PUBLICAÇÃO CDTN-816

TÉCNICAS E APLICAÇÕES DA ANÁLISE DA CONFIABILIDADE HUMANA EM INSTALAÇÕES NUCLEARES

Fausto Carvalho Pinto

Fausto Carvalho Pinto

Orientador: Ricardo Brant Pinheiro

TÉCNICAS E APLICAÇÕES DA ANÁLISE DA CONFIABILIDADE HUMANA EM INSTALAÇÕES NUCLEARES

Dissertação apresentada ao Curso de Ciências e Técnicas Nucleares da Escola de Engenharia da Universidade Federal de Minas Gerais, como requisito parcial para obtenção do grau de Mestre em Ciências e Técnicas Nucleares

Belo Horizonte

Dezembro de 1995

UNIVERSIDADE FEDERAL DE MINAS GERAIS

DEPARTAMENTO DE ENGENHARIA NUCLEAR
CURSO DE PÓS-GRADUAÇÃO EM CIÊNCIAS E TÉCNICAS NUCLEARES

TÍTULO DA DISSERTAÇÃO

"Técnicas e Aplicações da Análise da Confiabilidade Humana em Instalações Nucleares"

NOME DO ALUNO: Fausto Carvalho Pinto

Dissertação defendida e aprovada pela Comissão Examinadora constituida por:

Prof. Celso de Oliveira Loureiro, Doutor

Prof. Leonardo Márcio Vilela Ribeiro, Mestre

ORIENTADOR: Engº Ricardo Brant Pinheiro, Doutor

Belo Horizonte, 27 de dezembro de 1995.

Área de Concentração: Energia Nuclear

Este trabalho foi desenvolvido com o apoio do Centro de Desenvolvimento da Tecnologia Nuclear - CDTN, órgão da Comissão Nacional de Energia Nuclear - CNEN.

AGRADECIMENTOS

A publicação deste documento é fruto da colaboração de várias pessoas. Não poderia deixar de agradecer o apoio de todos os que direta ou indiretamente auxiliaram no esfoço para a sua realização. Embora existindo o risco de esquecer alguém, seria imperdoável de minha parte não agradecer àquelas pessoas que se empenharam para fazer deste um bom trabalho.

Agradeço ao meu orientador, Ricardo Brant Pinheiro, pelas sugestões, pela orientação e pela valorização do trabalho. Agradeço ao Vanderley de Vasconcelos pelo acompanhamento do trabalho desenvolvido, pela atenção, pelo incentivo, pelas sugestões e o apoio, sem o qual não teria sido possível realizar esta tarefa. Agradeço ao Roberto Stasiulevicius pelo apoio e dedicação nas sugestões para o desenvolvimento do exemplo relacionado com o Reator Triga IPR-R1, que contribuiram para melhorar o trabalho. Agradeço ainda ao Luiz Augusto Queiróz e Oliveira, pelo incentivo, aos operadores do Reator, Valter Alves de Amorin, Paulo Fernando Oliveira e Fausto Maretti Júnior, à Lenira Lúcia Santos Passos Ferreira e à Maria Mabel de Menezes Scotti, pelo inestimável auxílio quanto à bibliografia, e à Roselim Trópia Barreto, pela boa vontade em seu trabalho, que tornou possível e mais fácil realizar a tarefa de desenvolver e publicar essa dissertação.

Agradeço também a todos os colegas, amigos e amigas que de alguma forma contribuiram para a elaboração dessa dissertação.

RESUMO

A complexidade e a importância dos fatores humanos na operação de instalações nucleares é discutida e apresentada tendo em vista principalmente o risco associado à ocorrência de acidentes. Esta preocupação tem sido enfatizada pelos muitos incidentes que claramente são indicativos de que acidentes podem surgir pela interação inadequada entre o homem e os componentes de máquina do sistema. A análise e previsão destas interações são o objeto da *Análise da Confiabilidade Humana* de um sistema. Este trabalho apresenta, em resumo, informações referentes aos aspectos humanos, que podem ser utilizadas por especialistas no campo da Avaliação Probabilística de Segurança, baseado na utilização da Técnica de Previsão de Taxas de Erros Humanos. Além de algumas aplicações desta técnica são apresentadas também considerações sobre o estado-da-arte, a pesquisa e o desenvolvimento neste campo de trabalho, relacionados principalmente com a formação de um banco de dados confiável. Nos itens apresentados incluem-se a modelagem das ações dos operadores, a elaboração de procedimentos considerando aspectos relacionados à cognição, e a questão da interface homem-máquina, no projeto de sistemas de controle. Também é apresentado uma aplicação da técnica relativamente ao Reator Triga Mark 1 IPR-R1, do Centro de Desenvolvimento da Tecnologia Nuclear, cujos resultados indicam a necessidade de algumas modificações nos procedimentos de emergência para o mesmo.
A relevância da confiabilidade humana, considerando a indústria nuclear, abrange os projetistas e construtores de usinas, operadores, gerentes de segurança, engenheiros, a gerência superior, órgãos regulatórios e de licenciamento, e a pesquisa desenvolvida.

ABSTRACT

The complexity and importance of man-machine interface must be considered because accidents in Nuclear Power Plants derive mainly due to human failure. This awareness has been heightened by many incidents which clearly indicate that accidents are rarely the result of pure technical failures. Rather they arise from the inadequate interaction of the technical and human elements in the system. The analysis and prediction of this interaction are the objectives of *Human Reliability Analysis*. In this work information is presented in a manner that could be used by experts in the field of Probabilistic Safety Assessment, considering primarily the aspects of human errors. The Technique of Human Error Rate Prediction (THERP) is used in large scale to obtain data on human error. Applications of this technique are presented, as well as aspects of the state-of-the-art and of research and development of this particular field of work, where the construction of a reliable data bank is considered essential. The work include modeling of operators actions considering cognition aspects and man-machine interface related to control systems design. It is work is also developed an application of the THERP for the Triga Mark 1 IPR R-1 Reactor of the Centro de Desenvolvimento da Tecnologia Nuclear. The results indicate that some changes must be made in the emergency procedures of the Reactor, in order to achieve a higher level of safety. Considering the nuclear power industry, this field of work is important for plant designers, operators, safety managers, engineers, senior management, regulatory experts and researches.

LISTA DE ACRÔNIMOS

ACH - Análise da Confiabilidade Humana
AD - Alta Dependência
AIEA - Agência Internacional de Energia Atômica
APS - Avaliação Probabilística de Segurança
BDBA - "Beyond Design Basis Accident"
BD - Baixa Dependência
CANDU - "Canadian Deuterium Uraniun Reactor"
CDTN - Centro de Desenvolvimento da Tecnologia Nuclear
CLD - Controles Lógicos Programáveis
CNAAA - Central Nuclear Almirante Álvaro Alberto
CNEN - Comissão Nacional de Energia Nuclear
COPPE - Coordenação dos Programas de Pós-Graduação em Engenharia da UFRJ
CRT - "Cathode Ray Tube"
CTAS - Centro de Treinamento Avançado com Simulador de FURNAS
DBA - "Design Basis Accident"
DISC - Descarga ("Discharge")
DT - Dependência Total, ou dependência completa
DZ - Dependência Zero, ou independência total ou completa
ENU - Evento Não Usual
EOP - "Emergency Operational Procedure" - Procedimento operacional de emergência
EUA - Estados Unidos da América
FE - Fator de Erro
FEMA - "Federal Emergency Management Agency"
FURNAS - Furnas Centrais Elétricas SA
HEP - "Human Error Probability" - Probabilidade de erro humano
HEPB - Probabilidade de Erro Humano Básica
HEPC - Probabilidade de Erro Humano Condicional
HER - Human Error Rate - Taxa de Erros Humanos
IEN - Instituto de Engenharia Nuclear
IPR-R1 - Instituto de Pesquisas Radioativas - Reator 1
ISO - Isolamento
LO - Baixo
MOV- "Motor Operated Valve"
NASA - "North American Space Agency"
NRC - "Nuclear Regulatory Commission"
NUCLEN - Nuclebrás Engenharia e Serviços SA
OFP - "Overal Failure Probability" - Probabilidade de falha geral

OR - Operador de Reator
ORP - "Operator Recovery Probabilities" - Probabilidade recuperação do operador
OSART - "Operational Safety Review Teams"
PP - Bomba ("Pump")
PRCE - Programa de Remoção de Causa de Erro
PSF - "Performance Shaping Factors " - Fatores Influenciadores do Desempenho
PWR - "Pressurized Water Reactor" - Reator a Água Pressurizada
RECIRC - Recirculação
RELAP - "Reactor Excursion and Leak Analysis Programme"
RWST - " Refueling Water Storage Tank " - Tanque de armazenamento de água de recarregamento ou realimentação
SDCD - Sistemas Digitais de Controle Distribuido
SPDS - "Safety Parameters Display System" -Sistema Mostrador de Parâmetros de Segurança
SI - Injeção de Segurança - ("Safety Injection")
SRE - Supervisor de Reator
ST - Supervisor de Turno
THERP - " Technique for Human Error Rate Prediction" - Técnica de Previão de Taxas de Erros Humanos
TRAC - "Transient Reactor Analysis Code" - Código de Análise de Transitório de Reator
TMI - "Three Mile Island"
UFRJ - Universidade Federal do Rio de Janeiro
USA - "United States of America" - Estados Unidos da América
VV - Válvula

LISTA DE FIGURAS

		Página
2.4-1	Modelo de entradas (estímulos) e saídas (respostas) do sistema homem	10
2.4-2	Controle por pressão ("Pushbutton")	10
2.4-3	Representação de diferentes tipos de controle de rotação	11
2.4-4	Controle protegido por moldura (arma/desarma)	12
2.4-5	Controle protegido por cobertura móvel	12
2.4-6	Válvulas não rotuladas, dificultando a identificação e facilitando o acionamento errado	13
2.4-7	Controles protegidos por plástico, para evitar acionamento indevido	14
2.4-8	Etiquetas colocadas pelos operadores, para facilitar a visualização e ações indicadas	14
2.4-9	Grande quantidade de controles, dificultando a identificação e conseqüente manuseio	15
2.4-10	Configuração original e modificada	15
2.5-1	Situação inadequada de um operador em uma sala de controle	17
2.5-2	Dificuldade de alcançar a lâmpada dos anunciadores	17
2.5-3	Operador monitorando medidores situados numa posição muito alta	18
2.5-4	Controle e operação em painéis opostos, facilitando erros de acionamento de controles	18
2.5-5	Boa solução ergonômica, com procedimento transportado por carrinho de mão	19
2.5-6	Novo conceito de sala de controle	19
2.6-1	Freqüência de incidentes e falhas em reatores japoneses, em casos por reator-ano	20
2.6-2	Efeito de erros humanos na operação de usinas nucleares no Japão	21
2.6-3	Causas dos acidentes potenciais devido a fatores humanos em usinas nucleares	21
2.6-4	Razões para a leitura errada, principal causa potencial de acidentes em usinas nucleares no Japão	21
2.6-5	Comparação de tipos de erros e ação inadequada entre operadores dos EUA e do Japão	22
2.6-6	Resultado da comparação de fatores que contribuíram para as ações inadequadas	22

2.7-1	Modelo estruturado de interface homem-máquina comparado ao tradicional	25
2.8-1	Recursos gráficos obtidos por computador, indicando a direção tomada pela nuvem radioativa após a ocorrência de um hipotético acidente em uma usina nuclear	30
2.8-2	Recursos gráficos apresentando simulação de nuvem radioativa se deslocando, e sistema de parâmetros associados, relacionados ao ambiente, incluindo níveis de radioatividade	31
3.1-1	Comparação de três curvas representando três diferentes situações relacionadas com uma determinada variável e sua relação com o nível de alarme	36
4.3-1	Distribuição de incertezas, frações, média, e faixa simétrica de 90%	59
5.3-1	Árvore de eventos	69
5.3-2	Exemplo de árvore de falhas para um sistema hipotético	70
5.3-3	Diagramas apresentando árvores de falhas e THERP	72
5.3-4	Exemplo de árvore THERP com valores	74
6.5-1	Gráfico para triagem de HEPC para diagnóstico considerando tempo após sinal compelidor	83
6.5-2	Tempo para realização de diagnóstico	85
6.5.-3	Árvore THERP utilizando valores de triagem de HEPC para diagnóstico e uma ação crítica	86
6.5-4	Gráfico para estimativas de HEPC com base no modelo nominal para diagnóstico, considerando o tempo T em minutos depois de um alarme de situação anormal	87
6.5-5	Árvore THERP para diagnóstico	92
6.5-6	Comparação entre três gráficos de estimativas de HEP's para diagnóstico em salas de controle de usinas nucleares baseados em modelos das referências [1], [[62] e [63]	93
7.1-1	Painel apresentando sistema de sinais anunciadores	94
7.1-2	Árvore simplificada de eventos HRA para perda de alimentação de água no gerador de vapor	96
7.1.3	Árvore de falha expandida para o exemplo	99
7.2-1	Comutadores MOV de um conjunto maior, que devem ser acionados pelo operador	102
7.2-2	Árvore de eventos THERP para ações indicadas por procedimento após ocorrência de um LOCA	104
7.2-3	Árvore THERP modificada para a mudança do modo de injeção	107
8.1-1	Vista em corte do reator IPR-R1 mostrando o núcleo e o refletor	111
8.1-2	Esquema da mesa de operação	112
8.1-3	Detalhe do painel da mesa, com a localização dos mostradores A, B, e C, referentes ao controle de potência do reator IPR-R1 e de níveis de radiação gama na sala do reator (no painel III)	112

8.5-1	Árvore de falhas para o exemplo THERP / IPR-R1	121
8.5-2	Ações dos operadores após disparo de alarmes	123
8.5-3	Árvore THERP para o exemplo	127
A.1-1	Condições de segurança numa usina nuclear, apresentando a linha divisória dos Acidentes Base de Projeto e os Acidentes Além da Base de Projeto, inclusive Acidentes Severos	153
A.1-2	Conceito de defesa em profundidade na segurança de usinas nucleares	154
A.1-3	Tendências na filosofia de segurança dos reatores a partir de 1960	154
A.2-1	Barreiras passivas para confinamento dos produtos de fissão	159
A.2-2	Estágios no gerenciamento de acidentes no núcleo de um reator nuclear	162
B.3-1	Relação hipotética entre o desempenho e o estresse, considerando a carga de trabalho	166
B.3-2	Efeito do tempo na vigilância de um operador, em tarefas de monitoramento, com pouca necessidade de concentração	168
B.4-1	Gráfico comparando a vantagem de treinamento realizado continuamente no tempo, com o treinamento inicial apenas, para condições de emergência	171
B.6-1	Estimativa de desempenho humano após um LOCA por grande ruptura	175

LISTA DE TABELAS

3.1-1	Categoria de comportamento humano incorreto, aplicáveis à análise da confiabilidade humana	37
3.2-1	Fatores influenciadores do desempenho humano	40
4.3-1	Valores de HEP e Fatores de Erros associados	59
4.3.2	Probabilidades de erros humanos usados no WASH-1400	62
4.3-3	Exemplos de dados de probabilidade de não recuperação após a ocorrência de uma falha	64
5.1-1	Linhas Gerais da THERP para uso em Avaliação Probabilística de Segurança	67
5.2-1	Modelando o desempenho humano pela técnica THERP	67
5.2-2	Exemplo de decomposição na tarefa de trocar pneu furado em uma rodovia	68
5.3-1	Simbologia para o sistema em paralelo	73
5.4.-1	Níveis de dependências	76
6.3-1	Definição de termos relacionados à cognição	80
6.5-1	Dados para triagem de estimativas de HEPC e FE para diagnóstico dentro de um tempo T de eventos anormais anunciados num tempo próximo	84
6.5-2	Dados para triagem inicial para HEP's e EF's estimados, depois do diagnostico de um evento anormal, para ações baseadas em regras executadas pelo pessoal de operação	84
6.5-3	Dados de HEP's e FE's para diagnóstico de evento anormal para o pessoal da sala de controle de uma usina nuclear, baseado no modelo nominal para diagnóstico	88
6.5-4	Nível de dependência, considerando número de operadores de reator e consultores técnicos	89
6.5-5	Linhas gerais para ajustes de HEP utilizando o gráfico da Figura 6.5-4	90
6.5-6	Decréscimo estimado nas probabilidades nominais de erros humanos resultante de aplicação de boas práticas ergonômicas em Usinas Nucleares	91
7.1-1	HEPC considerando três operadores na sala de controle	95
8.5-1	Ajustes nos HEP's	127

C.1 Probabilidade de erros humanos condicionais aproximados e respectivas margens de incerteza para níveis de dependência, dada a falha na tarefa precedente 177
C.2 Modificações de HEP's estimados para efeito de estresse e níveis de dependência 178
C.3 Probabilidades estimadas de erros de ação na operação de controles manuais 178
C.4 Probabilidades estimadas de erros de omissão por item de instrução quando o uso de procedimentos escritos é especificado 179

SUMÁRIO

LISTA DE ACRÔNIMOS
LISTA DE FIGURAS
LISTA DE TABELAS

		Página
1	**INTRODUÇÃO**	**1**
1.1	**Objetivo do Trabalho**	**1**
1.2	**Organização do Trabalho**	**2**
2	**O SISTEMA HOMEM MÁQUINA**	**4**
2.1	**A contribuição do homem na operação e na segurança de usinas nucleares e outras instalações industriais**	**4**
2.2	**Principais Definições**	**6**
2.3	**Fatores Humanos em Instalações Complexas**	**7**
2.4	**Instrumentação e Controle**	**9**
2.4.1	Exemplos de controle na interação homem-máquina	10
2.4.2	Alguns problemas e soluções em instrumentação e controle	13
2.5	**Alguns Problemas Ergonômicos em Salas de Controle de Usinas**	**16**
2.6	**Alguns Números da Interface Homem-Máquina**	**20**
2.7	**Interface Homem-Computador e Automação**	**23**
2.8	**Sistemas Especialistas**	**30**
3	**O ERRO HUMANO**	**34**
3.1	**O que é Erro Humano no Trabalho**	**34**
3.2	**Fontes Básicas de Erros Humanos no Trabalho**	**39**
3.2.1	Fatores influenciadores do desempenho	39
3.2.2	Complexidade da tarefa	41
3.2.3	Abordagem da situação de trabalho	42
3.3	**Análise e Uso dos Dados de Erro**	**42**
3.4	**Estratégia para Lidar com o Erro Humano**	**43**
3.4.1	Trocar o operador	43
3.4.2	Mudar a situação de trabalho	44
3.4.3	Melhorar o lado humano da qualidade	45
3.4.4	Reduzir o impacto no sistema	46

4	**QUANTIFICAÇÃO DO ERRO HUMANO**	**48**
4.1	**Análise da Confiabilidade Humana**	**48**
4.1.1	Experiências no campo da análise da confiabilidade humana	49
4.1.2	Análise e previsão	49
4.1.3	Histórico	51
4.2	**O Problema dos Dados**	**51**
4.2.1	A generalização dos dados	52
4.2.2	Revisão dos dados básicos	54
4.2.3	Banco de dados de confiabilidade humana	55
4.2.4	Tratamento das incertezas pela Teoria dos Conjuntos Nebulosos	56
4.2.5	Tratamento das incertezas com o Teorema de Bayes	57
4.2.6	Tratamento das incertezas utilizando a distribuição lognormal	58
4.3	**Probabilidade de Erro Humano**	**60**
4.3.1	Utilização da HEP	61
4.3.2	Exemplos de utilização de dados de erros humanos	62
4.3.3	Dados de erros humanos pós-acidentes	64
4.3.4	Dados de recuperação	64
4.3.5	Exemplo de utilização de dados de recuperação	65
4.3.6	Dados de fatores influenciadores do desempenho	65
5	**TÉCNICA PARA A PREDIÇÃO DE TAXAS DE ERROS HUMANOS - THERP**	**66**
5.1	**Linhas Gerais da THERP**	**66**
5.2	**Modelando o Desempenho Humano**	**67**
5.3	**Representações Gráficas - Árvores Usadas em APS e ACH**	**68**
5..3.1	Árvore de eventos e árvore de falhas	68
5.3.2	Árvores de eventos THERP	71
5.4	**Dependências em Erros Humanos**	**74**
5.4.1	Dados e níveis de dependência	75
5.4.2	Exemplo de dependência	76
6	**AÇÕES DOS OPERADORES NA SALA DE CONTROLE**	**78**
6.1	**Operadores de Reator**	**78**
6.2	**Tarefas de Monitoramento ou de Vigilância**	**78**
6.3	**Tarefas Complexas**	**79**
6.4	**Outros Fatores Importantes para a Avaliação de Erros de Operadores em Salas de Controle de Usinas Nucleares**	**81**
6.5	**Diagnóstico de Eventos Anormais**	**82**
6.5.1	Modelo de triagem considerando fator tempo	82
6.5.2	Dados referentes ao modelo de triagem	83
6.5.3	Exemplo de triagem	85
6.5.4	Dados referentes ao modelo nominal de estimativas de HEP's	86
6.5.5	Exemplo de aplicação para modelo nominal	91

7	**EXEMPLOS DE APLICAÇÕES PRÁTICAS DA THERP**	**94**
7.1	**Aplicação de Injeção a Alta Pressão para Resfriamento do Núcleo**	**94**
7.2.1	Itemização da seqüência	96
7.2.2	Probabilidade total de falha	98
7.2	**Mudança no Modo de Injeção para Recirculação**	**100**
7.2.1	Análise inicial para a mudança de modo para recirculação	100
7.2.2	Reanálise para a mudança do modo de injeção para recirculação	106
8	**UTILIZAÇÃO DA THERP NA AVALIAÇÃO DA RESPOSTA DOS OPERADORES AO DISPARO DE ALARMES NO REATOR IPR-R1**	**110**
8.1	**O Reator IPR-R1**	**110**
8.1.1	Operação e controle do reator	110
8.1.2	Alterações no reator e na mesa de operações	112
8.1.3	Treinamento e qualificação dos operadores	113
8.2	**Considerações Sobre Segurança na Operação**	**114**
8.2.1	Acidentes e emergência	114
8.2.2	Condições de desligamento	115
8.2.3	Causas do aumento do nível de radioatividade	116
8.3	**Diagnóstico de ENU**	**116**
8.3.1	Condicões para diagnóstico - procedimentos	116
8.3.2	Período de tempo para a realização do diagnóstico	118
8.4	**Comentários Sobre APS e ACH para o Estudo Realizado**	**119**
8.4.1	Abrangência da ACH	119
8.4.2	Considerações sobre o estudo de APS para o reator de pesquisas da Universidade do Novo México para auxiliar na análise do reator IPR-R1	119
8.5	**Dados e Informações**	**120**
8.5.1	Situação considerada para a análise	120
8.5.2	Ações dos operadores após disparo de alarmes	122
8.5.3	Aspectos considerados na coleta de dados e informações	124
8.6	**Aplicação da THERP para o IPR-R1**	**125**
8.6.1	Modelagem e atribuição de valores aos HEP's	126
8.6.2	Modificações nas HEP's	127
8.6.3	Árvore THERP para o caso exemplo	129
8.6.4	Comentários e recomendações relativos ao exemplo apresentado	130
9	**COMENTÁRIOS FINAIS E CONCLUSÕES**	**133**
9.1	**Comentários**	**133**
9.2	**Conclusões**	**135**
	REFERÊNCIAS	**138**
	APÊNDICES	

APÊNDICE A

COMPREENDENDO O CONTEXTO DA SEGURANÇA EM USINAS NUCLEARES **146**

A.1 Segurança de Usinas Nucleares e Licenciamento **146**
A.1.1 Método determinístico adotado para o licenciamento 146
A.1.2 Segurança nuclear, percepção e aceitação de risco 147
A.1.3 Acidentes Além das Bases do Projeto, como critério para segurança 152
A.1.4 Acidentes Severos e condições de segurança numa usina nuclear 152
A.1.5 Defesa em profundidade 153
A.1.6 Avaliação Probabilística de Segurança - APS 155
A.1.7 Aumento da segurança em reatores de nova geração 156
A.2 A Segurança de uma Usina Nuclear e o Gerenciamento de Acidentes **158**
A.2.1 Segurança passiva e ativa de uma usina nuclear 158
A.2.2 Procedimentos operacionais de emergência e gerenciamento de acidentes 160

APÊNDICE B

ESTRESSE **163**

B.1 Generalidades **163**
B.2 Conceitos Relacionados ao Estresse **164**
B.3 A Carga de Trabalho e os Efeitos do Estresse **166**
B.3.1 Níveis de estresse 166
B.4 Respostas dos Operadores **170**
B.5 Estresse de Ameaça **172**
B.6 O Problema dos Dados para o Estresse de Ameaça **173**
B.7 A Regra do Dobro **176**

APENDICE C

TABELAS AUXILIARES **177**

1. INTRODUÇÃO

Para os propósitos da análise de confiabilidade na indústria, é feita uma dissociação entre o homem e a máquina. Entretanto, sem a interação entre estes dois componentes, o sistema como um todo torna-se inoperante.

Em inúmeras situações, o sistema homem-máquina pode ser melhorado. Filosoficamente, a máquina deve ser adaptada ao homem, porque são limitadas as capacidades do ser humano. No entanto, qualquer máquina pode ser aperfeiçoada e desenvolvida, com a utilização de novas tecnologias, até o ponto em que se torna extremamente confiável. Considerando esta situação e sendo inevitável a participação do homem, porque em última análise máquina alguma funciona sem ele, a alta confiabilidade do sistema fica comprometida. Isto porque a confiabilidade do homem é baixa e submetida a variações que dependem de diferentes fatores, difíceis de serem quantificados. Talvez o menos conhecido desses fatores seja o psicológico. Há situações em que a confiabilidade do homem tende a zero, ou seja, ele será a causa de falhas. Mas, mesmo considerando outros fatores, o homem é, atualmente, o fator chave na confiabilidade do sistema. Como a atuação humana pode ser melhorada, menos erros serão cometidos. Assim, a confiabilidade do sistema como um todo poderá ser melhorada.

1.1 Objetivo do Trabalho

Este trabalho foi realizado com a intenção de preencher uma lacuna percebida pelo autor, referente à pouca compreensão, pelos técnicos que trabalham na área de Análise Probabilística de Segurança no CDTN, da interação do elemento humano com sistemas (interface homem-máquina). O trabalho procura apresentar, de maneira bem abrangente, conhecimento necessário para compreensão da Análise da Confiabilidade Humana, principalmente aquele relacionado com instalações nucleares.

Neste trabalho são apresentadas informações sobre a Análise da Confiabilidade Humana aplicada a instalações industriais e em particular às nucleares. Este é um novo campo de estudos, que tem contribuído para que projetistas e engenheiros possam atuar de modo a diminuir erros humanos na operação de sistemas complexos, principalmente industriais.

Muitas informações são fornecidas de maneira que possam ser utilizadas por profissionais que atuam em Avaliação Probabilística de Segurança - APS, como iniciação à Análise da Confiabilidade Humana. Elas permitem compreender alguns fatores menos familiares ao campo das ciências exatas, principalmente aqueles referentes ao comportamento humano, e que devem ser considerados em projetos técnicos, por exemplo, de salas de controle de operação industrial.

Os métodos, modelos, dados e estimativas de probabilidades de erros humanos são apresentados com o propósito de possibilitar a modelagem e fornecer informações necessárias no desenvolvimento da análise da confiabilidade humana como parte de uma APS de instalações nucleares, principalmente usinas nucleoelétricas. Desta

forma, eles poderão auxiliar na tarefa de tornar mais confiáveis alguns sistemas e tornar mais efetiva a disponibilidade ou a confiabilidade operacional de características de segurança de componentes de instalações nucleares.

No trabalho, é ainda discutida a estreita relação da Análise da Confiabilidade Humana com a *interface homem-máquina,* um item que tem sido abordado em sistemas avançados visando a melhoria da segurança. A adoção de instrumentação digital, sistemas de controle avançados, salas de controles com concepção mais moderna e mais funcionais, tornam a ação do operador mais eficaz, tanto em situação normal quanto em casos de distúrbios de operação ou em situações anormais ou de acidentes.

Outro ponto importante também abordado é a tomada de decisão, um dos itens responsáveis pela maioria dos erros humanos na operação de usinas nucleares e de outras instalações. Na tomada de decisão há necessidade do desempenho de ações que demandam a experiência e conhecimentos adquiridos com o tempo, mas cuja incorporação em sistemas automatizados nem sempre são possíveis.

1.2 Organização do Trabalho

No capítulo 2 são discutidas as interrelações do sistema homem-máquina, incluindo considerações sobre fatores humanos em instalações complexas, o que envolve instrumentação e controle, problemas ergonômicos em salas de controle de usinas nucleares, automação e aplicação de sistemas especialistas. A importância quantitativa da atuação humana é evidenciada por estatísticas que confirmam, na maioria das vezes, o seu desempenho insatisfatório, quando confrontado com o desempenho da máquina, principalmente quando se considera a questão da segurança.

No capítulo 3 são apresentadas algumas definições relacionadas com o erro humano, sendo também discutido como se pode lidar com o erro, de maneira a reduzir o seu impacto na operação de sistemas.

No capítulo 4 são apresentadas informações sobre a Análise da Confiabilidade Humana - ACH e considerações sobre dados de erros humanos, exemplos de utilização dos mesmos e fatores influenciadores do desempenho.

No capítulo 5 é apresentada a Técnica para a Previsão de Taxas de Erros Humanos ("Technique for Human Error Rate Prediction - THERP" [1]) , que vem sendo utilizada por muitos analistas. São feitas algumas considerações sobre limitações da técnica, e precauções a serem observadas quando da sua utilização. Recursos gráficos como árvores de eventos, bem como considerações sobre dependência em erros humanos são também apresentados.

No capítulo 6 são discutidas as ações de operadores em salas de controle de instalações complexas, principalmente de usinas nucleares, sendo também apresentados modelos para determinação de probabilidades de ocorrência de erros humanos, com exemplos de aplicação.

No capítulo 7 são desenvolvidos exemplos de aplicação da THERP para facilitar a compreensão desta técnica, relacionados à operação na sala de controle.

No capítulo 8 é desenvolvido um exemplo de aplicação da técnica THERP considerando um item específico da operação do reator Triga IPR-R1, a saber, a resposta dos operadores ao alarme indicativo de aumento do nível de radioatividade. Este reator está localizado no Centro de Desenvolvimento da Tecnologia Nuclear - CDTN, da Comissão Nacional de Energia Nuclear - CNEN.

No capítulo 9 são os apresentadas as conclusões, e feitas considerações sobre as perspectivas da crescente aplicação da ACH.

No Apêndice A é apresentada uma visão geral dos aspectos relacionados com a segurança, considerando a atuação humana em várias situações, incluindo desde o projeto adequado de uma instalação industrial, até as facilidades oferecidas para sua operação. O homem é apresentado como um importante fator de segurança em uma usina nuclear, em decorrência de sua possibilidade de agir, podendo levar a operação a bom termo ou, ao contrário, influir decisivamente na evolução de acidentes, contribuindo negativamente.

No Apêndice B são apresentados e discutidos dados referentes ao estresse, um importante fator influenciador do desempenho humano, principalmente relacionado com a carga de trabalho de operadores.

No Apêndice C são apresentadas algumas tabelas auxiliares, referentes ao Capítulo 7.

2. O SISTEMA HOMEM-MÁQUINA

Em todos os sistemas complexos, o homem é parte essencial de um conjunto maior, porque é ele quem opera, toma decisões, enfim liga e desliga a máquina. Há, portanto, uma interação significativa entre homem e máquina, e é exatamente nesta interface que uma determinada situação pode mudar as condições de operação.

A análise da confiabilidade humana é utilizada, basicamente, para avaliar as ações humanas e os efeitos por elas produzidos em alguns sistemas. Assim, o ser humano pode ser compreendido como parte desse sistema, e sobre o qual tem o poder de agir. Os sistemas podem ser simples, como uma máquina de escrever, ou bem mais complexos, como um avião de grande porte, ou uma usina nuclear. Considerando as usinas nucleares, enfoque deste trabalho, torna-se necessário avaliar o que pode acontecer em decorrência de ações humanas.

2.1 A Contribuição do Homem na Operação e na Segurança de Usinas Nucleares e Outras Instalações Industriais

O homem é a última linha de defesa contra acidentes, com sua flexibilidade e capacidade de pensamento inovador e criativo. Inúmeras vezes a ação corretiva dos operadores de usinas nucleares impediu a ocorrência de acidentes [2]. Essa ação positiva foi decorrência do sucesso na interrupção de um estágio inicial de uma cadeia de eventos que poderia levar à ocorrência de um acidente.

Infelizmente, o inverso também ocorreu, ou seja, operadores cometeram erros e tiveram papel negativo: as conclusões de algumas análises de relatórios de eventos em usinas nucleares nos EUA, indicavam que os erros na operação e manutenção respondiam por 35% do risco de acidentes em geral [2].

Considerando esta situação, torna-se prioritário fazer com que as tarefas das equipes de operação de usinas nucleares contribuam positivamente para a segurança. Isto pode ser feito com uma programação adequada das tarefas, onde se deve perseguir o melhor desempenho dos operadores, tendo em vista a particularidade da sua relação com a máquina. Máquina, neste contexto, é uma generalização de todo um conjunto (ou parte deste conjunto) de instrumentos, equipamentos, componentes, medidores, controladores, computadores e outros dispositivos que fazem parte dos sistemas de operação e controle de uma usina nuclear. Este conceito é extensivo a qualquer outra instalação industrial, nuclear ou não, e a outros sistemas complexos.

Para comparação do impacto humano em falhas de sistemas, é citado em [3] que 50 a 80 % da contribuição para falhas de sistemas de segurança em usinas nucleares se deve ao fator humano, dos quais 63 % contribuem para a freqüência da fusão do núcleo em reatores de potência; na indústria química (dados de 1981) 80 a 90% de todos os incidentes são causados pelo homem; 87 % das causas de acidentes aéreos são atribuídas à falhas humanas (dados de 1985).

Também é reconhecido que, nos acidentes de Three Mile Island - 2 - TMI e de Chernobyl, o erro humano foi o maior contribuinte. Ainda de acordo com [3], a

2. O SISTEMA HOMEM-MÁQUINA

Em todos os sistemas complexos, o homem é parte essencial de um conjunto maior, porque é ele quem opera, toma decisões, enfim liga e desliga a máquina. Há, portanto, uma interação significativa entre homem e máquina, e é exatamente nesta interface que uma determinada situação pode mudar as condições de operação.

A análise da confiabilidade humana é utilizada, basicamente, para avaliar as ações humanas e os efeitos por elas produzidos em alguns sistemas. Assim, o ser humano pode ser compreendido como parte desse sistema, e sobre o qual tem o poder de agir. Os sistemas podem ser simples, como uma máquina de escrever, ou bem mais complexos, como um avião de grande porte, ou uma usina nuclear. Considerando as usinas nucleares, enfoque deste trabalho, torna-se necessário avaliar o que pode acontecer em decorrência de ações humanas.

2.1 A Contribuição do Homem na Operação e na Segurança de Usinas Nucleares e Outras Instalações Industriais

O homem é a última linha de defesa contra acidentes, com sua flexibilidade e capacidade de pensamento inovador e criativo. Inúmeras vezes a ação corretiva dos operadores de usinas nucleares impediu a ocorrência de acidentes [2]. Essa ação positiva foi decorrência do sucesso na interrupção de um estágio inicial de uma cadeia de eventos que poderia levar à ocorrência de um acidente.

Infelizmente, o inverso também ocorreu, ou seja, operadores cometeram erros e tiveram papel negativo: as conclusões de algumas análises de relatórios de eventos em usinas nucleares nos EUA, indicavam que os erros na operação e manutenção respondiam por 35% do risco de acidentes em geral [2].

Considerando esta situação, torna-se prioritário fazer com que as tarefas das equipes de operação de usinas nucleares contribuam positivamente para a segurança. Isto pode ser feito com uma programação adequada das tarefas, onde se deve perseguir o melhor desempenho dos operadores, tendo em vista a particularidade da sua relação com a máquina. Máquina, neste contexto, é uma generalização de todo um conjunto (ou parte deste conjunto) de instrumentos, equipamentos, componentes, medidores, controladores, computadores e outros dispositivos que fazem parte dos sistemas de operação e controle de uma usina nuclear. Este conceito é extensivo a qualquer outra instalação industrial, nuclear ou não, e a outros sistemas complexos.

Para comparação do impacto humano em falhas de sistemas, é citado em [3] que 50 a 80 % da contribuição para falhas de sistemas de segurança em usinas nucleares se deve ao fator humano, dos quais 63 % contribuem para a freqüência da fusão do núcleo em reatores de potência; na indústria química (dados de 1981) 80 a 90% de todos os incidentes são causados pelo homem; 87 % das causas de acidentes aéreos são atribuídas à falhas humanas (dados de 1985).

Também é reconhecido que, nos acidentes de Three Mile Island - 2 - TMI e de Chernobyl, o erro humano foi o maior contribuinte. Ainda de acordo com [3], a

experiência em 29 usinas nucleares francesas revelou que 59 % dos desligamentos foram devidos a ação do homem (dados de 1986).

As pessoas executam bem tarefas que requerem processamento de informação, resolução de problemas e tomada de decisões, mas o mesmo não é verdade para o desempenho de tarefas repetitivas, rotineiras, fatigantes, cansativas e que exijam manter um alto nível de atenção para longo período de tempo. É reconhecida a importância da qualificação psicológica, compreendendo: a rapidez de reação; os padrões de comportamento sob tensão; a capacidade de resolução de conflitos humanos; e a tomada de decisões em situações complexas [2].

Para lidar com tarefas difíceis ou complexas, é necessário que o homem tenha um conhecimento em profundidade, baseado num certo grau de educação ou conhecimento do assunto. Porém, a experiência mostra que pessoas com graduação escolar mais elevada nem sempre apresentam bom desempenho prático na realização de tarefas rotineiras.

É reconhecida a importância do treinamento e retreinamento, em particular usando simuladores. Quanto a este ponto, as referências [4, 5] citam que é uma crença comum entre especialistas em análise de acidentes, que o acidente de TMI não teria ocorrido se os operadores tivessem agido corretamente. A referência [5] e outros documentos consideram que o acidente não teria ocorrido se os operadores tivessem sido adequadamente treinados, fazendo a ressalva, no entanto, de que só o treinamento em simulador não teria capacitado os operadores a reverter os acontecimentos. Ou seja, há um certo limite, que leva em conta as diferenças entre condições reais e condições simuladas, para a qualificação de operadores em treinamento em simulador, conforme discutido no item 4.2.1 deste trabalho. É necessário complementar o treinamento em simuladores com treinamento em condições reais de operação, em sala de controle.

Também foi observado que pessoas muito bem treinadas e qualificadas algumas vezes cometem erros em situações relativamente simples. Em geral, o problema principal parece ser o de restringir o livre-arbítrio do ser humano sem destruir sua auto-estima, iniciativa e criatividade. O aumento do número de instruções e procedimentos detalhados resulta num desempenho mais mecânico de tarefas, que por sua vez diminuem o incentivo de pensar.

Podem ser citadas como as principais causas de erros humanos: a falta de cuidado ou de atenção; a circulação de informações inadequadas, sejam elas recebidas ou fornecidas (emitidas); e problemas de comunicação homem-homem (esta interface é mais problemática que a interface homem-máquina). A maioria dos erros ocorre durante os reparos e na manutenção, e em menor escala durante a operação [2]. Isso mostra a importância do gerenciamento e dos procedimentos, os quais são importantes também na detecção e correção de qualquer violação da operação. Para evitar os erros humanos, os seguintes pontos chaves são salientados: a boa gerência; a contínua monitoração de desempenho; o aprendizado com a experiência; o treinamento e retreinamento; o fornecimento de informações adequadas. O projeto tolerante a erros diminui a probabilidade de propagação de erros, contribuindo também para diminuir a proporção de erros humanos.

Ao se considerar as principais causas de erros humanos, alguns itens prioritários evidenciam-se para melhorar a qualidade do projeto da instalação, levando em conta os pontos fortes e fracos da ação humana [2]. Pela literatura disponível [1, 2],

percebe-se que muito esforço foi gasto em desenvolver critérios pelos quais se avalia a segurança de projeto de instalações contra acidentes, em relação à falha de equipamentos. Porém, um critério similar ainda não está adequadamente desenvolvido para a avaliação da segurança do projeto contra acidentes originados por erro humano. Critérios usados em alguns países incluem, por exemplo, o desencadear automático de certas funções de segurança, não sendo exigida nenhuma ação do operador no prazo de trinta minutos [2]. Estes critérios incluem alguma tolerância para certas operações incorretas do operador.

Em [6] é reconhecida a importância da influência do comportamento humano na gerência da segurança, dada a sua relação direta com possíveis erros humanos. É enfatizada nesta referência a necessidade de reduzir ao máximo possível a ocorrência de erros que afetem a segurança. Desta forma, os efeitos desses erros devem ser eliminados ou mitigados, quando possível e praticável, por uma abordagem sistemática, de maneira a alcançar uma alta tolerância aos erros humanos em instalações nucleares. Adicionalmente, exigências funcionais e qualificações devem ser definidas e alcançadas, dentro de uma meta estabelecida, através da seleção e treinamento do pessoal que trabalha nessas instalações.

Por outro lado, os operadores devem ser auxiliados a cumprir bem os requisitos do seu papel, através do melhoramento de seu desempenho. Desta forma, muitos melhoramentos têm sido feitos (ou estão em desenvolvimento) no sentido de informar ao operador, com dados mais adequados, a condição da instalação. Este seria um modo de fornecer um aviso precoce de ocorrências anormais logo no início, o que poderia ajudar ao operador no diagnóstico das causas e na determinação de ações corretivas. É previsível, portanto, que ocorra uma maior automação para operações normais e, também, para condições de distúrbios (ver itens 2.7 e 2.8). No Apêndice A são fornecidas informações complementares sobre as ações humanas, relacionadas com a segurança na operação de instalações complexas.

2.2 Principais Definições

O termo *Sistema Homem-Máquina* se refere a um sistema no qual as pessoas têm uma função de monitoração ou de operação. Quanto *à Interface Homem-Máquina*, refere-se a pontos de interação entre as pessoas e o sistema. Dessa forma, um *mostrador*, um *controle*, um *material escrito*, ou qualquer outro item que a pessoa usa ou observa é uma *interface* entre o homem e a máquina. É citado em [2] que "a interface homem-máquina pode ser vista como um conceito geral desenvolvido relativamente ao trabalho compartilhado entre o homem e a máquina, considerando as características de cada um e suas diferenças".

O termo *Fatores Humanos* refere-se à disciplina que se ocupa com o projeto de máquinas, com sua operação e o ambiente de trabalho, de tal forma que sejam adequados às capacidades e limites do homem. Este termo, muito usado nos EUA (Estados Unidos da América), é o que se convencionou chamar de Ergonomia em outros países, inclusive no Brasil. Também é usado o termo *Engenharia Humana*, embora em menor escala, com o mesmo significado. Note-se que a antítese desta disciplina é a tentativa de adaptar o homem à máquina, ou ao ambiente.

Confiabilidade é a antítese da probabilidade de erro: é a probabilidade que nenhum erro ocorra. É a probabilidade de desempenho, com sucesso, de uma missão ou

tarefa. Observa-se que o termo, aqui, não é usado à maneira de psicólogos, para denotar consistência ou repetibilidade de algumas medidas do desempenho humano - é probabilidade.

A referência [1] cita algumas definições de confiabilidade humana, que vem sendo aprimorada com o estudo da matéria. Define-se *confiabilidade humana* como a *probabilidade* de desempenho, com sucesso, de uma atividade humana necessária, seja para a *confiabilidade* ou para a *disponibilidade*, de um sistema. Ou seja, é a probabilidade de desempenho de uma ação humana exigida para que um sistema funcione satisfatoriamente, dentro de algumas condições (por exemplo, em um determinado período de tempo). Disponibilidade é a probabilidade um sistema ou componente estar disponível para uso, quando necessário.

Também se define a confiabilidade humana como a "probabilidade de que um trabalho ou tarefa seja completado com sucesso pelo pessoal em qualquer estágio requerido na operação de um sistema, dentro de um período mínimo de tempo exigido (se existe esta exigência)".

Numa concepção mais atual, de Swain e Guttmann [1], confiabilidade humana é definida como a probabilidade de que uma pessoa desempenhe corretamente alguma atividade requerida pelo sistema num período de tempo exigido (se o tempo é um fator limitante), e não desempenhe atividades estranhas que possam degradar o sistema.

2.3 Fatores Humanos em Instalações Complexas

Numa comparação entre documentos mais antigos e mais recentes, é possível confirmar-se a expectativa de desenvolvimento da automação em sistemas complexos e sua relação com os fatores humanos. Na referência [7], é discutida a situação existente em salas de controle, considerando principalmente o seu projeto, em instalações nucleares. Entre outros argumentos, é ponderado que existe pouca compreensão do impacto causado pela tecnologia do computador no campo dos fatores humanos, ou seja, como seria a interação entre o homem e sistemas automatizados. Embora esta situação tenha se modificado um pouco desde então (1985), prevê-se ainda muita pesquisa a ser desenvolvida para a real compreensão deste impacto.

Em [7] é feita uma breve analogia da indústria nuclear com a aeronáutica, tendo em vista os aviões usados comercialmente para transporte de passageiros. A perspectiva de então (1985) era de que a automação seria crescente, provavelmente atingindo um certo ponto em que seria limitada pela capacidade humana, já que, atualmente, ainda é inconcebível um sistema totalmente automatizado, que não necessite em absoluto da atuação ou monitoração do homem. Esta afirmativa é valida tanto para aeronaves quanto para outros sistemas onde a complexidade é grande, como em usinas nucleares.

Atualmente, quase todos os vôos operacionais são controlados automaticamente [8], desde o final da decolagem até a aproximação final do avião a seu destino, mantendo-se a tripulação mínima de duas pessoas, piloto e co-piloto. Nota-se em [7] a preocupação do "Federal Aviation Administration" (órgão com responsabilidades relacionadas à aeronáutica e ao tráfego aéreo nos EUA) relativamente à automatização de aeronaves: com a crescente automatização dos aviões, existe a possibilidade de que os

pilotos destes aviões não correspondam ao que se poderia exigir deles, quando solicitados em casos de emergências.

Esta preocupação não se revelou infundada, pois uma série de acidentes em aviões comerciais europeus de última geração confirmaram a necessidade de se considerar um limite para a automatização. Segundo os meios de comunicação, como, por exemplo o artigo do periódico "Veja" de maio de 1990 [8], e ISTOÉ SENHOR [9] de janeiro de 1992, os acidentes com o avião Airbus A300 ocorrido em 1988, em fevereiro de 1990 (na Índia) e em janeiro de 1992, (na França), trouxeram à tona uma grande discussão sobre o assunto. De acordo com [8], a rigorosa "Federal Aviation Administration" está investigando a hipótese de que a moderna tecnologia possa estar criando inadvertidamente uma nova forma de derrubar aviões, a dos erros dos computadores de bordo. No caso do Airbus A300, investigações paralelas levantaram suspeitas de que talvez as causas das quedas pudessem ser atribuídas ou pelo menos divididas com um equipamento crucial do avião - o sistema automático de controle de aceleração, que comanda a velocidade da aeronave e, portanto, sua capacidade de continuar voando. Suspeita-se que este dispositivo, inteiramente controlado por computadores no Airbus A320, possa sofrer interferências de fontes de radiação insuspeitadas, como, por exemplo, a fiação de alta-tensão de postes próximos à pista. Nos dois primeiros acidentes com o Airbus A320, os aviões caíram quando se preparavam para pousar, voando rente ao chão [9].

Os pontos fracos do Airbus A320 já teriam sido objeto de destaque e crítica de aviadores franceses que o pilotam desde o seu lançamento, conforme [9]. Até 1992, este avião, fabricado pelo consórcio franco-alemão "Airbus Industry", era a única aeronave comercial a dispor da tecnologia que permite que um conjunto de computadores seja capaz de operar todos os controles de vôo. Especialistas alegavam, em 1992, que, por causa desses recursos de informática e automação, o aparelho reduzia de forma perigosa a margem de manobra do piloto. Atualmente, outros aviões dispõem de sistemas automatizados para muitas das operações dos pilotos, mas a discução ainda persiste, sobre até que ponto a automatização não prejudica o desempenho do piloto, relativamente à segurança [9].

Ainda como comparação, em [7] o autor considera a possibilidade de que o painel de controle dos aviões comerciais, automatizados no máximo, pudesse ser o modelo dos protótipos para as salas de controle de instalações nucleares, no futuro.

Na indústria, sempre ocorreu o intercâmbio de tecnologias de diferentes áreas. A expectativa de [7], no sentido de uma automação ao máximo, dos sistemas de controles de instalações nucleares, notadamente para usinas geradoras de energia, vem se realizando. Também na indústria nuclear se admite um limite para a automação. Em julho de 1990 foi realizado em Munique um simpósio sobre o balanceamento da automação e ações humanas em instalações nucleares [10]. Neste simpósio, foi ressaltado que o desenvolvimento cada vez mais rápido de equipamentos eletrônicos, pode levar a uma ampla automação nos controles de usinas nucleares. A questão considerada essencial foi o grau adequado desta automação, levando em conta a confiabilidade do sistema, bem como aspectos ergonômicos e psicológicos do lado humano [10]. Na referência, ressalta-se o potencial para o uso de sistemas especialistas, o desenvolvimento de um analisador de instalações ["plant analyser"], e uma sala de controle de testes. Este último equipamento é considerado um passo a mais na direção da simulação completa de uma

usina nuclear em computador. Inclui a possibilidade de intervenção humana e a apresentação de dados da instalação, similar à dos projetos de painéis de salas de controle avançados. Com esta ferramenta, não somente os fenômenos durante transientes complexos, mas também a resposta de todo o sistema à intervenção humana no gerenciamento de acidentes, pode ser estudada e analisada.

O grau de automação está aumentando, indiscutivelmente, devido a fatores técnicos e sociais, e como resultado da tecnologia da informação. Por exemplo, em usinas nucleares deve-se decidir o nível adequado de automação, e então estabelecer as tarefas e funções para o homem e para a máquina, ou para uma combinação dos dois. É importante que a automação seja realizada de uma maneira suficientemente sistemática.

Alguns problemas práticos estão relacionados com as capacidades humanas, que permanecem substancialmente as mesmas, no decorrer do tempo, enquanto que os avanços na tecnologia resultam em mudanças rápidas, no que pode ser esperado da máquina. Um grande problema é que esta abordagem sugere uma separação de tarefas entre estes dois componentes, homem ou máquina, enquanto que, num moderno sistema homem-máquina, a necessidade é assegurar o trabalho complementar. O desafio para a engenharia de fatores humanos da indústria nuclear é produzir um sistema de operação homem-máquina que otimize os respectivos papéis do operador e do sistema semi-automático, de tal forma que possam funcionar em sintonia (ver itens 2.6 e 2.7).

2.4 Instrumentação e Controle

Na sala de controle de uma usina nuclear, a ação do operador corresponde à realização de uma ou mais atividades, indicada pelo diagnóstico de uma situação, por regras operacionais ou procedimentos escritos. Os controles manuais são os realizados pelos operadores ao atuar no sistema, através de conectores, ferramentas, botões, comutadores, válvulas operadas manualmente, teclados de computadores e outros.

Em geral, as ações dos operadores, quando estes não estão condicionados a seguir os passos de um procedimento, se tornam necessárias a partir de informações recebidas. Tais informações são dados que se apresentam ao homem, via seus órgãos sensitivos (visual, auditivo, etc.). Essas informações são dadas por diferentes instrumentos, em geral conhecidos por *mostradores*, em decorrência da predominância do sentido visual. Existem também os dispositivos adequados aos órgãos auditivos. Em alguns alarmes, os dispositivos são concomitantemente visuais e auditivos. Embora os outros sentidos ainda sejam negligenciados, funcionam auxiliarmente, não sendo de modo algum desprezíveis, quando se considera a sua contribuição na detecção de problemas. Por exemplo, o cheiro de algo queimando, a sensação de vibração ou calor, e a percepção decorrente do tato. Todos os sentidos do ser humano contribuem para que ele adquira maior conhecimento da situação e do meio em que se encontra. Os sentidos são, portanto, as entradas ("inputs") no sistema humano. Dito de outra forma, as entradas no sistema homem são os *estímulos*, terminologia da psicologia comportamental [11], que ativam *processos mediadores internos*, que geram as *respostas* ou saídas ("outputs") do sistema humano, que são, por sua vez, as entradas no sistema máquina.

A Figura 2.4-1, adaptada de [12], ilustra simplificadamente esse modelo de funcionamento, onde os termos *entrada* e *saída* são usados, neste trabalho, no lugar de estímulo e resposta usualmente utilizados em psicologia, de forma a homogeneizar a

terminologia. Apresenta-se também a linha de retroalimentação, ou seja, os resultados de alguma ação em particular fornecem informações que podem ser transformadas em dados, e assim funcionam como entradas adicionais ou complementares.

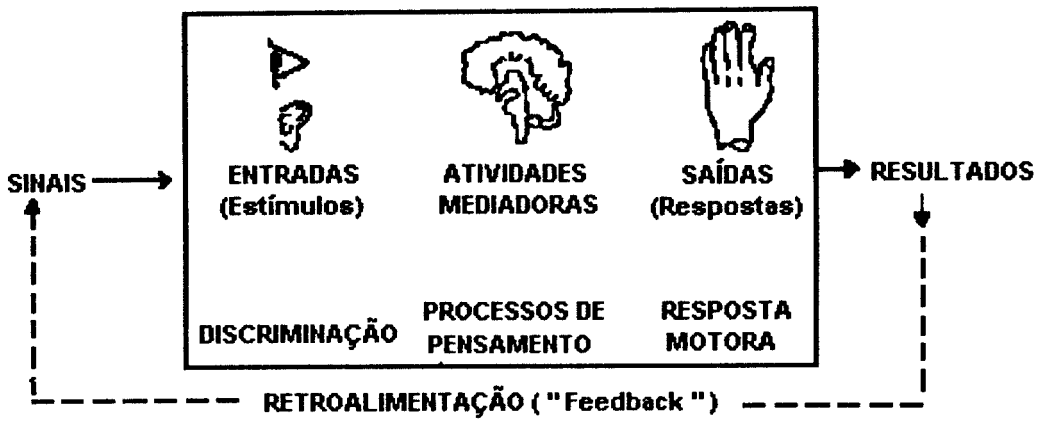


Figura 2.4-1 - Modelo de entradas (estímulos) e saídas (respostas) do sistema homem

2.4.1 Exemplos de controles na interação homem-máquina

Vários tipos de controles são utilizados em instalações industriais, abrangendo instalações radioativas e usinas nucleares. Por exemplo, controles manuais apresentam-se em diferentes formatos, tamanhos, texturas e cores. A diferença é para facilitar a percepção do tipo de controle e a função a que se destina, obviamente facilitando a operação de qualquer sistema, em um projeto bem realizado. Como a visão é a percepção mais requisitada, diferentes tipos e formatos de controles facilitam pistas táteis, quando, por exemplo, existe uma sobrecarga em mostradores que são utilizados na monitoração de diferentes parâmetros, que dificulta o acionamento inadequado. A Figura 2.4-2 apresenta controles do tipo botões de pressão, de concepção relativamente recente.

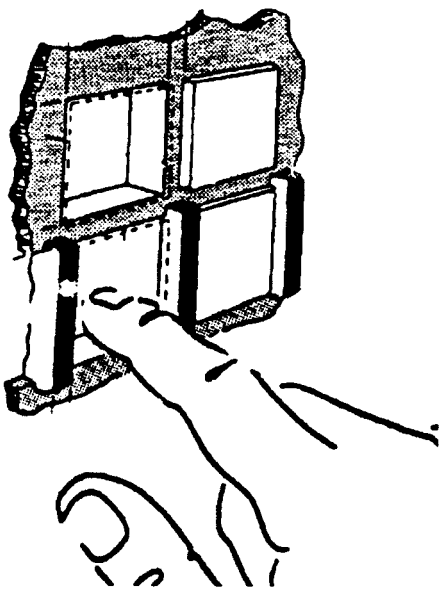


Figura 2.4-2 - Controle por pressão ("Pushbutton") [13]

Este tipo de controle continua, atualmente, ainda muito utilizado, compondo grandes painéis. Alguns desses tipos de controles podem também estar associados a sinais visuais e/ou auditivos intermitentes, de acordo com uma determinada freqüência. A freqüência de emissão destes sinais pode estar associada a um evento em particular. Por exemplo, baixa freqüência pode indicar o início de alguma situação não usual, enquanto que a alta freqüência pode indicar uma situação de emergência (alarme). Tais tipos de controle, associados a sinais visuais ou auditivos, também são conhecidos como anunciadores.

Controles mais modernos são, por exemplo, os Sistemas Digitais de Controle Distribuido (SDCD), Controles Lógicos Programáveis (CLP) e Controles Adaptativos, que adotam a informatização em graus variados. A influência desse tipo de controle e instrumentação e quais as suas conseqüências, por exemplo, em taxas de erros humanos, ainda não são bem conhecidas no campo da ACH. Os CLP's, por exemplo, são microcomputadores de controle especializados em lidar com variáveis digitais. Embora apresentem inúmeras vantagens, como elevada disponibilidade e facilidade de auto diagnóstico contínuo, oferecem também alguma dificuldade, por exemplo, para utilização em sistemas de segurança. Em [14], é feita uma proposta de utilização de CLP em funções de segurança e proteção de reatores nucleares. O autor cita que os sistemas que envolvem funções associadas à segurança de reatores nucleares, como intertravamento e proteção, têm feito uso de tecnologias baseadas em relés, em decorrência de sua alta confiabilidade e simplicidade. Equipamentos de complexidade bem maior, como o CLP, não têm condições de seguir o princípio de falha segura (quando o estado que o componente assume enquanto falho é previsível e seguro). Não é possível, por exemplo, prever em qual estado ficarão os barramentos de um microprocessador, que é o elemento básico do CLP, após a ocorrência de uma falha. Entretanto, é possível a sua utilização, tomando-se alguns cuidados [14]. Dados sobre a utilização de CLP em aplicações na área nuclear não são disponíveis, embora existam no Brasil inúmeros exemplos de aplicações de CLP em funções de intertravamento e de proteção de sistemas industriais perigosos, o que caracteriza a existência de conhecimento tecnológico neste campo.

A Figura 2.4-3, apresenta esquematicamente alguns tipos de controle de rotação (botões de girar e comutadores) para diferentes ações.

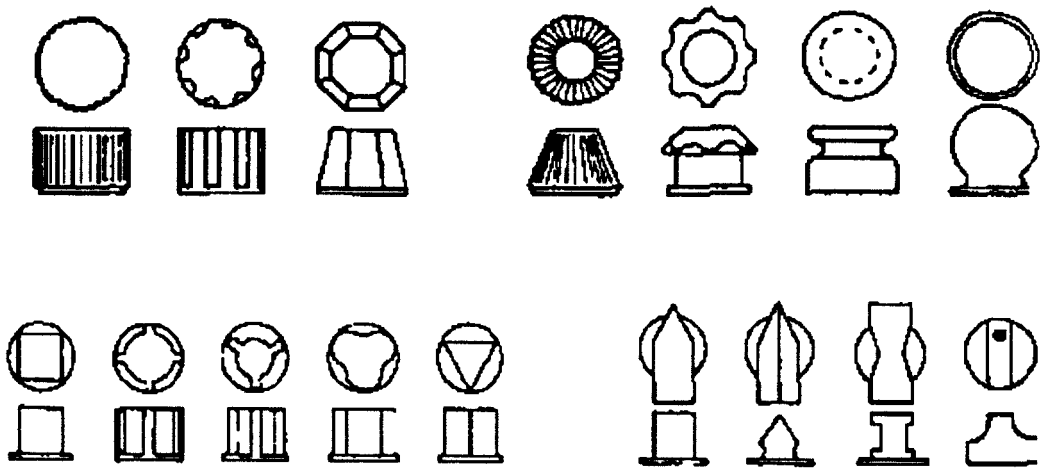


Figura 2.4-3 - Representação de diferentes tipos de controles de rotação [13]

A distinção entre a aparência e o toque torna mais difícil uma confusão entre eles. Diferentes controles são usados para diferentes propósitos: rotação múltipla, rotação fracionada e posicionamento específico (comutadores ou chaves de posição). Estes tipos de controles também são conhecidos por controles manuais contínuos, que podem ser ajustados para qualquer ponto dentro de sua faixa (como o potenciômetro), ou controles manuais discretos, os quais têm um número fixo de posições (ver exemplo no item 7.2).

As Figuras 2.4-4 e 2.4-5, apresentam alguns tipos de proteção de controles. Na Figura 2.4-4 é apresentado um controle de rotação protegido por uma moldura, o que impede o botão de girar, e na Figura 2.4-5 uma cobertura de plástico transparente, que impede o acesso não intencional ao controle. Somente retirando as proteções é possível acionar os controles.

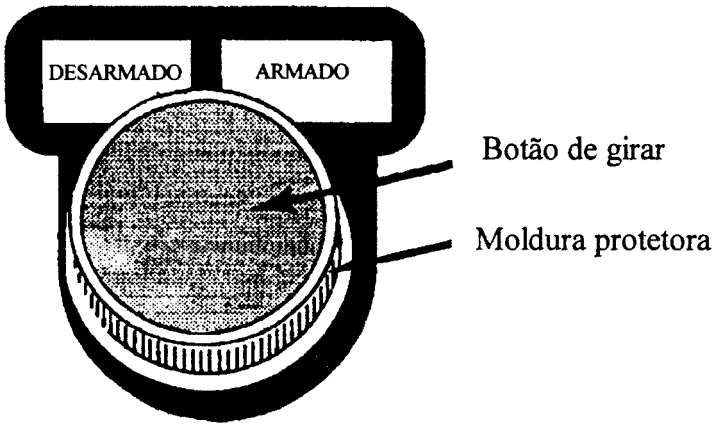


Figura 2.4-4 - Controle protegido por moldura (arma/desarma) [13]

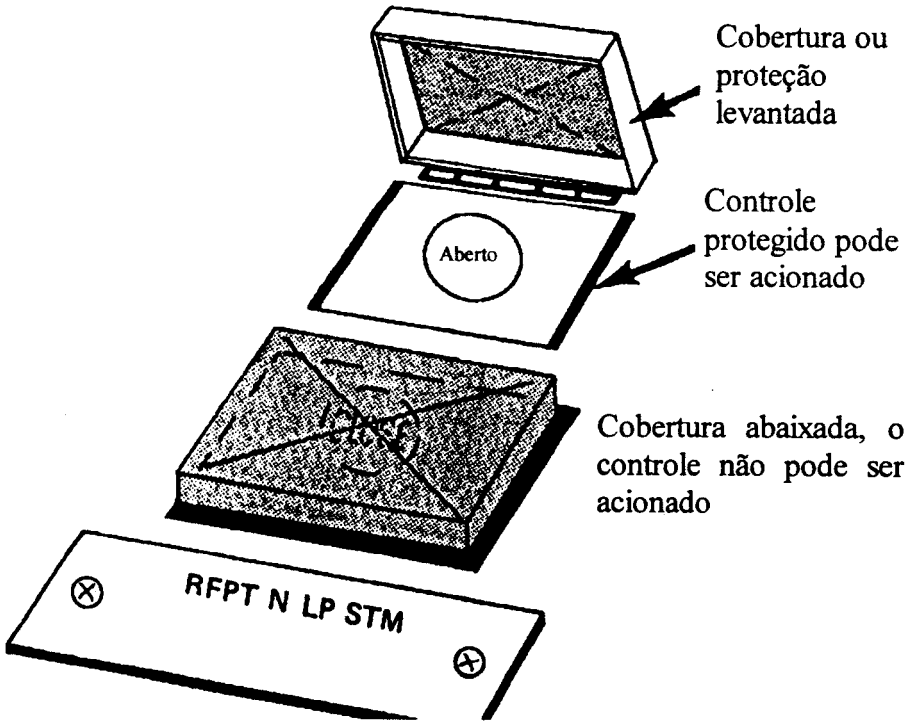


Figura 2.4-5 - Controle protegido por cobertura móvel [13]

2.4.2 Alguns problemas e soluções em instrumentação e controle

Existem instrumentos, ainda utilizados em usinas nucleares e outras indústrias, cuja leitura não é em unidades utilizadas pelo operador. Assim, alguns parâmetros (em gráficos, por exemplo) necessitam ser multiplicados por um determinado fator, conforme o mostrador, para converter as leituras em informações utilizáveis. A possibilidade de erro no desempenho de operações aritméticas é bem alta, e a exigência deste tipo de tarefa deve ser evitada sempre que possível, através de leituras diretas, nas unidades desejáveis. Um exemplo disso pode ser um instrumento que fornece indicações em Roentgen (unidade de radiação), sendo que, de fato, o operador necessita de dados de doses na unidade Sievert. Neste caso, o operador deverá fazer uma operação aritmética, (multiplicação) que pode comprometer resultados, ou seja, algum erro pode ocorrer, ao passo que um instrumento com leitura direta evitaria o mesmo.

Em [15], foi observado que existem instalações que apresentam medidores com diferentes escalas, em um mesmo sub-painel, comprometendo a leitura correta e a interpretação sem erro do operador. Não sendo o intervalo da escala o mesmo que dos outros medidores, as medidas poderão ser comprometidas.

Na Figura 2.4-6, são apresentadas válvulas não rotuladas, encontradas em uma usina nuclear. Estas válvulas não identificadas adequadamente podem ocasionar erros no acionamento de uma em lugar de outra, principalmente se localizadas muito próximas. Estas válvulas não se encontram nas salas de controle, mas fazem parte do equipamento que deve ser manuseado.

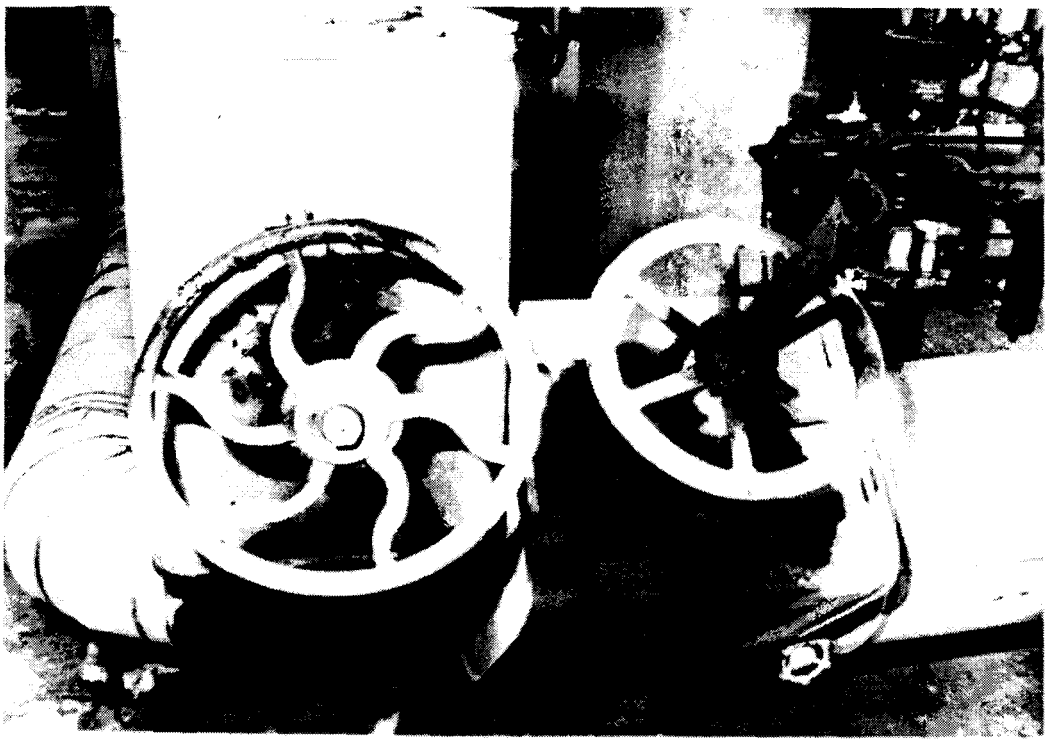


Figura 2.4-6 - Válvulas não rotuladas, dificultando a identificação e facilitando acionamento errado [15]

A Figura 2.4-7 apresenta alguns controles cobertos por uma proteção de plástico, ou seja, que só permite acionamento se essa proteção é retirada. A adoção dessa cobertura para o conjunto dos controles aparentemente resultou de atuações acidentais de um deles. Em outras instalações, analisadas na mesma época, não foram observados dispositivos protetores similares, embora em alguns casos alguns controles, individualmente, estivessem protegidos.

Controles que devem ser pressionados, a não ser que estejam protegidos contra acionamento acidental, são freqüentemente vulneráveis. É altamente provável que um acionamento acidental tenha ocorrido em outras instalações similares, muito embora não tenham sido adotadas medidas corretivas como a apresentada na Figura 2.4-7.

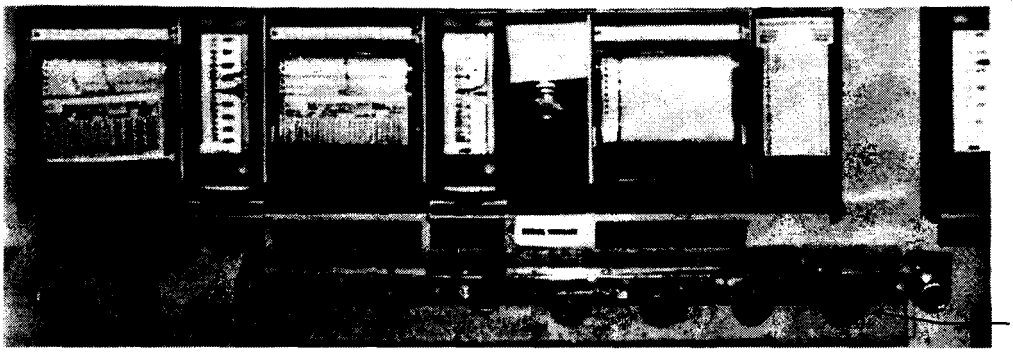


Figura 2.4-7 - Controles protegidos por plástico, para evitar acionamento indevido [15]

A Figura 2.4-8 apresenta informações adicionais incluídas em um painel pelos operadores, para facilitar a visualização do que deve ser feito, ou seja, classificar a operação ou o significado das leituras de alguns mostradores. Estas pequenas alterações tendem a favorecer a ação correta.

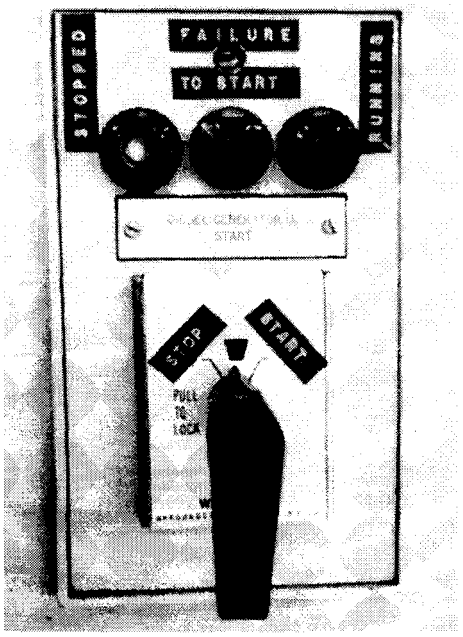


Figura 2.4-8 - Etiquetas colocadas pelos operadores, para facilitar a visualização e ações indicadas [16]

Na Figura 2.4-9 ilustra-se a grande quantidade de controles, que não estão dispostos em sub-painéis claramente identificáveis, controlando elementos relacionados entre si. A semelhança dos controles pode induzir a erros de operação.

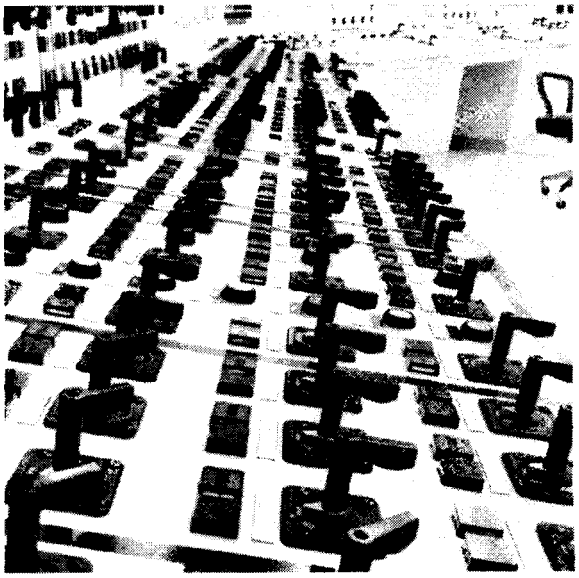


Figura 2.4-9 - Grande quantidade de controles, dificultando a identificação e conseqüente manuseio [16]

Na Figura 2.4-10, apresentam-se duas configurações, a original e a modificada, de um grupo de controles.

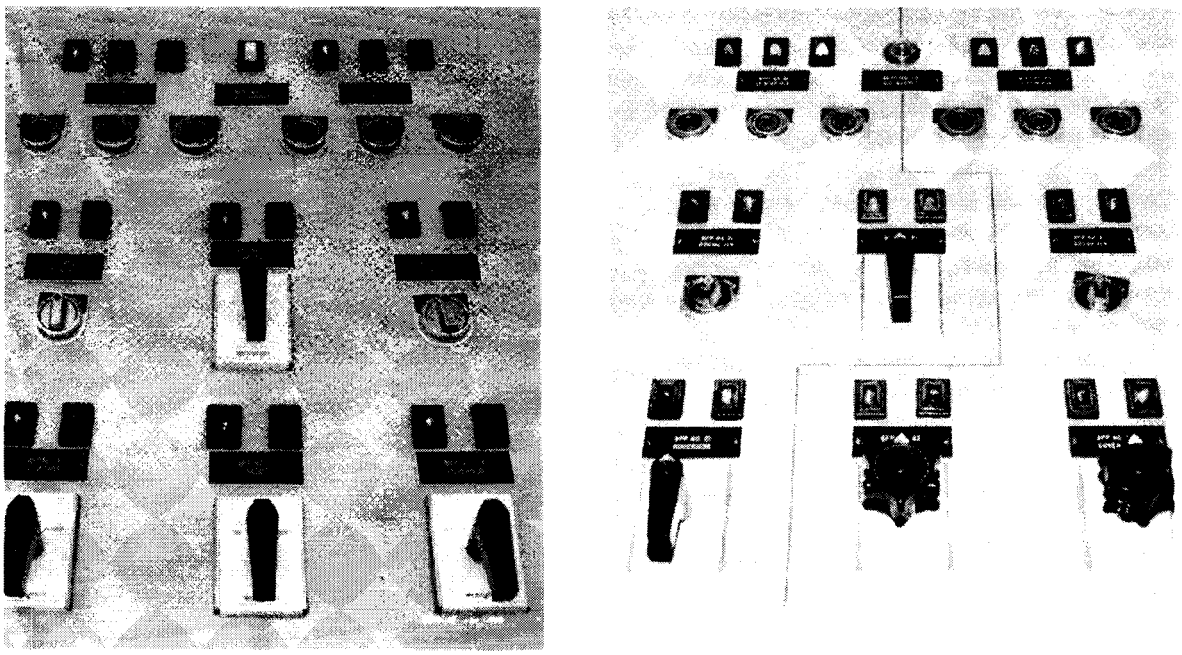


Figura 2.4-10 - Configuração original e modificada [16]

Esta modificação foi decorrente de manipulação anterior incorreta, que causou o desligamento do reator, sendo que posteriormente, foi mudada a configuração. A linha de demarcação separa controles com funções diferentes, e os comutadores foram

substituídos por outros de formato diferente, facilitando a identificação ou comparação pelo tato.

Na atualidade, existem controle mais modernos, principalmente os projetados com assistência da informática, como controles digitais e instrumentação digital. A automação, via informatização das salas de controle e operação, trouxe muitas vantagens para os operadores, principalmente quanto à possibilidade de facilitar suas tarefas. A interface homem-computador, como pode ser verificado no item 2.6 adiante, vem sendo sistematicamente estudada. No entanto, deve-se ressaltar que todos os tipos de controle aqui apresentados ainda são usados, e ainda serão usados por algum tempo, apesar da presença de controles informatizados.

2.5 Alguns Problemas Ergonômicos em Salas de Controle de Usinas

O principal objetivo geral do estudo [13] é fornecer dados ergométricos gerais para serem utilizados em projetos conceituais. O objetivo da aplicação de princípios ergométricos, é minimizar a ocorrência de operação inadequada de controles, de instrumentos, de manuseio de equipamentos e instalações quando da ocorrência de manutenção, em salas de controle. Este documento foi baseado em trabalhos desenvolvidos na área de fatores humanos em usinas nucleares, tais como o de Seminara e outros [16], de 1977. Não obstante estar, em parte, obsoleto, deve ser considerado que a vida útil de uma usina nuclear pode ultrapassar os trinta anos, e que muitas das situações apresentadas foram modificadas, à luz dos resultados dos estudos realizados. É o caso, por exemplo, de substituição de equipamentos e instrumentos aproveitando novas concepções, como técnicas avançadas de computação e novos dispositivos de controle. Esses trabalhos deram origem a grandes modificações dos projetos conceituais de novas salas de controle de usinas nucleares, ao apresentar soluções baseadas em problemas e adaptações reais adotadas durante o trabalho dos operadores.

As Figuras 2.5-1 a 2.5-5 [16] apresentam algumas das situações encontradas. Em linhas gerais, os autores constataram inúmeras inadequações, improvisações, deficiências generalizadas nos controles e instrumentos utilizados, além de situações de trabalho que não poderiam ser consideradas adequadas às tarefas dos operadores. Embora muitas das soluções encontradas fossem consideradas boas adaptações, para facilitar o trabalho do pessoal e melhorar os níveis de segurança, estas improvisações não deveriam se repetir em futuras salas de controle de usinas. Dessa forma, inúmeros equipamentos e instrumentos obsoletos serão substituídos, em usinas atualmente em operação, e equipamentos mais sofisticados, mais modernos e de concepção mais avançada, deverão ser considerados no projeto de futuras instalações.

A Figura 2.5-1 apresenta uma situação inadequada, onde a mesa do operador está situada de forma que ele fica de costas para os controles, obviamente dificultando a visualização de instrumentos, mostradores, medidores, induzindo também à falta de atenção. Note-se que, na figura, grandes painéis de controle poderiam ser visualizados, se a posição da mesa fosse invertida. Para este caso específico, a mudança seria positiva, já que na situação real não se apresentavam controles importantes em frente ao operador, para justificar a posição da mesa. As outras figuras, apresentadas seqüencialmente, apresentam situações variadas, que dificultam ou facilitam a ação dos

operadores. De modo geral, representam a realidade encontrada na situação de trabalho em usinas nucleares no final da década de 1970. Atualmente, a tentativa é de concentrar todos os instrumentos no campo de visão do operador, eliminando ou simplificando ao máximo as informações consideradas não essenciais.

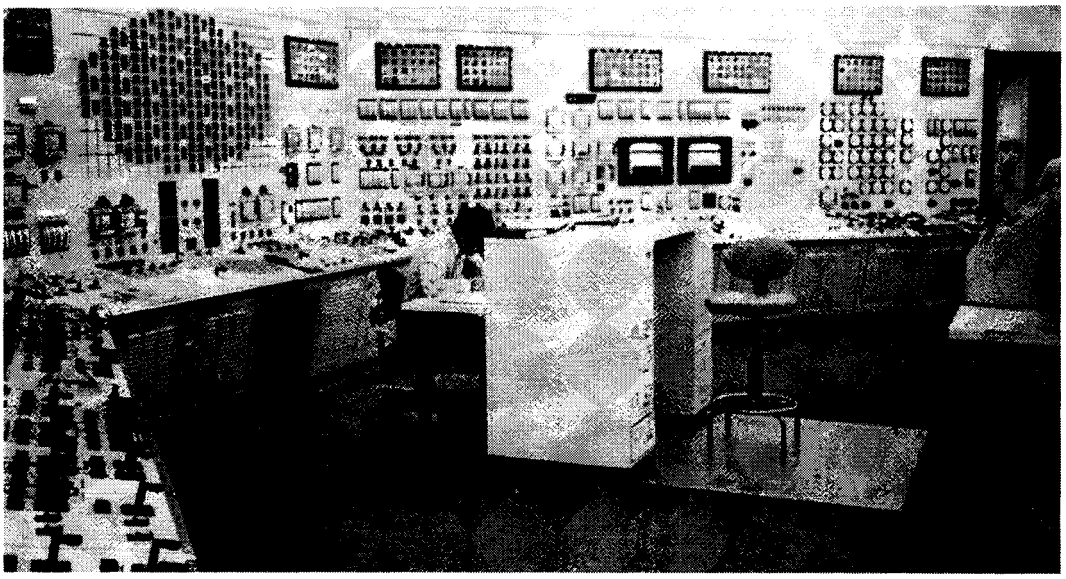


Figura 2.5-1 - Situação inadequada do operador em uma sala de controle [16]

A figura 2.5-2 apresenta a situação improvisada de um operador trocando a lâmpada de um anunciador, que se encontra numa posição alta e difícil de alcançar.

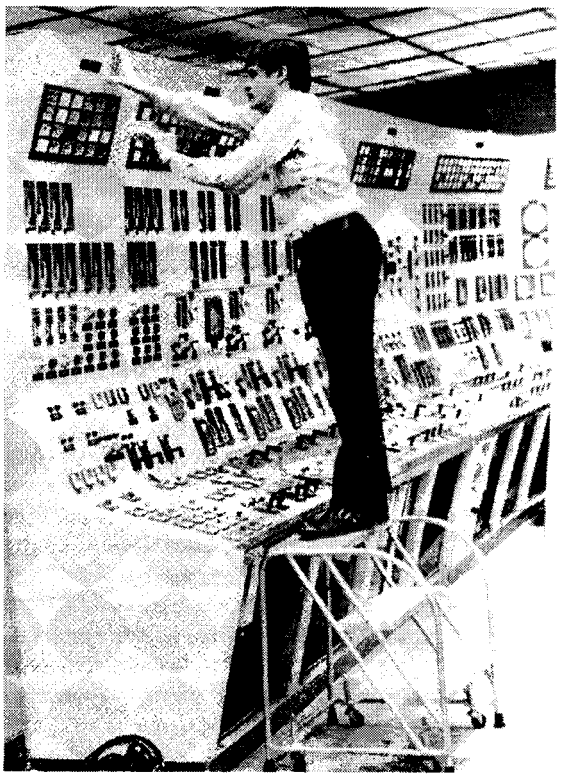


Figura 2.5-2 - Dificuldade de alcançar a lâmpada dos anunciadores [16]

A adaptação utilizada, no caso, não é uma boa medida ergonômica, pois o carrinho utilizado é inadequado para cumprir a função de apoio. Nota-se que o mesmo possui rodas, o que tende a causar acidente de queda do operador, se algum desequilíbrio ocorrer, por exemplo, se uma das lâmpadas cair e ele tentar recuperá-la.

As figuras 2.5-3 e 2.5-4 apresentam duas situações que dificultam as ações dos operadores em questão, de monitorar e agir. No primeiro caso, os monitores estão a uma altura de aproximadamente quatro metros do solo, dificultando a leitura.

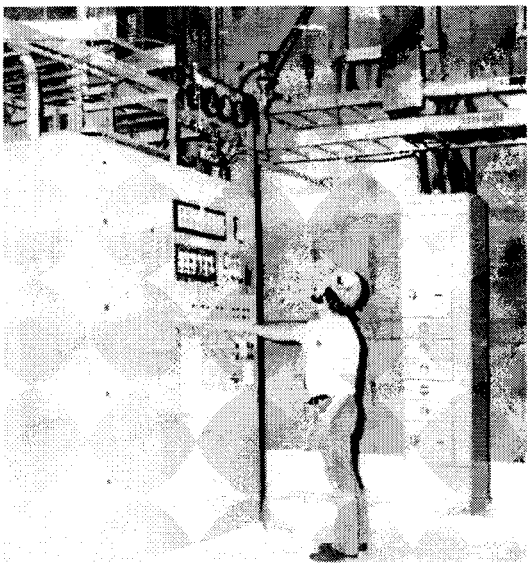


Figura 2.5-3 - Operador monitorando medidores situados numa posição muito alta [16]

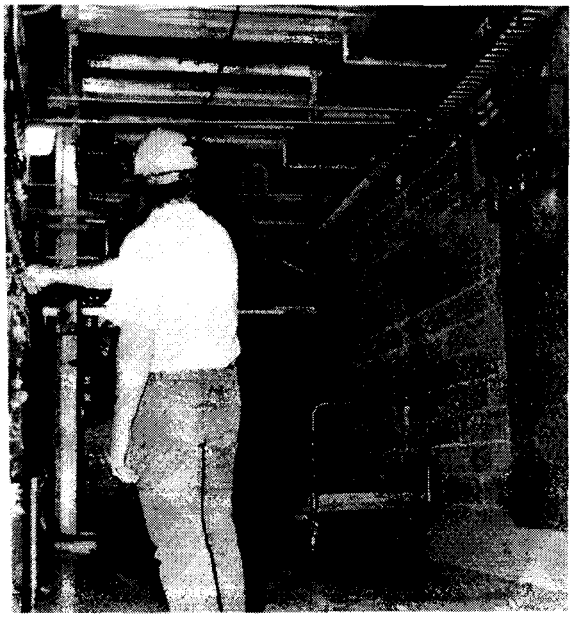


Figura 2.5-4 - Controle e operação em painéis opostos, facilitando erros de acionamento de controles [16]

No segundo caso, o operador olha um monitor situado em posição oposta aos controles que deve acionar, ou seja, estão em painéis opostos. No projeto de tais

controles, nem sempre é possível evitar situações como esta, mas não é, obviamente, a situação ideal para o operador.

A Figura 2.5-5 apresenta uma boa solução ergonômica, ao se usar um carrinho de mão tanto para estoque de procedimentos quanto para uma base para o manuseio dos mesmos, não interferindo em qualquer controle da mesa de operação.

Figura 2.5-5 - Boa solução ergonômica, com procedimento transportado por carrinho de mão [16]

A Figura 2.5-6 apresenta um croquis de um novo conceito de sala de controle, ou seja, assimilação de novos e mais eficientes painéis, instrumentos, e equipamentos, em um arranjo que leva em conta fatores ergométricos.

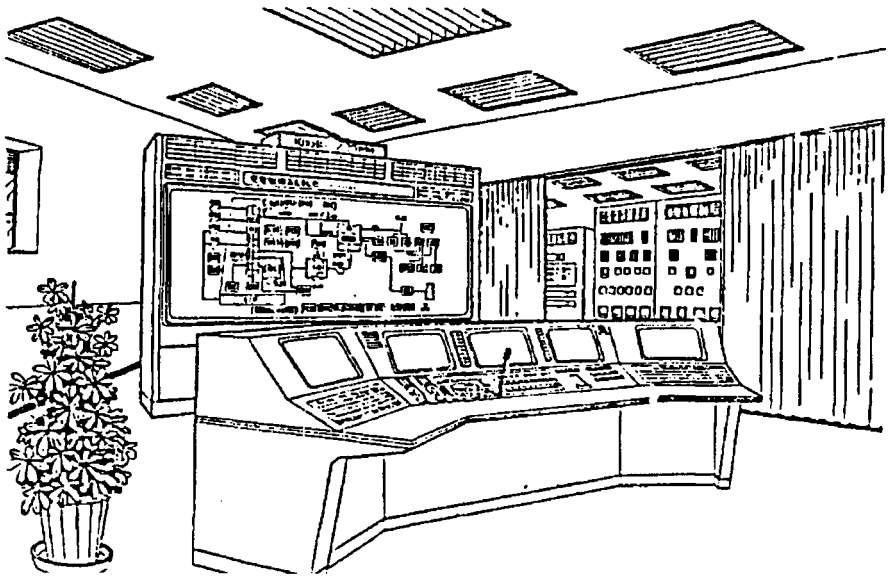


Figura 2.5-6 - Novo conceito de sala de controle [17]

2.6 Alguns Números da Interface Homem-Máquina

A interface homem-máquina é também estudada de maneira diferente, em cada país, dadas as suas particularidades culturais, e porque ainda não há normas internacionais universalmente aceitas sobre o assunto. Entretanto, alguns esforços vêm sendo realizados neste sentido, pela Agência Internacional de Energia Atômica - AIEA e outros órgãos internacionais.

Na referência [18] é apresentada uma avaliação do estado da arte e das perspectivas da interface homem-máquina, tendo em vista a operação e manutenção de usinas nucleares no Japão, que contava em 1990 com 34 usinas instaladas para produção de energia. Na referência, alguns números relativos à indústria japonesa de produção de energia elétrica de origem nuclear foram apresentados classificando genericamente falhas em reatores. O autor cita que a freqüência dos incidentes e falhas a cada reator-ano tem apresentado um decréscimo constante. No entanto, os incidentes e falhas causadas por erro humano têm se mantido no mesmo nível, representando, portanto, com o tempo, uma maior porcentagem do total. Os incidentes devidos a erros humanos que levaram ao desligamento automático de reator chegaram a 53%, e cerca de 15% levaram a redução da potência. Assim, os erros humanos chegaram a aproximadamente 70% do total. Fica claro, então, que os erros humanos são preponderantes, dentre os fatores que afetam a confiabilidade de uma usina nuclear. Na figura 2.6-1, são apresentados os dados de freqüência de incidentes e falhas em reatores japoneses no período de 1969 a 1986.

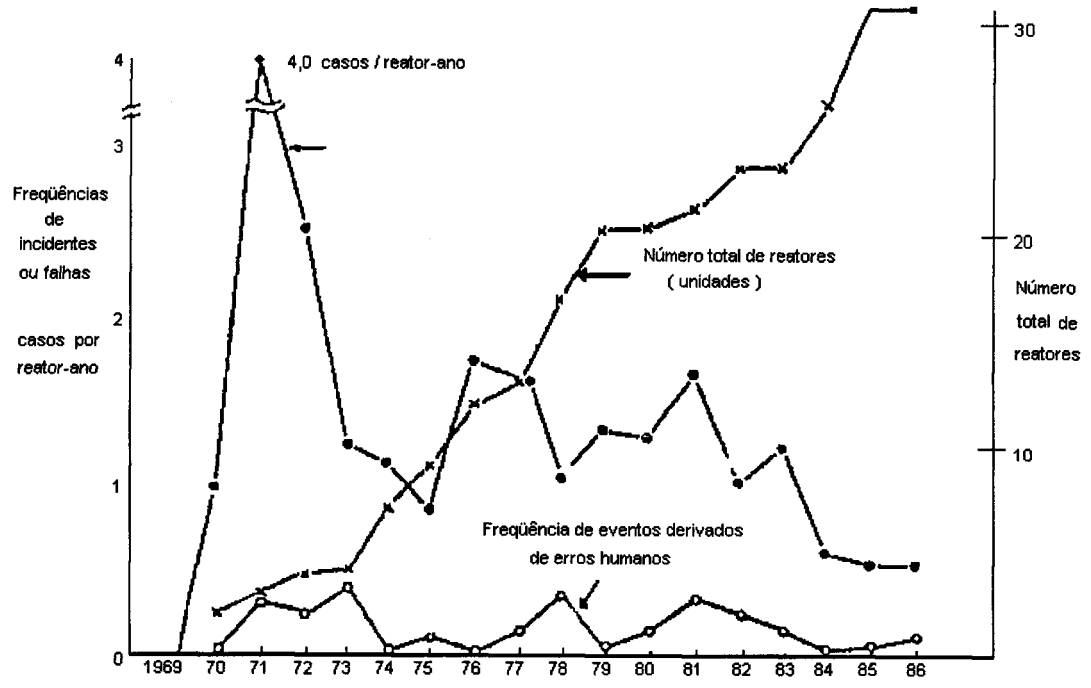


Figura 2.6-1 - Freqüência de incidentes e falhas em reatores japoneses, em casos por reator-ano [18]

A Figura 2.6-2, apresenta a proporção dos efeitos dos erros humanos na operação de usinas nucleares, ainda no Japão. Neste caso, o número total de erros humanos entre 1969 e 1985 foi de 41 casos.

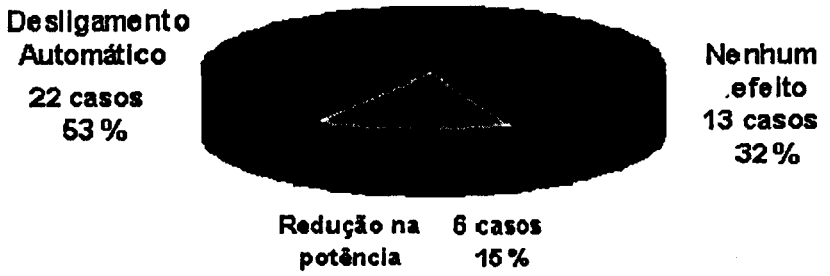


Figura 2.6-2 - Efeito de erros humanos na operação de usinas nucleares no Japão [18]

A Figura 2.6-3, adaptada de [19], que faz uma breve análise dos fatores humanos em usinas nucleares, apresenta sinteticamente as causas de acidentes potenciais.

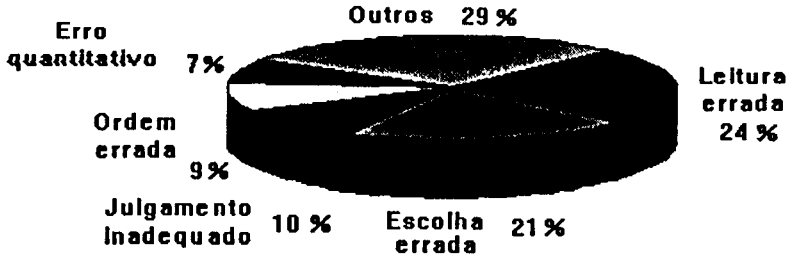


Figura 2.6-3 - Causas dos acidentes potenciais devido a fatores humanos em usinas nucleares [19]

A Figura 2.6-4 apresenta, complementarmente, as razões da principal causa potencial de acidentes, a leitura errada.

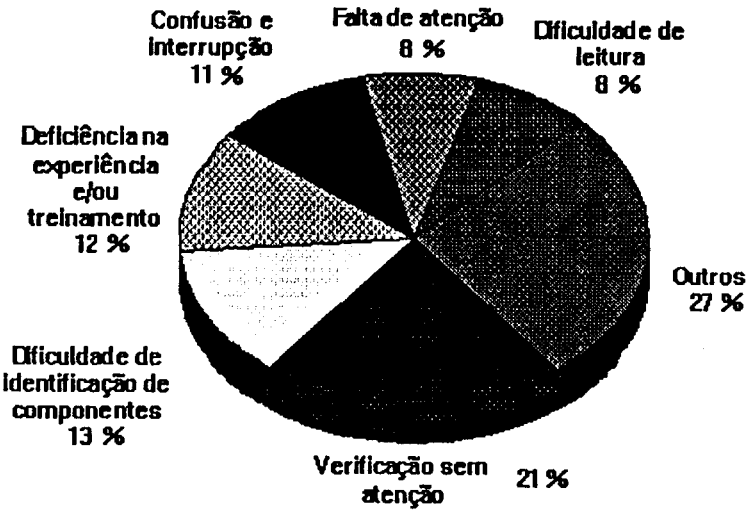
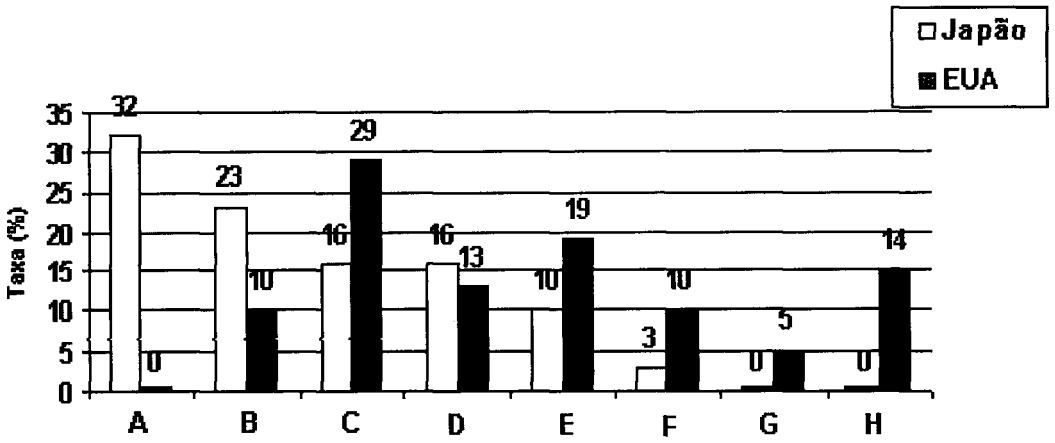


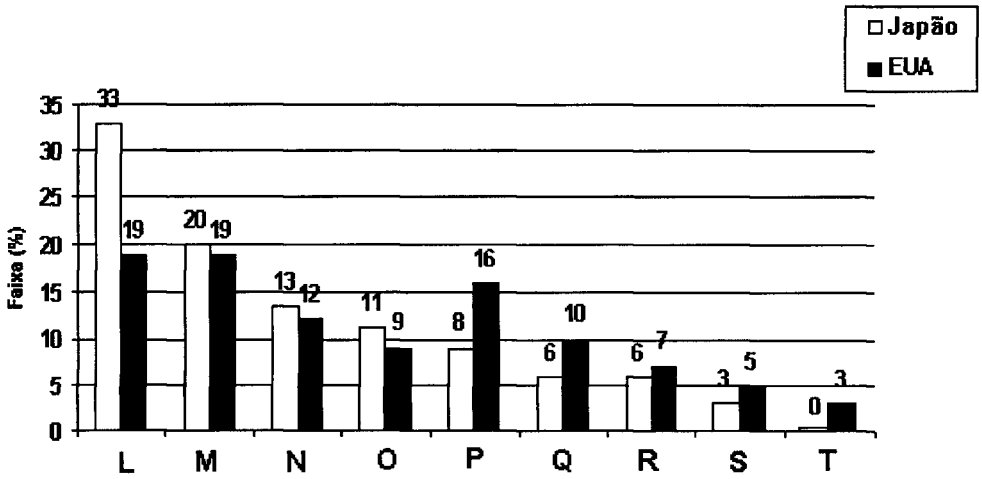
Figura 2.6-4 - Razões para a leitura errada, principal causa potencial de acidentes em usinas nucleares no Japão [19]

As Figuras 2.6-5, comparação de erros entre operadores do Japão e dos Estados Unidos, e 2.6-6, que apresenta o resultado da comparação, apresentam dados quanto aos tipos e fatores de erros [19]. Nota-se que há uma diferença nas taxas referentes aos itens das figuras, certamente devido a diferenças culturais, ou seja, entre operadores de usinas nos Estados Unidos e no Japão.



A - Deficiência Quantitativa
B - Ação inadequada
C - Omissão
D - Outros
E - Transposição
F - Ação fora do tempo
G - Fora de seqüência
H - Comunicação

Figura 2.6-5 - Comparação de tipos de erro e ação inadequada entre operadores dos EUA e do Japão [19]



L - Local de trabalho
M - Procedimentos
N - Gerencial/Supervisão
O - Fatores Pessoais
P - Comunicação
Q - Treinamento
R - Organização de trabalho
S - Implantação de mudanças
T - Esquema de trabalho

Figura 2.6-6 - Resultado da comparação de fatores que contribuíram para as ações inadequadas

Pelas figuras, pode-se inferir que alguns erros são mais importantes em um país que em outro. Por exemplo, a Figura 2.6-5 refere-se ao "modo de erro humano" ao

qual pertence a ação inadequada. A letra "C" correspondente ao fator "omissão", foi muito mais importante para os americanos que para os japoneses, ou seja, os americanos omitem mais. Da mesma forma, para os japoneses o fator mais importante é representado pela letra "A", deficiência quantitativa, ou seja, erros relacionados com associações de números e unidades, relativos a funções e operações na usina. Neste caso, os americanos não apresentaram falhas.A Figura 2.6-6 apresenta os fatores que causaram ou contribuíram para a ação inadequada. Neste caso, os procedimentos, item "M", se situam mais ou menos num mesmo patamar, embora no Japão sejam um pouco mais significativos, como fatores causadores de erros. Também nesta figura, apenas a título de exemplo, verifica-se que o item "P", comunicação, é causa de erro em maior grau nos EUA que no Japão.

De certa forma, os dados aqui apresentados sugerem que há necessidade de uma uniformização de métodos de avaliação e de coleta de dados.

2.7 Interface Homem-Computador e Automação

Com o desenvolvimento rápido da informática e sua aplicação cada vez maior em sistemas complexos de controle de instalações industriais, a interface homem-computador veio adicionar mais um ingrediente ao campo da interação homem-máquina. Por ser evidente que a participação do computador em sistemas de controle aumentará, não sendo possível prever até que ponto e em que grau isto poderá ocorrer, cresce de maneira proporcional o interesse em sistemas complexos homem-computador, na teoria e na prática, devido ao possível aumento do risco de falhas no sistema como um todo. Os problemas fundamentais desta interface, vale repetir, são pontuados especialmente com respeito à possibilidade de ocorrência de erros humanos.

Os principais critérios de projeto a serem observados para decidir quais as tarefas serão executadas por controle manual, e quais serão por controle automático são: a *freqüência*, a *velocidade* e a *complexidade* [10]. O homem é flexível, mas não é infalível. Ele pode fazer algumas coisas bem, e as máquinas podem fazer coisas que o homem não faz.

Em termos de uso da máquina, os computadores são bons na execução de tarefas bem definidas, com grande velocidade e precisão como, por exemplo, para aquisição, armazenamento e análise de grande quantidade de sinais [20, 21]. O ser humano, por outro lado, tem excelente performance em tarefas como visão, percepção da comunicação oral e auditiva, além do reconhecimento de complexos padrões espaciais e temporais, inclusive na presença de ruído, de dados distorcidos ou incompletos [21].

Ainda como comparação, os circuitos eletrônicos são várias ordens de grandeza mais rápidos do que os neurônios do cérebro. Estes últimos, por sua vez, utilizam paralelismo em larga escala, trabalhando simultaneamente, o que permite resolver problemas complexos [20]. Um exemplo seria o de definir o conceito da letra A, conforme apresentado em [20], nas suas mais diversas variações, a partir de conceitos de alto nível como tangentes, ângulos e outros. É uma tarefa difícil e de resultados limitados. No entanto, qualquer pessoa pode reconhecer facilmente a letra A, mesmo quando a mesma está incompleta. Por exemplo, mesmo em um texto com parte de uma frase coberta por uma folha é possível a uma pessoa reconhecer a letra A, bem como inferir as outras. Isto se deve a processos cognitivos que as pessoas internalizam, neste caso formando internamente um conceito do que seja a letra A que, quantitativamente, não pode ser

representado com facilidade. Essa capacidade cognitiva [22, 23] se desenvolve com o crescimento do ser humano e com a aprendizagem, a partir de seu nascimento. É claro que, no exemplo acima citado, deve-se considerar uma pessoa alfabetizada, ou seja, um indivíduo que foi submetido a um processo de aprendizagem de tal forma que pode ver e classificar os diversos tipos de letras nas mais diversas formas e contextos.

Na referência [21] é apresentada uma abordagem estruturada para a construção de uma perspectiva eficiente e confiável, relativa à interface homem-computador. O autor desenvolve a abordagem, tendo em vista o sistema homem-máquina e a modelagem da interface homem-computador. De acordo com esta abordagem, todo sistema homem-máquina, se observado de um referencial externo, comporta-se como qualquer outro sistema. Ou seja, apresenta um certo estado interno e reage aos estímulos com uma determinada resposta, conforme o estímulo. Entretanto, tal modelo (de entrada e saída, ou de estímulo e resposta, conforme apresentado na Figura 2.4-1) requer o conhecimento total do desempenho humano e outras características comportamentais, o que não é uma possibilidade de estudo realística. Por isto, o autor prefere uma abordagem estruturada, descrita resumidamente abaixo.

No modelo estruturado, o sistema homem-máquina completo é subdividido em três componentes, tornando-se mais facilmente modeláveis, individualmente, a partir de determinadas funções características de seus próprios modelos considerados separadamente. Essa modelagem estruturada não resolve todos os problemas, principalmente porque o desempenho e comportamento humano continuará difícil de ser avaliado. Entretanto, segundo o autor, esta partição em três componentes fornece uma maneira de como gerar bons modelos, ou seja, que represente bem os componentes determinísticos, além de simplificar a modelagem das tarefas dos componentes humanos. Complementarmente, pode resultar em uma estrutura dos modelos de sistema interconectado como um todo, de tal maneira que a simulação e também o projeto possam se desenvolver considerando um só sistema.

Os componentes são divididos em três: homens, máquinas e interfaces. Ou seja, a interface sendo um programa, um "software". Para simplificar, nenhuma subdivisão foi feita. Na Figura 2.7-1 é apresentado um esquema do modelo estruturado, de três componentes, comparado com o modelo convencional ou integral, que é o mesmo modelo apresentado na Figura 2.4-1. O ponto fraco desse modelo estruturado é que os componentes não são invariáveis, ou seja, dependem de como e em que o componente anterior foi interconectado com o subseqüente.

Deve-se notar, mais uma vez, que a modelagem do ser humano é a que apresenta dificuldades mais significativas, considerando a interface homem-computador [21] e também considerando as observações anteriores relativas à modelagem das ações do homem, aplicada à APS [24]. Primeiro, o desempenho e o comportamento humanos são altamente dependentes do ambiente, seja este o ambiente próximo ou mais abrangente, ou seja, onde se desenrola a sua vida. Em segundo lugar, o homem vive e age de uma maneira complexa e sua atividade é infinitamente rica, resultando em grandes dificuldades de modelagem, mesmo se apenas alguns itens forem considerados, dentre as múltiplas atividades: percepção de informações; tomada de decisão; transmissão de informações; comunicação e interação, além de outras. Finalmente, os homens podem ser caracterizados também pela sua incerteza, heurística, hesitações, sua múltipla personalidade e por diferentes parâmetros de percepções, representações cognitivas, estilos de pensamento, habilidades na tomada de decisão, idéias de ação no espaço, motivações, esquema de ações

e outras características. Isto, sem mencionar as muitas de suas propriedades dependentes de circunstâncias temporais, que são os fatores que influenciam o desempenho. Esses fatores, que são muitos, serão vistos no item 3.2.1, não considerando apenas o computador.

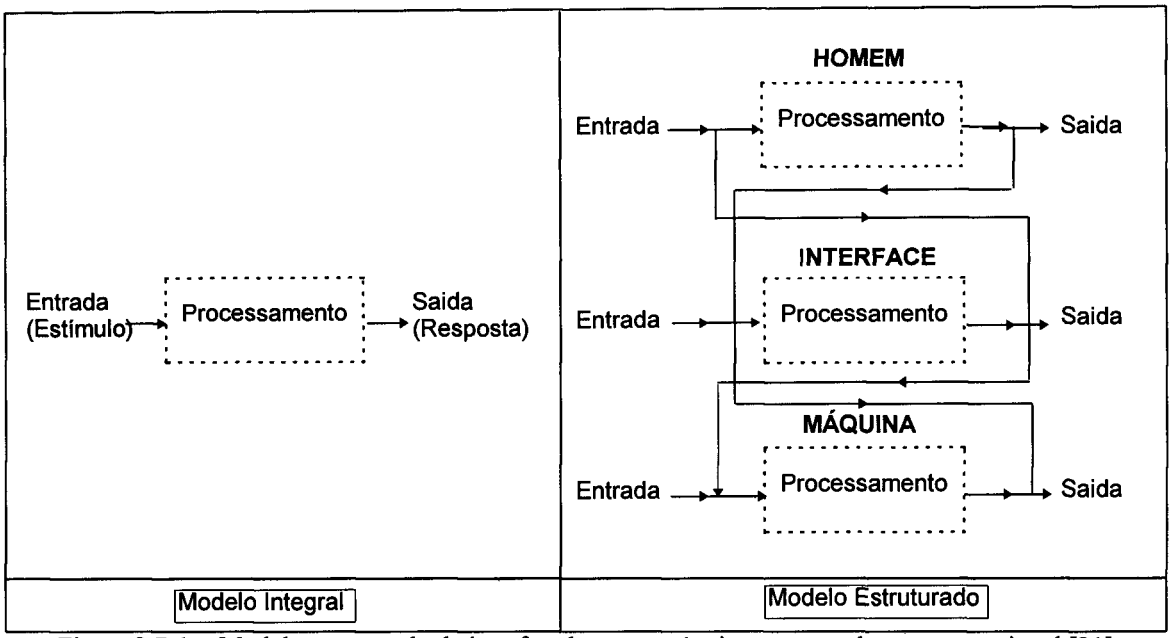


Figura 2.7-1 - Modelo estruturado de interface homem-máquina comparado ao convencional [21]

Os efeitos da grande quantidade de fatores que influenciam o desempenho, incluindo aqueles impossíveis de se levar em conta, na modelagem e na construção da interface homem-computador, não são fáceis de antecipar. Em decorrência de serem usados modelos incompletos na análise de sistema e em simulação, no projeto de sistemas e na sua execução geralmente a resultante é o funcionamento errôneo do sistema. Isso acontece devido aos seguintes fatores:

- comportamento e reações imprevistas do homem;
- erros humanos imprevisíveis;
- perturbação mútua dos modelos humanos e dos modelos de interface homem-computador, em decorrência de suas interconecções e dependências.

Ou seja, estes fatores inviabilizam um conhecimento mais profundo, que possa ser utilizado em um modelo adequado a situações reais. Dentre estas três possibilidades de fontes de erros no sistema, a primeira e a terceira são passíveis de uma certa correção, em sistemas bem projetados, mas os erros humanos são muito difíceis de serem gerenciados. Algumas razões são listadas, sobre este ponto:

- o homem não é compreendido;
- o homem é mal compreendido;
- o homem faz o diagnóstico errado;
- o homem toma uma decisão errada;
- a intervenção do homem é incorreta.

Nem sempre os erros humanos causam o mal funcionamento do sistema homem-máquina, por causa da existência de um projeto tolerante a erros. Assim, algumas ações humanas inadequadas, isto é, a intervenção errada do homem no sistema,

dependendo das informações recebidas, pode não causar erro no sistema. No entanto, é significativa a porcentagem de erros humanos que podem causar erros no sistema. Por outro lado, devido a algumas situações particulares do sistema, intervenções lógicas do homem podem resultar em funcionamento errado no sistema. Assim, talvez o propósito principal no projeto da interface homem-computador e a sua implantação seja geralmente o de minimização da probabilidade de erro do sistema como um todo. Em geral, essa minimização de falhas deve ser conseguida com um sistema que seja tolerante a erros, que permita a recuperação dos erros cometidos ou que permita a correção dos efeitos desses erros antes que as intervenções resultem em erro.

Se a ação humana no sistema é adequada e a operação resultante no sistema redunda em mal funcionamento, há um erro de lógica na interface. Se a ação humana é inadequada, mas o sistema continua funcionando bem, é porque o sistema é tolerante a erros humanos.

O aspecto crucial da interface homem-computador é o erro humano. Este vai persistir, e jamais será eliminado totalmente. A única possibilidade é reduzir seus efeitos na operação. Como não há um sistema totalmente isento de erros, e os investimentos para reduzi-los em muitos casos não são considerados compensadores, do ponto de vista financeiro, a chave para a solução será a aplicação de:

- sistemas tolerantes a erros;
- possibilidades de correção, ou seja, soluções que permitem o reconhecimento e correção dos erros humanos cometidos (recuperação);
- minimização das conseqüências, ou seja, manter segura a operação do sistema homem-máquina, mesmo sob efeito de intervenções humanas erradas.

Ao se considerar fatores humanos no projeto da interface homem-computador, deve-se tomar como base de projeto um conjunto coerente de asserções sobre o conhecimento e as habilidades humanas. A *Abordagem Cognitiva* do conhecimento vem sendo utilizada para esta finalidade. O termo *cognitivo* refere-se a um dos ramos da psicologia focalizada nos processos centrais do indivíduo, tais como: organização do conhecimento, processamento de informações, estilo de pensamento, comportamento relativos à tomada de decisão, além de outros [22, 23]. Neste modelo estruturado apresentado acima, o processamento de informações da mente humana consiste em recodificar e transformar os eventos estimuladores em representações mentais interrelacionadas.

Do ponto de vista da psicologia cognitiva, essas representações mentais, constituem a inteligência, sendo o produto de uma construção devido às perturbações do meio e à capacidade do organismo de ser perturbado e de responder a essa perturbação. De acordo com a definição de Piaget [25], a *Inteligência* constitui o estado de equilíbrio para o qual tendem todas as adaptações sucessivas de ordem sensório-motoras e cognitivas, bem como todas as mudanças assimiladoras e acomodativas entre o organismo e o meio. Dessa forma, o papel da interface homem-computador, como um programa, é perturbar o equilíbrio homem-máquina, sinalizando os eventos ocorridos no sistema, provocando uma determinada resposta [26]. Essa resposta, ou seja, a ação transformadora tomada pelo usuário, deve refletir a transformação sofrida pelo sistema em termos que sejam adequados às suas representações mentais. Dessa maneira, através do que for apresentado no monitor, o usuário reconhecerá o efeito de sua ação, e assim por diante, interativamente.

Muitos estudos e pesquisas apontam para alguns pontos importantes, como a utilização de sistemas avançados de apoio ao operador, incluindo os *Sistemas*

Especialistas. Parece ser da maior importância, também, o desenvolvimento de uma linguagem natural, embora apoiada em outros parâmetros, como funções chaves. Isso revela uma tendência de trocar a linguagem mais ampla utilizada no diálogo com o computador por um diálogo controlado ou limitado. Este é o caso de, por meio de uma memória associativa, colocar as entradas originais dentro de uma gama reduzida de palavras, com a eliminação de sinônimos. Conforme já adiantado no item 2.4, é importante também integrar melhor o homem e o computador, de forma que trabalhem juntos, e não de maneira concorrente [21]. Por exemplo, embora o desempenho computadorizado seja melhor, em grande parte dos casos, é conveniente respeitar os limites do ser humano.

Assim, respeitando os esquemas mentais do homem e seus modos de representação dos processos, deve ser mantida uma coerência com o critério de decisões humanas, mantendo um certo tipo de diálogo. O operador não deve, por exemplo, ser abruptamente informado sobre o resultado final de uma operação da máquina, mas deve participar intimamente da elaboração do resultado, compartilhando da elaboração do processo, melhorando a motivação e criando uma interdependência homem-computador [21]. Muitos outros fatores são objetos de estudos e, sendo a interface homem-computador um campo novo, é ainda cedo para o surgimento de muitos resultados objetivos. Somente para se dar uma idéia da dificuldade em se conseguir resultados objetivos, é possível fazer uma breve análise quanto ao problema da tomada de decisão. O intuito do sistema de apoio ao operador é melhorar a qualidade das decisões tomadas por ele, durante a operação de uma usina nuclear. Para que o projetista compreenda as exigências necessárias do sistema, é necessário utilizar algum tipo de modelo para a estruturação de informações necessárias em diferentes fases das tarefas de controle e monitoração. Uma proposta de modelagem, de Rasmussen [27], em essência divide a tarefa de *Tomada de Decisão* nos seguintes estágios:

- ativação dos processos mentais;
- observação;
- identificação;
- interpretação;
- avaliação;
- definição das tarefas;
- formulação dos procedimentos a serem tomados e
- execução das ações.

De acordo com [21, 27] o operador raramente acompanha estes passos, em sua seqüência estabelecida, freqüentemente pulando alguns destes estágios, baseando-se para tanto em sua experiência. Esta observação levou à definição de execução de tarefas para diferentes níveis de atividade mental, gerando comportamentos, chamados por Rasmussen [27], de comportamentos baseados na habilidade ou no talento ("skill-based"), em regras ("rule-based"); e no conhecimento ("knowledge-based"). Estes três níveis de comportamento foram desenvolvidos a partir de trabalhos anteriores, notadamente [28], e foram adotados em muitos outros trabalhos na área, que formam uma extensa bibliografia sobre o assunto, como em [29, 30].

Na referência [31] são discutidos os *tipos* de erros para tentar melhorar a modelagem do comportamento humano. O tipo de erro se relaciona com a origem presumida do mesmo, a nível de processos mentais e sua ação conseqüente, ou seja, decorrente daquele processo mental. Os processos mentais envolvidos foram denominados

estágios, e divididos em três principais: *planejamento, armazenagem e execução.* Obviamente, armazenagem se refere à memória, no contexto da psicologia cognitiva. Os tipos de erros associados a estes três estágios são relacionados com aqueles propostos por Rasmussen em [27]: a) enganos devido à falta de conhecimento ou especialização (desempenho baseado no conhecimento) e enganos baseados na falha ao utilizar este conhecimento (desempenho baseado em regras) quando associados ao planejamento; b) lapsos no desempenho baseado na habilidade, ocorrendo durante o estágio de armazenamento; e finalmente c) atos falhos que aparecem durante a execução das ações planejadas, usualmente devidos à falta de atenção. De acordo com [27], os tipos de erros são conceitualmente ligados aos estágios relacionados aos processos cognitivos.

Neste trabalho, não são aprofundados ou desenvolvidos os processos mentais, ou mesmo os conceitos a estes relacionados. As informações apresentadas acima tem apenas o objetivo de ilustrar a dificuldade da realização da modelagem do desempenho humano, devido à necessidade de consideração de inúmeros fatores.

Para propósitos da APS, o modelo proposto por Rasmussen [27] fornece um esquema aceitável de trabalho para identificar diferentes níveis de comportamento e mecanismos de erros a estes associados [29]. Dessa forma, o comportamento (ou desempenho) baseado na habilidade engloba atividades muito praticadas, repetidas, realizadas aparentemente com pouco esforço mental, como dirigir um carro numa rota familiar. Numa usina nuclear, *Atos Falhos* (segundo concepção adotada em [22] para "slips"), e *Lapsos* são associados com esse tipo de desempenho. Atos falhos são, por exemplo, seleção inadvertida de itens diferentes dos que deveriam ser acionados, como apertar um botão no lugar de outro. Lapsos são omissões ou erros de execução durante uma seqüência planejada de ações. Por exemplo, se a seqüência é girar um controle, apertar um botão e depois voltar a girar o controle, o lapso seria esquecer um destes itens.

Os *enganos* são associados a ações baseadas em regras e também a ações baseadas no conhecimento. Envolvem mecanismos de erros mais sérios, que ocorrem devido a erros de compreensão inadequada de uma situação e a seleção de um plano não adequado de ações resultantes. Isto envolve, por exemplo, a escolha de uma seqüência de ações, como acionar um controle relativo a uma função de segurança antes de uma outra que deveria ser executada previamente. Os enganos, quando associados ao desempenho baseado no conhecimento, podem ocorrer devido a uma carga excessiva de trabalho da memória ou à utilização de modelos mentais inadequados [29].

Para propósitos da APS, é importante estar alerta quanto a esses diferentes potenciais de erros, na medida em que fatores de recuperação dependem deles. Atos falhos e lapsos são fácil e rapidamente recuperáveis, desde que existam mecanismos de retorno ("feedback"), sendo que o comportamento do sistema é quase sempre reversível. Já os enganos são menos facilmente recuperáveis a curto prazo, pois pode ocorrer uma persistência no processo mental do operador, de tal forma que ele insista em realizar ações incorretas mesmo quando frente a inúmeras informações indicando que ele deve fazer de maneira diferente da que está fazendo (por exemplo, excesso de confiança, agindo contrariamente a algum item estabelecido em procedimento). Uma estrutura de recuperação deve estar disponível e ser bem enfática, no sentido de fornecer ao operador um aviso de que ele está agindo erroneamente, como por exemplo alarmes ou sinais, e deve haver um reforço no treinamento sempre que for detectada a necessidade. Os especialistas em ACH devem assegurar que os erros potenciais sejam identificados na estrutura da APS e que sejam devidamente levados em consideração [29].

Embora estes três níveis de comportamento sejam uma categorização para ações abrangentes, com relação à interface homem-computador, pode-se dizer que [26]:

a. no comportamento baseado no talento ou habilidade existe um contexto ambiental adequado para um comportamento do tipo imediato, à um evento correspondendo uma ação. Nesse contexto, a interface sinaliza e o usuário reage, provavelmente de forma correta e esperada.
b. no comportamento baseado em regras, o ambiente pode ser representado por um conjunto de regras lembradas ou escritas. Neste caso, o usuário deve seguir as regras a partir das quais foi selecionado um determinado plano comportamental, ou seja, são comportamentos conscientes de tarefas pré-planejadas e armazenadas na memória.
c. no comportamento baseado no conhecimento, o usuário recebe estímulos de eventos que não encontram associação com nenhuma representação mental conhecida. Ou seja, é uma experiência nova (ou relacionada a experiências não assimiladas anteriormente, ou esquecidas). Neste contexto, o usuário é levado pela sua experiência e treinamento a buscar, na memória, conceitos e associações que possam ser dinamicamente modificados e estendidos, visando adaptar-se à nova situação que se apresenta. Neste caso, a interface deve ser capaz de auxiliar o usuário, fornecendo novos dados relacionados com o evento, e com maior grau de detalhe. Para um usuário experiente, isso se aproxima muito do conceito de uso amigável ("user-friendly"), ou seja, uma programação que admita um diálogo.

É importante salientar que, de acordo com a teoria cognitiva, a aprendizagem, que se aproxima muito da situação apresentada no item c acima, é concebida como um processamento ativo da informação que é percebida, captada, processada e interiorizada [23]. O processamento adequado da informação por um indivíduo, e sua conseqüente retenção, só poderão ocorrer se ele relacionar a informação nova com o que já sabe, ou seja, seu conhecimento anterior.

Essa caracterização de comportamento oferece oportunidade aos especialistas em interface homem-máquina de privilegiar os dois comportamentos menos complexos, em qualquer projeto, favorecendo a não ocorrência de possíveis atuações erradas. No caso específico da interface homem-computador, deve-se facilitar a atuação do usuário, acrescentando novas informações e associações em representações mentais já existentes [21, 26]. Se o modelo mental não é atualizado, situações novas ou não planejadas já ocorridas não serão repetidas.

Em [32] é discutido o ponto de automação desejável ou alcançável. De certa forma, vai de encontro com as observações acima. Por exemplo, em decorrência do fato de só poderem ser automatizadas as funções previamente antecipadas no projeto, inclusive funções de segurança, a intervenção do operador no controle deve incluir aquelas situações que não foram consideradas e que não estão cobertas pelos sistemas automatizados. Considera-se que problemas de controle são casos raros em sistemas automatizados bem projetados. Assim, a intervenção do operador aparece como um problema, ou seja, se o mesmo tem condições de tomar decisões adequadamente em uma situação rara, para a qual ele tenha muito pouco preparo. Dessa forma, é possível que o melhor seja levar a automatização até um determinado nível em que o operador se depare ocasionalmente com alguns problemas, de modo que o mesmo experimente com mais freqüencia como gerenciar, sem o apoio de sistemas automatizados, alguma previsível situação anormal na instalação.

De acordo com [32], o equilíbrio entre as ações humanas e a automação na operação de instalações complexas depende de vários fatores, como os tecnológicos, econômicos, ergonômicos e sociais, que são interelacionados e podem variar com o tempo. Desde que os componentes físicos de instalações podem falhar, e os homens podem cometer erros, o nível de automação deve levar em conta todos estes fatores, de tal forma que seja bem aceito tanto pelos operadores quanto pela sociedade envolvida. De acordo com [32], mais pesquisa torna-se necessária neste campo, para a determinação de níveis adequados de automação de instalações complexas que tenham grandes potenciais de risco.

Considerando os níveis de desempenho humano para a execução de tarefas, deve ser lembrado que o comportamento mais suscetível a erros é o baseado no conhecimento e é neste que se enquadra a tarefa de tomada de decisões. É este nível, portanto, que deve ser privilegiado com pesquisas e investimentos. Este é um dos pontos onde se concentram esforços na melhora do desempenho humano, principalmente enfocadas no auxílio do computador nas tomadas de decisões [8].

2.8 Sistemas Especialistas

Desenvolvimentos recentes têm permitido ao operador receber informações adicionais através de recursos computacionais avançados (gráficos, desenhos, representações, modelos, etc.), como o apresentado na Figura 2.8-1.

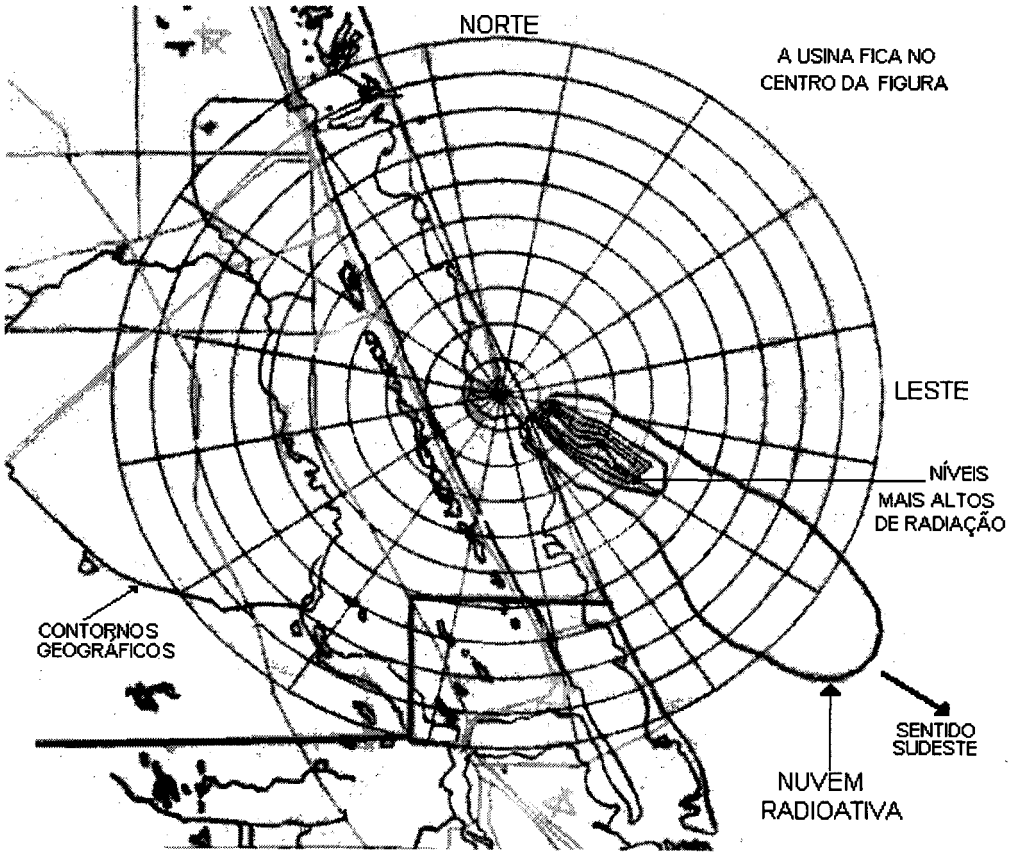


Figura 2.8-1 - Recursos gráficos obtidos por computador, indicando a direção tomada pela nuvem radioativa após a ocorrência de um hipotético acidente em uma usina nuclear [33]

A Figura 2.8-1, obtida a partir de um monitor de vídeo, é a representação de um mapa com uma usina nuclear no centro e uma nuvem radioativa que nele se origina, deslocando-se na direção sudeste, após a ocorrência de um acidente hipotético [33]. Deve-se notar que, quanto mais distante a nuvem estiver da usina, menor a concentração de material radioativo, portanto menores os níveis de radiação. A ilustração é originada de um programa desenvolvido pela "Federal Emergency Management Agency" - FEMA, órgão americano com responsabilidades em planejamento de emergência nos EUA.

No Brasil já existe algo similar ào programa utilizado pela FEMA, desenvolvido pela Coordenação dos Programas de Pós-Graduação em Engenharia da Universidade Federal de Rio de Janeiro - COPPE/UFRJ, que vem sendo utilizado por Furnas Centrais Elétricas SA - FURNAS, nos equipamentos utilizados no programa de segurança para a Central Nuclear Almirante Álvaro Alberto - CNAAA, em Angra dos Reis, Rio de Janeiro [34]. Apenas para comparação, a Figura 2.8-2 apresenta uma figura, obtida em um monitor de vídeo, do Sistema de Controle Ambiental da CNAAA.

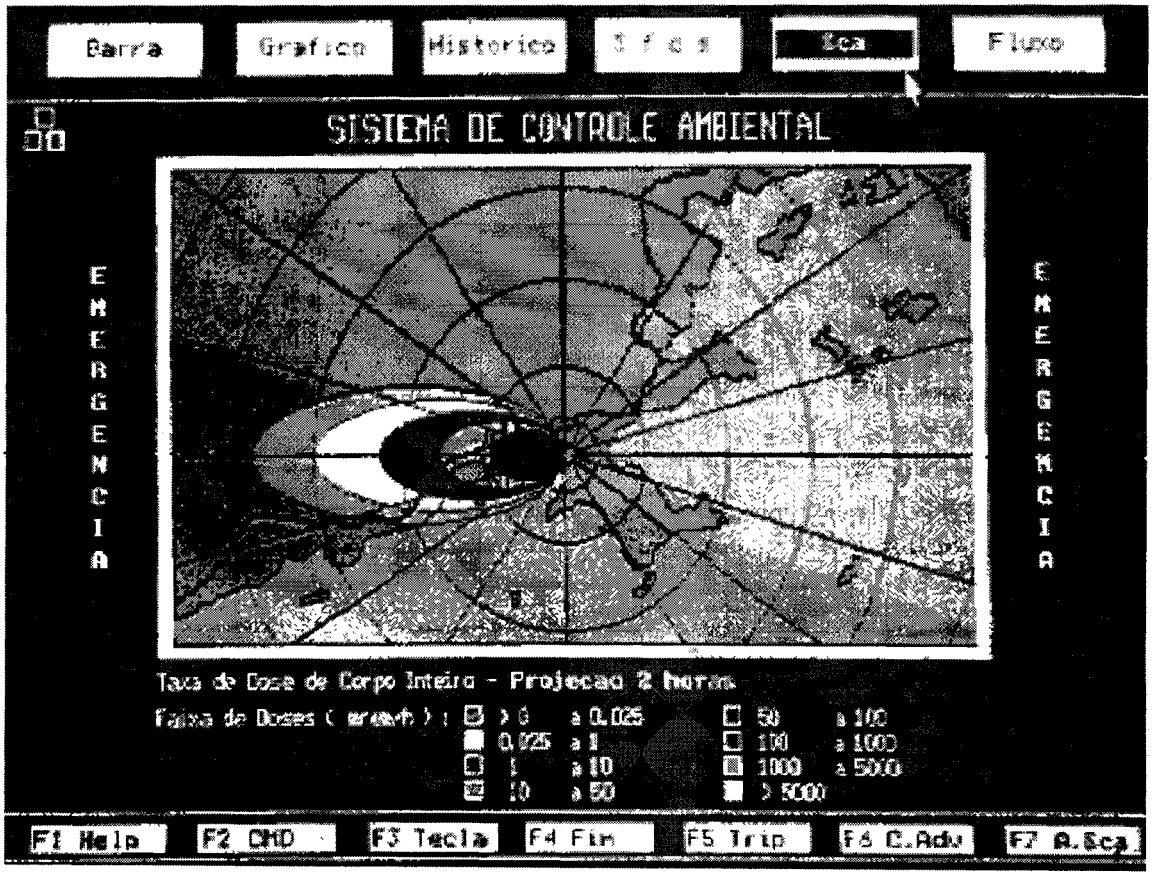


Figura 2.8-2 Recursos gráficos apresentando simulação de nuvem radioativa se deslocando, e sistema de parâmetros associados, relacionados ao meio ambiente, incluindo níveis de radioatividade [34]

A figura apresenta um sistema informatizado semelhante ao americano, com algumas modificações. A utilização do sistema com base em dados meteorológicos e radiológicos, permite monitorar o deslocamento de uma emissão atmosférica, fazendo projeções em tempo real do impacto radiológico ambiental associado à emissão.

É importante que tais sistemas avançados de computação forneçam informações necessárias de forma clara, de fácil compreensão, em lugar de mostrar apenas o que é tecnicamente possível, na forma de dados que operadores bem treinados compreendam, e saibam o que fazer a partir da interpretação dos referidos dados.

Essas informações baseadas em programas implementados em computadores também trazem à tona novos problemas, que ainda necessitam de um encaminhamento melhor, por exemplo, qual o curso de ação a ser seguido pelo operador, se a ele se apresentam informações conflitantes, quando comparadas, de equipamento convencional e de sistemas avançados. De certa forma, surgem novas possibilidades de erros humanos, pouco relatadas na bibliografia existente [35].

É necessário considerar cuidadosamente o problema de validade dos programas utilizados ("software") e o licenciamento dos referidos sistemas avançados, inclusive os sistemas especialistas. Enfim, considerando-se a importância do homem como um fator de segurança, torna-se necessária uma grande cooperação internacional para troca de experiência de operação, de treinamento em simuladores e de uso de recursos computacionais avançados.

Os mais recentes desenvolvimentos no campo da apresentação de dados são os *sistemas cognitivos ou sistemas especialistas*, que são basseados no conhecimento e fornecem nova qualidade de informações. Estes sistemas se encontram num estágio inicial, e vai demandar ainda algum tempo para se tornarem operacionais, embora pesquisas estejam sendo feitas mundialmente para desenvolvimento desta tecnologia [36]. O professor Edward Feigenbaum, da Universidade de Stanford, um dos principais pesquisadores neste campo, conceituou um sistema especialista como:

"Um programa inteligente de computador que usa conhecimento e procedimentos inferenciais, para resolver problemas que são bastante difíceis, ou seja, que requerem, para a sua solução, muita perícia humana. O conhecimento necessário para atuar a esse nível, mais os procedimentos inferenciais empregados, pode considerar-se um modelo da perícia dos melhores profissionais do ramo.O conhecimento de um sistema especialista consiste em fatos e heurísticas. Os fatos constituem um corpo de informação que é largamente compartilhado, publicamente disponível e geralmente aceito pelos especialistas em um campo. As heurísticas são, em sua maioria privadas, regras pouco discutidas de bom discernimento (regras de raciocínio plausível, regras da boa conjectura), que caracterizam a tomada de decisão a nível de especialista na área. O nível de desempenho de um sistema especialista é função principalmente do tamanho e da qualidade do banco de conhecimentos que possui".

Este conceito de Feigenbaum foi obtido da referência [36]. Os autores denominam de "engenheiros do conhecimento" aqueles profissionais que constroem os sistemas especialistas baseados no conhecimento. E ainda, referem-se à tecnologia de construção de tais sistemas como *engenharia do conhecimento*. Os sistemas especialistas, eram assim chamados em decorrência de terem sido os primeiros sistemas construídos entrevistando reconhecidos especialistas humanos e tentando apreender o conhecimento desse especialista. Atualmente, boa parte dos engenheiros do conhecimento referem-se a seus sistemas como sistemas cognitivos. Este termo, segundo [36], é mais conveniente porque não sugere que todos os sistemas construídos por meio de técnicas de engenharia do conhecimento possam apreender o que sabe um especialista humano. Entretanto, tem sido utilizado preferencialmente o termo sistemas especialistas, como se percebe em

publicações do Departamento de Ciência da Computação da Universidade Federal de Minas Gerais [20, 26].

Os sistemas especialistas são programas de computador que contêm grande abundância de conhecimentos de determinada especialidade. Empregam regras práticas ou heurísticas, para se concentrarem nos aspectos chaves de problemas particulares, e para manipularem descrições simbólicas a fim de discorrer sobre o conhecimento que lhes é fornecido. Trabalham pelo exame freqüente de um número de hipóteses contrárias simultaneamente, e fazem recomendações experimentais ou atribuem pesos às alternativas. Os sistemas especialistas interagem com um usuário quase da mesma maneira que um consultor humano o faz.

Na área nuclear em particular, e na industrial em geral, os sistemas especialistas podem auxiliar os operadores, podem prever alguns problemas e dar sugestões. Recentemente, construiram-se sistemas que contêm conhecimentos de situações de tomadas de decisões difíceis, muito úteis, mas dificilmente equivalentes às de especialistas humanos [36]. No entanto, é exatamente nesta área em particular que se esperam bons resultados práticos. A tomada de decisão é crucial, por exemplo, em condições emergenciais, onde situações não previstas podem acontecer no desenrolar dos eventos. Para que um programa funcione como um especialista humano, deve ser capaz de fazer o que um especialista humano comumente faz.

Diferentemente dos pesquisadores da inteligência artificial, cujo objetivo de estudo é principalmente, a resolução de problemas na teoria, os engenheiros do conhecimento concentram-se em reproduzir o comportamento de um especialista específico, quando empenhado em resolver um problema estritamente definido. Para isso, além de toda a capacidade e conhecimento que se exige de um especialista, um sistema especialista deve também oferecer o uso amigável, ou seja, uma programação que não faça com que o usuário se limite a respeitar simplesmente o que lhe é oferecido, fornecendo uma certa possibilidade de diálogo. Assim, um engenheiro do conhecimento combina uma grande dose de psicologia cognitiva com técnicas de programação simbólica para desenvolver sistemas especialistas.

3. O ERRO HUMANO

A importância de um erro humano depende de suas conseqüências sociais e econômicas. Se alguém esquece de colocar o selo no envelope, e coloca o envelope na caixa do correio, terá sua correspondência devolvida. No mínimo, haverá um atraso de alguns dias, em decorrência daquele esquecimento.

Para o erro acima, as conseqüências em geral, serão pequenas. Porém, se forem considerados outros erros, a situação se modifica. Na referência [37], são apresentados dados obtidos sobre acidentes aéreos, tomando por base estatísticas americanas. Nesta referência, que foi publicada em 1987, 70% dos acidentes investigados foram atribuídos à "falha do piloto". Esta categoria, ou seja, erro do piloto, é ampla e inclui tudo que não possa ser atribuído a defeitos mecânicos/elétricos e a bruscas variações do tempo, vão desde o controle inadequado do avião, ou seja, fora dos padrões esperados de um piloto qualificado, até o planejamento inadequado de vôo.

Se o esquecimento do selo, no exemplo anterior, tem conseqüências mínimas, o esquecimento de um procedimento de emergência, por parte de um piloto ou da tripulação como um todo, pode ter gravíssimas conseqüências. Embora as raízes psicológicas destes dois erros citados possam ser bastante similares, certamente o acidente com o avião é mais importante, e merecerá uma investigação cuidadosa. Pelo menos para buscar meios de prevenir outra ocorrência similar, pela análise dos dados obtidos, que deverão ser considerados posteriormente, tanto no projeto de outros aviões, quanto na melhoria da interface homem-máquina.

3.1 O que é Erro Humano no Trabalho

Em livros que tratam de psicologia industrial, sempre se considera importante o erro humano. Na referência [38], os autores enfatizam a ordem de grandeza e a constância dos erros humanos nas atividades de trabalho, principalmente na produção industrial. São ressaltados os problemas gerados por erros nas fases de trabalho, que terminam por impor medidas administrativas (a inspeção é uma delas) e de controle, que elevam os custos financeiros. Em algumas situações, os erros podem ter conseqüências tais que justifiquem todo e qualquer esforço para eliminá-los. Alguns erros podem ser extremamente críticos, e merecem que um grande esforço seja feito para tentar eliminar a possibilidade de sua ocorrência. Embora não seja lógico pensar na eliminação total dos erros humanos, pode-se considerar a possibilidade de reduzi-los a níveis aceitáveis.

Ao considerar qualquer redução da margem de erros a níveis razoáveis, é necessário dispor de informações relevantes sobre os tipos específicos de erros em questão, e sobre os tipos de comportamento humano e as variáveis da situação a eles relacionados. Na consideração dos tipos de erros, surge a questão básica que diz respeito ao que realmente constitui um erro. Uma definição operacional possível é a que considera erro humano qualquer desvio de um padrão de desempenho humano anteriormente estabelecido, exigido ou esperado, que resulta em: atraso indesejável, dificuldades, problemas, acidente, trabalho deficiente ou não execução do serviço. O erro humano é também sinônimo de trabalho deficiente, segundo alguns autores. Como o trabalho pode,

freqüentemente, ser considerado como variável ao longo de um período, é necessário caracterizar que tipo de trabalho é considerado inaceitável em relação a um padrão adequado. Inaceitável, neste caso, pode ser o que não corresponde às especificações desejáveis, ou que foge das margens de tolerância admitidas, considerando como trabalho a ação humana a ser desempenhada. De maneira semelhante, pode-se considerar como erro humano qualquer etapa de uma série de ações humanas que exceda alguns limites de aceitabilidade.

Alguns pontos específicos devem ser lembrados. Por exemplo, a sabotagem, em geral, não é considerada erro humano, pois decorre de ação ou omissão intencional, portanto com um propósito definido. Ao se caracterizar os erros em uma situação de trabalho, é útil determinar, se possível, os comportamentos humanos e as variáveis da situação associados com o tipo de erro. Embora seja geralmente difícil estabelecer relações básicas de causa e efeito, tal informação freqüentemente pode servir de base para a ação corretiva.

Nem todos os erros humanos redundam em degradação de um sistema. Um erro pode ser recuperado ou corrigido antes que resulte em conseqüências indesejáveis ao sistema, devido a um sistema de verificação, ou quando o próprio sistema detecta o erro (sistema tolerante a erros).

Embora a situação a respeito do erro humano venha se modificando devido ao considerável aumento de informações neste campo [22, 39], principalmente pelo aumento da quantidade de dados, conforme visto no item 2.7, ainda é difícil decidir satisfatoriamente o que é um erro humano. Em determinadas situações, essa dificuldade persiste, como alertado em [40]. Nesta referência, chama-se a atenção para a dificuldade de separar o satisfatório do insatisfatório, com relação ao desempenho humano. Em alguns casos, a atuação de um operador é diferente da requerida em regras ou normas, em função de sua experiência, treinamento, ou até mesmo de um certo bom senso. As vêzes, a interpretação literal de regras da empresa ou de regulamentos oficiais leva o operador a cometer algum erro, por exemplo, a inversão de dois passos de um procedimento. Erros de interpretação são favorecidos, de acordo com [1], se existem regras ou procedimentos contraditórios, ou se estes documentos não são claros e bem compreendidos.

A referência [40] cita algumas dificuldades que comprometem a correta interpretação de situações deste tipo. Por exemplo, se é exigido do operador que monitore um determinado instrumento para verificar se a situação está normal. A dificuldade, neste caso, é quanto à precisão destes termos, ou seja, o que constitui monitorar e/ou o que é normal. Em certos casos, o operador pode ser levado a elaborar hipóteses incorretas, que têm efeitos negativos, posteriormente. Esse tipo de erro é um erro crítico de cognição, ou seja, baseado no conhecimento, devido ao fato de que o operador tem que situar-se ante uma determinada condição apresentada, em que as normas ou procedimentos não estão bastante claros, sendo necessário um determinado nível de interpretação.

Em seguida é apresentado um exemplo, baseado em [40], para ilustrar o problema acima discutido. Em uma determinada situação, um operador deve desligar a instalação quando o nível da variável ultrapassar o nível de alarme, conforme as três situações ilustradas na Figura 3.1-1. No caso 1, o operador permite que a variável ultrapasse várias vezes o nível de alarme, envolvendo, portanto, erros múltiplos. No caso 2, apenas um erro é cometido. No caso 3, nenhum erro é cometido. Deve ser notado que os eventos podem levar a conseqüências bastante diferentes para a instalação.

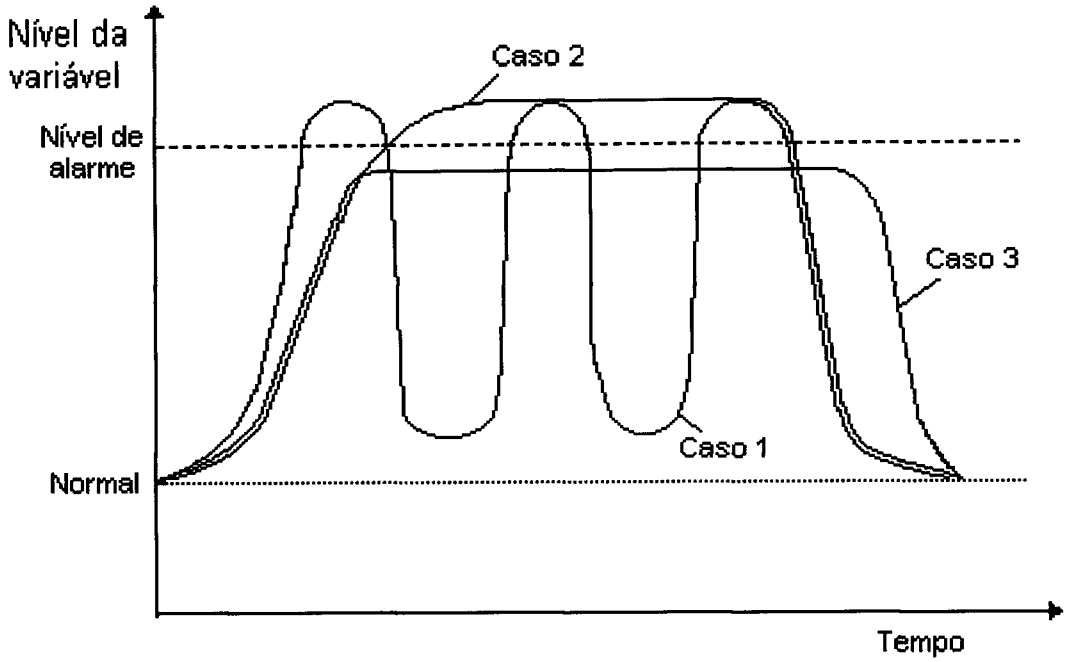


Figura 3.1-1 Comparação de três curvas representando três diferentes situações relacionadas com uma determinada variável e sua relação com o nível de alarme [40]

Existem várias possibilidades de se categorizar os erros humanos. Quando se considera um determinado sistema, o principal interesse está nos erros que constituem entradas erradas no mesmo, porque, em geral, é difícil corrigir erros durante algum processo já em evolução. A relação entre entradas no sistema homem e saídas do sistema homem, que em geral correspondem a entradas no sistema máquina, pode ser simplificadamente ordenada em três níveis ou componentes típicos: entrada; mediação (processos cognitivos) e saída (resposta ou resultado), conforme discutido no item 2.4.

Os erros podem ser atribuídos a um ou mais de um desses componentes do comportamento. No sistema homem-máquina, entradas incorretas são resultantes de respostas humanas erradas, ou seja, ao estímulo determinado esperava-se outra resposta. Sem considerar processos internos, as respostas humanas dão margem a diferentes sistemas de categorização, que relacionam as respostas humanas às exigências do sistema.

A seguinte categorização foi introduzida por Swain [41] e usada, desde então, por muitos especialistas em análise da confiabilidade humana: os erros humanos podem advir de uma *ação* ou de uma *omissão*.

Ou seja, uma pessoa pode cometer um erro se faz algo incorretamente, falha em fazer algo, ou falha em fazer algo no tempo adequado ou erra por omissão. Abaixo são apresentados dois exemplos, para esclarecer:

- erro de omissão: um mecânico coloca óleo novo no carro, sem colocar a tampa no reservatório de óleo. Neste caso, omitiu um passo da tarefa (perde óleo e suja a garagem).
- erro de ação: se no exemplo acima, o mecânico escolhe uma chave de boca de tamanho diferente do exigido, ele fez um erro de *seleção*. Se acondicionar óleo antes de esvaziar o carter, o erro é de *seqüência*. Se não terminar o trabalho no tempo permitido, será erro

de *tempo*. Se a tampa do reservatório não foi bem apertada, ficando frouxa, foi um erro *qualitativo*.

A Tabela 3.1-1 apresenta uma divisão desta categorização.

Tabela 3.1-1 - Categoria de comportamento humano incorreto, aplicável à Análise da Confiabilidade Humana [41]

Erros de OMISSÃO • Omitir a tarefa inteira; • Omitir um passo da tarefa. Erros de AÇÃO • Erros de seleção (controle, comando, etc.); • Erro de seqüência; • Erro de tempo - muito rápido (precipitação) - muito demorado (devagar demais); • Erro qualitativo (pouco ou muito).

Para o caso da análise da confiabilidade humana, que usa estimativas de probabilidades de erros humanos, é freqüentemente necessário que o especialista considere os processos comportamentais (e cognitivos) fundamentais. Isto porque, para fazer a modelagem de sistemas, é necessária a divisão em etapas, para facilitar a pesquisa de possíveis erros. Do ponto de vista de um sistema, uma ação humana (ou omissão) é um erro, se ele reduz ou tem o potencial para reduzir a probabilidade de encontrar algum resultado desejado em alguma função do sistema.

Quando se estuda a relação de erros humanos no desempenho de um sistema, procura-se saber quais tipos de erros e quão freqüentemente são cometidos. Para este propósito, a classificação de [41] é apropriada. Uma vez que erros identificados são muito freqüentes em uma dada situação de trabalho, a modelagem psicológica pode levar a meios de reduzir seu número. Na análise da confiabilidade humana, funções de alto nível, que exigem experiência, como a estratégia, resolução de problemas, tomada de decisões, apresentam dificuldades significativas, conforme discutido nos itens 2.7 e 2.8.

Para identificar o erro humano, deve-se identificar o *critério de desempenho*. O critério é, em geral, bem definido, discreto e bem conhecido pelo operador do sistema antes da execução de tarefa. Infelizmente, estas propriedades são estranhas às tarefas com alto nível de experiência exigida.

Por exemplo, considere-se a decisão de selecionar a melhor oferta de trabalho. Não há respostas corretas. O candidato deve otimizar a seleção com base em vários critérios de interesse, como salário, local, segurança, etc. Mesmo estas características são apenas previstas, mas não conhecidas. A escolha pode não ter sido a melhor, anos depois, ao se fazer uma reavaliação. Um outro exemplo é relativo a ações na bolsa de valores. Muitas vezes, um investimento é feito baseado nas últimas informações do mercado financeiro. Uma semana depois isto pode mudar. É difícil a consideração sobre o erro humano em tarefas onde a informação é incerta, ou onde os critérios mudam com o tempo.

Em instalações nucleares, como já visto nos itens 2.7 e 2.8, as decisões são tomadas envolvendo o comportamento baseado no conhecimento, ou seja, algum nível de interpretação é exigido dos operadores. As decisões podem ser auxiliadas por sistemas informatizados, mas há um limite em que será necessário uma decisão. A presença do homem é indispensável, por exemplo, em situações de emergência ou diagnóstico de situações complexas não previstas pelos computadores.

Tarefas complexas, que exigem conhecimento, como as anteriores, requerem otimização em vários critérios. Exigem uma consideração entre critérios diferentes e envolvem características quanto à variação no tempo. Além disso, *poderá não haver decisão certa ou errada.* Poderá haver uma melhor decisão para algumas situações, consideradas certas características e o tempo. Mas para um tempo maior, este conhecimento pode não corresponder à melhor situação. A análise da confiabilidade humana ainda não pode lidar adequadamente com o comportamento humano ou fazer previsões muito confiáveis nesses tipos de tarefas complexas, pelo menos considerando o atual nível de conhecimento dos fatores humanos.

É possível analisar o comportamento com diagnósticos que levem a decisões simples, direcionadas por regras. Pode-se estudar, em termos de erros humanos, o diagnóstico de falhas do sistema baseado em informações limitadas. A falha é devido à causa A ou_B e o operador deve inferir qual das duas causas é a correta pela aquisição de informações e testando suas hipóteses. Sua conclusão é correta ou incorreta. A sua ação corretiva é usualmente ditada mais pelos padrões de manutenção, pela prática de recuperação ou por regras de operação e menos pela avaliação de muitas informações que tendem a sobrecarregar a sua capacidade de processamento. De certa forma, a contribuição da psicologia cognitiva tem se revelado muito importante, como já visto nos itens 2.7 e 2.8, para os sistemas especialistas de apoio, oferecendo ao operador um auxílio para lidar com informações.

Ao se usar o termo psicologia cognitiva, compreende-se que se trata de uma linha de pensamento específica dentro da Psicologia: aquela derivada da Teoria do Processamento de Informações. Esta é uma abordagem que assume a possibilidade de se construir modelos sobre as estruturas do psiquismo humano. Este ramo da psicologia tem sido adotado para uso em ACH porque determinados resultados de pesquisas favorecem os estudos sobre a interação homem-máquina, principalmente com relação ao computador como parte de um sistema. Isto se baseia no reconhecimento de que os modelos computacionais de inteligência devem refletir, na sua própria estrutura, as teorias a respeito de como a inteligência se processa no psiquismo humano, e não somente utilizar os dados psicológicos para validar o comportamento de entrada e saída dos sistemas. Uma fonte concreta de teorias sobre as estruturas do psiquismo humano é a psicologia cognitiva.

Embora o esquema de Swain [41] de classificação dos erros receba algumas críticas, principalmente por parte de psicólogos que adotam a psicologia comportamental, porque não se baseia em disfunções do comportamento, ele é útil para selecionar os eventos de interesse. Similarmente à análise da confiabilidade de algum equipamento, na análise da confiabilidade humana dá-se atenção à resposta humana no contexto do sistema.

3.2 Fontes Básicas de Erros Humanos no Trabalho

Embora seja geralmente difícil isolar as causas reais dos erros individuais, é lógico postular que, teoricamente, eles podem ser atribuídos a duas classes ou fontes principais, ou a uma combinação das duas, isto é, fatores individuais ou pessoais e fatores da situação.

Apesar de haver vários indivíduos executando o mesmo trabalho na mesma situação, pode haver grandes diferenças em suas respectivas taxas de erro. Mas, nem sempre pode-se saber que tipos específicos de diferenças individuais deram origem a essas diferenças sistemáticas na taxa de erro. Por outro lado, a situação pode exercer importante influência na taxa de erro. As variáveis da situação podem abranger um campo bem extenso, tais como o projeto de equipamento ou ferramentas, o plano de trabalho, métodos de trabalho, duração dos períodos de trabalho, os recursos físicos disponíveis e o próprio ambiente.

3.2.1 Fatores influenciadores do desempenho

O termo Fatores Influenciadores do Desempenho ("Performance Shaping Factors - PSF's") foi introduzido por Swain [41] para descrever qualquer fator que influencie a confiabilidade humana. Tem sido adotado o termo, simplificadamente PSF, em grande parte da literatura especializada atual [1, 37].

Esses fatores influenciadores do desempenho, também conhecidos como fatores que afetam o desempenho, são classificados em *internos*, *externos* e *estressores*.

Na Tabela 3.2-1 é apresentada uma classificação de alguns Fatores Influenciadores do Desempenho para Sistemas Homem-Máquina, adaptada de [1].

Deve ser notado que alguns dos fatores influenciadores do desempenho listados não são encontrados em instalações nucleares atuais, mas são listados como exemplo para aplicação em outros sistemas homem-máquina. Outros fatores, como problemas particulares que afetam de alguma forma o nível do comportamento, por exemplo, problemas familiares, se situam no contexto dos extressores psicológicos, mas não são passíveis de serem avaliados corretamente.

Os *fatores influenciadores do desempenho internos* são aqueles que operam a partir do indivíduo, de suas características pessoais. São atributos humanos como habilidades e atitudes no trabalho. Se o treinamento foi adequado, geralmente os fatores influenciadores do desempenho internos têm um impacto menor que os externos na confiabilidade humana.

Os *estressores* são efeitos físico-fisiológicos e mental-psicológicos no homem. São causados por sua tarefa e seu papel no sistema homem-máquina. No Apêndice B são fornecidas e discutidas informações sobre o estresse.

Tabela 3.2-1 - Fatores influenciadores do desempenho humano

<table>
<tr><th colspan="2">Externos</th><th>Estressores</th><th>Internos</th></tr>
<tr><th>Características Circunstanciais</th><th>Características das Tarefas e Equipamentos</th><th>Estressores Psicológicos</th><th>Fatores Orgânicos</th></tr>
<tr><th>PSF´s gerais para uma ou mais tarefas em situação de trabalho</th><th>PSF´s específicos de tarefas em trabalhos</th><th>PSF´s que afetam diretamente a tensão mental</th><th>Características pessoais resultantes de influências externas e internas</th></tr>
<tr><td>Características arquitetônicas e/ou Qualidade do meio-ambiente: temperatura, umidade, qualidade do ar e nível de irradiação, iluminação, ruído e vibração/ Horas de trabalho/Horas livres/ Disponibilidade e adequação de equipamentos especiais, ferramental e provisões/Parâmetros operacionais/ Estrutura organizacional (p.ex. autoridade, responsabilidade, canais de comunicação)/Procedimento dos supervisores, cooperadores, representantes de sindicatos e pessoal de normas/Recompensas, reconhecimentos, benefícios, promoções, salário baixo, etc</td><td rowspan="3">Requisitos que exigem a utilização da percepção / Requisitos motores (velocidade, resistência, precisão)/Interação com painéis de controle/Interpretação/Tomada de decisão/Complexidade (carga de informações)/Limitações da tarefa/ Freqüência e repetição/Importância da tarefa/Memória de curto e longo período/ Capacidade de cálculo/ Feedback (obtenção de resultados)/ Adaptação aos tipos de tarefa: discreta ou contínua/Estrutura e meios de comunicação da equipe/Fatores ligados à interface homem-máquina: projetos de equipamentos essenciais, equipamentos de teste, etc.</td><td>Precipitação das ocorrências/Duração do estresse/Velocidade da tarefa/Carga da tarefa/Alto risco de exposição aos perigos/Ameaças (de falhas, perda do emprego)/Monotonia, degradação ou trabalho inexpressivo/Períodos de vigilância longos e irregulares/Conflitos motivados pelo desempenho no trabalho/Ausência reiterada ou comportamento negativo/Privação sensorial/Falta de atenção (ruído, luminosidade, agitação, cintilação, cor)</td><td rowspan="3">Treinamento e experiência anterior/ Estado da prática ou da habilidade corrente (qualificação/variáveis ligadas à personalidade e à inteligência/Motivação e atitudes/Estado emocional/Tensão mental ou física/Conhecimento dos padrões de desempenho requeridos/ Diferenças devidas ao sexo/Condição física/Atitudes baseadas na influência da família ou de outras pessoas ou agentes/ Identificações grupais</td></tr>
<tr><td>Instruções de Tarefas e Trabalhos

Procedimentos utilizados (escritos ou não)/Comunicações orais e escritas/ Precauções e advertências/Método de trabalho/Plano de ação para as instalações (política interna)</td><td>Estressores Fisiológicos
(Afetam diretamente a tensão física)

Duração do estresse/ Fadiga/Desconforto/ Fome ou sede/Temperaturas extremas/ Radiação/Pressões atmosféricas extremas/Insuficiência de oxigênio/ Vibração/Falta de movimentos físicos/ Alterações na saúde, como resfriados,ou gripe, etc</td></tr>
</table>

Os *fatores influenciadores do desempenho externos* são aqueles além do indivíduo, que aparecem por intermédio do ambiente ou da tarefa. Situações de tarefas e características de equipamentos que predispõem os trabalhadores ao incremento de erros incluem os seguintes [1]:

a. espaços de trabalho e leiautes inadequados
   Tarefas de precisão requerem espaços adequados de trabalho e leiautes apropriados. Se algumas partes não estão arranjadas de acordo com os procedimentos do conjunto, a probabilidade de selecionar uma parte incorreta aumenta. Uma cadeira ruim (assento não apropriado) ou projeto ruim do local de trabalho (mesa, controle, etc.) podem causar fadiga, produtividade decrescente e aumento de erros.
b. condições ambientais ruins
   Iluminação inadequada aumenta a dificuldade de realizar tarefas de precisão. Temperatura alta e nível de ruído alto diminuem a motivação e os níveis de esforço, e aumentam a taxa de erros.
c. projeto inadequado de engenharia dos fatores humanos
   Painéis de controle, assim como máquinas e equipamentos de testes mal projetados, revelam uma ergonomia ruim, prejudicando o desempenho. Por exemplo, similaridade de controles, como botões idênticos para diferentes funções.
d. procedimentos auxiliares de trabalho e treinamento inadequado
   Trabalhadores novatos cometem erros, se não são treinados ou iniciados na prática. Manuais de operação ruins e procedimentos ruins levam à incerteza e a erros do operador.
e. supervisão ruim
   Na supervisão se dá o retorno de como corrigir métodos incorretos. Se a supervisão não é boa, continua havendo margem para erros.

3.2.2 Complexidade da tarefa

A complexidade da tarefa é função da quantidade de informações que o trabalhador processa e a qualidade de raciocínio abstrato ou visualização requerida. Obviamente, os erros serão freqüentes se a tarefa for muito complexa. Em condições normais, a capacidade do trabalhador é suficiente, em geral, para a operação de qualquer instalação industrial. Em condições de emergência, há a introdução de complexidades que excedem a capacidade até dos mais habilitados trabalhadores.

Pode-se encontrar um ponto de saturação, como o aumento de carga de informações ao operador, a partir do qual não há mais o processamento de informação. O estresse leva a várias maneiras de compensar a sobrecarga, algumas das quais podem resultar em erro.

Para verificação da complexidade da tarefa, são importantes a freqüência, a repetitividade da tarefa, se a tarefa é mais crítica do que outra, as exigências de cálculo, além de outras considerações que devem ser feitas, como a tomada de decisões, interpretação, memória exigida a curto e longo prazo, ou se é uma atividade dinâmica ou não.

3.2.3 Abordagem da situação de trabalho

Analisar erros humanos, para estimar suas probabilidades, exige a compreensão dos aspectos pessoais e dos sistemas que predispõem a erros. A filosofia básica de engenharia dos fatores humanos advoga que o sistema deve ser projetado para o usuário, melhorando a confiabilidade do sistema.

Enquanto o pensamento industrial tradicional põe a culpa no trabalhador ou na sua falta de competência, a *abordagem da situação de trabalho* examina as demandas das tarefas, dos equipamentos e do ambiente de trabalho para as características que predispõem o trabalhador a cometer erros.

A estratégia da indústria tradicional tem confiado pesadamente na seleção de pessoal, na adequação dos trabalhadores às tarefas, em programas de treinamento e esquemas motivacionais que promovam o alerta mental para reduzir o erro e aumentar a produtividade. A abordagem da situação de trabalho enfatiza a identificação das condições de predisposição ao erro e sua eliminação ou modificação. Esta abordagem considera que os erros usualmente não ocorrem devido às atitudes ruins ou pobres do trabalhador, mas que essas atitudes são induzidas por condições de trabalho deficientes.

As Situações Tendentes a Erros [1] são identificadas como situações de trabalho onde os fatores ergonômicos são tão ruins que a ocorrência de erros é provável. Estas situações demandam dos trabalhadores o que não é compatível com suas capacidades, limitações, experiências e expectativas. Qualquer projeto que viole um forte estereótipo da população pode ser considerado como favorecendo ao erro.

Uma *Situação Tendente ao Acidente* é uma situação que favorece o erro humano resultando, provavelmente, em ferimentos ou danos no equipamento. O termo *propenso a acidente* é freqüentemente aplicado a pessoas específicas. Uma pessoa propensa a acidente é aquela que tem um número proporcionalmente maior de acidentes quando comparada com seus pares. Este conceito perdeu credibilidade quando uma análise estatística demonstrou que o pessoal conhecido como propenso a acidente não cometeu mais erros que o número esperado, se somente fosse considerado o acaso [42].

3.3 Análise e Uso dos Dados de Erro

Da discussão anterior, segue-se, logicamente, que uma possível ação corretiva dependerá do conhecimento sobre as principais fontes de erros humanos. Se há evidência de que os erros variam amplamente para os indivíduos engajados em trabalhos similares, as ações adequadas possíveis relacionam-se com a seleção, treinamento e motivação de pessoal. Com relação à seleção de pessoal, por exemplo, seria conveniente identificar, por meio de procedimentos metódicos de avaliação (testes, dados pessoais que impliquem motivações específicas, etc.) que podem ser usados para avaliar expectativas, quais indivíduos terão, geralmente, as menores taxas de erro. Os processos ou métodos de avaliação, bem como as considerações de motivação e de treinamento, são objeto de estudo da psicologia e não serão tratados neste trabalho.

Se há evidência de que as taxas de erro estão associadas com variáveis da situação (PSF's), o problema é identificar os aspectos particulares da situação que se relacionam com a alta taxa de erro, para se poder tomar alguma medida.

3.4 Estratégia para Lidar com o Erro Humano

3.4.1 Trocar o operador

O primeiro passo na redução do erro humano é identificar suas causas corretamente. Usualmente, a situação de trabalho pode ser melhorada através de um projeto ergonômico para reduzir erros e aumentar a produtividade. Porém, em alguns casos, a situação de trabalho é bem projetada e as tarefas são razoáveis, mas o trabalhador continua a cometer um número inaceitável de erros.

O desempenho insatisfatório pode ser devido a fatores pessoais, tais como:

- indivíduo com habilidade preferencial na mão esquerda (canhoto);
- visão insatisfatória (deficiente);
- surdez parcial;
- habilidades inadequadas.

Estas características e deficiências são usualmente detectadas em uma seleção de pessoal ou são superadas através de ajudas perceptuais (ex.: lentes de contato) e treinamento. Programas de treinamento no trabalho e períodos de qualificação podem privilegiar os novos trabalhadores, com consideração especial na forma de exigências menos rígidas. Porém, depois de um certo período, o pessoal recentemente contratado deve estar desempenhando seu trabalho nos padrões usuais esperados.

Indústrias que requerem desempenho altamente especializado ou decisões em posição de considerável responsabilidade e risco, usualmente exigem certificados de qualificação. Como exemplo, pode-se citar os pilotos de linhas aéreas e operadores de reatores nucleares. Para manter a qualificação, são necessários testes periódicos, inclusive exame médico e retreinamento (requalificação). O treinamento de operadores de usinas nucleares pode ser realizado em simuladores, em reatores de pesquisa, inicialmente, ou mesmo na própria instalação, no sistema de treinamento no trabalho ("on the job training" - ver item 4.2.1).

Freqüentemente, atributos físicos e mentais determinam se haverá uma boa interação entre o trabalhador e as tarefas a serem desempenhadas. Pessoas altas são, na maioria das vezes, melhores jogadores de basquete que as pessoas mais baixas. A tripulação dos tanques russos é selecionada a partir dos menores candidatos, dentre os soldados qualificados para a atuação em tanques. Ocorre muito, também, o deslocamento de um trabalhador de uma ocupação para outra, até que uma boa interação ocorra. Algumas pessoas jamais se sentem ajustadas em um trabalho onde o rodízio é essencial. Se as diferenças individuais são levadas em conta, depois de reconhecidas, os erros podem ser reduzidos.

Problemas de motivação e emocionais podem levar a erros não intencionais no local de trabalho. Trabalhadores com pouca motivação podem cometer erros inaceitáveis, que comprometem a segurança de uma instalação e abaixam o nível da moral de seus companheiros. Algumas vezes, uma alta taxa de erros é o primeiro sinal de alerta que o trabalhador apresenta, indicando que está tendo problemas emocionais. Quanto mais cedo isto é reconhecido pelo supervisor, mais cedo o problema poderá ser solucionado.

3.4.2 Mudar a situação de trabalho

Muito freqüentemente, o trabalhador leva a culpa de cometer erros, causando defeitos e iniciando acidentes, quando, de fato, a situação de trabalho por si mesma é mal projetada e predispõe o trabalhador ao erro. A abordagem da situação de trabalho reconhece que a situação pode ser melhorada, se se levar em conta as limitações humanas, dessa forma reduzindo a probabilidade de erro do operador.

Um processo industrial é tipicamente examinado por um engenheiro de segurança, por um ergonomista ou especialista em fatores humanos, ou um por perito treinado, de maneira que possa identificar situações que induzam a erros que possam levar a acidentes ou a altas taxas de defeito inaceitáveis em tal processo. Quando deficiências ergonômicas são identificadas, estes especialistas podem avaliar o impacto em erros e recomendar mudanças no projeto. As mudanças podem envolver modificações das condições ambientais, métodos de supervisão, projeto de equipamento, técnicas de processamento e equipamentos auxiliares.

Considerações práticas fazem esta abordagem suscetível à omissão de fatores importantes, os quais podem contribuir para geração de erros. Existe uma probabilidade grande de que o especialista não consiga observar, no momento em que ocorre, o erro que está sendo estudado, especialmente se se considerar que é um evento com baixa probabilidade de ocorrência. Uma abordagem alternativa para a identificação de erros causados pela situação envolve a participação de trabalhadores. Uma versão é chamada de *Programa de Remoção de Causa de Erro - RCE*, e consiste de seis elementos básicos, conforme a referência [42].

1. Supervisores de gerente, pessoal de engenharia e pessoal de produção são convencidos do valor do programa RCE;
2. Trabalhadores de produção e coordenadores dos grupos de remoção de causa de erros são treinados na técnica a ser empregada;
3. Trabalhadores do setor de produção aprendem a fazer os relatórios de erros e de situações tendentes a erros, analisar esses relatórios para determinar causas e desenvolver situações escolhidas do projeto para remover ou modificar adequadamente essas causas de erros.
4. Ergonomistas ou outros especialistas avaliam as situações escolhidas do projeto em termos de custo e benefício, e selecionam a melhor dessas situações, ou desenvolvem soluções alternativas;
5. O gerenciamento implementa as melhores soluções e reconhece os esforços do pessoal da produção nos programas de remoção de causa de erro, via implementação das mudanças sugeridas;
6. Auxiliado por dados de entrada, constantemente fornecidos pelo programa, ergonomistas e outros especialistas avaliam as mudanças no processo de produção, sugerindo mudanças conforme a necessidade.

Talvez o melhor fundamento empírico para o programa de remoção de causas de erro e o conceito de grupos que nele trabalham seja encontrado nos resultados de um estudo realizado por Chaney, citado em [37]. Embora este estudo não tenha sido especificamente dirigido à diminuição da geração de erros (o primeiro objetivo era o incremento da taxa de produção), a abordagem foi similar àquela empregada nos

programas de remoção de causa de erro. O estudo de Chaney mostrou três importantes descobertas, relevantes para a abordagem da remoção de causa de erro:

1. A participação dos trabalhadores num programa de melhoria da produção é possível quando o chefe do grupo utiliza técnicas apropriadas de motivação e participação;
2. Quanto maior o nível de participação dos trabalhadores, ou seja quanto mais estiverem envolvidos, melhores serão os resultados;
3. Sugestões de projeto para melhorar o desempenho nas operações industriais podem surgir a partir de tais programas.

As melhores condições relacionadas com a participação de trabalhadores para reduzir erros e produtos defeituosos são encontradas no Japão, nos *Círculos de Controle de Qualidade* (CCQ) [43]. O círculo de controle de qualidade consiste de um grupo pequeno de chefes de trabalhadores e operadores da linha de produção que ajudam na solução de problemas relacionados com a qualidade. O CCQ, como movimento, originou-se no Japão em 1963 e tem algumas similaridades com o grupo de remoção de causa de erro.

No Japão, alguns aspectos da sua prática industrial e cultural contribuem com a maior participação dos trabalhadores em tais programas, como por exemplo:

1. a não existência de um ambiente de culpa;
2. a aceitação de trabalhadores como parte do grupo de gerência da qualidade;
3. o reconhecimento do trabalhador como, de fato, um especialista no assunto;
4. a aceitação das recomendações dos grupos de trabalho nas ações da gerência.

Além disto, a gerência não se envergonha com a sua imperfeição, pois está sinceramente motivada para a descoberta de ineficiências e a sua correção.

3.4.3 Melhorar o lado humano da qualidade

Empresas e organizações em todo o mundo estão implementando programas de qualidade e, em particular, os também conhecidos como programas de *Qualidade Total*. Um número crescente de empresas reconhece que o investimento em qualidade é um dos mais lucrativos. Entretanto, foi somente no início dos anos 1980 que surgiu o interesse pela qualidade dos serviços e pelo comportamento humano [44] no contexto da qualidade.

Ao invés de se concentrar apenas na qualidade do produto, a nova consciência da qualidade enfoca a qualidade dos esforços do indivíduo. Trata-se de inspirar ou motivar as pessoas que produzem bens e serviços para que façam o melhor possível. Essa nova consciência de qualidade não substituirá as idéias tradicionais a respeito do assunto. O novo modo de pensar, segundo a referência [45], completa e amplia os antigos, acrescentando novas dimensões à idéia de desenvolvimento da qualidade, ou seja, melhorar as relações humanas, fortalecer a comunicação, formar espírito de equipe e manter padrões éticos elevados. Em [45] é discutida a idéia de que a mudança no desempenho do indivíduo deve ser realizada segundo a lógica da psicologia, devido à observação de que, dada uma série de circunstâncias, as pessoas e os grupos aos quais pertencem tendem a reagir, por inércia, sempre da mesma maneira. Ou seja, o modo de realizar o trabalho representa um reforço aos padrões antigos de desempenho, independente das tentativas de mudanças focalizadas nas rotinas de trabalho ou a nível organizacional que não considerem aspectos psicológicos. Por outro lado, em [45] se

considera positivamente as mudanças baseadas na lógica da psicologia, pois o ser humano se torna uma potencial fonte de criatividade que pode ser usada no trabalho.

As organizações que se interessam pelo desenvolvimento contínuo da qualidade enfatizam que a qualidade das pessoas é fundamental. A qualidade pessoal é a base de todos os outros tipos de qualidade. A qualidade pessoal é crucial para a auto-estima do indivíduo, a qual, por sua vez determina o seu em bem-estar, sua eficiência, suas atitudes e seu comportamento [45]. Com a aplicação dos conceitos de qualidade total, tem-se obtido melhoras no desempenho das pessoas. Com isso, diminui-se o número de erros nas atividades realizadas. Também as atividades das pessoas em relação à qualidade é um ponto importante, pois favorece o estabelecimento de uma *Cultura da Qualidade*, a qual influencia toda a empresa.

Ou seja, pode-se produzir sistemas extremamente confiáveis e seguros, que toleram os erros humanos, como já discutido anteriormente no capítulo 2 (ver também Apêndice A). A indústria aeronáutica evoluiu ao ponto onde é raro que um único erro cometido precipite um acidente fatal. De fato, o sistema tem tantas verificações, redundâncias, regras de segurança e padrões de qualidade, que são necessários vários (um mínimo de três a quatro) erros humanos sérios, executados em seqüência, para que ocorra um acidente grave.

Da mesma forma, a indústria nuclear também favorece esta *Cultura de Segurança*, e é possível perceber tais cuidados nos conceitos desenvolvidos dentro da filosofia da defesa em profundidade (ver Apêndice A). Poucas indústrias podem se dar ao luxo ou ter recursos para se tornarem tão sofisticadas como as indústrias aeronáutica, astronáutica, ou a nuclear, mas estas servem de modelo no qual outras indústrias podem se basear.

3.4.4 Reduzir o impacto no sistema

Na maioria dos casos, erros humanos não podem ser completamente eliminados, mas podem ser reduzidos a um nível tolerável. Existem sistemas nos quais os erros humanos têm sido reduzidos pela aplicação das técnicas descritas, mas continuam acima do nível tolerado. Entretanto, o impacto no sistema pode ser reduzido. Em outras palavras, o erro ocorre, mas o impacto decorrente no sistema pode ser reduzido ou eliminado quando se detecta este erro precocemente e quando se tomam o mais rapidamente possível as medidas de correção ou de mitigação das suas conseqüências.

Podem ser projetados sistemas nos quais ocorre uma degradação menos acentuada, em vez de falha total, como resposta a um erro humano crítico. A Agência Espacial Norte Americana ("North American Space Agency" - NASA) tem usado essa abordagem há décadas [1]. Quando ocorrem falhas em equipamentos ou erros humanos, estes são rapidamente detectados e recuperados antes que comprometam o sucesso da missão. Isto freqüentemente envolve lançar mão de *equipamentos de retorno*, que permitem a recuperação dos erros e a volta às condições de operação segura, sendo mantidos em linha para o caso de ser necessária sua atuação.

A indústria nuclear também utiliza sistemas de proteção preventiva e de mitigação. Dentre eles podem ser citados, nas usinas nucleares, o princípio de alívio da contenção e os procedimentos de emergência, em caso de perda de refrigeração do núcleo do reator. Com o alívio da contenção, as conseqüências de acidentes são diminuídas, e

com a utilização dos procedimentos de emergência, a fusão do nucleo é evitada em aproximadamente 90% dos casos [46].

A redundância é a chave para um sistema capaz de tolerar os erros. A redundância humana pode ser projetada para operações críticas. Inspetores ou pessoas que verificam ou inspecionam podem ser usados para verificar se uma tarefa humana foi desempenhada corretamente, ou no devido tempo. Também as máquinas podem ser usadas para monitorar o desempenho humano. Altímetros-radares para aeronaves foram desenvolvidas para fornecer redundância para altímetros barométricos, mas também podem alertar o piloto quando o avião desce abaixo de uma altitude previamente estabelecida como aceitável.

É importante notar que o aumento da redundância tem um limite para a confiabilidade do sistema, em decorrência das falhas de causa comum. Depois de um certo ponto, não se consegue mais aumentar o nível de confiabilidade. Falhas de modo comum ou falhas de causa comum são falhas de múltiplos componentes de um sistema devido a uma mesma causa ou evento.

4. QUANTIFICAÇÃO DO ERRO HUMANO

Para se fazer uma boa avaliação do contexto homem-máquina é necessário quantificar os erros humanos, de preferência com uso de probabilidades. O mais indicado é englobar o homem como parte de um sistema, composto de homens e de máquinas, porém analisá-los separadamente. A análise da máquina já vem sendo feita há tempos, sendo relativamente recente a análise do homem enquanto parte de um sistema. Isto vem sendo realizado com o nome genérico de Análise da Confiabilidade Humana que está inserida numa análise mais geral do sistema homem-máquina.

Considerando os números citados no capítulo 3, percebe-se que a porcentagem atribuída ao erro humano na aviação comercial é muito alta (70% em 1987) [37]. Uma explicação plausível para este fato é que o sistema máquina, isto é, o avião, teve uma evolução muito grande, até se tornar extremamente seguro. Pode-se dizer que o implacável efeito da gravidade terrestre incentivou a produção de aeronaves altamente confiáveis, além de ensejar inspeções freqüentes e regras rígidas de operação e manutenção. Da mesma forma isso ocorreu com as usinas nucleares, ou seja, tanto foi investido na confiabilidade de seus sistemas e componentes que o nível de segurança alcançado é considerado dos melhores da indústria em geral.

Por muitas razões, esta melhora geral nas condições da máquina e da sua operação não apresentou o mesmo ritmo, considerando-se o homem como parte do sistema. Ou seja, a taxa de falha do sistema diminui com a melhora dos equipamentos (aumento da confiabilidade de componentes não humanos), portanto ocorre um aumento da confiabilidade do sistema. Entretanto, aumenta a proporção resultante dos erros humanos quando o sistema é considerado como um todo. Isto porque a confiabilidade do homem não aumentou. Assim, para melhorar substancialmente a confiabilidade do sistema homem-máquina, é necessário concentrar os esforços na redução do erro humano. É impossível admitir que o homem não cometa erros ou que seja infalível. Como o homem tem as principais responsabilidades nas comunicações, no controle do tráfico aéreo, na tomada de decisões e na manutenção e no comando da aeronave, os seus erros dominam as estatísticas relacionadas com o transporte aéreo. De forma semelhante, com relação à indústria nuclear, a responsabilidade do homem nas falhas do sistema é grande, senão a principal.

A confiabilidade humana, como já visto, é muito baixa e, por enquanto, é difícil prever alguma mudança para melhor, a não ser com investimentos em educação, treinamento, pesquisas relativas aos mecanismos cognitivos, para compreensão de como e porquê o homem comete erros (modelagem), e melhoria nos projetos de equipamentos de controle, especialmente considerando a participação da informática e da automação.

4.1 Análise da Confiabilidade Humana - ACH

A Análise da Confiabilidade Humana ("Human Reliability Analysis - HRA") é um método pelo qual a confiabilidade humana pode ser estimada. A aplicação mais comum é na avaliação de atos humanos exigidos no contexto de um sistema.

A consideração sobre atos estranhos também é importante. A pessoa, considerada parte de um sistema, pode falhar naquilo que se supõe que ela deva fazer, mas pode também fazer algo completamente diferente do esperado, que pode degradar o sistema (por exemplo, acionar um controle totalmente fora das especificações ou de procedimentos). Este é o ramo fraco da análise da confiabilidade humana. Não é possível antecipar todas as ações humanas aparentemente estranhas e indesejáveis. O melhor que se pode fazer é identificar aquelas ações que têm maior potencial de degradação do sistema, ou seja, que afetam sua confiabilidade e disponibilidade. O estabelecimento de probabilidades estimadas para as ações humanas estranhas é difícil e as probabilidades estão submetidas a incertezas. Freqüentemente, o melhor que se pode fazer é estimar uma faixa bem grande de probabilidades de erros humanos que se acredita poder incluir a probabilidade verdadeira. Afortunadamente, as probabilidades de ações estranhas são usualmente bem baixas [1].

4.1.1 Experiências no campo da análise da confiabilidade humana

A Análise da Confiabilidade Humana modela as tarefas de maneira similar à Avaliação Probabilística de Segurança. Há uma combinação matemática para sintetizar a probabilidade de erro para a tarefa inteira ou para elemento de tarefa. Entretanto, a APS e a ACH se encontram em diferentes níveis, no seu desenvolvimento. Para equipamentos, máquinas, componentes e instrumentação, existem dados de utilização que, com o passar do tempo, tendem a aumentar o conhecimento de comportamento de componentes e melhorar os dados, que se tornam mais confiáveis. Infelizmente, poucas indústrias colecionam dados relativos à confiabilidade humana. Freqüentemente usam-se dados de laboratório, para situações bem específicas. Entretanto, torna-se cada vez mais patente a necessidade destes dados em confiabilidade humana, o que pode mudar a prática existente.

Três áreas que muito têm contribuído para o desenvolvimento deste campo de trabalho são a indústria nuclear, a aeronáutica e a astronáutica, devido aos padrões de qualidade exigidos em decorrência de uma grande preocupação com a segurança.

4.1.2 Análise e previsão

O propósito da Análise da Confiabilidade Humana é analisar o sistema homem-máquina e fazer uma previsão, quantitativa ou qualitativa, do potencial de erro humano. A análise qualitativa usada para projeto de um sistema ou modificação deste é uma das etapas a ser realizada com o propósito de reduzir os efeitos dos erros humanos no sistema até um nível considerado tolerável. Pode envolver uma análise informal da tarefa, uma avaliação de número de erros em um dado período (mesmo erro várias vezes em um mês, ou ano), uma avaliação das conseqüências ou custos envolvidos, e a decisão de ser ou não corrigida a situação, dependendo do que é considerado tolerável para o sistema. Quando vários erros potenciais estão sendo analisados, podem ser avaliados segundo uma escala graduada de 1 a 5 ou 7, para uma probabilidade relativa. Essa abordagem pode ser chamada de *semi-quantitativa*. No caso, é feita pelos especialistas em confiabilidade humana uma ponderação dando maiores valores a erros considerados mais prováveis [37].

A Análise da Confiabilidade Humana *quantitativa* pode ser usada na avaliação probabilística de segurança. O primeiro passo é compreender inteiramente a tarefa a ser desempenhada pelo operador e a sua relação com o desempenho do sistema.

Desta forma, a análise da confiabilidade humana torna-se parte de uma *análise de sistema homem-máquina*, que é um método geral usado para identificar e avaliar problemas de desempenho humano, potenciais ou existentes, considerando-se o contexto do sistema como um todo.

Os elementos principais desta análise do sistema homem-máquina estão itemizados abaixo:

a. compreender e descrever os objetivos do sistema e as funções de interesse;
b. compreender e descrever responsabilidades e critérios de desempenho na análise da tarefa;
   - identificar o comportamento específico requerido das pessoas;
   - identificar vários níveis de detalhe analítico;
   - avaliar a percepção, a cognição e o desempenho do homem (funções motoras);
   - avaliar, em termos de tempo requerido: retroalimentação; precisão exigida; comunicação; manipulação; controle; coordenação com outras tarefas;
c. avaliar características pessoais considerando a situação;
   - avaliar fatores externos que influenciam o desempenho;
   - considerar plantas do local; entrevistas com o pessoal; etc.
   - identificar habilidades, experiência, treinamento e motivação do pessoal que opera e mantém o sistema;
d. analisar tarefas considerando erros humanos potenciais;
   - comparar as capacidades e limitações do pessoal com as demandas da tarefa, de modo a evitar inadequação;
   - observar a situação de trabalho real (o analista deve, ele mesmo se possível, desempenhar a tarefa, para avaliar);
   - usar procedimentos escritos, etc;
e. estimar as probabilidades dos erros humanos potenciais;
   - estimar cada erro potencial descoberto no item anterior;
   - avaliar a freqüência, possibilidade de recuperação, gravidade da conseqüência potencial, custo da mudança para melhorar a situação (tudo relativo aos erros);
f. estimar as conseqüências dos erros humanos;
   - numa indústria, pode haver rejeição ao produto, quando submetido ao controle da qualidade;
   - numa indústria nuclear, um erro não corrigido pode levar a uma exposição à radiação;
   - uma sucessão de erros pode levar a uma catástrofe (ex.: acidente na usina nuclear de Chernobyl, Ucrânia);
   - alguns sistemas não sofrem sensivelmente com variações substanciais nas taxas de erros estimadas para algumas tarefas em particular;
   - fazer uma análise de sensibilidade (análise na qual uma ou mais estimativas de vários parâmetros são variados para observar seus efeitos no sistema ou em parte do mesmo - por exemplo, variar as probabilidades de erros humanos para verificar seu efeito na análise do sistema);
g. recomendar mudanças para melhorar o sistema;
   - opcional, para melhorar a confiabilidade;
   - formular soluções para áreas-problemas;
   - procurar soluções fáceis e não dispendiosas;

- reduzir a complexidade das tarefas;
- aumentar inspeções para melhorar o potencial da recuperação;
- melhorar a qualidade do treinamento;
- comparar o desempenho do sistema antes e depois (verificação).

4.1.3 Histórico

Uma das antigas Análises da Confiabilidade Humana, realizada nos laboratórios da SANDIA (Estados Unidos), em 1952, estimava especulativamente as probabilidades de erros humanos na faixa de 10^{-2} até 2. 10^{-2}, pelo fato de não haver dados mais consistentes [37].

A partir dos anos 1960, fez-se um esforço para desenvolver uma base de dados em confiabilidade humana. Várias técnicas surgiram e foram desenvolvidas, a partir de então. Nesta mesma época, especialistas alertavam sobre o perigo de considerar como eventos independentes os passos de uma determinada tarefa. Dependendo da complexidade da tarefa, isto pode não ficar muito claro. Assim, a Análise da Confiabilidade Humana adotou o critério conservativo. Ou seja, é sempre desejável fazer a previsão da confiabilidade conservativamente, de modo que qualquer maior discrepância com a realidade estará do lado de menores valores de erros e melhor desempenho do sistema.

A partir de 1967 houve grandes progressos e foi introduzido também um método para incluir as dependências dos eventos nas técnicas de análise da confiabilidade humana. Foi feita, então, uma tentativa de usar avaliações de especialistas e métodos de avaliação convencionais para desenvolver uma tabela de erros em tarefas aplicáveis, e calibrar esta escala (faixa de valores) com algumas taxas de erros humano mais conhecidas, obtidas principalmente de indústrias convencionais. Algumas técnicas foram desenvolvidas considerando a modelagem da probabilidade de erro levando em conta o período de tempo disponível como exigência da tarefa.

No começo dos anos 1970 a Técnica para Previsão de Taxas de Erros Humanos ("Technique of Human Error Rate Prediction - THERP"), desenvolvida por Swain [1], despontou como bastante aplicável à previsão do mundo real na indústria e a auxiliar na tomada de decisões sobre projetos industriais. Numerosos experimentos também foram feitos modificando variáveis (os Fatores Influenciadores do Desempenho) nos modelos de computador, fazendo-se as simulações e examinando os resultados.

Atualmente, têm sido feitos estudos no sentido de serem combinados os erros de ação e omissão, baseados nos conceitos de Swain [1], com os princípios de avaliação do desempenho baseado na habilidade, em regras e no conhecimento, na concepção de Rasmussen [27]. Já existem trabalhos em desenvolvimento a respeito disto, notadamente [31, 47], sendo importante esclarecer que esses estudos ainda se encontram em fase inicial. Deve-se notar que os conceitos de Swain [1] são mais difundidos.

4.2 O Problema dos Dados

Todas as técnicas de análise da confiabilidade humana necessitam de dados sobre erros humanos em algum ponto da análise. A síntese e as técnicas de simulação necessitam de probabilidades de erros humanos nominais como elementos básicos, que possam ser combinados ou manipulados de modo a refletir as seqüências específicas das

tarefas, também considerando os fatores influenciadores do desempenho relativos à situação considerada. Os dados são necessários para desenvolver a análise e também para dar validade às hipóteses, aos modelos, e aos procedimentos que dela fazem parte.

4.2.1 A generalização dos dados

Um erro feito por uma pessoa é único. Tem suas próprias causas, motivações, influências externas ou internas, seqüências de ações, impacto no sistema. Porém, admite-se que haja bastante similaridade nas características dos erros, para que possam ser agrupados em categorias. Considera-se também que erros similares, a partir de uma perspectiva comportamental e situacional, têm probabilidades de ocorrência similares. É esta premissa que permite aos analistas a previsão de probabilidades de erros humanos para algumas dadas condições. Se os dados de erros não podem ser assimilados ou combinados, e nem podem ser generalizados para uma gama particular de condições similares, então não poderá haver ciência da confiabilidade humana.

Um pré-requisito para uma base de dados é uma estrutura taxonômica para organizar os dados. A situação ideal, o uso mais eficiente dos dados existentes, prescreve uma estrutura taxonômica única, que qualquer um possa usar. Abordagens diferentes da análise da confiabilidade humana admitem variações no escopo de comportamento do homem, quando considerados para um ponto específico. Em [48] é feita uma comparação entre 14 métodos diferentes para a realização de ACH. Neste documento são discutidos entre alguns itens, os conceitos relacionados aos tipos de erros. Existe o esforço, por parte de alguns, de procurar alguns dados holísticos que possam ser aplicados a trabalhadores que completam com sucesso a tarefa funcional (por exemplo, pousar um avião). Outros desejam dados cobrindo elementos de tarefas (por exemplo, selecionar uma freqüência de rádio). E assim por diante. Infelizmente, devido à multiplicidade das abordagens teóricas da Análise da Confiabilidade Humana, ao nível de detalhes requeridos e às inúmeras diferentes áreas de aplicação (por exemplo, área nuclear, aviação, automobilismo, etc.), um consenso universal numa taxonomia generalizável é uma impossibilidade virtual. Estes fatores têm contribuído para inviabilizar um banco de dados de erros humanos nos moldes dos bancos de dados de confiabilidade de componentes de máquinas.

Um outro impedimento para a estruturação de um banco de dados de erros humanos é a variação do tipo de fontes a partir das quais os erros são coletados. Há quatro fontes básicas de dados em erros: trabalho na área, com dados obtidos em operação real; atividades em simuladores; experimentos de laboratório; e avaliação de especialistas. Dados obtidos em trabalho na área, em situação real, podem englobar dados reais de trabalhos ou tarefas similares [48]. A qualidade dos dados em geral segue a mesma ordem, isto é, os dados obtidos na atuação real são melhores que os obtidos em simuladores, e daí em diante. Os dados menos confiáveis, em razão do maior grau de subjetividade, são os decorrentes da avaliação de especialistas.

Um banco de dados deve conter informações tais que o usuário possa julgar sua qualidade e adotar um intervalo de confiança adequado. Na referência [1], é usado o termo *margem de incerteza* em lugar de limite do confiança usualmente adotado em estatística. O limite de confiança se baseia em dados obtidos de medidas diretas do desempenho humano de tarefas, excluindo dados subjetivos. Na maior parte das vezes, os dados em erros humanos são baseados em avaliações. No entanto, essas margens de incerteza funcionam similarmente aos limites de confiança (vide item 4.2.4). Os dados

devem estar bem documentados, com especificação dos fatores influenciadores do desempenho envolvidos, pessoais e situacionais (ambientais), incluindo também a ocasião em que foram obtidos, de preferência com a especificação da data de coleta. Neste ponto, é muito importante notar que as mudanças e variações em um sistema invalidam dados de sistemas originais, ou seja, sistemas ainda não submetidos a alterações.

No caso de uma operação real ou trabalho na área em que se está fazendo uma ACH, os dados de erros podem ser obtidos por meio de avarias registradas, deficiências do sistema, relatórios de inspeção, registros diários do estado do equipamento, registros de acidentes, ferimentos pessoais, etc. Esses dados podem ser resumidos de várias formas e, se acompanhados de análises estatísticas apropriadas, podem dar indicações das possíveis fontes de erro. Por exemplo, uma grande variação nas taxas de erros dos indivíduos no mesmo trabalho e na mesma situação pode indicar a necessidade de uma análise posterior das variáveis individuais associadas com a taxa de erro. Por sua vez, as diferenças significantes nas taxas de erro entre diferentes situações (tais como diferenças ambientais, métodos de trabalho, etc.) centralizam mais a atenção sobre os fatores da situação.

Os dados de área coletados da indústria são os mais aplicáveis às tarefas estudadas na análise da confiabilidade humana. Infelizmente, são os mais difíceis de serem coletados, pois o erro teria que ser observado por outra pessoa ou relatado pela que errou. Falar dos erros dos outros apresenta algumas dificuldades e há uma certa relutância em falar dos próprios erros. As melhores informações sobre erros humanos estão na área da aeronáutica e nuclear, mas nenhum documento em particular está adequadamente em condições de produzir dados aplicáveis às análises.

Quanto a este ponto em particular, foi concluído recentemente (1995) o levantamento e coleta de dados de operação, inclusive de falhas que incluem considerações sobre erros humanos, referentes à usina nuclear Angra - 1. Para isto foi realizado um trabalho conjunto de FURNAS CENTRAIS ELÉTRICAS S.A. e da NUCLEN ENGENHARIA E SERVIÇOS, desde o início do funcionamento desta usina, em 1985. Para realizar esta tarefa, foram utilizados os registros de operação daquela usina. Além disto, foi estabelecido um programa de coleta sistemática de dados de operação para a usina. Este trabalho proporcionará uma coleção de dados específicos de Angra - 1, que incluem considerações sobre falhas de componentes, sistemas e de erros humanos.

Na simulação, o uso experimental de protótipos, maquetes ou simuladores podem ajudar a identificar fontes potenciais de erros no projeto e no desenvolvimento de sistemas. Exercícios de simulação, que envolvam treinamento inicial ou retreinamento, ou uma qualificação para emissão de certificados, oferecem excelentes oportunidades para detectar erros (por exemplo, qualificação de soldadores). As oportunidades para erros, que constituem informação para o denominador de probabilidades de erros humanos, (ver equação 1, item 4.3) são observadas, assim como os erros (informação para o numerador). O uso de simulador implica em considerar o fato de que os participantes estão altamente motivados para desempenhar as tarefas, por isto considera-se as ações desempenhadas durante o treinamento como eventos não rotineiros. Desta forma, é preciso que o analista faça um ajuste ou uma "calibração" dos dados obtidos.

No Brasil, existe o Centro de Treinamento Avançado com Simulador - CTAS, em Mambucaba (Rio de Janeiro), pertencente a FURNAS. Seu equipamento é uma reprodução quase total dos painéis e mesas de controle da usina simulada (do tipo Angra - 2), abrangendo um sistema de computação digital utilizado para a simulação em

tempo real da usina [49]. As práticas nesse simulador são pré-programadas, com a definição das condições iniciais que representam as condições mais significativas de operação da usina. As condições iniciais podem ser geradas e armazenadas pelo sistema de computação, bem como um grande conjunto de mal funcionamentos com grau de complexidade que pode variar de uma simples falha de instrumento até um acidente com perda de refrigeração do reator. O grau de severidade dos mal funcionamentos, assim como suas causas e o instante da ocorrência, podem ser estabelecidos antecipadamente de tal forma que os treinandos desenvolvem as operações estabelecidas, sendo avaliadas as suas ações conforme padrões esperados de comportamento. Depois da realização de treinamentos, são elaborados relatórios com avaliação dos treinandos, o que também possibilita a geração de dados relacionados com o desempenho humano que podem ser aproveitados para um banco de dados.

Estudos experimentais também geram dados. A bibliografia das ciências comportamentais fornece alguns dados como tempo de reação e critérios de julgamento, mas os dados de erros são controlados (mantidos constantes em relação a outras variáveis ou não são coletados ou não são relacionados). Isto prejudica a avaliação em condições reais.

Uma análise das operações de trabalho e de suas seqüências pode servir para localizar problemas potenciais, onde um sistema novo ou modificado está sendo planejado. Essa análise, às vezes, é feita com base nos projetos técnicos ou em cópias dos originais com o objetivo de identificar fontes potenciais de erro antes do sistema ser desenvolvido.

A avaliação por especialistas é considerada por alguns autores como a fonte de dados menos válida [1, 38]. As desvantagens óbvias incluem a falta de familiaridade do especialista quanto às informações sobre as tarefas e quanto à quantificação (por exemplo, probabilidades). Por outro lado, leva menos tempo que as outras fontes para coletar dados. Essa avaliação de especialistas geralmente não produz dados estimados de probabilidades de erros humanos, mas dados qualitativos. Por outro lado, conforme o avanço do conhecimento de especialistas, principalmente considerando maior desenvolvimento do campo da psicologia cognitiva e também considerando a experiência acumulada com a operação de reatores, pode-se prever uma maior precisão de dados obtidos por especialistas no campo da ACH.

Note-se que os métodos de coleta de dados na área, no laboratório e com a avaliação de especialistas, serão úteis principalmente para a identificação das variáveis da situação (fatores influenciadores do desempenho) que podem estar associados a erros.

4.2.2 Revisão dos dados básicos

Algumas tentativas foram feitas para a estruturação de um banco de dados formal, com detalhes [1]. Na referência [50] foi feita uma revisão detalhada nos bancos de dados existentes, num esforço para avaliar os dados de erros humanos e os esquemas de categorização para aplicação da avaliação probabilística de segurança em instalações nucleares. Foram avaliados nove bancos de dados (da aviação e da indústria nuclear), considerando três categorias:

a. usuários (uso e especialidade);
b. processamento de dados e avaliação (por exemplo: quantificação e recuperabilidade);
c. coleta (custo, relevância).

Os critérios foram orientados para aplicação à operação de usinas nucleares e condições diferentes podem ser encontradas em outras aplicações.

4.2.3 Banco de dados de confiabilidade humana

Em seqüência ao documento [50], a "Nuclear Regulatory Commission - NRC", órgão regulador da indústria nuclear nos EUA, custeou um programa de pesquisas para desenvolver uma estrutura de trabalho conceitual e a implementação de procedimentos em um banco de dados de confiabilidade humana, que daria apoio às análises da confiabilidade humana realizadas para incorporação nas avaliações probabilísticas de segurança de usinas nucleares. Esses estudos deram origem a uma versão revisada da referência [50], o relatório NUREG/CR-2744, de fevereiro de 1983, Volume 2, "A data bank conception and sistems description" [51]. Neste documento, que usou uma bibliografia mais abrangente, os conceitos, métodos de processamento de dados e técnicas de composição de dados foram reavaliados num estudo de aplicabilidade. A referência [1] aproveitou grande parte deste trabalho e introduziu algumas modificações baseadas em resultados deste estudo para serem aplicados na indústria nuclear, sendo possível sua utilização na indústria em geral. Algumas das características que fazem com que as informações deste banco de dados [51] sejam atrativos e aplicáveis são:

1. os dados passam por uma triagem para assegurar que cumpram o critério mínimo (por exemplo: critérios quantitativos, como taxa de erros e probabilidade de erros humanos);
2. revisões administrativas e procedimentos são utilizados para minimizar a categorização inadequada de dados;
3. o banco de dados é estabelecido de maneira a receber dados de campo (de área), de simuladores, de laboratório, e dados analíticos (especialistas);
4. as informações obtidas sobre os fatores influenciadores do desempenho são adaptadas aos dados;
5. regras e procedimentos são estabelecidos para combinação de dados e sua graduação;
6. três níveis diferentes de especificidade oferecem flexibilidade na acumulação de dados de diferentes níveis de detalhes da análise de tarefa;
7. o usuário do banco de dados tem um conjunto de procedimentos para ajudá-lo a encontrar os dados de interesse apropriado;
8. informações adicionais são estabelecidas, visando esclarecer o usuário.

O propósito principal deste banco de dados é apoiar as atividades da Análise de Confiabilidade Humana em avaliações probabilísticas de segurança de usinas nucleares. Há necessidade, ainda, de se desenvolver um banco de dados mais abrangente, que atenda as exigências da análise da confiabilidade humana aplicáveis a outras áreas.

A referência [1] tem sido usada como fonte de dados confiáveis, citada em numerosa bibliografia relacionada com este campo de trabalho, sendo atualmente um documento indispensável para os especialistas do ramo.

Em 1990 foi realizado um encontro técnico em Viena, "Human reliability data collection and modeling", mas ainda não estão disponíveis informações sobre dados, a partir deste encontro. A referência [29] trata dos modelos e exigências de dados aplicáveis à Análise da Confiabilidade Humana.

Outros documentos têm sido publicados em várias áreas de aplicação, sempre enfatizando a necessidade de coletar dados mais consistentes. Dentre esses podem ser citados [52], que trata do desenvolvimento de dados de instalações não nucleares, de

1994, e [53], que é um manual para coleta de dados de reatores de pesquisas, de 1992. Entre outras considerações, a referência [53] cita a dificuldade da disponibilidade de dados e o esforço que tem sido empreendido pela AIEA no sentido de organizar um banco de dados consistente, não apenas para reatores de pesquisas, mas também para instalações do ciclo do combustível, além de instalações industriais convencionais.

4.2.4 Tratamento das incertezas pela Teoria dos Conjuntos Nebulosos

A confiabilidade e o desempenho humanos são afetados por muitos fatores, muitos dos quais não são bem conhecidos. Isso gera incertezas nos dados obtidos sobre erros humanos; as informações são insuficientes e, portanto, o conhecimento é impreciso. Existem, entretanto, algumas abordagens para seu tratamento.

A primeira abordagem considera que a incerteza envolvida nos fatores humanos pode não ser necessariamente probabilística, mas imprecisa ou nebulosa, conforme é tratada na *Teoria dos Conjuntos Nebulosos* [54], conhecida em inglês como "Fuzzy Set Theory". Nessa abordagem, algum esforço vem sendo feito no sentido de se desenvolver uma teoria pela qual as incertezas não probabilísticas ou nebulosas dos fatores humanos e as propriedades probabilísticas das máquinas possam ser tratadas consistentemente.

Na teoria dos conjuntos nebulosos, considera-se a palavra *probabilidade* como restrita aos eventos repetitivos, e o termo *possibilidade* quando se trata de expectativa de eventos não repetitivos. Probabilidade diz respeito ao aleatório, enquanto que o conceito de conjuntos nebulosos diz respeito à indeterminação. Medidas nebulosas são geralmente consideradas como escalas subjetivas.

Na aplicação da lógica nebulosa, o princípio básico é usar todas as informações disponíveis, inclusive as informações nebulosas obtidas por operadores humanos para iniciar um diagnóstico de falha. Em sistemas complexos, por exemplo, a detecção precoce de qualquer estado anormal, o diagnóstico de causa e o ajuste adequado são necessários para a prevenção de acidentes. Nesses casos, os sinais mais importantes são possivelmente detectados através da percepção do operador humano, tais como: cheiro; barulho; indicações não usuais de indicadores, ou padrões, ou instrumentos; qualquer sentimento não usual; sensação de desconforto; vibrações quase imperceptíveis e outros sinais. O diagnóstico usando esse tipo de informação nebulosa parece ser mais adequado, em muitos casos, do que informações convencionais da lógica determinística. Isso se aplica especialmente quando processos industriais complexos, tais como instalações nucleares, estão em condição de operação que foge da normalidade. As informações nebulosas, como um leve ou sutil cheiro de queimado, pode ser uma indicação de perigo imediato, mas não pode ser utilizado efetivamente por um dispositivo de controle de segurança automático baseado em lógica determinística.

Comparando com a análise probabilística, há alguns pontos favoráveis àquela abordagem dita nebulosa. De maneira geral, se um sistema é grande e complexo surgem vários modos de falha de componentes e taxas de falha humana para a análise. É possível a escolha de uma seqüência de eventos em que os dados devam ser considerados de forma diferente daquela relativa a outra seqüência hipoteticamente considerada. Os dados disponíveis se tornam, assim, ambíguos, para uma análise a ser feita por árvore de falhas, no contexto de uma análise probabilística. Por exemplo, em um determinado ponto, um erro de ação pode ser considerado como acionamento indevido de um controle que, se

considerado de outra forma, poderia ser acionamento de um controle no painél indevido. Em particular, os fatores humanos e efeitos ambientais causam ambigüidade, a qual não é compatível com a incerteza estatística utilizada na análise da árvore de falhas. Uma outra diferença da análise por árvore de falhas é que a falha de um componente influencia outro componente. A taxa de influência ou dependência não é, entretanto, claramente avaliada. É necessário adotar "julgamentos de fatores de engenharia". Nesses casos onde a análise de árvore de falhas fica sujeita a ambigüidades, como as discutidas acima, consideradas nebulosas, a teoria dos conjuntos nebulosos sugere a utilização do conceito de "possibilidade" no lugar de probabilidade. Nessa abordagem, não se considera adequado lidar com fatores humanos em termos de probabilidades.

A indeterminação, na teoria dos conjuntos nebulosos, é compreendida, na maioria das vezes, como ambigüidade subjetiva. Porém, pode ser usada num sentido mais abrangente, incluindo a ambigüidade probabilística. A possibilidade é compatível com probabilidade, dado que as portas "e" e "ou" utilizados na árvore de falhas são os mesmos em um caso ou outro.

4.2.5 Tratamento das incertezas com o Teorema de Bayes

Uma outra abordagem no tratamento de incertezas é a utilização do teorema de Bayes [55], que é uma ferramenta apropriada para aglutinar vários tipos de informações na especialização ou atualização de dados de falhas. O teorema de Bayes é fundamental para a atualização de probabilidades, a partir de novas evidências que se tornam disponíveis a partir de dados operacionais observados. Pode ser representado pela equação abaixo [56]:

$$f(\lambda/E) = \frac{f(\lambda).L(E/\lambda)}{\int f(\lambda).L(E/\lambda).d\lambda}$$

Na equação, f (λ/E) é a função densidade de probabilidade de λ dada a evidência E (distribuição " a posteriori "); f (λ) é a função densidade de probabilidade antes da evidência E (distribuição " a posteriori "); L (E/λ) é a função de probabilidade (probabilidade da evidência E dado λ). No Anexo 1 é apresentada uma aplicação numérica do teorema de Bayes.

Para o tratamento das incertezas usando o teorema de Bayes, estas são levadas em consideração estabelecendo-se uma curva de distribuição de probabilidade para cada uma das freqüências elementares. As curvas estabelecidas englobam todas as informações disponíveis obtidas durante um certo tempo, na prática. Estas informações são obtidas a partir do conhecimento que foi adquirido a respeito de um determinado componente ou, no caso, da confiabilidade humana. Os diversos tipos de informações devem ser combinados de modo a fornecer uma única curva de distribuição de probabilidade, para cada uma das freqüências elementares de falhas ou erros humanos. A combinação dessas informações e experiências é feita através de leis básicas de probabilidades e do teorema de Bayes. Com o tempo, novas evidências são obtidas. As informações contidas nessas evidências devem ser incorporadas às curvas de distribuição das taxas, também através do teorema de Bayes. Dessa forma, além da obtenção da curva de distribuição específica, o teorema de Bayes permite que a mesma seja atualizada na medida em que novas informações sejam obtidas. Ou seja, dados sobre a confiabilidade

humana, ou sobre algum dispositivo específico para os quais as informações estão sujeitas à imprecisão, vão sendo corrigidos com dados mais atuais.

Quando evidências operacionais de uma usina estão disponíveis, a especialização e a atualização contínua dos dados de falhas possibilitam que os resultados de uma avaliação probabilística a ser realizada sejam mais específicos para a usina analisada. Então, do ponto de vista da segurança, representam a situação atual ou atualizada da mesma. Caso não estejam disponíveis evidências operacionais, a realização de uma análise probabilística pode ser feita utilizando-se dados de falha genéricos. Em outras palavras, considerando que a usina pertença a uma população de usinas semelhantes, os dados desta população podem ser usados como dados de entrada para a realização de sua Avaliação Probabilística de Segurança.

A noção básica que fundamenta o enfoque adotado é a de que a probabilidade de ocorrência de um dado evento é uma medida do "grau de crença" do indivíduo na possibilidade de realização do evento em questão. Em outras palavras, a probabilidade incorpora o atual "estado de conhecimento" do evento em um dado instante. À medida que o conhecimento obtido aumenta pela incorporação de novas evidências, também a avaliação da probabilidade muda, de modo a refletir o novo estado de conhecimento sobre o assunto.

Para muitos componentes, não existe uma fonte de dados com conteúdo e formato que permita uma seleção não ambígua da distribuição antes do tratamento pelo teorema de Bayes. Por exemplo, nem sempre estão especificados, nos bancos de dados existentes, quais modos de falha estão representados, qual o ambiente para o qual os dados são aplicáveis, etc. Se são considerados dados em erros humanos, a dificuldade é ainda maior.

4.2.6 Tratamento das incertezas utilizando a distribuição lognormal

Qualquer estimativa de probabilidade de erro humano é associada a uma *incerteza*, como visto no item 4.2.1, que se refere à combinação de conhecimento imperfeito e variabilidade estocástica. Pelo fato das probabilidades de erros humanos estimados serem usualmente estimativas de desempenho baseadas em alguns dados relevantes em julgamento, a incerteza expressa reflete a variação das probabilidades de erros humanos previstos pela distribuição adotada, com base na experiência de funcionamento sem falha.

Embora uma coleta sistemática de dados reais não esteja disponível, a preponderância de dados disponíveis sobre o desempenho humano (por exemplo: tempo de reação) indicam que prevalece uma distribuição log-normal ou similar. A abordagem utilizada para o tratamento das incertezas, neste documento, é a utilizada na referência [1], ou seja, tratamento estatístico dos dados utilizando a distribuição lognormal e a adoção de margens de incerteza, como indicado no item 4.2.1. A distribuição lognormal tem sido utilizada nas Análises de Confiabilidade Humana de usinas nucleares, quando para estas é feita a Avaliação Probabilística de Segurança visando o seu licenciamento [57].

A distribuição de freqüência presumida para as variáveis das probabilidades de erros humanos relativas às pessoas e às condições de trabalho não têm sido consistentes na literatura. Em [58] foi adotada uma distribuição log-normal, por apresentar algumas vantagens em relação a outras distribuições, dentre as quais a possibilidade de utilização de programas de computador (por exemplo, os parâmetros de uma distribuição log-normal

podem ser imediatamente determinados pela especificação de dois de seus percentís). Além disso, em [1] é justificada a adoção dessa distribuição por ser a que mais se aproxima da realidade quando se trata de dados de desempenho humano.

No desempenho de pessoas qualificadas, as probabilidades de erros humanos devem cair nas extremidades da curva, perto da abcissa (ou seja, menores erros na distribuição).

Quando as probabilidades de erros humanos são atribuidas a *tarefas* ou *passos de tarefas* como estimativas de desempenho, são expressas como *pontos estimados* dentro de margens de incerteza. A faixa entre a margem superior e a inferior é adotada para incluir pelo menos 90% das probabilidades estimadas de erros humanos fazendo com que, dessa forma, a distribuição hipotética dos dados sem tratamento seja mais realísta.

Na figura 4.3-1 é apresentada a curva lognormal de distribuição de incertezas, observando-se as duas parcelas de 5%, correspondentes às margens de incerteza inferior e superior.

Incertezas em dados para erros humanos são geralmente descritas pela associação de um Fator de Erro - FE com as Probabilidades de Erros Humanos ('Human Error Probabilities - HEP's"). *Fator de erro* é a raiz quadrada da razão entre a margem de incerteza superior e a margem inferior.

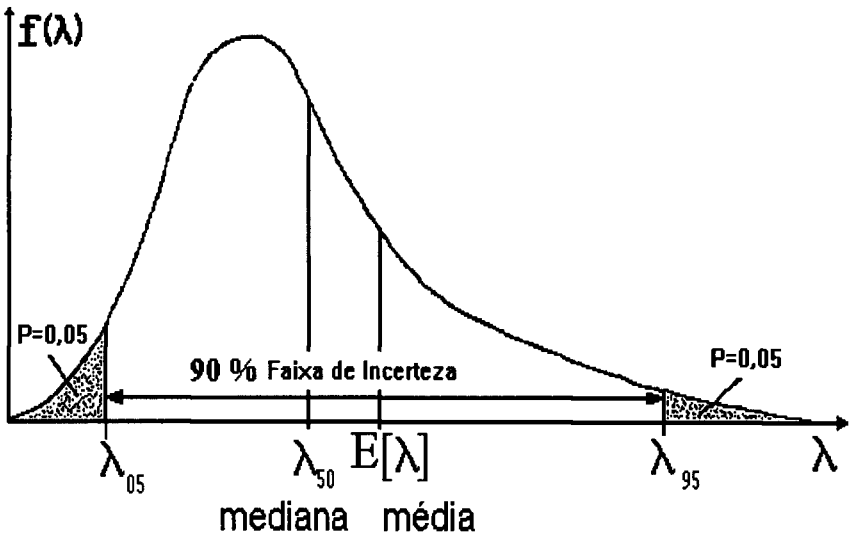


Figura 4.3-1 - Distribuição de incertezas, frações, média e faixa simétrica de 90%

Na referência [1] são encontrados os FE's específicos, sendo que alguns de seus valores característicos são dados na Tabela 4.3-1.

Tabela 4.3-1 - Valores de HEP e de Fatores de Erros associados

Valor do HEP (Mediana)	FE
10^{-1}	2
10^{-3}	3
10^{-5}	10

Com o HEP multiplicado pelo FE obtém-se o valor da probabilidade correspondente aos 95% da margem superior. Com o HEP dividido pelo FE obtém-se o valor da probabilidade correspondente aos 5% da margem inferior.

(HEP) 95% = HEP . FE
(HEP) 5% = HEP/FE

Estas são características da distribuição lognormal; as distribuições são propagadas através da Avaliação Probabilística de Segurança.

4.3 Probabilidade de Erro Humano

A *Probabilidade de Erro Humano* - HEP" é a probabilidade de que um erro ocorrerá, quando é dado o desempenho de uma tarefa (ou passo de tarefa, dependendo da complexidade). Ou seja, a probabilidade de ocorrência por ação [1], ou por demanda de uma tarefa.

Pode-se definir uma *tarefa* como sendo uma unidade de comportamento humano que contribui para a realização de algum objetivo de um sistema ou da função. *Passo de tarefa* ou *elemento de tarefa* é uma divisão arbitrária identificável de uma tarefa ou sub-tarefa. Usualmente consiste de algum tipo de informação que é apresentada ao operador, sendo que este necessita de um certo nível de processamento mental com relação à esta informação e, com base neste, finalmente desencadeia uma ação (resposta). Dependendo da complexidade de uma seqüência de ações a ser analisada, uma tarefa pode se resumir à um passo de tarefa.

Uma tarefa passo a passo, por exemplo, pode ser um procedimento de rotina, ou desempenho baseado em regras, no qual o nível de cognição do operador não é muito exigido. Um exemplo de tarefa pode ser um operador usinando uma parte de uma peça de acordo com uma especificação de projeto. Passos desta tarefa poderiam incluir:

- ligar a máquina;
- ajustar a máquina;
- centrar a peça, etc.

Usando a notação simplificada HEP para representar a Probabilidade de Erro Humano, tem-se:

$$HEP = \frac{\text{número de erros}}{\text{número de oportunidades de erros}} \qquad \text{(Equação 1)}$$

O denominador representa a exposição à tarefa ou elemento de interesse na tarefa. Infelizmente, o denominador da equação acima é freqüentemente difícil de se determinar, porque as oportunidades podem estar escamoteadas, não escritas, ou serem parte de um procedimento no qual seja difícil separar adequadamente os passos seqüenciais. Note-se que este é um ponto importante para o levantamento de um banco de dados, pois se forem registrados apenas erros não se poderá fazer uma comparação. É necessário que também se registre o número de sucessos. Na realidade, quando se trata de dados em desempenho humano, quase nunca se registra o número de sucessos na indústria.

Geralmente os dados de erros humanos são usados na forma de probabilidades de erros humanos, que podem ser atribuídas a erros de omissão e ação. A HEP, acima definida, é a probabilidade de um dado erro humano antes de serem considerados os fatores influenciadores do desempenho. É, portanto, a *HEP nominal.* A probabilidade de erro humano sem considerar a influência condicional das outras tarefas é a *HEP básica*, ou HEPB. A *HEP condicional*, ou HEPC, é a modificação da HEPB com o intuito de levar em conta as influências de outros eventos ou tarefas.

Algumas vezes, os dados em erros humanos são expressos como *Taxas de Erros Humanos* ("Human Error Rate - HER"). A taxa de erro humano é a probabilidade de ocorrência de erro por unidade de tempo. As taxas de erros humanos também podem ser atribuídas a erros de ação e omissão. Em geral são utilizados quando se trata de manutenção, pois nesse caso existe um período definido para as atividades, quando a manutenção é programada (preventiva). De maneira análoga ao caso de falhas de componentes em APS, as probabilidades de erros humanos e as taxas de erros humanos são atribuídas por demanda ou por um determinado período de tempo, respectivamente.

4.3.1 Utilização da HEP

A HEP é utilizada quando somente uma ação é considerada (caso usual). Então, a HEP é usada diretamente na APS como uma *indisponibilidade.* Quando ações múltiplas e repetidas são consideradas, a probabilidade da ocorrência de um erro em qualquer ação deve ser avaliada.

As taxas de erros humanos são utilizadas da mesma maneira geral que as taxas de falhas de componentes, ou seja, por unidade de tempo. Por exemplo, a probabilidade de um erro ser cometido em um tempo t é aproximadamente igual a HER multiplicada pelo tempo t. Isto é uma simplificação, já que $e^{\lambda t}$ é aproximadamente igual a λt, admissível para pequenas diferenças de tempo.

A Tabela 4.3.2 apresenta alguns exemplos de Probabilidades de Erros Humanos usadas em [58], também conhecido por relatório Rassmussen (ou relatório WASH - 1400), que, apesar de ser um documento relativamente antigo (1975), ainda serve de referência para muitos documentos mais recentes, dentre os quais a referência [1].

Quanto à Tabela 4.3-2, deve-se observar que:

a. modificações destas HEP's básicas podem ser feitas com base em fatores específicos relacionados com as tarefas avaliadas; por exemplo, no acionamento de controles, se existe diferença de cor, além de forma e tamanho, pode ser diminuida a HEP;
b. a menos que indicado de outra forma, as estimativas de taxas de erros não consideram pressão de tempo ou estresse relacionados com condições de acidente;
c. para a falha do operador em agir corretamente depois de 30 minutos (maioria das ações, como no caso de um LOCA - "Loss of Coolant Accident") sob condições de estresse extremamente alto, adota-se a HEP de 10^{-1} ;
d. quando nenhuma outra informação está disponível, usa-se como primeira estimativa a HEP de 0,003 para erros de ação ou omissão.

Tabela 4.3.2 - Probabilidades de erros humanos usados no WASH-1400 [58]

HEP Estimada	Atividade
10^{-3}	Seleção de um comutador (ou um par deles) dissimilar em forma ou em localização no painel, por outro que deveria ter sido usado, considerando-se não ter havido erro de decisão. Por exemplo, o operador atua em um comutador grande no lugar de um pequeno, adequado para a ação desejada.
3×10^{-3}	Erro humano de ação genérico; por exemplo, a leitura errada de rótulo ou etiqueta, ocasionando uma seleção errada de comutador.
10^{-2}	Erro humano de omissão genérico; quando não existe nenhum mostrador na sala de controle que indique a situação do item omitido. Exemplo: falha em recolocar manualmente a válvula de teste na sua configuração correta, depois da manutenção. Note-se que essa válvula é operada manualmente.
3×10^{-3}	Erros de omissão quando os itens omitidos estão dentro de ações previstas em procedimento, e não como acima descrito.
3×10^{-2}	Erros simples de cálculo com verificação não apropriada, por exemplo, sem repetir as contas para conferir.
3×10^{-1}	Falha do inspetor em reconhecer erro inicial do operador. Quando existe sinal de erro por um anunciador, esse erro, de valor alto, não se aplica a esse caso.
5×10^{-1}	Falha do inspetor em detectar posição indesejada em válvulas e outros controles durante inspeções, considerando que nenhuma lista de verificação é usada.

4.3.2 Exemplos de utilização de dados de erros humanos

Os exemplos apresentados, incluindo os dados, foram baseados na referência [59].

a. Depois de um teste numa bomba, a probabilidade de que o operador deixe a válvula fechada é 1×10^{-3} (por ação). Qual é a indisponibilidade da válvula devida a contribuição do erro humano?
Note-se que a ação correta era abrir a válvula depois dos testes de manutenção.

   $HEP = 1 \times 10^{-3}$.

   Indisponibilidade da válvula = HEP (permanece fechada) devida a erros humanos.
   Essa contribuição humana à indisponibilidade da válvula (HEP) é somada à contribuição da indisponibilidade da válvula devido ao "hardware", calculada usando a taxa de falha da válvula como componente, pois os eventos são independentes.

b. Quando da ocorrência de um acidente, espera-se que o operador desligue um determinado sistema seguindo procedimentos escritos. Um dos itens desse procedimento exige que o operador desligue dois controles manuais de rotação. Considerar a probabilidade de falha dele não acionar nenhum dos controles (dessa

forma não desligando o sistema, o que seria a ação correta), o que caracteriza a omissão, mesmo consultando o procedimento.

HEP = probabilidade do operador não entender o que está escrito ou de saltar o item relativo ao desligamento dos dois controles.

Nesse caso, os valores de HEP estão na faixa de 10^{-3} a 10^{-2} por omissão (resposta condicionada não se efetuou). Neste exemplo, usa-se o HEP como sendo a probabilidade de que os dois controles permaneçam ligados (a ação correta seria desligar os controles).

c. Dois pares de controles de rotação são adjacentes ao par que deve ser desligado, ao serem girados, como no exemplo anterior (b).
Considerar agora a probabilidade de falha para o desligamento inadvertido (não proposital) de um dos outros dois pares de controles.

$$HEP = HEP_1 \times HEP_2$$

HEP_1 = a probabilidade de omissão, ou seja, a probabilidade de que o par de controles não tenha sido desligado;

HEP_2 = a probabilidade de transposição, ou seja, de que um dos outros pares seja ligado, não correspondendo ao par que deveria ser desligado;

$HEP_1 = 10^{-3}$ a 10^{-2} = mesmo valores do exemplo anterior (b)

$HEP_2 = 5 \times 10^{-1}$ = alto potencial de transposição

Portanto, o valor de HEP a ser usado na APS é aquele que considera a probabilidade de que um dos pares especificados, que não o correto, tenha sido desligado. Prevaleceu a ação errada, e foi considerada a que tem um peso maior, HEP = 5×10^{-1} (usado na APS) e não (conservativamente) o produto das HEP1 e HEP2.

d. Existe uma válvula aberta em um local no qual é realizada manutenção, em intervalos de 30 dias (tempo T). Considerar a taxa de falha para fechamento inadvertido da válvula.

$$f = \frac{1}{T} = \text{freqüência de ação}$$

HEP = a probabilidade de que o operador feche, inadvertidamente, a citada válvula.

Para este caso, os valores de HEP estão na faixa de 10^{-4} a 10^{-3} (fechamento inadvertido de válvulas).
A taxa de erros humanos será, aproximadamente, pelas mesmas razões anteriores:

$$HER = HEP \times f = HEP \times \frac{1}{T} = HEP \times \frac{1}{720} \cong 1{,}5 \times 10^{-3} \text{ (por hora)}$$

$HER = HEP \times 1{,}5 \times 10^{-3}$

ou, $1{,}5 \times 10^{-6}$ para HEP = 10^{-3} ou $1{,}5 \times 10^{-7}$ para HEP = 10^{-4}.

Portanto, a HER estará na faixa compreendida entre $1{,}5 \times 10^{-7}$/hora a $1{,}5 \times 10^{-6}$/hora. A HER usada é a que corresponde à taxa de falha para fechamento inadvertido da válvula.

4.3.3 Dados de erros humanos pós-acidente

Erros humanos podem também ser classificados como pré-acidente e pós-acidente. Erros pré-acidentes são aqueles que ocorrem durante a operação da instalação, manutenção de rotina e testes.

A probabilidade de erros humanos pós-acidente não são bem conhecidos. Em geral, a probabilidade de erros humanos pós-acidentes são próximos de 1 (ou seja, o operador vai errar mesmo), pois o operador está sob tensão extrema, como por exemplo no caso de um grande LOCA, ou quando o operador tem pouco tempo para agir, por exemplo, uns poucos minutos.

4.3.4 Dados de recuperação

Também são usados dados de *Probabilidade de Recuperação* de erros humanos em APS, ("Operator Recovery Probabilities" - ORP). Recuperação ocorre quando o erro acontece e, por causa de uma atividade subseqüente, é corrigido. A ORP é a probabilidade de que o operador recupere o erro ou componente falho em tempo suficiente para desempenho com sucesso. A *Probabilidade de Não-Recuperação* é igual a unidade menos a Probabilidade de Recuperação.

A *Probabilidade de Falha Geral* ("Overal Failure Probability" - OFP) é: OFP = Probabilidade de Falha Inicial x Probabilidade de Não Recuperação.

A Tabela 4.3-3 apresenta alguns exemplos de dados com classes de recuperação, definidas pela descrição, obtidos da referência [1].

Tabela 4.3-3 - Exemplos de dados de probabilidade de não recuperação após a ocorrência de uma falha

Classe de Recuperação	Descrição	Valor numérico típico para a probabilidade de falha na recuperação de um evento (não consegue recuperar)
R1	A falha não parece ser recuperável num período de 20 a 30 minutos, seja da sala de operação ou no próprio equipamento que falhou	1,0
R2	A falha parece ser recuperável num período de 20 a 30 minutos e o equipamento se encontra acessível. A recuperação a partir da sala de controle não parece ser possível	0,5
R3	A falha parece ser recuperável num período de 20 a 30 minutos com ações a partir da sala de controle, mas a recuperação não é considerada de rotina	0,1
R4	A falha parece ser recuperável num período de 20 a 30 minutos, com ações a partir da sala de controle e é considerada de rotina	0,05

4.3.5 Exemplo de utilização de dados de recuperação

Quando uma válvula específica é inadvertidamente fechada, um sinal luminoso é ativado na sala de controle. A válvula pode permanecer fechada por pelo menos oito horas, sem que ocorra qualquer conseqüência. Qual é a probabilidade de que a válvula inadvertidamente fechada (isto é, a indisponibilidade) resulte em danos conseqüentes?

A probabilidade de falha geral é resultante da falha inicial multiplicada pela probabilidade de não recuperação, se considerados como eventos independentes (considerações sobre dependências em erros humanos são discutidas no Capítulo 5).

OFP = HEP x Probabilidade de Não-recuperação

No exemplo,

$OFP = 10^{-3} \times 0{,}05 = 5 \cdot 10^{-5}$

4.3.6 Dados de fatores influenciadores do desempenho

As probabilidades de erros humanos dadas na bibliografia existente sobre APS são aplicáveis em ambientes e estresses normais. Quando o ambiente de trabalho e o estresse mudam por alguma causa (por exemplo, quando pioram, devido às condições de trabalho ruins), as HEP's podem ser aumentadas para levar em conta essas variações específicas. De forma similar, se as condições são melhores, pode-se discutir as HEP's. Os fatores que aumentam ou diminuem as HEP's são os Fatores Influenciadores do Desempenho (PSF's), como visto no Capítulo 3:

$$(HEP)_{\text{Situação particular}} = (HEP)_{\text{Médio/Nominal}} \times PSF$$

Em geral, não existem dados suficientes disponíveis de PSF's. Os valores designados são avaliações baseadas em considerações sobre fatores humanos. Geralmente, os PSF's para situações de pré-acidente alteram de 2 a 10 vezes a HEP. No caso de situações favoráveis, a alteração na HEP varia de 1/2 a 1/10 vezes. É necessário um especialista em fatores humanos para avaliar situações complexas.

5. TÉCNICA PARA A PREVISÃO DE TAXAS DE ERROS HUMANOS

A técnica para a previsão de taxas de erros humanos, conhecida por THERP ("Technique for Human Error Rate Prediction"), é um método para análise de confiabilidade humana que avalia quantitativamente a influência de erros humanos na confiabilidade ou segurança de um sistema. O método usa uma representação esquemática que permite estabelecer uma relação entre atividades humanas com eventos do sistema, em interações que incluem níveis específicos de dependência. Esta representação é feita de maneira análoga à árvore de eventos, discutida no item 5.3.1.

A THERP pode ser definida de outra forma, como um "método de previsão de probabilidade de erros humanos e de avaliação da provável degradação do sistema homem-máquina causada por erros humanos, procedimentos, práticas operacionais, ou outras características do sistema e do homem que influenciam o comportamento do conjunto homem-máquina" [1].

Para propósitos de Avaliação Probabilística de Segurança (APS), a Análise da Confiabilidade Humana deverá incluir apenas aquelas tarefas realizadas pelo componente humano, que tenham um efeito importante no sistema ou na árvore de falhas. Dessa forma, nem todas as tarefas realizadas pelo homem serão analisadas e incluídas na Análise da Confiabilidade Humana. Aquelas consideradas irrelevantes ou desprezíveis, principalmente depois de feita uma análise da sensibilidade no sistema, são excluídas.

5.1 Linhas Gerais da THERP

A THERP pode ser usada na geração de estimativas quantitativas da confiabilidade de atividades humanas, dos efeitos dos PSF's, do desempenho dos equipamentos, e de outras influências do sistema. É um método rápido e relativamente simples (não um modelo hipotético) de suprir com informações e recomendações, os analistas que necessitem de estimativas quantitativas de efeitos dos erros humanos no desempenho do sistema.

A entrada dos resultados da THERP na análise do sistema pode ser utilizado com duas finalidades: recomendar mudanças no sistema e recalcular a probabilidade de falha do mesmo, num procedimento iterativo ou avaliar probabilidades.

A Análise de Sensibilidade, uma das etapas finais da técnica (ver Tabela 5.1-1) é uma análise no qual uma ou mais estimativas de vários parâmetros são variados, de modo a observar seus efeitos no sistema ou em alguma parte do mesmo.

Tabela 5.1-1 Linhas Gerais da THERP para uso em Avaliação Probabilística de Segurança

As quatro fases da Análise da Confiabilidade Humana
FAMILIARIZAÇÃO
Obtenção de informações
Visita à instalação
Revisão dos procedimentos e informações com base na análise do sistema
AVALIAÇÃO QUALITATIVA
Determinar os requisitos de desempenho / entrevistas com o pessoal da instalação
Avaliar a situação de desempenho
Especificar os objetivos do desempenho / análise da tarefa
Identificar o potencial de erros humanos / listar as operações relacionadas
Modelar o desempenho humano / desenvolver árvores THERP
AVALIAÇÃO QUANTITATIVA
Determinar as probabilidades de erros humanos / sucesso e falha
Fazer a estimativa dos efeitos dos PSF's / identificar e quantificar
Avaliar dependências
Considerar os fatores de recuperação dos erros humanos
Calcular a contribuição do erro humano para a probabilidade de falha do sistema
INCORPORAÇÃO
Executar a análise de sensibilidade
Entrar com os resultados na análise do sistema

5.2 Modelando o Desempenho Humano

A modelagem das tarefas, usando árvores de eventos e matemática convencional, para determinar a confiabilidade humana e calcular as probabilidades de sucesso, não apresenta dificuldades. A Tabela 5.2-1 apresenta um resumo de como se faz a modelagem em THERP, usando basicamente o procedimento de decompor e compor as tarefas [1].

Tabela 5.2-1 - Modelando o desempenho humano pela técnica THERP

Abordagem Geral para APS: Decomposição/Composição
1. Dividir o comportamento humano em pequenas etapas, ou seja, atividades simples;
2. Encontrar dados que se apliquem a estas etapas;
3. Recombinar as etapas em estimativas de HEP's para tarefas de APS.

A escolha de HEP's para os elementos individuais das tarefas dos ramos de falhas da árvore de eventos requer, no entanto, uma avaliação substancial por parte do analista. Por isto, é recomendado em [1] que alguém com conhecimentos da tecnologia do desempenho humano faça esta parte da análise. Do ponto de vista de um sistema, uma

ação humana (ou omissão) é um erro se reduz (ou tem o potencial para reduzir) a probabilidade de se encontrar algum resultado desejado.

A Tabela 5.2-2 apresenta um exemplo, para uso em THERP, de como é feita uma decomposição que, basicamente, constitui o início de uma análise de tarefa [1]. No caso, trata-se de trocar um pneu furado em uma rodovia, estando o veículo em movimento, inicialmente.

Tabela 5.2-2 - Exemplo de decomposição na tarefa de trocar pneu furado em uma rodovia

1. Preparar a saída da estrada
   a. olhar o retrovisor
   b. dar seta para direita
      Erro de Omissão - não ligar a seta
      Erro de Ação - ligar errado (esquerda)
   c. mudar para a pista da direita
2. Parar no acostamento
   a. reduzir a velocidade
      Erro de Ação - reduzir bruscamente a velocidade
   b. entrar no acostamento
   c. parar o veículo
      Erro de Omissão - não puxar o freio de mão
   d. executar a sinalização de segurança (triângulo, etc.)
      Erro de Omissão - não executar a sinalização
3. Identificar e tornar disponíveis as ferramentas e o pneu sobressalente necessários
4. Trocar o pneu
   a. bambear os parafusos/posicionar a roda
   b. suspender o carro com o macaco
      Erro de Ação - não colocar o macaco de forma adequada
   c. trocar o pneu
   d. apertar os parafusos até o ponto em que a roda esteja firme
   e. abaixar o carro
   f. apertar os parafusos para fixar a roda, com o carro no chão
5. Guardar o pneu furado e as ferramentas utilizadas
6. Retornar à estrada
   a. ligar o carro
   b. dar seta para a esquerda
      Erro de Omissão - não dar seta
      Erro de Ação - sinalizar errado (direita)
   c. olhar no retrovisor e arrancar

5.3 Representações Gráficas - Árvores Usadas em APS e ACH

5.3.1 Árvore de eventos e árvore de falhas

A APS utiliza representações gráficas para facilitar o trabalho. A primeira é a chamada *árvore de eventos*. Na árvore de eventos, pontos de decisão (nós) são definidos,

existindo duas ou mais possibilidades de saída, por exemplo, falha ou sucesso, sim ou não. Uma desta duas possibilidades pode incluir outras, que podem ser novamente reduzidas a duas possibilidades, e assim sucessivamente, dependendo da necessidade. Se a probabilidade em cada nó for conhecida, as probabilidades das seqüências podem ser calculadas.

As árvores de evento são úteis para a modelagem de cenários. Há várias situações onde um certo distúrbio pode iniciar diferentes cadeias de eventos com muitas conseqüências alternativas.

Um exemplo típico é um estudo de segurança de uma usina nuclear, onde uma gama de distúrbios potenciais é conhecido. Se um distúrbio ocorre, existem sistemas de segurança que devem funcionar. Se o primeiro sistema falha, existem usualmente outros sistemas que podem impedir um acidente sério. Cada cenário corresponde a uma certa combinação de sistemas que falham ou continuam a atuar com sucesso, levando a conseqüências distintas ou não de outros cenários.

Na Figura 5.3-1, é apresentado um exemplo de árvore de eventos.

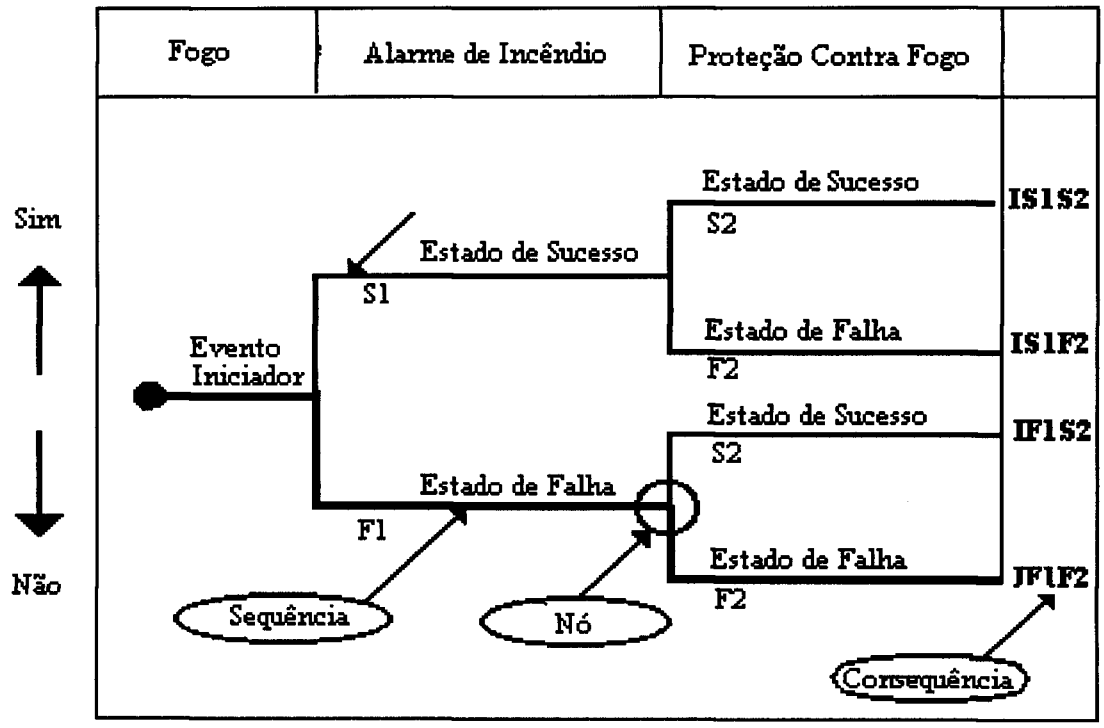


Figura 5.3-1 Árvore de eventos

Evento iniciador é qualquer desafio a uma instalação que exija uma resposta de um sistema de segurança para preservar sua integridade. A seleção de eventos iniciadores é uma tarefa básica em uma APS. Estado de sucesso e de falha correspondem respectivamente aos ramos de sucesso e falha em uma árvore de eventos. Nós são os pontos de decisão onde o ramo se divide em dois outros ramos, continuando com as opções de sucesso e falha (Figura 5.3-1). O cenário se define como a conseqüência de sucesso ou falha dos eventos.

As *árvores de falhas* são excelentes para análise de confiabilidade ou disponibilidade de sistemas. Neste caso, um "sistema " pode ser quase todo tipo de "hardware" ou processo, incluindo interações com pessoas e com o ambiente. Exemplos de questões que podem ser solucionadas por uma árvore de falhas incluem : se o sistema é suficientemente confiável ou não; quais os seus pontos fracos; e quais os componentes que devem ser melhorados para aumentar a confiabilidade.

A árvore de falha é baseada na avaliação de um estado ou evento indesejável, chamado de *evento topo*. A árvore de falha divide a falha do sistema em relações entre as falhas dos componentes. Quando dados numéricos referentes à confiabilidade podem ser atribuidos aos componentes, a confiabilidade do sistema pode ser calculada.

Quando a árvore de falha é completa, todas as combinações de falha que levam ao evento topo podem ser encontradas. Estas são chamadas de *cortes*. Um *corte mínimo* é o menor conjunto de eventos primários, condições de inibição, eventos falhas não desenvolvidas ou qualquer combinação destes, cuja ocorrência provoca a ocorrência do evento topo [56]. A confiabilidade do sistema pode ser calculada baseado nesses cortes mínimos.

A abordagem da árvore de falhas começa em uma falha e trabalha retrospectivamente, ou seja, na seqüencia cronológica inversa, utilizando o raciocínio dedutivo. Na Figura 5.3-2 é apresentada uma árvore de falhas, com valores de probabilidades atribuídas aos eventos básicos e ao evento topo para um caso de dois elementos redundantes ou em paralelo, P1 e P2, em série com elemento V1.

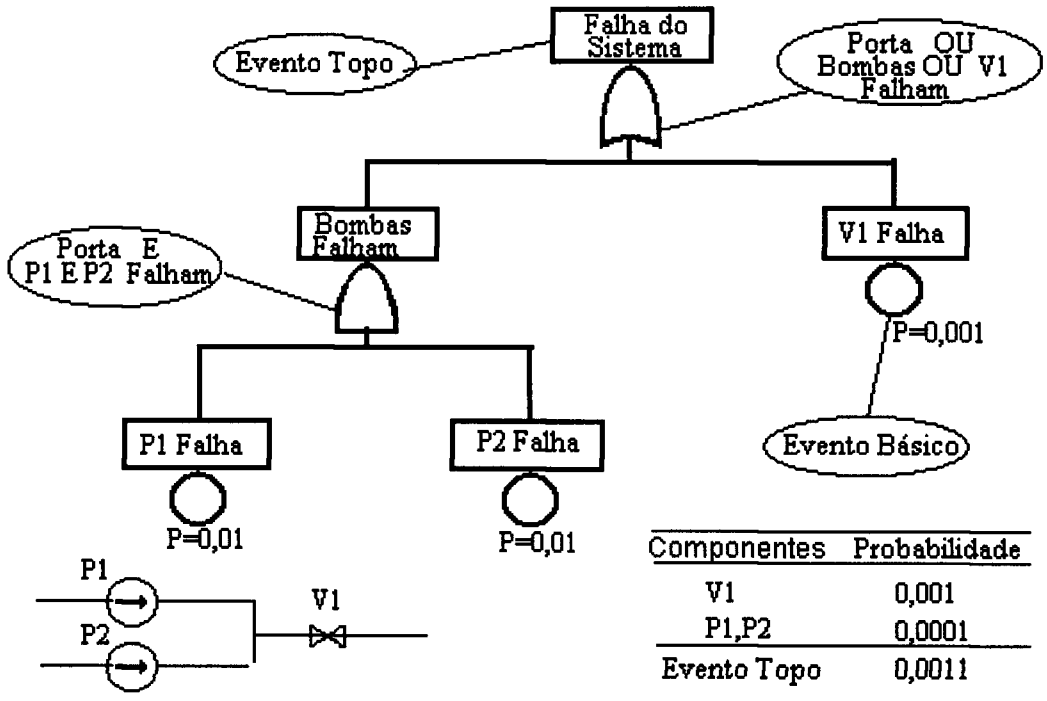


Figura 5.3-2 Exemplo de árvore de falhas para um sistema hipotético

Árvore de eventos e árvores de falhas são recursos normalmente utilizados em APS, não sendo necessário explicações mais detalhadas aqui, visto serem facilmente encontradas na bibliografia sobre o assunto. A bibliografia especializada dá informações mais detalhadas sobre essas representações gráficas [56, 58].

5.3.2 Árvore de Eventos THERP

O instrumento básico para modelar as tarefas e seqüências de tarefas é a árvore de eventos para análise da confiabilidade humana, ou simplificadamente árvore THERP, que também é conhecida como diagrama de árvore de probabilidades THERP.

Esta árvore de eventos começa em qualquer ponto conveniente de uma seqüência de atividades humanas, e utiliza o raciocínio indutivo cronologicamente, ou seja, uma tarefa depois a outra e assim por diante.

Na árvore de eventos THERP, cada desmembramento representa um processo de decisões binárias em cada nó ou ponto de decisão. Ou seja, as únicas escolhas possíveis são desempenho correto ou incorreto. A soma das probabilidades dos eventos só pode ser, portanto, igual a 1.

As probabilidades atribuídas para representar todas as atividades humanas nos ramos são probabilidades condicionais, exceto para o primeiro ramo. A não ser que o primeiro ramo represente o final de alguma outra ávore ou uma tarefa baseada em eventos anteriores prováveis; nesses casos ele será também uma probabilidade condicional.

O uso das probabilidades condicionais leva em conta a interdependência entre os ramos da árvore, outras influências (tarefas anteriores, número de pessoas envolvidadas, etc.), sendo, portanto, uma modificação do HEP básico. Erros graves podem ser cometidos se não forem consideradas as probabilidades condicionais nas estimativas de probabilidade em seus diversos caminhos (através da árvore).

Quando a estimativa das probabilidades condicionais de sucesso ou de falha em cada ramo da árvore THERP tiver sido determinada, a probabilidade de cada trajetória ou caminho na árvore é calculada multiplicando-se as probabilidades em todos os trechos desse caminho. Isto não corresponde a um modelo multiplicativo, ou seja, à simples multiplicação das probabilidades das tarefas, pois leva em conta as dependências entre as mesmas.

Nas árvores THERP sempre haverá uma ramificação binária, conforme visto acima. Sempre será feita a composição em apenas duas ramificações. Nos casos em que se tenha três estados para serem representados, é utilizado um artifício que engloba duas situações de um lado, e a terceira do outro. Por exemplo, considerando-se os três níveis de estresse a serem representados: nível de tensão muito baixo, ótimo, ou moderadamente alto. Neste caso, um ramo pode ser o correspondente ao nível de estresse muito baixo, enquanto que o outro ramo inclui os outros dois níveis de estresse (o Apêndice B fornece mais informações sobre estresse). Não se deve esquecer que a soma das probabilidades nos pontos terminais deverá ser necessariamente igual à unidade

As ramificações da árvore THERP podem representar ações humanas corretas ou incorretas, omissão, erros de discriminação ou processos relacionados com o resultado do desempenho humano. Dessa forma, podem ser representadas tanto as ações plausíveis, assim como as estranhas. Entretanto, nem todas as ações estranhas podem ser

identificadas por antecipação, assim como nem todos os eventos podem ser previstos na árvore THERP, em decorrência da multiplicidade de respostas possíveis de serem apresentadas pelo ser humano. Portanto, embora a previsão de erros muitas vezes tenha uma caráter especulativo, isso não elimina a necessidade de ser feita apesar da considerável variedade de hipóteses oferecida ao analista.

O método pode aceitar dados de quaisquer fontes. Obviamente, os dados adquiridos de situações industriais especificas, quando em análise, constituirão a melhor estimativa de erro para a tarefa (similaridade). Como estas informações são raras, outras fontes deverão ser usadas. Na referência [1] é apresentado um banco de dados, aceitáveis para utilização na indústria (inclusive a nuclear), obtidos a partir de várias fontes. Neste banco de dados, a probabilidade de erro humano ou estimativa é referida como HEP nominal na THERP. Ou seja, sem considerar situações específicas (PSF's). Quando o erro humano não está sendo considerado isoladamente, para a tarefa, usa-se a HEP condicional, que é uma modificação do HEP básico, que leva em conta outras influências (tarefas anteriores, número de pessoas envolvidas, etc.).

Na Figura 5.3-3 são apresentados os diagramas para os sistemas, em paralelo e em série, e as árvores THERP, conforme a referência [1]. Se os eventos têm qualquer influência, um sobre o outro, são considerados dependentes.

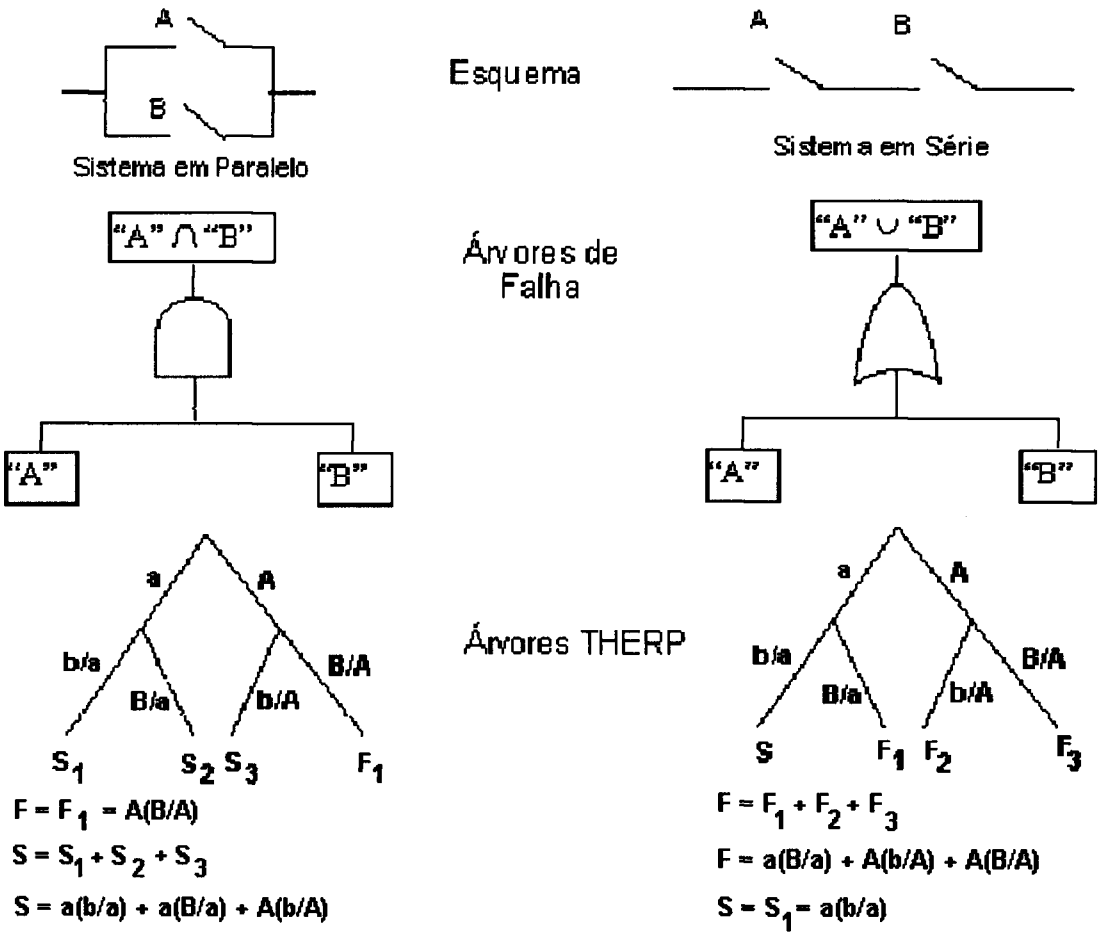


Figura 5.3-3 Diagramas apresentando árvores de falhas e THERP

Um dos maiores problemas na modelagem de tarefas que têm seqüências de comportamento, cada qual com sua probabilidade de falha, é a determinação de como a falha ou sucesso de uma tarefa pode ser relacionada com a falha de outra tarefa. Uma das vantagens da THERP é sua capacidade de levar em conta as interações com um modelo de dependência. Dois eventos são independentes se a probabilidade condicional de um evento é a mesma, caso o outro evento tenha ocorrido ou não. Ou seja, a probabilidade de sucesso na tarefa "B" é a mesma, considerando-se falha ou não na tarefa "A".

A Tabela 5.3-1 fornece a simbologia apresentada na Figura 5.3-3, com modificações para o sistema em paralelo e em série, aplicável em figuras de árvores THERP. A notação de árvores THERP também admite que se substitua, para simplificação, termos como b/A por b', B/A por B', e assim por diante.

Os cálculos referentes às probabilidades de sucesso, S, e de falha, F, são resumidos assim, para o sistema em paralelo:

$S = 1 - A\,(B/A) = a\,(b/a) + a\,(B/a) + A\,(b/A)$

$F = A(B/A)$

Para o sistema em série, $S = a\,(b/a)$ e $F = 1 - a(b/a) = a(B/a) + A(b/A) + A(B/A)$

Tabela 5.3-1 Simbologia para o sistema em paralelo

Tarefa "A" - a primeira tarefa (no caso, fechar a 1° chave do circuito); Tarefa "B" - a segunda tarefa (no caso, fechar a 2ª chave do circuito); a - probabilidade estimada de desempenho, com sucesso, da tarefa "A" (ou desempenho correto); A - probabilidade estimada de desempenho incorreto da ação humana (ou desempenho incorreto) na tarefa "A"; b/a - probabilidade estimada de desempenho com sucesso da tarefa "B", dado a; B/a - probabilidade estimada de desempenho sem sucesso da tarefa "B", dado a; b/A - probabilidade estimada de desempenho com sucesso da tarefa "B" dado A (sem sucesso), ou b'; B/A - probabilidade estimada de desempenho sem sucesso da tarefa "B", dado A (sem sucesso), ou B'; F_n = probabilidade de falha para o ramo n de falha na árvore; F = probabilidade de falha final para a árvore; S_n = probabilidade de sucesso final para o ramo n de sucesso na árvore; S = probabilidade de sucesso final para a árvore; b' - probabilidade estimada de desempenho, com sucesso, depois de falha no desempenho de "A" (equivalente a b/A); B' - probabilidade estimada de desempenho faltoso ou incorreto da tarefa "B", depois de "A" com falha (equivalente a B/A);
Nota: Por simplicidade, omite-se o "ocorrido A" e "ocorrido a", em b/a e B/a, e também em b/A e B/A, de maneira análoga.

A Figura 5.3-4 apresenta, para ilustração, a árvore THERP com os seguintes valores: a = 0,99; b' = 0,95, considerando um sistema em série, e em seguida os cálculos referentes a esta árvore.

$S = a \cdot b = 0{,}9801$

$F = 1 - ab = 1 - 0{,}9801 = 0{,}0199 \sim 0{,}02 \ (2.\ 10^{-2})$

ou

$F = a \cdot B + A \cdot b' + A \cdot B' = 0{,}0099 + 0{,}0095 + 0{,}0005 = 0{,}0199 \sim 0{,}02 \ (2 \cdot 10^{-2})$

Pode-se calcular para o sistema em paralelo de maneira análoga.

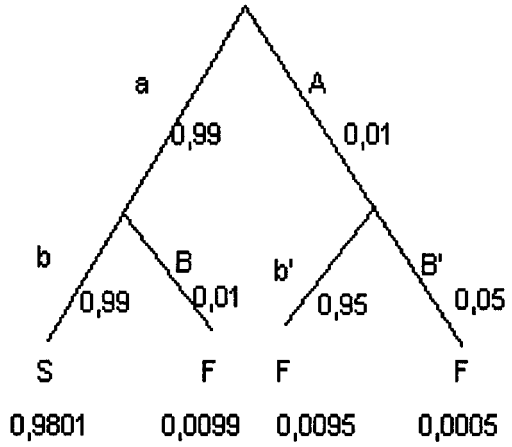


Figura 5.3-4 - Exemplo de árvore THERP com valores

5.4 Dependências em Erros Humanos

Um dos maiores problemas na modelagem de tarefas que têm seqüências de ações, cada qual com sua probabilidade de falha, é a determinação de como a falha ou sucesso de uma tarefa pode ser relacionada com a falha de outra tarefa. Uma das vantagens da THERP é sua capacidade de levar em conta as interações, com um modelo de dependência. Dois eventos são independentes se a probabilidade condicional de um evento é a mesma, caso o outro tenha ocorrido ou não. Ou seja, a probabilidade de sucesso da tarefa "B " é a mesma, considerando-se a falha ou não na tarefa "A " .

Se a independência entre as ações for erradamente adotada, os resultados das probabilidades de erros nas tarefas podem se tornar estimativas muito otimistas. O efeito disso pode ser tal que os resultados para a contribuição de falhas nos sistemas podem estar subestimados .

A dependência pode ocorrer entre pessoas, como por exemplo quando diversos técnicos fazem um trabalho juntos, ou quando um trabalhador verifica a precisão ou a exatidão do trabalho do outro (inspeção). Por exemplo, um aperta um parafuso, e outro verifica o torque, mas sem obedecer à especificação do manual. Neste caso, o último considerou que o primeiro realizou a tarefa corretamente. Se o primeiro errou, o outro vai

errar, porque não conferiu no manual, as instruções. Se os dois usaram o critério correto, a inspeção foi válida. Se o segundo usou o critério correto, a inspeção foi válida também.

Assim, a probabilidade de erro na inspeção (B) muda com o sucesso (a) ou falha (A) da tarefa de apertar o parafuso , ou seja:

$B = B/a < B/A$

Esse aumento em B/A reflete-se na árvore, evitando resultados superotimistas (da estimativa da probabilidade de erro no processo de apertar o parafuso e verificar o torque).

A dependência também pode ocorrer se um indivíduo desempenha várias tarefas, cada uma relacionada com a outra. Nos erros de omissão, a falha na primeira tarefa aumenta as chances de falha da segunda, e assim por diante. Às vezes, as tarefas são altamente relacionadas, e a seqüência inteira pode ser representada por somente uma HEP para omissão. Estas tarefas são consideradas completamente dependentes.

Em erros de ação, o fato de a primeira tarefa a ser feita erroneamente, sem recuperação, aumenta a probabilidade de as outras serem feitas incorretamente. Por exemplo, se o mecânico aperta um parafuso com torque errado, as chances são de que os outros parafusos idênticos, da seqüência, sejam também incorretamente apertados.

Note-se que a dependência pode ser indicada nas árvores de falha, usando-se diferentes símbolos associados aos seus padrões representativos. Tomando-se bastante cuidado, a dependência humana pode ser bem representada na árvore de falhas, obtendo-se, portanto, respostas para o problema da confiabilidade humana. Entretanto, considera-se mais fácil o cálculo das dependencias de ações humanas usando a representação da árvore THERP, pela visualização e pelas limitações aos aspectos considerados em ACH.

5.4.1 Dados e níveis de dependência

Em geral, não há dados específicos para dependências em erros humanos ou erros humanos de causa comum ("commom cause human errors "). Dado que um erro humano tenha sido cometido, a probabilidade para um segundo erro e erros posteriores a serem cometidos são obtidos por avaliação. A referência [1] discute alguns fatores a serem considerados na sua avaliação, e suas conclusões são abaixo resumidas.

$A_1 =$ o primeiro erro cometido

$A_2 =$ o segundo erro cometido

$P(A_1 \text{ e } A_2) = P(A_1) \times P(A_2/A_1)$

$= HEP(1) \times HEP(2/1)$

O modelo de dependência apresentado em [1] lida com as possibilidades desde a independência completa (o evento não é influenciado pelo evento anterior) até a dependência positiva total. A dependência positiva é a que admite por hipótese a existência de uma relação positiva entre eventos, tal que uma falha na primeira tarefa aumenta a probabilidade de falha na segunda tarefa. A mesma dependência existe para a probabilidade de sucesso. Na dependêrncia negativa, a probabilidade de ocorrência da primeira falha diminui a probabilidade de ocorrência da segunda falha.

Para efeito de simplificação, em [1] são definidos cinco níveis de dependências do segundo erro (e dos erros subseqüentes) com o primeiro. Os cinco níveis estão listados na Tabela 5.4-1, com a probabilidade associada aos níveis.

Note-se que, se a independência é completa, a probabilidade do evento 2, ocorrido ou não o evento 1, é sempre a probabilidade do evento 2.

Tabela 5.4.-1 - Níveis de dependências

Nível	HEP (2/1)
Independência total ou completa	HEP do evento 2 ou HEP (2)
Baixa	0,05
Média	0,15
Alta	0,5
Dependência completa ou total	1 (100%)

Estes valores também se aplicam aos erros subseqüentes (depois do segundo) cometidos. Se for necessário calcular mais detalhadamente a probabilidade de falha ou sucesso em uma dada tarefa "N " , dado o sucesso ou falha na tarefa "N - 1 ", pode-se usar de interpolações, no modelo de dependência adotado em [1]. Esta possibilidade não foi considerada no presente trabalho.

5.4.2 Exemplo de dependência

As situações apresentadas na Figura 5.3-3 podem ser usadas para ilustrar as definições anteriores. Tome-se o exemplo do sistema em paralelo, no qual as atividades humanas teriam de ser desempenhadas incorretamente para que o sistema falhe.

As trajetórias ab, aB, e Ab (conduzem ao sucesso, e a falha se reduz à trajetória AB, ou seja, as tarefas "A "e "B " são realizadas incorretamente (ou não realizadas, no caso).

Supondo-se que as tarefas "A "e " B " sejam a abertura de duas válvulas , depois da realização de uma manutenção periódica, o sistema funcionará adequadamente se pelo menos uma delas estiver aberta.

Quanto ao nível de dependência, suponha-se que as válvulas estão dispostas de tal maneira que, se o operador se esquecer de abrir a primeira válvula, se esquecerá também de abrir a segunda válvula. Neste caso, pode-se considerar um nível de dependência total ou de 100% , conforme a Tabela 5.4-1 .Isto significa atribuir um valor de 1 para a probabilidade de falha de "B ", ocorrido "A ". Considere-se ainda, para este exemplo, a HEP para abrir a válvula como sendo de 10^{-2}. Esta é uma probilidade alta, devido à situação considerada no exemplo dado. Tem-se, portanto, A.B = $10^{-2} \times 1 = 10^{-2}$

Entretanto, se fosse adotada a independência completa entre as duas atividades, o cálculo seria: A.B = $10^{-2} \times 10^{-2} = 10^{-4}$. Obviamente, este resultado não reflete a situação hipotética.

Este exemplo simples confirma a necessidade e a importância da incorporação da dependência entre os eventos representados na árvore THERP,

principalmente se for levada em conta a propagação de erros ao longo de árvores THERP maiores

Note-se dos exemplos que o nível de dependência é avaliado conforme as circunstâncias de desempenho da ação considerada. Esta é uma função do analista de fatores humanos, baseado em dados bibliográficos, na realidade ou na simulação, nas avaliações dos operadores no próprio local, ou em considerações dos próprios analistas, conforme discutido no item 4.2.1. No Brasil, o papel de analista de fatores humanos é desempenhado por engenheiros com algum conhecimento em psicologia, ou especialistas em ergonomia. Nos Estados Unidos, este especialista é, em geral, um psicólogo com conhecimento de engenharia ou sistemas complexos, ou um engenheiro com conhecimento no campo da psicologia e fatores humanos.

6. AÇÕES DOS OPERADORES NA SALA DE CONTROLE

Em aeronaves, astronaves, navios, submarinos e outras máquinas complexas, chama-se de *tripulação* o pessoal que, entre outras ações, controla, participa, interfere e comanda a máquina, fazendo parte de uma mesma turma, grupo ou equipe. O termo tripulação se aplica ao pessoal da sala de controle de usinas nucleares, sendo extensivo, também, a outras instalações industriais complexas.

Para o pessoal da sala de controle de instalações como usinas geradoras de energia, incluindo usinas nucleares, no Brasil, utilizam-se as formas compostas, como *pessoal de operação*, ou simplesmente *operadores de reator*.

6.1 Operadores de Reator

No caso de usinas nucleares, seria mais adequado usar *operadores de reator*, para o grupo de pessoas que ficam na sala de controle, em turnos de revezamento com períodos estabelecidos. Estes grupos de no mínimo três operadores, é chefiado por um *supervisor de turno*, que é, em geral, um operador de reator com mais experiência, e que foi qualificado para esta função, como ocorre, por exemplo, no caso da Central Nuclear Almirante Álvaro Alberto, das Centrais Eletricas de Furnas, em Angra dos Reis.

Esses grupos, em seus turnos de operação, são responsáveis pela operação diária da usina nuclear. Trabalham na sala de controle, onde permanecem a maior parte do tempo, pois é nesta sala que se localizam os painéis de controle, além de outros equipamentos e instrumentos. Ocasionalmente, saem da sala de controle para executar uma verificação ou fazer uma inspeção em locais determinados, podendo ou não usar roupas especiais de proteção, dependendo do que vão fazer, ou onde vão atuar.

Os operadores de reator podem ser *iniciantes*, *licenciados* ou *seniors*. Os *iniciantes* são aqueles em fase de treinamento, geralmente no trabalho, ainda não licenciados para a operação da instalação. Enquanto os operadores iniciantes cumprem funções auxiliares, como verificações e inspeções ("checklist"), os *operadores licenciados* cumprem as funções de operação em condições normais, (partida, desligamento, controle de nível de potência, calibração, etc) e em condições anormais (transitórios, emergências, etc). Algumas tarefas de manutenção também são da responsabilidade dos operadores de reator, como a troca de alguns equipamentos ou sua restauração (colocação em condições normais, depois de algum problema ocasional).

Os operadores de reator considerados mais experientes e qualificados são individualmente conhecidos como *operadores senior*, exigindo-se deles certas qualidades em seu perfil psicológico, que os habilitem para as ações de comando e tomada de decisão. Em geral, o supervisor de turno é um operador senior habilitado e qualificado para essa função.

6.2 Tarefas de Monitoramento ou de Vigilância

A tendência para a mecanização e automação sempre maiores está aumentando o número de trabalhadores para os quais a função principal é monitorar uma

operação ou um processo. Obviamente, embora auxiliados por instrumentos e equipamentos de todo o tipo, a função de monitorar se aplica aos operadores de uma usina nuclear. Por exemplo, em *tarefas de monitoramento* típicas (às vezes chamadas de *tarefas de vigilância*), a função do operador é dar sua atenção aos parâmetros de operação, para poder identificar circunstâncias ou eventos que exijam uma resposta adequada de sua parte. De modo geral, essas tarefas de monitoramento caracterizam-se por períodos prolongados de tempo, acompanhados de eventos estimuladores esporádicos, que devem ser identificados. São, de modo geral, tarefas mais simples, tarefas baseadas na habilidade, sendo as que exigem menor nível de cognição ou conhecimento dos operadores, conforme visto anteriormente.

A principal exigência para um operador é identificar corretamente todos ou a maioria dos eventos ou ocorrências que exigem a sua ação. Dados referentes a eventos são apresentados ao operador por vários dispositivos, tais como a tela do vídeo (monitor de computador), diferentes mostradores, painéis complexos, sinais visuais e auditivos, etc. Alguns sinais podem também ser detectados diretamente, em certos casos mesmo da sala de controle, tais como a percepção de uma mudança no ruído de uma máquina, a vibração causada por algum problema em um gerador de vapor (por exemplo), e outros casos. Basicamente, portanto, espera-se do operador a identificação exata de todos os estímulos relevantes, de tal modo que ele tome as ações corretas.

Na troca de turnos, deve ser feita pelos operadores uma *vistoria* ou *inspeção inicial*, pois é um instante de descontinuidade, onde tarefas iniciadas podem não ser completadas ou completadas de maneira diferente da prevista. Este momento é crítico, do ponto de vista da ocorrência de erros humanos. Depois, é feita uma *inspeção de rotina*, em intervalos de tempo definidos. Uma *inspeção ativa* é aquela na qual uma pessoa é direcionada para verificar itens específicos de equipamentos, usualmente via procedimentos escritos. Uma *inspeção passiva* é uma verificação relativamente casual para condições que apresentem desvios nas especificações técnicas associadas aos equipamentos ou instrumentos. Uma vistoria é uma inspeção que utiliza material escrito. Neste caso, a condição de cada item é verificada, com auxílio de uma caneta ou lápis e um impresso adequado. Uma *leitura* ("chek-reading") é a verificação de um ou mais mostradores, confirmando se cada parâmetro está dentro dos limites permitidos (especificações técnicas), não havendo necessidade de material escrito, embora possa ser usado.

6.3 Tarefas Complexas

Para as atividades baseadas em regras, a pessoa deve seguir procedimentos determinados, escritos ou não, para a execução das tarefas. São tarefas mais simples, cujo exemplo mais óbvio é uma verificação e alguma eventual correção.

No entanto, grande parte das atividades realizadas pelo pessoal de operação de uma usina são tarefas complexas, que muitas vezes exigem um diagnóstico e, portanto, um certo grau de conhecimento ou cognição. Isto envolve também elaboração mental e percepção, abrangendo os sentidos da pessoa. Alguns termos relacionados com a cognição foram definidos para uso em ACH, conforme Tabela 6.3-1 [1], comparados com definições baseadas em dicionário [60].

Tabela 6.3-1 - Definição de termos relacionados à cognição

Termo	Definição de dicionário	Para uso neste trabalho
Cognição	Ato ou processo de aprender ou conhecer, incluindo conhecimento anterior e avaliação (julgamento)	Restrito àqueles aspectos de comportamento envolvidos no diagnóstico de eventos anormais
Avaliação (Julgamento)	O processo de formação de uma opinião, por discernimento e comparação	Não usado no modelo da referência [1]. Usado apenas no contexto de estimativas realizadas por especialistas
Perceber	Obter conhecimento ou compreensão: estar ciente através dos sentidos	Usado no sentido bem restrito de "ciência de algo" sem o significado de compreensão. Ex.: "Estou sabendo que alguns anunciadores estão piscando"
Discriminar	Perceber as características peculiares de algo; distinguir um objeto de outro	Distinguir um sinal (ou uma gama de sinais) de outro (ou de outros).
Interpretar	Conceber, formular, formar idéia, à luz de critérios, avaliações ou circunstâncias pessoais	Atribuição de um significado a um padrão de sinais que foram discriminados. Ex : "o nível do refrigerante no tanque A está baixo, o que significa que a bomba não está funcionando"
Diagnóstico	Proposição, relato, afirmação ou conclusão relacionado com a natureza ou causa de algum fenômeno	Atribuição da causa mais provável do evento anormal com o nível exigido para identificar aqueles sistemas ou componentes cuja situação pode ser mudada, de modo a reduzir ou eliminar o problema.
Decidir	Fazer uma escolha ou julgamento	O termo "tomar decisão" (tomada de decisões) é usado em lugar de "decidir"
Tomada de decisão		1. Tomada de decisão como parte de um diagnóstico: o ato de escolher entre diagnósticos alternativos, ou estabelecer a causa mais provável dos padrões de estímulos associados com um evento anormal. 2. Tomada de decisão após o diagnóstico: o ato de escolher quais as ações a serem realizadas após ter sido feito o diagnóstico.
Ação	Consecução de algo, dentro de um período de tempo, em etapas, ou com possibilidades de repetição	Realizar uma ou mais atividades (Ex.: passos ou tarefas) indicados pelo diagnóstico, ou por regras de operação, ou por procedimentos escritos.

O *diagnóstico*, segundo a terminologia adotada em [1], "é a atribuição da(s) causa (s) mais provável (is) de um evento anormal, ou do nível exigido para a

identificação dos sistemas ou componentes cuja situação pode ser modificada, de modo a reduzir ou eliminar o problema". O diagnóstico inclui interpretação e, quando necessário, tomada de decisão referente às condições apresentadas pelo sistema de controle.

A *interpretação* é a atribuição de significados aos padrões de sinais ou estímulos que foram discriminados. Por exemplo, "o nível de refrigerante no tanque A está baixo, o que significa que a bomba não está funcionando, ou há um vazamento em algum lugar ou o instrumento/indicador não está funcionando adequadamente". Se há somente uma única causa possível para o sinal observado, a interpretação é equivalente ao diagnóstico.

Ainda quanto à terminologia, *discriminar* se refere à diferenciar um sinal de um elenco de sinais. Por exemplo, "o nível de refrigerante no tanque A é de 13 metros" ou, se há limites marcados (assinalados no medidor), "o nível de refrigerante está fora dos limites". Neste último caso, um certo nível de interpretação é oferecido ao operador, decorrente do projeto do instrumento, o mostrador. Por exemplo, o ponteiro passa do amarelo para o vermelho.

A *tomada de decisão* se dá em dois níveis:

1) tomada de decisão como parte de um diagnóstico - o ato de escolher entre diagnósticos alternativos, tendo por base os dados que se apresentam. Por exemplo, selecionar a causa mais provável dos padrões apresentados nos mostradores ou indicadores associados com um evento anormal;
2) tomada de decisão após o diagnóstico - o ato de escolher quais as ações a realizar depois que um diagnóstico for feito; na maioria dos casos, estas ações são prescritas por regras ou procedimentos, e a tomada de decisão, neste segundo momento no tempo, não é exigida.

6.4 Outros Fatores Importantes para a Avaliação de Erros de Operadores em Salas de Controle de Usinas Nucleares

Além dos fatores influenciadores do desempenho (PSF), das incertezas estatísticas e das dependências entre as tarefas, outros fatores são importantes e devem ser considerados.

Instruções orais e escritas ou seja, a comunicação entre pessoas, é algo que exige uma grande atenção. Quanto a procedimentos escritos, deve-se notar quem escreveu o que para quem. Em geral, no caso de salas de controle, engenheiros escrevem procedimentos para os operadores de reator, que em geral, têm um nível de conhecimento diferente. Isto provavelmente não se aplica ao Brasil, onde os operadores, em sua maioria, são graduados em física ou engenharia, portanto com o nível de qualificação superior ao exigido para operador de reator, mas se aplica bem a países desenvolvidos, como os Estados Unidos ou Japão, onde os operadores têm um nível de qualificação mais adequado ao cargo que exercem. Por isso, é necessário uma certa adaptação, para que o indivíduo para o qual se destina o procedimento seja capaz de saber o que deve fazer, e portanto, que os objetivos esperados sejam cumpridos. No caso dos Estados Unidos, foi constado que alguns operadores de reator não conseguiam entender procedimentos e também que os procedimentos levavam a resultados não esperados [1].

Um fator de grande importância está relacionado com a gerência e os controles administrativos utilizados. O uso de uma política apropriada de recursos

humanos incentiva e motiva o desempenho mais adequado dos empregados de uma usina nuclear, incluindo os operadores da sala de controle. Também é de grande importância a própria composição da gerência e os níveis de experiência desejáveis para os postos de comando, seja a nível administrativo ou técnico.

Com referência aos operadores de reator, são ressaltados dois aspectos da maior relevância: os fatores de recuperação relacionados com os erros cometidos, e o estresse, associado à situação de trabalho. Os fatores de recuperação previnem ou limitam as conseqüências indesejáveis de um erro humano. O *estresse* na situação de trabalho é discutido no Apêndice B.

6.5 Diagnóstico de Eventos Anormais

Em uma APS, é importante analisar e estimar as HEP's para as respostas do conjunto dos operadores da sala de controle de uma usina nuclear, considerando eventos específicos que resultem em situações anormais. Nesses casos, o desempenho baseado no conhecimento está envolvido, como por exemplo decidir qual o curso de ação a ser tomado ao lidar com um evento anormal. Dada à dificuldade de se encontrar dados aplicáveis a essas situações, modelos para estimar a probabilidade de erros humanos que ocorrem na realização de um diagnóstico em um determinado tempo são adotados por alguns autores, ainda numa fase experimental, como em [1]. Nesta referência, *modelo* é definido como uma abstração que representa simbolicamente a maneira pela qual um sistema funciona operacionalmente, não necessariamente incluindo, para implificação, todas as características nele existente. Os dois modelos adotados em [1] são simplificações para triagem ("screening") e para valores nominais de HEP's.

É importante compreender que os modelos para realizar diagnósticos são usados para estimar probabilidades de erros humanos para o pessoal da sala de controle, considerados coletivamente. Tais modelos fogem, portanto, dos padrões usuais, por exemplo, os de [1] que, na sua maioria, se referem ao desempenho de uma pessoa, individualmente. Foram consideradas grandes incertezas para as áreas-problemas citadas acima, para a estimativa da probabilidade de diagnóstico correto em função do tempo, depois de iniciada a condição anormal. Para fins de cálculo, considerou-se a hipótese de que a estimativa de tempo começa com um sinal compelidor. A validade desse modelo deve ser considerada, até que outros mais realísticos possam ser originados a partir de estudos em simuladores e inspeções detalhadas com dados de trabalho. Mesmo assim, os mesmos devem ser calibrados para o mundo real. O melhor seria que cada instalação fornecesse um treinamento de modo que a maioria dos problemas no diagnosticar pudesse ser eliminada, pela conversão da exigência de comportamento baseado no conhecimento em comportamento baseado em regras.As tabelas relacionadas e incluídas neste item foram adaptadas do capitulo 20 da referência [1].

6.5.1 Modelo de triagem considerando fator tempo

A *triagem* é um ensaio onde, aplicando-se valores conservativos às probabilidades de erros humanos, se avalia a relevância dos mesmos nos valores numéricos obtidos para uma análise probabilística de segurança.

Na Figura 6.5-1 é apresentado um gráfico baseado no modelo de triagem [1], no qual a probabilidade conjunta de erro humano (HEPC) para o diagnóstico é associada ao tempo após o disparo de um sinal compelidor (alarme) indicativo de situação anormal.

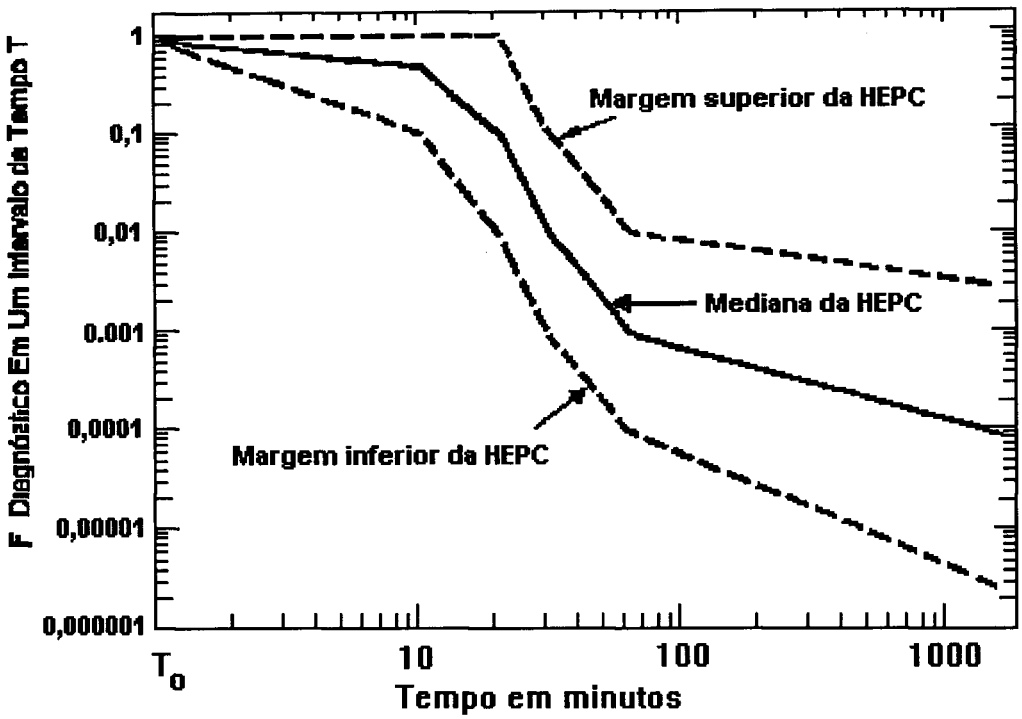


Figura 6.5-1 - Gráfico para triagem de HEPC para diagnóstico considerando tempo após sinal compelidor

Esta figura se aplica à triagem de probabilidades de erros humanos para diagnóstico de um evento anormal, pelo pessoal da sala de controle, num tempo T.

6.5.2 Dados referentes ao modelo de triagem

As Tabelas 6.5.1 e 6.5.2, para triagem de HEP's para ACH, são válidas apenas para condições de pós-acidente. A Tabela 6.5-1, modelo de triagem inicial, serve para estimativas de HEP's para diagnóstico e atividades associadas baseadas em regras, dentro de um tempo T.

Tempo próximo se refere aos casos nos quais o anunciador do segundo evento anormal ocorre enquanto o pessoal da sala de controle ainda continua engajado no diagnostico e nas respostas planejadas para lidar com o primeiro evento. Esta é uma situação específica, mas para uma análise inicial usa-se "dentro de 10 minutos" como definição de tempo próximo.

A Tabela 6.5-1 é válida para atividades desempenhadas pelo pessoal da sala de controle, e se refere a eventos anormais anunciados em um *tempo próximo* que, em geral, são alguns minutos, dependendo de situações específicas, avaliado pelo analista.

Tabela 6.5-1 - Dados para triagem de estimativas de HEPC e FE para diagnóstico dentro de um tempo T de eventos anormais anunciados num tempo próximo

Item	T (minutos* depois de T_0^+)	Mediana da HEPC para diagnóstico de um único evento ou da o primeiro evento	FE	Item	T (minutos* depois de T_0^+)	Medfiana da HEPC para diagnóstico do segundo evento^{++}	FE
(1)	1	1,0	--	(7)	1	1,0	--
(2)	10	0,5	5	(8)	10	1,0	--
(3)	20	0,1	10	(9)	20	0,5	5
(4)	30	0,01	10	(10)	30	0,1	10
				(11)	40	0,01	10
(5)	60	0,001	10	(12)	70	0,001	10
(6)	1500 (~ 1 dia)	0,0001	30	(13)	1510	0,0001	30

* para pontos entre os tempos fornecidos, as medianas e os fatores de erros podem ser escolhidos com ajuda da figura 6.5-1

\+ T_0 é um sinal compelidor de uma situação anormal, e é usualmente tomado como um padrão de anunciadores. A probabilidade de 1,0 (100%) é hipótese de que há uma situação anormal.

++ Designar HEP = 1,0 para o diagnostico do terceiro evento anormal e os subsequentes eventos anormais anunciados no tempo próximos. Para o primeiro e segundo evento as HEP's constam da tabela.

A Tabela 6.5-2 fornece os FE aplicáveis às HEP's para ações baseadas em regras, para o pessoal da sala de controle. Para o item 3 a HEP adotada é igual a 1 se um evento anormal está sendo analisado no caso de não existirem procedimentos; neste caos, é necessária uma avaliação posterior. Essa HEP pode ser reavaliada numa análise subsequente quando termos mais realísticos da falha forem desenvolvidos. Portanto, nesse caso conservativo, considera-se que o operador sempre erra. Os fatores de erro são grandes, refletindo a maior incerteza na atribuição de HEP's para triagem, quando comparado com os HEP's nominais.

Tabela 6.5-2 - Dados para triagem inicial para HEP's e FE's estimados, depois do diagnostico de um evento anormal, para ações baseadas em regras executadas pelo pessoal de operação.

Item	Erro potencial	HEP	FE
	Falha ao desempenhar incorretamente ações baseadas em regras, quando estão disponíveis procedimentos escritos:		
(1)	erros por cada passo crítico, sem fatores de recuperação	0,05	10
(2)	erros por cada passo crítico, com fatores de recuperação	0,025	10
	Falha ao desempenhar ações baseadas em regras, quando não existem ou não são usados procedimentos escritos.		
(3)	erros por cada passo crítico com ou sem fatores de recuperação	1,0	

6.5.3 Exemplo de triagem

Com relação ao comportamento cognitivo em avaliação probabilística de segurança, o que se procura é estimar probabilidades de diagnóstico com sucesso para diversos tempos após o início de um evento anormal. Isto é, para um dado evento ou para qualquer evento anormal considerado em APS, o analista estima quanto demora uma ação para ser realizada em seguida ao anúncio de evento anormal.

Apenas para ilustração, considere-se o exemplo, referente a uma única ação crítica que deve ser realizada no prazo máximo de 25 minutos depois da constatação do evento por sinal compelidor. Considere-se, por exemplo, que seja necessário manipular uma válvula para recirculação do refrigerante após um LOCA. Se a operação não é completada dentro de um determinado período de tempo, ocorre a falha do sistema. Deve ser considerado que essa ação não é uma atuação memorizada para ação de emergência sendo, portanto, necessária a consulta a procedimentos escritos. O exemplo apresentado foi adaptado de [1], incluindo figuras e tabelas.

O período de 25 minutos (conservativo) seria correspondente ao tempo para diagnóstico T_M da Figura 6.5-2.

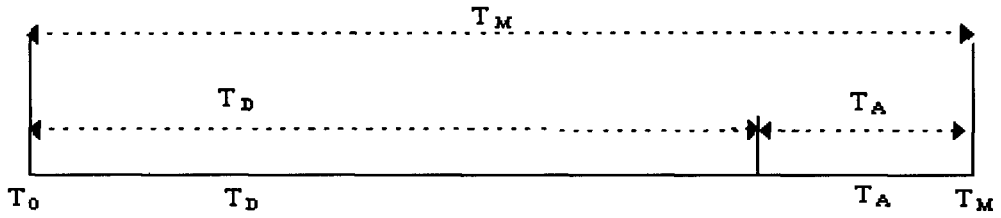


Figura 6.5-2 - Tempo para realização de diagnóstico

O analista de confiabilidade estima, se possível baseado em medidas reais obtidas de condições simuladas, ajustadas para as tensões maiores presumidas do mundo real, quanto tempo demora para desempenhar a atividade baseada em regras. Este seria o tempo T_A da figura. Esse valor de tempo é subtraído dos 25 minutos e o tempo restante (T_D) representa o tempo permitido para um diagnóstico correto. O analista então estima a probabilidade de fazer o diagnóstico correto para aquele tempo, utilizando a Tabela 6.5-1.

Com os dados apresentados, tem-se T_M = 25 minutos como o tempo máximo permitido para realizar o diagnóstico e para executar a única ação crítica requerida no pós-diagnóstico. Dado que o analista estima em 5 minutos o tempo necessário para realizar esta ação (T_A = 5 minutos), tem-se, portanto, 20 minutos para realizar o diagnóstico (T_D):

$T_D = T_M - T_A = 25 - 5 = 20$ minutos

Entrando com este dado na Tabela 6.5-1, tem-se, para 20 minutos e considerando uma única ação crítica, HEPC = 0,1. O que também seria encontrado se, opcionalmente, o gráfico da Figura 6.5-1 fosse utilizado.

Após a realização do diagnóstico, suponha-se o desempenho incorreto da ação a ser realizada, porém com algum fator de recuperação. Com o uso da Tabela 6.5-2 obtém-se a HEPC =0,025.

A Figura 6.5-3 apresenta a árvore THERP para esta situação, ou seja, triagem para situação anormal.

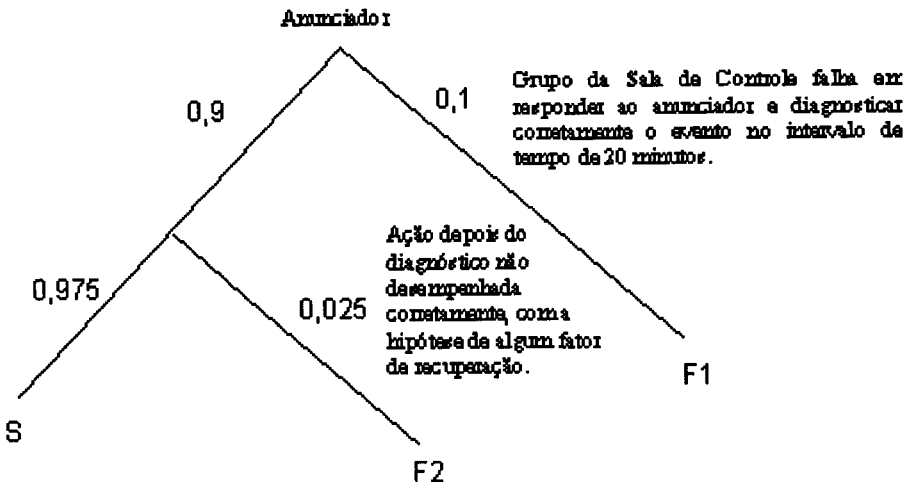


Figura 6.5.-3 - Árvore THERP utilizando valores de triagem de HEPC para diagnóstico e uma ação crítica

Na figura 6.5-3, tem-se:

F_1 - Falha do Grupo da Sala de Controle em não responder ao anunciador e diagnosticar corretamente o evento no intervalo de 20 minutos, conforme a Tabela 6.5-1, item 3, tem-se HEPC = 0,1.

F_2 - Desempenho incorreto da ação, depois do diagnóstico, com a hipótese de algum fator de recuperação, conforme Tabela 6.5-2, item 2, tem-se HEPC = 0,025.

Com a hipótese de uma ação crítica após o diagnóstico, tem-se:

$S = 0,9 \times 0,975 = 0,8774 \cong 0,9$

$F = 1 - S \cong 0,1$

ou

$F = F_1 + F_2 = 0,1 + (0,9 \times 0,025) = 0,1225 \cong 0,1$

6.5.4 Dados Referentes ao Modelo Nominal de Estimativas de HEP's

O modelo nominal de desempenho humano aqui considerado é o relacionado com o diagnóstico, considerando o tempo, numa sala de controle de uma usina nuclear. É em tudo similar ao modelo de triagem apresentado no item 6.5.1, as estimativas sendo, entretanto, mais realísticas, logo, não conservativas. As observações feitas para o modelo de triagem são válidas para o modelo nominal. As avaliações não são mais para se verificar se um item merece ser considerado em detalhe posteriormente, devendo os resultados ser incorporados à ACH e, se for o caso, à APS.

Tanto o gráfico apresentado na Figura 6.5-4, quanto a Tabela 6.5-3 [1], são utilizados para estimar HEP's para diagnóstico pelo pessoal da sala de controle, considerando o grupo de operadores, não o indivíduo. O gráfico é utilizado para se obter estimativas de HEP's conjuntas e as margens de incertezas para diagnóstico de evento anormal.

Entretanto, para a execução das atividades baseadas em regras subsequentes ao diagnóstico, toma-se o desempenho de uma pessoa. Para isto, se mais de uma pessoa estiver envolvida, deve ser feito um ajuste, usando a Tabela 6.5-4 [61]. Note-se que o modelo nominal para diagnóstico é aquele para o qual não são consideradas PSF's específicas para a situação.

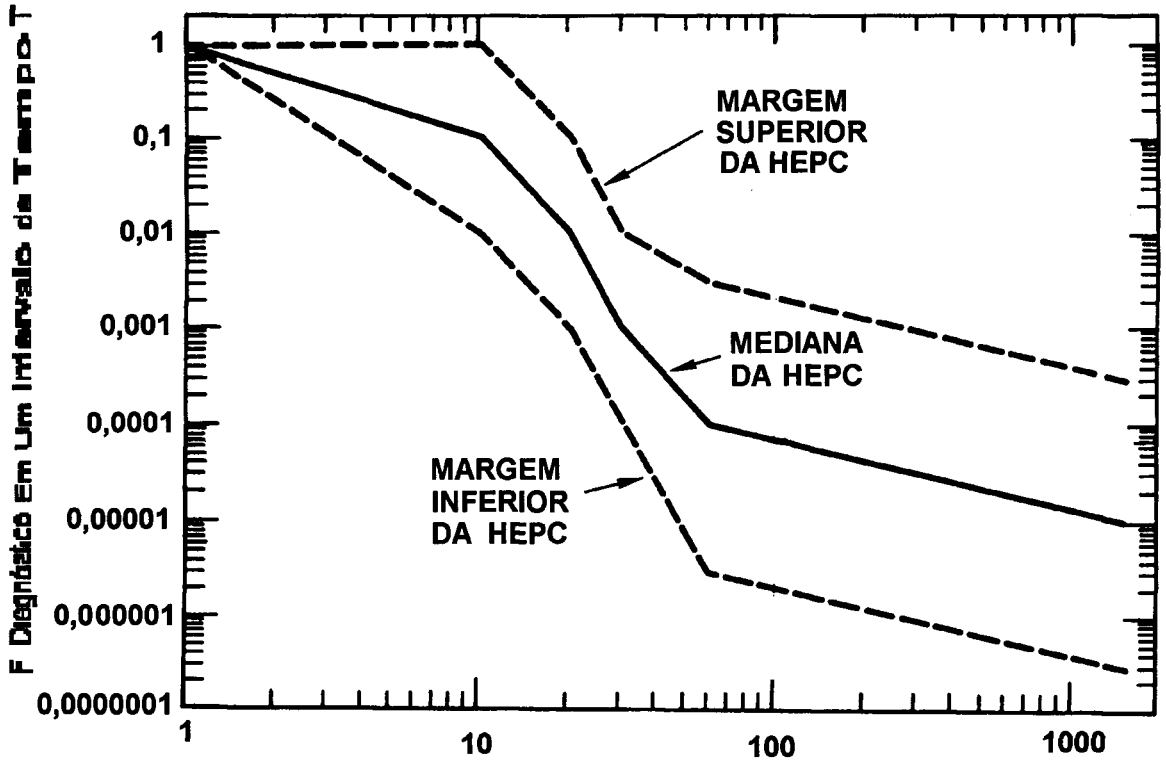


Figura 6.5-4 - Gráfico para estimativas de HEPC com base no modelo nominal para diagnóstico, considerando o tempo T em minutos depois de um alarme de situação anormal

A Tabela 6.5-4 se aplica aos operadores presentes na sala de controle disponíveis para tomar as ações posteriores ao diagnóstico e seus níveis de dependência. As hipóteses apresentadas são nominais, podendo ser modificadas para situações específicas.

Tabela 6.5-3 - Dados de HEP's e FE's para diagnóstico de evento anormal para o pessoal da sala de controle de uma usina nuclear, baseado no modelo nominal para diagnóstico

Nota: Os dados referem-se a estimativas de HEP's e FE's para o pessoal da sala de controle considerando-se o tempo, e valem apenas para o diagnóstico não incluindo o tempo requerido para desempenhar as tarefas após o diagnóstico.

Item	T depois de To em minutos	Mediana da HEPC para diagnóstico de um único evento, ou para o 1° evento	FE	Item	T depois de To em minutos	Mediana da HEPC para diagnóstico do 2° evento	FE	Item	T depois de To em minutos	Mediana da HEPC para diagnóstico do 3° evento	FE
(1)	1	1,0	--	(7)	1	1,0	--	(14)	1	1,0	--
(2)	10	0,1	10	(8)	10	1,0	--	(15)	10	1,0	--
(3)	20	0,01	10	(9)	20	0,1	10	(16)	20	1,0	--
(4)	30	0,001	10	(10)	30	0,01	10	(17)	30	0,1	10
				(11)	40	0,001	10	(18)	40	0,01	10
								(19)	50	0,0001	10
(5)	60	0,0001	30								
				(12)	70	0,0001	30				
								(20)	80	0,0001	30
(6)	1500	0,00001	30								
				(13)	1510	0,00001	30				
								(21)	1520	0,00001	30

Atenção: Todas as observações feitas para os dados referentes à triagem para diagnóstico são válidas para o os dados nominais. T_0 é o ponto de partida, ou de anúncio do evento.

Uma abordagem alternativa é realizar uma análise detalhada da tarefa, incluindo as ações após o diagnóstico. Nesse caso, o modelo nominal para diagnóstico não deverá ser usado. Obviamente, esta abordagem alternativa exigirá muito mais recursos de análise, como as de um especialista treinado e qualificado em comportamento humano.

Tabela 6.5-4 - Nível de dependência, considerando número de operadores de reator e consultores técnicos

	Tempo após reconhecimento de um evento anormal	Operadores de reatores atuando na unidade afetada *	Níveis de dependência interpessoal **
Item (1)	0 a 1 minuto	• Operador de reator em serviço	
(2)	em 1 minuto	• Operador de reator em serviço • operador senior (efetivo ou supervisor de turno)	Alto nível de dependência com o operador
(3)	aos 5 minutos	• Operador de reator em serviço • operador senior efetivo • supervisor de turno • (um ou mais operadores auxiliares +)	Alto nível de dependência entre o operador de reator e o operador sênior Baixo nível de dependência a nível moderado de dependência do supervisor de turno com os outros operadores
(4)	aos 15 minutos	• Operador de reator em serviço • operador senior efetivo • supervisor de turno • Supervisor técnico • (um ou mais operadores auxiliares +)	Alto nível de dependência entre o operador de reator e o operador senior Nível de dependência baixo a moderado do supervisor de turno com os demais operadores Nível de dependência baixo a moderado com os outros para diagnóstico e outros eventos mais importantes Alto nível de dependência ou dependência completa para operações detalhadas

Observações:

* Nenhum credito é dado a operadores de reatores além daqueles do turno

** Esta coluna indica a dependência entre as pessoas situadas na sala do reator. Os níveis de dependência são tomados como constantes com o tempo e podem ser modificados em uma análise específica para cada unidade.

\+ A disponibilidade de operadores auxiliares após de 5 minutos de reconhecimento do evento e o nível de dependência relacionados aos mesmos devem ser estimados levando em conta a unidade e a situação específica.

A Tabela 6.5-5 apresenta as linhas gerais para ajustar as probabilidades de erros humanos ao diagnóstico, considerando o tempo na sala de controle, pelo grupo que está operando o reator [1]. A tabela aplica-se ao gráfico da Figura 6.5-4. Os ajustes devem ser considerados pelo analista.

Tabela 6.5-5 - Linhas gerais para ajustes de HEP utilizando o gráfico da Figura 6.5-4

Item	Regras Gerais
(1)	Use margem superior da HEPC : (a) se o evento não é coberto em treinamento; ou (b) se o evento é coberto, mas não é praticado, exceto no treinamento inicial de operadores licenciados; ou (c) se a vistoria e as entrevistas com os operadores mostram que nem todos eles conhecem as características apresentadas em mostradores ou instrumentos associadas ao evento.
(2)	Use margem inferior da HEPC: (a) se o evento é um evento clássico bem conhecido (e estudado, como o incidente de TMI - 2) e os operadores praticaram o mesmo em exercícios simulados de requalificação; e (b) se a vistoria e entrevistas indicam que todos os operadores tem um bom reconhecimento verbal dos padrões de estímulos e sabem o que fazer, ou que procedimentos escritos devem seguir.
(3)	Use a Probabilidade Nominal de Erros Humanos: (a) se a única prática do evento é no exercício simulado de requalificação, sendo que todos os operadores participaram; ou (b) se nenhuma das regras acima se aplica, para limite superior ou inferior.

A Tabela 6.5-6 apresenta o decréscimo estimado nas probabilidades nominais de erros humanos, resultante da aplicação de boas práticas erganômicas em de usinas nucleares [1].

Os valores das Tabelas 6.5-5 e 6.5-6, se aplicam para a maioria das instalações industriais, principalmente as nucleares.

Quanto à observação referente às novas tecnologias de mostradores utilizando sistemas digitais e computadores, na Tabela 6.5-6, os dados de estimativas de erros humanos ainda não se encontram disponíveis, sendo necessário ainda muita pesquisa para incluir os mesmos em bancos de dados confiáveis. Neste aspecto, na referência [35] é observado que o desenvolvimento da automação e utilização de controles avançados, quando centradas na máquina, induz ao aparecimento de novos erros. De acordo com a mesma referência, isto poderia ser solucionado se a automação fosse centrada no homem, devido aos aspectos relacionados com o desempenho baseado no conhecimento, que é o mais envolvido quando se trata de diagnóstico ou de qualquer atividade onde exista interpretação.

Tabela 6.5-6 - Decréscimo Estimado nas Probabilidades Nominais de Erros Humanos Resultante de Aplicação de Boas Práticas Ergonômicas em Usinas Nucleares

Se existem	Decréscimo resultante nas probabilidades de erros humanos *
Boa prática de engenharia de fatores humanos no projeto de controles e mostradores ("displays") **	2 a 10
Uso de procedimentos escritos bem elaborados, de fácil compreensão, e de listas de verificações substituindo procedimentos tipicamente narrativos ***	3 a 10
Substituição de controles e mostradores que violam os estereótipos marcantes da população	> 10
Substituição de etiquetas de válvulas, de forma a indicar sua função - incluindo uma clara indicação do sistema com o qual a válvula está associada e também para mostrar claramente sua situação em operação normal	~ 5
Prática freqüente de respostas adequadas a situações potenciais de acidente ou outras situações anormais (essa prática deve incluir a requalificação periódica em simuladores dinâmicos e vistorias/inspeções, realizadas pelo menos uma vez por mês, para os principais problemas potenciais)	2 a 10

* Estes fatores, estimados, não são aditivos.

** Nenhuma avaliação é feita para novas tecnologias de mostradores usando CRT's ("Cathode Ray Tube") e "software" de computadores, como por exemplo o apresentado na Figura 2.8-1.

*** Nenhuma avaliação é feita para procedimentos orientados para o sintoma ("Symptom-Oriented Procedure" - "Emergency Operational Procedure"- EOP)

6.5.5 Exemplo de aplicação para modelo nominal

Em seguida, é apresentado um exemplo para ilustração do uso da Tabela 6.5-3. No caso, considera-se que o analista determinou T_M de 25 minutos, para o diagnóstico e a execução das ações. O analista de HRA determinou, por avaliações (vistorias, inspeções, etc), que o tempo de desempenho das várias ações críticas leva 5 minutos (T_A). Subtraindo, tem-se $T_M - T_A = 20$ minutos $= T_D$, que é o tempo para diagnóstico usado no primeiro ramo de falha da Figura 6.5-5.

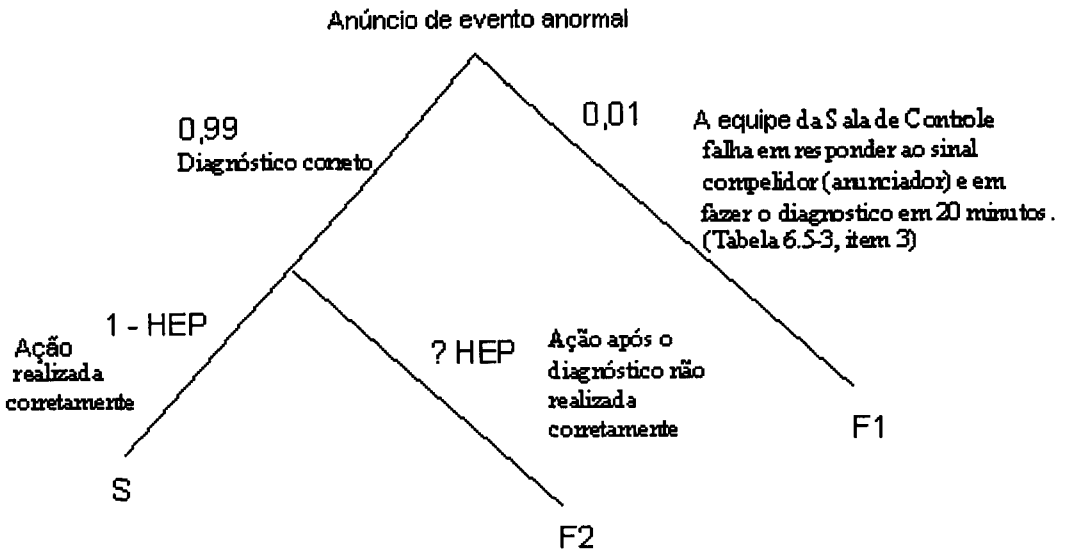


Figura 6.5-5 - Árvore THERP para diagnóstico

A Figura 6.5-5 apresenta a situação para HEP nominal, o ramo ["?HEP"] na árvore THERP representa outra árvore, ou árvores, as quais, no total, representam a soma de todos os caminhos de falha para erros de ação e omissão no desempenho de ações após o diagnóstico. As HEP's condicionais são estimadas a partir de critérios utilizados por especialistas [1]

Um aspecto importante, ainda não coberto pelo modelo, é o *falso diagnóstico*, que pode ocorrer quando os sintomas são em quase tudo parecidos aos do diagnóstico correto, exigindo uma maior experiência dos operadores de reator. É o caso, por exemplo, quando se considera que a equipe de operadores em uma usina do tipo PWR faz o diagnóstico de um LOCA, ao invés de uma ruptura de um tubo do gerador de vapor. Por causa disto o analista deve identificar os modos mais prováveis de falso diagnóstico para os eventos iniciadores de interesse numa avaliação probabilística de segurança. Dessa forma, êle poderá prever algumas ações e uma série de verificações para descubrir rapidamente o erro e se recuperem as ações realizadas, corrigindo qualquer problema ocasionado pela interpretação incorreta. É um campo a ser estudado mais detalhadamente, e já existe alguma bibliografia a respeito, citada na referência [1].

No atual modelo apresentado em [1], a equipe da sala de controle faz o diagnóstico errado ou não consegue fazê-lo, portanto evita incluir ações após o diagnóstico, por simplificação.

Note-se que os modelos de triagem e o nominal foram desenvolvidos em decorrência da importância dos erros em diagnósticos, os quais muitas vezes resultam em HEP's altas. O diagnóstico é reconhecidamente uma tarefa difícil e complexa, por exigir conhecimento e raciocínio e por estar associado a níveis de estresse mais elevados, quando relacionados com a pressão do fator tempo.

Na referência [62] é feita uma comparação entre diferentes gráficos baseados em modelos para estimativas de HEP's para diagnóstico. A Figura 6.5.6, adaptada desta referência, permite que uma comparação seja feita entre três gráficos, referentes a três modelos, sendo um aplicável a métodos desenvolvidos para APS para

reatores do tipo CANDU (reator canadense que utiliza água pesada como moderador e refrigerante).

No gráfico, elaborado a partir de algumas considerações referentes à expectativa de alarme durante eventos de uma usina do tipo CANDU, e pela estimativa do tempo disponível para a resposta dos operadores para a falha em diagnosticar um evento corretamente, foram estabelecidos os valores de 1, 0,01 e 0,001 para diferentes tempos (0,001 para 30 minutos).

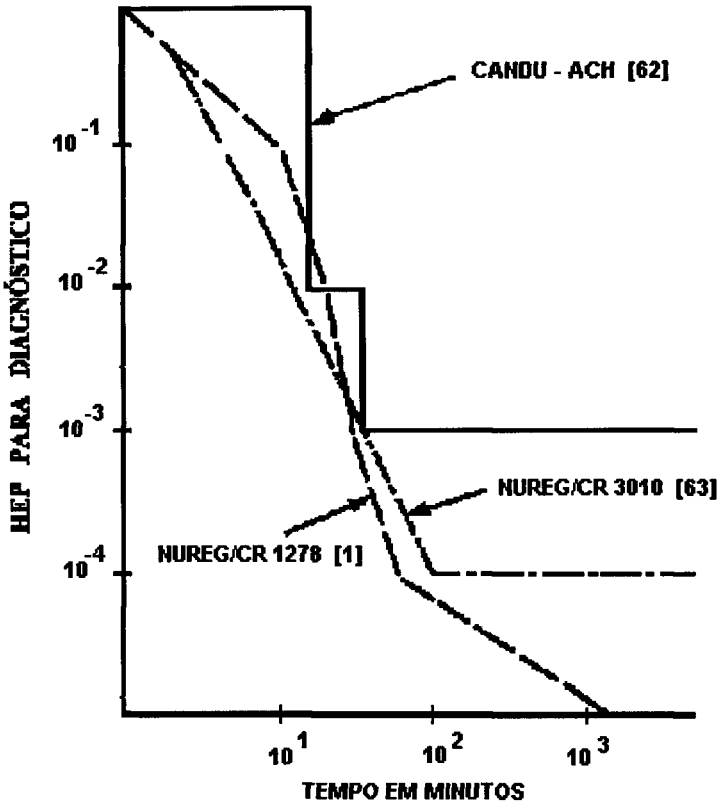


Figura 6.5-6 Comparação entre três gráficos de estimativas de HEP's para diagnóstico em salas de controle de usinas nucleares, baseados em modelos das referências [1], [[62] e [63]

As HEP's referentes à figura acima podem ser aumentadas ou diminuidas conforme alguns fatores dependendo da situação. No sistema CANDU, as probabilidades de erros são aumentadas por um fator de 10 quando a situação não resulta de alarmes diretamente ligados a algum evento relacionado a situação de emergência ou à possibilidade de acidente, ou quando a analise postula um erro anterior cometido pelo operador na mesma seqüencia de acidente.

7. EXEMPLOS DE APLICAÇÕES PRÁTICAS DA THERP

7.1 Aplicação de Injeção a Alta Pressão para Resfriamento do Núcleo de um Reator

O exemplo apresentado neste item foi baseado em um estudo [1] realizado em 1982, sendo bastante simplificado, com a finalidade de ilustrar a utilização da técnica THERP. Neste exemplo, o efeito do estresse não foi considerado, assim como também não foram utilizadas as margens de incerteza para as HEP's, considerando-se apenas valores nominais. Foram omitidos alguns fatores de recuperação (por exemplo, a utilização de "checklist" pelos operadores) que, se devidamente considerados, fariam com que alguns caminhos de falha se tornassem insignificantes, no mundo real. Para maior simplificação, também não foram considerados os efeitos de dependências entre indivíduos do pessoal de operação na sala de controle da usina nuclear.

O exemplo refere-se à perda de alimentação de água no gerador de vapor, tanto a normal quanto a alimentação de emergência, acarretando a não refrigeração adequada do núcleo do reator, o que pode ocasionar um acidente com fusão do núcleo, se não for restabelecida a função " feed and bleed " (*"alimentar e sangrar"*). Esta operação pode ser feita pelos operadores do reator, na sala de controle, com o uso do sistema de Injeção a Alta Pressão, propiciando a refrigeração necessária ao núcleo e evitando sua fusão. A figura 7.1-1 é apresentada para facilitar a compreensão do problema.

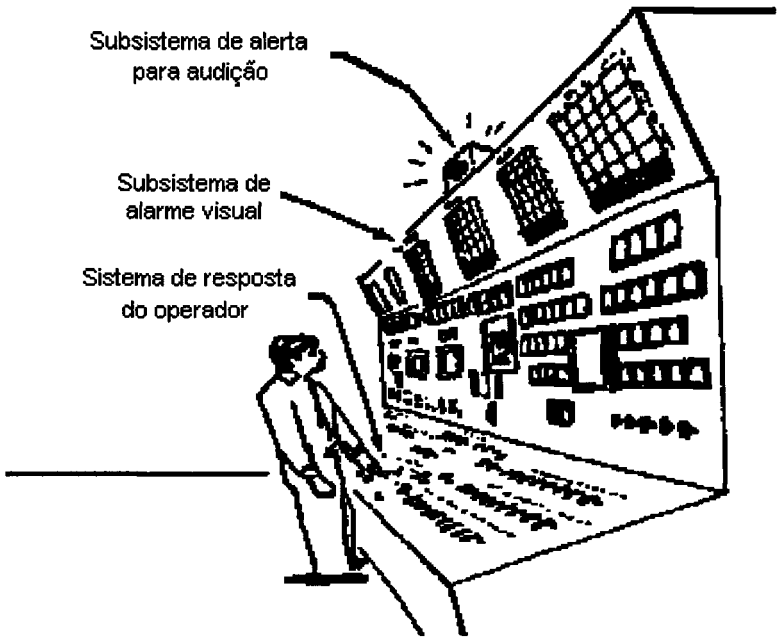


Figura 7.1-1 Painel apresentando sistema de sinais anunciadores [13]

O painel é composto de sub-painéis de anunciadores, os quais indicam funções específicas que fornecem indicações com luz intermitente, em alguns casos associados a sons, e a mostradores, instrumentos e alarmes. O alarme principal se situa na parte superior. Os controles principais ficam no nível das mãos, permitindo acionamento manual com facilidade, como se pode observar.

Nas figuras apresentadas no capítulo 2 podem ser verificados com mais detalhe alguns aspectos particulares como, por exemplo, a forma dos controles de acionamento manual e a disposição de painéis auxiliares.

Na análise da situação, foram identificadas as principais atividades humanas e os erros nos procedimentos para "alimentar e sangrar" vapor, após a perda simultânea da alimentação normal e da emergência dos geradores de vapor. Os eventos considerados são apresentados na Tabela 7.1-1, que fornece também os valores das estimativas de probabilidades de erros humanos para o grupo de três operadores. Nota-se que são probabilidades de erros humanos conjuntos (HEPC).

Tabela 7.1-1 HEPC considerando três operadores na sala de controle

	Eventos - Considerando 3 Operadores	HEPC
A	Omissão por não iniciar ações após o alarme (disparo sonoro do anunciador principal, associado a anunciadores indicativos de parâmetros fora de especificação)	0,00008
B	Diagnóstico errado relacionado com o padrão dos anunciadores associados ao alarme principal (parâmetros fora da especificação, decorrente de funções em situação diferente da condição normal)	0,01
C	Omissão por não responder adequadamente ao disparo do anunciador especial, indicativo de ação para correção de parâmetros fora das especificações	0,00015
D	Omissão por não acionar bombas de alimentação elétricas	0,0016
E	Omissão por não atuar no controle de válvulas	0,0016
G	Omissão por não iniciar ações em resposta ao anunciador referente a perda de alimentação	0,00001
H	Omissão por não atuar para restabelecer a vazão da água de alimentação	0,0016
K	Omissão por não iniciar o procedimento de "alimentar e sangrar"	0,0001

Na Figura 7.1-2 é apresentada a árvore THERP correspondente, representando atividades de um grupo de três operadores de reator licenciados, um dos quais é o supervisor de turno.

Na árvore simplificada, a linha tracejada a partir de um nó de um acerto, como em c e g , liga dois pontos a partir dos quais ocorre uma repetição do trecho da

árvore. Estes trechos são equivalente em termos de sucesso, não em termos de probabilidade. A árvore ilustra o mecanismo da lógica e de cálculo aplicáveis à probabilidade de falha do sistema em geral.

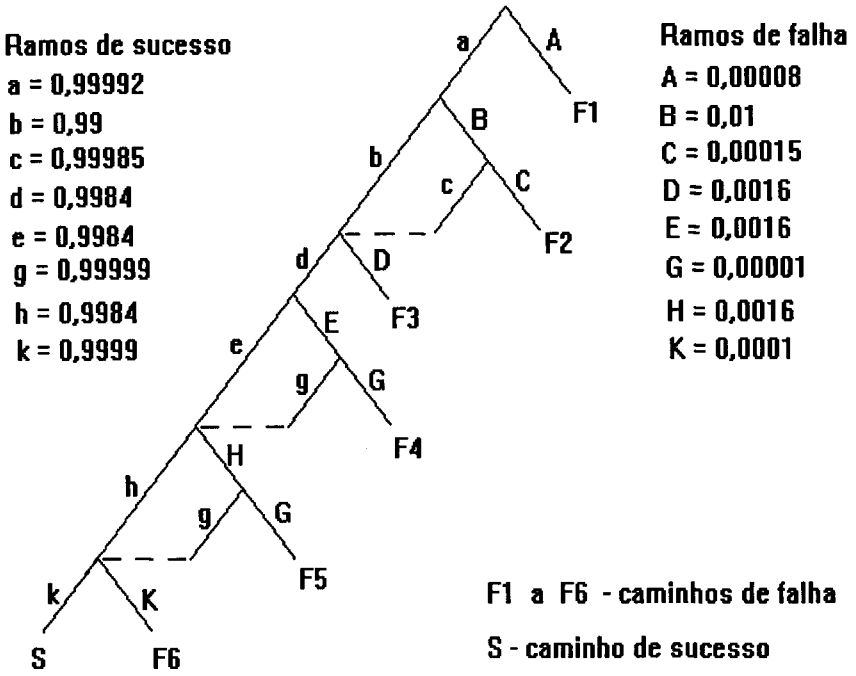


Figura 7.1-2 Árvore simplificada de eventos HRA para perda de alimentação de água no gerador de vapor

7.1.1 Itemização da seqüência

Neste problema simplificado, considerou-se que os operadores estão bem familiarizados com o procedimento de "alimentar e sangrar", de forma que erros de ação foram desconsiderados, levando-se em conta apenas erros de omissão.

Abaixo é apresentada a seqüência dos eventos por item, representadas as falhas por letras maiúsculas, e sucessos por minúsculas. As tarefas ou ações são representadas por letras maiúsculas entre aspas, conforme visto em 5.3.2.

Evento A - Omissão em agir após alarme.

Falha por omissão dos três operadores conjuntamente, por não executarem as ações esperadas após o desligamento do sinal de alarme sonoro principal e os sinais intermitentes de alguns anunciadores. Para o evento A foi designado o valor de 0,00008 para a HEPC, portanto, para o evento a, correspondente ao acerto, tem se 0,99992.

Pode parecer que o número 0,00008, adotado para a probabilidade de ocorrência do evento A, seja muito pequeno, contrariando as recomendações da bibliografia especializada, que recomenda cautela quendo se trata de probabilidades de erros humanos. No entanto, este número foi adotado, em lugar de 10^{-4} , em função de fatores considerados positivos na análise da tarefa. Mesmo assim, não se considera que reflete a realidade, dada a subjetividade da avaliação, e pode ser arredondado para 10^{-4},

sendo que a prática recomendada pela referência [1] é que se faça o arredondamento apenas na finalização do problema.

Evento B - Falha no diagnóstico

É atribuido a B - falha no diagnóstico por parte dos três operadores, o valor de 0,01, para a HEPC de B. Neste caso, há um fator de recuperação, representado pela tarefa "C ", conforme descrito adiante.Note-se que neste problema não será utilizado o modelo para diagnóstico, conforme visto no item 6.5.

Evento C - Omissão por não execução de ação corretiva da margem de saturação de vapor no pressurizador

Para C foi atribuido o valor de 0,00015, correspondente à falha em responder adequadamente ao disparo do anunciador especial, que indica que a margem de saturação do vapor no pressurizador excedeu limites toleráveis. Para c, tem-se 0,99985, que é um fator de recuperação, porque se espera que , ao ouvir o anunciador especial (indicativo de ação para correção de parâmetros fora de especificações), um dos operadores deve acionar um controle de ajuste para restabelecer condições favoráveis ao retorno à operação normal. Se B e C ocorrem, o sistema falha. Se c ocorre, ou seja, os operadores se orientam corretamente a partir da indicação do anunciador, uma nova seqüência de atividades tem início.

Evento D - Omissão dos operadores por não atuarem na ativação de bombas

No caso da ocorrência de c (ação corretiva após indicação do anunciador especial), o grupo de operadores será adequadamente alertado pelo anunciador, dando prosseguimento à seqüência de atividades. Note-se que, na árvore, o fim do caminho representado por aBc leva de volta ao caminho principal de sucesso. Assim, a seqüência aBc é equivalente à seqüência ab (em termos de acerto, não de probabilidade). Em lugar de repetir a árvore em seguida a c, coloca-se uma linha tracejada ligando os dois pontos, entendendo-se que uma só seqüência represente duas, conforme explicado anteriormente acima.

A tarefa omitida, explicitada em um item de procedimento escrito, é a atuação no funcionamento de bombas de alimentação elétricas, para restaurar a vazão de refrigerante. Se ocorrer D, o sistema falha, não sendo possível a recuperação, por isto, tal falha é designada como *falha humana de primeira ordem*, como A. Para D foi atribuido o valor de 0,0016 para a HEPC.

Evento E - Omissão por não atuar no controle de válvulas

Similarmente a D, o evento E representa a falha por ter sido omitido atender um item previsto em procedimento escrito, o de atuar no controle de válvulas relacionadas às bombas de acionamento elétrico. Mas, neste caso, existe um fator de recuperação (representado pela tarefa "G") que consiste em atuar após a indicação, por um anunciador, da ocorrência de perda de água de alimentação. De maneira análoga ao descrito anteriormente, se g ocorre, ou seja, não há erro, a linha tracejada mostra que o ramo Eg é equivalente, em termos de sucesso, ao ramo e, portanto, pode ser feita a mesma simplificação, isto é, a representação por uma linha pontilhada de retorno ao caminho de sucesso. Foi atribuido a E o valor 0,0016, e a e 0,9984.

Evento G - Omissão por não agir em resposta ao anunciador referente à perda de água de alimentação

Para G foi atribuido o valor 0,00001, correspondente à falha em se iniciar ações em resposta ao anunciador referente à perda de água de alimentação, indicado pela medida de vazão. Ocorrendo G o sistema falha. Caso g ocorra, ou seja, o desempenho dos operadores é o acertado, se um deles atua adequadamente após indicação do anunciador de perda de alimentação, tem-se então a recuperação, e a volta ao caminho de sucesso. Para g foi atribuido o valor de 0,99999

Evento H - Omissão pelo não restabelecimento da vazão de refrigerante

A tarefa "H" , restabelecer a vazão de refrigerante, é um item crítico especificado em procedimento escrito e, caso ocorra a omissão do operador, tem-se um erro similar ao erro da tarefa "E". Nos dois casos, "E" e "H", o fator de recuperação é o mesmo, representado pela tarefa "G". Para H, foi atribuído o valor para a HEPC de 0,0016.

Evento K - Omissão ao não iniciar a injeção a alta pressão

Para K, falha em iniciar a injeção a alta pressão, pelo uso adequado do método de alimentar e sangrar, foi atribuido o valor para a HEPC de 0,0001. Para k, o valor é de 0,9999.

7.1.2 Probabilidade Total de Falha

Para chegar à probabilidade total de falha, a equação exata de falha envolve a soma das probabilidades de todos os 18 caminhos de falha da árvore, listados abaixo. Deve ser notado que foi feita uma aproximação para os valores abaixo de 10^{-6}, depois das seqüências iniciais. O arredondamento foi feito considerando algarismos significativos, conforme a referência [64].

1) A	0,00008
2) aBC	0,0000015
3) aBcD	0,000016
4) abD	0,0015839
5) abdEG	$\sim 10^{-8}$ ($1,6x10^{-8}$)
6) abdEgHG	$\sim 10^{-11}$ ($2,6x10^{-11}$)
7) abdEghK	$\sim 10^{-7}$ ($1,6x10^{-7}$)
8) abdEgHgK	$\sim 10^{-10}$ ($2,6x10^{-10}$) P = 1, para g/g
9) abdeHG	$\sim 10^{-8}$
10) abdeHgK	$\sim 10^{-7}$
11) abdehK	0,0001
12) aBcdEG	$\sim 10^{-10}$
13) aBcdEgHG	$\sim 10^{-13}$
14) aBcdEgHgK	$\sim 10^{-12}$ P = 1, para g/g
15) aBcdeHG	$\sim 10^{-10}$
16) aBcdeHgK	$\sim 10^{-9}$
17) aBcdehK	$\sim 10^{-6}$
18) aBcdEghK	$\sim \underline{10^{-8}}$
	$\sim 0,00178 \sim 0,002$ (arredondado)

Na Figura 7.1-3 é apresentada a árvore expandida, com os detalhes de todos os caminhos de falha e sucesso. Nota-se que, para os caminhos 8 e 14, o segundo valor de g é 1, e não 0,99999, pois a probabilidade de g ocorrido g é igual a 1, ou seja, P(g/g) = 1.

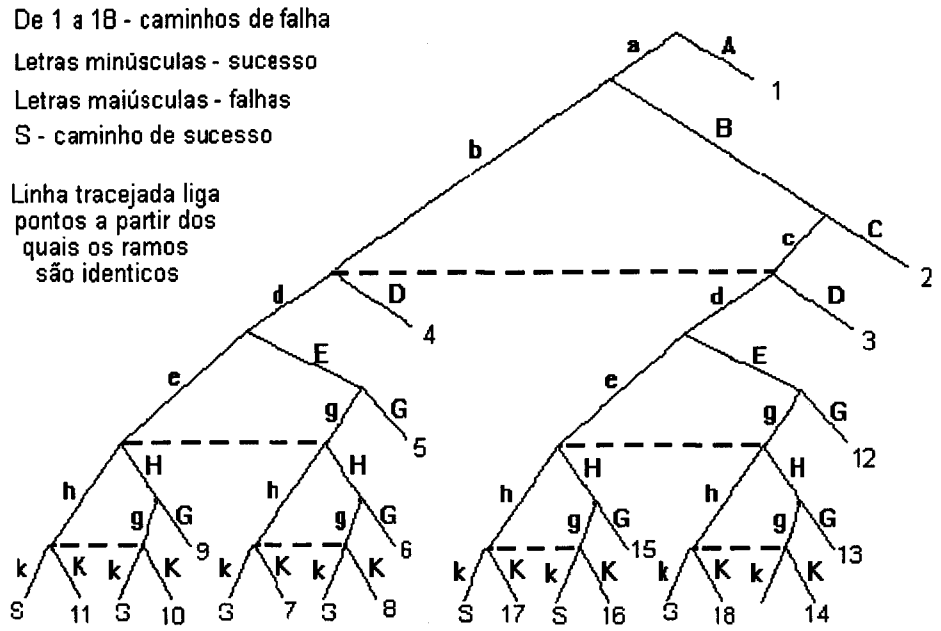


Figura 7.1.3 Árvore de falha expandida para o exemplo

Quando todos os HEP's são iguais a 0,01 ou menores, a equação exata de falha pode ser aproximada apenas pela soma dos caminhos primários de falha, ignorando todos os ramos de sucesso. Há seis caminhos de falha primários, ou seja, se ocorrerem, não há recuperação. Assim, uma aproximação para o termo de falha total, F, dado cada HEP < 0,01, é:

$$F\ (\text{HEP's} < 0{,}01) \approx A + BC + D + EG + HG + K$$

$$= 0{,}00008 + (0{,}01 \times 0{,}00015) + 0{,}0016 + (0{,}0016 \times 0{,}00001) + (0{,}0016 \times 0{,}00001) + 0{,}0001$$

$$= 0{,}0018 \sim 0{,}002$$

Os valores arredondados da aproximação e da equação exata são os mesmos. A precisão da aproximação decresce com o aumento dos termos ou o aumento dos valores.

Um outro meio de trabalhar o problema é usar a equação exata de sucesso, ou seja, calcular a probabilidade usando o caminho do sucesso, que é complementar ao caminho de falha:

$$S = a(b + Bc)\ d\ (e + Eg)\ (h + Hg)k$$

$$= 0{,}99992 \times [0{,}99 + (0{,}01 \times 0{,}99985)] \times 0{,}9984\ [0{,}9984 + (0{,}0016 \times 0{,}99999)] \times$$

$$[0{,}9984 + (0{,}0016 \times 0{,}99999)] \times 0{,}9999$$

$$= 0{,}9982188 \sim 0{,}998$$

As duas probabilidades somadas, de falhas e de sucessos, devem ser iguais a 1 (S + F = 1).

A árvore THERP apresentada e os cálculos efetuados são típicos do uso desta abordagem para estimativas simples. Porém, para a maioria dos trabalhos em APS, cada atividade humana em uma árvore de falhas é caracterizada por uma distribuição de HEP's. Com a árvore de eventos THERP acontece o mesmo, mas o termo de falha total é expresso como uma distribuição de HEP's, como descrito no item 6.3.

7.2 Mudança no Modo de Injeção para Recirculação

O exemplo apresentado a seguir foi baseado em um estudo realizado em [1], a partir de um problema considerado em [58]. A análise é realizada considerando a confiabilidade humana na mudança do modo de injeção para o modo de recirculação da refrigeração de emergência, num período de aproximadamente 30 minutos, após a ocorrência de um grande LOCA em uma central com dois reatores do tipo PWR ("Pressurized Water Reactor"). O núcleo do reator não pode ficar exposto, ou seja, sem um mínimo de água para mantê-lo coberto, pois pode fundir e causar as piores consequências possíveis para um reator nuclear. No caso do PWR, a água é o refrigerante, além de servir também como moderador e blindagem.

A troca de modos deve ser feita manualmente. Se não for feita corretamente, ou fora do período de tempo especificado, as conseqüências poderão ser muito sérias, pois as bombas necessárias para à refrigeração a longo prazo podem ser danificadas na tentativa de serem acionadas com o reservatório de água de reabastecimento (" Refueling Water Storage Tank " - RWST) vazio.

O refrigerante armazenado no RWST é usado no modo de injeção inicial para manter o reator com o nível de água suficiente. Antes que o refrigerante seja completamente esgotado, é necessário desempenhar as ações abaixo especificadas para bombear água de outro reservatório (reserva para drenagem em emergência) e recircular a mesma através do vaso do reator.

7.2.1 Análise inicial para a mudança para o modo de recirculação

A análise é baseada em dois parágrafos de procedimentos escritos entitulados "perda de refrigerante do reator ", que fazem parte dos procedimentos de emergência de uma central nuclear. Deve ser notado que foram mantidos os números e as siglas originais, pois estes caracteres também podem ser considerados como fazendo parte da dificuldade encontrada pelo operador quando deve trabalhar com procedimentos escritos. Também foi preservada, para este exemplo, a designação dos comutadores, até mesmo como fator ilustrativo da dificuldade de se trabalhar com grande quantidade de controles. Por exemplo, muitos números ou letras semelhantes podem confundir o operador e, neste caso, onde o procedimento deve servir para duas usinas na central citada, a numeração existente nos procedimentos não coincide com a numeração existente no painel de uma delas.

Numa situação real, são fatos como este que se apresentam ao operador, o que contribui para o aumento da probabilidade de falha, quando do acionamento de controles. Também ocorre que, como no Brasil, em países que importam equipamentos estrangeiros, seja mantida a linguagem original em mostradores, instrumentos, e outros dispositivos de controle. Isto, em alguns casos, também pode ser considerado como fatores contribuintes para o aumento da probabilidade de erros humanos, devido à uma necessidade de tradução, o que envolve sempre pelo menos um mínimo de interpretação.

Abaixo são explicitados os parágrafos do procedimento utilizado para as ações exigidas, adaptados de [1], sendo que *nível baixo* se refere ao original "low level", e *nível mais baixo* se refere ao "low low level", notações estas existentes na central utilizada como exemplo. "Sump" se refere ao reservatório de drenagem de água que se acumula no prédio da contenção, alimentado por eventuais vazamentos. As válvulas operadas por motor são identificadas por MOV ("Motor Operated Valves).

Item 4.8 - Quando a água chegar à indicação de nível baixo no RWST, correspondente a 14,5 % , e o Sistema de Limitação de Conseqüência for ativado na sua contagem inicial ("RESET PERMISSIVE" < 0,5 psig), completar as seguintes ações:

4.8.1 Abrir MOV-860A e B, para sucção de água do poço de coleta do edifício do reator ("sump") pelas bombas de baixa pressão do Sistema de Injeção de Segurança;

4.8.2 Parar os motores da bomba do "spray" da contenção e fechar as válvulas MS-103A, B, C, e D de suprimento de vapor da bomba de "spray" da turbina;

4.8.3 Fechar a bomba de sucção de "spray" e também as válvulas de descarga MOV-CS-100-A, 100B, 101A, B, C, e D.

Item 4.9 - quando a água chegar à marca do nível mais baixo no RWST, correspondente à 7%, completar as seguintes ações:

4.9.1 Fechar MOV-862, de sucção de água do RWST pelas bombas de injeção de baixa pressão;

4.9.2 Abrir o carregamento das bombas de sucção a partir da descarga das bombas da ponta baixa, abrindo MOV-863A e B.

A presente análise se limita aos passos 4.8.1, 4.9.1, e 4.9.2. Os comutadores envolvidos são os das válvulas MOV-1860A e B, MOV-1862 e os MOV-1863A e B, conforme apresentado parcialmente no esquema da Figura 7.2-1.

A figura representa esquematicamente parte de um painel. As duas linhas de comutadores apresentadas são as duas localizadas mais abaixo de um grupo de sete, na parte esquerda do painel composto de quatro segmentos, pertencentes à um conjunto maior.

Os procedimentos, originalmente escritos em inglês, não especificavam os dígitos iniciais correspondentes a todos os comutadores de uma série, referindo-se de forma completa apenas ao primeiro deles. Eram utilizados A ou B para identificar a qual das duas usinas se referia, omitindo, portanto, o dígito inicial, correspondente aos números, e às vezes nem a letra era usada. Isto foi considerado em [1] como uma falha do procedimento, considerando que se referiam a dois reatores, com diferentes designações para os comutadores das duas usinas da central considerada.

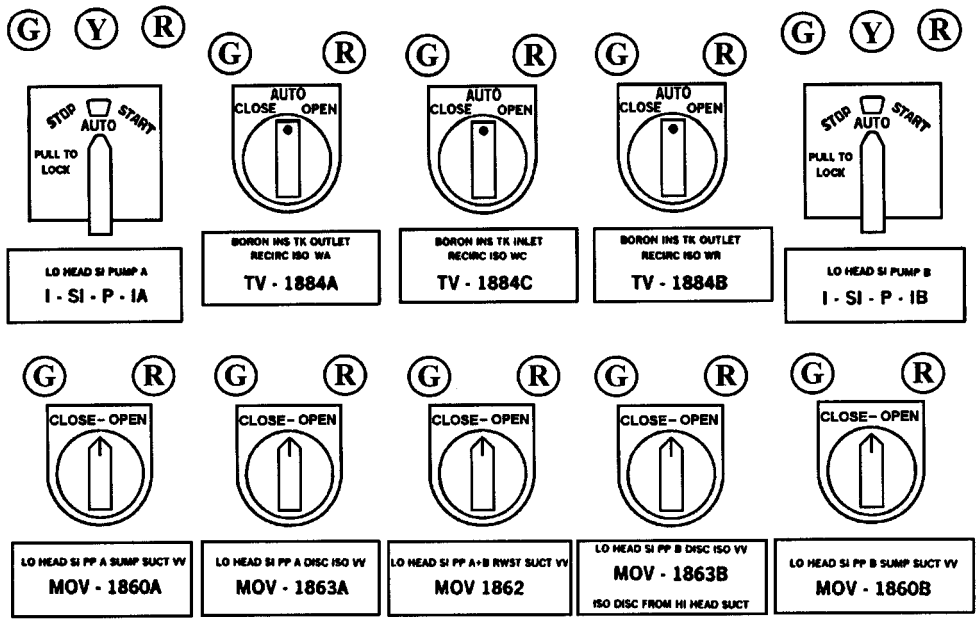


Figura 7.2-1 Comutadores MOV de um conjunto maior, que devem ser acionados pelo operador

No reator da unidade 1, a especificação era MOV-2860; no reator da unidade 2, era MOV-2860A. Devido a isto foi considerado, em [1] que deviam ser preparados procedimentos de emergência separados para cada usina, em lugar de serem aplicados conjuntamente para toda a central.

Na ilustração em preto e branco, as letras G, Y e R representam lâmpadas anunciadoras com filtros de cor verde, vermelho e amarelo que, juntamente com os comutadores relacionados, compõem o painel na sala de controle.

Existem duas ou três lâmpadas indicadoras acima de cada comutador: verde, representada por G, correspondendo à condição MOV fechada ou bomba parada; vermelha, representada por R, correspondendo à condição de MOV aberta ou bomba funcionando, e amarela, representada por Y, como uma condição intermediária. Antes que a marca de nível baixo seja alcançada, o MOV-1862 deve ser aberto (lâmpada vermelha) e as outras quatro são fechadas (lâmpadas verdes).

A terceira linha (a contar de baixo) de comutadores de válvulas MOV, não representada na Figura 7.2-1, consiste de cinco comutadores identicos em forma, tamanho e arranjo (disposição no painel). Os cinco comutadores da referida terceira linha, relevantes para a análise, são identificados como se segue, da esquerda para a direita:

LO HEAD SI PP A DISC ISO VV
MOV - 1864-A
ISO DISC FROM COLD LEGS

LO HEAD SI PP A RECIRC ISO VV
MOV - 1885-A

LO HEAD SI PP A&B RECIRC ISO VV
MOV - 1885-C

LO HEAD SI PP B RECIRC ISO VV
MOV - 1885-B

LO HEAD SI PP B DISC ISO VV
MOV - 1864-B
ISO DISC FROM COLD LEGS

Nesta linha, as lâmpadas vermelhas indicam a normalidade da condição aberta para as válvulas. As abreviações, no procedimento, correspondem a: LO - baixo; SI - injeção de segurança; PP - bomba; A - canal A; DISC - descarga; ISO - isolamento; VV - válvula; RECIRC - recirculação; B - canal B.

A indicação de nível baixo (14,5 %) será atingida em mais ou menos 20 a 30 minutos depois de um grande acidente de perda de refrigerante (LOCA - "Loss of Coolant Accident"). Quando a indicação de nível baixo for atingida, dá-se início às ações de uma sequência posterior, conforme o item 4.8, que devem ser desempenhadas dentro de dois minutos, (tempo disponível até que o nível mais baixo, 7 %, seja alcançado), devendo o operador estar pronto para tomar as ações seguintes, correspondentes às do item 4.9 do procedimento. A indicação do nível é fornecida por medidores que mostram o nível da água no RWST. Assim que as as marcas são alcançadas, anunciadores sonoros são ativados.

Duas questões são colocadas nesta análise:

1) Qual é a probabilidade de que nenhuma ação seja tomada quando a marca de nível baixo é alcançada ? Isto corresponde a um erro de omissão.

2) Qual é a probabilidade de que algum par de comutadores, outros que os das válvulas MOV-1860A e B, sejam manipulados ? Isto corresponde a um erro de ação.

Para responder à primeira questão, usa-se a HEP de 0,1, conforme informações complementares da Tabela 4.3-2 deste trabalho, que é uma compilação parcial da tabela de taxas de erros humanos da referência [58], apêndice G. Para a maioria das ações desempenhadas por operadores depois de 30 minutos da ocorrência de um grande LOCA, a recomendação é utilizar uma HEP básica de 10^{-1}. A hipótese do problema apresentado considera a presença de pelo menos três pessoas na sala de controle, aproximadamente 30 minutos após o início do acidente e que a ação será prontamente desempenhada, a menos que todas as três pessoas falhem em antecipar ou prever a marca de nível baixo. Em outras palavras, o operador deve estar alerta, de prontidão para desempenhar a atividade requerida. Julgou-se que o medidor indicativo de queda do nível de água do RWST faça com que os indivíduos presentes na sala de controle fiquem alertas para desempenhar a ação correspondente ao item 4.8.1 do procedimento, assim que necessária. Se nenhuma preparação for feita antes que o anunciador dispare na marca do nível baixo, as chances de completar o procedimento corretamente nos dois minutos requeridos seria grandemente reduzida.

Estima-se que cada uma das três pessoas tem uma probabilidade de 0,5 de falhar em perceber a indicação do medidor. O raciocínio adotado foi que, embora os operadores tenham conhecimento do procedimento de usar o refrigerante do RWST quando da ocorrência de um grande LOCA, sob a influência estressante de uma associação de vários alarmes tocando, e a condição de perigo para a instalação e de dano potencial ao meio ambiente, o melhor que se pode esperar é admitir uma probabilidade de aproximadamente 50 % por pessoa [1] de que ele irá verificar o medidor do nível do RWST antes que o anunciador dispare.

O medidor, neste caso, encontra-se num painel vertical localizado a alguns metros atrás do painel em que se encontram os comutadores a serem acionados. Esta não é a localização ideal de uma indicação que fizesse alguém lembrar-se de consultar o painel (um fator de recuperação), para alertar alguém que alguma ação deva ser desempenhada. A

HEP de 0,5 [1] representa o julgamento para a situação. Além disto, nenhum outro dado referente à tarefa (verificar o medidor do nível do RWST) se encontra disponível.

Em [1], foi avaliado que a probabilidade conjunta de que os três operadores falhem em perceber a possibilidade do uso do medidor de nível seria de 0,5 elevado a três, ou 0,125, arredondado para 0,1. Julga-se também que haveria uma probabilidade de que o pessoal da sala de controle antecipe o alarme associado ao nível baixo, mesmo que não monitorem o nível do RWST. Foi adotada a HEPB de 0,1, elevada ao cubo, para a probabilidade conjunta de que as três pessoas falhem em se preparar para os procedimentos a serem desempenhados após o indicador chegar à marca de nível baixo. Ou seja, 0,1 ao cubo, equivalente a três pessoas, igual a 0,001. Desta forma, a probabilidade conjunta de falha em antecipar a marca de nível baixo, associada com a falha em perceber e usar a leitura do medidor foi adotada como sendo de:

$$0{,}1 \times 0{,}001 = 0{,}0001.$$

Esta probabilidade é atribuída ao primeiro ramo de falha na árvore de eventos apresentada na Figura 7.2-2.

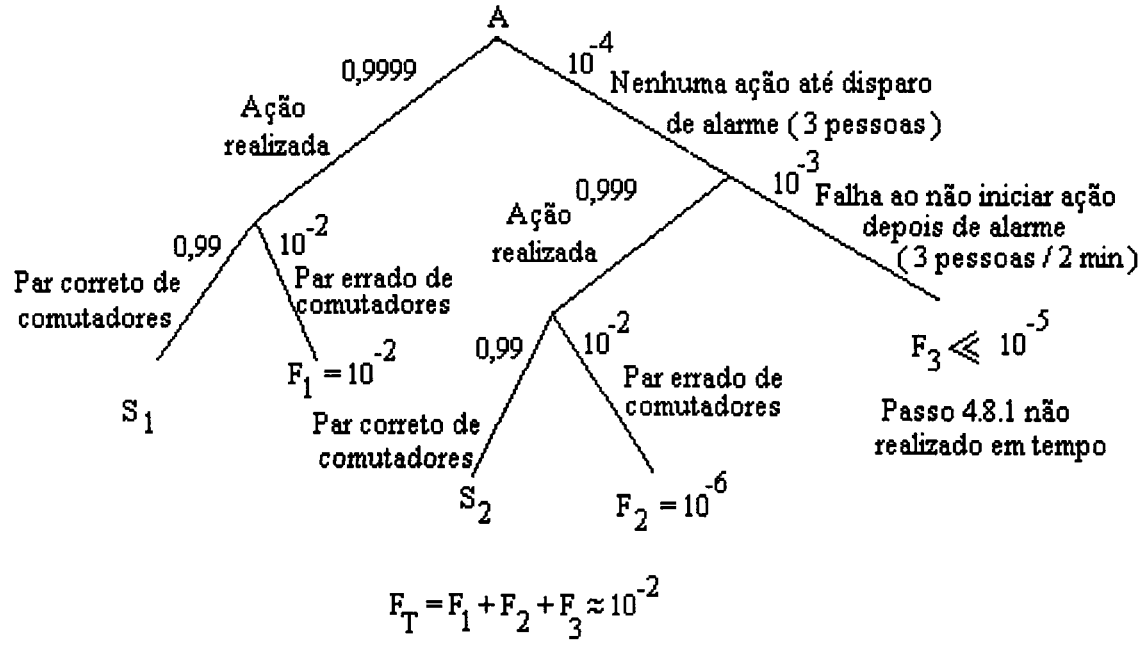


Figura 7.2-2 Árvore de eventos THERP para ações indicadas por procedimento após ocorrência de um LOCA

Quando o anunciador associado ao nível baixo dispara, a disponibilidade de tempo para os operadores em desempenhar os passos do item 4.8 do procedimento é de somente dois minutos. Considera-se que, se nenhuma ação tenha sido planejada até o momento em que o alarme dispara, algum grau de desorganização estava ocorrendo, atribuindo-se uma HEPB de 0,1 para cada um dos operadores. Uma probabilidade conjunta de 0,001 (0,1 ao cubo) foi estimada [1] para a falha de todos os três operadores realizarem as ações dentro do tempo previsto de dois minutos após o disparo do alarme. Esta probabilidade é mostrada no segundo ramo de falha da Figura 7.2-2 , levando à falha do evento F_3 , ou seja, passo 4.8.1 não desempenhado no tempo esperado.

O próximo passo da análise original foi assumir que pelo menos um dos três operadores consegue se preparar para o acionamento dos comutadores MOV-1860A e B. Pode-se perceber que pelo menos um dos operadores se preparava para as ações, pelos dois ramos designados como "ação realizada".

Isto leva à segunda questão: qual é a probabilidade que algum par de comutadores que não os MOV-1860A e B sejam acionados ?

Na árvore THERP isto é representado em dois lugares: nos ramos finais que levam a F1 e F2. A HEP condicional para esta tarefa foi estimada em 0,01. O raciocínio foi de que seria altamente provável que a responsabilidade para operar as válvulas seja de um operador apenas, ou seja, nenhuma redundância humana estaria disponível para recuperar um erro de desempenho do responsável pela atividade. Este julgamento foi baseado na observação dos operadores ao desempenhar tarefas análogas. A seleção errada de comutadores é o tipo de erro que poucos operadores aceitam como um erro possível, ou seja, não acreditam neste tipo de erro. Entretanto, é improvável que alguma pessoa iria conferir o operador que efetivamente desempenha a tarefa, ou seja, aciona os comutadores. A probabilidade básica de 0,1 foi avaliada e considerada muito alta para esta ação; preferiu-se adotar 0,01, como estimativa mais próxima [1] da ordem de grandeza.

Em uma reanálise (ver item 7.2.2) acredita-se que a hipótese de completa confiança no operador do reator para um passo tão importante não mais é adequada e, ao se refazer os cálculos, deve ser incluída a verificação pelo Supervisor de Turno, para este passo crítico dos procedimentos operacionais de emergência.

É possível, então, adotar HEPs para todos os ramos, considerando que a soma das probabilidade dos ramos de cada nó necessariamente seja de 1. Há três caminhos de falha: A, que leva a F3, com um valor de 10^{-7}, o qual é pequeno o bastante para ser desconsiderado. Dois caminhos levam à seleção errada de comutadores: de A para F_1 e de A para F_2. A probabilidade é calculada como:

$$\text{Caminho } A.F_2 = 10^{-4} \times 0{,}999 \times 10^{-2} \sim 10^{-6}$$

Na referência [58], de onde se originou este exemplo, esta pequena probabilidade foi desprezada. A probabilidade do caminho A para F1 foi calculada como:

$$A.F_1 = 0{,}999 \times 10^{-2} \sim 10^{-2}$$

Dada a probabilidade de 10^{-2} de selecionar um par errado de comutadores para acionar na ocasião em que a água atinge a marca do nível baixo, a questão que surge se refere a qual dos pares de comutadores errados são selecionados. A análise seguinte foi feita para estimar a probabilidade de *erros estranhos* relevantes. Julgou-se que os candidatos mais prováveis seriam os comutadores MOV-1863A e B: estes dois estão no mesmo painel, próximo ao par de comutadores desejados, e os números que os identificam e suas etiquetas são similares. A probabilidade de um par de comutadores da segunda linha na parte inferior ser selecionada é pequena, porque sua forma é diferente, além de a nomenclatura dos comutadores ser diferente (têm uma posição AUTO). Os comutadores da terceira linha a partir de baixo têm etiquetas similares àquelas dos comutadores desejados, mas os comutadores da extremidade, que são os candidatos com mais chances de serem escolhidos numa seleção errada, estão normalmente na posição de válvula aberto. Dessa forma, as suas lâmpadas indicadoras vermelhas fornecem uma pista de que eles não

são os comutadores corretos. Além disso, essa terceira sequência de comutadores está localizada mais distante dos comutadores desejados, sendo esta distância também um fator importante, como indicação para a sua não utilização.

Dado o erro inicial de selecionar algum par de comutadores que não os MOV-1860A e B, estima-se [58] que existe a probabilidade 0,75 de que o operador selecione os comutadores MOV-1863A e B e uma probabilidade 0,25 de que algum outro par de comutadores seja selecionado. Os valores 0,75 e 0,25 foram avaliados com base no leioute dos comutadores e representam o tipo de julgamento que independe das HEPs utilizadas na referência [1].

O erro de seleção errada dos MOV 1863A e B tem o seguinte fator de recuperação, na indicação de nível mais baixo (7%): no passo 4.9.2 presume-se que o operador fechará os MOV-1863A e B. Se foi cometido o erro de seleção, o operador encontrará estes comutadores já fechados. Isto indicará que alguma coisa está errada. Uma HEP de 0,1 foi adotada para o operador que não percebe o erro, ou seja, para a falha de não perceber algo errado, ao verificar que os comutadores que ele deveria fechar ja se encontravam fechados.

A estimativa total da probabilidade de falha para o passo 4.8.1, incluindo a falha em não desempenhar corretamente a ação de recuperação, é:

0,01 x 0,75 x 0,25 x 0,1 = 0,00075, a qual é arredondada para 0,001.

Deve ser notado que a HEP de 0,1 é a adotada em [58] para a maioria das ações dos operadores depois de 30 minutos de um grande LOCA (ver item 4.3.1).

Uma análise similar foi realizada para os passos 4.9.1 e 4.9.2, entretanto não será incluida neste trabalho. A análise descrita acima envolveu certa subjetividade, relativamente aos valores adotados para as HEP's. Entretanto, esta subjetividade não foi particularmente crucial para o estudo, porque o fator realmente importante que afetou os resultados gerais foi a ordem de grandeza das HEP's associadas e não seu valor exato.

Para um estudo de incerteza, que não será desenvolvido neste exemplo, a adoção de margens de incerteza associadas ao valor da estimativa final permitem a consideração de incertezas e erros na análise.

A análise detalhada tem seu valor como exemplo pelas seguintes razões:

1) o exercício de se considerar todos os modos plausíveis de ações do operador diminui a probabilidade de não considerar algum caminho de falha importante;

2) devido a algumas falhas existentes em dados de probabilidades de erro para tarefas em instalações nucleares, é necessário quebrar ou desmembrar ao máximo possível as ações dos operadores, de modo a se poder utilizar dados disponíveis;

3) a abordagem detalhada torna mais fácil para o analista fazer estimativas independentes para verificar, na fonte, qualquer discordância e assim resolver o problema.

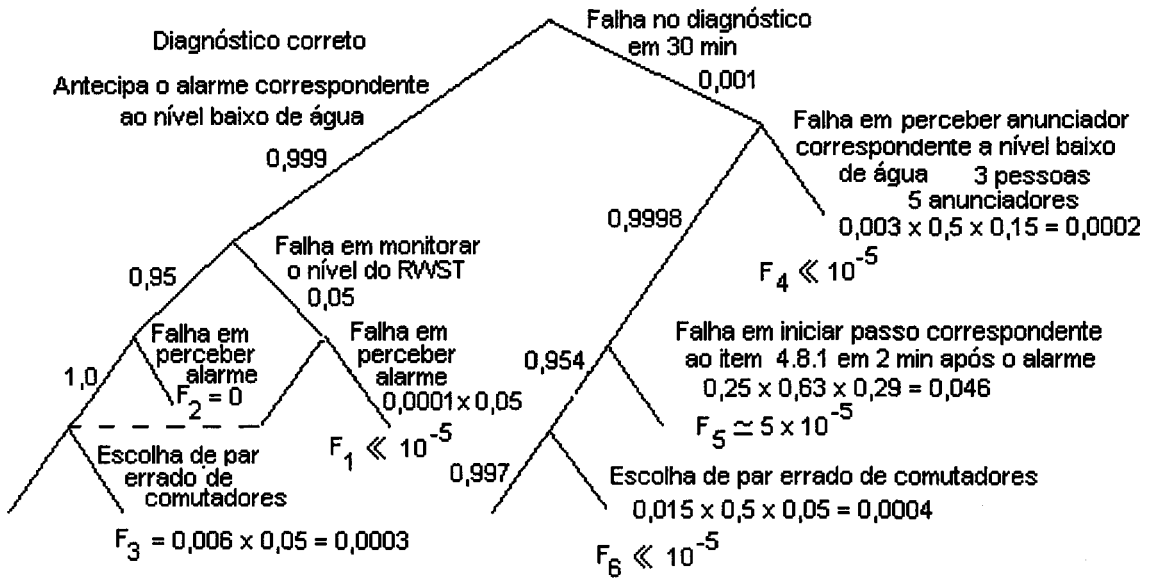
7.2.2 Reanálise para a mudança do modo de injeção para recirculação

No exercício seguinte verifica-se como o modelo de dependência, o modelo nominal de diagnóstico e o modelo aplicável ao conjunto de operadores modifica as estimativas encontradas originalmente. É feita uma reanálise do problema, ressalvando que o exercício é apenas ilustrativo, visto que, para ser mais realístico, teria de ser baseado em

uma análise detalhada de tarefas e em estudos realizados de acordo com a metodologia THERP.

Nessa nova análise, é usado o modelo nominal de diagnóstico, apresentado no item 6.5-4, para obtenção da estimativa de probabilidade de 0,001 (Tabela 6.5-3), relativa à hipótese de que o pessoal da sala de controle não faz o diagnóstico adequado aproximadamente 30 minutos depois de um grande LOCA. Esta falha na realização do diagnóstico significa que o pessoal da sala de controle não antecipou o disparo do alarme relativo ao nível baixo.

A Figura 7.2-3 é uma modificação da figura 7.2-2, neste caso considerando hipóteses diferentes.



$$F = F1 + F2 + F3 + F4 + F5 + F6 \simeq 0{,}0003$$

Figura 7.2-3 Árvore THERP modificada para a mudança do modo de injeção

Admite-se que, ao disparar o alarme, os três operadores serão envolvidos. Considerando um total de cinco anunciadores acionados, obtém-se da referência [1] uma HEP de 0,003 para a falha do primeiro operador em não notar o que precisa ser realizado, isto é, que ações teriam de ser tomadas. Considera-se, neste caso, um alto nível de dependência do Operador de Reator - OR, com o Supervisor de Reator - SRE, e um baixo nível de dependência a dependência moderada com o Supervisor de Turno - ST. Assumindo tais níveis de dependência para estas relações, conforme Tabela 6.5-4, adaptada de [1], itens 2 e 3, obtém-se os valores condicionais das HEP's como sendo de 0,5 e 0,15 (Tabela C.1, itens 4a e 3a, do Apêndice C, adaptada de [1]). Dessa forma, a HEPC para a falha em perceber o anunciador crítico é:

$0{,}003 \times 0{,}5 \times 0{,}15 = 0{,}0002$

O caminho de falha F_4 é:

$2 \times 10^{-4} \times 10^{-3} = 2 \times 10^{-7} << 10^{-5}$, valor que não é significativo em APS.

Se o anunciador é adequadamente percebido (probabilidade de 0,9998), julga-se que os operadores estarão, então, sob um nível de estresse estremamente alto, ou estresse de ameaça (ver Apêndice B). Isto se deve ao fato de que, nesse momento, eles percebem que correm um sério risco de falhar ao lidar com um possível acidente mais sério. Conseqüentemente, adota-se um valor para a HEP básica de 0,25 (Tabela C.2, item 7a, Apêndice C [1], que se refere às modificações de HEP's estimadas devido ao efeito do estresse e também considerando a experiência dos operadores, nesse caso, experientes) para a falha do operador que primeiro deveria realizar as ações previstas no item 4.8.1 do procedimento operacional de emergência considerado, dentro do período de 2 minutos após disparo do alarme relacionado ao nível baixo de água no reservatório. Esta HEP básica é multiplicada por 0,63 e por 0,29 (Tabela C.1, itens 4f e 2f respectivamente), para HEPC, devido à dependência do OR com o SRE e ST), resultando em 0,046. O valor do termo de falha para F_5 é, portanto, de aproximadamente 5×10^{-5}, não sendo, portanto, um contribuinte importante para o termo de falha total (F).

Se o operador inicia o passo 4.8.1 do procedimento no tempo previsto (probabilidade de 0,954), ainda existe a possibilidade de acionamento do par errado de comutadores, sendo esta uma tarefa passo a passo, conforme [1], e que, associado ao nível de estresse extremamente alto, implica em que o multiplicador da HEP básica de 0,003 (Tabela C.3, item 2) seja 5, resultando na HEP modificada de 0,015. As HEP"s condicionais para os outros dois operadores são estimadas em 0,5 e 0,05 (Tabela C.1, itens 4a e 2a), neste último caso dependência de SRE para ST), de forma que a HEPC para seleção do par errado de comutadores, que é o produto das três HEP's referentes a três operadores, é igual a 0,0004. O termo de falha final para F_6 é, portanto, muito menor que 10^{-5}, não sendo um contribuinte importante para a falha final.

Continuando com o caminho do diagnóstico correto, a estimativa de 0,999 indica que o evento foi adequadamente diagnosticado e o operador antecipa o alarme de nível baixo de água. Assim que o mesmo dispara, o operador iniciará os procedimentos indicados, começando pelo item 4.8.1. Desta forma, admite-se que tudo esteja sob controle a partir deste momento (nível de estresse passa a moderado), e que só o OR e o ST estejam envolvidos, estando o SRE e talvez algum técnico consultor chamado ao local engajados em outras atividades importantes, mas não relacionadas ao controle direto e à manutenção dos níveis adequados de água, conforme previsto no procedimento.

O OR deverá estar monitorando o medidor do nível de água do RWST, conforme indicado no procedimento escrito, o que é uma tarefa dinâmica, conforme definição na Tabela C.2. O HEP básico é 0,01 para erros de omissão (Tabela C.4, item 4) que, multiplicado por 5 para o caso de tarefa dinâmica desempenhada sob condições de estresse moderadamente alto (Tabela C.2 item 5), devido ao fato dos operadores manterem a situação sob controle, resulta no valor de 0,5. É improvável que o ST esteja ativamente envolvido na monitoração do nivel de água do RWST, o que, portanto, leva à hipótese de que só o OR esteja de fato ocupado com a verificação do nível de água. Isto, considerando que a ação após o alarme tenha sido desempenhada adequadamente. Para esta tarefa, considera-se que erros de ação sejam desprezíveis.

Mesmo que o OR falhe em responder à indicação do nível baixo no medidor do RWST, ele estará alerta para o anunciador associado ao nível baixo. Tanto o OR quanto o SRE estarão ativamente atentos para esse alarme específico, não importando

quantos outros alarmes possam estar disparando no momento. Dessa forma, uma HEP de 0,0001 foi adotada como básica, conforme recomendação de [1]. Foi avaliado um baixo nível de dependência (correspondendo a 0,05, conforme visto anteriormente) para o ST, portanto o HEPC, considerando OR e ST é 0,0001 x 0,05 = 5 x 10^{-6}. Multiplicando os valores para este caminho, tem-se:

0,999 x 0,05 x 5 x 10^{-6}, que é um valor muito pequeno (desprezível).

Se o operador monitora efetivamente o medidor do nível do RWST, assume-se que exista uma dependência completa para a percepção do alarme de nível baixo e o início imediato do passo 4.8.1 do procedimento. Desta forma, a probabilidade de falha condicionada à percepção do alarme é 0, e F_2 representa, portanto, um caminho nulo.

Continuando no caminho de sucesso completo, o erro a considerar é a seleção de par errado de comutadores. O HEP básico de 0,003 (Tabela C.3, item 2) é multiplicado por 2 para levar em consideração o nível de estresse moderadamente alto (Tabela C.2, item 4a) e também por 0,05 para o baixo nível de dependência com o ST (Tabela C.1, item 2a). Em F_3 são envolvidos dois caminhos de falha através do lado esquerdo da árvore de eventos THERP (Figura 7.2-3), mas somente um destes caminhos contribui significativamente para a probabilidade total de falha F. O caminho que não é considerado como contribuinte refere-se ao produto de 0,999 x 0,05 x 0,999995 x 0,0003 = 0,000015. O caminho contribuinte é 0,999 x 0,95 x 1,0 x 0,0003 = 0,0002847, que pode ser arredondado para 0,0003. Para ser exato, F_3 é a soma dos dois caminhos, ou 0,000015 + 0,0002847 = 0,0002997, que arredondado é 0,0003.

O termo de falha final de 0,0003 é o único termo de falha considerável, e representa a probabilidade de falha total para a reanálise. Este valor é aproximadamente um terço do valor calculado no item 7.2.1. Note-se que, em [58], para uma análise baseada em situação similar, o termo de falha final foi calculado como sendo aproximadamente 0,01, ou seja, bem maior que os resultados dos cálculos realizados neste item aqui apresentado.

Estes valores, 0,001 para 7.2.1 e 0,0003 para 7.2.2, muito mais baixos do que o calculado em [58], não são surpreendentes, pois há uma diferença de oito anos entre a referência [58] e a referência [1], sendo esta última a mais recente dentre as duas. Na verdade, no período entre os dois trabalhos, muito foi realizado em termos de treinamento, práticas de operação e adequação das organizações, segundo as recomendações adotadas na filosofia de segurança a partir de meados da década de 1970, ou seja, a ênfase para lidar com situações de emergência, conforme discutido no Apendice B. Essa filosofia foi a base para a prática mais freqüente de simulação de grandes LOCA's em usinas nucleares.

Em [1], que foi o documento básico adotado para este exemplo de aplicações da técnica THERP, é citado que a redução no valor da probabilidade final se deve ao fato de se considerar que o ST esteja diretamente envolvido na seleção do par correto de comutadores a acionar para promover a recirculação. Essas considerações, feitas depois de uma série de entrevistas com operadores e supervisores de operadores de usinas nucleares nos EUA, após a ocorrência do acidente de TMI, deram suporte às atuais hipóteses, adotadas no item 7.2. Na análise anterior realizada [58], o envolvimento do ST não foi considerado como foi em [1].

8. UTILIZAÇÃO DA THERP NA AVALIAÇÃO DA RESPOSTA DOS OPERADORES AO DISPARO DE ALARMES NO REATOR IPR - R1

O estudo apresentado neste trabalho não pretende ser abrangente, mas uma contribuição para técnicos que tenham dificuldades em utilizar estimativas de probabilidades de erros humanos usando a THERP. Pode ser útil como um exemplo prático de aplicação da técnica. As informações e os dados obtidos neste trabalho se relacionam com a utilização da mesa de operação e controle original, atualmente em operação no reator nuclear de pesquisa IPR-R1, e não com a nova mesa, que a substituirá em breve.

8.1 O Reator IPR-R1

O IPR-R1 é um reator nuclear de pesquisas do tipo Triga Mark I, fabricado pela Gulf General Atomic. Nas condições atuais de operação, a sua potência térmica máxima é de 100 kW, com fluxo máximo de nêutrons térmicos de $4{,}4x10^{12}$ $n.cm^{-2}.s^{-1}$.As informações que se referem à operação do reator IPR-R1, foram obtidas das referências [65, 66] e de outros documentos, referenciados oportunamente no texto.

O reator IPR-R1 tem entre suas finalidades a produção de radioisótopos, a análise por nêutron-ativação de espécimes diversos, pesquisa na área de tecnologia nuclear e de reatores, treinamento de operadores e formação de especialistas. Destaca-se que, mesmo sendo o IPR-R1 um reator de pesquisa, em suas instalações foi realizado o Curso de Treinamento em Operadores de Reatores de Pesquisa - CTORP [67], considerado um treinamento padrão básico para operadores de reator de pesquisa e também uma etapa inicial do treinamento de operadores de reatores de potência (CNAA, Angra 1 e 2).

8.1.1 Operação e Controle do Reator

Na Figura 8.1-1 é apresentado um esquema representativo, mostrando o conjunto núcleo e refletor do IPR-R1, antes das modificações realizadas nos últimos anos, onde podem ser observados os sistemas de irradiação e outros componentes.

A operação do reator é feita sempre com a presença de no mínimo dois Operadores de Reator na sala, sendo um deles o Supervisor, que é um operador sênior. Eles são responsáveis pela operação do reator em todas as condições, sejam estas normais, apresentando distúrbios, ou anormais. Os operadores verificam e controlam todas as funções essenciais do reator através da mesa de operação. Nesta mesa estão instalados os medidores, registradores, relés, módulos eletrônicos diversos, sistemas lógicos e outros. As variáveis indicadas e as condições de alarme mostradas na mesa representam os parâmetros mais importantes para sua operação.

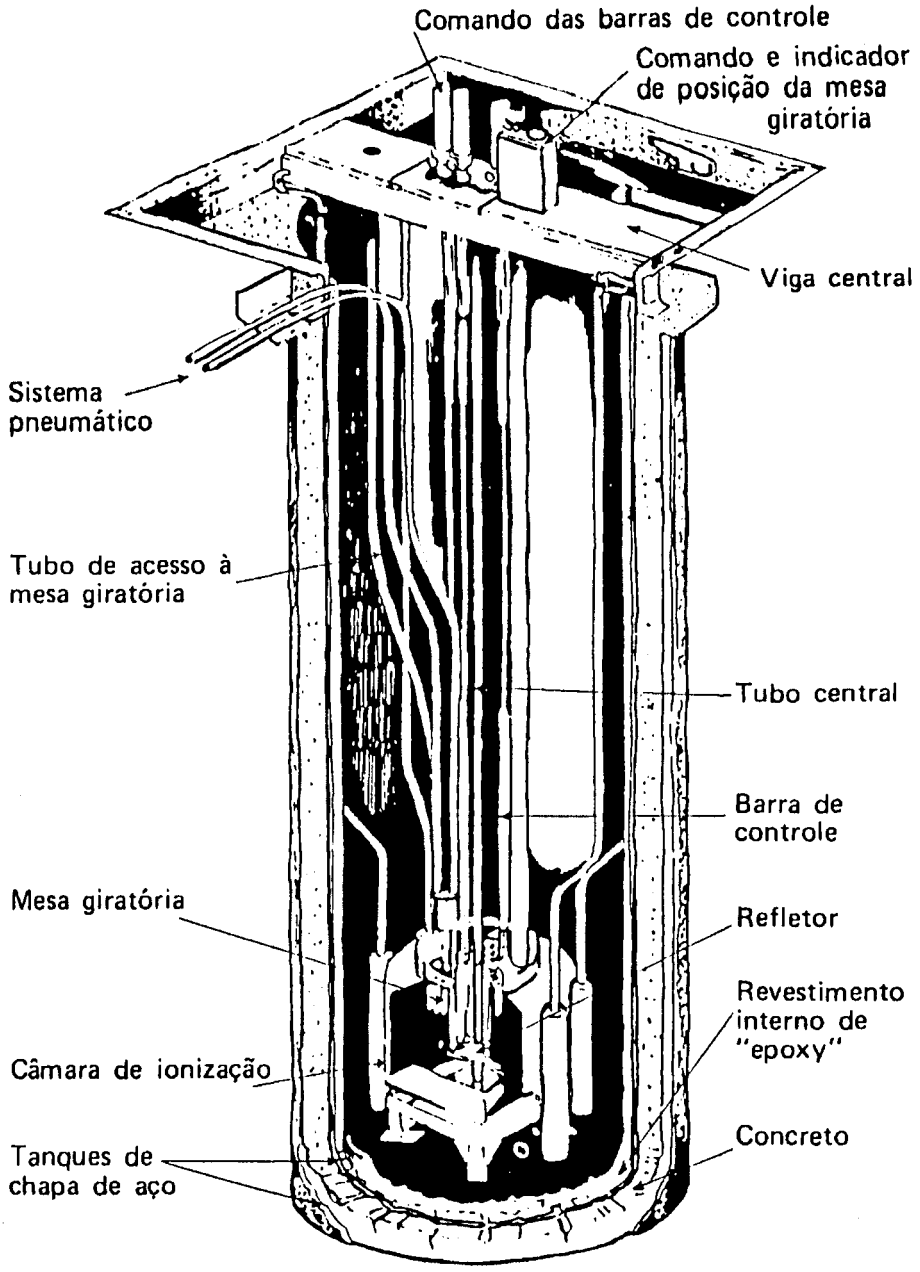
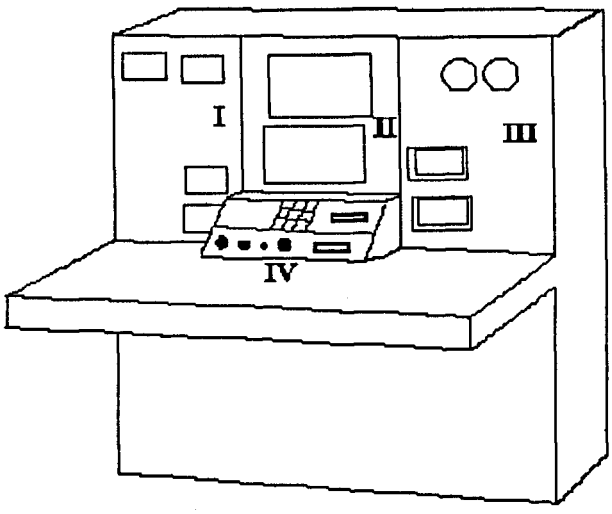


Figura 8.1-1 Vista em corte do reator IPR-R1 mostrando o núcleo e o refletor

Colocar em funcionamento (atingir a criticalidade e elevar a potência ao nível desejado) e desligar o reator são tarefas realizadas pelos operadores, segundo um plano de trabalho estabelecido para cada operação, sempre envolvendo algum experimento ou treinamento. Caso seja necessário, o reator pode ser desligado por medida de segurança, o que representa a situação de real interesse deste trabalho.

Nas Figuras 8.1-2 e 8.1-3 são apresentadas ilustrações esquemáticas referentes ao painel da mesa do reator, e aos mostradores associados aos alarmes relacionados aos níveis de radioatividade, indicados e representados pelas letras A, B e C.



I - Controle de temperatura, água, condutividade, e controle do período do reator

II - Registradores linear e logarítmico

III - Medidores de radiação e de potência (% Power)

IV - Acionadores manuais das barras de controle e sinalização de controle do reator

Figura 8.1-2 Esquema da mesa de operação

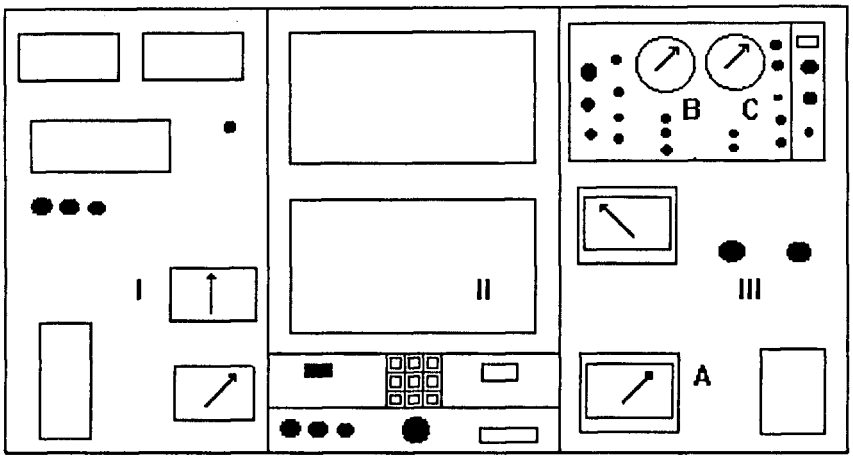


Figura 8.1-3 Detalhe do painel da mesa, com a localização dos mostradores A, B, e C, referentes ao controle de potência do reator IPR-R1 e de níveis de radiação gama na sala do reator (no painel III)

8.1.2 Alterações no reator e na mesa de operações

Está previsto o aumento de potência do reator IPR-R1 para 250 kW, e para tanto está sendo providenciado o seu licenciamento [57], para o qual é aconselhável a realização de uma APS [68]. Nessa APS devem ser considerados os fatores humanos, o que deve incluir a realização também de uma ACH, principalmente relacionados com alguns pontos específicos onde a ação humana seja considerada relevante para a segurança da operação [53, 68, 69].

Devido às dificuldades em sua manutenção, a atual mesa de operação do reator será substituida por outra já montada, de concepção moderna. Isso será feito de forma gradativa, sendo que a nova mesa terá parte de seus sistemas e parte dos sinais ligados à mesa antiga, de modo que a operação continue com esta última, enquanto não sejam aprovados os sistemas da primeira. Entretanto, enquanto não for instalada e licenciada a nova mesa, projetada no CDTN e construida no Instituto de Engenharia

Nuclear - IEN, a operação do reator continuará com a mesa antiga. Depois das mudanças previstas, a ACH poderá ser complementada, com as considerações relativas à nova mesa.

A referência [70] apresenta uma comparação entre a mesa original da General Atomic, em operação, e que foi sendo modificada com o tempo, e a nova mesa, que a substituirá. Dentre as várias modificações, a instrumentação da nova mesa inclui uma central de alarmes. Além disso, várias condições de funcionamento serão observadas em mostradores, facilitando ao operador uma indicação mais precoce das causas geradoras de alarmes. Para obter informações rápidas e precisas sobre as condições de funcionamento e anormalidades durante a operação, foi aumentado o número de anunciadores, de modo a facilitar a visualização pelo operador. Cada nova indicação da mesa contribuirá, por meio da inclusão de novos dados ou parâmetros mais elaborados, para facilitar a operação segura do reator.

Algumas mudanças já foram efetuadas na instalação, dentre as quais mudanças nos seguintes componentes ou sistemas: tanque de liga especial de alumínio; sistema de refrigeração com trocador de calor água-água até 300 kW; registradores para canais lineares e logarítmicos indicadores de potência; medidores de radiação, temperatura, condutividade e controle do nível de água; sistema de desmineralização utilizando resinas troca ionicas em leitos separados; mecanismo de acionamento de barras de controle [70].

As mudanças realizadas foram feitas segundo os critérios estabelecidos para modificações realizadas em instalações semelhantes [71], de forma a preservar os níveis de segurança. É importante lembrar que, na indústria em geral e também em instalações complexas, como é o caso do IPR-R1, as modificações em processos, equipamentos e também em painéis de instrumentação e controle, podem ocasionar problemas inusitados. Isso é devido a que surgem situações que podem não ter sido previstas no projeto das modificações, em geral ocasionando problemas e podendo levar à um aumento na probabilidade de falhas do sistema [71, 72].

O desempenho humano pode ser prejudicado em decorrência de modificações em sistemas complexos. Em [71] é feita uma observação explícita quanto a modificações em que a participação de erros humanos associados com sistemas ou dispositivos podem levar ao aumento na probabilidade de falhas no sistema.

8.1.3 Treinamento e qualificação dos operadores

Os operadores são treinados e qualificados para operar o reator em condições diversas, de forma que o desempenho esperado dos mesmos não seja facilmente comprometido ou afetado por variações ou distúrbios das condições de operação.

Conforme a metodologia utilizada neste trabalho, os operadores foram solicitados a prestar informações, tanto sobre a parte técnica quanto observações sobre experiências pessoais relativas ao próprio desempenho. A experiência obtida em vários anos de operação do reator confere aos operadores a condição de especialistas em sua área de atuação.

Os operadores são submetidos a retreinamento periódico, a fim de manter os padrões exigidos para a operação do reator e de suas condições físicas e de saúde, conforme exigências específicas em normas reguladoras da CNEN [73, 74].

8.2 Considerações Sobre Segurança na Operação

8.2.1 Acidentes e emergência

O reator IPR-R1 é dotado de segurança inerente, pelo coeficiente pronto negativo de temperatura, e tem sido operado com segurança há mais de trinta e cinco anos. Nenhum dos possíveis acidentes previstos com este reator podem gerar conseqüências graves. Mesmo assim, acidentes podem acontecer, liberando material radioativo para o meio ambiente, resultando na contaminação do mesmo. Dentre os acidentes previsíveis de ocorrer, destacam-se, por serem os que poderiam resultar em maiores conseqüências para trabalhadores, população em geral e meio ambiente [75, 76]:

- ruptura do encamisamento de um elemento combustível - pode acontecer pelo desgaste do material estrutural (eletrólise no meio e processo de corrosão) ao longo do tempo e por estar submetido a pressões internas devido a formação dos gases de fissão;
- acidente de reatividade - possível de ocorrer durante a partida e a operação, e em experimentos com alterações na reatividade do reator;
- perda parcial de parte da água de refrigeração e blindagem - pode ocorrer devido a um vazamento no circuito de refrigeração, ou a uma possível fuga no poço do reator.

Em decorrência destas possibilidades de acidentes, e também para atender aos requisitos de licenciamento, foi implementado um plano de emergência para o IPR-R1. Este plano abrange procedimentos de atuação específicos para condições de emergência, além das especificações técnicas (limites) de operação aplicáveis, cujo objetivo é prevenir ou minimizar possíveis conseqüências hipotéticas decorrentes de algum acidente.

Deve ser lembrado que, na preparação de Relatórios de Análise de Segurança de instalações nucleares ou radioativas, e que também abrangem reatores de pesquisa como o IPR-R1, são considerados alguns acidentes, seus eventos iniciadores e conseqüências, o que envolve a preparação de planos de enfrentamento às situações de emergência (incluíndo os procedimentos operacionais de emergência, conforme concepções mais atuais da filosofia de segurança - ver Anexo A) [77, 78].

No documento "Plano de Emergência do Reator IPR-R1" [75], está definido o nível de emergência *Evento Não Usual - ENU*, que se configura segundo algumas condições a partir das quais torna-se necessário desligar o reator. ENU é definido como "a situação que se configura no instante em que se verificar, no reator ou em áreas próximas, uma das condições iniciais que indique possível degradação no grau de segurança, podendo resultar em um potencial significativo de acidente envolvendo liberação de material radioativo e/ou irradiação de pessoal envolvido na sala do reator ". Caso as condições de operação impliquem na ocorrência de um ENU, o reator deve ser imediatamente desligado, conforme ítem explícito no procedimento operacional incluso ao Plano de Emergência, " Ocorrência de ENU no reator IPR-R1 " [76], específico para atuação em emergência.

8.2.2 Condições de desligamento

Uma das condições iniciais consideradas para o ENU é o aumento do nível de radiação acima de limites operacionais especificados na sala do reator, indicado pelo disparo de alarmes, e que pode resultar em perda de segurança operacional ou acidente.

O Operador é o principal elemento de atuação no Plano de Emergência, sendo responsável por todas as condições de operação. Juntamente com o Supervisor, tem como uma de suas atribuições diagnosticar o ENU e promover o desligamento ("scram") do reator, se este for o caso. Para isto, as barras de controle são introduzidas rapidamente, por gravidade, a fim de desligar o reator, compensando imediatamente o excesso de reatividade em razão de alguma condição que configure degradação da segurança ou prejuízo para os sistemas do reator. Com este procedimento, são evitadas possíveis conseqüências que possam colocar em risco os operadores, o reator, outros trabalhadores e algumas áreas próximas dos limites físicos das instalações do reator.

Em condições anormais de operação, o reator é desligado automaticamente ou com a participação do operador. No caso de um pico de reatividade positiva, o reator é desligado automaticamente com a queda brusca das barras de controle ("scram"), devido ao curto período ou por excursão de potência além do limite estabelecido.

O disparo de alarme devido à reatividade também pode ocorrer devido à retirada brusca de amostras de materiais altamente absorvedores de nêutrons, ou que possuem alta capacidade de retenção de produtos de fissão. Neste caso, o reator se desliga automaticamente e sinaliza o motivo do desligamento. O alarme pode disparar também devido à movimentação de algum material especial perturbador da reatividade (cádmio, boro, etc). Neste último caso, o reator não desliga, apenas perde o canal de potência. Estas operações especiais não fazem parte do escopo usual de operações, portanto não estão sendo consideradas neste exemplo.

No caso de ruptura do revestimento do combustível (a espessura do encamisamento é de 0,7 mm de alumínio, ou 0,5 mm de aço inoxidável), pode ocorrer liberação de gases de fissão e amostras (alvos para irradiação, como, por exemplo minérios), contaminando a água do poço do reator e resultando no disparo do alarme de aumento do nível de radioatividade. Neste caso, o operador deve desligar imediatamente o reator e adotar os devidos procedimentos para recuperação das condições normais de segurança de operação do reator.

Alguns critérios para desligar o reator, em determinadas circunstâncias e para alguns sistemas devem ser obedecidos, de forma a preservar esses sistemas. Por exemplo, o desligamento do reator, em caso de aumento da radioatividade na água de circulação, tem prioridade sobre a circulação de água pelo sistema de resina, de modo a evitar que esta tenha sua radiação de fundo, ("background") aumentada. Portanto, desliga-se o reator, procede-se à desmineralização, se necessário, e reinicia-se a operação, posteriormente. Este é um critério de preservação de sistemas do reator.

Com relação ao estresse de operadores do reator IPR-R1, não se espera, mesmo em situações de emergência, que se sintam seriamente ameaçados por alguma condição anormal e que possa levar a algum acidente, já que as conseqüências de acidentes são bem limitadas, devido à segurança inerente típica de reatores modelo Triga.

8.2.3 Causas do aumento do nível de radioatividade

Devido à possibilidade de acidentes, conforme descrito em 8.2.1, o aumento do nível de radioatividade pode ocorrer provocado por algum sistema defeituoso do reator ou devido a falha de algum componente, resultando no disparo de alarmes. Isto implica em danos a sistemas do reator, com perda de segurança.

A ruptura do revestimento do combustível ou a perda de água do poço (perda de blindagem e refrigeração) causa aumento do nível de radioatividade na sala. No caso de perda de água no poço, um sensor auxiliar de nível dispara antes do alarme que acusa aumento da radioatividade. Se o reator estiver operando e o sistema de refrigeração estiver desligado por mais de meia hora, outro alarme pode ser disparado antes daquele referente ao nível de radioatividade. Portanto, para que dispare o alarme de radioatividade no poço do reator, indicativo de acidente, a causa pode ser devido à contaminação da água; retirada de amostras; ruptura do revestimento combustível ou nível de água do poço abaixo do limite considerado normal.

O disparo de alarme também pode ser causado por alguma falha na condução da operação, podendo resultar em perda irreversível de segurança e, ocasionalmente, em emergência e acidente. Por outro lado, a falha na condução da operação pode ser reversível, como no caso de esquecimento, pelo operador, de ligar o exaustor para renovação do ar da sala, caso o reator esteja operando há muitas horas.

Outra possível condição que pode elevar o nível de radiação acima de limites permitidos, sem estar, no entanto, relacionada com a possibilidade de perda imediata de segurança seria o caso da mesa giratória de irradiação do reator ter sido preenchida com grande volume de amostras. Depois de algumas horas de operação, isto pode ser a causa de disparo de alarmes.

Eventualmente, o disparo de alarmes pode ser causado por fontes radioativas como amostras irradiadas nos experimentos realizados, gases resultantes de produtos irradiados originados de espécimes armazenadas provisoriamente ou outros resultantes de materiais estocados na sala do reator ou em outros locais próximos.

No caso do reator estar funcionando continuamente, pode ocorrer acúmulo de gases contendo nuclídeos radioativos na sala, podendo causar o disparo de alarmes. São gases naturais formados na irradiação de ar e água, como ^{41}Ar e ^{16}N, e eventualmente produtos de fissão decorrente de vazamentos do recipiente de amostras que contenham materiais físseis ou férteis (Urânio e Tório).

8.3. Diagnóstico de ENU

8.3.1 Condições para diagnóstico - procedimentos

Como visto, existem diferentes causas possíveis de disparo de alarmes relacionados com o aumento do nível de radioatividade. Nem sempre o disparo destes alarmes indica perda substancial de segurança, implicando em condição de desligamento do reator, [76].

Desligar o reator de forma não prevista ou planejada implica prejuízo ou atraso em algum experimento em andamento. Assim, devem ser feitas verificações, pelos

operadores, no sentido de confirmar a necessidade do desligamento devido ao aumento do nível de radioatividade, no menor prazo de tempo possível.

Existem três possibilidades, conforme discutido em 8.2, para o disparo de alarme associado ao nível de radioatividade. Na primeira, algum problema em sistemas do reator causa o disparo de alarme, em decorrência de falha ou defeito de algum componente, ou ainda devido a erro de operação, que ocasiona perda de segurança e, portanto, o reator deve ser desligado. Outra possibilidade é quando a perda de segurança não é irreversível, ou seja, existem condições de recuperação para a normalidade (por exemplo, formação de ^{41}Ar em operações de longa duração). A última possibilidade é que o reator ou seus sistemas não se encontram envolvidos no aumento da radioatividade, portanto indicando causas externas, tais como fontes, inadvertidamente movimentadas na sala de reator. Neste caso, o reator só deve ser desligado se não for encontrada a causa do disparo do alarme, dentro de um determinado período de tempo. Isto, por medida de segurança, para que os operadores não fiquem expostos à irradiação ou possível contaminação.

Para verificar as causas do aumento do nível de radioatividade, e confirmar qualquer hipótese relacionada com a operação do reator, o operador utiliza mostradores e medidores da mesa de operação, contadores portáteis disponíveis na sala e também outros indicadores associados a alguns sistemas auxiliares. Por exemplo, as caixas protetoras do sistema primário possuem sensores de temperatura, radioatividade e condutividade da água, que podem fornecer indicações importantes, e facilitar o reconhecimento de uma determinada condição anormal ou de distúrbio na operação, ajudando na determinação da causa do aumento do nível de radioatividade.

As verificações de condições, de níveis e de valores em mostradores e instrumentos permitem, pela sua interpretação, que o operador confirme se o disparo de alarme corresponde ou não a uma situação de emergência ou ENU (atribuições e responsabilidades estabelecidas nas referências [75, 76]).

Se o operador chega à conclusão que o disparo de alarmes é decorrente de defeito ou problema em sistemas do reator (situação anormal), podendo ocasionar perda de segurança (distúrbios de operação), ele desliga o reator. No caso de ser outra a conclusão do operador, isto é, que o alarme disparou por causas que aparentemente não afetem a segurança, então a ação, quando possível, é a de procurar a causa e realizar ajustes de operação.

Se as verificações permitem indicar condições para ajustes de recuperação, de modo que a operação do reator seja restabelecida, considera-se que o mesmo volta a operar em condições normais, portanto sem necessidade de desligar o reator, preservando-se a experiência em curso.

Dessa forma, no período de tempo entre a constatação do aumento do nível de radiação, indicado pelo disparo de alarmes, e a ação efetiva de desligar o reator, este ainda continua em operação, baseado em algumas regras e considerações dos operadores que levam em conta fatores relacionados com o tempo e as condições de segurança. Existem, então, ações não cobertas por procedimentos, correspondendo a associar uma determinada causa ao alarme, ou seja, a realização do *diagnóstico* de ENU.

A realização de diagnóstico pressupõe interpretação, portanto fazendo uso do desempenho baseado no conhecimento, o que implica, conforme as referências [30, 31], em mais alta probabilidade de ocorrência de erros humanos, quando comparado com desempenho sem necessidade de interpretação.

Para o caso do IPR-R1, as ações correspondentes ao diagnóstico poderiam ser incluídas em procedimentos, de forma a privilegiar o desempenho baseado em regras que, em comparação com o desempenho baseado no conhecimento, resulta em estimativas menores de probabilidades de erros humanos. Assim, em lugar de interpretações, comuns em atividades onde exista algum nível de improvisação, podem ser utilizadas verificações simples, como "checklists", que facilitem ao operador a determinação da causa do disparo de alarme e direcionar suas ações subseqüentes.

O simples fato de prever algumas possibilidades, tentando ampliar ao máximo o seu escopo, e direcionar ações dos operadores conforme itens específicos, assegura ações planejadas, que devem ser avaliadas em treinamentos e revisadas se necessário. Evitar a ocorrência de imprevistos diminui ou elimina a necessidade de recorrer ao desempenho baseado no conhecimento. Adicionalmente, deve-se considerar que procedimentos são documentos dinâmicos e, como tal, à medida em que são reavaliados em treinamentos, podem ser reestruturados , de forma a se tornarem progressivamente mais eficazes.

8.3.2 Período de tempo para a realização do diagnóstico

O período de tempo que seria suficiente e seguro para o operador diagnosticar o ENU, após o disparo de alarme referente a alto nível de radioatividade, não é indicado em procedimento algum, ficando a critério do Operador e do Supervisor, que deve estar presente, sendo consultado sobre a ação de desligar o reator. Na situação de fato, o diagnóstico deve ser feito no menor tempo possível. Se não for encontrada a causa do aumento do nível de radioatividade em um determinado período de tempo, o reator deverá ser desligado.

Depois de constatado o aumento do nível de radioatividade, uma posição conflitante de opiniões entre o Operador e o Supervisor pode causar dificuldades quanto ao momento ideal de desligar o reator. Embora prevaleça a orientação do Supervisor, esta interface homem-homem poderia ser eliminada com alguns critérios bem estabelecidos para a ação de desligar o reator, desde que incluída em ítem de algum procedimento. O principal destes critérios seria estipular um determinado período de tempo após o qual o reator seria desligado. Ou seja, configurada a situação de emergência ou ENU, e possivelmente considerando outras indicações, o Operador desliga o reator.

Também para o fator tempo, a necessidade de desempenho baseado no conhecimento pode ser modificada para ações baseadas em regras. Para efeito do presente trabalho, o período de tempo para o diagnóstico foi estipulado como sendo de 10 minutos, em lugar de "menor tempo possível". Esta estimativa foi adotada considerando a opinião dos operadores e de técnicos que têm ou tiveram uma grande experiência de operação do reator (note-se que a reatividade não está sendo considerada). Um dos operadores , com apoio do outro atualmente licenciado, considerou 1 minuto suficiente, e mais tempo para operadores com menor experiência. Um dos técnicos que tomaram parte na operação do reator por muitos anos, consultado a respeito, considerou 3 minutos um tempo adequado, para operadores experientes. Os operadores e técnicos consultados foram considerados especialistas para este ajuste, nas condições estudadas de operação do IPR-R1, conforme critérios e ressalvas baseadas na referência [1]. Uma das ressalvas dessa referência é que o operador treinado, em geral, sempre considera a disponibilidade de tempo suficiente para a

execução de tarefas em condições de emergência, revelando um certo otimismo, com o que especialistas em ACH nem sempre estão de acordo.

8.4 Comentários Sobre APS e ACH para o Estudo Realizado

O que se faz numa Avaliação Probabilística de Segurança é avaliar um sistema, verificando as contribuições das falhas de cada componente ou subsistema em termos numéricos, considerando determinadas situações, inclusive as contribuições de erros humanos.

Algumas ações humanas podem ser consideradas irrelevantes, se não contribuem decisivamente para uma falha. Entretanto, numa situação de emergência ou pré-emergência, quase sempre serão as ações humanas as que mais contribuirão para uma possível falha do sistema. Em qualquer instância onde seja necessária, a atuação humana é um importante fator a ser considerado.

Deve ser lembrado que situações de emergência por si mesmas já causam alterações no desempenho humano, podendo fazer com que este seja inadequado ou mesmo, em algumas condições, inaceitável. Nesses casos, quase sempre a contribuição do desempenho humano é o fator chave na probabilidade de falha do sistema homem-máquina, contribuindo negativamente e comprometendo o desempenho do sistema como um todo.

8.4.1 Abrangência da ACH

O presente estudo para o reator IPR-R1 leva em conta apenas as ações para a realização do diagnóstico de uma possível condição de emergência (ENU). Assim, serão importantes as tarefas de verificação, por parte dos operadores, após o disparo de um ou mais alarmes, que correspondem ao diagnóstico de uma hipotética emergência no reator IPR-R1. As ações subseqüentes dependeriam do diagnóstico, ou seja, desligar o reator, ou, ao contrário, controlar a causa do aumento do nível de radioatividade, ou eliminar alguma possível causa, isto é, remover fontes indevidamente localizadas

Uma importante observação diz respeito à avaliação probabilística de segurança dos sistemas do reator IPR-R1. Como esta APS ainda não foi realizada, as ações humanas consideradas neste trabalho são aquelas ligadas à operação do reator no caso de condições de emergência ou pré-emergência, portanto em condições tradicionalmente consideradas relevantes pela bibliografia existente e pela experiência adquirida na operação de sistemas complexos.

8.4.2 Considerações sobre o estudo de APS para o reator da Universidade do Novo México, para auxiliar na análise do reator IPR-R1

Durante o período de 1990 a 1991 foi realizado um trabalho de APS para o reator de pesquisas da Universidade do Novo México [79]. Este reator, fabricado pela "Aerojet General Nucleonics", tem baixa potência, utiliza um composto de UO_2 enriquecido como combustível, com moderador de polietileno, refletor de grafita, blindagem de chumbo e água. A sua operação é realizada pela inserção e retirada de barras de controle e de segurança, analogamente ao IPR-R1. Embora o referido reator seja de

concepção diferente do IPR-R1, ambos são do tipo utilizado em pesquisa, e como tal tendo finalidades análogas às citadas no item 8.1.

Neste ítem serão são ressaltados alguns comentários a respeito deste trabalho, como possível fonte de comparação com a APS a ser ainda realizada para o IPR-R1, focalizando a THERP lá realizada.

A APS realizada para o reator da Universidade do Novo México tinha o objetivo de obter dados sobre a probabilidade e conseqüência do máximo acidente postulado para aquele reator, que implique na liberação de material radioativo. No trabalho realizado, detectou-se um potencial significativo de erros humanos que poderiam precipitar ou aumentar a probabilidade de ocorrência do máximo acidente postulado. Ou seja, em determinados sistemas analisados, os erros humanos poderiam contribuir decisivamente para possíveis falhas, ocasionando acidente. Em decorrência disto foi realizada, subseqüentemente, uma Análise da Confiabilidade Humana, para avaliar o impacto da ação humana sobre a segurança do sistema. Foi utilizada a técnica THERP para avaliar os valores de probabilidades de erros humanos.

O trabalho ressaltou a importância do homem com relação à segurança do reator de pesquisa da Universidade do Novo México. A contribuição do erro humano para a probabilidade de falha da integridade do tanque do núcleo, na análise das tarefas pré-acidentes foi considerada muito alta (12%). Esta alta probabilidade, devido ao fato de não haver fatores de recuperação, à alta dependência e ao fato de ser um sistema em série, indicou que as ações dos operadores favoreciam a ocorrência do máximo acidente postulado. A HEPB adotada para cada tarefa, na análise deste sistema, foi de 0,03, com fator de erro de 0,5.

As tarefas consideradas em [79] foram: as pré-acidentais, ou aquelas que, se desempenhadas incorretamente, poderiam resultar na não disponibilidade dos sistemas analisados, e as pós-acidentais. As tarefas pré-acidentais consideradas concentraram-se nos erros de restauração ou recuperação, ou seja, nos ajustes de operação que permitiriam que o sistema retornasse às condições seguras ou normais de operação. Os procedimentos direcionavam o operador para o desligamento imediato do reator, desde que configurada a ocorrência de anormalidade. Assim, o desligamento manual do reator foi considerado como uma tarefa estritamente de pós-diagnóstico

Os resultados obtidos a partir da análise da confiabilidade humana pós-acidentais indicaram a possibilidade de melhoria em alguns pontos. Considerou-se que um ajustamento no desempenho dos operadores poderia melhorar os resultados obtidos, principalmente quanto à preparação mais adequada para enfrentar condições de emergência.

8.5 Dados e Informações

8.5.1 Situação considerada para a análise

O ENU leva em conta outras possibilidades, além da constatação ou indicação de alto nível de radioatividade na sala do reator. Para este trabalho, foi considerada apenas a ocorrência de alto nível de radioatividade na sala, indicada pelo disparo de alarmes.

Foi descartado o acionamento indevido dos alarmes, ou seja, mal funcionamento de seus componentes. Isto deve ser considerado em uma APS, já que são componentes elétrico-mecânicos ou eletrônicos . O mal funcionamento acontece quando, por exemplo, por algum motivo, o alarme dispara sem ter sido ativado após atingido o nível de radioatividade estabelecido para acionar o mesmo. Neste trabalho, supõe-se que os alarmes e seus componentes sejam confiáveis. Entretanto, é importante ressaltar que, no caso de alarmes que disparam indevidamente com muita freqüência, o operador termina por duvidar da confiabilidade do mesmo e assimilar uma confiança em excesso. Se o alarme dispara, o operador tende a considerar que o problema não está relacionado com o reator e, portanto, não considera que haja alguma ameaça à segurança ou à integridade dos sistemas do reator.

Em geral, essa situação de alarmes que funcionam indevidamente tende a diminuir o nível de estresse de operadores para muito baixo (Figura B.3-1, do Anexo B), comprometendo o seu desempenho na atuação em condições de emergência, podendo colocar em risco a segurança da operação.

Na Figura 8.5-1 é apresentado o último ramo da árvore de falhas representando a situação e considerando duas possibilidades de desligamento do reator, automático ou manual.

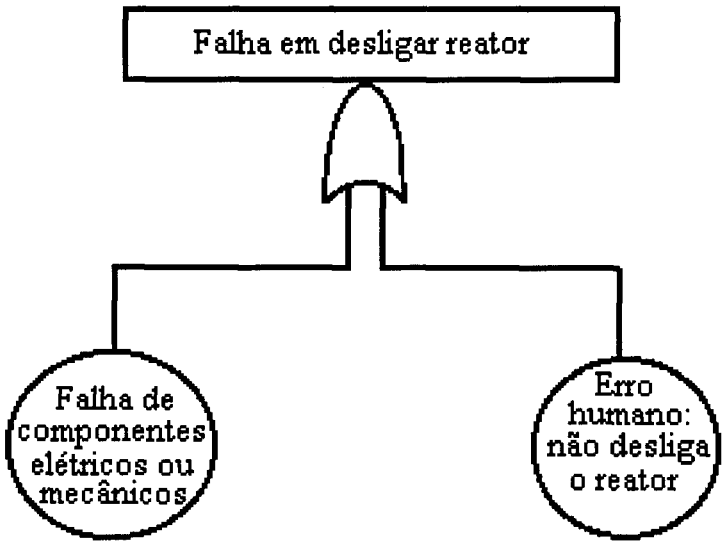


Figura 8.5-1 Árvore de falhas para o exemplo THERP / IPR-R1

O estudo realizado teve como objetivo avaliar o impacto das ações ou omissões humanas na condição específica de desligamento não planejado do reator por medida de segurança. Para isto foi utilizada a técnica THERP, considerando-se que:

- ocorre um aumento do nível de radioatividade na sala do reator, causando disparo de alarmes;
- são considerados alarmes associados ao aumento do nível de radioatividade;
- por hipótese, os alarmes funcionam perfeitamente, ou seja, são componentes confiáveis;
- não ocorre o desligamento automático do reator, sendo necessária ação do operador.

Não foi considerado o acidente de reatividade, porque nesse caso específico, haverá desligamento automático.

O desligamento automático não ocorre, descartado o acidente de reatividade. Portanto, somente o erro humano, é considerado na THERP, ou seja, o operador não desliga o reator num determinado período de tempo (situação atual). Uma opção para esta indefinição quanto ao tempo para se desligar o reator é estabelecer um período de tempo de 10 minutos.

8.5.2 Ações dos operadores após o disparo de alarmes

Para este trabalho, foram feitas algumas simplificações, uma das quais a de considerar que, quando três alarmes disparam ao mesmo tempo, isto corresponde de fato ao aumento do nível de radioatividade originado em sistemas do reator. Esta é uma boa aproximação da realidade, já que o disparo de três alarmes representa uma forte indicação de aumento do nível de radioatividade originado nos sistemas do reator, em condições reais, desprezando as falhas de modo comum que pudessem ser consideradas.

O fluxograma apresentado na Figura 8.5-2 resume as ações dos operadores, em sequência ao disparo de alarmes relacionados com o aumento do nível de radioatividade.

Obviamente, as ações consideradas não seguirão necessariamente uma determinada ordem, visto que algumas variações ocorrem dependendo de elaboração mental do próprio operador

Por simplificação, o excesso de amostras nos dispositivos de irradiação e a contaminação da água do poço por amostras não foram considerados no fluxograma.

O ponto de partida é o disparo de um ou mais dos alarmes associados ao aumento do nível de radiação na sala do reator. O operador responde ao alarme ou não. Neste último caso trata-se de omissão, cuja probabilidade de ocorrência é muito pequena. Na resposta ao alarme, os operadores verificam se há indicações contraditórias ou conflitantes nos mostradores dos medidores ("gama-meter" e outros), na mesa de operação, indicados por A, B e C na Figura 8.1-3.

Como se considera que o disparo de três alarmes ao mesmo tempo corresponde a um problema originado nos sistemas do reator, os mostradores da mesa indicam que há alta atividade de radiação na sala do reator. Ou seja, componentes do reator podem ter sido danificados, ocasionando a liberação de algum material radioativo, provocando o disparo dos alarmes.

Em seguida, o operador deve verificar outros indicadores dos sistemas relacionados com o reator, como indicadores de condutividade. Por exemplo, verifica-se as condições da água do poço do reator, ou a água de circulação, usando detectores de radiação e outros.

Sendo detectado nível alto de radioatividade em algum local que permita a sua associação com um dos sistemas relacionados à operação, o operador deve verificar a possibilidade de não ter sido acionado o sistema de exaustão, e também a possibilidade da ocorrência de movimentação de amostras na mesa após horas de operação. Dependendo desta verificação, ele deve desligar o reator ou ligar o sistema de exaustão. Neste último caso, novas verificações devem ser feitas, confirmando ou não se o nível de radioatividade diminui. Se não diminuir dentro de um certo período, ou se não houver indicação positiva

de que vai diminuir, o reator deve ser desligado, por tratar-se de condição de perda de segurança.

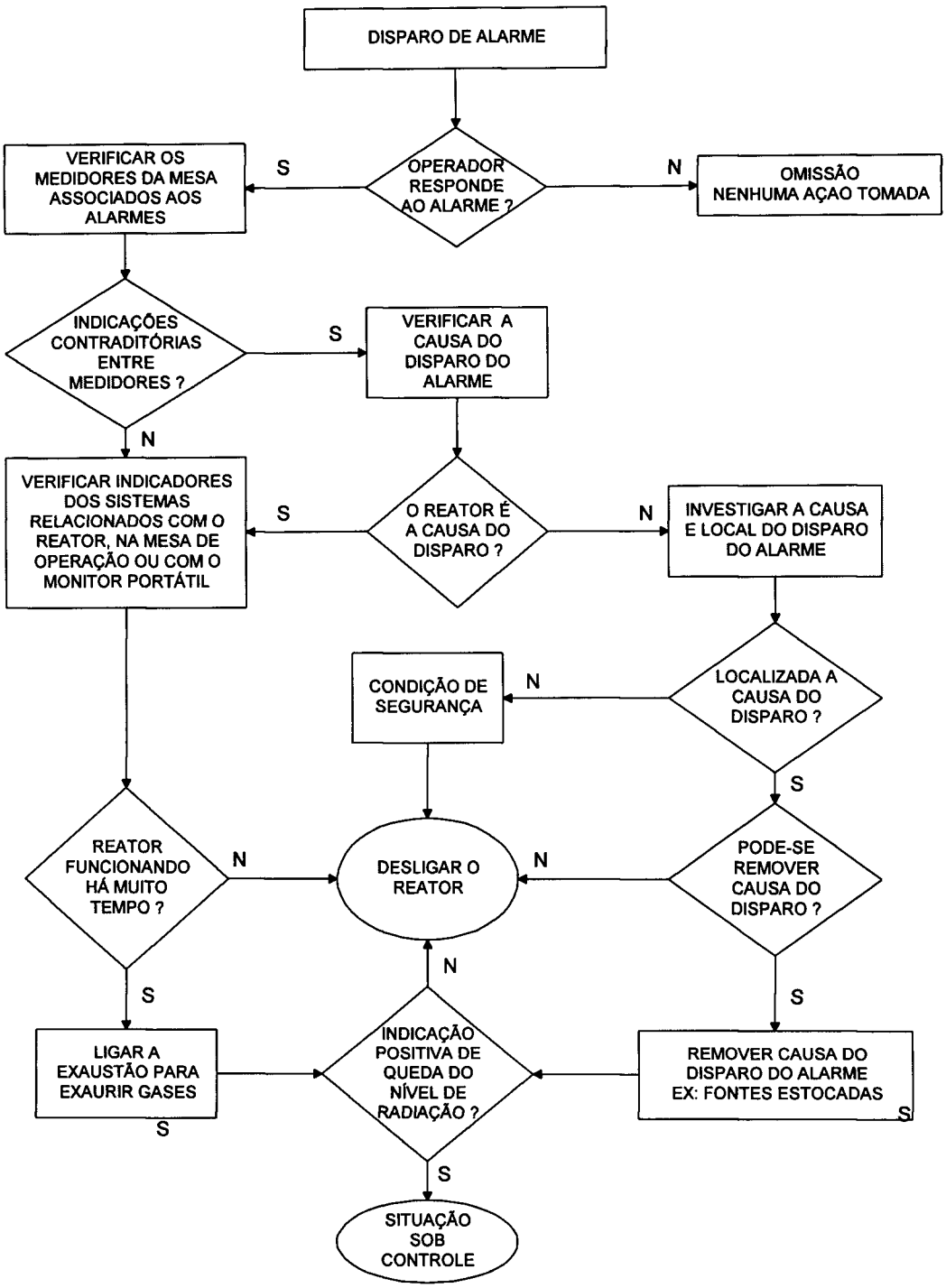


Figura 8.5-2 Ações dos operadores após disparo de alarmes

Portanto, o disparo do alarme de radioatividade no poço do reator pode ser decorrente da contaminação da água por amostras, por causa de ruptura de revestimento

combustível, ou por outras razões, como a liberação de gases radioativos devido à operação do reator por muito tempo.

Sendo confirmada a causa do aumento do nível de radiação nos sistemas relacionados à operação do reator e que não permitam um ajuste, a ação específica indicada é o seu desligamento, pois pode haver comprometimento do grau de segurança.

Por outro lado, havendo discordância nas indicações dos três mostradores da mesa, ou se um ou dois alarmes dispararam, a indicação pode ser a de que o problema é resultante de alguma outra causa e não de sistemas do reator. Neste caso, o operador vai verificar porque um ou dois alarmes não dispararam, ou porque não dispararam todos os alarmes.

8.5.3 Aspectos considerados na coleta de dados e informações

Para o presente trabalho, assim como acontece em muitos outros, não foram isoladamente seguidos os passos da THERP conforme discutido em itens anteriores, em decorrência da realização de atividades que podem ser efetuadas ao mesmo tempo, de modo que ocorre uma superposição de etapas. A primeira parte das etapas previstas para a realização da THERP, compreendida como a *familiarização,* foi a coleta de dados e informações sobre alguns sistemas, necessários ao presente nível de estudo, com base nos documentos referenciados e também diretamente por informações obtidas em entrevistas com o pessoal envolvido na operação do reator.

A *avaliação qualitativa* foi realizada pelo estudo de desempenho dos operadores, que incluiu considerações sobre a mesa de operação, a verificação dos controles e as limitações consideradas, como considerar três alarmes disparando uma indicação positiva de aumento do nível de radioatividade nos sistemas do reator, em lugar de forte indicação, como exposto anteriormente. Informações prestadas pelos operadores foram verificadas com a observação dos mesmos ao operar o reator e avaliadas segundo critérios contidos na referência [1].

As avaliações realizadas basearam-se, portanto, em dados obtidos na análise das tarefas dos operadores, nos procedimentos aplicáveis, e em outros fatores que influenciam o desempenho do sistema, como o estresse. O movimento ou deslocamento dos operadores para o desempenho da resposta ao alarme foi incluido no período de tempo considerado no item 8.3.2.

De acordo com o exposto no Anexo B, item B.3.1, o nível de estresse extremamente alto está associado a ameaças ao bem-estar individual, à auto-estima ou ao status profissional do operador, e isto não é pertinente para os operadores do IPR-R1. O nível de estresse considerado foi o de moderadamente alto, para as situações estabelecidas. Operadores menos experimentados, como seria o caso de iniciantes na operação do reator, poderiam, em algumas circunstâncias, ficar mais sujeitos ao estresse do que o Supervisor ou um Operador sênior, o que está de acordo com o recomendado na bibliografia disponível sobre o assunto [1, 48]. Por simplificação, outros fatores não foram aplicados, como por exemplo considerações sobre o projeto da mesa e a interface homem máquina.

Com as informações e os dados adquiridos, foram verificadas as exigências do desempenho, e sua avaliação, para as tarefas de operação do reator em condições normais e simulando situações específicas de emergência. Assim, os objetivos e as

exigências do desempenho de cada tarefa e a identificação de erros potenciais foram avaliados.

A *avaliação quantitativa* foi realizada usando os critérios e dados básicos e recomendações da referência [1], como o ajustamento para modificar algumas probabilidades específicas de erros humanos para as condições reais observadas. Para isto, foram consideradas as avaliações e observações dos operadores e do pessoal responsável pelo reator.

Em resumo, para a modelagem das ações dos operadores em seguida ao disparo de alarme, e o desenvolvimento da árvore THERP, foram realizadas as seguintes etapas da avaliação quantitativa: atribuição de HEP's; identificação e estimativa de efeitos de PSF's; avaliação da dependência entre os operadores e as ações; e avaliação de fatores de recuperação. A estimativa da contribuição do erro humano para a falha do sistema foi, então, calculada, utilizando-se os dados obtidos.

8.6 Aplicação de THERP para o IPR-R1

O enfoque neste estudo é estimar o erro humano na realização de diagnóstico, considerando a ruptura de revestimento de elemento combustível após várias horas de operação do reator. O problema refere-se, portanto, à falha de um componente mecânico. Por razões de segurança e conforme o critério de preservação dos sistemas do reator, este deve ser desligado.

Para a ruptura do revestimento combustível, conforme a simplificação adotada no item 8.5.2, três alarmes disparam, não havendo discrepância nos indicadores dos mostradores A, B e C da mesa. Os três fornecem indicações positivas de aumento do nível de radioatividade. Entretanto, este sintoma apresentado para o operador pode ser associado a outra condição, ou seja, no caso, gases originados pela operação do reator (irradiação de ar, água, liberação de produtos de fissão de amostras). Assim, duas possíveis diferentes causas para o mesmo sintoma dificultam a realização do diagnóstico correto. Para simplificação, considera-se que o volume de amostras não ultrapassou o limite que permitisse o aumento do nível de radioatividade de tal forma que pudesse ocasionar o disparo de alarmes.

Conforme o fluxograma apresentado na Figura 8.5.2, quando as indicações dos mostradores não são conflitantes, o operador sabe que a causa do disparo dos alarmes se refere ao reator ou a sistemas associados. Ele deve, portanto, verificar indicadores desses sistemas, para confirmar a hipótese de ruptura do revestimento do elemento combustível.

Tendo condições de realizar o diagnóstico correto, ou seja, identificar os sistemas que influenciam ou componentes cuja situação implica algum dano, dentro de um período de tempo especificado, o operador desliga o reator. Do contrário, ou seja, a partir de diagnóstico incorreto, ele deve ligar o exaustor, para expelir os gases, já que este é o procedimento previsto, dado que o reator já está funcionando há muito tempo. Esta opção entre uma ou outra alternativa é a etapa de *tomada de decisão,* conforme visto anteriormente. Em seguida, ele deve monitorar o nível de radioatividade, de modo a acompanhar o decaimento (verificar se tende a diminuir). Portanto, a realização do diagnóstico correto implica em desempenho correto da ação de desligar o reator. A ação de recuperação correta implica em ter o reator desligado no tempo previsto. E o

diagnóstico incorreto implica no desempenho de ação não adequada para o momento, embora esteja dentro do escopo de ações a serem desempenhadas, porém numa outra situação.

8.6.1 Modelagem e atribuição de valores aos HEP's

Abaixo são resumidas as ações e atribuidas as HEP's nominais aos eventos correspondentes.

A - para a omissão em não responder ao disparo de alarme, foi estipulado o valor 10^{-4} com fator de erro de 10 [1], considerado adequado para a situação descrita em 8.5.2.

B - para erro na verificação dos sistemas associados ao reator, de maneira a confirmar a ruptura do revestimento de elemento combustível, foi atribuido o valor de 3.10^{-3}, com fator de erro de 5, com base em [1], e que consta deste trabalho na Tabela 4.3.-2. Este valor corresponde a uma estimativa genérica básica usada quando não existem valores específicos para algum caso determinado. Para o exemplo apresentado, a verificação é o próprio diagnóstico e, como ressaltado anteriormente, ao diagnóstico corresponde uma ação desempenhada. Portanto, para diagnóstico correto, reator desligado, e para diagnóstico incorreto, exaustor ligado.

Considera-se que os eventos B e b são eventos independentes do evento a, já que as tarefas para a realização do diagnóstico são apenas iniciadas pelo disparo de alarmes. Para erro na ação de recuperação, ou seja, não desligar o reator, foram utilizados os seguintes dados, utilizando a Tabela 5.4-1, para níveis de dependência:

C' - sem especificar o tempo para desligar o reator, utiliza-se a HEP = 1 em decorrência de ser considerado nível de dependência total com relação à tarefa anterior, ou seja, como o operador falhou na primeira tarefa, continuará em falha na subseqüente, não desligando o reator. Para trabalhar com incertezas, são adotados os valores 1 para a margem superior, e 0,5 para a margem inferior, considerando o nível de dependência completo, dada a falha na tarefa anterior, conforme referência [1].

C - especificando o período de tempo de 10 minutos para desligar o reator, utiliza-se a HEP de 0,5 em decorrência de ser considerado alto nível de dependência, com relação à tarefa anterior. Isto devido a que o período de tempo estipulado tem o efeito de diminuir o nível de dependência com a tarefa anterior. Neste caso, para a incerteza, adota-se o valor de 1 para a margem superior, e de 0,25 para a margem inferior, para alto nível de dependência, dada a falha na tarefa anterior, conforme referência [1]. Nos dois casos, trata-se de probabilidade condicional, ou seja, considera-se a dependência de uma tarefa com a outra.

A Tabela 8.5-1 apresenta o resumo das considerações e ajustes nos HEP's nominais, indicando a alternativa de desligamento com período de tempo estipulado (evento C para alta dependência) e a situação atual (evento C' para dependência total), cuja HEP corresponde a 1, logicamente c sendo igual a zero, na árvore. Para os itens C e C' , que incluem um certo grau de dependência, utilizam-se as margens inferior (M Inferior) e superior (M Superior) de incerteza, equivalentes aos fatores de erro.

Tabela 8.5-1 Ajustes nos HEP's

AJUSTES NAS PROBABILIDADES DE ERROS HUMANOS - HEP's					
EVENTO	HEP	AJUSTE NO ESTRESSE	OUTROS PSF"s	FATOR DE ERRO	HEPB
A	10^{-4}	–	–	10	10^{-4}
B	3×10^{-3}	2	2 x 2		$2{,}4 \times 10^{-2}$
				Margem Superior / Margem Inferior	HEPC *
C'	1		–	0,5 - 1	1 DT **
C	0,5	–	–	0,25 - 1	0,5 AD***

* HEP Condicional ** Dependência Total *** Alto Nível de Dependência

Na Figura 8.5-3 é apresentada a árvore THERP para o exemplo considerado, com período de tempo estipulado de 10 minutos para desligar o reator.

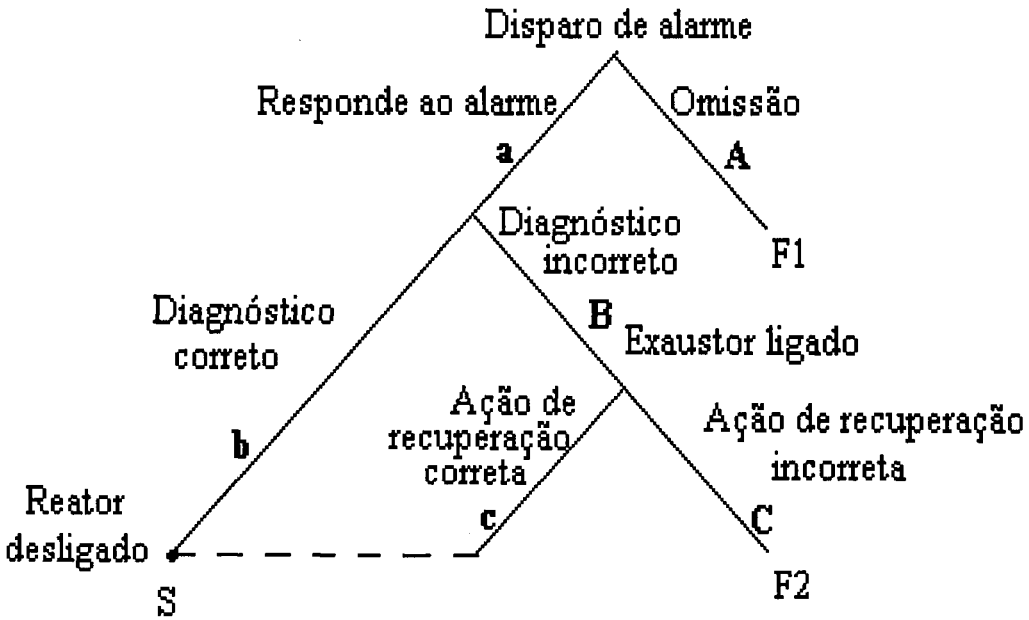


Figura 8.5-3 Árvore THERP para o exemplo

8.6.2 Modificações nas HEP's

Ajustes ou modificações foram feitos para PSF's considerados no problema. Não foram considerados todos os PSF's em razão da simplificação deste exemplo. Considerou-se as tarefas "A " e "B " como eventos independentes, ou seja, conforme a referência [1], dependência zero.

Para o evento "A", nenhuma modificação foi feita, portanto continua o valor de 10^{-4}. Apenas convém lembrar que alarmes falsos freqüentes induzem o operador a não confiar neles, obviamente predispondo os mesmos a erros, que podem conduzí-los a

negligenciar a resposta imediata. Obviamente, se for considerada essa situação de alarmes defeituosos, o nível de dependência deverá ser modificado, já que a resposta do operador, considerada independente do componente elétrico-mecânico " alarme ", passaria a ter influência na ação do operador.

Para o evento "B", verificou-se que ítens não cobertos em procedimentos (as verificações realizadas) supõem um certo grau de improvisação. A não existência de um tempo especificado nos procedimentos também é um fator que influência negativamente o desempenho.

Para este ponto específico foi considerada uma alternativa à situação atual, ao se estipular um período de tempo de 10 minutos entre o disparo de alarmes e a ação efetiva de desligar o reator, para efeito de realização desta análise. Este tempo somente deverá ser considerado para efeito de exercício, visto que, para ser incorporado a algum procedimento, deve-se levar em conta as implicações decorrentes das condições impostas pelo processo de licenciamento [68, 69, 77].

Uma outra observação é relativa à periodicidade dos retreinamentos. A referência [1] considera que a prática não freqüente de respostas adequadas a situações potenciais de acidentes ou outras situações anormais prejudica a realização da tarefa, conforme discutido no item B.4, do Anexo B.

Para situações semelhantes, relativas aos eventos A e B, a referência [1] considera alguns fatores de ajuste que abrangem uma faixa ampla, com relação à utilização de PSF's. Para as duas situações explicitadas acima, considera-se um fator dois aplicável em cada uma, como um ajuste relativamente pequeno.

Existe uma certa subjetividade nos fatores adotados para as duas situações acima explicitadas nesta correção, porém foi adotada devido à escassez de dados específicos. A menor preocupação com a precisão nos dados, pelo menos nesta primeira avaliação, deve-se a que, neste trabalho, a ênfase é colocada no procedimento ao se fazer a análise, mesmo que com um certo comprometimento da precisão dos resultados, considerando também que o exemplo apresentado tem uma função mais didática. Uma análise de sensibilidade, para avaliar a importância relativa de duas situações possíveis, será realizada no final.

O nível de estresse considerado foi o de moderadamente alto, de acordo com a referência [1], devendo ser aplicado para a tarefa " B " um fator de correção 2 (adotar o valor dobrado da HEP nominal) à estimativa de erro humano adotada. Isto, porque se considera a tarefa sendo executada como passo a passo, não rotineira e desempenhada por pessoal qualificado, segundo recomendações da referência [1].

O evento "C", corresponde a uma ação de recuperação, existindo dependência com a falha na tarefa anterior, que foi a tentativa de fazer as verificações para o diagnóstico. Como o operador falhou na tentativa seguinte a probabilidade de erro nominal tende a aumentar, conforme a referência [1], tornando-se igual a 1 para dependência total.

Quando se trata de desempenho humano, quase todas as dependências têm relação com os processos mediativos. Neste caso, a mediação humana pode induzir a um novo erro. Pode-se dizer que o operador persistirá no processo de decisão que o levou a cometer o primeiro erro, ou seja, existe um fator de dependência associado a uma possível insistência em manter a opinião anterior. Não foi modificada a HEP com relação aos PSF's, considerados incluídos na ação de recuperação.

8.6.3 Árvore THERP para o caso exemplo

Numa árvore THERP, como a apresentada na Figura 8.5-3, os ramos de um nó resultam sempre em 1. Por exemplo, a + A = 1, e assim por diante. Logicamente, S + F1 + F2 = 1.

O caminho total de falha é: F = F1 + F2. Os caminhos de falha são: A e aBC . Os caminhos de sucesso são: ab e aBc.

a = 1 - A = 1 - 0,0001 = 0.9999

Substituindo pelos valores adotados, F1 = 0,0001 e F2 = 0,9999 x $2{,}4.10^{-2}$ x 0,5 tem-se:

F = 0,0001 + 0,0119988 = 0,0120988 ≈ $1{,}2.10^{-2}$

Para a situação atual, ou seja, período de tempo não especificado, os caminhos são os mesmos, substituindo-se C por C'. Calculando tem-se:

F = F1 + F2 = 0,0001 + 0,9999 x $2{,}4.10^{-2}$ x 1 ≈ $2{,}4.10^{-2}$

Ou seja, conforme a metodologia apresentada, o simples fato de se estipular um período de tempo para a realização do diagnóstico, após o qual deve-se desligar o reator, independentemente de considerações subjetivas dos operadores, diminui por um fator de dois a probabilidade de erro humano na resposta aos alarmes associados aos níveis de radioatividade.

Para realizar a análise da sensibilidade, consideram-se as incertezas, ou seja, aplica-se o fator de erro adequado à estimativa de HEP encontrada. No caso deste exemplo em particular, pela sua relativa simpliciade, não se considera necessário avaliar a propagação de erros. Para problemas mais complexos, pode-se utilizar essa ferramenta, de modo que o valor encontrado incorpore a influencia da propagação de erros nas probabilidades.

Considerando-se as incertezas, aplicam-se valores de fatores de erros para a HEP, de modo a estimar o pior caso e o melhor caso. Para a alternativa de tempo estipulado, são feitas as avaliações, para o melhor e pior caso da estimativa de probabilidade de erro humano.

Conforme a referência [1], para tarefas que consistem de desempenho de procedimentos passo a passo, mas realizados em circunstâncias não rotineiras, e considerando o nível de estresse moderadamente alto, para HEP's estimados maiores que 0,001 , o fator de erro aplicável é 5.

Para o pior caso, considerando o período de tempo 10 minutos, tem-se a HEP multiplicada pelo fator de erro, e para o melhor caso, dividindo, como se segue:

$F_{\text{Pior caso}}$ = FE x HEP = 5 x ($1{,}2 \times 10^{-2}$) = 5 x 0,012 = 0,06

$F_{\text{Melhor caso}}$ = FE X HEP = ($1{,}2 \times 10^{-2}$) / 5 = 0,012 / 5 = 0,0024

Analogamente, se considerado o período de tempo não estipulado tem-se:

$F_{\text{Pior caso}}$ = FE x HEP = 5 x ($2{,}4 \times 10^{-2}$) = 5 x 0,024 = 0,12

$F_{\text{Melhor caso}}$ = FE X HEP = ($2{,}4 \times 10^{-2}$) / 5 = 0,024 / 5 = 0,0048

Estes valores encontrados para o pior caso, em qualquer das duas situações de tempo consideradas, são altos, quando comparados com os valores de probabilidades de falhas de componentes do reator, abaixo de 10^{-4}.

Os valores encontrados para o melhor caso, nas duas situações de tempo consideradas, estão mais próximos de valores estimados para erros humanos em situações semelhantes [1], mesmo assim um pouco mais altos. Além disso, ainda se encontram num patamar mais alto, comparando com valores de probabilidades de falhas de componentes, como citado acima.

O valor a ser utilizado na APS, em algum ponto de uma determinada árvore de falhas, é a estimativa encontrada utilizando os HEP's básicos, ou seja, $2,4 \times 10^{-2}$ para a situação atual, ou $1,2 \times 10^{-2}$ se for considerado o período de tempo de 10 minutos para desligar o reator, conforme explicitado anteriormente. Caso algumas modificações sejam feitas seguindo as recomendações deste trabalho, poderá ser obtida uma melhora na confiabilidade do sistema, via diminuição das probabilidades de erros humanos.

8.6.4 Comentários e recomendações relativos ao exemplo

Com relação às estimativas de probabilidades de erros humanos, os resultados encontrados para o exemplo são considerados altos, principalmente quando comparados a probabilidades de componentes não humanos, e também levando em conta resultados de outras análises.

Comparando-se com o estudo realizado para o reator da Universidade do Novo México [79], verifica-se que as probabilidades básicas de erros humanos adotadas para o reator IPR-R1 foram menores que para as tarefas pré-acidentes utilizadas para aquele reator, ou seja, 0,03, com fator de erro 0,5. Entretanto, observa-se que os valores dos resultados das estimativas de probabilidades de erros humanos não estão muito distantes, 0,12 para um dos sistemas analizados para o reator do Novo México, 0,012 para o reator IPR-R1 (valor nominal estimado).

Nos dois trabalhos, uma atenção especial foi dada aos procedimentos e ao treinamento. Estes foram considerados os pontos fracos, e onde, com maior eficácia, se podem modificar alguns itens de maneira a melhorar a confiabilidade, diminuindo as HEP's. No decorrer do capítulo 8 foram discutidas algumas situações, não sendo necessário repetí-las.

No presente trabalho, os fatores influenciadores do desempenho considerados, principalmente os procedimentos e o estresse, contribuiram negativamente para o resultado das ações a serem desempenhadas.

Como visto anteriormente, as ações de verificação não estão cobertas em procedimentos. Assim, alguns passos omitidos na tarefa desempenhada pelos operadores para a realização do diagnóstico implicam em um certo grau de improviso, exigindo desempenho baseado em conhecimento. Apesar da excelente qualificação dos operadores, isto compromete um resultado adequado. Além disto, como não existem explicitamente nos procedimentos, os operadores não são adequadamente treinados na época da requalificação. Portanto, uma primeira sugestão é incluir estas ações em procedimentos, utilizando "check lists", que, se bem elaborados, podem também evitar a necessidade de desempenho baseado no conhecimento. Se o desempenho para a situação prevista for apenas baseado em regras, não haverá necessidade de um diagnóstico, e sim de uma

verificação. Por isto, também o nível de estresse diminui, contribuindo para a diminuição das HEP's.

Neste caso, um investimento simples e com custo muito baixo, compreendendo a revisão ou elaboração de procedimentos, resulta num aumento da confiabilidade dos operadores e, portanto, da segurança da operação.

Na análise da tarefa desempenhada pelos operadores para a realização do diagnóstico, ou seja, na atual resposta aos alarmes, foi verificada a não existência de procedimentos escritos cobrindo todos os passos de tarefas realizados. Além disso, não está estabelecido explicitamente um período de tempo para a realização do diagnóstico, após o qual o reator seria desligado para favorecer a segurança. Isto implica em um certo grau de subjetividade dos operadores para tomar a decisão de desligar o reator.

Como os procedimentos operacionais de atuação no reator para enfrentar condições de emergência não levam explicitamente em conta um período de tempo específico, a inclusão deste item representaria uma maior aproximação com a realidade, pois algum tempo é necessário para realizar a tarefa.

No procedimento de emergência, considera-se que a alta atividade seria causa para o desligamento do reator, sem entrar na questão do tempo. Este ponto poderia ser contornado estipulando-se uma condição ideal para desligamento do reator, ou seja, estipular um determinado tempo e também um determinado nível de atividade, independente de quaisquer considerações subjetivas dos operadores quanto a este ponto específico.

Um maior rigor aplicado aos procedimentos existentes que consideram a movimentação, no recinto, de amostras radioativas que podem disparar alarmes, deve também melhorar alguns fatores influenciadores do desempenho, por exemplo, tornando mais difícil ou eliminando uma das possíveis situações consideradas para o disparo dos alarmes, desta forma facilitando as verificações dos operadores.

A inclusão em procedimentos dos itens que compõem a realização do diagnóstico, a especificação de um período de tempo para a realização do mesmo, somado ao aumento da freqüencia dos treinamentos, favorece o desempenho dos operadores. Isto é devido a que:

- os procedimentos seriam reavaliados e revisados segundo a conformidade das ações dos operadores com os itens específicos, aumentando progressiva e continuamente a eficácia dos mesmos;

- a partir da análise da tarefa com os procedimentos já modificados, seriam identificadas situações em que fosse possível substituir desempenho baseado em conhecimento por desempenho baseado em regras, de modo a minimizar interpretações e, consequentemente, as HEP's (simulação);

- análogamente, seria possibilitada a substituição de desempenho baseado em regras para desempenho baseado na habilidade (posteriormente).

A análise indica também a possibilidade de melhoria em alguns pontos, dentre os quais um ajustamento no desempenho dos operadores quanto à preparação mais adequada para enfrentar condições de emergência. Isto é possível com um treinamento mais adequado, tentando fazer a previsão de eventos considerados não importantes ou desprezíveis, mas que podem ter um efeito negativo na medida em que exigem interpretações em condições não adequadas, ou seja, em situações de emergência.

Considerar um tempo para desligar o reator em circunstâncias imprevisíveis e incluir verificações do Supervisor para as ações desempenhadas pelo operador, por exemplo, podem contribuir para melhorar as ações de recuperação.

Com relação à interface homem-máquina, devido às circunstâncias atuais de reformas e modificações realizadas, em andamento, ou ainda a serem executadas, pode-se citar que, em função da nova mesa e da atual disposição na sala do reator, obteve-se uma possível melhora quanto ao tempo de deslocamento necessário parra executar as tarefas, tendo em vista as novas opções apresentadas na nova mesa, quanto à parte de instrumentação, mostradores e indicadores. Embora a mesa de operação não tenha sido analisada, sua existência comprova uma filosofia de ajustamento aos objetivos de segurança por parte do CDTN, que sempre devem ser procurados. Dentre algumas opções, por exemplo, sempre deve ser considerado possível e desejável o aumento da confiabilidade de sistemas.

O projeto da nova mesa de operação apresenta evidentes melhorias, quando comparada com o funcionamento da mesa original, principalmente quanto aos aspectos de segurança. A concepção da nova mesa adota uma arquitetura mais atual, por exemplo, a parte de controle de operação se encontra em um console de dimensões reduzidas, enquanto que os componentes, pelos menos os que o operador não utiliza freqüentemente, estão separados deste.

A utilização de componentes mais confiáveis e mais modernos na mesa do reator, e um leiaute que se aproxima das concepções mais modernas também favorece o aumento na confiabilidade, dentro de alguns princípios ergonômicos simplificadamente discutidos no item 2 deste documento, como por exemplo a disposição adequada de mostradores e detectores de radiação e a inclusão de uma central de alarmes no painel.

A nova mesa é mais complexa, talvez dificultando, de certa forma, a operação. Mesmo assim, pode-se considerá-la mais favorável às ações de recuperação, já que mais itens foram considerados em seu projeto, facilitando a compreensão de eventos. Se existem mais fatores de recuperação, como indicações de mais parâmetros e mais opções de atuação, as HEP's são reduzidas e, dessa forma, diminuem as incertezas quanto ao desempenho de tarefas específicas. A dificuldade adicional quanto ao maior número de instrumentos pode ser balanceada pela aplicação de procedimentos bem elaborados.

Ainda quanto ao treinamento, de um modo geral pode-se afirmar que, sendo baseado em procedimentos que cobrem o maior número de ítens possível, facilita inclusive a qualificação de operadores novatos, uma necessidade atual do CDTN, já que o corpo técnico da instituição tem sofrido uma redução substancial devido à não substituição de funcionários aposentados.

Finalmente, deve-se notar que os resultados obtidos em análises da confiabilidade humana eventualmente a serem realizadas para o IPR-R1 ou para qualquer outra instalação (nuclear ou não) poderão ser importantes na avaliação da confiabilidade de seus sistemas com a participação humana. Também com referência ao aumento do nível de segurança de operação do IPR-R1, poderão constituir uma importante indicação de novos pontos a serem considerados.

9. COMENTÁRIOS FINAIS E CONCLUSÕES

9.1 Comentários

Para a operação apropriada de uma usina nuclear, é importante fornecer um suporte adequado aos operadores, para que possam lidar com a complexidade das tarefas da operação, principalmente no que diz respeito ao diagnóstico e à tomada de decisões. Existem diferentes processos físicos envolvidos com grande quantidade de componentes, e a dinâmica da instalação pode às vezes se revelar imprevisível. O projeto dos sistemas de controle e apoio deve incluir controles, mostradores e instrumentos adequados, de tal forma que as necessidades específicas do operador possam ser satisfeitas em todas as situações operacionais previsíveis. Isto significa que as informações fornecidas devem ser estruturadas de acordo com as tarefas de tomada de decisão e também devem levar em conta as preferências específicas do operador, como por exemplo, o que a média deles acha que é mais apropriado. O sistema deve, também, ser projetado e montado de maneira consistente e lógica, de forma a evitar erros desnecessários dos operadores.

Para instalações nucleares e industriais em geral, os itens importantes a serem considerados nos controles incluem considerações antropométricas e a observação das limitações do ser humano quanto ao processamento de informações. Quanto às considerações referentes à complexidade, devem ser definidas a prioridade das tarefas, estabelecida a hierarquia entre procedimentos de ação, e feita uma estruturação adequada das informações. Para evitar erros e enganos, deve-se simplificar o que for possível, incluir funções de ajuda em "softwares", possibilitar avisos e indicações, e proporcionar outras facilidades de suporte.

A referência [80], bastante atual, aplicável a instalações complexas em geral, incluindo as nucleares, considera a dificuldade de lidar com os erros humanos e, em linhas gerais, recomenda atenção para os pontos que foram discutidos neste trabalho. Por exemplo, considera que, apesar da crescente aplicação de técnicas de automação em indústrias e outras organizações, é impossível eliminar completamente o envolvimento humano na operação e manutenção de sistemas. Nessa referência, chama-se a atenção para o fato de que a contribuição de erros humanos para a não confiabilidade pode ser devida a vários estágios do ciclo do produto. Além disso, cita que as falhas nos sistemas, decorrentes de erros humanos, podem ser devidas a uma não compreensão do funcionamento do equipamento, a falta de entendimento do processo, a ausência de cuidados, esquecimento, capacidade de avaliação limitada, ausência de procedimentos e instruções de correção, e inadequações físicas.

Um outro ponto muito importante, também discutido neste trabalho, é com relação à modelagem do desempenho humano. Apesar de ser um assunto que vem preocupando os analistas de confiabilidade humana há bastante tempo [81], continua sendo importante o investimento nesta área, como citado em [21]. Este ponto leva a um outro, também muito importante, que é a necessidade que existe de atuação conjunta entre dois especialistas genéricos, o especialista em APS e o especialista em ACH. A referência [82] sugere que a responsabilidade pela incorporação das interações humanas em uma

APS seja compartilhada entre estes dois especialistas. O papel do especialista em APS deve abranger algum conhecimento de modelagem do desempenho humano, incluindo aspectos de cognição, embora a ênfase deva estar centrada no sistema. Enquanto isto, espera-se que o analista de fatores humanos, ou especialista em ACH, compreenda os métodos básicos da APS e as operações envolvidas no controle de instalações complexas, como usinas nucleares, acrescentando conhecimento especializado a respeito do ser humano a ser considerado.

Confirmando bibliografias anteriores, a referência [80] cita que, embora não seja possível eliminar todas as fontes de erros, é possível minimizar alguns deles pela seleção adequada e treinamento de pessoal, padronização de procedimentos, simplificação de esquemas de controles, diagramas e painéis, e outras medidas de incentivo / motivação para a realização correta das tarefas necessárias. O projetista de sistemas deve assegurar-se de que a operação do equipamento seja tão simples quanto possível, com praticamente nenhuma probabilidade de erro. O operador deve se sentir confortável em seu trabalho e não deve estar sujeito a estresse desnecessário. A seguinte lista de verificações é fornecida em [80], podendo servir como base para avaliar as expectativas do projetista quanto ao desempenho do operador:

1) A posição do operador é confortável para o manuseio dos controles ?

2) Algum dos itens para operação requer esforço físico excessivo ?

3) A iluminação do local de trabalho e dos locais próximos é satisfatória ?

4) A temperatura da sala causa algum desconforto ao operador ?

5) Os níveis de ruídos e as vibrações estão dentro dos limites toleráveis ?

6) A disposição dos equipamentos elimina movimentações desnesserárias do operador?

7) O julgamento ou avaliação do operador pode ser reduzido ou minimizado, posteriormente, após reavaliações sucessivas de seu desempenho?

Observa-se no último item desta lista de verificações, uma preocupação com o desempenho humano, chamando a atenção para a redução do desempenho baseado no conhecimento. Ou seja, a interpretação e as avaliações que prejudicam o desempenho humano, muitas vezes no decorrer do tempo, podem ser substituidas por desempenho baseado em regras ou mesmo em habilidade, assim favorecendo a diminuição de possíveis probabilidades de erros humanos a serem consideradas. Isto porque o desempenho humano deve ser reavaliado e otimizado, em função de novos parâmetros ou situações incorporadas nos sistemas ou em procedimentos, ou quando verificada a sua importância no treinamento.

Com todos esses cuidados, os operadores humanos ainda continuam sujeitos a cometer erros. Um erro humano pode ou não causar uma falha. De acordo com a referência [80], portanto, as medidas quantitativas referentes à confiabilidade humana são necessárias, de forma a representar o mais corretamente possível a confiabilidade total do sistema. Esta argumentação também se preocupa com o aumento da confiabilidade do sistema a partir do aumento da confiabilidade do sistema-homem.

Em alguns pontos importantes, com relação a algum sistema em particular, a contribuição humana poderá ser determinante para a falha do mesmo. A existência de sistemas que facilitem o reconhecimento de erros por parte de operadores, e a possível

indicação de alternativas favorece a diminuição da probabilidade de erros. Em decorrência deste item, é que se torna importante o desenvolvimento de sistemas especialistas, conforme já discutido.

Atualmente, a aplicação de recursos de informática, e a melhoria de muitos componentes relacionados com a atuação humana, como mostradores, sistemas de controle, e outros, têm contribuído positivamente para a segurança. Note-se que as ações humanas, principalmente em condições de emergência, são favorecidas, quando se leva em conta a filosofia da defesa em profundidade e o gerenciamento de situações de emergência. Nestas condições de emergência, o operador, por meio de procedimentos específicos adequados a situações determinadas, tem um papel fundamental e a informática tem contribuído com programas que facilitam o diagnóstico e a tomada de decisões.

Como alertado no capítulo 2 e em [83], é necessário assegurar a validade dos programas de computador utilizados. Para instalações nucleares em geral, estes programas devem ser criteriosamente verificados, tanto considerando o licenciamento das instalações, quanto considerando também a possibilidade de erros, já que, sendo os mesmos elaborados por seres humanos, estão também sujeitos a erros humanos. De acordo com [84], os profissionais do campo da informática aceitam como inevitável erros de projeto em programas, que só se tornam confiáveis após uma série de revisões. Entretanto, isto não é aceitável em sistemas de segurança. Algumas medidas devem ser tomadas para minimizá-los, como evitar ambigüidades decorrentes da linguagem utilizada, utilizar especificações precisas das exigências que um sistema deve satisfazer, e fazer a revisão dos programas com especialistas da área em questão. Por exemplo, para sistemas de segurança, uma revisão deve ser realizada em programas específicos, por especialistas em segurança, e não por especialistas em computação, ou somente por especialistas em computação.

Ainda quanto à utilização de computadores, em [61] é apresentado um programa para a propagação de margens de incerteza por árvores THERP, não estando disponíveis, entretanto, códigos de computadores mais abrangentes que permitam um suporte para a realização de análises de confiabilidade humana.

9.2 Conclusões

O presente trabalho procurou apresentar a técnicos que utilizam a avaliação probabilística de segurança aspectos relativos à análise da confiabilidade humana, ou seja, porque, onde e como se devem avaliar os fatores humanos, em que nível se encontra o estado-da-arte, e quais as possibilidades de lidar com o erro humano de modo a diminuir seus efeitos em sistemas complexos e, portanto, aumentando a confiabilidade dos mesmos.

No decorrer do trabalho foram apresentadas algumas situações encontradas em instalações complexas, (usinas nucleares), dentre as quais algumas que podem comprometer o desempenho dos operadores. Estas últimas se devem, em boa parte, a projetos que não consideram alguns princípios ergonômicos importantes de maneira apropriada, resultando na necessidade de improvisar soluções, as quais nem sempre são adequadas, podendo muitas vezes piorar as condições de operação. Tais situações podem levar ao que se chama de *situação tendente ao erro*, ou seja, na qual o operador tem maior probabilidade de incorrer em erro, podendo, em certos casos, provocar acidentes, ou

causar problemas operacionais desnecessários. Por outro lado, algumas vezes o improviso de soluções por parte dos operadores pode facilitar as suas ações, sendo bastante eficazes no sentido de melhorar o seu desempenho e podendo contribuir para a melhoria de projetos posteriores.

Os exemplos de aplicação da Técnica de Previsão de Taxas de Erros Humanos - THERP, muito aplicada no campo da avaliação da confiabilidade humana, são apresentados para familiarizar os interessados em aprofundar os estudos nesta área, sendo fornecidos, adicionalmente, alguns dados em probabilidades de erros humanos e sobre *fatores influenciadores do desempenho.*

Uma aplicação simples, porém prática, considerando a situação específica de resposta dos operadores aos alarmes no reator Triga IPR-R1 foi desenvolvida, como contribuição à difusão da técnica. Nesse exemplo de aplicação, foi demonstrada a eficácia da técnica e pôde-se tirar conclusões quanto aos procedimentos de emergência do reator, que devem ser atualizados, com a inclusão de alguns ítens que podem contribuir para substituir o desempenho baseado no conhecimento dos operadores por desempenho baseado em regras, o que leva à diminuição de probabilidade de erros humanos na operação do reator. Verificou-se também que os treinamentos para enfrentar situações de emergência devem ser realizados mais freqüêntemente, de modo a permitir aos operadores uma atuação mais segura, nessas situações anormais.

Embora sendo o campo da APS já bastante conhecido no Brasil, por exemplo na COPPE, em FURNAS, na CNEN e em outras instituições, o presente trabalho, pela sua abrangência, parece ser pioneiro, quanto ao aspecto da confiabilidade humana. Representa, também, uma colaboração entre áreas afins, na medida em que existe um certo nível de interdisciplinaridade envolvendo o projeto de sistemas de controle e operação e a alguns aspectos do comportamento humano. Quanto a este último item, vale dizer que vem crescendo a aplicação de princípios da psicologia da cognição nessa interface com a engenharia de projetos de sistemas complexos, particularmente quanto a considerações de segurança de sistemas operação.

Este trabalho pode ser eventualmente utilizado como fonte bibliográfica suplementar em programas de requalificação de operadores de reatores nucleares, exigidos pelas normas da CNEN, nos aspectos que se referem à APS e à ACH, embora este não tenha sido o objetivo específico do trabalho.

Em função da importância do homem no nível de confiabilidade dos sistemas, o desenvolvimento desta área de estudos torna-se cada vez mais necessário, na medida em que existe uma crescente demanda para aplicação da Avaliação Probabilística de Segurança. Isto se deve ao fato de que esta técnica vem sendo utilizada para atender exigências cada vez mais rigorosas relativas à segurança de instalações industriais, exigidas por órgãos reguladores governamentais responsáveis pelo seu licenciamento e fiscalização, por empresas de seguros, entidades sindicais e profissionais, dentre outras.

Conforme discutido no trabalho, a criação de um banco de dados sobre erros humanos é de grande importância. É muito importante a criação de um sistema de coleta sistemático de informações, como por exemplo o registro de erros com relação às oportunidades para os erros, (soma de erros mais acertos). Isto deve ser feito de forma que seja possível uma avaliação confiável dos dados, o que inclui considerações a respeito das circunstâncias em que estes foram obtidos, por exemplo, quais as condições existentes na ocasião da ocorrência do erro (fatores influenciadores do desempenho). O banco de dados

deve conter informações sobre as incertezas dos dados, ou seja, distribuições, desvios, fatores de erro, etc.

No simulador de Furnas, em Angra dos Reis, que utiliza um modelo de sala de controle de usina nuclear do tipo PWR para o treinamento de operadores, são coletados dados e informações referentes ao desempenho humano em várias condições de operação. Outras indústrias também têm seus bancos de dados referentes à atuação humana no controle de sistemas complexos, como a indústria química, automobilística, e a aeronáutica. Entretanto, não existe ainda, ao que me consta, uma filosofia de coleta e análise mais abrangente para o desenvolvimento de um banco de dados que seja aplicável à industria nacional como um todo. Isto, talvez seja um ideal a ser perseguido, tendo em vista que é no campo da indústria que o erro humano tem provado ser, em decorrência da sua importância relativa quando comparado com a confiabilidade de componentes, causa de acidentes e prejuízos que nem sempre, necessariamente, deveriam acontecer.

Este trabalho traz também como contribuição a identificação das áreas da ACH onde devem ser investidos recursos de pesquisa e desenvolvimento para que os projetos sejam equilibrados em termos de falhas de compontes e erros humanos. Como exemplo podem ser citados a modelagem do desempenho humano, e os sistemas especialistas, programas de computador que favorecem a compreensão de fatores complexos na operação de instalações industriais.

Como sugestão para trabalhos futuros, sugere-se a modelagem do sistema-homem, principalmente visando modelos que incluam a psicologia cognitiva, dentro do campo da Ergonomia. Engenheiros com algum conhecimento de *Psicologia Cognitiva* seriam os profissionais que mais contribuição poderiam oferecer ao estudo desta matéria. Também como sugestão para outros trabalhos, pode-se pensar no desenvolvimento de códigos de computadores que pudessem aplicar as técnicas da Análise da Confiabilidade Humana.

Para finalizar, deve-se lembrar que o investimento em pesquisas no campo da automação e do desenvolvimento de sistemas especialistas é de grande importância para os estudiosos dos fatores humanos, aqui incluídos os profissionais que trabalham com a interface homem-máquina, principalmente na área da informática.

REFERÊNCIAS

[1] SWAIN, A. D., GUTTMAN, H. E. Handbook of human reliability analysis with emphasis in nuclear power plant applications. Albuquerque, N. M.: Sandia National Laboratories, 1983 (NUREG - CR - 1278).

[2] ROSEN, M. et al. Man as a safety factor in nuclear power plant operation; his abilities and limitations. In: INTERNATIONAL CONFERENCE ON MAN-MACHINE INTERFACE IN THE NUCLEAR INDUSTRY, Tokyo, 15 - 19 Feb. 1988, Proceedings... Vienna: IAEA, 1988. p. 751- 760.

[3] CARUSO, G. J. Importancia de los factores humanos en la seguridad de las isntalacionaes nucleares. Seguridad Radiologica, n. 1, p. 60 - 72, Sept 1990.

[4] INTERNATIONAL CONFERENCE ON RADIATION AND SOCIETY: COMPREHENDING RADIATION RISK, Paris, 24 - 28 Oct 1994. Proceedings... Vienna: IAEA, 1988. v. 1.

[5] PERKINS, T. Simulation technology in operator training. IAEA Bulletin, v. 27, n. 3, p. 18 - 24, Autumn 1985.

[6] INTERNATIONAL ATOMIC ENERGY AGENCY. The safety of nuclear instalations, safety fundamentals. Vienna: 1993. (Safety Series n. 110).

[7] HAGEN, E. W. ed. Technical Note: Potential human factors deficiencies in the design of local control stations and operator interfaces in nuclear power plants. Nuclear Safety , v. 26, n. 3, p. 313 - 317, May / June, 1985.

[8] COMPUTADOR sob suspeita. VEJA, São Paulo, p. 51, 23 Maio 1990.

[9] O AVIÃO intelectual. ISTOÉ SENHOR, São Paulo, p. 27, 29 Jan. 1992.

[10]BALANCING AUTOMATION AND HUMAN ACTION IN NUCLEAR POWER PLANTS, Munich, 9 - 13 July 1990. Proceedings ... Vienna: IAEA, 1991.

[11]CABRAL, A., NICK, E. Dicionário técnico de psicologia. São Paulo: Cultrix, 1983.

[12]SABUNDIAN, G. Curso de treinamento interregional sobre a segurança na operação de plantas nucleares de potência: prevenção e gerenciamento de acidentes. São Paulo: IPEN, 1991. (Relatório de viagem)

[13]NUCLEAR REGULATORY COMMISSION (Estados Unidos). Guidelines for control room design reviews. Washington, D. C. : 1981 (NUREG -0700)

[14]CANAZIO, P. P. L. M. ; GONÇALVES JR., J. C. G. Utilização de controladores lógicos programáveis em funções de segurança de reatores nuleares. In: 5 CONGRESSO GERAL DE ENERGIA NUCLEAR, Rio de Janeiro, 28 ago. - 2 set. 1995. Anais ... Rio de Janeiro: ABEN, 1995. p. 245 - 252.

[15]SWAIN, A. D. Human factors/man-machine interface; human reliability. In: IAEA TRAINING COURSE IN PROBABILISTIC SAFETY ASSESSMENT FOR NUCLEAR POWER PLANT OPERATION. Argonne, 1988. Lecture ... Argonne: IAEA, 1988 (Lecture 38.3.1).

[16]SEMINARA, J. L. et al. Human factors in the nuclear control room. Nuclear Safety v. 18, n.6, p. 774 - 790, Nov - Dec 1977.

[17]HAYAKAWA, H. et al. Concepts of integrated information and control systems for future nuclear power plants. In: INTERNATIONAL CONFERENCE ON MAN-MACHINE INTERFACE IN THE NUCLEAR INDUSTRY, Tokyo, 15 - 19 Feb. 1988. Proceedings... Vienna: IAEA, 1988. p. 295 - 304.

[18]AISAKA, K. Current status of and future prospects for the man-machine interface in Japan. In: INTERNATIONAL CONFERENCE ON MAN-MACHINE INTERFACE IN THE NUCLEAR INDUSTRY, Tokio, 15 - 19 Feb. 1988, Proceedings... Vienna: IAEA, 1988. p. 21 -28.

[19]TSUKUDA, H. ; MIYAIOKA, S. Studies on human factors in nuclear power plants. In: INTERNATIONAL CONFERENCE ON MAN-MACHINE INTERFACE IN THE NUCLEAR INDUSTRY, Tokyo, 15 - 19 Feb. 1988. Proceedings... Vienna: IAEA, 1988. p. 41 - 50.

[20]PUJOL, J. C. F. Aplicação de redes neuronais no processamento digital de imagens. Belo Horizonte: 1994: Disssertação (Mestrado) - Departamento de Ciência da Computação - Instituto de Ciências Exatas da Universidade Federal de Minas Gerais, 1994.

[21]BÁLINT, L. A structural aproach to constructing perspective efficient and reliable human-computer interfaces. In: INTERNATIONAL ATOMIC ENERGY AGENCY. User requirements for decision support systems used for nuclear power plant accident prevention and mitigation. Vienna, 1988. (TECDOC - 529 p. 37 - 62).

[22]EYSENK, M. W. ; KEANE, M. T. Psicologia cognitiva - um manual introdutório. Porto Alegre, Editora Artes Médicas, 1994.

[23]DIAS, R. , GRAMISCELLI, M. M. Prática de ensino e aprendizagem de língua estrangeira. Belo Horizonte: Editora da UFMG, 1987.

[24]INTERNATIONAL ATOMIC ENERGY AGENCY Probabilistic safety assessment A report by the International Nuclear Vienna: 1992. (Safety Series n. 75 - INSAG-6).

[25]LERBET, G. Piaget. Paris, Éditions Universitaires, 1970.

[26]PINTO, J. A. Uma metodologia de desenvolvimento de interfaces homem-máquina e sua aplicação no sistema integrado de supervisão. Belo Horizonte: 1993.: Dissertação (Mestrado) - Departamento de Ciência da Computação - Instituto de Ciências Exatas da Universidade Federal de Minas Gerais, 1993.

[27]RASMUSSEN, J. Skills, rules and knowledge; signal, signs, and symbols, and other distinctions in human performance models. IEEE transactions on systems, man, and cybernetics, v. SMC - 13, n. 3, May - June, p. 257 - 266, 1983.

[28]NORMAN, D. A. Categorization of action slips. Psychological Review, v. 88, n. 1, p. 1 - 15, 1981.

[29]INTERNATIONAL ATOMIC ENERGY AGENCY Models and data requirements for human reliability analysis, Vienna: 1989. (TECDOC - 499).

[30]INTERNATIONAL ATOMIC ENERGY AGENCY. Procedure for conducting human reliability analysis in probabilistic safety assessment Vienna. [1993 ?].

[31]REASON, J. Modeling the basic error tendencies of human operators. Reliability Engineering and System Safety, v. 22, 137-153, 1988.

[32]SHINOHARA, Y. Comments on the balance between automation and human actions. In: INTERNOTIONAL ATOMIC ENERGY AGENCY. International working group on nuclear power plant control and instrumentation: the role of automation human in nuclear power plants. 1992. p. 147 - 153.

[33]JASKE, R. T. FEMA's computerized aids for accident assessment. In: INTERNATIONAL SYMPOSIUM ON EMERGENCY PLANNING FOR NUCLEAR FACILITIES, Rome, 4 - 8 Nov. 1985. Proceedings...Vienna: IAEA, 1986. p. 181 - 203.

[34]FURNAS CENTRAIS ELÉTRICAS. As usinas termelétricas e a questão ambiental. Rio de Janeiro, 1993.

[35]NAITO, N. et al. An intellligent human-machine system based on an ecological interface design concept. Nuclear Engineering and Design, v. 154, p. 97 - 108, Mar, 1995

[36]HARMON, P., KING, D. Sistemas especialistas - a inteligência artificial chega ao mercado. Rio de Janeiro: Campus, 1988.

[37]MILLER, D. P. , SWAIN, A. D. Human error and reliability. In: SALVENDY, G. Handbook of human factors. Albuquerque, N. M. : Sandia National Laboratories, 1987.

[38]TIFFIN, J., McCORMIC, E. J. Psicologia Industrial, São Paulo: EPU, 1975. v. 2.

[39]ALVARENGA, M. A. B.; CAULLIRAUX, H. B. Fatores humanos - conscientização para incremento da segurança nuclear. In: CONGRESSO GERAL DE ENERGIA NUCLEAR 3 Rio de Janeiro, 22 - 27 Jan. 1990 Anais...Rio de Janeiro, ABEN, 1990. v. 2, p 21 - 30.

[40]SHERIDAN, T. B. Human error in nuclear plants. Technology Review, v. 82, n. 4, p. 22 - 33, Feb. 1980.

[41]SWAIN, A. D. A method for performing a human factors reliability analysis (Monograph SCR-685) Albuquerque, N. M. Sandia National Laboratories, 1963.

[42]SWAIN, A. D. Design of industrial jobs a worker can and will do. Human Factors, v. 15, n. 2, p 129 - 136, 1973.

[43]JURAN, J. M., The quality control circle phenomenon, Industrial Quality Control, v. 23, p. 329 - 336, 1967

[44]MOELLER, C. O lado humano da qualidade. São Paulo: Livraria Editora Pioneira, 1992.

[45]GRINNELL, J. R. Jr. Optimize the human system. Quality Progress, v. 27, n. 11, p. 63 - 67, Nov. 1994.

[46]SELVATICI, E. Considerações sobre acidentes severos para as usinas nucleares de Angra 2 e 3. In: SIMPÓSIO SOBRE ASPECTOS DE SEGURANÇA DE USINAS NUCLEARES NA AMÉRICA LATINA. Rio de Janeiro, 1991. Anais...Rio de Janeiro, Seção Latino-Americana da American Nuclear Society, p VI - 37 - VI - 57, 1991

[47]GERTMAN, D. I. Representing cognitive activities and errors in HRA trees. Advances in human reliability. Transactions of the American Nuclear Society, v. 65, p. 101 -102, Jun. 1992.

[48]SWAIN, A. D. Comparative Evaluation of methods for human reliability analysis. Köln: Gesellschaft für Reaktorsicherheit, 1989. (GRS - 71).

[49]FURNAS CENTRAIS ELÉTRICAS. Centro de treinamentos avançado com simulador. Rio de Janeiro, 1993.

[50]TOPMILLER, D. A. ECKEL, J. S. KOZINSKY, E. J. Human reliability data bank for nuclear power plant operations, v. 1 : a review of existing human reliability data banks. Albuquerque, N. M.: Sandia National Laboratories, 1982. (NUREG/CR - 2744).

[51]TOPMILLER, D. A. ECKEL, J. S. KOZINSKY, E. J. Human reliability data bank for nuclear power plant operations, v. 2 : a data bank conception and systems description, v. 2, Albuquerque, N. M.: Sandia National Laboratories, 1983. (NUREG/CR - 2744).

[52]BERNHARD, H. C. ET AL. Savannah river site human error data base development for nonreactor nuclear facilities. Albuquerque, Los Alamos Technical Associates, 1994.

[53]INTERNATIONAL ATOMIC ENERGY AGENCY. Manual on reliability data collection for research reactor PSAs Vienna. 1992. (TECDOC 636)

[54]NISHIWAKI, Y. Human Factors and fuzzy set theory for safety analysis, In : INTERNATIONAL ATOMIC ENERGY AGENCY SEMINAR ON INPLICATIONS OF PROBABILISTIC RISK ASSESSMENT, Blackpool, 18 - 22 Mar. 1985. : Proceedings ... Vienna: IAEA, 1987. p. 253 - 274

[55]APOSTOLAKIS, G. E. et al. Data specialization for plant specific risk studies. Nuclear Engineering and Design, v. 56, n. 2, p. 321 - 329, 1980.

[56]VASCONCELOS, V. Aplicação da metodologia da árvore de falhas na análise de risco em sistemas complexos. Belo Horizonte: 1984. Dissertação (Mestrado em Ciências e Técnicas Nucleares - Escola de Engenharia da Universidade Federal de Minas Gerais), 1984

[57]COMISSÃO NACIONAL DE ENERGIA NUCLEAR, Licenciamento de instalações nucleares, Rio de Janeiro: 1984. (CNEN-NE-1.04).

[58]NUCLEAR REGULATORY COMISSION (Estados Unidos). Reactor Safety Study; an assessment of accident risks in U. S. commercial nuclear power plants. Washington, D. C.:1975 (NUREG - 75/014; WASH - 1400).

[59]VESELY, W. E. In: IAEA TRAINING COURSE IN PROBABILISTIC SAFETY ASSESSMENT FOR NUCLEAR POWER PLANT OPERATION. Argonne, 1988. Lecture... : IAEA, 1988.

[60]FERREIRA, A. B. de H. Novo dicionário da língua portuguesa. Rio de Janeiro: Nova Fronteira, 1986.

[61]NUCLEAR REGULATORY COMISSION (Estados Unidos) Accident sequence evaluation program human reliability analysis procedure Washington D. C. : 1987. (NUREG/CR-4772).

[62]MORE, R. F., FISHER, J. R. Man-machine interface developments in CANDU PHWR control centres. In: INTERNATIONAL CONFERENCE ON MAN-MACHINE INTERFACE IN THE NUCLEAR INDUSTRY, Tokyo, 15 - 19 Feb. 1988. Proceedings... Vienna: IAEA, 1988. p. 567 - 577.

[63]HALL, R. E. Post event human decision errors: operator action tree / time reliability correlation. Upton, N.Y.: Brookhaven National Lab., 1982. (NUREG/CR 3010).

[64]CAMPOS, M. M. Arredondamento de valores numéricos - algarismos significativos. Belo Horizonte: Centro de Desenvolvimento da Tecnologia Nuclear, 1992. (Nota Informativa SA - 01/92).

[65]NUCLEBRAS. Relatório de Análise de Segurança do Reator TRIGA IPR - R1. Belo Horizonte: 1982.

[66]NUCLEBRAS. Manual de operação do Reator IPR - R1. Belo Horizonte: 1982.

[67]NUCLEBRAS. Curso de treinamento de operadores em reatores de pesquisa. 4. edição. Belo Horizonte: 1980.

[68]INTERNATIONAL ATOMIC ENERGY AGENCY Probabilistic Safety Assessment for research reactors, Vienna: 1986. (TECDOC 400).

[69]INTERNATIONAL ATOMIC ENERGY AGENCY Application of probabilistic safety assessment in research reactors, Vienna, 1989, (IAEA TECDOC-517).

[70]FERNANDES, M. P. Comparação entre a nova instrumentação proposta para o reator IPR-R1 e a original. Belo Horizonte: Centro de Desenvolvimento da Tecnologia Nuclear, 1992. (Nota Técnica AT-003/92).

[71]INTERNATIONAL ATOMIC ENERGY AGENCY. Safety in the utilization and modification of research reactors. Vienna, 1994. (Safety Series n. 35 G2).

[72]KLETZ, T. A. Eliminating potential process hazards. Chemical Engineering, v. 92, n. 7, p. 48 - 68, 1 Apr. 1985.

[73]COMISSÃO NACIONAL DE ENERGIA NUCLEAR. Licenciamento de operadores de reatores nucleares. Rio de Janeiro: 1979. (CNEN-NE-1.01).

[74]COMISSÃO NACIONAL DE ENERGIA NUCLEAR. Requisitos de saúde para operadores de reatores nucleares. Rio de Janeiro: 1980. (CNEN-NE-1.06).

[75]NUCLEBRAS. Plano de emergência do reator IPR-R1. Belo Horizonte: 1985. (Procedimento - PD-007)

[76]COMISSÃO NACIONAL DE ENERGIA NUCLEAR. Ocorrência de evento nào usual com o reator IPR-R1. Belo Horizonte: 1989. (Procedimento - PD-014).

[77]INTERNATIONAL ATOMIC ENERGY AGENCY. Safety assessment of research reactor and preparation of the safety analysis report Vienna: 1994. (Safety Series - 35-G1).

[78]BASTL, W.; Märkl, H. The key role of advanced man-machine systems for future nuclear power plants. In: INTERNATIONAL CONFERENCE ON MAN-MACHINE INTERFACE IN THE NUCLEAR INDUSTRY, Tokyo, 15 - 19 Feb. 1988. Proceedings... Vienna: IAEA, 1988. p. 645 - 661.

[79]BRUMBURG, G. P. , HEGER, A. S. A human reliability analysis of the University of New México's AGN-201M nuclear research reactor. Lawrence: Lawrence Livermore National Laboratory, 1992.

[80]AGGARWAT, K. K., Reliability Engineering: Topics in Safety, reliability and quality Dordrecht: Kluwer Academic, 1993.

[81]SIEGEL, A. I. , WOLF, J. J. Man-machine simulation models - psicosocial and performance interaction. New York: John Wiley & Sons, 1969.

[82]INTERNATIONAL ATOMIC ENERGY AGENCY. Proceedures for conducting probabilist safety assessment of nuclear power plants (level 1) Vienna, 1992. (Safety Series n 50-P-4).

[83]INTERNATIONAL ATOMIC ENERGY AGENCY. Software important to safety in nuclear power plants Vienna, 1994. (Technical Report Series n 367).

[84]PARNAS, D. L. , ASMIS, G. J. K. , MADEY, J. Assessment of safety-critical software in nuclear power plants. Nuclear Safety, v. 32, n. 2, p. 189 - 198, April-June 1991.

[85]OLIVEIRA, L. F. S. A quantificação da segurança nuclear. Jornal do Brasil, Rio de Janeiro, 20 fev. 1983. Caderno de Ciência e Tecnologia.

[86]CAMARGO, C. T. M. , GIBELLI, S. M. O. O papel da análise probabilística de segurança no licenciamento de Angra-I. In: LAS/ANS SYMPOSIUM ON NUCLEAR ENERGY AND ENVIRONMENT, Rio de Janeiro, 27 Jun - 1 Jul 1993. Proceedings... Rio de Janeiro: American Nuclear Society, 1993. p. II-15 - II-22.

[87]DURR, M. et al. Twenty years of providing information on nuclear power - The experience of EDF. In: INTERNATIONAL CONFERENCE ON THE NUCLEAR POWER OPTION, Vienna, 5 - 8 Sep 1994.. Proceedings... Vienna: IAEA, 1995 p 379-392.

[88]BISCONTI, A. S. Public support for nuclear energy in the 21st century. In: INTERNATIONAL CONFERENCE ON THE NUCLEAR POWER OPTION. 5 - 8 Set 1994, Proceedings ...Vienna: IAEA, 1995. p 367-371.

[89]SOUZA, J. .A. .M. A energia nuclear e o meio ambiente. In: CONGRESSO GERAL DE ENERGIA NUCLEAR 5. Rio de Janeiro, 28 Ago. - 2 Set. 1994. Anais... Rio de Janeiro, ABEN, 1994. v. 2, p 709 - 715.

[90]ROSA, L. P. Aspectos técnicos e institucionais da segurança dos reatores nucleares no Brasil. In: COLÓQUIO INTERNACIONAL SOBRE SEGURANÇA DE REATORES À ÁGUA PRESSURIZADA, Rio de Janeiro, 11 - 12 Ago 1986. Anais ...Rio de Janeiro. Associação Brasileira de Ciências, 1986. p. 391 - 201.

[91]BIRKHOFER, A., JAHNS, A. Severe Accidents: analysis, strategies and accident management in the Federal Republic of Germany. In: INTERNATIONAL SYMPOSIUM ON SEVERE ACCIDENTS IN NUCLEAR POWER PLANTS. 1988, Sorrento. Proceedings... Vienna: IAEA, 1988. p. 13 - 25.

[92]DE LA CRUZ, F. Dias. Conceptos nuevos asociados a los planes de emergencia nuclear; analisis en cuarto nivel. Revista de la Sociedad Nuclear Espanhola, v.3, n. 74, p. 26 - 29, abr. 1989.

[93]IAEA BULLETIN. Nuclear power: the new generation. Vienna: IAEA, v. 31, n. 3, 1989.

[94]CESTARI, D. M. Uma contribuição ao estudo do controle de catástrofes no Brasil, sob o prisma das representações sociais. In: 5 CONGRESSO GERAL DE ENERGIA NUCLEAR Rio de Janeiro, 28 ago. - 2 set. 1995. Anais ... Rio de Janeiro: ABEN, 1995, p. 737 - 741.

[95]INTERNATIONAL ATOMIC ENERGY AGENCY. Advances in reliability analysis and probabilistic safety assessment for nuclear power reactors. Vienna: 1994. (TECDOC-737).

[96]GESELLSCHAFT FUR REACTORS SICHERHEIST MBH. German risk study nuclear power plants phase b; a sumary. Köln: 1990. (GRS - 74).

[97]MARTINEZ, A. S., SCHIRRU, R., THOMÉ, Z. D. Improving safety parameter display systems for normal operation. In: INTERNATIONAL CONFERENCE ON MAN-MACHINE INTERFACE IN THE NUCLEAR INDUSTRY, Tokyo, 15 - 19 Feb. 1988. Proceedings... Vienna: IAEA, 1988. p. 391 - 400

[98]KRUGMANN, U., ROTH-SEEFRID, H. Accident management for KWU/PWR nuclear power plants. In: INTERNATIONAL CONFERENCE ON MAN-MACHINE INTERFACE IN THE NUCLEAR INDUSTRY, Tokio. 15 - 19 Feb. 1988. Proceedings... Vienna: IAEA, 1988. p. 675 -683

[99]ALBRECHT, K. O gerente e o estresse - faça o estresse trabalhar por você. Rio de Janeiro: Zahar, 1988 .

[100]PARKER, S. P. Mc Graw-Hill dictionary of scientific and technical terms. 5. ed. New York: Mc Graw-Hill, 1994.

[101]ROSSI, A. M. Autocontrole: nova maneira de controlar o estresse. Rio de Janeiro: Editora Rosa dos Tempos, 1991.

APÊNDICE A

COMPREENDENDO O CONTEXTO DA SEGURANÇA EM USINAS NUCLEARES

A.1 Segurança de Usinas Nucleares e Licenciamento

O licenciamento de uma instalação nuclear é um processo no qual se avalia se o projeto, a construção, o comissionamento, a operação e o descomissionamento (desativação) da mesma podem ser realizados com segurança, não acarretando riscos indevidos para o público. Essa verificação é feita pelo órgão governamental competente, no Brasil, a Comissão Nacional de Energia Nuclear - CNEN, pelo exame do Relatório Final de Análise de Segurança [57]. Neste documento, que deve ser elaborado pela concessionária operadora da usina e submetido à CNEN, são apresentadas análises minuciosas do projeto da instalação. Sendo considerado satisfatório o Relatório Final de Análise de Segurança, é concedida a licença de operação. Este relatório permite que se verifique a segurança da usina nuclear, considerando acidentes hipotéticos e, a partir daí, prever algumas de suas conseqüências. Isto tem sido feito com base num método chamado de *determinístisco*, e tem sido empregado em todos os países produtores de energia elétrica de origem nuclear [85, 86].

No licenciamento, portanto, deve-se tentar prever ocorrências e pensar em como evitar essas ocorrências, pela aplicação de medidas corretivas, seja no projeto da instalação, seja nos sistemas de segurança desenvolvidos para a mesma. Assim, estudam-se os acidentes e as maneiras de evitá-los. Se esses acidentes não podem nem mesmo ser controlados, e neste caso já será uma condição de emergência, deve-se estudar o que fazer para mitigar as suas conseqüências [86].

Cabe notar que o licenciamento em instalações nucleares obedece a padrões bem mais rígidos que os exigidos por órgãos governamentais para a maioria das instalações industriais.

A.1.1 Método determinístico adotado para o licenciamento

O método determinístico de licenciamento de usinas nucleares baseia-se na fixação dos chamados *Acidentes Base de Projeto* ("Design Basis Accidents" - DBA) [85, 86]. Estes acidentes base de projeto consideram situações previsíveis de ocorrer em uma usina nuclear, em determinadas condições altamente desfavoráveis. Devem ser minuciosamente analisados pelos proprietários da mesma e os resultados obtidos devem constar do Relatório Final de Análise de Segurança.

Os Acidentes Base de Projeto são analisados a partir de modelos matemáticos do comportamento neutrônico e termo-hidráulico da usina para situações específicas. Esses modelos matemáticos são implementados em códigos de computador,

tais como o RELAP ("Reactor Excursion and Leak Analysis Programme"), ou o TRAC ("Transient Reactor Analysis Code").

A concessionária deve demonstrar que determinados parâmetros previamente estabelecidos, tais como a temperatura do revestimento do combustível, a pressão no interior do edifício da contenção e outros, não ultrapassam certos valores considerados seguros, enquadrando-se dentro de critérios fixados em normas. Para atingir este objetivo, todo projeto de reator nuclear incorpora uma série de sistemas de segurança, os quais devem satisfazer ainda a um outro critério determinístico, denominado *Critério de Falha Única*, segundo o qual todo componente ativo (bombas, motores, válvulas, sensores, etc.) relacionado com a segurança deve ser redundante. Com a aplicação destes critérios determinísticos, o nível de segurança da indústria nuclear de geração de energia elétrica atingiu altos padrões e se situa entre os melhores da indústria moderna [85].

Entretanto, apesar do bom nível de segurança alcançado, um forte movimento de oposição à utilização da energia nuclear se estabeleceu em todo mundo, principalmente nos Estados Unidos e Alemanha, a partir do começo da década de 1970. Mesmo considerando que esta tendência possa ser revertida, pela compreensão de que as outras fontes de energia são também causadoras de problemas, principalmente ecológicos e ambientais, um dos principais aspectos levantados pelos opositores da energia nuclear está relacionado com a segurança do público [4, 85]. Surgiram então, a partir de 1970, os primeiros questionamentos quanto à possibilidade de não funcionamento de qualquer dos sistemas de segurança da usina, e do risco decorrente desta possibilidade. Apareceram também questões relacionadas pela não inclusão de acidentes que considerassem a fusão do núcleo do reator. No processo determinístico de licenciamento, tais acidentes são considerados virtualmente impossíveis. Na realidade, embora bastante improváveis, eles são teoricamente possíveis. Dado este fato, um novo campo de discussão vem crescendo em importância, a *percepção do risco*.

A.1.2 Segurança nuclear, percepção e aceitação de riscos

Considera-se que um importante fator que favorece a opinião positiva do público em relação às instalações nucleares é o aumento da sua segurança. Entretanto, isto não é o suficiente, dadas as particularidades da conceituação de risco e dos fatores envolvidos na percepção e na aceitação do mesmo.

É inquestionável que a questão da aceitação pública é fundamental para o desenvolvimento da indústria nuclear. Isto se deve a que, sendo favorável a opinião do público em geral, a indústria nuclear é favorecida. A opinião do público é favorável quando a percepção do risco relacionado com a indústria nuclear não é um fator de impedimento da construção de usinas nucleares. Por isso a questão da percepção do risco vem crescendo em importância e gerando discussões e debates entre profissionais das ciências exatas e das ciências humanas, além de abranger leigos e instituições das mais diversas tendências. Nota-se em [4] que, freqüentemente, existe uma discordância em relação às dimensões dos riscos tecnológicos, acentuadamente quanto aos riscos decorrentes da indústria nuclear, por parte de especialistas e do público. Isto tem, em geral, provocado uma dificuldade de comunicação entre estes dois grupos interessados na segurança, os especialistas e o público leigo, e pode às vezes tornar-se impossível, devido a uma desconfiança mútua.

Em decorrência disso, torna-se interessante discutir alguns aspectos da questão, tendo em vista sua relação com o que é de interesse deste trabalho, o fator humano, mais especificamente a confiabilidade humana.

Primeiramente, é necessário esclarecer que a palavra "risco" tem vários significados comuns e é freqüentemente usada para propósitos específicos não cobertos por nenhum de seus significados. Entretanto, neste trabalho é usada uma definição mais objetiva, a ser tratada no item A.1.6 adiante.

Ao se tratar de avaliação de risco, obviamente deve-se atentar para a aceitabilidade do risco. Os riscos são usualmente avaliados para propósitos específicos, notadamente para melhorar a base de decisões. A questão de ser o risco aceitável ou não não tem resposta incondicional e se assemelha a questões que dependem de vários fatores, como por exemplo, perguntar se cinco Reais é muito, ou se a situação de um determinado paciente é muito grave [4]. O que é aceitável ou não aceitável não é o risco isoladamente, mas a situação de risco, ou a prática que causa o risco. Para responder à questão da aceitabilidade do risco, deve-se considerar não somente o risco, mas também o benefício da prática, assim como os riscos e os benefícios de situações ou práticas alternativas. Ou seja, ao julgar ou avaliar um determinado risco, uma pessoa olha também para o benefício relacionado. Por exemplo, a pessoa viaja de avião porque chega mais rápido, mas acredita que corre um risco maior do que se viajasse de carro, embora as estatísticas de acidentes absolutamente não confirmem isto. Esta pode ser uma das razões porque o risco percebido difere de avaliações mais objetivas dos riscos. Deve-se lembrar que qualquer avaliação de risco tem componentes subjetivos [4].

O risco, conforme [4], tem uma posição proeminente na vida social e nas discussões existentes quanto à qualidade de vida. Está relacionado aos fundamentos da existência para os indivíduos, organizações e sociedades, sendo percebido através das preocupações relativas à poluição do ambiente, produção de energia, escassez de recursos, e outros itens. Assim, o risco vem se tornando um item muito importante [4] nas discussões científicas e públicas. Vários acidentes industriais de larga escala ocorridos recentemente (Bhopal, Minamata, Chernobyl, etc), foram causas de grandes preocupações com respeito à segurança do público, quanto à comunicação com o público a respeito dos riscos, e quanto ao próprio gerenciamento dos riscos [4]. O risco também se constitui parte usual da vida de uma pessoa e esforços no sentido de redução dos mesmos representam uma tentativa de melhorar a qualidade de vida, como por exemplo a preocupação com o uso do cinto de segurança em veículos, para diminuir as conseqüências graves em caso de acidente.

De maneira geral, a percepção de risco é, no presente, um campo muito ativo de pesquisa [4]. As experiências humanas, reações e comportamentos são direcionados por percepções muito subjetivas da "realidade". As percepções de risco comuns, inclusive as percepções de riscos associados à radioatividade, são baseadas em experiência e critérios subjetivos e avaliações intuitivas. Obviamente, a abordagem técnica para o risco é centrado num conceito que envolve probabilidade e conseqüência, conforme item A.1.6.

O estudo das avaliações intuitivas de risco é importante para compreender as reações do público quanto à tecnologia e seu impacto no ambiente e na saúde. As pesquisas relacionadas com a percepção de risco são freqüentemente motivadas para auxiliar em questões políticas e nas tomadas de decisão, pelo exame de como as pessoas avaliam e julgam atividades perigosas e novas tecnologias. Existe uma grande

discrepância nas avaliações de como deve ser realizado o desenvolvimento de uma determinada sociedade [4], especificamente quanto à utilização de novas tecnologias, ou sua utilização em larga escala, em particular quanto ao uso de energia nuclear para produção de eletricidade.

É importante lembrar que uma grande mudança de atitude em relação à indústria nuclear começou com os acontecimentos de TMI, em 1979, sendo fortalecida mais ainda uma opinião contrária após abril de 1986, em decorrência do acidente de Chernobyl [4]. Estes dois eventos implicaram em um efeito negativo na percepção, por parte da população, dos riscos relacionados com atividades de geração de energia elétrica por usinas nucleares. De acordo com [4], os itens mais importantes relacionados com isto foram: o seu potencial catastrófico, com respeito à população em risco; o fato de não ser voluntária a exposição à radioatividade; e o pouco controle que os indivíduos tiveram sobre o evento e suas conseqüencias. A energia nuclear, além disso, é ainda considerada uma tecnologia nova e perigosa e o seu funcionamento não é familiar para as pessoas comuns. Também foi importante na avaliação negativa do público, o fato de que detalhes dos efeitos na saúde causados pela radiação serem desconhecidos pelas pessoas comuns e, em certa medida, até pela ciência.

Na França, assim como em muitos outros países, a ocorrência do acidente de Chernobyl resultou numa rápida perda de confiança na indústria nuclear, principalmente em usinas geradoras de eletricidade, por parte do público Em seguida, são apresentados alguns números mostrando isto, de acordo com [87]. Na França, resultados de pesquisa indicavam que, em dezembro de 1985, 62% das pessoas eram a favor da energia nuclear, e 35% eram contra. Em maio de 1986, imediatamente após a ocorrência em Chernobyl, a proporção mudou para 51% a favor e 47% contra. Em novembro daquele ano, a situação foi modificada para 46% a favor e 52% contra, tendo havido uma ligeira recuperação de maio de 1987 para 51% a favor e 46% contra. Isto na França, um país tradicionalmente conhecido por ter uma opinião pública mais favorável à energia nuclear do que outros países, como os Estados Unidos.

De acordo com [87], a atitude dos responsáveis pela política nuclear deve ser de abertura e transparência, ou seja, a informação ao público deve ser honesta, clara, realista; deve haver participação do público nas decisões referentes à indústria nuclear, o que leva a discussões também quanto ao aspecto de acidentes nucleares; uma "cultura nuclear" deve ser favorecida em escolas e utilizando meios de comunicação. Todos estes pontos devem levar a uma "boa reputação" da energia nuclear [87]. Isto é assim considerado porque tende a mudar a imagem comumente associada à energia nuclear, nascida com a bomba atômica. Esta imagem é percebida, através de meios de comunicação de massa, segundo [88], freqüentemente como uma metáfora do mal ou da destruição. É esta imagem negativa que cria a percepção exagerada do risco que muitos observadores vêem como influência principal na opinião pública. Nesta mesma referência, entretanto, se reconhece que a percepção de risco realmente afeta as atitudes do público. Apesar de fatores sociológicos e psicológicos que influenciam a opinião pública, a reação mais intensa à energia nuclear foi decorrente dos acontecimentos em TMI e Chernobyl. Simplesmente pelo fato de terem acontecido, na percepção do público a segurança das instalações nucleares não era exatamente a apregoada pelos responsáveis, como por eles divulgada. Como citado em [89], o problema não foi tratado adequadamente. Entretanto, em [88, 89] é observado que as atitudes da opinião pública com relação à energia nuclear são influenciadas também quando se relacionam com as necessidades e os benefícios da

energia elétrica. As atitudes positivas têm sido relacionadas com o enfoque acima citado, de maior discussão com o público. O acidente de Goiânia, em 1987, embora não se relacionasse com usinas nucleares, teve um efeito negativo sobre a opinião pública brasileira, em relação à questão nuclear.

Com a crescente preocupação com a segurança, inúmeras análises foram feitas após os acontecimentos em TMI e Chernobyl, de modo a saber das causas e de como poderiam ser evitadas, ou seja, porque aconteceram estes acidentes e como evita-los, no futuro. Os resultados das análises mostraram que a intervenção inadequada dos operadores, ao agirem em função de eventos no sistema, pioraram a situação e ocasionaram o aumento das proporções dos acidentes. O acidente de TMI, embora não tenha ocasionado danos de grande monta ao meio ambiente, resultou num maior acirramento das discussões e nas exigências por mais qualidade na segurança nuclear, introduzindo o binômio homem-máquina como fator preponderante na investigação e prevenção de acidentes.

Em [90], numa simplificação que serve aos propósitos deste documento, foi feito um paralelo entre os eventos de TMI e Chernobyl. Em TMI houve um acidente com perda de refrigeração do núcleo do reator, causado por um simples defeito de uma válvula do circuito secundário, agravado pela interrupção dos circuitos de água em paralelo, por esquecimento pela manutenção, que deixou as válvulas fechadas (erro humano). Não teria havido maior conseqüência caso o operador não tivesse agido como se estivesse fechada a válvula do pressurizador (que ficou aberta), desligando o sistema de refrigeração de emergência por engano, deixando o núcleo parcialmente descoberto de água, de modo que ocorreu o superaquecimento das varetas de combustíveis e sua conseqüente fusão (novamente erro humano).

Ou seja, o sistema de segurança funcionou, mas foi desativado por falha humana. Este cenário poderia ter sido previsto, numa avaliação probabilística de risco. Como a sua probabilidade é considerada muito pequena, não foi considerada nos critérios determinísticos. Simplesmente não se esperava que isto pudesse acontecer.

Em Chernobyl, o reator estava quase desligado, a 7% de potência normal, quando o operador cometeu uma dupla falha por adição local de reatividade, provocando uma excursão de reatividade global, elevando a potência para 50% da normal. Como em TMI, houve falha humana. Nas versões oficiais, portanto, o fator humano foi o crucial. Os acidentes poderiam ter sido evitados, se houvesse melhor preparação dos operadores [5].

No caso de Chernobyl, as conseqüências de grande monta provocaram mais ainda a indignação do público e, também, como conseqüência, forçaram a mobilização da comunidade nuclear, na exigência de que providências fossem tomadas. A partir de então, inúmeros congressos internacionais voltaram-se exclusivamente ao estudo da interface homem-máquina e fatores humanos, no sentido de identificar falhas e prevení-las. Provavelmente a opinião públlica não estivesse inteiramente convencida de que o homem fosse o maior responsável por acidentes, após Chernobyl. Entretanto, depois dos resultados das investigações mostrando este fato e do reconhecimento que a comunidade nuclear estava empenhada em resolver ou dimunuir os problemas relacionados com a participação humana em acidentes, houve uma pequena recuperação da confiança do público [5].

Uma conseqüência imediata das análises foi o aumento das exigências quanto à segurança, por parte de órgãos reguladores e fiscalizadores [5]. Ainda como conseqüência das análises realizadas, para aumentar a segurança nas usinas nucleares, foi

considerado necessário melhorar o desempenho humano. Assim, foi intensificado o esforço no sentido de conhecer mais sobre os fatores humanos, principalmente por órgãos internacionais, como a Agência Internacional de Energia Atômica - AIEA, bem como por órgãos governamentais e privados de vários países. A idéia é que, melhorando o desempenho humano, a segurança das usinas nucleares, também será melhorada. Isso deve ocasionar, espera-se, um efeito positivo na aceitação, pelo público, da energia nuclear. De certa forma, já há sinais disto, conforme os dados apresentados anteriormente, que mostram uma ligeira recuperação da confiança do público quanto à energia nuclear na França. Deve-se notar que este país é, reconhecidamente, um dos que mais investem na área de confiabilidade humana. O que ficou bastante claro é que, ao questionar a segurança e o risco das instalações nucleares, o público contribuiu para uma atitude mais positiva dos responsáveis pela energia nuclear quanto ao fator humano, que não era desconhecido, mas também não era adequadamente considerado. Em 1975 foi publicado o relatório WASH 1400, também conhecido como Relatório Rasmussen [58], no qual já se alertava para a importância dos erros humanos em instalações nucleares.

Programas relacionados com a segurança nuclear, implementados a partir de 1982, pela AIEA, têm como um dos seus objetivos o aumento do conhecimento a respeito do desempenho humano, através da aquisição e avaliação de dados relacionados com o desempenho humano. Apenas para citar alguns, conforme [39], existem desde 1983 o "Operational Safety Review Teams - OSART ", desde 1982 o "Incident Reporting System - IRS", desde 1985 o "Operational Safety Indicators Programme - OSIP", desde 1986 o "Assessment of Safety Significant Event Teams - ASSET".

Entretanto, o que realmente importa considerar é que falhas humanas poderiam ter sido previstas, caso uma APS tivesse sido desenvolvida, conforme recomendada em [58], suportada por uma ACH para as condições de operação, nas duas usinas, em TMI e Chernobyl. O que se tornou óbvio então é que os erros humanos deveriam ter sido tratados com maior profundidade. Houve uma aceleração, a partir de então, nos estudos referentes aos fatores humanos na operação de usinas nucleares.

É certo que a opinião pública deu sua contribuição para que se estudasse a fundo a participação do homem na segurança de usinas nucleares. Já que o homem é o maior responsável por acidentes, então será necessário melhorar seu desempenho, ou substituí-lo por sistemas automatizados, o que não é possível, pelo menos integralmente [35, 36]. Por outro lado, espera-se que a melhora dos fatores humanos favoreça a maior aceitação, por parte do público, da energia nuclear, já que, com tantos investimentos para conhecer e favorecer o desempenho do homem, certamente deve ser melhorada a segurança nas usinas nucleares.

No Brasil, o acidente de Goiânia contribuiu, de início, para uma atitude negativa da população com relação à tecnologia envolvendo radioatividade e, por associação, à questão da energia nuclear. Entretanto, os esforços imediatos da CNEN parecem ter contribuído para uma certa recuperação da confiança do público. Na verdade, o que se constatou foi um enorme desconhecimento do público quanto à tecnologia nuclear, o que contribuia para uma atitude de desconfiança e de medo. Conforme [4], as pessoas devem participar das questões que envolvem sua segurança. Não há, em Goiânia, nenhuma usina nuclear, mas a educação da população do país como um todo deve incluir o conhecimento de tecnologias, sua implementação e os riscos e benefícios decorrentes. Assim, como ocorre na França {4}, a tendência é que apareça um questionamento positivo sobre a questão da tecnologia e suas aplicações, no contexto da percepção de risco.

A.1.3 Acidentes Além da Base de Projeto, como critério para segurança

Uma usina nuclear é projetada e construída com base nos *Acidentes Bases de Projeto* tendo, portanto, seus sistemas de segurança adequados a estes. Entretanto, depois dos acidentes de Three Mile Island e Chernobyl, nos quais erros humanos tiveram um papel preponderante [4, 5], verificou-se que a fusão do núcleo do reator é possível, embora altamente improvável. Um novo fator, portanto, foi introduzido nas considerações técnicas correntes. Isto devido a que, apesar dos vários sistemas de segurança existentes, pode haver uma falha, ou um encadeamento de falhas, que terminem por ocasionar um acidente. Mesmo considerando a alta qualidade dos produtos e processos industriais envolvidos, obtidos pela aplicação de princípios da *Garantia da Qualidade* [85], defeitos, falhas e erros podem acontecer. E essas falhas podem envolver, simultaneamente, falhas de sistemas, materiais, processos, equipamentos de segurança, instrumentação e controle, especificações técnicas e erros humanos.

Quando um acidente evolui até um determinado ponto a partir do qual não pode mais ser controlado usando procedimentos usuais de operação, pode significar que aqueles critérios utilizados no projeto foram insuficientes. Neste caso, enquadram-se os *Acidentes Além da Bases de Projeto* ("Beyond Design Basis Accident") [86, 91]. Tais acidentes não são admitidos como critério técnico para o projeto de uma usina, porque o investimento em segurança inviabilizaria o custo. Entretanto, mesmo descartados os Acidentes Além da Base de Projeto, eles podem ser usados para o *PLanejamento de Emergência* [92] e são estudados suplementarmente, em outro tipo de análise: a Avaliação Probabilística de Segurança. Deve-se notar ainda que estes acidentes não são inteiramente considerados na especificação dos sistemas de segurança. Entretanto, sendo profundamente estudados pela APS, permitem a otimização destes últimos.

A.1.4 Acidentes Severos e condições de segurança numa usina nuclear

Os Acidentes Além da Base de Projeto englobam os chamados *Acidentes Severos*, sendo ambos confundidos, às vezes, porque neles existe a hipótese da ocorrência de degradação do núcleo do reator. Um acidente severo é aquele que excede a base de projeto o suficiente para causar falhas de estruturas, materiais ou sistemas, sem os quais o resfriamento do núcleo não pode ser apropriadamente garantido por meios normais. A gravidade de um Acidente Severo depende do grau de danos causados ao combustível e do grau de perda da integridade da contenção. Entretanto, diferentemente dos Acidentes Além da Base de Projeto, não ocorre a fusão total do núcleo do reator [91], pois considera-se que o núcleo ainda pode ser resfriado.

Os Acidentes Severos são caracterizados pela baixa probalidade de ocorrência, como também pela possível existência de grande número de vítimas. É uma classe de acidentes que vem merecendo mais estudo, porque considera que os sistemas de segurança existentes poderiam minimizar a possibilidade de ocorrência de situações potencialmente mais perigosas, como a fusão total do núcleo do reator.

Na Figura A.1-1 são apresentadas, esquematicamente, as condições de segurança numa usina nuclear [91], demarcando as linhas entre os acidentes considerados.

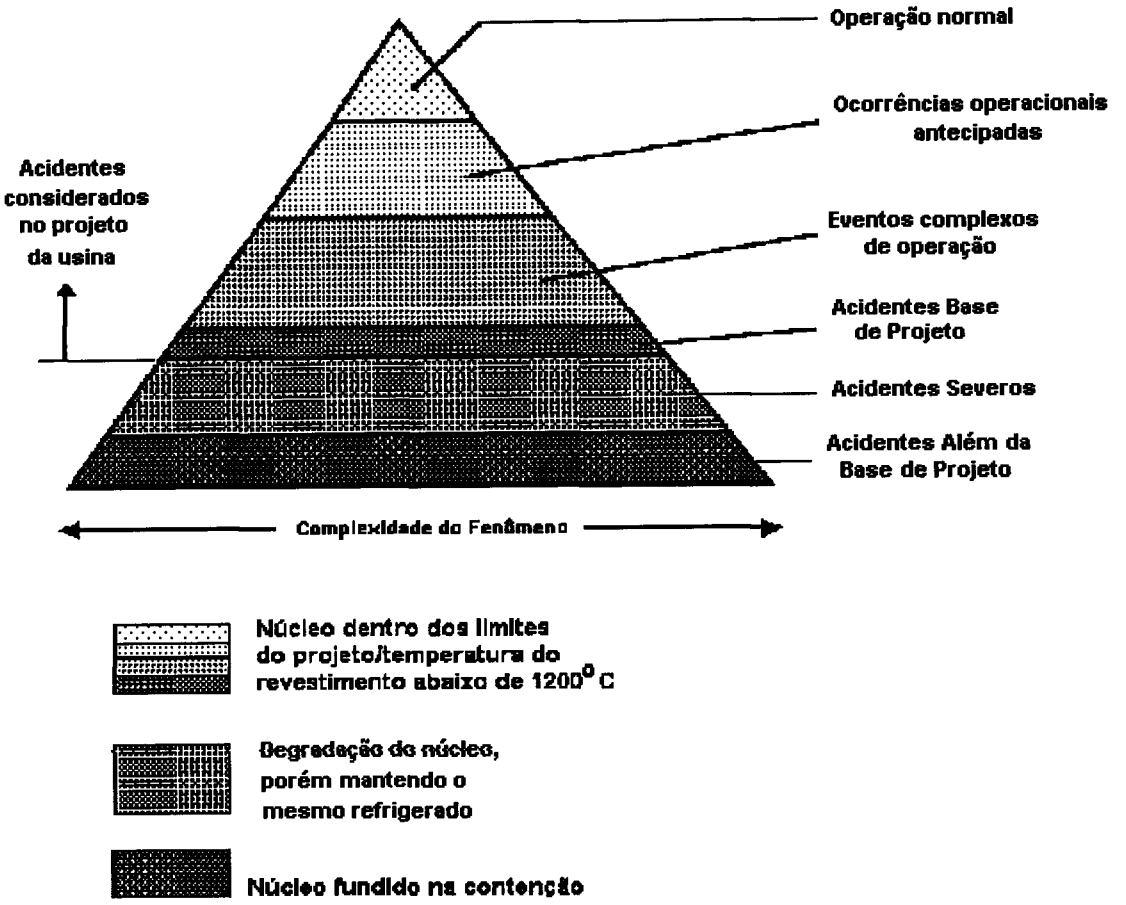


Figura A.1-1 - Condições de segurança numa usina nuclear, apresentando a linha divisória dos Acidentes Base de Projeto e os Acidentes Além da Base de Projeto, inclusive Acidentes Severos

A.1.5 Defesa em profundidade

Defesa em profundidade é um conjunto de critérios de proteção que se traduzem em medidas tomadas em níveis específicos de situação do reator. Com utilização da defesa em profundidade, espera-se evitar a fusão total do núcleo do reator, se de fato acontecer um acidente.

Como se percebe pela Figura A.1-2, a defesa em profundidade começa na garantia da qualidade, o que tende a aumentar a confiabilidade dos componentes, passa por melhoria geral nos conceitos de projeto, até chegar na melhor atuação possível dos sistemas e dispositivos de segurança. A ação humana também é altamente considerada, no desenvolvimento dos Procedimentos Operacionais de Emergência.

É o conceito de defesa em profundidade que permite uma atuação sistemática na gerência do acidente, diminuindo suas proporções. Observando-se a figura acima, percebe-se que até o nível 3, inclusive, as faixas referem-se às exigências de licenciamento (bases de projeto). O nível 4, refere-se aos Acidentes Além da Bases de Projeto. Neste caso, a idéia é reduzir os riscos residuais, ao lidar com falhas, acidentes e com os Acidentes Severos.

Na Figura A.1.2 é ilustrado o conceito de defesa em profundidade.

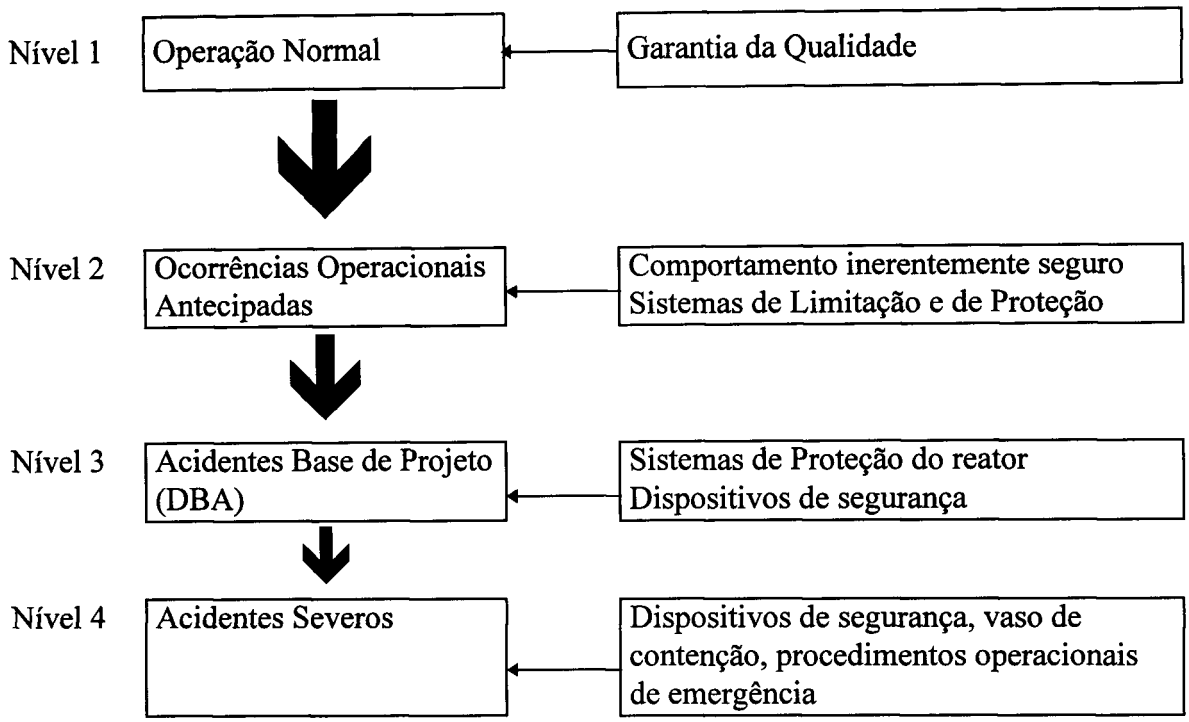


Figura A.1-2 - Conceito de defesa em profundidade na segurança de usinas nucleares [91]

A titulo de ilustração, na Figura A.1-3 é apresentada a tendência da filosofia de segurança dos reatores, a partir de 1960 [78].

<table>
<tr><th>Década de 1960</th><th>Década de 1970</th><th>Pós TMI</th><th>Pós Chernobil</th><th>Reatores de nova geração</th></tr>
<tr><td>Operação normal</td><td>Operação normal</td><td rowspan="3">Detecção precoce de falhas
Operação orientada para o evento</td><td>Operação normal</td><td rowspan="3">Adoção de novos conceitos, como por exemplo a adoção de projeto privilegiando a segurança passiva, reatores inovativos</td></tr>
<tr><td>-</td><td>Operação prejudicada</td><td>Operação prejudicada</td></tr>
<tr><td>Acidentes</td><td>Acidentes</td><td>Acidentes</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>Acidentes além das bases do projeto</td><td></td></tr>
<tr><td>Lidando com acidentes (envelope de acidentes)</td><td>Prevenção de acidentes Tentativa de evitar acidentes</td><td>Lidando com acidentes de modo orientado para o sintoma</td><td colspan="2">Gerenciamento de acidentes
Procedimentos operacionais de emergência</td></tr>
<tr><td></td><td colspan="4">Considerações sobre desempenho humano, abrangendo conceitos de projeto interface homem-máquina. Melhoramentos nas salas de controle, e nos procedimentos operacionais de emergência.
Tentativas de prevenir manipulação indevida do sistema</td></tr>
</table>

Figura A.1-3 - Tendências na filosofia de segurança dos reatores a partir de 1960

Nos reatores de nova geração, são usados critérios de projeto e de sistemas de segurança que diminuem a possibilidade da ocorrência de acidentes, e por isto são chamados também de *reatores inerentemente seguros*. Seus componentes aumentam a segurança intrínseca do reator, contribuindo positivamente para a melhoria do sistema em geral [78, 93].

A.1.6 Avaliação Probabilística de Segurança - APS

Por mais cuidadoso que seja o projeto de uma usina nuclear, quando se utiliza o método determinístico, sempre haverá uma probabilidade de falha decorrente da não postulação de alguns acidentes na avaliação de segurança. A APS é empregada, portanto, para suprir esta falha, ou seja, avaliar o risco residual não considerado.

A característica probabilística do conceito de risco é que deu origem ao nome anteriormente utilizado: Avaliação Probabilística de Risco ("Probabilistic Risk Assessment"), substituído posteriormente por Avaliação Probabilística de Segurança - APS (" Probabilistic Safety Assessment"). Esta mudança foi decorrente de uma melhor avaliação da terminologia empregada, sendo a última considerada mais adequada, quando relacionada a sistemas de segurança.

Na literatura especializada, o risco é conceituado como o produto da probabilidade de ocorrência pela conseqüência do evento. Para efeito de compreensão, a equação abaixo define brevemente o que seja risco, conforme as referências [4, 56]:

$$\text{Risco}\left[\frac{\text{Conseqüência}}{\text{Unidade de Tempo}}\right] = \text{Freqüência}\left[\frac{\text{Evento}}{\text{Unidade de Tempo}}\right] \times \text{Magnitude}\left[\frac{\text{Conseqüência}}{\text{Evento}}\right]$$

Em [4] se discute com maior profundidade o conceito de risco, conforme aplicado a diversas disciplinas. Para uso neste trabalho, será suficiente a definição acima. Uma observação deve ser feita, entretanto, quanto a referência [94], que discute o conceito de risco no contexto da psicologia social, abrangendo também a percepção de risco, conceito discutido no item A.1.2. De certa forma, o mais importante nesta referência é que se insere na perspectiva de discussão mais ampla da energia nuclear por parte de setores diferentes daqueles especializados no setor nuclear. A autora cita que o conceito de risco abrange ambigüidades decorrentes da definição do risco em várias disciplinas, não havendo uma definição única. Isto também é esclarecido em [4], embora nesse caso os autores tenham estabelecido critérios de utilização, como por exemplo definições para aplicações técnicas.

As usinas nucleares vêm sendo objeto de Avaliação Probabilística de Segurança [82, 85], feita em duas etapas: avaliação da probabilidade de ocorrência de todos os acidentes possíveis e imagináveis; e exame das conseqüências para o público de cada acidente avaliado (análise de conseqüências). O acoplamento do resultado destas duas etapas fornece o valor numérico correspondente ao risco global decorrente da operação da usina. A grande vantagem da APS é que todos os cenários de acidentes podem ser detalhados e explicitamente incluídos. Mas, a contribuição de cada tipo de acidente pode ser facilmente explicitada. Observe-se aqui que os cenários de acidentes admitem a participação do homem que, reconhecidamente, é a causa de muitos deles, por exemplo, a causa preponderante dos acidentes de TMI e Chernobyl..Os valores numéricos obtidos

numa APS fornecem uma visão bastante precisa dos fatores que mais contribuem para o risco, o que pode ser usado para indicar onde devem ser feitos investimentos no sentido de se melhorar a segurança da instalação. Ou seja, são indicados pontos fracos da instalação e, com base nisto, as devidas correções podem ser feitas.

Os sistemas de segurança das usinas nucleares são normalmente projetados para terem alta confiabilidade, porque são usados componentes de alta qualidade e que apresentam taxas de falha pequenas. Em decorrência desta alta confiabilidade dos sistemas de segurança, os eventos de interesse considerados na APS, como os Acidentes Severos, são considerados eventos raros (baixa probabilidade de ocorrência). Órgãos regulatórios de vários países já exigem a realização complementar de uma Avaliação Probabilística de Segurança de cada usina em fase de licenciamento, em paralelo com a avaliação determinística atualmente exigida [86].

Apesar da boa receptividade da APS, o rápido desenvolvimento e aumento do uso de sua metodologia nos anos recentes tem sido acompanhado por algum exagero de sua capacidade, conforme [24]. Ainda de acordo com esta referência, isto também é válido quanto à aplicabilidade dos seus resultados em análise de segurança, projeto de instalações e na regulamentação e controle de práticas operacionais. Dentre as precauções sugeridas por este documento, estão os cuidados com alguns fatores, como as incertezas, as falhas de modo comum e, principalmente, com os fatores humanos. Quanto aos fatores humanos especificamente, a maior dificuldade considerada em [24] é quanto a modelagem, embora haja nesta referência o reconhecimento de avanços nesta área.

Em [95] são apresentados diversos trabalhos sobre o avanço da Avaliação Probabilística de Segurança para usinas nucleares em escala mundial, notando-se uma crescente utilização da metodologia. Além disso, nota-se também uma grande preocupação com a análise de confiabilidade humana, mostrando sua importância com relação à confiabilidade de sistemas complexos.

A.1.7 Aumento da segurança em reatores de nova geração

Depois da ocorrência do acidente de TMI, em Harrisburg, nos Estados Unidos, o método de licenciamento baseado na avaliação quantitativa de risco (APS) para o público vem recebendo uma atenção cada vez maior, a nível internacional. Isto porque verificou-se que o acontecido, uma cadeia de eventos que terminaram por ocasionar o acidente, poderia ter sido prevista e, portanto, pela aplicação de algumas ações corretivas, poderia ter sido interrompida, evitando a catástrofe. Na ocasião do acidente, segundo as análises realizadas com base em metodologia probabilística, as falhas humanas foram muito significativas, comprometendo uma possível reversão do processo. Foi constatado que vários erros humanos poderiam ter sido evitados e se, ao contrário, tivesse ocorrido o desempenho mais adequado dos operadores, o acidente não teria sido tão sério, conforme esclarecido anteriormente. Especialistas em avaliação da confiabilidade humana constataram, por meio de análises realizadas a posteriori, que vários erros decorreram de uma prática ergonômica não adequada, muito aquém da desejável [1]. Além disso, se anteriormente tivesse sido realizada uma Avaliação Probabilística de Segurança, complementada por uma Análise da Confiabilidade Humana naquela usina nuclear, as ações humanas certamente teriam sido consideradas com mais atenção.

É de se notar que a ocorrência do acidente de Chernobyl, na Ucrânia, apenas reforçou as conclusões das análises realizadas: a não realização de uma APS, com o suporte de uma ACH, possibilitou uma perigosa degradação da segurança. Eventos que poderiam ter sido interrompidos não o foram, por falha de equipamentos e também, não menos importante, pela inadequação do desempenho humano que poderia reverter ou impedir o desenvolvimento do acidente [92].

Também foi verificado que, com a ocorrência destes dois acidentes envolvendo o núcleo dos reatores, a estimativa de probabilidade de uma vez em um milhão de anos foi comprometida, porque aconteceram dois em uma década (1979 e 1986) [92]. O que não era para acontecer "nunca" (probabilidade de 10^{-6}/ano) aconteceu duas vezes. Foi necessário, portanto, fazer uma reavaliação de todos os aspectos envolvidos. Como conseqüência das análises decorrentes, muitas modificações foram consideradas, sugeridas e introduzidas nos projetos conceituais das usinas nucleares, na concepção das salas de controle, nas especificações técnicas de funcionamento, nos manuais de operação, no treinamento do pessoal de operação e até nas bases dos planejamentos de emergência.

Em decorrência das análises realizadas, ocorreram reavaliações nas filosofias de projeto. Por exemplo, equipamentos anteriormente considerados bons, do ponto de vista da eficiência ou do rendimento, além de outros parâmetros positivos, começaram a ser vistos como inadequados do ponto de vista dos Acidentes Severos, ou dos Acidentes Além da Base de Projeto. Por outro lado, equipamentos considerados não muito bons são hoje considerado mais adequados, porque são equipamentos que diminuem, travam, impedem ou dificultam o desenvolvimento de acidentes, do ponto de vista fenomenológico e, portanto, são fatores de diminuição do risco [93].

As mudanças em vários itens levaram à concepção de reatores de nova geração [93], nos quais são incorporados conceitos avançados, principalmente através de:

- melhoria das características de segurança;
- redução do custo da energia gerada;
- redução do risco comercial do empreendimento.

A melhoria das características de segurança tem sido feita pela incorporação de sistemas adicionais de segurança passiva, que é realizada por meio de componentes com sistemas cujo funcionamento não implica em um acionamento externo. Dentro desta concepção, incluem-se a contenção dos reatores, estruturas de blindagem da radiação, queda de barras de controle induzidas por gravidade, além de outros. Dessa forma, nos reatores ditos inerentemente seguros, procura-se substituir todos os elementos ativos de segurança por elementos passivos, visando obter o máximo de segurança no seu funcionamento. Além disso, a inclusão de modificações no projeto, permitem um período de tolerância ("grace period") para o operador que, para estes reatores inerentemente seguros, seria praticamente infinito. O período de tolerância é o período após a constatação de um incidente ou acidente, durante o qual o funcionamento do reator continua seguro, mesmo sem a ação do operador [2].

Outras modificações estão sendo pesquisadas ou implementadas, pelos projetistas e construtores de centrais nucleares, pelos operadores e pelos órgãos fiscalizadores, além das anteriormente descritas, para aumentar a segurança do funcionamento dos reatores de nova geração.

Com isto, é possível voltar a pensar em valores de 10^{-6}/ano, ou até mesmo valores ainda menores, para a probabilidade de ocorrência de acidentes do porte dos ocorridos em Harrisburg e Chernobyl, como 10^{-7} ou 10^{-8} [46, 92].

A.2 A Segurança de uma Usina Nuclear e o Gerenciamento de Acidentes

É fato reconhecido que o desempenho do ser humano, em situação de estresse, fica comprometido, como ocorre em situações de emergência. Em certas circunstâncias, o desempenho se deteriora a ponto de impedir as ações, favorecendo os erros e as condições propícias a acidentes [1]. Isso ocorre em circunstâncias variadas, em sistemas diversos e se aplica com muito maior propriedade nos casos em que as conseqüências de acidentes envolvem o público, por exemplo nos casos de acidentes aéreos, acidentes de trânsito, acidentes industriais e em situações envolvendo fenômenos naturais rigorosos.

Também é o caso de acidentes em instalações nucleares, para os quais contribuem também os problemas relacionados com a radioatividade. Estes incluem os problemas reais, como a contaminação de pessoas, locais e equipamentos, e incluem também problemas fictícios, quando o risco é insignificante, mas o desconhecimento de muitas pessoas em relação à matéria potencializa e amplifica possíveis conseqüências. Por isto, algumas vezes os recursos acionados no combate à uma situação emergencial são exagerados, aumentando desnecessariamente os custos e também os riscos decorrentes [95].

A.2.1 Segurança ativa e passiva de uma usina nuclear

A segurança de uma usina nuclear incorpora medidas chamadas ativas e passivas. As *medidas passivas* de proteção do público são projetadas para confinar a radioatividade. São, basicamente, barreiras que resistem às forças originadas a partir de liberações acidentais de energia, impedindo ou reduzindo o lançamento de material radioativo para o exterior da usina.

A Figura A.2-1 apresenta esquematicamente as barreiras passivas [96] para um reator do tipo "Pressurized Water Reactor - PWR" da "SIEMENS/KWU".

A própria pastilha de material cerâmico, que constitui o combustível nuclear, e que tem ponto de fusão muito alto, é a primeira barreira. A segunda barreira é o tubo de revestimento do combustível, onde são colocadas as pastilhas, que é resistente ao calor, à corrosão e à radiação. A terceira barreira é a Fronteira do Sistema Primário do Reator, que inclui o vaso de pressão, o gerador de vapor, as bombas principais de circulação de refrigerante, e as tubulações. Este sistema é envolvido por uma contenção de concreto e blindagem de aço. O reator inteiro é enclausurado dentro de um edifício de contenção, que é a barreira final. As contenções dos reatores podem resistir a altas pressões, calor e uma grande variedade de perigos externos, como furacões, maremotos e terremotos, além de explosões e quedas de avião [57]. Todas estas barreiras impedem ou reduzem a probabilidade de liberação de material radioativo para o meio ambiente externo. Em última análise, é o rompimento desta contenção o mais complexo de todos os acidentes, e que implica maiores conseqüências (Acidente Além da Base de Projeto). Estas barreiras passivas são o nível mais elementar da defesa em profundidade, sendo os componentes básicos de alta confiabilidade de uma usina nuclear.

As *medidas ativas* de proteção da população incluem os vários sistemas de segurança intrínsecos da instalação, tais como o Sistema de Refrigeração de Emergência e

o Sistema de Bloqueio da Contenção. Atualmente, é também utilizado o Sistema Mostrador de Parâmetros de Segurança [97] ("Safety Parameter Display Systems" - SPDS) que apresenta um conjunto de parâmetros em uma tela de vídeo na sala de controle. Esses parâmetros incluem dados relacionados com: controle da reatividade; refrigeração do núcleo do reator; Remoção do Calor do Sistema Primário; integridade do Sistema de Refrigeração de Reator; controle da radioatividade e integridade da contenção.

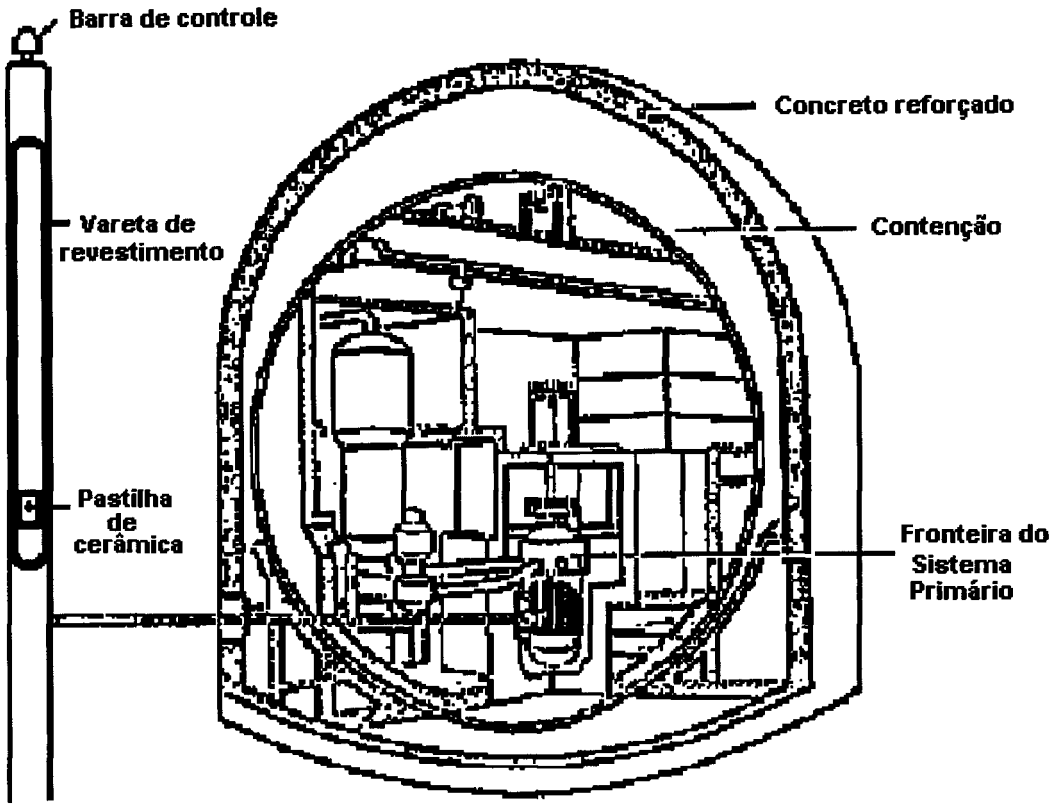


Figura A.2-1 - Barreiras passivas para confinamento dos produtos de fissão

Este sistema funciona de maneira diferenciada para a operação normal e para a operação em situação de emergência. Neste último caso, uma gama limitada de parâmetros é sistematicamente avaliada, de maneira a determinar a condição de cada função. Quando uma função crítica não é satisfeita, a linha de ação para recuperar a função (restabelecer os parâmetros satisfatórios) é indicada. A recuperação da função implica no retorno ao estado de segurança da usina, no qual todas as funções críticas são completamente satisfeitas. Este sistema favorece o operador no diagnóstico correto das condições do reator, já que, com uma gama limitada de informações sendo oferecida, a probabilidade de erro humano diminui [1].

Em decorrência da grande automação dos sistemas de proteção, limitação e controle de usinas nucleares, por exemplo, do tipo PWR da KWU, foi estipulado um tempo de 30 minutos de tolerância antes que seja tomada qualquer ação de emergência por parte do pessoal de operação na sala de controle da usina. Estes 30 minutos são mundialmente aceitos e considerados suficientes para que o pessoal de operação seja informado das condições do reator, com a ajuda do sistema SPDS [97].

A.2.2 Procedimentos operacionais de emergência e gerenciamento de acidentes

Se de fato o evento se configurar como um acidente potencial (ou real, conforme indicações), passa-se a um outro nível de procedimentos, os Procedimentos para Gerenciamento de Acidentes. Na Central, são utilizados os Procedimentos Operacionais de Emergência [46, 98] que, aplicados em situações particulares de condições de segurança, têm o objetivo:

- de ajudar os operadores no diagnóstico do evento específico causador do evento anormal (transiente) ou acidente, de forma a possibilidar a mitigação das conseqüências dessa situação e
- direcionar as ações dos operadores necessárias para mitigar as conseqüências dos eventos anormais e acidentais, quando estes eventos estiverem associados aos parâmetros de operação que excederam alguns limites estabelecidos.

Estes procedimentos são utilizados pelo pessoal da sala de controle da usina nuclear e, em geral, estão juntos a um manual de operação de emergência, normalmente separados do manual de operação normal.

Os procedimentos operacionais de emergência são procedimentos formais escritos, especialmente elaborados para apoiar o pessoal de operação, na resposta aos eventos anormais. Esses procedimentos são, de fato, o estabelecimento de uma seqüência de ações a serem obedecidas pelo operador, de forma a verificar a resposta apropriada dos sistemas de proteção do reator e para identificar, gerenciar e aliviar um acidente.

Os operadores de reator são treinados para seguir os procedimentos operacionais de emergência. Deve-se notar ainda que estes procedimentos são elaborados considerando-se a capacidade do ser humano, facilitando seu diálogo com o sistema computadorizado, e considera a experiência operacional para o tipo de usina considerada obtida anteriormente. Do ponto de vista do operador, estes procedimentos operacionais de emergência facilitam as ações a serem tomadas.

Os procedimentos operacionais de emergência estão subdivididos em duas classes: orientados para o evento (ou para o controle do evento), e orientado para o sintoma (ou para função) [98].

Os *procedimentos orientados para o evento* enfatizam eventos ou sistemas associados com uma condição anormal de operação, em lugar de lidar com os sintomas relacionados ou funções. Um evento, por exemplo, poderia ser um acidente de perda de refrigerante, em decorrência de, por exemplo, ruptura numa tubulação, LOCA ("Loss of coolant accident"). Os procedimentos orientados para o evento requerem dos operadores o diagnóstico do evento especifico que está causando o transiente ou acidente. Assim, este operador estará apto a agir de modo a sanar o problema ou mitigar as conseqüências do transiente ou acidente.

Os *procedimentos orientados para o sintoma* estão ligados aos sintomas resultantes de um evento anormal. Fornecem guias de como verificar a adequação de funções em níveis compatíveis com a segurança, quando essas se apresentam degradadas. Os procedimentos orientados para o sintoma ou função são escritos de tal maneira que o operador não tem que diagnosticar um evento para manter a instalação em condições de segurança, ou seja, o seu trabalho é facilitado. Neste caso, ele tem que verificar e manter os parâmetros críticos da operação, por exemplo temperatura ou pressão, podendo utilizar impressos, tais como gráficos ou mesmo textos narrativos.

Na referência [46] são apresentados dados baseados no estudo de risco alemão para a usina PWR (semelhante a Angra 2) Biblis B, que indicam que a aplicação correta de procedimentos operacionais de emergência diminuem em muito a probabilidade de ocorrência de acidentes. Por exemplo, o efeito da aplicação dos procedimentos de *alimentar e sangrar* ("feed and bleed") diminuem em aproximadamente 89% a probabilidade de fusão do núcleo do reator e tem o efeito de reduzir em aproximadamente para 10% a probabilidade de fusão do núcleo a baixa pressão, portanto mitigando o acidente. Somente 1% da freqüência total das seqüencias levando à ocorrência de um Acidente Severo continuaria até a fusão do núcleo a alta pressão. Como visto anteriormente, isso tem o efeito de diminuir a probabilidade de ocorrência de Acidentes Severos, para o patamar de 10^{-7} ou 10^{-8}.

As medidas de controle de um acidente numa usina nuclear começam na sua sala de controle. O pessoal de operação gerencia o acidente, tentando impedir o seu prosseguimento, diminuindo possíveis conseqüências. A gerência do acidente é possível com um certo grau de confiabilidade, com a pronta refrigeração do núcleo do reator. Se continua sendo possível o resfriamento do núcleo, devem-se manter as medidas adotadas, como por exemplo, alimentar e sangrar. Se não for possível, outras medidas deverão ser tomadas:

- reter os produtos de fissão dentro de estrutura da contenção;
- retardar a falha da contenção;
- reduzir e controlar os produtos de fissão liberados.

Porém, se a degradação do núcleo continuar, a previsão dos fenômenos relevantes torna-se incerta. A partir de determinado ponto, a seqüência dos eventos não pode ser pré-calculada, e torna-se imperativa a tomada de decisão com relação às ações de proteção da população circunvizinha à usina nuclear, ou seja, ativar o Plano de Emergência externo. Este consiste, basicamente, de medidas de proteção da população, considerando a irreversibilidade da situacão na usina, na qual ocorre um acidente que não pode mais ser controlado, ou que pode se tornar de difícil controle num curto período de tempo após o acidente.

A Figura A.2-2 apresenta um resumo de três estágios no gerenciamento de acidentes no nucleo de um reator nuclear, apenas para ilustração.

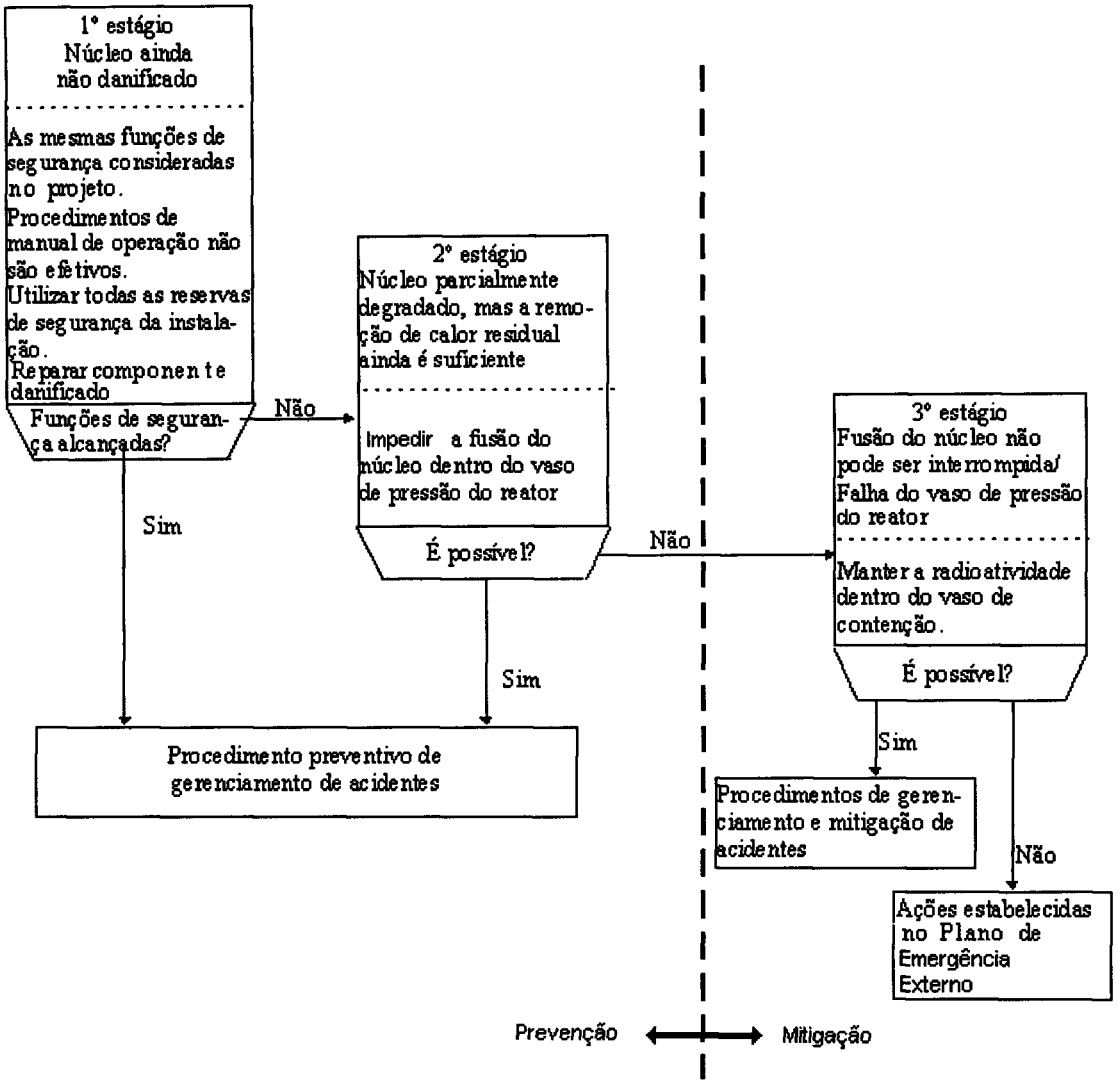


Figura A.2-2 - Estágios no gerenciamento de acidentes no núcleo de um reator nuclear [98]

APÊNDICE B

ESTRESSE

B.1 Generalidades

Dois tipos de reações que ocorrem no organismo humano são provocadas por estímulos sensoriais (luminosos, térmicos, etc.): uma específica, que vai se manifestar como resposta adequada à peculiaridade de estímulo (exemplo: sentir frio e ficar arrepiado), e outra não específica, que é a *reação de estresse*. O estresse, portanto, é parte do processo de percepção do organismo a estímulos *externos*. O que ocorre na reação de estresse é a excitação do sistema nervoso e a liberação de substâncias químicas capazes de alterar o equilíbrio homeostático (estabilidade interna do corpo humano). Basicamente, a reação de estresse é uma mobilização das defesas do corpo (a nível fisiológico), a fim de atender a alguma circunstância ambiental. Trata-se de parte do processo de adaptação do organismo ao meio.

O estresse (ou reação de estresse) compreende três fases ou estágios, sendo um processo demorado, chamado por Hans Selye [99] de Síndrome de Adaptação Geral. Síndrome, por definição, é um grupo de indícios e sintomas que ocorrem simultaneamente e caracterizam uma doença.Os estágios são os seguintes: a reação de alarme, o estágio da resistência e o estágio da exaustão.

A reação de alarme tem início alguns segundos após a percepção da causa do estresse pelo indivíduo, envolvendo processos fisiológicos autônomos. O organismo do indivíduo se prepara para reagir fisicamente à situação: a pressão sobe, o coração pulsa mais rápido; a respiração se torna mais pesada e rápida; os músculos se contraem; e as mãos e os pés se tornam mais frios e suados. O indivíduo está pronto para lutar ou fugir ("fight or flight syndrome"), segundo a concepção de Selye [99]. Dada a sua importância para a sobrevivência do homem primitivo, esta resposta ficou programada no corpo do ser humano. Essa reação biológica do homem continua a mesma, atualmente. Entretanto, apesar do aumento da violência nas grandes cidades, o estresse mental produzido no presente é mais sutil e freqüente, e tem sido mediado mais pelas reações sócio-econômicas do que pela iminência de perigo físico imediato.

Na referência [99], foi observado que as mudanças ocorridas no corpo humano durante os estados de forte emoção são bastante padronizadas, isto é, os processos fisiológicos envolvidos são os mesmos, independentemente do tipo de emoção sentida. Para todos os efeitos práticos, a raiva provoca as mesmas alterações químicas que o medo, por exemplo. Por outro lado, as pessoas reagem de forma distinta aos estímulos ambientais, sendo que o desempenho de cada um é diferente, estando ligado à experiência de vida e às reações aprendidas (como, por exemplo, treinamento), além de outras características pessoais, como fatores psicológicos, como, por exemplo, a personalidade.

Portanto, o estresse é basicamente o mesmo para todas as pessoas, embora o fator que cause o estresse possa ser diferente (medo, raiva, sensação de perigo e outros). Este fator predominante da causa do estresse é chamado de *pressão* [99], e refere-se às características de uma situação que pode ser problemática para o indivíduo, e que eqüivale à exigência de algum tipo de adaptação, que reflete a tentativa do corpo de manter o equilíbrio natural. Esta pressão pode ser de origem física, psicológica ou psicossocial, dentre outras, e não é necessariamente negativa. Uma grande alegria ou a emoção de ver reunidas várias pessoas queridas, por exemplo, causa a mesma reação biológica na pessoa, ou seja, a que se refere a um conjunto específico de condições bioquímicas do corpo humano. Em resumo, a pressão está na situação apresentada, em alguma possível perturbação do ambiente próximo. O estresse está na pessoa, como um componente natural do funcionamento humano que tende a reagir àquela perturbação, buscando um ponto de equilíbrio. Por isso, uma situação nova ou um ambiente desconhecido podem ser causadores de estresse, representando um tipo de pressão à qual o indivíduo deve responder, ou se adaptando ou retirando-se da presença deste fator, quando possível.

Em seguida à reação de alarme ou estágio de estresse inicial, ocorre o estágio de adaptação ou resistência, se os estímulos aos quais é submetido o organismo continuam, sendo mantida a intensidade desses estímulos (a natureza e a intensidade dos estímulos é variável).

Nesse estágio, o organismo vai se adaptando; a capacidade de resistência do corpo realmente aumenta para responder às exigências da situação. Posteriormente, o organismo tende a voltar ao normal, com suas funções restabelecidas e estabilizadas.

O estágio de exaustão ocorre caso não ocorra uma adaptação, ou seja, quando a volta do organismo às condições anteriores não foi possível realizar-se. Nesse caso, o nível de resistência vai progressivamente diminuindo e surgem alterações orgânicas, como fenômenos citolíticos, enfartes, necroses e outras, podendo prejudicar seriamente o organismo.

B.2 Conceitos Relacionados ao Estresse

Até 1936, o termo estresse era apenas um termo técnico usado em engenharia, de acordo com [100] sendo a "força atuando em uma unidade de área em um material sólido, resistindo à separação, compactação ou deslizamento que tendem a ser induzidos por forças externas". Para um engenheiro, "stress" e "strain", ou "tensão" e "resistência (à deformação)" estão quantitativamente relacionados e bem definidos em conceitos associados, como *tensão de deformação* e outros. O interessante é que existe uma certa similaridade de conceitos usados nas áreas de engenharia e psicologia. Por exemplo, na mesma referência [100], estresse é "um estímulo ou uma sucessão de estímulos de tal magnitude que tende a romper o equilíbrio interno do organismo de animais superiores", como o homem. Quer dizer, a forças (ou estímulos) externas, correspondem reações internas que tendem a manter um determinado equilíbrio.

Em 1936, Hans Selye [99] introduziu uma definição de estresse no campo das ciências biológicas como sendo "o estado manifestado por uma sindrome específica, constituída por todas as alterações não específicas produzidas num sistema biológico".

Atualmente, o termo estresse tem sido usado em lugar de tensão embora no ramo das ciências médicas ainda exista uma certa diferenciação, por alguns autores, entre

estresse, como sendo a reação de um organismo, e tensão, como a reação de origem emocional. No entanto, as causas fundamentais são as mesmas, ou seja, estão relacionadas ao reconhecimento de situações que se aparesentam ao organismo, modificando um determinado ambiente, e à tentativa deste de se adaptar ao mesmo. Tendo como base o dicionário Aurélio [60], "estresse é o conjunto de reações do organismo a agressões de ordem física, psíquica, infecciosas e outras, capazes de perturbar o equilíbrio natural do organismo. *Estressor* seria o agente produtor do estresse, enquanto *estressar* seria produzir estresse".

Nesta mesma referência, encontra-se *tensão*, como vindo do latim "tensione" (rigidez em certas partes do organismo), que provocam uma grande aplicação ou concentração física ou mental. Também pode ser considerada *fadiga*. Segundo a referência [101], *estresse* é uma palavra derivada do latim, que foi popularmente usada durante o século XVII para representar adversidades ou aflição. Em fins do século XVIII seu uso evoluiu para denotar força, pressão ou esforço, exercido principalmente pela própria pessoa, seu organismo e mente.

Do ponto de vista da referência [11], tensão é:

a. em fisiologia, estiramento a que um músculo, tendão ou qualquer outro tecido orgânico é forçado por uma contração, em qualquer momento dado;
b. sensação que acompanha o esforço muscular;
c. na psicologia do comportamento, o estado emocional que resulta da insatisfação de necessidades ou do bloqueio de uma atividade dirigida no sentido da realização de um propósito inadiável.

Neste último sentido, é correto dizer que um indivíduo se comporta sob estresse emocional (ou seja, o fator tempo também é um agente causador de estresse).

Em resumo, para um profissional da área médica ou psicólogo, estresse é a resultante mental, emocional e física aos estímulos externos. Em algumas circunstâncias, o estresse é auto-gerado, ou decorre de fatores internos. E, ao contrário do que acontece nos campos da engenharia ou física, onde o estresse é mensurável (carga por unidade de área), no campo da psicologia ou medicina, o estresse não é sempre mensurável, embora possa ser constatado por efeitos facilmente observáveis.

Do ponto de vista da referência [1], o estresse é a "tensão mental ou física, se estendendo de um estado mínimo de estimulação, indo até a uma sensação de ameaça ao bem estar de alguém, exigindo ação", que é o conceito adotado neste trabalho. Ainda segundo a mesma referência, estresse também pode ser definido como a "resposta humana a um estressor". Os efeitos do estresse no desempenho humano são curvilíneos, se estendendo de uma faixa de baixo desempenho (quando há falta de estimulação suficiente), passando pelo desempenho ótimo (ótimo nível de estresse) até um nível de desempenho extremamente alto (em ambiente onde exista um alto nível de estresse), tendendo a ser ameaçador. Os conceitos acima são adotados neste trabalho, para utilização em APS e ACH.

De qualquer maneira, o sentimento de diversos analistas de confiabilidade humana é que o modelo fornece estimativas razoáveis dos efeitos de estresse no desempenho.

Toda esta discussão anterior serve para mostrar que a área de estresse é muito vasta. Considerando apenas o estresse relacionado ao desempenho humano uma PSF importante, existe dificuldade na sua quantificação, e há muitas incertezas associadas às tentativas de quantificá-lo. Grande parte deste Apêndica B se refere a um aspecto muito

restrito desta área: o desempenho de pessoal habilitado na operação de uma usina nuclear. Esta abordagem constitui uma simplificação deliberada do tópico para os propósitos de interpretar ou traduzir os PSF's de estresse, de forma a tornarem-nos manipuláveis pelos analistas com responsabilidades na condução de análises da confiabilidade humana. As hipóteses e racionalizações que são apresentadas, adotadas de [1], provavelmente serão adequadas também para industrias convencionais.

B.3 A Carga de Trabalho e os Efeitos do Estresse

Dados obtidos de efeitos de estresse são muitos localizados, não havendo, até agora, um tratamento abrangente dos efeitos de estresse no desempenho, embora o problema tenha sido alvo de muitas e sérias atenções e estudos [1]. Os dados existentes são particularmente esparsos, sobre o desempenho de pessoal técnico atuando sob estresse em condições estabelecidas. Em seguida é apresentada uma tentativa de aplicar o pouco que se sabe sobre estresse, relacionado ao desempenho de pessoal de operação de usinas nucleares.

B.3.1 Níveis de estresse

A clássica curva de estresse relacionada com o desempenho é apresentada na Figura B.3-1 [1].

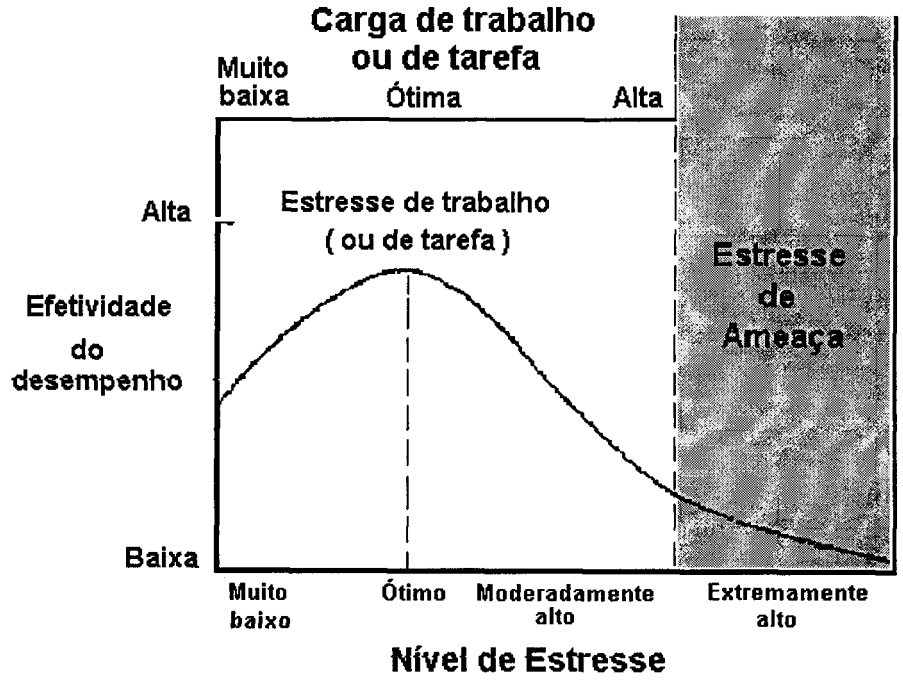


Figura B.3-1 Relação hipotética entre o desempenho e o estresse, considerando a carga de trabalho

Note-se que a Figura B.3-1 apresenta a divisão entre o estresse de trabalho (ou tarefa) e o estresse de ameaça. A curva indica que o desempenho segue uma relação curvilínea com estresse, indo de um valor para o estresse bastante baixo até valores extremamente altos.

Para os fins de análise de confiabilidade humana, considera-se adequado representar a faixa contínua de estresse por somente quatro níveis. Estes níveis, usados na referência [1] e aqui adotados, são os seguintes:

a. Muito Baixo (estímulos insuficientes para manter alerta o operador);
b. Ótimo (nível facilitador);
c. Moderadamente Alto (ligeiramente a moderadamente perturbador);
d. Extremamente Alto (muito perturbador).

Para os propósitos da Análise de Confiabilidade Humana, considera-se que seja *moderadamente perturbador* o nível de estresse moderadamente alto (em lugar de ligeiramente perturbador). Adota-se a designação de *alto nível de estresse* para os níveis moderadamente alto e extremamente alto de estresse.

Os três primeiros níveis de estresse são atribuídos à carga de trabalho, e o quarto nível é atribuído ao sentimento de ameaça. No lugar dos últimos dois níveis associados ao estresse designa-se:

c. carga pesada de trabalho (chega perto ou excede a capacidade humana normal; moderadamente perturbador);
d. estresse de ameaça (implica em reações emocionais; muito perturbador).

Os efeitos dos três primeiros níveis podem ser estimados aplicando-se fatores modificadores (PSF) às probabilidades de erros humanos. O último nível (ameaça) é qualitativamente diferente dos outros três. O seu efeito ultrapassa ou sobrecarrega os outros PSF's. Por esta razão, é atribuída uma diferente faixa de HEP's à situação de estresse de ameaça. Nota-se que a discussão que se segue está limitada ao estresse associado à carga de trabalho, tais como as que são desenvolvidas em usinas nucleares. Neste caso, o estresse de origem física não é considerado, devido ao fato de que um estresse mínimo está associado a uma eventual exigência de uso de roupa protetora em ambientes sujeitos à radiação, que ocorre somente em situações específicas. Este seria o caso, por exemplo, da necessidade do operador se deslocar até lugares onde existe contaminação, como nas proximidades do gerador de vapor, para eventuais conserto e manutenção. Fatores sociológicos, como o relacionamento entre patrão e empregado, problemas domésticos, salariais e outros, dentre os quais os efeitos da aplicação de política governamental através de medidas econômicas e financeiras não estão incluídos na Análise de Confiabilidade Humana (embora colaborem com uma inevitável contribuição, muitas vezes significativas, ao desempenho do ser humano no trabalho). Dessa forma, os dados usados para aplicação de estresse em ACH são considerados, inicialmente, para um nível ótimo.

Ao se desenvolver uma análise da confiabilidade humana deve-se decidir se o nível de estresse é ótimo, e se não for este o caso, como fazer para modificar as HEP's associadas. A referência [1] discute com maior nível de detalhes o problema do estresse, orientando quanto à determinação de níveis associados com as várias tarefas usuais relacionadas ao trabalho em usinas nucleares. Apenas para ilustrar, serão apresentados alguns exemplos, considerado a carga de trabalho.

No caso de *carga de trabalho com nível de estresse muito baixo*, a efetividade de uma pessoa diminui muito rapidamente. A pessoa consegue se concentrar, em média, trinta minutos, caso não haja estímulos suficientes para manter a atenção. É o caso, por exemplo, de um inspetor verificando um grande número de itens uniformes ou executando tarefas de vigilância em geral. Pessoas altamente qualificadas estão mais sujeitas a experimentar o baixo nível de estresse (a tarefa se torna desinteressante ou

monótona e aborrecida) e gradualmente vão perdendo a atenção (sua atenção vai sendo desviada para outras coisas).

Na Figura B.3-2, adaptada de [1], é apresentado um gráfico mostrando o efeito do tempo na vigilância do operador de usina nuclear, em tarefas passivas, com baixa taxa de variação de sinais. Pela figura se percebe que, por exemplo, em até meia hora neste tipo de trabalho, não há um efeito significativo, entretanto, para uma hora o efeito já é bem apreciável, sendo o efeito muito negativo para uma hora e meia.

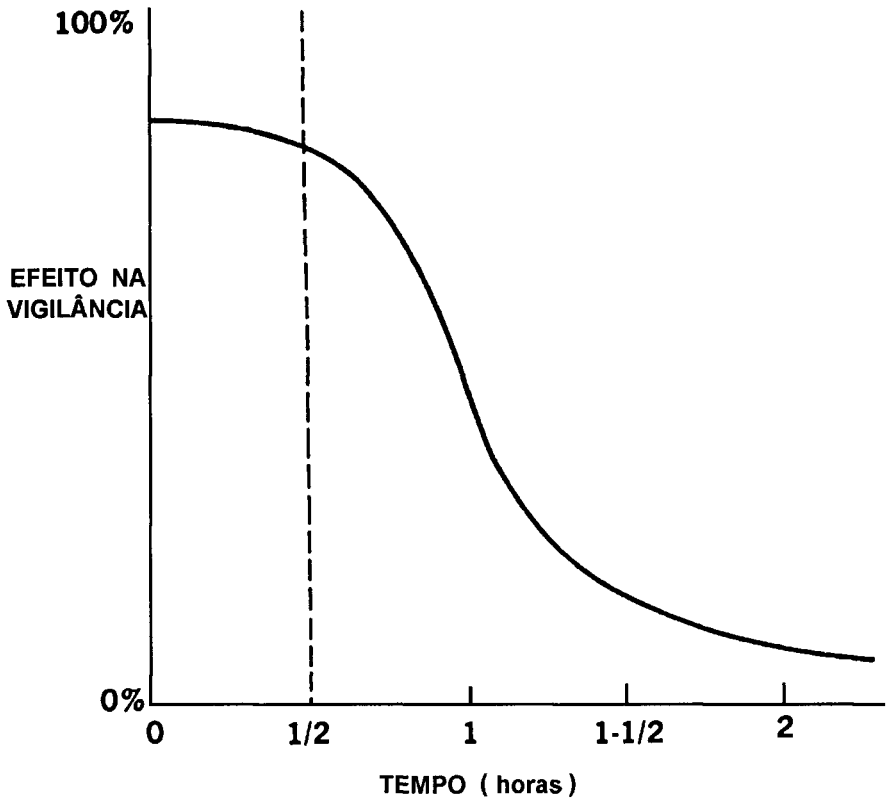


Figura B.3-2 Efeito do tempo na vigilância de um operador, em tarefas de monitoramento, com pouca necessidade de concentração

Pessoas com menor qualificação mantêm o interesse em tais tarefas. É de se notar que estão sendo consideradas tarefas rotineiras e não ocasionais (que, existindo num período curto e exigindo atenção da pessoa, não chegam a ser desinteressantes). Tem-se constatado o bom desempenho de pessoas levemente deficientes, do ponto de vista da capacidade mental, em tarefas industriais simples, como operadores de elevador, por exemplo. Devido ao nível de qualificação exigido para operadores de usinas nucleares, é improvável que pessoas como estas sejam aproveitadas na indústria nuclear. Por outro lado, deve ser notado que, em conseqüência, um aumento na probabilidade de erros pode acontecer nesses períodos em que é necessário trabalhar em tarefas monótonas, típicas de vigilância. Por isto mesmo, em troca de turnos, o operador que entra em serviço faz uma verificação geral nos instrumentos e controles de uma usina nuclear em operação.

No caso de *ótima carga de trabalho*, as tarefas têm um mínimo de diversificação, de modo a manter a atenção da pessoa. São tarefas ou condições de trabalho em que predominam , ou existem (por exemplo):

- interação ativa entre a pessoa e o ambiente;
- conversação com os colegas de trabalho;
- leitura de mostradores;
- ajuste de controles;
- tomada de decisões, com a condição de que a pessoa possa atuar sem pressa;
- testes de manutenção;
- calibração;
- vistoria inicial (troca de turno);
- leitura de mostradores iluminados;
- motivação para o trabalho.

No caso de *tarefas com alta carga de trabalho*, exige-se da pessoa um desempenho que se aproxima do limite de sua capacidade. A maioria das pessoas, nessas condições, experimenta uma certa degradação em seu desempenho. Um exemplo simples de limite seria o de uma pessoa interpretando dados em um mostrador, cuja capacidade de apresentação fosse maior que a capacidade de apreensão ou de leitura daquela pessoa.

No caso de um operador de reator, este poderá, por exemplo, priorizar as seqüências de várias sub-tarefas que compõem a sobrecarga, desta forma achatando o pico. Depois, ele decide ignorar as sub-tarefas consideradas não essenciais (porque, em decorrência de treinamento realizado, ele sabe ou supõe que não afetarão a operação de maneira catastrófica). Outros estratagemas ou artifícios são empregados, dependendo da situação. Tendo em vista o estratagema utilizado, o operador está mais sujeito a cometer erros quando desempenha tarefas com alta carga de trabalho, em relação ao ótimo nível de estresse.

De qualquer forma, como visto nos Capítulos 2 e 6, a tendência atualmente é diminuir a quantidade de informações apresentadas em mostradores ou monitores de computadores, limitando a apresentação, para o operador de usinas nucleares, àquelas informações realmente necessárias.

Nota-se uma carga excessiva de informações em situações como as emergência, que chegam a exigir 100% da capacidade normal do operador. Nestas condições, o operador usa técnicas pessoais, além do incremento da capacidade física que acontece em decorrência de mudanças fisiológicas do organismo, provocadas pela atividade das glândulas adrenais (reação de alarme no estresse).

Para o analista de ACH, surge a questão de determinar o que é uma alta carga de trabalho, em situações de operação numa usina nuclear. Fica claro que, quanto mais capaz e experiente a pessoa, melhor lidará com a emergência, sem sofrer séria degradação no seu desempenho. Porém, o analista não irá determinar os níveis de habilidade e experiência dos operadores (assunto para avaliação psicológica de potencial). Como solução conservativa à questão, sugere-se que certas situações, correntes em usinas nucleares, possam ser classificadas como as que impõem uma sobrecarga ao operador. Exemplos disso seriam:

- transientes simples, que envolvam o desligamento do reator e da turbina, num determinado limite de tempo;
- certas tarefas que devem ser desempenhadas ao ligar e desligar o reator, considerando-se um tempo determinado (sub-tarefas críticas);
- trabalho realizados em ambientes radioativos, nos quais devem ser usadas roupas especiais de proteção.

As situações que impõem a pressão do tempo no desempenho podem, em geral, ser classificadas como sobrecarga (carga alta ou elevada de trabalho). A tomada de decisão, por exemplo, sofre uma degradação maior do que o desempenho de tarefas bem conhecidas, pois existe sempre a possibilidade de uma decisão errônea, mesmo que a recuperação posterior seja possível. Este assunto foi discutido anteriormente, no Capítulo 2. Uma situação que exija resposta rápida é também um exemplo de alta carga de trabalho.

B.4 Respostas dos Operadores

Alguns operadores poderão responder a um evento não usual de maneira calma e fria. Outros poderão tentar uma fuga mental da realidade, negando que algo esteja acontecendo. Outros ainda poderão se apavorar, chegando mesmo ao pânico. A diversidade de reações é função de muitos fatores influenciadores do desempenho. Provavelmente os três mais importantes são, considerando o estresse:

- a estabilidade emocional do operador;
- o nível de familiaridade com a condição não usual (treino, habilidade, experiência com outras condições semelhantes);
- a extensão na qual as informações são obtidas a partir dos instrumentos, em função da situação (balanço entre qualidade e quantidade de informações fornecidas ao operador para apoio a suas ações).

Embora existam testes psicológicos para a avaliação da estabilidade emocional de indivíduos, existem muitos fatores que tornam difícil, na prática, prever a estabilidade emocional do operador em situações reais. Em geral, conforme [1], os testes psicológicos para avaliação de desempenho individual na operação de usinas nucleares ainda se encontram num estágio de credibilidade que deixa a desejar.

Fatores individuais como a capacidade de reação a uma determinada condição ou situação, ou a capacidade de agir sob condições de estresse ou de emergência, somente aparecem em condições reais e em algumas situações em simuladores [1]. A área onde mais se tem experiência com relação aos fatores acima expostos, é a área militar, como explicitado em [1]. Entretanto, mesmo nesta área, o que importa é o treinamento e a vivência, ou seja, a experiência. De maneira geral, isto também é verdade para outros campos, onde a necessidade de treinamento é decorrente da complexidade de operações a serem realizadas, como na indústria e na aeronáutica.

Quanto à capacidade e experiência em responder a uma situação não usual, considerando operadores de usinas nucleares, o problema que surge é em relação ao treinamento. Depois de completado o treinamento formal (inicial) do operador, este raramente recebe prática posterior (retreinamento) para lidar com situações de emergência, a não ser quando da requalificação (períodos distintos em diferentes países). Isto envolve lidar com um número relativamente pequeno de amostras de possibilidades de emergências em um simulador dinâmico. Dessa forma, para os tipos de emergências para os quais não foram realizados exercícios nos simuladores, e que podem representar situações novas, a tendência será de ocorrer uma degradação das capacidades individuais. Esta situação pode não ser tão ruim, se depois do treinamento em simuladores, treina-se na própria instalação onde o operador trabalha, usando-se artifícios de controle e escolhendo-se alguns cenários adequados.

Na Figura B.4-1, ilustra-se a vantagem do treinamento contínuo, comparado com o não treinamento posterior para condições de emergência [1].

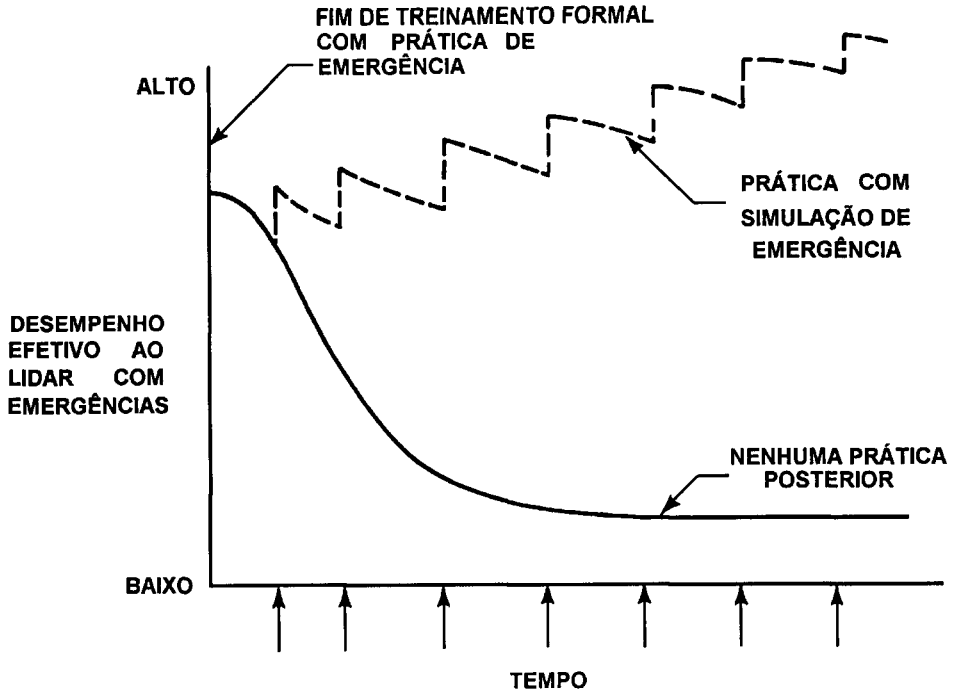


Figura B.4-1 Gráfico comparando a vantagem de treinamento realizado continuamente no tempo, com o treinamento inicial apenas, para condições de emergência

O terceiro fator crítico relativo ao estresse, é a adequação ergonométrica do equipamento. Até no início da década de 1980, reconhecia-se que o projeto de sistemas de operação e controle de usinas nucleares existente na época não era adequado às limitações físicas das pessoas, como por exemplo os limites antropométricos, conforme exemplos já apresentados no Capítulo 2 [1, 16]. Além disso, considerava-se que a indústria nuclear dava pouca atenção à disciplina "ergonomia".

Também não se reconhecia o nível de capacidade do operador em diagnosticar eventos anormais, baseando-se no que via nos instrumentos, e qual seria sua resposta, como seqüência desse fato. Estes fatores foram discutidos anteriormente, nos Capítulos 2 e 6.

No acidente de Three Mile Island, essas limitações se manifestaram por atos incorretos e diagnósticos demorados ou tardios, piorando uma condição que, por si só, já era séria, caracterizando um certo despreparo dos operadores ao lidar com tal situação. Parece que grande parte do estresse experimentado pelo operador de reator em uma situação de emergência se deve à sua falta de habilidade em diagnosticar a causa da emergência. Isto ocorreu em Three Mile Island porque os mostradores não apresentavam todos os dados essenciais de modo imediatamente utilizável (compreensível), ou não ajudaram o operador a "filtrar" os dados, observando apenas aqueles não imediatamente necessários.

Embora esse tipo de situação venha melhorando, com a aplicação dos atuais sistemas utilizando computadores e sistemas especialistas, não deverá desaparecer totalmente, e por isso continuará ainda a ser um problema. Esta falta de habilidade para

dimensionar prontamente a situação é uma experiência estressante, como tem sido observado em exercícios de simulação [1].

Os três fatores influenciadores do desempenho descritos até agora estão interrelacionados, ou seja, o operador que não souber lidar com situações anormais de forma adequada, muito provavelmente não atuará bem no diagnóstico e na resposta a situações mais sérias. De qualquer maneira, até que a pessoa esteja realmente capacitada para o diagnóstico e resposta a uma situação, permanece favorecida a tendência ao comportamento inadequado ou prejudicado.

As altas probabilidades de erros humanos e fatores de erro associados ao desempenho sob estresse, apresentadas na referência [1], podem parecer pessimistas, mas são justificadas, tendo em vista que os fatores ergonômicos são inadequados para muitas usinas existentes (boa parte das usinas é antiga, e muitas delas ainda continuarão funcionando por muito tempo). Também contribui para isto o treinamento apenas superficial que os operadores recebem para lidar com situações de emergência; quanto a este aspecto o Brasil não pode ser considerado excessão.

B.5 Estresse de Ameaça

O estresse de ameaça corresponde ao nível que se denomina "extremamente alto", como já visto [1]. É qualitativamente diferente dos outros três níveis, porque envolve o componente emocional: a ameaça ao bem estar e à segurança de alguém. No caso do pessoal de usinas nucleares, ela raramente significa uma ameaça física sendo, usualmente, uma ameaça à auto-estima ou ao "status" profissional. As salas de controle de usinas nucleares são estremamente seguras, e é muito difícil alguma ameaça concreta à segurança dos operadores.A ameaça a auto-estima pode engendrar medo de ação disciplinar, perda de emprego, ou sentimento de perda de confiança frente aos superiores, por não conseguir lidar com a situação em nível adequado.

Quando qualquer evento anormal ocorre, as atividades envolvidas na restauração das condições seguras de operação impõem um alto nível de carga de trabalho para cada operador. Isto corresponde ao nível de estresse moderadamente alto. Se a resposta do sistema às ações do operador é a esperada, o operador sabe que tem o sistema sob controle, e normalmente não sente qualquer ameaça, medo ou receio. Se, entretanto, o sistema não responde conforme o esperado, com as ações tomadas pelo operador, é provável que este sinta que perdeu o controle, e se sentirá ameaçado. Pode surgir uma sensação que se traduzirá assim: "o sistema está me fazendo de bobo?". Tal situação pode surgir no caso de erro no diagnóstico de um evento, no caso de transientes múltiplos, ou em qualquer caso no qual o sistema não responde satisfatoriamente. Ou seja, contraria a expectativa, nas tentativas de restauração dos controles à situação normal.

A falha no diagnóstico pode resultar de erro do operador ou de apresentação inadequada de informação sobre a condição da instalação (como ocorreu no acidente de TMI). Transientes múltiplos podem causar frustração, por exemplo, quando os operadores não esperam mais que uma falha de cada vez, sendo que informações de diferentes eventos são apresentados nos mostradores e/ou indicadores, confundindo e complicando o diagnóstico. Dessa maneira, o entendimento da equipe de operação é de que não tem a instalação sob controle, já que não foi constatada a causa de um problema em particular, e isso se traduz como uma fonte de ameaça à equipe. O sentimento de ameaça envolve

reações emocionais, com níveis de intensidade e efeitos no desempenho que diferem de indivíduo a indivíduo. Na maioria dos casos, as reações emocionais têm um efeito adverso no desempenho.

No caso de um LOCA por pequena ruptura (acidente com perda limitada de refrigeração de reator) ou no caso da evolução não abrupta de um LOCA (acidente com perda de refrigeração à uma taxa baixa), não se espera um nível de estresse do operador maior que o correspondente à alta carga de trabalho. Em alguns incidentes envolvendo LOCA's por pequenas rupturas, o nível de estresse pode não ser muito alto, inicialmente, mas eventos subseqüentes podem provocar o aumento do nível de estresse. No acidente de TMI, que envolveu um LOCA de pequena vazão, alguns dos operadores entrevistados posteriormente ao acidente consideraram-se em vários momentos sob efeito de níveis extremamente altos de estresse (ameaça) [1]. Isto enfatiza a premissa de que o sentimento de perda de controle da máquina ou sistema resulta num estresse crescente.

Há uma grande variabilidade na percepção de ameaça. Uma situação que parece ameaçadora ou assustadora para um operador novato, pode ser percebida como de rotina por uma pessoa mais experiente. Pode-se fazer uma analogia com a seguinte situação: um motorista experiente não se sentirá ameaçado ao entrar em uma rodovia movimentada, ao passo que um motorista novato, que nunca dirigiu antes em nenhuma rodovia, poderá sentir medo.

A curva de estresse tem a intenção de representar a relação entre desempenho e o nível percebido de ameaça, que varia com os atributos de cada indivíduo, tal como a experiência.

Um outro nível de ameaça, também importante, relacionado com o estresse, é quanto à percepção de risco, que foi discutida resumidamente no Apêndice A. Em qualquer instalação complexa existe um risco que não pode deixar de ser considerado. Para esse risco, deve haver uma preparação para situações de emergência, caso aconteça algum problema mais sério e que fuja ao controle. Considerando o caso brasileiro, a Usina Nuclear Angra 1 tem, implantado, um sistema de resposta a situações de emergência, que já causou muita polêmica. A situação chegou a um tal ponto que, em decorrência de ação judicial, o seu funcionamento foi impedido, por algum tempo (1994). Não cabe, aqui, discutir o assunto; entretanto, é importante deixar claro que a indústria nuclear não pode ir contra a opinião da população, se esta reclama de um risco que está correndo. É importante avaliar as dimensões desse risco, como discuti-lo com a sociedade e se ele pode ser aceito [4]. O Brasil não tem tradição de enfrentamento de grandes catástrofes, como terremotos, vulcões, furacões, guerras, se bem que outras trajédias fazem parte da cultura brasileira, como a seca do nordeste ou as enchentes no sul e sudeste do país. A central nuclear de Angra veio trazer um aspecto novo à questão: o risco tecnológico. O estresse é importante, se não o fator mais significativo, na percepção de risco e na aceitação do risco por uma determinada população. Fatores econômicos, sociais e psicológicos estão envolvidos, mas o estresse, individual ou coletivo, não pode ser descartado.

B.6 O Problema de Dados para o Estresse de Ameaça

A maioria dos experimentos com estresse de ameaça se refere a tarefas artificiais, em situações nas quais o sujeito submetido à experiência está claramente ciente de que nada catastrófico resultará de qualquer inaptidão de sua parte; portanto, suas

reações emocionais são mínimas [1], não representando a realidade, ou seja, seria um absurdo que, em uma simulação, alguém viesse realmente a sentir estar correndo perigo.

Existem situações reais, como um candidato a emprego realizando um exame de qualificação e outras situações semelhantes, onde a demanda de cumprir um objetivo determinado contribui para, em certos casos, sentir um estresse de ameaça. Entretanto, na maioria absoluta dessas situações, a conseqüência fica restrita às expectativas do indivíduo ou de um pequeno grupo, não chegando a constituir uma ameaça à segurança em nenhum instante. Em outras áreas, o estresse de ameaça é extremamente importante, como a situação de um goleiro na decisão por penaltis de um campeonato de futebol, ou mesmo a dos jogadores que vão chutar em gol para decidir a disputa. Entretanto, também não são situações que possam colocar algum tipo de segurança em risco, obviamente não numa relação direta, porque o que acontece depois do jogo, envolvendo a torcida, tem conotações emocionais que fogem do escopo deste trabalho, ficando no campo da sociologia e áreas afins.

Fontes bibliográficas relacionadas a assuntos militares indicam um grande aumento do nível de estresse [1], principalmente em combate real. A ênfase do treinamento de militares, está sempre, de algum modo, relacionada a situações de emergência. Para operadores de usinas nucleares, a resposta a uma situação de emergência representa somente uma pequena parte do treinamento, como discutido no item B.4, pois quase todas as tarefas a serem desempenhadas são rotineiras, para um nível de estresse quase sempre ótimo.

O maior nível de estresse que se pode prever, em usinas nucleares, está relacionado com a ocorrência de um acidente de perda de refrigeração. Em 1800 reatores-ano nunca ocorreu um LOCA [1], conforme descrito considerando a pior situação possível (dados de 1982). Entretanto, em [58] é usado um LOCA por grande ruptura como exemplo de situação que resulta num nível extremamente alto de estresse para os operadores. Em seguida à ocorrência de um LOCA deste tipo, a confiabilidade humana deve ser baixa, não somente por causa do estresse, mas também em decorrência da incredulidade do operador no acidente. Para o pessoal de operação de uma usina nuclear, a probabilidade de ocorrência de um LOCA é considerada tão baixa que, por alguns momentos, uma resposta potencial (do ser humano) será a de não acreditar nas indicações dos painéis de operação e controle. Sob tais condições, estima-se que nenhuma ação deverá ser tomada por pelo menos um minuto, e se alguma ação for tomada nesse minuto provavelmente será inadequada, resultando em erro.

A Figura B.6-1 apresenta uma estimativa de desempenho humano após a ocorrência de um LOCA por grande ruptura (por exemplo, do tipo "guilhotina") [1]. Com relação a esta curva de desempenho, considerando os estudos da referência [1], a probabilidade de erro foi avaliada em 0,9, cinco minutos depois de um LOCA por grande ruptura, em 0,1 depois de 30 minutos, e em 0,01 após duas horas (Figura B.6-1). Esta figura foi adaptada de [1], utilizando dados de [58].

Na Figura B.6-1, a linha contínua indica as probabilidades de erros humanos estimadas aplicáveis se o sistema de recuperação automática (Sistema de Refrigeração de Emergência) opera normalmente, mitigando os efeitos do acidente. Por outro lado, como indicado pela linha tracejada, a HEP estimada enquanto persistir a condição de estresse de ameaça será de 0,25. A margem de incerteza, conforme conceito discutido no item 4.2.5, relacionada com a estimativa de 0,25 para HEP é relativamente grande (0,005 a 1,0) para permitir que se considere o desempenho bom de alguns

indivíduos, e o de outros, "ser uma parte do problema". Como já visto, a Figura B.6-1 é baseada nas hipótese consideradas na referência [1], e se aplica a um único operador, sob condição de nível de estresse extremamente alto (estresse de ameaça).

Numa situação realística, mais que um operador estará presente na sala, devendo a HEPC (conjunta) ser calculada segundo os procedimentos da referência [1], descrito de maneira sucinta neste documento, no Capítulo 5, para tal situação. Esta referência fornece indicações de como devem ser modificados os HEP's básicos para um operador de reator (individualmente), de forma a considerar a presença de outras pessoas, o que, de maneira geral, tende a aumentar a confiabilidade do pessoal na sala do reator.

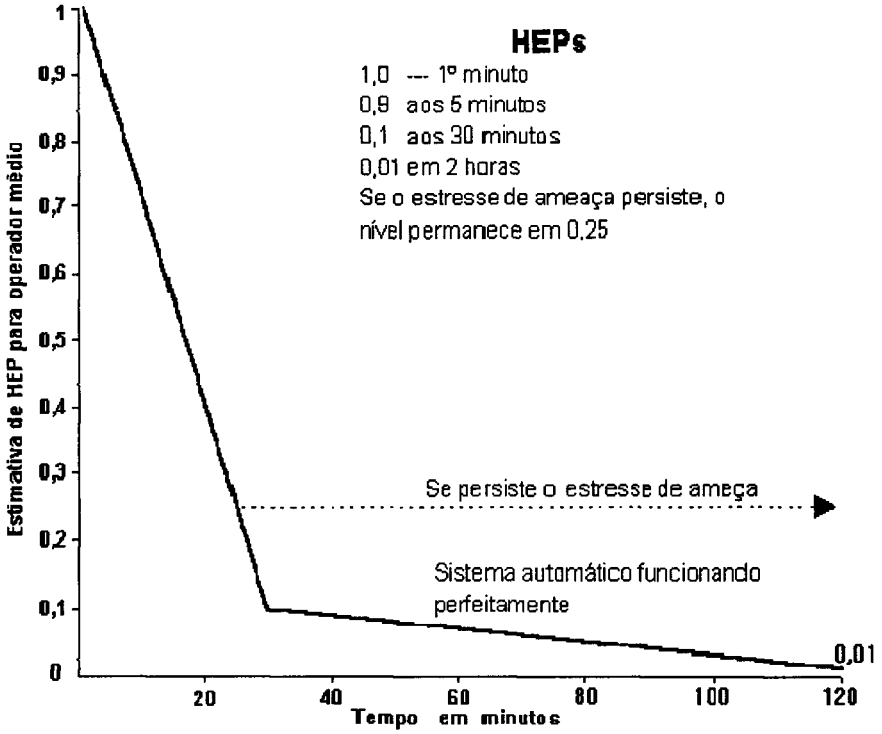


Figura B.6-1 - Estimativa de desempenho humano após um LOCA por grande ruptura

Por outro lado, neste mesmo exemplo, poderá ocorrer também uma redução da máxima confiabilidade teórica, em razão da dependência entre as pessoas na sala de controle do reator. Isto porque, em alguns casos, a consideração com a autoridade de um operador senior, ou com um outro operador de maior experiência, pode diminuir a confiança em determinada resposta a uma situação específica, considerada por um operador novato como a melhor, mesmo que este esteja certo. As probabilidades de erros humanos derivadas, em conseqüência da consideração de outras pessoas presentes, obedecerá a algumas regras, segundo critérios estabelecidos em [1]. Assim, por exemplo, considerando a Figura B.6-1, aos 30 minutos a HEP de 0,1 para um único operador deverá ser modificada (a presença de outras pessoas é também um fator influenciador do desempenho) considerando-se a hipótese de HEPC. Por exemplo, de 0,55 para um segundo operador (com alta dependência, relativo ao primeiro operador) e um HEP condicional de 0,15 para o supervisor técnico e o consultor técnico presentes na sala (portanto, quatro pessoas). Para o supervisor técnico e o consultor técnico, deve ser considerada baixa dependência (entre eles). Aplicando-se os dados, a HEP conjunta para as quatros pessoas em trabalho no turno será:

$$0,1 \times 0,55 \times 0,15 \times 0,15 = 0,0012 = 0,001$$

A dependência entre as pessoas varia com o estresse relacionado à situação e com a diferença da autoridade (real ou percebida), obviamente alterando a máxima confiabilidade teórica, como citado acima. A dependência entre um operador iniciante (novato) e um operador senior será normalmente maior que a dependência entre um supervisor de turno e um operador senior pois, certamente este último terá uma maior autonomia (em relação ao operador com menos experiência). Em geral, a dependência ao se considerar todas as pessoas cresce com o aumento do nível de estresse.

B.7 A Regra do Dobro

Há um corolário importante relacionado com a curva de desempenho apresentada na Figura B.6-1, para a condição de alta carga de trabalho. Esse corolário se aplica quando o tempo disponível para tomar ações corretivas é muito limitado. Nos trabalhos iniciais de Swain [1] foi desenvolvida um teoria do comportamento relativo ao estresse, cujo principal fator de pressão foi o tempo. Essa teoria sustenta que, caso um dado erro tenha sido cometido e reconhecido como tal, ou que a ação corretiva após um erro falhou nos seus propósitos pretendidos, a probabilidade de erro para as tentativas subseqüentes de ações corretivas dobram, ou seja, a probabilidade de erro aumenta por um fator dois. Por exemplo, se um único trabalhador, sob pressão severa do fator tempo, tenha uma tarefa cuja HEP correspondente é 0,1 e falha na primeira tentativa, na tentativa seguinte a HEP será de 0,2, na terceira de 0,4 e, na quarta tentativa, a HEP se aproximará de um.

Essas condições limitantes correspondem à completa desorganização do indivíduo, que se desestrutura e perde o controle da situação. Embora não esteja desenvolvida na referência [1], a teoria de Swain sugere que os resultados dos erros iniciais, sob alta carga de trabalho, induz a um sentimento de perda de controle, o que engendra o próximo nível de estresse, o de ameaça. Qualquer ação que falhe na restauração do controle pretendido aumenta a sensação de ameaça.

Estudos experimentais de pousos em portas-aviões, realizados por pilotos da marinha americana, indicam que, em tentativas repetidas, depois de uma falha inicial, a curva de estresse se aproxima da regra do dobro [1]. Esta é uma estimativa conveniente para o desempenho de um único indivíduo trabalhando. No caso de uma usina nuclear, o trabalho é realizado em equipe, e não individualmente. Entretanto, a regra do dobro não perde a validade, e se aplica à equipe, já que os modelos de desempenho de equipes levam em consideração as dependências entre os seus componentes.

Contrariamente à regra do dobro, existe uma variação baseada na hipótese de que, se um erro é cometido em ótimas condições de trabalho, que favorecem a tentativa seguinte, a HEP deverá ser reduzida por um fator dois [1]. Isso ocorre porque a pessoa estará mais cautelosa e prestará mais atenção se existir uma boa disponibilidade de tempo para a execução da tarefa. Essa seria uma regra que poderia ser aplicada se não fosse tão limitado o conhecimento dos modos possíveis de comportamento humano. Sendo assim, não se pode justificar a adoção da hipótese, a não ser em situações bem conhecidas e dentro de limitações aplicáveis. Portanto, seu uso em Análise de Confiabilidade Humana não é generalizado.

APÊNDICE C

TABELAS AUXILIARES

Tabela C.1 Probabilidade de erros humanos condicionais aproximados e respectivas margens de incerteza para níveis de dependência, dada a falha na tarefa precedente

Item	Níveis de dependência	Probabilidades básicas de erros humanos – HEPB's		
		(a)	(b)	(c)
(1)	DZ*	≤ 0,01	0,05 (FE = 5)	0,1 (FE = 5)
		(d)	(e)	(f)
		0,15 (FE = 5)	0,2 (FE = 5)	0,25(FE = 5)
Item	Níveis de dependência	Probabilidades básicas de erros humanos – HEPB's Margens de incerteza inferior a superior **		
		(a)	(b)	(c)
(2)	BD	0,05 (0,015 a 0,15)	0,1 (0,04 a 0,25)	0,15 (0,05 a 0,5)
(3)	MD	0,15 (0,04 a 0,5)	0,19 (0,07 a 0,53)	0,23 (0,1 a 0,55)
(4)	AD	0,5 (0,25 a 1,0)	0,53 (0,28 a 1,0)	0,55 (0,3 a 1,0)
(5)	DT	1,0 (0,5 a 1,0)	1,0 (0,53 a 1,0)	1,0 (0,55 a 1,0)
		(d)	(e)	(f)
(2)	BD	0,19 (0,05 a 0,75)	0,24 (0,06 a 1,0)	0,29 (0,08 a 1,0)
(3)	MD	0,27 (0,1 a 0,75)	0,31 (0,1 a 1,0)	0,36 (0,13 a 1,0)
(4)	AD	0,58 (0,34 a 1,0)	0,6 (0,36 a 1,0)	0,63 (0,4 a 1.0)
(5)	DT	1,0 (0,58 a 1,0)	1,0 (0,6 a 1,0)	1,0 (0,63 a 1,0)

Os valores dos HEPC's e sua margens de incerteza são aproximados. Todos os valores são baseados em pessoal qualificado, isto é, com mais de seis mêses de experiência nas tarefas consideradas para análise.

DZ* - Dependência Zero, ou independência completa. Assim, DZ = HEPB. Fatores de erros são baseados em [1].
+ É adequada a interpolação entre os valores estabelecidos para os HEPC's e suas margens de incerteza para valores de HEPB's dentre os listados na tabela, para a maioria dos estudos de APS.

AD - Alta dependência
MD - Média dependência, ou dependência média
BD - Baixa dependência
DT - Dependência total ou completa

Tabela C.2 Modificações de HEPS's estimados para efeito de estresse e níveis de experiência

Item	Nível de estresse	Modificador para pessoal qualificado	Modificador para pessoal novato
	Muito baixo e Ótimo	a	b
(1)	(Carga de trabalho muito leve) Ótimo (Carga de trabalho adequada)	x2	x2
(2)	Passo a passo	x1	x1
(3)	Dinâmico	x1	x2
	Moderadamente alto		
(4)	Passo a passo	x2	x4
(5)	Dinâmico	x5	x10
	Extremamente alto (Estresse de ameaça)		
(6)	Passo a passo	x5	x10
(7)	Dinâmico * e diagnóstico	0,25 (FE = 5)	0,5 (FE = 5)

* Neste caso, os valores não são modificadores, são HEP's para serem usados em tarefas dinâmicas.

Tabela C.3 Probabilidades estimadas de erros de ação na operação de controles manuais

Item	Erros potenciais	HEP	FE
(1)	Acionamento indvertido de um controle	*	
	Seleção de controle incorreto em painel com controles semelhantes		
(2)	Identificado somente por etiqueta	0,003	3
(3)	Arranjados em bem delineados grupos funcionais	0,001	3
(4)	Os quais são parte de umbem definido leiaoute mímico	0,0005	10
	Girar o controle de rotação na direção errada		
(5)	Quando não há violação de estereótipo populacional	0,0005	10
(6)	Quando o seu projeto viola um estereótipo populacional forte e as condições de operação são normais	0,05	5
(7)	Quando o seu projeto viola um forte estereótipo populacional e a operação é realizada em condições de estresse alto	0,5	5
(8)	Girar um comutador de duas posições na direção errada ou deixá-lo na marca errada	*	
(9)	Posicionar um comutador de rotação na marca errada	0,001	10
(10)	Falha em completar a mudança de estado de um componente, se o controle deve ser segurado até o fim da operação	0,003	3
(11)	Selecionar um interruptor de circuito em um grupo de interruptores de circuito densamente agrupados e identificados somente por etiquetas	0,005	3
(12)	Selecionar um interruptor de circuito em um grupo de interruptores de circuito densamente agrupados, mas com fatores influenciadores de desempenho mais favoráveis	0,003	3
(13)	Conectar incorretamente um conector	0,003	3

Os HEP's são para erros de ação, não incluindo quaisquer erros de decisão em relação ao controle a acionar.
* Consultar texto

Tabela C.4 Probabilidades estimadas de erros de omissão por item de instrução quando o uso de procedimentos escritos é especificado.

Item	Omissão de passos	HEP	FE
	Quando procedimentos com material de apoio são corretamente utilizados, em listas de verificações		
(1)	Lista curta, menor que dez itens	0,001	3
(2)	Lista grande, maior que dez itens	0,003	3
	Quando procedimentos sem material de apoio são utilizados, ou quando procedimentos com material de apoio são utilizados incorretamente		
(3)	Lista curta, menor que dez itens	0,003	3
(4)	Lista grande, maior que dez itens	0,01	3
(5)	Quando procedimentos escritos estão disponíveis e devem ser utilizados, mas não são	0,05	5

OBSERVAÇÃO: em todas as tabelas, pode ser necessário consultar o texto da referência [1], para compreensão de todas as implicações. As tabelas deste Anexo 3 são apenas para efeito de compreensão do problema apresentado no item 7.2, e para ilustrar a maneira como são apresentadas em [1].