COPPE/UFRJ

ANÁLISE DE UM SISTEMA SIMPLIFICADO DE CONTROLE DIGITAL PROPOSTO PARA O PRESSURIZADOR DE UMA USINA NUCLEAR ATRAVÉS DE UM MODELO DE SIMULAÇÃO DINÂMICA

Jonathan Marcello de Oliveira Pinto

Dissertação de Mestrado 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 Mestre em Engenharia Nuclear.

Orientador: Paulo Fernando Ferreira Frutuoso e Melo

Rio de Janeiro

Fevereiro de 2010

ANÁLISE DE UM SISTEMA SIMPLIFICADO DE CONTROLE DIGITAL PROPOSTO PARA O PRESSURIZADOR DE UMA USINA NUCLEAR ATRAVÉS DE UM MODELO DE SIMULAÇÃO DINÂMICA

Jonathan Marcello de Oliveira Pinto

DISSERTAÇÃO 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 MESTRE EM CIÊNCIAS EM ENGENHARIA NUCLEAR.

Examinada por:

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

Prof. Antônio Carlos Marques Alvim, Ph. D.

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

RIO DE JANEIRO, RJ - BRASIL

FEVEREIRO DE 2010

Pinto, Jonathan Marcello de Oliveira

Análise de um sistema simplificado de controle digital proposto para o pressurizador de uma usina nuclear através de um modelo de simulação dinâmica/ Jonathan Marcello de Oliveira Pinto. – Rio de Janeiro: UFRJ/COPPE, 2010.

XIII, 66 p.: il.; 29,7 cm.

Orientador: Paulo Fernando Ferreira Frutuoso e Melo

Dissertação (mestrado) – UFRJ/ COPPE/ Programa de Engenharia Nuclear, 2010.

Referencias Bibliográficas: p. 53-56.

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

Dedicada às pessoas que

amo

AGRADECIMENTOS

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

Ao meu pai pela compreensão e respeito.

Aos meus amigos, pelo espairecimento e apoio oferecidos.

À música que me leva ao equilíbrio nos momentos difíceis.

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

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

ANÁLISE DE UM SISTEMA SIMPLIFICADO DE CONTROLE DIGITAL PROPOSTO PARA O PRESSURIZADOR DE UMA USINA NUCLEAR ATRAVÉS DE UM MODELO DE SIMULAÇÃO DINÂMICA

Jonathan Marcello de Oliveira Pinto

Fevereiro / 2010

Orientador: Paulo Fernando Ferreira Frutuoso e Melo

Programa: Engenharia Nuclear

Este trabalho apresenta uma aplicação da metodologia DFM (*Dynamic Flowgraph Methodology)* em um sistema digital de controle proposto para o pressurizador (PZR) das usinas nucleares atuais. O estudo consiste na modelagem DFM desse sistema de controle e de suas interações com o processo a ser controlado. Três preocupações existentes na literatura foram consideradas na análise: A modelagem do sistema, levando-se em consideração uma visão holística, a incorporação dos resultados da análise de falhas a uma APS (Análise Probabilística de Segurança) já existente e a identificação de falhas de *software*, principal componente de um sistema digital.

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. Além disso, a DFM identifica falhas estritamente ligadas ao *software* contribuindo para a confiabilidade destes elementos.

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

ANALYSIS OF A SIMPLIFIED DIGITAL CONTROL SYSTEM PROPOSED FOR A NUCLEAR POWER PLANT PRESSURIZER THROUGH A DYNAMIC MODEL SIMULATION

Jonathan Marcello de Oliveira Pinto

February / 2010

Advisor: Paulo Fernando Ferreira Frutuoso e Melo

Department: Nuclear Engineering

This paper presents an application of the methodology DFM (Dynamic Flowgraph Methodology) on a digital control system proposed for the nuclear power plant pressurizer (PZR). The study approaches the DFM modeling of the control system and its interaction with the controlled process. Three concerns in the literature were considered in the failure analysis: The system modeling, taking into account a holistic point of view, the incorporation of the analysis results in existing PRA (Probabilistic Risk Assessment) and the identification of software failures, the main component of a digital system.

The results show that the methodology provides an efficient failure analysis of the system considering all the possible interation between its components. In addition, the DFM identifies failures strictly related to the software contributing to the reliability of these elements.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

LISTA DE SÍMBOLOS

CCMT	CELL TO CELL MAPPING TECHNIQUE
DFM	DYNAMIC FLOWGRAPH METHODOLOGY
FMEA	FAILURE MODE AND EFFECT ANALYSIS
PI	PRIME IMPLICANTS
PWR	PRESSURIZED WATER REACTOR
PZR	PRESSURIZER

1 INTRODUÇÃO

Tendo em vista a crescente incorporação de sistemas digitais em plantas 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.

A metodologia DFM (*Dynamic Flowgraph Methodology*) [3] [4] [10] [11] [18] [19] é uma das que mais cumpre os requisitos para uma modelagem de sistemas dinâmicos. Ela consiste em retirar as variáveis de maior relevância do sistema analisado, discretizá-las em estados que refletem 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.

Para ilustrar a técnica foi considerado um sistema digital de controle simplificado baseado no funcionamento do pressurizador (PZR) em usinas nucleares. O estudo se baseou na modelagem DFM desse sistema de controle e de suas interações com o processo a ser controlado.

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.

O capítulo 4 descreve brevemente o sistema de controle do pressurizador proposto.

No capítulo 5 encontra-se a modelagem DFM do sistema proposto.

O capítulo 6 explicita os resultados obtidos na análise de falhas do sistema.

O capítulo 7 encerra o trabalho com as 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 *software*s 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 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 [5], 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.

Uma abordagem para a confiabilidade de *software* 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] [6].

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 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 [6]. 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 sistemas analógicos em diversos aspectos, vantajosos ou não [1]:

- Sistemas digitais trabalham com lógicas flexíveis e expansíveis, enquanto sistemas analógicos possuem uma lógica fixa.
- Sistemas digitais trabalham com lógicas seqüenciais e os sistemas analógicos trabalham com lógicas combinacionais.
- *Softwares* não possuem condições de estresse ligadas a fatores externos e, por isso, não podem ser modelados através das técnicas convencionais de confiabilidade de sistemas.
- Sistemas digitais operam com discretizações de variáveis enquanto sistemas analógicos trabalham em tempo contínuo.
- Sistemas digitais possuem diversas interações com o processo controlado e operadores. Além disso, existem diversas dependências entre seus componentes (*hardware*, *software*).
- 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 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 predizer futuras falhas.
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 conseqüências 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 conjuntos mínimos de corte, 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 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:

- Markov/CCMT (*Cell to Cell Mapping Technique*) – Consiste em discretizar as variáveis de processo e calcular 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 [4] [7] [8] [9].
- DFM – Representação discreta do sistema de controle e do processo controlado tendo as relações de causalidade entre suas variáveis relacionadas de forma dinâmica [3] [4] [10] [11] [17] [18] [19] [20].
- 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 [12].
- Metodologia de Redes de Petri – Um modelo gráfico de representação do sistema digital, utilizando os mesmos princípios transições de

estados utilizados na abordagem clássica de sistemas operacionais [13].

- Metodologia de testes – Consiste em executar inúmeros testes e verificar falhas ou não em *softwares* [14].
- 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 [15].
- Metodologia Black-Box – Uso de um processo não-homogênio de Poisson para predizer a confiabilidade de sistemas [16].

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

- 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 falhas e sua modelagem pode 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, porém elas precisam ser validadas. 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, mas só pode ser utilizado em *softwares* (excluindo os demais componentes do sistema digital).
- Metodologia de Redes de Petri – Modela bem 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, faz suposições imprecisas acerca do desenvolvimento do *software*.

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, 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 dados de falha podem ser problemáticos para o modelo desenvolvido através desta metodologia. Também, os modelos de Markov/CCMT requerem um volume de informação muito grande, o que inviabiliza em muitos casos 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, [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 [2] [17] [18]. 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 simulação. Os dados de falha foram obtidos através de histórico operacional.

Ambas as metodologias propostas foram aplicadas a este sistema e seus resultados foram muito semelhantes qualitativa e quantitativamente [2] [18]. A DFM não apresentou precisão no tempo exato de ocorrência dos eventos, mas demonstrou possuir um alto nível de detalhamento das interações do sistema e de seus componentes. A técnica Markov/CCMT é mais rica em informações acerca do tempo exato das falhas.

Por fim, concluiu-se que ambos os métodos possibilitam a transferência de resultados para análises existentes. A metodologia Markov/CCMT necessita de uma etapa intermediária para a incorporação de seus resultados, o que não ocorre com a metodologia DFM [1] [4]. A utilização do *software* SAPHIRE foi proposta como plataforma de incorporação destes resultados [2] [18].

2.3 ESTUDO REALIZADO

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. A descrição das interações entre o sistema de controle e os demais subsistemas e variáveis de processo e a possibilidade de incorporação de seus resultados em análises existentes dão maior credibilidade a estes métodos.

Baseada na vasta aplicação encontrada na literatura e acessibilidade ao método, a DFM foi escolhida como objeto de estudo. Este método já foi utilizado para modelar dependências entre sistemas digitais de controle e falhas humanas [18], falhas de sistemas de controle em plantas nucleares [17] e falhas em sistemas digitais de controle em sistemas espaciais [20], por exemplo. Sua incorporação de resultados em análises probabilísticas de segurança não depende de nenhuma técnica intermediária, como depende a metodologia Markov/CCMT [1] [4]. Além disso sua facilidade na análise de erros de *softwares,* devido à sua modelagem mais simplista, reforça seu uso.

Para a construção do modelo foi utilizado um demo do toolset DYAMONDA® disponibilizado pela empresa ASCA® inc.

Como ilustração da metodologia, um sistema simplificado de controle digital baseado no pressurizador (PZR) de uma usina nuclear foi proposto como estudo de caso.

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. 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 do primeiro passo de construção do modelo, a análise pode ser realizada seguindo dois caminhos:

- Análise dedutiva – Consiste em definir um evento topo e rastrear as menores combinações possíveis de estados de componentes que levam a ele. É a análise utilizada em eventos topo de falha.
- Análise indutiva – Consiste na definição de eventos iniciadores e análise de suas conseqüências 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).

A DFM trabalha com o conceito de implicativos diretos **(***prime implicants* ou PI). Estes são representações lógicas multivaloradas semelhantes aos cortes mínimos encontrados em árvores de falhas [3] [10] [11]. Estas lógicas também possuem uma relação de causalidade semelhante aos resultados encontrados em análises de modos de falha e suas conseqüências (FMEA).

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 podem ser usados para representar os diversos estados em que o sistema analisado possa se encontrar [11].

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 [3] [10] [11]:

- Variáveis de Processo (VP) – Representam as principais variáveis físicas e do sistema, contínuas ou discretas. Estas variáveis são discretizadas em um número de estados que refletem 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, equações que governam seu comportamento 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 assuma um determinado valor, em função de outras variáveis. É utilizado para de 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. 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.

3.3 EXEMPLO DE UM MODELO DFM

O exemplo a seguir ilustra a metodologia DFM. A Figura 1 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.

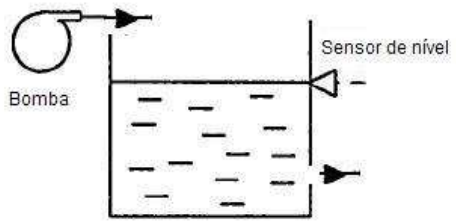

Figura 1: Sistema de Exemplo

Tabela 1: Lógica do sistema exemplo de controle

NÍVEL DE ÁGUA	BOMBA
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.

Condição do sensor (VC)	**Condição da bomba (VC)**
Normal	Normal
Falho Baixo	Falha Ligada
Falho Alto	Falha Desligada
Nível de água (VP)	**Bomba (VP)**
Vazio (até 5%)	Ligada
Baixo (até 30%)	Desligada
Normal (até 95%)	**Injeção de água (VP)**
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 2 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).

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

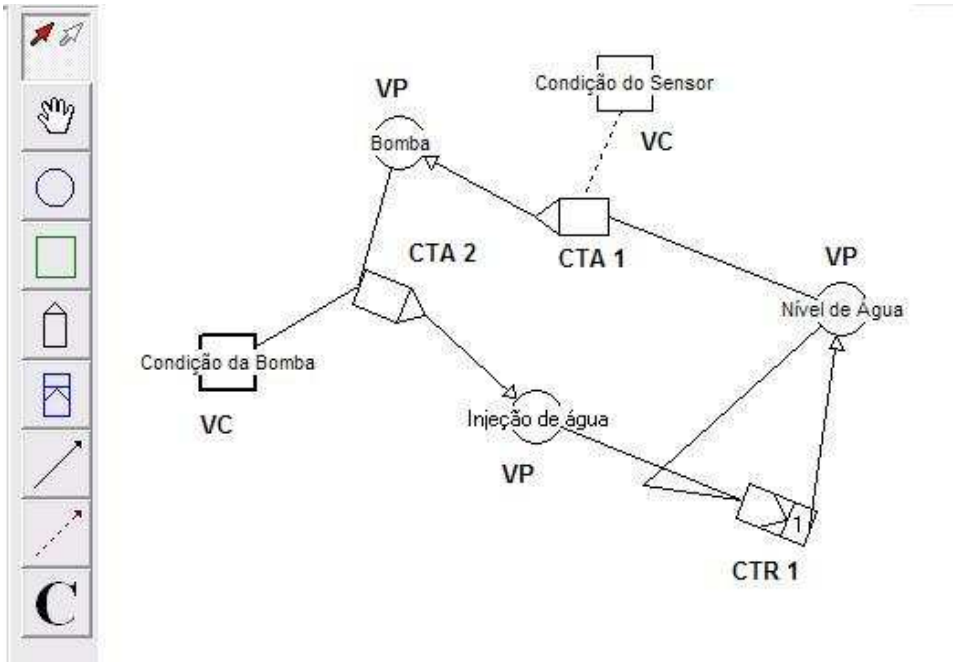

Figura 2: Modelo DFM do exemplo

Tabela 3: CTA 1

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 4: CTA 2

Bomba	Condição da bomba	**Injeção de água**
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	**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

O sinal “+” na Tabela 5 representa o estado da variável no passo de tempo seguinte ao passo 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. O nível de água é limitado a “Vazio” e “Transbordando”.

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

Utilizando o *toolset* e estabelecendo como evento topo o evento “Nível de água Transbordando em t=0”, 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 em t=0”, a DFM exibe os resultados da Tabela 7:

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

Número do implicativo	Implicativo Direto
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 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) [3] [4].

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 O SISTEMA DE PRESSURIZAÇÃO DO REATOR PWR

4.1 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 grupo de aspersores, estes presentes na zona de vapor [21].

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, aumento de pressão. Este processo continua até a variável atingir o valor nominal de 157 bar. Se a pressão aumenta, os grupos de aspersores são acionados, condensando o vapor e aliviando a pressão. Estes aspersores jogam água vinda da perna fria do reator através de uma linha de aspersão [21].

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 são acionadas, com o reator já desarmado, com a finalidade de garantir a integridade do sistema [21].

A Figura 3 ilustra o pressurizador e seus componentes [21].

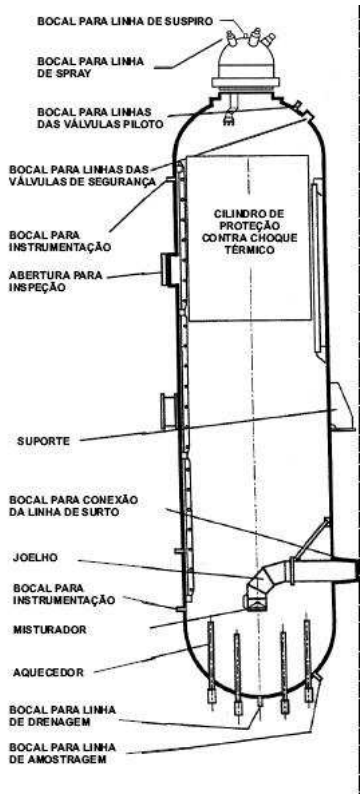

Figura 3: Pressurizador de uma usina PWR [21]

4.2 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, uma válvula de alívio com uma válvula piloto e uma válvula de segurança com uma válvula piloto.
- Os grupos de aquecedores e de aspersores atuarão juntos.
- Os modos de falhas 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 nível e Falha Aberta e Falha Fechada para as válvulas.

A Figura 4 ilustra o sistema digital proposto. A Tabela 8 sumariza a lógica de controle do sistema.

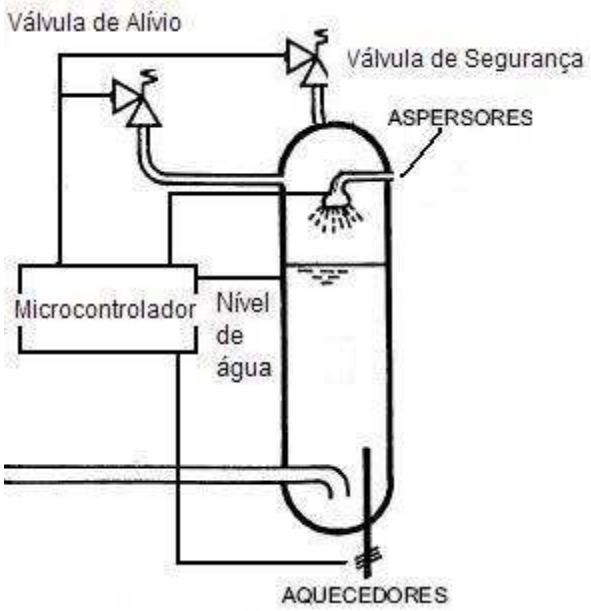

Figura 4: Sistema digital proposto

Tabela 8: Lógica de controle do sistema digital proposto

Pressão	**Aquecedores**	**Aspersores**	**Válvula de Alívio**	**Válvula de Segurança**
Muito Baixa	Ligados	Desligados	Fechada	Fechada
Baixa	Ligados	Desligados	Fechada	Fechada
Pouco Baixa	Ligados	Desligados	Fechada	Fechada
Normal	Desligados	Desligados	Fechada	Fechada
Pouco Alta	Desligados	Ligados	Fechada	Fechada
Alta	Desligados	Ligados	Aberta	Fechada
Muito Alta	Desligados	Ligados	Aberta	Aberta

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

5 MODELAGEM DFM DO SISTEMA PROPOSTO

5.1 MODELAGEM

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 parâmetros chaves do sistema de controle e por isso se tornarão variáveis de processo (VP) na modelagem DFM. A pressão é o parâmetro chave do processo controlado e por isso se tornará também uma VP. Os estados nas quais estas variáveis são discretizadas são mostradas na Tabela 9. Para a variável de pressão, os seguintes limites foram considerados [21]:

- 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 9: Discretização das variáveis de processo do modelo do pressurizador

Variável de Processo (VP)	**Estado**
Pressão	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)
Válvula de Alívio	Aberta
	Fechada
Válvula de Segurança	Aberta
	Fechada
Grupo de Aquecedores	Ligado
	Desligado
Grupo de Aspersores	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 10.

Tabela 10: Variáveis de condição do modelo do pressurizador

Variável de Condição (VC)	Estado
Estado do Sensor	Falho Alto
	Normal
	Falho Baixo
Estado do Grupo de Aquecedores	Falho Ligado
	Normal
	Falho Desligado
Estado do Grupo de Aspersores	Falho Ligado
	Normal
	Falho Desligado
Estado da Válvula de Alívio	Falha Aberta
	Normal
	Falha Fechada
Estado da Válvula de Segurança	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 11, 12, 13 e 14 representam as decisões das primeiras caixas

de transferência (CTA). Elas foram elaboradas por inspeção a partir da lógica de controle do sistema. As Tabelas 15, 16, 17 e 18 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 “acréscimo de pressão pelo grupo de aquecedores” e “decréscimo 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 A1 do Apêndice A é a principal tabela de decisão do modelo associada à única 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 necessária a aquisição do histórico de pressão de operação de uma usina nuclear [21]. A Tabela B1 do Apêndice B contém este histórico. Conforme explicado no item 3.2, um dos métodos de formulação das tabelas é através de simulações. A partir do histórico obtido, testes de aderência e gráficos de probabilidade foram elaborados com a finalidade de se verificar a melhor distribuição de probabilidade para estes dados [22] [23]. Também foi construído um histograma para este fim [23]. Verificou-se como a melhor alternativa uma distribuição normal de média 156,62 bar e desvio padrão de 0,428 bar. Estes procedimentos estão nas Tabelas C1, C2 e C3 respectivamente no Apêndice C. Em seguida, valores médios para cada faixa de pressão foram estimados. Dados de alívio/aumento de pressão dos mecanismos de controle foram obtidos de [21] e estão expostos na Tabela 19. 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 A1, a pressão se encontra no estado “Muito Baixa” com um valor médio estimado a partir da distribuição de 139,99 bar. Como há a atuação do grupo de aquecedores, existe um acréscimo de 5 bar no tempo de atuação do dispositivo, segundo a Tabela 19. Isto

leva o valor médio de 139,99 para 144,99 bar, que se encontra no intervalo “Baixa” de pressão.

Tabela 11: CTA 1 do sistema analisado

Estado do Sensor	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 12: CTA 2 do sistema analisado

Estado do Sensor	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 13: CTA 3 do sistema analisado

Estado do Sensor	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 14: CTA 4 do sistema analisado

Estado do Sensor	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 15: 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 16: CTA 6 do sistema analisado

Grupo de Aspersores	Estado do Grupo de Aspersores	**Decréscimo de Pressão**
Ligado	Normal	Com Decréscimo

Desligado	Normal	Sem Decréscimo
-	Falho Ligado	Com Decréscimo
-	Falho Desligado	Sem Decréscimo

Tabela 17: CTA 7 do sistema analisado

Válvula de Alívio	Estado da Válvula de Alívio	**Decréscimo de Pressão**
Aberta	Normal	Com Decréscimo
Fechada	Normal	Sem Decréscimo
-	Falha Fechada	Sem Decréscimo
-	Falha Aberta	Com Decréscimo

Tabela 18: CTA 8 do sistema analisado

Válvula de Segurança	Estado da Válvula de Segurança	**Decréscimo de Pressão**
Aberta	Normal	Com Decréscimo
Fechada	Normal	Sem Decréscimo
-	Falha Fechada	Sem Decréscimo
-	Falha Aberta	Com Decréscimo

Tabela 19: Dados dos dispositivos de controle

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

5.2 DADOS UTILIZADOS

A modelagem DFM possibilita uma análise quantitativa de seus resultados a partir das probabilidades dos estados de suas variáveis. Utilizando-se os dados de falha dos dispositivos de controle presentes em [24] e [25] e a distribuição de probabilidade estimada anteriormente para a pressão, estas probabilidades foram estimadas da maneira descrita abaixo e estão explicitadas na Tabela 20.

Para os dispositivos de controle em modo contínuo, considerou-se o tempo de operação de uma usina nuclear de um ano para o cálculo da inconfiabilidade. Para os dispositivos de controle de demanda, considerou-se uma demanda de operação. Foram considerados os modos de falha genéricos para cada dispositivo. As probabilidades da pressão em cada faixa discretizada foram calculadas a partir da integração da função densidade de probabilidade da distribuição no intervalo considerado.

Para algumas probabilidades de pressão, valores muito próximos de zero foram estimados, porém o valor nulo não foi utilizado no intuito de não se zerar alguns resultados antes que qualquer análise fosse realizada.

Tabela 20: Probabilidades de estado das variáveis do modelo

Dispositivo	**Estado**	**Probabilidade**
Sensor de Nível	Falho Alto	0,033
	Falho baixo	
Grupo de Aquecedores	Falho Ligado	0,018
	Falho Desligado	
Grupo de Aspersores	Falho Ligado	0,046
	Falho Desligado	
Válvula de Alívio	Falha Aberta	0,004
	Falha Fechada	
Válvula de Segurança	Falha Aberta	0,007
	Falha Fechada	
Pressão	Muito Alta	< 10E-166
	Alta	< 10E-96
	Pouco Alta	< 10E-14
	Normal	9,078 x 10E-1
	Pouco Baixa	9,218 x 10E-2
	Baixa	< 10E-81
	Muito Baixa	< 10E-295

6 ANÁLISE DO MODELO DFM

6.1 ANÁLISE DEDUTIVA

O modelo DFM, 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 suas conseqüências.

Para a análise de falhas do sistema, o modo dedutivo é o modo mais indicado. No sistema em questão, dois eventos topos são de interesse: “Pressão Muito Alta” e “Pressão Muito Baixa”, representando as falhas no controle do pressurizador e posterior *trip* do reator.

Para a realização da análise, utilizou-se o *toolset* DYAMONDA® disponibilizado pela empresa ASCA inc® [3].

Na primeira análise de “Pressão Muito Alta”, buscam-se o menor número de combinações de estados das variáveis chave 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 34 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 as válvulas estarem perfeitas e fechadas e o spray estar funcionando corretamente e desligado, ou na forma de frase:

- *Pressure was Very High @ t=0 and*
- *Relief Valve State was Normal @ t=-1and*
- *Relief Valve was Closed @ t=-1 and*
- *Safety Valve State was Normal @ t=-1and*
- *Safety Valve was Closed @ t=-1 and*
- *Pressurizer Spray was Off @ t=-1 and*
- *Spray State was Normal @t=-1*

onde t=-1 representa a notação da ferramenta para um instante qualquer antes da atuação de quaisquer dos dispositivos de controle, o resultado são os 3 implicativos diretos explicitados na Tabela 21.

Tabela 21: Implicativos diretos do evento topo “Pressão Muito Alta”

#1 (P#1≅0)	**#2 (P#2≅0)**	**#3 (P#3≅0)**
Pressure was High at time -1	*Pressure was High at time -1*	*Pressure was Very High at time -1*
Relief Valve State was Normal at time -1	*Relief Valve State was Normal at time -1*	*Relief Valve State was Normal at time -1*
Safety Valve State was Normal at time -1	*Safety Valve State was Normal at time -1*	*Safety Valve State was Normal at time -1*
Sensor State was Failed Low at time -1	*Sensor State was Failed Low at time -1*	*Sensor State was Failed Low at time -1*
Spray State was Normal at time -1	*Spray State was Normal at time -1*	*Spray State was Normal at time -1*
Heater State was Normal at time -1	*Heater State was Failed On at time -1*	

No primeiro implicativo a informação errônea do sensor em “Falho Baixo” juntamente com a condição do grupo de aquecedores em “Normal” possibilita o acionamento dos mesmos, elevando a pressão de “Alta” para “Muito Alta”.

Similarmente, no segundo implicativo, o erro do grupo de aquecedores em “Falho Ligado” eleva a pressão a “Muito Alta”. Neste caso, a condição do sensor em “Falho Baixo” foi necessária para que os demais dispositivos de alívio não pudessem ser acionados.

No terceiro implicativo, a falha no sensor em “Falho Baixo” não aciona nenhum dos dispositivos de alívio, mantendo a pressão que está em “Muito Alta”. A informação acerca dos aquecedores é irrelevante nesse caso, pois no estado “Normal” ou “Falho Ligado”, o acréscimo de pressão levaria a mesma ao nível mais alto. No caso de “Falho Desligado”, a pressão se manteria da mesma forma em “Muito Alta”.

Percebe-se, pelo valor de probabilidade ao lado de cada implicativo, que na prática é improvável a ocorrência de qualquer um deles. A justificativa é o fato de a pressão apresentar uma probabilidade muito baixa se encontrar nos estados expostos nos implicativos.

Similarmente, para a análise de “Pressão Muito Baixa:

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

o resultado são 32 implicativos diretos. Supondo que as informações que servirão de contorno consistam agora em o sensor de nível estar funcionando corretamente e o grupo de aquecedores estar desligado e funcionando, ou na forma de frase:

- *Pressure was Very Low @ t=0 and*
- *Sensor State was Normal @ t=-1and*

- *Heater was Off @ t=-1 and*
- *Heater State was Normal @t=-1*

o resultado é o implicativo direto explicitado na Tabela 22.

Tabela 22: Implicativo direto do evento topo “Pressão Muito Baixa”

#1 (P=1,0609E-06)
Pressure was Normal at time -1
Sensor State was Normal at time -1
Heater State was Normal at time -1
Safety Valve State was Failed Opened at time -1
Relief Valve State was Failed Opened at time -1
Spray State was Failed On at time -1

Neste implicativo, as falhas dos dispositivos de alívio abaixam a pressão a “Muito Baixa”. Nem mesmo o fato do sensor de nível estar em “Normal”, bem como o grupo de aquecedores, possibilita um acréscimo de pressão que compense a queda disponibilizada pelos outros mecanismos.

Percebe-se que a ocorrência do *trip* deste implicativo é muito mais provável em comparação ao *trip* do evento topo anterior, devido ao fato da probabilidade de pressão estar em “Normal” ser alta.

Os valores de probabilidade assumem grande importância, pois podem ser utilizados em uma política de manutenção através da classificação das falhas mais importantes.

A análise dedutiva da DFM possibilita a visualização das interações entre todos os componentes do sistema em questão de forma dinâmica considerando, por exemplo, o seqüenciamento 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 por sensores, atuadores e *software* (implícito na lógica que comanda algumas tabelas de decisão), e o processo controlado (variável de pressão).

Análises indutivas também poderiam ser realizadas no modelo com o intuito de verificação de *design* do sistema estudado, bem como para estabelecimento de estudos de modos de falha (FMEAS, por exemplo).

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

6.2 INCORPORAÇÃO DOS RESULTADOS EM RELATÓRIOS EXISTENTES NA ANÁLISE DE SEGURANÇA

O processo de substituição de malhas analógicas por sistemas digitais é gradativo e, por isso, diversos sistemas digitais ainda coexistem com sistemas analógicos nas mais variadas plantas industriais. Sendo assim, é preciso que os resultados da análise de falhas de um sistema digital possam ser incorporados aos resultados existentes em relatórios da análise de segurança relativos às malhas

analógicas. Somente assim é possível a realização de análises como, por exemplo, incertezas e de importância para estes resultados, como as que são realizadas para as demais árvores de falha.

Os resultados da análise DFM cumprem este quesito. Pode-se incorporá-los utilizando-se uma ferramenta tradicional de análise de falhas, como o *software* SAPHIRE, por exemplo [26]. Este procedimento é ilustrado a seguir.

O SAPHIRE solicita a importação de um arquivo texto de extensão .ftl escrito em um formato específico. Tomando como exemplo os resultados da análise de falhas do evento topo “Pressão Muito Baixa”, o arquivo .ftl seria escrito como se segue:

```
JONATHAN,SUBPRESSAO=
SUBPRESSAO      OR
        SUBPRESSAO_SUBSISTEMA_1
         SUBPRESSAO_SUBSISTEMA_2
        SUBPRESSAO_CONTROLEPRESSURIZADOR
        ETC...

SUBPRESSAO_CONTROLEPRESSURIZADOR            OR
        IMPLICATIVO_1

IMPLICATIVO_1    AND
        PRESSAO_NORMAL_T-1
        GAQUECEDORES_NORMAL_T-1
        SENSOR_NORMAL_T-1
        GASPERSORES_FALHO_LIGADO_ T-1
         VALVULAALIVIO_FALHA_ABERTA_ T-1
        VALVULASEGURANÇA_FALHA_ABERTA_ T-1
```

onde “SUBPRESSAO” representa o evento topo, “SUBPRESSAO_SUBSISTEMA1, 2, ETC...” representam os *trips* de subpressão relativos ao demais sistemas analógicos e “SUBPRESSAO_CONTROLEPRESSURIZADOR” representa o *trip* por subpressão do sistema digital de controle do pressurizador.

A Figura 5 ilustra a árvore de falha gerada pelo *software* SAPHIRE. Uma vez construído e acoplado, o trecho da árvore de falha passa a integrar a análise probabilística de segurança.

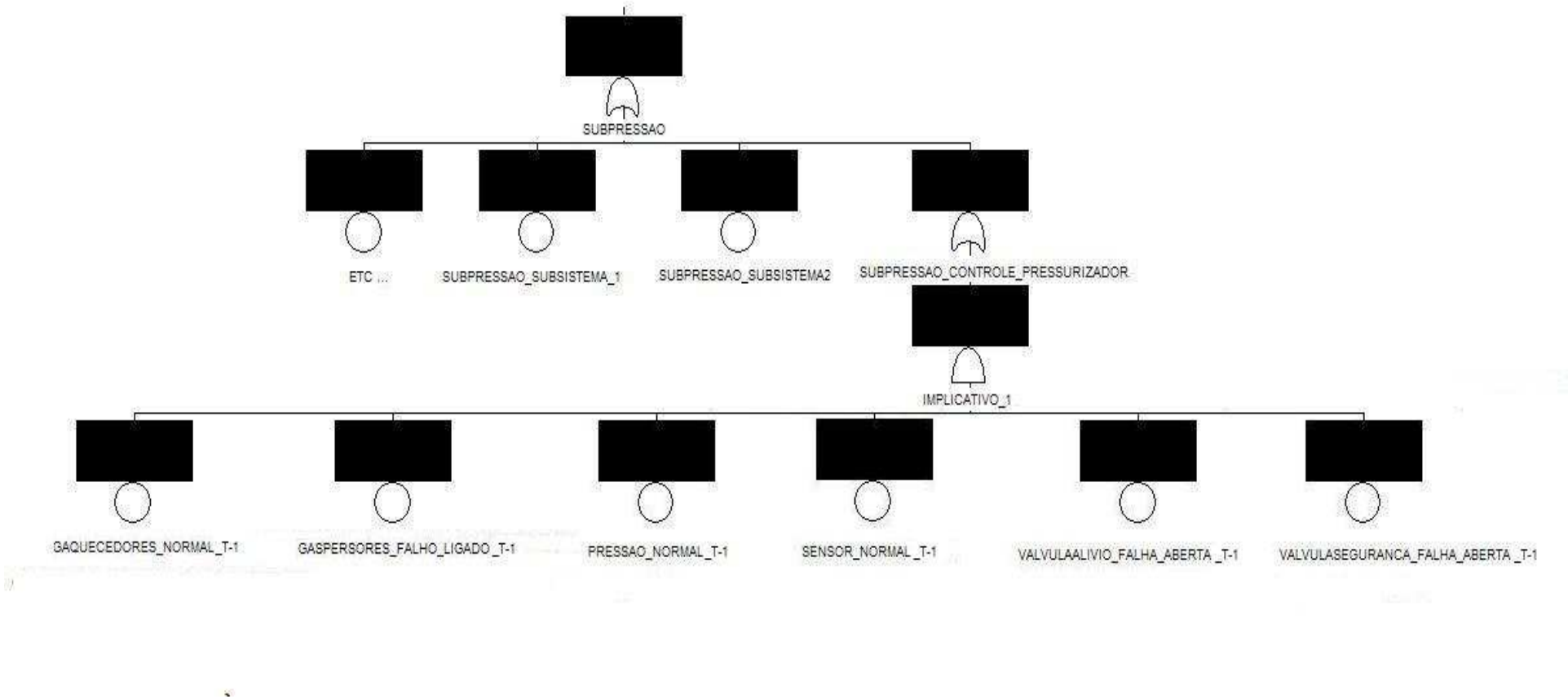

Figura 5: Trecho da árvore de falhas do evento topo “*Trip* por Subpressão”

6.3 IDENTIFICAÇÃO DE ERROS DE *SOFTWARE*

Como dito anteriormente, sistemas digitais são compostos por dispositivos físicos e *softwares* executados em um microprocessador. O *software*, portanto, é um elemento característico de um sistema digital executando toda a lógica realizada outrora por malhas analógicas complexas. Porém, como não se sabe ao certo como modelar a confiabilidade de um *software*, dada a sua flexibilidade de programação e ao fato de não se saber exatamente quando um determinado módulo irá ser executado, qualquer ferramenta que possiblite a identificação de falhas será de grande valia na confiabilidade destes elementos. A metodologia DFM através de seu modo indutivo consegue identificar erros ligados ao *software.* Este procedimento é ilustrado no exemplo a seguir.

A falha de *software* pode ocorrer de duas formas. A primeira é o erro de concepção de algoritmo, quando o programador não entende ao certo o procedimento e implanta o código de maneira errônea. A segunda falha é erro de programação, que consiste na desatenção do responsável na hora da redação do código. Ambas as falhas resultam em um código de programa falho. Apresenta-se como exemplo um erro hipotético de pseudocódigo no sistema do pressurizador:

...

{

Pressure >= Very High *then* Heater = ***FALSE*** *and Spray* = ***TRUE*** *and Relief Valve= TRUE*

Safety Valve= TRUE

} *//código certo*

...

{

Pressure >= Very High *then* Heater = ***TRUE*** *and Spray* = ***FALSE*** *and Relief Valve= TRUE*

Safety Valve= TRUE

} *//código errado*

As Tabelas 11 e 12 da modelagem DFM seriam modificadas pelo analista responsável para o conteúdo das Tabelas 23 e 24:

Tabela 23: CTA 1 do sistema modificada

Estado do Sensor	Pressão	**Grupo de Aquecedores**
Normal	Muito Alta	**Ligado**
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 24: CTA 2 do sistema modificada

Estado do Sensor	Pressão	**Grupo de Aspersores**
Normal	Muito Alta	**Desligado**
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

Aqui se nota a mudança de comportamento dos dispositivos de controle grifado em negrito.

Realizando a análise de falha:

- *Pressure was Very High @ t=0 and*
- *Sensor State was Normal @ t=-1 and*
- *Heater State was Normal @ t=-1 and*
- *Relief Valve State was Normal @t=-1*

O resultado são os dois implicativos diretos da Tabela 25.

Tabela 25: Implicativos diretos da análise de falhas de *software*

#1 (≅0)	**#2 (≅0)**
Pressure was Very High at time -1	*Pressure was Very High at time -1*
Heater State was Normal at time -1	*Heater State was Normal at time -1*
Relief Valve State was Normal at time -1	*Relief Valve State was Normal at time -1*
Sensor State was Normal at time -1	*Sensor State was Normal at time -1*
Spray State was Normal at time -1	*Spray State was Failed Off at time -1*
Safety Valve State was Failed Closed at time -1	*Safety Valve State was Failed Closed at time -1*

A princípio, nada de anormal é observado até que o responsável pela análise observe incongruências nos resultados. Nas condições do primeiro implicativo, o grupo de aquecedores estaria desligado, o grupo de aspersores estaria ligado, a válvula de alívio estaria aberta e, estando a válvula de emergência “Falha Fechada”, ela não proporcionaria o alívio esperado. O resultado desta combinação, segundo a Tabela A1, resultaria em uma queda de pressão de “Muito Alta” para “Normal”, o que não ocorre segundo o implicativo. Nas condições do segundo implicativo, o grupo de aquecedores estaria desligado, a válvula de alívio estaria aberta e, estando a válvula de emergência “Falha Fechada” e o grupo de aspersores “Falho Desligado”, estes não

proporcionariam o alívio esperado. O resultado desta combinação, segundo a Tabela A1, resultaria em uma queda de pressão de “Muito Alta” para “Alta”, o que não ocorre segundo o implicativo. Ou seja, a modelagem está errada e é necessário buscar a sua causa. A melhor forma de se verificar isto é realizar uma análise indutiva dando como parâmetros de entrada os implicativos diretos da análise anterior e verificando os passos executados pelo *toolset*. Realizando a análise:

- *Pressure was Very High at time -1*
- *Heater State was Normal at time -1*
- *Relief Valve State was Normal at time -1*
- *Sensor State was Normal at time -1*
- *Spray State was Normal at time -1*
- *Safety Valve State was Failed Closed at time -1*

No modo indutivo observam-se os passos ilustrados na Figura 6. Verifica-se que os aquecedores e aspersores são acionados de maneira errônea, pois o sensor estando “Normal” e a pressão “Muito Alta” deveriam resultar em aquecedores e aspersores “Desligados” e “Ligados” respectivamente. O responsável então procura saber por que as tabelas de decisão que relacionam as variáveis de processo estão proporcionando tais resultados. Em uma conversa com o programador (Analista), ele verifica que o código de programa está errado, descobrindo assim o porquê do erro de modelagem.

Neste exemplo, é clara a interação da falha de *software* (implícito na lógica que comanda as tabelas de decisão) com os estados dos demais componentes, demonstrando que sua análise deve vislumbrar o ambiente em que ele está inserido.

A DFM, neste caso, se mostra como uma eficiente alternativa na busca por erros de *software*, contribuindo para a análise de falhas deste elemento em sistemas digitais.

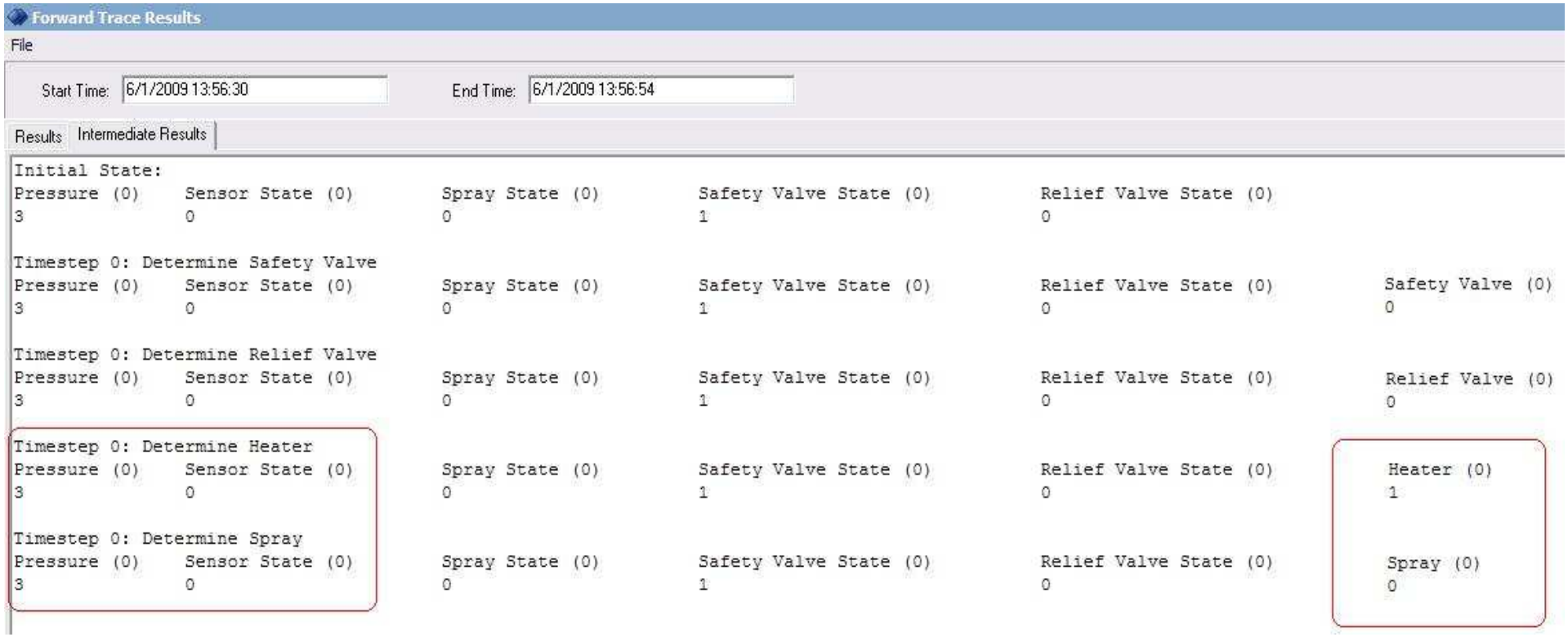

Figura 6: Erro de *Software*. Passos executados pelo *toolset* no modo indutivo.

7 CONCLUSÕES E RECOMENDAÇÕES

O presente trabalho consistiu no estudo da metodologia DFM (*Dynamic Flowgraph Methodology*) na modelagem da confiabilidade de sistemas digitais. Três preocupações existentes na literatura foram abordadas, a modelagem do sistema propriamente dito, a incorporação de resultados da metodologia em relatórios existentes na análise probabilística de segurança e a identificação de falhas de software.

A DFM mostra-se eficaz na modelagem das interações dos diversos componentes de um sistema digital (dispositivos físicos e *software*, este último implícito na lógica que comanda uma ou mais tabelas de decisão). Através dos implicativos diretos, ela possibilita a visualização dos possíveis estados do sistema, falhos ou não. Sua análise dedutiva permite um estudo de falhas eficiente, rastreando as causas de um evento topo dado. Sua análise indutiva pode ser utilizada na mitigação de falhas encontradas na análise dedutiva bem como para a verificação de especificações do sistema. Também pode ser utilizada na elaboração de uma FMEA, verificando quais as conseqüências de condições iniciais dadas. Uma limitação da metodologia é que é necessário pleno conhecimento do sistema tanto para a modelagem quanto para as mitigações. Porém uma vez construído, o sistema pode ser analisado para diversos modos de falha e eventos topos de interesse. No âmbito da construção do modelo, técnicas de modularização podem ser desenvolvidas a fim de tornar possível o uso de *templates* e conseqüente facilitação no processo de modelagem.

O estudo realizado manteve-se fiel à realidade, utilizando dados reais de uma usina PWR. Este fato retirou a relevância de alguns aspectos da modelagem DFM, como por exemplo, alguns estados da variável pressão. Na prática, estes estados mostraram ser de improvável ocorrência e isso ficou explícito nos resultados das

análises, como por exemplo, na probabilidade de ocorrência dos implicativos diretos. Trabalhos futuros poderiam utilizar uma segunda abordagem consistindo na realização de simulações onde novas funções densidade de probabilidade seriam geradas a fim de se cobrir todas as faixas dos estados considerados. Deste modo, justificar-se-ia a modelagem proposta para o sistema.

Como diversos sistemas digitais ainda coexistem com malhas analógicas, é importante que os resultados apresentados por qualquer metodologia possam ser incorporados em relatórios já existentes na análise probabilística de segurança. Somente assim, estudos de incertezas e importância, por exemplo, podem ser elaborados para os sistemas digitais tais quais são feitos para os demais sistemas na análise de falhas. A DFM demonstrou estar apta a incorporar seus resultados aos que já existem nos relatórios. Porém, cuidados devem ser tomados na incorporação para que não se crie redundâncias e ambigüidades. Trabalhos futuros podem incluir o desenvolvimento de ferramentas computacionais para a incorporação automática destes resultados aos relatórios.

Por último, dado que o *software* é elemento fundamental e característico de um sistema digital, e o fato dele não possuir uma abordagem para a confiabilidade totalmente definida, é interessante a existência de uma ferramenta que possibilite a verificação de falhas e posterior correção destes elementos. A DFM demonstrou ser uma alternativa viável através do uso de seu modo indutivo em conjunto com os resultados de falha obtidos no modo dedutivo do sistema digital estudado. Neste modo, portanto, é possível a realização de diversos testes de *design* do *software* para fins de depuração e eliminação de falhas. Porém, tal qual para a questão da modelagem, é necessário o pleno conhecimento por parte do analista do corpo do código e da lógica envolvida. Trabalhos futuros podem ser realizados no desenvolvimento de ferramentas geradoras de entradas para o *software* utilizando o modo indutivo da DFM no intuito de aumentar a confiabilidade destes elementos com a eliminação de falhas de programação.

Deste modo, o presente estudo contribui para a literatura como mais um trabalho da metodologia DFM na análise de confiabilidade de sistemas digitais críticos de controle e segurança. Espera-se que no âmbito da engenharia nuclear, ele sirva como estímulo para novos estudos, contribuindo para a área.

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 (2006).

[2] STAMATELATOS, M., *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*, *chapter 11*, NASA, Washington D.C, 2002.

[3] 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 (1996).

[4] S. GUARRO, T. ALDEMIR, 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 (2007).

[5] 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, Acesso em: 26 jan. 2010, 22:07:00.

[6] SYSTEM SAFETY SOCIETY *e-Handbook of Software safety*, Disponível em: www.system-safety.org/Documents/Software_System_Safety_Handbook.pdf, Acesso em: 26 jan. 2010, 22:07:00.

[7] 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, 1431-1436, Elsevier, New York (1991).

[8] ALDEMIR, T., *Computer-Assisted Markov Failure Modeling of Process Control Systems, IEEE transactions on Reliability*, R-36, pp. 133-144 (1987).

[9] 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).

[10] GARRET, C. J., APOSTOLAKIS, G., *Automated Hazard Analysis of Digital Control Systems*, *Reliab.Engng & System Safety*, 77, pp. 1-17 (2002).

[11] YAU, M., APOSTOLAKIS G., GUARRO, S., *The Use of Prime Implicants in Dependability Analysis of Software Controlled Systems*, *Reliability Engineering and System Safety*, 62, pp. 23-32 (1998).

[12] 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. 2002.

[13] BALAKRISHMAN, M., TRIVEDI, K., *Stochastic Petri Nets for reliability analysis of communication network applications with alternate routing, Reliab. Engng & System Safety* , 53(1996), pp. 243-259.

[14] 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. (June 2004).

[15] DO-178B, *Software Considerations In Airborne Systems And Equipment Certification*, RTCA inc, Washington, 1992.

[16] SCHNEIDEWIND, N. F., KELLER, T. W., *Applying Reliability Models to the Shuttle, IEEE Software*, July 1992, pp. 28-33.

[17] YAU, M., GUARRO, S., *A Benchmark System for Comparing Reliability Modeling Approaches for Digital Instrumentation and Control Systems*, *Nuclear Technology*, 165, pp. 53-95 (2008).

[18] GUARRO, S., ALDEMIR, T., MANDELLI, D., *A Benchmark Implementation of Two Dynamic Methodologies for the Reliability Modeling o Digital Instrumentation and Control Systems*, NUREG/CR-6985, U.S Nuclear Regulatory Commission (2009).

[19] 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 (2001).

[20] 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 49,* pp. 335-353, 1995.

[21] 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.

[22] SOONG, T.T., *Fundamentals of Probability and Statistics for Engineers*, 1 ed, New York, John Wiley & Sons Ltd, 2004.

[23] MONTGOMERY DOUGLAS C., RUNGER GEORGE C., *Applied Statistics - Probability for Engineers*, 3 ed, New York, John Wiley & Sons Ltd, 2004.

[24] IEEE STD 500-1984, *Equipment Reliability Data for Nuclear-Power Generating Stations*, IEEE and John Wiley & Sons, New York, 1984.

[25] IAEA-TECDOC-478, *Component Reliability Data for Use in probabilistic Safety Assessment*, International Atomic energy Agency, Vienna, 1988.

[26] BECK, S. T., WOOD, S. T., SMITH, C. L., et al., *Systems Analysis Programs for Hands-On Integrated Reliability Evaluations (SAPHIRE) Summary Manual*, NUREG/CR-6116, U.S Nuclear Regulatory Commission (2008).

APÊNDICE A

Tabela A1: CTR do sistema analisado

Pressão	Grupo de Aquecedores	Grupo de Aspersores	Válvula de Alívio	Válvula de Segurança	**Pressão +**
Muito Baixa	Desligado	Desligado	Fechada	Fechada	Muito Baixa
	Desligado	Desligado	Fechada	Aberta	Muito Baixa
	Desligado	Desligado	Aberta	Fechada	Muito Baixa
	Desligado	Desligado	Aberta	Aberta	Muito Baixa
	Desligado	Ligado	Fechada	Fechada	Muito Baixa
	Desligado	Ligado	Fechada	Aberta	Muito Baixa
	Desligado	Ligado	Aberta	Fechada	Muito Baixa
	Desligado	Ligado	Aberta	Aberta	Muito Baixa
	Ligado	Desligado	Fechada	Fechada	Baixa
	Ligado	Desligado	Fechada	Aberta	Muito Baixa
	Ligado	Desligado	Aberta	Fechada	Baixa
	Ligado	Desligado	Aberta	Aberta	Muito Baixa
	Ligado	Ligado	Fechada	Fechada	Muito Baixa
	Ligado	Ligado	Fechada	Aberta	Muito Baixa
	Ligado	Ligado	Aberta	Fechada	Muito Baixa
	Ligado	Ligado	Aberta	Aberta	Muito Baixa
Baixa	Desligado	Desligado	Fechada	Fechada	Baixa
	Desligado	Desligado	Fechada	Aberta	Baixa
	Desligado	Desligado	Aberta	Fechada	Baixa

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

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

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

APÊNDICE B

Tabela B1: Histórico de pressão de uma usina PWR [21]

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 C1: Gráficos de probabilidade para a distribuição normal

i	P	F(t)	F(t)-1			Distribuição Normal	
1	155,7	0,028571	-1,90222			y	x
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 C2: Histograma de Pressão

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

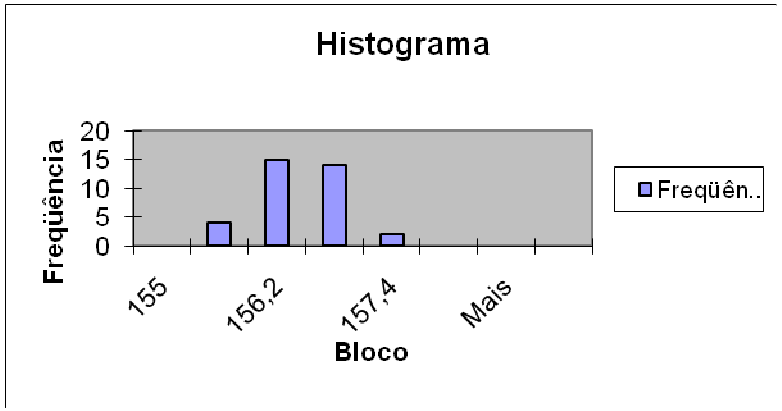

Tabela C3: Teste de aderência para a distribuição normal

i	P	F(t)				Fo(t)	Diferença	Maior Diferença
1	155,7	0,028571429				0,01584903	0,012722399	**0,251419039**
2	155,7	0,057142857				0,01584903	0,041293828	**Adere com até 99% de confiança**

3	156	0,085714286				0,073850709	0,011863577	
4	156,1	0,114285714				0,112335936	0,001949778	**Média**
5	156,2	0,142857143				0,163370619	0,020513476	**156,62**
6	156,3	0,171428571				0,227471671	0,0560431	
7	156,4	0,2				0,303731074	0,103731074	**Desvio**
8	156,4	0,228571429				0,303731074	0,075159646	**0,428265998**
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