



ANÁLISE DE FALHAS HUMANAS EM UM SISTEMA DIGITAL DE UMA USINA  
NUCLEAR UTILIZANDO UMA METODOLOGIA HÍBRIDA DFM/ATHEANA/FUZZY

Jonathan Marcello de Oliveira Pinto

Tese de Doutorado apresentada ao Programa de Pós-graduação em Engenharia Nuclear, COPPE, da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Doutor em Engenharia Nuclear.

Orientador: Paulo Fernando Ferreira Frutuoso e  
Melo

Rio de Janeiro  
Fevereiro de 2014

ANÁLISE DE FALHAS HUMANAS EM UM SISTEMA DIGITAL DE UMA USINA  
NUCLEAR UTILIZANDO UMA METODOLOGIA HÍBRIDA DFM/ATHEANA/FUZZY

Jonathan Marcello de Oliveira Pinto

TESE SUBMETIDA AO CORPO DOCENTE DO INSTITUTO ALBERTO LUIZ  
COIMBRA DE PÓS-GRADUAÇÃO E PESQUISA DE ENGENHARIA (COPPE) DA  
UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS  
NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE DOUTOR EM CIÊNCIAS EM  
ENGENHARIA NUCLEAR.

Examinada por:

---

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

---

Prof. José Antonio Carlos Canedo Medeiros, D.Sc.

---

Dr. Pedro Luiz da Cruz Saldanha, D.Sc.

---

Dr. Antonio César Ferreira Guimarães, D.Sc.

---

Prof. Marcelo Ramos Martins, D.Sc.

---

Prof. Enrique Andrés López Droguett, Ph.D.

RIO DE JANEIRO, RJ - BRASIL  
FEVEREIRO DE 2014

Pinto, Jonathan Marcello de Oliveira

Análise de falhas humanas em um sistema digital de uma usina nuclear utilizando uma metodologia híbrida dfm/atheana/fuzzy/ Jonathan Marcello de Oliveira Pinto. – Rio de Janeiro: UFRJ/COPPE, 2014.

XIV, 158 p.: il.; 29,7 cm.

Orientador: Paulo Fernando Ferreira Frutuoso e Melo  
Tese (doutorado) – UFRJ/ COPPE/ Programa de Engenharia Nuclear, 2014.

Referencias Bibliográficas: p. 116-127.

1. DFM. 2. Sistema Digital. 3. ATHEANA. 4. Fuzzy. I. Melo, Paulo Fernando Ferreira Frutuoso e. II. Universidade Federal do Rio de Janeiro, COPPE, Programa de Engenharia Nuclear. III. Título.

*“Artista e cientista têm  
sua religião, os outros  
precisam de uma.” (citação  
de Goethe por Freud)*

## AGRADECIMENTOS

A Deus, por me dar a oportunidade de viver esta experiência.

Ao meu pai pela compreensão e respeito.

À minha mãe pelo suporte oferecido.

Aos meus amigos, pelo esparecimento e apoio oferecidos.

À música que me leva ao equilíbrio nos momentos difíceis.

Ao Profs. Paulo Fernando Ferreira Frutuoso e Melo e Pedro Luiz da Cruz Saldanha pela disponibilidade, ensinamentos, orientação e apoio oferecidos durante o desenvolvimento deste trabalho.

Aos participantes da pesquisa de opinião, pela paciência e boa vontade.

À equipe da Eletronuclear pelos dados fornecidos e utilizados neste trabalho.

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

ANÁLISE DE FALHAS HUMANAS EM UM SISTEMA DIGITAL DE UMA USINA NUCLEAR UTILIZANDO UMA METODOLOGIA HÍBRIDA DFM/ATHEANA/FUZZY

Jonathan Marcello de Oliveira Pinto

Fevereiro / 2014

Orientador: Paulo Fernando Ferreira Frutuoso e Melo

Programa: Engenharia Nuclear

O trabalho apresenta uma aplicação da metodologia DFM (Dynamic Flowgraph Methodology) e da técnica ATHEANA (A Technique for Human Error Analysis) em um sistema digital de controle proposto para o pressurizador (PZR) das usinas nucleares atuais. O estudo consiste na modelagem DFM/ATHEANA desse sistema de controle e de suas interações com o processo a ser controlado e com o operador. Posteriormente, uma complementação dos resultados obtidos foi realizada através de coleta de opiniões de especialistas em conjunto com a teoria fuzzy.

No âmbito da confiabilidade humana, a DFM, juntamente com a técnica ATHEANA, consegue modelar  $n$  modos de falha para equipamentos e seres humanos (erros de omissão e erros de comissão), além de  $n$  fatores que influenciam o desempenho humano. Os resultados obtidos demonstram que a metodologia possibilita uma análise de falhas eficiente do sistema digital enxergando todas as possíveis interações existentes entre seus componentes. Através dos implicativos diretos, ela mostra as combinações de eventos de falha que levam à falha do sistema.

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

HUMAN FAILURE ANALYSIS OF A DIGITAL CONTROL SYSTEM IN NUCLEAR  
POWER PLANT THROUGH AN HYBRID DFM/ATHEANA/FUZZY METHODOLOGY

Jonathan Marcello de Oliveira Pinto

February / 2014

Advisor: Paulo Fernando Ferreira Frutuoso e Melo

Department: Nuclear Engineering

The paper presents a DFM (Dynamic Flowgraph Methodology) and ATHEANA (A Technique for Human Error Analysis) application to a digital control system proposed for the pressurizer of current PWR plants. The study consisted in modeling this control system and its interactions with the controlled process and operator through an integrated DFM/ATHEANA approach. The results were complemented using expert opinions in conjunction with fuzzy theory.

In terms of human reliability, DFM, along with ATHEANA, can model equipment failure modes, operator errors (omission/commission) and human factors that combined with plant conditions, influence human performance. The results show that the methodology provides an efficient failure analysis of digital systems identifying all possible interactions between components. Through prime implicants, the methodology shows the events combinations that lead to system failure.

## ÍNDICE

	PÁGINA
<b>1 INTRODUÇÃO.....</b>	<b>1</b>
<b>2 REVISÃO BIBLIOGRÁFICA .....</b>	<b>4</b>
2.1 O <i>SOFTWARE</i> EM SISTEMAS DIGITAIS .....	4
2.2 CONFIABILIDADE DE SISTEMAS DIGITAIS .....	6
2.3 ANÁLISE DE FALHAS HUMANAS.....	11
2.4 COLETA DE OPINIÕES.....	21
2.5 A LÓGICA FUZZY.....	24
2.6 AGREGAÇÃO FUZZY DE OPINIÕES.....	28
2.7 ESTUDO PROPOSTO .....	29
<b>3 DFM (<i>DYNAMIC FLOWGRAPH METHODOLOGY</i>).....</b>	<b>32</b>
3.1 DESCRIÇÃO DA METODOLOGIA.....	32
3.2 ELEMENTOS DO MODELO DFM .....	33
3.3 EXEMPLO DE UM MODELO DFM .....	34
<b>4 ATHEANA (<i>A TECHNIQUE FOR HUMAN ERROR ANALYSIS</i>).....</b>	<b>43</b>
4.1 DESCRIÇÃO DA TÉCNICA.....	43
4.2 ETAPAS DA TÉCNICA.....	46
<b>5 COLETA DE OPINIÕES E AGREGAÇÃO FUZZY.....</b>	<b>59</b>
5.1 MÉTODO DE COLETA DE OPINIÕES.....	59
5.2 MÉTODO DE AGREGAÇÃO FUZZY.....	62
<b>6 O SISTEMA DE PRESSURIZAÇÃO DO REATOR PWR.....</b>	<b>64</b>
6.1 SISTEMA REAL.....	64
6.2 SISTEMA PROPOSTO.....	65
<b>7 MODELAGEM DFM/ATHEANA DO SISTEMA PROPOSTO.....</b>	<b>68</b>
7.1 MODELAGEM DO SISTEMA DIGITAL.....	68
7.2 MODELAGEM DO COMPORTAMENTO HUMANO.....	76



<b>8 ANÁLISE DFM/ATHEANA DO SISTEMA PROPOSTO.....</b>	<b>89</b>
8.1 ANÁLISE DEDUTIVA.....	89
8.2 ANÁLISE INDUTIVA.....	94
<b>9 OPINIÕES DE ESPECIALISTAS E AGREGAÇÃO FUZZY DOS RESULTADOS.....</b>	<b>102</b>
9.1 QUESTIONÁRIOS APLICADOS.....	102
9.2 RESPOSTAS E AGREGAÇÃO DAS OPINIÕES.....	105
9.3 CÁLCULO DA PROBABILIDADE DO HFE.....	107
9.4 COMPARAÇÃO COM DADOS DA LITERATURA.....	109
<b>10 CONCLUSÕES E RECOMENDAÇÕES.....</b>	<b>112</b>
<b>REFERÊNCIAS .....</b>	<b>116</b>
<b>APÊNDICE A.....</b>	<b>128</b>
<b>APÊNDICE B.....</b>	<b>132</b>
<b>APÊNDICE C.....</b>	<b>133</b>
<b>APÊNDICE D.....</b>	<b>138</b>
<b>APÊNDICE E.....</b>	<b>142</b>
<b>APÊNDICE F.....</b>	<b>145</b>

## ÍNDICE DE FIGURAS

	Pág
Figura 1: Contribuição humana na frequência de dano ao núcleo [72].....	12
Figura 2: Tipos de ações humanas [3].....	14
Figura 3: Classificação de diversas HRA [65].....	15
Figura 4: Classificação das HRA por tipo de análise [3].....	15
Figura 5: Evolução do dano ao núcleo após um incidente em função dos tipos de ações humanas [3].....	18
Figura 6: Necessidade de incorporação dos resultados de uma HRA em uma APS [71].....	19
Figura 7: Etapas da lógica Fuzzy [35].....	24
Figura 8: Processo de fuzzificação.....	25
Figura 9: Método de defuzzificação por centro de gravidade [86].....	27
Figura 10: Sistema de exemplo .....	35
Figura 11: Modelo DFM do sistema exemplo.....	37
Figura 12: Processo cognitivo utilizado na ATHEANA [25].....	44
Figura 13: Estrutura de uma análise ATHEANA [24].....	46
Figura 14: Etapas da técnica ATHEANA [6].....	50
Figura 15: Desmembramento do HFE em ações inseguras [6].....	51
Figura 16: Análise da possibilidade de recuperação do HFE analisado [6].....	54
Figura 17: Incorporação do HFE em uma APS [6].....	57
Figura 18: Etapas realizadas na coleta de opiniões de especialistas [4].....	59
Figura 19: Pressurizador de uma usina PWR [96].....	65
Figura 20: Sistema digital proposto.....	66
Figura 21: Passos executados pelo <i>tool/set</i> no modo indutivo.....	101
Figura 22: Mapeamento dos perfis dos especialistas.....	104

## ÍNDICE DE TABELAS

	Pág
Tabela 1: Lógica do sistema exemplo de controle.....	35
Tabela 2: Discretização das variáveis do modelo.....	35
Tabela 3: CTA 1.....	38
Tabela 4: CTA 2.....	38
Tabela 5: CTR 1.....	38
Tabela 6: Implicativos diretos do evento topo “Nível de água transbordando em t=0” .....	39
Tabela 7: Implicativos diretos do evento topo “Nível de água Vazio em t=0”.....	40
Tabela 8: Possíveis escolhas de ações inseguras para um HFE [6].....	52
Tabela 9: Tabela de probabilidades iniciais sugeridas para ações humanas [6].....	56
Tabela 10: Lógica de controle do sistema digital proposto.....	67
Tabela 11: Discretização das variáveis de processo do modelo do pressurizador.....	69
Tabela 12: Variáveis de condição do modelo do pressurizador.....	70
Tabela 13: CTA 1 do sistema analisado.....	72
Tabela 14: CTA 2 do sistema analisado.....	73
Tabela 15: CTA 3 do sistema analisado.....	73
Tabela 16: CTA 4 do sistema analisado.....	74
Tabela 17: CTA 5 do sistema analisado.....	74
Tabela 18: CTA 6 do sistema analisado.....	75
Tabela 19: CTA 7 do sistema analisado.....	75
Tabela 20: CTA 8 do sistema analisado.....	75
Tabela 21: Dados dos dispositivos de controle [96].....	76

Tabela 22: Modos de falha humana escolhidos para o modelo DFM.....	78
Tabela 23: PSF considerados no modelo DFM.....	78
Tabela 24: Outras variáveis do modelo DFM.....	78
Tabela 25: CTA 9 do sistema analisado.....	81
Tabela 26: CTA 10 do sistema analisado.....	81
Tabela 27: CTA 11 do modelo analisado.....	82
Tabela 28: CTA 12 do sistema analisado.....	83
Tabela 29: CTA 13 do modelo analisado.....	85
Tabela 30: CTA 14 do sistema analisado.....	86
Tabela 31: CTA 15 do modelo analisado.....	86
Tabela 32: CTR 2 do sistema analisado.....	87
Tabela 33: CTA 16 do modelo analisado.....	88
Tabela 34: CTA 17 do modelo analisado.....	88
Tabela 35: Lógica do evento topo de falha "Pressão Muito Alta".....	90
Tabela 36: Lógica do evento topo de falha "Pressão Muito Baixa".....	90
Tabela 37: Implicativos diretos do evento topo "Pressão Muito Alta".....	92
Tabela 38: Implicativos diretos do evento topo "Pressão Muito Baixa".....	93
Tabela 39: Implicativo #1 para quantificação pela ATHEANA.....	98
Tabela 40: Implicativo #2 para quantificação pela ATHEANA.....	98
Tabela 41: Implicativo #3 para quantificação pela ATHEANA.....	99
Tabela 42: Implicativo #4 para quantificação pela ATHEANA.....	99
Tabela 43: Pesos das opiniões dos especialistas consultados.....	105
Tabela 44: Intervalos <i>fuzzy</i> utilizados na coleta de opiniões.....	106
Tabela 45: Opiniões <i>fuzzy</i> agregadas.....	107
Tabela 46: Probabilidade <i>fuzzy</i> do HFE estudado.....	108
Tabela 47: Análise de importância de cada fator da quantificação ATHEANA.....	108

Tabela 48: Comparação dos dados de falha com dados da literatura.....	111
Tabela A.1: CTR 1 do sistema analisado.....	128
Tabela B.1: Histórico de pressão de uma usina PWR.....	132
Tabela C.1: Gráficos de probabilidade para a distribuição normal.....	133
Tabela C.2: Histograma de Pressão.....	135
Tabela C.3: Teste de aderência para a distribuição normal.....	136
Tabela D.1: Escala de valores para os contextos.....	139
Tabela D.2: Escala de valores para as ações inseguras.....	139
Tabela F.1: Opiniões dos especialistas acerca das probabilidades de contextos e ações humanas seguras.....	145
Tabela F.2: Pontuações dos especialistas obtidas através do formulário de perfil.....	147
Tabela F.3: Cálculo dos centroides das opiniões fuzzy.....	148
Tabela F.4: Cálculo dos índices de similaridade entre as opiniões dos especialistas.....	149
Tabela F.5: Índice de concordância médio calculado para cada especialista.....	153
Tabela F.6: Cálculo dos índices de concordância relativa entre os especialistas.....	155
Tabela F.7: Cálculo do índice de consenso entre as opiniões fuzzy.....	157

## LISTA DE SIGLAS

APS	ANÁLISE PROBABILÍSTICA DE SEGURANÇA
ATHEANA	A TECHNIQUE FOR HUMAN ERROR ANALYSIS
CCMT	CELL TO CELL MAPPING TECHNIQUE
CTA	CAIXA DE TRANSFERÊNCIA
CTR	CAIXA DE TRANSIÇÃO
DFM	DYNAMIC FLOWGRAPH METHODOLOGY
EFC	ERROR FORCING CONTEXT
EOC	ERROR OF COMMISSION
EOO	ERROR OF OMISSION
HFE	HUMAN FAILURE EVENT
HRA	HUMAN RELIABILITY ANALYSIS
LCA	LIGAÇÃO DE CAUSALIDADE
LCO	LIGAÇÃO DE CONDIÇÃO
NRC	NUCLEAR REGULATORY COMMISSION
PI	PRIME IMPLICANTS
PSF	PERFORMANCE SHAPING FACTORS
PWR	PRESSURIZED WATER REACTOR
PZR	PRESSURIZER
UA	UNSAFE ACT
VC	VARIÁVEL DE CONDIÇÃO
VP	VARIÁVEL DE PROCESSO

# 1 INTRODUÇÃO

Tendo em vista a crescente incorporação de sistemas digitais nas indústrias atuais, devido às suas inúmeras vantagens frente aos sistemas analógicos, percebeu-se a necessidade de uma abordagem específica do ponto de vista da confiabilidade e análise de riscos [1]. Isto porque um sistema digital reflete inúmeras interações entre *hardware*, *software*, variáveis de processo e ações humanas. Ao mesmo tempo, o *software*, elemento fundamental e característico de um sistema digital, não possui uma abordagem de confiabilidade bem definida [2], tal qual existe para os demais componentes físicos do sistema.

Concomitantemente, existe uma eminente preocupação com a existência de falhas humanas nas mais diversas plantas industriais [3-12]. Atualmente, sabe-se que estas falhas não podem ser tratadas separadamente do contexto onde os operadores estão inseridos. Sabe-se ainda que estas falhas não ocorrem de maneira aleatória, mas através de um processo cognitivo do ser humano podendo ser classificadas tanto em falhas de omissão ou enganos propriamente ditos [3, 6-9, 12].

A metodologia DFM (*Dynamic Flowgraph Methodology*) [13-22] é uma das que mais cumpre os requisitos para uma modelagem de sistemas dinâmicos (sistemas digitais, por exemplo). Ela consiste em retirar as variáveis de maior relevância do sistema analisado, discretizá-las em estados que reflitam seus comportamentos, estabelecer a lógica que as conecta através das chamadas tabelas de decisões, e por fim, realizar uma análise do sistema buscando-se, por exemplo, as causas raízes (implicativos diretos) de um evento topo de falha.

A técnica ATHEANA (*A Technique for Human Error Analysis*) [6, 23-26] corresponde a uma análise de falhas humanas estruturada. Integrante das chamadas técnicas de segunda geração [3, 6, 8-10], incorpora o processo cognitivo em sua

análise, lidando tanto com erros de omissão (ausência de resposta) quanto os chamados erros de comissão (resposta errônea) que ocorrem em um dado contexto da planta.

No que diz respeito à quantificação de falhas humanas, a elicitación de especialistas para a obtenção de informações, em situações onde os dados são escassos, está se tornando uma prática recorrente em trabalhos científicos [27-30]. Esta prática associada à teoria fuzzy [31-41] possibilita a manipulação de valores numéricos (probabilidades, por exemplo), através de variáveis linguísticas e relações matemáticas consolidadas, além da associação de incertezas à análise [42-47].

Para a realização do trabalho foi considerado um sistema digital de controle simplificado baseado no funcionamento do pressurizador (PZR) em usinas nucleares. No cenário proposto, as interações com o operador da central foram analisadas de maneira conjunta. O estudo se baseou na modelagem DFM e ATHEANA desse sistema de controle e na análise integrada das interações entre os componentes do sistema, o processo e o operador. A DFM realizou a etapa intermediária da ATHEANA de busca dos contextos de erro (combinações das condições da planta e dos fatores formadores do desempenho humano) que induzem as ações inseguras. Posteriormente, uma complementação dos resultados obtidos foi realizada através de coleta de opiniões de especialistas em conjunto com a teoria fuzzy.

O presente trabalho está estruturado da forma descrita a seguir.

O Capítulo 2 apresenta a revisão bibliográfica realizada na fase inicial do trabalho. No Capítulo 3 a metodologia DFM é apresentada em detalhes. No Capítulo 4 a ATHEANA é descrita. No Capítulo 5 a metodologia de elicitación de especialistas e a técnica de agregação de opiniões são apresentadas. O Capítulo 6 descreve o sistema de controle do pressurizador proposto. No Capítulo 7 encontra-se a modelagem DFM/ATHEANA do sistema proposto. O Capítulo 8 explicita os resultados obtidos na análise de falhas humanas do sistema. O Capítulo 9 complementa os resultados obtidos na análise do capítulo anterior utilizando as opiniões de especialistas e a teoria



fuzzy. O Capítulo 10 encerra o trabalho com as discussões, conclusões e recomendações.

## 2 REVISÃO BIBLIOGRÁFICA

### 2.1 O SOFTWARE EM SISTEMAS DIGITAIS

Muitas das plantas atuais estão substituindo seus sistemas de instrumentação e controle analógicos por sistemas de tecnologia digital. Estes sistemas são compostos por dispositivos físicos (*hardwares*), rotinas ou *softwares* executados em um microprocessador e dispositivos de instrumentação, como sensores e atuadores. Os principais motivos para esta substituição são os ganhos em flexibilidade, custos, e confiabilidade proporcionados por sistemas orientados a *software*. Esses ganhos decorrem do fato da programação possuir alta capacidade de modificação/manutenção sem a necessidade de substituições e conseqüentemente gastos adicionais, o que não é verdadeiro em malhas analógicas. Além disso, uma vez que o *software* é completamente depurado, não existe a possibilidade de envelhecimento e, portanto, ele continuará a executar as suas funções por tempo indeterminado.

Todavia, não existe um programa perfeito. Seu processo de desenvolvimento pressupõe falhas humanas de implantação, falhas de documentação e erros de caráter cognitivo. Nesse sentido, é necessária uma abordagem de confiabilidade que modele o comportamento de aplicativos. Segundo [48], confiabilidade de *software* é a probabilidade de que um programa ou rotina não irá causar uma falha por um determinado período de tempo e sob determinadas condições. Esta probabilidade é função de seus parâmetros de entrada e de seu uso, bem como da existência de *bugs* no código do programa. Em outras palavras, a confiabilidade de *software* é ligada ao contexto em que ele está inserido, ou seja, ao sistema e/ou ambiente externo que geram entradas para ele. Diferentemente da abordagem clássica para componentes físicos, *hardwares*, por exemplo, o *software* não se deteriora com o tempo, pelo

contrário, através do processo de depuração espera-se que sua incidência de falhas diminua (desde que não haja reprogramação no código e conseqüentemente introdução de novos *bugs*). Existe uma dependência temporal na confiabilidade, na medida em que, com o uso contínuo do *software*, espera-se que o mesmo execute gradualmente seus módulos e com isso possibilite a descoberta de falhas que até então não eram reveladas. No entanto, não se sabe ao certo quando um determinado módulo do *software* irá ser executado e, por isso, esta dependência temporal não é bem definida. Enquanto as reduções de custos e flexibilidade proporcionadas por sistemas orientados a *software* são vastamente reconhecidas, sua análise de confiabilidade ainda se encontra em fase de desenvolvimento devido às dificuldades decorrentes da complexidade, flexibilidade e interações presentes em tais sistemas.

Diversas abordagens estão evoluindo no campo da confiabilidade de *softwares* [9, 37, 49-52]. Uma abordagem consiste em rastrear todos os possíveis erros do sistema digital via metodologias dinâmicas, buscando aqueles erros que têm como causa raiz uma falha de aplicativo em conjunto com determinadas condições externas. Em seguida, calculam-se as probabilidades condicionais do *software* falhar dadas aquelas condições e, juntamente com as probabilidades de ocorrência das mesmas, encontra-se a probabilidade de falha do programa. Finalmente, determinam-se os riscos, criticalidades e propõem-se modificações mitigadoras [2, 53].

Percebe-se então, segundo esta abordagem, a necessidade de se estudar a confiabilidade de um programa computacional segundo uma visão holística do sistema e ambiente em que ele está inserido, ou seja, uma visão que englobe informações de todas as outras variáveis do sistema digital que interagem com o *software*. Esta visão não se restringe somente a componentes físicos, ela extrapola os limites organizacionais do estudo da confiabilidade de sistemas digitais críticos de segurança e controle. Dado que os componentes destes sistemas dinâmicos interagem entre si, com as variáveis de processos e com seres humanos, há uma necessidade na análise de segurança de se integrar especialistas de todas as áreas no estudo da

confiabilidade [53]. Todos os profissionais devem prover informações de suas áreas na modelagem do sistema e discutir os resultados de maneira conjunta.

## 2.2 CONFIABILIDADE DE SISTEMAS DIGITAIS

Os sistemas digitais diferem dos analógicos em diversos aspectos, vantajosos ou não [1]:

- Sistemas digitais trabalham com lógicas flexíveis e expansíveis, enquanto sistemas analógicos possuem uma lógica fixa;
- *Softwares* não possuem condições de estresse ligadas a fatores externos e, por isso, não podem ser modelados através das técnicas convencionais de confiabilidade de componentes/equipamentos;
- Sistemas digitais operam com discretizações de variáveis enquanto sistemas analógicos trabalham em tempo contínuo;
- Erros de *software* podem permanecer não-revelados por um longo período de tempo. Há ainda a possibilidade de introdução de novos modos de falha através da reprogramação no decorrer dos anos;
- Sistemas digitais introduzem erros de truncamento e arredondamento devido às suas aproximações;
- Estes sistemas compartilham dados, funções e equipamentos, o que melhora os seus desempenhos, mas os deixam altamente propensos às falhas de causa comum.

A abordagem tradicional de confiabilidade com a utilização de árvores de falhas possui um caráter estático, não contemplando as interações dinâmicas presentes em tais sistemas, como atrasos de sensoriamento e processamento, informações de

memória, *loops* de lógica, antecipações de estado, etc. Portanto, há a necessidade de se encontrar uma metodologia de confiabilidade que leve em consideração estes aspectos sem deixar de lado as exigências já existentes na análise de segurança.

Para a modelagem de sistemas dinâmicos, os requisitos abaixo precisam ser atendidos [1]:

1. O modelo deve prever falhas futuras;
2. O modelo deve cobrir as particularidades referentes ao sistema em questão;
3. Se for o caso, o modelo deve realizar suposições válidas e plausíveis e as consequências das violações destas suposições devem ser identificadas;
4. O modelo deve representar quantitativamente e com precisão as dependências entre eventos de falha;
5. O modelo deve ser projetado de tal maneira que não seja difícil que um analista aprenda seus conceitos e os implante;
6. Os dados usados no processo de quantificação devem ser verdadeiros;
7. O modelo deve ser capaz de distinguir falhas de causa comum;
8. O modelo deve ser capaz de distinguir erros que causem falha de função e falhas intermitentes;
9. O modelo deve prover informações relevantes aos usuários, como cortes mínimos, probabilidade de falhas e incertezas associadas aos resultados;
10. A metodologia deve possibilitar a incorporação dos resultados em relatórios existentes na análise probabilística de segurança;
11. O modelo não deve requerer um elevado número de informações sobre o estado da planta.

Metodologias dinâmicas encontradas na literatura foram consultadas a fim de se verificar o cumprimento dos requisitos. As indicadas para a modelagem de sistemas digitais são [1]:

- Markov/CCMT (*Cell-to-Cell Mapping Technique*) – Consiste em discretizar as variáveis de processo e calcular as suas probabilidades de transição, definir os estados de cada componente do sistema digital e suas respectivas probabilidades e por fim realizar o cálculo da probabilidade de falha do sistema através de matrizes de transição das variáveis do modelo [14, 54-56].
- DFM – Representação discreta do sistema de controle e do processo controlado tendo as relações de causalidade entre as suas variáveis relacionadas na forma de tabelas dinâmicas [13-22, 57-58].
- Metodologia bayesiana – Representa a estrutura e funcionamento de *softwares* através de um modelo bayesiano. Baseia-se em percorrer todos os caminhos possíveis do *software*, atualizando seus dados de falhas e confiabilidade [59].
- Redes de Petri – É um modelo gráfico de representação do sistema digital, utilizando os mesmos princípios de transições de estados utilizados na abordagem clássica de sistemas operacionais [60].
- Metodologia de testes – Consiste em executar inúmeros testes e verificar falhas ou não em *softwares* [61].
- Metodologia baseada nas regras de desenvolvimento de *softwares* – Consiste em aproximar a confiabilidade de um programa em um sistema digital baseado na maneira como ele foi programado e como ele seguiu as regras de desenvolvimento [62].
- Metodologia Black-Box – Uso de um processo não-homogêneo de Poisson para predizer, indiretamente, a confiabilidade de sistemas através da modelagem da confiabilidade de *softwares* [63].

Baseado em uma análise comparativa das metodologias e de seus exemplos encontrados na literatura, a Ref [1] enxerga, nas modelagens, algumas vantagens e dificuldades:

- Markov/CCMT (*Cell-to-Cell Mapping Technique*) – Capaz de realizar uma boa modelagem das interações do sistema de controle e processo controlado, mas sua análise demanda um volume muito grande de dados de falha e sua modelagem tende a se tornar muito complexa. Seus resultados podem ser incorporados às análises probabilísticas de segurança.
- DFM – Realiza uma boa modelagem das interações do sistema de controle com as demais variáveis através de tabelas verdade dinâmicas. Seus resultados podem ser incorporados às análises probabilísticas de segurança.
- Metodologia bayesiana – É capaz de incorporar novos valores de falhas durante sua análise de confiabilidade, porém não enxerga de maneira holística as dependências entre falhas.
- Redes de Petri – Modela bem as interações do sistema de controle, porém o tamanho do modelo pode tomar dimensões inviáveis.
- Metodologia baseada nas regras de desenvolvimento e testes em *softwares* – Seus resultados podem ser incorporados às análises probabilísticas de segurança, mas só pode ser utilizado em *softwares* (excluindo os demais componentes do sistema digital) e só pode ser aplicada na fase de desenvolvimento do *software*.
- Metodologia Black-Box – Requer um volume de informações muitas vezes indisponível. Além disso, os resultados da análise não podem ser incorporados em APS.

Não há uma regulamentação e uma metodologia escolhidas até o presente momento. Deste fato, decorre a importância da análise comparativa dos métodos propostos. Nenhum método satisfaz todos os requisitos apresentados para uma modelagem de sistemas dinâmicos. Baseado em uma análise subjetiva e da experiência acumulada e reportada na literatura [1], as metodologias DFM e Markov são as que atendem ao maior número dos requisitos, cada uma com diferentes vantagens e limitações. Enquanto a DFM parece ser a metodologia preferida, ainda não está claro se ela realiza de maneira correta a análise das interações dinâmicas presentes em sistemas digitais, devido ao fato de não trabalhar com o tempo exato de falhas e sim através de discretizações do tempo. Tais problemas podem ser evitados na modelagem Markov/CCMT, mas a obtenção de dados de falha pode ser problemática para o modelo desenvolvido através desta metodologia. Os modelos de Markov/CCMT requerem um volume de informação muito grande, o que em muitos casos, não torna prática a sua utilização.

Outra característica importante que as metodologias propostas devem considerar é a possibilidade de incorporação de seus resultados às análises probabilísticas de segurança, uma vez que ainda existem diversos sistemas analógicos coexistindo com a instrumentação digital em plantas atuais. Por isso, a Ref [1] propõe como trabalho futuro, o estudo de um sistema *benchmark* utilizando as duas metodologias para fins de comparação.

Assim sendo, um sistema digital de controle da água de alimentação do gerador de vapor de um reator PWR foi proposto como *benchmark* de comparação das metodologias [14, 17, 57]. Este sistema tem por finalidade manter o nível de água do gerador de vapor dentro da faixa de operação através de uma bomba e válvulas de controle. O comportamento dinâmico de seus parâmetros foi modelado através de simulações. Os dados de falha foram obtidos através de um histórico operacional.



As duas metodologias propostas foram aplicadas a esse sistema e seus resultados foram muito semelhantes qualitativa e quantitativamente [14, 17]. A DFM não apresentou precisão do exato instante de ocorrência dos eventos, mas demonstrou possuir um alto nível de detalhamento das interações do sistema e de seus componentes. A metodologia Markov/CCMT é mais rica em informações acerca do tempo exato das falhas.

Por fim, concluiu-se que os dois métodos possibilitam a transferência de resultados para análises de segurança existentes. A metodologia Markov/CCMT necessita de uma etapa intermediária para a incorporação de seus resultados, o que não ocorre com a DFM [14, 17]. A utilização do *software* SAPHIRE foi proposta como plataforma de incorporação destes resultados [14, 17].

Baseada na vasta aplicação encontrada na literatura, modelagem simplista, análise sistêmica, chancela da NRC e acessibilidade ao método, a DFM foi escolhida como objeto de estudo deste trabalho. Ela é detalhada no Capítulo 3.

## **2.3 ANÁLISE DE FALHAS HUMANAS**

Como visto, a confiabilidade dos sistemas atuais envolve diversas interações entre os componentes do sistema, *hardware*, *software*, instrumentação, organização e operadores. Estudos recentes demonstram que é grande a contribuição humana para a falha destes sistemas [3-4, 6, 11-12, 64-73]. A Figura 1 ilustra este fato. Na Ref [3] é possível encontrar uma extensa discussão sobre diversos acidentes ocorridos nas mais diversas áreas, frutos de falhas humanas.

Uma das explicações para o crescimento da participação do homem em acidentes é que ao longo dos anos a confiabilidade dos demais componentes físicos evoluiu muito mais do que a confiabilidade humana. Isto explica o surgimento de técnicas de análise de falha humana, ou *Human Reliability Analysis (HRA)*, que

estudam o comportamento humano, nas diversas organizações e plantas industriais de maneira qualitativa e quantitativa [3, 9, 12].

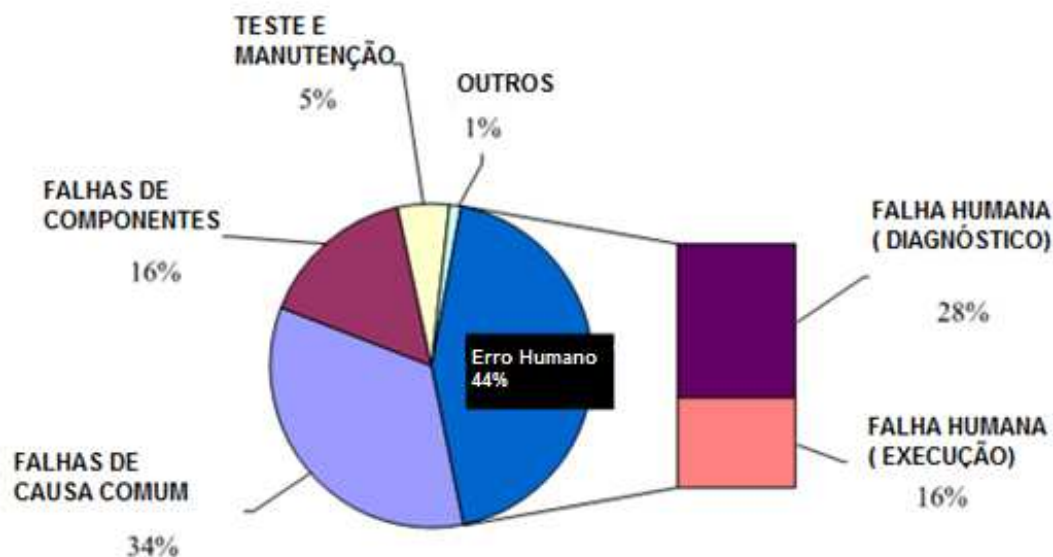


Figura 1: Contribuição humana para a frequência de dano ao núcleo [72]

No início, essas técnicas expunham o conceito de que a falha é o resultado da deficiência do ser humano em realizar determinadas ações, ocorrendo de maneira aleatória. O contexto, ambiente e organização onde o ser humano está inserido somente seria levado em consideração como fator modificador da probabilidade de ocorrência destas ações. Estes conceitos fazem parte das chamadas técnicas de primeira geração [3, 7, 9, 12, 38, 65, 67, 70, 74-75]. Posteriormente, este conceito foi sendo deixado para trás à luz de uma nova ideia. O histórico de acidentes deixou claro que o contexto imprime a maior importância à ocorrência de falhas humanas, determinando o tipo de tarefa que será executada (ou omitida), bem como a sua frequência de ocorrência. O processo cognitivo (busca da informação, interpretação, tomada de decisão e execução) deve ser considerado. Estes conceitos fazem parte das chamadas técnicas de segunda geração [3, 7, 9-10, 12, 38, 65, 67, 70, 74, 76-77].

Estas técnicas ainda estão em desenvolvimento. A escolha de uma HRA específica ainda não é trivial, sendo necessário um número maior de estudos comparativos e de validação [12, 74, 78-79]. Estes estudos devem considerar, de maneira dinâmica, as interações entre o operador e os demais elementos da planta [3, 7, 9, 11, 12, 66, 68-69].

Em [68] são apresentadas as boas praticas para uma análise eficiente de falhas humanas. Neste estudo, fazem-se recomendações para a identificação dos diversos tipos de ações de operadores.

As Refs [3, 11, 64-65, 68-69, 80] mencionam a importância dos fatores humanos em uma usina nuclear, abordando os três tipos de falhas humanas (Figura 2): falhas relacionadas a eventos pré-iniciadores (falhas do tipo A), como por exemplo, manutenções imperfeitas; falhas relacionadas a eventos iniciadores (tipo B), como acionamentos indevidos e falhas relacionadas a eventos pós-iniciadores (tipo C) como ações de recuperação executadas de maneira errônea ou simplesmente não executadas.

Na Ref [64] é mencionada a importância de cada um destes tipos de ações no histórico de acidentes existente e são relatadas medidas de prevenção para a não-ocorrência das mesmas. Na Ref [73] é investigado um método original de quantificação de falhas de manutenção (pré-iniciadoras). Na Ref [68] são explicitadas as boas práticas que devem ser encontradas em qualquer HRA e as recomendações na identificação e quantificação dos três tipos de falhas. A Ref [11] investiga extensivamente, em diversas fontes da literatura, os tipos de tarefas que podem vir a ser executadas erroneamente ou não executadas, ordenando-as com relação às suas contribuições para a confiabilidade da planta.

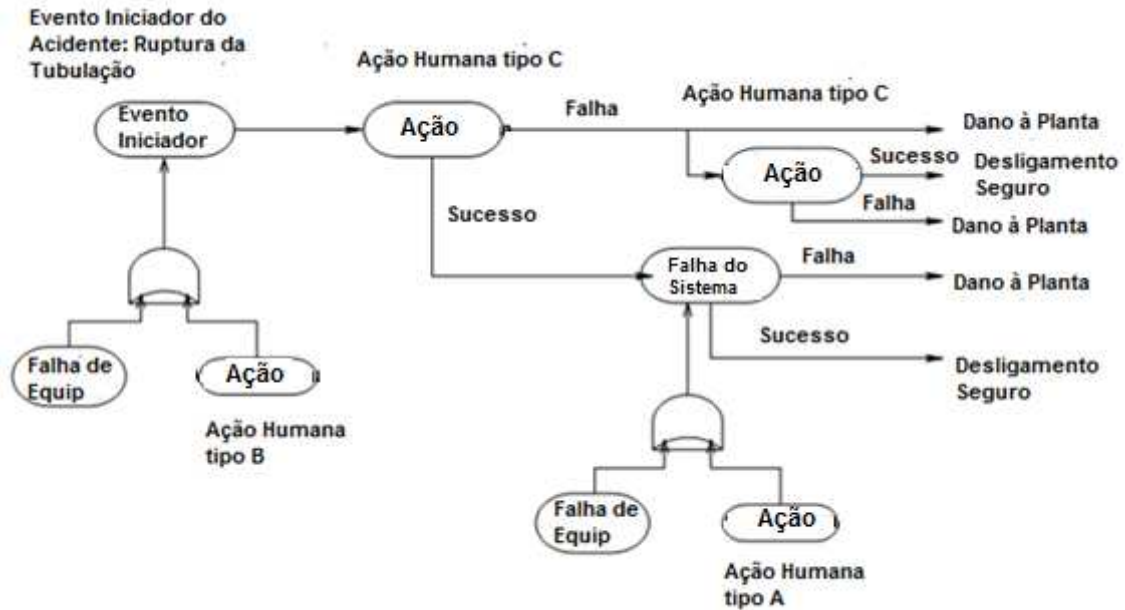


Figura 2: Tipos de ações humanas [3]

Em [3-4, 6, 11-12, 69, 75] possíveis causas para esses erros como fadiga, emocional, drogas, falta de habilidade, condições adversas de trabalho e instrumentação, etc, são mencionadas e estudadas. Estas causas são chamadas de fatores formadores do desempenho humano (*Performance Shaping Factors, PSF*).

Em [79] são estudadas as dependências entre diferentes PSF. Em [3] e [6] as dependências entre falhas humanas são apontadas como primordiais em uma análise de HRA. Estes trabalhos abordam as interações entre um grupo de operadores e entre as ações de um mesmo operador. A Ref [65] realiza uma classificação das HRA existentes na literatura (Figura 3). A Figura 4 ilustra HRA fundamentadas em tipos de tarefas, HRA baseadas em relações temporais e HRA fundamentadas nos contextos que cercam os operadores. A escolha de uma HRA varia dentre critérios como o tipo de dados que irá se utilizar até a complexidade da planta em estudo, tendo suas vantagens e desvantagens discutidas em [3].

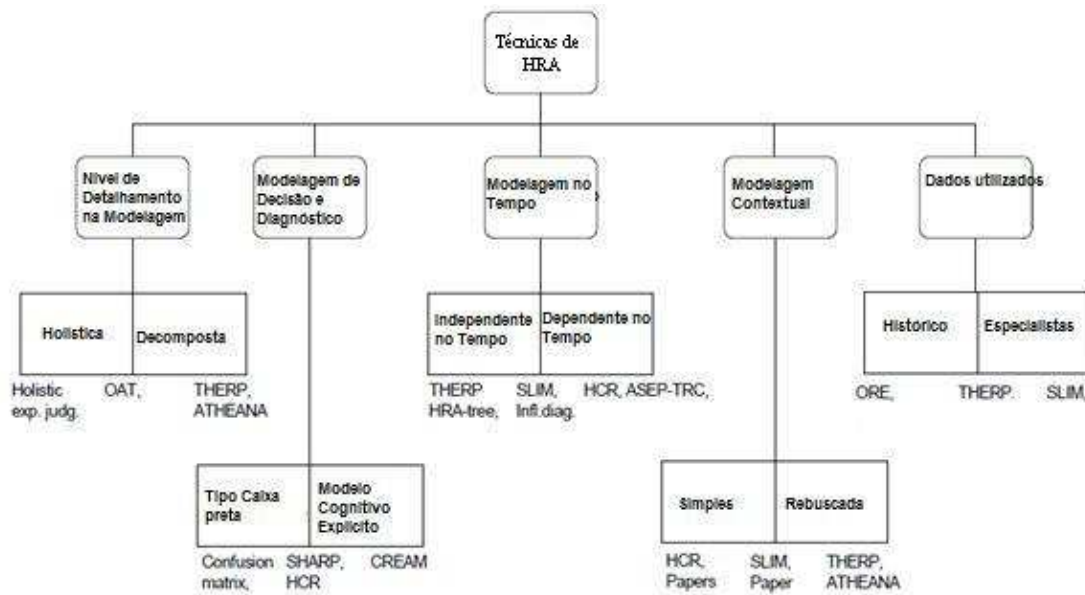


Figura 3: Classificação de diversas HRA [65]

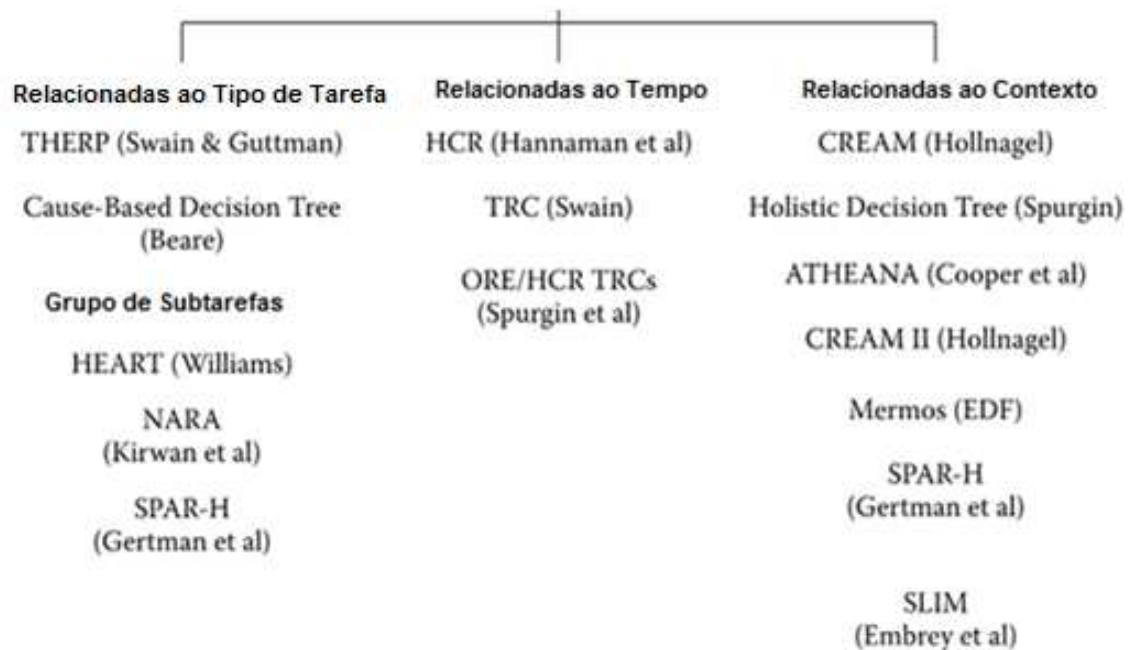


Figura 4: Classificação das HRA por tipo de análise [3]

A quantificação é quase um assunto à parte no âmbito das técnicas de análise de falhas humanas. As HRA de primeira ou segunda gerações possuem um esquema próprio de quantificação [6-7, 12, 75]. Algumas necessitam do apoio de outras HRA (NARA e CREAM, por exemplo) [12]. Em todas elas é explicitada a dificuldade de se abordar a confiabilidade de maneira quantitativa, motivo pelo qual até hoje existem discussões acerca do tema.

Uma das formas de se obter resultados quantitativos é através da opinião de especialistas. Na obtenção destas opiniões, cuidados especiais devem ser tomados na escolha dos participantes, documentação, número de participantes, elaboração de questões, etc. Devem ser utilizados tanto especialistas em confiabilidade humana como especialistas de operação da planta [3, 67].

As técnicas devem se preocupar com os dados utilizados para a quantificação. Atualmente, existem diversas fontes para as técnicas [3, 67, 71-72, 78-79, 81]:

- Dados operacionais (NUCLARR, CORE-DATA, OPERA );
- Simulações;
- Opiniões de especialistas.

Os bancos de dados operacionais não estão atrelados a nenhuma técnica específica, podendo ser utilizados se a planta em questão não possuir um histórico de falhas suficiente. Resultados de simulações também podem ser utilizados. Estes últimos têm grande importância qualitativa na identificação de falhas e contextos, porém sua abordagem quantitativa ainda é duvidosa. Opiniões de especialistas são úteis em identificar tanto fatores formadores do desempenho humano quanto em estimar probabilidades de falhas de ações. Também são grandes provedores de dados em plantas com pouco histórico [3].

Na Ref [81] é ilustrado como a base de dados OPERA de confiabilidade humana foi desenvolvida através de simulações. Nas Refs [8] e [82] diversas

simulações são realizadas com a finalidade de validar os resultados quantitativos advindos de HRA. Na Ref [10] a técnica de segunda geração CREAM é modificada e utilizada para estimar probabilidades de falha para o comportamento humano.

Ainda sobre as HRA, de primeira e segunda geração, são encontrados estudos comparativos e descritivos na literatura, abordando os pontos negativos e positivos de cada técnica [3, 7, 12, 65, 80]. Na Ref [7] por exemplo, uma extensa pesquisa levou a 72 técnicas encontradas no âmbito da confiabilidade humana. Destas 72, 35 foram consideradas de grande relevância e 17 com grande potencial de aplicabilidade, segundo critérios de validação, número de referências, número de aplicações, vantagens e desvantagens, etc. As técnicas são explicitadas segundo um esquema bastante completo: origem, descrição, estudos de validação, campo de aplicação, disponibilidade de *tool/sets*, referências, prós e contras, etc, sendo assim um bom ponto de apoio no estudo de HRA.

Na Ref [12] foi estabelecido um método de estudo e classificação das muitas HRA permitindo uma extensa pesquisa das mesmas além de diversas conclusões. Neste estudo, as técnicas são classificadas segundo seus princípios de modelagem, método de aplicação e esquema classificador. O estudo ainda enfoca a principal diferença entre as técnicas de primeira e segunda gerações.

A necessidade de representação das ações humanas em APS existentes influenciou o pensamento de que elas ocorrem de maneira aleatória, podendo ser executadas ou não, quando demandadas. Quando não executadas, estas falhas são denominadas erros de omissão (EOO) [3, 11-12, 68]. Porém, o ser humano é influenciado pelo meio (contexto) que o cerca, podendo realizar ações errôneas quando assim achar conveniente (utilizando-se de um processo cognitivo [3]). Sendo assim, ele não se comportaria como um “equipamento”, agindo somente quando solicitado. As ações humanas errôneas que possam vir a ocorrer são chamadas de erros de comissão (EOC) [3, 11-12, 68, 76] e compõem a filosofia das técnicas de segunda geração. A Figura 5 ilustra o comportamento da frequência de dano ao

núcleo em função do tipo de falha humana. Fica clara a importância dos chamados erros de comissão (EOC).

Além disso, há a necessidade de se verificar métodos de incorporação dos resultados em APS existentes [3, 12, 67-68, 71, 77]. A Figura 6 ilustra isso. Após o estabelecimento da sequência de acidentes envolvendo falhas de sistema e falha humanas, faz-se necessária a estimativa das frequências e consequências destas sequências para a efetiva incorporação.

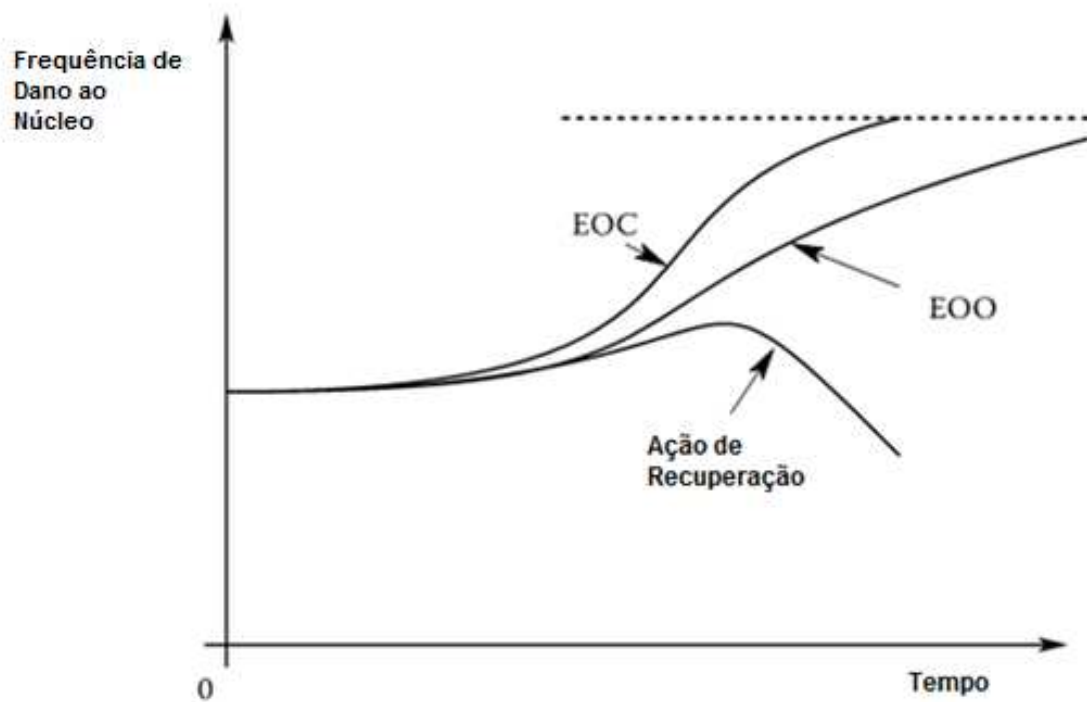


Figura 5: Evolução do dano ao núcleo após um incidente em função dos tipos de ações humanas [3]



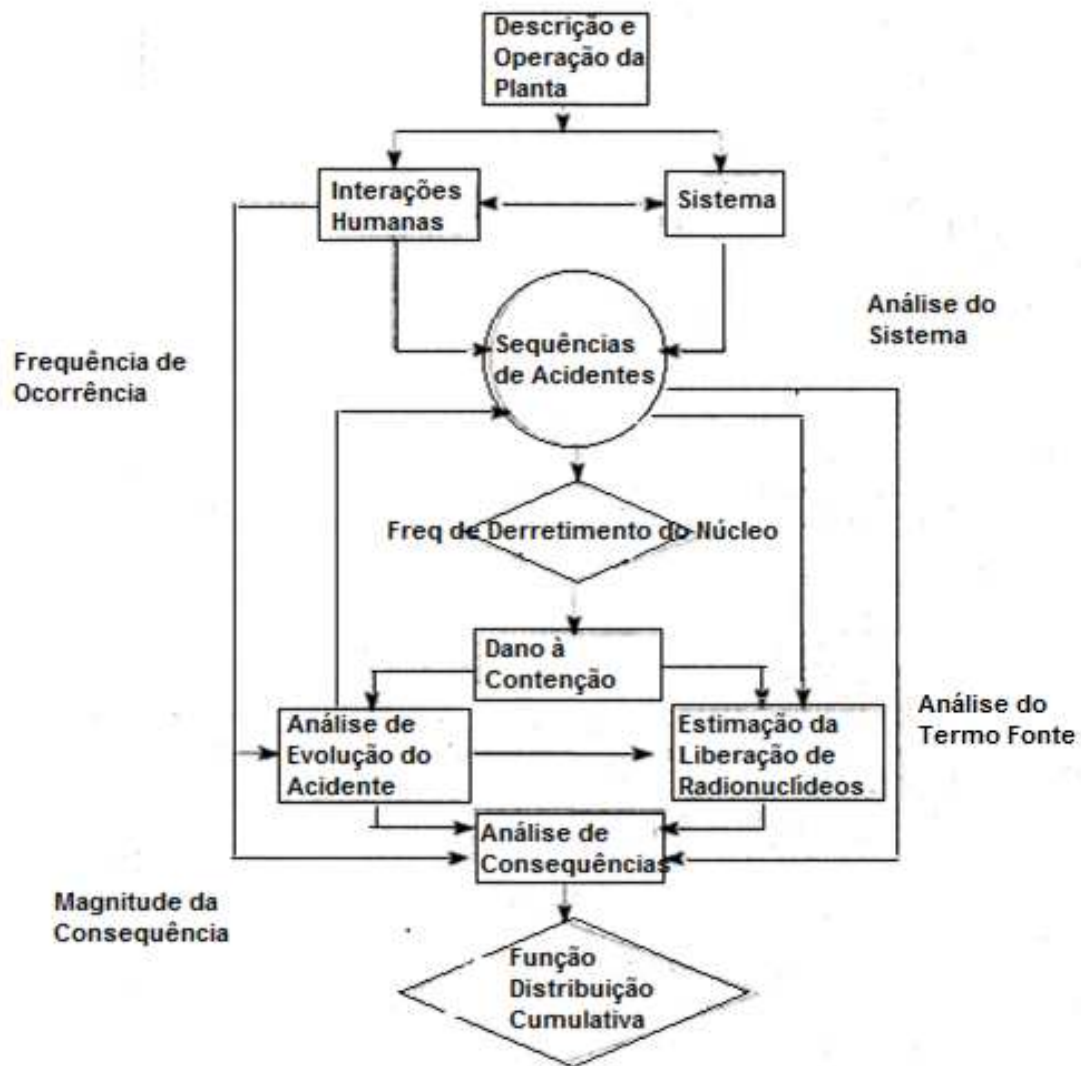


Figura 6: Necessidade de incorporação dos resultados de uma HRA em uma APS [71]

A Ref [12] aponta as técnicas de segunda geração como as mais aptas a abordar os erros de comissão. Uma destas técnicas chama-se ATHEANA (*A Technique for Human Error Analysis*).

A ATHEANA é indicada pela NRC para o estudo da confiabilidade humana. Ela se destaca pela modelagem das interações entre o operador e o contexto onde ele está inserido. Além disso, existe a possibilidade de incorporação dos resultados às APS existentes. A ATHEANA começa com a identificação de eventos de falha humana (*HFE*), representando o evento básico da APS relacionado à perda de função de um componente/sistema. Após, ações inseguras (*UA*), são identificadas como as ações

responsáveis pela ocorrência dos HFE. Em seguida, os contextos nos quais estas ações acontecem são discriminados. Os contextos (*EFC*) são combinações de condições específicas da planta e fatores formadores do desempenho humano, tais como fadiga, estresse, ruído, instrumentação, etc. Ao final, todos esses fatores são levados em conta de maneira dependente na quantificação das probabilidades de ocorrência dos HFE. A quantificação é realizada através da opinião de *experts* seguindo os princípios expostos acima [3, 6, 23, 67].

Diversos trabalhos foram produzidos acerca da ATHEANA, muitos deles sob a chancela da NRC [6, 24-26, 83-84]. O intuito destes trabalhos foi o de disseminar os conceitos da técnica, exemplificando sempre que possível a sua aplicação.

A ATHEANA é uma técnica que considera os erros de comissão e de omissão explicitados. Ela modela o comportamento humano através de um modelo cognitivo de processamento da informação em quatro etapas: monitoração, entendimento da situação, planejamento e execução [6, 11]. Além disso, ela considera as interações entre os diversos componentes da planta e se preocupa em realizar uma integração entre a HRA e a APS. Por estes motivos e pela chancela da NRC, esta técnica foi utilizada no trabalho no âmbito da confiabilidade humana. Ela é detalhada em seu guia [6] e no Capítulo 4.

## 2.4 COLETA DE OPINIÕES

A Ref [28] cita que lidar com a complexidade e incertezas de sistemas exige a participação de *experts*. A necessidade da opinião de especialistas surge de diversas formas: quando não existem dados suficientes para se estabelecer uma quantificação ou quando o assunto em questão é recente ou ainda quando lidamos com incertezas na análise. Especialistas atuam na área de meteorologia, política, finanças, etc, e são fontes valiosas de informação [28-29]. Um especialista é definido como uma pessoa qualificada e com muita experiência em um determinado assunto responsável por fornecer respostas às questões levantadas [29]. Candidatos a especialistas são: pesquisadores, cientistas e engenheiros com competência na área de estudo, disponibilidade de participação e com habilidades de comunicação [4, 28].

O número de participantes não é fixo, porém deve ser o suficiente para garantir a diversidade e credibilidade das opiniões [4, 28]. A Ref [29] cita as vantagens das elicitções em grupo e os cuidados que se deve ter em convocar um número maior de participantes frente aos imprevistos que possam vir a ocorrer. É essencial selecionar pessoas com conhecimentos de engenharia básica, tecnologia, operação, manutenção e risco [28].

A presença de um integrador de opiniões é necessária para a condução do processo de elicitção. O integrador é responsável por selecionar os participantes, contatá-los, prover a descrição do assunto, descrever o processo de elicitção, elaborar o questionário, coletar as opiniões e escolher o método de agregação dos resultados [28].

Na elaboração das questões, diversos cuidados devem ser tomados para a construção de um bom questionário, pois a negligência dos participantes pode gerar sérios problemas na acurácia dos resultados. Deve ser elaborada uma introdução com uma breve descrição do processo. As questões devem ser claras, sem ambiguidades,

sem negativas, sem abreviações, curtas, sem tendências, seguindo um sequenciamento lógico [4, 28-29]. As questões podem ser abertas ou fechadas. Os dados podem ser numéricos ou linguísticos [4, 28, 85]. O questionário não deve conter informações de maneira desordenada e deve conter campos para as observações. A Ref [85] apresenta procedimentos de teste e revisões dos questionários bem como exemplos de erros mais comuns encontrados em trabalhos na literatura.

As questões devem ser enviadas aos participantes com antecedência, evitando assim que imprevistos no decorrer do processo atrapalhem a obtenção dos resultados. Caso necessário, treinamentos devem ser realizados com os especialistas para a estimação de parâmetros estatísticos [4, 27, 28].

Na elicitación, um processo heurístico é realizado pelo participante, passando pela compreensão da questão, busca pelas evidencias/fatos, estimação e resposta. (28) (85). A forma de contato pode variar do envio de emails a telefonemas e entrevistas, cada uma com suas vantagens e desvantagens [85].

Após a elicitación, o método de agregación escolhido deve ser aplicado e os resultados analisados. Durante todo o processo, a documentação deve ser realizada e os registros preservados [28].

Muitos estudos utilizando as opiniões de especialistas [4-5, 30, 37-39] são encontrados na literatura. Na Ref [4], encontra-se o processo de coleta de opiniões acerca de falhas humanas em procedimentos de radioterapia com a utilização conjunta de redes bayesianas. Neste estudo, 8 passos para o processo de elicitación foram definidos: seleção das questões, seleção de especialistas, treinamento do método de elicitación, apresentação das questões, elicitación propriamente dita, crítica dos dados, cálculo das probabilidades e documentação. Os resultados serviram para identificar as falhas humanas de maior importância ocorridas em radioterapia. Neste trabalho, as dificuldades do processo são explicitadas, porém sua utilidade é evidenciada.

Na Ref [30] foi desenvolvido um trabalho com opiniões de *experts* acerca da estimação de probabilidades de ataques cardíacos em seres humanos. Neste trabalho foi desenvolvida uma ferramenta computacional para a agregação de opiniões e estimação de distribuições de probabilidade. Os questionários foram enviados por email aos participantes. Em suas observações, o estudo também enfatiza as dificuldades no processo de obtenção das respostas.

Nas Refs [5, 37-39], o processo de coleta de opiniões é combinado com a teoria fuzzy [31-36] cujos princípios são explicitados na seção seguinte. Em [38-39] as opiniões tratam da confiabilidade humana em ensaios não-destrutivos nas mais variadas plantas industriais. Diversos PSF e probabilidades de falha de ações humanas são estimadas através de variáveis lingüísticas (utilizando os princípios da teoria fuzzy para o tratamento de incertezas). Por fim, essas opiniões são agregadas considerando o peso da opinião de cada especialista. Nas conclusões, estes trabalhos enfatizam que o processo de coleta de opiniões e escolha de participantes pode ser alvo de estudos adicionais.

Na Ref [5] é apresentado um trabalho similar acerca da influência dos PSF na estimação de probabilidades de falhas humanas em plantas nucleares. Novamente, opiniões de especialistas foram coletadas seguindo a teoria fuzzy e considerando o peso da opinião de cada participante. O principal objetivo do trabalho foi o de estimar probabilidades de falhas humanas para a incorporação em APS existentes. Conclusões acerca de melhoria nos procedimentos e nas condições da planta foram obtidas neste estudo.

Na Ref [37], a mesma linha de raciocínio foi retomada avaliando agora atributos de confiabilidade em softwares.

No presente estudo as recomendações encontradas na literatura [4, 28, 85] acerca da elaboração de questionários, planejamento de trabalho, formas de contatação dos *experts*, diversidade e número de opiniões foram consideradas. 6 dos 8 passos derivados do estudo da Ref [4] foram utilizados, considerados o mais

relevantes ao processo. A sistemática é descrita na seção 5.1. A experiência da utilização de variáveis linguísticas (linguagem natural do ser humano) como instrumento de coleta das opiniões e da utilização dos conceitos da teoria dos números fuzzy (descritos na seção seguinte) no tratamento das incertezas epistemológicas [38-39] foi utilizada na elaboração dos questionários, constante na fase final trabalho.

## 2.5 A LÓGICA FUZZY

A lógica fuzzy foi proposta primeiramente para tratar a complexidade, imprecisões e não-linearidades de sistemas de maneira otimizada [31]. Ela representa as incertezas, possibilidades e aproximações do conhecimento humano presentes nas variáveis, através do uso de variáveis linguísticas e informações qualitativas, ao contrário da lógica tradicional. Nesta última, uma variável pode pertencer ou não a um determinado conjunto. Na lógica fuzzy, uma variável pode pertencer a  $n$  conjuntos com diferentes graus de pertinência.

No parágrafo seguinte, são descritos os princípios básicos desta lógica. Estes princípios estão ilustrados na Figura 7. Aprofundamentos neste assunto são encontrados em [31].



Figura 7: Etapas da lógica Fuzzy [35]

Na lógica fuzzy, uma variável recebe um tratamento linguístico bem como os valores atribuídos a ela. Deste fato, decorrem as vantagens de se utilizar esta técnica para o tratamento de opiniões de especialistas e suas incertezas associadas em tomada de decisão [32, 35-39]. O primeiro passo da técnica é a fuzzyficação. Ela consiste em transformar um determinado valor numérico em uma variável fuzzy com um grau de pertinência associado. A Figura 8 ilustra este procedimento.

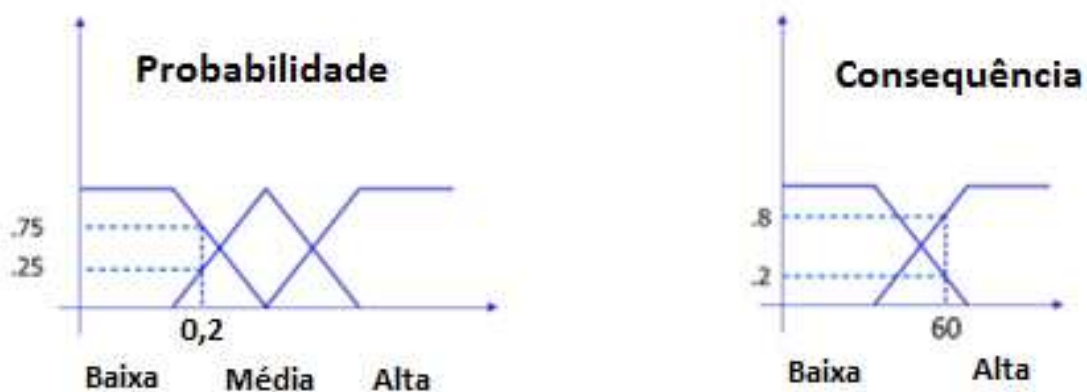


Figura 8: Processo de fuzzyficação

Neste exemplo a variável “Probabilidade”, com o valor de 0,2, é considerada “Média” com 0,25 de pertinência e “Baixa” com 0,75 de pertinência. A variável “Consequência”, com o valor de 60 mortes, é considerada “Alta” com 0,8 de pertinência e “Baixa” com 0,2 de pertinência.

O próximo passo da lógica consiste na ativação das regras definidas pelos especialistas. Este fato mostra o porquê desta lógica ser aplicada em tomada de decisões e sistemas de controle, por exemplo. As regras assumem a seguinte forma:

**IF A = Média e B = Alta THEN C = Alto**

**IF A = Baixa e B = Baixa THEN C = Baixo**

Na ativação das regras, são utilizados algoritmos de inferência, sendo o algoritmo de Mandani o mais comum [31]. Neste algoritmo, as implicações retornam o menor grau de pertinência das variáveis e o grau de pertinência para a variável de saída é o maior grau de pertinência encontrado nas implicações. Exemplo: se A é “Média” com 0,4 de pertinência e “Baixa” com 0,6 e se B é “Alta” com 0,3 de pertinência e “Baixa” com 0,7, as regras abaixo são ativadas:

**IF A = Média e B = Alta THEN C = Alto**

**IF A = Baixa e B = Alta THEN C = Baixo**

**IF A = Média e B = Baixa THEN C = Alto**

**IF A = Baixa e B = Baixa THEN C = Alto**

Na primeira regra, o grau de pertinência para a variável C é 0,3 por ser o menor dentre A e B. Na segunda regra, a variável C é “Baixo” com grau de pertinência de 0,3 também. Na terceira regra, o grau de pertinência resultante é de 0,4. Na quarta e última regra o grau de pertinência resultante é de 0,6. Como na primeira, terceira e quarta regras a variável C resulta em “Alto”, esta variável assume o maior valor de pertinência segundo o algoritmo de Mandani, ou seja, 0,6. O resultado final é: C = (Baixo:0,3; Alto:0,6).

O passo seguinte da lógica fuzzy é a defuzzificação. Este procedimento transforma os valores linguísticos assumidos pela variável em valores reais, ou seja, o processo inverso da fuzzificação. Para isto, podem ser aplicados diversos métodos existentes na literatura, sendo o do centro de gravidade o mais comum [31]. A Figura 9 ilustra este passo. Neste exemplo, a variável de saída após o processo de inferência assumiu os valores “Adolescente” com 0,6 de pertinência e “Adulto jovem” com 0,2. O processo de defuzzificação por centro de gravidade expõe um valor de 15,3 anos.



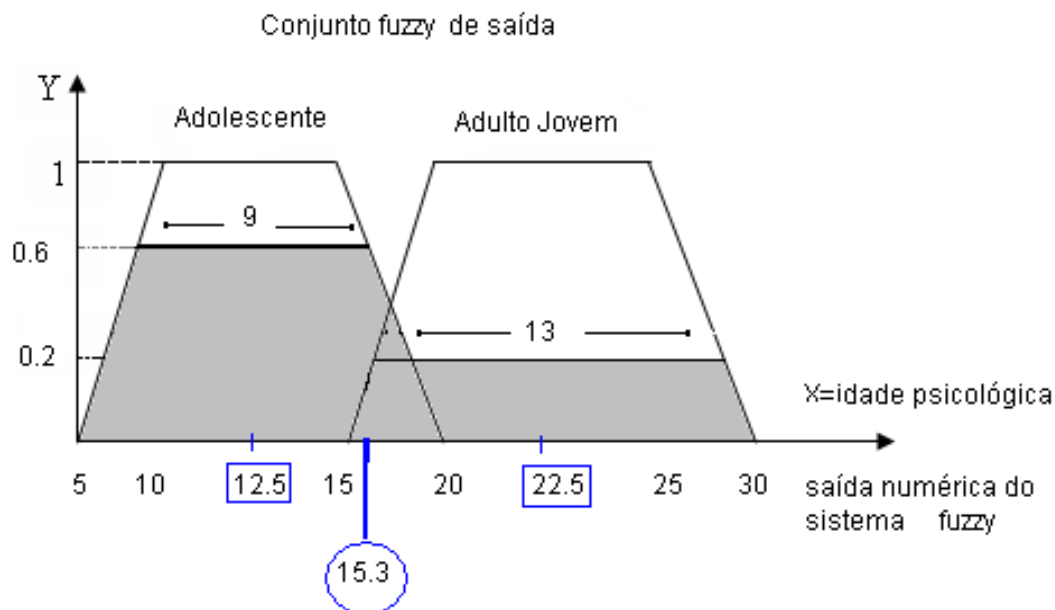


Figura 9: Método de defuzzificação por centro de gravidade [86]

Na Ref (34), a lógica fuzzy é utilizada para analisar os riscos de atividades humanas em plantas nucleares. As variáveis fuzzy são: Probabilidades de falhas humanas (entrada), Severidade (entrada) e Risco (saída). Os algoritmos de Mandani e centro de gravidade são utilizados. Para a construção do conjunto de regras, são utilizadas opiniões de especialistas.

Na Ref [35] a lógica é aplicada em conjunto com a metodologia de análise de falhas humanas CREAM. Neste estudo as variáveis fuzzy são: Fatores formadores do desempenho humano (entrada) e Probabilidade de falha humana (saída). São utilizados os algoritmos de Mandani e do centro de gravidade. Para a construção do conjunto de regras, são utilizadas novamente as opiniões de especialistas.

Na Ref [32] são estudadas as dependências entre tarefas humanas com o auxílio da técnica fuzzy. Na Ref [33], os riscos de desastres naturais são considerados utilizando os conceitos de probabilidade fuzzy. Na Ref [36] a lógica fuzzy é combinada com a simulação de Monte Carlo para a análise de riscos em construções. Em [40, 46-47, 75, 87-89] são encontradas aplicações da álgebra dos números fuzzy.

A lógica fuzzy é aplicada em estudos de riscos financeiros, previsões, otimizações, área da saúde, controle não-linear, etc, pelo seu tratamento de incertezas, imprecisões e ambiguidades encontradas nas tomadas de decisão. No presente trabalho, os conceitos da teoria dos conjuntos fuzzy e da álgebra dos números nebulosos (adição, multiplicação, divisão) foram utilizados na etapa de quantificação dos resultados obtidos através das opiniões dos especialistas. O tratamento das incertezas epistemológicas foi realizado através do uso das variáveis linguísticas. O mecanismo da máquina de inferência fuzzy [31] não foi utilizado neste trabalho.

## **2.6 AGREGAÇÃO FUZZY DE OPINIÕES**

Em trabalhos envolvendo a obtenção de opiniões de especialistas, surge naturalmente a preocupação acerca da agregação destas opiniões. Diversos métodos são utilizados em diferentes trabalhos. Estes métodos são matemáticos e/ou estatísticos [23, 45], utilizados em diferentes contextos.

Na utilização da teoria fuzzy para a elicitación de *experts*, também são encontrados métodos de agregação. Na Ref [41] é desenvolvido um método de agregação de opiniões fuzzy de especialistas acerca de diversos parâmetros com diferentes alternativas. Similarmente, na Ref [46] um método é utilizado com o auxílio da álgebra fuzzy. Na Ref [42] é introduzido um método para determinar o peso da opinião de cada especialista e posterior agregação das opiniões. Na Ref [43], um índice de similaridade é definido através da razão entre as áreas dos números fuzzy. Em seguida, um índice médio é utilizado para ponderar as opiniões de cada especialista até se chegar ao número fuzzy agregado. A Ref [44] é uma evolução do estudo anterior considerando o peso de cada especialista no índice de ponderação

médio. A finalidade do método é a de se chegar a um número fuzzy refletindo as  $n$  opiniões de especialistas.

Não há unanimidade sobre utilização de qualquer destes métodos. O estudo apresentado em [44] consiste em um processo sistemático de cálculo das variâncias das opiniões com a utilização das informações acerca dos perfis dos envolvidos. Por este motivo e por sua fácil aplicabilidade, ele foi utilizado neste trabalho. O método é descrito na Seção 5.2.

## 2.7 ESTUDO PROPOSTO

No contexto do estudo da confiabilidade de sistemas digitais, duas metodologias são destacadas como as mais indicadas para a modelagem de sistemas digitais: Markov/CCMT e DFM [1, 14, 17]. A descrição das interações entre o sistema de controle, demais subsistemas, operadores e variáveis de processo além da possibilidade de incorporação de seus resultados em APS existentes dão maior credibilidade a estes métodos.

Baseada na vasta aplicação encontrada na literatura, modelagem simplista, análise sistêmica, chancela da NRC e acessibilidade ao método, a DFM foi escolhida como objeto de estudo. Este método já foi utilizado para modelar as dependências entre sistemas digitais de controle e falhas humanas [17], falhas de sistemas de controle em plantas nucleares [57] e falhas em sistemas digitais de controle em sistemas espaciais [58], por exemplo. Sua incorporação de resultados em análises probabilísticas de segurança não depende de nenhuma técnica intermediária, como a metodologia Markov/CCMT [1, 14]. Além disso, sua facilidade na análise de erros de *softwares*, devido à sua modelagem mais simplista, reforça o seu uso.

A técnica ATHEANA, como a DFM, é bastante disseminada na literatura. Sua análise contextual estruturada, busca conjunta por erros de comissão e omissão,

possibilidade de incorporação dos resultados às APS, número de referências e aval da NRC dão credibilidade ao método. Por estas razões, ela foi escolhida para modelar o comportamento humano em sistemas digitais juntamente com a metodologia DFM.

Quantitativamente, os resultados foram refinados através de opiniões de especialistas em conjunto com a teoria fuzzy. A experiência da utilização de variáveis linguísticas (linguagem natural do ser humano) como instrumento de coleta das opiniões no tratamento das incertezas epistemológicas reforçou o uso dos conceitos desta lógica.

As opiniões foram agregadas. O método empregado consiste em um processo sistemático de cálculo das variâncias das opiniões com a utilização das informações acerca dos perfis dos envolvidos. Por este motivo e por sua fácil aplicabilidade, ele foi utilizado neste trabalho.

Para a construção do modelo foi utilizado um demo do toolset DYMONDA® disponibilizado pela empresa ASCA®, inc [13].

Como ilustração, um sistema simplificado de controle digital baseado no pressurizador (PZR) de uma usina nuclear, composto por sensores, atuadores e um *software* de controle em um microprocessador, foi proposto como estudo de caso. No cenário proposto, foram analisadas as interações com o operador da central de maneira conjunta. O estudo se baseou na modelagem DFM e ATHEANA desse sistema de controle e na análise integrada das interações entre os componentes do sistema, o processo e o operador. A DFM realizou a etapa intermediária da ATHEANA de busca dos contextos de erro (combinações das condições da planta e dos fatores formadores do desempenho humano) que induzem às ações inseguras. Desta maneira procurou-se preencher a lacuna existente na literatura com relação à modelagem e análise sistêmica, tanto no âmbito dos sistemas digitais, quanto no âmbito da confiabilidade humana. Posteriormente, foi realizada uma complementação dos resultados obtidos através de coleta de opiniões de especialistas em conjunto com

a teoria fuzzy, numa tentativa de se quantificar os resultados e promover decisões baseadas no risco.

### 3 DFM (*DYNAMIC FLOWGRAPH METHODOLOGY*)

#### 3.1 DESCRIÇÃO DA METODOLOGIA

A DFM é uma metodologia de modelagem de sistemas dinâmicos atualmente muito utilizada na análise de confiabilidade de sistemas digitais críticos de controle e segurança [17, 19, 21]. Ela consiste em modelar tanto o sistema de controle quanto o processo a ser controlado através de seus parâmetros chaves, que são discretizados em estados que descrevem seus comportamentos. As relações temporais e de causalidade entre estes parâmetros são definidas através de tabelas de decisões formuladas por especialistas das respectivas áreas e através de simulações. Ao final da etapa de construção do modelo, a análise pode ser realizada seguindo dois caminhos [1, 13, 17]:

- Análise dedutiva – Consiste em definir um evento topo e rastrear as menores combinações possíveis de estados dos componentes que levam a ele. É a análise utilizada em eventos topo de árvores de falha.
- Análise indutiva – Consiste na definição de eventos iniciadores e análise de suas consequências no modelo. É utilizada em conjunto com os resultados da análise dedutiva para a reprodução das falhas encontradas no sistema e posterior mitigação. Também pode ser utilizada para verificar o funcionamento do sistema de acordo com as suas especificações (verificação de *design*).

A análise consiste em percorrer todas as combinações presentes nas tabelas do modelo, realizando simplificações quando necessário e tendo como ponto de partida o evento topo (condições iniciais) dado(as) [90-92].

A DFM trabalha com o conceito de implicativos diretos (*prime implicants* ou PI). Os implicativos diretos representam as combinações mínimas dos estados das variáveis suficientes para causar um evento topo de interesse. A união de todos os implicativos diretos é equivalente ao evento topo. Eles são usados para representar os diversos estados em que o sistema analisado pode se encontrar [13, 15-17, 90-92].

A DFM possibilita a incorporação dos resultados em APS existentes como indicado em [13-14, 17].

### **3.2 ELEMENTOS DO MODELO DFM**

O modelo DFM constrói uma rede de causalidade e transições temporais entre seus elementos. Tais elementos são descritos a seguir [13, 15-16]:

- Variáveis de Processo (VP) – Representam as principais variáveis físicas, variáveis do sistema, ações humanas, etc, contínuas ou discretas. Estas variáveis são discretizadas em um número de estados que refletem os seus comportamentos. O número de estados pode variar de acordo com o compromisso fidelidade x complexidade da modelagem;
- Ligações de Causalidade (LCA) – Conectam as variáveis de processo explicitando a relação de causalidade que há entre elas de maneira qualitativa;
- Caixas de Transferência (CTA) – Representam as funções, contínuas ou não, que relacionam as variáveis do modelo. Demonstram a relação de causalidade através de tabelas de decisão. As tabelas de decisão são construídas através do conhecimento empírico do sistema, discussões entre especialistas, equações que governam o comportamento das variáveis ou simulações;
- Caixas de Transição (CTR) – São caixas de transferência que levam em consideração a dinâmica entre as variáveis através da definição do passo de

tempo. O passo de tempo é o intervalo necessário para que uma variável assumira um determinado valor, em função de outras variáveis. É usado para descrever funções de *software* e *clocks* de processamento, por exemplo;

- Variáveis de Condição (VC) – representam condições das variáveis de processo;
- Ligações de Condição (LCO) – conectam as variáveis de condição às caixas de transferência ou caixas de transição. Similares às ligações de causalidade.

O primeiro passo de construção do modelo consiste na retirada dos principais componentes do sistema físico e do sistema de controle (automático ou manual). Eles se tornarão as variáveis de processo do modelo (VP). Comportamentos discretos das variáveis são representados através das variáveis de condição (VC). O passo seguinte consiste na discretização destas variáveis em estados que reflitam os seus comportamentos. Em seguida, estas variáveis são conectadas às caixas de transferência (CTA) e caixas de transição (CTR), refletindo as relações temporais e de causalidade entre elas. Todas as possíveis combinações de estados das variáveis do modelo são descritas nas tabelas de decisões, cada uma associada a sua respectiva CTA/CTR [13, 15, 17].

### **3.3 EXEMPLO DE UM MODELO DFM**

O exemplo a seguir ilustra a metodologia DFM. A Figura 10 mostra um tanque de água com uma vazão de consumo. Uma bomba acoplada ao tanque realiza um controle bem simples, descrito na Tabela 1. O objetivo do controle é manter o nível de água em normal. Considera-se que a vazão é menor do que a injeção de água proporcionada pelo sistema de controle.



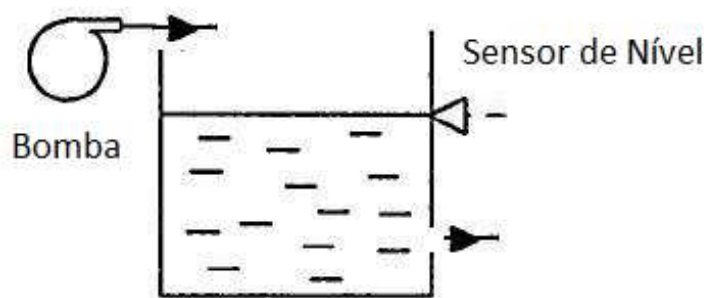


Figura 10: Sistema de exemplo

Tabela 1: Lógica do sistema exemplo de controle

<b>NÍVEL DE ÁGUA</b>	<b>BOMBA</b>
BAIXO	LIGADA
NORMAL	DESLIGADA

No sistema acima as variáveis de processo escolhidas foram: o nível de água do tanque, bomba de controle e injeção de água representando as variáveis chaves do processo controlado e do sistema de controle respectivamente. As variáveis de condição escolhidas foram: condição do sensor de nível e condição da bomba, representando todas as possíveis condições do sistema de controle. Para simplificar, foi considerado que uma vez falho, o dispositivo não retorna ao estado normal. As variáveis são discretizadas segundo a Tabela 2.

Tabela 2: Discretização das variáveis do modelo.

<b>Condição do sensor (VC)</b>	<b>Condição da bomba (VC)</b>
Normal	Normal
Falho Baixo	Falha Ligada

Falho Alto	Falha Desligada
<b>Nível de água (VP)</b>	<b>Bomba (VP)</b>
Vazio (até 5%)	Ligada
Baixo (até 30%)	Desligada
Normal (até 95%)	<b>Injeção de água (VP)</b>
Transbordando (100%)	Com Injeção
	Sem Injeção

As variáveis do modelo são interligadas através de caixas de transferência/transição, cada uma com uma tabela de decisão associada. A Figura 11 mostra o modelo construído em uma das telas do *toolset*. Os círculos representam as variáveis de processo (VP) do modelo. Os quadrados representam as variáveis de condição do modelo (VC). Os pentágonos representam as caixas de transição (CTA) e os retângulos representam as caixas de transferência do modelo (CTR). Para cada uma destas caixas, tabelas de decisão são associadas.

As tabelas de decisão foram construídas através do conhecimento empírico da lógica de controle e estão explicitadas nas Tabelas 3, 4 e 5.

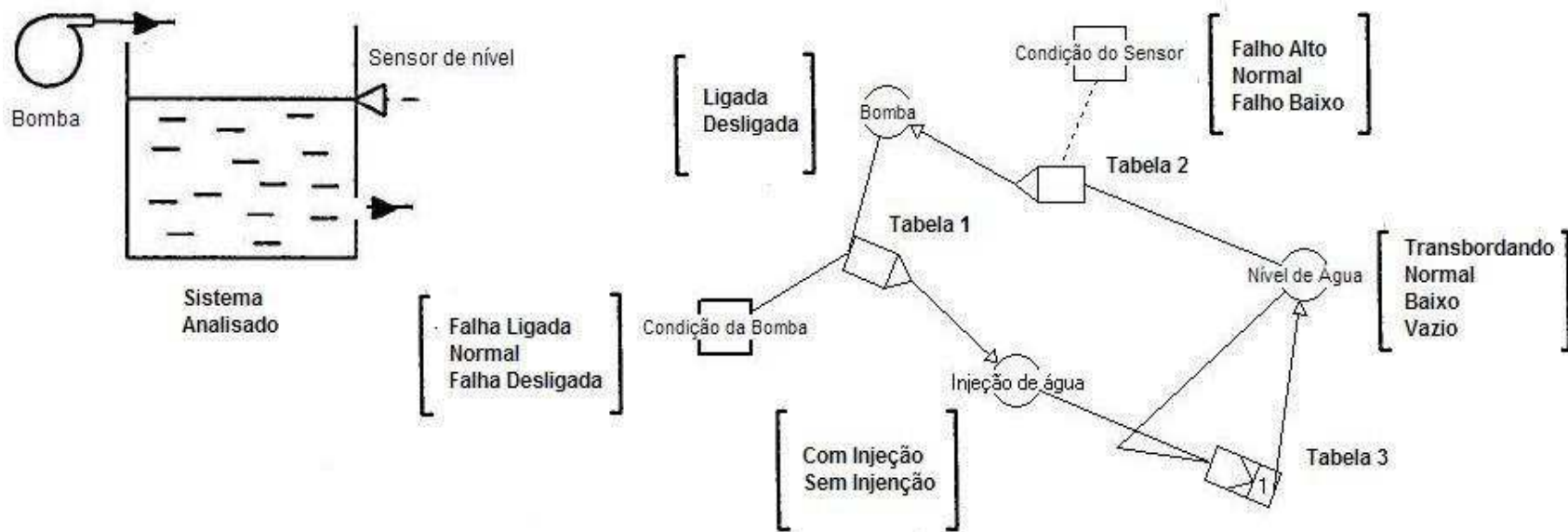


Tabela 1

Bomba	Condição da bomba	Injeção de água
Ligada	Normal	Com Injeção
Desligada	Normal	Sem Injeção
-	Falha Ligada	Com Injeção
-	Falha Desligada	Sem Injeção

Tabela 2

Condição do Sensor	Nível de água	Bomba
Normal	Vazio	Ligada
Normal	Baixo	Ligada
Normal	Normal	Desligada
Normal	Transbordando	Desligada
Falho Alto	-	Desligada
Falho Baixo	-	Ligada

Tabela 3

Injeção de água	Nível de água	Nível de água+
Com Injeção	Vazio	Baixo
Com Injeção	Baixo	Normal
Com Injeção	Normal	Transbordando
Com Injeção	Transbordando	Transbordando
Sem Injeção	Vazio	Vazio
Sem Injeção	Baixo	Vazio
Sem Injeção	Normal	Baixo
Sem Injeção	Transbordando	Normal

Figura 11: Modelo DFM do sistema exemplo

Tabela 3: CTA 1

Condição do sensor	Nível de água	<b>Bomba</b>
Normal	Vazio	Ligada
Normal	Baixo	Ligada
Normal	Normal	Desligada
Normal	Transbordando	Desligada
Falho Alto	-	Desligada
Falho Baixo	-	Ligada

Tabela 4: CTA 2

Bomba	Condição da bomba	<b>Injeção de água</b>
Ligada	Normal	Com Injeção
Desligada	Normal	Sem Injeção
-	Falha Ligada	Com Injeção
-	Falha Desligada	Sem Injeção

Tabela 5: CTR 1

Injeção de água	Nível de água	<b>Nível de água+</b>
Com Injeção	Vazio	Baixo
Com Injeção	Baixo	Normal
Com Injeção	Normal	Transbordando
Com Injeção	Transbordando	Transbordando
Sem Injeção	Vazio	Vazio
Sem Injeção	Baixo	Vazio

Sem Injeção	Normal	Baixo
Sem Injeção	Transbordando	Normal

O sinal “+” na Tabela 5 representa o estado da variável no passo de tempo seguinte ao das variáveis de entrada. O passo de tempo considerado foi o intervalo suficiente para a aquisição do sinal e posterior transição de nível realizado através da ação da bomba ou da vazão de consumo.

Em seguida, realiza-se a análise de falhas utilizando o modo dedutivo da DFM. Neste modo, a análise consiste em percorrer todas as combinações de estados presentes nas tabelas do modelo, realizando simplificações quando necessário e tendo como ponto de partida um evento topo dado.

Utilizando o *tool/set* e estabelecendo como evento topo o evento “Nível de água Transbordando”, representando uma falha no sistema de controle, a modelagem DFM exibe os resultados apresentados na Tabela 6.

Tabela 6: Implicativos diretos do evento topo “Nível de água Transbordando em  $t=0$ ”

Número do implicativo	Implicativo direto
1	Bomba Falha Ligada em $t=-1$
	Nível de Água Transbordando em $t=-1$
2	Bomba Falha Ligada em $t=-1$
	Nível de Água Normal em $t=-1$
3	Bomba Normal em $t=-1$
	Sensor Falho Baixo em $t=-1$
	Nível de Água Normal em $t=-1$
4	Bomba Normal em $t=-1$
	Sensor Falho Baixo em $t=-1$

	Nível de Água Transbordando em t=-1
--	-------------------------------------

Nos implicativos de número 1 e 2 percebe-se que uma falha na bomba em “Ligada” leva o nível de água a atingir o valor “Transbordando”, dado que seu estado já estava próximo desta situação. Nos implicativos de número 3 e 4, percebe-se que a falha do sensor em “Baixo” leva à ação errônea de ligar a bomba que por sua vez eleva o nível de água ao limite crítico.

Similarmente para o evento de falha “Nível de água Vazio”, a DFM exibe os resultados da Tabela 7.

Tabela 7: Implicativos diretos do evento topo “Nível de água Vazio em t=0”

<b>Número do implicativo</b>	<b>Implicativo Direto</b>
1	Bomba Normal em t=-2
	Sensor Normal em t=-2
	Nível de Água Vazio em t=-2
	Bomba Normal em t=-1
	Sensor Falho Alto em t=-1
2	Bomba Normal em t=-2
	Nível de Água Vazio em t=-2
	Bomba Falha Desligada em t=-1
3	Bomba Normal em t=-2
	Sensor Falho Alto em t=-2
	Nível de Água Baixo em t=-2
	Bomba Falha Desligada em t=-1
4	Bomba Normal em t=-2
	Nível de Água Normal em t=-2

	Sensor Falho Alto em $t=-2$
	Bomba Falha Desligada em $t=-1$
5	Bomba Normal em $t=-2$
	Nível de Água Normal em $t=-2$
	Sensor Normal em $t=-2$
	Bomba Falha Desligada em $t=-1$
6	Bomba Normal em $t=-2$
	Nível de Água Normal em $t=-2$
	Sensor Normal em $t=-2$
	Bomba Normal em $t=-1$
	Sensor Falho alto em $t=-1$

No implicativo 1, a falha do sensor em “Alto” em  $t=-1$  desliga a bomba e leva o nível de água ao estado “Vazio”. No implicativo 2, a falha da bomba em “Desligada” no instante  $t=-1$  leva ao evento topo. Os implicativo 3 e 4 mostram que a falha da bomba em “Desligada” e o nível “Baixo” em  $t=-1$  levam o nível ao menor valor em  $t=0$ . O nível estava em “Baixo” no implicativo 4 no instante  $t=-1$  devido à falha do sensor em “Falho Alto” no passo anterior. No implicativo 5, a falha da bomba é responsável pela ocorrência do evento topo. No implicativo 6, a falha do sensor leva o nível ao estado “Vazio”.

Nesta análise, observa-se a utilização de 2 passos de tempo, diferentemente da análise do evento topo anterior. O número de passos de tempo define o detalhamento da análise, mas exige um maior custo computacional, ficando a critério do analista a sua escolha. Quanto à duração deste passo de tempo, ela depende estritamente do sistema analisado (tempo de amostragem, processamento e atuação dos componentes envolvidos) [13-14, 17, 19, 21].

No exemplo acima, a DFM foi aplicada a um sistema de *loop* fechado, onde se realizam atualizações de estado a partir de informações anteriores. Porém, não há nenhuma restrição quanto ao uso em sistemas de lógica mais simples.

Um fato relevante é que o modelo consegue levar às possíveis falhas do sistema de controle levando em consideração, sempre, as interações entre o sistema de controle e as demais variáveis. Além disso, uma vez construído, o mesmo modelo pode ser utilizado para diversas análises que se queira, de maneira dedutiva ou indutiva.



## 4 ATHEANA (A TECHNIQUE FOR HUMAN ERROR ANALYSIS)

### 4.1 DESCRIÇÃO DA TÉCNICA

A ATHEANA é uma das técnicas de análise de falhas humanas da segunda geração. Ela é fruto de pesquisas, muitas delas coordenadas pela NRC, que culminaram no documento NUREG 1880 [6]. Ao contrário dos primeiros estudos nesta área, que consideravam as falhas humanas como aleatórias (partindo do princípio de que ao operador cabia simplesmente responder ou não a uma determinada demanda), a ATHEANA se preocupa em modelar os chamados erros de comissão, os enganos cometidos pelos operadores em determinadas situações, sejam eles de natureza pré, pós ou iniciadora de acidentes [3, 6-8,12].

As situações devem ser minuciosamente detalhadas, pois o contexto exerce forte influência sobre o estado emocional e dispõe os recursos que o operador possui em situações de demanda. A ATHEANA representa mais realisticamente as interações entre o operador e a planta pois conceitua os chamados EFC (*Error Forcing Contexts*): combinações dos convencionais PSF (*Performance Shaping Factors*) encontrados na literatura e as condições da planta. Desta forma, um determinado erro humano, seja ele um erro de omissão ou de comissão, pode ser provocado por mais de uma combinação de condições da planta e situações condicionantes (EFC), assim como um mesmo contexto pode provocar diversos tipos de erros humanos. Todos estes princípios foram retirados das lições aprendidas nos eventos ocorridos em acidentes como os de Chernobyl e TMI [6, 24, 26].

As situações condicionantes (ou PSF) englobam tanto situações organizacionais como o nível de treinamento, nível de ruído, disponibilidade de recursos, pressão de trabalho, etc, quanto situações comportamentais como, nível de estresse e fadiga.

O fator cognitivo, comportamental e psicológico é característico das técnicas de análise de falhas humanas de segunda geração. A ATHEANA, particularmente, considera um modelo cognitivo da informação em quatro etapas (Figura 12): monitoração, entendimento da situação, planejamento das ações e execução. Outras técnicas consideram este modelo ou outros derivados. Estas etapas ocorrem de maneira interativa, sendo atualizadas a todo o momento em uma situação de demanda ao operador.



Figura 12: Processo cognitivo utilizado na ATHEANA [25]

A monitoração consiste na atividade de observação dos sinais da planta e variáveis de interesse. O entendimento da situação se baseia no modelo mental da planta construído pelo operador no desenvolvimento do incidente/acidente através de seu treinamento e conhecimento prévio. Este modelo é continuamente atualizado pela atividade de monitoração e tem influência direta na atividade de planejamento. A monitoração, por sua vez, também é guiada pelo entendimento da situação. O planejamento consiste na tomada de decisão baseada no modelo mental da planta do operador. Ele tem por base os procedimentos disponíveis, grau de conhecimento e treinamentos realizados. A execução consiste no ato em si de realizar uma ação,

baseado na decisão da atividade de planejamento. Uma discussão interessante acerca das interações entre estas quatro etapas é feita em [6, 24].

Em cada uma destas etapas, claramente, podem ser identificados modos de falhas humanas. Na monitoração, por exemplo, o operador pode simplesmente não olhar um indicador (erro de omissão) ou olhar um indicador errado (erro de comissão). No entendimento da situação, o operador pode desenvolver um modelo mental errado da planta, gerando expectativas errôneas. No planejamento, pode ser tomada uma decisão errada. Na execução, existem diversos meios em que um operador pode errar o acionamento de um botão ou simplesmente não acioná-lo [24].

Todos os modos de falha possuem causas diretamente ligadas ao contexto no qual o operador está inserido (Ex: Um modelo mental errôneo ou uma decisão tomada de maneira equivocada podem ser frutos de um treinamento mal realizado, fadiga ou ainda falha na instrumentação ao redor). Desta maneira, a ATHEANA foca sua atenção na identificação destes contextos. Diversos estudos já foram realizados com a ATHEANA e conclusões interessantes foram desenvolvidas acerca de melhorias em fatores condicionantes e instrumentação [83-84, 93].

A técnica se preocupa ainda com a integração com a análise probabilística de segurança, dado que esta última é a base do estudo de riscos das plantas atuais. Esta integração se dá através da definição do evento de falha humana (HFE) que, segundo [6, 24-26, 84] é o evento básico modelado na APS que representa uma falha de função, componente ou sistema decorrente de um ou mais atos inseguros humanos (EX: Evento de falha: “Falha no sistema de injeção de alta pressão”; HFE: “Operador falha em acionar o sistema de alta pressão”). O HFE reflete o ponto de vista da APS com relação às falhas humanas. Os atos inseguros são os erros de omissão ou comissão que resultam em uma condição insegura da planta. No exemplo dado, os atos inseguros poderiam ser: “Operador inicia sistema de alta pressão erroneamente” ou “Operador não inicia sistema de alta pressão quando necessário”.

O processo básico de análise da ATHEANA baseia-se na procura de atos inseguros e EFC, de maneira interativa e dependente que levam, em última instância, ao HFE (Figura 13). O processo consiste em uma procura *top-down* partindo do HFE, que é definido de maneira genérica ou detalhada, chegando aos EFC e aos UA (atos inseguros ou *unsafe acts*) associados. Esta busca segue as quatro etapas do processo cognitivo de processamento da informação. Pode-se pensar neste mecanismo de busca como um processo de HAZOP centrado na confiabilidade humana, que foi refinado no decorrer dos anos [24-26, 94] até se chegar ao guia definitivo proposto pela NRC [6]. Este guia é detalhado a seguir.

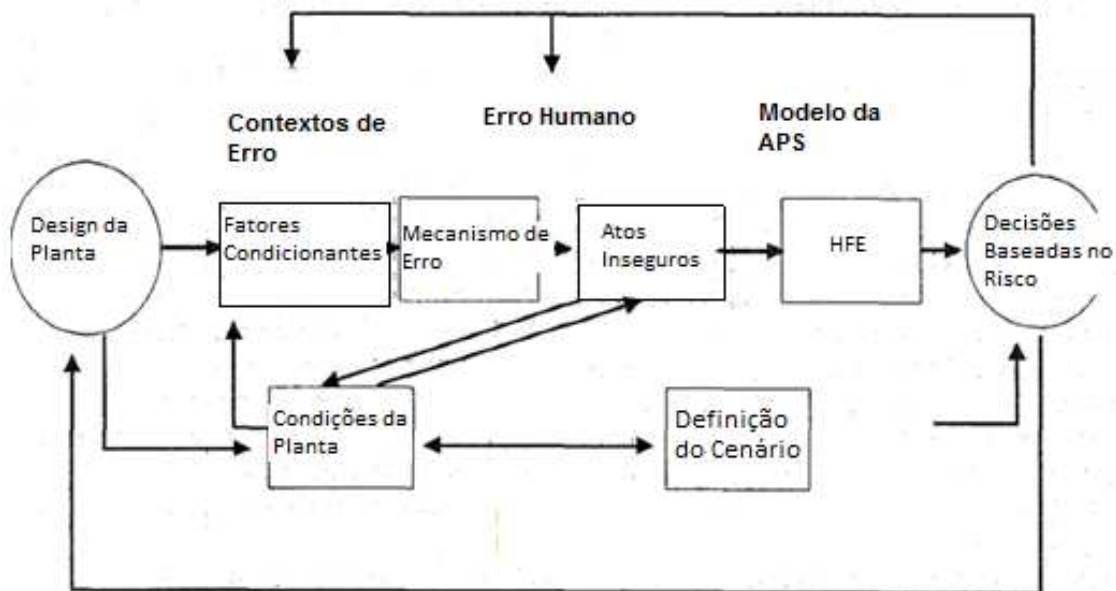


Figura 13: Estrutura de uma análise ATHEANA [24]

## 4.2 ETAPAS DA TÉCNICA

O guia definitivo da ATHEANA [6] é o principal documento da técnica. Desenvolvido a partir do ano de 2000, o guia contém as evoluções e conclusões das

questões levantadas acerca do assunto durante anos, propondo os passos necessários à realização de uma análise de falhas humanas (Figura 14).

O primeiro passo consiste em definir o assunto a ser abordado, a equipe multidisciplinar de *experts* que realizará a análise e a coleta das informações necessárias [6].

A equipe multidisciplinar deve ser composta por um especialista em análise de confiabilidade humana, um especialista em análise probabilística de segurança da planta em estudo, operadores e especialistas em termodinâmica, dentre outros [6]. O especialista em confiabilidade humana é o líder da análise, *expert* em ATHEANA e em ciência comportamental.

A coleta das informações necessárias compreende os dados específicos de *design*, procedimentos, operações, dados de natureza termo-hidráulica e demais informações da planta.

O segundo passo da técnica consiste na definição do escopo de análise com relação à planta. Este passo deve ser realizado pelo responsável pela confiabilidade humana e o especialista em análise de segurança. Exemplos de questões desta etapa [6]:

- Quais modos de falhas humanas serão abordados?
- Quais sistemas de segurança serão considerados?
- Quais eventos iniciadores (eventos topos de falha) serão considerados?
- Quais funções de segurança serão abordadas?
- Quais modos de falha de equipamentos serão utilizados?
- Que nível de detalhamento será atingido?

O terceiro passo consiste na definição do “contexto nominal” ou cenário inicial de análise. Nesta etapa, dentro do escopo de análise da planta definido no passo

anterior, definem-se as condições iniciais da planta, suas variáveis, o estado do(s) operador (es), o estado inicial dos equipamentos e sistemas englobados na análise, atividades em progresso, eventos iniciadores e finalmente as premissas que serão adotadas. Este passo deve ser realizado pelo especialista em confiabilidade humana em conjunto com o especialista em análise de segurança da planta [6].

A partir do quarto passo as etapas realizadas fazem parte exclusivamente da ATHEANA. Os passos anteriores refletem até então as boas práticas na análise de confiabilidade humana. O quarto passo representa a definição do HFE (evento de falha humana) e dos atos inseguros associados baseados nas condições do cenário definido no passo anterior. O evento de falha humana é definido como um evento da APS que causa uma perda/falha de função de um sistema ou componente. Os atos inseguros são ações humanas de omissão ou comissão que em última instância levam ao evento de falha humana. É importante frisar que o HFE é o resultado de uma ou mais ações inseguras que levam à perda de funcionalidade de um sistema/componente. Isto permite que o HFE seja a integração entre a análise de falhas humanas e a APS. Ações de interesse envolvem o início, controle, operação, isolamento ou término de um equipamento/sistema [6].

Na definição do HFE, os analistas devem considerar as funções que o operador vai executar em resposta ao cenário definido, baseado nos procedimentos e treinamentos. Para auxiliar na definição, o HFE pode ser desmembrado ainda em dois ou mais atos inseguros conforme ilustrado na Figura 15. A Tabela 8 auxilia nas possíveis escolhas de um HFE e de seu desmembramento [6].

O quinto passo consiste na identificação dos chamados *error forcing contexts* (EFC), combinações dos fatores formadores do desempenho humano, ou *performance shaping factors* (PSF) com as condições da planta. Esses EFC são as condicionantes para o ocorrência do HFE e das ações inseguras relacionadas a ele. Esta etapa deve ser realizada por toda a equipe de análise com auxílio de entrevistas ao pessoal da planta e dados de simulações com operadores [6].

Sequências de eventos devem ser determinadas para o cenário definido até se chegar ao HFE em questão. Para cada uma destas sequências a lista de PSF deve ser revista para permitir a identificação dos PSF mais relevantes. Informações específicas da planta devem ser incorporadas nas discussões acerca da evolução de cada uma das sequências. As interações entre os diversos fatores devem ser levadas em consideração. O guia da ATHEANA dispõe de uma lista de fatores que foi consolidada durante anos de pesquisa na área de confiabilidade humana. Exemplos destes fatores são: nível de treinamento, acesso aos procedimentos, nível de estresse, fadiga, condições ambiente, tempo disponível para realização de tarefas, dentre outros [6].

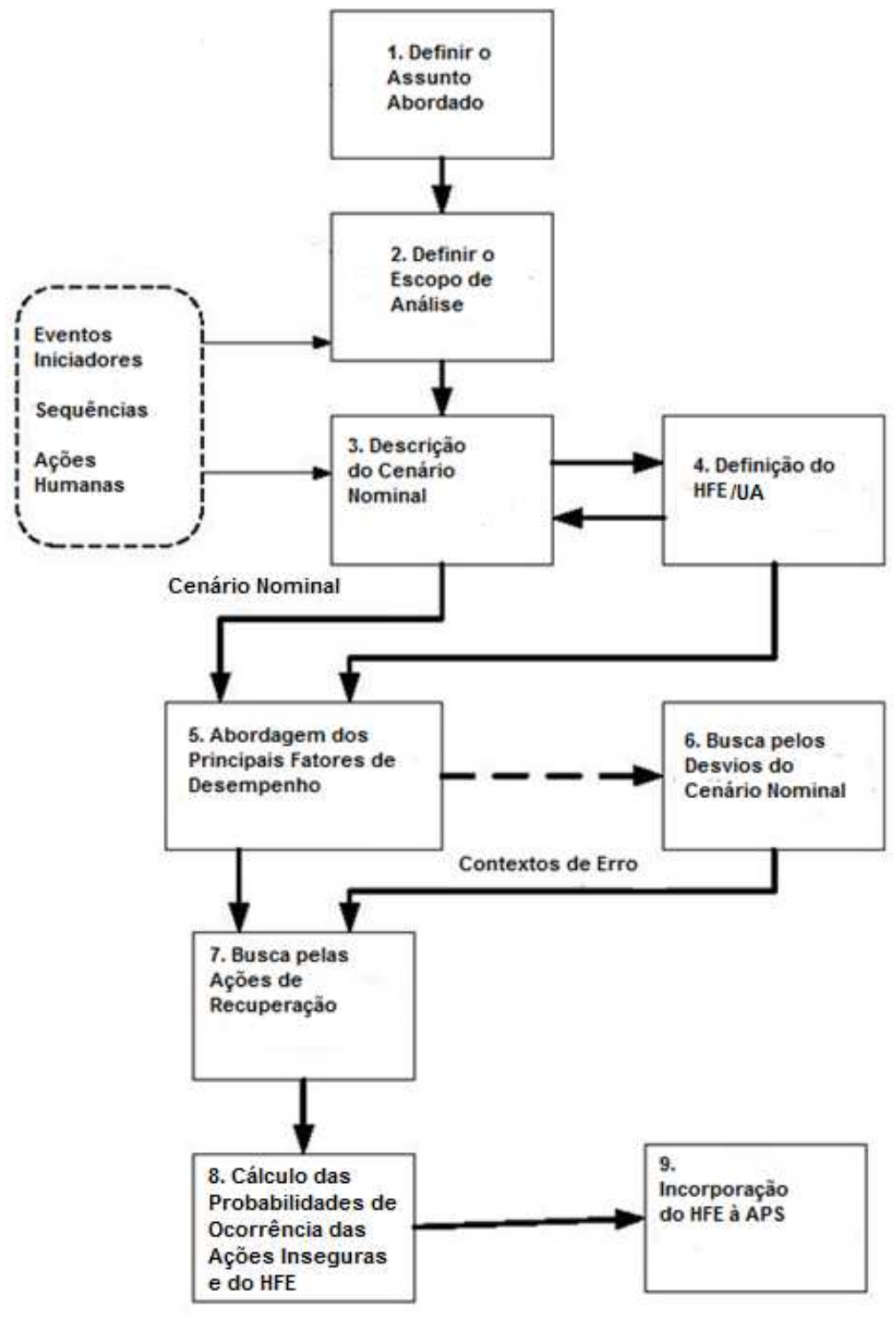
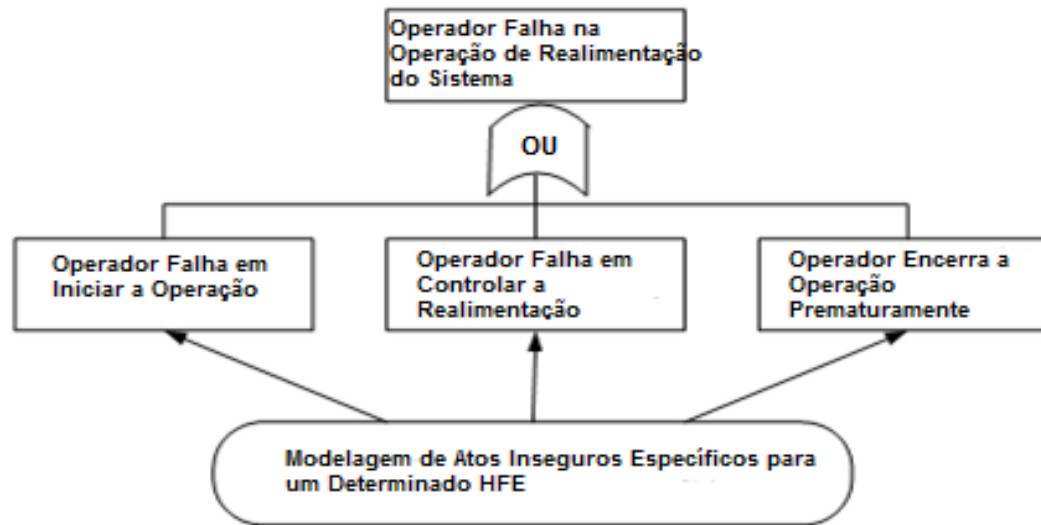


Figura 14: Etapas da técnica ATHEANA [6]





OU

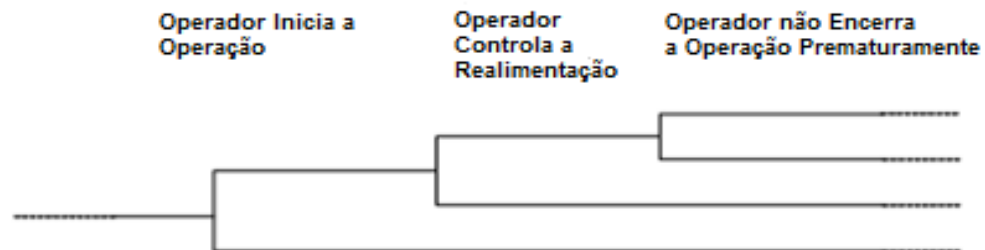


Figura 15: Desmembramento do HFE em ações inseguras [6]

Tabela 8: Possíveis escolhas de ações inseguras para um HFE [6]

Falha funcional do equipamento na APS	EOO ou EOC?	Exemplos de ações inseguras
Equipamento falha em iniciar automaticamente	EOO	Operador falha em iniciar o dispositivo manualmente
	EOC	Operador impede o início do dispositivo
Equipamento falha em continuar operação pelo período da missão	EOC	Operador impede a operação do dispositivo
Equipamento falha em ser acionado manualmente quando requerido	EOO	Operador falha em iniciar dispositivo manualmente quando requerido ou inicia o dispositivo tardiamente
	EOC	Operador inicia prematuramente o dispositivo ou quando não requerido
Equipamento falha em ser operado quando requerido	EOO	Operador falha em operar o dispositivo quando necessário
	EOC	Operador passa a operar o dispositivo inapropriadamente
Equipamento falha em manter o <i>status</i> desejado	EOO	Operador falha em manter o <i>status</i> do dispositivo
	EOC	Operador muda o <i>status</i> do dispositivo inapropriadamente
Equipamento falha em ser parado manualmente	EOO	Operador falha em parar o dispositivo ou o pára tardiamente
	EOC	Operador pára o dispositivo precocemente ou quando não requerido
Equipamento falha em se manter parado	EOC	Operador reinicia dispositivo inapropriadamente

As dependências entre os diferentes PSF devem ser consideradas bem como as dependências entre as diversas ações humanas que possam ocorrer durante cada sequência do cenário nominal [6].

O quinto passo consiste na identificação dos EFC, para o cenário definido, que levam ao HFE analisado. O sexto passo consiste em procurar desvios do cenário nominal, ou seja, outros cenários, que por sua vez possam conter diferentes combinações de condições da planta e fatores formadores do desempenho humano (PSF) que levam ao mesmo HFE. Para a realização desta etapa, a equipe de análise discute os desvios do cenário nominal através de técnicas de HAZOP e WHAT IF [94-95], gerando variações das condições da planta e PSF encontrados inicialmente. O guia da ATHEANA contém tabelas que auxiliam na utilização de palavras guia do HAZOP e perguntas do WHAT IF. Nesta etapa é extremamente recomendável que o processo seja devidamente documentado por se tratar de uma discussão extensa e multidisciplinar [6].

O sétimo passo consiste em analisar todos os EFC provenientes dos desvios do cenário nominal com relação às possibilidades de ações humanas de recuperação e, conseqüentemente, não ocorrência do HFE analisado. Como estes EFC são menos relevantes que os do cenário nominal, caso a possibilidade de recuperação do HFE seja alta para estes EFC, eles podem ser eliminados das análises posteriores, caso contrário, eles irão contribuir conjuntamente com os EFC identificados para o cenário nominal. Esta análise é de natureza qualitativa de maneira geral. A Figura 16 ilustra o procedimento [6].

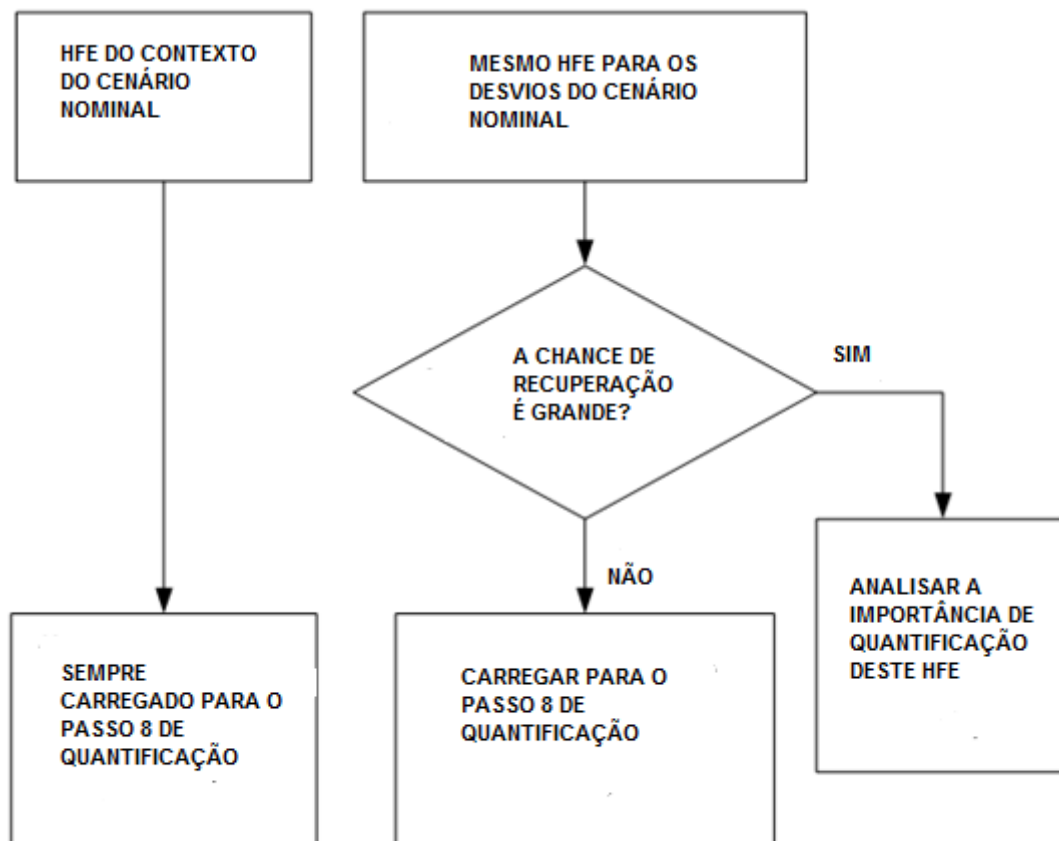


Figura 16: Análise da possibilidade de recuperação do HFE analisado [6]

O oitavo passo consiste na quantificação do HFE. Este passo utiliza a elicitación de especialistas na área, como indicado no guia [6] e constante em alguns trabalhos já publicados [4, 23, 27, 37-38]. Estes especialistas são operadores, engenheiros de usina, analistas de confiabilidade e pesquisadores que se baseiam em sua experiência e conhecimento para responder questões específicas da planta. As opiniões consistem nas probabilidades de ocorrência dos EFC e UA identificados como indicado na Eq (1) [6]. A Eq (1) indica que para um determinado cenário S e seus EFC, deve-se quantificar as UA identificadas para todos os EFC de maneira condicional. O resultado final é a probabilidade de ocorrência do HFE analisado.

$$P(\text{HFE}|\text{S}) = \sum_j \sum_{i(j)} P(\text{EFC}_i|\text{S}) * P(\text{UA}_j|\text{EFC}_i, \text{S}) \quad (1)$$

Em outras palavras, a probabilidade do HFE é o somatório das probabilidades de ocorrência dos contextos identificados multiplicados pelas probabilidades das ações humanas dado estes contextos, para cada ação identificada (j) e para cada contexto identificado (i).

O número de especialistas pode variar de 3 a 6 para representar suficientemente o universo de opiniões, sem deixar o processo exaustivo [6]. As incertezas devem ser levadas em consideração e o especialista em análise de segurança é o responsável por reunir todas as informações e convertê-las em estimativa numéricas. O guia da ATHEANA dispõe de uma tabela inicial de calibração (Tabela 9) das probabilidades que devem ser discutida entre os especialistas bem como o processo para se chegar a uma distribuição de probabilidade conjunta. Basicamente, os contextos são apresentados e se pergunta com que frequência uma determinada ação humana pode ocorrer nas situações dadas, bem como a frequência de ocorrência das mesmas, baseada na experiência dos especialistas tendo como ponto de partida a Tabela 9.

As dependências entre ações humanas secundárias dentro de uma ou mais sequências de eventos (EFC) devem ser levadas em consideração, mesmo não existindo uma formalização do tratamento destas dependências como o próprio guia explicita [6]. As interações entre diferentes ações humanas secundárias fazem parte dos contextos dados para a quantificação do HFE e devem ser apresentadas no processo de eliciação de opiniões.

Finalmente todo o processo, extenso em sua natureza, deve ser documentado.

Tabela 9: Tabela de probabilidades iniciais sugeridas para ações humanas [6]

<b>Circunstâncias</b>	<b>Probabilidade</b>	<b>Significado</b>
O operador falhará certamente	1.0	A falha certamente acontecerá. O operador não realizará a ação corretamente.
O operador tem altas chances de falhar	~ 0.5	5 de 10 falharão. O nível de dificuldade é suficientemente alto para que o operador falhe.
O operador falhará ou não	~ 0.1	1 de 10 falhará. O nível de dificuldade é moderado e falhas eventuais acontecerão.
O operador tem baixas chances de falhar	~ 0.01	1 de 100 falhará. O nível de dificuldade é muito baixo para que o operador falhe.
É improvável que o operador falhe	~ 0.001	1 de 1000 falhará. A ação requerida é tão fácil que é inconcebível que o operador falhe.

O nono e último passo consiste na incorporação dos resultados da ATHEANA em APS existentes. O procedimento pode ser realizado de duas formas, como ilustra a Figura 17. Na primeira opção, o HFE pode ser diretamente incorporado com sua probabilidade estimada na etapa anterior. Na segunda, todas as ações encontradas e seus contextos associados são incorporados através de novos trechos em árvores de eventos ou árvores de falha. A segunda maneira é mais interessante, para ilustrar as diferentes sequências de falha, porém deixa o cálculo do modelo sobrecarregado.

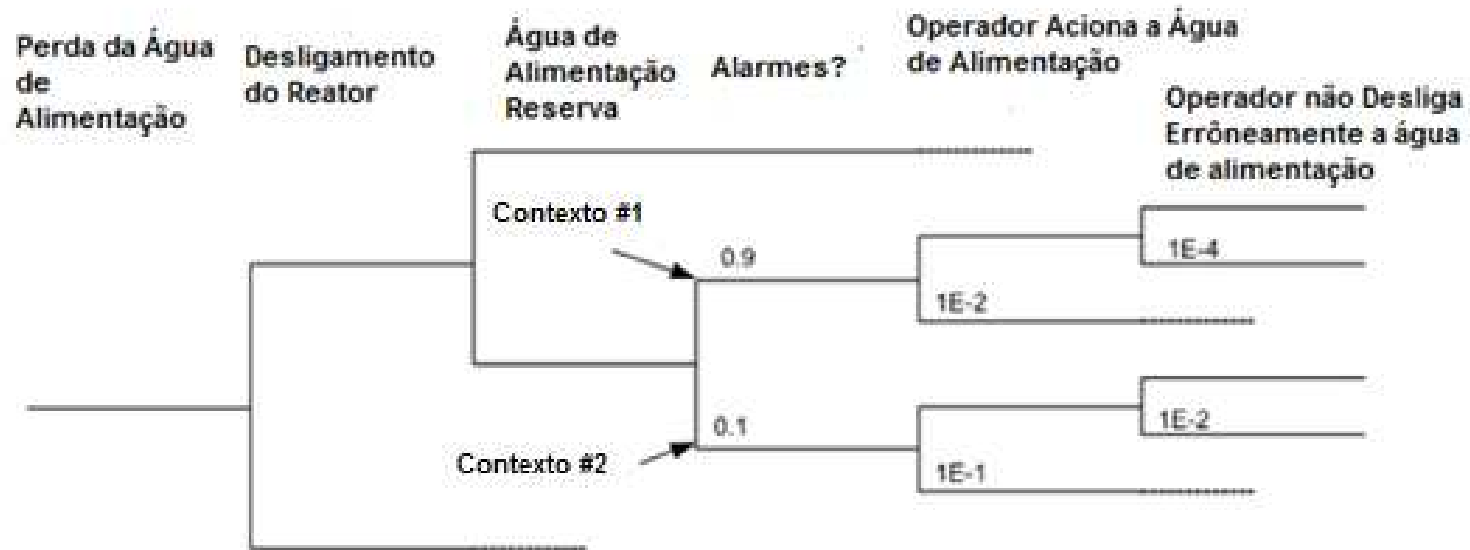


Figura 17: Incorporação do HFE em uma APS [6]

Ao final da aplicação da técnica, recomenda-se a revisão de todos os passos pela equipe de análise bem como a documentação de todo o processo.

Em suma, após a definição inicial do escopo de análise e do cenário da planta, a ATHEANA procura as combinações das condições da planta e dos fatores formadores do desempenho humano que geram mecanismos de erro aos operadores. Estes mecanismos provocam a ocorrências dos atos inseguros, que em última instância, levam ao evento de falha humana ou à ação insegura que provoca a perda de funcionalidade de um equipamento ou sistema. O HFE, uma vez identificado e quantificado, é o ponto de ligação entre a APS e a análise de confiabilidade humana.



## 5 COLETA DE OPINIÕES E AGREGAÇÃO FUZZY

### 5.1 MÉTODO DE COLETA DE OPINIÕES

O processo de coleta de opiniões de especialistas utilizado no trabalho se baseia na experiência obtida e explicitada em [4]. As etapas básicas do processo são ilustradas na Figura 18:

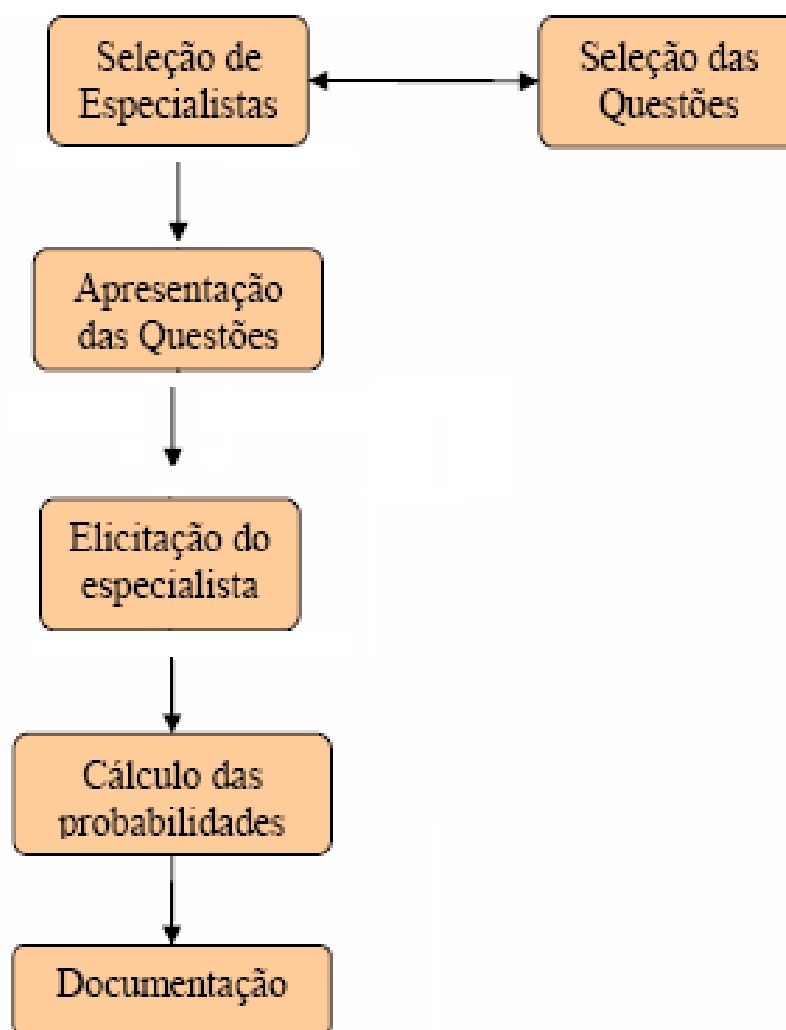


Figura 18: Etapas realizadas na coleta de opiniões de especialistas [4]

Na primeira etapa, seleção de especialistas, devem ser requisitadas as autoridades no assunto como professores, mestres, doutores, engenheiros, pesquisadores, etc. É importante que não existam conflitos de interesse entre os membros. O tamanho do grupo é variável, refletindo a diversidade de opinião, confiabilidade do resultado e a preocupação de se trabalhar com uma margem de segurança, dado que os membros da análise podem vir a desistir [29]. Os peritos devem demonstrar competências através de experiência profissional, publicações, consultorias, pesquisas, etc [4, 29-30].

Na seleção de questões, é elaborada uma lista de questões através de experimentos e/ou observações acerca do evento em questão. O questionário deve ser estruturado de maneira a coletar os dados com um número mínimo de erros. Para isso as Refs [4, 30, 85] reúnem orientações de como elaborar uma lista de questões.

As questões devem ser claras, específicas e devem seguir um sequenciamento lógico. Podem ser do tipo abertas (respostas em formato livre) ou fechadas (com opções limitadas de respostas), sendo que as primeiras são mais adequadas a dados numéricos, porém apresentam algumas dificuldades [4, 29]:

- O questionário pode se tornar cansativo;
- A entrada dos dados pode ser dificultada pela grafia do informante;
- Há a necessidade de uma análise de coerência da resposta do informante.

No presente trabalho, adotou-se a utilização das questões fechadas com dados do tipo variáveis linguísticas [85]. Essa escolha proporciona uma simplificação no processo de formulação, aquisição de informações além de tratar as incertezas intrínsecas às opiniões com o auxílio da teoria fuzzy [30, 38-39, 85].

A redação das questões deve ser simples, sem abreviações, jargões, ambiguidades e terminologias específicas. Estas devem estar agrupadas em blocos

lógicos. Evita-se o uso de sentenças negativas e longas. O número de questões deve ser reduzido ao mínimo. O elaborador deve garantir o sigilo das informações e reservar um campo para observações dos participantes [29, 85].

No terceiro passo, as questões são apresentadas aos especialistas. A forma de apresentação varia desde entrevistas individuais e coletivas a correspondências [85]. É importante que as questões sejam enviadas com antecedência para os envolvidos. Neste trabalho, foi adotado o método de troca de informações por email com os envolvidos, proposto como uma alternativa em [85].

Na elicitación do especialista, o processo heurístico é realizado pelo informante na resolução do questionário [30]. O estudo [85] ressalta o processo seguido pelo especialista no fornecimento de opiniões composto por quatro etapas: Compreensão das questões, retomada dos fatos, estimación e resposta. Caso ocorra a escolha por questões abertas, um passo de crítica dos dados deve ser incorporado ao processo de elicitación para excluir as respostas que, porventura, possam estar fora do contexto da análise. É importante que sejam levadas em consideração as observações do informante nesta etapa [4].

No passo de cálculo das probabilidades, diversos métodos matemáticos estão disponíveis para o tratamento dos dados. O procedimento adotado depende dos tipos de questões e de dados escolhidos na análise. No presente trabalho, foi utilizado um método de agregación das variáveis fuzzy, apresentado na seção 5.2 [38-39, 44].

Por fim, todo o processo deve ser documentado, pois é gerado um grande número de respostas na elicitación. A experiência, os procedimentos e as dificuldades se tornam relevantes em todo o processo e por isso também devem ser registrados [4, 30,85].

## 5.2 MÉTODO DE AGREGAÇÃO FUZZY

Na literatura muitos trabalhos são encontrados utilizando opiniões de especialistas [4, 27-28, 30]. Alguns destes trabalhos usam a elicitaco de *experts* em conjunto com a teoria fuzzy [5, 37-39, 41-42, 46-47]. Nestes ltimos, a dificuldade de se agregar opinies em formato fuzzy  verificada e so aplicadas diferentes metodologias para resolver a questo [37, 39]. Elas se baseiam em construir uma matriz de opinies e calcular ndices de similaridade seguindo o raciocnio de minimizao das distncias dos valores fornecidos.

O mtodo empregado neste trabalho e exposto em [43-44]  uma evoluo destas metodologias. Ele se baseia em calcular graus de concordncia entre as opinies fuzzy coletadas. Os formatos dos nmeros nebulosos podem variar segundo os preceitos da teoria fuzzy [31]. Para  $n$  nmeros fuzzy (refletindo  $n$  opinies de especialistas) em formato triangular  $[R_i=(a_i, b_i, c_i)]$ , onde  $i=1\dots n$ , o clculo  realizado primeiramente atravs da proporcionalidade  $S_{ij}$  entre os centroides das reas dos nmeros, dois a dois:

$$x_i = 1/3 * (a_i + b_i + c_i)$$

$$y_i = 1/3 * (a_i + 4*b_i + c_i) / (a_i + 2*b_i + c_i) \quad (2)$$

Onde  $x_i$  e  $y_i$  representam os centroides do nmero fuzzy  $R_i$

$$S_{ij} = [\min \{x_i, x_j\} * \min \{y_i, y_j\}] / [\max \{x_i, x_j\} * \max \{y_i, y_j\}] \quad (3)$$

Em seguida, o grau médio  $A(E_i)$  e o grau relativo  $RAD_i$  são calculados para cada especialista:

$$A(E_i) = 1 / (n-1) * \sum_{j=1, j \neq i}^n S_{ij} \quad (4)$$

$$RAD_i = A(E_i) / \sum_{j=1}^n A(E_j) \quad (5)$$

Os pesos das opiniões são levados em consideração no cálculo do grau médio de consenso  $CDC_i$ , para cada especialista:

$$CDC_i = \beta * \varepsilon_i + (1 - \beta) * RAD_i \quad (6)$$

Onde  $\beta$  é o índice que pondera a parcela do consenso entre os especialistas e a parcela do peso de cada especialista, sendo seu valor de livre escolha.  $\varepsilon_i$  é o peso da opinião de cada especialista. Ao final, a agregação é realizada, para cada especialista, para cada grau médio de consenso calculado:

$$R = \sum_{i=1}^n (CDC_i * R_i) \quad (7)$$

O número fuzzy final  $R$  representa o número fuzzy agregando todas as opiniões. No documento é apresentado um exemplo numérico para melhor compreensão [44]. Este método, dentre outros [37-38, 42-43], busca a semelhança entre opiniões através de um modelo matemático e índices de concordância.

## 6 O SISTEMA DE PRESSURIZAÇÃO DO REATOR PWR

### 6.1 SISTEMA REAL

O sistema de pressurização de um reator PWR tem como função controlar as variações de pressão do refrigerante decorrentes de variações de carga ou transientes. O principal elemento deste sistema é o pressurizador (PZR). Ele é um vaso de pressão eletricamente aquecido, contendo zonas de vapor e água. Durante a operação, a pressão é mantida a 157 bar por intermédio de aquecedores na zona de água. Durante variações de potência, as variações de pressão são mantidas através de 3 grupos de aquecedores e de 4 grupos de aspersores, estes presentes na zona de vapor [96].

Se a pressão cair por motivos de variação na carga ou transientes, os grupos de aquecedores irão entrar em funcionamento, um a um, proporcionando a inserção de vapor na respectiva zona, e conseqüentemente, aumentando a pressão. Este processo continua até a variável atingir o valor nominal de 157 bar. Se a pressão aumenta, são acionados os grupos de aspersores, condensando o vapor e aliviando a pressão. Estes aspersores jogam água vinda da perna fria do reator através de uma linha de aspersão [96].

Caso a pressão não diminua (aproximadamente 166 bar), uma válvula de alívio é acionada liberando vapor para o tanque de alívio. Por último, se a pressão atingir o limite de projeto (próximo de 175 bar), válvulas de segurança serão acionadas, com o reator já desarmado, com a finalidade de garantir a integridade do sistema [96]. Em último caso, exige-se a intervenção do operador na sala de controle através do desarme manual.

A Figura 19 ilustra o pressurizador e seus componentes [96].

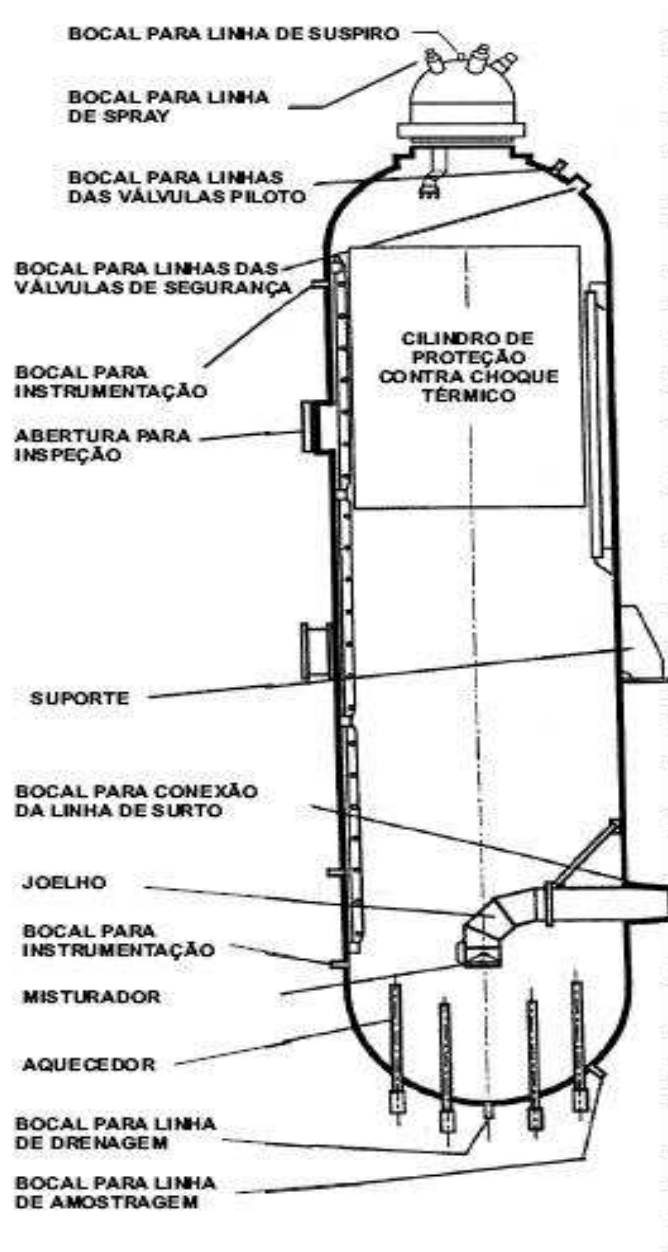


Figura 19: Pressurizador de uma usina PWR [96]

## 6.2 SISTEMA PROPOSTO

O sistema utilizado na modelagem e simulação presentes no estudo se baseia no sistema de pressurizador descrito acima. Ele contém a mesma filosofia de funcionamento implantada por um controle via rotina em um microprocessador,

sensores e atuadores (um sistema digital), porém com algumas simplificações e suposições na planta controlada. São elas:

- O sistema de controle é composto pelos aquecedores, aspersores, um sensor de pressão (leitura direta do nível de água), uma válvula de alívio com uma válvula piloto e uma válvula de segurança com uma válvula piloto. Além disso, considera-se um microcontrolador que executa um software de controle;
- Os grupos de aquecedores e de aspersores atuarão juntos;
- Os modos de falha considerados para cada componente são: Falho Ligado e Desligado para o grupo de aquecedores, Falho Ligado e Desligado para o grupo de aspersores, Falho Alto e Baixo para o sensor de pressão e Falha Aberta e Falha Fechada para as válvulas;
- Existe um operador na sala de controle responsável pelo desarme manual.

A Figura 20 ilustra o sistema digital proposto. A Tabela 10 sumariza a lógica de controle contido no *software* do sistema.

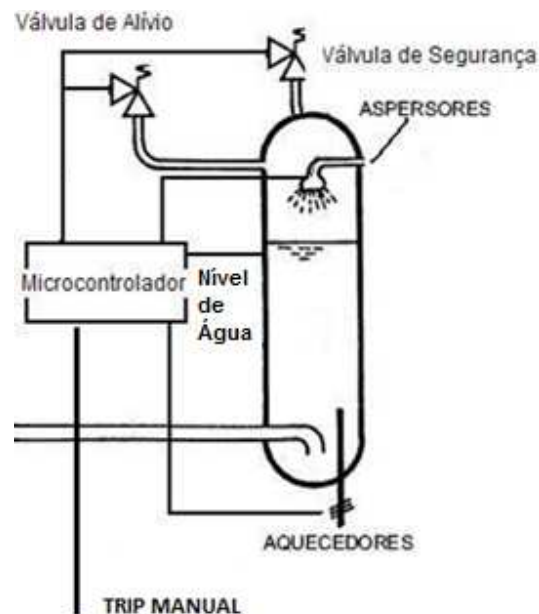


Figura 20: Sistema digital proposto



Tabela 10: Lógica de controle do sistema digital proposto

<b>Pressão</b>	<b>Aquecedores</b>	<b>Aspersores</b>	<b>Válvula de Alívio</b>	<b>Válvula de Segurança</b>	<b>Desarme Manual</b>
Muito Baixa	Ligados	Desligados	Fechada	Fechada	Não acionado
Baixa	Ligados	Desligados	Fechada	Fechada	Não acionado
Pouco Baixa	Ligados	Desligados	Fechada	Fechada	Não acionado
Normal	Desligados	Desligados	Fechada	Fechada	Não acionado
Pouco Alta	Desligados	Ligados	Fechada	Fechada	Não acionado
Alta	Desligados	Ligados	Aberta	Fechada	Não acionado
Muito Alta	Desligados	Ligados	Aberta	Aberta	Acionado

O capítulo seguinte explicita a modelagem DFM realizada para este sistema.

## 7 MODELAGEM DFM/ATHEANA DO SISTEMA PROPOSTO

A modelagem do sistema digital apresentada neste capítulo se baseia na proposta apresentada na seção 2.7 e no capítulo anterior. Esta modelagem procurou realizar a etapa da ATHEANA de buscas dos EFC e UA associadas de maneira dinâmica através da metodologia DFM.

### 7.1 MODELAGEM DO SISTEMA DIGITAL

O sistema proposto no capítulo anterior possui 4 mecanismos de controle de pressão acionados por um microprocessador que executa uma lógica de controle via *software*. Estes 4 atuadores: controle de aquecimento, controle de aspersão e os dois controles das válvulas, representam os dispositivos chaves do sistema de controle e por isso se tornarão variáveis de processo (VP) na modelagem DFM. A pressão é a variável chave do processo controlado e por isso se tornará também uma VP. Os estados nos quais estas variáveis são discretizadas são mostradas na Tabela 11. Para a variável de pressão, os seguintes limites foram considerados [96]:

- 175 bar – Limite de pressão de projeto do reator.
- 169 bar – Pressão de atuação da válvula de segurança.
- 166 bar – Pressão de atuação da válvula de alívio.
- 160 bar – Atuação dos aspersores.
- 156 bar – Atuação dos aquecedores.
- 131 bar - Limite de pressão de projeto do reator.

Dentro destes limites, faixas de pressão foram estabelecidas visando discriminar a atuação dos dispositivos de controle.

Os grupos de aquecedores e aspersores só podem assumir os estados básicos “Ligado” e “Desligado”. As válvulas por sua vez assumem os estados “Aberta” e “Fechada”.

Tabela 11: Discretização das variáveis de processo do modelo do pressurizador

<b>Variável de Processo (VP)</b>	<b>Estado</b>
<b>Pressão</b>	Muito Alta (169 – 175 bar)
	Alta (166 – 169 bar)
	Pouco Alta (160 – 166 bar)
	Normal (156 – 160 bar)
	Pouco Baixa (148 – 156 bar)
	Baixa (140 – 148 bar)
	Muito Baixa (131 – 140 bar)
<b>Válvula de Alívio</b>	Aberta
	Fechada
<b>Válvula de Segurança</b>	Aberta
	Fechada
<b>Grupo de Aquecedores</b>	Ligado
	Desligado
<b>Grupo de Aspersores</b>	Ligado
	Desligado

Como serão considerados os modos de falha dos componentes, variáveis de condição (VC) precisam ser definidas no modelo e associadas as suas respectivas variáveis de processo. A partir das considerações feitas no capítulo anterior, podem-se estabelecer as variáveis de condição explicitadas na Tabela 12.

Tabela 12: Variáveis de condição do modelo do pressurizador

<b>Variável de Condição (VC)</b>	<b>Estado</b>
<b>Estado do Sensor de Pressão</b>	Falho Alto
	Normal
	Falho Baixo
<b>Estado do Grupo de Aquecedores</b>	Falho Ligado
	Normal
	Falho Desligado
<b>Estado do Grupo de Aspersores</b>	Falho Ligado
	Normal
	Falho Desligado
<b>Estado da Válvula de Alívio</b>	Falha Aberta
	Normal
	Falha Fechada
<b>Estado da Válvula de Segurança</b>	Falha Aberta
	Normal
	Falha Fechada

A próxima etapa consiste na interligação das variáveis do modelo passando pelas caixas de transferência e caixas de transição. Cada um destes elementos possui uma tabela de decisão associada que explicita a relação de causalidade que há entre as variáveis. As Tabelas 13, 14, 15 e 16 representam as decisões das primeiras caixas de transferência (CTA). Elas foram elaboradas por inspeção a partir da lógica de controle do sistema executado pelo *software*. As Tabelas 17, 18, 19 e 20 representam os acréscimos/ decréscimos de pressão exercidos pelos mecanismos de controle ou pelos possíveis modos de falha dos mesmos. Nota-se o aparecimento de variáveis auxiliares de modelagem nestas tabelas, como “acrécimo de pressão pelo grupo de aquecedores” e “decrécimo de pressão pela válvula de segurança”. Estas variáveis servem como passo intermediário da transformação de pressão e facilitam a modelagem, mas elas poderiam ser omitidas.

A Tabela A.1 do Apêndice A é a principal tabela de decisão do modelo associada a uma caixa de transição (CTR) existente. Esta caixa representa a mudança de pressão devido à atuação dos mecanismos de controle no intervalo de tempo de atuação. Para a sua elaboração foi necessário o histórico de pressão de operação de uma usina nuclear. A Tabela B.1 do Apêndice B contém os valores típicos de uma usina PWR. Conforme explicado na seção 3.2, um dos métodos de formulação das tabelas é o uso de simulações. A partir do histórico obtido, testes estatísticos (testes de aderência e gráficos de probabilidade) foram elaborados com a finalidade de se verificar a melhor distribuição de probabilidade para estes dados [97-98]. Também foi construído um histograma para este fim [98]. Verificou-se como a melhor alternativa uma distribuição normal de média 156,62 bar e desvio padrão de 0,428 bar, com aderência de até 99% de confiança e índice de determinação  $r^2 = 0,832$  [97-98]. Estes procedimentos estão nas Tabelas C.1, C.2 e C.3 do Apêndice C, respectivamente. Em seguida, foram estimados os valores médios, a partir da distribuição encontrada, para cada faixa de pressão. Foram obtidos dados de alívio/aumento de pressão dos mecanismos de controle [96] expostos na Tabela 21. O raciocínio consiste em verificar

qual o valor médio resultante da pressão após a atuação dos dispositivos de controle. Por exemplo, na linha 9 da Tabela A.1, a pressão se encontra no estado “Muito Baixa” com um valor médio nesta faixa de 139,99 bar, estimado a partir da distribuição encontrada. Como há a atuação do grupo de aquecedores, existe um acréscimo de pressão de 5 bar no intervalo de tempo de atuação deste dispositivo, segundo a Tabela 21. Isto leva o valor médio de 139,99 para 144,99 bar, que se encontra no intervalo “Baixa” de pressão. Tudo isso ocorre caso não haja o acionamento do desarme manual por parte do operador. Caso contrário, o decréscimo de pressão pelo acionamento do desarme manual leva a pressão ao seu estado mais baixo.

Tabela 13: CTA 1 do sistema analisado

Estado do Sensor de Pressão	Pressão	Grupo de Aquecedores
Normal	Muito Alta	Desligado
Normal	Alta	Desligado
Normal	Pouco Alta	Desligado
Normal	Normal	Desligado
Normal	Pouco Baixa	Ligado
Normal	Baixa	Ligado
Normal	Muito Baixa	Ligado
Falho Baixo	-	Ligado
Falho Alto	-	Desligado

Tabela 14: CTA 2 do sistema analisado

Estado do Sensor de Pressão	Pressão	Grupo de Aspersores
Normal	Muito Alta	Ligado
Normal	Alta	Ligado
Normal	Pouco Alta	Ligado
Normal	Normal	Desligado
Normal	Pouco Baixa	Desligado
Normal	Baixa	Desligado
Normal	Muito Baixa	Desligado
Falho Baixo	-	Desligado
Falho Alto	-	Ligado

Tabela 15: CTA 3 do sistema analisado

Estado do Sensor de Pressão	Pressão	Válvula de Alívio
Normal	Muito Alta	Aberta
Normal	Alta	Aberta
Normal	Pouco Alta	Fechada
Normal	Normal	Fechada
Normal	Pouco Baixa	Fechada
Normal	Baixa	Fechada
Normal	Muito Baixa	Fechada
Falho Baixo	-	Fechada

Falho Alto	-	Aberta
------------	---	--------

Tabela 16: CTA 4 do sistema analisado

Estado do Sensor de Pressão	Pressão	Válvula de Segurança
Normal	Muito Alta	Aberta
Normal	Alta	Fechada
Normal	Pouco Alta	Fechada
Normal	Normal	Fechada
Normal	Pouco Baixa	Fechada
Normal	Baixa	Fechada
Normal	Muito Baixa	Fechada
Falho Baixo	-	Fechada
Falho Alto	-	Fechada

Tabela 17: CTA 5 do sistema analisado

Grupo de Aquecedores	Estado do Grupo de Aquecedores	Acréscimo de Pressão
Ligado	Normal	Com Acréscimo
Desligado	Normal	Sem Acréscimo
-	Falho Ligado	Com Acréscimo
-	Falho Desligado	Sem Acréscimo



Tabela 18: CTA 6 do sistema analisado

Grupo de Aspersores	Estado do Grupo de Aspersores	<b>Decréscimo de Pressão</b>
Ligado	Normal	Com Décrécimo
Desligado	Normal	Sem Décrécimo
-	Falho Ligado	Com Décrécimo
-	Falho Desligado	Sem Décrécimo

Tabela 19: CTA 7 do sistema analisado

Válvula de Alívio	Estado da Válvula de Alívio	<b>Decréscimo de Pressão</b>
Aberta	Normal	Com Décrécimo
Fechada	Normal	Sem Décrécimo
-	Falha Fechada	Sem Décrécimo
-	Falha Aberta	Com Décrécimo

Tabela 20: CTA 8 do sistema analisado

Válvula de Segurança	Estado da Válvula de Segurança	<b>Decréscimo de Pressão</b>
Aberta	Normal	Com Décrécimo
Fechada	Normal	Sem Décrécimo
-	Falha Fechada	Sem Décrécimo
-	Falha Aberta	Com Décrécimo

Tabela 21: Dados dos dispositivos de controle [96]

<b>Dispositivo</b>	<b>Alívio/Aumento de pressão por intervalo de tempo de atuação</b>
Grupo de Aquecedores	+ 5 bar
Grupo de Aspersores	-8 bar
Válvula de Alívio	-3 bar
Válvula de Segurança	-6 bar

## 7.2 MODELAGEM DO COMPORTAMENTO HUMANO

De maneira similar, o comportamento humano pode ser modelado através dos elementos da DFM em conjunto com os conceitos da ATHEANA. Desta forma, todos os modos de falha humana e suas causas podem ser modelados. No sistema considerado, existe um operador na sala de controle responsável pelo desarme manual do reator. Seguindo o processo cognitivo da ATHEANA, para cada uma das quatro etapas, diferentes modos de falha do operador (ações inseguras) existentes na literatura e/ou frutos de experiência podem ser considerados e incorporados ao modelo. Em seguida, diferentes causas ou EFC, combinações das condições da planta e dos fatores externos e internos do desempenho humano, são relacionadas a cada um dos modos de falha que, em última instância, levam ao evento de falha humana HFE.

Os modos de falha humana apresentados na Tabela 22 são exemplos escolhidos, um para cada etapa do processo cognitivo, retirados da literatura consultada [6, 99-100]. Não há nenhum impedimento para que  $n$  ações inseguras que se conheça possam ser incorporadas. Porém quanto mais refinado, mais complexo o modelo e sua análise. Os modos de falha são representados como variáveis de condição no modelo DFM.

Similarmente, para cada modo de falha escolhido, possíveis causas para as ações humanas são incorporadas ao modelo como VC e VP. Estas causas (EFC) são condições de variáveis e/ou dispositivos da planta e fatores formadores do desempenho humano (PSF). Estes PSF também são retirados da literatura e/ou experiência [6, 99-100]. Novamente, podem ser modelados tantos PSF quantos se queira. Para fins de exemplificação, dois PSF foram escolhidos e discretizados em dois estados cada. Eles são apresentados na Tabela 23. Condições da planta foram modeladas anteriormente ou foram inseridas nesta etapa. Foi o caso das variáveis: Indicador de pressão, Estado do indicador e Estado do atuador de desarme manual, explicitadas na Tabela 24 com seus respectivos estados associados.

Outras variáveis foram modeladas para complementar a lógica envolvendo os processos cognitivos, são elas: Nível de pressão previsto pelo operador, Nível de pressão atual considerado pelo operador, Decisão do operador, Ação do operador e Decréscimo de pressão pelo desarme manual. Foi considerado um número de estados que representasse suficientemente a lógica entre as variáveis. Por exemplo, para as variáveis de instrumentação só foram considerados os estados “Normal” e “Falho”. Para as de entendimento da situação pelo operador, foram consideradas as situações de pressão com o acréscimo do estado “Incerto”. Para as variáveis de planejamento e execução, dentro do cenário descrito, só fazem sentido os estados “Desarme acionado” e “Desarme não acionado”. Estas variáveis são apresentadas na Tabela 24.

Tabela 22: Modos de falha humana escolhidos para o modelo DFM

<b>Processo Cognitivo</b>	<b>Modo de Falha</b>
Monitoração	Operador não Lê a Indicação de Pressão
Entendimento da Situação	Operador Constata uma Situação de Maneira Errônea
Planejamento	Operador Toma uma Decisão Errônea
Execução	Operador Erra o Acionamento do Desarme Manual

Tabela 23: PSF considerados no modelo DFM

<b>Variáveis PSF</b>	<b>Estados</b>
Nível de Fadiga do Operador	Operador Fadigado
	Operador Não Fadigado
Nível de Treinamento da Planta	Nível de Treinamento Ruim
	Nível de Treinamento Bom

Tabela 24: Outras variáveis do modelo DFM

<b>Variáveis</b>	<b>Estados</b>
Indicador de Pressão ( <b>Etapa de</b>	Indefinido
	Muito Alta

<b>Monitoração)</b>	Alta
	Pouco Alta
	Normal
	Pouco Baixa
	Baixa
	Muito Baixa
Estado do Indicador ( <b>Etapa de Monitoração)</b>	Normal
	Falho
Nível de Pressão Previsto pelo Operador ( <b>Etapa de Monitoração e Entendimento da Situação)</b>	Incerto
	Muito Alta
	Alta
	Pouco Alta
	Normal
	Pouco Baixa
	Baixa
	Muito Baixa
Nível de Pressão Atual Considerado pelo Operador ( <b>Etapa de Monitoração e Entendimento da Situação)</b>	Incerto
	Muito Alta
	Alta
	Pouco Alta
	Normal
	Pouco Baixa
	Baixa
	Muito Baixa
Estado do Atuador	Normal

de Desarme Manual ( <b>Etapa de Execução</b> )	Falho
Decisão do Operador ( <b>Etapa de Planejamento</b> )	Iniciar o Desarme
	Não Iniciar o Desarme
Ação do Operador ( <b>Etapa de Execução</b> )	Realiza o Desarme
	Não Realiza o Desarme
Decréscimo de Pressão pelo Desarme Manual ( <b>Etapa de Execução</b> )	Com Décrécimo
	Sem Décrécimo

Em seguida são definidas as tabelas de decisão das CTA e CTR relacionadas à modelagem de confiabilidade humana.

A Tabela 25 mostra a relação entre a pressão e sua indicação na sala de controle em função do estado do indicador. A Tabela 26 explicita a lógica da primeira etapa do processo cognitivo: monitoração. Ela foi elaborada por inspeção. Nota-se que caso não haja um erro de monitoração, o estado atual da variável pressão é entendida pelo operador. Caso haja uma falha de instrumentação do indicador, o estado de pressão previsto pelo operador é dado como estado corrente desta variável por ele. O mesmo ocorre caso aconteça a ação insegura “Operador não lê a indicação de pressão”.

A Tabela 27 explicita as possíveis causas da ação insegura acima. Para a definição destas tabelas, é recomendável a utilização de discussões de especialistas

com auxílio da metodologia HAZOP [13, 17]. As tabelas do presente estudo foram definidas de maneira simplificada, por inspeção, seguindo o conhecimento adquirido na bibliografia. Na Tabela, na ocorrência do PSF “Operador fadigado”, admite-se que há a ocorrência da ação humana “Operador não lê a indicação de pressão”.

Tabela 25: CTA 9 do sistema analisado

Pressão	Estado do Indicador	Indicador de Pressão
-	Falho	Indefinido
Muito Alta	Normal	Muito Alta
Alta	Normal	Alta
Pouco Alta	Normal	Pouco Alta
Normal	Normal	Normal
Pouco Baixa	Normal	Pouco Baixa
Baixa	Normal	Baixa
Muito Baixa	Normal	Muito Baixa

Tabela 26: CTA 10 do sistema analisado

Modos de Falha de Monitoração	Nível de Pressão Previsto pelo Operador	Indicador de Pressão	Nível de Pressão Atual Considerado pelo Operador
Sem Erro	-	Muito Alta	Muito Alta
		Alta	Alta
		Pouco Alta	Pouco Alta
		Normal	Normal

		Pouco Baixa	Pouco Baixa
		Baixa	Baixa
		Muito Baixa	Muito Baixa
Operador não Lê a Indicação de Pressão	Incerto	-	Incerto
	Muito Alta		Muito Alta
	Alta		Alta
	Pouco Alta		Pouco Alta
	Normal		Normal
	Pouco Baixa		Pouco Baixa
	Baixa		Baixa
	Muito Baixa		Muito Baixa
-	Incerto	Indefinido	Incerto
	Muito Alta		Muito Alta
	Alta		Alta
	Pouco Alta		Pouco Alta
	Normal		Normal
	Pouco Baixa		Pouco Baixa
	Baixa		Baixa
	Muito Baixa		Muito Baixa

Tabela 27: CTA 11 do modelo analisado

Nível de Fadiga do Operador	Modos de Falha de Monitoração
Operador Fadigado	Operador não Lê a Indicação de Pressão



Operador Não Fadigado	Sem Erro
-----------------------	----------

A Tabela 28 explicita a lógica da terceira etapa do processo cognitivo: planejamento. Ela foi elaborada por inspeção. Nota-se que caso não haja um erro de planejamento, o operador toma a decisão correta de acionar a chave de desarme manual no caso de pressão “Muito Alta”. Caso haja uma falha no planejamento, o operador toma uma decisão errônea e admite-se que a lógica de desarme não é cumprida.

A Tabela 29, de maneira similar à Tabela 27, explicita as possíveis causas da ação insegura acima. Na tabela, na ocorrência do PSF “Operador fadigado” ou “Nível de treinamento ruim”, admite-se que há a ocorrência da ação humana “Operador toma uma decisão errônea”. Não existindo ambos os PSF, não há erro nesta etapa do processo cognitivo.

Tabela 28: CTA 12 do sistema analisado

Modos de Falha de Planejamento	Nível de Pressão Atual Considerado pelo Operador	<b>Decisão do Operador</b>
Operador Toma uma Decisão Errônea	Incerto	Iniciar o Desarme
	Muito Alta	Não Iniciar o Desarme
	Alta	Iniciar o Desarme

	Pouco Alta	Iniciar o Desarme
	Normal	Iniciar o Desarme
	Pouco Baixa	Iniciar o Desarme
	Baixa	Iniciar o Desarme
	Muito Baixa	Iniciar o Desarme
Sem Erro	Incerto	Não Iniciar o Desarme
	Muito Alta	Iniciar o Desarme
	Alta	Não Iniciar o Desarme
	Pouco Alta	Não Iniciar o Desarme
	Normal	Não Iniciar o Desarme
	Pouco Baixa	Não Iniciar o Desarme

	Baixa	Não Iniciar o Desarme
	Muito Baixa	Não Iniciar o Desarme

Tabela 29: CTA 13 do modelo analisado

Nível de Fadiga do Operador	Nível de Treinamento da Planta	<b>Modos de Falha de Planejamento</b>
Operador Fadigado	-	Operador Toma uma Decisão Errônea
-	Nível de Treinamento Ruim	Operador Toma uma Decisão Errônea
Operador Não Fadigado	Nível de Treinamento Bom	Sem Erro

A Tabela 30 explicita a lógica da quarta etapa do processo cognitivo: execução. Nota-se que caso não haja um erro de execução, o operador realiza a ação planejada por ele. Caso haja uma falha de execução, o operador não consegue implantar o desarme manual, se assim o quiser.

A Tabela 31, de maneira similar à Tabela 27, explicita as possíveis causas da ação insegura acima. Na Tabela, na ocorrência do PSF “Operador fadigado” ou condição da planta “Estado do atuador de desarme manual falho”, admite-se que há a

ocorrência da ação humana “Operador erra o acionamento do desarme manual”. Não existindo ambos os fatores, não há erro nesta etapa do processo cognitivo

Tabela 30: CTA 14 do sistema analisado

Modos de Falha de Execução	Decisão do Operador	Ação do Operador
Sem Erro	Iniciar o Desarme	Realiza o Desarme
Sem Erro	Não Iniciar o Desarme	Não Realiza o Desarme
Operador Erra o Acionamento do Desarme Manual	-	Não Realiza o Desarme

Tabela 31: CTA 15 do modelo analisado

Nível de Fadiga do Operador	Estado do Atuador de Desarme Manual	Modos de Falha de Execução
Operador Fadigado	-	Operador Erra o Acionamento do Desarme Manual
Operador Não Fadigado	Normal	Sem Erro
-	Falho	Operador Erra o Acionamento do Desarme Manual

A Tabela 32 explicita a lógica da segunda etapa do processo cognitivo: entendimento da situação. Nota-se que caso haja um erro de entendimento da situação, o operador não consegue prever o valor assumido pela variável pressão. Caso não haja nenhum erro, o operador segue a mesma lógica de transição de pressão executada pelo sistema digital explicitada na Tabela A.1.

A Tabela 33, de maneira similar à Tabela 27 explicita as possíveis causas da ação insegura acima. Na Tabela, na ocorrência do PSF “Operador Fadigado”, admite-se que há a ocorrência da ação humana “Operador constata uma situação de maneira errônea”. Não existindo o PSF, não há erro nesta etapa do processo cognitivo.

Tabela 32: CTR 2 do sistema analisado

Modos de Falha de Entendimento da Situação	Nível de Pressão Atual Considerado pelo Operador	<b>Nível de Pressão Previsto pelo Operador +</b>
Operador Constata uma Situação de Maneira Errônea	Muito Alta	Incerto
	Alta	
	Pouco Alta	
	Normal	
	Pouco Baixa	
	Baixa	
	Muito Baixa	
-	Incerto	Incerto
Sem Erro	Muito Alta	Pouco Baixa
	Alta	Pouco Baixa

	Pouco Alta	Pouco Baixa
	Normal	Normal
	Pouco Baixa	Pouco Alta
	Baixa	Pouco Baixa
	Muito Baixa	Baixa

Tabela 33: CTA 16 do modelo analisado

Nível de Fadiga do Operador	Modos de Falha de Entendimento da Situação
Operador Fadigado	Operador Constata uma Situação de Maneira Errônea
Operador Não Fadigado	Sem Erro

A Tabela 34 reflete simplesmente o decréscimo de pressão gerado pelo desarme manual. Esta variável, juntamente com a variável “Pressão”, representa o elo entre a modelagem DFM/ATHEANA da confiabilidade humana e do sistema digital.

Tabela 34: CTA 17 do modelo analisado

Ação do Operador	Decréscimo de Pressão pelo Desarme Manual
Realiza o Desarme	Com Decréscimo
Não Realiza o Desarme	Sem Decréscimo

## 8 ANÁLISE DFM/ATHEANA DO SISTEMA PROPOSTO

### 8.1 ANÁLISE DEDUTIVA

O modelo DFM/ATHEANA, após construído, pode ser analisado de duas formas: através do modo dedutivo, onde se define um evento topo de interesse e buscam-se as causas que levam a ele, ou através do modo indutivo onde condições iniciais são dadas e buscam-se as suas consequências [13, 14].

Para a análise de falhas do sistema, o modo dedutivo é o mais indicado. No sistema em questão, dois eventos topo são de interesse: “Pressão Muito Alta” e “Pressão Muito Baixa”, representando as falhas no controle do pressurizador e/ou falhas do operador em determinadas situações. Os HFE representam as falhas humanas relacionadas à perda da função de desarme do sistema considerado, conforme a definição do Capítulo 4. Para o sistema pode-se definir o HFE: “Falha do operador em acionar o desarme manual”. Segundo a Tabela 8, linhas 3 e 4, as ações humanas inseguras (UA) relacionadas a este HFE podem ser: “Falha do operador em iniciar o desarme manual” (EOO) e “Operador inicia desarme manual erroneamente” (EOC), representando as ações humanas relacionadas à perda de função do sistema de controle na ocorrência dos eventos topo de falha citados acima.

As Tabelas 35 e 36 ilustram como os dois eventos topos de falha podem ocorrer.

Tabela 35: Lógica do evento topo de falha "Pressão Muito Alta"

EOO (Falha do operador em iniciar o desarme manual)	Falha no Sistema de Controle	<b>Pressão Muito Alta</b>
Não ocorre	Não ocorre	Não ocorre
Não ocorre	Ocorre	Não ocorre
Ocorre	Não ocorre	Não ocorre
Ocorre	Ocorre	Ocorre

Tabela 36: Lógica do evento topo de falha "Pressão Muito Baixa"

EOC (Operador inicia desarme manual erroneamente)	Falha no Sistema de Controle	<b>Pressão Muito Baixa</b>
Não ocorre	Não ocorre	Não ocorre
Não ocorre	Ocorre	Ocorre
Ocorre	Não ocorre	Ocorre
Ocorre	Ocorre	Ocorre

Como observado, o evento topo de falha "Pressão Muito Alta" se comporta como um AND das falhas humana e do sistema. O evento topo de falha "Pressão Muito Baixa" se comporta como um OR das mesmas falhas.

Para a realização da análise, utilizou-se o *toolset* DYMONDA® disponibilizado pela empresa ASCA inc® [13].

Na primeira análise de "Pressão Muito Alta", busca-se o menor número de combinações de estados das variáveis chaves do sistema, ou implicativos diretos, que levem a esse evento topo de falha. Na forma de sentença do *toolset*:



- ***Pressure Very High @ t=0***

onde  $t=0$  é uma notação da ferramenta, indicando que o evento topo ocorre no instante final da análise. O resultado são 374 implicativos diretos. Mas, supondo que o analista tenha algumas informações acerca do *status* da planta antes da análise, estas podem servir como condições de contorno. Supondo que as informações consistam em que as válvulas, sprays, aquecedores, o indicador e o dispositivo de desarme manual estejam perfeitos, além da variável pressão se encontrar no estado “Muito Alta”, caracterizando a falha do sistema de controle:

- *Pressure was Very High @ t=-1 and*
- *Relief Valve State was Normal @ t=-1 and*
- *Safety Valve State was Normal @ t=-1 and*
- *Heaters State was Normal @ t=-1 and*
- *Indicator State was Normal @ t=-1 and*
- *Switch State was Normal @ t=-1 and*
- *Spray State was Normal @ t=-1*

onde  $t=-1$  representa a notação da ferramenta para um instante qualquer antes da mudança de pressão, o resultado são os 2 implicativos diretos explicitados na Tabela 37.

Tabela 37: Implicativos diretos do evento topo “Pressão Muito Alta”

#1	#2
<i>Pressão Muito Alta em t=-1</i>	<i>Pressão Muito Alta em t=-1</i>
<i>Válvula de Alívio Normal em t=-1</i>	<i>Válvula de Alívio Normal em t=-1</i>
<i>Válvula de Segurança Normal em t=-1</i>	<i>Válvula de Segurança Normal em t=-1</i>
<i>Aspersores Normais em t=-1</i>	<i>Aspersores Normais em t=-1</i>
<i>Aquecedores Normais em t=-1</i>	<i>Operador Não Fadigado em t=-1</i>
<i>Indicador Normal em t=-1</i>	<i>Indicador Normal em t=-1</i>
<i>Atuador do Desarme Manual Normal em t=-1</i>	<i>Atuador do Desarme Manual Normal em t=-1</i>
<i>Operador Fadigado em t=-1</i>	<i>Aquecedores Normais em t=-1</i>
<i>Sensor de Pressão Falho Baixo em t=-1</i>	<i>Sensor de Pressão Falho Baixo em t=-1</i>
	<i>Nível de Treinamento Ruim em t=-1</i>

Similarmente, para a análise de “Pressão Muito Baixa:

- **Pressure Very Low @ t=0**

o resultado são 90 implicativos diretos. Supondo que as condições de contorno consistam agora em o sensor de pressão, aquecedores, sprays, dispositivo de desarme manual e indicador estarem funcionando corretamente, além da variável pressão se encontrar no estado “Muito Baixa”, caracterizando a falha no sistema de controle:

- *Pressure was Very Low @ t=1 and*
- *Pressure Sensor State was Normal @ t=-1 and*
- *Heaters State was Normal @ t=-1*

- *Indicator State was Normal @ t=-1*
- *Switch State was Normal @ t=-1*
- *Spray State was Normal @ t=-1*

o resultado são os 3 implicativos diretos explicitados na Tabela 38. Observa-se que estes implicativos diretos refletem tanto estados normais quanto os estados falhos das variáveis e cada um deles representam um EFC da ATHEANA, pois constam de fatores humanos (PSF) e condições de operação da planta.

Tabela 38: Implicativos diretos do evento topo “Pressão Muito Baixa”

#1	#2	#3
<i>Pressão Muito Baixa em t=-1</i>	<i>Pressão Muito Baixa em t=-1</i>	<i>Pressão Muito Baixa em t=-1</i>
<i>Válvula de Segurança Normal em t=-1</i>	<i>Sensor de Pressão Normal em t=-1</i>	<i>Sensor de Pressão Normal em t=-1</i>
<i>Sensor de Pressão Normal em t=-1</i>	<i>Aspersores Normais em t=-1</i>	<i>Aspersores Normais em t=-1</i>
<i>Aspersores Normais em t=-1</i>	<i>Aquecedores Normais em t=-1</i>	<i>Aquecedores Normais em t=-1</i>
<i>Aquecedores Normais em t=-1</i>	<i>Indicador Normal em t=-1</i>	<i>Indicador Normal em t=-1</i>
<i>Indicador Normal em t=-1</i>	<i>Atuador do Desarme Manual Normal em t=-1</i>	<i>Atuador do Desarme Manual Normal em t=-1</i>
<i>Atuador do Desarme Manual Normal em t=-1</i>	<i>Válvula de Segurança Falha Aberta em t=-1</i>	<i>Operador Não Fadigado em t=-1</i>
<i>Operador Não Fadigado</i>		<i>Nível de Treinamento</i>

<i>em t=-1</i>		<i>Ruim em t=-1</i>
<i>Nível de Treinamento</i>		<i>Válvula de Segurança</i>
<i>Ruim em t=-1</i>		<i>Falha Fechada em t=-1</i>

A visualização da ocorrência dos eventos topo pelos implicativos diretos é feita através do modo indutivo (Figura 21).

## 8.2 ANÁLISE INDUTIVA

A melhor forma de se verificar a ocorrência dos eventos topo é realizar uma análise indutiva dando como parâmetros de entrada os implicativos diretos da análise anterior e verificando os passos executados pelo *toolset*. No modo indutivo, a cada linha, observa-se a assunção de valor de uma variável em função dos valores das demais variáveis nas linhas anteriores. Deste modo, é possível observar todo o desenvolvimento das condições iniciais até a ocorrência do evento topo. Realizando a análise do primeiro implicativo do evento topo “Pressão Muito Alta”:

<b>#1</b>
<i>Pressão Muito Alta em t=-1</i>
<i>Válvula de Alívio Normal em t=-1</i>
<i>Válvula de Segurança Normal em t=-1</i>
<i>Aspersores Normais em t=-1</i>
<i>Aquecedores Normais em t=-1</i>
<i>Indicador Normal em t=-1</i>
<i>Atuador do Desarme Manual Normal em t=-1</i>
<i>Operador Fadigado em t=-1</i>

*Sensor de Pressão Falho Baixo em t=-1*

No modo indutivo observam-se os passos executados como os ilustrados na Figura 21. Verifica-se que a falha do sensor de pressão em “Falho Baixo” provoca o acionamento dos aquecedores do sistema. A fadiga do operador provoca um erro de monitoração, entendimento da situação, planejamento e execução, segundo as premissas adotadas na modelagem do sistema no capítulo anterior. O erro de execução, em última instância, provoca o não acionamento do desarme manual. Como a pressão já se encontrava em um estado crítico e os aquecedores do sistema foram acionados, a pressão não é reduzida e o evento topo ocorre.

No segundo implicativo:

<b>#2</b>
<i>Pressão Muito Alta em t=-1</i>
<i>Válvula de Alívio Normal em t=-1</i>
<i>Válvula de Segurança Normal em t=-1</i>
<i>Aspersores Normais em t=-1</i>
<i>Operador Não Fadigado em t=-1</i>
<i>Indicador Normal em t=-1</i>
<i>Atuador do Desarme Manual Normal em t=-1</i>
<i>Aquecedores Normais em t=-1</i>
<i>Sensor de Pressão Falho Baixo em t=-1</i>
<i>Nível de Treinamento Ruim em t=-1</i>

Verifica-se no mesmo modo indutivo que o nível de treinamento ruim provoca uma falha no planejamento e uma decisão errônea do operador em não acionar o desarme manual. Esta falha associada à falha do sistema de controle em acionar os

aquecedores (devido à falha do sensor em “Falho Baixo”) e ao fato da pressão já se encontrar em seu estado crítico, leva à ocorrência do evento topo.

Esses dois implicativos demonstram a ocorrência do evento topo “Pressão Muito Alta” na ocorrência de ambos os acontecimentos: Falha humana E Falha de sistema, conforme a Tabela 35.

Analisando o primeiro implicativo do evento topo “Pressão Muito Baixa”:

<b>#1</b>
<i>Pressão Muito Baixa em t=-1</i>
<i>Válvula de Segurança Normal em t=-1</i>
<i>Sensor de Pressão Normal em t=-1</i>
<i>Aspersores Normais em t=-1</i>
<i>Aquecedores Normais em t=-1</i>
<i>Indicador Normal em t=-1</i>
<i>Atuador do Desarme Manual Normal em t=-1</i>
<i>Operador Não Fadigado em t=-1</i>
<i>Nível de Treinamento Ruim em t=-1</i>

Verifica-se que o nível de treinamento ruim provoca uma falha de planejamento e uma decisão errônea do operador em acionar o desarme manual. Esta falha leva à ocorrência do evento topo.

No segundo implicativo:

<b>#2</b>
<i>Pressão Muito Baixa em t=-1</i>
<i>Sensor de Pressão Normal em t=-1</i>
<i>Aspersores Normais em t=-1</i>

<i>Aquecedores Normais em t=-1</i>
<i>Indicador Normal em t=-1</i>
<i>Atuador do Desarme Manual Normal em t=-1</i>
<i>Válvula de Segurança Falha Aberta em t=-1</i>

Verifica-se que a falha da válvula de segurança em “Falha Aberta” e o fato da pressão já se encontrar em seu estado crítico, leva à ocorrência do evento topo.

No terceiro implicativo:

<b>#3</b>
<i>Pressão Muito Baixa em t=-1</i>
<i>Sensor de Pressão Normal em t=-1</i>
<i>Aspersores Normais em t=-1</i>
<i>Aquecedores Normais em t=-1</i>
<i>Indicador Normal em t=-1</i>
<i>Atuador do Desarme Manual Normal em t=-1</i>
<i>Operador Não Fadigado em t=-1</i>
<i>Nível de Treinamento Ruim em t=-1</i>
<i>Válvula de Segurança Falha Fechada em t=-1</i>

Verifica-se que o nível de treinamento ruim provoca uma falha de planejamento e uma decisão errônea do operador em acionar o desarme manual. Esta falha leva à ocorrência do evento topo.

Desta maneira é possível a visualização de quais ações inseguras ocorrem dentro de um determinado EFC (implicativo direto).

Os três implicativos acima demonstram a ocorrência do evento topo “Pressão Muito Baixa” na ocorrência de pelo menos um dos acontecimentos: Falha humana (Ex: implicativo #1) OU falha de sistema (Ex: implicativo #2), conforme Tabela 36.

Em termos de quantificação para a ATHEANA, podem-se separar os implicativos diretos analisados em PC (Condições da planta), PSF e ações humanas como nas Tabelas 39, 40, 41 e 42. Nota-se que o segundo implicativo do evento topo pressão “Muito Baixa” não tem importância na análise de falhas humanas ATHEANA, pois se trata de um implicativo refletindo uma falha unicamente do sistema digital de controle.

Esses implicativos são utilizados para a elaboração dos questionários necessários à quantificação pela ATHEANA apresentados no capítulo seguinte.

Tabela 39: Implicativo #1 para quantificação pela ATHEANA

<b>PC(s)</b>	<b>PSF(s)</b>	<b>Ações Humanas</b>
<i>Nível de Pressão Muito Alto</i>	<i>Operador Fadigado</i>	<i>Operador Toma uma Decisão Errônea</i>
Válvula de Segurança Normal		<i>Operador não Checa o Indicador</i>
Indicador de Pressão Normal		<i>Operador Erra o Dispositivo de Acionamento Manual</i>
Aquecedores Normais		<i>Operador Constata uma Situação de Maneira Errônea</i>
Aspersores Normais		
Válvula de Alívio Normal		
<i>Sensor de Pressão Falho</i>		
Atuador do Desarme Manual Normal		



Tabela 40: Implicativo #2 para quantificação pela ATHEANA

<b>PC(s)</b>	<b>PSF(s)</b>	<b>Ações Humanas</b>
<i>Nível de Pressão Muito Alto</i>	<i>Planta com Mau Treinamento</i>	<i>Operador Toma uma Decisão Errônea</i>
Atuador do Desarme Manual Normal		
Indicador de Pressão Normal		
Aquecedores Normais		
Aspersores Normais		
Válvula de Alívio Normal		
Válvula de Segurança Normal		
<i>Sensor de Pressão Falho</i>		

Tabela 41: Implicativo #3 para quantificação pela ATHEANA

<b>PC(s)</b>	<b>PSF(s)</b>	<b>Ações Humanas</b>
<i>Nível de Pressão muito Baixo</i>	<i>Planta com Mau Treinamento</i>	<i>Operador uma Toma Decisão Errônea</i>
Sensor de Pressão Normal		
Indicador de Pressão Normal		
Aquecedores Normais		
Aspersores Normais		
Válvula de alívio Normal		
Válvula de Segurança Normal		
Atuador do Desarme Manual Normal		

Tabela 42: Implicativo #4 para quantificação pela ATHEANA

<b>PC(s)</b>	<b>PSF(s)</b>	<b>Ações Humanas</b>
<i>Nível de Pressão Muito Baixo</i>	<i>Planta com Mau Treinamento</i>	<i>Operador uma Toma Decisão Errônea</i>
Atuador do Desarme Manual Normal		
Indicador de Pressão Normal		
Aquecedores Normais		
Aspersores Normais		
Válvula de Alívio Normal		
Sensor de Pressão Normal		
<i>Válvula de Segurança Falha</i>		

A análise dedutiva da DFM/ATHENA possibilita a visualização das interações entre todos os componentes do sistema em questão de forma dinâmica considerando, por exemplo, o sequenciamento de estados dos mesmos. Estes são aspectos importantes na modelagem de sistemas digitais. Nos implicativos acima, por exemplo, verificam-se as interações entre o sistema de controle, formado pelo sensor, atuadores e *software* (implícito na lógica que comanda algumas tabelas de decisão), o processo controlado (variável de pressão) e as ações do operador.

Uma vez construído o modelo DFM/ATHEANA, pode ser analisado inúmeras vezes através de seus dois modos, tornando-se uma ferramenta eficaz no estudo de falhas e especificações do sistema.

**Forward Trace Results**

File

Start Time:  End Time:

Results Intermediate Results

```

Initial State:
Pressure (0)   Sensor State (0)   Spray State (0)   Safety Valve State (0)   Relief Valve State (0)
3             0                   0                 1                         0

Timestep 0: Determine Safety Valve
Pressure (0)   Sensor State (0)   Spray State (0)   Safety Valve State (0)   Relief Valve State (0)   Safety Valve (0)
3             0                   0                 1                         0                       0

Timestep 0: Determine Relief Valve
Pressure (0)   Sensor State (0)   Spray State (0)   Safety Valve State (0)   Relief Valve State (0)   Relief Valve (0)
3             0                   0                 1                         0                       0

Timestep 0: Determine Heater
Pressure (0)   Sensor State (0)   Spray State (0)   Safety Valve State (0)   Relief Valve State (0)   Heater (0)
3             0                   0                 1                         0                       1

Timestep 0: Determine Spray
Pressure (0)   Sensor State (0)   Spray State (0)   Safety Valve State (0)   Relief Valve State (0)   Spray (0)
3             0                   0                 1                         0                       0

```

Figura 21: Passos executados pelo *tool/set* no modo indutivo

## 9 OPINIÕES DE ESPECIALISTAS E AGREGAÇÃO FUZZY DOS RESULTADOS

### 9.1 QUESTIONÁRIOS APLICADOS

Os implicativos obtidos no capítulo anterior foram a base para o desenvolvimento dos questionários necessários à quantificação pela ATHEANA. Seguindo os princípios explicitados no Capítulo 5, acerca da elaboração de questionários, procurou-se da maneira mais simples e lógica possível obter os dados necessários à quantificação da Eq (1):

$$P(\text{HFE}|\text{S}) = \sum_j \sum_{i(j)} P(\text{EFC}_i|\text{S}) * P(\text{UA}_j|\text{EFC}_i, \text{S})$$

onde, no estudo em questão,  $j=1,2$ ,  $\text{UA}_1$ : Falha do operador em iniciar o desarme manual (EOO) e  $\text{UA}_2$ : Operador inicia desarme manual erroneamente (EOC), representando os atos inseguros relacionados ao HFE estudado (Falha do operador em acionar o desarme manual). Com relação aos contextos,  $i=1,2$  e  $\text{EFC}_{11}$  e  $\text{EFC}_{12}$  são os implicativos das Tabelas 39 e 40, respectivamente.  $\text{EFC}_{21}$  e  $\text{EFC}_{22}$  são os implicativos das Tabelas 41 e 42. Procurou-se obter dos especialistas as opiniões acerca das frequências de ocorrência dos contextos (PSF e condições da planta) e probabilidades de ocorrência das ações humanas inseridas nestes contextos e identificadas nos implicativos diretos (Tabelas 39 a 42), que em última instância, levam à ocorrência dos atos inseguros e ao HFE relacionado. 12 especialistas foram contatados. 10 deles aceitaram participar do processo de elicitación. Procurou-se uma diversidade das opiniões através da busca por diferentes perfis de atuação. Os questionários foram enviados por email aos participantes. Estes questionários foram

elaborados com questões agrupadas, textos simples e com sentenças lógicas. Para cada contexto, perguntou-se a sua frequência de ocorrência e a probabilidade de ocorrência das ações inseguras, identificadas nos implicativos diretos. Foi dada uma breve descrição do cenário e solicitou-se que cada especialista marcasse a opção que achasse a mais correta. As escalas seguiram um padrão linguístico, facilitando a aquisição dos dados e das incertezas, que foram tratadas posteriormente com a teoria *fuzzy*. Um campo para observações foi reservado para complementação da opinião. O modelo final pode ser visto no Apêndice D. Dois pontos merecem destaque:

- Segundo o guia da ATHEANA [6], a descrição das interações entre  $n$  ações humanas secundárias em um mesmo contexto que levam aos UA de interesse ainda não foram formalmente abordadas e definidas. Embora isso ocorra, o mesmo guia recomenda que tais interações sejam consideradas. Nos questionários, as interações entre ações humanas foram consideradas através da arguição em forma de conjunção das mesmas, dado um determinado contexto. Desta forma as dependências ficam implícitas nas opiniões.
- Como visto, um implicativo direto é a conjunção mínima de fatores que levam ao evento topo. Esses fatores englobam tanto as situações normais (elementos em funcionamento) quanto as anormais (elementos falhos). Nos questionários, porém, tendo em vista a simplicidade na sua elaboração, foram arguidos somente os fatores anormais. Os fatores normais são considerados implicitamente, por dedução.

Como foram considerados os pesos das opiniões de cada especialista para a etapa de agregação (vide Capítulo 5) foi elaborado um questionário baseado em [37]. Nele constam diversas questões que classificam o especialista segundo o esquema de

pontuação apresentado no Apêndice E (Este esquema de pontuação não é exposto ao especialista). Para cada subitem (e para cada item em última instância), o especialista recebe uma pontuação. Essa pontuação segue uma lógica de encaixe de perfil ao assunto abordado. O peso de cada questão foi arbitrado baseado no trabalho desenvolvido em [37] com adaptações. Ao final, a pontuação de cada especialista foi normalizada, refletindo o peso de cada um [37]. O questionário do Apêndice E também possibilitou um mapeamento dos perfis dos especialistas, ilustrado na Figura 22.

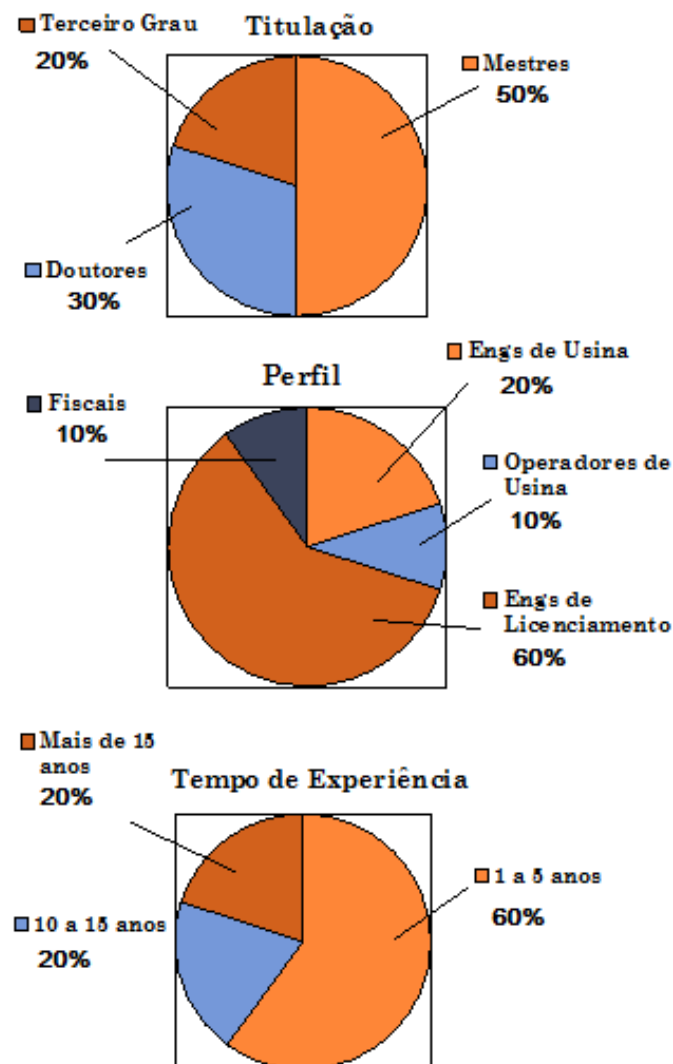


Figura 22: Mapeamento dos perfis dos especialistas

No mapeamento constatou-se a heterogeneidade de opiniões. A grande maioria delas são advindas de especialistas com pouco tempo de experiência (1 a 5 anos). Porém a maior parte dos *experts* tem formação específica na área de atuação (mestrado ou doutorado). Operadores e engenheiros de usina, detentores do conhecimento acerca da operação da planta, são a menor parte dos dez especialistas consultados.

O processo de elicitación dos especialistas durou 6 meses e foi a etapa mais demorada de todo o trabalho.

## 9.2 RESPOSTAS E AGREGAÇÃO DAS OPINIÕES

A Tabela F.1 do Apêndice F ilustra as opiniões obtidas de dez especialistas na área nuclear. Estas opiniões foram obtidas através dos questionários descritos no parágrafo anterior. A Tabela F.2 ilustra a pontuação obtida para cada especialista no mapeamento de perfil. A Tabela 43 ilustra os respectivos pesos, obtidos através de normalização das pontuações totais obtidas nos questionários, para cada *expert*.

Tabela 43 – Pesos das opiniões dos especialistas consultados

<b>ESPECIALISTA</b>	<b>Peso</b>
E1	8%
E2	8%
E3	13%
E4	8%
E5	6%
E6	15%
E7	8%
E8	14%
E9	16%
E10	5%

Para o processo de coleta de opiniões em formato *fuzzy*, fez-se necessária a definição dos intervalos *fuzzy* para cada variável linguística. Baseado na experiência obtida na Ref [34] e nos valores recomendados em [5-6], estabeleceram-se os intervalos ilustrados na Tabela 44

Tabela 44 – Intervalos *fuzzy* utilizados na coleta de opiniões

<b>Probabilidade de ocorrência das ações</b>	<b>Intervalo <i>fuzzy</i></b>		
<b>Muito Alta</b>	0,1	0,55	1
<b>Alta</b>	0,01	0,255	0,5
<b>Moderada</b>	0,001	0,0505	0,1
<b>Baixa</b>	0,0001	0,00505	0,01
<b>Muito Baixa</b>	0,000005	0,0005025	0,001
<b>Frequência de ocorrência dos contextos</b>	<b>Intervalo <i>fuzzy</i></b>		
<b>Muito Alta</b>	0,9	0,95	1
<b>Alta</b>	0,55	0,75	0,95
<b>Moderada</b>	0,35	0,5	0,65
<b>Baixa</b>	0,05	0,25	0,45
<b>Muito Baixa</b>	0	0,05	0,1

Após a definição dos intervalos *fuzzy*, o método da Ref [44] foi aplicado nas opiniões da Tabela F.1 do Apêndice F. A primeira etapa de cálculo dos índices de similaridade das opiniões envolve primeiramente o cálculo dos centróides das opiniões *fuzzy*, Eq (2). Este cálculo está explícito na Tabela F.3. A Tabela F.4 ilustra o cálculo dos índices de similaridade entre as opiniões dos especialistas, calculados dois a dois conforme a Eq (3). As Tabelas F.5 e F.6 ilustram o cálculo das Eqs (4) e (5) na busca dos índices médios de concordância e de concordância relativa. A Tabela F.7 implanta a Eq (6) no cálculo do grau de consenso entre as opiniões. Para a realização deste cálculo, fez-se necessária a definição do coeficiente de consenso  $\beta$  entre os especialistas. Este coeficiente pondera a parcela que considera o peso da opinião de cada especialista juntamente com a parcela do grau de consenso calculado na Eq (5).



Para fins práticos, este coeficiente foi considerado como  $\beta=0,5$  [44]. Foram utilizados os pesos de cada especialista obtidos na Tabela 43 neste cálculo. Por fim, a Tabela 45 ilustra as opiniões *fuzzy* agregadas após todo o processo segundo a Eq (7). Observam-se os intervalos de probabilidade obtidos para cada fator quantificado.

Tabela 45 – Opiniões fuzzy agregadas

<b>C#1</b>			<b>A#1 C#1</b>		
5,58%	17,67%	29,75%	1,11%	13,54%	25,97%
<b>C#2</b>			<b>A#2 C#2</b>		
10,83%	25,86%	40,89%	0,88%	9,50%	18,12%
<b>C#3</b>			<b>A#3 C#3</b>		
10,15%	27,26%	44,37%	0,36%	10,41%	20,45%
<b>C#4</b>			<b>A#4 C#4</b>		
7,12%	23,30%	39,49%	1,10%	13,38%	25,66%

Onde C# representa um dos contextos encontrados nos implicativos diretos e A# compreende algum dos atos inseguros encontrados.

### 9.3 CÁLCULO DA PROBABILIDADE DO HFE

O cálculo da probabilidade do HFE, segundo a Eq (1), é realizado com o auxílio da álgebra dos números fuzzy, permitindo a adição, multiplicação e divisão destes números [40, 87-89, 101-103]. A Tabela 46 mostra o intervalo de probabilidade do HFE “Falha do operador em acionar o desarme manual”.

Tabela 46 – Probabilidade fuzzy do HFE estudado.

P(HFE )		
0,27%	10,80%	34,34%

Observa-se a ocorrência do HFE com uma probabilidade de até 34,34%. A variância entre os valores do intervalo fuzzy é fruto das propagações das variâncias de cada fator calculado na etapa de agregação. Essas variações decorrem de diversos fatores. Simplificações e suposições na modelagem inicial, método de elicitação utilizado, qualidade do processo de elicitação, incertezas epistemológicas no processo heurístico dos especialistas, nível de conhecimento atrelado ao perfil de cada especialista, definições dos intervalos fuzzy e o peso das opiniões são alguns dos fatores a serem citados. Para uma verificação da consistência dos resultados foi realizada uma análise comparativa com dados da literatura (seção 9.4).

Para a incorporação dos resultados em uma APS, podem ser utilizados os métodos explicitados no Capítulo 4 e Figura 9.

Pela Eq (1) observa-se que a conjunção das probabilidades de ocorrência dos contextos e das ações errôneas, dado um determinado cenário, são cortes mínimos do HFE em questão. Desta forma, é possível realizar um estudo de importância de cada ação(ões) humana(s) e/ou contextos na ocorrência de um HFE. Utilizando novamente a álgebra *fuzzy* [101-103], observa-se a importância de cada fator na quantificação na Tabela 47.

Tabela 47 – Análise de importância de cada fator da quantificação pela ATHEANA

IMPORTÂNCIA NO HFE	
C#1(A#1 C#1)	22,14%
C#2(A#2 C#2)	22,74%
C#3(A#3 C#3)	26,26%
C#4(A#4 C#4)	28,86%

Novamente, para as decisões baseadas em risco, estas análises de importância indicam o foco que deve ser dado nas melhorias a serem implantadas. Nos resultados expostos acima, por exemplo, um enfoque poderia ser dado na melhoria das condições da planta e fatores condicionantes do C#4 (Contexto 4) e nos procedimentos e treinamentos relacionados à A#4 (Ação insegura #4).

## 9.4 COMPARAÇÃO COM DADOS DA LITERATURA

Uma comparação com dados de falhas humanas encontrados na literatura foi realizada visando verificar a coerência dos resultados obtidos. Em alguns casos estes dados não estavam disponíveis. A comparação consistiu em verificar os dados de probabilidade das ações humanas encontradas no modelo com os dados de diversas fontes. A Tabela 48 sumariza este estudo.




As células em branco na Tabela 48 indicam a concordância entre os dados, ou seja, que os dados encontrados na literatura se situam dentro do intervalo *fuzzy* calculado no estudo. As células em cinza indicam a discordância. Os dados encontrados na Ref [105] e Ref [99] estão fora dos intervalos (0,81 % para a ação A#1 e 0,80 % para a ação A#4, em termos absolutos, em comparação com os extremos mínimos dos intervalos das ações). O mesmo ocorre para a ação A#2 (0,88 % para os dados encontrados nas Refs [100], [105] e [99], e 0,75 % para os dados encontrados na Ref [106], em termos absolutos, em comparação com o extremo mínimo do intervalo). Para a ação A#3, os dados encontrados na Ref [106] estão dentro do intervalo. Os dados encontrados nas Refs [105] e [99] estão fora do intervalo por 0,06 %, em termos absolutos, em comparação com o extremo mínimo do intervalo. Os dados encontrados na Ref [100] estão fora do intervalo em 1,55 %, em termos absolutos, em comparação com o extremo máximo do intervalo.

As discrepâncias vêm dos fatores discutidos anteriormente no cálculo da  $P(HFE)$ . Além disso, os dados da literatura são não homogêneos (advindos de diferentes processos de estimação), e este fato contribui para a variância observada. Mesmo com essas restrições, os resultados indicam uma boa concordância com os dados registrados nas fontes consultadas, já que apenas pequenas discrepâncias foram detectadas .

Tabela 48 – Comparação dos dados de falha com dados da literatura

				REF [75]	REF [104]	REF [105]	REF [99]	REF [100]	REF [106]	REF [107]
<b>A#1</b>	1,11%	13,54%	25,97%	5,00%	XXX	0,30%	0,30%	22,00%	16,00%	XXX
<b>A#2</b>	0,88%	9,50%	18,12%	XXX	XXX	~0,00%	~0,00%	~0,00%	0,13%	XXX
<b>A#3</b>	0,36%	10,41%	20,45%	5,00%	XXX	0,30%	0,30%	22,00%	16,00%	XXX
<b>A#4</b>	1,10%	13,38%	25,66%	5,00%	XXX	0,30%	0,30%	22,00%	16,00%	XXX

	DADOS NÃO DISPONÍVEIS
	DADOS DENTRO DO INTERVALO
	DADOS FORA DO INTERVALO

## 10 CONCLUSÕES E RECOMENDAÇÕES

O presente trabalho consistiu no estudo da metodologia DFM (*Dynamic Flowgraph Methodology*) integrada à técnica ATHEANA (*A Technique for Human Error Analysis*) na modelagem da confiabilidade de sistemas digitais e de suas interações com o operador, de maneira qualitativa e quantitativa.

A metodologia DFM é indicada pela NRC na modelagem do comportamento dinâmico das principais variáveis de um sistema digital. A ATHEANA também é indicada pela NRC como apta a modelar o comportamento humano dentro de contextos da planta. Ambas se preocupam com a incorporação dos resultados a uma APS.

Durante a realização do trabalho, verificou-se a necessidade de uma equipe multidisciplinar, tanto na modelagem quanto na análise de sistemas com topologias complexas e um número muito grande de variáveis. Embora o sistema estudado tenha sido de topologia simples e com poucas variáveis, fez-se necessário o uso de um número grande de simulações e análises na fase de modelagem. Com mais variáveis, certamente o modelo estaria mais refinado e fidedigno à realidade, porém isto demandaria um número muito maior de especialistas, o que não foi o objetivo deste trabalho. Na análise propriamente dita do modelo, as inúmeras combinações de estados que levaram aos eventos topo demandam uma averiguação minuciosa e demorada da consistência dos resultados. Constata-se, portanto que um pleno conhecimento do sistema e das metodologias/técnicas aplicadas é necessário e que uma diversidade de conhecimento tanto na modelagem quanto na análise do sistema também é imprescindível. Por outro lado, uma vez construído, o modelo torna-se uma ferramenta eficaz na análise de riscos do sistema, gerando resultados consistentes em tempo computacional. Estes resultados são de suma importância nas decisões baseadas no risco no âmbito da confiabilidade de sistemas digitais e no estudo da

confiabilidade humana. A DFM/ATHEANA mostra-se eficaz na modelagem das interações dos diversos componentes de um sistema digital tais como sensores, atuadores, *software* (implícito na lógica que comanda algumas tabelas de decisão), variáveis de processo e as ações do operador, sendo elas pré, iniciadoras ou pós-iniciadoras de eventos. Através dos implicativos diretos, ela possibilita a visualização dos possíveis estados do sistema. Sua análise dedutiva permite um estudo de falhas eficiente, rastreando as causas de um evento topológico dado. Sua análise indutiva pode ser utilizada na mitigação de falhas encontradas na análise dedutiva, bem como para a verificação de especificações do sistema. No âmbito da construção do modelo, técnicas de modularização podem ser desenvolvidas a fim de tornar possível o uso de *templates* e consequente facilitação no processo de modelagem.

Na confiabilidade humana, a DFM, juntamente com a técnica ATHEANA, consegue modelar  $n$  modos de falha para equipamentos e seres humanos (EEO e EOC), além de  $n$  fatores que influenciam o desempenho humano. A DFM facilita o processo intermediário da ATHEANA de buscas dos contextos que provocam falhas humanas através de seu modo dedutivo. No modo indutivo, a DFM facilita a busca por falhas humanas associadas, gerando então os fatores necessários à quantificação da ATHEANA. Futuros trabalhos envolvendo a metodologia DFM/ATHEANA em sistemas de topologia complexa e com um número maior de operadores são sugestões de estudos para a evolução no campo da confiabilidade humana em sistemas dinâmicos.

Na quantificação dos resultados, o uso da teoria dos conjuntos *fuzzy* possibilitou a manipulação de variáveis linguísticas no processo de coleta de opiniões de especialistas indicado pela ATHEANA como a melhor opção para a quantificação. A teoria fuzzy já está consagrada e utilizada em diversas áreas inclusive na coleta e agregação de opiniões de especialistas. A experiência obtida nesta última foi utilizada e sua importância foi constatada. Fez-se necessário também o estudo da álgebra fuzzy (adição, produto, e divisão dos números) para a manipulação dos resultados, o que não apresentou maiores dificuldades.

No processo de coleta e agregação das opiniões, fez-se necessária uma busca pela melhor elaboração dos questionários e escolha dos participantes. Novamente, foi utilizada a experiência obtida em estudos anteriores. Na escolha e convocação dos especialistas, verificou-se o quanto o processo é trabalhoso e demorado, constatando-se então a necessidade de se trabalhar com uma margem de erro no número de participantes, devido às desistências, e também com uma margem de erro no prazo estipulado para a obtenção das opiniões. Esta etapa foi a mais demorada e não dependeu exclusivamente do autor deste trabalho o que, em outras circunstâncias, poderia comprometer o resultado final. Trabalhos futuros envolvendo a coleta de opiniões devem levar em consideração estes aspectos e a experiência obtida em todos os trabalhos envolvendo este processo.

Os resultados obtidos foram alvo de comparações com dados da literatura e constataram-se discrepâncias. Estas discrepâncias têm como fundamentação diversos fatores tais como: simplificações e suposições na modelagem inicial, método de elicitação utilizado, qualidade do processo de elicitação, incertezas epistemológicas no processo heurístico dos especialistas, nível de conhecimento atrelado ao perfil de cada especialista, definições dos intervalos fuzzy e o peso das opiniões. Mesmo com essas restrições, os resultados indicaram uma boa concordância com os dados registrados nas fontes consultadas. Futuramente, análises de sensibilidade dos diferentes fatores podem ser implantadas: diferentes técnicas de elicitação e agregação de opiniões podem ser aplicadas e as variações nos resultados analisadas. O impacto do número de opiniões e da qualidade dos participantes nos resultados pode ser verificado. Também podem ser analisados os resultados advindos da participação de integrantes de uma só classe (operadores, por exemplo) no processo de coleta de opiniões. A busca por definições de intervalos fuzzy a serem aplicados em estudos semelhantes pode ser consolidada.

Como sugestões de trabalhos, sistemas *benchmark* que possuam informações de falhas já estudadas podem ser analisados utilizando a metodologia deste trabalho,



tendo seus resultados comparados com os dados já encontrados. As demais técnicas/metodologias de análise de falhas de sistemas digitais e/ou confiabilidade humana podem ser combinadas e seus resultados podem ser comparados com dados da literatura ou com os resultados deste trabalho além das informações presentes nos demais estudos envolvendo o tema.

Sistemas de diversas topologias podem ser analisados utilizando a abordagem deste trabalho, tendo a preocupação de reunir um número de especialistas suficiente para a modelagem e análise. Trabalhos futuros podem incluir o desenvolvimento de ferramentas computacionais para a incorporação automática dos resultados das análises aos relatórios de APS.

Deste modo, o presente estudo contribui para a literatura como um trabalho das abordagens DFM/ATHEANA na análise de confiabilidade de sistemas digitais e na análise de confiabilidade humana. O trabalho é uma primeira tentativa de preencher a lacuna existente na literatura com relação à modelagem e análise sistêmica, tanto no âmbito dos sistemas digitais, quanto no âmbito da confiabilidade humana, na sua abordagem qualitativa. A complementação dos resultados obtidos através de coleta de opiniões de especialistas em conjunto com a teoria fuzzy gerou resultados que podem ser incorporados à APS, facilitando as decisões baseadas no risco.

## REFERÊNCIAS BIBLIOGRÁFICAS

- [1] ALDEMIR, T., BUCCI, P., MANGAN, L. T., *et al.*, *Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plants*, NUREG/CR-6901, U.S Nuclear Regulatory Commission, Washington DC, 2006.
- [2] STAMATELATOS, M., *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*, Chapter 11, NASA, Washington D.C, 2002.
- [3] SPURGIN, J., *Human Reliability Assessment Theory and Practice*, 1 ed, Florida, CRC Press, 2010.
- [4] GOMES, E., *Análise de Confiabilidade Humana de Procedimentos de Radioterapia Via Redes Bayesianas*, Tese de Doutorado, Programa de Engenharia Nuclear, COPPE/UFRJ, Rio de Janeiro, 2011.
- [5] NASCIMENTO, C. S., MESQUITA, R. N., *A Human Error Probability Estimate Methodology Based on Fuzzy Inference and Expert Judgment on Nuclear Plants*, INAC 2009, Rio de Janeiro, Outubro de 2009.
- [6] FORESTER, J., COOPER, S., LOIS, E., *et al.*, *ATHEANA User's Guide*, NUREG-1880, U.S Nuclear Regulatory Commission, Washington DC, 2007.
- [7] BELL, J., HOLROYD, J., *Review of Human Reliability Assessment Methods*, Health and safety Laboratory, HSE Books, 1 ed, Buxton, 2009.
- [8] FORESTER, J., BYE, A., DANG, V., *et al.*, *An Empirical Study of HRA Methods Overall Design and Issues*, IEEE Eight Conference on Human Factors and Power Plants, California, August, 2007.
- [9] ZIO, E. *Reliability Engineering: Old Problems and New Challenges*, *Reliability Engineering and System Safety*, v. 94, pp. 125-141, 2009.
- [10] FUJITA, Y., HOLLNAGEL, H., *Failures without Errors: Quantification of Context in HRA*, *Reliability Engineering and System Safety*, v. 83, pp. 145-151, 2004.

- [11] LIAO,H., CHANG, J., *Human Performance in Control Rooms of Nuclear Power Plants: A Survey Study*, Human Factors and Ergonomics in Manufacturing & Service Industries, v. 21, pp. 412-428, August, 2011.
- [12] HOLLNAGEL, H., *Cognitive Reliability and Error Analysis Method*, Elsevier Science, New York, 1998.
- [13] GUARRO, S., YAU, M., MOTAMED, M., *Development of Tools for Safety Analysis of Control Software in Advanced Reactors*, NUREG/CR-6465, U.S Nuclear Regulatory Commission, Washington DC, 1996.
- [14] GUARRO, S., ALDEMIR, T., YAU, M., *Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments*, NUREG/CR-6942, U.S Nuclear Regulatory Commission, Washington DC, 2007.
- [15] GARRET, C. J., APOSTOLAKIS, G., *Automated Hazard Analysis of Digital Control Systems*, *Reliability Engineering and System Safety*, v. 77, pp. 1-17, 2002.
- [16] YAU, M., APOSTOLAKIS G., GUARRO, S., *The Use of Prime Implicants in Dependability Analysis of Software Controlled Systems*, *Reliability Engineering and System Safety*, v. 62, pp. 23-32, 1998.
- [17] GUARRO, S., ALDEMIR, T., MANDELLI, D., *A Benchmark Implementation of Two Dynamic Methodologies for the Reliability Modeling of Digital Instrumentation and Control Systems*, NUREG/CR-6985, U.S Nuclear Regulatory Commission, Washington DC, 2009.
- [18] GUARRO, S., MILICI, A., MULVIHILL, R., *Extending the Dynamic Flowgraph Methodology (DFM) to Model Human Performance and Team Effects*, NUREG/CR-6710, U.S Nuclear Regulatory Commission, Washington DC, 2001.
- [19] LIXUAN, L., AL-DABBAGH, A., *Dynamic Flowgraph Modeling of Process and Control Systems of a Nuclear Based Hydrogen Production Plant*, *International Journal of Hydrogen Energy*, v. 35, pp. 9569-9580, 2010.

- [20] APOSTOLAKIS, G., GARRET, G., *Context in the Risk Assessment of Digital Systems, Risk Analysis*, v. 19, N 1, pp. 23-32, 1999.
- [21] LIXUAN, L., AL-DABBAGH, A., *Reliability Modeling of Networked Control Systems Using Dynamic Flowgraph Methodology, Reliability Engineering and System Safety*, v. 95, pp. 1202-1209, 2010.
- [22] GUARRO, S., GARRET, C., APOSTOLAKIS, G., *The Dynamic Flowgraph Methodology for Assessing the Dependability of Embedded Software Systems, IEEE Transactions on Systems. Man. And Cybernetics*, v. 25, NO 5, pp. 824-840, 1995.
- [23] FORESTER, J., COOPER, S., SIU, N., *et al.*, *Expert Elicitation Approach for Performing ATHEANA Quantification, Reliability Engineering and System Safety*, v. 83, pp. 207-220, 2004.
- [24] THOMPSON, C., COOPER, S., BLEY, D., *et al.*, *The Application of ATHEANA: A Technique for Human Error Analysis, IEEE Sixth Annual Human Factors Meeting*, Orlando FL, June 1997.
- [25] THOMPSON, C., COOPER, S., BLEY, D., *et al.*, *Knowledge-base for the New Human Reliability Analysis Method, ATHEANA, International topical meeting on probabilistic safety assessment - moving toward risk based regulation*, Park City UT, October 1996.
- [26] FORESTER, J., WHITEHEAD, D., KOLACZKOWSKI, A., *et al.*, *Philosophy of ATHEANA, Second International Workshop on Human Reliability Models*, Seattle WA, March 1999.
- [27] MULLIN, T., *Experts' Estimation of Uncertain Quantities and its Implications for Knowledge Acquisition, IEEE Transactions on Systems. Man. And Cybernetics*, v. 19, NO 3, pp. 616-625, 1989.
- [28] KLIR, J., AYUUB, B., *Uncertainty Modeling and Analysis in Engineering and the Sciences, Chapman and Hall*, 2006.

- [29] MARTINO, J., *Technological Forecasting for Decision Making*, 3 ed, Mcgraw-Hill, Dayton, Ohio, 1993.
- [30] LEAL, J., WORDSWORTH, S., LEGOOD, R., et al., *Eliciting Expert Opinion for Economic Models: An Applied Example*, *Value in Health*, v. 10, NO 3, pp. 195-203, 2007.
- [31] XEXEO, G., *Fuzzy Logic, Computing Science Department and Systems and Computing Engineering Program*, UFRJ, Rio de Janeiro, 2002.
- [32] ZIO, E., BARALDI, P., LIBRIZZI, M., et al., *A Fuzzy set-based Approach for Modeling Dependence Among Human Errors*, *Fuzzy Sets and Systems*, v. 160, pp. 1947-1964, 2009.
- [33] KARIMI I., HULLERMEIER, E., *Risk Assessment System of Natural Hazards: A new approach based on Fuzzy Probability*, *Fuzzy Sets and Systems*, v. 158, pp. 987-999, 2007.
- [34] LI, Z., LI-CAO, D., GUO-HUA, C., *Fuzzy Logic-based Approach for Identifying the Risk Importance of Human Error*, *Safety Science*, v. 48, pp. 902-913, 2010.
- [35] KIRANOUDIS, C., MARKATOS, N., NIVOLIANITOU, Z., et al., *A Fuzzy Modeling Application of CREAM Methodology for Human Reliability Analysis*, *Reliability Engineering and System Safety*, v. 91, pp. 706-716, 2006.
- [36] SADEGHI, N., FAYEK, A., PEDRYCZ, W., *Fuzzy Monte Carlo Simulation and Risk Assessment in Construction*, *Computer Aided Civil and Infrastructure Engineering*, v. 25, pp. 238-252, 2010.
- [37] BELCHIOR, A.,, *Um Modelo Fuzzy para Avaliação da Qualidade de Software*, *Tese de Doutorado, Programa de Engenharia de Sistemas e Computação*, UFRJ, Rio de Janeiro, 1997.
- [38] MOREÍ, J., *Aplicação da Lógica Fuzzy na Avaliação da Confiabilidade Humana nos Ensaios não Destrutivos por Ultra Som*, *Tese de Doutorado, Programa de Engenharia Metalúrgica e de Materiais*, COPPE/UFRJ, Rio de Janeiro, 2004.

- [39] MORE, J., GUIMARÃES, A. *Metodologia Fuzzy para Avaliação da Confiabilidade Humana nos End. Por Ultra-Som, XXI Congresso Nacional de Ensaio Não-Destrutivos*, São Paulo, Agosto de 2002.
- [40] GANOULIS J., ANAGNOSTOPOULOS, P., MBIMBAS, I., *Fuzzy Logic – Based Risk Analysis of Water Pollution,, Environment Hydraulics and Eco-Hydraulics*, China, September 2001 .
- [41] YE, J., *Multicriteria Fuzzy Decision-Making Method based on a Novel Accuracy Function under Interval-Valued Intuitionistic Fuzzy Environment*, *Expert Systems with Applications*, v. 36, pp. 6899-6902, 2009.
- [42] CHEN, Z., YANG, W., *A New Multiple Attribute Group Decision Making Method in Intuitionistic Fuzzy Setting*, *Applied Mathematical Modeling*, v. 35, pp. 4424-4437, 2011.
- [43] LU, C., LAN, J., WANG, Z., *Aggregation of Fuzzy Opinions Under Group Decision-Making based on Similarity and Distance*, *Journal of Systems Science and Complexity* 19, pp. 63-71, 2006.
- [44] YANG, J., LI, Q., *Aggregation of Fuzzy Opinions with Area Between the Centroid Point and the Original Point under Group Decision Making*, *IEEE International Conference on Fuzzy System*, pp. 163-167, China, June 2008.
- [45] CLEMEN, R., WINKLER, R., *Combining Probability Distributions from Experts in Risk Analysis*, *Risk Analysis*, v. 20, pp. 155-156, 2000.
- [46] LIU, P., *A Weighted Aggregation Operators Multi-Attribute Group Decision-Making Method Based on Interval-Valued Trapezoidal Fuzzy Numbers*, *Expert Systems with Applications*, v. 38, pp. 1053-1060, 2011.
- [47] HSU, H., CHEN, C., *Aggregation of Fuzzy Opinions under Group Decision Making Environment*, *Fuzzy Sets and Systems*, 2002, pp. 279-285, 1996.
- [48] GARRETT C., APOSTOLAKIS, G., *Context and Software Safety Assessment*, HESSD'98, pp. 46-57, 1998. Disponível

em:[http://www.dcs.gla.ac.uk/~johnson/papers/seattle\\_hessd/georgechris-p.pdf](http://www.dcs.gla.ac.uk/~johnson/papers/seattle_hessd/georgechris-p.pdf),

Acesso em: 26 jan. 2010.

- [49] KOH, K., SEONG, P., SMV model-based Safety Analysis of Software Requirements, *Reliability Engineering and System Safety*, v. 94, pp. 320-331, 2009.
- [50] YANG, B., LI, X., XIE, M., *et al.*, A Generic data-driven Software Reliability Model with Model Mining Technique, *Reliability Engineering and System Safety*, v. 95, pp. 671-678, 2010.
- [51] HU, Q., XIE, M., LEVITIN, G., *et al.*, Robust Recurrent Neural Network Modeling for Software Fault Detection and Correction Prediction, *Reliability Engineering and System Safety*, v. 92, pp. 332-340, 2007.
- [52] DOHI, T., YASUI, K., OSAKI, S., *Software Reliability Assessment Models Based on Cumulative Bernoulli Trial Processes*, *Mathematical and Computer Modeling*, v. 38, pp. 1177-1184, 2003.
- [53] SYSTEM SAFETY SOCIETY *e-Handbook of Software safety*, Disponível em: [www.system-safety.org/Documents/Software\\_System\\_Safety\\_Handbook.pdf](http://www.system-safety.org/Documents/Software_System_Safety_Handbook.pdf), Acesso em: 26 jan. 2010.
- [54] ALDEMIR, T., *Utilization of the Cell-To-Cell Mapping Technique to Construct Markov Failure Models for Process Control Systems*, G. APOSTOLAKIS (Ed.), *Probabilistic Safety Assessment and Management: PSAM1*, pp. 1431-1436, Elsevier, New York, 1991.
- [55] ALDEMIR, T., *Computer-Assisted Markov Failure Modeling of Process Control Systems*, *IEEE transactions on Reliability*, R-36, pp. 133-144, 1987.
- [56] BUCCI, P., KIRSCHENBAUM, J., ALDEMIR, T., *et al.*, *Constructing Dynamic Event Trees From Markov Models*, M. STAMATALETOS and H. S. BLACKMAN (Eds.), *PSAM8: Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management, CD-ROM Version*, Paper # 369, ASME Press, Inc., 2006.

- [57] YAU, M., GUARRO, S., *A Benchmark System for Comparing Reliability Modeling Approaches for Digital Instrumentation and Control Systems*, *Nuclear Technology*, v. 165, pp. 53-95, 2008.
- [58] GUARRO S., YAU M., APOSTOLAKIS G., *Demonstration of the Dynamic Flowgraph Methodology using the Titan II Space Launch Vehicle Digital Flight Control Software*, *Reliability Engineering and System Safety*, v. 49, pp. 335-353, 1995.
- [59] ZHANG Y., GOLAY, M. M., *Development of a Method for Quantifying The Reliability of Nuclear Safety-Related Software*, *PSAM6: Proceedings of the 6th International Conference on Probabilistic Safety Assessment and Management*, CDROM Version, Elsevier Science Ltd., San Juan, Puerto Rico, 2002.
- [60] BALAKRISHMAN, M., TRIVEDI, K., *Stochastic Petri Nets for reliability analysis of communication network applications with alternate routing*, *Reliability Engineering and System Safety*, v. 53, pp. 243-259, 1996.
- [61] LI, B., LI, M., SMIDTS, C., *Integrating Software into PRA: A Test-Based Approach*, *PSAM 7-ESREL'04*, C. Spitzer, U. Schmocker, V. N. Dang (Eds.), Springer – Verlag, London U.K, 2004.
- [62] DO-178B, *Software Considerations in Airborne Systems And Equipment Certification*, RTCA inc, Washington, 1992.
- [63] SCHNEIDEWIND, N. F., KELLER, T. W., *Applying Reliability Models to the Shuttle*, *IEEE Software*, July 1992, v. 9, pp. 28-33.
- [64] VAURIO, J., *Human Factors, Human Reliability and Risk Assessment in License Renewal of a Nuclear Power Plant*, *Reliability Engineering and System Safety*, v. 94, pp. 1818-1826, 2009.
- [65] PEKKA, P., *Human Reliability Analysis Methods for Probabilistic Safety Assessment*, *Technical Research Centre of Finland*, Espoo, 2000.



- [66] CACCIABUE, P.C., *Modelling and Simulation of Human Behaviour for Safety Analysis and Control of Complex Systems*, *Safety Science*, v. 28, No 2, pp. 97-110, 1998.
- [67] SPURGIN, J., *HRA Requirements for PRA's*, *IEEE Conference on Human Factors and Power Plants*, Monterey CA, 2007.
- [68] FORESTER, J., COOPER, S., LOIS, E., *et al.*, *Good Practices for Implementing Human Reliability Analysis (HRA)*, NUREG-1792, U.S Nuclear Regulatory Commission, Washington DC, 2005.
- [69] KOVAL, D., FLOYD, H., *Human Element Factors Affecting Reliability and Safety*, *IEEE Transactions on Industry Applications* 34, No 2, 1998.
- [70] KHAN, F., *Human Factors Special Issue (Preface)*, *Journal of Loss Prevention in the Process Industries*, v. 21, pp. 225-226, 2008.
- [71] FULLWOOD, R., *Probabilistic Safety Assessment in the Chemical and Nuclear Industries*, Butterworth & Heinemann, Woburn MA, 2000.
- [72] PARK, J., JUNG, W., KIM, J., *A Simulator Study and its Application to an HRA in NPPs*, *IEEE Conference on Human Factors and Power Plants*, Monterey CA, 2007.
- [73] KIM, M., SEONG, P., KANG, H., *et al.*, *Quantification of Unavailability caused by Random Failures and Maintenance Human Errors in Nuclear Power Plants*, *Nuclear Engineering and Design*, v. 240, pp. 1606-1613, 2010.
- [74] REER, B., *Review of Advances in Human Reliability Analysis of Errors of Commission, Part 1: EOC identification*, *Reliability Engineering and System Safety*, v. 93, pp. 1105-1122, 2007.
- [75] SWAIN AD., GUTTMANN, HE., *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Final report*, NUREG/CR-1278. U.S Nuclear Regulatory Commission, Washington DC, 1983.

- [76] REER, B., *Review of Advances in Human Reliability Analysis of Errors of Commission, Part 1: EOC identification, Reliability Engineering and System Safety*, v. 93, pp. 1091-1104, 2008.
- [77] PARRY, G., *Book Review, Reliability Engineering and System Safety*, v. 53, pp. 99-101, 1996.
- [78] KIRWAN, B., BASRA, G., TAYLOR-ADAMS, S. E., *CORE-DATA: A computerized Human Error Database for Human Reliability Support, IEEE Sixth Annual Human Factors Meeting, Orlando FL, June 1997.*
- [79] GERTMAN, D., BLACKMAN, H., HALLBERT, B., *et al., The use of Empirical Data Sources in HRA, Reliability Engineering and System Safety*, v. 83, pp. 139-143, 2004.
- [80] STETKAR, J., *Overview of Human Reliability Analysis Methods, National Training Course on Probabilistic Safety Assessment, Islamabad, Pakistan, 2005.*
- [81] PARK, J., JUNG, W., *A Database for Human Performance under Simulated Emergencies of Nuclear Power Plants, Nuclear Engineering and Technology*, v. 37, No5, pp. 491-502, 2005.
- [82] FORESTER, J., LOIS, E., DANG, V.N., *et al., Human Reliability Analysis (HRA) in the Context of HRA Testing with Empirical Data, IEEE Conference on Human Factors and Power Plants, Monterey CA, 2007.*
- [83] THOMPSON, C., WHITEHEAD, D., KOLACZKOWSKI, A., *Quantification Results from an Application of a New Technique for Human Error Analysis (ATHEANA) at a Pressurized Water Reactor, International conference on probabilistic safety assessment and management (PSAM4), New York NY, September 1998.*
- [84] FORESTER, J., WHITEHEAD, D., KOLACZKOWSKI, A., *et al., Results of a nuclear Power Plant Application of a New Technique for Human Error Analysis (ATHEANA), OECD/NEA specialists meeting on human performance in operational events, Chattanooga TN, October 1997.*

- [85] SCB, *Design your Questions Right – How to Develop, test, Evaluate and Improve Questionnaires*, Statistiska Centralbyran, Sweden, September, 2004.
- [86] NASSAR., S., *Métodos de Defuzzificação*, Departamento de Informática e Estatística, Universidade Federal de Santa Catarina, Florianópolis, 2010.
- [87] GAO, S., ZHANG, Z., CAO, C., *Multiplication Operation on Fuzzy Numbers*, *Journal of Software*, v. 4, NO 4, pp. 331-338, 2009.
- [88] MPIMPAS, H., ANAGNOSTOPOULOS, P., GANOULIS, J., *Uncertainty of Model Parameters in Stream Pollution*, *Journal of Hydroinformatics*, v. 10, NO 3, pp. 189-200, 2008.
- [89] PINHO A., *Aplicação de Números Fuzzy Triangulares em Análises de Investimentos em Situações de Incerteza – Método Baseado na Teoria dos Jogos*, Dissertação de Mestrado, Departamento de Produção, Escola Federal de Engenharia de Itajubá, Itajubá MG, 1997.
- [90] MOTT, H., T., *Determination of the Irredundant Normal Forms of a Truth Function by Iterated Consensus of the Prime Implicants*, *IRE Transactions on Electronic Computer*, v. 9, pp 245-282, 1960.
- [91] OGUNBIYI, I., E., HENLEY, E., J., *Irredundant Forms and Prime Implicants of a Function with Multistate Variables*, *IEEE Transactions on Reliability*, v.30, NO 1, pp 39-42, 1981.
- [92] GARRIBBA, S., GUAGNINI, E., MUSSIO, P., *Multiple-Valued Logic Trees: Meaning and Prime Implicants*, *IEEE Transactions on Reliability*, v.34, NO 5, pp 463-472, 1985.
- [93] DOUGHERTY, E., *Human Errors of Commission Revisited: An Evaluation of the ATHEANA Approach*, *Reliability Engineering and System Safety*, v. 60, pp. 71-82, 1998.
- [94] ARNALDOS, J., VILCHEZ, J., DUNJÓ, J., *et al.*, *Hazard and Operability (HAZOP) Analysis. A Literature Review*, *Journal of Hazardous Materials*, v. 173, pp. 19-32, 2010.

- [95] KLETZ, T., *Hazop – Past and Future, Reliability Engineering and System Safety*, v. 55, pp. 263-266, 1997.
- [96] Eletronuclear, *Componentes do Reator e do Sistema de refrigeração do Reator, JÁ/JE*, Curso de Formação de Operador Licenciável, CFOL-01, Eletrobrás Termonuclear S. A., Rio de Janeiro, janeiro, 2001.
- [97] SOONG, T.T., *Fundamentals of Probability and Statistics for Engineers*, John Wiley & Sons Ltd, New York, 2004.
- [98] MONTGOMERY D. C., RUNGER G. C., *Applied Statistics - Probability for Engineers*, John Wiley & Sons Ltd, New York, 2004.
- [99] KIRWAN, B., *A Guide to Practical Human Reliability Assessment*, Taylor & Francis, London, 1994.
- [100] BLACKMAN, H., GERTMAN, D., *Human Reliability and Safety Analysis Data Handbook*, John Wiley & Sons, Inc, New York, 1994.
- [101] CHUTIA, R., MAHANTA, S., DATA, D., *Arithmetic of Triangular Fuzzy Variable from Credibility Theory, International Journal of Energy, Information and Communications*, v. 2, issue 3, 2011.
- [102] YOSHIKAWA, A., *Mutuality Measures Corresponding to Subjective Judgment Similarity and Matching, Fuzzy Systems Conference Proceedings*, v.1, pp. 33-37, 1999.
- [103] AKTHER, T., AHMAD, S., *A Computational Method for Fuzzy Arithmetic Operations, Applied Mathematics and Computation*, v. 185, pp. 169-177, 2007.
- [104] KLETZ, T., *An Engineer View's of Human Error*, Bell & Bam Limited, Glasgow, 2001.
- [105] BEARE, A., N., DORRIS, R., E., BOVELL, C., R., *et al., A Simulated-Based Study of Human Errors in Nuclear Power Plant Control Room Tasks*, NUREG/CR-3309, U.S Nuclear Regulatory Commission, Washington DC, 1984.

- [106] WILLIAMS, J., C., *A proposed Method for Assessing and Reducing Human error*,  
*Proceedings of the 9th Advance in Reliability Technology Symposium*,  
University of Bradford, Yorkshire, pp. B3/R/1 – B3/R/13, 1986.
- [107] GILMORE, W., E., *Nuclear computerized library for assessing reactor reliability*  
(*NUCLARR*), U.S Nuclear Regulatory Commission, Washington DC, 1990.

## APÊNDICE A

Tabela A.1: CTR 1 do sistema analisado

Pressão	Grupo de Aquecedores	Grupo de Aspersores	Válvula de Alívio	Válvula de Segurança	Desarme Manual	Pressão +
Muito Baixa	Desligado	Desligado	Fechada	Fechada	Não acionado	Muito Baixa
	Desligado	Desligado	Fechada	Aberta	Não acionado	Muito Baixa
	Desligado	Desligado	Aberta	Fechada	Não acionado	Muito Baixa
	Desligado	Desligado	Aberta	Aberta	Não acionado	Muito Baixa
	Desligado	Ligado	Fechada	Fechada	Não acionado	Muito Baixa
	Desligado	Ligado	Fechada	Aberta	Não acionado	Muito Baixa
	Desligado	Ligado	Aberta	Fechada	Não acionado	Muito Baixa
	Desligado	Ligado	Aberta	Aberta	Não acionado	Muito Baixa
	Ligado	Desligado	Fechada	Fechada	Não acionado	Baixa
	Ligado	Desligado	Fechada	Aberta	Não acionado	Muito Baixa
	Ligado	Desligado	Aberta	Fechada	Não acionado	Baixa
	Ligado	Desligado	Aberta	Aberta	Não acionado	Muito Baixa
	Ligado	Ligado	Fechada	Fechada	Não acionado	Muito Baixa
	Ligado	Ligado	Fechada	Aberta	Não acionado	Muito Baixa
	Ligado	Ligado	Aberta	Fechada	Não acionado	Muito Baixa
	Ligado	Ligado	Aberta	Aberta	Não acionado	Muito Baixa
Baixa	Desligado	Desligado	Fechada	Fechada	Não acionado	Baixa
	Desligado	Desligado	Fechada	Aberta	Não acionado	Baixa
	Desligado	Desligado	Aberta	Fechada	Não acionado	Baixa
	Desligado	Desligado	Aberta	Aberta	Não acionado	Muito Baixa
	Desligado	Ligado	Fechada	Fechada	Não acionado	Muito Baixa
	Desligado	Ligado	Fechada	Aberta	Não acionado	Muito Baixa

	Desligado	Ligado	Aberta	Fechada	Não acionado	Muito Baixa
	Desligado	Ligado	Aberta	Aberta	Não acionado	Muito Baixa
	Ligado	Desligado	Fechada	Fechada	Não acionado	Pouco Baixa
	Ligado	Desligado	Fechada	Aberta	Não acionado	Baixa
	Ligado	Desligado	Aberta	Fechada	Não acionado	Pouco Baixa
	Ligado	Desligado	Aberta	Aberta	Não acionado	Baixa
	Ligado	Ligado	Fechada	Fechada	Não acionado	Baixa
	Ligado	Ligado	Fechada	Aberta	Não acionado	Muito Baixa
	Ligado	Ligado	Aberta	Fechada	Não acionado	Baixa
	Ligado	Ligado	Aberta	Aberta	Não acionado	Muito Baixa
Pouco Baixa	Desligado	Desligado	Fechada	Fechada	Não acionado	Pouco Baixa
	Desligado	Desligado	Fechada	Aberta	Não acionado	Pouco Baixa
	Desligado	Desligado	Aberta	Fechada	Não acionado	Pouco Baixa
	Desligado	Desligado	Aberta	Aberta	Não acionado	Baixa
	Desligado	Ligado	Fechada	Fechada	Não acionado	Baixa
	Desligado	Ligado	Fechada	Aberta	Não acionado	Baixa
	Desligado	Ligado	Aberta	Fechada	Não acionado	Baixa
	Desligado	Ligado	Aberta	Aberta	Não acionado	Muito Baixa
	Ligado	Desligado	Fechada	Fechada	Não acionado	Pouco Alta
	Ligado	Desligado	Fechada	Aberta	Não acionado	Pouco Baixa
	Ligado	Desligado	Aberta	Fechada	Não acionado	Normal
	Ligado	Desligado	Aberta	Aberta	Não acionado	Pouco Baixa
	Ligado	Ligado	Fechada	Fechada	Não acionado	Pouco Baixa
	Ligado	Ligado	Fechada	Aberta	Não acionado	Baixa
	Ligado	Ligado	Aberta	Fechada	Não acionado	Pouco Baixa
	Ligado	Ligado	Aberta	Aberta	Não acionado	Baixa
Normal	Desligado	Desligado	Fechada	Fechada	Não acionado	Normal
	Desligado	Desligado	Fechada	Aberta	Não acionado	Pouco Baixa
	Desligado	Desligado	Aberta	Fechada	Não acionado	Pouco Baixa
	Desligado	Desligado	Aberta	Aberta	Não acionado	Baixa
	Desligado	Ligado	Fechada	Fechada	Não acionado	Pouco Baixa

	Desligado	Ligado	Fechada	Aberta	Não acionado	Baixa
	Desligado	Ligado	Aberta	Fechada	Não acionado	Baixa
	Desligado	Ligado	Aberta	Aberta	Não acionado	Muito Baixa
	Ligado	Desligado	Fechada	Fechada	Não acionado	Pouco Alta
	Ligado	Desligado	Fechada	Aberta	Não acionado	Pouco Baixa
	Ligado	Desligado	Aberta	Fechada	Não acionado	Normal
	Ligado	Desligado	Aberta	Aberta	Não acionado	Pouco Baixa
	Ligado	Ligado	Fechada	Fechada	Não acionado	Pouco Baixa
	Ligado	Ligado	Fechada	Aberta	Não acionado	Baixa
	Ligado	Ligado	Aberta	Fechada	Não acionado	Pouco Baixa
	Ligado	Ligado	Aberta	Aberta	Não acionado	Baixa
Pouco Alta	Desligado	Desligado	Fechada	Fechada	Não acionado	Pouco Alta
	Desligado	Desligado	Fechada	Aberta	Não acionado	Pouco Baixa
	Desligado	Desligado	Aberta	Fechada	Não acionado	Normal
	Desligado	Desligado	Aberta	Aberta	Não acionado	Pouco Baixa
	Desligado	Ligado	Fechada	Fechada	Não acionado	Pouco Baixa
	Desligado	Ligado	Fechada	Aberta	Não acionado	Baixa
	Desligado	Ligado	Aberta	Fechada	Não acionado	Pouco Baixa
	Desligado	Ligado	Aberta	Aberta	Não acionado	Baixa
	Ligado	Desligado	Fechada	Fechada	Não acionado	Pouco Alta
	Ligado	Desligado	Fechada	Aberta	Não acionado	Normal
	Ligado	Desligado	Aberta	Fechada	Não acionado	Pouco Alta
	Ligado	Desligado	Aberta	Aberta	Não acionado	Normal
	Ligado	Ligado	Fechada	Fechada	Não acionado	Normal
	Ligado	Ligado	Fechada	Aberta	Não acionado	Pouco Baixa
	Ligado	Ligado	Aberta	Fechada	Não acionado	Pouco Baixa
	Ligado	Ligado	Aberta	Aberta	Não acionado	Pouco Baixa
Alta	Desligado	Desligado	Fechada	Fechada	Não acionado	Alta
	Desligado	Desligado	Fechada	Aberta	Não acionado	Pouco Alta
	Desligado	Desligado	Aberta	Fechada	Não acionado	Pouco Alta
	Desligado	Desligado	Aberta	Aberta	Não acionado	Normal



	Desligado	Ligado	Fechada	Fechada	Não acionado	Normal
	Desligado	Ligado	Fechada	Aberta	Não acionado	Pouco Baixa
	Desligado	Ligado	Aberta	Fechada	Não acionado	Pouco Baixa
	Desligado	Ligado	Aberta	Aberta	Não acionado	Pouco Baixa
	Ligado	Desligado	Fechada	Fechada	Não acionado	Muito Alta
	Ligado	Desligado	Fechada	Aberta	Não acionado	Pouco Alta
	Ligado	Desligado	Aberta	Fechada	Não acionado	Alta
	Ligado	Desligado	Aberta	Aberta	Não acionado	Pouco Alta
	Ligado	Ligado	Fechada	Fechada	Não acionado	Pouco Alta
	Ligado	Ligado	Fechada	Aberta	Não acionado	Normal
	Ligado	Ligado	Aberta	Fechada	Não acionado	Pouco Alta
	Ligado	Ligado	Aberta	Aberta	Não acionado	Pouco Baixa
Muito Alta	Desligado	Desligado	Fechada	Fechada	Não acionado	Muito Alta
	Desligado	Desligado	Fechada	Aberta	Não acionado	Pouco Alta
	Desligado	Desligado	Aberta	Fechada	Não acionado	Alta
	Desligado	Desligado	Aberta	Aberta	Não acionado	Pouco Alta
	Desligado	Ligado	Fechada	Fechada	Não acionado	Pouco Alta
	Desligado	Ligado	Fechada	Aberta	Não acionado	Pouco Baixa
	Desligado	Ligado	Aberta	Fechada	Não acionado	Normal
	Desligado	Ligado	Aberta	Aberta	Não acionado	Pouco Baixa
	Ligado	Desligado	Fechada	Fechada	Não acionado	Muito Alta
	Ligado	Desligado	Fechada	Aberta	Não acionado	Alta
	Ligado	Desligado	Aberta	Fechada	Não acionado	Muito Alta
	Ligado	Desligado	Aberta	Aberta	Não acionado	Pouco Alta
	Ligado	Ligado	Fechada	Fechada	Não acionado	Alta
	Ligado	Ligado	Fechada	Aberta	Não acionado	Pouco Alta
	Ligado	Ligado	Aberta	Fechada	Não acionado	Pouco Alta
	Ligado	Ligado	Aberta	Aberta	Não acionado	Normal
-	-	-	-	-	Acionado	Muito Baixa

## APÊNDICE B

Tabela B.1: Histórico de pressão de uma usina PWR

Data	Pressão ao final do dia (Bar)	Data	Pressão ao final do dia (Bar)	Data	Pressão ao final do dia (Bar)
29/08/2009	156,4	13/09/2009	156,8	28/09/2009	156,4
30/08/2009	156,7	14/09/2009	156,8	29/09/2009	156,1
31/08/2009	156,8	15/09/2009	156,8	30/09/2009	156,0
01/09/2009	156,4	16/09/2009	156,8	01/10/2009	157,8
02/09/2009	157,8	17/09/2009	156,4	02/10/2009	156,5
03/09/2009	156,9	18/09/2009	156,4		
04/09/2009	156,8	19/09/2009	156,6		
05/09/2009	156,7	20/09/2009	156,8		
06/09/2009	156,8	21/09/2009	156,8		
07/09/2009	156,6	22/09/2009	156,6		
08/09/2009	156,8	23/09/2009	155,7		
09/09/2009	156,8	24/09/2009	155,7		
10/09/2009	156,8	25/09/2009	156,2		
11/09/2009	156,8	26/09/2009	156,4		
12/09/2009	156,7	27/09/2009	156,3		

## APÊNDICE C

Tabela C.1: Gráficos de probabilidade para a distribuição normal

i	P	F(t)	F(t)-1	Distribuição Normal	
				y	x
1	155,7	0,028571	-1,90222		
2	155,7	0,057143	-1,57922	-1,90222	155,7
3	156	0,085714	-1,36763	-1,57922	155,7
4	156,1	0,114286	-1,20405	-1,36763	156
5	156,2	0,142857	-1,06757	-1,20405	156,1
6	156,3	0,171429	-0,94854	-1,06757	156,2
7	156,4	0,2	-0,84162	-0,94854	156,3
8	156,4	0,228571	-0,74356	-0,84162	156,4
9	156,4	0,257143	-0,65218	-0,74356	156,4
10	156,4	0,285714	-0,56595	-0,65218	156,4
11	156,4	0,314286	-0,48374	-0,56595	156,4
12	156,4	0,342857	-0,40468	-0,48374	156,4
13	156,5	0,371429	-0,32807	-0,40468	156,4
14	156,6	0,4	-0,25335	-0,32807	156,5
15	156,6	0,428571	-0,18001	-0,25335	156,6
16	156,6	0,457143	-0,10763	-0,18001	156,6
17	156,7	0,485714	-0,03582	-0,10763	156,6
18	156,7	0,514286	0,035817	-0,03582	156,7
19	156,7	0,542857	0,107634	0,035817	156,7
20	156,8	0,571429	0,180012	0,107634	156,7

21	156,8	0,6	0,253347			0,180012	156,8
22	156,8	0,628571	0,328072			0,253347	156,8
23	156,8	0,657143	0,404678			0,328072	156,8
24	156,8	0,685714	0,483739			0,404678	156,8
25	156,8	0,714286	0,565949			0,483739	156,8
26	156,8	0,742857	0,652179			0,565949	156,8
27	156,8	0,771429	0,74356			0,652179	156,8
28	156,8	0,8	0,841621			0,74356	156,8
29	156,8	0,828571	0,948535			0,841621	156,8
30	156,8	0,857143	1,067571			0,948535	156,8
31	156,8	0,885714	1,204047			1,067571	156,8
32	156,8	0,914286	1,367628			1,204047	156,8
33	156,9	0,942857	1,57922			1,367628	156,8
34	157,8	0,971429	1,902216			1,57922	156,9

## LEGENDA

i: Índice da amostra

P: Pressão

F(t): Função distribuição acumulada de probabilidade

F(t)-1: Inversa da função distribuição acumulada de probabilidade

Tabela C.2: Histograma de Pressão

Bloco	Frequência
155	0
155,6	4
156,2	15
156,8	14
157,4	2
158	0
Mais	0

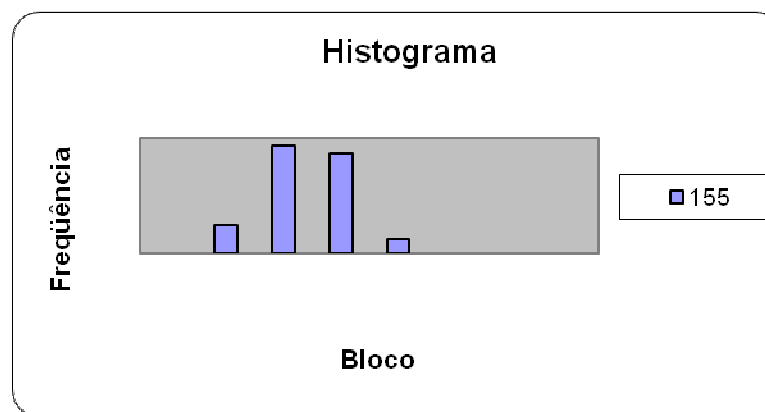


Tabela C.3: Teste de aderência para a distribuição normal

<b>i</b>	<b>P</b>	<b>F(t)</b>				<b>Fo(t)</b>	<b>Diferença</b>	<b>Maior Diferença</b>
1	155,7	0,028571429				0,01584903	0,012722399	<b>0,251419039</b>
2	155,7	0,057142857				0,01584903	0,041293828	<b>Adere com até 99% de confiança</b>
3	156	0,085714286				0,073850709	0,011863577	
4	156,1	0,114285714				0,112335936	0,001949778	<b>Média</b>
5	156,2	0,142857143				0,163370619	0,020513476	<b>156,62</b>
6	156,3	0,171428571				0,227471671	0,0560431	
7	156,4	0,2				0,303731074	0,103731074	<b>Desvio</b>
8	156,4	0,228571429				0,303731074	0,075159646	<b>0,428265998</b>
9	156,4	0,257142857				0,303731074	0,046588217	
10	156,4	0,285714286				0,303731074	0,018016789	
11	156,4	0,314285714				0,303731074	0,01055464	
12	156,4	0,342857143				0,303731074	0,039126069	
13	156,5	0,371428571				0,389662152	0,018233581	
14	156,6	0,4				0,481376186	0,081376186	
15	156,6	0,428571429				0,481376186	0,052804757	
16	156,6	0,457142857				0,481376186	0,024233329	
17	156,7	0,485714286				0,574091196	0,08837691	
18	156,7	0,514285714				0,574091196	0,059805481	
19	156,7	0,542857143				0,574091196	0,031234053	
20	156,8	0,571428571				0,662866676	0,091438104	
21	156,8	0,6				0,662866676	0,062866676	
22	156,8	0,628571429				0,662866676	0,034295247	

23	156,8	0,657142857				0,662866676	0,005723818	
24	156,8	0,685714286				0,662866676	0,02284761	
25	156,8	0,714285714				0,662866676	0,051419039	
26	156,8	0,742857143				0,662866676	0,079990467	
27	156,8	0,771428571				0,662866676	0,108561896	
28	156,8	0,8				0,662866676	0,137133324	
29	156,8	0,828571429				0,662866676	0,165704753	
30	156,8	0,857142857				0,662866676	0,194276182	
31	156,8	0,885714286				0,662866676	0,22284761	
32	156,8	0,914285714				0,662866676	0,251419039	
33	156,9	0,942857143				0,743379434	0,199477709	
34	157,8	0,971428571				0,997068056	0,025639484	
35	157,8	1				0,997068056	0,002931944	

#### LEGENDA

i: Índice da amostra

P: Pressão

F(t): Função distribuição acumulada de probabilidade estimada

Fo(t): Função distribuição acumulada de probabilidade real



COPPE/UFRRJ

**UNIVERSIDADE  
FEDERAL DO  
RIO DE  
JANEIRO**

**COPPE –  
PROGRAMA DE  
ENGENHARIA  
NUCLEAR**

## APÊNDICE D

### Questionário de Avaliação de Contextos e Ações Humanas Inseguras

#### 1. Objetivo

Determinar as frequências de ocorrência de determinados contextos em centrais nucleares e as probabilidades de ações humanas inseguras nestes contextos.

#### 2. Descrição do cenário

O cenário consiste no sistema de controle do pressurizador e um operador na sala de controle. O sistema é composto de aquecedores no fundo do pressurizador, aspersores no topo, uma válvula de alívio e uma válvula de segurança de emergência. Existe o sensoriamento do nível de pressão e a indicação deste nível na sala de controle. O operador é responsável, dentre outras atividades, pelo acionamento do desarme manual de sobre pressão quando necessário.

#### 3. Instruções de preenchimento

Baseado em sua opinião e/ou experiência e conhecimento, atribua valores de 0 a 4, segundo a escala apresentada na Tabela D.1, aos contextos apresentados. Atribua também valores de 5 a 9, segundo a escala apresentada na Tabela D.2, às ações humanas inseguras associadas a cada um destes contextos.



Tabela D. 1– Escala de valores para os contextos

<b>ESCALA</b>	<b>EQUIVALÊNCIA</b>	<b>INTERPRETAÇÃO</b>
0	<i>Frequência de ocorrência muito baixa</i>	Indica uma situação quase inexistente.
1	<i>Frequência de ocorrência baixa</i>	Indica um baixo grau de presença da situação.
2	<i>Frequência de ocorrência moderada</i>	Indica um grau de presença moderada (aceitável) do contexto.
3	<i>Frequência de ocorrência alta</i>	Indica um alto grau de presença do contexto.
4	<i>Frequência de ocorrência muito alta</i>	Indica que a situação é corriqueira.

Tabela D. 2 – Escala de valores para as ações inseguras

<b>ESCALA</b>	<b>EQUIVALÊNCIA</b>	<b>INTERPRETAÇÃO</b>
5	<i>Probabilidade de ocorrência muito baixa</i>	Indica uma chance quase nula de ocorrência das ações inseguras, dado o contexto.
6	<i>Probabilidade de ocorrência baixa</i>	Indica uma chance baixa de ocorrência das ações inseguras, dado o contexto.
7	<i>Probabilidade de ocorrência moderada</i>	Indica uma chance razoável de ocorrência das ações inseguras, dado o contexto.
8	<i>Probabilidade de ocorrência alta</i>	Indica uma chance alta de ocorrência das ações inseguras, dado o contexto.
9	<i>Probabilidade de ocorrência muito alta</i>	Indica uma chance muito grande de ocorrência das ações inseguras, dado o contexto.

Nome do Avaliador: \_\_\_\_\_

Email: \_\_\_\_\_ Instituição: \_\_\_\_\_

#### 4. Avaliação

<b>1. Contexto #1</b>	<b>Técnica de Avaliação:</b> Pesquisa de opinião
<b>Definição:</b> <input type="checkbox"/> Na sua opinião, com que frequência a conjunção de eventos ocorre: ( <b>SENSORIAMENTO de pressão FALHO E NÍVEL DE TREINAMENTO dos operadores RUIM E PRESSÃO no nível MÁXIMO permitido</b> )?	<b>Valores</b> 0 1 2 3 4
<b>Comentários:</b>	

<b>2. Ações Inseguras #1</b>	<b>Técnica de Avaliação:</b> Pesquisa de opinião
<b>Definição:</b> <input type="checkbox"/> Dentro do contexto #1 acima, qual a probabilidade do <b>operador tomar uma decisão errônea</b> ?	<b>Valores</b> 5 6 7 8 9
<b>Comentários:</b>	

<b>3. Contexto #2</b>	<b>Técnica de Avaliação</b> Pesquisa de opinião
<b>Definição:</b> <input type="checkbox"/> Na sua opinião, com que frequência a conjunção de eventos ocorre: ( <b>SENSORIAMENTO de pressão FALHO E OPERADOR se encontra FADIGADO E PRESSÃO no nível MÁXIMO permitido</b> )?	<b>Valores</b> 0 1 2 3 4
<b>Comentários:</b>	

<b>4. Ações Inseguras #2</b>	<b>Técnica de Avaliação</b> Pesquisa de opinião
<b>Definição:</b> <input type="checkbox"/> Dentro do contexto #2 acima, qual a probabilidade do <b>operador não checar</b> a indicação de pressão na sala de controle, <b>entender a situação</b> de maneira <b>errônea</b> , <b>tomar uma decisão errônea</b> e ainda <b>errar o acionamento</b> do dispositivo de desarme manual?	<b>Valores</b> 5 6 7 8 9
<b>Comentários:</b>	

<b>5. Contexto #3</b>	<b>Técnica de Avaliação:</b> Pesquisa de opinião
<b>Definição:</b> <input type="checkbox"/> Na sua opinião, com que frequência a conjunção de eventos ocorre: ( <b>NÍVEL DE TREINAMENTO dos operadores RUIM E PRESSÃO no nível MINIMO permitido</b> )?	<b>Valores</b> 0 1 2 3 4
<b>Comentários:</b>	

<b>6. Ações Inseguras #3</b>	<b>Técnica de Avaliação:</b> Pesquisa de opinião
<b>Definição:</b> <input type="checkbox"/> Dentro do contexto #3 acima, qual a probabilidade do operador tomar uma decisão errônea?	<b>Valores</b> 5 6 7 8 9
<b>Comentários:</b>	

<b>7. Contexto #4</b>	<b>Técnica de Avaliação:</b> Pesquisa de opinião
<b>Processo de Avaliação:</b> <input type="checkbox"/> Na sua opinião, com que frequência a conjunção de eventos ocorre: ( <b>NÍVEL DE TREINAMENTO dos operadores RUIM E VÁLVULA DE SEGURANÇA FALHA E PRESSÃO no nível MINIMO permitido</b> )?	<b>Valores</b> 0 1 2 3 4
<b>Comentários:</b>	

<b>8. Ações Inseguras #4</b>	<b>Técnica de Avaliação:</b> Pesquisa de opinião
<b>Definição:</b> <input type="checkbox"/> Dentro do contexto #4 acima, qual a probabilidade do operador tomar uma decisão errônea?	<b>Valores</b> 5 6 7 8 9
<b>Comentários:</b>	



COPPE/UFRJ

**UNIVERSIDADE  
FEDERAL DO RIO  
DE JANEIRO**

**COPPE –  
PROGRAMA DE  
ENGENHARIA  
NUCLEAR**

## APÊNDICE E

### Questionário de Identificação do Perfil do Especialista

Nome do Avaliador:

\_\_\_\_\_

Email: \_\_\_\_\_

Instituição:

\_\_\_\_\_

Avaliador:

1. Marque as atividades que exerce/exerceu na área nuclear (Marque mais de uma se for o caso):

- a. Professor Universitário (0,2 PONTO)
- b. Engenheiro de Usina (0,8 PONTO)
- c. Engenheiro de Licenciamento (0,5 PONTO)
- d. Operador de Usina (1 PONTO)
- e. Pesquisador (0,2 PONTO)
- f. Outros: \_\_\_\_\_ (0,1 PONTO)

2. Quantas atividades de Análise de Confiabilidade já realizou?

- a. Nenhuma (0 PONTO)
- b. Até 3 (0,25 PONTO)
- c. Até 5 (0,5 PONTO)
- d. Até 10 (0,75 PONTO)
- e. Mais que 10 (1 PONTO)

**3. Como você classificaria seu entendimento em Análise de Confiabilidade?**

- a. Nenhum (0 PONTO)
- b. Baixo (0,25 PONTO)
- c. Razoável (0,5 PONTO)
- d. Alto (0,75 PONTO)
- e. Excelente (1 PONTO)

**4. Qual sua titulação (Marque uma opção)?**

- a. Segundo Grau (0,2 PONTO)
- b. Terceiro Grau (0,6 PONTO) Área:
- c. Especialização (0,7 PONTO) Área:
- d. Mestrado (0,8 PONTO) Área:
- e. Doutorado (1 PONTO) Área:

**5. Marque a quantidade de publicações que já realizou na área de Análise de Confiabilidade**

**a. Congressos:**

- i. Nenhuma (0 PONTO)
- ii. Até 3 (0,25 PONTO)
- iii. Até 5 (0,5 PONTO)
- iv. Até 10 (0,75 PONTO)
- v. Mais que 10 (1 PONTO)

**b. Artigos Nacionais:**

- i. Nenhuma (0 PONTO)
- ii. Até 3 (0,5 PONTO)
- iii. Até 5 (1 PONTO)
- iv. Até 10 (1,5 PONTO)
- v. Mais que 10 (2 PONTO)

**c. Artigos Internacionais:**

- i. Nenhuma (0 PONTO)**
- ii. Até 3 (1 PONTO)**
- iii. Até 5 (2 PONTO)**
- iv. Até 10 (3 PONTO)**
- v. Mais que 10 (4 PONTO)**

**6. Marque seu tempo de experiência na área de Análise de Confiabilidade**

- a. Entre 1 a 5 anos (0,25 PONTO)**
- b. Entre 5 a 10 anos (0,5 PONTO)**
- c. Entre 10 a 15 anos (0,75 PONTO)**
- d. Mais que 10 anos (1 PONTO)**

## APÊNDICE F

Tabela F. 1 – Opiniões dos especialistas acerca das probabilidades de contextos e ações humanas inseguras

<b>ESPECIALISTA</b>	<b>OPINIÃO FUZZY CONTEXTO#1</b>	<b>OPINIÃO FUZZY AÇÕES#1</b>	<b>OPINIÃO FUZZY CONTEXTO#2</b>	<b>OPINIÃO FUZZY AÇÕES#2</b>
<b>E1</b>	MB	MA	B	A
<b>E2</b>	MB	A	B	MA
<b>E3</b>	MB	MB	MB	MB
<b>E4</b>	MB	A	MB	B
<b>E5</b>	B	M	B	A
<b>E6</b>	M	A	M	M
<b>E7</b>	MB	MB	MB	MB
<b>E8</b>	B	B	B	B
<b>E9</b>	B	B	M	M
<b>E10</b>	B	B	B	B
	<b>OPINIÃO FUZZY CONTEXTO#3</b>	<b>OPINIÃO FUZZY AÇÕES#3</b>	<b>OPINIÃO FUZZY CONTEXTO#4</b>	<b>OPINIÃO FUZZY AÇÕES#4</b>
<b>E1</b>	M	M	MB	MA
<b>E2</b>	B	A	B	A
<b>E3</b>	B	M	B	MB
<b>E4</b>	MB	A	MB	A
<b>E5</b>	B	M	B	M
<b>E6</b>	M	A	M	A
<b>E7</b>	MB	MB	MB	MB
<b>E8</b>	B	M	B	B
<b>E9</b>	B	B	B	B
<b>E10</b>	B	B	B	B

Legenda:

MA – Muito Alta

A – Alta

M – Moderada

B – Baixa

MB – Muito Baixa



Tabela F. 2 – Pontuações dos especialistas obtidas através do formulário de perfil

	ITEM 1	ITEM 2	ITEM 3	ITEM 4	ITEM 5	ITEM 6
<b>ESPECIALISTA</b>						
<b>E1</b>	0,5	0,25	0,5	0,8	1,75	0,25
<b>E2</b>	0,5	0,25	0,5	0,8	1,75	0,25
<b>E3</b>	1,8	1	0,75	0,6	0	0,75
<b>E4</b>	0,5	0,25	0,75	0,8	1,75	0,25
<b>E5</b>	0,8	0,25	0,25	0,7	0	0,25
<b>E6</b>	0,5	1	1	1	2,5	1
<b>E7</b>	0,5	0,25	0,75	0,8	1,75	0,25
<b>E8</b>	1,3	1	0,5	1	2,25	0,75
<b>E9</b>	0,5	1	0,75	1	4	1
<b>E10</b>	0,1	0,25	0,75	0,8	0	0,25

Tabela F. 3 – Cálculo dos centroides das opiniões *fuzzy*

ESPECIALISTA	$X_{iC\#1}$	$Y_{iC\#1}$	$X_{iA\#1}$	$Y_{iA\#1}$	$X_{iC\#2}$	$Y_{iC\#2}$	$X_{iA\#2}$	$Y_{iA\#2}$
E1	0,05	0,5	0,55	0,5	0,25	0,5	0,255	0,5
E2	0,05	0,5	0,255	0,5	0,25	0,5	0,55	0,5
E3	0,05	0,5	0,000503	0,5	0,05	0,5	0,0005025	0,5
E4	0,05	0,5	0,255	0,5	0,05	0,5	0,00505	0,5
E5	0,25	0,5	0,0505	0,5	0,25	0,5	0,255	0,5
E6	0,5	0,5	0,255	0,5	0,5	0,5	0,0505	0,5
E7	0,05	0,5	0,000503	0,5	0,05	0,5	0,0005025	0,5
E8	0,25	0,5	0,00505	0,5	0,25	0,5	0,00505	0,5
E9	0,25	0,5	0,00505	0,5	0,5	0,5	0,0505	0,5
E10	0,25	0,5	0,00505	0,5	0,25	0,5	0,00505	0,5
ESPECIALISTA	$X_{iC\#3}$	$Y_{iC\#3}$	$X_{iA\#3}$	$Y_{iA\#3}$	$X_{iC\#4}$	$Y_{iC\#4}$	$X_{iA\#4}$	$Y_{iA\#4}$
E1	0,5	0,5	0,0505	0,5	0,05	0,5	0,55	0,5
E2	0,25	0,5	0,255	0,5	0,25	0,5	0,255	0,5
E3	0,25	0,5	0,0505	0,5	0,25	0,5	0,0005025	0,5
E4	0,05	0,5	0,255	0,5	0,05	0,5	0,255	0,5
E5	0,25	0,5	0,0505	0,5	0,25	0,5	0,0505	0,5
E6	0,5	0,5	0,255	0,5	0,5	0,5	0,255	0,5
E7	0,05	0,5	0,000503	0,5	0,05	0,5	0,0005025	0,5
E8	0,25	0,5	0,0505	0,5	0,25	0,5	0,00505	0,5
E9	0,25	0,5	0,00505	0,5	0,25	0,5	0,00505	0,5
E10	0,25	0,5	0,00505	0,5	0,25	0,5	0,00505	0,5

Tabela F. 4 – Cálculo dos índices de similaridade entre as opiniões dos especialistas

SijC#1	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10
E1		1	1	1	0,2	0,1	1	0,2	0,2	0,2
E2	1		1	1	0,2	0,1	1	0,2	0,2	0,2
E3	1	1		1	0,2	0,1	1	0,2	0,2	0,2
E4	1	1	1		0,2	0,1	1	0,2	0,2	0,2
E5	0,2	0,2	0,2	0,2		0,5	0,2	1	1	1
E6	0,1	0,1	0,1	0,1	0,5		0,1	0,5	0,5	0,5
E7	1	1	1	1	0,2	0,1		0,2	0,2	0,2
E8	0,2	0,2	0,2	0,2	1	0,5	0,2		1	1
E9	0,2	0,2	0,2	0,2	1	0,5	0,2	1		1
E10	0,2	0,2	0,2	0,2	1	0,5	0,2	1	1	
SijA#1	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10
E1		0,463636	0,000914	0,463636	0,091818	0,463636	0,000914	0,009182	0,009182	0,009182
E2	0,463636		0,001971	1	0,198039	1	0,001971	0,019804	0,019804	0,019804
E3	0,000914	0,001971		0,001971	0,00995	0,001971	1	0,099505	0,099505	0,099505
E4	0,463636	1	0,001971		0,198039	1	0,001971	0,019804	0,019804	0,019804
E5	0,091818	0,198039	0,00995	0,198039		0,198039	0,00995	0,1	0,1	0,1
E6	0,463636	1	0,001971	1	0,198039		0,001971	0,019804	0,019804	0,019804
E7	0,000914	0,001971	1	0,001971	0,00995	0,001971		0,099505	0,099505	0,099505
E8	0,009182	0,019804	0,099505	0,019804	0,1	0,019804	0,099505		1	1
E9	0,009182	0,019804	0,099505	0,019804	0,1	0,019804	0,099505	1		1
E10	0,009182	0,019804	0,099505	0,019804	0,1	0,019804	0,099505	1	1	

<b>SijC#2</b>	<b>E1</b>	<b>E2</b>	<b>E3</b>	<b>E4</b>	<b>E5</b>	<b>E6</b>	<b>E7</b>	<b>E8</b>	<b>E9</b>	<b>E10</b>
<b>E1</b>		1	0,2	0,2	1	0,5	0,2	1	0,5	1
<b>E2</b>	1		0,2	0,2	1	0,5	0,2	1	0,5	1
<b>E3</b>	0,2	0,2		1	0,2	0,1	1	0,2	0,1	0,2
<b>E4</b>	0,2	0,2	1		0,2	0,1	1	0,2	0,1	0,2
<b>E5</b>	1	1	0,2	0,2		0,5	0,2	1	0,5	1
<b>E6</b>	0,5	0,5	0,1	0,1	0,5		0,1	0,5	1	0,5
<b>E7</b>	0,2	0,2	1	1	0,2	0,1		0,2	0,1	0,2
<b>E8</b>	1	1	0,2	0,2	1	0,5	0,2		0,5	1
<b>E9</b>	0,5	0,5	0,1	0,1	0,5	1	0,1	0,5		0,5
<b>E10</b>	1	1	0,2	0,2	1	0,5	0,2	1	0,5	
<b>SijA#2</b>	<b>E1</b>	<b>E2</b>	<b>E3</b>	<b>E4</b>	<b>E5</b>	<b>E6</b>	<b>E7</b>	<b>E8</b>	<b>E9</b>	<b>E10</b>
<b>E1</b>		0,463636	0,001971	0,019804	1	0,198039	0,001971	0,019804	0,198039	0,019804
<b>E2</b>	0,463636		0,000914	0,009182	0,463636	0,091818	0,000914	0,009182	0,091818	0,009182
<b>E3</b>	0,001971	0,000914		0,099505	0,001971	0,00995	1	0,099505	0,00995	0,099505
<b>E4</b>	0,019804	0,009182	0,099505		0,019804	0,1	0,099505	1	0,1	1
<b>E5</b>	1	0,463636	0,001971	0,019804		0,198039	0,001971	0,019804	0,198039	0,019804
<b>E6</b>	0,198039	0,091818	0,00995	0,1	0,198039		0,00995	0,1	1	0,1
<b>E7</b>	0,001971	0,000914	1	0,099505	0,001971	0,00995		0,099505	0,00995	0,099505
<b>E8</b>	0,019804	0,009182	0,099505	1	0,019804	0,1	0,099505		0,1	1
<b>E9</b>	0,198039	0,091818	0,00995	0,1	0,198039	1	0,00995	0,1		0,1
<b>E10</b>	0,019804	0,009182	0,099505	1	0,019804	0,1	0,099505	1	0,1	
<b>SIJC#3</b>	<b>E1</b>	<b>E2</b>	<b>E3</b>	<b>E4</b>	<b>E5</b>	<b>E6</b>	<b>E7</b>	<b>E8</b>	<b>E9</b>	<b>E10</b>
<b>E1</b>		0,5	0,5	0,1	0,5	1	0,1	0,5	0,5	0,5
<b>E2</b>	0,5		1	0,2	1	0,5	0,2	1	1	1

<b>E3</b>	0,5	1		0,2	1	0,5	0,2	1	1	1
<b>E4</b>	0,1	0,2	0,2		0,2	0,1	1	0,2	0,2	0,2
<b>E5</b>	0,5	1	1	0,2		0,5	0,2	1	1	1
<b>E6</b>	1	0,5	0,5	0,1	0,5		0,1	0,5	0,5	0,5
<b>E7</b>	0,1	0,2	0,2	1	0,2	0,1		0,2	0,2	0,2
<b>E8</b>	0,5	1	1	0,2	1	0,5	0,2		1	1
<b>E9</b>	0,5	1	1	0,2	1	0,5	0,2	1		1
<b>E10</b>	0,5	1	1	0,2	1	0,5	0,2	1	1	
<b>SijA#3</b>	<b>E1</b>	<b>E2</b>	<b>E3</b>	<b>E4</b>	<b>E5</b>	<b>E6</b>	<b>E7</b>	<b>E8</b>	<b>E9</b>	<b>E10</b>
<b>E1</b>		0,198039	1	0,198039	1	0,198039	0,00995	1	0,1	0,1
<b>E2</b>	0,198039		0,198039	1	0,198039	1	0,001971	0,198039	0,019804	0,019804
<b>E3</b>	1	0,198039		0,198039	1	0,198039	0,00995	1	0,1	0,1
<b>E4</b>	0,198039	1	0,198039		0,198039	1	0,001971	0,198039	0,019804	0,019804
<b>E5</b>	1	0,198039	1	0,198039		0,198039	0,00995	1	0,1	0,1
<b>E6</b>	0,198039	1	0,198039	1	0,198039		0,001971	0,198039	0,019804	0,019804
<b>E7</b>	0,00995	0,001971	0,00995	0,001971	0,00995	0,001971		0,00995	0,099505	0,099505
<b>E8</b>	1	0,198039	1	0,198039	1	0,198039	0,00995		0,1	0,1
<b>E9</b>	0,1	0,019804	0,1	0,019804	0,1	0,019804	0,099505	0,1		1
<b>E10</b>	0,1	0,019804	0,1	0,019804	0,1	0,019804	0,099505	0,1	1	
<b>SijC#4</b>	<b>E1</b>	<b>E2</b>	<b>E3</b>	<b>E4</b>	<b>E5</b>	<b>E6</b>	<b>E7</b>	<b>E8</b>	<b>E9</b>	<b>E10</b>
<b>E1</b>		0,2	0,2	1	0,2	0,1	1	0,2	0,2	0,2
<b>E2</b>	0,2		1	0,2	1	0,5	0,2	1	1	1
<b>E3</b>	0,2	1		0,2	1	0,5	0,2	1	1	1
<b>E4</b>	1	0,2	0,2		0,2	0,1	1	0,2	0,2	0,2
<b>E5</b>	0,2	1	1	0,2		0,5	0,2	1	1	1

<b>E6</b>	0,1	0,5	0,5	0,1	0,5		0,1	0,5	0,5	0,5
<b>E7</b>	1	0,2	0,2	1	0,2	0,1		0,2	0,2	0,2
<b>E8</b>	0,2	1	1	0,2	1	0,5	0,2		1	1
<b>E9</b>	0,2	1	1	0,2	1	0,5	0,2	1		1
<b>E10</b>	0,2	1	1	0,2	1	0,5	0,2	1	1	
<b>SijA#4</b>	<b>E1</b>	<b>E2</b>	<b>E3</b>	<b>E4</b>	<b>E5</b>	<b>E6</b>	<b>E7</b>	<b>E8</b>	<b>E9</b>	<b>E10</b>
<b>E1</b>		0,463636	0,000914	0,463636	0,091818	0,463636	0,000914	0,009182	0,009182	0,009182
<b>E2</b>	0,463636	1	0,001971	1	0,198039	1	0,001971	0,019804	0,019804	0,019804
<b>E3</b>	0,000914	0,001971	1	0,001971	0,00995	0,001971	1	0,099505	0,099505	0,099505
<b>E4</b>	0,463636	1	0,001971		0,198039	1	0,001971	0,019804	0,019804	0,019804
<b>E5</b>	0,091818	0,198039	0,00995	0,198039		0,198039	0,00995	0,1	0,1	0,1
<b>E6</b>	0,463636	1	0,001971	1	0,198039		0,001971	0,019804	0,019804	0,019804
<b>E7</b>	0,000914	0,001971	1	0,001971	0,00995	0,001971		0,099505	0,099505	0,099505
<b>E8</b>	0,009182	0,019804	0,099505	0,019804	0,1	0,019804	0,099505		1	1
<b>E9</b>	0,009182	0,019804	0,099505	0,019804	0,1	0,019804	0,099505	1		1
<b>E10</b>	0,009182	0,019804	0,099505	0,019804	0,1	0,019804	0,099505	1	1	

Tabela F. 5 – Índice de concordância médio calculado para cada especialista

<b>AiC#1</b>		<b>AiA#1</b>	
<b>E1</b>	0,544444	<b>E1</b>	0,168011
<b>E2</b>	0,544444	<b>E2</b>	0,302781
<b>E3</b>	0,544444	<b>E3</b>	0,146143
<b>E4</b>	0,544444	<b>E4</b>	0,302781
<b>E5</b>	0,5	<b>E5</b>	0,111176
<b>E6</b>	0,277778	<b>E6</b>	0,302781
<b>E7</b>	0,544444	<b>E7</b>	0,146143
<b>E8</b>	0,5	<b>E8</b>	0,263067
<b>E9</b>	0,5	<b>E9</b>	0,263067
<b>E10</b>	0,5	<b>E10</b>	0,263067
<b>AiC#2</b>		<b>AiA#2</b>	
<b>E1</b>	0,622222	<b>E1</b>	0,213674
<b>E2</b>	0,622222	<b>E2</b>	0,126698
<b>E3</b>	0,355556	<b>E3</b>	0,14703
<b>E4</b>	0,355556	<b>E4</b>	0,271978
<b>E5</b>	0,622222	<b>E5</b>	0,213674
<b>E6</b>	0,422222	<b>E6</b>	0,200866
<b>E7</b>	0,355556	<b>E7</b>	0,14703
<b>E8</b>	0,622222	<b>E8</b>	0,271978
<b>E9</b>	0,422222	<b>E9</b>	0,200866
<b>E10</b>	0,622222	<b>E10</b>	0,271978

<b>AiC#3</b>		<b>AiA#3</b>	
<b>E1</b>	0,081395	<b>E1</b>	0,140475
<b>E2</b>	0,124031	<b>E2</b>	0,104643
<b>E3</b>	0,124031	<b>E3</b>	0,140475
<b>E4</b>	0,046512	<b>E4</b>	0,104643
<b>E5</b>	0,124031	<b>E5</b>	0,140475
<b>E6</b>	0,081395	<b>E6</b>	0,104643
<b>E7</b>	0,046512	<b>E7</b>	0,009037
<b>E8</b>	0,124031	<b>E8</b>	0,140475
<b>E9</b>	0,124031	<b>E9</b>	0,057567
<b>E10</b>	0,124031	<b>E10</b>	0,057567
<b>AiC#4</b>		<b>AiA#4</b>	
<b>E1</b>	0,066265	<b>E1</b>	0,074027
<b>E2</b>	0,12249	<b>E2</b>	0,133407
<b>E3</b>	0,12249	<b>E3</b>	0,064392
<b>E4</b>	0,066265	<b>E4</b>	0,133407
<b>E5</b>	0,12249	<b>E5</b>	0,049242
<b>E6</b>	0,066265	<b>E6</b>	0,133407
<b>E7</b>	0,066265	<b>E7</b>	0,064392
<b>E8</b>	0,12249	<b>E8</b>	0,115909
<b>E9</b>	0,12249	<b>E9</b>	0,115909
<b>E10</b>	0,12249	<b>E10</b>	0,115909



Tabela F. 6 – Cálculo dos índices de concordância relativa entre os especialistas

<b>RADiC#1</b>		<b>RADiA#1</b>	
E1	0,108889	E1	0,074027
E2	0,108889	E2	0,133407
E3	0,108889	E3	0,064392
E4	0,108889	E4	0,133407
E5	0,1	E5	0,049242
E6	0,055556	E6	0,133407
E7	0,108889	E7	0,064392
E8	0,1	E8	0,115909
E9	0,1	E9	0,115909
E10	0,1	E10	0,115909
<b>RADiC#2</b>		<b>RADiA#2</b>	
E1	0,123894	E1	0,103435
E2	0,123894	E2	0,061332
E3	0,070796	E3	0,071174
E4	0,070796	E4	0,131659
E5	0,123894	E5	0,103435
E6	0,084071	E6	0,097235
E7	0,070796	E7	0,071174
E8	0,123894	E8	0,131659
E9	0,084071	E9	0,097235
E10	0,123894	E10	0,131659

<b>RADiC#3</b>		<b>RADiA#3</b>	
E1	0,0813953	E1	0,140966
E2	0,124031	E2	0,090259
E3	0,124031	E3	0,140966
E4	0,0465116	E4	0,090259
E5	0,124031	E5	0,140966
E6	0,0813953	E6	0,090259
E7	0,0465116	E7	0,00465
E8	0,124031	E8	0,140966
E9	0,124031	E9	0,019746
E10	0,124031	E10	0,140966
<b>RADiC#4</b>		<b>RADiA#4</b>	
E1	0,0662651	E1	0,074027
E2	0,12249	E2	0,133407
E3	0,12249	E3	0,064392
E4	0,0662651	E4	0,133407
E5	0,12249	E5	0,049242
E6	0,0662651	E6	0,133407
E7	0,0662651	E7	0,064392
E8	0,12249	E8	0,115909
E9	0,12249	E9	0,115909
E10	0,12249	E10	0,115909

Tabela F. 7 – Cálculo do índice de consenso entre as opiniões *fuzzy*

<b>CDCiC#1</b>		<b>CDCiA#1</b>	
<b>E1</b>	0,092053	<b>E1</b>	0,074622
<b>E2</b>	0,092053	<b>E2</b>	0,104312
<b>E3</b>	0,119164	<b>E3</b>	0,096915
<b>E4</b>	0,095258	<b>E4</b>	0,107517
<b>E5</b>	0,077712	<b>E5</b>	0,052333
<b>E6</b>	0,101637	<b>E6</b>	0,140562
<b>E7</b>	0,095258	<b>E7</b>	0,07301
<b>E8</b>	0,121483	<b>E8</b>	0,129437
<b>E9</b>	0,12859	<b>E9</b>	0,136545
<b>E10</b>	0,076793	<b>E10</b>	0,084747
<b>CDCiC#2</b>		<b>CDCiA#2</b>	
<b>E1</b>	0,099555	<b>E1</b>	0,089326
<b>E2</b>	0,099555	<b>E2</b>	0,068275
<b>E3</b>	0,100118	<b>E3</b>	0,100307
<b>E4</b>	0,076212	<b>E4</b>	0,106643
<b>E5</b>	0,089658	<b>E5</b>	0,079429
<b>E6</b>	0,115894	<b>E6</b>	0,122476
<b>E7</b>	0,076212	<b>E7</b>	0,076401
<b>E8</b>	0,13343	<b>E8</b>	0,137312
<b>E9</b>	0,120626	<b>E9</b>	0,127208
<b>E10</b>	0,088739	<b>E10</b>	0,092622

<b>CDCiC#3</b>		<b>CDCiA#3</b>	
<b>E1</b>	0,078306	<b>E1</b>	0,107846
<b>E2</b>	0,099624	<b>E2</b>	0,08993
<b>E3</b>	0,126735	<b>E3</b>	0,134957
<b>E4</b>	0,06407	<b>E4</b>	0,093135
<b>E5</b>	0,089727	<b>E5</b>	0,097949
<b>E6</b>	0,114556	<b>E6</b>	0,12618
<b>E7</b>	0,06407	<b>E7</b>	0,045332
<b>E8</b>	0,133498	<b>E8</b>	0,14172
<b>E9</b>	0,140606	<b>E9</b>	0,107374
<b>E10</b>	0,088808	<b>E10</b>	0,055576
<b>CDCiC#4</b>		<b>CDCiA#4</b>	
<b>E1</b>	0,070741	<b>E1</b>	0,074622
<b>E2</b>	0,098854	<b>E2</b>	0,104312
<b>E3</b>	0,125965	<b>E3</b>	0,096915
<b>E4</b>	0,073946	<b>E4</b>	0,107517
<b>E5</b>	0,088957	<b>E5</b>	0,052333
<b>E6</b>	0,106991	<b>E6</b>	0,140562
<b>E7</b>	0,073946	<b>E7</b>	0,07301
<b>E8</b>	0,132728	<b>E8</b>	0,129437
<b>E9</b>	0,139835	<b>E9</b>	0,136545
<b>E10</b>	0,088038	<b>E10</b>	0,084747