INDISPONIBILIDADE DO SISTEMA DE REMOÇÃO DE CALOR RESIDUAL DE ANGRA I POR REDES BAYESIANAS CONSIDERANDO FALHAS DEPENDENTES

Many Ribeiro Santos Gomes

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(es): Paulo Fernando Ferreira Frutuoso e Melo
José de Jesús Rivero Oliva

Rio de Janeiro
Fevereiro de 2015

INDISPONIBILIDADE DO SISTEMA DE REMOÇÃO DE CALOR RESIDUAL DE ANGRA I POR REDES BAYESIANAS CONSIDERANDO FALHAS DEPENDENTES

Many Ribeiro Santos Gomes

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. José de Jesús Rivero Oliva, D.Sc.

_____

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

_____

Prof. Carlos André Vaz Junior, D.Sc.

RIO DE JANEIRO, RJ - BRASIL

FEVEREIRO DE 2015

Gomes, Many Ribeiro Santos

Indisponibilidade do sistema de remoção de calor residual de Angra I por redes bayesianas considerando falhas dependentes/Many Ribeiro Santos Gomes. – Rio de Janeiro: UFRJ/COPPE, 2015.

XIII, 53 p.: il.; 29,7 cm.

Orientadores: Paulo Fernando Ferreira Frutuoso e Melo.

José de Jesús Rivero Oliva.

Dissertação (mestrado) – UFRJ/ COPPE/ Programa de Engenharia Nuclear, 2015.

Referências Bibliográficas: p. 48-50.

1. Falhas Dependentes. 2. Árvore de Falhas. 3. Redes Bayesianas. 4. Sistema de Segurança. I. Melo, Paulo Fernando Ferreira Frutuoso e. *et al*. II. Universidade Federal do Rio de Janeiro, COPPE, Programa de Engenharia Nuclear. III. Título.

"Se um homem começar com certezas, ele deverá terminar em dúvidas; mas se ele se satisfizer em começar com dúvidas, ele deverá terminar em certezas."

Francis Bacon

AGRADECIMENTOS

A Deus em primeiro lugar, por nunca me permitir desistir mesmo em face aos maiores desafios.

Ao professor Paulo Fernando Frutuoso e Melo, em especial, por seu apoio incansável, além de estímulo para a minha evolução e paciência constante.

Ao professor José de Jesús Rivero Oliva, por incentivar sempre os questionamentos sobre as coisas dadas como certas.

Aos professores Pedro Luiz da Cruz Saldanha e Antonio Carlos Marques Alvim, por sempre responderem prontamente as minhas necessidades estudantis.

À minha mãe, Neide, por sua firmeza ao me educar e amor incondicional.

À minha filha, Ingrid, ser iluminado que me orgulha diariamente e que me dá a oportunidade de melhorar sempre.

Ao meu marido, Carlos, por me mostrar que companheirismo é inerente a boas pessoas e com isso fazer com que nossa relação floresça cada dia mais.

Por último, agradeço a todos aqueles que contribuíram, direta ou indiretamente, para a conclusão 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.)

INDISPONIBILIDADE DO SISTEMA DE REMOÇÃO DE CALOR RESIDUAL DE ANGRA I POR REDES BAYESIANAS CONSIDERANDO FALHAS DEPENDENTES

Many Ribeiro Santos Gomes

Fevereiro/2015

Orientadores: Paulo Fernando Ferreira Frutuoso e Melo
José de Jesús Rivero Oliva

Programa: Engenharia Nuclear

Este trabalho tem como objetivo modelar por redes bayesianas o sistema de remoção de calor residual (SRCR) da central nuclear de Angra I, utilizando o mapeamento por árvore de falhas identificando sistematicamente todos os possíveis modos de ocorrência de um grande acidente de perda de refrigerante (grande LOCA). A atenção especial está nos eventos dependentes como os sistemas ponte e com ocorrências de falhas de causa comum. Foram usados os softwares Netica™, da Norsys Software Corporation, Python 2.7.5 para a modelagem por redes bayesianas e o Microsoft Excel para a modelagem das árvores de falhas. Trabalhar com eventos dependentes usando redes bayesianas tem soluções equivalentes às propostas por outros modelos, além de simples compreensão e maior facilidade de aplicação e modificação ao longo da análise. Os resultados obtidos para a indisponibilidade desse sistema foram satisfatórios, o que mostra que na maioria dos casos esse sistema estará disponível para mitigar os efeitos de um acidente como o descrito acima.

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

UNAVAILABILITY OF THE RESIDUAL SYSTEM HEAT REMOVAL OF ANGRA 1 BY BAYESIAN NETWORKS CONSIDERING DEPENDENT FAULTS

Many Ribeiro Santos Gomes

February/2015

Advisors: Paulo Fernando Ferreira Frutuoso e Melo
José de Jesús Rivero Oliva

Department: Nuclear Engineering

This work intends to model by Bayesian networks the residual heat removal system (SRCR) of Angra I nuclear power plant, using fault tree mapping for systematically identifying all possible modes of occurrence of a major loss of coolant accident (large LOCA). The focus is on dependent events, such as the bridge system structure of the residual heat removal system and the occurrence of common cause failures. We used the Netica™ tool kit, the Norsys Software Corporation and Python 2.7.5 for modeling Bayesian networks and Microsoft Excel for modeling fault trees. Working with dependent events using Bayesian networks is equivalent to the solutions proposed by other models, beyond simple understanding and ease of application and modification throughout the analysis. The results obtained for the unavailability of the system were satisfactory, showing that in most cases the system will be available to mitigate the effects of an accident as described above.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

AF – Árvore de Falhas

APS – Avaliação Probabilística de Segurança

AS – Análise de Segurança

B – Bomba

EB – Evento Básico

ED – Evento Dependente

ET – Evento Topo

FCC – Falha de Causa Comum

FSAR – *Final Safety Analysis Report*

IRC – *Inside Reactor Containment*

IMB – *Inside Missile Barrier*

LOCA – *Loss of Coolant Accident*

LOCAG – *Loss of Coolant Accident* Guilhotina

LPIS – *Low Pressure Injection System*

NRC – *Nuclear Regulatory Commission*

OMB – *Outside Missile Barrier*

ORC – *Outside Reactor Containment*

PRA – *Probabilistic Risk Analysis*

PWR – *Pressurized Water Reactor*

RB – Rede Bayesiana

RHR – *Residual Heat Removal*

RCS – *Reactor Coolant System*

RPS – *Reactor Protection System*

SRCR – Sistema de Remoção de Calor Residual

SREN – Sistema de Resfriamento de Emergência do Núcleo

TAAR **–** Tanque de Armazenamento de Água de Reabastecimento

TPC – Tabela de Probabilidade Condicional

Capítulo 1

Introdução

Um dos objetivos em análise de segurança de centrais nucleares é o estudo do comportamento previsto da instalação nuclear durante toda sua vida, em situações normais, transitórias e de acidentes postulados, com o objetivo de determinar a adequação de itens para prevenir acidentes e atenuar as consequências dos acidentes que possam ocorrer. Para que isto seja possível, os sistemas de segurança precisam ser constantemente estudados e adequados ao longo do tempo.

O acidente de perda de refrigerante (LOCA) é considerado como acidente de base de projeto de uma central nuclear a água leve, pois é o que possui o maior potencial de liberação de produtos radioativos. O LOCA é causado por uma ruptura no circuito primário de refrigeração, que é uma das barreiras de proteção do núcleo do reator, (GLASSTONE & SESONSKE, 1994).

Com o objetivo de mitigar os efeitos desse acidente, existe uma contenção metálica que limita a liberação de radioatividade para o meio ambiente e o sistema de refrigeração de emergência do reator, que tem a missão de fornecer, em tempo hábil, uma quantidade suficiente de refrigerante para evitar a fusão do núcleo do reator. Particularmente, no caso de acidentes de perda de refrigerante no circuito primário com diâmetro equivalente igual a pelo menos 6 polegadas, a central nuclear é dotada de um sistema capaz de injetar água borada de um tanque de reserva. Este sistema é denominado sistema de remoção de calor residual (FSAR, 2010).

O objetivo do trabalho desenvolvido foi a identificação dos possíveis modos de falhas do sistema, elaboração de sua rede bayesiana representativa e definição das probabilidades a priori dos nós raízes, além do preenchimento da Tabela de Probabilidade Condicional (TPC) para os demais nós da rede.

A análise do acidente em estudo usa uma árvore de falhas (AF) e a adapta para o modelo de redes bayesianas (RB); este último tem novas possibilidades, como, por exemplo, a consideração de eventos dependentes (ED), particularmente falhas de componentes redundantes devido a causas comuns, as chamadas falhas de causa comum. Antes da utilização de RB, os ED eram modelados usando, por exemplo, Cadeias de Markov, porém, isto era extremamente trabalhoso. Será percebido então, que a operação

dos dispositivos de segurança da central assegura a integridade do elemento combustível, da geometria de refrigeração do núcleo e do edifício da contenção, (LEWIS, 1996), (MODARRES, 2006).

Inicialmente, tratou-se da identificação dos possíveis modos de falhas do sistema, da elaboração da sua RB representativa, da definição das probabilidades a priori dos nós raízes e do preenchimento da Tabela de Probabilidade Condicional (TPC) para os demais nós da rede.

Para o desenvolvimento da RB foi utilizado o procedimento de conversão de uma AF apresentada em (FRUTUOSO E MELO, 1981) e que é mostrada de maneira simplificada nas Figuras 4.11 até 4.19. Este procedimento, apesar de conveniente, corria o risco de transferir à RB as limitações da AF, e para que isto não ocorresse, precisou-se incluir entre os nós da RB as dependências que antes não estavam modeladas na AF (KHAKZAD, 2013).

As TPC também foram foco de reavaliação, com o objetivo de garantir sua representatividade e incluir na modelagem possíveis incertezas a respeito do estado dos nós filhos, dados os estados dos nós pais. Ao concluir o mapeamento da RB através da AF, a rede foi calculada usando o *software* Netica™ [1], que foi escolhido por sua disponibilidade e facilidade de manuseio.

O objetivo fundamental de estudos de confiabilidade e risco é o de dar recursos para um processo de tomada de decisão. Comumente, as variáveis que comandam o processo são sujeitas a incertezas e a variações aleatórias, os resultados dos estudos devem englobar modelos estatísticos que descrevam o comportamento de variáveis aleatórias adequadamente e devem ser simples o suficiente para que possam ser empregados pelo tomador de decisão.

Em função da frequente limitação de informações estatísticas e da dificuldade de obtenção de tais informações de especialistas, além dos custos envolvidos com seu levantamento, o número de parâmetros necessários para a descrição de tais modelos deve ser minimizado. Assim, considerando a crescente complexidade dos sistemas, o processo deve ser eficiente o suficiente para que possa ser aplicado a sistemas reais (MODARRES, 2006).

As probabilidades tentam sumarizar infinitas possibilidades para eventos relacionados. De outra maneira as representações seriam extremamente complexas ou até

[1] http://www.norsys.com/tutorials/netica/nt_toc_A.htm

inviáveis. Deste modo, ao menos aproximadamente, observa-se que com simplificações é possível enfrentar problemas complexos (AMYOTTE et al., 2011).

Estas questões vêm reduzindo ao longo do tempo o foco em procedimentos tradicionais como a AF e novas técnicas como as RB vêm recebendo maior atenção. Então, além de evidenciar o potencial das RB comparada com as técnicas mais tradicionais usadas para a análise de sistemas, será mostrado um procedimento para a elaboração da RB a partir da conversão de uma AF previamente elaborada.

O presente trabalho procura discutir a aplicação de RB a partir da conversão e adaptação de uma AF para a modelagem de ED no LPIS.

A metodologia empregada é apresentada no Capítulo 2, mostrando em que consiste o diagrama de blocos, o funcionamento da AF e da RB, além de apresentar o conceito de dependência entre falhas para o cálculo da confiabilidade de sistemas de segurança.

O Capítulo 3 é reservado para apresentar alguns conceitos do Sistema de Refrigeração de Emergência do Núcleo.

No Capítulo 4 apresenta-se o estudo de caso para que seja feita a discussão de um problema postulado, fazendo-se assim o uso da modelagem que enfatiza o sistema com componentes que possuem Falhas de Causa Comum (FCC) e o sistema com componentes em ponte. Dessa forma, é possível verificar quais as vantagens de se usar as RB para o tratamento desses problemas.

Conclusões e recomendações acerca dos resultados obtidos no trabalho e recomendações para trabalhos futuros são apresentadas no Capítulo 5.

Capítulo 2

Metodologia

Os conceitos apresentados neste item são de grande importância para os cálculos empregados ao longo deste texto.

O método de diagrama de blocos permite a compreensão das relações entre subsistemas ou componentes e a técnica de árvore de falhas permite a representação de causas de eventos indesejados no sistema estudado. Essas duas ferramentas são normalmente aplicadas em análise de confiabilidade e fornecem uma visão do arranjo e do funcionamento do sistema e, posteriormente, o resultado do cálculo de atributos de confiabilidade, como a disponibilidade do sistema.

2.1 Diagrama de blocos

O diagrama de blocos é uma das ferramentas mais usadas para a análise de confiabilidade de sistemas e permite a avaliação do efeito da falha de um item na confiabilidade do sistema. Cada item que compõe o sistema é representado por um bloco e o conjunto de blocos é arranjado no diagrama de acordo com sua configuração física e/ou funcional dentro do sistema, deste modo o entendimento das relações existentes entre os itens do sistema é facilitado.

Como resultado desta representação e dependendo da sua configuração física e/ou funcional, o sistema em análise pode ser representado por uma sequência de blocos em série (Figura 2.1 a), paralelo (Figura 2.1 b), uma combinação de sequências em série e em paralelo (Figura 2.1 c), ou por uma sequência de blocos com uma configuração complexa (Figura 2.1 d), isto é, que não permite sua decomposição em uma combinação de sequências em série e/ou paralelo. Quando um sistema é considerado complexo, recomenda-se o uso da técnica de árvore de falhas (MARTINS, 2013).

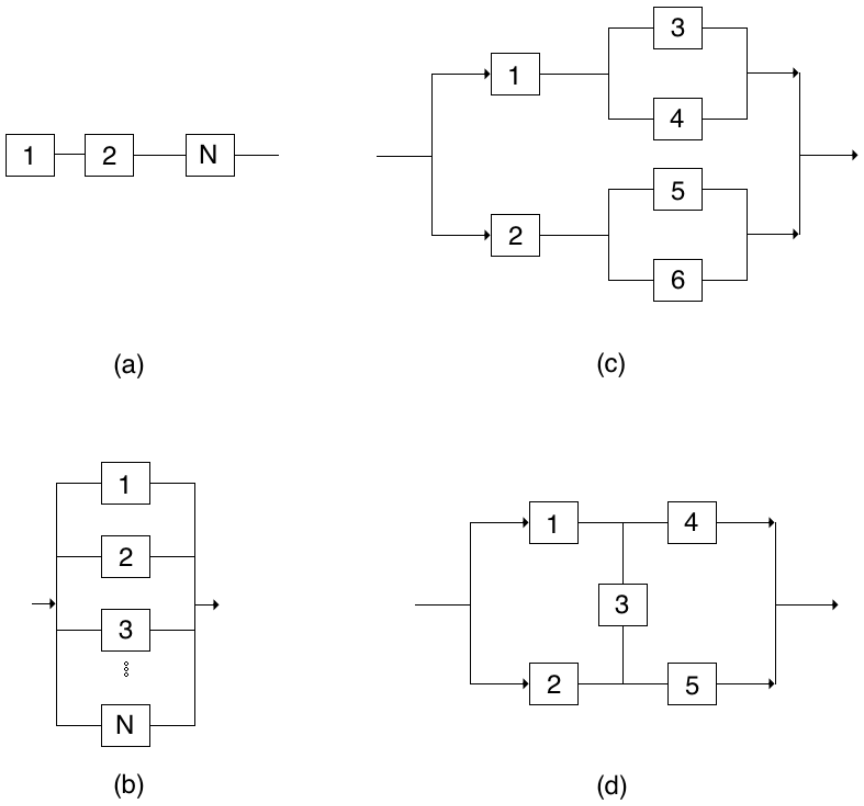


Figura 2.1 – Possíveis configurações de sistemas: (a) sistema em série; (b) sistema em paralelo; (c) sistema série-paralelo; (d) sistema complexo, (MARTINS, 2013).

2.2 Árvore de falhas

As árvores lógicas podem ser utilizadas tanto para uma avaliação qualitativa quanto quantitativa de um sistema e usam um raciocínio dedutivo para determinar as possíveis causas de um evento de interesse localizado no topo da árvore que pode ser a falha ou sucesso na execução de uma determinada missão. Caso o evento topo seja a falha de um sistema na execução de uma determinada missão, a árvore é dita de falhas, caso contrário a árvore é dita de sucesso, (LEWIS, 1996).

A análise da confiabilidade por meio de árvore de falhas tem sua origem em programas aeroespaciais e é uma das mais importantes técnicas utilizadas não somente em estudos de confiabilidade de sistemas como também em análise de riscos e são amplamente divulgadas desde o início da década de 60, (FRUTUOSO E MELO, 1981).

A Comissão Reguladora Nuclear Norte-Americana (NRC) começou a recomendar uma análise probabilística de segurança após o acidente de Three Mile Island em 1979, e

nessa época, publicou o (NUREG-0492, 1981); este documento foi de vital importância, visto que passou a ser considerada a referência técnica para a construção e aplicação da técnica de árvore de falhas.

As árvores de falhas possibilitam a avaliação da ocorrência do evento topo em função da ocorrência de múltiplos eventos que se combinam de acordo com a lógica do sistema sob análise; esta lógica é representada na árvore pela combinação de eventos básicos e/ou intermediários através de portões lógicos. A Figura 2.2 (a) mostra um diagrama de blocos que tem o componente A em paralelo com os componentes B e C que estão em série, a Figura 2.2 (b) mostra a mesma configuração da Figura 2.2 (a) representada por uma árvore de falhas, ou seja, para que o evento topo T falhe, A tem que falhar e B ou C também têm que falhar, e finalizando, a Figura 2.2 (c) representa a mesma configuração da Figura 2.2 (a) representada por uma árvore de sucesso, ou seja, para que o evento topo T funcione, A tem que funcionar ou B e C tem que funcionar.

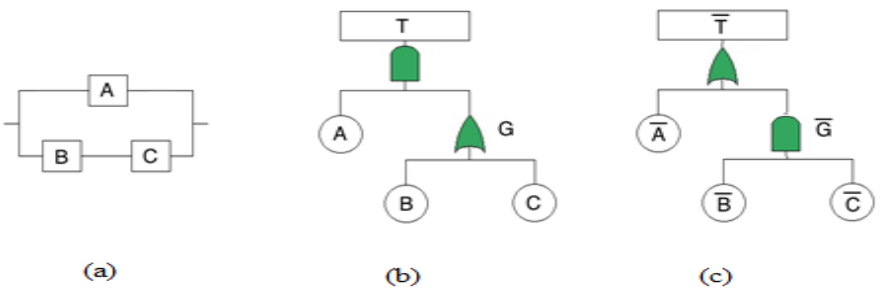


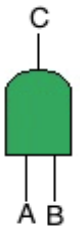
Figura 2.2 – Diagrama de Blocos, árvore de falhas e de sucesso de um sistema

Ao longo do texto, alguns símbolos comumente usados em uma árvore lógica serão usados. A título de esclarecimento as Tabelas 2.1 e 2.2 mostram estes símbolos e suas respectivas descrições.

Tabela 2.1 – Principais símbolos usados em uma árvore lógica

TIPO DO EVENTO	SÍMBOLO DO EVENTO	DESCRIÇÃO
Evento Básico		É considerado um evento iniciador
Evento intermediário ou de conexão		Evento que resulta da combinação de eventos básicos e/ou de outros eventos intermediários
Evento não desenvolvido		Evento não desenvolvido por falta de interesse ou informação
Evento de transferência		Evento que serve para indicar que o desenvolvimento de uma parte da árvore se encontra em outra página

Tabela 2.2 – Portões comumente usados em uma árvore lógica

Nome do portão	Símbolo do portão	Descrição	Interpretação do resultado
Portão E (AND)		O evento de saída ocorre se todos os eventos de entrada ocorrerem	$C = A \cap B$ $C = A.B$
Portão OU (OR)		O evento de saída ocorre se pelo menos um dos eventos de entrada ocorre	$C = A \cup B$ $C = A + B$
Portão OU exclusivo		O evento de saída ocorre se apenas um dos eventos de entrada ocorre	$C = (\bar{A} \cap B) \cup (A \cap \bar{B})$ $C = (\bar{A}.B) + (A.\bar{B})$

2.3 Dependência entre falhas

Os sistemas complexos ou simplesmente sistemas com múltiplos componentes normalmente apresentam uma concentração de falhas ou eventos de perigo nas interfaces ou dependências existentes entre seus componentes, subsistemas e ambiente externo. As falhas resultantes destas dependências, geralmente, são difíceis de ser identificadas, tratadas ou modeladas, contudo, se não consideradas, podem comprometer gravemente a qualidade dos resultados obtidos em estudos de confiabilidade ou análises de risco, pois, nesse caso, podem ocasionar estimativas otimistas de indisponibilidades ou inconfiabilidades de sistemas de segurança.

Dois eventos A e B são dependentes se $P(A|B) \neq P(A).P(B)$ ou seja, $P(A|B) = P(A|\bar{B})$ e, de modo geral, $P(A|B) \geq P(A).P(B)$, isto é, principalmente nos sistemas que apresentam vários níveis de proteção, a análise considerando as falhas como sendo independentes, comumente, superestima a confiabilidade do sistema. Neste trabalho a atenção será voltada para o tipo de dependência chamada de falhas de causa comum.

Em geral, a dependência entre eventos de falha é decorrente do ambiente (interno ou externo) onde se encontram o equipamento e/ou as pessoas envolvidas (MODARRES, 2006).

Os aspectos internos podem ser subdivididos em três categorias: 1) desafios internos; 2) dependências entre sistemas; 3) dependências entre componentes, (MODARRES, 2006).

Os aspectos externos são eventos ambientais naturais ou causados pelo homem que os tornam dependentes. Um exemplo disto é o aumento da taxa de falha de um equipamento devido à exposição à umidade, (MODARRES, 2006).

As dependências intersistêmicas e entre componentes podem ser classificadas em quatro categorias: 1) funcionais, 2) equipamento compartilhado, 3) físicas e 4) causadas pelo homem, (MODARRES, 2006).

Falhas de causa comum são consideradas, geralmente, como "... um subconjunto dos eventos dependentes em que dois ou mais estados falhos de componentes existem ao mesmo tempo, ou em um intervalo de tempo curto e são o resultado direto de uma causa compartilhada." (MOSLEH *et al*., 1988)

O tratamento quantitativo de falhas de causa comum em análises de confiabilidade é feito por meio de métodos paramétricos, em que o percentual de falhas de causa comum é levado em conta por um ou mais parâmetros. O primeiro desses métodos é o denominado do parâmetro β (MOSLEH *et al*., 1988), que será discutido e empregado neste trabalho. Métodos para o tratamento de eventuais falhas de causa comum parciais, como o modelo α, podem ser encontrados em (MOSLEH *et al*., 1988).

2.3.1 Modelo do fator β

De acordo com (NUREG/CR-5485, 1998), o modelo β é o mais antigo para a consideração de falhas de causa comum; para usá-lo, primeiramente identificam-se os componentes sujeitos a possíveis FCC, dividem-se então as possíveis falhas em duas categorias distintas: as falhas independentes e as dependentes, de tal modo que a taxa total de ocorrência de falha (λ_T) nestes componentes possa ser descrita como a soma das frequências de ocorrência de uma falha independente (λ_I) e a de uma falha dependente (λ_C), ou seja:

$$\lambda_{T=}\lambda_I+\lambda_C \qquad (1)$$

O modelo define o fator β como o percentual de falhas que ocorrem em função da FCC em relação ao total de falhas, assim:

$$\beta = \frac{\lambda_C}{\lambda_T} \quad (2)$$

O (NUREG/CR-5485, 1998) recomenda o uso deste modelo para uma avaliação quantitativa preliminar conservadora do efeito de possíveis falhas de causa comum na confiabilidade dos sistemas.

Quando dados específicos não estão disponíveis para a estimação do fator β, estimativas obtidas para outros setores industriais, sistemas ou mesmo componentes podem ser usados em uma avaliação preliminar. Numa planta nuclear, o valor estimado de β, a partir do registro de falhas para diferentes categorias de componentes, evidenciou que seu valor médio é de 0,1, (MOSLEH, 1991). Este valor médio também é verificado no registro de falhas em outros setores e pode ser considerado como genérico.

2.4 Redes bayesianas

As redes bayesianas são também conhecidas como redes de opinião, redes causais ou gráficos de dependência probabilística; são definidas como modelos gráficos para raciocínio baseadas na incerteza, nas quais os nós representam as variáveis, podendo ser discretas ou contínuas, e os arcos representam a conexão direta entre eles, (CHARNIAK, 1991).

Foram desenvolvidas no início dos anos 80 com o objetivo de facilitar a tarefa de predição em sistemas de Inteligência Artificial (IA) e vêm se tornando o método padrão para a construção dos sistemas que se fundamentam no conhecimento probabilístico, sendo aplicáveis a atividades como engenharia, medicina, etc.

As redes bayesianas são uma maneira concisa para representar conjunções de probabilidade mostrando, de modo direto e estruturado, as dependências entre as variáveis de um domínio. Elas têm esse nome devido ao fato de trabalhar com conhecimento incerto e incompleto, tratado inicialmente por meio do Teorema de Bayes, (MARTINS, 2013).

As primeiras aplicações de redes bayesianas em estudos de confiabilidade foram publicadas em (ALMOND, 1992), que propôs o seu uso para a avaliação da confiabilidade do sistema de resfriamento de um reator nuclear, (MARTINS, 2013).

A aplicação de redes bayesianas como um formalismo adequado para estudos de confiabilidade e risco vem resultando em uma série de publicações, que discutem as suas vantagens e desvantagens, quando comparada com técnicas tradicionais, como o diagrama de blocos e a árvore de falhas, como em (AMYOTTE et al., 2011).

As redes bayesianas se mostram muito interessantes quando se faz necessário o uso conjunto de informações obtidas na avaliação, acompanhamento e/ou monitoramento do sistema em questão e de informações obtidas a partir de especialistas. A identificação de exemplos de interesse em comum aproxima pesquisadores de redes bayesianas e inteligência artificial de pesquisadores interessados em confiabilidade e risco.

A pesquisa mostra que inúmeros trabalhos descrevem a aplicação de RB nas mais diversas áreas, como por exemplo, para a realização de diagnóstico médico (GOMES, 2011); para a interpretação linguística (CHARNIAK e GOLDMAN, 1989); para a proposição de processo decisório baseado em um sistema de informação geográfica (STRASSOPOULOU *et al.*, 1998) e na área jurídica (FENTON e NEIL, 2000).

2.4.1 Conceitos

A probabilidade de ocorrência de um evento E pode ser interpretada como a medida de frequência em que o evento E ocorre ou como a crença de que o evento E ocorrerá em um experimento único. A interpretação da probabilidade como frequência em uma série de experimentos repetidos é vista como interpretação objetiva, enquanto que a interpretação de probabilidade como grau de crença é vista como interpretação subjetiva ou bayesiana. Assim, a probabilidade sempre dependerá do conhecimento de quem a provê ou do que se assume como verdade de acordo com a interpretação bayesiana.

Uma rede bayesiana é um grafo direcionado acíclico (DAG) em que cada nó representa uma variável aleatória que pode ser discreta ou contínua. Estes nós são ligados por arcos direcionados que representam a dependência entre as variáveis do domínio que está sendo modelado e não é possível passar duas vezes por determinado nó seguindo um caminho que respeite as orientações dos arcos. Se um dado arco parte do nó A e chega ao nó B, então A é pai de B e B é filho de A.

A principal característica das redes bayesianas usadas neste trabalho é a possibilidade do tratamento probabilístico de dependências entre eventos a partir da especificação das causas que influenciam cada efeito. Quantitativamente, cada nó recebe uma distribuição de probabilidades condicionais mostrando a influência dos nós pais.

Sendo ambos, pais e filho, variáveis com um número finito de estados (variáveis discretas) as probabilidades condicionais para cada estado do nó filho são apresentadas na Tabela de Probabilidades Condicionais (TPC). A TPC representa a probabilidade de um dado nó se apresentar em cada um dos possíveis estados, dados os estados dos nós pais. Deste modo, considerando variáveis booleanas, um nó com k pais deverá apresentar 2^k linhas (ou colunas) em sua TPC. Um nó que não possui pais tem apenas as probabilidades iniciais relacionadas a cada possível estado, probabilidades estas conhecidas como probabilidades marginais, (MARTINS, 2013).

2.4.2 Probabilidade condicional e conjunção de probabilidades

A probabilidade de ocorrência do evento A dado que o evento B ocorreu previamente é a probabilidade condicional de A dado B**,** isto é, $P(A|B)$.

$$P(A,B) = P(A|B)P(B) \tag{3}$$

Na eq. (3), $P(A,B)$ representa a probabilidade de ocorrência simultânea dos eventos A e B, evento este representado por $A\hat{}B$. Caso os eventos A e B sejam independentes $P(A,B) = P(A)P(B)$, uma vez que, nesta situação, $P(A|B) = P(A)$. A possibilidade de representação desta relação de dependência é um diferencial importante das redes bayesianas para a modelagem de sistemas complexos em relação à técnica da árvore de falhas, onde os eventos ligados a uma porta "E" são considerados como independentes.

Como a relação $P(A,B) = P(B,A)$ deve ser satisfeita, escreve-se então a equação do Teorema de Bayes:

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)} \tag{4}$$

A Eq. (4) é fundamental para a inferência da probabilidade dos nós da rede a partir da verificação de uma evidência. A conjunção de probabilidades entre duas ou mais variáveis representa as probabilidades de ocorrência de cada combinação dos possíveis estados destas variáveis.

A modelagem do problema usando redes bayesianas permite a representação simplificada do domínio de problemas complexos considerando suas relações de

dependências relevantes. Ao considerar as relações de dependência corretamente, esta representação pode ser feita de uma forma compacta e muito útil para a modelagem de problemas com muitas variáveis em seu domínio.

É importante ressaltar que o detalhamento da rede, através da inclusão de nós ou de relações de dependência, pode trazer dificuldades para encontrar as probabilidades para povoar a rede (preencher as TPC). O que se deve ponderar é a relação entre os ganhos com este detalhamento e os custos para se obter as informações necessárias a este preenchimento.

Para um maior detalhamento de modelagem da RB recomenda-se (LEITE, 2014) e (MARTINS, 2013).

A título de exemplo, a Figura 2.3 representa a montagem de três AF e suas respectivas TPC. Neste caso a Figura 2.3 (a) representa o portão E, a Figura 2.3 (b) representa o portão OU e a Figura 2.3 (c) representa o portão OU exclusivo. Em cada caso, apresentam-se a árvore de falhas, a rede bayesiana correspondente e a tabela de probabilidades condicionais. Nesta tabela 'v' representa o fato de que o evento ocorre, enquanto a letra 'f' representa que o evento não ocorre. $P(C = v)$ representa as combinações de ocorrência ou não de A e B e sua contribuição para a ocorrência de C. Por exemplo, na Fg. 2.3 (a), somente a primeira consideração (A e B ocorrem) contribuem para a ocorrência de C.

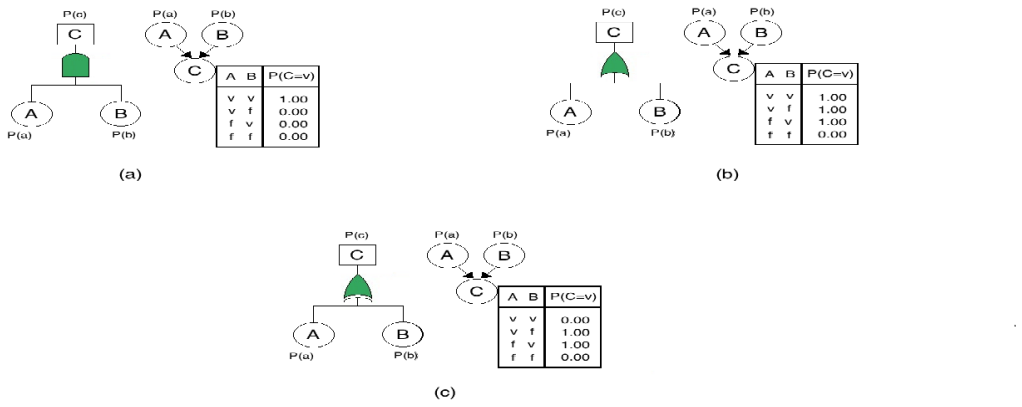


Figura 2.3 – Conversão de Árvore de Falhas em Redes Bayesianas

2.5 Netica™

Netica™ é um programa desenvolvido pela Norsys Software Corp., empresa especializada em software de RB. As informações do site[2] da empresa dizem que o programa já está em desenvolvimento desde 1992, tornou-se disponível para comercialização em 1995.

Através do Netica™, podem ser analisados modelos probabilísticos, removendo ou adicionando influencias causais, otimizando uma decisão no tempo, entre outros. Estas operações podem ser feitas através de apenas um clique do *mouse*, o que torna o Netica™ adequado para pesquisa e ensino de redes de opinião, (DIONISIO, 2014).

[2] http://www.norsys.com/tutorials/netica/nt_toc_A.htm

CAPÍTULO 3

SISTEMA DE REFRIGERAÇÃO DE EMERGÊNCIA DO NÚCLEO

Para a elaboração deste capítulo as referências foram obtidas do (FSAR, 2010) e de (FRUTUOSO E MELO, 1981).

O sistema a ser estudado, isto é, aquele que realiza a fase de injeção ativa a baixa pressão, é um dos subsistemas que constituem o Sistema de Refrigeração de Emergência do Núcleo (SREN).

Este capítulo começa com uma discussão do acidente de perda de refrigerante, em seguida, mostra o sistema de refrigeração de emergência do núcleo, onde é analisado o subsistema de interesse, discutindo-se então o funcionamento do mesmo após a ocorrência do acidente de perda de refrigerante do tipo guilhotina.

3.1 Acidente de Perda de Refrigerante (LOCA)

O pior acidente de perda de refrigerante em reatores a água pressurizada é uma ruptura do tipo guilhotina em uma das pernas frias do circuito primário, a qual resulta na mais alta temperatura local do revestimento do combustível.

O acidente começa com uma ruptura instantânea da tubulação da perna fria, entre a bomba principal e o vaso de pressão do reator. O refrigerante no estado subresfriado sofre uma rápida despressurização, até que a pressão de saturação seja atingida.

A redução da pressão no sistema e a alta pressão no edifício da contenção são condições anormais que aparecem na fase de despressurização, sendo detectadas pela instrumentação e controle, ativando então o sistema de refrigeração de emergência do núcleo.

A temperatura do revestimento das barras sobe rapidamente após a ocorrência da ruptura, devido à redução do escoamento e ao aumento do título termodinâmico local, que fazem com que o fluxo crítico de calor seja excedido. Como a eficiência de remoção de calor pelo refrigerante cai, há uma redistribuição do calor armazenado e uma maior equalização de temperaturas entre o combustível e o revestimento.

Ainda que haja um grande aumento na fração de vazios no núcleo, o que faz com que o reator seja desligado, há ainda geração de calor no combustível devido às fissões por nêutrons atrasados e ao decaimento dos produtos de fissão.

Na fase de despressurização, a água de refrigeração de emergência é injetada nas pernas frias e escoa através do espaço anular do vaso do reator em direção à câmara plena inferior. No entanto, o escoamento pode ser desviado em volta do núcleo e descarregado diretamente para a contenção pela perna fria que sofreu ruptura.

No fim da fase de despressurização, o núcleo está imerso em vapor saturado ou superaquecido, e o circuito primário está praticamente vazio. O SREN continua a injetar água e a câmara plena inferior começa a encher. Cerca de 30 segundos após o início do acidente, o nível de água atinge a parte inferior do núcleo, o que define o período chamado de fase de reenchimento. O período compreendido entre o final do reenchimento da câmara plena inferior e o reenchimento do núcleo é chamado de fase de reinundação.

A Figura 3.1 mostra um modelo simplificado de uma ruptura na perna fria entre uma bomba e o núcleo.

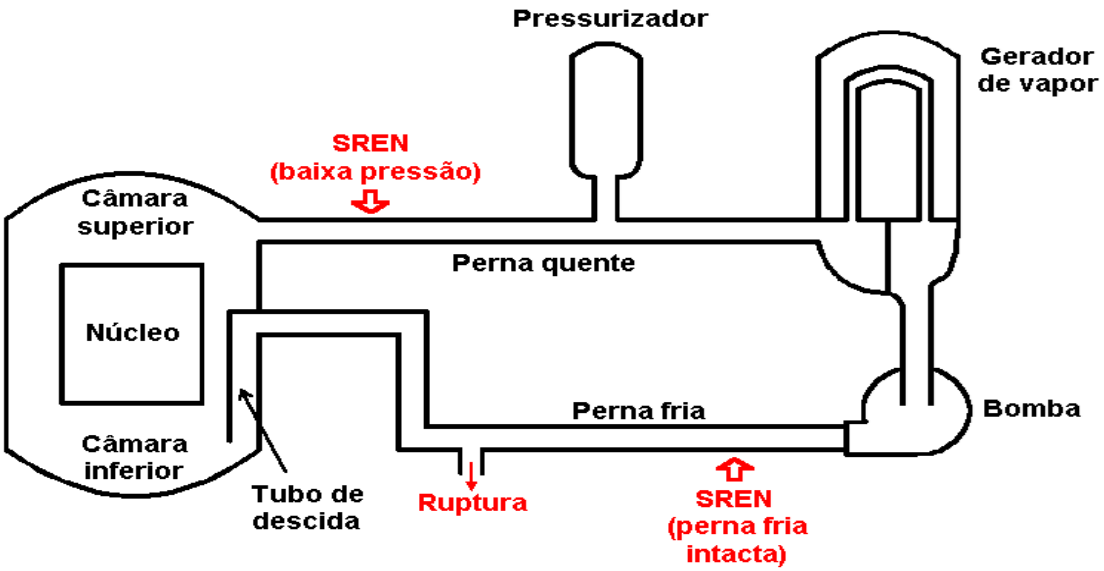


Figura 3.1 – Exemplo de LOCA, Adaptada de (GLASSTONE & SESONSKE, 1994).

3.2 Uma Visão Geral do Sistema de Refrigeração de Emergência do Núcleo

O sistema de refrigeração de emergência do núcleo é projetado para proteger o núcleo do reator contra as possíveis consequências de algum acidente, principalmente o LOCA. Um controle automático detecta a ocorrência do acidente e coordena a operação das diversas partes do sistema, de acordo com as circunstâncias do acidente. Seus

principais componentes são os acumuladores, as bombas de injeção de segurança e as bombas de remoção de calor residual.

A Figura 3.2 mostra de forma simplificada os dispositivos técnicos de segurança de um PWR, em especial a Figura 3.2 mostra que o sistema de remoção de calor residual está ligando o tanque de armazenamento de água de reabastecimento ao núcleo do reator.

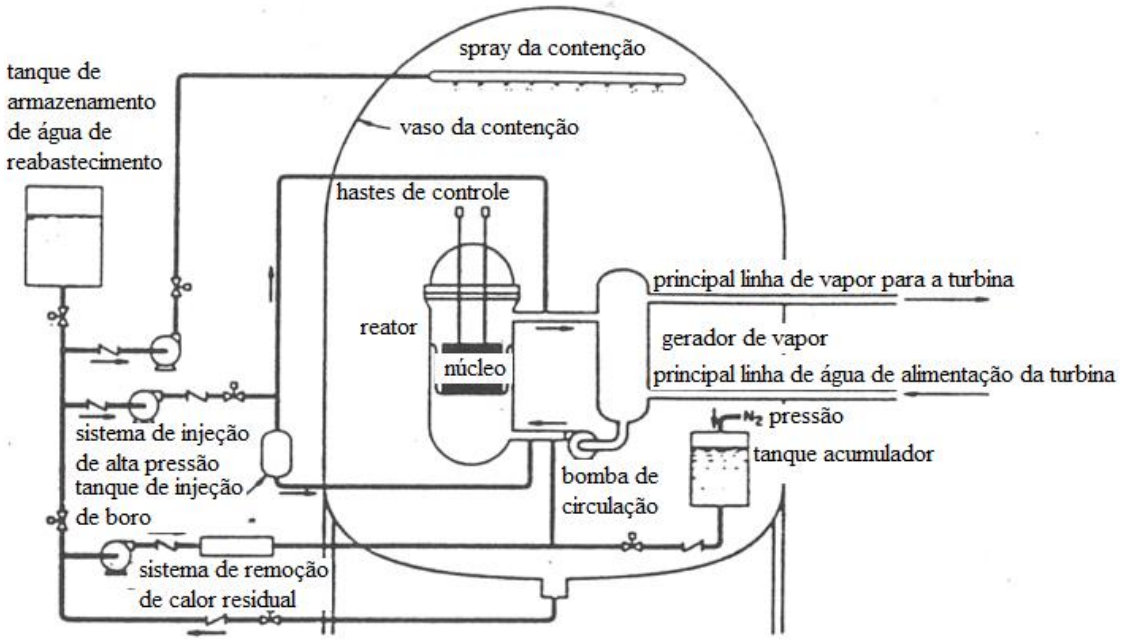


Figura 3.2 – Dispositivos técnicos de segurança de um PWR, Adaptada de (COTRELL, 1973).

A função principal do SREN é suprir de água borada o núcleo do reator após o acidente para resfriar e limitar o aumento de temperatura do material que reveste o combustível, evitando assim que haja dano ao núcleo e, consequentemente, evitando a fuga de materiais radioativos para o meio ambiente.

O SREN tem muitos subsistemas independentes, cada qual caracterizado por redundância de equipamentos e caminhos de escoamento, permitindo flexibilidade na operação e no resfriamento contínuo do núcleo, mesmo com a falha de algum componente do subsistema.

3.3 Sistema de Injeção de Refrigerante de Emergência a Baixa Pressão

O sistema de injeção a baixa pressão (LPIS) transfere o calor residual proveniente do sistema de refrigeração do reator para o sistema de resfriamento do componente com o objetivo de reduzir a temperatura do refrigerante do reator à temperatura de desligamento a frio a uma taxa controlada durante a segunda parte do resfriamento normal da planta e mantém esta temperatura até que se dê partida novamente na planta.

Esse sistema também é usado para transferir a água de recarga entre a cavidade de reabastecimento e o tanque de armazenamento de água de abastecimento, antes e depois das operações de reabastecimento.

Durante a geração de energia e operação de desligamento quente, o LPIS não está em serviço, mas está alinhado para operação como parte do sistema de resfriamento de emergência do núcleo.

Ele faz parte do conjunto de componentes do SREN que realiza a função de injetar água borada a baixa pressão no vaso do reator durante a fase de injeção ativa. Este sistema possui duas funções, uma em operação normal e outra em acidente. Neste trabalho, será avaliada a função em acidente.

A Figura 3.3 apresenta um esquema simplificado do LPIS.

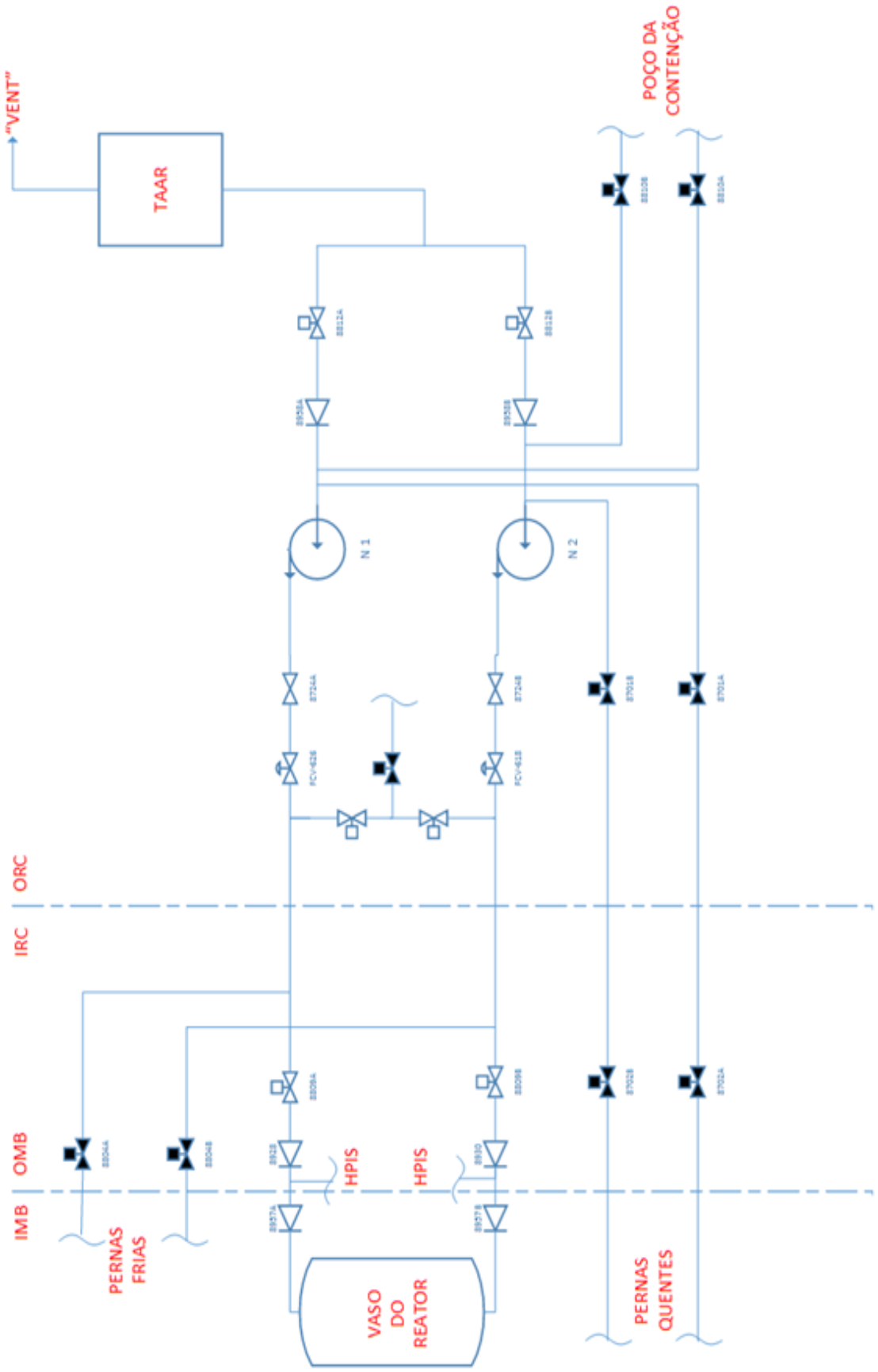


Figura 3.3 – Esquema do LPIS

3.3.1 Descrição do Sistema

O sistema de injeção a baixa pressão consiste em dois trens de vazão paralelos, cada um consistindo de um trocador de calor residual, uma bomba de remoção de calor residual e tubulações associadas, além de válvulas e instrumentação necessárias para o controle da operação. Cada linha de entrada para o sistema é ligada à perna quente de um circuito de resfriamento do reator, enquanto que cada linha de retorno está ligada à perna fria de um circuito de resfriamento do reator através das linhas de injeção de acumuladores.

As funções em acidente do LPIS em conjunto com a parte alta da *head* do sistema de resfriamento de emergência do núcleo fornecem injeção de água borada a partir do tanque de armazenamento de água de recarga ao interior do vaso do reator, durante a fase de injeção, após um LOCA.

Em sua capacidade como sistema de resfriamento de emergência, o LPIS fornece para a parte baixa o *head* do núcleo, a longo prazo, capacidade de recirculação para a refrigeração do núcleo após a injeção na fase de acidente de perda de refrigerante (LOCA).

Os principais componentes deste sistema são:

a) Bombas de Remoção de Calor Residual

Duas bombas são usadas para fornecer um grande escoamento de água borada a baixa pressão para o sistema de refrigeração do reator. Além disso, elas também recirculam água do poço da contenção para o reator e para a sucção das bombas de alta pressão. Estas bombas são centrífugas, verticais e movidas a motores elétricos.

b) Tanque de Armazenamento de Água de Recarregamento (TAAR)

A capacidade deste de tanque é de 28500 galões de água borada (a 2000 ppm) à pressão atmosférica. Ele deve fornecer água borada para inundar o compartimento do reator por ocasião da recarga de combustível e, caso ocorra um acidente de perda de refrigerante, deve suprir as bombas de injeção de segurança, as bombas de remoção de calor residual, bem como as bombas de *spray* da contenção. A capacidade deste tanque é dimensionada de modo a preencher a exigência de encher o canal de recarregamento. Esta capacidade fornece uma quantidade de água borada para assegurar:

a) Um volume de água borada suficiente para preencher o vaso do reator acima dos orifícios de entrada e saída;

b) Um volume de água borada suficiente para prevenir totalmente o retorno à criticalidade, com o reator desligado a frio e todas as barras de controle, exceto a mais reativa, inseridas no núcleo;

c) Um volume de água no poço da contenção suficiente para permitir o início da recirculação.

c) Válvulas

Como somente os principais componentes do sistema estão sendo comentados, apenas algumas válvulas serão descritas.

a) 8804 A, B

São válvulas de portão operadas a motor, que isolam as linhas de retorno das bombas de remoção de calor residual para o sistema de refrigeração do reator durante a fase de *cooldown*. Na fase de operação normal da usina, estas válvulas estão fechadas e permanecem assim na fase de injeção.

b) 8807 A, B

São válvulas operadas a motor, situadas na linha de conexão dos dois trens do LPIS e que normalmente estão abertas durante a operação normal da usina, permanecendo assim na fase de injeção.

c) 8809 A, B

São válvulas de portão operadas a motor, que estão normalmente abertas durante a operação normal da usina, permanecendo assim durante a fase de injeção de segurança.

d) 8810 A, B

São válvulas de portão operadas a motor, situadas nas duas linhas de sucção do poço da contenção para a sucção das bombas de remoção de calor residual; estão normalmente fechadas durante a operação normal da usina e só são abertas durante a fase de recirculação.

e) 8812 A, B

São válvulas de portão operadas a motor, situadas nos trens do LPIS e normalmente estão abertas durante a operação normal da usina. Fornecem sucção para as bombas de remoção de calor residual na fase de injeção ativa.

Ao receberem o sinal de injeção de segurança, as válvulas de isolamento deste subsistema são abertas e as bombas partem, fornecendo água borada do TAAR diretamente ao vaso de pressão, através de duas linhas redundantes. O funcionamento de uma das bombas garante o desempenho adequado do sistema.

3.3.2 Disponibilidade e Confiabilidade do Sistema

O sistema é equipado com duas bombas de remoção de calor residual e dois trocadores de calor residual dispostos em caminhos de escoamento independentes. Estes dois caminhos separados tem capacidade de união para garantir a segurança do sistema de injeção a baixa pressão. A perda de um caminho de escoamento do sistema de remoção de calor residual não negaria a capacidade do sistema de resfriamento de emergência do núcleo, pois os dois caminhos de escoamento fornecem redundância completa para as necessidades de segurança.

A título de observação, quando o tanque de injeção de boro foi concebido deveria conter um valor nominal de 12 por cento em peso de solução de ácido bórico concentrado, mas, percebeu-se que esta concentração não era necessária, visto que uma concentração menor garantia a segurança do processo. Assim, atualmente, opera com menores concentrações desta solução, em uma gama de 1,24 - 1,3 por cento em peso (2.500 a 3.000 ppm de boro), (FSAR, 2010). Ele é conectado à descarga das bombas de injeção de segurança. Durante a atuação do sinal de injeção de segurança, as bombas de injeção de segurança fornecem a pressão para injetar a solução de ácido bórico para a refrigeração do sistema do reator quando são abertas as válvulas de isolamento.

3.4 Operação do SREN, após a ocorrência de um LOCA

A eficiência do SREN é estimada através da capacidade de manter o núcleo inundado, ou de reinundá-lo após um acidente de perda de refrigerante, até mesmo após uma (postulada) grande área de ruptura.

Tanto as bombas de injeção de segurança como as de remoção de calor residual foram projetadas para atuar a plena capacidade, em cerca de 20 seg após a recepção do sinal de injeção de segurança. Este sinal é ativado em qualquer um dos seguintes casos:

- Baixa pressão no pressurizador;
- Alta pressão na contenção;
- Baixa pressão na linha de vapor;
- Atuação manual.

O SREN opera em três fases distintas, a saber:

- Fase de injeção passiva;
- Fase de injeção ativa;
- Fase de recirculação.

A operação inicial após a ocorrência de um LOCA é completamente automática, dada através do sinal de injeção de segurança. Os geradores diesel partirão independentemente de haver ou não *blackout* na usina.

Para acidentes de perda de refrigerante do tipo guilhotina, que tem como característica uma queda rápida de pressão do sistema de refrigeração do reator, a injeção é feita através dos caminhos de injeção de *heads* de alta e baixa pressão. Contudo, a maior parte da injeção é feita através do *head* de baixa pressão, que é o foco deste estudo. Neste tipo de acidente, o operador somente monitora a partida do equipamento de segurança e a abertura adequada das válvulas de segurança.

Se o operador considerar que as condições que delimitam o acidente de perda de refrigerante (durante o período anterior à atuação do sinal de injeção de segurança) indicam que a injeção de segurança é necessária, ele pode iniciar o sinal de injeção de segurança manualmente, a partir da sala de controle principal.

Mesmo que haja somente o mínimo de energia disponível, caracterizada pelo funcionamento de somente um dos dois geradores diesel, o equipamento passível de ser empregado na refrigeração de emergência é composto por uma das bombas de injeção de segurança, uma das bombas de remoção de calor residual e os dois acumuladores, não sendo considerada a água injetada pelo acumulador ligado à perna fria que sofreu ruptura, a qual é lançada diretamente na contenção e coletada pelo poço existente na mesma. Nesta situação, o sistema deve funcionar qualquer que seja o tamanho da ruptura na perna fria, incluindo a ruptura do tipo guilhotina.

3.5 Fase de injeção

Os principais componentes do SREN, que fornecem refrigeração do núcleo de emergência imediatamente após uma perda de líquido refrigerante são os acumuladores (um para cada circuito), duas bombas de injeção de segurança (*head* alta) e as duas bombas de remoção de calor residual (*head* baixa).

Os acumuladores, que são componentes passivos, descarregam nas pernas frias da tubulação de refrigeração do reator, quando a pressão diminui abaixo de cerca de 750 psig (52,7 kg/cm^2) rapidamente garantindo refrigeração do núcleo para grandes rupturas.

O sinal de injeção de segurança abre as válvulas de isolamento e o SREN parte as bombas de injeção de segurança e bombas de remoção de calor residual, as útlimas em geral só partem caso sejam rupturas a partir do diâmetro de 6 polegadas. As bombas de injeção de segurança de *head* alta succionam a partir do tanque de armazenamento de

água de recarga e do tanque de injeção de boro que está localizado na descarga das bombas de injeção de segurança de *head* alta, (FSAR, 2010).

As bombas de remoção de calor residual entregam água através de duas entradas que penetram na tubulação de descida no vaso do reator.

Em uma análise de grande LOCA, a bomba de remoção de calor residual não atua até que a pressão do sistema atinja cerca de 150 psia (10,5 kg/cm^2). Durante esta fase de purga do acidente, a principal fonte de fornecimento de líquido de arrefecimento externo é o acumulador ligado ao circuito intacto (o acumulador ligado ao circuito que sofre a ruptura é assumido como completamente perdido na análise). No entanto, quando o acumulador fica vazio na parte posterior da fase de reenchimento do transiente, torna-se o sistema de remoção de calor residual a principal fonte de fornecimento do líquido de refrigeração para manter o resfriamento do núcleo e para a sua eventual recuperação.

O tanque de injeção de boro, o qual está localizado na *head* alta de segurança, fornece resfriamento nas pernas frias e também água borada (2500 ppm a 3000 ppm de boro); é isolado a partir do sistema de refrigeração do reator por duas válvulas motorizadas de retenção em série, normalmente fechadas, operadas por válvulas de gaveta. É isolado dos acumuladores por três válvulas de retenção em série normalmente com válvulas de portão fechadas. O reservatório é isolado das bombas de injeção de segurança de *head* alta por duas válvulas paralelas de portão operadas a motor e normalmente fechadas.

As válvulas de isolamento no alto da *head* de injeção na contenção do reator, inicialmente, não recebem um sinal para abrir. Isto faz com que todo a vazão das bombas de injeção de segurança de *head* alta fluam através da perna fria contendo o tanque de injeção de boro.

É importante notar que um sinal de injeção de segurança é gerado tanto para rupturas de linha de vapor quanto para rupturas do sistema primário (acidente de perda de refrigerante). O atraso de tempo de cerca de três minutos de duração ocorre cada vez que o sinal de injeção de segurança é recebido.

Como a fase de injeção do acidente é encerrada antes do tanque de armazenamento ser completamente esvaziado, todos as tubulações permanecem cheias com água quando a recirculação é iniciada. A indicação do nível de água e alarmes na recarga do tanque de armazenamento de água dão ao operador aviso amplo para terminar a fase de injeção. Indicadores de nível adicionais são fornecidos no reservatório da contenção que também indicam que a injeção pode ser encerrada e a recirculação iniciada.

Capítulo 4

Estudo de Caso

Uma maneira de elaborar um diagnóstico para um sistema relativamente simples sugere a execução de 3 etapas: Identificação dos possíveis modos de falha do sistema, elaboração da sua rede bayesiana representativa e definição das probabilidades a priori dos nós raízes, além do preenchimento da TPC para os demais nós da rede, (LAMPIS e ANDREWS, 2008).

O preenchimento das TPC dos nós que não são raízes é feito automaticamente a partir da tradução dos portões lógicos das AF para os correspondentes nós da RB, o que é uma facilidade adicional em relação à elaboração da RB a partir da análise direta do sistema, (MARTINS, 2013).

A modelagem de sistemas ou de uma rede de eventos usando AF é limitada pela dificuldade de representação de domínios com muitas variáveis ou variáveis com múltiplos estados e também pela dificuldade de representação de relações de dependência ou pela necessidade de um grande número de informações para a representação do domínio, informações que muitas vezes são indisponíveis ou pouco intuitivas.

A taxa de falha λ é a taxa de falha genérica do componente e envolve a falha em função de qualquer um de seus modos de falha e pode ser obtida de banco de dados, dados de campo ou teste de confiabilidade.

O tratamento de eventos de causa comum usando RB é feito incluindo-se uma probabilidade de ocorrência do evento na TPC. Após definida a rede, ela deve ser analisada tanto qualitativa quanto quantitativamente para certificar-se da sua representatividade.

De acordo com o trabalho de (LEITE, 2014), as RB geraram resultados bem de acordo com os modelos de Markov e decomposição pivotal, no entanto, as RB são muito mais fáceis de serem modeladas do que os métodos citados acima.

Usualmente, no ambiente industrial, o uso das RB é feito para a especificação do período de manutenção de uma unidade de produção visando a minimização da indisponibilidade da unidade, (MARTINS, 2013).

4.1 Sistema com componente em ponte

Consideremos que o componente E é inserido para conectar duas linhas de componentes redundantes de um sistema, na Figura 4.1 os nós representam os componentes.

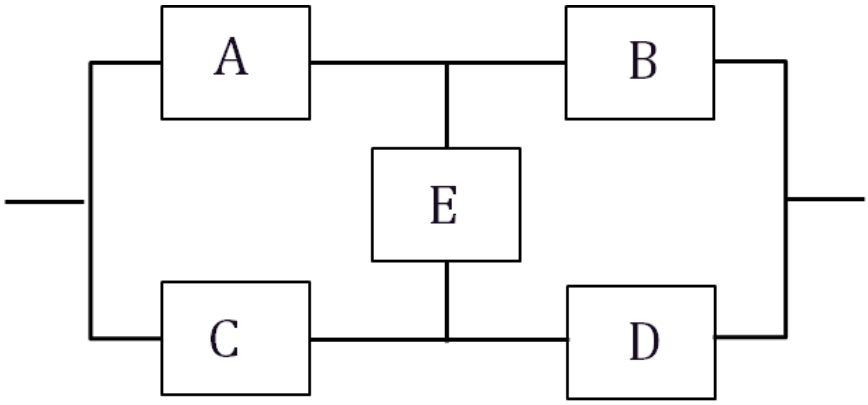


Figura 4.1 – Sistema em ponte

O sistema ponte da Figura 4.1 pode ser modelado por uma RB da Figura 4.2 considerando os nós A, B, C, D e E como as confiabilidades (dadas em %) de cada um desses componentes. A Tabela 4.1 tem todas as possibilidades de configuração do sistema, isto é, o Netica gerou todas as combinações possíveis para os componentes e o analista preencheu a coluna "LOCAG" a partir da observação de todas as linhas que mostraram se o sistema funcionava ou não naquela determinada combinação, sendo especificadas entre elas as que fazem com que o sistema funcione.

Por exemplo se A, C e E estão funcionando o sistema opera, porém se A, C e E estão falhos o sistema não opera.

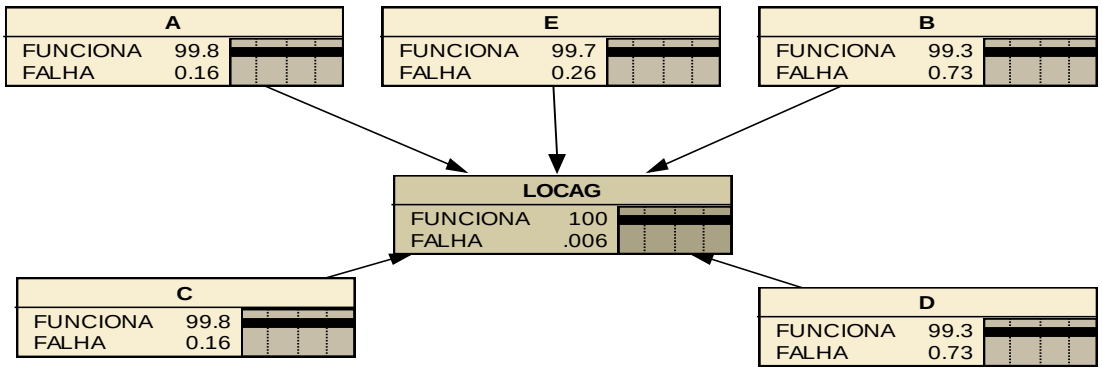
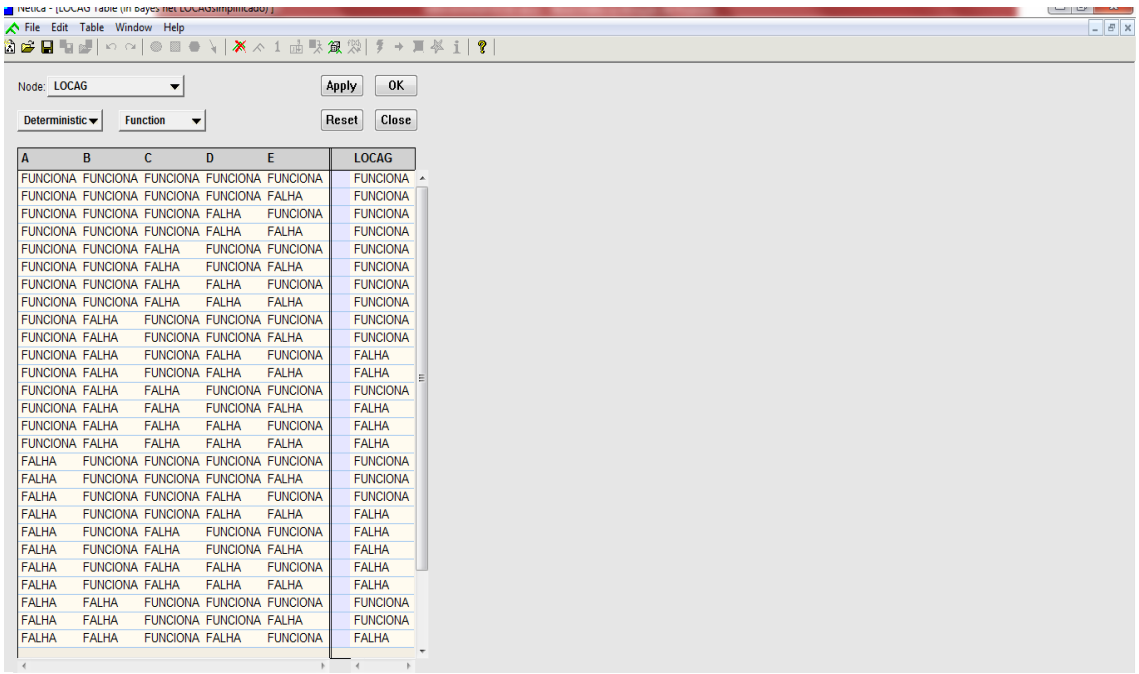


Figura 4.2 – Rede bayesiana para o sistema ponte

Tabela 4.1 – Tabela de Probabilidade Condicional do LOCAG



A	B	C	D	E	LOCAG
FUNCIONA	FUNCIONA	FUNCIONA	FUNCIONA	FUNCIONA	FUNCIONA
FUNCIONA	FUNCIONA	FUNCIONA	FUNCIONA	FALHA	FUNCIONA
FUNCIONA	FUNCIONA	FUNCIONA	FALHA	FUNCIONA	FUNCIONA
FUNCIONA	FUNCIONA	FUNCIONA	FALHA	FALHA	FUNCIONA
FUNCIONA	FUNCIONA	FALHA	FUNCIONA	FUNCIONA	FUNCIONA
FUNCIONA	FUNCIONA	FALHA	FUNCIONA	FALHA	FUNCIONA
FUNCIONA	FUNCIONA	FALHA	FALHA	FUNCIONA	FUNCIONA
FUNCIONA	FUNCIONA	FALHA	FALHA	FALHA	FUNCIONA
FUNCIONA	FALHA	FUNCIONA	FUNCIONA	FUNCIONA	FUNCIONA
FUNCIONA	FALHA	FUNCIONA	FUNCIONA	FALHA	FUNCIONA
FUNCIONA	FALHA	FUNCIONA	FALHA	FUNCIONA	FALHA
FUNCIONA	FALHA	FUNCIONA	FALHA	FALHA	FALHA
FUNCIONA	FALHA	FALHA	FUNCIONA	FUNCIONA	FUNCIONA
FUNCIONA	FALHA	FALHA	FUNCIONA	FALHA	FALHA
FUNCIONA	FALHA	FALHA	FALHA	FUNCIONA	FALHA
FUNCIONA	FALHA	FALHA	FALHA	FALHA	FALHA
FALHA	FUNCIONA	FUNCIONA	FUNCIONA	FUNCIONA	FUNCIONA
FALHA	FUNCIONA	FUNCIONA	FUNCIONA	FALHA	FUNCIONA
FALHA	FUNCIONA	FUNCIONA	FALHA	FUNCIONA	FUNCIONA
FALHA	FUNCIONA	FUNCIONA	FALHA	FALHA	FALHA
FALHA	FUNCIONA	FALHA	FUNCIONA	FUNCIONA	FALHA
FALHA	FUNCIONA	FALHA	FUNCIONA	FALHA	FALHA
FALHA	FUNCIONA	FALHA	FALHA	FUNCIONA	FALHA
FALHA	FUNCIONA	FALHA	FALHA	FALHA	FALHA
FALHA	FALHA	FUNCIONA	FUNCIONA	FUNCIONA	FUNCIONA
FALHA	FALHA	FUNCIONA	FUNCIONA	FALHA	FUNCIONA
FALHA	FALHA	FUNCIONA	FALHA	FUNCIONA	FALHA

Neste trabalho, o sistema ponte mostrado de forma simplificada na Figura 4.1 foi usado, porém, para que se chegasse aos valores de confiabilidade dos nós mostrados na Figura 4.2, o sistema usado como base foi o LPIS que é mostrado na Figura 4.3 e cujos possíveis modos de falha, bem como suas indisponibilidades são apresentados no Apêndice A. Ou seja, cada nó representa a confiabilidade que foi obtida a partir de uma rede bem maior levando em consideração as possíveis falhas associadas às várias válvulas e bombas pertencentes ao LPIS.

Os dados de entrada $\tilde{Q}$ (mediana) e f (fator de erro) são fornecidos em (FRUTUOSO E MELO, 1981). Para o cálculo da média foi utilizada a fórmula $\bar{Q} = \tilde{Q}.exp\left\{\frac{1}{2}\left[\frac{ln(f)}{1,645}\right]^2\right\}$, (KUMAMOTO E HENLEY, 1996), pois as incertezas são representadas por uma distribuição lognormal, ela será introduzida como as indisponibilidades dos nós da RB e da AF.

Deste modo, usando os dados calculados na Apêndice A, obtém-se a RB da Figura 4.4, que foi adaptada para ser vista como um sistema ponte usando supercomponentes e criando assim os nós A, B, C, D e E representados na Tabela 4.2.

Tabela 4.2 - Nomenclatura de nós associados aos supercomponentes

Nome do Nó	Componentes
A	Válvulas 8957A, 8928 e 8809A
B	Válvulas FCV-626, 8724A, 8958A e 8812A Bomba de injeção número 1
C	Válvulas 8957B, 8930 e 8809B
D	Válvulas FCV-619, 8724B, 8958B e 8812B Bomba de injeção número 2
E	Válvulas 8807A e 8807B

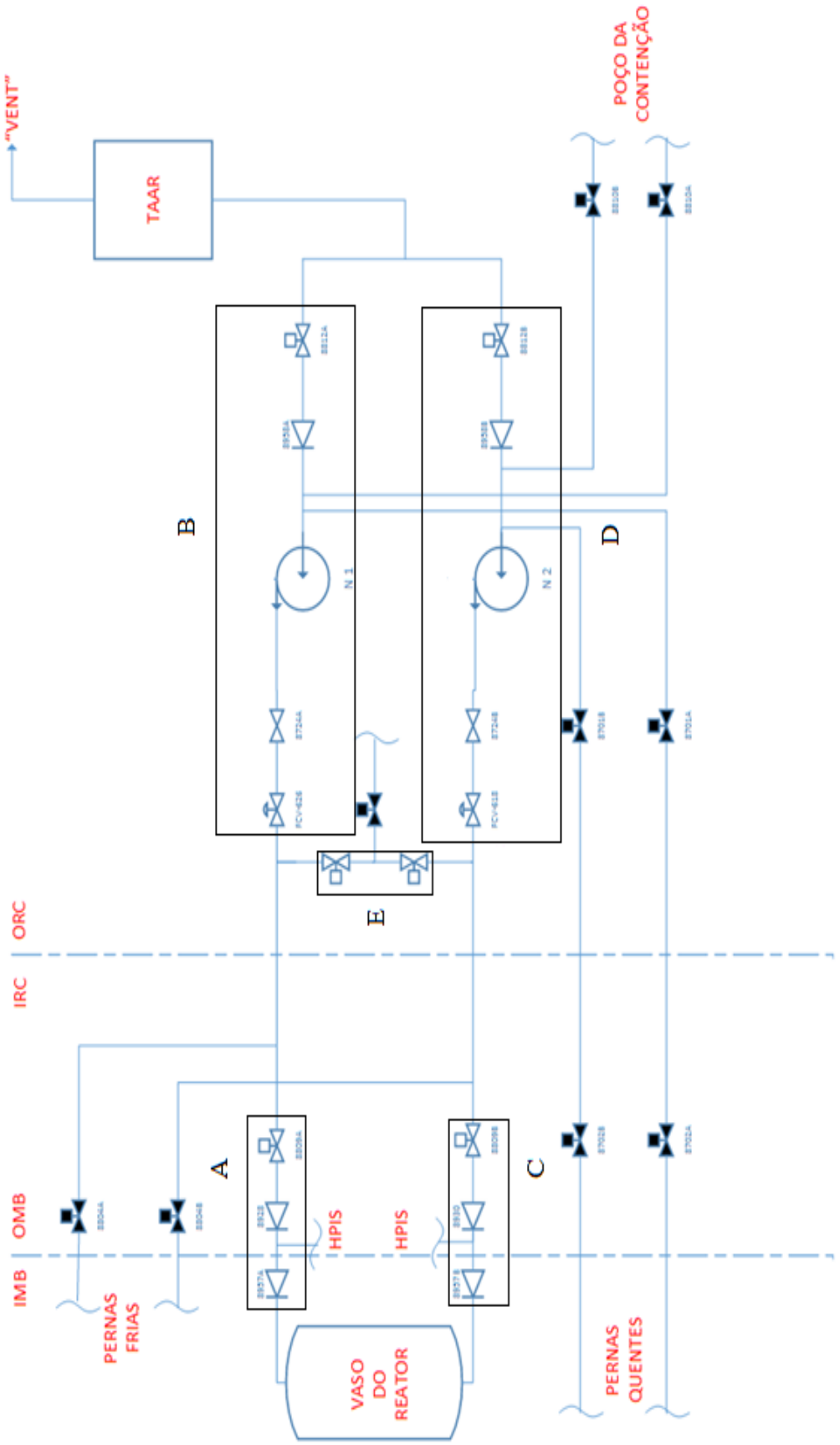


Figura 4.3 – LPIS modelado usando o sistema ponte

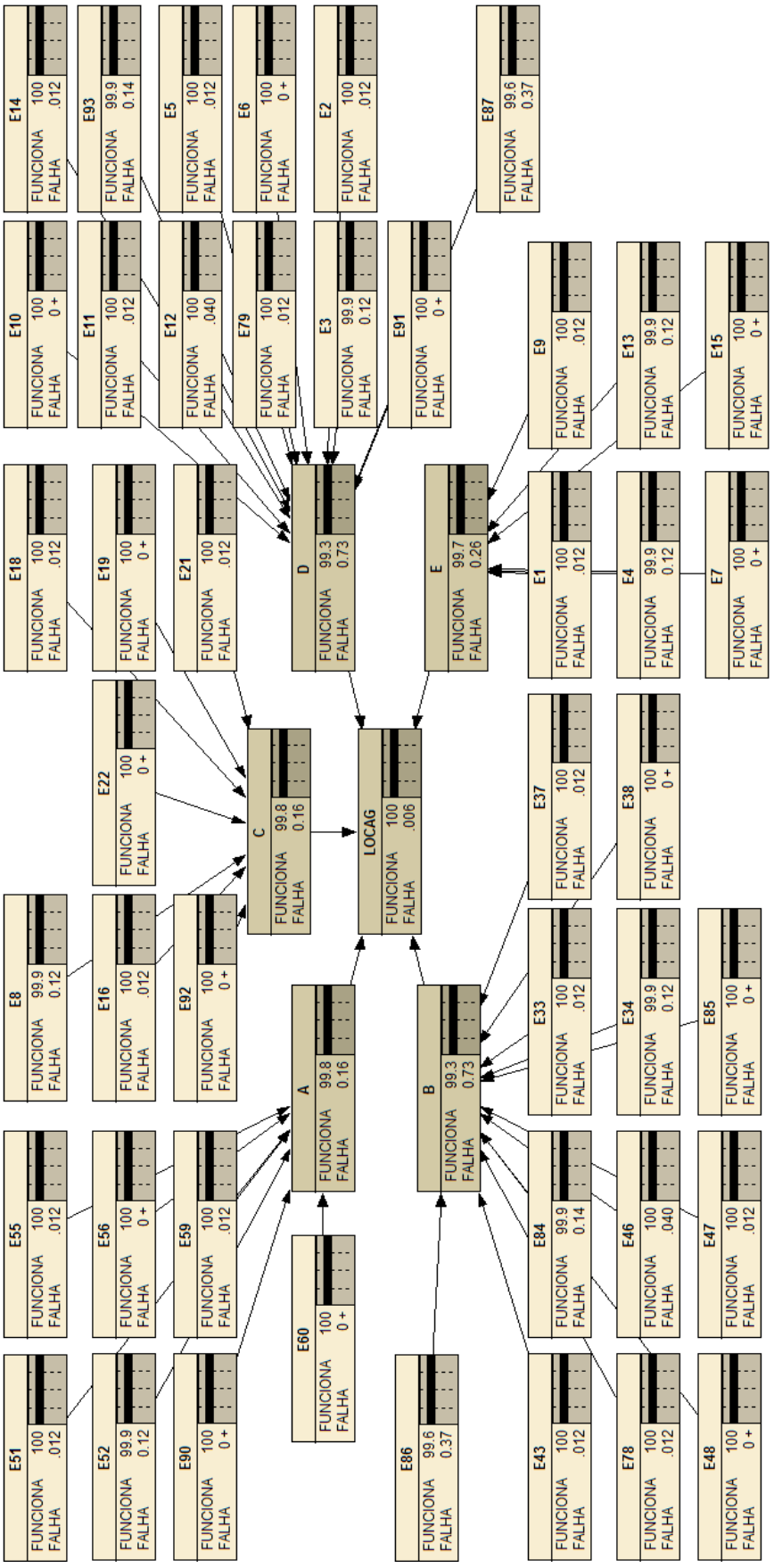


Figura 4.4 – LOCAG

Usando as mesmas falhas apresentados no Apêndice A para o modelo utilizado na Figura 4.4, foi feito o cálculo do LOCAG usando uma árvore de falhas com a ferramenta Excel. Para este cálculo foi usada a fórmula da decomposição pivotal $P(LOCAG) = P(A|E).P(E) + P(A|\bar{E}).P(\bar{E})$, (LEWIS, 1996), que significa que a probabilidade do sistema falhar após um LOCA Guilhotina é igual a probabilidade do sistema falhar dado que o nó E falhou multiplicado pela probabilidade de que o nó E falhe somado a probabilidade do sistema falhar dado que o nó E não falhou multiplicado pela probabilidade de que o nó E não falhe, o cálculo desta árvore está mostrado na Figura 4.5.

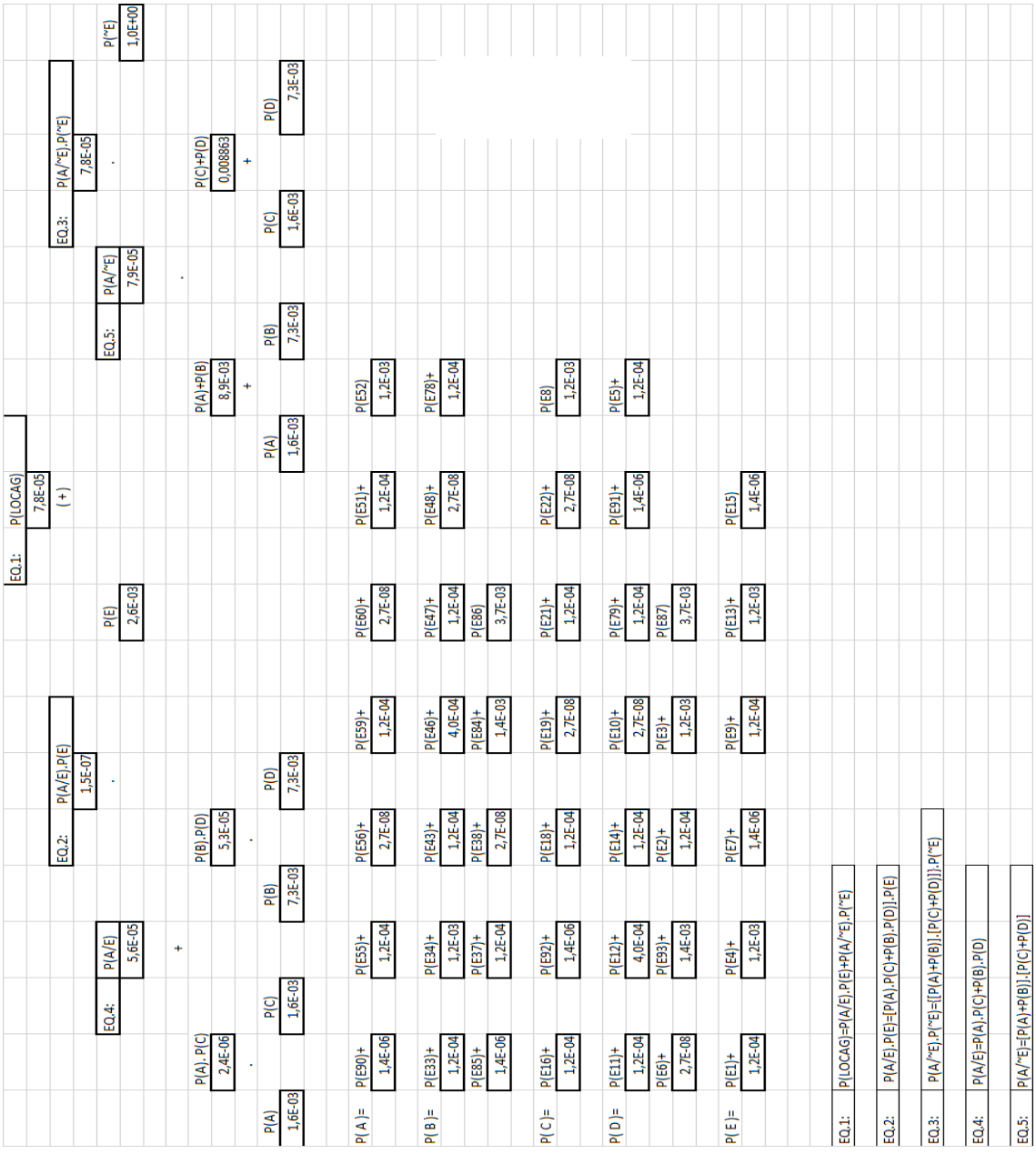


Figura 4.5 – Árvore de Falhas no Excel representando o LOCAG

As pesquisas de (ESTEVÃO, 2013) e (LEITE, 2014) já apontavam que os resultados obtidos para a indisponibilidade do LOCAG da RB e da AF seriam muito próximos, nesta análise a diferença entre eles foi de aproximadamente 2.10^{-5}, ou seja, as RB podem ser usadas e adaptadas de tal forma, que resultados equiparados aos das análises feitas por AF sejam obtidos.

4.2 Falha de causa comum

Comumente, considera-se que eventos similares envolvendo itens similares ou idênticos possuem a mesma probabilidade de ocorrência. Tal consideração é referenciada na literatura como princípio da simetria, (MARTINS, 2013).

Para o caso da FCC considerada para o sistema da Figura 4.6, as bombas B1 e B2 são dois componentes ativos e em paralelo que compõem o sistema, consideraremos que a FCC ocorre nestas bombas. No estudo em questão, considerou-se que as taxas de falha são iguais.

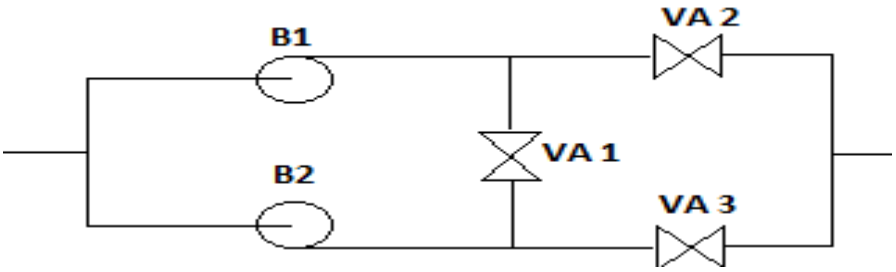


Figura 4.6 – Ponte contendo bombas e válvulas (LEITE, 2014)

O modelo mostrado na Figura 4.7 fez o cálculo da confiabilidade levando em consideração que o sistema possui componentes sujeitos a falhas que afetam todos os componentes e adicionalmente falhas independentes para cada um dos componentes, (LEITE, 2014).

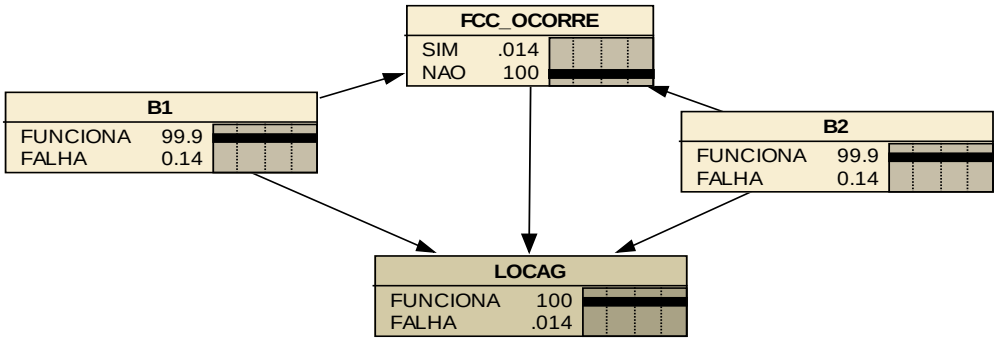


Figura 4.7 – Rede bayesiana para dois componentes em paralelo ativo levando-se em conta uma FCC

A TPC do nó "FCC_OCORRE" admite que a rede leve em conta uma FCC para o cálculo da confiabilidade.

Com a motivação de mostrar a eficácia da modelagem através de RB para o cálculo da confiabilidade de um sistema, serão feitas algumas simulações para variados valores de β e serão observadas as mudanças dos resultados na confiabilidade do LOCAG considerando como base o sistema de remoção de calor residual de Angra I.

Nessas simulações, é considerado que as bombas possuem taxa de falha independente e taxa de falha de causa comum. Como é possível modelar com RB um sistema de componentes em ponte e a FCC entre componentes, torna-se viável unir esses dois raciocínios para a ilustração de algumas RB no estudo apresentado.

Montada a RB, as TPC são preenchidas com as confiabilidades dos componentes e com as chances de ocorrerem FCC. Ao realizar esses passos, é possível compilar a RB, obtendo assim o resultado da confiabilidade do sistema para cada caso analisado.

A Figura 4.8 apresenta a rede completa, onde o valor assumido para β será de 10%, como considerando β igual a 15%, β igual a 20% e β igual a 40%, a rede permanece a mesma e os único nós que mudam são os "FCC_OCORRE" e "LOCAG" então não houve necessidade de repetição das imagens da rede para que fosse feita e mostrada uma inicial análise de sensibilidade que é apresentada na Figura 4.9. Estes valores serão assumidos pois na década de 80 eles eram considerados neste tipo de estudo. Atualmente, o valor médio usado para β no ambiente nuclear é de 0,1, o que mostra um avanço em termos de minimização da influência das falhas de causa comum no sistema.

Os valores usados na TPC do nó "FCC_OCORRE" são calculados abaixo.

$$\text{Caso } \beta = 10\% \rightarrow \lambda_C = \frac{0,1.0,0014}{1-0,0014} = 0,00014 \quad (6)$$

$$\text{Caso } \beta = 15\% \rightarrow \lambda_C = \frac{0,15.0,0014}{1-0,0014} = 0,00021 \quad (7)$$

$$\text{Caso } \beta = 20\% \rightarrow \lambda_C = \frac{0,2.0,0014}{1-0,0014} = 0,00028 \quad (8)$$

$$\text{Caso } \beta = 40\% \rightarrow \lambda_C = \frac{0,4.0,0014}{1-0,0014} = 0,00056 \quad (9)$$

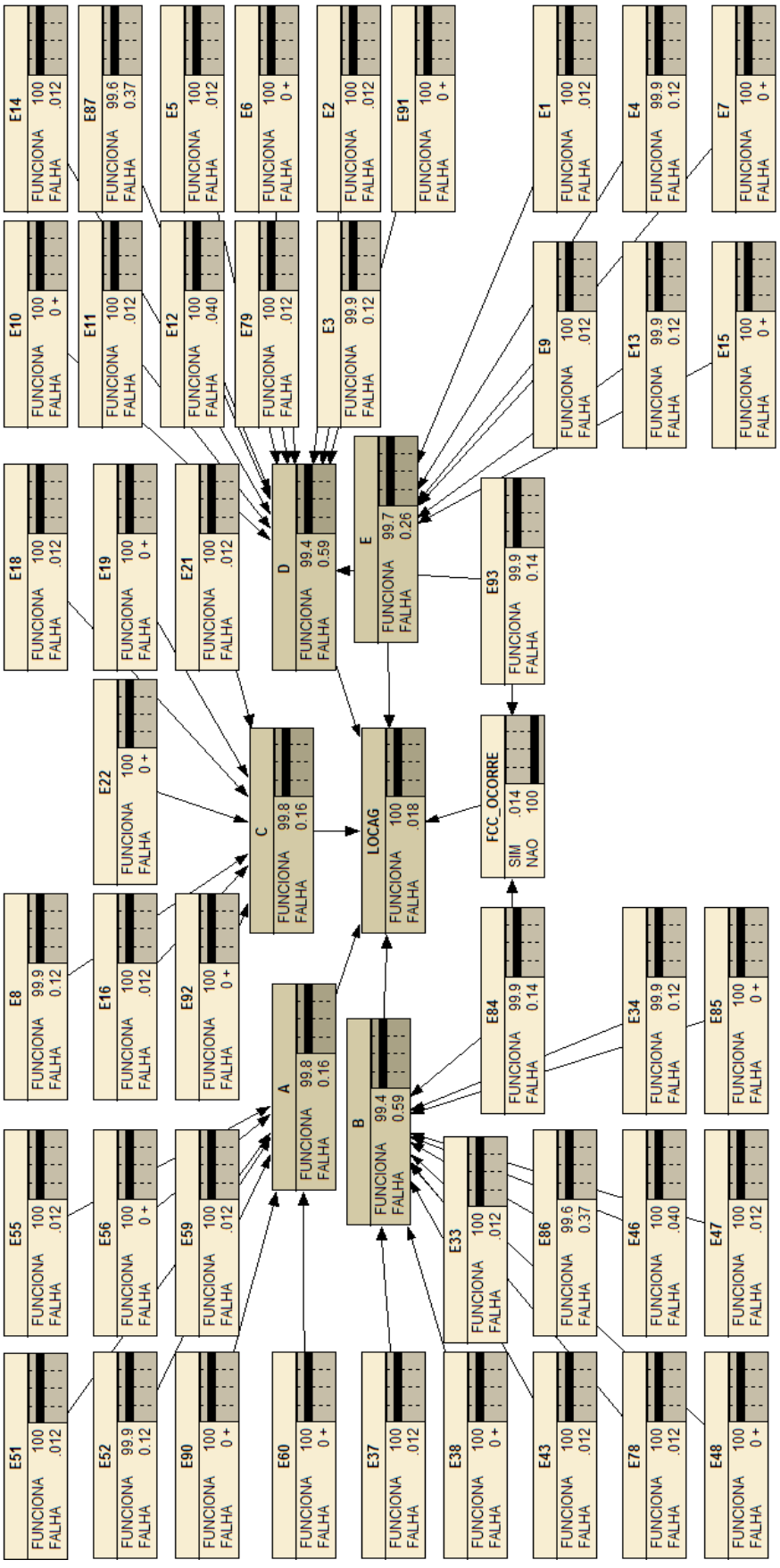


Figura 4.8 – Beta igual a 10%

O que é possível observar claramente é que todos os valores dos nós permanecem iguais, exceto os valores dos nós “FCC_OCORRE” e “LOCAG” que mudam conforme os valores de beta são variados, a variação dos valores do LOCAG em relação a variação dos betas é apresentada na Figura 4.9.

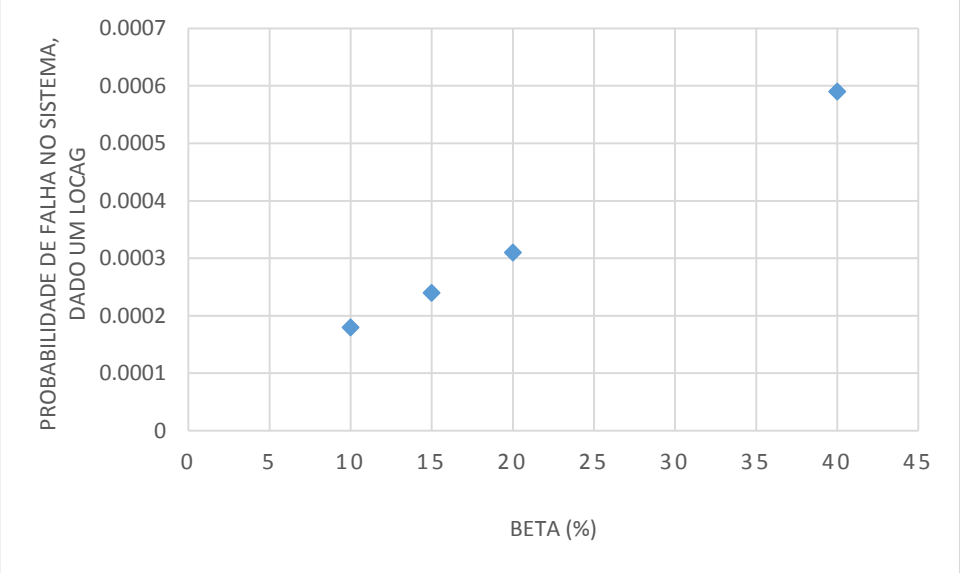


Figura 4.9 – Análise do impacto na indisponibilidade do sistema dada a variação de β.

Os resultados da análise mostram a flexibilidade das redes bayesianas para modelar eventos dependentes. Especificamente, foi necessário usar esse modelo para tratar a ligação das linhas redundantes do sistema de remoção de calor residual, o mesmo que pode ser feito através do método de decomposição pivotal e a falha de causa comum entre a s bombas de RHR.

A árvore de falhas que foi obtida a partir da simplificação do trabalho de (FRUTUOSO E MELO, 1981) é apresentada a seguir através das Figs. 4.10 a 4.18, como observação ressalta-se que o sinal “S” significa sinal de injeção de segurança.

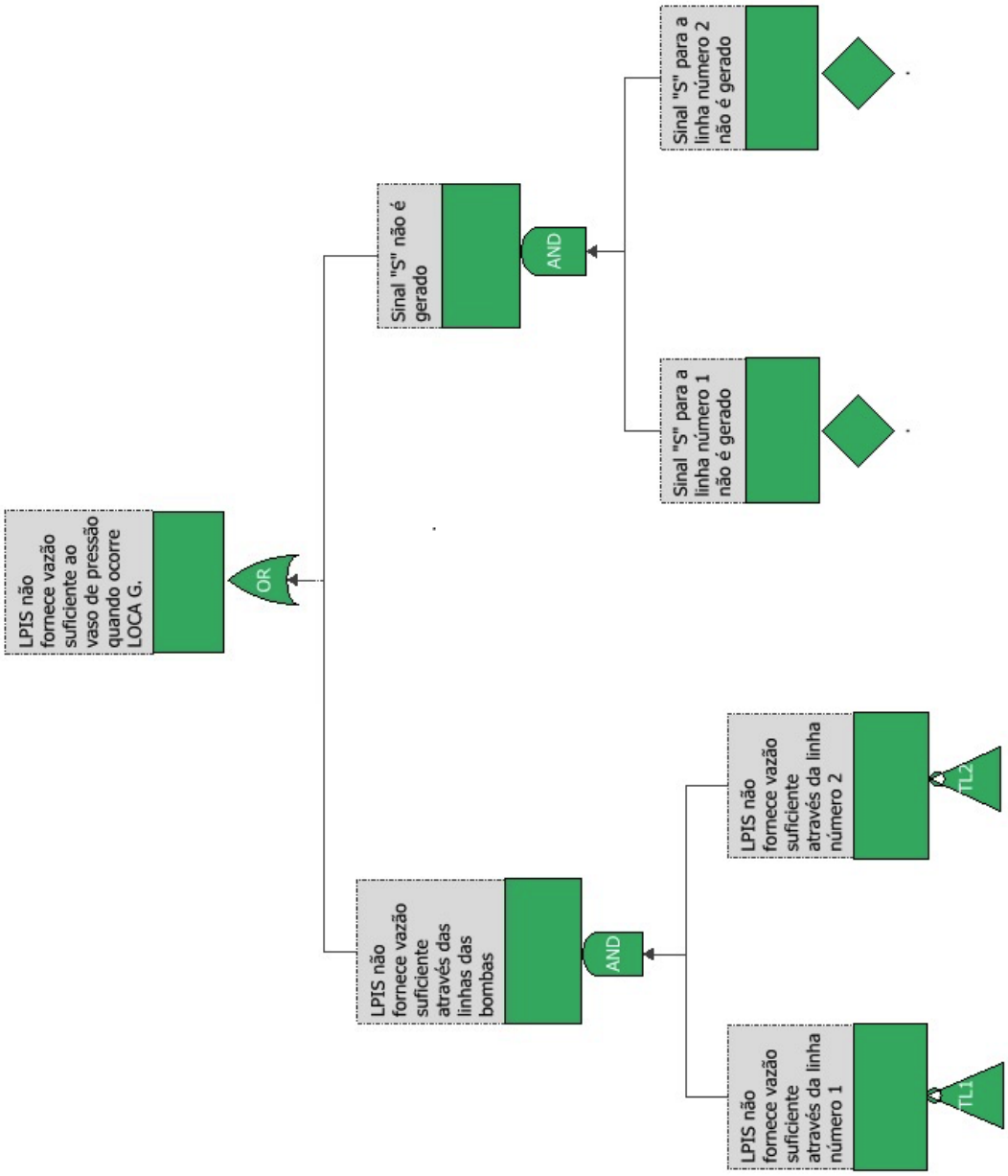


Figura 4.10 – Árvore de falhas simplificada para utilização na Rede Bayesiana

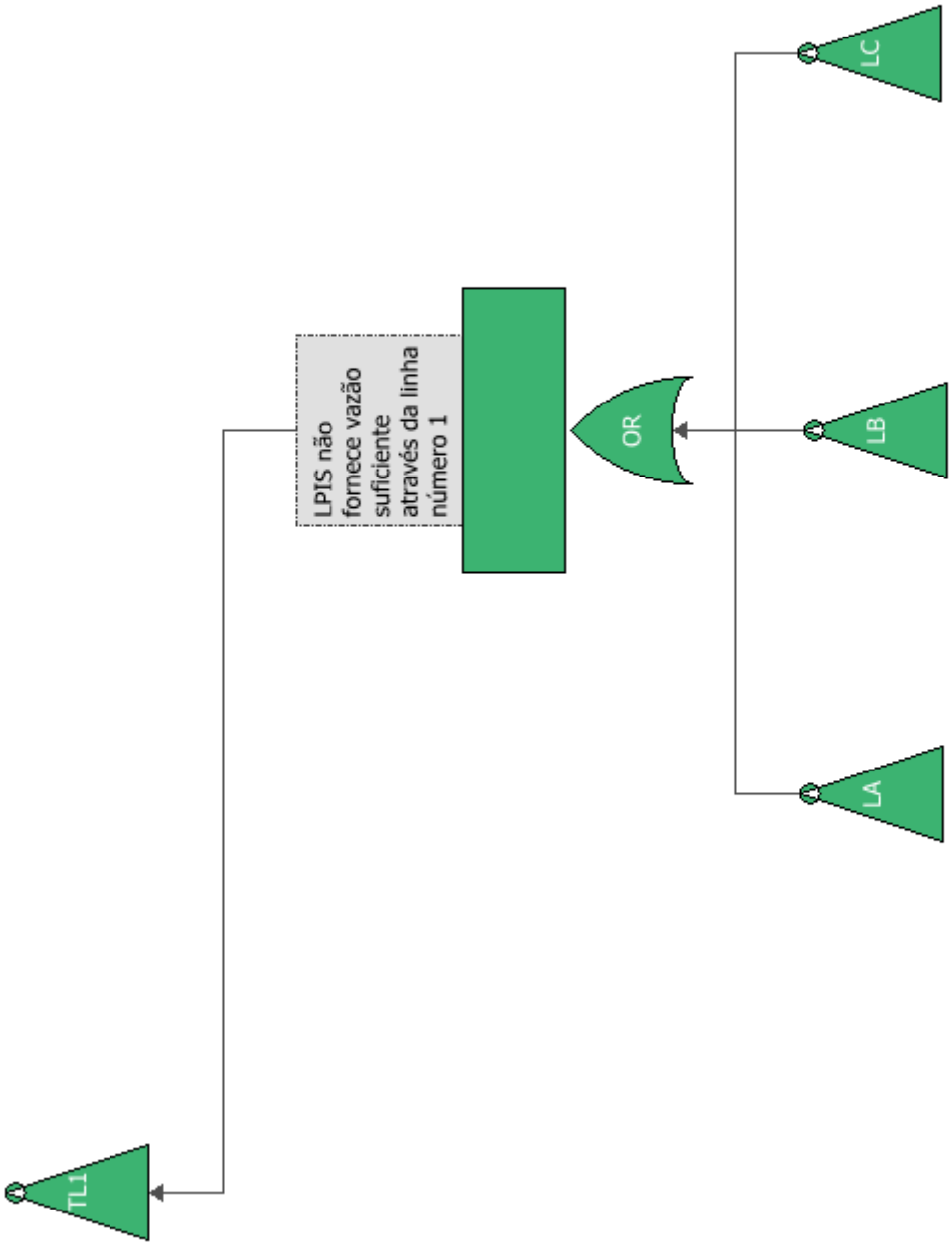


Figura 4.11 – Árvore de falhas simplificada para utilização na Rede Bayesiana (cont.)

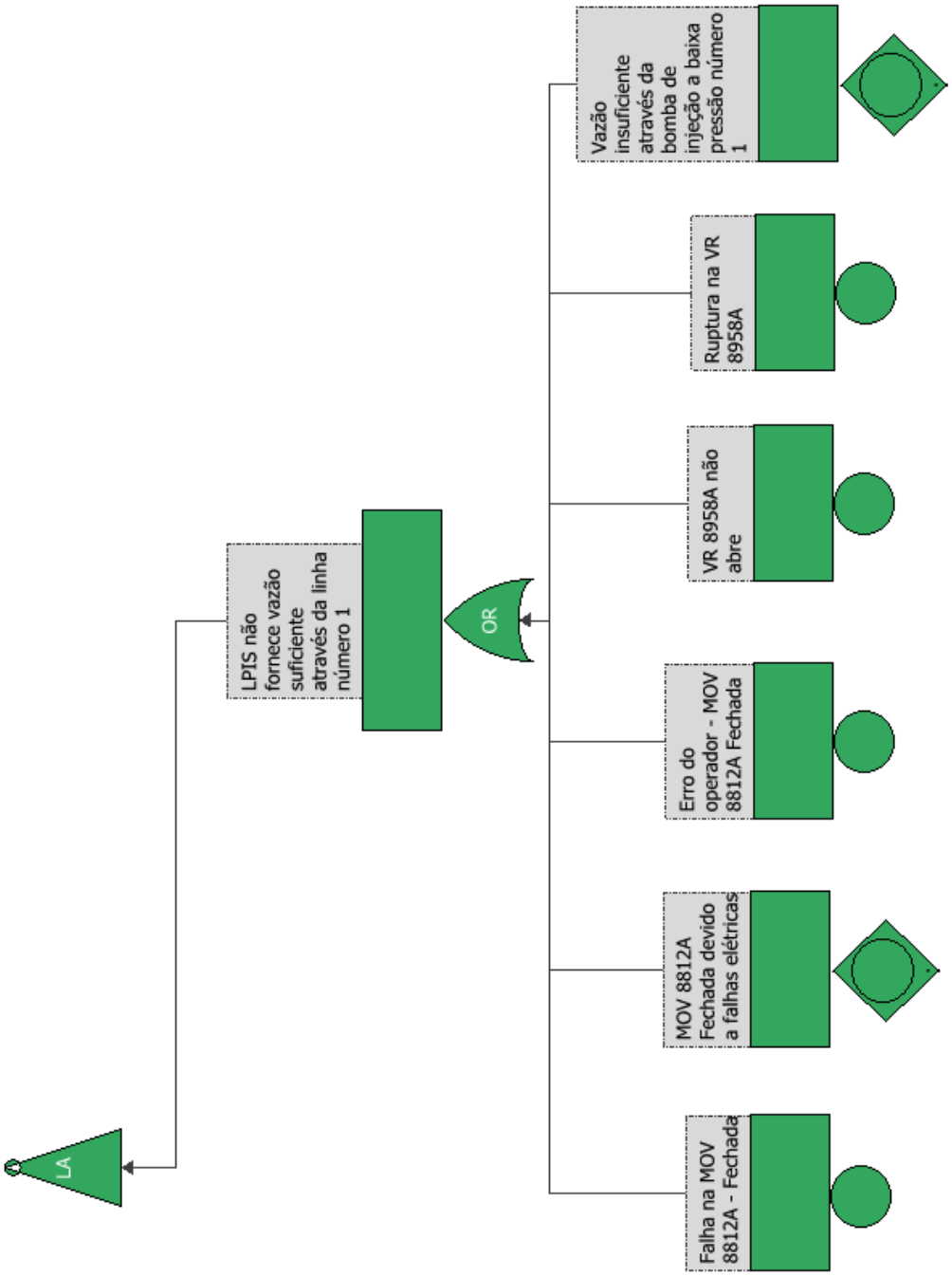


Figura 4.12 – Árvore de falhas simplificada para utilização na Rede Bayesiana (cont.)

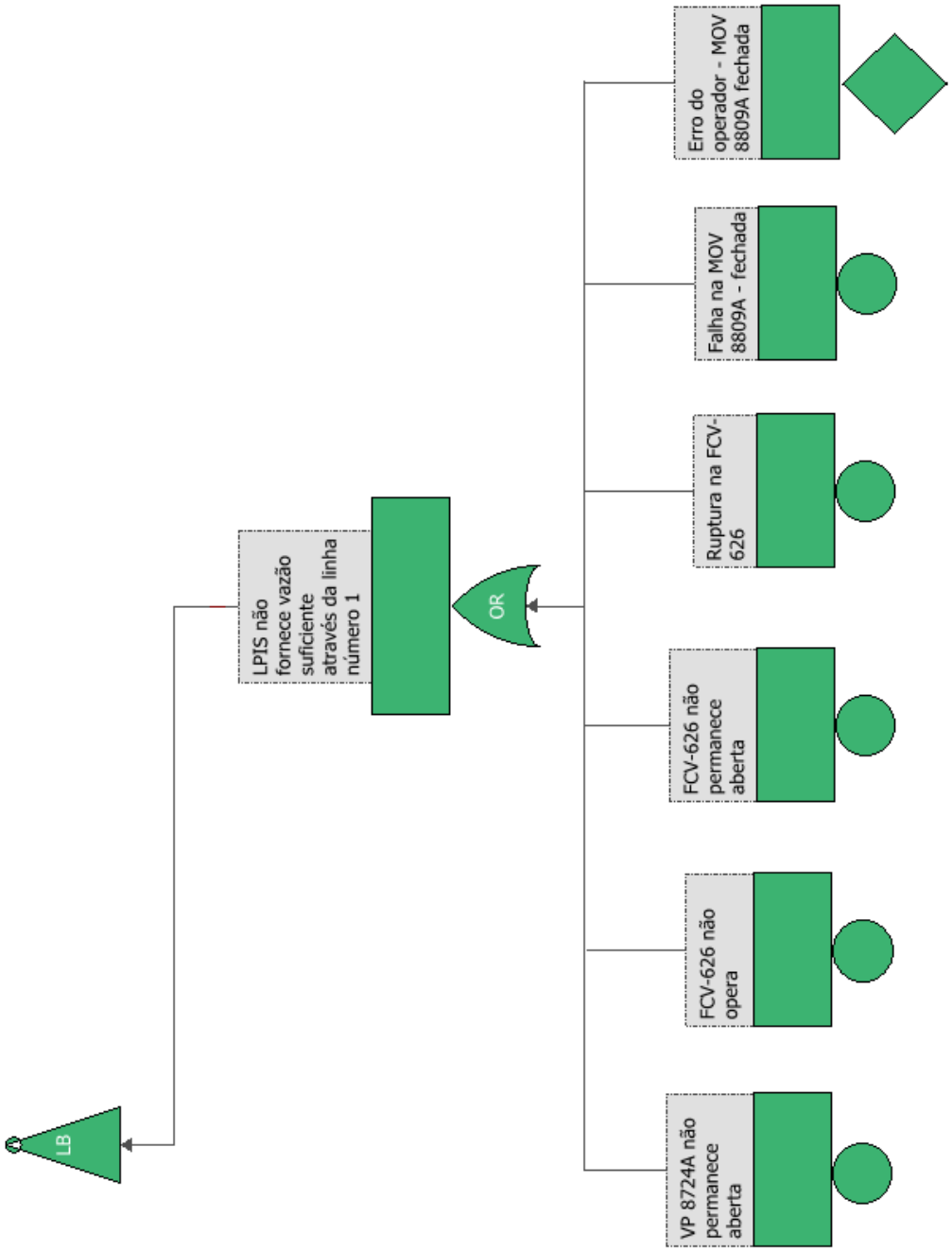


Figura 4.13 – Árvore de falhas simplificada para utilização na Rede Bayesiana (cont.)

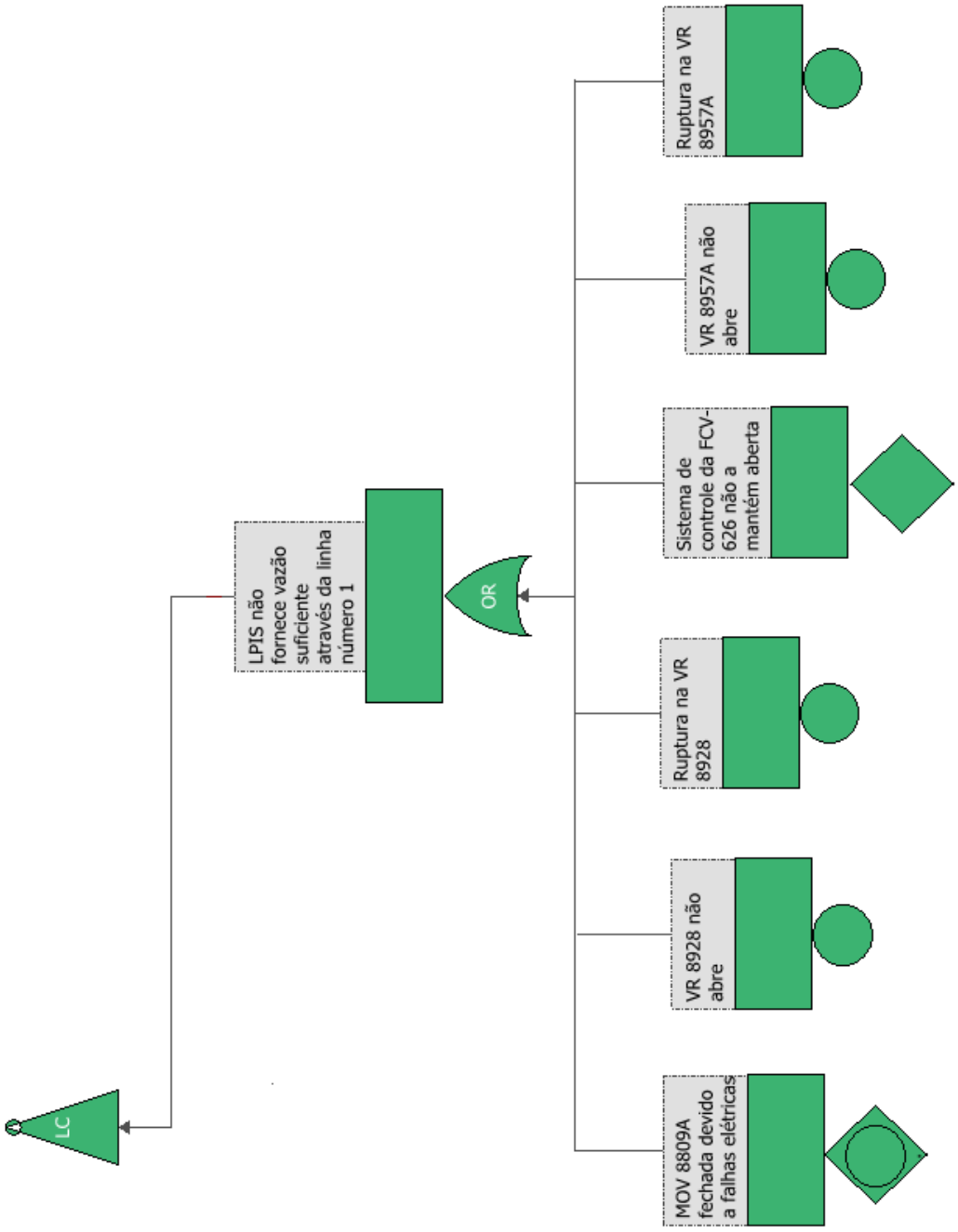


Figura 4.14 – Árvore de falhas simplificada para utilização na Rede Bayesiana (cont.)

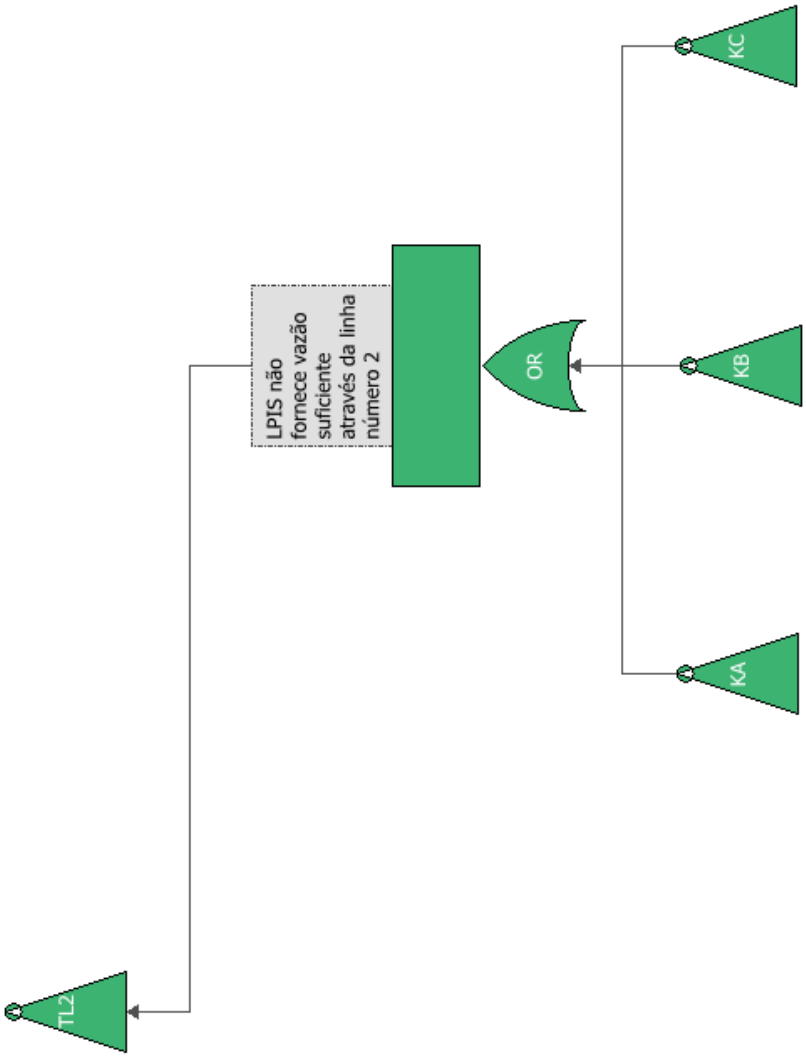


Figura 4.15 – Árvore de falhas simplificada para utilização na Rede Bayesiana (cont.)

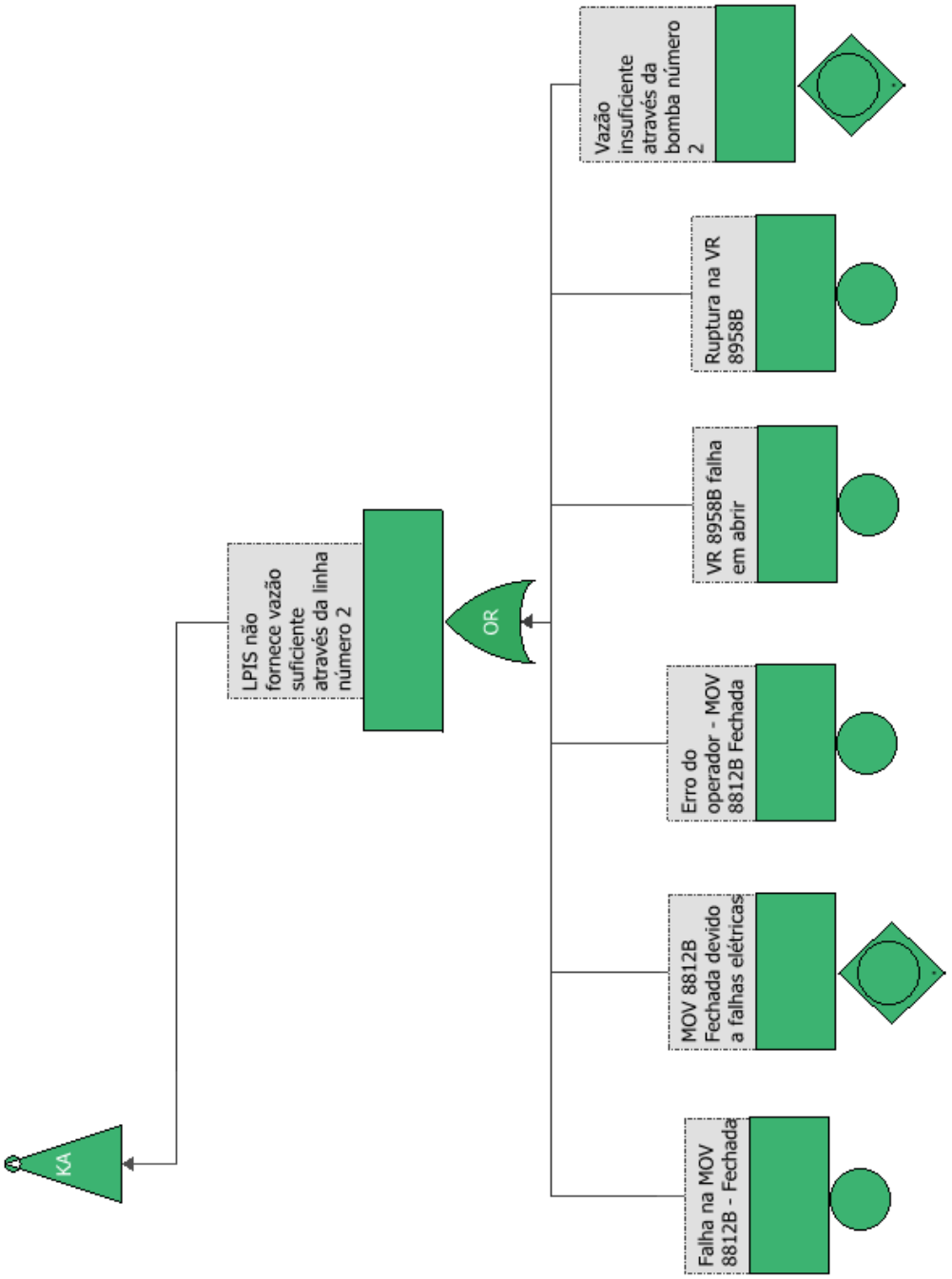


Figura 4.16 – Árvore de falhas simplificada para utilização na Rede Bayesiana (cont.)

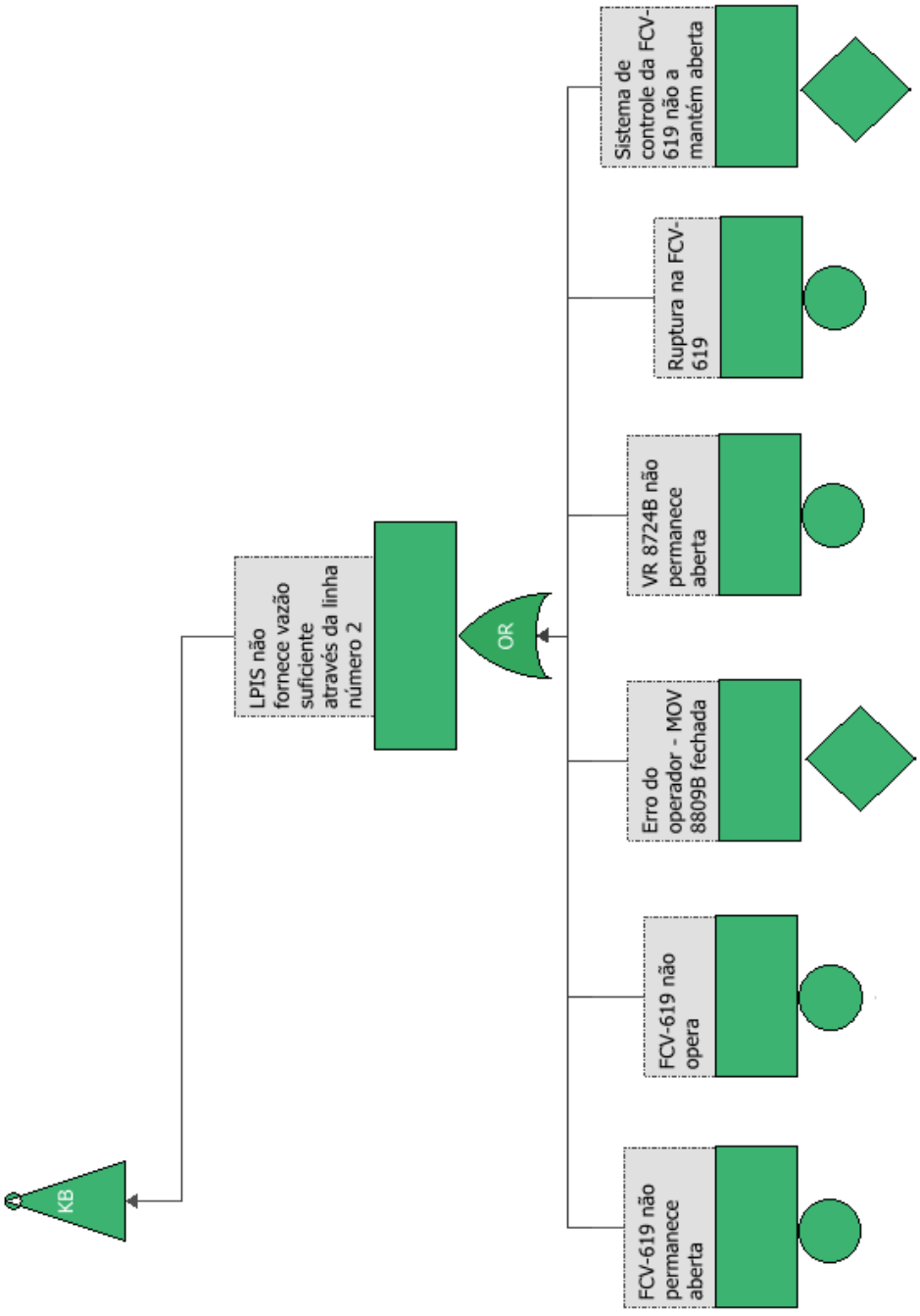


Figura 4.17 – Árvore de falhas simplificada para utilização na Rede Bayesiana (cont.)

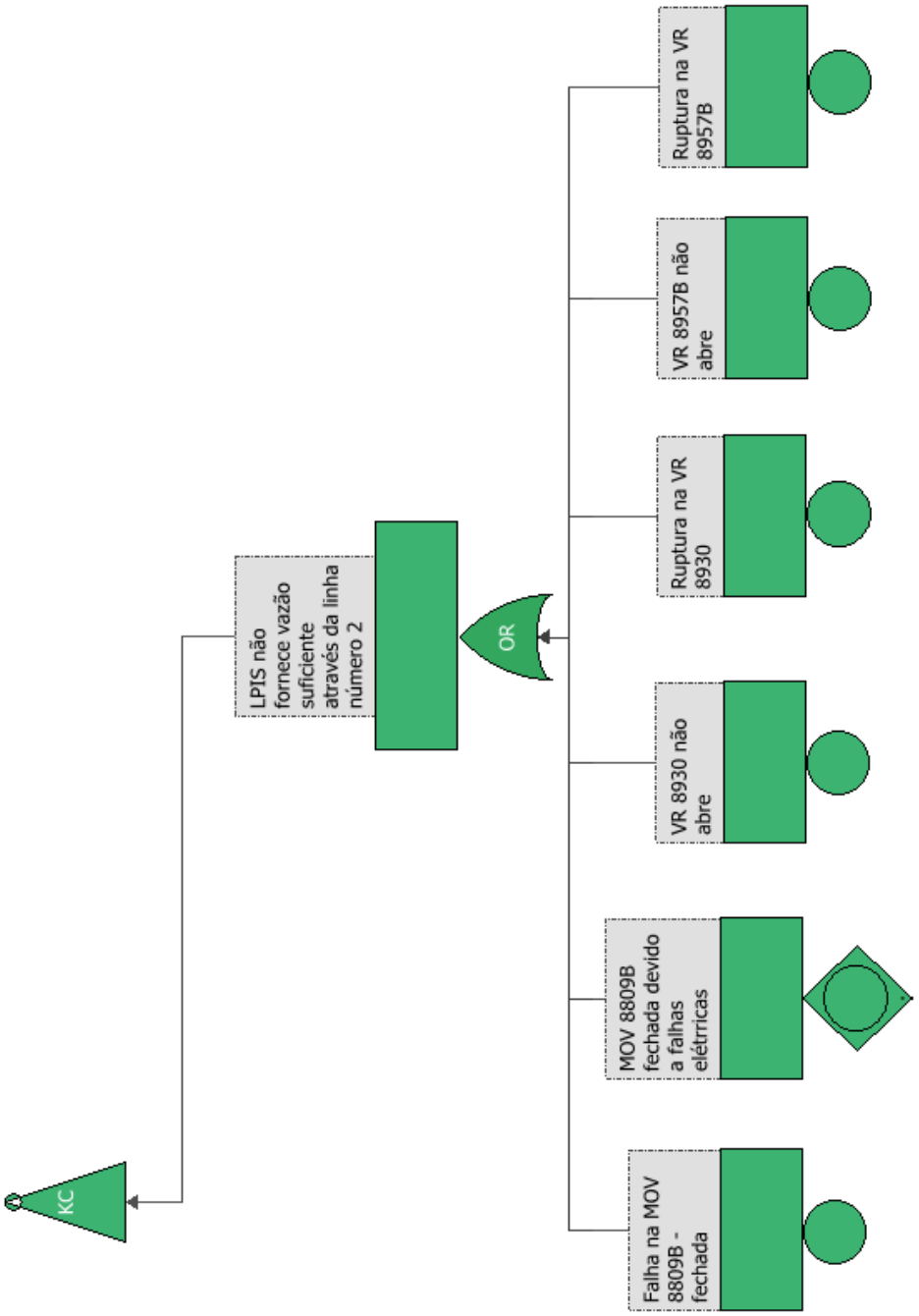


Figura 4.18 – Árvore de falhas simplificada para utilização na Rede Bayesiana (cont.)

Capítulo 5

Conclusões e Recomendações

Os modelos básicos e as técnicas normalmente usadas em estudos de confiabilidade foram discutidos e mostraram que, apesar de bem consolidados, os resultados dependem fundamentalmente da qualidade das informações referentes às taxas ou probabilidades de falhas que usualmente não são conhecidos ou passíveis de uma estimativa com a precisão desejada.

Assim, torna-se essencial o processo de atualização das informações consideradas no início do processo, à medida que novas informações sejam disponibilizadas ou evidências sejam constatadas durante a operação do sistema analisado, o que justifica a importância do procedimento descrito para a atualização de informações utilizadas em um primeiro momento.

A consideração da dependência entre falhas também é extremamente importante para a modelagem adequada da confiabilidade de sistemas e, apesar de modelos existentes já serem vistos como clássicos para a consideração de falhas de causa comum, a modelagem da dependência entre equipamentos ou componentes pode ser aperfeiçoada através do uso das redes bayesianas. As redes bayesianas são então vistas como uma técnica altamente promissora para estudos de confiabilidade e de risco por sua facilidade de manuseio e rapidez de resposta, itens essenciais para a análise de segurança.

Como uma das vantagens da conversão da AF ou diagrama de blocos em uma RB, tem-se a possibilidade de realização de inferências e análises do tipo *what if* ainda na fase de projeto ou quando uma nova evidência for obtida do sistema. Isto é, estendendo-se a análise de AF para a RB, a possibilidade de fazer simulações sobre diferentes estados do sistema identifica os elementos e os seus modos de falha mais prováveis.

Os resultados da análise mostram a flexibilidade das redes bayesianas para modelar eventos dependentes. Especificamente, foi necessário usar esse modelo para tratar a ligação das linhas redundantes do sistema de remoção de calor residual, o mesmo que pode ser feito através do método de decomposição pivotal e a falha de causa comum entre as bombas de RHR, porém de maneira muito mais ágil usando as RB.

Os resultados obtidos para a indisponibilidade do sistema de remoção de calor residual após um LOCA Guilhotina usando a RB e a AF foram muito próximos, é

importante ressaltar que nesta análise todos os eventos são considerados independentes e a diferença entre eles foi de aproximadamente 2.10^{-5}, ou seja, as RB podem ser usadas e adaptadas de tal forma, que resultados equiparados aos das análises feitas por AF sejam obtidos.

O que é possível observar claramente sobre o impacto das falhas de causa comum é que a confiabilidade do sistema diminui conforme os valores atribuídos a β aumentam, isto é, ao considerarmos que todos os eventos que influenciam a confiabilidade do sistema são independentes, obtemos a indisponibilidade de 6.10^{-5}. Porém, ao considerarmos a falha de causa comum entre as bombas, com $\beta = 10\%$, obtemos a indisponibilidade de 18.10^{-5}, ou seja, a confiabilidade do sistema diminuiu significativamente, o que mostra que ao não se considerar eventos dependentes estamos superestimando a confiabilidade do sistema.

Presumindo que haja interesse em melhorar a confiabilidade do SRCR, é recomendável considerar a melhoraria da confiabilidade do componente mais crítico; neste trabalho, este componente é representado pelos sinais de injeção de segurança para os trens 1 e 2, porém, em geral, há um custo associado. Sendo assim, a RB poderia ser usada para observar o impacto na confiabilidade do sistema em função da melhoria do componente ou subsistema crítico.

Apesar do uso das RB se mostrar promissor para aplicação em estudos de confiabilidade, risco e segurança, o uso das chamadas redes bayesianas híbridas (RBH), bem como a representação de dependências temporais ainda são tópicos em desenvolvimento e não estão disponíveis em boa parte dos softwares comerciais, (MARTINS, 2013).

A recomendação para que as RBH sejam melhor desenvolvidas e distribuídas em maior escala para os softwares comerciais é devido ao fato de que são elas que usam simultaneamente variáveis discretas, para representar os possíveis estados do sistema, e variáveis contínuas, para representar as condições de operação, porém, infelizmente, a inferência exata em redes híbridas só é possível para poucas e simples configurações de sistemas e densidades de probabilidades, citando como exemplo as distribuições exponenciais, limitando sua aplicação em estudos de confiabilidade e risco.

Referências Bibliográficas

AMYOTTE, P., KHAKZAD, N., KHAN F., 2011, *Safety Analysis in process facilities:comparison of fault tree and Bayesian network approaches.* Reliability Engineering and System Safety, v.96, pp. 925–932.

ANGRA 1, 2010, *Final Safety Analysis Report*, Rev. 35, Eletrobras Termonuclear, Rio de Janeiro, RJ, Brasil.

CHARNIAK, E., GOLDMAN, R., 1989, *A semantics for probabilistic quantifier-free first-worder languages with particular application to story understanding*. Proceedings of the Eleventh International Joint Conference on Artificial Intelligence, pp. 1074-1079.

CHARNIAK, E., 1991, *Bayesian Network without Tears.* IA Magazine, v.12 (4), pp. 50-63.

COTRELL W. B., 1973, *The ECCS Rule-Making Hearing*, Nuclear safety v.15 (1), pp. 30-55.

DIONIZIO D.P., 2014, *Tomada de decisão na manutenção de geradores diesel de emergência de centrais nucleares por redes bayesianas.* Dissertação de M. Sc., COPPE/UFRJ, Rio de Janeiro, RJ, Brasil.

ESTEVÃO L.B., 2013, *Estudo da indisponibilidade de um Sistema de segurança de uma central nuclear a água leve.* Dissertação de M. Sc., COPPE/UFRJ, Rio de Janeiro, RJ, Brasil.

FENTON N., NEIL M., 2000, *The Jury Observation Fallacy and the use of Bayesian networks to present probabilistic legal arguments.* Bulletin of the Institute of Mathematics and its Applications, v36, pp. 180–187.

FRUTUOSO E MELO, P.F., 1981, *Análise da confiabilidade dos sistemas ativos de injeção de segurança de Angra I.* Dissertação de M. Sc., COPPE/UFRJ, Rio de Janeiro, RJ, Brasil.

GLASSTONE S. & SESONSKE A., 1994, *Nuclear Reactor Engineering*, Chapman & Hall, New York.

GOMES E. C., 2011, *Análise de confiabilidade humana de procedimentos de radioterapia via redes bayesianas*. Tese de D. Sc., COPPE/UFRJ, Rio de Janeiro, RJ, Brasil.

KHAKZAD, N., KHAN F., AMYOTTE, P., 2013, *Risk-based design of process systems using discrete-time Bayesian networks.* Reliability Engineering and System Safety, 109, pp. 5–17.

KUMAMOTO, H., HENLEY, E.J., 1996, *Probabilistic Risk Assessment and Management for Engineers and Scientists*. IEEE Press, New York, p. 542.

LAMPIS M., ANDREWS J.D., 2008, *Bayesian Belief Networks for System Fault Diagnostics.* Quality and Reliability Engineering International, DOI: 10.1002/qre. 978.

LEE, C.J. E LEE, K.J., 2006, *Application of Bayesian network to the probabilistic risk assessment of nuclear waste disposal*, Reliability Engineering and System Safety, v.91, pp. 515-532.

LEITE, V. C., 2014, *Modelagem por redes bayesianas de eventos dependentes no cálculo de atributos de confiabilidade de sistemas de segurança de instalações nucleares*. Trabalho de Conclusão de Curso, Escola Politécnica, Universidade Federal do Rio de Janeiro, Rio de Janeiro, RJ, Brasil.

LEWIS, E.E., 1996, *Introduction to Reliability Engineering*, John Wiley & Sons, Inc., New York.

MARTINS, M., 2013, *Considerações sobre Análise de Confiabilidade e Risco*. Tese de Livre Docência, Escola Politécnica, Universidade de São Paulo, São Paulo.

MODARRES M., 2006, *Risk Analysis in Engineering*, Taylor & Francis, Boca Raton, Florida.

MOSLEH A., FLEMING N., PARRY W., *et al.*, 1988, *Procedures for treating Common Cause Failures in Safety and Reliability Studies*, v. 2, NUREG/CR- 4780.

MOSLEH A., 1991, *Common-cause failure: An analysis methodology and examples*. Reliability Engineering and System Safety, v. 34, pp. 249–292.

Norsys Software Corp. (2014) Netica tutorial disponível em < http://www.norsys.com/tutorials/netica/nt_toc_A.htm >

NRC, 1981. *Fault Tree Handbook*, NUREG-0492, U.S. Nuclear Regulatory Commission, Washington, D. C.

NRC, 1998. *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment,* NUREG/CR-5485, U.S. Nuclear Regulatory Commission, Washington, D. C.

SPIEGELHALTER, D., FRANKLIN, R., BULL, K., 1989, *Assessment, criticism and improvement of imprecise subjective probabilities for a medical expert system.* Proceedings of the Fifth Workshop on Uncertainty in Artificial Intelligence; pp. 335-342.

STASSOPOULOU, A., PETROU M., KITTLER, J., 1998, *Apliccation of the Network Bayesian in a GIS based decision making system*. International Journal of Geographical Information Science, v. 12, pp. 23-45.

U.S. Nuclear Regulatory Commission, October, 1975, *An Assessment of Accident Risks in U.S. Commercial Nuclear Plants,* WASH – 1400, (NUREG 75/014).

APÊNDICE A – Dados de entrada para LPIS

Número do evento	Nome do evento	Descrição	Indisponibilidade $\tilde{Q}$ (Mediana)	Fator de erro, f	$\bar{Q}$ (Média)
1	E1	Falha na MOV 8807A fechada	1,0E-04	3	1,2E-04
2	E2	Falha na MOV 8812B fechada	1,0E-04	3	1,2E-04
3	E3	Erro do operador MOV 8812B fechada	1,0E-03	3	1,2E-03
4	E4	Erro do operador MOV 8807A fechada	1,0E-03	3	1,2E-03
5	E5	VR8958B não abre	9,5E-05	3	1,2E-04
6	E6	Ruptura na VR8958B	1,0E-08	10	2,7E-08
7	E7	MOV 8807A fechada devido a falhas elétricas	7,7E-07	6	1,4E-06
8	E8	Erro do operador MOV8809B fechada	1,0E-03	3	1,2E-03
9	E9	Falha na MOV 8807B fechada	1,0E-04	3	1,2E-04
10	E10	Ruptura na FCV-619	1,0E-08	10	2,7E-08
11	E11	FCV-619 não permanece aberta	9,5E-05	3	1,2E-04
12	E12	FCV-619 não opera	3,2E-04	3	4,0E-04
13	E13	Erro do operador MOV 8807B fechada	1,0E-03	3	1,2E-03

14	E14	VP8724 não permanece aberta	9,5E-05	3	1,2E-04
15	E15	MOV 8807B fechada devido a falhas elétricas	7,7E-07	6	1,4E-06
16	E16	Falha na MOV 8809B fechada	1,0E-04	3	1,2E-04
17	E18	VR8930 não abre	9,5E-05	3	1,2E-04
18	E19	VR8930 ruptura	1,0E-08	10	2,7E-08
19	E21	VR8957B não abre	9,5E-05	3	1,2E-04
20	E22	VR8957B ruptura	1,0E-08	10	2,7E-08
21	E33	Falha na MOV8812A fechada	1,0E-04	3	1,2E-04
22	E34	Erro do operador MOV8812A fechada	1,0E-03	3	1,2E-03
23	E37	VR8958A não abre	9,5E-05	3	1,2E-04
24	E38	Ruptura na VR8958A	1,0E-08	10	2,7E-08
25	E43	VR8724 não permanece aberta	9,5E-05	3	1,2E-04
26	E46	FCV-626 não opera	3,2E-04	3	4,0E-04
27	E47	FCV-626 não permanece aberta	9,5E-05	3	1,2E-04
28	E48	FCV-626 ruptura	1,0E-08	10	2,7E-08
29	E51	Falha na MOV8809A fechada	1,0E-04	3	1,2E-04
30	E52	Erro do operador MOV8809A fechada	1,0E-03	3	1,2E-03
31	E55	VR8928 não abre	9,5E-05	3	1,2E-04

32	E56	VR8928 ruptura	1,0E-08	10	2,7E-08
33	E59	VR8957A não abre	9,5E-05	3	1,2E-04
34	E60	VR8957A ruptura	1,0E-08	10	2,7E-08
35	E78	Sistema de controle da FCV626 falha em mantê-la aberta	9,5E-05	3	1,2E-04
36	E79	Sistema de controle da FCV619 falha em mantê-la aberta	9,5E-05	3	1,2E-04
37	E84	Vazão insuficiente através da bomba número 1	1,1E-03	3	1,4E-03
38	E85	MOV8812A fechada devido a falhas elétricas	7,7E-07	6	1,4E-06
39	E86	Sinal “S” para o trem número 1 não é gerado	3,4E-03	2	3,7E-03
40	E87	Sinal “S” para o trem número 2 não é gerado	3,4E-03	2	3,7E-03
41	E90	MOV8809A fechada devido a falhas elétricas	7,7E-07	6	1,4E-06
42	E91	MOV8812B fechada devido a falhas elétricas	7,7E-07	6	1,4E-06
43	E92	MOV8809B fechada devido a falhas elétricas	7,7E-07	6	1,4E-06
44	E93	Vazão insuficiente através da bomba número 2	1,1E-03	3	1,4E-03