Universidade Federal
do Rio de Janeiro
Escola Politécnica

MÓDULOS DE DIAGNÓSTICO DO SISTEMA INTELIGENTE DE SUPORTE AO DIAGNÓSTICO DE ANGRA I

João Pedro da Silveira Câmara Augusto

Projeto de Graduação apresentado ao Curso de Engenharia Nuclear da Escola Politécnica, Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Engenheiro.

Orientador: Roberto Schirru

Rio de Janeiro

Fevereiro de 2017

MÓDULOS DE DIAGNÓSTICO DO SISTEMA INTELIGENTE DE SUPORTE AO DIAGNÓSTICO DE ANGRA I

João Pedro da Silveira Câmara Augusto

PROJETO DE GRADUAÇÃO SUBMETIDO AO CORPO DOCENTE DO CURSO DE ENGENHARIA NUCLEAR DA ESCOLA POLITÉCNICA DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE ENGENHEIRO NUCLEAR.

Examinado por:

Prof. Roberto Schirru, D. Sc.

Prof. Claudio Marcio de Nascimento Abreu Pereira, D. Sc.

Prof. Eduardo Gomes Dutra do Carmo, D. Sc.

RIO DE JANEIRO, RJ - BRASIL
FEVEREIRO DE 2017

Augusto, João Pedro da S. C.

Módulos de Diagnóstico do Sistema de Suporte ao Diagnóstico de Angra I / João Pedro da S. C. Augusto - Rio de Janeiro: UFRJ/ ESCOLA POLITÉCNICA, 2017.

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

Orientador: Roberto Schirru

Projeto de Graduação – UFRJ/ POLI/ Engenharia Nuclear, 2017.

Referências Bibliográficas: p. 46-48.

1. Inteligência Artificial. 2. Sistemas de Diagnóstico. 3. Sistema Especialista. I. Schirru, Roberto. II. Universidade Federal do Rio de Janeiro, Escola Politécnica, Curso de Engenharia Nuclear. III. Módulos de Diagnóstico do Sistema de Suporte ao Diagnóstico de Angra I

AGRADECIMENTO

Agradeço principalmente ao professor, orientador e amigo Roberto Schirru a quem eu devo grande parte de minha formação profissional, acadêmica e pessoal, por todas as oportunidades e influências positivas que me moldaram entre tantas brincadeiras, conselhos e aulas.

Agradeço a todos os participantes do LMP por sempre estarem disponíveis a ajudar e por tornarem o laboratório um ótimo ambiente de trabalho e convívio.

Agradeço a todos meus amigos do curso de Engenharia Nuclear que tornaram os últimos cinco anos os melhores anos de minha vida. Agradeço em especial a fami*lh*a por almoçar duas vezes comigo. Agradeço aos meus amigos Diguin, Hugin, Carlin, Papaibson, Dodo e Dedé pelo companheirismo e por todas as experiências e momentos marcantes durante nossa formação.

Por fim, agradeço a minha família que sempre me apoiou e desejou o melhor para mim.

Resumo do Projeto de Graduação apresentado à Escola Politécnica/ UFRJ como parte dos requisitos necessários para a obtenção do grau de Engenheiro Nuclear.

MÓDULOS DE DIAGNÓSTICO DO SISTEMA INTELIGENTE DE SUPORTE AO DIAGNÓSTICO DE ANGRA I

João Pedro da Silveira Câmara Augusto

Fevereiro/2017

Orientador: Roberto Schirru

Curso: Engenharia Nuclear

Alarmes são fundamentais para atrair a atenção de operadores a problemas ou condições que requerem providências imediatas. Em Usinas Nucleares, complexos sistemas de segurança monitoram e avisam à sala de controle, muitas vezes pela ativação de alarmes, condições operacionais e fatores de segurança. Quando um desligamento de emergência ou transiente acontece, um único problema pode ocasionar o surgimento de uma avalanche de alarmes que acaba dificultando o diagnóstico da causa do problema na usina e da situação da usina. Nesse cenário, a diferença de tempo entre esses eventos é normalmente da ordem de milissegundos. Sistemas em tempo real de suporte ao diagnóstico podem processar a informação contida na avalanche, auxiliando no trabalho dentro da sala de controle. É apresentado aqui um sistema genérico em tempo real, baseado em inteligência artificial, de suporte ao diagnóstico da causa-raiz de desligamento da usina e de determinação da situação de emergência. O objetivo é dar suporte à sala de controle ao facilitar a identificação de causa-raiz por meio da análise da sequência de eventos e diminuir a carga de trabalho dos operadores ao monitorar e fazer a inferência lógica da situação de emergência da usina, sendo responsável por um rápida classificação do estado da usina em caso de eventos anormais.

Palavras-chave:Diagnóstico, Sistema Especialista, Inteligência Artificial, Engenharia de Fatores Humanos

Abstract of Undergraduate Project presented to POLI/UFRJ as a partial fulfillment of the requirements for the degree of Nuclear Engineer.

DIAGNOSTIC MODULES OF THE ANGRA I's INTELLIGENT DIAGNOSIS SUPPORT SYSTEM

João Pedro da Silveira Câmara Augusto

Fevereiro/2017

Advisor: Roberto Schirru

Course: Nuclear Engineering

Alarms are fundamental to focus the operator's attention on on-going problems or conditions that require immediate action. In nuclear power plants, complex safety systems monitor and warn the control room, most of the time by activating alarms, operational conditions or safety factors. When a emergency shutdown or transient occurs, a single problem can trigger an alarm avalanche that dificults the diagnosis of cause and the power plant emergency state. In these scenarios, the time lapse between alarms is usually measured in miliseconds. Real-time diagnosis support systems plays a major role by processing the information in the alarm avalanche, helping the control room to diagnose problems. This paper presents a real-time generic system, based on artificial intelligence, which aims to help the operators in diagnosing the shutdown root-cause and to determine the emergency situation level. The system's role is to support the control room by analysing the sequence of events before a shutdown, giving hints about what happened and to decrease the operator's workload by monitoring and doing the logic inference of the current plant emergency state, being responsible for a quick classification of the plant's emergency classification level.

Keywords:Diagnosis, Expert System, Artificial Inteligence, Human Factors Engineering

SIGLAS

UFRJ - Universidade Federal do Rio de Janeiro

CNEN - Comissão Nacional de Energia Nuclear

NEI - *Nuclear Energy Institute*

SCRAM - Desligamento de emergência por injeção de barras de controle

ATWS - *Antecipated Transient Without SCRAM*

SICA - Sistema Integrado de Computadores de Angra

SE - Sistema Especialista

BC - Base de Conhecimento

MI - Motor de Inferência

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

As usinas nucleares desempenham um papel importante no contexto de geração elétrica mundial. Dados coletados em maio de 2016 indicam que 30 países fazem uso de energia nuclear para geração elétrica, operando um total de 450 reatores de potência além de 60 novos reatores sendo construídos em 15 países [1]. A geração elétrica mundial é de aproximadamente 392 GWe, suprindo aproximadamente 11% [2] do mercado mundial de energia. A maior parcela de geração se encontra na América do Norte, especialmente nos Estados Unidos. Na Ásia, é representada principalmente pela China, país que apresenta maior número de novos reatores em construção, e pelo Japão. Por outro lado, países europeus, como França, Suíça, Suécia e Finlândia mostram dependência da energia nuclear maior que um quarto da capacidade energética do país. [3]

No Brasil, as usinas de Angra I e Angra II representam um total de 1.3% do balanço energético total do país, alimentando a rede elétrica brasileira com aproximadamente 2 GWe, com fator de capacidade próximo a 90% para ambas as usinas[4]. Além disso, o país possui uma terceira usina em construção, Angra III, cuja capacidade elétrica de projeto é de 1405 MWe e apresenta 58,4% das obras concluídas [5].

O fator segurança constitui-se o no principal foco de estudo na área nuclear. Desde a concepção da ideia de produção elétrica por usinas nucleares de potência, se conhece os perigos associados ao uso de radiação, seus efeitos na saúde humana e no meio ambiente. A construção de instalações nucleares deve obedecer a três objetivos de segurança nuclear [6]: o objetivo geral de segurança nuclear, o objetivo

de radioproteção e objetivos técnicos de segurança nuclear. Os objetivos gerais, que englobam a proteção de trabalhadores, da sociedade e do meio ambiente, se baseiam no estabelecimento e manutenção de níveis de defesa. Os objetivos de radioproteção visam garantir níveis aceitáveis de exposição à radiação para operação da instalação, garantir exposição mínima em caso de liberações acidentais e garantir o princípio ALARA - *as low as reasonably achievable* de radioproteção. Por último, os objetivos técnicos de segurança ditam que devem ser tomadas todas as medidas possíveis para prevenir acidentes em instalações e mitigar sua consequência, caso ocorra.

Com o intuito de garantir tais objetivos, é aplicado o conceito de defesa em profundidade, constituído por 5 níveis de defesa. O primeiro nível é a prevenção de operações anormais, que é garantida pelo projeto conservador da usina e construção civil, mecânica e operacional com materiais e componentes de alta confiabilidade. O segundo nível é o controle de operações anormais, constituído pelo sistema de detecção de parâmetros anormais e pelo sistema de controle da usina. O terceiro e quarto níveis se relacionam com o controle de acidentes, sendo o terceiro nível responsável pelo o controle de acidentes postulados na base de projeto e o quarto nível pelo controle de acidentes severos. Finalmente, o quinto nível de defesa é a mitigação de consequência em caso de acidente e liberação de material radioativo.

Acidentes anteriores como TMI - Three Mile Island e Chernobyl mostraram como é imprescindível a existência de uma cultura de segurança na indústria nuclear e como o fator humano pode se tornar uma causa de falha comum em cenários de acidentes severos. Nesse contexto, a engenharia de fatores humanos tem como objetivo facilitar a tomada de decisão dos operadores a auxiliar a tomada da consciência situacional da planta e de seus parâmetros críticos.

Usinas nucleares dependem de seus sistemas de monitoramento para gerar energia elétrica de forma segura. Por essa razão, tais sistemas são complexos e devem agregar informação sobre todas as variáveis cruciais para operação segura e seus processos correntes. Entretanto, a quantidade de informações existentes em um sistema de monitoramento dificulta o diagnóstico de eventos quando uma grande ca-

deia de alarmes é acionada, excedendo a capacidade cognitiva do operador humano. A tarefa de diagnóstico em tais cenários é um desafio real devido a capacidade limitada do cérebro humano de processar e visualizar informação em um curto período de tempo. Além disso, a condição física, psicológica e de estresse dos operadores pode ocasionar um diagnóstico errado do evento e consequente atuação que poderia agravar a situação da usina.

Durante a operação, um evento anormal ou acidente pode causar o desligamento do reator pelo sistema de controle para proteger a integridade física da usina, seja sem a queda de barra, no ATWS ou com queda de barra de segurança. Esse evento é conhecido como TRIP [1] e o religamento da usina depende do estudo desse evento e da determinação de sua causa-raíz, realizada através da elaboração de um relatório detalhado de evento significante, composto pela descrição temporal dos acontecimentos que precederam o desligamento do reator.

Um relatório de evento significante deve conter informações sobre: a condição da usina antes do evento anormal, explicitando seu modo de operação e potência no momento; descrição do evento e todos os procedimentos que estavam sendo atuados no momento do evento anormal; modo de descoberta do desligamento do reator, indicando posição de barras e alarmes que indicam desligamento; e por fim, investigação detalhada do evento incluindo todas as possíveis causas discutidas pelos profissionais responsáveis e a determinação final de uma causa-raiz.

Por outro lado, de forma concorrente, parâmetros físicos devem continuar sendo monitorados em tempo real para garantir a ciência do operador em caso de quebra de algum nível de defesa ou necessidade de tomada de ação por parte da sala de controle.

Dessa forma, buscando otimizar tomadas de decisões, sistemas de diagnóstico podem ser usados para dar suporte aos operadores na sala de controle. Esses sis-

[1] Trip é o nome dado ao desligamento de segurança do reator, seja por inserção de barras de segurança no caso do SCRAM ou pela injeção de boro no sistema primário no caso do ATWS.

temas são responsáveis por avaliar a condição de diversas variáveis, em tempo real, ao simular o comportamento de um operador que, em princípio, possui capacidade de processamento de grande quantidade de informações em pouco espaço de tempo e de forma acurada. A fim de reduzir o tempo necessário para tomada de decisão e erros induzidos pelo excesso de informação, os sistemas de diagnóstico devem aliar a capacidade de processamento de sinais lógicos e devem expor ao operador apenas a informação necessária em certo contexto.

O problema de diagnóstico e identificação de acidentes ou condições adversas em usinas nucleares é bem conhecido na literatura. Em geral, são aplicados sistemas especialistas devido ao caráter geral do algoritmo e sua capacidade de acomodar dados específicos de cada usina. Conhecimento gerais e de tais características são bem definidos pela experiência prática e formação teórica dos operadores de usina e servem como base de funcionamento do programa.

Alvarenga M. A., em sua tese de doutorado submetida à COPPE UFRJ [7], aplica três diferentes algoritmos no ramo de inteligência artificial para montar um sistema de diagnóstico de acidentes. A união de redes neuronais, algoritmos genéticos e lógica nebulosa se provou efetivo no diagnóstico de acidentes ao acertar todos os 16 acidentes simulados de um reator PWR com modelos determinísticos.

Salmon D. R., em sua dissertação de mestrado submetido à COPPE UFRJ [8], propõe um sistema especialista baseado em níveis progressivos de diagnóstico para identificação de acidentes em tempo real para usinas nuclear do tipo PWR. O sistema especialista monitora 64 parâmetros da usina, identificando operação anormal e fazendo diagnóstico do evento em quatro níveis progressivos de diagnóstico até que seja encontrado o tipo específico de acidente.

Medeiros [9] publicou que é possível fazer a discriminação de transientes pela aplicação de algoritmo de enxame. O algoritmo conhecido como enxame de partículas aloca centroides que definem classes de acidentes. Outros trabalhos buscam a classificação de acidentes por meio da aplicação de diferentes algoritmos de

otimização [10]. Atualmente, estuda-se a capacidade de sistemas de classificação otimizados responder "Não Sei", reduzindo a probabilidade de erro no diagnóstico [11].

O sistema de diagnóstico proposto no trabalho aqui apresentado é composto por dois módulos de diagnóstico distintos, que atuam como suporte ao segundo e quinto nível de segurança. O primeiro é o módulo de diagnóstico da condição de situação emergência que é responsável pelo monitoramento em tempo real de variáveis críticas para o funcionamento da usina e inferência lógica da situação de emergência da mesma, auxiliando a tomada de decisões em caso de atuação do plano de emergência. O segundo, o módulo de diagnóstico de desligamento que é responsável pelo suporte ao processo de determinação da causas-raíz de desligamento do reator, seja por falhas em componentes ou transientes.

O sistema, atualmente em operação na usina de Angra I, foi desenvolvido a partir de um contrato entre a Eletronuclear e o Laboratório de Monitoramento de Processos COPPE/UFRJ, em 2014, e fez o uso de projetos de pesquisa como base de desenvolvimento. O sistema faz uso de dois conhecimentos distintos para inferência do diagnóstico e seu funcionamento: a documentação de classificação de situação de emergência da usina de Angra I serve como guia para a classificação de situação de emergência da usina pelo sistema. Por outro lado, para o suporte ao diagnóstico de causa-raiz, aplica-se o conhecimento dos operadores da usina no processo de determinação baseado no histórico de TRIPs da usina. Todas as informações necessárias para o funcionamento do sistema vêm de duas fontes: sequência de eventos da usina de Angra I, aplicado no diagnóstico de desligamento e variáveis em tempo real do Sistema Integrado de Computadores de Angra I, para determinação da situação de emergência.

A documentação de classificação da situação de emergência é composta por um conjunto de regras, abordando áreas críticas de monitoramento da usina, como liberação de radionuclídeos, mal funcionamento de sistemas de segurança, quebra de barreiras físicas, integridade do combustível nuclear e outros que podem ocasionar liberação de material radioativo e causar danos ao meio interno e externo da usina.

Sendo assim, tais regras têm como objetivo classificar a situação da usina em cinco níveis de emergência que são responsáveis por determinar ações internas, externas ou evacuação da área. Os níveis de emergência classificados são: Condição Normal, Evento Não Usual, Alerta, Emergência de Área e Emergência Geral.

Como um sistema de diagnóstico busca mimetizar a habilidade de um operador de vasto conhecimento em identificar um cenário e suas causas, técnicas de inteligência artificial e representação de conhecimento são aplicadas. Especificamente, é utilizado um algoritmo de inteligência artificial conhecido como Sistema Especialista, que por meio da avaliação de uma base de conhecimento sobre o problema e dadas suas condições atuais, consegue encontrar o diagnóstico, nesta aplicação em tempo real, para o problema. Um Sistema Especialista é um algoritmo, no caso em questão, de diagnóstico que faz uso do conhecimento de especialistas, representado em sua base de conhecimento, e de um motor de inferência, para inferir uma conclusão relativa a um problema dentro de sua área de expertise.

Os módulos de diagnóstico do sistema foram desenvolvidos na linguagem Python 2.7, dada sua facilidade de trabalhar com conjuntos de regras e árvores lógicas de forma recursiva. Python é uma linguagem de código e distribuição livre, multi-plataforma, interpretada, de tipagem dinâmica e manejo de memória automático comumente utilizada no meio acadêmico devido a sua sintaxe simples e de rápido desenvolvimento [12]. Por fim, divide-se esse trabalho nos seguintes capítulos de forma a facilitar a abordagem do tema.

O Capítulo 2 fundamenta a teoria necessária para definição de sistemas de suporte ao operador. Neste capítulo se define a necessidade e o funcionamento de sistemas de monitoramento e alarme e como estes são atuados na sala de controle de uma usina nuclear. É abordado o tema de Inteligência Artificial, seu conceito básico de criação e história. Ainda dentro do contexto de Inteligência Artificial, é explicado a dinâmica de representação do conhecimento em regras, árvores lógicas e as metodologias utilizadas para o mesmo dentro da área de ciência da computação. Por fim, é fundamentado o que são sistemas especialistas, o objetivo de sua criação,

história e como o algoritmo é capaz de fazer um diagnóstico por meio da mimetização do trabalho de especialistas ao resolver um problema em sua área.

O Capítulo 3 é responsável por apresentar o problema ao leitor, especificando como o algoritmo utilizado se aplica aos problemas específicos para a usina nuclear de Angra I. Se apresenta, fundamenta e especifica o modo de representação das bases de conhecimento necessárias para o funcionamento do sistema de suporte. É abordado o documento de classificação de plano de emergência da usina de Angra I e como seu conhecimento é representado em formas de regras lógicas. Para o módulo de diagnóstico de causa-raiz de desligamento, é explicado como se estrutura a relação de alarmes presentes na sequência de eventos, precedente ao sinal de TRIP do reator. Posterior a fundamentação da base de conhecimento, o algoritmo de diagnóstico é detalhado e como é feita a inferência para cada caso, diferenciando a forma de funcionamento dos módulos de suporte e explicando seu funcionamento. Inicialmente é feita a introdução ao módulo de diagnóstico de TRIP, abordando o problema e o sistema especialista modificado aplicado ao problema e um exemplo de teste. A seguir, é abordado o módulo de diagnóstico de classificação de situação de emergência, introduzindo o funcionamento das regras lógicas que ditam tal classificação, o funcionamento do sistema especialista baseado em regras aplicado e o teste feito a um caso real.

O Capítulo 4 tem caráter expositivo de resultados e do sistema por completo. Nesse capítulo se mostra o sistema por completo, suas ferramentas e aplicação em tempo real na usina de Angra I.

O Capítulo 5 conclui o trabalho e enfoca sua importância como sistema de suporte ao operador no diagnóstico de problemas complexos e em curto período de tempo. Finalmente, são feitas sugestões de trabalhos futuros de ferramentas capazes de aprimorar a capacidade do sistema agir ao se alimentar com novas regras geradas.

Capítulo 2

Fundamentação Teórica

Esse capítulo aborda os algoritmos aplicados no trabalho. É introduzido e explicado a noção de monitoramento e alarmes em plantas de geração e sua importância no controle da usina. Posteriormente, se fundamenta o ramo no qual o presente trabalho se baseia que é a Inteligência Artificial, explicitando objetivos e tentativas de alcançá-la. Entra-se então no tema de representação do conhecimento, fundamental para o entendimento e funcionamento do algoritmo aplicado e por fim a explicação do algoritmo de Sistema Especialista em si.

2.1 Monitoramento e Alarmes

Usinas nucleares são compostas por diversos subsistemas responsáveis pelo controle de seus parâmetros e sua segurança. Esses sistemas interagem entre si de diversas formas e o conhecimento dessas interações entre sistemas é essencial para o projeto e operação da planta [13]. Por outro lado, nem sempre é possível manter o controle completo de todas essas interações, requisitando assim uma ação ativa da sala de controle da usina. Nesse contexto, sistemas de monitoramento e alarmes são essenciais para informar e alertar os operadores de possíveis desvios de operação e parâmetros de processo.

Um sistema de alarme é um elemento fundamental em qualquer sala de controle e interface entre o operador e a planta. Tradicionalmente, em usinas de controle analógico, o sistema era baseado em lâmpadas de indicação e avisos sonoros. Apesar de projeto analógico, a usina nuclear de Angra I atualmente apresenta computado-

res em sua sala de controle, apresentando então sistema híbrido de monitoramento. Usinas mais modernas, fazem o uso exclusivo de computadores para apresentar ao operador, de forma gráfica ou em texto, a lista de alarmes da usina.

Sistema de alarmes são sistemas que monitoram, agrupam, calculam e exibem variáveis e parâmetros a um operador. Todo sistema de alarme deve seguir quatro princípios fundamentais de funcionamento: utilidade, segurança, monitoramento de performance e investimento [14].

No aspecto de utilidade, os sistemas de alarme devem ser projetados para cumprir um objetivo específico dada certa necessidade e dentro da capacidade de resposta dos operadores. Isso significa que a informação exibida pelo sistema deve ser relevante ao operador no momento de sua exibição, indicar claramente o que significa e qual ação deve ser tomada e ser indicada de forma a não sobrecarregar a capacidade cognitiva dos operadores.

Um sistema de alarme deve contribuir de forma efetiva a segurança da usina, dos trabalhadores, sociedade e meio ambiente. Para isso, todos os equipamentos que apresentam necessidade de monitoramento devem ser devidamente identificados e todas as ações requeridas bem definidas e dentro dos protocolos de operação. Deve-se garantir a confiabilidade e performance do sistema de alarmes dada sua importância na segurança da usina. Para isso, é importante sua manutenção e identificação de falhas.

Por último, a criação e projeto de um sistema de alarmes deve seguir altos padrões de qualidade e evitar problemas operacionais que podem comprometer a segurança da usina. O desenvolvimento do sistema deve seguir uma metodologia bem estruturada onde todos os alarmes são justificados por razões de segurança, ambientais ou financeiras.

Em resumo, alarmes são sinais que devem ser reconhecidos pelo operador, seja por indicação visual ou sonora, por indicar uma condição anormal na usina. Alarmes

em geral indicam problemas que requerem ação ativa do operador já que podem significar que algum parâmetro se aproxima de um valor que poderia comprometer a segurança de um sistema ou subsistema. Devem obedecer a três princípios básicos:

- Todo alarme deve ter um propósito bem definido.
- Todo alarme deve ter uma resposta bem definida.
- Toda resposta deve ter uma quantidade adequada de tempo disponível para ser conduzida.

A figura 2.1 estrutura de forma macroscópica o funcionamento de um sistema de alarme. O sistema une respostas de sensores com fatores limitantes e os exibe ao operador de forma visual ou sonora. O operador, com capacidade de racionalização do estímulo sensorial proveniente do sistema, contextualiza e interpreta suas saídas e age por meio de comandos.

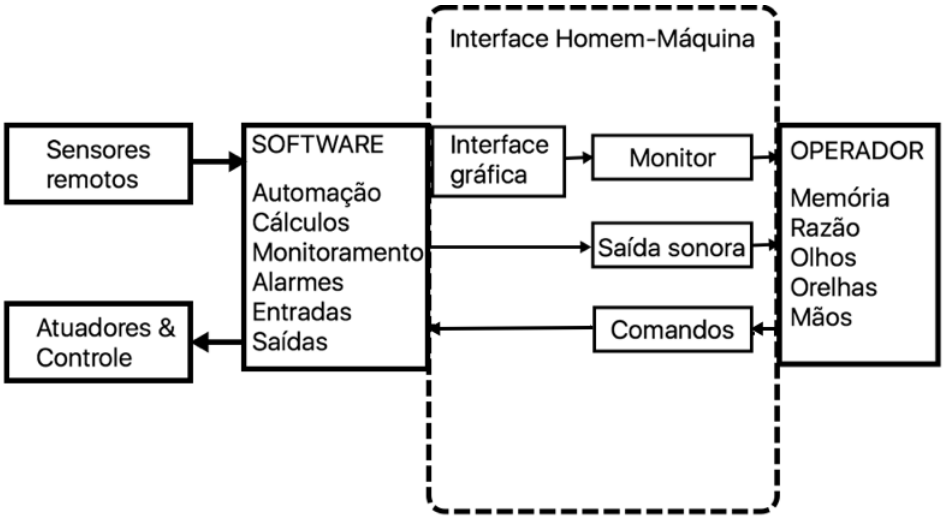

Figura 2.1: Diagrama de funcionamento de um sistema de alarmes.

A utilização de sistemas de monitoramento e alarme é aliada à necessidade de redução de riscos de uma instalação. O monitoramento de parâmetros da usina é uma das ferramentas aplicadas para reduzir os riscos para um nível tolerável. Em plantas industriais, principalmente usinas nucleares, diversos aspectos de construção e funcionamento são planejados para reduzir a probabilidade de condições anormais. Diversos níveis de proteção buscam tal redução, desde a escolha de componentes

mecânicos até o projeto conservador da planta e de parâmetros operacionais. Nessa conjuntura, o monitoramento de sistemas tem como objetivo controlar, limitar e proteger os sistemas de condições sub-ótimas ou que tragam risco à segurança física do sistema.

2.1.1 Sequência de Eventos

A sequência de eventos é o registro de eventos, como a ativação de alarmes, em conjunto com sua data de acontecimento. Essa ferramenta é amplamente utilizada por operadores ao tentar entender o motivo de um evento ou a causa de uma condição anormal na usina. Por meio da análise de tal registro, é possível inferir a causa-raiz de eventos, como o desligamento automático de turbinas ou de um reator nuclear pelo sistema de proteção do reator. Por essa razão, a sequência de eventos, é uma das principais fontes de alimentação de fatos para sistemas de diagnóstico que, por meio de uma análise de relação lógica e temporal entre sinais ou alarmes, consegue imitar o comportamento de análise de um operador e inferir diagnósticos ou conclusões de forma rápida e acurada. A tabela 2.1 exemplifica uma sequência de eventos resumida registrada em uma usina.

A sequência de eventos pode conter outros argumentos dependendo dos requisitos do sistema da usina. O campo referência contêm o nome que a variável recebe; data/hora se refere ao horário, até milissegundos, que o sistema teve conhecimento da mudança de valor da variável; o campo valor armazena o valor binário da variável, em geral, representando o estado ou situação de algum componente ou parâmetro, como aberto/fechado ou inferior/superior a um certo limite; validade se refere à legitimidade de leitura da variável, podendo ser 0 caso um sensor se encontre quebrado ou fora de funcionamento.

Referência	Datahora	Valor	Validade
B1	2016/10/21 19:49:03:253	1	1
B352	2016/10/21 19:50:10:521	0	1
K92	2016/10/21 19:51:09:010	0	0
B8000	2016/10/21 19:52:50:316	1	0

Tabela 2.1: Sequência de Eventos

2.2 Inteligência Artificial

A inteligência artificial é um dos ramos da ciência da computação mais recentes, tendo início logo após a segunda guerra mundial. Mais precisamente, a ideia de inteligência artificial surgiu junto com a criação da primeira máquina que viria a ser desenvolvida para o que chamamos hoje de computador. A primeira definição do que pode ser considerada inteligência artificial foi concebida por Alan Turing, na formulação do teste de Turing em 1950. O teste de Turing foi projetado com o intuito de definir operacionalmente o que seria uma inteligência artificial em vez de listar características de um ser inteligente. Turing propôs que um interrogador humano enviasse perguntas à máquina que responderia concordantemente. A máquina é considerada inteligente se o interrogador não conseguir distinguir se as respostas foram de fato formuladas pela máquina ou por um operador humano. Para conseguir aprovação no teste, a máquina deveria ter, no mínimo, as capacidades de processamento de linguagem natural, representação do conhecimento, raciocínio automatizado e aprendizado [15].O aprendizado de máquinas consideradas inteligentes, muitas vezes é feita de mesma forma como é feito o aprendizado humano, por meio da exposição à informação e recompensa ao alcançar objetivos. Essas capacidades podem ser consideradas pilares da inteligência humana e por isso se enquadra no ramo de IA que busca mimetizar habilidades e características humanas.

De forma mais abrangente, IA é uma abordagem que busca entender, modelar, replicar inteligência e processos cognitivos [16], sejam eles humanos ou de outros seres vivos. A modelagem da inteligência busca inspiração, em maior parte, em princípios biológicos e se utiliza de ferramentas matemáticas, computacionais,

lógicas e mecânicas para sua representação. Além disso é uma das áreas mais gerais e multidisciplinares, com contribuições de autores de diversas áreas, desde engenharia até psicologia e filosofia.

Em minha visão, a inteligência artificial é o ramo do conhecimento que busca modelar entendimento de como analisar e racionalizar processos e como o conhecimento é transmitido. Na engenharia, em geral, a IA vêm como suporte a tarefas que, a princípio, poderiam ser feitas por humanos. Entretanto, devido a sua complexidade de informações, e não necessariamente complexidade lógica, torna o cérebro humano um gargalo no processo de racionalização da informação e nos força recorrer a maquinas para garantir o processamento acurado da mesma. Sendo assim, ao recorrer a inteligência artificial, deve-se garantir a representação lógica fiel ao conhecimento que se deseja reproduzir e a veracidade das informações que são entregues à entidade responsável pela inferência.

Adicionalmente, na engenharia, algoritmos de inteligência artificial são amplamente utilizados para resolver problemas ou otimizar diversos processos. Seus usos variam desde aplicação em robótica, seja para navegação autônoma ou aprendizado de processos industriais, até aplicações puramente em software, como o desenvolvimento de simuladores inteligentes para treinamento de operadores ou otimização de problemas matemáticos combinatórios [17][18][19].

2.3 Representação do Conhecimento

A representação do conhecimento é o ramo em computação que faz a ligação entre a entidade racional e dados reais por meio de uma lógica matemática. No contexto de inteligência artificial, é a forma de representação de uma informação com o intuito de que um computador possa aplicar o conhecimento O conhecimento pode ser representado de diversas formas e deve ser suficiente para entendimento e inferência ou racionalização do processo. A engenharia ontológica busca a representação das coisas por meio da geração de estruturas gerais que podem ser preenchidas posteriormente com suas características específicas. De forma abstrata,

busca-se representar objetos, suas características e interrelações.

A representação geral de conhecimento é feita de diversas formas [15], entretanto, no caso em tempo real, representa-se normalmente pela definição de classes e funções, regras ou árvores lógicas. Antes de exemplificar os tipos de representação, definimos operadores lógicos booleanos, que são operadores responsáveis por unir sentenças lógicas entre si. A tabela a seguir define os operadores booleanos:

		Operadores						
A	B	NÃO	E	OU	XOU		Operador	Significado
1	1	0	1	1	0		NÃO $\neg$	Negação
0	0	1	0	0	0		E $\wedge$	Disjunção
1	0	-	0	1	1		OU $\vee$	Conjunção
0	1	-	0	1	1		XOU $\oplus$	Conjunção Exclusiva

Tabela 2.2: Operadores Lógicos

2.3.1 Representação por classes

Classes são um dos primeiros conceitos de abstração em linguagens de programação, se diferenciando de estruturas básicas que buscavam apenas o armazenamento e agrupamento de dados. Elas são entidades de linguagens de programação de alto nível que buscam generalizar algo por meio da estruturação de suas funções e propriedades, de forma não específica. Nesse contexto, definimos que classes são estruturas gerais, que apresentam atributos e métodos relativos à o que representa; e instâncias são representantes específicos de uma classe. A representação por classes segue o conceito de lógica de predicados, onde se define relações e o predicado é o indicador de funções de relação entre objetos. Tomamos o seguinte exemplo como nossa base de conhecimento:

"A pessoa que retirar a espada Excalibur da pedra será o novo rei."

Nessa frase, podemos generalizar as estruturas de forma que temos a instância

Excalibur, pertencente a uma classe Espada; a classe Pessoa, que pode tentar retirar a espada da pedra; e a classe Rei, assumida pela Pessoa que conseguir retirar a Espada Excalibur. Definimos então os operadores ASK e TELL.

TELL	Adiciona sentenças à base de conhecimento
ASK	Consulta conhecimento fundamentado na base
BC	Base de conhecimento

Definimos:

- TELL(BC, Pessoa(Arthur))
- TELL(BC,$\forall x$ Pessoa(x).Removeu(Espada(Excalibur),Pedra) $\implies$ Rei(x))
- TELL(BC,Pessoa(Arthur).Removeu(Espada(Excalibur),Pedra))

Sendo assim, podemos inferir de nossa base de conhecimento:

ASK(BC,Rei(Arthur)) deve retornar verdadeiro

De mesma forma:

TELL(BC,Pessoa(John).Removeu(Espada(Enferrujada),Pedra))
ASK(BC,Rei(John) deve retornar falso.

2.3.2 Representação por regras

Regras são estruturas de representação que buscam, por meio de um conjunto de condições lógicas booleanas ou de lógica nebulosa[20], chegar a uma conclusão. A representação em regras é feita pela avaliação de um conjunto de condições que levam a consequentes, ou conclusões, que podem afetar o restante das regras. Dependendo do problema, a estruturação do conhecimento em regras pode ser hierárquico, ou seja, o consequente de uma regra pode influenciar no antecedente de outra regra com prioridade diferente, e por esse motivo, a avaliação é ordenada conforme a prioridade

entre regras. A representação em regras deve assumir o seguinte formato:

SE ANTECEDENTE **ENTÃO** CONSEQUENTE
SE ANTECEDENTE **ENTÃO** CONSEQUENTE$_1$ **SENÃO** CONSEQUENTE$_2$

O modelo de regras acima é conhecido como *Modus Ponens*. Isso significa que a inferência lógica só é feita no sentido $ANTECEDENTE \rightarrow CONSEQUENTE$, e o contrário, $ANTECEDENTE \leftarrow CONSEQUENTE$, não é verdadeiro.

De tal forma que, um conjunto de regras deve ser suficiente para cobrir todas as possíveis entradas e saídas de uma lógica. Por exemplo:

"Mamíferos são animais vertebrados, homeotérmicos que apresentam glândula mamária."

Pode ser representado no formato de regras:

SE VERTEBRADO **E** HOMEOTÉRMICO **E** MAMAS **ENTÃO** MAMÍFERO

Sendo assim, conhecendo certas características de um animal, podemos determinar se é um mamífero.

2.3.3 Representação por árvores

Árvores são estruturas bem conhecidas em engenharia. Por exemplo, são amplamente utilizadas para cálculo de falha de um sistema baseado nas falhas de seus componentes constituintes no que chama-se de árvore de falhas. Generalizando, árvores lógicas são diagramas lógicos compostos por grafos [1], nos quais suas funções são operadores lógicos que ilustram a relação lógica entre nós de uma árvore. Diversas representações podem estar associados à estrutura de grafos, por exemplo, redes semânticas nas quais os vértices representam conceitos e arestas suas relações semânticas. Entretanto, nesse trabalho, buscamos uma representação lógica boole-

[1]Grafos são ternos (V,A,f) que associam arcos, representados no conjunto finito A, e pares de vértices, representados no conjunto finito V por meio de uma função f.

ana entre eventos em uma árvore. Para isso, os operadores são portões lógicos e podem se relacionar com eventos, vértices presentes no fim de uma árvore, ou com outros vértices. Os portões lógicos comumente aplicados em engenharia são [21]:

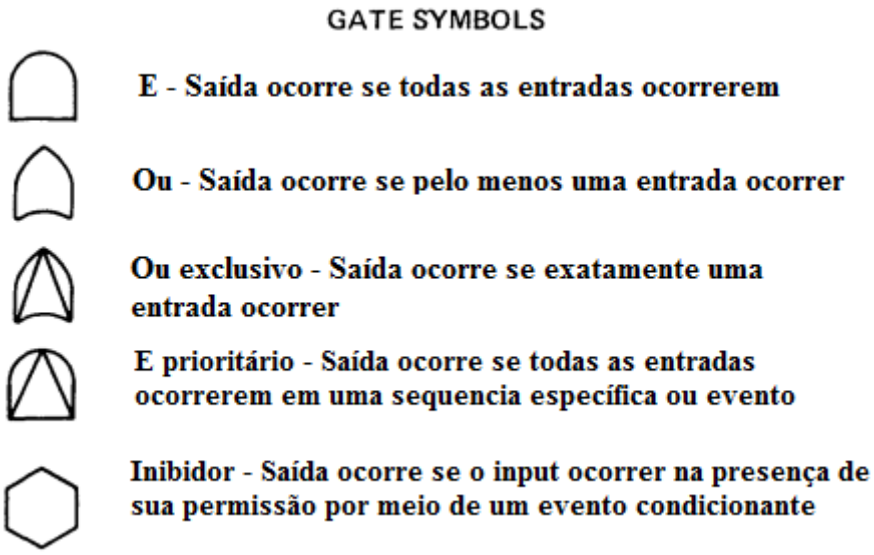

Figura 2.2: Portões Lógicos

Tomamos então como exemplo o caso de um estudante universitário que deseja ir ao mercado comprar comida. O intuito de tal representação lógica é, dado um conjunto de eventos iniciais, determinar a saída da árvore, ou, dada a saída da árvore, tentar formular possíveis caminhos e eventos iniciais que geraram tal saída.

Por mais simples que seja o exemplo, tal representação pode se tornar complexa ao levar em consideração diversos nós e eventos, sendo necessária a aplicação de algoritmos para indução ou dedução baseado na estrutura da árvore.

2.4 Sistema Especialista

O sistema apresentado neste trabalho faz o uso de um algoritmo de inteligência artificial conhecido como Sistema Especialista. Essa seção trata aspectos gerais do algoritmo e seu funcionamento.

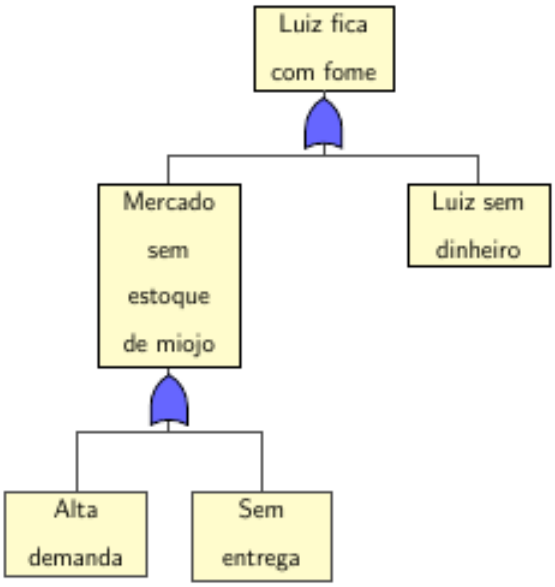

Figura 2.3: Representação lógica em árvore

2.4.1 História e Definição

Sistemas Especialistas ou Sistemas baseado em Conhecimento foram desenvolvidos nos anos 60 pelo *Stanford Heuristics Programming Project* como um novo método inteligente de encontrar soluções para problemas complexos, como diagnóstico de doenças. Edward Feigenbaum, conhecido como o pai dos sistemas especialistas, o define como "um programa de computador inteligente que usa conhecimento e procedimentos de inferência para resolver problemas difíceis suficiente que requerem significante expertise humana para sua solução". Em outras palavras, um sistema especialista é um sistema computacional que emula a capacidade de decisão de um profissional humano de uma área.

A principal diferença de um sistema especialista em relação à outros sistemas de diagnóstico ou decisão é a modularização e independência de suas partes constituintes. O sistema é composto por uma base de conhecimento, onde se constitui a heurística do problema por meio de sua representação computacional, e por um motor de inferência, responsável por gerar novos fatos.

Sistemas especialista tem aumentado sua popularidade devido à sua introdução comercial na década de 80 [22]. Atualmente, são aplicados em diversas áreas da

ciência da computação, engenharia e outras ciências que apresentam domínios de problemas bem definidos.

Desde sua criação, diversos SE's foram construídos com diferentes propósitos. A tabela a seguir exemplifica alguns sistemas e usas respectivas aplicações:

Nome	Descrição
PROSPECTOR	Sistema aplicado em prospecção de minério. Descobriu um depósito de molibdênio com valor aproximado de 100 milhões de dólares.
R1[23]	Sistema que seleciona componentes eletrônicos para sistemas de computador VAX de acordo com o pedido do cliente.
DENDRAL[24]	Sistema aplicado para elucidação de estruturas químicas.
CADUCEUS[25]	Sistema de diagnóstico de doenças humanas.
PUFF[26]	Sistema de diagnóstico e consulta para doenças pulmonares.

Tabela 2.3: Sistemas Especialista famosos

2.4.2 Funcionamento de um Sistema Especialista

Um sistema especialista é composto por dois módulos e sua memória de processamento:

- Base de Conhecimento (**BC**)
- Motor de Inferência (**MI**)
- Memória de Trabalho (*workmemory*)

A base de conhecimento é onde toda heurística relativa ao problema é representada. Essa pode ser modificada ou adaptada a novos conhecimentos sem que haja necessidade de remodelamento do motor de inferência. Essa característica é essencial para o caráter genérico do algoritmo, facilitando sua aplicação em diversos problemas de diagnóstico. Se o modo de racionalização for similar, o conhecimento pode se tornar mais especializado ou completo pela inserção de novas regras ou estruturas representativas na BC. Por outro lado, não se busca em sistemas especialista a abrangência de diversos problemas em uma mesma base de conhecimento já que os problemas podem necessitar de diferentes modos de seleção de regras.

Um sistema especialista é caracterizado pelo paradigma de representação do conhecimento em sua BC. Como discutido na seção anterior, alguns tipos de representação são : árvores lógicas, regras e por classes. Além desses, existem formas de representação em frames e redes semânticas.

O motor de inferência é o módulo responsável por unir fatos de um problema com o conhecimento representado na BC, sendo capaz de gerar novos fatos e conclusões. O motor de inferência une os fatos com o conhecimento ao avaliar as condições, o antecedente no caso de regras, do conhecimento representado.

Memória de trabalho é o nome dado aos fatos entregues ao sistema, após devida representação computacional, na forma de variáveis binárias, numéricas ou outro tipo de representação de acordo com o esperado na base de conhecimento. A seguir é exposto um diagrama de funcionamento de um sistema especialista.

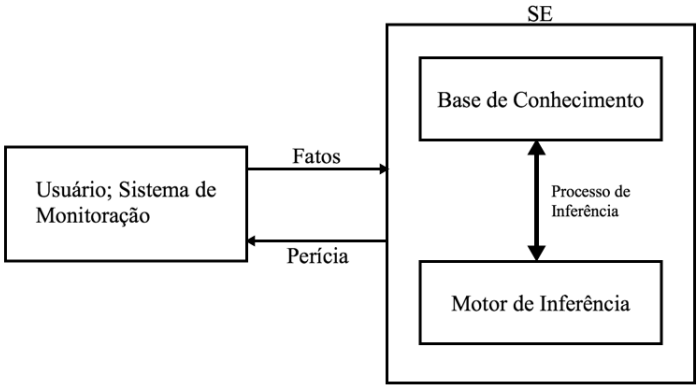

Figura 2.4: Diagrama de funcionamento de um sistema especialista.

Seguindo a figura 2.4, o processo de inferência lógica pelo MI é feito pela união dos fatos coletados sobre o problema, seja por meio de entrada manual do usuário ou dados provenientes de outro sistema, com as regras lógicas na base de conhecimento. Por fim, a perícia sobre o problema é entregue ao usuário. Caso um fato presente em uma regra não esteja disponível na memória, o motor de inferência tenta avaliar a regra mantendo sempre seu sentido lógico. Caso a lógica seja completa sem esse fato, a regra pode ser executada, caso contrário é ignorada. O encadeamento de informações pode ser feita de duas formas diferentes:

- Encadeamento para Frente - *forward*
- Encadeamento para Trás - *backward*

O encadeamento para frente parte da suposição de que são conhecidos fatos sobre um problema e o sistema se utiliza da BC para criar novos fatos, conclusões ou tomar ações. Por outro lado, o encadeamento para trás começa com uma suposição inicial e tenta provar ela, por meio de consulta a BC e fundamentação das hipóteses pelos fatos na memória. A diferença principal entre os encadeamentos é a orientação. A inferência para frente é guiada pelos fatos enquanto a inferência para trás, pelo objetivo.

O processo lógico de um sistema especialista é, em geral, dividido em subobjetivos que são mais fáceis de se provar ou alcançar do que o objetivo final do problema como um todo. Dessa forma, um objetivo final é alcançado ao se alcançar uma determinada combinação de subobjetivos. Essa forma de raciocínio por meio da aplicação de casos singulares para alcançar um objetivo maior definem o raciocínio indutivo.

Por fim, vale mencionar que apesar de a avaliação da base de conhecimento não ter um custo muito alto computacionalmente, a quantidade de regras e variáveis tende a crescer muito com a dimensão do problema estudado, podendo se tornar custosa a inserção de conhecimento na BC e alimentação de variáveis.

Capítulo 3

Algoritmos e Ferramenta de Diagnóstico

3.1 Apresentação do Problema

Usinas de geração elétrica, em especial usinas nucleares, apresentam uma complexidade de segurança muito maior do que outras plantas de processo. Buscando reduzir riscos, sistemas vitais para segurança da usina apresentam redundâncias e existe a necessidade de constante monitoramento dos parâmetros desses sistemas. Pelo lado da segurança física da usina, é essencial que a capacidade de monitoramento, controle de parâmetros e resposta à alarmes se mantenha constante e eficiente. Por outro lado, a complexidade da usina torna o monitoramento uma tarefa custosa para operadores cuja capacidade cognitiva varia de acordo com a quantidade de informação, condições pessoais e de ambiente de trabalho.

Por determinação da CNEN Norma NN-1.14 Seção 5 - Notificação de Eventos, a organização operadora da usina deve notificar a CNEN a ocorrência de declaração de situação de emergência no prazo máximo de uma hora. Por esse motivo, existe um conjunto de parâmetros e variáveis que, em conjunto, determinam a situação de emergência da usina e devem ser examinadas.

A mesma norma determina, na Seção 6 - Relatório de Eventos deve comunicar a CNEN eventos significantes, como operação ou condição de equipamentos não permitida pelas especificações técnicas, mal funcionamento de equipamentos e consequente desligamento automático do reator. Esse eventos devem ser classificados de acordo com a subseção 6.2 e preenchidos de acordo com a subseção 6.3. Essa subseção determina no relatório a especificação da causa-raiz responsável pelo

evento. Essa análise de causa pode se tornar demorada já que, muitas vezes, pode ser o mal funcionamento de equipamentos de segurança cuja detecção de falha não é trivial.

O sistema de suporte ao diagnóstico desenvolvido nesse trabalho foi projetado com o objetivo de auxiliar os operadores na sala de controle a cumprir essas duas determinações. Por esse motivo, o sistema é composto por dois módulos em tempo real que, separadamente, são capazes de monitorar, inferir e expor ao operador, na IHM, as informações relativas a estes processos. O intuito é reduzir a carga de trabalho e análise dos operadores, aumentando o tempo de resposta e tomada de decisão em caso de emergência.

O módulo de classificação de situação de emergência faz o uso de regras lógicas para inferência da situação da usina, atendendo assim ao definido na seção 5. O módulo de suporte ao diagnóstico de causa-raiz aplica o conhecimento dos operadores, representado na estrutura de árvores, para auxiliar o processo de determinação de causa-raiz, cumprindo o requerido no relatório de evento significante e consequentemente acelerando o processo de religamento da usina, quando possível.

Por fim, o sistema aqui desenvolvido é alimentado, em tempo real, por variáveis binárias, digitais e analógicas provenientes de outro sistema que integra variáveis e computadores da usina de Angra I. O Sistema Integrado de Computadores de Angra - SICA é um sistema de monitoramento que aplica inteligência artificial para representar e calcular dependências entre parâmetros que devem ser monitorados na usina. Essa relação é mapeada em uma rede de objetos hierarquizada onde regras e condições em tempo real são aplicadas aos objetos, por meio de operadores e topologia em rede. Por fim, o sistema distribui o valor final das variáveis dependentes e as recalcula sempre que necessário.

3.2 Base de Conhecimento

As bases de conhecimento utilizadas para formulação dos módulos de diagnóstico foram:

- Documentação de Classificação de Situação de Emergência da Usina Nuclear Angra I
- Conhecimento dos operadores relativo à análise de causa-raiz no evento de trip do reator.

3.2.1 Classificação de Situação de Emergência

A documentação de classificação de situação de emergência é um documento, baseado no NEI 99-01 (Apêndice B), composto por diversas categorias de reconhecimento de perigos causados pela usina ou que possam atingir a usina, podendo afetar sua segurança física. A situação da usina é determinada a partir de cinco categorias de reconhecimento que tem como principal objetivo mitigar danos causados , como liberações radiológicas.

A Níveis de Radiação **A**normais e Efluentes Radiológicos.

D Má Função em Sistemas em **D**esligado Frio ou Recarregamento

F Degradação em Barreira de Produto de **F**issão

R **R**iscos e Outras Condições que Afetem a Segurança da Usina

S Má Função em **S**istema

Cada pagina do documento apresenta um diagrama de classificação de situação de emergência que se enquadra nos tópicos acima. As condições presentes em cada categoria são aplicáveis dependentemente do modo de operação da usina. Por exemplo, a categoria **D** é somente aplicável se a usina estiver no modo de Desligamento Frio ou em Recarregamento. A usina pode assumir os seguintes seis modos de operação:

1. Operação à potência
2. Partida
3. Prontidão Quente
4. Desligado Quente
5. Desligado Frio
6. Recarregamento

Em conjunto, o modo de operação da usina e as condições presentes em cada categoria de reconhecimento, classificam a usina em cinco situações de emergência:

1. Condição Normal
2. Evento Não Usual - ENU
3. Alerta
4. Emergência de Área
5. Emergência Geral

O diagrama de condições de reconhecimento, por meio de operadores lógicos, relaciona um conjunto de sinais e valores limitantes à uma classificação de emergência da usina dependendo das condições dadas. A representação do conhecimento no documento facilitou a representação computacional em regras hierarquizadas de acordo com a prioridade da emergência. Cada bloco do diagrama equivale ao antecedente de regras cujo consequente, em conjunto com o valor do bloco anterior, é a classificação de situação de emergência da usina.

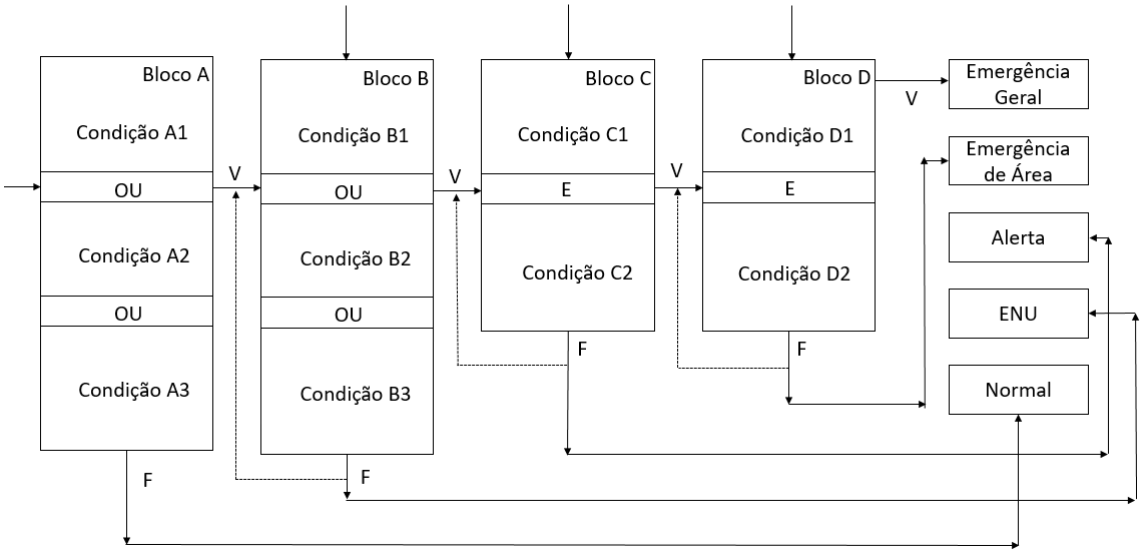

Figura 3.1: Esquematização de classificação de situação de emergência.

O esquema pode ser transcrito para o seguinte conjunto de regras:

1. **SE** A1 OU A2 OU A3 **ENTÃO** BLOCOA = VERDADEIRO
2. **SE** B1 OU B2 OU B3 **ENTÃO** BLOCOB = VERDADEIRO
3. **SE** C1 E C2 **ENTÃO** BLOCOC = VERDADEIRO
4. **SE** D1 E D2 **ENTÃO** BLOCOD = VERDADEIRO
5. **SE** BLOCOA == FALSO **ENTÃO** CLASS1 = NORMAL
6. **SE** BLOCOA E BLOCOB == FALSO **ENTÃO** CLASS1 = ENU
7. **SE** BLOCOB E BLOCOC == FALSO **ENTÃO** CLASS1 = ALERTA
8. **SE** BLOCOC E BLOCOD == FALSO **ENTÃO** CLASS1 = EMERGENCIA DE AREA
9. **SE** BLOCOD **ENTÃO** CLASS1 = EMERGENCIA GERAL

No formato escrito, as regras devem ser avaliadas de forma hierarquizada, ou seja, respeitando a ordem de 1 até 9. No exemplo, CLASS1 significa a classificação de situação de emergência da usina para o tema que compõe o documento 1. A base

de conhecimento total de classificação é composta por diversos documentos que tratam um conjunto de sistemas e parâmetros que devem ser monitoradas.

A seguir encontra-se um exemplo que é aplicável em todos os modos de operação, a classificação de situação baseada nos níveis de radiação anormais e de efluentes radiológicos (**A**). Nesse caso, os valores limitantes respeitam normas de proteção radiológica da CNEN e os níveis de emergência superiores são acusados pelos medidores de dose externa ao sítio, requerendo ações de proteção.

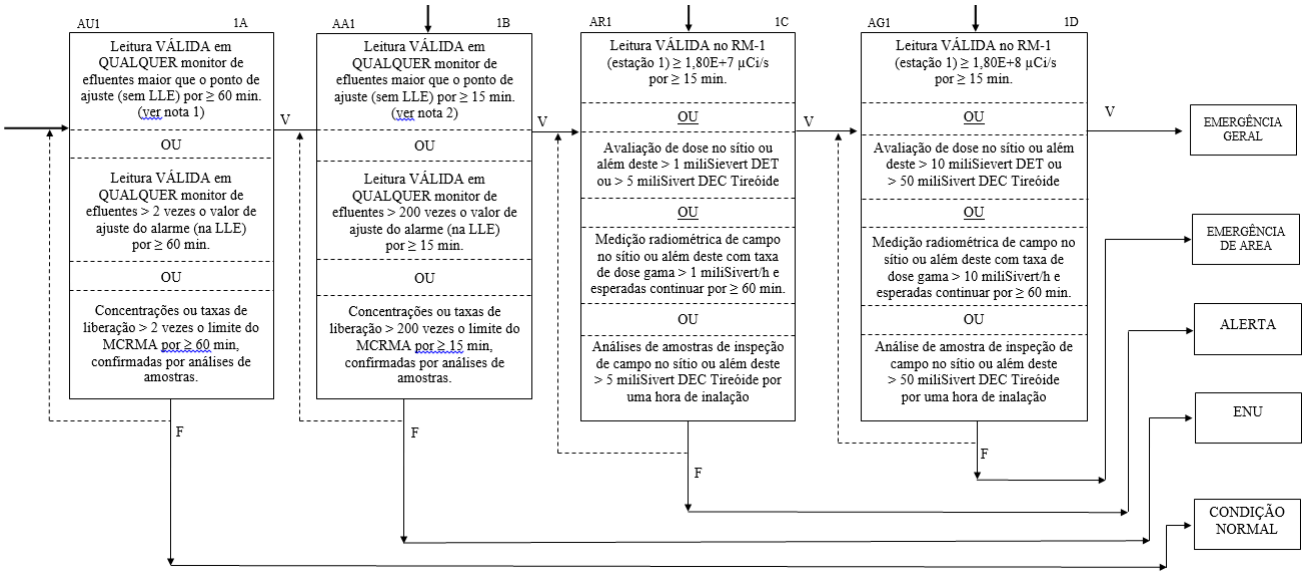

Figura 3.2: Diagrama de classificação categoria A

O modelo de regras segue o mesmo formato demonstrado anteriormente. Como a categoria é aplicável em todos os modos de operação, não é necessário a introdução do modo de operação no conjunto de regras. O Apêndice C expõe a complexidade para representação do diagrama de classificação acima em um bloco de regras necessário para representação completa do conhecimento.

3.2.2 Causas de desligamento de emergência

A ferramenta de suporte ao diagnóstico de causa de desligamento de emergência vem de uma necessidade de relatar ao orgão regulador, a CNEN, o motivo do desligamento de emergência, seja por inserção de barra de controle ou injeção de água

borada. A usina tem seu religamento aprovado uma vez que a causa-raiz do trip é comunicada ao orgão regulador e aceita por este. O diagnóstico é feita por análise dos operadores, seja por experiência operacional e conhecimentos teóricos do funcionamento da planta. Muitas vezes, o diagnóstico não é simples já que é causado pelo mal funcionamento de algum componente ou sistema.

A base de conhecimento, nesse caso, é preenchida por profissionais que montam a relação lógica e dependência temporal entre notificações do sistema de alarmes na forma de árvores lógicas, representando incidentes que causaram o desligamento do reator. Essas relações partem de hipóteses básicas de funcionamento de plantas de processos:

1. Notificações dependentes ocorrem por fluxo de material
2. Notificações dependentes ocorrem por erro de configuração no sistema de alarmes (redundância de alarmes)
3. Notificações dependentes ocorrem por intervenção do operador

No caso de usinas nucleares, um transiente pode afetar mais de um sistema e seus parâmetros monitorados e, por esse motivo, pode-se indicar a hipótese número 1 como maior causa de avalanche de alarmes.

Petrangeli [6] indica os sinais que acionam desligamento rápido do reator e seu respectivo tempo de atraso. Esses sinais são essenciais pois indicam ao sistema de diagnóstico por onde começar a buscar a causa do desligamento.

Origem	Limite	Atraso (s)
Alto fluxo de neutrôn	118%	0.5
ΔT do núcleo (sobretemperatura)	Automático	6
ΔT do núcleo (sobrepotência)	Automático	6
Alta pressão no pressurizador	16.65 MPa	2
Baixa pressão no pressurizador	12.31 MPa	2
Baixo fluxo de recirculação	87%	1
Trip da turbina	-	1
Baixo nível no gerador de vapor	-	2
Alto nível no gerador de vapor	-	2

Tabela 3.1: Sinais de desligamento

3.3 Módulo de Diagnóstico de Situação de Emergência

3.3.1 Introdução

O módulo de diagnóstico situação de emergência é responsável por inferir a classificação completa da situação de emergência da usina. A classificação é dada pela avaliação de regras presentes no documento de plano de emergência da usina de Angra I. As regras são avaliadas em tempo real a partir da união de variáveis analógicas, digitais e calculadas, provenientes do Sistema Integrado de Computadores de Angra I, perguntas em tempo real ao operador do sistema de acordo com a demanda do SE e do processamento de alarmes críticos.

O objetivo do módulo apresentado é entregar, em tempo real, a classificação da situação de emergência da usina de Angra I, facilitando o trabalho dos operadores, aumentando o tempo de resposta disponível e diminuindo drasticamente erros causados por falhas cognitivas ou não obediência a procedimentos.

3.3.2 Metodologia

Devido a necessidade de se inferir um conjunto de regras que se remete a um diagrama, apresentado em 3.2.1, foi aplicado um sistema especialista tradicional. A base de conhecimento é composta pela transcrição dos diagramas de classificação conjuntos de regras que apresentam hierarquia de inferência em relação ao seu nível de emergência. A hierarquia é aplicada devido à necessidade de avaliação de todos os blocos - conjuntos de condições, antes da conclusão final do sistema em relação à situação de emergência presente na usina.

O motor de inferência é o código responsável por unir variáveis e regras, com o intuito de preencher sua memória de trabalho com novos valores e/ou novas variáveis geradas pelas regras. A seguir, apresenta-se um pseudocódigo para o funcionamento do motor de inferência, que pode ser modificado de acordo com a necessidade de processamento do programador.

```
0 atualiza a memória de trabalho
1 enquanto regras podem ser executadas:
        2 resolve conflito por seleção de prioridade e seleciona regra
        2 avalia antecedente da regra
                3 executa consequente
                4 atualiza memória de trabalho com novo valor ou variável
                5 queima regra no ciclo
6 retorna nova memória de trabalho
```

Figura 3.3: Pseudocódigo do Motor de Inferência

O ato de "queimar"a regra, significa que, uma vez executada, a regra não pode ser executada novamente no mesmo ciclo de aquisição de variáveis.

Seguindo o pseudocódigo para o bloco de regras exposto em 3.2.1, podemos resolver o exemplo. Com o intuito de facilitar a explicação, a resolução de conflitos e

avaliação de antecedentes são feitas sobre o mesmo índice de execução (2), como exposto na figura. No caso exemplificado, como as variáveis BLOCO representam um conjunto de condições fora de limites de segurança, enquanto não houver inferência de tais variáveis, seus valores são mantidos como FALSO. Na memória de trabalho a seguir, exibe-se apenas variáveis com valor VERDADEIRO.

Memória de Trabalho	Ordem de Execução
A1 VERDADEIRO	$>> 0 \rightarrow 1$
B1 VERDADEIRO	$>> 2 \rightarrow 3 \rightarrow 4 \rightarrow 5$ *executou regra 1., adicionou valor para BLOCOA*
C1 VERDADEIRO	
C2 VERDADEIRO	$>> 2 \rightarrow 3 \rightarrow 4 \rightarrow 5$ *executou regra 2., adicionou valor para BLOCOB*
	$>> 2 \rightarrow 3 \rightarrow 4 \rightarrow 5$ *executou regra 3., adicionou valor para BLOCOC*

Após a execução parcial das regras, a memória de trabalho atualizada e o motor de inferência pode continuar a execução:

Memória de Trabalho	Ordem de Execução
A1 VERDADEIRO	$>> 2 \rightarrow 3 \rightarrow 4 \rightarrow 5$ *executou regra 8., adicionou valor para CLASS1 como EMÊRGENCIA DE AREA*
B1 VERDADEIRO	
C1 VERDADEIRO	
C2 VERDADEIRO	$>> 6$ *retorna classificação de situação de emergência para interface homem-máquina*
BLOCOA VERDADEIRO	
BLOCOB VERDADEIRO	
BLOCOC VERDADEIRO	

Seguindo a metodologia apresentada, após a execução de todos os blocos de regras representativos de cada categoria de reconhecimento, temos a classificação de situação de emergência da usina de forma rápida, confiável e principalmente, com necessidade mínima de interação com o operador.

O módulo de classificação de situação de emergência atua em tempo real e infere uma nova classificação para cada categoria sempre que a memória de trabalho é atualizada pelo SICA. Uma vez executado o algoritmo, a memória de trabalho com novos valores modificados pelo SE é passada para a interface homem-máquina que é responsável por exibir na tela a classificação ou requerer do operador toda e qualquer interação com o sistema, como a necessidade de resposta manual de perguntas.

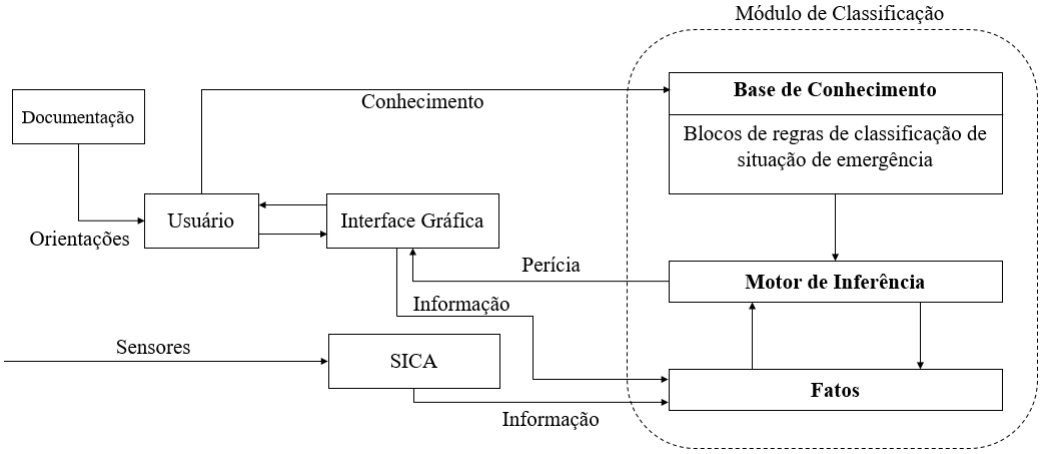

Figura 3.4: Diagrama de comunicação do módulo de classificação

A figura 3.4 mostra como o fluxo de informação se direciona no sistema. O usuário inicialmente insere no sistema conhecimento sobre o funcionamento da classificação de situação de emergência, em forma de regras. Em funcionamento, o sistema é alimentado por variáveis, em tempo real, do SICA e de respostas respondidas pelo operador na interface homem-máquina. Havendo capacidade de resposta, o sistema exibe ao usuário sua perícia, ou seja, classificação de situação da usina.

3.4 Módulo de Suporte ao Diagnóstico de Causa-raiz de Trip

3.4.1 Introdução

O módulo de diagnóstico de causa-raiz é responsável auxiliar na determinação do motivo do desligamento de emergência da usina. O diagnóstico é dado pela avaliação dos sintomas e a relação lógica e temporal do conjunto de causas.

O principal objetivo do módulo apresentado é ser uma ferramenta genérica de diagnóstico para ser aplicado em qualquer tipo de planta industrial, seja de processamento ou de geração elétrica. É aplicado um sistema especialista modificado cujo motor de inferência trabalha de cima para baixo, ou seja, a partir de um evento, tenta-se provar o que ocasionou esse evento. O SE é alimentado por um algoritmo de similaridade que filtra apenas os eventos pertinentes ao acidente que o SE tenta provar. A base de conhecimento é composta por árvores lógicas e a inferência da causa é feita pela relação entre regras de procedimento com a lógica e diferença temporal entre os sinais.

3.4.2 Metodologia

Antes de explicar a metodologia, definimos a nomenclatura aplicada.

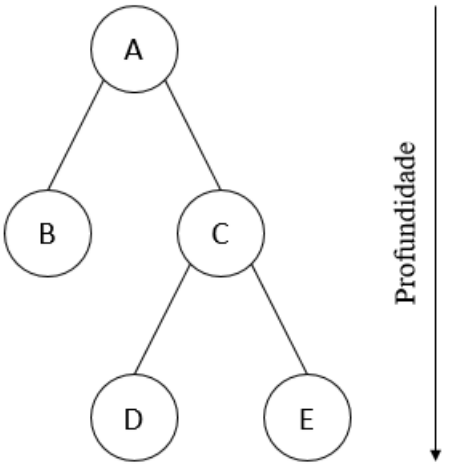

Figura 3.5: Figura suporte para exemplificação de nomenclatura

Seguindo a figura 3.5, definimos como nó pai o nó que apresenta ligação com outros nós de profundidade superior. Na figura, A é nó pai de B e C, C é nó pai de D e E. Consequentemente, definimos B e C como nó filho de A e D e E como nó filho de C. Além disso, definimos B, D e E, nós que não apresentam ligações com profundidades superiores, como nós folha.

A sequência de evento é analisada pelo algoritmo de similaridade a partir do topo da árvore - o evento de desligamento, percorrendo ramo por ramo até encontrar um evento que indique o fim da ramo. O fim pode ser indicado por um nó folha, ou seja, um nó que não apresenta ligação com nenhum outro nó de maior profundidade, ou caso a similaridade entre o acidente representado e a sequência de eventos seja concluída. Considera-se a similaridade concluída quando a sequência de eventos não contêm mais nenhum nó filho do nó pai que está sendo analisado. No caso em que os ramos não terminam com um nó folha, o diagnóstico será indicado como similaridade parcial com o evento selecionado na base de conhecimento.

O diagnóstico feito pelo algoritmo de similaridade começa procurando por árvores na base de conhecimento que apresentam o mesmo nó no topo da árvore. Filtrada tais árvores, a cada iteração, é percorrido uma profundidade da árvore para cada ramo, a partir do topo até o fim da árvore, correspondendo os nós com eventos presentes na sequência de eventos dependendo do operador lógico do nó pai. Os

nós que apresentam correspondência na sequência de eventos então determinam os novos ramos que serão percorridos na próxima iteração do algoritmo. A figura a seguir ilustra como funciona a filtragem dos eventos.

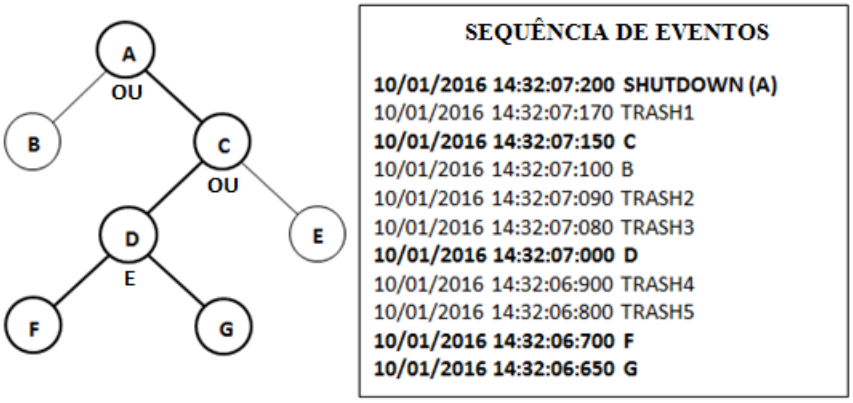

Figura 3.6: Exemplificação do funcionamento

Na sequência de eventos experimental representada na figura 3.6, o alarme de desligamento representado por A é o topo da árvore de acidente. A partir deste ponto, a sequência de eventos é processada de cima para baixo, conferindo a correspondência dos nós na árvore com os eventos registrados. Consequentemente, C é entregue ao sistema especialista para sua validação. Em seguida, é entregue D que por fim chega-se a causa final de F e G.

No exemplo, os eventos indicados como TRASH são eventos que não possuem significância para a análise, por não estarem presentes na estrutura da árvore, mas aparecem na sequência de eventos por necessidade de registro.

O processo de validação dos eventos ao acidente selecionado é feito por um sistema especialista que aplica regras de protocolo baseadas no conhecimento dos operadores da usina. A regra de validação apresenta dependência lógica e temporal entre os registros no SOE.

1. Eventos cuja diferença temporal entre o seu tempo de registro e seus eventos causa (nós filho) são maiores que o limite pré determinado na base de

conhecimento, não correspondem.

2. No caso do operador lógico OU, o evento causa(nó filho) correspondente é o evento cuja diferença temporal entre seu tempo e o tempo de registro do nó pai é a menor.

3. No caso de conflito na regra acima, ou seja, a diferença temporal seja a mesma, o algoritmo de similaridade para.

4. No caso de operador lógico E, todos os eventos causa (nós filho) devem ser válidos e presentes no SOE.

5. No caso de operador lógico E, caso todos os eventos causa sejam válidos e presentes no SOE, todos são validados para correspondência e percorridos pelo algoritmo.

6. No caso do operador lógico IGUAL, o evento causa deve estar presente no SOE.

7. Se nenhuma nó novo for correspondido, o algoritmo para.

Finalmente, após analisar todas as árvores na base de conhecimento, o sistema especialista exibe como solução a sequência de eventos que conseguiu chegar ao fim da árvore, ou seja, encontrou um ou mais nós folha, ou a árvore que percorreu um maior número de profundidades. No caso de não haver a seleção de nenhum possível diagnóstico, o sistema responde "Não Sei". Sendo assim, vale mencionar que a capacidade de auxiliar no diagnóstico depende de quão completo é representado o conhecimento de análise de eventos dos operadores na BC. A capacidade de acomodar uma grande quantidade de estruturas de conhecimento e o ganho em diagnóstico ao inseri-las, pode tornar a base de conhecimento um banco de dados de relações ontológicas dependendo da magnitude do problema.

O módulo de suporte ao diagnóstico é acionado sempre que um evento de desligamento é detectado. Quando isso ocorre, a sequência de eventos é entregue ao sistema especialista que é responsável por analisá-la e escolher árvore ou árvores que possam ser semelhantes ao ocorrido. Selecionadas, essas árvores de eventos são processadas pelo motor de inferência que, uma vez selecionado um diagnóstico, passa

a informação completa, desde as causa(s)-raiz até o evento de desligamento, para a interface gráfica, onde é exibida para o operador.

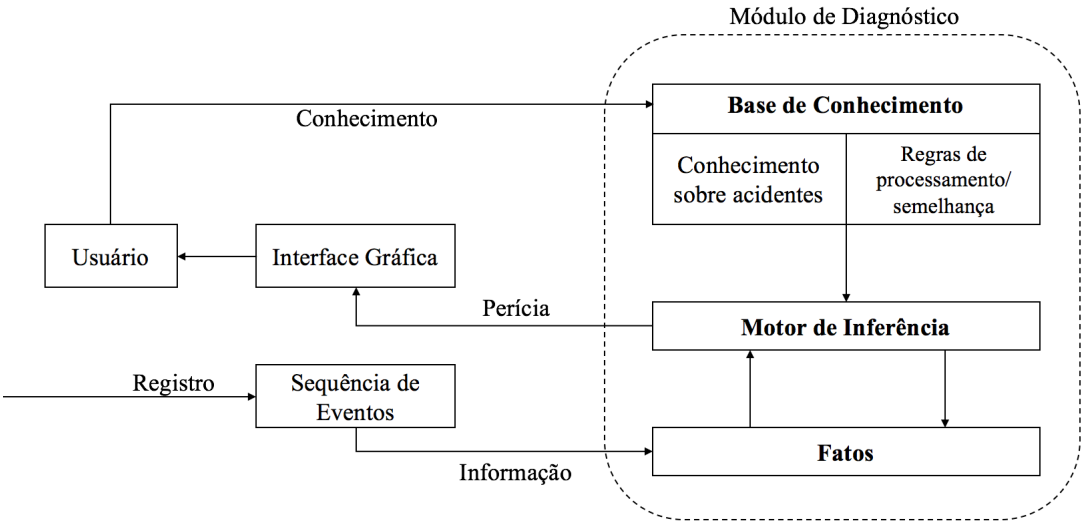

Figura 3.7: Diagrama de comunicação do módulo de diagnóstico

Seguindo o fluxo de informação da figura 3.7, o usuário insere conhecimento sobre eventos que podem causar desligamento do reator na base de conhecimento. Ao detectar um desligamento, o sistema é automaticamente ativado e alimentado pela sequência de eventos, composta por eventos prescendentes ao trip. O sistema analisa a sequência e exibe sua perícia na interface homem-máquina ao operador que por fim termina a análise da causa-raiz de desligamento.

Capítulo 4

Resultados e Apresentação do Sistema Inteligente de Suporte ao Diagnóstico

Nesse capítulo, inicialmente, apresenta-se como o conhecimento é inserido na interface gráfica da base de conhecimento, para ambos os módulos. Em seguida, é apresentada a interface principal do sistema, na qual se exibe como operar os módulos descritos nesse trabalho.

4.1 Apresentação do Módulo de Classificação de Situação de Emergência

Como definido anteriormente, a BC do sistema especialista responsável pelo módulo, é composta por bloco de regras que representam a documentação especificada pela usina. Dentro da base de conhecimento, existe uma estruturação em blocos e local específico para adição de lógica como indicado na figura 4.1 e 4.2 respectivamente.

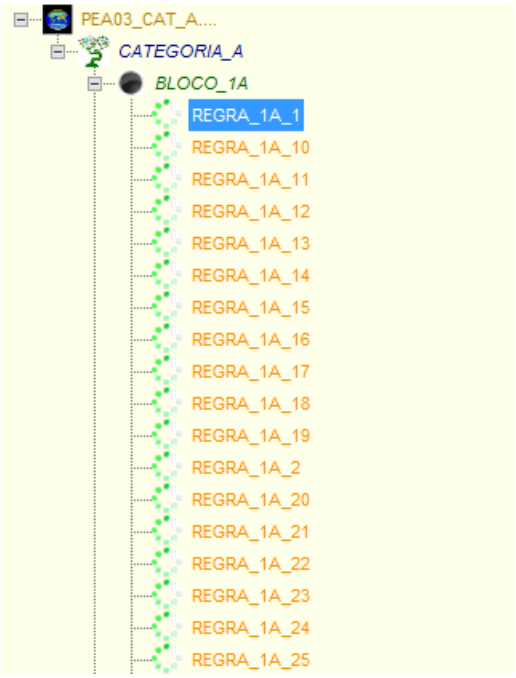

Figura 4.1: Estrutura de regras na interface da base de conhecimento

A hierarquia é subdividida em documentação, no exemplo **P**lano de **E**mergência **A**mbiental 03, equivalente ao **P**lano de **E**mergência **L**ocal; categoria, já apresentada em 3.2.1; e por fim, blocos de regras. Cada regra assume o formato antecedente/consequente e é formada por variáveis coletadas em tempo real pelo SICA, perguntas ao operador ou variáveis intermediárias que podem ser criadas para facilitar a leitura da regra. A variável `CAIXA_1_1A` é um exemplo desse tipo de variável intermediária criada.

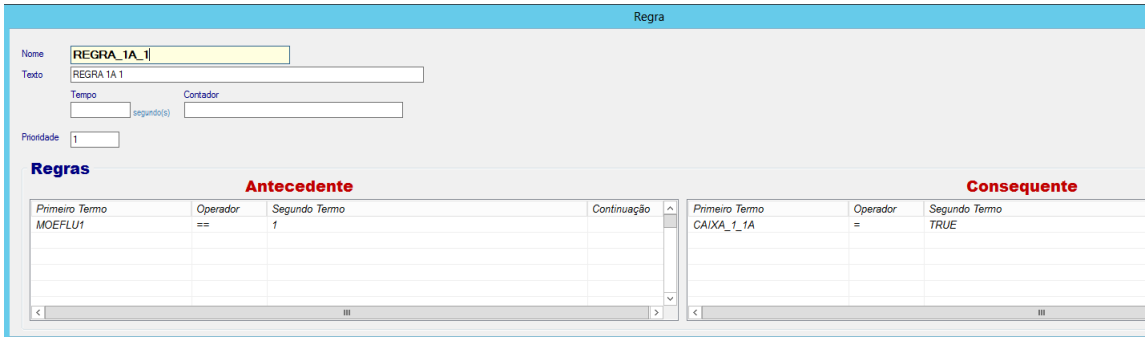

Figura 4.2: Formação da regra na interface da base de conhecimento

Uma vez que todo conhecimento é inserido e distribuído para o sistema especialista, esse pode então, em tempo real, inferir a classificação da situação de

emergência da usina para a sala de comando. Como já mencionado, existem informações que não se encontram disponíveis no sistema de monitoramento, e portanto, se transformam em perguntas ao operador, marcado pela cor roxa. A partir desse ponto, a interface exibida nesse trabalho é a do SISD de Angra I, para ser operada na sala de controle.

Figura 4.3: Pergunta ao operador na interface do SISD

Além disso, nota-se na figura 4.3 que a categoria A se encontra na cor vermelha. Esse é um indicativo de que um dos seus blocos constituintes apresentam classificação de EMERGÊNCIA GERAL. Por outro lado, a categoria S, figura 4.4, apresenta a cor roxa, indicando uma pendência de resposta do operador. Ao clicar na categoria desejada, pode-se ainda observar a classificação da situação de emergência para cada diagrama constituinte da categoria.

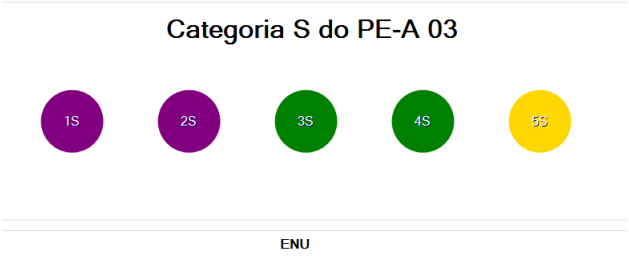

Figura 4.4: Classificações na categoria S na interface do SISD

Por fim, deve-se lembrar que como o sistema atua em tempo real, as classificações e pendências de resposta do operador podem mudar automaticamente sem interação com o sistema.

4.2 Apresentação do Módulo de Suporte ao Diagnóstico de Causa-raiz de desligamento

A base de conhecimento do módulo de suporte ao diagnóstico de causa raiz de desligamento é composto por árvores lógicas, ou seja, relações lógicas entre alarmes e/ou parâmetros que ativam o desligamento de segurança da usina. De mesma forma como no módulo previamente apresentado, as informações sobre tais relações são inseridas na base de conhecimento e posteriormente distribuídas para o SE. A estrutura lógica exemplo, na figura 4.5, será utilizada para explicar o funcionamento do módulo de suporte e possíveis implicações de seu diagnóstico.

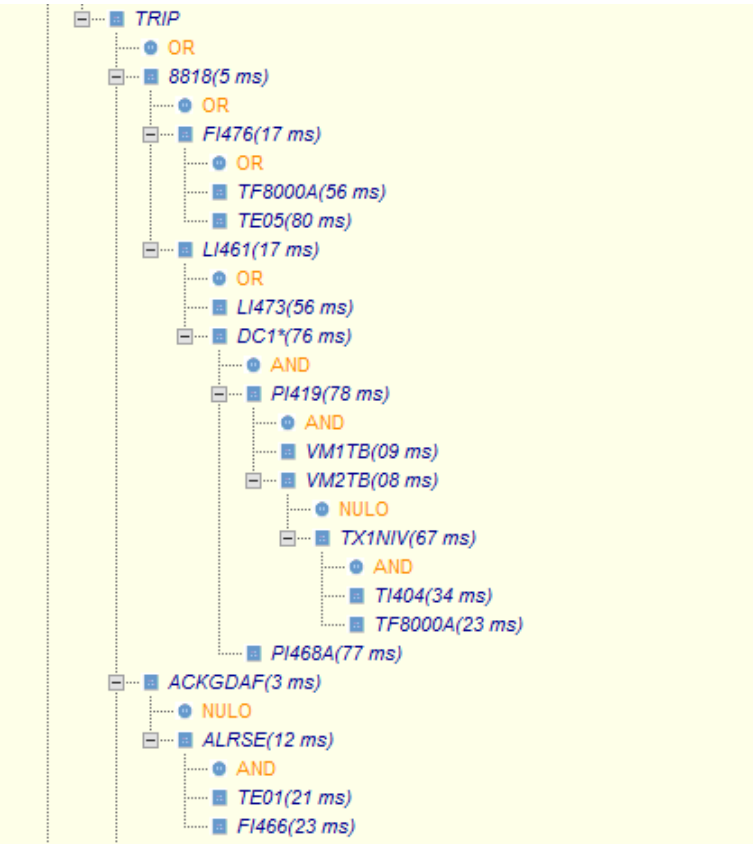

Figura 4.5: Exemplo de conhecimento de desligamento na interface da base de conhecimento

Para adição das relações lógicas e temporais, a estruturação é feita por determinação de cada nó pai, seus respectivos nós filho, operador e relação temporal como mostra a figura 4.6.

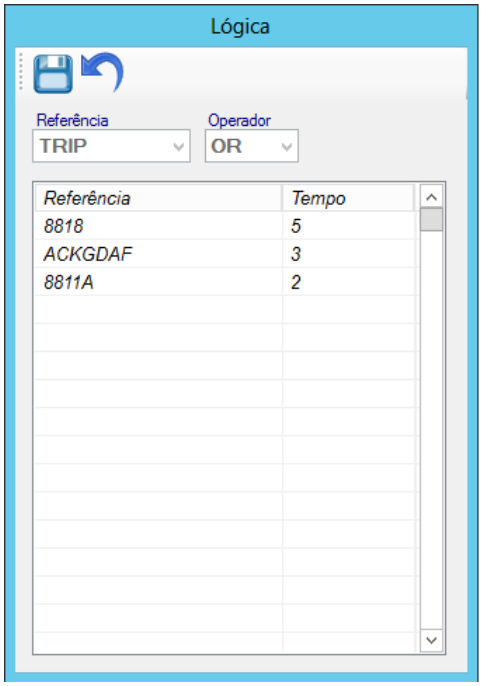

Figura 4.6: Formação da árvore na interface da base de conhecimento

Uma vez distribuída para o SE, o módulo de suporte ao diagnóstico é ativado sempre que ocorre o desligamento do reator e consequentemente uma sequência de eventos é gerada para alimentação do SE. Enquanto isso não ocorre, o módulo fica em espera. A seguir, a ferramenta de suporte ao diagnóstico é ativada e entrega para a interface do SISD a resposta de seu diagnóstico.

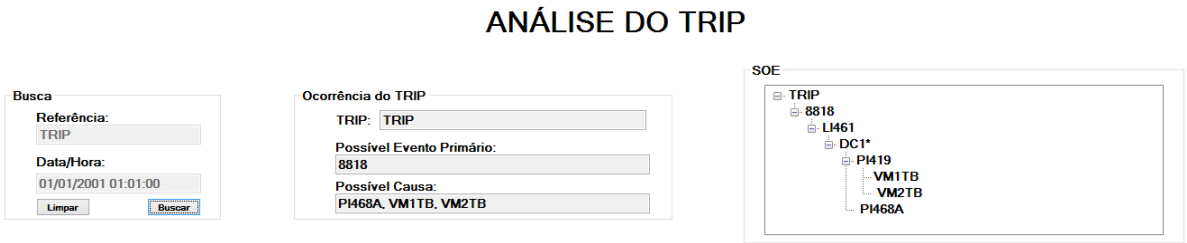

Figura 4.7: Diagnóstico do módulo de suporte ao diagnóstico de desligamento na interface do SISD

No Apêndice D se encontra a sequência de eventos utilizada para simular o diagnóstico na figura acima.

A Figura 4.7 mostra como deve ser lido o diagnóstico do sistema. Na área "Ocorrência do TRIP" são expostas três informações para auxiliar o operador. Em "TRIP", mostra-se o evento topo que causou o desligamento; em "Possível Evento Primário", mostra-se o evento ou eventos de profundidade 1 que levaram ao acionamento do evento em "TRIP"; em "Possíveis Causas" são exibidas por fim, os eventos de maior profundidade, encontrados no SOE, que podem facilitar no diagnóstico da causa-raiz do desligamento. No lado direito, em SOE, exibe-se o ramo percorrido até chegar no evento topo de desligamento.

Os resultados exibidos na tela não são necessariamente a causa-raiz de desligamento na usina, porém servem como guia para os operadores chegarem a uma possível causa. No exemplo, nota-se que foi dado em "Possíveis Causas" alarmes do tipo VM1TB e VM2TB. Esses alarmes são indicadores de vibração do mancal das turbinas 1 e 2. A exibição de tais eventos devem ser investigados mais profundamente para se determinar a causa da vibração excessiva, podendo indicar a necessidade de troca de algum componente, que por fim, seria a causa-raiz do problema.

Capítulo 5

Conclusões

Os modelo computacional apresentado nesse trabalho, o sistema especialista, é um de vários métodos para diagnóstico e classificação. Cada problema estudado ou aplicação real deve corresponder o tipo de problema com o melhor modelo aplicável para o caso. Tal correspondência é dependente de como a informação está disponível ao usuário, como a representação lógica pode ser feita com o intuito de cobrir completamente todos os cenários possíveis do problema e por fim, como o processo de inferência e racionalização do problema é feito. O Sistema de Suporte ao Diagnóstico vêm com o intuito de suprir a necessidade de automatização de processos lógicos durante a operação da usina, tanto para diminuir a carga de trabalho dos operadores, como para facilitar a resposta a situações adversas.

Nesse cenário, a aplicação de um sistema especialista se mostrou a mais viável devido a sua capacidade de aliar velocidade de processamento da informação a maior facilidade de representação das informações necessárias para modelar o problema em regras e árvores. O propósito do sistema é servir como suporte às operações na sala de controle e por esse motivo, não se deve utilizar suas respostas sozinhas como base para decisões críticas. Além disso, vale ressaltar a diferente atuação dos módulos constituintes do sistema. O módulo de classificação de situação de emergência, devido a existência de uma documentação da usina que estrutura os procedimentos a serem feitos para determinação da situação, tem capacidade de fazer o diagnóstico completo, uma vez que todas as informações necessárias estão disponíveis para o SE. Por outro lado, o módulo de suporte ao diagnóstico de desligamento tem como base o conhecimento dos operadores que se baseiam em acontecimentos passados e por

isso, muitas vezes são incompletos. Dessa forma, o diagnóstico serve apenas como um direcionamento a análise da causa-raiz de desligamento.

Buscando otimizar o aproveitamento do sistema, estuda-se a possibilidade de implementação de uma ferramenta de análise estatística de eventos para alimentação da base de conhecimento do módulo de suporte ao diagnóstico de desligamento. Vogel-Heuser *et al.*[27] propõe a aplicação de um método de reconhecimento de padrões em avalanche de alarmes, baseado em dados coletados por sistemas automatizados de produção. O reconhecimento de padrões seria feito a partir da análise de frequência de sequência de notificações do sistema de alarmes. Por fim, uma análise mais aprofundada dessas sequências poderia estruturar ramos de árvores de eventos e consequentemente se inferir suas relações lógicas.

Atualmente, em prol do reconhecimento e divulgação do trabalho, o módulo de suporte ao diagnóstico de causa-raiz foi aceito para apresentação na *International Conference on Applied Mathematics and Computer Science* em Roma, Itália.

Referências Bibliográficas

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, ***Power Reactor Information System***. *https://www.iaea.org/pris/*

[2] WORLD NUCLEAR ASSOCIATION, ***Information Library***. *http://www.world-nuclear.org/information-library/*

[3] NUCLEAR ENERGY INSTITUTE, ***World Statistics***. *http://www.nei.org/Knowledge-Center/Nuclear-Statistics/World-Statistics*

[4] MINISTÉRIO DE MINAS E ENERGIA, ***Balanço Energético Nacional, Relatório Final 2016***. *https://ben.epe.gov.br*

[5] ELETRONUCLEAR, ***Central Nuclear Angra 3***. *http://www.eletronuclear.gov.br/aempresa/centralnuclear/angra3.aspx*

[6] PETRANGELI, G., ***Nuclear Safety***. Elsevier Butterworth-Heinemann, 2006

[7] ALVARENGA, M. A. B., *Diagnóstico do Desligamento de um Reator Nuclear atraés de Técnicas Avançadas de Inteligência Artificial*, Tese de D.sc, COPPE/UFRJ, Rio de Janeiro, RJ, Brasil, 1997.

[8] SALMON, D., *Sistema Especialista baseado em Níveis Progressivos de Diagnóstico para Identificação de Acidentes em Usina Nuclear PWR*, DissertaÃ§Ã£o de Mestrado, COPPE/UFRJ, Rio de Janeiro, RJ, Brasil, 2013.

[9] MEDEIROS, J. A. C. C., SCHIRRU, R., "Identification of nuclear power plant transients using the Particle Swarm Optimization algorithm", ***Annals of Nuclear Energy***, v. 35, pp. 576–582, 2008.

[10] NICOLAU, A. S., SCHIRRU, R., "QDPSO and Minkowski Distance Applied to Transient Diagnosis System" ***ICAART 2014 - Proceedings of the 6th***

International Conference on Agents and Artificial Intelligence, v. 1, pp. 611–616, 2014.

[11] NICOLAU, A. S., SCHIRRU, R., "A New Methodology for Diagnosis System with Don't Know Response for Nuclear Power Plant" ***Annals of Nuclear Energy***, v. 100, pp. 91–97, 2017.

[12] PYTHON, ***About Python***. *https://www.python.org/about/*

[13] GLASSTONE, S., SESONSKE, A., ***Nuclear Reactor Engineering*** *Reactor Systems Engineering*. Chapman & Hall, Inc. 1994

[14] Engineering Equipment and Materials User's Association, ***Alarm Systems*** *A guide to design, management and procurement*. EEMUA, 1999

[15] RUSSEL, S., NORVIG, P., ***Inteligência Artificial***. 2ed, Elsevier, 2004

[16] FRANKISH, K., RAMSEY, W. M., Cambridge University, ***The Cambridge Handbook of Artificial Intelligence***. Cambridge University Press, 2014

[17] SILVEIRA, P. C., R., *Robô baseado em Tecnologia Celular Android e Lógica Nebulosa para Inspeção e Monitoração em Usinas Nucleares*, DissertaÃ§Ã£o de Mestrado, COPPE/UFRJ, Rio de Janeiro, RJ, Brasil, 2013.

[18] AGHINA, M. A. C., MÓL, A. C. A., LANDAU, L., JORGE, C. A. F., CUNHA, G. G., LAPA, C. M F., ESPÍRITO SANTO, A. C., PEREIRA, C. M. N. A., FREITAS, V. G. G., NOMIYA, D. V., "Non-conventional Interfaces for Human-system Interaction in Nuclear Plants Virtual Simulations" ***Progress in Nuclear Energy(New Series)***, v. 59, pp. 33–43, 2012.

[19] CÂMARA AUGUSTO, J. P. S. C., NICOLAU, A. S., SCHIRRU, R., "PSO with Dynamic Topology and Random Keys method applied to Nuclear Reactor Reload" ***Progress in Nuclear Energy(New Series)***, v. 83, pp. 191–196, 2015, ELSEVIER.

[20] NOVÁK, V., PERFILIEVA, I., MOČKOŘ, J., ***Mathematical Principles of Fuzzy Logic***. Kluwer Academic, 1999

[21] U.S NUCLEAR REGULATORY COMISSION, ***NUREG-0492,*** *Fault Tree Handbook*. 1981

[22] HAYES-ROTH, F., WATERMAN, D. A., LENAT, D. B., ***Building Expert Systems*** ADDISON-WESLEY PUBLISHING COMPANY, INC 1983

[23] MCDERMOTT, J., "R1: A rule-based configurer of computer systems.", ***Technical Report, Department of Computer Science. Carnegie-Mellon University, Pittsburgh, Pa.***,

[24] LINDSAY, R. K., BUCHANAN, B. G., FEIGENBAUM, E. A., LEDERBERG, J., ***The DENDRAL project***, McGraw-Hill, New York

[25] POPLE, H. E., Jr. MYERS, J. D., MILLER, R. A., ***DIALOG: A model of diagnostic logic for internal medicine.***, IJCAI 4, pp. 848–855, 1975

[26] FEIGENBAUM, E. A., ***The art of artificial intelligence: Themes and case studies of knowledge engineering***, IJCAI 5, pp. 1014-1029, 1977

[27] VOGEL-HEUSER, B., SCHUTZ, D., FOLMER, J., "Criteria-based alarm flood pattern recognition using historical data from automated production systems (aPs)" ***Mechatronics***, v. 31, pp. 89–100, 2015, ELSEVIER.

Apêndice A

CNEN NN 1.14 - Notificação de Eventos

4.7 RELATÓRIO DE PARADA

4.7.1 Após cada *Parada* da usina, deverá ser apresentado um *Relatório de Parada - RP*, abrangendo:

a) o Programa ALARA, incluindo, para as atividades de maior impacto radiológico, as metas previstas e os valores atingidos para a dose coletiva e a dose média dos trabalhadores. Em caso de não alcance dessas metas, esse fato deve ser justificado;
b) as principais ocorrências com impacto na área de Proteção Radiológica;
c) a quantidade de rejeitos radioativos sólidos gerados, por tipo de rejeito;
d) as atividades dos efluentes líquidos e gasosos liberados e a dose *no grupo crítico*;
e) as modificações de projeto implementadas;
f) o programa de treinamento; e
g) os resultados da Inspeção em Serviço.

4.7.2 Referir como foram utilizadas as experiências de *Paradas* anteriores na atual programação.

4.7.3 Apresentar uma visão crítica das atividades desenvolvidas, incluindo seus pontos positivos e negativos, e as recomendações para a próxima *Parada*, objetivando a redução de doses;

4.7.4 Comparar os valores atingidos durante a *Parada* com aqueles obtidos em *Paradas* anteriores, em termos de dose coletiva.

5. NOTIFICAÇÃO DE EVENTOS

5.1 REQUISITOS GERAIS

5.1.1 A *organização operadora* deverá notificar à *CNEN* a ocorrência de:

a) Declaração de situação de emergência;
b) *Eventos* não iniciadores de situação de emergência ou que ainda não tenham sido identificados como tal.

5.1.2 A *organização operadora* deverá manter um canal de comunicação aberto e contínuo com a *CNEN*, durante o curso do *evento* ou da situação de emergência.

5.1.3 A *organização operadora* deverá notificar à *CNEN*, em tempo hábil, durante o curso do *evento* ou da situação de emergência:

a) qualquer degradação adicional no nível de *segurança* ou nas condições da *usina*, incluindo aquelas que requeiram ativação do Plano de Emergência, caso esse não tenha sido ativado anteriormente;
b) qualquer mudança de uma classe de emergência para outra;
c) informações sobre parâmetros relevantes para a caracterização do nível de *segurança* da *usina*;
d) resultados relevantes de análises de condições e comportamento da *usina*;
e) a identificação da necessidade da adoção de qualquer ação de proteção, que divirja de uma condição da *Autorização para Operação* ou de uma *especificação técnica* necessária para proteger a saúde e a *segurança* do público. Essa notificação deve ser feita antes da ação protetora ser executada ou, não sendo exeqüível, o mais breve possível após o fato consumado;
f) a eficácia das respostas automáticas ou das medidas de proteção tomadas;
g) informações relativas ao comportamento da *usina* que não tenha sido adequadamente interpretado;
h) a declaração de encerramento do *evento* ou da situação de emergência.

5.2 EVENTOS INICIADORES DE SITUAÇÃO DE EMERGÊNCIA

A *organização operadora* deve notificar à *CNEN*, tão logo quanto possível e no prazo máximo de uma hora, a declaração de qualquer situação de emergência.

5.3 EVENTOS NÃO INICIADORES DE SITUAÇÃO DE EMERGÊNCIA

Quando o *evento* não promover a declaração de situação de emergência ou ainda não tenha sido identificado como tal, a O*rganização Operadora* deve notificar à *CNEN*, tão logo quanto possível e no prazo máximo de uma ou quatro horas, conforme aplicável, a ocorrência de qualquer dos *eventos* relacionados

abaixo:

5.3.1 Notificações em até 1 hora:

1. Início de qualquer desligamento da unidade requerido pelas *especificações técnicas.*
2. Qualquer desvio das e*specificações técnicas,* realizado intencionalmente, necessário para garantir a *segurança* do público e do meio ambiente, quando nenhuma ação, consistente com as condições da *autorização para operação*, puder proporcionar, de imediato, uma proteção adequada ou equivalente.
3. Qualquer *evento* ou condição, durante a operação, que possa levar a *usina*, incluindo suas principais barreiras de *segurança*, a uma condição seriamente degradada, incluindo:
    a. Uma condição não analisada que comprometa significativamente a sua *segurança*; ou
    b. Uma condição fora das *bases de projeto*; ou
    c. Uma condição não coberta por procedimentos de operação ou de emergência.
4. Qualquer fenômeno natural ou outra condição externa, que possa levar a uma ameaça real à *segurança* da *usina*, ou dificulte significativamente a execução das tarefas necessárias à operação segura da mesma.
5. Circunstância de perda ou redução da capacidade de avaliação de uma eventual emergência.[1]
6. Circunstância de perda ou redução da capacidade de comunicação ou acesso, que possa comprometer a execução do Plano de Emergência Local.
7. Qualquer *evento* que possa levar a uma ameaça real à *segurança* da *usina* ou dificulte significativamente a execução das atividades necessárias para a operação segura da *usina*, incluindo incêndio, liberação de gases tóxicos e ou liberação de radioatividade.

5.3.2 Notificações em até 4 horas:

1. Qualquer *evento* em que, estando o reator desligado, tenha sido identificada uma configuração que, caso o reator estivesse em operação, teria colocado a *usina*, incluindo suas principais barreiras de *segurança*, numa condição seriamente degradada ou em uma condição não analisada que poderia comprometer significativamente a *segurança* da *usina*.
2. Qualquer *evento* ou condição que resulte em uma atuação automática ou manual indevida, de qualquer *função de segurança*, incluindo o sistema de proteção do reator, exceto quando a atuação resulta de uma atividade previamente planejada durante testes ou operação do reator.
3. Qualquer *evento* ou condição que, isoladamente, poderia ter impedido o cumprimento das *funções de segurança* das estruturas ou sistemas necessários para:
    a) desligar o reator e mantê-lo em uma condição segura em desligado; ou
    b) remover o calor residual; ou
    c) controlar a liberação de material radioativo; ou
    d) mitigar as conseqüências de um *acidente*.

6. RELATÓRIOS DE EVENTOS

6.1 A *organização operadora* deve submeter à *CNEN* um relatório dos *eventos*, no prazo máximo de 30 dias após a descoberta do mesmo, para qualquer *evento* classificado segundo a subseção 6.2. desta norma.

6.1.1 A *organização operadora* deve relatar o *evento* independentemente do modo de operação da *usina,* do nível de potência, da estrutura, do sistema ou do componente onde se iniciou o *evento*.

6.1.2 A *organização operadora* deve submeter à *CNEN*, no prazo de 30 dias, um relatório dos *eventos* que não se enquadrem nas classes da subseção 6.2, sempre que o *evento* seja considerado relevante para a *segurança*.

6.2. CLASSIFICAÇÃO DE EVENTOS

6.2.1 A *organização operadora* deve classificar os *eventos* da seguinte forma:

[1] por exemplo: perda de parte significativa dos indicadores ou instrumentos na sala de controle ou do Sistema de Monitoração dos Parâmetros de Segurança.

a) Classe 1: *Eventos* relacionados às e*specificações técnicas*:
   1) qualquer desligamento requerido pelas *Especificações Técnicas*; ou
   2) qualquer operação ou condição não permitida pelas e*specificações técnicas*, de acordo com a norma CNEN-NE-1.26, item 4.6; ou
   3) qualquer desvio das e*specificações técnicas,* realizado intencionalmente, necessário para garantir a *segurança* do público e do meio ambiente, quando nenhuma ação, consistente com as condições da *Autorização para Operação*, puder proporcionar de imediato uma proteção adequada ou equivalente, conforme a norma CNEN-NE-1.04.

b) Classe 2: Qualquer *evento* que tenha levado a *usina*, incluindo suas principais barreiras de *segurança,* a uma condição seriamente degradada ou a:
   1) uma condição não analisada que tenha comprometido de forma significativa a *segurança* da *usina*;
   2) uma condição fora das *bases de projeto* da *usina*; ou
   3) uma condição não coberta pelos procedimentos de operação ou de emergência da *usina.*

c) Classe 3: Qualquer fenômeno natural ou outra condição externa que tenha levado a uma ameaça real à *segurança* da *usina,* ou dificultado a execução das tarefas necessárias à operação segura da *usina*.

d) Classe 4: Qualquer *evento* que tenha resultado em uma atuação automática ou manual de qualquer *dispositivo técnico de segurança*, incluindo o sistema de proteção do *reator*, exceto quando:
   1) a atuação resultou de uma atividade previamente planejada durante testes ou operação do *reator*;
   2) a atuação não foi prevista e:
      — ocorreu enquanto o sistema estava corretamente fora de serviço; ou
      — ocorreu após a *função de segurança* ter sido realizada.

e) Classe 5: Qualquer *evento*[2] que, sozinho, poderia ter impedido a realização da *função de segurança* de sistemas e estruturas, necessária para:
   1) desligar o *reator* e mantê-lo numa condição segura em desligado; ou
   2) remover o calor residual; ou
   3) controlar a liberação de material radioativo; ou
   4) mitigar as conseqüências de um *acidente*.

f) Classe 6: Qualquer *evento* no qual uma causa única ou condição que tenha provocado a inoperabilidade de um componente ou grupo de componentes em um único trem ou canal redundante em mais de um sistema de *segurança*, ou a inoperabilidade de canais ou trens redundantes em um mesmo sistema.
   1) desligar o *reator* e mantê-lo numa condição segura em desligado; ou
   2) remover o calor residual; ou
   3) controlar a liberação de material radioativo; ou
   4) mitigar as conseqüências de um *acidente*.

g) Classe 7: Qualquer liberação de efluentes radioativos por via aérea, que possa expor o público a níveis de radiação que acarretam doses superiores aos limites primários estabelecidos para indivíduos do público, de acordo com a Norma CNEN-NE-3.01.

h) Classe 8: Qualquer liberação de efluentes líquidos radioativos, que possa expor o público a níveis de radiação que acarretem doses superiores aos limites primários estabelecidos para indivíduos do público, de acordo com a Norma CNEN-NE-3.01.

i) Classe 9: Qualquer *evento* que tenha levado a uma ameaça real à *segurança* da *usina* ou que tenha dificultado significativamente os seus trabalhadores de executarem as tarefas necessárias para a operação segura do *reator*, incluindo incêndio, liberação de gases tóxicos ou liberação de radioatividade.

6.3 REQUISITOS DE RELATÓRIO

6.3.1 IDENTIFICAÇÃO

O relatório deverá conter os seguintes requisitos de identificação:

a) Nome da unidade onde o evento ocorreu;

b) Título do evento, incluindo uma descrição concisa do principal problema ou assunto associado ao evento;

[2] Os *eventos* abrangidos nesta Classe 5 podem incluir um ou mais erros de procedimento, *falhas* de equipamentos e/ou descoberta de deficiências no projeto, na análise, na fabricação ou na construção. Entretanto, *falhas* individuais de componentes não precisam ser relatadas neste item, caso o equipamento redundante nesse mesmo sistema esteja operável e disponível para realizar a função de *segurança* para o qual foi projetado.

c) Data do evento;
d) Número do relatório;
e) Modo de operação da unidade - como definido nas Especificações Técnicas - no momento em que ocorreu o evento;
f) Percentual da potência nuclear autorizada na qual o reator estava operando quando ocorreu o evento;
g) Classificação do evento segundo a escala INES da agência internacional de energia atômica;
h) Quando o evento for classificado como emergência, colocar a identificação da classe de acordo com o plano de emergência;
i) Classe de *evento* desta Norma em que o mesmo se enquadra e que requereu a emissão do relatório;

6.3.2 CONTEÚDO

O conteúdo do relatório deve incluir:

a) uma descrição do *evento,* contendo:

1) uma narração clara e específica do evento tal que os leitores familiarizados com o projeto de reatores nucleares, mas não familiarizados com o projeto da usina em particular, possam entendê-lo completamente . Essa descrição, sob o ponto de vista da operadora, deve incluir desenhos, figuras, gráficos, tabelas, fotografias e outros recursos que permitam um completo entendimento do evento.
2) as seguintes informações específicas sobre o *evento* em questão:
   i) condições de operação da *usina* antes do *evento*;
   ii) condições das estruturas, componentes ou sistemas que estavam inoperáveis no início do *evento* e que contribuíram para o mesmo;
   iii) data e hora aproximada das ocorrências;
   iv) a *causa-raiz* de cada *falha* de componente ou sistema ou de erro pessoal, se conhecida;
   v) modo de *falha*, o mecanismo (causa imediata) e/ou o efeito de cada componente que falhou, se conhecidos;
   vi) a função de cada componente e o nome dos sistema referidos no relatório, de acordo com a nomenclatura utilizada na *usina*.
   vii) para *falhas* de componentes com múltiplas funções, a inclusão da lista dos sistemas ou funções secundárias que também foram afetados;
   viii) para *falhas* que causaram a inoperabilidade de um trem de um sistema de *segurança*, o tempo estimado desde a descoberta da *falha* até o trem ter retornado à condição de *operável*;
   ix) o método de descoberta de cada *falha* do componente ou sistema ou do erro de procedimento;
   x) as ações do operador que afetaram o curso do *evento*, incluindo erros de operadores, deficiências em procedimentos, ou ambos, que contribuíram para o *evento*. Para cada erro de operador, a *organização operadora* deve discutir:
   — se o erro foi um erro cognitivo (por exemplo, *falha* em reconhecer a condição atual da *usina* ou a natureza do evento *ou* em perceber quais sistemas deveriam estar funcionando,) ou um erro de procedimento;
   — se o erro foi contrário ao estabelecido em um procedimento aprovado, se foi um resultado direto de um erro em um procedimento aprovado ou se estava associado com uma atividade ou tarefa não coberta por um procedimento aprovado;
   — qualquer característica não usual do local de trabalho (por exemplo, calor, ruído) que diretamente contribuiu para o erro; e
   — a qualificação do pessoal envolvido;
   xi) respostas de sistemas de *segurança* iniciadas automática ou manualmente e;
   xii) a identificação de cada componente que falhou durante o *evento*;

b) Uma avaliação das conseqüências do *evento* para a *segurança* e suas implicações. Essa avaliação deve incluir a disponibilidade de outros sistemas ou componentes que poderiam ter realizado a mesma função que aqueles que falharam durante o *evento*;
c) A descrição das ações corretivas planejadas como resultado do *evento*, incluindo aquelas que objetivam reduzir a probabilidade de que *eventos* similares ocorram no futuro;
d) Referência a *eventos* similares ocorridos anteriormente na *usina*, discutindo, quando for o caso, o porquê das ações corretivas adotadas não terem evitado a repetição do *evento*.

6.4 DISPOSIÇÕES COMPLEMENTARES

A *organização operadora* poderá requerer à *CNEN*, com uma justificativa adequada, exceções aos requisitos de relatório.

Apêndice B

NEI 99.01 - Classificação de Situação de Emergência

3.7 Emergency Classification Level Descriptions

There are three considerations related to emergency classification levels. These are:

(1) The potential impact on radiological safety, either as known now or as can be reasonably projected;

(2) How far the plant is beyond its predefined design, safety, and operating envelopes; and

(3) Whether or not conditions that threaten health are expected to be confined to within the site boundary.

The ICs deal explicitly with radiological safety impact by escalating from levels corresponding to releases within regulatory limits to releases beyond EPA Protective Action Guideline (PAG) plume exposure levels. In addition, the "Discussion" sections below include off-site dose consequence considerations that were not included in NUREG-0654 Appendix 1.

NOTIFICATION OF UNUSUAL EVENT (NOUE):

Events are in progress or have occurred which indicate a potential degradation of the level of safety of the plant or indicate a security threat to facility protection has been initiated. No releases of radioactive material requiring off-site response or monitoring are expected unless further degradation of safety systems occurs.

Discussion: Potential degradation of the level of safety of the plant is indicated primarily by exceeding plant technical specification Limiting Condition of Operation (LCO) allowable action statement time for achieving required mode change. Precursors of more serious events should also be included because precursors do represent a potential degradation in the level of safety of the plant. Minor releases of radioactive materials are included. In this emergency classification level, however, releases do not require monitoring or off-site response.

ALERT:

Events are in progress or have occurred which involve an actual or potential substantial degradation of the level of safety of the plant or a security event that involves probable life threatening risk to site personnel or damage to site equipment because of HOSTILE ACTION. Any releases are expected to be limited to small fractions of the EPA PAG exposure levels.

Discussion: Rather than discussing the distinguishing features of "potential degradation" and "potential substantial degradation," a comparative approach would be to determine whether increased monitoring of plant functions is warranted at the Alert level as a result of safety system degradation. This addresses the operations staff's need for help, independent of whether an actual decrease in plant safety is determined. This increased monitoring can then be used to better determine the actual plant safety state, whether escalation to a higher emergency classification level is warranted, or whether de-escalation or termination of the emergency classification level declaration is warranted. Dose consequences from these events are small fractions of the EPA PAG plume exposure levels.

SITE AREA EMERGENCY (SAE):

Events are in progress or have occurred which involve actual or likely major failures of plant functions needed for protection of the public or HOSTILE ACTION that results in intentional damage or malicious acts; 1) toward site personnel or equipment that could lead to the likely failure of or; 2) that prevent effective access to, equipment needed for the protection of the public. Any releases are not expected to result in exposure levels which exceed EPA PAG exposure levels beyond the site boundary.

Discussion: The discriminator (threshold) between Site Area Emergency and General Emergency is whether or not the EPA PAG plume exposure levels are expected to be exceeded outside the site boundary. This threshold, in addition to dynamic dose assessment considerations discussed in the EAL guidelines, clearly addresses NRC and off-site emergency response agency concerns as to timely declaration of a General Emergency.

GENERAL EMERGENCY (GE):

Events are in progress or have occurred which involve actual or IMMINENT substantial core degradation or melting with potential for loss of containment integrity or HOSTILE ACTION that results in an actual loss of physical control of the facility. Releases can be reasonably expected to exceed EPA PAG exposure levels off-site for more than the immediate site area.

Discussion: The bottom line for the General Emergency is whether evacuation or sheltering of the general public is indicated based on EPA PAGs, and therefore should be interpreted to include radionuclide release regardless of cause. In addition, it should address concerns as to uncertainties in systems or structures (e.g. containment) response, and also events such as waste gas tank releases and severe spent fuel pool events postulated to occur at high population density sites. To better assure timely notification, EALs in this category must primarily be expressed in terms of plant function status, with secondary reliance on dose projection. In terms of fission product barriers, loss of two barriers with loss or potential loss of the third barrier constitutes a General Emergency.

3.8 Emergency Classification Level Thresholds

The most common bases for establishing these boundaries are the technical specifications and setpoints for each plant that have been developed in the design basis calculations and the Final Safety Analysis Report (FSAR).

For those conditions that are easily measurable and instrumented, the boundary is likely to be the EAL (observable by plant staff, instrument reading, alarm setpoint, etc.) that indicates entry into a particular emergency classification level. For example, the main steam line radiation monitor may detect high radiation that triggers an alarm. That radiation level also may be the setpoint that closes the Main Steam Isolation Valves (MSIV) and initiates the reactor trip/scram. This same radiation level threshold, depending on plant specific parameters, also may be the appropriate EAL for a direct entry into an emergency classification level.

In addition to the continuously measurable indicators, such as coolant temperature, coolant levels, leak rates, containment pressure, etc., the FSAR provides indications of the consequences associated with design basis events. Examples would include steam pipe breaks, MSIV malfunctions, and other anticipated events that, upon occurrence, place the plant immediately into an emergency classification level.

Another approach for defining these boundaries is the use of a plant specific probabilistic safety assessment (PSA - also known as probabilistic risk analysis, PRA). PSAs have been completed

for all individual plants PSAs can be used as a good first approximation of the relevant ICs and risk associated with emergency conditions for existing plants. Each plant has an Individual Plant Evaluation (IPE) and an Individual Plant Evaluation for External Events (IPEEE). Generic insights from a PSA/ PRA, the IPE, IPEEE and related severe accident assessments which apply to EALs and emergency classification level determinations are:

1. Core damage frequency at many BWRs is dominated by sequences involving prolonged loss of all AC power. In addition, prolonged loss of all AC power events are extremely important at PWRs. This would indicate that should this occur, and AC power is not restored within 15 minutes, entry into the emergency classification level at no lower than a Site Area Emergency, when the plant was initially at power, would be appropriate. This implies that precursors to loss of all AC power events should appropriately be included in the EAL structure.

2. For severe core damage events, uncertainties exist in phenomena important to accident progressions leading to containment failure. Because of these uncertainties, predicting containment integrity may be difficult in these conditions. This is why maintaining containment integrity alone following sequences leading to severe core damage may be an insufficient basis for not escalating to a General Emergency.

3. PRAs show that leading contributors to latent fatalities were containment bypass, large LOCA with early containment failure, Station Blackout longer than 6 hours (e.g., LOCA consequences of Station Blackout), and reactor coolant pump seal failure. This indicates that generic EAL methodology must be sufficiently rigorous to address these sequences in a timely fashion.

Another critical element of the analysis to arrive at these threshold (boundary) conditions is the time that the plant might stay in that condition before moving to a higher emergency classification level. In particular, station blackout coping analyses performed in response to 10 CFR 50.63 and Regulatory Guide 1.155, "Station Blackout," may be used to determine whether a specific plant enters a Site Area Emergency or a General Emergency directly, and when escalation to General Emergency is indicated. The time dimension is critical to the EAL since the purpose of the emergency classification level for state and local officials is to notify them of the level of mobilization that may be necessary to handle the emergency. This is particularly true when a Site Area Emergency or General Emergency is IMMINENT. Establishing EALs for such conditions must take estimated evacuation time into consideration to minimize the potential for the plume to pass while evacuation is underway.

Regardless of whether or not containment integrity is challenged, it is possible for significant radioactive inventory within containment to result in EPA PAG plume exposure levels being exceeded even assuming containment is within technical specification allowable leakage rates. With or without containment challenge, however, a major release of radioactivity requiring off-site protection actions from core damage is not possible unless a major failure of fuel cladding allows radioactive material to be released from the core into the reactor coolant. NUREG-1228, "Source Estimations During Incident Response to Severe Nuclear Power Plant Accidents," indicates that such conditions do not exist when the amount of clad damage is less than 20%.

3.9 Emergency Action Levels

Planned evolutions involve preplanning to address the limitations imposed by the condition, the performance of required surveillance testing, and the implementation of specific controls prior to knowingly entering the condition in accordance with the specific requirements of the site's Technical Specifications. Activities which cause the site to operate beyond that allowed by the site's Technical Specifications, planned or unplanned, may result in an EAL threshold being met or exceeded. Planned evolutions to test, manipulate, repair, perform maintenance or modifications to systems and equipment that result in an EAL value being met or exceeded are not subject to classification and activation requirements as long as the evolution proceeds as planned and is within the operational limitations imposed by the specific operating license. However, these conditions may be subject to the reporting requirements of 10 CFR 50.72.

Classifications are based on evaluation of each Unit. All classifications are to be based upon valid indications, reports or conditions. Indications, reports or conditions are considered valid when they are verified by (1) an instrument channel check, or (2) indications on related or redundant indications, or (3) by direct observation by plant personnel, such that doubt related to the indication's operability, the condition's existence, or the report's accuracy is removed. Implicit in this definition is the need for timely assessment.

With the emergency classification levels defined, the thresholds that must be met for each EAL to be placed under the emergency classification level can be determined. There are two basic approaches to determining these EALs. EALs and emergency classification level boundaries coincide for those continuously measurable, instrumented ICs, such as radioactivity, core temperature, coolant levels, etc. For these ICs, the EAL will be the threshold reading that most closely corresponds to the emergency classification level description using the best available information.

For discrete (discontinuous) events, the approach will have to be somewhat different. Typically, in this category are internal and external hazards such as FIRE or earthquake. The purpose for including hazards in EALs is to assure that station personnel and off-site emergency response organizations are prepared to deal with consequential damage these hazards may cause. If, indeed, hazards have caused damage to safety functions or fission product barriers, this should be confirmed by symptoms or by observation of such failures. Therefore, it may be appropriate to enter an Alert status for events approaching or exceeding design basis limits such as Operating Basis Earthquake (OBE), design basis wind loads, FIRE within VITAL AREAS, etc. This would give the operating staff additional support and improved ability to determine the extent of plant damage. If damage to barriers or challenges to Critical Safety Functions (CSFs) have occurred or are identified, then the additional support can be used to escalate or terminate the emergency classification level based on what has been found. Of course, security events must reflect potential for increasing security threat levels.

Plant emergency operating procedures (EOPs) are designed to maintain and/or restore a set of CSFs which are listed in the order of priority for restoration efforts during accident conditions. While the actual nomenclature of the CSFs may vary among plants, generally the PWR CSF set includes:

- Subcriticality
- Core cooling
- Heat sink
- Pressure-temperature-stress (RCS integrity)
- Containment

- RCS inventory

There are diverse and redundant plant systems to support each CSF. By monitoring the CSFs instead of the individual system component status, the impact of multiple events is inherently addressed, e.g., the number of operable components available to maintain the critical safety function.

The EOPs contain detailed instructions regarding the monitoring of these functions and provides a scheme for classifying the significance of the challenge to the functions. In providing EALs based on these schemes, the emergency classification level can flow from the EOP assessment rather than being based on a separate EAL assessment. This is desirable as it reduces ambiguity and the time necessary to classify the event.

As an example, consider that the Westinghouse Owner's Group (WOG) Emergency Response Guidelines (ERGs) classify challenges as YELLOW, ORANGE, and RED paths. If the core exit thermocouples exceed 1200 degrees F or 700 degrees F with low reactor vessel water level, a RED path condition exists. The ERG considers a RED path as "... an extreme challenge to a plant function necessary for the protection of the public ..." This is almost identical to the present NRC NUREG-0654 description of a site area emergency, "... actual or likely failures of plant functions needed for the protection of the public ..." It reasonably follows that if any CSF enters a RED path, a Site Area Emergency exists. A general emergency could be considered to exist if core cooling CSF is in a RED path and the EOP function restoration procedures have not been successful in restoring core cooling.

Although the majority of the EALs provide very specific thresholds, the Emergency Director must remain alert to events or conditions that lead to the conclusion that exceeding the EAL is IMMINENT. If, in the judgment of the Emergency Director, an IMMINENT situation is at hand, the classification should be made as if the threshold has been exceeded. While this is particularly prudent at the higher emergency classification levels (as the early classification may provide for more effective implementation of protective measures), it is nonetheless applicable to all emergency classification levels.

3.10 Treatment of Multiple Events and Classification Level Upgrading

The above discussion deals primarily with simpler emergencies and events that may not escalate rapidly. However, usable EAL guidance must also consider rapidly evolving and complex events. Hence, emergency classification level upgrading and consideration of multiple events must be addressed.

When multiple simultaneous events occur, the emergency classification level is based on the highest EAL reached. For example, two Alerts remain in the Alert category. Or, an Alert and a Site Area Emergency is a Site Area Emergency. Further guidance is provided in RIS 2007-02, Clarification of NRC Guidance for Emergency Notifications During Quickly Changing Events.

Emergency classification level upgrading for multi-unit stations with shared safety-related systems and functions must also consider the effects of a loss of a common system on more than one unit (e.g. potential for radioactive release from more than one core at the same site). For example, many two-unit stations have their control panels for both units in close proximity within the same room. Thus, control room evacuation most likely would affect both units. There are a number of other systems and functions which may be shared at a given multi-unit station. This must be considered in the emergency classification level declaration and in the development of appropriate site specific ICs and EALs based on the generic EAL guidance.

Although the majority of the EALs provide very specific thresholds, the Emergency Director must remain alert to events or conditions that lead to the conclusion that exceeding the EAL is IMMINENT. If, in the judgment of the Emergency Director, an IMMINENT situation is at hand, the classification should be made as if the threshold has been exceeded. While this is particularly prudent at the higher emergency classification levels (as the early classification may provide for more effective implementation of protective measures), it is nonetheless applicable to all emergency classification levels.

3.11 Emergency Classification Level Downgrading

Another important aspect of usable EAL guidance is the consideration of what to do when the risk posed by an emergency is clearly decreasing. A combination approach involving recovery from General Emergency's and some Site Area Emergency's and termination from NOUEs, Alerts, and certain Site Area Emergency's causing no long term plant damage appears to be the best choice. Downgrading to lower emergency classification levels adds notifications but may have merit under certain circumstances.

3.12 Classifying Transient Events

For some events, the condition may be corrected before a declaration has been made. The key consideration in this situation is to determine whether or not further plant damage occurred while the corrective actions were being taken. In some situations, this can be readily determined, in other situations, further analyses (e.g., coolant radiochemistry sampling, may be necessary). Classify the event as indicated and terminate the emergency once assessment shows that there were no consequences from the event and other termination criteria are met.

Existing guidance for classifying transient events addresses the period of time of event recognition and classification (15 minutes). However, in cases when EAL declaration criteria may be met momentarily during the normal expected response of the plant, declaration requirements should not be considered to be met when the conditions are a part of the designed plant response, or result from appropriate Operator actions.

There may be cases in which a plant condition that exceeded an EAL was not recognized at the time of occurrence but is identified well after the condition has occurred (e.g., as a result of routine log or record review), and the condition no longer exists. In these cases, an emergency should not be declared.

Reporting requirements of 10 CFR 50.72 are applicable and the guidance of NUREG-1022, Event Reporting Guidelines 10 CFR 50.72 and 50.73, should be applied.

3.13 Operating Mode Applicability

The plant operating mode that existed at the time that the event occurred, prior to any protective system or operator action initiated in response to the condition, is compared to the mode applicability of the EALs. If an event occurs, and a lower or higher plant operating mode is reached before the emergency classification level can be declared, the emergency classification level shall be based on the mode that existed at the time the event occurred.

For events that occur in Cold Shutdown or Refueling, escalation is via EALs that have Cold Shutdown or Refueling for mode applicability, even if Hot Shutdown (or a higher mode) is entered during any subsequent heat-up. In particular, the fission product barrier EALs are applicable only to events that initiate in Hot Shutdown or higher.

MODE APPLICABILITY MATRIX

	Recognition Category						
Mode	**A**	**C**	**D**	**E**	**F**	**H**	**S**
Operating	X				X	X	X
Startup	X				X	X	X
Hot Standby	X				X	X	X
Hot Shutdown	X				X	X	X
Cold Shutdown	X	X				X	
Refueling	X	X				X	
Defueled	X	X				X	
None			X	X			

3.14 BWR Operating Modes (Follow site specific Technical Specifications)

Power Operations (1):	Mode Switch in Run
Startup (2):	Mode Switch in Startup/Hot Standby or Refuel (with all vessel head bolts fully tensioned)
Hot Shutdown (3):	Mode Switch in Shutdown, Average Reactor Coolant Temperature >200 °F
Cold Shutdown (4):	Mode Switch in Shutdown, Average Reactor Coolant Temperature ≤ 200 °F
Refueling (5):	Mode Switch in Shutdown or Refuel, and one or more vessel head bolts less than fully tensioned.
Defueled (None):	All reactor fuel removed from reactor pressure vessel. (Full core off load during refueling or extended outage).

3.15 PWR Operating Modes (Follow site specific Technical Specifications)

Power Operations (1):	Reactor Power > 5%, Keff ≥ 0.99
Startup (2):	Reactor Power ≤ 5%, Keff ≥ 0.99
Hot Standby (3):	RCS ≥ 350 °F, Keff < 0.99
Hot Shutdown (4):	200 °F < RCS < 350 °F, Keff < 0.99
Cold Shutdown (5):	RCS < 200 °F, Keff < 0.99
Refueling (6):	One or more vessel head closure bolts less than fully tensioned
Defueled (None):	All reactor fuel removed from reactor pressure vessel. (Full core off load during refueling or extended outage)

Apêndice C

Regras de classificação de situação de emergência categoria A

IF MODO_DE_OPERACAO == 1 THEN CATEGORIA_A = TRUE AND CATEGORIA_F = TRUE AND CATEGORIA_S = TRUE AND CATEGORIA_S = TRUE

IF MODO_DE_OPERACAO == 2 THEN CATEGORIA_A = TRUE AND CATEGORIA_F = TRUE AND CATEGORIA_S = TRUE AND CATEGORIA_S = TRUE

IF MODO_DE_OPERACAO == 3 THEN CATEGORIA_A = TRUE AND CATEGORIA_F = TRUE AND CATEGORIA_S = TRUE AND CATEGORIA_S = TRUE

IF MODO_DE_OPERACAO == 4 THEN CATEGORIA_A = TRUE

IF MODO_DE_OPERACAO == 5 THEN CATEGORIA_A = TRUE

IF CATEGORIA_A == TRUE AND (CATEGORIA_A == TRUE) THEN RESP_PEA_CAT_2A = "PER-OP: QUEDA NÃO PLANEJADA DE NIVEL DE ÁGUA EM ÁREAS DE RECARREGAMENTO - VER NOTA 1 - E AUMENTO DA LEITURA VÁLIDA E NÃO PLANEJADA R02/R05 OU AUMENTO POR UM FATOR DE 1000 NOS NIVEIS NORMAIS DE LEITURA - VER NOTA 2- VÁLIDA E NÃO PLANEJADA EM QUALQUER MONITOR DE ÁREA OU EM MEDIÇÃO RADIOMÉTRICA DE CAMPO?" AND COR_PEA_CAT_2A = "ROXO" AND CAIXA_NUM_2A = 1

IF CATEGORIA_A == TRUE AND (MOEFLU1 == 1) THEN CAIXA_1_1A = TRUE

IF CATEGORIA_A == TRUE AND (CAIXA_1_2A <> "") THEN RESP_PEA_CAT_2A = "PER-OP: COMBUSTÍVEL IRRADIADO DESCOBERTO OU A DESCOBRIR FORA DO VASO DO REATOR OU ALARME VÁLIDO DO R02 - R05 DEVIDO A DANO EM COMBUSTÍVEL IRRADIADO OU ALARME VÁLIDO DO R02 - R05 DEVIDO A PERDA DE NÍVEL EM ÁREAS DE RECARREGAMENTO - VER NOTA 1 - OU TAXA DE DOSE MAIOR QUE 0.15 MILISIVERT/HORA NA SALA DE CONTROLE OU NA ESTAÇÃO DE CONTROLE DE ALARMES - ECA-1" AND COR_PEA_CAT_2A = "ROXO" AND CAIXA_NUM_2A = 2

IF CATEGORIA_A == TRUE AND (CAIXA_1_1A <> "" AND MOEFLU2 == 1) THEN CAIXA_2_1A = TRUE AND AUX_1A = 1

IF CATEGORIA_A == TRUE AND (CAIXA_NUM_2A == 1 AND COR_PEA_CAT_2A == "ROXO" AND PER_OP_RET_1_2A == TRUE) THEN CAIXA_1_2A = TRUE

IF CATEGORIA_A == TRUE AND (CAIXA_NUM_2A == 2 AND COR_PEA_CAT_2A == "ROXO" AND PER_OP_RET_2_2A == TRUE) THEN CAIXA_2_2A = TRUE

IF CATEGORIA_A == TRUE AND (CONT_1A_LIGA == 1) THEN COR_PEA_CAT_1A = "MARRON" AND RESP_PEA_CAT_1A = "AGUARDANDO"

IF CATEGORIA_A == TRUE AND (CAIXA_NUM_2A == 1 AND COR_PEA_CAT_2A == "ROXO" AND PER_OP_RET_1_2A == FALSE) THEN CAIXA_1_2A = FALSE

IF CATEGORIA_A == TRUE AND (CAIXA_2_1A <> "" AND AUX_1A_1 == 1 AND AUX_1A == 1) THEN CAIXA_3_1A = TRUE AND AUX_1A = 2

IF CATEGORIA_A == TRUE AND (CAIXA_NUM_2A == 2 AND COR_PEA_CAT_2A == "ROXO" AND PER_OP_RET_2_2A == FALSE) THEN CAIXA_2_2A = FALSE

IF CATEGORIA_A == TRUE AND (CAIXA_2_2A == TRUE) THEN RESP_PEA_CAT_2A = "ALERTA" AND COR_PEA_CAT_2A = "LARANJA"

IF CATEGORIA_A == TRUE AND (CONT_1A_2_LIGA == 1) THEN COR_PEA_CAT_1A = "MARRON" AND RESP_PEA_CAT_1A = "AGUARDANDO"

IF CATEGORIA_A == TRUE AND (CAIXA_1_2A == TRUE AND CAIXA_2_2A == TRUE) THEN RESP_PEA_CAT_2A = "ALERTA" AND COR_PEA_CAT_2A = "LARANJA"

IF CATEGORIA_A == TRUE AND (CAIXA_3_1A <> "" AND AUX_1A_1 == 2 AND AUX_1A == 2) THEN CAIXA_4_1A = TRUE

IF CATEGORIA_A == TRUE AND (CAIXA_1_2A == TRUE AND CAIXA_2_2A == FALSE) THEN RESP_PEA_CAT_2A = "ENU" AND COR_PEA_CAT_2A = "AMARELO"

IF CATEGORIA_A == TRUE AND (MOEFLU1 <> 1) THEN RESP_PEA_CAT_1A = "PER_OP: LEITURA VÁLIDA EM QUALQUER MONITOR DE EFLUENTES > 2 VEZES O VALOR DE AJUSTES DO ALARME - NA LLE- POR >=60 MIN OU CONCENTRAÇÕES OU TAXAS LIBERAÇÃO > 2 VEZES O LIMTE DO MCRMA POR >= 60 MIN CONFIRMADAS POR ANALISES DE AMOSTRAS" AND COR_PEA_CAT_1A = "ROXO" AND CAIXA_NUM_1A = 1

IF CATEGORIA_A == TRUE AND (CAIXA_1_2A == FALSE AND CAIXA_2_2A == FALSE) THEN RESP_PEA_CAT_2A = "CONDIÇÃO NORMAL" AND COR_PEA_CAT_2A = "VERDE"

IF CATEGORIA_A == TRUE AND (MOEFLU2 <> 1 AND CAIXA_1_1A <> "") THEN CAIXA_NUM_1A = 2 AND AUX_1A = 1 AND RESP_PEA_CAT_1A = "PER-OP: LEITURA VÁLIDA EM QUALQUER MONITOR DE EFLUENTES > 200 VEZES O VALOR DE AJUSTE DO ALARME - NA LLE- POR > = 15 MIN OU CONCENTRAÇÕES OU TAXAS DE LIBERAÇÃO > 200 VEZES O LIMTE DO MCRMA POR > = 15 MIN CONFIRMADAS POR ANÁLISES DE AMOSTRAS?" AND COR_PEA_CAT_1A = "ROXO"

IF CATEGORIA_A == TRUE AND (GCRREAL < 18000000 AND CAIXA_2_1A <> "") THEN AUX_1A = 2 AND CAIXA_NUM_1A = 3 AND COR_PEA_CAT_1A = "ROXO" AND RESP_PEA_CAT_1A = "PER-OP: AVALIAÇÃO DE DOSE NO SITIO OU ALEM DESTE > 1 miliSivert DET OU > 5 miliSivert DEC TIREOIDE OU MEDIÇÃO RADIOMÉTRICA DE CAMPO NO SITIO OU ALEM DESTE COM TAXA DE DOSE GAMA > 1 miliSivert/H E ESPERADAS CONTINUAR POR > = 60 MIN OU ANÁLISES DE AMOSTRAS DE INSPEÇÃO DE CAMPO NO SITIO OU ALEM DESTE > 5 miliSivert DEC TIREOIDE POR UMA HORA DE INALAÇÃO "

IF CATEGORIA_A == TRUE AND (GCRREAL < 18000000 AND CAIXA_3_1A <> "" AND AUX_1A == 2) THEN RESP_PEA_CAT_1A = "PER-OP: AVALIAÇÃO DE DOSE NO SITIO OU ALEM DESTE > 10 miliSivert DET OU > 50 miliSivert DEC TIREOIDE OU MEDIÇÃO RADIOMÉTRICA DE CAMPO NO SITIO OU ALEM DESTE COM TAXA DE DOSE GAMA > 10 miliSivert/H E ESPERADAS CONTINUAR POR > = 60 MIN OU ANÁLISES DE AMOSTRAS DE INSPEÇÃO DE CAMPO NO SITIO OU ALEM DESTE > 50 miliSivert DEC TIREOIDE POR UMA HORA DE INALAÇÃO" AND COR_PEA_CAT_1A = "ROXO" AND CAIXA_NUM_1A = 4

IF CATEGORIA_A == TRUE AND (CAIXA_NUM_1A == 1 AND COR_PEA_CAT_1A == "ROXO" AND PER_OP_RET_1_1A == TRUE) THEN CAIXA_1_1A = TRUE

IF CATEGORIA_A == TRUE AND (CAIXA_NUM_1A == 2 AND COR_PEA_CAT_1A == "ROXO" AND PER_OP_RET_2_1A == TRUE) THEN CAIXA_2_1A = TRUE AND AUX_1A = 1

IF CATEGORIA_A == TRUE AND (CAIXA_NUM_1A == 3 AND COR_PEA_CAT_1A == "ROXO" AND PER_OP_RET_3_1A == TRUE) THEN CAIXA_3_1A = TRUE AND AUX_1A = 2

IF CATEGORIA_A == TRUE AND (CAIXA_NUM_1A == 4 AND COR_PEA_CAT_1A == "ROXO" AND PER_OP_RET_4_1A == TRUE) THEN CAIXA_4_1A = TRUE

IF CATEGORIA_A == TRUE AND (CAIXA_NUM_1A == 1 AND COR_PEA_CAT_1A == "ROXO" AND PER_OP_RET_1_1A == FALSE) THEN CAIXA_1_1A = FALSE

IF CATEGORIA_A == TRUE AND (CAIXA_NUM_1A == 2 AND COR_PEA_CAT_1A == "ROXO" AND PER_OP_RET_2_1A == FALSE) THEN CAIXA_2_1A = FALSE AND AUX_1A = 1

IF CATEGORIA_A == TRUE AND (CAIXA_NUM_1A == 3 AND COR_PEA_CAT_1A == "ROXO" AND PER_OP_RET_3_1A == FALSE) THEN CAIXA_3_1A = FALSE AND AUX_1A = 2

IF CATEGORIA_A == TRUE AND (CAIXA_NUM_1A == 4 AND COR_PEA_CAT_1A == "ROXO" AND PER_OP_RET_4_1A == FALSE) THEN CAIXA_4_1A = FALSE

IF CATEGORIA_A == TRUE AND (CAIXA_4_1A == TRUE) THEN RESP_PEA_CAT_1A = "EMERGENCIA GERAL" AND COR_PEA_CAT_1A = "VERMELHO"

IF CATEGORIA_A == TRUE AND (CAIXA_1_1A == TRUE AND CAIXA_2_1A == TRUE AND CAIXA_3_1A == TRUE AND CAIXA_4_1A == TRUE) THEN RESP_PEA_CAT_1A = "EMERGENCIA GERAL" AND COR_PEA_CAT_1A = "VERMELHO"

IF CATEGORIA_A == TRUE AND (CAIXA_1_1A == TRUE AND CAIXA_2_1A == TRUE AND CAIXA_3_1A == TRUE AND CAIXA_4_1A == FALSE) THEN RESP_PEA_CAT_1A = "EMERGENCIA DE AREA" AND COR_PEA_CAT_1A = "MAGENTA"

IF CATEGORIA_A == TRUE AND (CAIXA_1_1A == TRUE AND CAIXA_2_1A == TRUE AND CAIXA_3_1A == FALSE AND CAIXA_4_1A == FALSE) THEN RESP_PEA_CAT_1A = "ALERTA" AND COR_PEA_CAT_1A = "LARANJA"

IF CATEGORIA_A == TRUE AND (CAIXA_1_1A == TRUE AND CAIXA_2_1A == FALSE AND CAIXA_3_1A == TRUE AND CAIXA_4_1A == FALSE) THEN RESP_PEA_CAT_1A = "EMERGENCIA DE AREA" AND COR_PEA_CAT_1A = "MAGENTA"

IF CATEGORIA_A == TRUE AND (CAIXA_1_1A == TRUE AND CAIXA_2_1A == FALSE AND CAIXA_3_1A == FALSE AND CAIXA_4_1A == FALSE) THEN RESP_PEA_CAT_1A = "ENU" AND COR_PEA_CAT_1A = "AMARELO"

IF CATEGORIA_A == TRUE AND (CAIXA_1_1A == FALSE AND CAIXA_2_1A == TRUE AND CAIXA_3_1A == TRUE AND CAIXA_4_1A == FALSE) THEN RESP_PEA_CAT_1A = "EMERGENCIA DE AREA" AND COR_PEA_CAT_1A = "MAGENTA"

IF CATEGORIA_A == TRUE AND (CAIXA_1_1A == FALSE AND CAIXA_2_1A == TRUE AND CAIXA_3_1A == FALSE AND CAIXA_4_1A == FALSE) THEN RESP_PEA_CAT_1A = "ALERTA" AND COR_PEA_CAT_1A = "LARANJA"

IF CATEGORIA_A == TRUE AND (CAIXA_1_1A == FALSE AND CAIXA_2_1A == FALSE AND CAIXA_3_1A == TRUE AND CAIXA_4_1A == FALSE) THEN RESP_PEA_CAT_1A = "EMERGENCIA DE AREA" AND COR_PEA_CAT_1A = "MAGENTA"

IF CATEGORIA_A == TRUE AND (CAIXA_1_1A == FALSE AND CAIXA_2_1A == FALSE AND CAIXA_3_1A == FALSE AND CAIXA_4_1A == FALSE) THEN RESP_PEA_CAT_1A = "CONDIÇÃO NORMAL" AND COR_PEA_CAT_1A = "VERDE"

IF CATEGORIA_A == TRUE AND (GCRREAL >= 18000000) THEN CONT_1A_LIGA = 1

IF CATEGORIA_A == TRUE AND (CONT_1A_LIGA == 1 AND CONT_1A_CONTADOR >= 900) THEN AUX_1A_1 = 1

IF CATEGORIA_A == TRUE AND (GCRREAL >= 18000000) THEN CONT_1A_2_LIGA = 1

IF CATEGORIA_A == TRUE AND (CONT_1A_2_LIGA == 1 AND CONT_1A_2_CONTADOR >= 900) THEN AUX_1A_1 = 2

Apêndice D

Sequência de eventos para simulação

PACONTD
(2016,12,27,18,00,00,02) FI476 1
(2016,12,27,18,00,00,02) DPADRD 1
(2016,12,27,18,00,00,04) VM2TB 1
(2016,12,27,18,00,00,06) VM1TB 1
(2016,12,27,18,00,00,06) FI477 1
(2016,12,27,18,00,00,09) PI468A 1
(2016,12,27,18,00,00,10) NAPZRD 1
(2016,12,27,18,00,00,10) PI419 1
(2016,12,27,18,00,00,14) LI461 1
(2016,12,27,18,00,00,15) 8811A 1
(2016,12,27,18,00,00,16) 8818 1
(2016,12,27,18,00,00,18) TRIP 1
(2016,12,27,18,00,00,20) BFBRRD 1
(2016,12,27,18,00,00,21) PACONTD 1
(2016,12,27,18,00,00,22) B62_G1 1
(2016,12,27,18,00,00,24) B61_G1 1
(2016,12,27,18,00,00,27) GA101 1
(2016,12,27,18,00,00,34) DAXBDRD 1

Onde PACONTD é o evento que indica desligamento do reator, sendo como base de filtro dos eventos que ocorreram antes dele. O número ao lado da referência é o valor assumido pela variável binária.