tarefa ou erro individual é função dos fatores que influenciam o desempenho (PSF, Performance shaping factor) existentes na situação. Existe um número, extremamente grande de PSF's. Normalmente, os PSF's, que são

considerados nas análises do SLIM, são os que possuem influencias diretas nos erros tais como níveis de treinamento, qualidade dos procedimentos, nível de distração, qualidade da informação de retorno (feedback) de uma ação, nível de motivação, etc., às vezes denominados de fatores que influenciam a performance (PIF, performance influencing factors).

Nos procedimentos do SLIM, as tarefas são graduadas, numericamente, em relação aos PIFs que influenciam a probabilidade de erro. Estas graduações, como já dito anteriormente, são combinadas, para cada tarefa, para dar um índice chamado de índice de probabilidade de sucesso (SLI-success likelihood index). Este índice é então convertido em probabilidade por meio de uma relação geral entre o SLI e a probabilidade de erro, o qual é desenvolvido usando tarefas com probabilidades e SLI conhecidos. Estas são chamadas de tarefas de calibração.

O processo de quantificação é realizado em 7 estágios:

1. Formar grupos de operação homogenea;
2. Decisão baseada nos PIFs relevantes;
3. Gradue cada operação em cada PIF;
4. Atribua pesos se adequado;
5. Cálculo do índice da probabilidade de sucesso;
6. Converter os índices de probabilidade de sucesso em probabilidades; e
7. Realizar a análise de sensibilidade.

Para ilustrar a quantificação do método SLIM, será utilizado um exemplo hipotético de enchimento de um tanque, em que são necessárias tarefas básicas de abrir/fechar válvulas e bloquear seu manuseio, observar níveis e outras operações simples. Do total das ações para realizar esta tarefa, serão tratadas somente 4, descritas a seguir:

1. Fechar válvula de teste;

2. Fechar válvula do tanque;

3. Apertar parafuso de bloqueio;

4. Colocar dispositivo de tranca na válvula.

1- Formar grupos de operação homogenea.

O primeiro passo é agrupar as operações que são prováveis de serem influenciadas pelos mesmos PIFs. As quatro operações acima envolvem ações físicas para as quais não existe nenhum sinal de retorno se forem, indevidamente, realizadas. As operações (2) e (3) são consideradas, para efeito do exemplo, terem consequências significantes se tal ocorrer. É verdadeiro assumir, portanto, que a probabilidade de erro será determinada pelo mesmo grupo de PIFs para todas as operações deste grupo de atividades.

2- Decisão baseada nos PIFs relevantes.

Idealmente, bancos de dados deveriam ser desenvolvidos nas empresas tais que PIFs predefinidos seja associados com categorias particulares de tarefas. Se isto não for o caso, o analista decide um grupo de PIFs adequado. No exemplo é assumido que os principais PIFs que determinam a probabilidade de erro são estresse causado pelo tempo, nível de experiência, nível de distração e qualidade dos procedimentos.

3- Gradue cada operação em cada PIF

Uma graduação numérica na escala de 1 a 9 é feita para cada operação em relação a cada PIF. Normalmente, o final de cada escala representa a melhor ou pior condição do PIF. Por exemplo, um alto nível de estresse causado pelo tempo disponível poderia ter o valor 9, o que poderia implicar em um aumento do número de erros. Entretanto, para o caso de nível de experiência, o valor 9 poderia representar um ótimo valor, correspondendo a um operador altamente experiente. O fato de que o

mesmo valor pode ter significados diferentes para diferentes PIFs, estes devem ser levados em consideração pelo analista. Com o programa de computador disponível para a técnica SLIM (EMBREY, 1994b), estes ajustes são feitos, automaticamente. A tabela 3.5.4.a abaixo mostra as graduações feitas para o exemplo de ações escolhidas.

Estas graduações podem ser interpretadas da seguinte maneira: no caso do PIF de estresse, todas as operações têm um nível alto, exceto **fechar a válvula de teste**, onde o estresse é baixo. Os operadores são muito experientes em realizar as tarefas. A distração é, moderadamente, alta para **fechar a válvula de teste**, para as demais é baixa. Os Procedimentos são fracos para **apertar parafuso de bloqueio** e **colocar dispositivo de tranca na válvula.**

Tabela- 3.5.4.a - Classificação dos PIFs

Tarefa	**Estresse**	**Experiência**	**Distração**	**Procedimento**
Fechar vv. de teste	4	8	7	6
Fechar vv. do tanque	8	8	5	6
Apertar parafuso de bloqueio	8	7	4	2
Colocar dispositivo de tranca na válvula.	8	8	4	2

4- Atribua pesos se adequado

Baseado na experiência do analista ou em alguma teoria de erro, é possível atribuir pesos para os vários PIFs para representar a influência relativa que cada PIF possui em todas as tarefas do grupo que está sendo avaliado. Neste exemplo é assumido que, em geral, o nível de experiência tem a menor influência neste tipo de erro e o estresse é o mais influente. O efeito relativo dos diferentes PIFs pode ser expresso pelos seguintes valores:

- Estresse pelo tempo 0,4
- Distrações 0,3
- Procedimentos 0,2
- Experiência 0,1

Deve ser observado que o analista deve atribuir pesos, somente, se ele possuir, realmente, conhecimento ou evidência de que estes são adequados. A atribuição dos pesos não é mandatório em SLIM. Se os pesos não são usados, a técnica assume que todos os PIFs são de igual importância na contribuição da probabilidade de sucesso ou falha geral.

5- Cálculo do índice da probabilidade de sucesso

O SLI é dado pela seguinte expressão:

$$SLI_J = \sum RijWi$$

onde SLI_J é o SLI da tarefa *j*; W_i é a importância normalizada do peso para o PIF *i* (a soma dos pesos é igual a 1); e R_{ij} é o valor da tarefa no PIF *i*. O SLI para cada tarefa é a soma dos pesos das classificações de cada tarefa em relação a cada PIF.

Para calcular os SLIs, os dados da tabela 3.5.4.a devem ser escalonados para levar em conta o fato que alguns dos pontos ideais estão em extremidades diferentes na escala de graduação. Rescalonar também converte a escala original de 1 a 9 para 0 a 1. A formula a seguir converte a classificação inicial para a rescalonada:

$$RR = [1 – abs (R - IP)] / [4 + abs (5 - IP)]$$

Onde RR é o valor rescalonado; R é a graduação original e IP é o valor ideal para a escala onde a classificação é feita.

A precisão desta fórmula pode ser verificada substituindo os valores 1 e 9 para escalas onde o ponto ideal é tanto 1 quanto 9. A fórmula converte o valor original para 0,0 ou 1,0, adequadamente.

Aplicando esta fórmula nos valores da tabela 3.5.4.a obtem-se a tabela 3.5.4.b, a qual contêm os valores escalonados, os pesos atribuídos para os PIFs e os índices das probabilidades de sucesso calculado para cada tarefa.

Tabela- 3.5.4.b - Classificação rescalonada dos PIFs

Operação	**Estresse**	**Experiência**	**Distração**	**Procedimento**	**SLIs**
Fechar vv. teste	0,63	0,88	0,25	0,63	0,54
Fechar vv. tq.	0,13	0,88	0,50	0,63	0,41
Apertar parafuso de bloqueio	0,13	0,75	0,63	0,13	0,34
Colocar dispositivo de tranca na válvula.	0,13	0,88	0,63	0,13	0,35
Pesos	0,4	0,1	0,3	0,2	

6- Converter os índices de probabilidade de sucesso em probabilidades

Os SLIs representam uma medida da probabilidade de que a operação terá sucesso ou falha, uma em relação à outra. Para converter a escala de SLI para a escala de probabilidades, é necessário calibrá-la. Se um número, razoavelmente, grande de operações do grupo que está sendo avaliado possuem probabilidades conhecidas (por exemplo, os dados resultantes de um incidente que foram colecionados por um longo período de tempo), então é possível executar uma análise de regressão que irá encontrar a linha que melhor se adapta entre os valores de SLI e suas correspondentes probabilidades de erros. A equação da regressão resultante

pode ser, então, utilizada para calcular as probabilidades de erros para as outras operações do grupo pela substituição do SLIs na equação de regressão.

Se não existirem dados suficientes para permitir o cálculo de uma relação empírica entre os SLIs e as probabilidades de erro, como, normalmente, é o caso, então deve ser utilizada uma relação matemática. A forma usual desta relação é uma log-linear, como mostrado abaixo:

$$\text{Log(HEP)} = \text{A SLI} + \text{B} \qquad (1)$$

Onde HEP é a probabilidade de erro humano e *A* e *B* são constantes.

Esta suposição (PONTECORVO, 1965) está baseada, parcialmente, em evidências experimentais que mostram uma relação log-linear entre a avaliação dos fatores que afetam o desempenho em atividades de manutenção e execução reais de tarefas. Para calcular as constantes A e B da equação, pelo menos duas tarefas com SLIs e probabilidades de erros devem estar disponíveis no grupo de tarefas em avaliação.

No exemplo em discussão, foi considerado que existem poucos registros de teste de válvulas deixadas na posição aberta. Pelo outro lado, apertar parafusos de bloqueio são, frequentemente, encontrados soltos quando a atividade é concluída. Baseando-se nestas evidências e na frequência em que estas operações são realizadas, as seguintes probabilidades podem ser atribuídas a estes erros:

Probabilidade de deixar a válvula de teste aberta = 1×10^{-4}

Probabilidade de não apertar os parafusos de bloqueio = 1×10^{-2}

Estes valores e os correspondentes SLIs para estas tarefas (da tabela 3.5.4.b) são substituídos na equação geral (1). O resultado da equação pode ser usado para calcular as constantes A e B. Substituindo estes valores na equação geral (1) tem-se a seguinte equação de calibração:

$$\text{Log(HEP)} = -2{,}303\ \text{SLI} + 3{,}166 \qquad (2)$$

Se os valores de SLI da tabela 3.5.4.b para outras duas tarefas do grupo forem substituídos nesta equação, a probabilidade resultante de erro será a seguinte:

Tarefa A: Probabilidade de não abrir a válvula do tanque = $1{,}8 \times 10^{-3}$

Tarefa B: Probabilidade de não fixar o dispositivo de tranca = $7{,}5 \times 10^{-3}$

7- Realizar a análise de sensibilidade

A natureza da técnica do SLIM a torna muito útil para análises “e se” para investigar os efeitos de trocar alguns valores de PIF nas probabilidades de erros resultantes. Por exemplo, existe alto nível de estresse para ambas as tarefas acima (valor do estresse=8, melhor valor=1). Os efeitos de redução do estresse para valores mais moderados podem ser investigados atribuindo o valor de 5 para cada tarefa. Isto altera o SLI e se o novo valor de SLI for substituído na equação (2) a mudança na probabilidade será a seguinte:

Tarefa A: Probabilidade de não abrir a válvula do tanque = $5{,}6 \times 10^{-5}$

Tarefa B: Probabilidade de não fixar o dispositivo de tranca = $2{,}4 \times 10^{-4}$

Uma intervenção alternativa que poderia ser realizada, é fazer um valor ideal para procedimentos (valor=9). Alterando o valor de procedimentos para este novo valor em todas as tarefas (ao invés da redução do estresse), produz o seguinte resultado:

Tarefa A: Probabilidade de não fechar a válvula do tanque = $3{,}2 \times 10^{-4}$

Tarefa B: Probabilidade de não fixar o dispositivo de tranca = $1{,}3 \times 10^{-4}$

Então, o efeito de tornar ideal o PIF procedimentos, provoca o aumento de uma ordem de magnitude para a tarefa B comparada com a tarefa A (veja tabela 3.4.4.c). Isto é porque o procedimento para a tarefa A já estava mais alto, no valor 6, onde

havia espaço para melhoramentos da tarefa B a qual foi graduada em 2 (veja tabela 3.5.4.a).

Tabela- 3.5.4.c Efeito da melhora em procedimentos na probabilidade de erro calculada usando SLIM.

	Probabilidade de erro original	**Após melhorias em procedimentos**	**Melhorias na relação antes/depois**
Tarefa A	$1,8 \times 10^{-3}$	$3,2 \times 10^{-4}$	5,6
Tarefa B	$7,5 \times 10^{-3}$	$1,3 \times 10^{-4}$	57,7

Como conclusão (EMBREY *et al.*, 1994b), a técnica SLIM é um método altamente flexível que permite considerável liberdade para executar análises do tipo "o que - se". Como a maioria das técnicas de quantificação de confiabilidade humana, ela requer dados concretos, preferencialmente, da própria planta. Na ausência de tais dados, os valores de calibração devem ser gerados por julgamento especializado feitos por pessoal experiente da usina.

3.5.5 ASEP- Programa de Avaliação da Sequência de Acidente (Accident Sequence Evaluation Program)

A metodologia ASEP está descrita no NUREG/CR-4772 (SWAIN, 1987) e é uma versão reduzida do método THERP. A aplicação do THERP, realiza uma abordagem profunda e requer um tempo e mão de obra consideráveis, incluindo uma equipe de especialistas nas áreas de confiabilidade humana, analistas de sistemas, pessoal técnico da planta e outros. O ASEP foi criado, baseado no método THERP/Handbook (SWAIN & GUTTMANN, 1983), porém incorporou várias simplificações no modelo de desempenho humano, a fim de se tornar um método que requer tempo e mão de obra reduzidos, porém fornecendo estimativas de

probabilidade de erro humano, para atividades realizadas durante condições de operação normal à potência e condições pós-acidente, com suficiente precisão para uso nas APS's.

3.5.6 SHARP – Procedimento Sistemático da Confiabilidade da Ação Humana (Systematic Human Action Reliability Procedure)

Em virtude das diversas metodologias de análise de confiabilidade humana criou-se uma certa dificuldade em decidir qual metodologia utilizar e quando. Para facilitar esta tarefa, HANNAMAN *et al.* (1984b) criaram um procedimento, Systematic Human Action Reliability Procedure (SHARP), para ajudar os analistas a incorporar as interações humanas nos estudos de APS de uma maneira sistematizada, completa e de fácil revisão. Segundo o IAEA-TECDOC-592 (1991), SHARP não é um modelo nem uma técnica, mas um meio de orientar a seleção de um modelo ou técnica de análise de confiabilidade humana. Especificamente, indica as opções disponíveis em relação à representação das ações dos operadores (THERP, OATS, etc.) e o tipo de modelo ou de dados para dar base às várias técnicas de ACH.

SHARP consiste de sete passos, onde cada passo endereça a uma tarefa específica de ACH. Cada passo é constituído de atividades e regras.

SHARP classifica as ações humanas em cinco tipos diferentes, para então, indicar um método de análise mais adequado para a ação em questão.

3.6 Considerações sobre os métodos apresentados

Como visto, os métodos apresentados consideram ações dos operadores que estão previstas, de alguma maneira, nos diversos tipos de procedimentos existentes nas planta. As falhas das ações requeridas envolvem erros de omissão, isto é, o operador não faz o que deveria fazer e, desta maneira, coloca a planta em um estado degradado.

Entretanto, ações não requeridas em procedimentos, portanto não modeladas nas atuais ACH's e, por conseguinte, não consideradas pelas APS's para o cálculo do risco total, tem ocorrido em vários eventos, as quais degradaram as condições de segurança da planta. O anexo A apresenta 6 eventos ocorridos que caracterizam estas ações.

A identificação de tais ações (erros de comissão) e os contextos em que as mesmas são mais possíveis de ocorrerem, assim como as suas quantificações para inclusão nas APS's serão vistas no Capítulo 4.

Capítulo 4

METODOLOGIA ATHEANA

4.1 Introdução

A metodologia ATHEANA (NUREG-1624, Rev. 1, 2000), originou-se da análise (AEOD/E95-01, 1995) de sérios acidentes ocorridos, onde foi constatado que, certas ações do operador (erros de comissão) não descritas em procedimentos e que degradavam substancialmente as condições do acidente, não estavam adequadamente representadas nas APS's. Os métodos de ACH utilizados possuem limitações significativas em identificar falhas humanas potenciais, do tipo (erros de comissão) ocorrido em TMI e Chernobyl, e em determinar as suas probabilidades.

Em vista disto e para atender às novas diretrizes de regulamentação e fiscalização da NRC, baseadas em informações de risco (risk-informed), esta patrocinou um estudo para criar uma nova metodologia que contemplasse este tipo de falha humana, para que as APS's passassem a refletir mais realisticamente o comportamento humano em eventos operacionais.

Este capítulo se destina a apresentar as bases, características e os processos da metodologia ATHEANA, conforme descrito no NUREG-1624, Rev. 1 (2000), com a finalidade de prover uma familiarização com esta metodologia e as bases para as discussões dos próximos capítulos, tema principal desta tese.

4.1.1 Fatores complicadores em eventos

As análises dos acidentes mostraram que existe, tipicamente, um conjunto de fatores complicadores (condições da planta), os quais não são considerados nas APS's. Os seguintes exemplos ilustram estes fatores:

- Cenários que desviam da expectativa do operador, o qual está baseado no seu treinamento e experiência, ou seja, o comportamento da planta está diferente do esperado.
- Múltiplas falhas e indisponibilidade de equipamentos (especialmente aquelas que são dependentes ou causadas pelo homem), que vão além daquelas utilizadas no seu treinamento ou nas análises de segurança, ou seja, o comportamento da planta não é entendido.
- Problemas de instrumentação, para os quais os operadores não foram, totalmente, preparados e que podem causar interpretações erradas do evento, ou seja, as indicações do estado e do comportamento da planta não são reconhecidos.
- Condições da planta não estão descritas nos procedimentos, ou seja, os procedimentos existentes não são aplicáveis para a situação existente.

4.1.2 Mecanismos de erro

Estudos recentes das ciências comportamentais contribuíram para entender que as condições da planta associadas com fatores centrados no homem (como por exemplo, interface homem-máquina, estresse, pressão do tempo, conteúdo e formato dos procedimentos e treinamento, os quais são denominados fatores que formatam o desempenho (PSF, performance shaping factors)), criam condições e oportunidades (um contexto que força ao erro: EFC, error-forcing context) que disparam mecanismos psicológicos que podem levar o homem a realizar uma ação, denominada ação insegura (UA), a qual pode degradar as condições de segurança da planta. Em muitas das vezes, estes mecanismos não são, por si só, maus comportamentos, mas são mecanismos que permitem ao homem executar ações rápidas e de grande habilidade. Por exemplo, frequentemente, os operadores diagnosticam uma ocorrência pela comparação com um padrão já conhecido. Na maioria das vezes, isto é um modo

eficiente e rápido de responder a um evento. Entretanto, se o evento difere levemente do evento rotineiro, existe a tendência do operador de rapidamente selecionar e utilizar um padrão mais próximo e agir como se este fosse um evento rotineiro. Em circunstâncias rotineiras, esta rápida identificação leva a respostas eficientes e no tempo requerido; entretanto, se o evento não for rotineiro, o mesmo processo pode levar a uma resposta inadequada.

4.2 Metodologia ATHEANA

A metodologia ATHEANA, diferentemente dos métodos tradicionais que buscam quantificar os erros humanos de uma forma randômica e em condições previstas de acidente, visa identificar e estimar as probabilidades de ocorrência das situações, em condições não-usuais, nas quais o operador pode tomar ações que tornam a planta menos segura.

Para suportar esta metodologia, foi criado um banco de dados (COOPER *et al.*, 1995), denominado Human System Event Classification Scheme, HSECS, para documentar e classificar os eventos operacionais analisados e permitir estudos posteriores.

A metodologia fornece orientações para analisar (tanto retrospectivamente quanto prospectivamente) o tipo de desempenho humano inadequado (erro de comissão), que contribui para o risco e que pode ser, totalmente, integrado com a APS. Está organizada em torno de uma plataforma de trabalho multidisciplinar, a qual é aplicada, diretamente, às análises retrospectivas de eventos operacionais e fornece uma base para as análises prospectivas. A estrutura sistematizada das diferentes dimensões que influenciam as interações homem/sistema, representadas nesta plataforma juntamente com as pesquisas dos contextos de demandas cognitivas (as quais são orientadas por considerações de elementos de processamento cognitivo da

informação), proporciona uma clareza e completeza do processo de modelagem do erro humano para as APS's.

4.2.1 Plataforma de trabalho multidisciplinar

Esta plataforma multidisciplinar surgiu de um estudo prévio (NUREG/CR-6265, 1995), iniciado em fevereiro de 1992, e que serviu de base para o desenvolvimento da ATHEANA. A plataforma envolve uma equipe multidisciplinar (operação e engenharia de usina, APS, fatores humanos e ciências comportamentais) e permite utilizar o conhecimento e o entendimento destas disciplinas relevantes para analisar o desempenho humano significativo para o risco, em acidentes de usinas nucleares.

O conceito fundamental da plataforma é que muitas das ações inseguras resultam da combinação das condições da planta e dos fatores que formatam o desempenho, associados a estas condições, os quais disparam os mecanismos de erro nos operadores da planta.

A figura 4.1 é a representação gráfica desta plataforma. Os elementos relacionados com a performance humana (principalmente os relacionados com as disciplinas de fatores humanos, ciências comportamentais e engenharia) estão localizados no lado esquerdo da figura. São os fatores que formatam o desempenho (PFS), as condições da planta e os mecanismos de erro. Estes elementos representam as informações necessárias para descrever as influências fundamentais na ação insegura e, portanto, explicar porque a pessoa pode executar esta ação. Os elementos da direita da figura, representados pelos eventos de falha humana (HFE, human failure event) e a definição do cenário (cenário específico de acidente), representam o modelo da APS. Os elementos da ação insegura e dos eventos de falha humana (HFE), representam o ponto de integração entre os modelos de análise de confiabilidade humana (ACH) e análise probabilística de acidentes (APS).

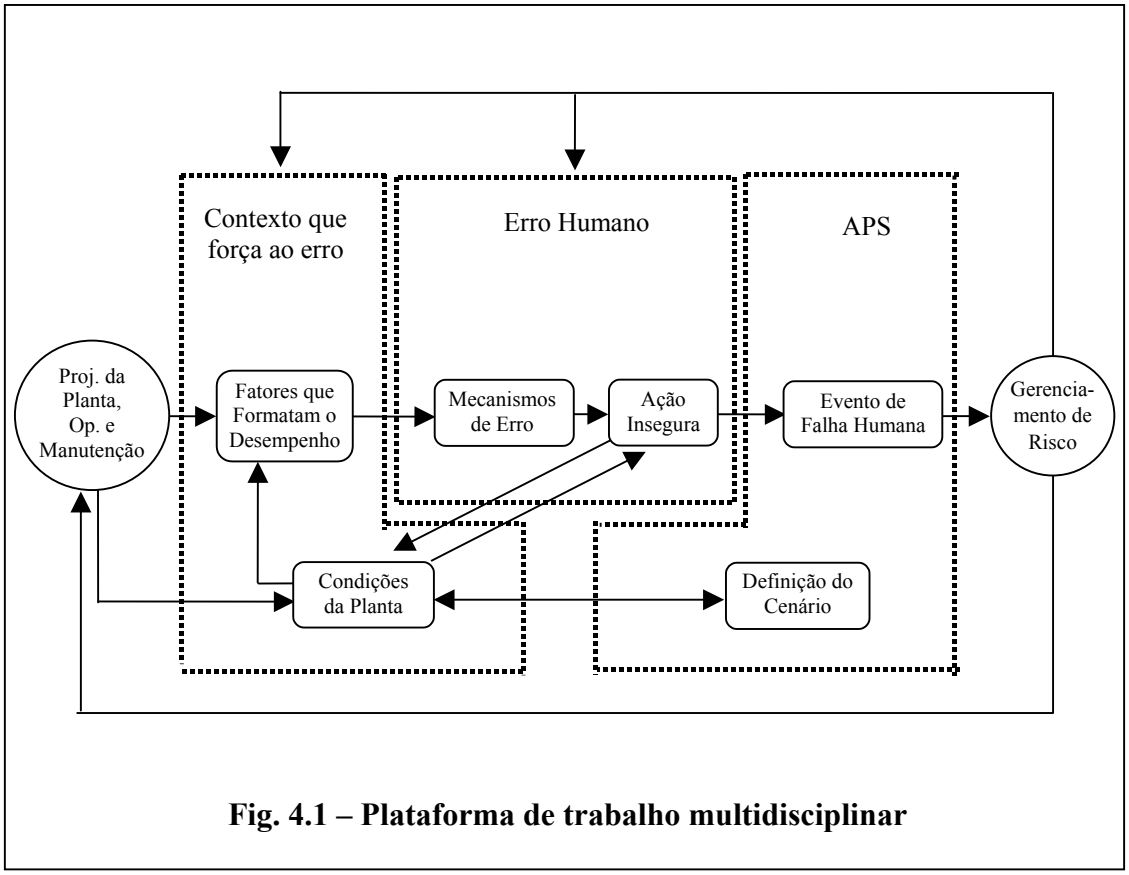


Fig. 4.1 – Plataforma de trabalho multidisciplinar

4.2.1.1 Contexto que força ao erro (EFC, error-forcing context)

O EFC é o efeito combinado dos fatores que formatam o desempenho (PSF) e das condições da planta, que cria uma situação na qual o erro humano é provável de ocorrer. As análises dos eventos têm mostrado que o EFC envolve, tipicamente, a combinação de condições não analisadas da planta, as quais estão além do treinamento normal dos operadores, e os PSF's relacionados com procedimentos. Estas condições da planta, podem ativar um mecanismo de erro humano relacionado, por exemplo, com a avaliação inadequada da situação (fazer um quadro errado da situação). Consequentemente, quando estas condições da planta e os PSF's

associados dispararem os fatores psicológicos internos (mecanismos de erro), eles podem levar a uma rejeição em acreditar nas evidências que se contrapõem ao diagnóstico inicial errado ou a falha em reconhecer aquelas evidências, resultando em um erro subsequente (por exemplo, erro de comissão), culminando em um acidente catastrófico.

As "condições da planta" incluem a configuração física da planta, as condições de disponibilidade e confiabilidade dos sistemas componentes e instrumentação e controle, parâmetros do processo (por exemplo, reatividade do núcleo, nível de potência, pressão, temperatura e inventário do sistema de refrigeração do reator) e outros fatores (não usuais e condições dinâmicas) que resultam em uma configuração ou comportamento não usual da planta.

Os fatores que formatam o desempenho representam as influências centradas no homem que podem afetar o seu desempenho. Elas são relativas a:

- procedimentos;
- treinamento;
- comunicação;
- supervisão;
- interface homem-sistema;
- fatores organizacionais;
- estresse;
- condições ambientais;
- tempo;
- carga de trabalho; e
- disponibilidade de recursos (ajuda ao operador)

Um exemplo de PSF pode ser um procedimento cujo conteúdo está incorreto (por exemplo, a sequência dos passos está errada), incompleto (por exemplo, uma determinada condição não é contemplada), ou confuso (por exemplo, direcionamento

ambíguo) e que contribuem para uma falha de avaliação da situação ou planejamento da resposta.

4.2.1.2 Erro humano

O erro humano pode ser caracterizado como uma divergência entre uma ação realizada e uma ação que deveria ter sido realizada, que tem um efeito ou conseqüência fora da tolerância requerida pelo sistema em questão com o qual o homem está interagindo.

Este significado de erro humano é diferente do utilizado pela APS, a qual considera erro humano como sendo a falha causada pelo homem, isto é, a conseqüência do erro. Para as ciências comportamentais, o interesse está nos fundamentos das causas dos erros.

Para a ATHEANA, o erro humano compreende o mecanismo básico do erro humano e as consequências deste mecanismo, que é a ação insegura (UA).

Os mecanismos de erro são utilizados para descrever os mecanismos psicológicos que contribuem para o erro humano, que podem ser disparados por uma condição particular da planta e dos PSF's.

As ações inseguras (UA, unsafe action) são aquelas ações tomadas, inadequadamente, pelo pessoal da planta, ou não tomadas quando necessário, que resultam em uma degradação das condições de segurança da planta. A designação "ação insegura" não implica que o homem foi a causa do problema; os operadores são levados, pelas circunstâncias e pelas condições presentes, a executar estas ações que degradam a segurança. Nestas circunstâncias, a pessoa não cometeu um erro de conhecimento; ela estava executando uma ação que, no momento, parecia ser correta.

4.2.1.3 Modelo da APS

O modelo de APS identificado na plataforma ATHEANA não é diferente daqueles existentes nas metodologias usuais de APS. No caso presente, a APS é um cliente final do processo de ACH. A APS é utilizada para estimar a freqüência de um determinado cenário que leva a planta à condições inaceitáveis, como por exemplo fusão do núcleo. Ela converte o modelo lógico em modelo probabilístico. Para isto deve obter a probabilidade de cada evento, representado no modelo, inclusive os eventos de falha humana. Quando as atividades relacionadas ao desempenho humano são analisadas para serem incluídas nas APS's, isto é feito no contexto dos eventos de falha humana (HFE), aplicável a um determinado cenário específico de acidente, definido pelo estado da planta e representado pelo modelo lógico da APS. Os HFE's são modelados nas APS's para representar falhas de funções, sistemas ou componentes, como resultado de ações humanas que degradam as condições de segurança da planta.

Um evento básico da APS representa uma mudança incorreta no estado do equipamento afetado dentro do contexto das definições de eventos no modelo da árvore de eventos. Como o estado da planta não muda, instantaneamente, ao ocorrer uma falha humana, os HFE's são definidos para representar, não somente o erro cometido, como também a falha do pessoal da planta em reconhecer que um erro foi executado e, desta maneira, não realizar quaisquer ações corretivas antes de ocorrer uma mudança do estado da planta. Dependendo do que se deseja que o HFE represente, este pode ser associado com uma sequência completa de uma árvore de eventos ou com um corte mínimo gerado pela solução do modelo da APS. O nível de decomposição adequado do cenário é aquele necessário para satisfazer a definição única de um HFE com respeito ao impacto das condições da planta na probabilidade do HFE.

As definições dos cenários das APS's fornecem uma descrição mínima das condições da planta requeridas para desenvolver a APS e definir os HFE's adequados. Exemplos:

- evento iniciador (por exemplo, transientes, pequena perda de refrigerante do reator, perda de potência elétrica externa, etc.);
- modo de operação;
- nível de calor de decaimento (para APS em desligado);
- Estado da função/sistema/componente ou configuração

O nível de detalhes para a definição dos cenários pode ser variado e pode ser a nível:

- funcional;
- de sistema; e
- do estado de componentes (isto é, falha ou sucesso de componentes ou, usando a terminologia de analistas de sistemas, cortes)

4.2.2 Comentários iniciais sobre a metodologia ATHEANA

A ATHEANA foi desenvolvida para subsidiar as aplicações das APS's. Entretanto, pode ser usada como uma ferramenta para análises qualitativas como por exemplo, para classificar, segundo um determinado grau de importância, várias alternativas que se apresentam, ou até mesmo para identificar cenários e EFC's, sem a necessidade de quantificar a sua contribuição para o risco. Igualmente, os cenários problemáticos, identificados em sua pesquisa, podem ser utilizados no treinamento de operadores, sem a necessidade de sua quantificação. Adicionalmente, a ATHEANA, também é utilizada para análise de eventos operacionais ocorridos (análise retrospectiva).

Como identificado nos eventos operacionais analisados, existe uma distinção marcante entre os eventos reais ocorridos e os descritos nos métodos atuais de ACH:

eventos reais, frequentemente, incluem erros de comissão (EOC) pós-acidente, os quais são, minimamente, considerados nas APS's e ACH's atuais, e que são, fortemente, influenciados pelo contexto específico do acidente; por sua vez, o contexto específico de um evento, frequentemente, se afasta das condições nominais da planta assumidas durante operação à potência.

Consequentemente, a modelagem adotada pela ATHEANA difere, significativamente, das utilizadas pelos métodos atuais de ACH. A premissa fundamental da ATHEANA é que os HFE's significativos ocorridos após o início do evento, especialmente os EOCs, representam situações nas quais, os contextos do evento (condições da planta e PSF's), virtualmente, levam o operador a errar. A definição dos HFE's e suas quantificações estão baseadas nos EFC dos eventos, especialmente, nas condições não usuais. A ATHEANA tem uma preocupação especial em identificar certas condições específicas que se apresentam em forma de desvios do comportamento da planta em relação ao que o operador espera ver ou ao que está descrito nos procedimentos de operação/treinamento, que criam diferenças entre a expectativa e o comportamento real da planta. Este enfoque representa uma diferença significativa em relação aos métodos tradicionais de ACH, nos quais os eventos de falha humana são definidos e quantificados como sendo o resultado de falhas randômicas do operador, que ocorrem sob condições nominais de acidentes. Em vista disto, a modelagem feita pela ATHEANA envolve um modelo de quantificação diferente. Em particular, deve prover uma abordagem melhor e mais completa para identificar e definir os HFE's de interesse e inserí-los nos modelos das APS's. Como resultado, novas atividades são requeridas para a aplicação da ATHEANA, além daquelas dos métodos tradicionais de ACH, para identificar os HFE's não previamente incluídos nas APS's, juntamente com as UA's contribuidoras e os EFC's associados. Os analistas de ACH buscam identificar combinações de condições anormais, juntamente com PSF's associados, que aumentam, fortemente, a

probabilidade de ocorrência das UA's. Os analistas utilizam os conhecimentos das causas das falhas humanas extraídas da psicologia e da análise da experiência operacional. Além dos elementos acima, ATHEANA envolve algumas das tarefas típicas existentes nos métodos tradicionais de ACH.

A representação, em ATHEANA, dos HFE's pós-acidente, provenientes de EOC, é similar à representação dos EOO utilizada pelos métodos atuais (por exemplo, eles serão identificados e definidos em termos de falha de função da planta, sistema ou componentes). Porém, a definição de EOO está baseada em falhas de ações manuais do operador em iniciar ou mudar o estado dos equipamentos da planta. Portanto, a definição de EOO, tipicamente, é dita, por exemplo, como "o operador falha em partir uma bomba." Os EOC devem ser definidos diferentemente, uma vez que, geralmente, os EOCs pós-acidente resultam de um dos seguintes modos pelos quais, os operadores podem causar a falha da função da planta, sistema ou componentes:

- desligando equipamentos que estão operando;
- desviando sinais de partida automática de equipamentos;
- mudando a configuração da planta de maneira que anula intertravamentos que são projetados para evitar danos aos equipamentos; e
- esgotando, excessivamente, ou divergindo recursos da planta (por exemplo, água).

Para as APS's, a premissa da ATHENA é incluir, somente aqueles HFE's para os quais uma razão plausível e provável pode ser determinada. Um HFE pode resultar de uma entre diversas UA's. A aplicação da ATHEANA visa, para cada HFE, identificar e definir as UA's e os EFC's associados. Os EFC's identificados (por exemplo, as condições da planta e os PSF's associados) e seus mecanismos de erros básicos são os meios de caracterizar as causas das falhas humanas. Uma UA pode resultar de uma entre várias causas diferentes.

Na aplicação da ATHEANA, os HFE's serão classificados de acordo com a probabilidade das UA's contribuidoras, e estas, por sua vez, de acordo com as probabilidades dos EFC's. Portanto, a quantificação de um HFE, usando ATHEANA, está baseada na resposta das seguintes questões:

- Quais UA's pode resultar no HFE para o qual a probabilidade está sendo quantificada?
- Quais EFC's pode resultar em executar cada uma das UA's iniciais?
- Quais EFC's pode resultar na falha de recuperação de cada UA inicial?
- Quão provável é a ocorrência destes EFC's?

4.3 A Importância das condições da planta e do contexto

A análise dos eventos operacionais, que subsidiaram o projeto de desenvolvimento da ATHEANA, identificou um aspecto importante que foi o reconhecimento de que as condições da planta são influências chaves no desempenho do operador e que estas condições podem ser muito mais diversificadas do que as representadas pelos métodos, atualmente, existentes de ACH e APS. Esta seção descreve as considerações apresentadas pela ATHEANA, das condições da planta e seus contextos associados, como fatores importantes para a sua metodologia.

4.3.1 A importância do contexto

ATHEANA, no seu desenvolvimento, considerou os estudos mais recentes das ciências comportamentais (REASON, 1990, HOLLNAGEL, 1993) sobre a natureza interativa do erro humano e o comportamento da planta, a qual sugere que é essenciais analisar os fatores centrados no homem (PSF's, tais como interface homem-máquina, conteúdo e formato dos procedimentos e treinamento) e as condições da planta que requerem ações e criam as necessidades de interação homem-sistema (instrumentos descalibrados, equipamentos não disponíveis e outras

configurações não usuais e circunstâncias operacionais). Estes fatores não são independentes entre si e, como a própria experiência já demonstrou, a sua interação, sob condições desfavoráveis, leva as pessoas a cometer erros quando realizando ações em resposta a um acidente.

Para identificar as condições mais favoráveis que levam ao erro, as análises dos PSF's devem considerar que as condições da planta variam, significativamente, dentro de um mesmo cenário definido pelas árvores de eventos e árvores de falhas das APS e que, em certas condições, demandam mais dos operadores do que em outras.

Por exemplo, a disposição dos indicadores e controles pode ser, perfeitamente, adequada para uma determinada condição nominal assumida nas APS. Entretanto, desvios das condições nominais podem ocorrer e esta disposição dos indicadores e controles influenciar o operador a cometer erros em resposta ao acidente. Um exemplo de tal desvio, ocorrido em TMI-2, foi a localização por onde ocorreu a perda de refrigerante. As condições típicas assumidas para um acidente de pequena perda de refrigerante incluía a queda de nível do pressurizador, mas não a indicação de posição da válvula de alívio do pressurizador (PORV, power operated relief valve). Todavia, o desvio criado pelo vazamento pela PORV tornou estas indicações muito mais importantes, acrescido do fato que, a condição nominal esperada não ocorreu (o nível ao invés de descer, subiu).

Simplesmente, pode-se dizer que, é mais provável ocorrerem falhas dos operadores em cenários associados à APS, onde houver um desvio das condições típicas nominais, as quais criam um desafio significativo para os operadores, do que erros humanos randômicos em condições nominais assumidas pelos analistas de APS. Esta posição, que é muito mais significativa do que erros humanos randômicos, é sustentada pelas análises dos acidentes e quase-acidentes (NUREG-1275, Vol. 8, 1992, NUREG/CR-6093, 1994, NUREG/CR-6265, 1995), ocorridos em usinas

nucleares. A importância do contexto também tem sido considerada por outros métodos avançados de ACH (NUREG-1624, Rev.1¸ 2000).

A importância dos contextos não usuais (desvios) é consistente com a experiência descrita por instrutores de simuladores, que afirmam que “os operadores podem ser induzidos a errar” pela criação de um conjunto particular de condições da planta e fixação mental (mindset) do operador (NUREG-1624, Rev.1¸ 2000).

Os desvios de contextos que desafiam, significativamente, os operadores, apresentam-se sob vários tipos, conforme foi observado nas análises dos eventos que apresentaram um alto potencial de degradação da segurança. Eles incluem:

- Desvios físicos: a planta comporta-se, diferentemente, do que é esperado dos cenários típicos da APS. As indicações das condições da planta poderão ser, significativamente, diferentes das expectativas dos operadores e das bases dos procedimentos e treinamentos dos operadores;
- Desvios temporais: as escalas de tempo das condições da planta são diferentes daquelas assumidas nos cenários das APS’s e podem afetar a escala de tempo na qual o operador deve atuar. Os sintomas podem ocorrer mais lentamente, fora de sequência ou mais rapidamente, do que aqueles assumidos em procedimentos e treinamentos, causando diferentes tipos de impactos nos operadores;
- Desvios das causas dos eventos iniciadores: falhas parciais em equipamentos ou em sistemas suportes podem criar um conjunto de sintomas inesperados, que podem confundir ou enganar o operador e levá-lo a agir indevidamente ou a demorar em tomar uma ação; e
- Desvios associados com falhas do sistema de instrumentação: afetam (dificultam) a habilidade do operador de entender as condições da planta e, portanto, o planejamento das respostas adequadas. Adicionalmente, as falhas na instrumentação podem causar todos os tipos de desvios acima.

Estes tipos de desvios podem levar o operador a errar. Por exemplo, quando a planta se comporta de uma maneira diferente da expectativa do operador (uma diferença entre as condições da planta e o seu treinamento), o operador pode responder de acordo com suas expectativas e a ação resultante pode levar a perda de um equipamento importante ou de uma função, que é necessária para a condição, atualmente, em andamento. Em TMI-2, os operadores acreditavam que o sistema do reator estava indo para a condição sólida e desligaram o sistema de injeção de segurança, o que levou a perda de resfriamento e fusão parcial do núcleo. Exemplos de eventos operacionais mais recentes, apresentados abaixo, indicam que, apesar das mudanças em treinamento e desenvolvimento de novos procedimentos, estes desvios (mismatches, diferenças entre o real e o esperado) continuam a ser uma preocupação para a operação.

Segundo a ATHEANA, a APS, para ser uma ferramenta efetiva para medir e controlar o risco, deve ser capaz de, realisticamente, incorporar aquelas falhas humanas que são causadas pelas condições anormais da planta, assim como aquelas que ocorrem, randomicamente, durante condições nominais de acidentes.

O conceito de desvios (mismatch) é utilizado pela ATHEANA para fornecer uma base para as pesquisas das condições ou situações que desafiam os operadores. Alguns tipos de desvios são utilizados para identificar contextos específicos que podem causar falhas.

4.3.2 Efeitos das condições da planta e do contexto na operação

Os eventos descritos a seguir, foram analisados usando a plataforma de trabalho multidisciplinar como orientação para os fatores importantes que influenciam o desempenho humano.

4.3.2.1 Revisão de eventos usando ATHEANA

A descrição (NUREG-1624, Rev.1¸ 2000) dos dois eventos abaixo ilustra os fatos vistos anteriormente. Todos os eventos envolvem erros humanos importantes pós-acidente, os quais são o foco da ATHEANA.

(1) TMI-2: em 3 de março de 1979, ocorreu um transiente de perda de água de alimentação principal, com o conseqüente desarme automático do reator. As bombas de água de alimentação de emergência partiram automaticamente, mas um erro de alinhamento de válvulas impediu o fluxo para os geradores de vapor. Um cartão de aviso de manutenção encobriu a indicação de que estas válvulas tinham sido fechadas. Uma válvula de alívio do pressurizador abriu, automaticamente, em resposta ao aumento de pressão do circuito primário e não fechou (travou aberta). Entretanto, a sua indicação, na sala de controle, era de que tinha fechado. O operador falhou em reconhecer que esta válvula não fechou, por cerca de 2 horas, resultando em perda de água de refrigeração do reator. Adicionalmente, os operadores reduziram o fluxo de injeção de segurança de alta pressão para o vaso do reator por 3,5 horas, porque estavam preocupados em evitar tornar o sistema de refrigeração do reator "sólido" (causaria perda de controle de pressão), resultando em um resfriamento inadequado do reator e sérios danos ao núcleo do reator. O evento foi terminado quando novos operadores que entraram em serviço identificaram a válvula aberta e a fecharam.

(2) Crystal River 3*:* em 8 de dezembro de 1991, um transiente de pressão ocorreu durante elevação de potência, logo após a partida do reator. Uma válvula de spray do pressurizador abriu totalmente e travou aberta. Entretanto, a sua indicação na sala de controle, mostrava que a mesma estava fechada. Os

operadores falharam em reconhecer que a válvula de spray tinha permanecido aberta. Os operadores, acreditando que a queda de pressão era devido a uma contração de volume causado por um resfriamento qualquer, retiraram as barras de controle para aumentar a potência. Esperavam que o aumento de temperatura iria criar um fluxo de água para o pressurizador, o que poderia recuperar a pressão. Entretanto, a pressão continuou a cair e o reator desarmou por baixa pressão. Após o desarme, a pressão continuou a cair até o ponto de armação dos dispositivos de engenharia relacionados à segurança (ESF). O operador desviou a atuação automática e por 6 minutos este sistema esteve impedido de operar, embora requerido. O supervisor do operador, posteriormente, orientou para desfazer o bloqueio e o sistema de injeção de segurança entrou em operação, automaticamente. A pressão foi controlada pela injeção de alta pressão. O transiente de pressão foi encerrado após o fechamento da válvula de isolamento da válvula de spray, por orientação de um outro supervisor, alheio ao turno de operação.

Estes eventos ilustram os conceitos básicos da ATHEANA. Em TMI-2, a interrupção do fluxo de injeção foi um EOC que resultou em sérios danos ao núcleo. Em Crystal River 3, o desvio do ESF foi, também, um EOC que impediu a atuação da injeção de segurança no sistema de refrigeração do reator. Entretanto, esta ação insegura do operador foi recuperada sem ocorrer danos ao núcleo.

O contexto teve um importante papel nestes eventos. Em TMI-2, as condições da planta contribuíram para o evento incluindo a preexistência do erro de alinhamento das válvulas de água de alimentação de emergência e da válvula de alívio que travou aberta. Isto, combinado com os fatores negativos que formatam o desempenho, incluindo o cartão de aviso de manutenção que obstruía a indicação de posição das válvulas de água de alimentação de emergência, o erro de indicação de posição da

válvula de alívio e a falta de procedimento para as condições específicas do evento. Outras indicações de que a válvula de alívio tinha permanecido aberta foram mal interpretadas e desprezadas pelos operadores. Adicionalmente, o treinamento dos operadores tinha enfatizado o perigo das condições sólidas da planta, levando os operadores a se concentrarem no problema errado.

O acidente de Crystal River 3 envolveu fatores similares, especialmente, a válvula de spray aberta e a sua indicação de posição errada. Não havia procedimento para orientar o diagnóstico e corrigir a perda de controle de pressão.

Aplicando os conceitos do modelo de processamento da informação para estes eventos, em todos eles a avaliação da situação foi crítica. Em TMI-2, os operadores não reconheceram que a válvula de alívio tinha permanecido aberta e que o núcleo estava superaquecendo. Em Crystal River 3, os operadores não reconheceram que a válvula de spray estava aberta e causando o transiente de queda de pressão. Estes problemas de avaliação da situação envolvem, tanto as fontes das informações (por exemplo, a instrumentação) como as suas interpretações. Em TMI-2, os operadores erraram duas vezes, em interpretar a indicação de temperatura da tubulação de dreno da válvula de alívio, atribuindo a alta temperatura de entrada no núcleo do reator e do circuito do sistema de refrigeração do reator, à uma falha da instrumentação. Eles também foram levados a errar pela indicação da posição da válvula de alívio. Também, alguns indicadores chaves estavam localizados nos painéis traseiros e a impressora do computador dos parâmetros da planta fazia a impressão com 2 horas de atraso. Em Crystal River 3, os operadores, inicialmente, conjeturaram que o transiente de pressão foi causado por uma contração do sistema de refrigeração do reator. Indicadores da planta não relacionados com o evento, assim como a indicação errada da posição da válvula de spray e a ciclagem (sem sucesso) da mesma foram tomadas como suporte para esta hipótese.

4.3.2.2 Outros relatórios

Vários outros estudos de acidentes confirmam os princípios básicos da ATHEANA. Segundo o NUREG-1624, Rev.1 (2000), as análises de acidentes em transporte e aviação e a revisão de acidentes em plantas químicas indicaram que, um contexto que força ao erro está, frequentemente, presente em sérios acidentes envolvendo o controle operacional humano nestas industrias. REASON (1990) identificou importantes fatores contextuais em vários acidentes sérios, incluindo o acidente de TMI-2 e a explosão do ônibus espacial Challenger, em janeiro de 1986. As análises de acidentes em usinas nucleares descritas no NUREG-1275, Vol. 8 (1992) identificaram condições não nominais da planta e procedimentos associados deficientes para estas condições, como, fortemente, influenciando 8 entre 11 eventos que foram significativamente afetados pelas ações humanas. De 11 eventos, 6 envolveram EOC. O relatório AEOD/E95-01 (1995) da NRC, identificou 14 eventos, em um período de 41 meses (ver Anexo A), nos quais os ESF foram inadequadamente desviados, todos eles considerados como EOC. O NUREG/CR-6208 (1994) identificou a avaliação da situação e o planejamento da resposta como importantes fatores em experimentos em simulador envolvendo situações de demanda cognitiva (isto é, situações não totalmente cobertas por procedimentos ou treinamento porque as condições da planta, para o evento específico simulado, eram diferentes das nominais). Também, o programa (BEARE *et al.*, 1991) Operator Reliability Experiment (ORE) do Electric Power Research Institute (EPRI), cita que, 70% dos erros dos operadores ou quase-erros (near-misses) observado nos experimentos de simulador, independentemente, do tipo de reator, foram categorizados como erros de processamento de informação ou de diagnóstico e tomada de decisão.

4.4 Perspectivas das ciências comportamentais

Na seção 4.2 foi mostrado que uma das partes da plataforma, que serve de base para a metodologia ATHEANA, é a relação entre as ações inseguras, mecanismos de erro e contextos que forçam ao erro. Esta relação pode ser obtida de duas fontes paralelas, porém, complementares: (1) de um entendimento das falhas humanas derivadas dos modelos de comportamento humano criado dentro das disciplinas de ciências comportamentais e, (2) de uma análise dos eventos operacionais.

Segundo o NUREG-1624, Rev.1 (2000), as conclusões dos estudos dos últimos 30 anos das causas dos erros humanos é que, poucos erros são de causa randômica e a maioria pode ser explicada pela maneira como o homem processa a informação em situações complexas e de alta demanda. Portanto, o entendimento das bases do processo cognitivo associado com a monitoração, tomada de decisões e controle da planta e como estes podem levar ao erro humano é de fundamental importância para a sua análise.

O processamento da informação pode ser descrito por um modelo básico de representação, que descreve as atividades humanas requeridas para fazer face às condições anormais e de acidentes. Este modelo envolve, basicamente, quatro passos cognitivos:

(1) avaliação da situação

(2) monitoração/deteção

(3) planejamento da resposta

(4) implementação da resposta

4.4.1 Análise do desempenho humano cognitivo

A figura 4.2 ilustra as principais atividades cognitivas fundamentais relativas ao desempenho humano.

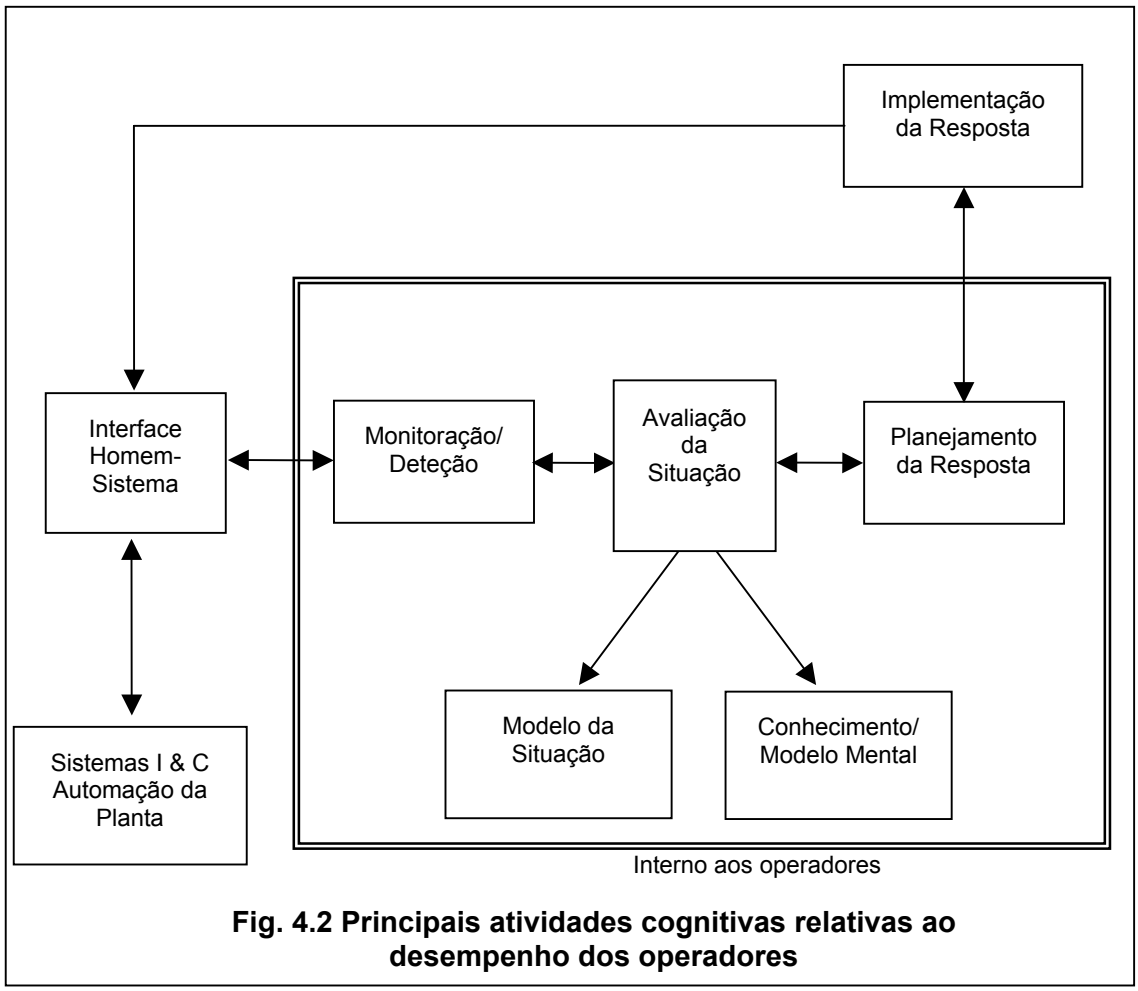


Fig. 4.2 Principais atividades cognitivas relativas ao desempenho dos operadores

4.4.1.1 Avaliação da situação

Quando as pessoas se defrontam com situações anormais, rapidamente, elas tentam construir uma explicação lógica, coerente para estas observações. Este processo é chamado de avaliação da situação. A avaliação da situação envolve o desenvolvimento e atualização, constante, de uma representação mental dos fatores conhecidos ou imaginados (hipóteses) que podem estar afetando o estado da planta

naquele momento. A representação mental, resultante da avaliação da situação, é referida como um modelo da situação. O modelo da situação é o entendimento que a pessoa tem de uma situação específica corrente e este é, constantemente, atualizado a cada nova informação recebida.

A avaliação da situação é similar, em significado, a diagnóstico, mas com um aspecto mais amplo. Diagnóstico refere-se à pesquisa das causas de sintomas anormais. Avaliação da situação envolve explicações que são geradas para justificar condições normais e anormais.

Os operadores, baseados em seus conhecimentos e entendimentos gerais sobre a planta e como ela opera, avaliam a situação para gerar um modelo. O conhecimento do operador é obtido através de treinamento e pode variar, desde detalhes específicos de conhecimento, até princípios genéricos abstratos que são aplicáveis a uma ampla classe de situações. A ATHEANA considera quatro tipos diferentes de conhecimentos (de episódios, estereotípicos, modelo mental e de procedimento) que são utilizados para gerar e manter atualizado, o modelo da situação.

O modelo da situação é utilizado para gerar uma expectativa, que inclui os eventos que estão ocorrendo no momento, como eles se comportam com o tempo e as consequências que podem ocorrer. A expectativa é utilizada para procurar por evidências, que confirmam o modelo da situação criado. A expectativa também é utilizada para explicar os sintomas observados. Se um novo sintoma for consistente com sua expectativa, o operador tem uma pronta explicação para a situação e reforça a sua confiança no modelo da situação criado. Por outro lado, se o novo sintoma não for consistente com sua expectativa, este sintoma pode ser ignorado ou mal interpretado, de maneira a torná-lo consistente, novamente, com a sua expectativa. Entretanto, se o novo sintoma for devidamente reconhecido como um comportamento não esperado da planta, então, neste caso, a necessidade de revisar o modelo da

situação torna-se evidente. Por conseguinte, a avaliação da situação pode envolver o desenvolvimento de uma hipótese para o que está ocorrendo e então procurar por evidência.

A avaliação da situação pode resultar na deteção de alguma anormalidade no comportamento da planta que não tinha sido ainda observada, na deteção de sintomas e alarmes que não foram vistos ou observados no momento em que apareceram e na identificação de falhas de sensores e maus funcionamentos da planta.

4.4.1.2 Monitoração e deteção

Monitoração e deteção referem-se às atividades de extração das informações do meio ambiente. Elas são influenciadas por dois fatores fundamentais: as características do ambiente e o conhecimento e expectativa da pessoa.

A monitoração que é orientada pelas características do ambiente são, frequentemente, denominadas de monitoração orientada por dados (data-driven monitoring). Este tipo de monitoração é afetado pelo formato da informação, seu destaque físico (por exemplo, tamanho, cor, som, etc.). Características especiais destes destaques físicos (intensidade do som, tipos de cores, etc.), permitem ao operador identificar informações mais importantes. O comportamento da informação (velocidade e faixa de variação) sendo monitorada, também afeta este tipo de monitoração.

A monitoração também pode ser iniciada pelo operador, baseada no seu conhecimento e expectativa ou por um procedimento específico (por exemplo, durante troca de turno onde é feita uma revisão de todo o painel de controle). Este tipo de monitoração é, tipicamente, referida como monitoração orientada pelo conhecimento (knowledge-driven) e pode ser vista como uma monitoração ativa.

Em situações anormais, onde o operador se defronta com informações contendo mais variáveis do que pode realisticamente monitorar, o operador tem que

decidir o que monitorar e quando mudar a sua atenção. Estas decisões são fortemente dirigidas pelo modelo da situação que o operador criou, o qual também é utilizado para determinar se um sinal é significativo e se indica uma anormalidade real ou uma falha de instrumentação.

4.4.1.3 Planejamento da resposta

Planejamento da resposta se refere ao processo de tomar a decisão de qual ação executar. Em geral, envolve o modelo da situação criado, para identificar objetivos, gerar planos de resposta alternativos, avaliar planos de resposta e selecionar o plano de resposta mais adequado para o modelo da situação corrente. Em determinadas situações, alguns destes passos podem não ser necessários, por exemplo, quando existirem procedimentos escritos e julgados adequados para a situação corrente, então, a necessidade de gerar um plano de resposta em tempo real pode ser desnecessário. Entretanto, mesmo com a existência destes procedimentos, alguns dos aspectos do planejamento da resposta precisam ser ainda realizados. Por exemplo:

(1) Identificar os objetivos adequados de acordo com sua avaliação da situação;

(2) Selecionar o procedimento adequado;

(3) Avaliar se as ações definidas no procedimento são suficientes para atingir os objetivos; e

(4) Adaptar o procedimento à situação, se necessário.

É importante para o operador monitorar a efetividade do plano de resposta, mesmo quando está descrito em procedimentos estabelecidos. A monitoração inclui a avaliação das consequências de uma ação particular executada, requerida pelo procedimento, e avaliação da adequabilidade do andamento do procedimento, para atingir os objetivos. Isto permite ao operador detetar quando o procedimento não está

atingindo os seus objetivos, quando contém erros ou quando ocorrem erros na realização dos passos.

Outra atividade cognitiva incluída no planejamento da resposta é a adaptação do plano. Isto inclui preencher alguma deficiência no procedimento, adaptar o procedimento a uma situação específica e redirecionar o andamento do procedimento.

4.4.1.4 Implementação da resposta

Implementação da resposta refere-se a tomar as ações específicas de controle, como planejadas, para executar a tarefa.

O resultado das ações implementadas é monitorado pelo retorno (feedback) das informações. Dois aspectos podem tornar a implementação da resposta difícil: a observação indireta e o tempo de resposta. Os processos da planta não são diretamente observados, eles precisam ser inferidos através de indicações e então, erros podem ocorrer neste processo. Os sistemas das usinas nucleares são, relativamente, lentos em responder, comparadas com outros tipos de sistemas, tais como aviões. Estes fatos tornam difícil determinar se as ações de controle estão tendo os efeitos desejados. Nestes casos, a habilidade do operador, em prever os estágios futuros usando modelos mentais, pode ser mais importante em controlar as ações de resposta do que o retorno da informação.

4.4.2 Fatores cognitivos que afetam o desempenho do operador

Três classes de fatores cognitivos afetam a qualidade das respostas da maioria das atividades cognitivas e desta maneira, afetando o desempenho dos operadores. Elas são: conhecimento, recursos de processamento e fatores estratégicos. Poderão surgir erros quando existir uma desigualdade entre o estado destes fatores (isto é, das fontes cognitivas disponíveis para o operador) e as demandas impostas pela situação.

4.4.2.1 Fatores do conhecimento

Dois problemas devem ser considerados em relação à influência dos fatores do conhecimento: conteúdo e acesso. O conteúdo está relacionado com o conhecimento, já visto anteriormente. O acesso, também conhecido como recuperação da memória (memory retrieval) é altamente dependente do contexto. Significa dizer que particularidades (“dicas”) do contexto facilitarão a recuperação das informações da memória; quanto mais “dicas” houver, maior a probabilidade de que a informação será acessada.

Existem outros fatores que influenciam a recuperação da memória tornando algum tipo de informação mais facilmente recuperável do que outra: fatos que aconteceram recentemente (recency), fatos que ocorrem com uma frequência maior (frequency) e fatos similares (similarity). Em algumas circunstâncias, estes fatores poderão recuperar informações que não são totalmente adequadas para a situação. Por exemplo, se uma determinada situação inclui fatos que são similares a um evento ocorrido recentemente, o operador poderá recuperar as informações deste evento e interpretar como se a situação presente fosse a mesma.

Adicionalmente, informações relevantes que o operador possa ter, podem nunca serem recuperadas. Por exemplo, se uma situação que raramente ocorre, possui fatos em comum com um evento que é mais familiar, o operador pode falhar em reconhecer o evento raro quanto este ocorrer porque ele interpretará a informação como um indicativo do evento familiar.

4.4.2.2 Fatores dos recursos de processamento

As atividades que os operadores executam utilizam recursos de processamento cognitivo. Entretanto, as pessoas não possuem recursos cognitivos, tais como atenção e memória, numa quantidade infinita. Pelo contrário, existe uma quantidade limitada que deve ser distribuída entre as tarefas que estão sendo

executadas, as quais apresentam, quase sempre, diferenças em termos de demanda dos processos cognitivos. Se uma tarefa requer grande quantidade de recursos cognitivos, como atenção e memória, então haverá pouca disponibilidade destes recursos para executar outras atividades. Se um grupo de atividades utilizar quase todo o recurso de processamento disponível, então novas tarefas serão atrasadas até os recursos estarem, novamente, disponíveis. Se uma tarefa necessitar de mais recursos do que os disponíveis, então a execução desta tarefa poderá ficar prejudicada, talvez se tornando lenta, imprecisa ou propensa a erros.

A execução de tarefas familiares e bem treinadas necessita de poucos recursos cognitivos e são realizadas de uma maneira quase automática. Entretanto, quando a tarefa não for familiar, os limites dos recursos de processamento da informação tornam-se aparentes, o operador não mais responde de uma maneira automática, pelo contrário, torna-se lento, cauteloso e processa a informação de uma maneira serial. O processamento da informação torna-se mais em um controle consciente. Este tipo de processamento analítico drena, rapidamente, os recursos. Para superar tais demandas cognitivas, o operador tende a usar, cuidadosamente, atalhos, sem necessitar fazer uma análise completa da situação, denominados “heurísticos”. Este processo reduz os esforços e os recursos cognitivos e a incerteza de situações não familiares. Entretanto, por não fazer uma análise completa, poderá levar a um modelo de situação impreciso e a um planejamento inadequado da resposta.

4.4.2.3 Fatores estratégicos

Os fatores estratégicos influenciam as escolhas em situações de incerteza e de riscos, potencialmente, altos. Isto inclui situações onde existem múltiplos conflitos de objetivos, pressão do tempo e recursos limitados. Um exemplo seria a decisão de quando terminar a injeção de segurança, utilizada para mitigar certos tipos de

acidentes. Se a injeção for deixada operar por muito tempo, pode levar ao enchimento excessivo do pressurizador; no caso oposto, poderia haver uma redução significativa do resfriamento do núcleo do reator podendo levar a danos ao mesmo.

Estas situações também criam um conflito entre o custo e a produtividade, como por exemplo, no caso de um desligamento desnecessário do reator versus o custo da falha em tomar uma ação preventiva.

Existem, também, situações críticas de decisões relacionadas ao momento em que se deve executar uma determinada ação. Dentro das limitações de recursos de processamento e tempo disponível, em situações em que o operador tem que decidir em tomar uma ação corretiva, logo no início, baseada em informações limitadas, ou atrasar a resposta até outras informações tornarem-se disponíveis e uma melhor análise poder ser feita. Por um lado, em situações dinâmicas, de altas consequências potenciais (para o risco ou produtividade), o custo de esperar pode ser alto. Por outro lado, o custo de tomar uma decisão imediata e incorreta, também poderá ser alto.

Portanto, nas decisões que o operador está prestes a fazer, é necessário considerar, explicitamente, os fatores estratégicos que são prováveis de afetar o desempenho, incluindo a presença de múltiplos objetivos que se interagem, as vantagens da escolha de um em relação ao outro e vice-versa e as pressões presentes que mudam este critério de decisão para o que apresentar as melhores vantagens.

4.4.3 Falhas nas atividades cognitivas dos operadores

As falhas dos operadores podem ocorrer em qualquer uma das quatro principais atividades cognitivas (monitoração ou deteção, avaliação da situação, planejamento da resposta e implementação da resposta). Em situações de demanda cognitiva, a sequência típica da solução dos problemas pode assumir os seguintes quatro passos:

(1) Uma revisão geral é iniciada após o disparo de alarmes e sinalizações ou outros indicadores. A atenção do operador é dividida entre uma variedade de atividades de aquisição de dados;

(2) O operador se concentra em um grupo específico de indicadores e faz uma avaliação inicial da situação;

(3) O operador estrutura os recursos de atenção para procurar dados que confirmem a sua hipótese; e

(4) O operador pode ficar preso na hipótese e falhar em observar mudanças no estado da planta ou novos desenvolvimentos.

O operador pode, eventualmente, tomar conhecimento de mudanças subseqüentes, mas o processo é dificultado pela atenção sendo direcionada para a hipótese inicial e pelas limitações gerais do processo. Erros cognitivos originam-se das limitações do conhecimento, acesso às informações, recursos de processamento e fatores estratégicos. Estes erros cognitivos poderão ocorrer em qualquer uma das quatro atividades cognitivas principais, como mostrados a seguir.

4.4.3.1 Falhas na monitoração e deteção

O erro primário na monitoração e deteção é a falha em detetar ou observar as indicações da planta. Esta falha é função de:

- destaque físico da indicação;
- se a monitoração da indicação é uma prática padrão;
- a relevância da indicação;
- prioridade da monitoração em relação a outras atividades; e
- disponibilidade de recursos de atenção.

A monitoração é, freqüentemente, dirigida pelo conhecimento. A informação que o operador escolher a monitorar é determinada pelo seu modelo da situação,

onde, normalmente, o fator, influência da confirmação (influence bias), o direciona para procurar por evidências que confirmem sua hipótese, ao invés de evidências que a negam.

4.4.3.2 Falhas na avaliação da situação

A falha primária da avaliação da situação é falhar em interpretar, corretamente, uma observação. Ao observar as indicações, o operador faz um questionamento para identificar a qualidade da informação no que se refere à consistência com o seu entendimento das condições da planta, se a informação é esperada, isto é, se explica a situação existente, se o sinal é espúrio ou real, etc. Se o operador determinar que a observação é válida e não esperada, então ele inicia uma avaliação da situação que expliquem as observações. Entretanto, estas avaliações iniciais estão sujeitas a erros, onde o operador pode chegar a explicações incorretas das suas observações. Vários fatores podem influenciar como uma pessoa interpreta uma dada informação. Um deles está relacionado com o processo de recuperação da memória, já discutido anteriormente. Outro fator está relacionado com o processo da avaliação da situação. As pessoas estão mais propensas a procurar por informações consistentes com seus modelos da situação corrente. Isto está relacionado com o princípio da influência da confirmação. Uma vez gerada a hipótese para explicar um grupo de indicações, novas indicações serão explicadas, provavelmente, em termos da hipótese inicial ou então serão ignoradas. Uma falha em revisar a avaliação da situação, quando nova evidência é introduzida, é chamada de erro de fixação.

4.4.3.3 Falhas no planejamento da resposta

A falha primária durante o planejamento da resposta é falhar em estabelecer um plano de resposta correto. O planejamento da resposta envolve estabelecer objetivos, desenvolver um plano de resposta, que por seu turno envolve identificar e

executar procedimentos predefinidos, verificar se estes estão atingindo seus objetivos e, caso negativo, fazer modificações e adaptações para isto. Falhas no planejamento da resposta envolvem erros em todas estas etapas, que podem variar desde o uso de procedimentos errados, decisões incorretas, modelos da situação inadequados, deficiências de conhecimento, percepção inadequada do risco, até avaliações de ações fora do tempo, etc.

4.4.3.4 Falhas na implementação da resposta

A falha primária da implementação da resposta é falhar em executar as ações requeridas para a tarefa. Considerando erros de implementação, é assumido que o indivíduo pretende tomar as ações corretas mas, devido a um lapso de memória ou a uma ação não intencionada, falha em executar a ação requerida (erro de omissão); ou executa uma ação errada, sem intenção, ou executa a ação incorretamente.

Vários fatores podem contribuir para este tipo de erro: lapso de memória, erro ao ler um procedimento ou executar a ação pretendida (slip), falha de comunicação, etc.

4.4.4 Elementos contribuidores do contexto que força ao erro na operação de usinas nucleares de potência

O contexto, no qual os indivíduos estão inseridos (isto é, condições da planta e fatores que formatam o desempenho) é que determinará quais características serão ativadas ou implementadas em certas situações e se elas serão adequadas ou não. Como apresentado anteriormente, quando o mecanismo de processamento leva a uma ação inadequada com conseqüências que degradam a segurança, devido às influências do contexto , ele é referido como mecanismo de erro.

Um grupo importante de fatores relacionados ao contexto, provável de contribuir para um potencial mecanismo particular de erro tornar-se operativo em

cenários de acidentes, é o comportamento dos parâmetros que refletem os aspectos críticos das condições da planta, como por exemplo, o nível e pressão dos geradores de vapor. É suposto que, o comportamento de parâmetros críticos em relação ao tempo e um em relação ao outro, em conjunto com fatores relevantes que formatam o desempenho, tais como treinamento e experiência dos operadores, procedimentos da planta e a natureza da interface homem-máquina, tem um impacto significativo nas manifestações dos mecanismos de erro humano. A hipótese básica é que as características do cenário do acidente, representadas pelo comportamento dos parâmetros críticos, podem trazer à tona ou interagir com certos comportamentos humanos (por exemplo, complacência, ansiedade) que facilitam a ocorrência de uma ação insegura ou criam situações que tornam inadequados ou ineficazes, certos mecanismos de processamento. É reconhecido, também que, o comportamento dos parâmetros críticos pode ter impactos diferentes, dependendo do estágio do processamento da informação no qual o indivíduo está engajado, isto é, deteção, avaliação da situação, planejamento da resposta ou implementação da resposta. Mais ainda, os fatores que afetam o desempenho, que irão contribuir para a probabilidade de ocorrência da ação insegura, estão relacionados ao comportamento específico da planta e ao seu impacto no operador.

4.4.4.1 Características dos parâmetros e dos cenários

Um grande número de aspectos relativos ao comportamento dos parâmetros, em cenários de acidentes, tem sido identificado como influenciando, potencialmente, a probabilidade de certos mecanismos de erro tornarem-se operativos e então contribuir para uma ação insegura. O primeiro grupo está baseado em uma extensão das “palavras guias” e dos conceitos utilizados na análise HAZOP (ELLIS K. R., 1992). O segundo grupo está baseado em um conjunto de características catalogadas por Woods, Roth, Mumaw e seus colegas (WOODS *et al.*, 1994, MUMAW & ROTH,1992,

PEROTTY & WOODS,1997), que tentam descrever porque os cenários problemáticos são difíceis. A noção básica é que este cenário (os quais, por definição, se desenvolvem no tempo) contém dispositivos que criam oportunidades para tornar o processamento normal da informação humana e suas ações, inadequados ou ineficazes, essencialmente por criar demandas cognitivas não usuais.

4.4.4.1.1 Influência dos parâmetros

Um grupo de descrições (por exemplo, uma pequena ou grande variação de um parâmetro, um valor alto ou baixo, indicações falsas de alarmes, variações lentas ou rápidas, etc.) pode ser usado para representar o comportamento dos parâmetros que refletem as condições dinâmicas da planta, resultante de um dado evento iniciador e das contribuições do sistema falhado. Estes parâmetros poderão variar (ou não) de acordo com as condições existentes na planta e o interesse é o quanto uma variação particular nestes parâmetros poderá interagir com as características humanas de processamento da informação e levar a uma ação insegura. Por exemplo, uma pequena taxa de variação de um parâmetro pode não ser detetada no tempo certo e mesmo se fosse, ela poderia induzir complacência durante os estágios iniciais de um acidente. Além disto, se os operadores já tivessem formado uma expectativa do que está ocorrendo, uma pequena variação em um parâmetro poderia ser desprezada devido a fatores como fixação no erro, procura de confirmação ou outro mecanismo de erro qualquer.

4.4.4.1.2 Influência do cenário

As características da evolução de um cenário (incluindo o comportamento dos parâmetros críticos) podem complicar o desempenho do operador durante os diferentes estágios do processamento da informação e contribuir para o operador executar uma ação insegura. Por exemplo, um cenário que começa parecendo ser um

simples problema (baseado em fortes porém incorretas e incompletas evidências) pode levar os operadores a tomar ações aparentemente adequadas, mas que os tornam resistentes à mudanças ou insensíveis para informações corretas que aparecem mais tarde (garden path problem); os operadores são levados a formar uma forte, porém errada hipótese, que os impede de considerar adequadamente as informações posteriores.

4.4.5 Considerações sobre as características do comportamento humano

Esta seção descreve as características do comportamento humano que podem resultar em ações inseguras e em eventos de falha humana. Existe uma gama de conhecimentos das ciências comportamentais, já desenvolvida, que permite ao analista entender os tipos de influências que podem levar o operador a interpretar, erroneamente, as condições da planta ou falhar em preparar uma resposta adequada resultando em danos à planta (ver Anexo B). Tais falhas não são randômicas, porém são influenciadas pelo contexto nos quais os operadores estão colocados (isto é, as condições da planta e os fatores que formatam o desempenho).

4.5 Preparação para a análise ATHEANA

Para a aplicação destes processos é necessário realizar certas atividades preparatórias, que incluem:

- seleção do tipo de análise (retrospectiva, prospectiva ou ambas);
- seleção e treinamento da equipe multidisciplinar que irá aplicar ATHEANA;
- reunir informações básicas; e
- planejar o uso de simulador.

4.5.1 Seleção do tipo de análise

A ATHEANA pode ser usada em três tipos de análise: (1) retrospectiva, (2) prospectiva ou (3) ambas.

O escopo da análise retrospectiva é a análise de um evento real ocorrido da planta. O cenário escolhido deve ter uma ou mais falhas humanas *pós-iniciador* que, se não corrigida, pode resultar em uma falha funcional da planta com o potencial de causar dano ao núcleo; pode ter sido, ou não, previamente, modelada na APS como um evento de falha humana, HFE. A finalidade desta análise é atualizar os bancos de dados das APS's ou ACH's e/ou descobrir ações corretivas para evitar sua repetição, ou ambos.

Para a análise prospectiva, a finalidade da ATHEANA é dar suporte às análises de eventos de falhas humanas, HFE's, pós-iniciador. Isto é porque, durante as análises dos eventos, realizadas no desenvolvimento da ATHEANA, o HFE pós-iniciador foi que representou a falha funcional da planta com o potencial de levar a danos ao núcleo. O HFE pré-iniciador, somente torna-se importante quando cria dependências que podem interferir com o sucesso das ações pós-iniciador.

4.5.2 Seleção e treinamento da equipe multidisciplinar

A ATHEANA é aplicada por uma equipe multidisciplinar, com a liderança de um analista de ACH. A equipe deve ser formada por pessoas que possuem um conhecimento e experiência da planta suficientes para fornecer informações e responder às perguntas do processo ATHEANA.

É recomendado que a equipe inclua, pelo menos, os seguintes tipos de membros:

- um analista de ACH;
- um analista de APS;

- um instrutor de operadores (com conhecimento de treinamento em simuladores);
- um operador senior de reator; e
- um especialista da área termo-hidráulica.

A equipe pode ser complementada por outros especialistas, se necessário.

O treinamento da equipe envolve, entre outros, a familiarização com características de acidentes severos, os princípios básicos e processos da ATHEANA e das ciências comportamentais e cognitivas, etc. A revisão de alguns dos eventos (mínimo de dois) documentados no banco de dados HSECS (COOPER *et al.,* 1995) é desejável.

4.5.3 Reunir informações básicas

Como nos métodos tradicionais de ACH, devem ser reunidas informações básicas da planta relevantes para a análise, como projeto dos sistemas, procedimentos, desenhos, experiência operacional, histórico de falhas de equipamentos e instrumentação. Adicionalmente, todas as informações relevantes relativas à tarefa, objeto da análise, devem ser identificadas e colecionadas, assim como a documentação e resultados da APS. Posteriormente, durante a realização da análise, novas informações poderão ser necessárias. Outra fonte de informação, muito valiosa, é a experiência e as informações do pessoal da usina, as quais não estão registradas, formalmente.

A finalidade desta tarefa é desenvolver um entendimento do ambiente onde o operador está colocado.

4.5.4 Uso do simulador

A facilidade do simulador em reproduzir um evento e permitir alternativas operacionais é muito útil no processo ATHEANA porque facilitam a identificação de

ações inseguras, possíveis mecanismos de erros e contextos que forçam ao erro. Igualmente, as discussões com os operadores que estão operando o simulador, permitem tirar informações relevantes para o processo de análise, como expectativas, dificuldades, facilidades, etc.

4.6 Análise retrospectiva da ATHEANA

O objetivo básico da ATHEANA era, originalmente, identificar e quantificar ações humanas não adequadamente representadas nas análises probabilísticas de risco, APS (análise prospectiva). Para o seu desenvolvimento, vários eventos operacionais foram analisados, de uma maneira padronizada, onde foi criado um banco de dados, HSECS (COOPER *et al.*, 1995), para registrar todas as informações e detalhes identificados nestas análises. Entretanto, como esta análise evoluiu, tornou-se evidente que esta abordagem era muito útil, além do mero desenvolvimento para a abordagem prospectiva da ATHEANA. Desta maneira, este processo foi incorporado à ATHEANA como um processo de análise retrospectivo.

A abordagem retrospectiva pode ser aplicada, extensivamente, usando a plataforma de trabalho descrita na seção 4.2.1. Tanto os eventos nucleares quanto os não nucleares podem ser, facilmente, analisados usando esta plataforma e seus conceitos básicos.

A finalidade da análise retrospectiva é obter um entendimento das causas das falhas humanas em eventos operacionais, significativas para o risco. Para isto, o analista deve responder às seguintes questões:

- O que aconteceu?
- Quais foram as consequências?
- Por que isto aconteceu (isto é, quais foram as causas)?

As características importantes da análise retrospectiva incluem:

- um sumário do que aconteceu no evento;

- identificação das falhas funcionais importantes;
- linha de tempo dos eventos;
- um sumário das ações humanas importantes e suas causas aparentes;
- um sumário dos fatores contextuais importantes (isto é, condições da planta e fatores que formatam o desempenho), antes, durante e após o evento; e
- um registro dos diagnósticos do evento mostrando as condições da planta e as respostas dados pelos operadores, como uma função do tempo.

Os resultados das análises podem ser incluídos no banco de dados para uso futuro ou servir de base para o entendimento dos fatores que afetam o desempenho humano e para propor medidas corretivas para reduzir a probabilidade de ocorrências similares no futuro. O uso de ATHEANA, para análise retrospectiva, representa uma mudança marcante em relação aos outros métodos de análise de acidentes porque ATHEANA é projetada para identificar eventos de falha humana (HFE) como modelados nas APS's[1] e suas causas básicas.

A ATHEANA postula que a ação insegura ocorre dentro de um contexto que força ao erro que pode ser, especificamente, identificado. A análise de confiabilidade humana deve ser capaz de identificar estes contextos, com a finalidade de estimar a probabilidade destas condições e as prováveis consequências, em termos de ações humanas inadequadas ou falhas delas, quando necessárias. O contexto que força ao erro são as condições que o gerente e o pessoal da planta pode influenciar.

O processo é iterativo e subjetivo, baseado em registros reais do evento, assim como possíveis suposições sobre o evento e suas causas.

[1] Como discutido anteriormente, a APS deve ser considerada como uma abordagem geral para configurar, analisar e entender o risco e a segurança, ao invés de, simplesmente, um conjunto de ferramentas tais como análises de árvores de eventos/falhas, comuns na indústria nuclear. O sentido de APS deve ser entendido como examinar o risco através de processos sucessivos de aproximação, começando com uma estrutura de possíveis cenários que podem levar à danos, e continuando, primeiro, com uma avaliação do risco baseada em julgamento, e depois, com cálculos, sucessivamente, mais rigorosos como requeridos pela seriedade da situação, práticas da indústria e recursos disponíveis.

A análise retrospectiva começa com o cenário real para identificar as falhas funcionais que foram causadas pelo comportamento humano. Ela examina todos os dados do evento para descobrir os contextos que forçam ao erro.

A análise retrospectiva compreende os seguintes passos:

(1) Identificar o evento de interesse;

(2) Identificar as falhas funcionais, os HFE's e as UA's;

(3) Identificar as causas das UA's incluindo condições da planta e PSF's; e

(4) Documentar os resultados.

Os resultados da análise retrospectiva podem ser sumarizados em um diagrama de fluxo, como mostrado na figura 4.3, que representa o sumário do exemplo A do NUREG-1624, Rev.1 (2000), que é a análise do acidente de TMI-2. A análise é executada na direção inversa do diagrama, isto é, os HFE's e as UA's são identificados antes das falhas do processamento da informação, dos PSF's e dos contribuidores das condições da planta.

4.6.1 Identificar o evento de interesse

Normalmente, os eventos de interesse possuem as seguintes características:

- consequências severas ou potencialmente severas;
- operação ocorreu além dos limites de uma boa operação; e
- necessitou grandes intervenções do operador no controle da planta.

O analista deve fazer uma descrição completa do evento, descrevendo as condições dos principais parâmetros da planta antes e depois do acidente, inclusive identificando problemas ou deficiências pré-existentes. Os fatores inesperados ocorridos também deverão ser anotados.

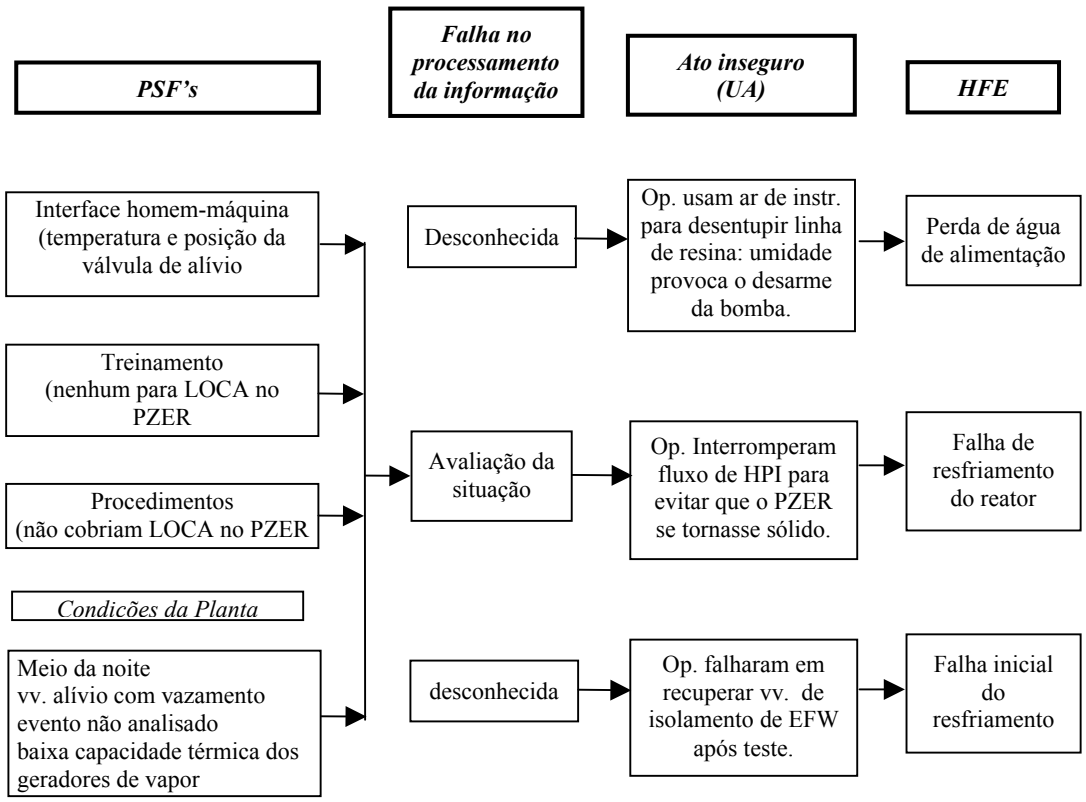


Fig. 4.3 Sumário da análise retrospectiva de TMI-2

4.6.2 Identificar as falhas funcionais, os HFE's e as UA's

As falhas funcionais são, normalmente, modeladas nas APS's e podem ser falhas de função, sistemas ou componentes. Por exemplo, no acidente de Crystal River 3, onde a válvula de spray falhou aberta, a falha funcional foi a perda de controle de pressão do SRR.

Um HFE é uma falha funcional que é o resultado de uma ou mais ações inseguras. Ações inseguras são ações indevidamente tomadas pelo pessoal da usina ou ações não tomadas quando necessário, que resultar em uma degradação das condições de segurança.

O analista deve examinar as informações para identificar as ações humanas realizadas que levaram ao evento de falha humana. Para isto, deve construir uma listagem da sequência de eventos (diagnosis log), que é uma representação, em ordem cronológica, das condições da planta e das ações do operador ocorridas desde o início do evento até a recuperação e estabilização da planta, no final do evento. Cada ação do operador ou falha de equipamento, que parece ter contribuído para o agravamento ou mitigação das consequências do evento indesejado, deve ser incluído em uma tabela e representado, graficamente, em uma relação cronológica de ações e falhas ocorridas durante o evento. Dependências entre ações e eventos são identificadas em uma tabela de dependência humana. Ações e eventos dependentes possuem uma forte influência no contexto que força ao erro.

A figura 4.3 é um exemplo da relação entre os HFE's e as UA's, relativas à análise do evento de TMI-2.

4.6.3 Identificar as causas das ações inseguras

A análise chave do processo ATHEANA é determinar as causas das UA's pela identificação das falhas do processamento da informação e dos contextos que forçam ao erro, o qual é composto dos PSF's e contribuidores significativos das condições da usina.

4.6.3.1 Falhas do processamento da informação

É impossível para o analista determinar, precisamente, o que o operador estava pensando quando tomou a ação insegura. Quando razoável, o analista poderá postular o que causou o operador tomar a UA, baseada nas condições do momento, declarações dos operadores, etc. Mas, frequentemente, somente as falhas no processamento da informação, evidenciada pelo comportamento dos operadores, poderá ser acessada.

4.6.3.2 Fatores que formatam o desempenho

O analista deve examinar, cuidadosamente, as informações colhidas sobre o evento, para identificar os PSF's que, quando combinados com as condições da planta, podem ser esperado, causar um mecanismo de erro e uma UA. Em outras palavras, o analista procura fatores que podem ajudar a predispor o operador a cometer um erro.

As causas básicas dos PSF's podem estar relacionadas com treinamento, procedimento incompleto ou deficiente, hora do dia, fatores organizacionais ou interface homem-máquina deficiente. É útil para o analista sumarizar qual foi a influência mais negativa nas ações supostas ou mencionadas pelos participantes do evento, assim como a influência mais positiva.

4.6.3.3 Condições significativas da planta

Como parte do contexto que força ao erro, o analista deve, também, sumarizar a condição da planta mais significativa que difere das condições esperadas da planta. Normalmente, isto inclui condições extremas e não usuais, condições pré-existentes contribuintes, falhas múltiplas de equipamentos e transições em progresso.

4.6.4 Preparar as conclusões

O analista deve agrupar, para cada UA, as condições da planta e os PSF;s que ele acredita terem causado a falha no processamento da informação e que culminou no ato inseguro. Pode ocorrer que existam mais de um mecanismo de erro para cada UA.

4.6.5 Documentar os resultados da análise

O analista deve documentar, em formato adequado, suas observações, discussões, pontos de vista e deficiências encontradas. O Anexo C ilustra esta documentação.

4.7 Análise prospectiva da ATHEANA

A análise prospectiva da ATHEANA tem por objetivo básico, identificar certos tipos de erros (erro de comissão) potenciais, os quais não são tratados pelos métodos atuais de análise de confiabilidade humana. Isto representa uma diferença marcante em relação aos métodos atualmente em uso, os quais estão mais dedicados a quantificar as chances de erros humano em condições nominais de acidente. A análise dos eventos ocorridos, que foi a base para a ATHEANA, identificou que os erros (erros de comissão) humanos mais significativos para o risco, são fortemente influenciados pelo contexto do evento (EFC), isto é, pelas condições da planta e os fatores que formatam o desempenho (PSF) e que este contexto, frequentemente, é diferente das condições operacionais assumidas pelas APS's. Para tratar os elementos do EFC (que vão além do tipo e escopo do contexto considerado pelos métodos de ACH anteriores), ATHEANA requer um novo modelo de quantificação. Particularmente, a quantificação das probabilidades dos HFE's correspondentes está baseada nas estimativas de quão provável ou frequente as condições da planta e os PSF's concorrem para criar o EFC's, ao invés de estimativas de ocorrência randômica de falha humana. Esta abordagem envolve uma mistura de técnicas de análise que envolve o julgamento, por operadores e analistas experientes, para quantificar a probabilidade de uma classe específica de EFC e a probabilidade do ato inseguro, dado aquele contexto.

A análise prospectiva é composta dos seguintes elementos essenciais:

- integrar a tarefa na perspectiva de APS e da ACH da ATHEANA;
- identificar os eventos de falha humana e as ações inseguras que são relevantes para a tarefa;
- para cada evento de falha humana ou ação insegura, identificar as razões das ocorrências de tais eventos (isto é, os elementos do EFC que são as condições da planta e fatores que formatam o desempenho). Isto é feito através de uma abordagem bem estruturada e controlada;
- Quantificar os EFC's e a probabilidade de cada ação insegura, dado o seu contexto; e
- Avaliação do resultado da análise em termos da tarefa para a qual a análise foi realizada.

Para isto, foi desenvolvido um processo de pesquisa e de quantificação de EFC's, o qual é único. A pesquisa foi estruturada para procurar, entre outras coisas, as condições da planta que podem confundir o operador, de maneira que ele desenvolva, incorretamente, uma avaliação da situação ou planejamento da resposta e execute uma ação insegura. ATHEANA assume que ações inseguras significativas ocorrem como resultado da combinação de influências associadas com as condições da planta e fatores específicos centrados no homem que disparam os mecanismos de erros.

O processo prospectivo consiste de 10 passos principais, conforme está ilustrado na figura 4.4. Os 10 passos são:

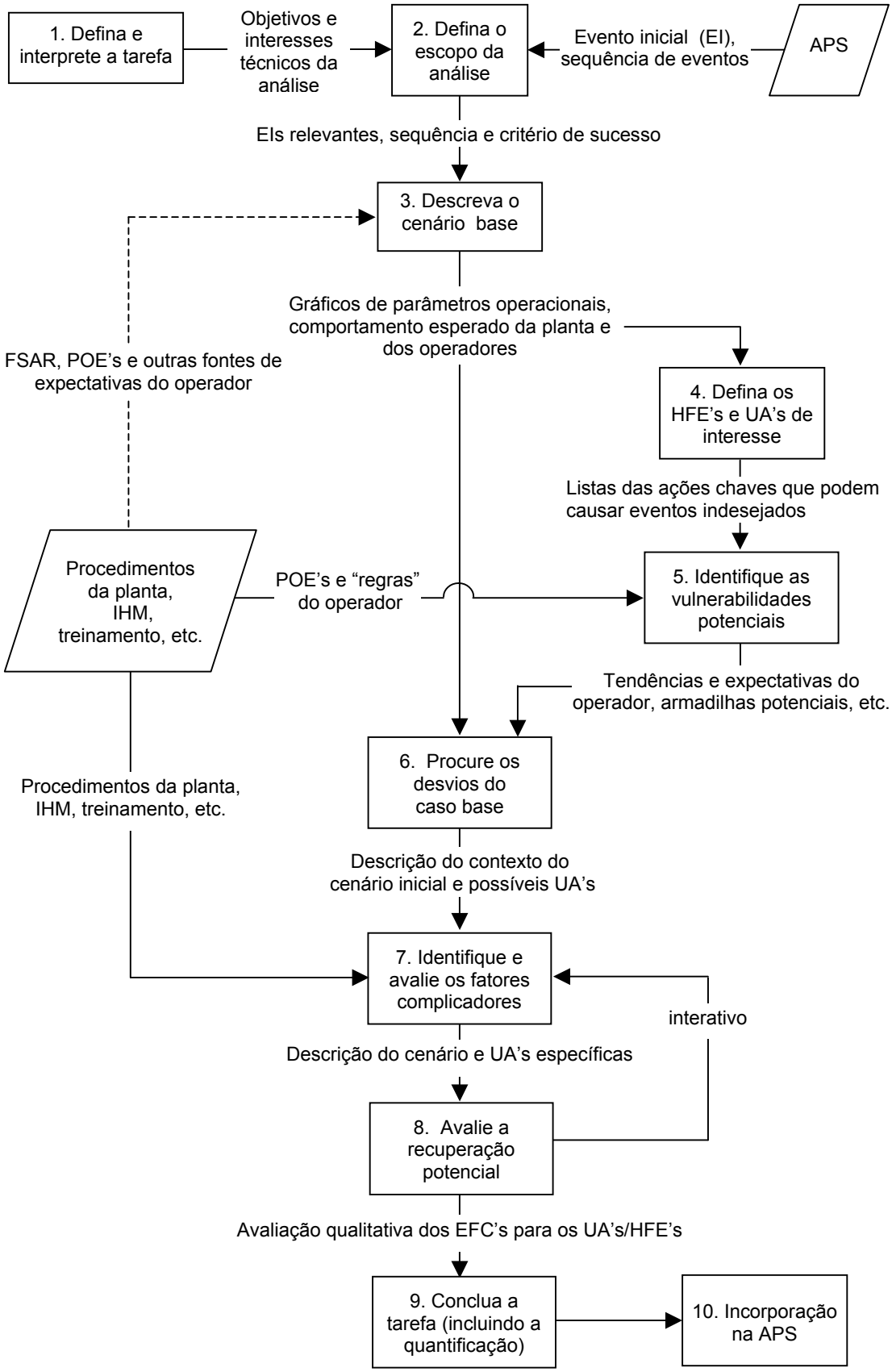


Fig. 4.4 Processo de pesquisa prospectiva da ATHEANA

4.7.1 Passo 1: Interpretação da tarefa

A finalidade deste passo é definir os objetivos da análise sendo realizada, isto é, porque está sendo feita. ATHEANA pode ser utilizada para várias aplicações de ACH, desde um estudo completo para a APS até estudos especiais focalizando uma tarefa específica. Para aplicações em APS, normalmente, ATHEANA focalizará as contribuições significativas do homem para o risco e para a segurança, que são assuntos de particular interesse para os gerentes ou para o órgão regulatório.

É importante que, a descrição da tarefa a ser analisada fique bem claro, em uma linguagem técnica e sucinta, indicando, se possível, as fronteiras e os objetivos gerais da análise e a sua relação com o risco e a APS, se disponível.

4.7.2 Passo 2: Escopo da análise

Este passo limita o escopo da análise pela aplicação da tarefa definida no passo 1 e, se necessário, por razões práticas, estabelece limites adicionais do escopo pelo estabelecimento de prioridades das características da sequência do evento. Estas prioridades são usadas para restringir, adicionalmente, o escopo da análise e dirigí-la para os eventos, potencialmente, de alto risco. Embora a ATHEANA possa ser usada, tanto para aplicações em APS como para outras aplicações, o processo de estabelecer prioridades está baseado nos modelos de APS, específicos da planta, e nos conceitos gerais de importância para o risco. O primeiro limite é selecionar a classe do evento iniciador e o iniciador associado a ser analisado (tabela 4.6a). Restrições (prioridades) no escopo serão então consideradas, posteriormente, para cada iniciador selecionado, equilibrando os recursos de análise com as necessidades específicas do projeto.

No que se refere às restrições, o NUREG-1624, Rev 1 (2000) apresenta a tabela 9.2 que fornece uma lista de sugestões de prioridades relativas às características de iniciadores e à sequências de acidentes de alta prioridade (tais

Tabela 4.6a
Lista genérica de classes de eventos iniciadores e iniciadores associados

Classe de eventos iniciadores	Exemplo de iniciadores
Transientes (internos) – com e sem água de alimentação disponível	Perda de potência elétrica externa Perda de água de alimentação principal Perda de vácuo Desarme da turbina Desarme do reator Fechamento da válvula de isolamento de vapor principal (MSIV, main steam isolation valve) Perda de água de circulação
LOCA	Grande Pequeno Médio
Falha de sistemas suporte	Perda de HVAC (ventilação e ar condicionado) Perda de água de serviço Perda de ar de instrumentos Perda das barras de DC (corrente contínua) Perda das barras de AC (corrente alternada) Perda das barras de instrumentação Perda de água de resfriamento de componentes Perda de água de resfriamento do edifício do reator
Eventos externos	Fogo Distúrbios sísmicos Enchentes Vendavais
Outros/especiais	LOCA de interface entre sistemas ATWS (transiente previsto sem desligamento do reator ou antecipated transiente without scram) Ruptura de tubos dos geradores de vapor Ruptura de linha de água de alimentação principal Falha do vaso do reator (p.ex. choque térmico pressurizado)
Modos alternativos	Potências reduzidas e desligamentos

como, um grande LOCA, falha de resfriamento a longo prazo, falhas de sistemas de suporte, fogo) e, a tabela 9.3, com sugestões de características de funções da planta e

sistemas associados (tais como, falha de HPI, pequena ou nenhuma redundância de sistema ou equipamento para substituição de uma função, em caso de falha) que tem, potencialmente, alta importância para o risco, sob a perspectiva humana.

O produto do passo 2 é um grupo de iniciadores selecionados (ou uma classe completa de iniciadores, se desejável) para o qual a tarefa (passo 1) será analisada. Isto fornece uma limitação para a análise e, portanto, delimita um contexto global, assim como estabelece um relacionamento com a APS. Adicionalmente, o desenvolvimento das prioridades dos cenários e das funções da planta é usado nos passos 3, 4 e 6, para orientar a análise.

4.7.3 Passo 3: Cenário base

Neste passo, o cenário será definido e caracterizado para o iniciador escolhido. O cenário deve ter uma descrição mais realista possível, do comportamento da planta e dos operadores, em relação à tarefa e ao iniciador, pois o mesmo fornecerá uma base de onde serão identificados e definidos os desvios de tais expectativas, que será realizada no passo 6.

O cenário ideal deverá ser (fig. 4.5):

- Um modelo de consenso comum entre os operadores: deverá ser um cenário bem definido e entendido e de consistência entre os operadores;
- Bem definido, operacionalmente: coberto por procedimentos, treinamento, experimentado operacionalmente ou em simulador e que a resposta do operador e dos equipamentos sejam bem entendidas;
- Bem definida em relação aos aspectos físicos: os princípios de física, termo-hidráulica, neutrônica e outros cálculos estejam bem definidos. Estas características e a característica de estar bem documentada, é chamada de "análise da referência" para o cenário;

- Bem documentado: uma descrição bem ampla, baseada em documentos oficiais tais como RFAS ou APS; e
- Realista: deverá ser consistente com o comportamento da planta.

O produto do passo 3 é uma descrição completa do cenário a ser analisado o qual está baseado em um modelo de consenso dos operadores e nas análises de referências relevantes, se ambos existirem. No caso ideal, quando ambos existirem, esta descrição deverá incluir:

- uma lista de causas assumidas para o evento inicial;
- uma breve descrição geral da seqüência de eventos esperada, começando antes do desarme do reator;
- uma descrição das condições iniciais assumidas da planta;
- uma descrição detalhada da sequência cronológica esperada e o comportamento da planta (mostrada pelos parâmetros funcionais chaves) e a resposta dos sistemas e equipamentos da planta;
- a trajetória esperada dos parâmetros chaves, registradas no tempo, que são as indicações do estado da planta para os operadores;
- alguma suposição com respeito ao comportamento esperado da planta e as respostas esperadas dos sistemas ou equipamentos e dos operadores (por exemplo, equipamentos assumidos estarem indisponíveis, falhas simples de sistemas assumidas terem ocorrido); e
- ações chaves esperadas do operador durante a progressão do cenário.

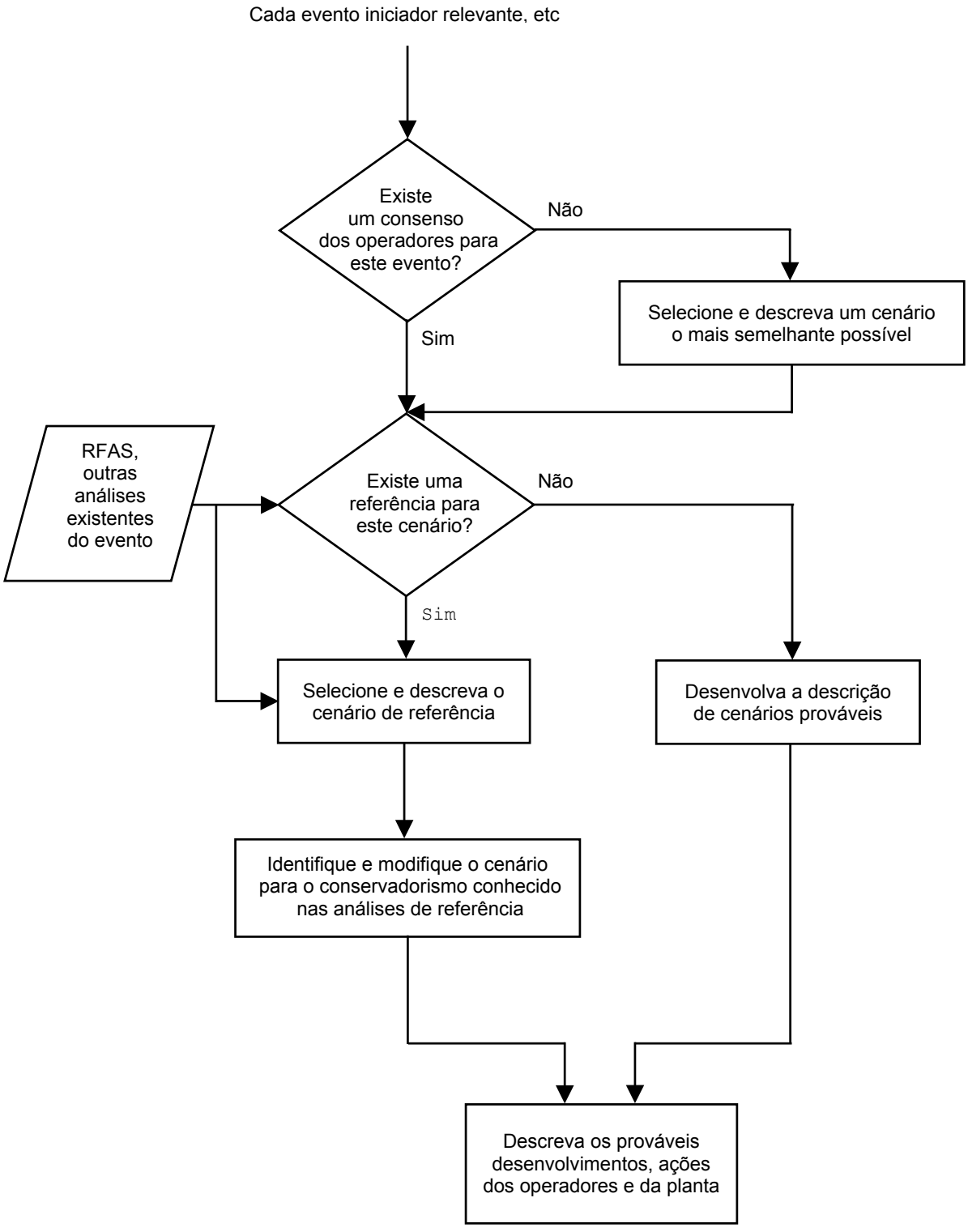


Figura 4.5: passo 3 – descrição do cenário base

4.7.4 Passo 4: Os HFE's e as UA's

O cenário criado no passo 3 será analisado para identificar e definir os possíveis HFE's e/ou UA's. Entretanto, o passo 1 já pode ter definido algum HFE ou UA, como sendo de interesse. Alternativamente, alguns dos próximos passos também poderão identificar a necessidade de novos HFE's ou UA's. Consequentemente, na sequência da análise poderá requerer voltar a este passo.

O "evento de falha humana", HFE, é um termo da APS que requer os conceitos de APS para a sua definição. Por outro lado, uma "ação insegura", UA, não está, especificamente, ligado a APS, mas permite ao analista fazer uma ponte entre o comportamento humano e a APS. As definições destes termos são:

Evento de falha humana: um evento básico que é modelado nos modelos lógicos da APS (árvore de eventos e árvores de falhas) e que representam a falha de uma função, sistema ou componente e que é o resultado de uma ou mais ações inseguras.

Ação insegura: uma ação indevidamente tomada, ou não tomada quando necessário, pelo pessoal da planta, que resulta em uma degradação das condições de segurança da planta.

ATHEANA assume que, inicialmente, identificará os HFE's e depois as UA's. Entretanto, posteriormente, se ocorrer retorno a este passo, poderá haver a necessidade de rever, somente, uma destas identificações.

O HFE é, tipicamente, de natureza funcional (por exemplo, resfriamento pelo secundário no desligamento da usina) e pode estar incluído no passo 1. Em outro momento, poderá ser mais benéfico definir uma ação insegura específica (por exemplo, colocar as bombas de injeção de alta pressão em posição bloqueada (pull-

to-lock position)), para representar a atividade de interesse. Em qualquer caso, estas são as ações indesejadas do operador, para as quais o processo ATHEANA está sendo usado para determinar o EFC, que poderá propiciar a ocorrência destas ações.

A ATHEANA fornece um processo sistematizado que leva a identificação do HFE's, que é composto de 7 tarefas. Algumas das quais já podem ter sido realizadas nos passos anteriores ou até mesmo, em alguns casos, não haver a necessidade de serem realizadas. Os HFE's, para cada função representada na árvore de eventos para o iniciador considerado, pode ser identificado realizando as seguintes tarefas:

(1) Identificar se a tarefa é (a) necessária ou (b) indesejada (com respeito aos requisitos de resposta ao acidente para o iniciador ou a sequência específica);

(2) Identificar o(s) sistema(s) ou equipamento(s) que realiza(m) a função;

(3) Identificar a situação do pré-iniciador do(s) sistema(s) ou equipamento(s) (isto é, operando, em reserva, passiva);

(4) Identificar o critério de sucesso funcional para o(s) sistema(s) ou equipamento(s);

(5) Identificar o modo de falha funcional (HFE) do(s) sistema(s) ou equipamento(s);

(6) Decidir se erros de comissão (EOC), erros de omissão (EOO) ou ambos os tipos de erros são relevantes para a tarefa selecionada; e

(7) identificar as descrições aplicáveis de possíveis falhas humanas (UA), que podem ser selecionadas como candidatas para as descrições de eventos de falha humana, HFE.

A ATHEANA (NUREG-1624, Rev. 1, 2000) fornece 3 tipos de tabelas para servir como guia para realizar a tarefa acima, isto é, para a identificação do HFE e da UA, que causou o HFE. Na primeira tabela, que trata dos itens 1 a 5 acima, chega-se na identificação do "modo de falha funcional", o qual é transformado em um código de "categoria do modo de falha funcional". Este código remete para a segunda tabela, cujo produto final, é a descrição de falha humana no sistema ou equipamento, a qual

também é transformado em um código, correspondente à falha humana identificada. Este código remete para a terceira e última tabela, que na verdade, é constituído por 5 tabelas (para diferentes combinações de tipos de erros (EOO e EOC), tipo de falha do sistema/equipamento (partir/parar manual ou automaticamente), falhas em ações de recuperação, modo de operação (passivo, ativo) onde se chega, finalmente, à identificação (descrição) da ação insegura que causou o HFE de interesse.

Em algumas aplicações da análise prospectiva, o passo 1 já pode ter definido, inicialmente, um modo de falha funcional ou até mesmo, a ação insegura. Nestes casos, portanto, não haverá necessidade de passar por todo o processo acima. ATHEANA fornece uma tabela simplificada para, dado o modo de falha funcional, identificar a descrição da ação insegura.

Vale lembrar que a perda de uma função de segurança pode ser causada por mais de um modo de falha funcional (árvore de falhas da APS) e que cada modo de falha funcional pode ser causado por diferentes tipos de ações inseguras. As tabelas citadas acima contemplam este fato. Por exemplo, a perda de resfriamento por HPI pode ser causada ou por baixo fluxo (devido a poucos trens estarem operando ou por estrangulamento da válvula) ou pelo desligamento ou operação intermitente, erroneamente, das bombas.

Um modo de falha pode ser ativado por várias maneiras. Por exemplo, o operador pode fazer uma das seguintes ações inadequadas:

- não usar (por exemplo, falhar em dar partida) um sistema;
- causar dificuldades para o uso de um sistema (por exemplo, colocar uma chave de partida de bomba na posição bloqueada ou esgotar uma fonte de recursos); e
- danificar (mesmo, permanentemente) um equipamento de um sistema.

Muitas das falhas humanas e ações inseguras resultam, diretamente, em falhas funcionais, ou perda completa da função. Entretanto, falhas de controle

envolvem, mais frequentemente, o efeito da falha do equipamento nas funções do sistema (sub-resfriamento, como no exemplo acima).

Consequentemente, a análise da ação insegura deverá considerar, por exemplo, as seguintes falhas de controle:

- muito ou pouco (por exemplo, controlando a posição de uma válvula, quantidade);
- muito cedo ou muito tarde (tempo);
- muito rápido ou muito lento (taxa);
- muitas vezes ou poucas vezes (frequência);
- muito curto ou muito longo (duração);
- muitos ou poucos trens (quantidade e taxa); e
- demais ou de menos (quantidade e taxa).

O produto final do passo 4 é:

- uma lista dos HFE's e suas respectivas descrições, relevantes para a tarefa e para cada árvore de evento (ou um específico iniciador) da APS e
- as UA's associadas com cada HFE identificado.

4.7.5 Passo 5: Vulnerabilidades potenciais no conhecimento do operador

Este é um passo preliminar para as pesquisas dos desvios do cenário base que serão identificados nos passos 6 e 7. Em particular, este passo é dirigido para encontrar as vulnerabilidades potenciais no conhecimento básico do operador em relação aos eventos iniciadores ou aos cenários de interesse, os quais podem resultar nos HFE's ou UA's identificados na passo 4. Por exemplo, serão identificadas as implicações das expectativas do operador e as surpresas ("armadilhas") associadas, inerentes ao evento iniciador ou ao cenário base, as quais podem representar vulnerabilidades na resposta do operador.

As deficiências encontradas no conhecimento do operador servirão, no passo 6, para dirigir as pesquisas para as áreas de maior vulnerabilidade do operador.

As armadilhas potenciais, inerentes à maneira como o operador pode responder ao evento inicial ou ao cenário base, podem ser identificadas através de quatro etapas:

(1) Investigação das potenciais vulnerabilidades nas expectativas do operador em relação ao cenário:

A ATHEANA analisa as diversas influências que o evento iniciador pode criar no operador, considerando os fatores que afetam o seu processamento da informação e apresenta uma tabela mostrando as vulnerabilidades potenciais do operador que podem resultar de diferentes características do evento iniciador. Dado o tipo geral do iniciador ou do evento do cenário base (identificado na descrição do cenário base realizado no passo 3, por exemplo, um evento que é treinado com relativa frequência), este deve ser comparado com as características dos eventos apresentados na tabela (que no caso deve corresponder a mesma descrição), o qual terá, associado, a vulnerabilidade potencial para este iniciador ou evento. As vulnerabilidades potenciais, normalmente, incluem desvios entre o evento real e as expectativas do operador para o evento, desvios entre o evento real e as regras que o operador espera aplicar no evento e eventos, para os quais, o conhecimento do operador é limitado e as regras conhecidas e o treinamento não são aplicáveis. Estes desvios, que vão de encontro às vulnerabilidades identificadas na tabela, deverão ser identificados no cenário base, os quais ajudarão na análise de desvios que será realizada no passo 6.

(2) Entendimento da cronologia do cenário base e de qualquer dificuldade inerente, associada com a resposta requerida:

A sequência natural de um cenário possui, normalmente, as seguintes fases:

- condições iniciais ou cenário pré-desarme;

- iniciador ou eventos, aproximadamente, simultâneos;
- operação inicial dos equipamentos e resposta do operador;
- fase de estabilização; e
- resposta dos operadores e dos equipamentos, a longo-prazo.

O desenvolvimento cronológico do cenário, considerando estas fases é muito útil, porque mostrará as bases para muitos dos critérios de sucesso operacional de equipamentos e, claramente, identificará os períodos de mínima e máxima vulnerabilidades à uma intervenção humana inadequada. Esta cronologia e os desvios de cenários, que serão identificados no passo 6, servirão para selecionar os HFE's, UA's e EFC.

(3) Identificação das tendências das ações dos operadores e regras informais:

As tendências das ações do operador são ações esperadas serem realizadas quando um indicador de parâmetro chave mostrar um comportamento diferente do normal (Por exemplo, para um nível que está, anormalmente, baixo ou caindo, a tendência do operador é fechar as válvulas de saída, para interromper a drenagem, ou ligar as bombas, para repor inventário). Estas tendências foram baseadas nos procedimentos de emergência e de condições anormais, treinamento recebido, assim como em práticas e regras informais que também são partes da psiquê humana. A ATHEANA fornece uma tabela (tabela 9.12.a) de tendências de ações do operador, que deve ser utilizada para identificar aquelas tendências que podem levar a HFE's e UA's de interesse e as correspondentes condições da planta, que levam a estas tendências. As condições da planta podem predispor os operadores a seguir estas tendências e então, elas deverão ser examinadas, como parte do próximo passo do processo. Adicionalmente, deverá ser identificada alguma regra informal (por exemplo, o histórico de que certos indicadores podem prender e não indicar, corretamente, o valor do parâmetro, principalmente, em condições dinâmicas), que poderá ser

relevante como um possível fator contribuidor para induzir os HFE's e as UA's de interesse.

(4) Avaliação das regras formais e dos procedimentos de emergência, esperados serem utilizados em resposta ao cenário:

O uso de um diagrama de fluxo ou diagrama lógico do procedimento ajuda a destacar os passos relevantes onde são feitas as tomadas de decisões e as ações a serem executadas e/ou monitoradas. Estes diagramas de fluxo evidenciam:

- a localização de pontos de ramificação de um procedimento para outro;
- pontos onde são requeridos desligar equipamentos, que são, particularmente, relevantes ao cenário; e
- pontos onde são requeridos grandes realinhamentos de equipamentos.

Os POE's e outras regras formais definem as respostas que o operador deverá tomar, de acordo com a progressão do evento. Porém, estes pontos podem ser, particularmente, vulneráveis a erros, pelo operador, como entrar em um procedimento errado ou desligar e/ou reconfigurar, incorretamente, um equipamento. Portanto, em cada ponto de decisão ou onde parecer necessário, acrescentar informações para destacar:

- ações que devem ser tomadas;
- ambiguidade potencial; e
- um julgamento da importância de tomar uma ramificação errada ou uma ação inadequada.

O produto do passo 5, que são as vulnerabilidades potenciais, será utilizado como referência para auxiliar nos estágios de pesquisas de desvios.

4.7.6 Passo 6: Pesquisa dos desvios do cenário base

A experiência tem demonstrado que os eventos sérios não ocorrem nos cenários bases descritos nas APS's, pelo contrário, cenários com desvios significativos (cenários divergentes) do cenário base são os que tem levado às maiores dificuldades para os operadores. Este passo tem a finalidade de identificar, através de uma pesquisa bem estruturada, os desvios do cenário base, que são prováveis de ocorrer e resultar em ações inseguras, significativas para o risco. A pesquisa é dirigida para identificar desvios físicos reais, no comportamento e nas condições da planta. Desvios (falsos) indicados por falha de instrumentação ou na percepção, errônea, dos operadores serão pesquisados no passo 7.

Este passo contém quatro tipos de pesquisas para identificar as características que estarão presentes no cenário divergente:

(1) Pesquisa dos desvios físicos em relação ao cenário base:

Esta primeira pesquisa utiliza palavras guias, semelhantes à metodologia HAZOP, Hazard and Operability studies (KNOWLTON, 1992), para identificar e definir como os cenários podem se desviar do caso base e com isto causar complexidades que podem contribuir para o EFC's.

Alguns tipos de palavras guias utilizadas são:

Palavra guia	Significado
Não	um desvio que nega o cenário base
Mais	um desvio que representa um aumento quantitativo
Menos	um desvio que representa uma diminuição quantitativa
Muito rápido/lento	um desvio que representa uma mudança na velocidade ou na taxa esperada

Considerando as vulnerabilidades potenciais identificadas no passo 5, as palavras guias sugeridas devem ser aplicadas ao evento iniciador ou ao cenário como um todo, para determinar se as mudanças no iniciador ou no cenário (isto é, os

desvios) podem resultar em ações do operador relevantes para os HFE's ou UA's de interesse. Ao aplicar cada palavra guia, deve ser identificado como o iniciador ou o cenário pode se tornar diferente do caso base (isto é, os possíveis desvios), assim como a importância de cada desvio potencial.

Para os desvios físicos identificados, deve ser verificado se o mesmo poderia ter sido causado por uma simples ação do operador, particularmente, um erro do tipo slip ou lapse, o qual é de difícil recuperação ou até mesmo irrecuperável[2]. Tais ações podem ser causadas pelos tradicionais problemas de fatores humanos (por exemplo, interface homem-máquina) ou por leituras ou interpretações erradas de indicadores pelo operador. Estes problemas ocorrem, normalmente, quando a progressão do cenário é muito rápida ou confusa, alguma coisa acontece que interrompe a percepção comum que a equipe tem do problema, encorajando a ações independentes ou interfere no relacionamento e comunicação da equipe, ou um desentendimento a respeito das condições do estado da planta, onde a interpretação errada, manifestada por um operador, é aceita por toda a equipe.

A seguir, deverão ser identificados quais UA's e HFE's de interesse que poderão ser causados pelas características dos desvios identificados. Isto é feito com o uso de tabelas constante do NUREG-1624, Rev. 1 (2000), capítulo 9, onde, para cada característica dos desvios identificados acima, é identificado: (1) se existe uma tendência do operador em cometer uma UA e HFE e (2) se o tipo de erro identificado corresponde a algum HFE ou UA, relevantes para a tarefa de interesse. Finalmente, o mecanismo de erro, aplicável à UA ou HFE e associados com as condições da planta, será identificado a partir do tipo de erro identificado.

[2] Um equipamento é definido estar irrecuperável quando ele não pode ser atuado no momento em que é requerido porque o mesmo está bloqueado, desabilitado ou com danos irreparáveis devido a uma ação do operador, ou por outro lado, impedido de operar devido à condições criadas após uma ação do operador. A identificação de falhas irrecuperáveis dependerá do conhecimento da cronologia do cenário e do projeto de equipamentos e sistemas, dependências entre sistemas e equipamento, controles do operador, etc.

Também deverão ser identificadas (com o uso das tabelas) as características dos parâmetros relevantes do cenário, em relação aos três primeiros estágios do processamento da informação. Estas características podem ter uma particular influência nos operadores e resultar numa possível UA. Para isto, é identificado, inicialmente, o possível tipo de erro que pode ocorrer. A seguir, deve ser determinado se o tipo de erro identificado corresponde a algum dos HFE's ou UA's que são relevantes para a tarefa de interesse. Finalmente, devem ser identificados quais mecanismos de erros estão associados com o tipo de erro considerado. Dos possíveis mecanismos de erros, deve-se determinar qual mecanismo de erro pode ser aplicável para o HFE ou UA, considerando as condições da planta associadas.

(2) Pesquisa das regras relevantes: avaliar as regras (decisões chaves relacionadas com procedimentos formais) com respeito aos possíveis desvios.

As características (dos desvios) identificadas acima serão avaliadas em relação aos procedimentos, para identificar se o correto cumprimento dos procedimentos e das regras levarão a algum HFE causado pelas diferenças dos parâmetros ou pela cronologia (tempo) em relação aos assumidos nos procedimentos. Se houver diferenças, então o procedimento está, tecnicamente, incorreto e tais diferenças serão analisadas, posteriormente, como um EFC inicial.

Esta pesquisa é semelhante a executada no passo 5, porém, neste caso, os pontos de decisão das regras formais e informais serão avaliados considerando as características dos desvios identificados na primeira pesquisa do passo 6, ao invés do cenário base. Devem ser, também, identificadas as condições da planta, no caso, os desvios do cenário base, que podem disparar o uso de regras formais ou informais, de uma maneira tal que podem levar à ações inseguras.

(3) Pesquisa de dependências entre sistemas suporte:

Os históricos de acidentes tem demonstrado que eventos sérios podem ser influenciados por dependências entre sistemas suporte. Por exemplo, o evento de TMI-2, foi iniciado pelo fechamento das válvulas de AAE, que por sua vez, foi causado pela entrada de umidade no sistema de ar de instrumentos. Portanto, um método eficiente de pesquisa das condições da planta que produzem contextos que forçam ao erro, deve contemplar dependências entre os sistemas suporte e os sistemas de segurança ou os sistemas operacionais.

A importância de tais dependências é dupla:

Se o sistema que falhou e causou o desarme do reator é requerido para as ações pós-desarme então, uma possível dependência, complicada e inesperada, deste sistema com sistemas suportes pode complicar ou atrasar a resposta do operador.

A falha de um sistema suporte que acabou ocasionando o desarme do reator, causa uma falha adicional, complicada e inesperada, em um sistema requerido operar pós-desarme, dificultando o diagnóstico e desta maneira, afetando a resposta do operador.

Uma vez identificadas as dependências, deve ser investigado quais possíveis eventos resultaram na falha do sistema suporte. Em particular, devem ser identificadas aquelas falhas que podem ter efeitos amplos em, não somente no sistema que falhou e causou o desarme do reator, mas também em sistemas de segurança que são requeridos operar em resposta à acidentes.

(4) Pesquisa das tendências do operador e tipos de erros:

Identificar quais tendências dos operadores e tipos de erros correspondem aos HFE's e UA's de interesse.

Esta quarta pesquisa é realizada, essencialmente, em ordem "inversa", se comparada com as três primeiras pesquisas. Inicialmente, são identificados os

possíveis tipos de erros devido às tendências do operador, que podem causar os HFE's ou UASs de interesse e depois, as condições da planta e regras associadas com tais impropriedades da resposta do operador. Esta pesquisa serve como uma varredura para ver se algum caso possível foi esquecido nas pesquisas anteriores.

A pesquisa consiste de duas tarefas: identificar (1) as tendências do operador que originam os HFE's e UA's e (2) os tipos de erros que originam os HFE's e UA's de interesse. Em ambos os casos, a atividade final é identificar as condições da planta e as regras que podem levar às tendências do operador e tipos de erros de interesse. Esta pesquisa utiliza as tendências e vulnerabilidades descobertas no passo 5 e pesquisa desvios que poderiam disparar aquelas tendências que resultariam em ações inseguras para o cenário.

Após a conclusão das pesquisas acima, as características dos diferentes desvios que foram identificados, serão combinadas para desenvolver uma descrição do cenário divergente, orientada pelas vulnerabilidades potenciais identificadas no passo 5.

Para isto, inicialmente, as características encontradas devem ser sumarizadas. Estas representam os elementos do EFC inicial (isto é, as condições da planta, talvez algum PSF e as explicações do comportamento do operador associado com os elementos contextuais), o qual será trabalhado nos próximos passos. Após, deve ser desenvolvida uma descrição do cenário divergente (que leva aos HFE's e UA's de interesse), o qual deve ser, significativamente, diferente do cenário base.

O desenvolvimento destes cenários divergentes requer um bom conhecimento da operação da planta. Este desenvolvimento é similar ao utilizado para criar cenários para treinamento em simulador, por isto a ajuda de instrutores e pessoal licenciado é de grande valor. Igualmente, o cenário divergente criado, poderá ou deverá ser exercitado no simulador, para fazer possíveis refinamentos.

4.7.7 Passo 7: Identificação e avaliação dos fatores complicadores e ligações com os PSF's

Este passo expande e aprimora a definição do EFC iniciada no passo 6. Como mostrado na figura 4.6, devem ser considerados o seguinte:

- fatores que formatam o desempenho (PSF);
- condições físicas adicionais, tais como:
  - falhas adicionais de equipamentos, problemas de configuração ou indisponibilidades;
  - falhas de indicadores;
  - condições da planta que pode confundir o operador; e
  - fatores não formalmente considerados nas APS's

Este passo pode ser realizado, se necessário, iterativamente com a quantificação (passo 10). Em particular, a quantidade de fatores complicadores, que serão introduzidos no EFC, são melhores estimados se baseados em considerações de quantificação.

Se o contexto, identificado no passo 6, for julgado suficientemente forte (fortemente definido pelos desvios físicos), então, somente os PSF's disparados por este contexto serão identificados neste passo. Se, por outro lado, o contexto identificado no passo anterior requerer fatores adicionais, então ambas as categorias de fatores complicadores (PSF e condições da planta) serão identificados.

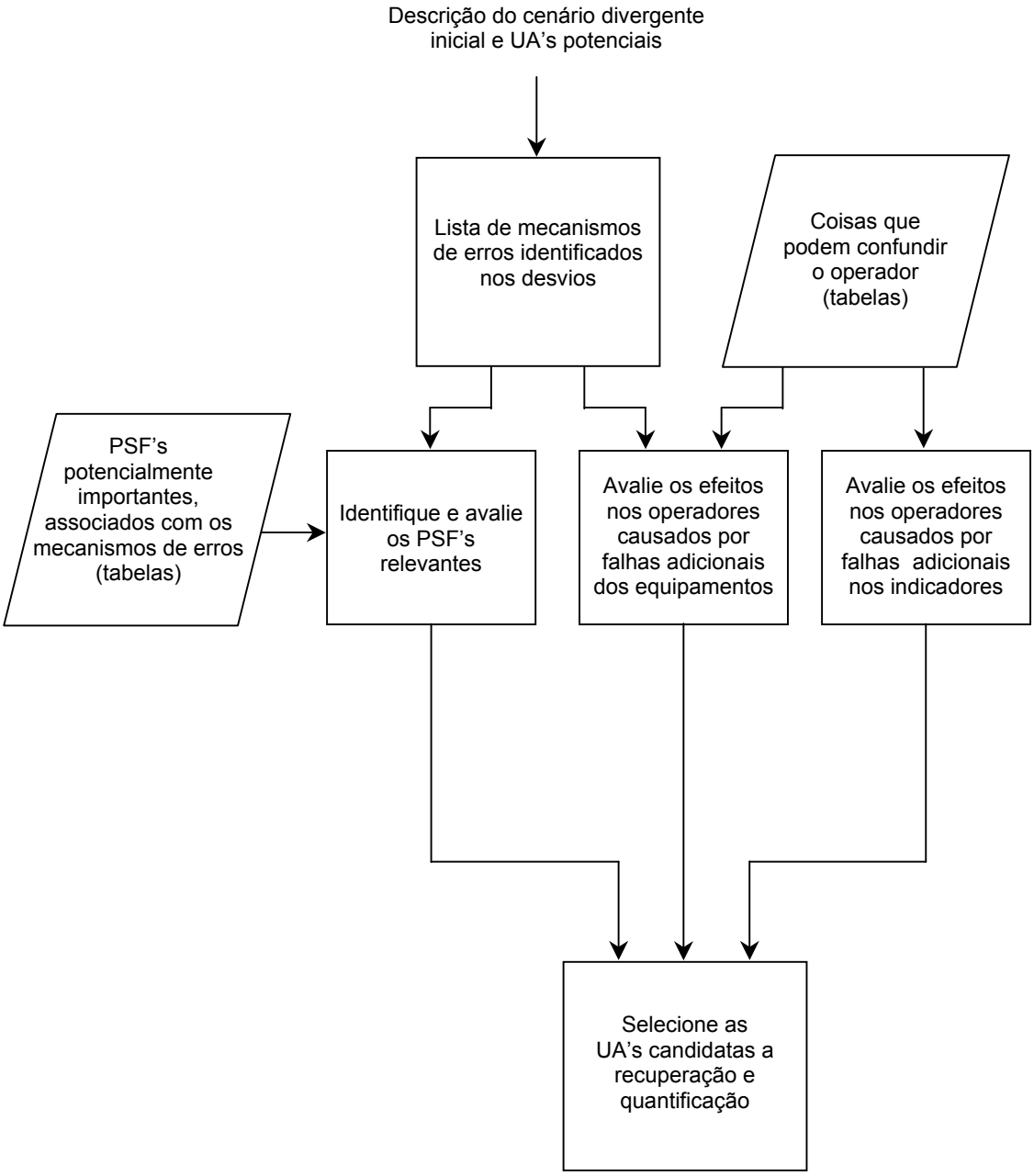


Fig. 4.6 Avaliação dos fatores complicadores

Inclusão de PSF's:

Existem dois tipos de PSF's que poderão ser incluídos no cenário divergente, inicialmente, definido no passo 6. São eles:

- PSF's que são disparados pelo contexto já definido; e
- PSF's adicionais que não são específicos do contexto.

PSF's que são disparados pelo contexto identificado no passo 6 incluem aqueles que estão relacionados às condições específicas da planta e aqueles associados com os tipos e mecanismos de erro. Exemplos incluem:

- Qualquer PSF relevante constante das tabelas 9.15b e 9.16b do NUREG-1624, Rev 1 (2000), associado com um mecanismo de erro identificado;
- Procedimentos não aplicáveis ao cenário divergente específico ou, por outro lado, são de difícil implementação;
- Localização de painéis que dificultam, aos operadores, a monitoração do estado da planta ou a realização de tarefas requeridas em resposta ao cenário divergente; e
- Alta carga de trabalho do operador devido à falhas múltiplas de equipamentos, etc., em cenários divergentes.

Os PSF's relacionados às condições específicas da planta são, normalmente, relacionados com:

- procedimentos
- treinamento
- comunicação
- supervisão
- funcionários
- interface homem-máquina
- fatores organizacionais
- estresse

- condições ambientais
- fatores estratégicos tais como conflitos múltiplos em objetivos, pressão do tempo, recursos limitados.

Os PSF's relacionados aos tipos ou mecanismos de erro, dado o contexto do cenário, estão identificados nas tabelas 9.15b e 9.16b do NUREG-1624, Rev 1 (2000) . Em alguns casos, alguns PSF's podem já ter sido identificados no passo 6. Neste caso, estes PSF's deverão ser revistos para identificar se são aplicáveis ao cenário divergente considerado.

Em alguns casos, a pesquisa do passo 6 não incluiu o mecanismo de erro. Nestes casos, os PSF's devem ser considerados mais globalmente usando recursos tais como a lista de PSF's dada acima e as condições da planta que são usadas para descrever o cenário divergente. Os PSF's identificados desta maneira são específicos do contexto mas não foram focalizados como um mecanismo de erro identificado.

Os demais PSF's, que não são específicos (disparados) do contexto, são identificados através de considerações da definição do cenário divergente e da revisão da lista de PSF's. Exemplos de tais PSF's (que não são específicos a nenhum desvio, entretanto podem ser específicos da planta) são:

- o impacto da hora do dia no desempenho do operador;
- estresse ou carga de trabalho (de origem não específica); e
- diretrizes gerenciais gerais ou outras orientações.

Entretanto, a inclusão de tais PSF's, que não são disparados ou ativados pelo contexto, deve ser muito cuidadosa, em selecionar os PSF's que podem representar vulnerabilidades que podem contribuir significativamente para o EFC.

Outra razão desta restrição é que os PSF's não disparados pelo contexto podem reduzir a probabilidade do EFC. Por isto, a preocupação deve ser em incluir somente aqueles PSF's que podem aumentar a probabilidade de uma ação insegura

associada com o HFE, isto é, de aumentar as chances de que os operadores tomarão ações inseguras.

Condições físicas adicionais:

Igualmente, como a inclusão de PSF's visto anteriormente, poderão ser incluídas mais condições físicas no EFC inicial, identificado no passo 6. Entretanto, da mesma forma como ocorreu com os PSF's adicionais, tais condições físicas poderão reduzir a probabilidade ou a freqüência do HFE.

Como ilustrado nos exemplos de eventos reais analisados e na experiência operacional, os eventos sérios envolvem, normalmente, elementos contextuais que podem estar relacionados com uma ou mais das seguintes categorias de desvio das condições da planta: física, informação, equipamentos e configuração da planta. Os desvios físicos foram contemplados no passo 6. Conseqüentemente, os seguintes tipos de condições adicionais da planta podem ser considerados:

- falhas adicionais de equipamentos, problemas de configuração ou indisponibilidades;
- indicações de falhas;
- condições da planta que podem ser confusas para o operador; e
- fatores não normalmente considerados nas APS's.

Igualmente, como na pesquisa das condições físicas, deverá ser investigado se existem falhas irrecuperáveis causadas por slip ou lapse (tanto de interações do operador com equipamentos quanto erros de leitura ou de interpretações de indicadores), relativas aos fatores acima, que podem afetar as condições da planta.

A tabela 4.6b contém exemplos de causas falhas de equipamentos, problemas de configuração ou indisponibilidades não modeladas.

Inicialmente, devem ser consideradas aquelas condições já identificadas ou aquelas que são uma extensão dos contextos já definidos no passo 6. Por exemplo,

TABELA 4.6b Exemplo de falhas de equipamentos, problemas de configuração e indisponibilidades	
Tipo de condições da planta	**Exemplos**
Resposta de equipamentos	Falhas randômicas (incluindo falhas múltiplas, atuações espúrias)
	Falhas induzidas pelo iniciador
	Falhas induzidas pelo modo (por exemplo, equipamento inoperável ou indisponível durante condições de desligamentos)
	Falhas de modo comum
	Outras falhas dependentes (por exemplo, falhas por sistemas suporte ou por efeitos cascata, induzidos pelo homem, etc.)
	Problemas operacionais pré-existentes
	Operação degradada
	Além das bases de projeto
	Induzidas pelo homem (tanto falhas latentes quanto falhas ativas)
Configuração da planta	Atividades concorrentes (como elas afetam as ações requeridas do operador para responder ao acidente)
	Falhas latentes (como elas afetam as ações requeridas do operador para responder ao acidente; veja também, como acima, resposta dos equipamentos, induzidas pelo homem)
Indisponibilidades	Indisponibilidades realísticas (por exemplo, todos os trens fora de operação para manutenção)

se falhas de equipamentos já são parte do cenário divergente do passo 6, estas falhas podem ser explicadas por falhas de modo comum ou outras falhas dependentes. O conhecimento do projeto e da operação da usina é crucial em identificar tais extensões plausíveis ou ligações ao contexto, previamente, definido. Pela inclusão de condições adicionais que são relacionadas com EFC definidos inicialmente, o EFC inicial será fortalecido com uma mínima redução da probabilidade do HFE.

Para a avaliação e inclusão destas condições físicas adicionais, no cenário original gerado no passo 6, a ATHEANA fornece tabelas com exemplos para falhas de indicadores (com tipos diferentes de falhas e de causas) (tabela 9.18), para condições da planta (físicas e de comportamento) que podem confundir o operador (tabela 9.19 a 9.21) e para fatores que podem ser importantes para o desempenho do operador que não são, normalmente, consideradas pelas APS's (Tabela 5.7).

Se elementos novos foram considerados, neste passo, então, a descrição do cenário divergente inicial deverá ser revisada para refletir estas novas considerações. Em particular, as novas condições da planta ou os fatores que formatam o desempenho devem ser integrados na descrição do cenário. Estas novas condições da planta ou PSF's podem ativar mecanismos de erros diferentes ou adicionais.

Com a conclusão deste passo, o EFC é agora considerado, suficientemente, forte para fazer os cálculos das probabilidades dos HFE's e das UA's desejados.

4.7.8 Passo 8: Avaliação do potencial para recuperação

Dada a descrição do contexto, onde foi gerado o erro inicial em responder a um desvio específico do cenário divergente, é possível que, mais tarde, durante o desenvolvimento da sequência do acidente, o operador reconheça o seu erro e seja capaz de corrigir a ação inicial antes que ocorram danos ao núcleo ou uma falha de função.

Neste passo, com as considerações das oportunidades para a recuperação (ou mais precisamente, a não recuperação) dos erros iniciais, que serão analisadas, as definições de HFE e dos EFC associados serão completadas. Este passo, como envolve a extensão do contexto definido nos passos anteriores, ele também é iterativo com os passos 6 e 7. Durante a análise, se for garantido que um HFE pode ser

recuperado, a análise pára e passa para a solução da tarefa. Caso contrário, a análise continua de acordo com a discussão abaixo.

A definição dos HFE's ou das UA's e o contexto associado (representada pela descrição do cenário modificado) correspondem a um erro inicial. Dado este erro inicial, é possível que, mais tarde, na sequência do acidente, este erro seja reconhecido e os operadores estejam aptos a corrigir suas ações iniciais antes que ocorram danos ao núcleo ou alguma outra falha funcional. Portanto, a análise deve investigar quais oportunidades existem para correção com sucesso.

Na avaliação para a recuperação, devem ser considerados os seguintes elementos, na análise das ações de recuperação potenciais:

- Definição de uma possível ação de recuperação, se o UA/HFE foi realizado:
- Tempo disponível para realizar as ações de recuperação, de maneira a evitar consequências sérias (por exemplo, dano ao núcleo);
- A existência e o momento (quando) de sintomas adicionais, que podem alertar os operadores para a necessidade de recuperação e fornecer informações suficientes para identificar as ações de recuperação aplicáveis;
- A existência e o momento (quando) de recursos adicionais (por exemplo, pessoal) que pode auxiliar na recuperação; e
- Uma avaliação da intensidade dos sinais da necessidade de recuperação, com respeito ao EFC inicial (isto é, condições da planta, PSF's, e mecanismos de erro associados) e, consequentemente, a probabilidade do sucesso da recuperação.

Considerando as ações acima, inicialmente, deve-se decidir quais são as ações de recuperação necessárias. Isto está baseada no entendimento de qual função ou equipamento de segurança falhou ou foi desafiado, como resultado da UA/HFE. Adicionalmente, deve-se determinar o tempo necessário para realizar estas ações antes que ocorram os danos indesejados. A partir destas informações deve-se

desenvolver uma progressão do cenário divergente, começando na perda inicial ou na degradação de função ou equipamento de segurança.

O registro da progressão do cenário deve destacar mudanças previstas nas condições e nos parâmetros chaves da planta, assim como qualquer novo sinal, provável de ocorrer, como resultado da progressão do cenário. Estes novos sinais e os recursos que foram identificados (os quais são avaliados quanto à sua importância) formarão a base para definir elementos contextuais adicionais que estarão associados com a não recuperação.

Entretanto, o tempo disponível para correção é um fator preponderante. Pouco tempo ou nenhum tempo disponível para recuperação, desde o erro inicial, tornará as chances para recuperação bem reduzidas. Se o tempo for suficiente, deve-se olhar para as dependências potenciais entre a descrição do cenário divergente (isto é, o EFC) da ação insegura inicial e a falha em corrigir a ação inicial. A falha em corrigir a ação insegura inicial pode ser ocasionada por vários motivos: o modelo mental (avaliação da situação) é muito difícil de corrigir; os operadores podem estar distraídos (ou muito ocupados) com outras atividades, que não viram os sintomas e perderem a oportunidade para reagir; e, finalmente, porque os operadores sempre podem justificar o atraso de suas ações além do tempo requerido, especialmente, se os equipamentos da planta estão normais ou retornam à operação (ou falharam por slip ou lapse) e as consequências da ação de recuperação são consideradas extremas. Estas possíveis oportunidades de recuperação perdidas deverão ser avaliadas para identificar se estes sinais da anormalidade se mostravam, realmente, necessitado de atenção urgente, em relação aos possíveis motivos que levaram o operador a não tomar nenhuma ação de recuperação. Quaisquer novos elementos do EFC resultantes que estão associados com as ações de recuperação devem ser acrescentados no EFC da ação insegura inicial, de maneira a completar o EFC para o HFE que será modelado na APS.

Finalmente, deve-se comparar o contexto do EFC desenvolvido neste passo, com as características de sérios acidentes e com os fatores complicadores não usualmente modelados nas APS's, listados nas tabela 5.6 e 5.7 do NUREG-1624 (2000), respectivamente. Estas duas tabelas podem ser consideradas como modelo de referências para os contextos que forçam ao erro.

As análises de recuperação podem adicionar novos elementos à descrição do cenário divergente (ou contexto que força ao erro). Portanto, como nos casos anteriores, a descrição do cenário deve ser reintegrada considerando os resultados desta análise. Como no passo 7, os elementos adicionados ao contexto que induz ao erro, resultantes da análise de recuperação podem ativar mecanismos de erro diferentes ou adicionais.

O produto do passo 8 é a finalização do EFC para o HFE e UA's de interesse, como parte da descrição geral do cenário divergente. Entretanto, como dito inicialmente, iterações entre este passo e o passo de quantificação (9) poderá ser necessário.

4.7.9 Passo 9: Quantificação dos EFC's e das UA's

ATHEANA foi criada visando, principalmente, a modificar o processo da representatividade do desempenho humano nas análises probabilísticas de segurança, onde foi constatado, pela análise da experiência operacional, que os métodos vigentes não contemplavam, adequadamente, a ação do operador, vista nos acidentes sérios. Adicionalmente, o crescimento do interesse do órgão regulatório americano, NRC, em dirigir suas ações de fiscalização em informações baseadas em risco (APS), concorreram para a criação da metodologia ATHEANA e no desenvolvimento do seu processo de quantificação. Entretanto, durante o seu desenvolvimento, este processo também se mostrou útil para uma variada gama de análises, desde análises puramente qualitativas, até análises exaustivamente

quantitativas, passando por análises quantitativas simplificadas. Por exemplo, se o interesse for em determinar se “existe alguma maneira pela qual o operador pode ser levado a desligar o sistema de injeção de segurança, prematuramente, durante um médio LOCA?” então a análise não precisa ser quantitativa, uma análise qualitativa daria a resposta a esta questão. Em outras aplicações, pode ser desejado saber alguma informação sobre a contribuição relativa para o risco em termos de se determinar qual é a probabilidade de ocorrer uma ação insegura dada a existência de um determinado mecanismo de erro. Quando a quantificação da probabilidade não é requerida, o julgamento pode ser simplificado a uma simples comparação relativa, do tipo de “alto”, “médio” ou “baixo”, quando pode se determinar, por exemplo, que um projeto A é melhor ou pior do que o projeto “B”.

A abordagem quantitativa difere, significativamente, dos métodos tradicionais de ACH, porque, enquanto estes estimam a chance de ocorrer um erro humano (randômico) em condições nominais de acidentes (ou sob outras condições especificadas nas árvores de eventos e árvores de falhas das APS’s), a ATHEANA avalia a probabilidade de uma classe específica de contextos que forçam ao erro dentro de uma larga faixa de condições alternativas que podem existir na definição de um cenário e então, avaliar a probabilidade condicional de uma ação insegura ocorrer, dada a ocorrência deste contexto.

A análise quantitativa aborda 3 processos independentes, porém inter-relacionados entre si. São eles:

(1) a probabilidade do EFC em um cenário específico;

(2) a probabilidade das UA’s, condicionadas a este contexto, que podem causar os eventos de falha humana; e

(3) a probabilidade de que estas UA’s não serão recuperadas antes que uma falha catastrófica ocorra (tipicamente, danos ao núcleo, como modelado nas APS’s).

Estes três processos de quantificação não são diferentes, conceitualmente, da abordagem dos demais métodos de ACH. Entretanto, existem dois aspectos que os diferenciam: primeiro, tanto as UA's quanto as falhas em recuperar são, extremamente, dependentes do contexto. Por exemplo, se o operador desligar determinado equipamento, baseado na sua avaliação da situação, de que o mesmo não é necessário, é muito improvável que ele revisará esta avaliação, mesmo se ocorrer pequenas mudanças no contexto, que o levou a tomar a ação inicial. Segundo, a UA e sua ação de recuperação são, fortemente, dependentes entre si. Por exemplo, no acidente de TMI-2, os operadores mantiveram a injeção de segurança desligada por várias horas, mesmo com indicações contrariando esta ação. Em outras palavras, uma vez tomada uma ação, o operador permanecerá nesta decisão mesmo se ocorrerem mudanças no contexto (fatores psicológicos do processamento da informação).

(1) A quantificação do EFC, normalmente, é baseada na árvore de eventos da APS, para um determinado evento iniciador. Por exemplo, supor uma árvore de eventos (simplificada) para um médio LOCA (fig. 4.7), onde está representada a função de injeção de segurança (resfriamento do núcleo). Esta representação indica que, se ocorrer uma falha da função de injeção de segurança, isto causará um resfriamento deficiente do reator e levará, diretamente, a dano ao núcleo. Neste caso, o objetivo da análise a ser realizada é a ação humana que termina, prematuramente, a injeção de segurança. A quantificação, segundo a metodologia ATHEANA, é calcular a probabilidade da ocorrência do contexto, EFC, onde poderia ocorrer esta ação insegura, a própria UA e a falha em recuperar esta UA.

O EFC é constituído por dois elementos diferentes, porém, fortemente dependentes entre si, que são as condições da planta e os fatores que formatam o desempenho, PSF. Estes dois elementos são quantificados, separadamente, para

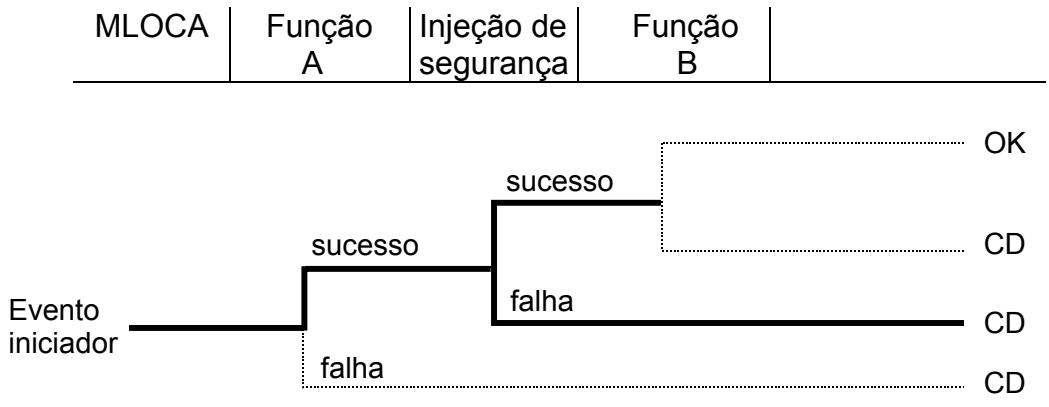


Figura 4.7 – Árvore de eventos simplificada para o MLOCA

juntos, fornecer a probabilidade total do EFC.

As condições da planta incluem o estado físico da planta, a operabilidade dos equipamentos e as operações e evoluções que estão sendo realizadas. Estas condições, poderiam incluir, por exemplo, o evento iniciador e suas influências na planta. Adicionalmente, inclui modos de falhas não usuais e comportamentos anormais de equipamentos modelados pelas APS's e também, equipamentos não, normalmente, modelados, tais como indicadores e partes relacionadas com sistemas de controle e de instrumentação.

Para quantificar as probabilidades destas condições, deve ser coletada uma série de informações específicas da planta, relacionadas com o EFC de interesse, o qual foi definido no passo 9. As seguintes informações poderão ser necessárias:

- Frequência do iniciador;
- Freqüência de certas condições da planta (por exemplo, parâmetros da planta, comportamento da planta), dentro de um tipo específico de iniciador;
- Frequências de certas configurações da planta, evoluções, etc.;

- Probabilidade de falhas de equipamentos, instrumentos, indicadores, etc.;
- Probabilidade de falhas dependentes de múltiplas peças de equipamentos, instrumentação, indicadores, etc.;
- Indisponibilidade (principalmente, múltiplas) de equipamentos, instrumentação, indicadores, etc. devido a testes ou manutenções;
- Frequências de reparos, calibrações e outras falhas humanas latentes que resultam em (principalmente, múltiplas) falhas de equipamentos, instrumentação, indicadores, etc.; e
- A probabilidade dos PSF's específicos, se presentes, como definido nos passos 6 e 7; e
- avaliação de complexidades adicionais.

Os tipos de informações necessárias para a quantificação da probabilidade dos EFC's usando ATHEANA, dependerão dos elementos dos EFC's identificados no processo de pesquisa. Algumas destas informações poderão estar, prontamente, disponíveis na planta. Outras dependerão de cálculos de engenharia (alguns já poderão estar disponíveis para outras aplicações, como para a própria APS) ou de julgamento, tanto qualitativo quanto quantitativo, de especialistas. Se não existirem dados disponíveis para gerar as frequências e probabilidades necessárias, o pessoal da planta deverá ser entrevistado para se obter as necessárias informações para gerar a quantificação. Em alguns casos, o pessoal experiente da usina poderá dar informações baseadas na sua própria experiência ou no seu conhecimento. A equipe que está aplicando a ATHEANA deverá transformar estas informações para a forma requerida para a análise. Em outros casos, estas pessoas poderão passar, somente, informações qualitativas que requererão grandes interpretações e manipulações (e, provavelmente, algum julgamento por parte da equipe ATHEANA) antes de produzirem as adequadas informações necessárias para a quantificação.

Quanto aos fatores que formatam o desempenho, PSF, deverão ser considerados dois tipos:

- PSF's que são disparados ou ativados pelas condições da planta de um determinado cenário divergente, definido nos passos 6 e 7; e
- Outros PSF's que não são específicos para o contexto do cenário divergente.

Os PSF's ativados pelo contexto, na grande maioria dos casos, terão a probabilidade de ocorrência igual a 1,0 (por exemplo, para alguns cenários poderia ser a inexistência de procedimento específico, treinamento ou indicações disponíveis para o contexto específico). Existem cenários, em que o PSF é aplicável para somente uma determinada faixa de condições existentes. Nestes casos, se a freqüência ou a probabilidade destas condições puderem ser determinadas, então o PSF ativado poderá ser avaliado. Em alguns casos, os PSF's negativos influenciam, apenas, uma certa fração dos operadores.

Os PSF's que não são específicos (isto é, genéricos) em relação ao contexto, mas que ainda são específicos da planta deve se verificar, primeiro, se existe alguma condição da planta que poderia tornar estes PSF's mais prováveis de ocorrer. Se existir, então deve se considerar a inclusão destas condições ao EFC, de acordo com as orientações dos passos 6 e 7. No caso do PSF's não serem ligados a nenhuma condição da planta, então, os instrutores e o pessoal da usina deverão ser consultados para se determinar a probabilidade destes. Deve-se procurar identificar, também, aqueles PSF's cujas influências aumentam a probabilidade da ocorrência da combinação EFC e UA's. A inclusão de PSF's que não são disparados pelas condições da planta, inevitavelmente, reduzirá a probabilidade do EFC, mas aumentará a probabilidade da UA. O resultado líquido destas mudanças, na probabilidade, poderá ser um aumento ou uma diminuição. Portanto, deverão ser avaliados aqueles PSF's onde aumentam esta combinação. Outros PSF's poderão ser interligados a uma variedade de fatores, tais como, regras informais (isto é, "do jeito

que nós fazemos, aqui"), treinamento prático, operação e experiência em simulador, sala de controle, projeto da planta, etc.

(2) A quantificação das ações inseguras deverá considerar os seguintes três tipos de condições, que determinam como a probabilidade da UA será estimada:

1- O EFC é tão forte que a ocorrência da UA é, praticamente, certa;
2- O EFC não é tão forte que não causa aumento da probabilidade da UA, se comparada com o contexto normal da APS; e
3- A influência do EFC é variada onde a probabilidade pode recair em algum ponto entre estes extremos.

Na estimativa da probabilidade da UA, inicialmente, é requerido que se inicie as estimativas daquelas ações inseguras que não precisam de um alto nível de precisão. No caso, são as condições do nível 1 acima, onde a probabilidade de ocorrência pode ser estimada em 0,5. Esta probabilidade pode ser aplicável para aqueles casos onde o contexto, que se apresenta ao operador, parece ser, totalmente, consistente com o ponto de vista do operador, onde a UA é a coisa certa a fazer nestas circunstancias. Um exemplo poderia ser um evento onde as informações da planta estão falhas ou confusas, mas está de acordo com os critérios dos procedimentos, para os quais existe redundância limitada ou desprezível e a ação é normal e esperada para aquilo que os operadores acreditam estar ocorrendo. Em outras palavras, o contexto é, extremamente, compelidor.

Para a condição 2, o EFC pode ser considerado, excepcionalmente, fraco. Nestes casos, ATHEANA recomenda utilizar métodos tradicionais de ACH, que não são dirigidos para erros causados por EFC. Entretanto, na prática, estas condições que não forçam, significativamente, ao erro , podem ser identificadas e eliminadas quando das avaliações realizadas nos passos 6 e 7 do processo.

Entretanto, na prática, muitos, ou talvez, a maioria dos contextos cairão entre os extremos citados acima (condição 3). Nestes casos, existem duas possibilidades para as estimativas da probabilidade da ação insegura, dado o contexto:

1- Situações onde os instrutores de operadores experientes observaram situações similares das condições da planta, no treinamento, e observaram que uma fração, consistente, da equipe de operadores executou as mesmas UA's sendo modeladas.
2- Situações requerendo estimativas da probabilidade da UA usando métodos de modelagem.

A situação preferencial é aquela na qual os instrutores dos operadores podem fornecer o seu julgamento como uma informação, relevante, para a quantificação da ação insegura, baseado no fato de que os instrutores:

- possuem um grande conhecimento da experiência operacional (sua própria e de todo o pessoal licenciado);
- Conhecem como os operadores reagem às situações;
- Possuem estatísticas de falhas, portanto possuem um entendimento da probabilidade de falhas; e
- Sabem como criar cenários, onde os operadores irão falhar.

Para estes casos existem diversas técnicas disponíveis para estruturar o cálculo de tais probabilidades. Por exemplo, aquelas discutidas por SEAVER & STILLWELL (1983) no NUREG/CR-2743, BUDNITZ *et al*. (1997) e OTWAY & WINTERFELDT (1992). Adicionalmente, os Apêndices B a E do NUREG-1624 (2000), ilustram várias abordagens para quantificação das UA's.

Para a estimativa das UA's usando a modelagem, a metodologia ATHEANA discute duas bases distintas para estimar a probabilidade, entre as várias abordagens existentes. Em ambos os casos, é requerido um julgamento sobre quão relativamente compelidor ou intenso é o contexto que força ao erro. Isto é feito em uma escala onde

os pontos extremos da faixa de valores de probabilidade são conhecidos: em uma extremidade, a probabilidade é igual a 1,0 e na outra, corresponde ao valor estimado da probabilidade do erro humano calculado pelos métodos tradicionais de ACH, que considera, pelo menos, algumas mínimas contribuições de contextos negativos (por exemplo, disponibilidade de tempo ou layout do painel). A quantificação da UA pela ATHEANA, portanto, precisa estimar onde a influência exercida pelo contexto está (Figura 4.8).

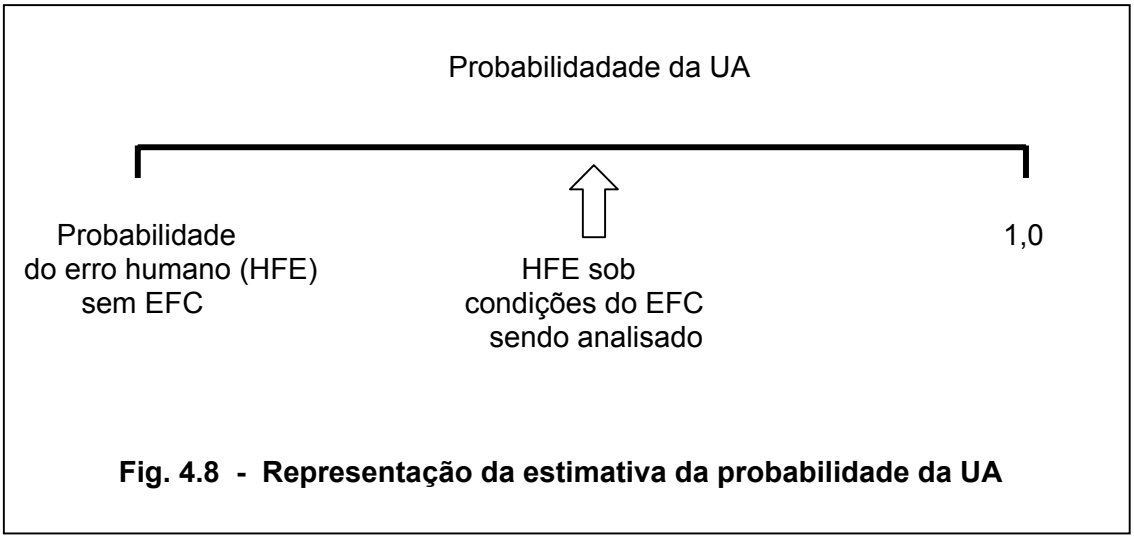


Fig. 4.8 - Representação da estimativa da probabilidade da UA

Para identificar onde as condições sendo analisadas se localizam, a ATHEANA (NUREG-1624, Rev. 1, 2000) sugere os dois métodos. Entretanto, deve-se reconhecer que não existe um método absoluto para este julgamento. A parte importante deste processo é para explicar as bases para a avaliação, quais fatores são considerados importantes e porque.

O primeiro método, denominado HEART (WILLIAMS, 1988), fornece uma base para avaliar o grau no qual o contexto influencia a probabilidade de falha. O método

consiste de dois passos: (1) Identificar, numa tabela (Tabela 4.6c), a descrição genérica da atividade que mais se aproxima do contexto da ação que está sendo analisada, e depois (2) aplicar um fator (multiplicador, tabela 4.6d), que corresponde ao PSF, para ajustar a probabilidade. As probabilidades de falhas usando HEART são, tipicamente, mais altas do que a maioria dos métodos tradicionais de ACH. Por exemplo, probabilidades de erro humano naquelas situações onde o EFC não é compelidor, muito, frequentemente, caem em uma faixa onde o limite inferior é da ordem de 10^{-3} a 10^{-4}, como mostrados nas avaliações de IPEs do NUREG-1560 (1996), embora eventos, para os quais existe, por exemplo, um tempo limitado para ações, pode ter uma probabilidade, significativamente, mais alta.

Tabela 4.6c - Probabilidade de falhas de tarefas genéricas do HEART

Descrição da tarefa genérica	**Probabilidade de falha**
Totalmente não familiar, realizada numa velocidade sem idéia real das prováveis consequências	0,55 (0,35- 0,97)
Tarefa complexa requerendo alto nível de compreensão ou habilidade	0,16 (0,12 – 0,28)
Tarefa relativamente simples, executada rapidamente, necessita pouca atenção	0,09 (0,06 – 0,13)
Rotineira, praticada intensamente, tarefa rápida envolvendo relativamente baixo nível de habilidade	0,02 (0,007 – 0,045)
...	...

Tabela 4.6.d - Fatores que formatam o desempenho do HEART	
Contexto que induz ao erro	**Acréscimo máximo na probabilidade de falha**
Não familiar com a situação, que é, potencialmente, importante, mas que ocorre infrequentemente ou é nova	17
Tempo disponível para deteção ou correção insuficiente	11
Uma relação sinal/ruído baixa	10
Um meio para cancelar ou sobrepor informações ou dispositivos de controle que é rapidamente acessível	9
Uma diferença entre o modelo do operador e aquele imaginado pelo projetista	8
...	...

Um segundo método para verificar onde o EFC se localiza no gráfico da figura 4.8, é o SLIM (EMBREY *et al.,* 1984), método de índice da probabilidade de sucesso, apresentado no capítulo 3. Na aplicação deste método, existem várias questões que precisam ser respondidas:

- Dado o contexto, qual é a probabilidade de disparo dos mecanismos de erros?
- Uma vez disparado o mecanismo de erro, qual é a probabilidade de ocorrer uma ação insegura?
- Uma vez ocorrida a UA, qual é a probabilidade de que ela levará a um evento de falha humana, com dano ao núcleo?

O método pode ser usado, individualmente, para qualquer uma destas três fases ou de uma maneira integrada. Os apêndices B a E da ATHEANA (NUREG-1624, Rev. 1, 2000), ilustram a avaliação de uma maneira integrada.

Como visto no passo 6, quando do desenvolvimento do cenário divergente, PSF's e condições da planta estão associados com mecanismos de erros. Quanto mais negativos forem os PSF's e as condições da planta, presentes em um cenário,

mais provável será a ocorrência de mecanismos de erros e, potencialmente, de ações inseguras. Portanto, o primeiro passo em acessar a probabilidade é julgar quais condições da planta e PSF's associados com um determinado mecanismo de erro são mais importantes e o grau para o qual estes PSF's existem no cenário sendo analisado.

No segundo passo, será avaliada a probabilidade da ação insegura, dada a ocorrência do mecanismo de erro, usando-se, novamente, a escala de graduação do SLIM. Os seguintes mecanismos de erros são considerados, potencialmente, muito prováveis de resultar em ações inseguras:

- Visão de túnel;
- Fixação;
- Tendência para confirmação;
- Complacência;
- Satisfação;
- Incredulidade;
- Explicação simples para problema complexo;
- Eventos tipo garden-path;
- Informações confusas;
- Eventos mascarados; e
- Eventos com múltiplas tarefas se sucedendo muito rapidamente.

Eventos nos quais, estes mecanismos de erros estão presentes podem ser considerados ter uma alta probabilidade de ocorrência de uma ação insegura.
Existem poucos mecanismos de erros considerados ter uma baixa probabilidade de levar à ações inseguras. Por exemplo:

- discriminação limitada;
- relutância;

- impasse; e
- últimas chances nos planos.

Os demais mecanismos de erros são considerados ter probabilidade moderada de resultar em ações inseguras.

(3) O estágio final do processo de avaliação é o cálculo da probabilidade de que a ação insegura perdurará até o evento de falha e consequentemente, causando o evento indesejado, usualmente dano ao núcleo, conforme nos contextos típicos de APS. Este estágio se concentra em várias atividades de recuperação que podem evitar a continuidade da ação insegura até o ponto de dano ao núcleo. São elas:

- Ocorrência de alarmes ou outras indicações que se seguem à ação insegura que podem levar a um questionamento quanto a presteza da ação tomada ou não tomada;
- Oportunidade para novas equipes questionarem o que está ocorrendo; e
- Potencial de alterações posteriores do estado da planta que podem levar a novos alarmes e indicações.

Para analisar as oportunidades para cada uma destas atividades levar a uma efetiva recuperação da ação insegura e ao término da sequência do acidente é necessário uma detalhada avaliação do tempo restante da sequência do acidente, quais informações irão aparecer (dicas e sinais) e como estas informações serão avaliadas em relação aos mecanismos de erros iniciais e à ação insegura resultante. Por exemplo, a sequência de sinais no tempo precisa ser comparada com o tempo disponível para recuperação no contexto da sequência inicial e no seu desenvolvimento. Deve ser avaliada a probabilidade total de não-recuperação para o total da cadeia de sinais que será desenvolvida durante o tempo disponível.

A quantificação da probabilidade de não recuperação para a cadeia de sinais está condicionada ao EFC e a UA originais e ao contexto revisado que aparece devido

a UA e a cadeia de sinais gerados. Não existe fórmula para este processo. O processo está, fortemente, apoiado em julgamentos baseados no conhecimento utilizado nos passos anteriores da quantificação.

As probabilidades estimadas dos EFC, da UA e da sua recuperação possuem um determinado grau de incerteza. As probabilidades das condições da planta são, largamente, advindas da experiência e de outros dados de operação, da mesma maneira que os outros parâmetros são obtida nas tradicionais tarefas de quantificação das APS's. Por exemplo, para aqueles PSF's independentes do contexto, uma abordagem para estimar as incertezas pode ser a experiência e julgamento pelo pessoal da usina, da mesma maneira utilizada para as probabilidades das condições da planta.

Como visto anteriormente, existem três maneiras diferentes de estimar as probabilidades das UA's. Estratégias diferentes serão utilizadas para cada caso. Inicialmente, para aqueles casos onde a probabilidade da ocorrência da UA é, virtualmente certa, a recomendação é usar uma incerteza na faixa de 0,5 a 1,0.

Segundo, para os casos onde o pessoal da usina tem uma grande experiência de treinamento em cenários similares, nos quais uma consistente fração da equipe comete a UA de interesse. Neste caso, se o número de equipes sendo avaliada e o número de vezes que cometeram a UA está registrado, estes dados podem ser utilizados para desenvolver uma distribuição de incertezas. Se um grupo de indivíduos experientes fornecerem as estimativas e não existem dados registrados, então existe um processo para gerar uma distribuição de incertezas baseada na estimativa coletiva.

Com relação ao método HEART (WILLIAMS, 1988), este fornece faixas de incertezas para as probabilidades de falhas para descrições genéricas de tarefas. Elas devem ser usadas de forma mais consistente com o próprio método.

4.7.10 Passo 10: Incorporação dos HFE's nas APS's

Como mostrado no capítulo 2, figura 2.4, a falha humana pode estar presente, em quatro oportunidades, nos modelos de APS: eventos iniciadores, árvores de eventos, árvores de falhas e ações de recuperação.

Uma vez que, os dados utilizados para identificar e quantificar a freqüência da maioria dos eventos iniciadores provém da própria experiência da planta e da indústria, não existe nenhum requisito relativo à decomposição dos eventos iniciadores, em eventos induzidos pelo homem ou não. Também, não é necessário modelar como tais erros humanos podem ocorrer. Entretanto, isto é aplicável quando existir uma pequena ou nenhuma dependência entre a causa do evento iniciador e como o pessoal da planta responderá ao desdobramento da sequência do evento. Se tal relação existir, o processo ATHEANA ajudará a descobrir estas relações através da identificação e definição do contexto que força ao erro. Nestes casos, seria desejável desenvolver ou modificar o modelo da APS existente para acrescentar o iniciador específico que causou o HFE considerado de potencial interesse (isto é, alguns deles poderão ser analisados como evento iniciador separado).

O local onde a incorporação do processo ATHEANA, normalmente, ocorrerá, é na árvore de eventos. Isto é devido ao fato de que os HFE's, definidos pela ATHEANA, serem considerados de mais alta prioridade, pois tendem a levar, diretamente, para o resultado indesejável, que é dano ao núcleo. Os HFE's devem ser definidos de tal maneira, a capturar os erros de comissão (considerados de mais alta prioridade) e os erros de omissão que foram esquecidos para o presente caso de APS e que podem causar o efeito global indesejado. Por exemplo, o resfriamento do núcleo do tipo encher e drenar (feed-and-bleed) pode não ter o sucesso esperado porque o operador falha em iniciá-lo (uma forma de omissão que é, normalmente, encontrado nas APS correntes) ou porque o operador, prematuramente, interrompeu o feed-and-bleed, pensando que não era mais necessário (um erro de comissão a ser incluído usando a

ATHEANA). O local específico, na árvore de eventos, onde estará representado o HFE identificado pela ATHEANA, dependerá de como ele se relaciona, cronologicamente, com a demanda das funções e sistemas envolvidos em responder ao evento iniciador, onde, sua inclusão fornecerá a análise mais eficiente de todas as sequência possíveis representadas na árvore de eventos e a dependência lógica dos outros eventos para com o HFE na sequência. Adicionalmente, poderá ser desejável, ou até mesmo requerido, que, se o sucesso ou falha subseqüente, na sequência, poderia alterar, significativamente, o tratamento do HFE incorporado (por exemplo, pelo fornecimento de novas dicas para ações), a árvore de eventos poderia necessitar de incluir múltiplos HFE's que são similares. Entretanto, a definição e/ou quantificação poderiam ser diferentes devido às possíveis diferenças no tempo, estado da planta, etc. A figura 4.9 mostra a árvore de eventos antes da incorporação da ATHEANA e a figura 4.10 ilustra uma possível maneira de incorporar o HFE da ATHEANA na árvore de eventos da APS. Nesta ilustração, a incorporação trata de falha humana em iniciar ou manter a função requerida até a obtenção do sucesso final. Neste caso, o HFE é representado pela inclusão de um ramo adicional específico na árvore de eventos, cujo insucesso pode levar, diretamente, a dano ao núcleo.

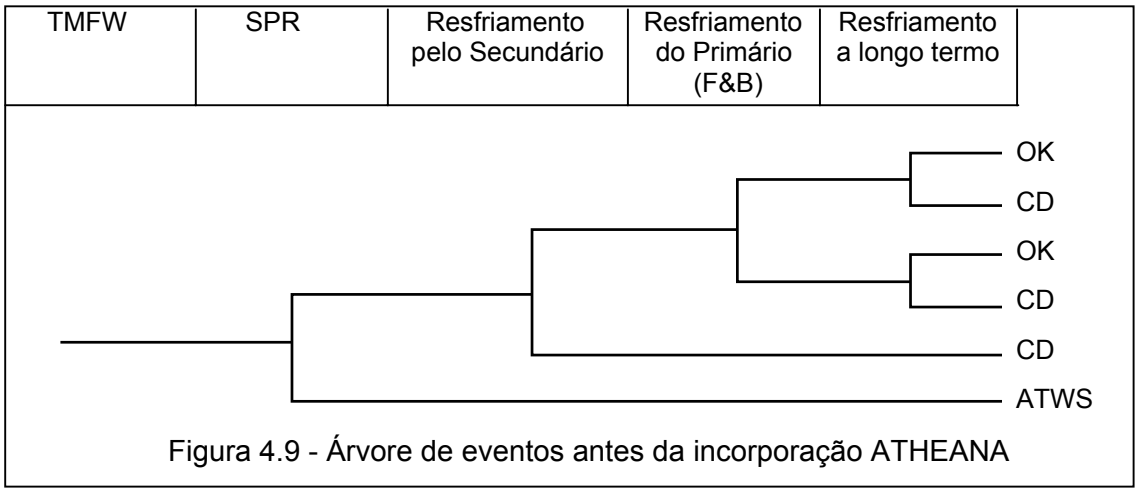


Figura 4.9 - Árvore de eventos antes da incorporação ATHEANA

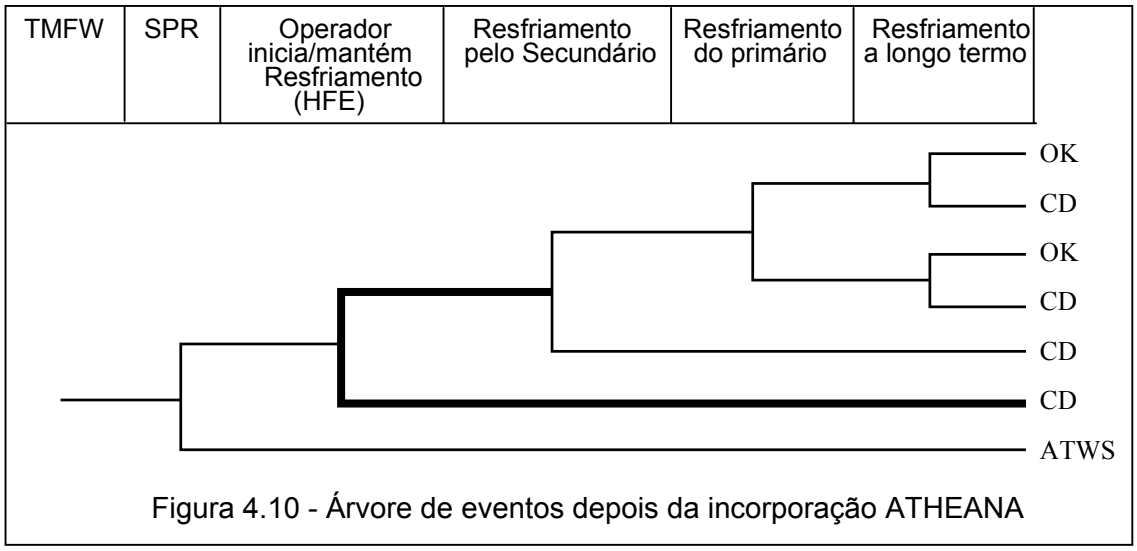


Figura 4.10 - Árvore de eventos depois da incorporação ATHEANA

Conceitualmente, a incorporação da metodologia ATHEANA na árvore de eventos poderá eliminar algumas das falhas funcionais ou de sistemas causadas por falha humana e modeladas como erro pós-iniciador, nas árvores de falhas das APS's. Isto ocorre porque os HFE's identificados pela ATHEANA incluirão, em seu escopo e definição, aqueles eventos (tipicamente, erros de omissão), correntemente, incluídos nas árvores de falhas. Entretanto, alguns HFE's pré-iniciadores e alguns HFE's pós-iniciadores, relacionados com equipamentos específicos poderão permanecer nas árvores de falhas.

Como o desenvolvimento da ATHEANA, até o momento, ainda não tratou de HFE pré-iniciadores, o escopo, definição e quantificação destes eventos na APS poderão ser diferentes. O desenvolvimento da ATHEANA, até o momento, tem se preocupado com larga faixa de eventos que levam diretamente a dano ao núcleo.

Igualmente, como nas árvores de falhas, alguns dos eventos de recuperação, normalmente, adicionados nas sequências de corte (cut set), após a solução e quantificação inicial da APS, podem ser eliminados quando os HFE's da ATHEANA forem, amplamente, definidos para incluir falhas em recuperação do erro original. Por

exemplo, a “falha em trocar para uma fonte alternativa de água” pode existir, como um evento de recuperação, em alguma sequência de corte que envolva perda de fonte primária de água. Entretanto, se um HFE, definido pela ATHEANA, for inserido no modelo, o qual envolve a “falha em assegurar um adequado suprimento de água (incluindo as considerações de troca para uma fonte alternativa, quando necessário)”, então, o evento de recuperação, originalmente, citado não será mais necessário, uma vez que a ampla definição do evento pela ATHEANA já incluirá esta falha de recuperação. Até a obtenção da solução inicial da ATHEANA, todas as possíveis considerações de recuperação podem não serem evidentes. Portanto, poderá haver, ainda, a necessidade de aplicar alguns dos eventos de recuperação como é feito atualmente.

O processo de incorporação do HFE’s da ATHEANA poderá reduzir o número total de diferentes HFE’s nas APS’s e o número de vezes que múltiplos HFE’s aparecem em uma mesma sequência de corte (devida a ampla definição dos HFE’s identificados pelo uso da ATHEANA). Entretanto, a eliminação total de múltiplos HFE’s na mesma sequência de corte pode não ser possível. Quando esta condição não acontece, deverá ser usada a mesma propriedade de dependências entre HFE’s na sequência de corte durante a quantificação da sequência final usando as técnicas atuais de HRA/APS.

CAPÍTULO 5

AVALIAÇÃO QUALITATIVA DA METODOLOGIA ATHEANA

5.1 Introdução

ATHEANA foi criada com a intenção de preencher uma lacuna ou limitação existente nos métodos atuais de ACH, que é analisar, mais realisticamente, o desempenho humano, mais precisamente, os erros de comissão, envolvidos nas ações de resposta a eventos sérios.

ATHEANA consolida os processos psicológicos básicos que influenciam o ser humano e que o forçam a realizar ações inadequadas, em um processo sistematizado para identificar estas condições e possibilitar a sua quantificação.

O relatório (ACRS Letter Reports, 1999) emitido pelo Advisory Committee on Reactor Safeguards, ACRS, (órgão da NRC que revê estudos específicos relativos à segurança e fornece assessoria independente para o processo de tomada de decisões de alto nível da NRC), da 468$^{a.}$ reunião do ACRS cita que no final da década de 1980 já era sentida a necessidade de um modelo de ACH de segunda geração que deveria pesquisar, profundamente, as causas do erro humano, uma vez que os métodos existentes não consideravam os conceitos das ciências comportamentais e cognitivas. O foco era no “erro humano”, com uma conotação de culpa. Neste sentido, a atenção foi direcionada para examinar os elementos do contexto que poderiam disparar mecanismos de erros cognitivos, os quais poderiam levar às ações inseguras. A ATHEANA é o primeiro trabalho realizado para desenvolver um modelo de desempenho humano baseado neste novo paradigma. FUJITA (1992), já comentava que as próximas gerações de ACH deveriam considerar conceitos psicológicos porque os engenheiros eram criticados pelos psicólogos, por tentarem tratar o ser humano como uma simples máquina ao invés de tentar identificar as causas psicológicas básicas dos erros.

Apesar de já terem transcorrido quase 9 anos desde sua primeira edição (COOPER *et al.*, 1996), a ATHEANA ainda apresenta deficiências que dificultam e, de uma certa maneira, impedem a sua aplicação em larga escala, como atualmente ocorre com os métodos de primeira geração, como por exemplo o THERP (SWAIN & GUTTMANN, 1983). Os próprios autores (ACRS Committee Meeting Transcripts, 2004) reconhecem que foram feitos poucos esforços para tornar a implementação da ATHEANA mais amigável, pois ela não é facilmente utilizada por pessoas não especializadas na metodologia. ATHEANA ainda não é uma metodologia completa, pois em determinados trechos de seu processo de pesquisas ou até mesmo no passo relacionado com a quantificação, ela utiliza ferramentas de outras metodologias existentes (HEART (WILLIAMS, 1988), SLIM (EMBREY *et al., 1984)* e THERP (SWAIN & GUTTMANN*, 1983)*). Esta "deficiência" foi criticada (NUREG-1624, Rev. 1, 2000) por especialistas que avaliaram a metodologia.

Todas estas deficiências são de conhecimento de seus autores e da própria NRC que, para auxiliar na utilização da metodologia, emitiram dois trabalhos (FORESTER *et al*., 2002, 2003), para servir de orientação suplementar para a quantificação, isto é, para a quantificação dos HFE's, EFC's e UA's. Mesmo com estas publicações, o processo de quantificação continua sendo largamente baseado na avaliação de especialistas de ACH, daí a dificuldade de que a mesma seja implantada como um método de uso geral.

Entretanto, assim como ocorreu com as metodologias de primeira geração, que levaram mais de 20 anos, desde os seus primeiros estudos nos anos de 1950/1960 (SWAIN, 1990), onde alguns cientistas e engenheiros viram a necessidade de, não somente identificar, mas também quantificar o potencial do erro humano, até a edição do THERP/Handbook (SWAIN & GUTTMANN, 1983), que é um método de ACH largamente aceito e utilizado e que solidificou o processo de ACH. A ATHEANA, assim como outros métodos de análise de confiabilidade humana de segunda geração, está

passando por um processo de maturação que começou no início dos anos 1990, mesmo antes de sua criação e levará alguns anos até atingir a maturidade necessária para a sua ampla utilização.

5.2 Vantagens e desvantagens da metodologia

É inegável a contribuição desta metodologia para o aperfeiçoamento da representatividade das análises probabilísticas de segurança, APS, uma vez que a mesma visa incluir nas APS's, a contribuição dos eventos de falha humana causados pelo chamado erro de comissão, EOC, para o risco total de dano ao núcleo, os quais não estão, atualmente, representados (portanto, a freqüência de dano ao núcleo das APS's atuais está subestimada pelo valor desta contribuição). Como será visto mais adiante (FUKUDA *et al.*, 2000), testes realizados com esta metodologia concluíram que esta contribuição representa um valor muito pequeno (da ordem de 4%), podendo, em certos casos ser, até, desprezada. Entretanto, como o processo de quantificação ainda não se apresenta totalmente definido como um método único, fazendo uso de outros métodos já consagrados e utilizados (como por exemplo, THERP (SWAIN & GUTTMANN, 1983), SLIM (EMBREY *et al.*, 1984), HEART (WILLIAMS, 1988)), e, principalmente, de julgamento do especialistas, o processo de quantificação poderá apresentar uma grande variação.

Porém, como dito anteriormente, no desenvolvimento da ATHEANA foi identificado que os benefícios desta metodologia não se restringia apenas às aplicações nas APS's (quantificação do risco). O seu bem estruturado processo de pesquisa dos eventos de falha humana, dos contextos que forçam ao erro e das ações inseguras, associados com os fatores psicológicos que influenciam o desempenho humano permite a identificação de deficiências de treinamento, procedimentos, comunicação e interface homem-máquina, o qual proporciona grandes melhorias nestas áreas resultando em melhorias significativas para a operação segura das

usinas nucleares. A análise retrospectiva utilizada, inicialmente, para a identificação dos contextos e das ações inseguras e para a formação de um banco de dados para serem utilizados nas análises prospectivas, também se tornou uma ferramenta útil na análise de causa-raiz e na identificação de ações corretivas mais efetivas de eventos envolvendo a participação humana.

Entretanto, por ser uma atividade multidisciplinar que envolve, necessariamente, a participação de especialistas de diversas áreas, como psicologia, fatores humanos, engenharia, APS, treinamento e operação de usinas, possui custos associados elevados. Além disto, existem outras deficiências que tornam o seu uso ainda em caráter experimental. Por não possuir um processo de quantificação único estabelecido, permite variações neste processo, como foi identificado por REER *et al.* (1999), o qual não concordou com a utilização do método HEART (WILLIAMS, 1988), pois os tipos de erros mencionados neste método não são compatíveis com a abordagem proposta pela ATHEANA (por exemplo, HEART não considera mecanismos de erros). REER *et al.* (1999) preferiu utilizar o método INTENT (GERTMAN *et al.,* 1992*)* por achar que este método possui características que melhor se adaptam ao comportamento observado na análise. DOUGHERTY (1998) também utilizou a metodologia INTENT (GERTMAN *et al.,* 1992*)* na sua avaliação, por ser mais representativa. O passo 9, de quantificação, como destacado no ACRS SubCommittee Meeting (1999) foi comentado ser "uma decepção" e de "não ser uma quantificação e sim, uma opinião numérica".

A aplicação do método gera, também, uma vasta documentação, a qual nem sempre é requerida para o evento sendo analisado. Portanto, um processo de filtragem (screening) de eventos poderia ser útil para ajudar na escolha dos processos de busca mais específicos.

É reconhecido (BLEY *et al.,* 1999) que, muitos dos aspectos da ATHEANA poderão ser melhorados pelo desenvolvimento de um sistema automatizado de

suporte ao usuário. O processo de pesquisa, o qual está sendo refinado, pode tornar-se menos trabalhoso e mais consistente se ele for guiado por um programa de computador interativo, com perguntas e um padrão de respostas pré-estabelecido, para guiar o usuário. A habilidade para relacionar o processo de pesquisa dos EFC's com um banco de dados de eventos reais poderia colocar esta pesquisa em um processo baseado em exemplos.

5.3 Testes de aplicação da metodologia

Desde a sua primeira edição, NUREG/CR-6350 (COOPER et al, 1996), até a revisão atual (NUREG-1624, Rev. 1, 2000), alguns estudiosos (STUTZKE & DOUGHERTY, 1996, DOUGHERTY, 1998, REER *et al.*, 1999, e FUKUDA *et al.*, 2000) realizaram testes de aplicação da metodologia, onde se depararam com variadas dificuldades, principalmente, na parte de quantificação da análise prospectiva. O próprio NUREG-1624, Rev.1 (2000), incorporou várias das sugestões e comentários feitos por 4 renomados e respeitados especialistas em ACH e APS (Dr. Eric Hollnagel, Dr. Pietro Carlo Cacciabue, Dr. Oliver Sträter e Mr. Stuart R. Lewis), especialmente, convidados para realizar uma análise (peer review) da metodologia, além de 20 outras pessoas interessadas em ACH.

Edward Dougherty, que é um crítico, muitas das vezes, exageradamente, severo, de assuntos relacionados com ACH, comentou a ATHEANA, em dois de seus diversos trabalhos publicados. No primeiro, em parceria com STUTZKE (1996) comentou a primeira versão da ATHEANA (NUREG-6350, 1996), onde concluiu que a mesma ainda era imatura e que não podia ser implementada naquela época. Aguardava por futuros trabalhos de melhorias nas orientações da implementação do método e de dados quantitativos de suporte, de maneira que os analistas de APS pudessem aplicar ATHEANA sem a necessidade de se basear, tão extensivamente, em especialistas de fatores humanos ou psicológicos. No segundo trabalho,

DOUGHERTY (1998), apresentou uma análise de um exercício de aplicação da ATHEANA, tendo como base a primeira versão da metodologia, publicada no NUREG/CR-6350 (COOPER *et al.,* 1996), em um evento real ocorrido na usina nuclear de Ft. Calhoun, USA, em 1985, onde, novamente, criticou duramente o processo de quantificação, afirmando que um cálculo de superior qualidade é possível, em relação ao apresentado, o qual é tão, obviamente, imperfeito, que prejudicou os autores, a NRC e, especialmente, a industria nuclear. Quanto ao processo de modelagem, DOUGHERTY (1998) sugere o modelo que HOLLNAGEL (1996) chamou de "confiabilidade cognitiva" e que os resultados da análise seriam mais significativos se houvesse uma análise do contexto global dos procedimentos de emergência, pessoal suplementar à equipe de sala de controle e outras redundâncias criadas após TMI-2. Concluiu que, enquanto isto não for feito, as análises de EOC, utilizando esta versão da ATHEANA, terão sempre um risco desprezível, como justamente os analistas de risco sempre assumiram ser o caso. Dougherty se referia mais exatamente em considerar possíveis ações de recuperação mais realistas em função do tempo disponível para tal, em vista do evento se desenrolar mais vagarosamente, e também de fatores de dependência entre as ações.

Outra aplicação da metodologia ATHEANA foi feita por especialistas do Institute of Nuclear Safety/Nuclear Power Engineering Corporation, Japão. FUKUDA *et al.* (2000), fizeram uma aplicação da ATHEANA (NUREG-1624, Rev.1, 2000) em um acidente de ruptura de tubos dos geradores de vapor. Apesar de não apresentar um trabalho com evidências suficientes para uma revisão mais detalhada (não existe informações suficientes para confirmação dos cálculos e não foram considerados os pontos de vista operacionais), as conclusões a que chegaram foram de que aplicação, segundo as orientações da ATHEANA, é possível, e que o aumento da freqüência de dano ao núcleo devido a erros de comissão, neste tipo de acidente, foi estimada ser 4% (estes valores deveriam ser confirmados, posteriormente, por uma nova aplicação

considerando fatores de operação). O aumento total da freqüência de danos ao núcleo, devido aos HFE's identificados na avaliação para este acidente, foi estimada ser 6,7E-9/ano (a freqüência de danos ao núcleo, sem considerar estes HFE's é de 1,6E-7/ano).

Outro debate sobre ATHEANA foi o trabalho apresentado por REER et al., (1999), que envolveu um estudo comparativo de cinco metodologias de segunda geração, na análise do acidente de perda de água de alimentação ocorrido na usina de Davis-Besse, USA, em 1985. Esta foi uma análise qualitativa comparativa das metodologias e não uma análise qualitativa de cada uma. Entretanto, foi ressaltado, em relação à ATHEANA, que ela apresenta algumas inconsistências sobre o uso da classificação do erro humano no processo de pesquisa e análise, alguns passos da pesquisa e quantificação apresentam dificuldades de execução devido à falta de clareza e há geração de muitos dados, mas é um método de alta utilidade. REER *et al.* (1999) também comenta que muitos dos detalhes coletados nas fases de pesquisa não serão utilizados na quantificação. Especialmente, os relacionados com recuperação e dependência parecem estar subrepresentados no processo de análise e quantificação. Porém, de maneira geral, a abordagem e os conceitos desenvolvidos pela metodologia ATHEANA estão adequados para o tratamento dos erros de comissão.

5.4 Estado atual da metodologia

Após terem se passados alguns anos (de 2000 a 2004) com poucos avanços (somente dois trabalhos emitidos pelos autores (FORESTER *et al.*, 2002, 2003)), a NRC (ACRS Committee Meeting Transcript, 2004) retomou o interesse pelas metodologias de segunda geração e emitiu um documento, em julho de 2004 (NUREG-1792, 2004), em versão preliminar para comentários, relativo à "Boas Práticas para a Implementação da Análise de Confiabilidade Humana, ACH", com a

finalidade de dar suporte para a avaliação probabilística de risco e a implementação do Regulatory Guide (RG) 1.200 (DRAFT REGULATORY GUIDE 1.200, 2004). O Regulatory Guide 1.200 descreve uma abordagem aceitável para determinar a adequabilidade técnica dos resultados das APS's para as atividades baseadas em informações de riscos. O NUREG-1792 (2004) é um documento de boas práticas de ACH, de natureza genérica e não está associado a nenhum método ou ferramenta específico que poderia ser empregado para realizar a ACH, uma vez que existem vários e todos eles possuem pontos fortes e limitações quanto ao seu uso e aplicabilidade. Este NUREG cita que, a sua elaboração foi baseada na experiência passada de execução de ACH (por exemplo, NUREG-1150, 1990), de revisão de ACH (por exemplo, nos IPEs, (NUREG-1560, 1996)) e nas lições aprendidas no desenvolvimento de métodos de ACH (por exemplo, THERP e ATHEANA). Como boa prática, a NRC entende que a atribuição de uma probabilidade de erro humano, isoladamente, não é mais uma boa prática. As interações das respostas dos equipamentos e dos operadores devem ser investigadas e modeladas, convenientemente, onde o contexto da seqüência do acidente é um processo complexo e de múltiplas facetas que pode afetar a definição do evento de falha humana, o qual deve ter a sua probabilidade estimada. Com as recomendações do NUREG-1792 (2004), que considera erros pré e pós-iniciador, a NRC, praticamente, inclui os critérios da ATHEANA como boas práticas, citando, claramente, onde aplicável, que a ATHEANA é um método aceitável (além de outros), porém sem requerer, diretamente, o seu uso.

Por outro lado, o NUREG-1792 (2004) declara, especificamente, que os erros de comissão estão além dos requisitos atuais da APS e não são, explicitamente, tratadas pelo Regulatory Guide 1.200. Entretanto, consistente com o estado da arte de ACH, recomenda que as futuras APS/ACH atentem para identificar e modelar, não somente os erros de omissão, como é feito, atualmente, mas, também, os erros de

comissão potenciais importantes. Neste sentido, o NUREG-1792 (2004) cita alguns métodos que podem ser utilizados, entre eles, a ATHEANA. Entretanto, destaca que, o uso do risco em qualquer atividade de avaliação deve, pelo menos, assegurar que as condições que favorecem uma provável ocorrência de EOC não existam. Neste sentido, o NUREG-1792 (2004) recomenda uma segunda boa prática que é a de identificar as condições que propiciam a ocorrência de EOC e tomar as medidas corretivas necessárias para a sua eliminação. Neste sentido, o NUREG-1792 (2004) oferece uma orientação, onde pode-se observar a forte influência da filosofia da ATHEANA. Entretanto, destaca que, discussões adicionais sobre situações que podem facilitar a ocorrências de EOC são fornecidas pela ATHEANA (NUREG-1624, Rev.1, 2000), CESA (REER *et al.,* 2004) e JULIUS *et al.* (1995). Conclui ressaltando que, se a primeira boa prática, a qual não é requerida pelo Regulatory Guide 1.200, não for tomada, permitirá que o risco total calculado seja otimista, por não considerar esta fonte adicional de risco (EOC). Entretanto, considera que os contextos que levam a EOC são relativamente raros, mas quando acontecem existe uma alta probabilidade que o EOC ocorrerá. Finalmente, recomenda, pelo menos, executar a segunda boa prática (se a primeira não for realizada), para pelo menos identificar, qualitativamente, aquelas condições da planta que podem levar os operadores a cometer erros de comissão e então, corrigí-las, se necessário.

Como dito, inicialmente, este NUREG-1792 (2004), de boas práticas para a implementação de ACH, está sob a forma preliminar para comentários. Porém, pode-se observar, claramente, que a quantificação dos EOCs ainda é uma dificuldade a ser corrigida e que o processo de pesquisa de cenários, embora trabalhoso, já pode ser considerado como adequado. Entretanto, tanto o processo de pesquisa quanto o de quantificação ainda necessitam de melhorias para a implantação generalizada da metodologia.

CAPÍTULO 6

CONCLUSÕES

A filosofia da ATHEANA marcou um importante avanço no aprimoramento da análise de confiabilidade humana ao considerar os contextos, nos quais os operadores estão inseridos, como possuidores de características que podem proporcionar a ocorrência da falha humana. A identificação e quantificação destes contextos e das ações inseguras que eles favorecem, permitem quantificar a probabilidade do evento de falha humana (erro de comissão) que será considerada para o cálculo do risco total de dano ao núcleo, realizado pela APS, permitindo, desta maneira, torná-la mais representativa das falhas humanas reais observada nos eventos importantes ocorridos, as quais não estão, presentemente contempladas.

ATHEANA não substitui os métodos tradicionais de ACH, os quais tratam dos erros de omissão e tem o seu uso garantido. ATHEANA é um método complementar que trata dos erros de comissão e foi criada para preencher esta lacuna.

A metodologia ATHEANA envolve uma associação de fatores físicos, relativos ao comportamento dos parâmetros e informações das condições da planta, com fatores psicológicos centrados no homem, que afetam a sua maneira de processar a informação.

Os benefícios obtidos de sua aplicação (retrospectiva e prospectiva), conforme descritos no NUREG-1624, Rev.1 (2000), são amplos e, indiscutivelmente, úteis e importantes para a segurança operacional. A sua total implementação, como prevista neste NUREG, certamente trará um nível maior de segurança na operação de usinas nucleares.

Entretanto, como visto, ela precisa de melhorias para corrigir algumas deficiências que dificultam a sua utilização, principalmente do processo de quantificação. Este, como já foi comentado por outros especialistas, necessita de um

processo mais formal (matemático). Embora orientações (FORESTER *et al.*, 2003) para quantificação baseada em julgamento de especialistas tenham sido emitidas, elas não contemplam satisfatoriamente esta necessidade porque sempre estará dependente de especialistas e nem sempre eles possuem as mesmas experiências com operação, ACH e APS. A exemplo de outros desenvolvimentos (como THERP (SWAIN & GUTTMANN, 1983) e ASEP (SWAIN, 1987)), é esperado que façam algumas simplificações na metodologia, com a finalidade de torná-la mais prática e corrigir, também, as demais deficiências observadas.

Apesar de alguns resultados preliminares indicarem uma pequena contribuição para o risco total (talvez pelo método ainda não estar totalmente aperfeiçoado), ela apresenta, sob o ponto de vista qualitativo, uma grande vantagem que é a identificação de fraquezas de treinamento e procedimentos, interface homem-máquina e possíveis modos de falhas e precursores de iniciadores, os quais devem ser corrigidos, segundo a 2ª. boa prática sugerida pelo NUREG-1792 (2004).

Esta metodologia não possui ainda requisitos regulatórios no seu país de origem (Estados Unidos). Até o momento foi emitido um documento, ainda em fase de comentários, sugerindo o uso das metodologias de segunda geração, onde se inclui a ATHEANA, mas sem a necessidade de quantificação pois o tipo de erro que ela aborda, erro de comissão, ainda não é requerido constar nas APS's. O desenvolvimento do estado da arte, provavelmente trará, em um futuro ainda indeterminado, esta quantificação. A aplicação da ATHEANA em outros países, por exemplo, no Brasil, dependerá ainda da sedimentação desta arte. Mas, como a exemplo de outros processos já implantados, como a Análise Probabilística de Segurança e a Regra de Manutenção, esta metodologia, se for reconhecida como importante para a segurança, certamente também será utilizada no Brasil.

Atualmente, a utilização desta metodologia nas usinas nucleares Angra 1 e Angra 2 da Central Nuclear Almirante Álvaro Alberto em Angra dos Reis, esbarra, além

das dificuldades inerentes à própria metodologia (que espera-se que sejam melhoradas) em algumas dificuldades estruturais locais.

As duas usinas são de tecnologias diferentes. Enquanto a usina de Angra-1 possui a maioria de suas funções de segurança controladas manualmente (exceto a partida inicial dos equipamentos em resposta ao evento iniciador) durante a evolução dos acidentes, Angra-2 possui uma grande automação, onde, nos primeiros 30 minutos após a ocorrência de um evento iniciador, não é requerida nenhuma ação manual do operador. A ATHEANA foi criada levando em consideração a tecnologia americana como é o caso de Angra 1. Para Angra 2 esta metodologia poderá ser aplicada para ações do operador de médio e longo prazo (após os 30 minutos), e necessitará, provavelmente, de adaptações e mudanças, mas sem desconsiderar o foco principal que é a pesquisa dos contextos que forçam ao erro. Existem outros métodos de segunda geração mais relacionados com usinas automatizadas, como por exemplo MERMOS (BIEDER *et al.*, 1998), desenvolvido na França. Portanto, superadas as dificuldades atuais, é perfeitamente viável a aplicação da metodologia ATHEANA em Angra-1, uma vez que esta já possui a sua própria APS, que é um dos requisitos básicos. A APS de Angra 1 utilizou os métodos THERP (SWAIN & GUTTMANN, 1983) e ASEP (SWAIN, 1987) de análise de confiabilidade humana. Acredita-se que um dos problemas seja o custo operacional do projeto. A relação custo/benefício deverá ser avaliada, adequadamente, uma vez que, para a sua total aplicação é necessário uma equipe multidisciplinar e uma infra-estrutura adequada, conforme descrito no NUREG-1624, Rev.1 (2000). Como é sabido, Angra-1 não tem simulador e nem instrutores de simulador, pois este treinamento é feito no exterior. A ausência destes dois requisitos introduz uma certa deficiência na configuração da equipe e no planejamento e verificação dos cenários, altamente, importantes. Entretanto, alguns dos diversos aspectos da metodologia poderão ser aplicados mais facilmente, como é o caso da análise retrospectiva e da identificação de contextos

propensos ao erro humano, conforme sugerido pela 2ª. boa prática do NUREG-1792 (2004).

A emissão do NUREG-1792 (2004), embora, ainda em fase preliminar, em cuja estrutura pode-se constatar a essência da metodologia ATHEANA, marcou o início de uma nova era para a análise de confiabilidade humana, onde o contexto, associado com fatores centrados no homem, passou a ser considerado de importância significativa nas prováveis ações do operador que poderão causar um evento de falha humana. O mesmo processo, lento, porém gradual, ocorreu com outros desenvolvimentos da arte, como por exemplo, com a própria Análise Probabilística de Segurança (GENERIC LETTER 88-20, 1988), no final da década de 1980, e a Regra de Manutenção (REGULATORY GUIDE 1.160, 1995), na década de 1990.

Com a implantação deste novo marco (NUREG-1792, 2004) relativo à utilização de metodologias de segunda geração, é esperado que novas orientações e melhorias sejam emitidas para permitir o seu uso geral e irrestrito.

Espera-se que desenvolvimento total e a sedimentação definitiva desta metodologia não leve os mesmos 20 anos (aproximadamente) como ocorreu com as metodologias de primeira geração e que, também não seja impulsionada por uma falha catastrófica, tipo TMI-2 ou Chernobyl, mas sim pelo bom senso e cultura de segurança que devem prevalecer tendo em vista a segurança requerida na operação de usinas nucleares.

REFERÊNCIAS

ACRS Committee Meeting Transcript, 2004, "512th ACRS Meeting, Good Practices for Implementing Human Reliability Analysis", May 06, 2004, US Nuclear Regulatory Commission, Washington, DC.

ACRS Letter Reports, 1999, Advisory Committee on Reactor Safeguards, Letter to Dr. William D. Travers, Executive Director for Operation, U.S. Nuclear Regulatory Commission, "NUREG-1624, Rev. 1, Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA)", December 15, 1999.

ACRS Letter Reports, 2004, Advisory Committee on Reactor Safeguards, Letter to Dr. William D. Travers, Executive Director for Operation, U.S. Nuclear Regulatory Commission, "Good Practices for Implementation Human Reliability Analysis", May 13, 2004.

AEOD/E95-01, 1995, *Engineering Evaluation - Operating Events with Inappropriate Bypass or Defeat of Engineered Safety Features,* Office of Analysis and Evaluation of Operational Data (AEOD), Nuclear Regulatory Commission, Washington, DC, July.

BEARE, A. N., GADDY, C. D., PARRY, G. W., SINGH, A.J., 1991, "An Approach for Assessment of the Reliability of Cognitive Response for Nuclear Power Plant Operating Crews," in G. Apostolakis (ed.) *Probabilistic Safety Assessment & Management (PSAM),* Elsevier Science, New York.

BELLO, G.C., & COLOMBARI, V., 1980, Empirical technique to estimate operator's errors (TESEO), *Reliability Engineering,* 1980, 1, 3.

BIEDER, C., LE-BOT, P., DESMARES, E., Bonnet, J. L., Cara, F., 1998, "MERMOS: EDF's new advanced HRA method". In: *Probabilistic Safety Assessment and Management (PSAM 4)*, A. Mosleh and R.A.Bari (eds), Springer-Verlag, New York.

BLEY, D., COOPER, S, WREATHAL, J., *et al.* 1999, Report (Conference), Philosophy of ATHEANA, *International Workshop on Human Reliability Models,* Seattle, WA, USA, Sep.

BUDNITZ, R.J., APOSTOLAKIS, G., BOORE, D. M., COPPERSMITH, K. J., CORNELL, C. A., MORRIS, P. A., 1997, *Recommendation for Probabilistic Seismic Hazard Analysis Guidance on Uncertainty and Use of Experts,* NUREG/CR-6372, Lawrence Livermore National Laboratory, Livermore, CA. April.

CACCIABUE, P.C., COJAZZI, and PARISI, P., 1996, "A dynamic HRA method based on a taxonomy and a cognitive simulation model, in Probabilistic Safety Assessment and Management", P.C.Cacciabue and I.A. Papazogou (eds.):Springer-Verlag, London.

COLAS, A., 1997, “The Human Factor in the Nuclear Industry”. In: *Human Performance in Operational Events - Specialists Meeting Proceedings*, pp. 21-26, AIEA, NEA, OECD, Chattanooga, Tennessee, USA, October.

COMER, M. K., SEAVER, D. A., STILWELL, W. G., & GADDY, C. D., 1984, *Generating Human Reliability Estimates Using Expert Judgment: Paired Comparisons and Direct Numerical Estimation (Vol.1).* NUREG/CR-3688. Washington, D.C.: U.S. Nuclear Regulatory Commission.

COOPER, S. E., LUCKAS, W. J., WREATHALL, J., 1995, *Human-System Event Classification Scheme (HSECS) Data Base*, BNL TECHNICAL REPORT NO. L-2415/95-1, Brookhaven National Laboratory, Dublin, OH, December 21.

COOPER, S. E., RAMEY-SMITH, A., WREATHAL, J., PARRY, G.W, BLEY, D.C., TAYLOR, J. H., LUCKAS, W. J., 1996, *A Technique for Human Error Analysis (ATHEANA),* NUREG/CR-6350, Brookhaven National Laboratory, Upton, NY, April.

DOUGHERTY, E., 1998, Human errors of commission revisited: an evaluation of the ATHEANA approach, *Reliability Engineering and System Safety,* v. 60, pp. 71-82.

DRAFT REGULATORY GUIDE 1.200, 2004, *An Approach for Determining The Technical Adequacy of Probabilistic Risk Assessment Results For Risk-Informed Activities.* U.S. Nuclear Regulatory Commission, Washington, DC, February.

ELLIS K. R., 1992, *An Introduction to Hazard and Operability Studies: The Guide Word Approach,* Chemetics International Co. Ltd., October.

EMBREY, D. E., HUMPHREYS, P. C., ROSA, E. A., KIRWAN, B., & REA, K., 1984, SLIM-MAUD: *An Approach to Assessing Human Error Probabilities Using Structured Expert Judgment,* NUREG/CR-3518, Upton, N.Y.: Brookhaven National Laboratory.

EMBREY, D. E., LUCAS, D. A., 1989, Personal Communication.

EMBREY, D. E., 1994a, *Guidelines for Preventing Human Error in Process Safety.* Center for Chemical Process Safety of the American Institute of Chemical Engineers, CCPS/AICHE, New York.

EMBREY, D. E., 1994b, *Software Guides for Human Reliability Quantification,* Human Reliability Associates Ltd., 1, School House, Higher Land, Dalton, Wigan, Lancs, England.

EPRI TR-100259, 1992, *An Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment.* June.

FORESTER, J., BLEY, D., COOPER, S., SIU, N., WREATHAL, J., 2002, Current Status of the ATHEANA Quantification Process and Data Needs, OECD/NEA Working Group WG-Risk Assessment, *Building the New HRA: Strengthening the Link between Experience and HRA ,* Munich, Germany, January.

FORESTER, J., BLEY, D., COOPER, S., LOIS, E., SIU, N., KOLACZKOWSKI, A., WREATHALL, J., 2003, Expert elicitation approach for performing ATHENA quantification, *Reliability Engineering and System Safety,* v. 83, pp. 207-220.

FUJITA, Y., 1992, Human reliability analysis: a human point of view*, Reliability Engineering and System Safety,* v. 38, pp. 71-79*.*

FUKUDA, M., UCHIDA, T., HIRANO, M., 2000, Trial Application of ATHEANA to SGTR in Level 1 PSA for a Japanese PWR, *PSAM 5, International Conference on Probabilistic Safety Assessment and Management,* Osaka (Japan), 27 Nov-1 Dec 2000, pp. 1535-1540.

GENERIC LETTER 88-20, 1988, "Individual Plant Examination for Severe Accident Vulnerabilities – 10CFR$50.54(f)", U.S. Nuclear Regulatory Commission, Washington, DC, November 23.

GERTMAN, D. I., BLACKMAN, H. S., HANEY, L. N., SEIDLER, K. S., & HAHN, H. A., 1992, "INTENT: a method for estimating human error probabilities for decision-based errors", *Reliability Engineering & System Safety,* v. 35, pp. 127-136.

HANNAMAN, G. W., SPURGIN, A. J. & LUKIC, Y. D., 1984a, *Human Cognitive Reliability Model for PRA Analysis.* NUS-4531, Palo Alto, Calif.: Electric Power Research Institute.

HANNAMAN, G. W., SPURGIN, A.J., & LUKIC, Y. D. 1984b, Systematic Human Action Reliability Procedures (SHARP). Palo Alto, Calif.: Electric Power Research Institute, EPRI NP-3583.

HOLLNAGEL, E., 1988, *Cognitive Reliability and Error Analysis Method (CREAM).* York: Elsevier Science, New York.

HOLLNAGEL, E., 1993, Reliability of Cognition: Foundations of Human Reliability Analysis, Plenum Press, New York.

HOLLNAGEL, E., 1996, Reliability analysis and operator modeling. *Reliability Engineering & System Safety,* v. 52, pp. 327-337.

IAEA-TECDOC-592, 1991, *Case study on the use of PSA methods: human reliability analysis,* International Atomic Energy Agency: Wagramerstrasse, Vienna, Austria, April.

JULIUS, J., JORGENSON, E., PARRY, G. W., and MOSLEH, A. M., 1995, "A Procedure for the Analysis of Error of Commission in a Probabilistic Safety Assessment of a Nuclear Power Plant at Full Power," *Reliability Engineering and System Safety,* v. 50, pp. 189-201.

KIRWAN, B.,1990, Human Reliability Assessment, In J. R. Wilson & E. N. Corlett (Eds.)., 1990, *Evaluation of Human Work, a Practical Ergonomics Methodology*. Washington, DC: Taylor and Francis.

KLETZ, T., 2001, *Learning from Accidents*. Gulf Professional Publishing, Oxford, UK.

KNOWLTON, R. E, 1992, *An Introduction to Hazard and Operability Studies: The Guide Word Approach,* Chemetics International, October.

MUMAW, R. J. & ROTH, E. M., 1992, How to be more devious with a training simulator: Redefining scenarios to emphasize cognitively difficult situations. *Simulation Multi-Conference: Nuclear Power Plant Simulation and Simulators.* Orlando, FL, April 6-9.

MUNGER et al., 1962 *An Index of Electronic Equipment Operability: Data Store.* Report AIR-C43-1/62-RP(1), Pittsburgh PA: American Institute for Research.

NUREG/CR-3010, 1982, *Post-Event Human Decision Errors: Operator Action Tree/Time Reliability Correlation,* Washington, D.C.: U.S. Nuclear Regulatory Commission.

NUREG/CR-6093, 1994, *An Analysis of Operational Experience During LP&S, and A Plan for Addressing Human Reliability Assessment Issues*, Brookhaven National Laboratory, and Sandia National Laboratories, Albuquerque, NM, Upton, NY. June.

NUREG/CR-6208, 1994, *An Empirical Investigation of Operator Performance in Cognitively Demanding Simulate Emergencies,* Westinghouse Science and Technology Center, July.

NUREG/CR-6265, 1995*, Multidisciplinary Framework for Human Reliability Analysis with an Application to Errors of Commission and Dependencies*. U.S Nuclear Regulatory Commission, Washington, DC.

NUREG/CR-6823, 2003, *Handbook of Parameter Estimation for Probabilistic Risk Assessment*, US-Nuclear Regulatory Commission, Washington, DC, September.

NUREG-75/014, 1975, *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400.* U. S. Nuclear Regulatory Commission, Washington, DC, October.

NUREG-1150, Vol. 2, 1990, *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants,* U.S. Nuclear Regulatory Commission, Washington, DC, December.

NUREG-1275, Vol. 8, 1992, *Operating Experience Feedback Report – Human Performance in Operating Events,* U.S. Nuclear Regulatory Commission, Washington, DC, December.

NUREG-1560, 1996, *Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance,* U.S. Nuclear Regulatory Commission, Washington, DC, October.

NUREG-1624, Rev. 1, 2000, *Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA)*, U.S. Nuclear Regulatory Commission, Washington, DC.

NUREG-1792, 2004, Draft Report for Comments, Good Practices for Implementing Human Reliability Analysis (HRA), U.S. Nuclear Regulatory Commission, Washington, DC, July.

OCONEE, P.R.A., 1984, *A Probabilistic Risk Assessment of Oconee Unit 3.* NSAC/60. Palo Alto, Calif.: Nuclear Safety Analysis Center, Electric Power Research Institute.

OTWAY, H., WINTERFELDT, von O., 1992, "Expert judgment in risk analysis and management: Process, context and pitfalls. "*Risk Analysis,* pp. 12(1).

PEROTTY, J. W., and WOODS, D. D., 1997, *A Cognitive Analysis of Anomaly Response in Space Shuttle Mission Control. Cognitive Systems Engineering Laboratory (CSEL),* CSEL 97-TR-02, The Ohio State University, Columbus OH, March, Prepared for NASA Johnson Space Center.

PHILLIP, L.D., EMBREY, D.E., HUMPHREYS, P., & SELBY, D.L., 1990. A Sociotechnical Approach to Assessing Human Reliability. In R.M. Olivier & J.A. Smith (Eds.), *Influence Diagrams, Belief Nets and Decision Making: Their Influence on Safety and Reliability,* New York: Wiley.

PICKARD, LOWE & GARRICK, INC., 1983, *Seabrook Station Probabilistic Safety Assessment,* PLG-0300, Newport Beach, CA: Pickard, Lowe & Garrick.

PONTECORVO, A. B., 1965, A Method of Prediction of Human Reliability. *Annals of Reliability and Maintenance* 4, 337-342.

POTASH, L.M., STEWART, M., DEITZ, P.E., LEWIS, D.M., & DOUGHERTY, E.M., 1981, Experience in integrating the operator contributions in the PRA of actual operating plants. In: *Proceedings of the ANS/ENS Topical Meeting on Probabilistic Risk Assessment,* Port Chester, New York, La Grange Park, III: American Nuclear Society.

PRA-COURSE, P-107, 1997, *"PRA for Technical Managers P*-107". NRC Technical Training Center, Chattanooga, TN, US-Nuclear Regulatory Commission, Chattanooga, TN, February 1997.

REASON, J.T., 1990, *Human Error,* Cambridge University Press, New York.

REER, B., STRÄTER, O., DANG, V. N., HIRSCHBERG, S., 1999, A Comparative Evaluation of Emerging Methods for Errors of Commission Based on Application to the Davis-Besse (1985) Event, Paul Scherrer Institut & GRS, Nuclear Energy and Safety, PSI Bericht Nr. 99-11, December.

REER, B., DANG, V. N., and HIRSCHBERG, S., 2004, "The CESA Method and Its Application in a Plant-Specific Pilot Study on Errors of Commissions," *Reliability Engineering and System Safety,* v. 83, pp. 187-205.

REGULATORY GUIDE 1.160, 1995, "Monitoring the Effectiveness of Maintenance at Nuclear Power Plants", U.S. Nuclear Regulatory Commission, Washington, DC.

SEAVER, D., STILLWELL, W. G, 1983, *Procedure for Using Expert Judgment to Estimate HEPs in Nuclear Power Plant Operations.* NUREG/CR-2743, Idaho National Engineering Laboratory, Idaho Falls, ID.

SENDERS, J. W., MORAY, N., & SMILEY, A. 1985, *Modeling Operator Cognitive Interactions in Nuclear Power Plant Safety Evaluation,* Report prepared for the Atomic Energy Control Board, Ottawa, Canada.

STRÄTER, O., and BUBB, H., 1998, "Assessment of human reliability based on evaluation of plant experience: requirements and implementation". *Reliability Engineering and System Safety,* 63:199-219.

STUTZKE, M. A., DOUGHERTY, E. M., 1996, Finding the Dominant Risk: A Review of the ATHEANA Method, *Human Factors and Reliability Analysis*, v. 75, pp.86-88.

SWAIN, A. D. & GUTTMANN, H. E., 1983, *Handbook of Human Reliability with Emphasis on Nuclear Power Plant Applications Final Report*, NUREG/CR-1278, Rev. 1, US-Nuclear Regulatory Commission, Washington, DC, August.

SWAIN, A. D.,1987, *Accident Sequence Evaluation Program Human Reliability Analysis Procedure,* NUREG/CR-4772, US-Nuclear Regulatory Commission, Washington, DC, February.

SWAIN, A. D., & WESTON, L. M., 1988, An approach to the diagnosis and misdiagnosis of abnormal conditions in post-accident sequences in complex man-machine systems. In: L.Goodstein, H.Andersen & S.Olsen (Eds.), *Tasks, Errors and Mental Models,* London: Taylor & Francis.

SWAIN, A.D., 1990, Human Reliability Analysis: Need, Status, Trends and Limitations, *Reliability Engineering and System Safety,* v. 29, pp. 301-313.

WILLIAMS, J. C., 1988, A Data-based Method for Assessing and Reducing Human Error to Improve Operational Performance, Paper presented at 1988 IEEE Fourth Conference on Human Factors and Power Plants, IEEE.

WOODS, D. D., 1982, *Operator Decision Behavior during the Steam Generator Tube Rupture at the Ginna Nuclear Power Stations,* Research Report 82-1C57-CONRM-OR2. Pittsburgh, Penn.: Westinghouse R & D Center.

WOODS, D. D., JOHANNESEN, L. J., COOK, R.I., and SARTER, N.B., 1994, *Behind Human Error: Cognitive Systems, Computers, and Hindsight,* Crew System Ergonomics Information Analysis Center (CSERIAC), Ohio State University, Wright-Paterson Air Force Base, Columbus, OH, December.

WREATHALL, J., 1982, *Operator Action Trees: An Approach to Quantifying Operator Error Probability During Accident Sequences,* NUS-4159, Gaithersburg, Md: NUS Corporation.

GLOSSÁRIO

Ações inseguras (UA)	(unsafe actions) – são ações, indevidamente, tomadas, ou não tomadas quando necessário, pelo pessoal da planta, que resultam em uma condição de segurança degradada.
Análise probabilística de segurança (APS)	A APS de uma planta é um processo analítico que quantifica o risco potencial, associado com o projeto, operação e manutenção da planta, para a saúde e segurança do público.
Árvore de eventos	Uma rede lógica que pode ser quantificável que inicia com um acidente ou evento iniciador e progride através de uma série de ramos que representam possíveis desempenhos de sistemas, ações humanas ou fenômenos que podem levar a um estado seguro ou estável ou um estado indesejável, tais como danos ao núcleo ou falha da contenção.
Árvore de falhas	Uma representação gráfica que mostra a relação lógica entre falhas; fornece uma descrição concisa e ordenada de várias combinações de possíveis eventos de falhas dentro de um sistema, os quais podem resultar em algum evento predefinido e indesejável de um sistema.
Atividades cognitivas	É o processo mental do operador associado com (1) avaliação da situação, (2) monitoração e deteção, (3) planejamento da resposta e (4) implementação da resposta.
Condições da planta	É a condição da planta definida pela combinação de suas propriedades físicas e condições dos equipamentos, incluindo a medida de parâmetros operacionais.
Contexto que força ao erro (EFC)	(EFC- error forcing context) - é a situação que aparece quando uma particular combinação de PSF's e condições da planta criam um ambiente no qual as ações inseguras são mais prováveis de ocorrerem.
Erro humano	Para a comunidade da APS, o termo "erro humano" tem sido, frequentemente, usado para se referir às falhas de sistemas ou equipamentos causadas pelo homem. Entretanto, em ciências comportamentais, este termo é usado, frequentemente, para descrever as falhas psicológicas básicas que podem causar a ação humana que leva à falha dos equipamentos. Portanto, em ATHEANA, o termo "erro humano" é usado, somente, de uma maneira muito geral, com os termos evento de falha humana, ação insegura e mecanismos de erros sendo usados para descrever aspectos mais específicos de erro humano.

Erros de comissão Um evento de falha humana resultante de uma ação insegura que, quando tomada, leva à uma mudança na configuração da planta com a conseqüência de uma degradação do estado da planta. Por exemplo, desligamento de bombas de injeção de segurança que estão funcionando, fechamento de válvulas e bloqueio de sinais e ações automáticas.

Quando é feita uma ação que não deveria ter sido feita. (slip, lapse,mistake). As consequências da ação são piores do que se não tivesse tomado ação alguma.

Erros de omissão Um evento de falha humana resultante da falha em realizar uma ação requerida e que leva a uma mudança, ou não, inadequada, da configuração da planta, com a conseqüência de uma degradação do estado da planta. Exemplos incluem a falha em iniciar um equipamento requerido, ou bloquear o sinal para despressurização automática.

Quando não é feita a ação pretendida ou planejada.(slip, lapse)

Evento de falha humana (HFE) Evento de falha humana (human failure event)- evento básico que é modelado nos modelos lógicos de APS (árvore de eventos e árvore de falhas) e que representa a falha de uma função, sistema ou componente o qual é o resultado de uma ou mais ações inseguras.

Evento iniciador São eventos iniciadores que podem desafiar os sistemas e componentes da planta.

Falha ativa É uma ação intencional ou não intencional que tem uma conseqüência negativa imediata para o sistema.

Falha latente Uma ação ou decisão errada cujas conseqüências somente se tornarão aparentes após um certo período de tempo quando outras condições ou eventos combinarem com o erro original para produzir uma conseqüência negativa para o sistema.

Fatores cognitivos Fatores cognitivos que afetam a qualidade das respostas das principais atividades cognitivas e assim, afetando o desempenho dos operadores. As três classes de fatores cognitivos são conhecimento, recursos de processamento e fatores estratégicos. Erros aparecem quando existe uma diferença entre o estado destes fatores cognitivos e as demandas impostas pela situação.

Fatores que formatam o desempenho (PSF) (performance shaping factors) - É um conjunto de influências no desempenho de uma equipe de operadores, resultante das características da planta, da equipe e de cada operador relacionadas com o homem. Estas características incluem procedimento, treinamento e aspectos de fatores humanos dos dispositivos de indicação e controle da planta.

Feedback (retorno)	É a informação de retorno do resultado de uma ação ou comando realizado.
Fixation error (Erro de fixação)	É a falha em revisar, adequadamente, a avaliação da situação quando chegar nova informação.
Heurísticos	Pertence ou é relacionado com uma formulação, usualmente, especulativa que serve como um guia para investigação ou solução de um problema.
Influência da freqüência (Frequency bias)	Eventos que ocorrem freqüentemente são mais fáceis de lembrar do que os que ocorrem raramente. Isto pode levar as pessoas de ter a tendência de interpretar informações recebidas sobre um evento em termos dos eventos que ocorrem freqüentemente ao invés dos eventos improváveis ou que ocorrem raramente.
Influência devido à similaridade (Similarity bias)	Os operadores são influenciados em lembrar de eventos que tem características (mesmo superficialmente) similares ao cenário, particularmente, se o evento lembra um evento "clássico" usado no treinamento ou discutido, intensivamente, entre os operadores.
Influências para a confirmação (Confirmation bias)	É a tendência que os indivíduos tem de procurar ou interpretar as indicações de maneira que confirmem suas expectativas. O resultado pode ser uma falha em revisar, adequadamente, opiniões e interpretações quando surgirem informações novas e conflitantes.
Influências por fatos recentes (Recency bias)	Eventos que aconteceram recentemente são lembrados mais facilmente do que eventos que ocorreram há muito tempo atrás. Na tentativa de entender as informações que estão chegando sobre um evento, as pessoas tendem a interpretar estas informações em termos dos eventos que ocorreram mais recentemente, ao invés de eventos importantes que ocorreram em um passado mais distante.
Lapse (lapso)	Erro causado pelo esquecimento do operador em tomar a ação requerida ou planejada.
Mecanismo de erro	É um mecanismo psicológico que pode causar uma determinada ação insegura e é disparada por uma combinação particular de fatores que formatam o desempenho, PSF, e as condições da planta. Mecanismos de erros não são, frequentemente, comportamentos ruins, mas representam mecanismos pelos quais as pessoas frequentemente executam, eficientemente, trabalhos com habilidade. Entretanto, em contextos errados, estes mecanismos podem levar a uma ação humana inadequada que causa consequências contra a segurança.
Mismatch (não igual)	É quando existe uma diferença na comparação entre parâmetros ou formulações.

Mistake (engano)	São erros originados no processamento cognitivo de mais alta ordem, envolvendo o julgamento de uma informação, estabelecendo um objetivo e decidindo como executá-lo. Neste tipo de erro, a ação do operador foi como planejada mas os planos eram inadequados para atingir as condições seguras requeridas.
Modelo de APS	É um modelo lógico que consiste, geralmente, de árvores de eventos, árvores de falhas e outras ferramentas analíticas e é construído para identificar cenários que levam à condições inaceitáveis da planta, tais como danos ao núcleo. O modelo é usado para estimar as frequências dos cenários pela conversão do modelo lógico em modelo de probabilidades. Para atingir este fim, estimativas devem ser obtidas para a probabilidade de cada evento do modelo, incluindo HFE's.
Modelo do processamento da informação	É uma descrição geral das atividades humanas cognitivas requeridas para responder, as condições anormais ou de acidentes. O modelo usado em ATHEANA considera ações em responder à anormalidades e que envolvem quatro passos: (1) monitoração/deteção, (2) avaliação da situação, (3) planejamento da resposta e (4) implementação da resposta.
Modelo mental	É a representação mental que integra o entendimento humano de como os sistemas e a planta trabalham. O modelo mental permite às pessoas simular, mentalmente, o desempenho da planta e dos sistemas, para prever ou antecipar o comportamento da planta e dos equipamentos.
Regras	Regras são orientações que os operadores seguem para realizar as suas atividades, na planta. Regras podem ser formais ou informais. Regras formais são instruções ou requisitos escritos específicos, para os operadores, e autorizados para uso pelo gerente da planta. Fontes de regras informais incluem programas de treinamento, discussões entre os operadores, experiência e práticas passadas.
Slip (deslize)	Erro devido ao operador realizar uma ação errada, indevidamente, em desacordo com a ação pretendida ou planejada.
Violation (violação)	Uma violação ocorre quando uma ação intencional é feita, a qual, deliberadamente, ignora qualquer regra operacional conhecida, restrições ou procedimentos. Esta definição exclui aquelas ações que são tomadas, deliberadamente, com a intenção de danificar sistemas, as quais são classificadas como sabotagem.
Visão de túnel	É a tendência que as pessoas tem em se concentrar, somente, nas informações que são relacionadas com suas hipóteses, negligenciando outras informações importantes.

ANEXO A

EVENTOS OPERACIONAIS IMPORTANTES

A.1 Introdução

O estudo (AEOD/E95-01, 1995) da NRC, denominado Engineering Evaluation – Operating Events with Inappropriate Bypass or Defeat of Engineered Safety Features, foi realizado por considerar que um adequado controle dos sistemas de segurança é um elemento essencial para manter a segurança do reator, conforme foi evidenciado pelos acidentes de TMI e de Chernobyl e que, a experiência operacional e a literatura sobre erros humanos tem mostrado que a recuperação dos sistemas de segurança, isolados indevidamente, nem sempre será realizada com sucesso.

O estudo, que originou o relatório, analisou os eventos operacionais ocorridos no período de dezembro de 1991 a maio de 1995. Este estudo identificou vários eventos onde os operadores anularam ou bloquearam, indevidamente, as atuações automáticas dos dispositivos de engenharia relacionados a segurança (ESF, Engineered Safety Features, que são sistemas de segurança destinados a prevenir ou mitigar as consequências de acidentes) e concluiu que a intervenção humana pode ser um importante modo de falha e que, estes eventos, apesar de não terem causado conseqüências mais sérias para a segurança, são considerados como precursores de eventos sérios.

Dos eventos analisados, quatorze foram relacionados com o cancelamento ou bloqueio da operação automática dos dispositivos de engenharia relacionados a segurança. Quatro deles se destacam como dignos de nota. Em dois eventos (Crystal River Unit 3 e South Texas Project Unit 2), a injeção de segurança foi desviada ou cancelada, indevidamente, pelos operadores. Os demais estão mais relacionados com

violações dos requisitos das especificações técnicas causadas, principalmente, por deficiências de procedimentos ou de treinamento.

As descrições a seguir, baseadas no relatório AEOD/E95-01 (1995), visam destacar, especificamente, as ações inadequadas tomadas durante os eventos. As mesmas não se propõem a fazer uma completa descrição dos mesmos, sob o ponto de vista operacional.

A.2 Revisão dos principais eventos operacionais

A.2.1 Crystal River Unit 3

Sumário do evento:

Durante um evento, onde ocorreu uma despressurização não identificada do circuito primário, um operador bloqueou a atuação dos dispositivos de segurança, sem orientação direta dos procedimentos e contrária aos requisitos das Especificações Técnicas; o operador licenciado agiu sem orientação de seu supervisor e não informou ao restante da equipe de operação, que tinha bloqueado tais sistemas. Este fato atrasou, consideravelmente, a normalização dos sistemas.

Descrição do evento:

Em 8 de dezembro de 1991, durante a partida da unidade, quando o reator estava a 10% de potência e preparando para rolar a turbina, ocorreu uma pequena despressurização do sistema primário, a qual foi, imediatamente, sentida pelos operadores. Uma válvula de spray do pressurizador falhou aberta apesar de sua indicação mostrá-la fechada. Os operadores não identificaram este fato, de imediato, desconhecendo as razões da queda de pressão até cerca de uma hora após, quando a válvula de isolamento da válvula de spray foi fechada. O reator desarmou por baixa pressão e, como a queda de pressão não parou, um membro da equipe isolou a atuação automática de vários sistemas de segurança (injeção de segurança de alta-

pressão, água de alimentação de emergência, geradores diesel de emergência) por cerca de 6 minutos. Durante 16 segundos ocorreu demanda real do sistema de injeção de segurança sem ocorrer a sua operação. Após o fechamento da válvula de isolamento da válvula de spray foi possível readquirir o controle manual da pressão.

O operador fez este isolamento antes da identificação da causa da queda da pressão. Esta ação não foi orientada por procedimentos e nem pelo supervisor dos operadores, que desconheceu este fato por vários minutos. Os sistemas, somente, foram colocados em modo automático quando outro supervisor, alheio à equipe que estava em serviço, identificou os alarmes provenientes deste isolamento.

Apesar de haver procedimentos de emergência que orientavam o fechamento da válvula de isolamento, este não foi seguido porque não tinha ocorrido nenhuma operação automática dos sistemas de segurança, a qual dirigiria para esta ação (esta atuação foi bloqueada na fase inicial do evento).

A.2.2 South Texas Project Unit 2

Sumário do evento:

Um sistema de segurança teve sua operação automática bloqueada, contrariando os requisitos das especificações técnicas; a operação de outro sistema de segurança não foi reiniciada apesar de recomendada por um procedimento de emergência; e um sistema de segurança, indevidamente, bloqueado, não foi prontamente recuperado.

Descrição do evento:

Em 24 de dezembro de 1991, uma falha mecânica no dispositivo de movimentação de uma válvula de spray causou, indevidamente, a sua abertura. Rapidamente, a pressão do sistema primário diminuiu causando o desligamento automático do reator por baixa pressão, acompanhado por injeção de segurança e isolamento da contenção. Com o isolamento da contenção, ocorreu a interrupção de ar

de instrumento utilizado para abertura da válvula, o que permitiu o seu fechamento automático (falha fechada), situação que era requerida pelas condições atuais da planta. Este fechamento interrompeu a queda de pressão, cuja causa ainda era ignorada pelos operadores, permitindo aos operadores readquirir o controle manual da pressão e estabilizar a planta, saindo desta maneira, das operações orientadas pelos procedimentos de emergência. A seguir, quando o isolamento da contenção foi normalizado, o retorno do suprimento de ar de controle para a válvula de spray fez com que a mesma abrisse, novamente, (porque ainda persistia a falha que causava a sua abertura), provocando nova queda de pressão, a valores inferiores ao ponto da atuação automática do sistema de injeção de segurança, porém sem a sua atuação porque a mesma estava bloqueada por um outro sinal automático. Este sinal de bloqueio automático é proveniente da posição aberta dos disjuntores de desarme do reator e quando a atuação de injeção de segurança já tenha ocorrido.

Esta situação requeria a ação manual do operador de atuar a injeção de segurança. Entretanto o mesmo, incorretamente, assumiu que o critério do procedimento de emergência para término da injeção de segurança ainda persistia, apesar de já ter realizado todas as ações requeridas pelo procedimento (entretanto, tratava-se de uma nova situação de emergência, onde o procedimento deveria ser, novamente, executado).

A injeção de segurança automática, somente, foi habilitada duas horas após concluir as ações do procedimento de emergência, quando os disjuntores de desarme do reator foram fechados. Este evento motivou mudanças nos procedimentos de emergências.

A.2.3 Oconee Unit 3

Sumário do evento:

Um sistema de segurança foi isolado durante um evento, devido ao seguimento inadequado das ações de um procedimento, contrariando as especificações técnicas. O sistema isolado não foi, prontamente, identificado nem normalizado.

Descrição do evento:

Em 26 de janeiro de 1993, ocorreu um desarme do reator quando este operava a 100% de potência. Seguindo as ações do procedimento de emergência para recuperação do desarme, enquanto os operadores transferiam o suprimento de água de alimentação dos geradores de vapor, do sistema de emergência para o sistema principal, ocorreu uma perda das condições de alimentação de emergência, quando ambos os controles das válvulas de controle de fluxo de água de alimentação de emergência não foram colocados na posição automática, como requerido por procedimentos. Esta condição foi descoberta 5,5 horas mais tarde.

A.2.4 North Anna Unit 2

Sumário do evento:

Um sistema de segurança foi isolado durante um evento contrariando as especificações técnicas e os procedimentos. Práticas de monitoração das condições da planta eram fracas e nem todos os supervisores foram informados de que o sistema estava isolado; um supervisor orientou, inadequadamente, o isolamento de um sistema de segurança.

Descrição do evento:

Em 16 de abril de 1993, ocorreu atuação da proteção diferencial do gerador, causando desarme do gerador, da turbina e do reator. Foram implementados os procedimentos de emergência para recuperação da planta. Durante a execução dos procedimentos de recuperação do desarme do reator, ocorreu um resfriamento

excessivo do circuito primário. Em resposta, os operadores desligaram as bombas motorizadas de água de alimentação, colocando as chaves de controle na posição removida e bloqueada, e fecharam as válvulas de vapor para a bomba turbinada de água de alimentação de emergência, isolando completamente o suprimento de água de alimentação de emergência para os geradores de vapor. Esta situação perdurou por cerca de 18 minutos. Os procedimentos de emergência requerem controlar o fluxo de água de alimentação de emergência, para manter nível nos geradores de vapor, quando a planta estiver nestas condições. O resfriamento excessivo ocorreu antes de se atingir os passos dos procedimentos e as condições da planta (nível adequado nos geradores de vapor e o restabelecimento de água de alimentação principal), que permitem interromper o fluxo ou desligar as bombas de água de alimentação de emergência. O operador que estava coordenando a execução do procedimento identificou o erro de alinhamento, e portanto, a inoperabilidade do sistema auxiliar, quando reviu um passo do procedimento, mais à frente da ação que estava sendo executada, o qual requeria colocar o sistema de água de alimentação de emergência na posição de espera, pronto para operar automaticamente. O sistema foi prontamente colocado como requerido.

Neste evento, o sistema de água de alimentação de emergência estava desligado quando ocorreu um sinal válido para operação automática (muito baixo nível nos geradores de vapor). A partida automática permaneceu isolada por 18 minutos. O operador que isolou o sistema de água de alimentação de emergência estava preocupado com uma possível degradação da bomba, caso esta operasse com fluxo mínimo, se a válvula de descarga da bomba fosse fechada. O operador acreditava que poderia restabelecer fluxo mais rapidamente pela partida da bomba do que pela abertura da válvula de descarga.

A.2.5 Wolf Creek

Sumário do evento:

Um sistema de emergência foi isolado quando era requerido estar operável pelas especificações técnicas. Este isolamento não foi recuperado no tempo adequado devido a deficiências nas práticas de supervisão das condições da planta envolvendo passagem de turno e inspeção do painel principal.

Descrição do evento:

Em 8 de maio de 1993, durante a partida da unidade, foi feito uma mudança do modo de operação (criticalidade do reator) com ambas as bombas motorizadas de água de alimentação de emergência inoperáveis (suas manoplas de partida automática não estavam na posição requerida). Esta condição é contrária e não atende aos requisitos das especificações técnicas.

Esta situação permaneceu por cerca de 13 horas e por duas mudanças de turno das equipes de operação, durante as quais não ocorreu nenhum questionamento sobre os requisitos para estas bombas. A bomba turbinada permaneceu operável.

A.2.6 Catwaba Unit 2

Sumário do evento:

Algumas válvulas dos sistemas de emergência estavam fechadas após um evento, quando é requerido estarem abertas, pelas especificações técnicas. Esta situação não foi corrigida em um tempo aceitável.

Descrição do evento:

Em 18 de outubro de 1994 ocorreu um desarme automático do reator durante testes do sistema de proteção do reator. Após o desarme, as bombas de água de alimentação de emergência partiram, como requerido, alimentando os geradores de vapor. 8 horas após, os operadores receberam orientação para transferir a alimentação dos geradores de vapor para o sistema principal de água de alimentação.

Durante esta manobra, as bombas de água de alimentação de emergência foram isoladas e o controle de fluxo foi ajustado em zero. Isto causa o fechamento das válvulas de controle de fluxo de água de alimentação de emergência para os geradores de vapor. Estas operações foram contrárias aos requisitos das especificações técnicas para o modo de operação em curso.

ANEXO B

ILUSTRAÇÃO DOS PRINCÍPIOS DA ATHEANA PELA EXPERIÊNCIA OPERACIONAL

A revisão e análise dos eventos operacionais tem sido, largamente, utilizadas para o desenvolvimento e demonstração dos princípios da ATHEANA (NUREG-1624, Rev.1, 2000). Igualmente, os princípios e conceitos das ciências comportamentais, descritos anteriormente, também foram confirmados usando exemplos da experiência operacional.

As análises dos eventos, segundo as perspectivas da ATHEANA, foram tratadas em vários documentos . Um deles foi o desenvolvimento de uma estrutura de banco de dados, denominado Human-System Event Classification Scheme (HSECS) (COOPER *et al.*, 1995), criado para dar suporte ao desenvolvimento da ATHENA, o qual está baseado na experiência operacional. Este banco de dados passou, desde sua criação, por alguns refinamentos, sentidos durante o desenvolvimento da ATHEANA. Os exemplos do apêndice A do NUREG-1624, Rev.1 (2000), documentam a análise de seis eventos que usaram estes refinamentos mais recentes.

Esta seção apresenta um extrato de alguns dos eventos analisados para ilustrar:

- como a experiência operacional confirma as perspectivas da ATHEANA, em acidentes sérios;
- a importância e utilidade dos conceitos das ciências comportamentais;
- o que são ações inseguras (UA), incluindo erros de comissão;
- como as UA's ocorrem e a influência do contexto que força ao erro (EFC) na sua ocorrência; e
- elementos de UA's e EFC's dos eventos reais.

Particularmente, a maior dificuldade em aplicar ATHEANA, prospectivamente (em ACH), é a identificação das ações inseguras (UA) e os respectivos contextos que

forçam ao erro (EFC), para levar a identificação dos eventos de falha humana (HFE). Os extratos mostrados a seguir, tentam estabelecer uma conexão entre as UA's e os EFC's e as suas influências observadas no desempenho humano.

B.1 Contribuição do homem e do contexto que força ao erro em eventos operacionais ocorridos

Os dois eventos, descritos na seção 4.3.2.1, demonstram que o contexto que força ao erro teve uma participação importante em eventos nucleares sérios. Esta seção apresenta, resumidamente, as condições da planta e os fatores que formatam o desempenho (PSF) negativos que criaram os contextos que forçam ao erro nestes eventos e uma breve explanação, de como estes EFC's podem ser relacionados a um ou mais estágios do processamento da informação.

B.1.1 Condições da planta e dos PSF's

Em TMI-2, as duas condições da planta que contribuíram para o evento foram a pré-existência do desalinhamento das válvulas de água de alimentação de emergência e a válvula de alívio do pressurizador que travou aberta. Elas combinaram com os PSF's negativos, que incluíam a obstrução, por um cartão de manutenção, do indicador de posição da válvula de água de alimentação de emergência, a falsa indicação de posição da válvula de alívio e a ausência de procedimentos para as condições específicas do evento. O treinamento do operador que, enfatizava os perigos de se ter condições sólidas da planta, levaram o operador a se concentrar no problema errado. De maneira geral, havia um desencontro (mismatch) entre as condições reais da planta e as informações de ajuda ao operador (por exemplo, treinamento, experiência) para este evento.

No evento de Crystal River 3, a abertura indevida da válvula de spray e o erro de indicação de sua posição criaram um contexto que força ao erro. Não havia procedimento que orientasse o diagnóstico e nem a correção da perda de controle de

pressão do sistema de refrigerante do reator. Consequentemente, da mesma maneira que o evento de TMI-2, havia um desencontro (mismatch) entre as condições atuais da planta e os sistemas de ajuda ao operador tais como procedimentos e indicadores de posição de válvula.

B.1.2 Falhas nos estágios de processamento da informação

A análise destes eventos revela que a avaliação da situação e a atualização do modelo da situação foram ruins. A análise indica que os operadores foram muito bons em desprezar as informações que não se encaixavam nas suas expectativas. Isto pode resultar em uma avaliação da situação incorreta e impedir atualizações do modelo da situação, no momento certo.

Em TMI-2, os operadores não reconheceram que a válvula de alívio estava aberta e que o núcleo do reator estava superaquecendo, portanto, o modelo da situação não foi atualizado. Em Crystal River 3, os operadores não reconheceram que a válvula de spray estava aberta e era a causa do transiente de pressão. As informações contrárias a isto foram desprezadas.

Estas avaliações das situações e atualizações dos modelos das situações envolveram tanto as fontes de informações (por exemplo, a instrumentação), quanto as suas interpretações: Em TMI-2, os operadores leram, erroneamente, o indicador de temperatura da linha de dreno da válvula de alívio duas vezes e então atribuíram, a alta temperatura de entrada do núcleo do reator e temperatura do circuito do SRR, à falha de instrumentação. Eles também foram confundidos pela indicação, errônea, da posição da válvula de alívio. Inclusive, alguns indicadores importantes estavam localizados nos painéis traseiros e a listagem da impressora do computador dos parâmetros da usina imprimia com 2 horas de atraso. Em Crystal River 3, os operadores, inicialmente, conjeturaram que o transiente de pressão era causado por uma contração do inventário do SRR. Diversos indicadores da planta, assim como o

erro do indicador de posição da válvula de spray e a ciclagem (sem sucesso) do controle da válvula de spray, foram tomados para embasar esta hipótese.

B.2 Análise do contexto que força ao erro

Enquanto a definição de HFE especifica qual consequência ocorrerá na planta, nos sistemas e ao nível de componente, a definição da UA está relacionada com modo de falha específico do sistema e componente, incluindo o momento da falha (por exemplo, término antecipado da operação de um sistema de emergência, que era necessário permanecer operando).

Por outro lado, o relacionamento entre uma ação insegura e um contexto que força ao erro específico são muito difíceis de definir e requerem a avaliação conjunta das causas psicológicas e físicas (já foi visto anteriormente que, diferentes EFC's podem resultar em uma mesma UA e diferentes UA's podem resultar em um mesmo HFE). Para estabelecer os relacionamentos entre uma UA e os EFC's, vários EFC's e elementos do EFC devem ser analisados para determinar seus impactos na execução da UA.

B.2.1 Contexto que força ao erro e ações inseguras

Os eventos analisados fornecem elementos para o entendimento das UA's e dos EFC's. Esta seção mostrará como os elementos dos EFC's (PSF's e condições da planta) afetam os quatro estágios do processamento da informação, descritos anteriormente.

B.2.1.1 Contexto que força ao erro na deteção

As falhas na deteção observadas nos eventos analisados foram as seguintes:

- operadores desconheciam às condições reais da planta;
- operadores desconheciam a gravidade das condições da planta; e
- operadores desconheciam a degradação continuada das condições da planta.

Baseado nos eventos dos exemplos utilizados, as falhas de instrumentação são esperadas ser a causa predominante das falhas de deteção.

Em geral, problemas na deteção de um acidente ou nas condições de um acidente são considerados serem raras. Devido ao alto número de alarmes e outras indicações disponíveis durante operação, a probabilidade dos operadores não saberem de que alguma coisa está errada e de que alguma ação é necessária, é baixa.

B.2.1.2 Contexto que força ao erro na avaliação da situação

A falha na avaliação da situação pode levar o operador a desenvolver um modelo da situação das condições e do comportamento da planta errado. Problemas de instrumentação ou de interpretação são as influências predominantes nestas falhas. Outros fatores também podem contribuir com este tipo de falha, como por exemplo, a intervenção do operador com a planta e seus sistemas (imediatamente, antes ou durante o evento e com ou sem conhecimento dos demais operadores da sala de controle) pode mascarar os sintomas do evento ou fazer com que eles sejam mal interpretados. Uma vez que os operadores desenvolvem um modelo de situação, eles procuram, tipicamente, por evidências que confirmem suas hipóteses (REASON, 1990) e desenvolvem explicações racionais, porém erradas, para desprezar evidências que são contrárias ao seu modelo da situação.

B.2.1.3 Contexto que força ao erro no planejamento da resposta

Falha no planejamento da resposta resulta quando o operador falha em selecionar ou desenvolver uma ação correta requerida pelo cenário do acidente. As maiores contribuições de falha no planejamento da resposta, além da avaliação errada da situação, são deficiências em procedimentos e treinamento fraco. A experiência passada mostrou cinco categorias de falhas no planejamento da resposta:

(1) os operadores selecionam planos não aplicáveis;

(2) os operadores seguem planos pré-estabelecidos que são errados ou incompletos;

(3) os operadores não seguem plano nenhum;

(4) não existem planos pré-estabelecidos, os operadores tem que se basear no seu próprio conhecimento; e

(5) os operadores dão, inadequadamente, prioridade a uma função da planta ao invés de outra.

O evento de Crystal River 3 ilustra a terceira e a quinta categoria. Na terceira categoria, a pesquisa dos operadores para determinar as causas de transiente de pressão do SRR foi direcionado pela suas avaliações da situação erradas e desta maneira excluíram as orientações dos procedimentos que poderiam ter terminado o evento mais cedo. Os operadores também usaram, inadequadamente, passos do procedimento (utilizados para desligamentos/resfriamentos) que é o bloqueio do sistema de atuação dos dispositivos de segurança de emergência e atuação automática de injeção de alta pressão. A justificativa era de que ele estava ajustado muito conservativamente e era possível reverter a queda de pressão (isto é, os operadores tinham um pouco mais de tempo para reverter a queda de pressão). Na quinta categoria , os operadores terminaram a injeção de segurança de alta pressão (sem orientação de procedimentos) muito cedo devido à preocupação do pressurizador ficar sólido.

B.2.1.4 Contexto que força ao erro na implementação da resposta

Os maiores contribuidores para falhas na implementação da resposta, identificados nos eventos analisados, são os PSF's, apesar das condições da planta poderem, também, afetar o desempenho geral dos operadores. Os problemas de falhas na implementação da resposta se classificam em três categorias:

(1) passos importantes do procedimento não são realizados;

(2) falhas de comunicação; e

(3) falhas de equipamentos interferem com a habilidade do operador em responder.

O evento de Crystal River ilustra a primeira categoria, quando os operadores mudaram de um procedimento para outro, antes de completar a seção que teria direcionado os operadores a tomar ações que poderiam ter terminado o evento. Contudo, os operadores são treinados para saber que é uma boa prática revisar todas as seções restantes de um procedimento para verificar passos importantes antes de se transferir para outro.

B.2.2 Fatores que formatam o desempenho

As análises de eventos realizadas mostraram que as condições da planta possuem papel importante em todos os eventos. Adicionalmente, os PSF's negativos contribuíram para deteriorar o desempenho humano. Como visto, fatores ambientais e ergonômicos deficientes, condições e/ou situações da planta não familiares e inexperiência afetam o desempenho dos operadores. Os seguintes PSF influenciam, negativamente, o desempenho dos operadores:

- capacidade do desempenho humano em um nível baixo;
- limitações de tempo;
- carga de trabalho excessiva;
- condições e/ou situações da planta não familiares;
- inexperiência;
- uso não otimizado dos recursos humanos; e
- fatores ambientais e ergonômicos.

O NUREG-1624, Rev. 1 (2000) apresenta exemplos destes PSF's mais tradicionais. Apesar da baixa probabilidade dos PSF's, por si só, dispararem os mecanismos de erros, os exemplos mostrados ilustram que tais fatores podem distrair

os operadores das atividades críticas ou interferir/inibir, drasticamente, a habilidade de executar atividades. Em alguns casos, os PSF's foram ativados por condições específicas da planta no contexto do evento (por exemplo, falta de treinamento ou experiência dos operadores para as condições atuais da planta). Em outros casos, os PSF's parecem ser genéricos ou insensíveis à especificidade do evento (por exemplo, condições ambientais).

B.2.3 Lições importantes das análises dos eventos

As análises dos eventos, tais como os apresentados no anexo A do NUREG-1624, Rev.1 (2000) e outros, forneceram uma série de características que foram documentadas e servem de referência para as análises e pesquisas realizadas pela ATHEANA.

As análises de eventos mostraram que as UA's são mais prováveis de serem causadas, em parte, por problemas reais de instrumentação ou falhas na interpretação das indicações existentes. Os EFC's, entretanto, são mais prováveis de existir quando falhas na instrumentação ou erros de interpretação são combinados com procedimentos deficientes (provavelmente disparado ou revelado por condições específicas da planta). Estes fatos embasaram o desenvolvimento das pesquisas de EFC's e UA's.

ANEXO C
Three Mile Island 2
Pequeno LOCA com perda de refrigerante do reator
28 de março de 1979

[NUREG-1624, Rev. 1]

C.1 IDENTIFICAÇÃO DO EVENTO – Three Mile Island 2

Nome da planta:	**Three Mile Island 2**
Tipo/vendedor da planta:	**PWR/B&W**
Data/hora do evento:	**28/03/1979, 04:00**
Tipo do evento:	**pequeno LOCA com perda de refrigerante do reator**
Evento secundário:	**Desarme do reator com falha de todo o SAAA**
Condições da usina:	**a plena potência (100%)**
Fontes das informações:	**Three Mile Island Report of NRC's Special Inquiry Group (Rogovin, et al.), Janeiro de 1980; Analysis of Three Mile Island - Unit 2 Accident, NSAC-1, Nuclear Safety Analysis Center, July 1979 and Supplement 1, October 1979.**
Dados registrados por:	**John Wreathall, Contractor (TWWG), 614-791 9264**

C.2 SUMÁRIO DO EVENTO

Descrição do evento: A usina nuclear de Three Mile Island, unidade 2 (TMI-2) sofreu um desarme da turbina e o consequente desarme do reator, por perda de água de alimentação principal. A perda de água de alimentação ocorreu devido ao ingresso de umidade no sistema de ar de instrumentos usado para controlar a válvulas de purificação do condensado. O ingresso da umidade no ar, foi proveniente do uso de ar, pelo operador, quando tentava desobstruir um linha de transferência de resina; o ar foi, indevidamente, utilizado, porque estava perto da linha obstruída. Após o desarme do reator, o sistema de água de alimentação de emergência (SAAE) falhou em fornecer resfriamento para os geradores de vapor, do tipo direto, uma passagem, porque as válvulas de entrada da AAE estavam fechadas (provavelmente, como consequência de uma falha de uma manutenção anterior). Os operadores estavam alheios, inicialmente, de que as válvulas de AAE estavam fechadas porque alguns cartões de isolamento de equipamentos bloqueavam esta indicação. A pressão do sistema primário subiu e fez a válvula de alívio do pressurizador ciclar para aliviar a alta pressão. Imediatamente após, a válvula de alívio de emergência do pressurizador (ERV) prendeu aberta. Entretanto, os operadores estavam alheios ao fato da válvula de alívio ter prendido aberta porque a indicação de posição da válvula mostrava a posição demandada da válvula (isto é, se a solenóide, que opera a válvula, está energizada ou não) e não a sua posição real. Uma segunda indicação, de que a válvula estava aberta (alta temperatura da linha de alívio), foi desprezada pelo operador uma vez que já era sabido que esta válvula costuma vazar

Devido a indicação de nível do pressurizador estar indicando alto e subindo, o operador entendeu que o sistema estava indo para a "condição sólido". Isto é, a bolha de vapor existente no topo de pressurizador estava se reduzindo para zero, o que significa, potencialmente, perder o controle da pressão do sistema primário e a possibilidade de causar um acidente de perda de refrigerante (LOCA). Os operadores eram provenientes do programa nuclear da marinha, no qual a situação "indo para sólido" representa a maior preocupação operacional. Devido à esta preocupação, os operadores reduziram a injeção de segurança de alta pressão (HPI), virtualmente, para injeção nula, dentro dos 5 minutos após o evento inicial. O fluxo de HPI foi, efetivamente, zero pelas 4 horas seguintes. Três minutos após, às 04:08 h, os operadores descobriram que as válvulas de AAE estavam fechadas e as abriram, restaurando o fluxo de água de resfriamento para os geradores de vapor. Às 04:20 h e 04:38 h, os operadores não reconheceram a existência de um LOCA quando o disco de ruptura do tanque de drenos do refrigerante do reator (TDRR)

falhou e quando os alarmes de alto nível do poço da contenção atuaram. Às 06:18 h, os operadores fecharam a válvula de bloqueio da válvula de alívio do pressurizador mas não fizeram nenhuma tentativa de restabelecer a HPI até às 08:17 h. Devido à falta de fluxo de injeção de alta pressão, um fluxo em duas fases estava se formando no sistema primário. Pelas 05:14 h, o fluxo em duas fases provocou sérias vibrações na bomba B do refrigerante do reator que levou os operadores a desligá-la. Cerca de 30 minutos após, às 05:41, os operadores desligaram a bomba A do refrigerante do reator devido à vibrações significativas. Estas bombas permaneceram desligadas até às 19:50 h, quando os operadores as religaram e, desta maneira, estabelecendo um fluxo forçado de refrigeração no sistema primário.

Durante os dias seguintes, operadores e a NRC analisaram e responderam ao questionamento de formação de hidrogênio no sistema primário.

Surpresas do evento: Os operadores desconsideraram a possibilidade de haver duas fases no sistema primário por um tempo prolongado mesmo com numerosos sintomas de LOCA, sua conseqüência nas bombas de refrigerante do reator e danos ao núcleo mostrados pelas indicações dos termopares do núcleo.

Ações corretivas da licenciada: A indústria e a NRC implementaram mudanças significativas nas práticas relacionadas com o projeto de fatores humanos na sala de controle, as bases e o projeto dos procedimentos de operação de emergência e a abordagem do treinamento da indústria.

Sumário da ATHEANA:
Desvio do Cenário "esperado":

- O caminho da descarga via válvula de alivio operada à potência (PORV, power operated relief valve) para o LOCA não era esperado. A conseqüência deste desvio foi que os operadores ficaram confusos com a indicação de nível do pressurizador subindo o que levou a acreditar que o sistema de refrigerante do reator (SRR) estava indo para a condição "sólida".
- Em relação à via de descarga, o fato de que as indicações associadas com a PORV não eram, diretamente, medidas de sua posição física, mas do sinal de demanda, levou os operadores a não acreditar que a válvula estava aberta. Esta discrepância na informação foi um desvio significativo da expectativa.
- A falha completa do sistema de água de alimentação de emergência em partir (devido a não restauração do alinhamento após serviços de manutenção prévios) na perda de água de alimentação foi um desvio do cenário esperado para o caso de perda de água de alimentação.
- Comportamento do SRR, após o ponto de saturação ter sido atingido, foi um desvio significativo do esperado pelo operador e pela NRC.

Desvios chaves:

- O comportamento das indicações do SRR (particularmente o nível do pressurizador) comparado com o treinamento e os procedimentos guias do operador para um pequeno LOCA foi um desvio.
- A indicação de posição da PORV do pressurizador comparada com sua posição real (tanto a indicação da posição da válvula, quanto a temperatura da linha à jusante) criaram um desvio.
- A importância relativa do risco do SRR indo para sólido verso os riscos da condição de duas fases.
- A convicção de que os termopares de saída do vaso do reator estavam falhados baseados nas suas indicações muito altas.

Influências mais negativas:

- A **experiência prévia (PSF)** do operador, particularmente, seu treinamento na marinha, criou uma convicção que "indo para sólido" era, justamente, a pior condição que a planta poderia ter. O **treinamento (PSF)** do pessoal de TMI não tinha contemplado esta experiência e os **procedimentos (PSF**) não foram, particularmente, úteis para esta situação.
- Muitos dos indicadores, que poderiam ter ajudado os operadores a reconhecer as condições da planta, estavam localizadas de tal maneira que eles não eram visíveis da área normal de trabalho da sala de controle **(interface homem-máquina – PSF).**
- Os operadores não foram treinados para reconhecer um provável LOCA via válvula de alívio do pressurizador onde os sintomas normais de um pequeno LOCA (queda do nível do pressurizador) é invertido **(treinamento – PSF).**
- O problema básico de muitas destas deficiências foi a falha da indústria em reconhecer a importância de um pequeno LOCA, tanto em termos de sua importância para o risco, quanto para suas diferença em relação a um LOCA bases de projeto (grande), em termos de quais sintomas podem existir e as respostas requeridas do operador **(condições dinâmicas não esperadas, condições da planta)**.

Influências mais positivas: (que poderiam ter evitado ou mitigado o evento)

- A influência mais positiva foi o envolvimento de pessoas de fora que, eventualmente, identificaram a resposta adequada para o evento (**condições da planta**).

- Em vários (mas não todos) casos, a instrumentação existente, tais como os drenos do poço da contenção e a pressão no TDRR, poderia ter revelado, se observadas pelo operador, a existência do LOCA. Inclusive o sistema de controle pressão do reator, se observado, poderia ter revelado que o refrigerante do reator estava em duas fases. (**instrumentação – PSF**).

Importância do evento:

- Este evento representa o único acidente envolvendo substancial dano ao núcleo em usinas em operação comercial de potência nos Estados Unidos.

Condições extremas ou não-usuais: inicialmente, nenhuma. Posteriormente, o nível do SRR caiu até o ponto de descobrimento do núcleo resultando em dano ao núcleo.

Condições contribuidoras pré-existentes: o sistema de AAE isolado, provavelmente, exacerbado pelo transiente de pressão do SRR. O vazamento pela PORV mascarou alguns dos sintomas do travamento da válvula na posição aberta.

Informações confusas ou erradas: indicação de posição da PORV mostrava que a válvula estava fechada.

Informação rejeitada ou ignorada: leitura dos termopares de saída do núcleo foi ignorada e dada como falhada.

Falhas múltiplas de equipamentos: perda de água de alimentação principal; sistema de AAE isolado; PORV presa aberta.

Transição em progresso: desobstrução da linha do leito de resinas do sistema de purificação de condensado.

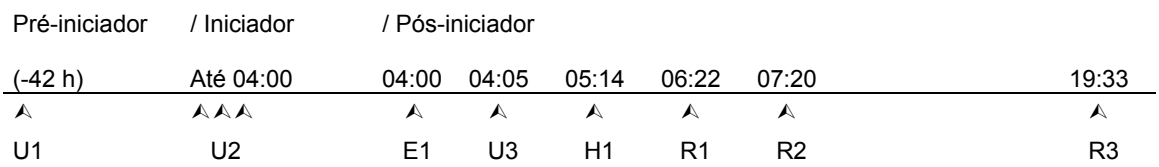
Similaridades com outros eventos: sintomas do LOCA do pressurizador similar ao SRR "indo para sólido", um evento de grande preocupação para a equipe com experiência na área nuclear da marinha.

CONDIÇÃO DOS PARÂMETROS CHAVES	
CONDIÇÕES INICIAIS	**CONDIÇÕES DE ACIDENTE**
Nível de potência: 97% **Temperatura do SRR(º F):** nominal **Pressão do SRR:** nominal (cerca de 2255 psig) **Nível do SRR:** nominal **Outros:** nominal	**Nível de potência:** desarmado **Temperatura do SRR(º F):** 590-780 **Pressão do SRR:** 400 - 2365 psi **Nível do SRR:** mínimo~3 pés acima do topo do núcleo ativo **Outros:** temperatura do combustível acima de 2500 º F

Condições/configurações iniciais da planta	**Condições/configurações de acidente da planta**
Configuração: (1) Condições nominais à potência (2) Equipe estava respondendo à problemas na estação de purificação de condensado (3) Unidade 1 estava em desligado quente. **Condições pré-existentes exigindo atenção:** (1) válvulas de bloqueio de AAE fechadas. (2) Válvula de alivio do pressurizador (ERV) tinha um histórico de vazamento, com indicação de temperatura alta na linha de descarga (3) Válvulas de spray e aquecedores do pressurizador estavam em controle manual. **Iniciador:** (1) Desarme da turbina por perda de água de alimentação levou ao desarme do reator por alta pressão no SRR.	**Respostas automáticas:** (1) Sistema de AAE com partida automática (2) Válvulas ERV cicladas para aliviar a alta pressão do SRR. (3) Bomba de injeção de alta pressão 1A e 1C partiram por baixa pressão do SRR (Sinal de atuação do ESF). **Falhas:** (1) As válvulas de bloqueio de AAE estavam fechadas (assumida uma falha latente após uma manutenção anterior), desta maneira impedindo o resfriamento pelo secundário por 8 minutos no início do evento. (2) A ERV prendeu aberta.

C.3 SUMÁRIO DAS AÇÕES

Linha de tempo do evento



Ações inseguras e outros eventos:
Convenção: U = ações inseguras

E = falhas de equipamentos (significativa para o evento)

H = ações não erradas (não de recuperação)

R = ações de recuperação

Ações inseguras e outros eventos:	
ID	**DESCRIÇÃO**
U1	Válvulas de bloqueio de AAE deixadas fechadas (provavelmente de uma manutenção realizada 42 horas antes do evento iniciador)
U2	Operadores usam ar de instrumento na tentativa de desobstruir a linha de transferência de resina – leva ao evento iniciador
E1	Válvula de alívio do pressurizador prende aberta
U3	Operadores ajustaram HPI para evitar que o pressurizador ficasse sólido
H1	Operadores desligam as bombas do SRR na indicação de alta vibração
R1	Operadores fecham a válvula de bloqueio da válvula de alívio do pressurizador
R2	Operadores, manualmente, iniciam fluxo adicional de HPI
R3	Operadores religam as bombas do SRR

DEPENDÊNCIAS HUMANAS		
ID	**MECANISMO DE DEPENDÊNCIA**	**DESCRIÇÃO**
	Nenhum	

Análise das ações inseguras		
U1: *desconhecida, mas provável EOO, slip: válvula não restabelecida após manutenção*		
Contexto que força ao erro		
Condições da planta	**PSF's**	**Falhas no processamento da informação**
Evolução e atividades: 1) É assumido que as válvulas foram deixadas fechadas após trabalhos prévios de manutenção apesar do pessoal envolvido naquele trabalho terem comunicado que as válvulas estavam posicionadas corretamente. *Configuração:* 2) Desconhecida. *Impacto na planta:* 1) Impediu o resfriamento inicial pelo secundário, o qual agravou o transiente de pressão após a perda de água de alimentação.	Desconhecido	Desconhecido
U2: *EOC: Operadores usam ar de instrumento para tentar desobstruir uma linha de transferência de resina – umidade entrou na linha de suprimento de ar (AI) (pode ser um problema de engano ou erro intencional o uso de AI com finalidade diferente do projeto, mas nenhuma informação foi fornecida).*		
Contexto que força ao erro		
Condições da planta	**PSF's**	**Falhas no processamento da informação**
Evolução e atividades: 1) Os operadores estavam tendo dificuldades em transferir a resina da estação de purificação de condensado para um tanque de recebimento. Tentativa de desobstruir a linha de transferência bloqueada estava em andamento por cerca de 11 horas.	Desconhecida	Desconhecida

U3: *EOC: mistake: operadores, taxativamente, terminaram a HPI para evitar que o pressurizador ficasse sólido*		
Contexto que força ao erro		
Condições da planta	**PSF's**	**Falhas no processamento da informação**
Evolução e atividades: 1) Os operadores estavam respondendo à operação de controles automáticos na fase imediata de pós-evento. *Configuração:* 1) A planta desarmou por alta pressão do SRR após perda de água de alimentação; caminho de fluxo de injeção de água de alimentação de emergência estava bloqueado pelas válvulas deixadas fechadas (conseqüência de U1). HPI partiu injetando, automaticamente. LOCA pela ERV descarregou via pressurizador. *Impacto na planta:* 1) Causou grave dano ao núcleo.	*Interface homem-máquina:* 1) O indicador de posição da ERV era baseado no sinal de demanda, não na posição real da válvula. Muitas indicações que poderiam ter evitado a interpretação errada estavam localizados em painéis traseiros. *Treinamento:* 1) Operadores não foram treinados em LOCA's via linhas de alívio do pzer. 2) Operadores persistiram em acreditar que "indo para sólido" era o maior perigo em TMI. *Procedimentos:* 1) O procedimento de LOCA não possuía diretrizes específicas para um LOCA pela ERV.	*Avaliação da situação:* 1) Os operadores criaram um modelo da situação incorreta devido aos seguintes fatores: - nível do pressurizador indicou alto e subindo - posição indicada da ERV era fechada quando, na verdade, estava aberta. - A linha de descarga da ERV tinha um histórico de indicar alta temperatura, devido a um vazamento.

C.4 SEQUÊNCIA DE EVENTOS DO ACIDENTE

Hora	Progressão do acidente & sintoma [1]	Resposta [2]
Antes de 04:00	Unidade a 97% de potência e em condições nominais. Os operadores estavam tentando desobstruir a linha de transferência de resina da estação de purificação de condensado usando ar de instrumento com uma lança **(U2).**	
04:00:37	As válvulas do sistema de purificação do condensado fecharam devido à umidade que penetrou no ar de instrumento. A turbina desarmou devido à perda de água de alimentação.	
04:00:45	O reator desarmou por alta pressão no SRR	
04:00:49	Válvula de alivio de emergência do pressurizador (ERV) ciclaram e então prendeu aberta **(E1)**.	Nenhuma. A indicação na sala de controle mostra o sinal "demandado" para fechamento da válvula e não a sua posição "real".
04:05:15	Nível do pressurizador era 363" e subindo	Operadores reduziram o fluxo de HPI para evitar que o sistema ficasse sólido – procedimentos estabelecem que o nível do pressurizador não deve ultrapassar 400" **(U3).**
04:08:55		Os operadores descobrem que as válvulas de bloqueio de AAE estavam fechadas e as abrem, estabelecendo um fluxo de AAE para os geradores de vapor.
04:14-04:20	O disco de ruptura do tanque de drenos do refrigerante do reator (TDRR) falha.	Os operadores notaram a queda de pressão no TDRR mas falharam em diagnosticar um LOCA pela ERV.
04:25-07:??	Alta temperatura da linha de descarga da ERV.	Os operadores consideram, por duas vezes, a alta temperatura ser um efeito do calor residual da abertura inicial da válvula.
04:38	Informado que as bombas do poço da contenção estavam operando.	Operador desligou as bombas.
04:40+	Medido baixa concentração de boro e aumento da contagem de nêutrons no reator.	O significado deste comportamento não foi entendido (indicação de que o núcleo estava secando).
05:00	Temperatura do edifício da contenção está em 170^{O} F, pressão em 2,5 psi.	Aparentemente não foi observado.
05:14	Ambas as bombas de refrigerante do reator (BRR) do circuito B indicam vibração significativa.	Os operadores desligam as BRR's do circuito B. **(H1)**
05:41	As BRR's do circuito A indicam vibração significativa.	Os operadores desligam as BRR's do circuito A. **(H1)**
06:18	Alta temperatura da linha de descarga da ERV,	Operadores solicitaram uma medição da temperatura da linha da ERV e fecharam a sua válvula de bloqueio 4 minutos mais tarde. **(R1)**
06:45-06:54		Os operadores tentam partir as BRR's – bomba 2B opera por poucos segundos e desarma; as outras bombas não partiram
06:55		Declarada Emergência de Área

07:13		Os operadores reabrem a válvula de bloqueio da ERV; a temperatura da linha de descarga aumenta.
07:17		Os operadores tornam a fechar a válvula de bloqueio
07:20		Os operadores, manualmente, iniciam o sinal de injeção de segurança, a bomba 1C de água de reposição do refrigerante do reator parte. **(R2)**
07:24	A leitura do nível de radiação no edifício do reator indica 8 R/h.	Declarada Emergência Geral.
08:17-08:27	A bomba 1A de água de reposição do refrigerante do reator desarma.	Bomba 1B parte, automaticamente, bomba 1C é partida manualmente.
19:33-19:50		A BRR 1A é partida manualmente, desligada e novamente partida.

(1) Um grande número de alarmes e indicações ocorreram durante o evento, muitos dos quais eram indicativos do evento.

(2) Os operadores realizaram várias ações, além das listadas acima, que tiveram importante papel no evento.