COPPE/UFRJ

UMA ABORDAGEM DA REGULAMENTAÇÃO COM INFORMAÇÃO DO RISCO DA ANÁLISE DE SEGURANÇA DE SISTEMAS DE INSTRUMENTAÇÃO E CONTROLE DIGITAL APLICADOS A CENTRAIS NUCLEARES

Paulo Adriano da Silva

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

Orientador: Paulo Fernando Ferreira Frutuoso e Melo

Rio de Janeiro

Março de 2010

UMA ABORDAGEM DA REGULAMENTAÇÃO COM INFORMAÇÃO DO RISCO DA ANÁLISE DE SEGURANÇA DE SISTEMAS DE INSTRUMENTAÇÃO E CONTROLE DIGITAL APLICADOS A CENTRAIS NUCLEARES

Paulo Adriano da Silva

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

Examinada por:

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

Prof. Antonio Carlos Marques Alvim, Ph.D.

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

Prof. Marcio Nele de Souza, D.Sc.

Dr. Sérgio de Queiroz Bogado Leite, Ph.D.

RIO DE JANEIRO, RJ - BRASIL

MARÇO DE 2010

Silva, Paulo Adriano

Uma abordagem da regulação com informação do risco da análise de segurança de sistemas de instrumentação e controle digital aplicados a centrais nucleares/ Paulo Adriano da Silva. – Rio de Janeiro: UFRJ/COPPE, 2010.

XIV, 136 p.: il.; 29,7 cm.

Orientador: Paulo Fernando Ferreira Frutuoso e Melo

Tese (doutorado) – UFRJ/ COPPE/ Programa de Engenharia Nuclear, 2010.

Referencias Bibliográficas: p. 95-105.

1. Sistemas de Instrumentação e Controle Digital 2. Defesa em Profundidade e Diversidade. 3. Informação do Risco. I. Melo, Paulo Fernando Ferreira Frutuoso e. II. Universidade Federal do Rio de Janeiro, COPPE, Programa de Engenharia Nuclear. III. Titulo.

Bem aventurado o homem que encontra sabedoria, e o homem que adquire conhecimento. (Provérbios 3 : 13)

AGRADECIMENTOS

A Deus, pela oportunidade de fazer o Doutorado.

Ao Professor Paulo Fernando Ferreira Frutuoso e Melo pela aceitação de minha solicitação de orientação, pela amizade iniciada e desenvolvida ao longo destes anos, pelo respeito e pela confiança.

Ao Dr. Pedro Luiz da Cruz Saldanha, pela amizade, confiança, parceria, respeito, conhecimento e sabedoria durante este projeto. Sem sua participação esta tese de doutorado seria impossível.

A minha esposa Giovana Karin Pádua da Silva, pelo carinho e incentivo em continuar.

Aos Engenheiros Eustério Benitiz Furieri e João Márcio Lima do Nascimento da CNEN, pelo apoio, suporte e incentivo.

Aos membros da banca avaliadora, profissionais de grande competência, com cujas valiosas contribuições tive a honra de contar para enriquecer este trabalho.

Aos meus amigos e colegas da CNEN pelo incentivo e apoio.

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

UMA ABORDAGEM DA REGULAMENTAÇÃO COM INFORMAÇÃO DO RISCO DA ANÁLISE DE SEGURANÇA DE SISTEMAS DE INSTRUMENTAÇÃO E CONTROLE DIGITAL APLICADOS A CENTRAIS NUCLEARES

Paulo Adriano da Silva

Março/2010

Orientador: Paulo Fernando Ferreira Frutuoso e Melo

Programa: Engenharia Nuclear

Este trabalho apresenta uma proposta de metodologia baseada na informação do risco para a avaliação da I & C digital, utilizando o estudo de eventos operacionais ocorridos em usinas nucleares junto com o conceito de defesa em profundidade e diversidade, que servirá de complemento à atual abordagem determinística e de base para a tomada de decisão do licenciamento dessa nova tecnologia digital, considerando que as metodologias para incorporar as probabilidades de falhas de sistemas digitais em uma avaliação probabilística de segurança (APS) específica, estão em processo de desenvolvimento e validação.

Esta abordagem possibilita identificar os principais tipos de falhas de sistemas I & C digitais, com potencial para as falhas de causa comum (FCC), como também a avaliação dos modos de falha dominantes. Desta forma, possibilita definir medidas defensivas que resultem em ações reguladoras para minimizar possíveis vulnerabilidades do sistema de I & C digital.

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

A RISK-INFORMED REGULATORY APPROACH TO THE SAFETY ANALYSIS OF DIGITAL INSTRUMENT AND CONTROL SYSTEMS OF NUCLEAR POWER PLANTS

Paulo Adriano da Silva

March/2010

Advisor: Paulo Fernando Ferreira Frutuoso e Melo

Department: Nuclear Engineering

This thesis proposes a methodology based on risk information to evaluate digital I & C systems, considering the study of operational events occurring in nuclear power plants together with the concept of defense in depth and diversity, which will complement the current deterministic approach and the basis for the decision-making of the licensing of new digital technology, considering that methodologies for incorporating the probabilities of failures of digital systems in a specifically probabilistic safety assessment (PSA) are still under development and validation.

This approach makes it possible to identify the main failures types of digital I & C systems, with the potential for common-cause failures (CCF), as well as evaluating the dominant failure modes. It allows for defining countermeasures that will result in regulatory actions to minimize potential vulnerabilities of digital I & C systems.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

LISTA DE SIGLAS

ABWR	*Advanced Boiling Water Reactor*
AIChE	*American Institute of Chemical engineers*
ANS	*American Nuclear Society*
ANSI	*American National Standards Institute*
APS	Avaliação Probabilística de Segurança
ASME	*American Society of Mechanical Engineers*
ASTM	*American Society for Testing Materials*
BRR	Bombas de Refrigeração do Reator
BTP	*Branch Technical Position*
CE	*Combustion Engineering Inc.*
CFR	*Code of Federal Regulations, USA*
CNEN	Comissão Nacional de Energia Nuclear
CPCS	*Core Protection Calculation System*
D3	*Defense-in-Depth and Diversity*
DFM	*Dynamic Flowgraphs Methodology*
DNB	*Departure from Nucleate Boiling*
DTS	Dispositivos Técnicos de Segurança
EDA	*Efficient Decomposition and Aggregation*
EPR	*European Pressurized Water Reactor*
EPRI	*Electric Power Research Institute*
FCC	Falha de Causa Comum
FH	Falha de Hardware
FIHS	Falha da Interface Homem-Sistema
FS	Falha Simples
FSAR	*Final Safety Analysis Report*
FSOFT	Falha de Software
GV	Gerador de Vapor
HPS	*Health Physics Society*
I & C	Instrumentação e Controle
IAEA	*International Atomic Energy Agency*
IEEE	*Institute for Electrical and Electronics Engineers*

IEC	*International Electrotechnical Commission*
IHS	Interface Homem-Sistema
INMM	*Institute of Nuclear Materials Management*
INPO	*Institute of Nuclear Power Operations*
IRS	*Incident Reporting System*
ISA	*Integrated Safety Assessment;*
KTA	*Kerntechnischer Ausschuss (German Committee for Nuclear Technologies)*
LER	*License Event Report*
LOCA	*Loss of Coolant Accident*
MAFIC-D	Monitoração e Avaliação de Falhas de Instrumentação e Controle Digital
NPI	*Nuclear Power International*
NRC	*Nuclear Regulatory Commission*
NSAC	*Nuclear Safety Analysis Center*
PLC	*Programmable Logic Controller*
PWR	*Pressurized Water Reactor*
RAS	Relatório de Avaliação de Segurança
SPR	Sistema de Proteção do Reator
SRP	*Standard Review Plan*
SRR	Sistema de Refrigeração do Reator
TECDOC	*Technical Document*
VGB	*Vereinigung der Grosskraftwerksbeatrieber*
V&V	Verificação e Validação
WANO	*World Association of Nuclear Operators*

1 INTRODUÇÃO

1.1 APRESENTAÇÃO

O desenvolvimento na área de instrumentação e controle (I & C), durante os últimos 25 anos, tem sido muito rápido. Foram introduzidos os sistemas digitais com desempenho melhorado em vários setores da indústria, como por exemplo: instalações químicas, usinas de exploração e refino de petróleo, usinas térmicas, instalações automotivas, etc. Estes novos sistemas de I & C tiram proveito da tecnologia digital, tendo tratamento sofisticado e eficiente de medidas e sinais de controle, com velocidade de resposta alta, confiabilidade, flexibilidade e versatilidade.

A adoção desta tecnologia tem sido mais lenta em usinas nucleares. A razão foi devido aos esforços em obter evidências que comprovassem que os sistemas de I & C digital podem ser usados com segurança em sistemas aplicados à segurança nuclear, como, por exemplo, o Sistema de Proteção do Reator (SPR), garantindo o correto funcionamento de todas as suas funções.

Muitas usinas nucleares foram modernizadas e outras planejam fazer a modernização de sua I & C, motivadas principalmente pela:

- Obsolescência de equipamentos analógicos e a dificuldade de se encontrar peças de reposição;
- Como parte do projeto de extensão da vida útil qualificada;
- Possibilidade de introduzir novas funções que melhorem e auxiliem a segurança e operação da usina, como por exemplo, uma Interface Homem-Sistema (IHS) mais amigável.

Atualmente, os novos reatores em construção estão sendo projetados com I & C digital.

Embora a I & C digital em usinas nucleares esteja, em parte, incentivada por obsolescência de equipamento analógico, o problema de obsolescência não desaparecerá com a implantação de equipamento digital, pois devido ao rápido desenvolvimento tecnológico da I & C digital, a obsolescência pode ser até mesmo um problema maior com equipamento digital do que com o equipamento analógico. Com isso, os usuários de equipamento de I & C digital devem estar atentos para assegurar a operabilidade do sistema de I & C durante toda a vida útil da instalação.

1.2 OBJETIVO

Em usinas nucleares, o uso de computadores e software tem crescido muito, em parte devido à obsolescência dos equipamentos analógicos e também devido à necessidade de melhorar e assegurar níveis satisfatórios de disponibilidade e segurança da instalação. Hoje em dia, os softwares são encontrados em aplicações relacionadas à segurança (Sistema de Proteção do Reator – SPR) e também em aplicações de controle e monitoração (computador de processo da usina).

O uso de software em usinas nucleares não é novo. Banco de dados, sistemas de supervisão paralela (por exemplo: software de funções críticas de segurança), programas de cálculo (por exemplo: programas de cálculos de neutrônica e termohidráulica) e controles de tarefas, são chamados de software essenciais. Cada vez mais os computadores ficam padronizados e comuns, minimizando a obsolescência e possibilitando a substituição dos mesmos devido a mau funcionamento ou envelhecimento.

O software usado em I & C digitais de Sistemas de Proteção do Reator são menos comuns, mas muitos países já introduziram essa nova tecnologia. Estes incluem Canadá, França, Coréia do Sul, Suécia, Reino Unido, Republica Tcheca, Hungria, Japão, Alemanha entre outros, havendo, no entanto, preocupações

significativas sobre a introdução de software na indústria nuclear, devido à confiabilidade, integridade e desempenho.

Desde a década de 90, têm havido fortes argumentos que questionam a segurança de aplicações de sistemas digitais em centrais nucleares. O relatório publicado em 1997 pelo *National Research Council* (NAP,1997) resume estes argumentos. O relatório destaca que métodos apropriados para a avaliação da segurança e confiabilidade são as chaves para estabelecer a aceitabilidade da instrumentação digital (I & C) em sistemas de segurança e controle de centrais nucleares. Os sistemas críticos de segurança em uma usina nuclear adotam os conceitos de redundância e monitoração para tolerância à falha e estes conceitos podem ser adaptados a sistemas digitais.

Os sistemas digitais oferecem para as centrais nucleares uma melhora potencial na segurança e confiabilidade, considerando o aumento da confiabilidade do hardware e a capacidade de detectar falhas. Entretanto, existem limitações na orientação e no consenso da modelagem da confiabilidade dos softwares dos sistemas digitais.

As metodologias para incorporar as probabilidades de falhas de sistemas digitais em uma avaliação probabilística de segurança (APS) específica, tais como: *Dynamic Flowgraphs Methodology (DFM)* e Markov (NRC, 2005), estão em processo de desenvolvimento e validação.

Na ausência de modelos probabilísticos dinâmicos que sejam utilizados na APS, podem-se buscar métodos que utilizem a informação do risco complementando os estudos determinísticos já incorporados ao projeto.

A abordagem proposta nessa tese tem por base a informação do risco e consiste em avaliar os eventos operacionais utilizando o relacionamento entre os seguintes critérios de confiabilidade: falha, tipo de falha, taxa de falha, níveis de defesa em profundidade e diversidade (Apêndices A e B).

O objetivo dessa abordagem é possibilitar a identificação dos principais modos de falhas dos sistemas digitais, com potencial para as falhas de causa comum (FCC) no software, possíveis vulnerabilidades do sistema de I & C digital, como também a avaliação das causas dominantes destes modos de falha.

Uma vez identificada a falha dos sistemas digitais, pode-se verificar o impacto que ela pode causar na segurança da instalação e em que pontos do projeto o sistema digital pode estar vulnerável, observando as quebras de barreiras de segurança definidas na metodologia de defesa em profundidade e diversidade (*Defense-in Depth and Diversity - D3*). Desta forma, os dados de eventos operacionais de usinas nucleares poderão complementar a atual abordagem determinística e servirão de base para a tomada de decisão ao licenciamento dessa nova tecnologia digital.

O tratamento dos dados de falha, retirado da experiência operacional, permitirá também comparações de desempenho dos sistemas I & C digitais entre usinas nucleares.

Como ferramenta de apoio à metodologia foi desenvolvido o programa MAFIC-D que facilita e auxilia a aplicação dos relacionamento entre os critérios de confiabilidade, a análise dos relacionamentos e a coleta de dados. Essa ferramenta é um software desenvolvido com a linguagem Visual Basic versão 6.0, na forma de um banco de dados.

1.3 ORGANIZAÇÃO DO TRABALHO

Esta tese está dividida em oito capítulos conforme descrito a seguir.

O Capítulo 2 apresenta uma revisão bibliográfica referente à área de avaliação de segurança para sistemas de instrumentação e controle digital de usinas nucleares, que serviram de base para esta tese.

O Capítulo 3 apresenta uma visão geral da estrutura do sistema de I & C analógico e digital de usinas nucleares e descreve as filosofias alemã e americana para o sistema de proteção do reator.

O Capítulo 4 descreve o processo de licenciamento para usinas nucleares no Brasil, mostrando os principais critérios adotados. Apresenta ainda um histórico do licenciamento dos sistemas digitais aplicado pela NRC em usinas americanas e as principais normas utilizadas.

O Capítulo 5 descreve as duas metodologias aplicadas à avaliação de defesa em profundidade (D3) de sistemas I & C digital: a metodologia apresentada pela NRC, que mostra uma abordagem determinística da avaliação defesa em profundidade e diversidade e a apresentada pelo EPRI, que mostra uma abordagem utilizando a Avaliação Probabilística de Segurança (APS) aplicando informação do risco.

O Capítulo 6 apresenta a metodologia proposta nesta tese, baseada na informação do risco para a avaliação da I & C digital, utilizando o estudo de eventos operacionais ocorridos em usinas nucleares em conjunto com o conceito de defesa em profundidade e diversidade (D3). Descreve o programa MAFIC-D, que foi a ferramenta construída para a aplicação da metodologia.

O Capítulo 7 apresenta os resultados gerados através do programa MAFIC-D utilizando o método proposto.

Finalmente, o Capítulo 8 apresenta as conclusões e contribuições deste trabalho e as novas direções para continuação desta linha de pesquisa.

O Apêndice A apresenta uma tabela dos relacionamentos dos critérios de confiabilidade.

O Apêndice B apresenta um fluxograma de bloco com todos os relacionamentos aplicados pela metodologia.

O Apêndice C apresenta a tabela com todos os eventos operacionais utilizados no programa MAFIC-D para a validação da metodologia proposta.

O Apêndice D mostra os requisitos mínimos que um relatório de evento operacional deve ter para que o analista possa retiras todas as informações requeridas para aplicar a metodologia proposta nesta tese.

O Apêndice E apresenta o código fonte do relacionamento dos critérios de confiabilidade do programa MAFIC-D.

2 REVISÃO BIBLIOGRÁFICA

O TECDOC-1016 (IAEA, 1998) identifica metodologias, orientações, processos, preocupações e boas práticas para ajudar na modernização de sistemas de I & C. Esse documento foi escrito a partir da experiência das operadoras de usinas nucleares na identificação da necessidade de modernização dos sistemas de I & C analógicos, com dificuldade de obtenção de peças de reposição e que foram projetados em sua maioria há mais de 30 anos, sendo substituídos, agora, por sistemas digitais mais modernos, com a preocupação de manter o desempenho e a segurança dos sistemas de segurança e operação da usina.

BASTL e BOCK (1998) apresentam as principais etapas do processo de qualificação e avaliação alemã (teste, normas e procedimentos) aplicado aos sistemas I & C digitais da Siemens (Teleperm XS/XP) importantes para a segurança, desenvolvido especificamente para aplicações em usinas nucleares.

O TECDOC-1066 (IAEA, 1999a) foi elaborado com a participação e a contribuição de peritos da Bélgica, França, Alemanha, Itália, República da Coréia, Suécia, Reino Unido e Estados Unidos, com o objetivo de desenvolver uma metodologia para a determinação de requisitos e especificações necessárias para o projeto de atualização do sistema de I & C analógico para sistema I & C digital.

O Technical Report 384 (IAEA, 1999b) fornece informações sobre a eficácia da Verificação e Validação (V&V) de sistemas de I & C baseados em computador e os métodos disponíveis para se fazer a V&V. Este documento trata principalmente dos softwares presentes em sistemas digitais importantes para a segurança e a operação de usinas nucleares.

FISCHER e PIEL (1999) mostram, com base no julgamento de engenharia, as medidas mais importantes para aumentar a independência dos trens redundantes de sistema I & C digital de segurança de uma usina nuclear. Este estudo traz uma

discussão objetiva sobre a necessária e justificável diversidade de sistema I & C digital de segurança, levando em consideração a experiência operacional.

O Safety Guide NS-G 1.1 (IAEA, 2000) traz orientações sobre os requisitos de segurança, projeto, V&V, instalação e comissionamento a ser utilizado para o software de sistemas importantes para a segurança em centrais nucleares, para todas as fases do ciclo de vida destes sistemas na usina. O foco principal do Safety Guide NS-G 1.1 é a preparação da documentação que será utilizada para uma adequada demonstração da segurança e confiabilidade dos sistemas importantes para a segurança baseados em computador.

SHIN *et alii* (2001) apresentam uma avaliação abrangente para demonstrar a capacidade dos reatores coreanos da nova geração de lidar com os eventos base de projeto simultaneamente com as falhas de causa comum (FCC) digitais dos Sistemas de Proteção do Reator (SPR). Uma metodologia de análise foi desenvolvida utilizando os eventos base de projeto acompanhado de FCC nos SPR digitais, categorizados como eventos além da base de projeto. O resultado demonstrou que uma variedade de meios diversos, tais como: sistemas alternativos de proteção, sistemas de controle e ações do operador são eficazes na mitigação de eventos base de projeto com FCC nos SPR digitais.

O Safety Guide NS-G 1.3 (IAEA, 2002a) fornece orientações sobre o projeto, Interface Homem-Sistema (IHS), identificação e classificação de sistemas de I & C importantes para a segurança nas centrais nucleares.

O TECDOC-1327 (IAEA, 2002b) fornece recomendações gerais para auxiliar as operadoras, os fornecedores e órgãos reguladores envolvidos no licenciamento de sistemas I & C digitais, com o objetivo de promover uma harmonização no licenciamento dos sistemas de I & C, aplicado à modernização da I & C, melhoramentos, substituição, nova instalação, e outros aspectos da I & C digital. O documento foi baseado no reconhecimento da diversidade presente no licenciamento de sistemas de I & C digital praticado por diversos países. O TECDOC-1327 foi o

primeiro passo no sentido de harmonizar o processo de obtenção de licença dessa nova tecnologia.

GARRETT e APOSTOLAKIS (2002) estudam uma abordagem para validar os requisitos de segurança de sistemas digitais baseada na Dynamic Flowgrafic Methodology (DFM) para fazer analises do risco. A DFM é uma abordagem desenvolvida para a modelagem e análise integrada dos componentes de hardware e software de um sistema. O objetivo da metodologia é complementar as abordagens tradicionais, que geralmente seguem a filosofia de separar as análises de confiabilidade de hardware e software. Essas análises podem ser usadas para identificar riscos desconhecidos no sistema de controle do reator. O método tem obtido êxito na identificação de mecanismos de falhas desconhecidos.

KANG e SUNG (2002) apresentam os resultados de um estudo de caso que analisa o projeto de um sistema de segurança digital através da técnica de árvore de falhas. O estudo de caso é executado para o sistema digital de proteção de reator de uisnas nucleares, com o objetivo de avaliar a segurança e a confiança do mesmo. O estudo demonstrou que alguns fatores, tais como: falha de causa comum, mecanismos mitigadores tolerantes a falhas e probabilidade de falha de software afetam notavelmente a segurança do sistema.

FLEMING e SILADY (2002) mostram definições de defesa em profundidade e propõem soluções para os problemas técnicos identificados no estudo, analisando as características do projeto do reator, a fim de empregar as estratégias de prevenção e mitigação de acidentes. A aplicação desta abordagem é demonstrada com o uso de exemplos de reatores a água pressurizada e reatores a alta temperatura resfriados a gás.

LI *et alii* (2002) apresentam um estudo de confiabilidade feito no primeiro reator de pesquisa chinês com sistema de proteção do reator (SPR) digital. O estudo demonstra que, para garantir a segurança, a confiabilidade e reduzir o risco, algumas medidas tiveram que ser tomadas. As medidas adotadas no processo de

desenvolvimento incluem: a arquitetura de defesa em profundidade, um hardware com padrão comercial e a separação de software de classe de segurança do software que não é de classe de segurança. Como resultado do estudo, o SPR digital demonstrou ser seguro e confiável e a autoridade reguladora chinesa começou a aplicar essa metodologia nas centrais nucleares de potência.

O TECDOC-1389 (IAEA, 2004b) fornece orientações e boas práticas de gerenciamento do projeto de modernização de I & C, incluindo a avaliação de todo o sistema de I & C para determinar o que pode ser mantido com sucesso e o que precisa ser modernizado. O TECDOC traz também duas abordagens para a modernização da I & C. A primeira, é a de desligar a usina e fazer de uma vez toda a modernização da I & C. A segunda abordagem é realizar a modernização da I & C durante as paradas para recarga de combustível. Este estudo foi elaborado devido à necessidade de modernização da I & C de muitas usinas nucleares que operam com seus sistemas há quase 30 anos, em geral, consistindo de tecnologia antiga, apresentando obsolescência, envelhecimento, problemas com peças de reposição e com o desempenho, bem como o aumento dos custos para manter um desempenho aceitável.

O TECDOC-1402 (IAEA, 2004b) aborda questões de envelhecimento e obsolescência dos sistemas de I & C em termos de gerenciamento do ciclo de vida da usina e renovação da licença de operação, não só do ponto de vista da segurança, mas também no contexto do custo de manutenção do sistema de I & C. O documento fornece as informações sobre o envelhecimento, obsolescência e o acompanhamento do desempenho dos equipamentos de I & C, que são classificados como equipamentos de segurança e/ou equipamentos relacionados com a segurança, operados em ambientes severos em centrais nucleares que são importantes no gerenciamento da vida útil da usina, não só para o funcionamento normal, mas também, e mais importante, para a operação pós-acidente.

LU e JIANG (2004) apresentam uma visão geral da aplicação da avaliação probabilística de segurança em três áreas dos sistemas de I & C digitais de usinas nucleares, garantia da qualidade, testes periódicos, e projeto da instrumentação e controle. O documento aborda também tópicos reguladores da aplicação da APS em centrais nucleares que adotam os sistemas de I & C digitais.

HUANG *et alii* (2007) analisam eventos de falha de software de I & C digital de usinas ABWR, utilizando com método baseado em simulação (PCTran-ABWR). O estudo de caso desta pesquisa inclui: (1) análise FCC de software para os principais sistemas de controle digitais; e (2) eventos postulados de falhas de software de I & C digital de ABWR que foram relatados à NRC (*Licensee Event Report - LER*) ou a IAEA (*Incident Reporting System - IRS*). O trabalho concluiu que este método pode investigar com mais detalhes o comportamento dinâmico do sistema de I & C digital do que outras abordagens. Algumas interações inesperadas podem ser observadas por este método, se o mesmo for bastante detalhado.

XING *et alii* (2007) abordam neste trabalho um modelo de análise de confiabilidade baseada em uma estrutura hierárquica para os sistemas baseados em computadores com falhas de causa comum (FCC). Este estudo concluiu que a análise de confiabilidade torna-se difícil quando existem dependências entre os componentes, introduzidas pelas FCC, observadas em componentes que estão em diferentes níveis hierárquicos.

KANG e JANG (2007) quantificam a segurança dos sistemas digitais de proteção do reator das usinas nucleares coreanas com base na Avaliação Probabilística de Segurança (APS). Quinze modelos de árvore de falhas para o Sistema de Desarme do Reator (SDR) e sete para os Dispositivos Técnicos de Segurança (DTS) foram construídos e integrados no modelo de avaliação de segurança da usina. O resultado do estudo de sensibilidade mostra os limites de risco da usina e os efeitos das falhas dos equipamentos digitais sobre o risco total da usina.

BICKEL (2008) resume uma revisão da experiência operacional da primeira geração de usinas nucleares nos Estados Unidos que utilizam sistemas digitais de proteção do reator. A experiência operacional acumulada de 1984 a 2006 dos sistemas de proteção reator da geração digital é de 1,27 milhões de horas (aproximadamente 145,5 anos). Com base nesta revisão da experiência operacional de sistemas digitais, uma série de cálculos de risco foi realizada para avaliar a segurança com estes eventos de falha observados. Com os resultados obtidos neste trabalho, foi possível estabelecer requisitos de confiabilidade para os sistemas de proteção do reator que podem ser relacionados com os objetivos reguladores de segurança e de experiência operacional.

CHUANG *et alii* (2008) apresentam um resumo dos requisitos reguladores que estão sendo aplicados no projeto dos sistemas digitais das duas usinas nucleares ABWR (*Lungmen Nuclear Power Plant – LMNPP*), que estão atualmente em construção em Taiwan. O sistema de instrumentação e controle de Lungmen é o sistema digital da Siemens. Além das principais questões reguladoras, o trabalho também aborda as lições aprendidas com o licenciamento do projeto do sistema de I & C digital de Lungmen.

MODARRES (2009) propõe e discute as implicações de uma estrutura reguladora, em grande parte probabilística, utilizando uma melhor estimativa, informação do risco, e métodos baseados no desempenho. Esta estrutura baseia-se na avaliação probabilística contínua do desempenho de sistemas críticos de segurança, estruturas, componentes e procedimentos que asseguram a realização de um amplo conjunto de tecnologias de proteção, mitigação e prevenção em todas as fases das operações da usina. A estrutura proposta utiliza a tradicional defesa em profundidade do projeto e a filosofia reguladora de operação.

ZITROU *et alii* (2010) propõem um modelo matemático que associa tópicos operacionais, gerenciais e de características de projeto de um sistema com susceptibilidade a eventos com falha causa comum (FCC). O modelo, conhecido como

Geometric Scaling (GS), permite investigar o efeito do risco em modificações de projeto de sistemas. Com base em uma estrutura bayesiana, o modelo GS permite a representação de incertezas, a atualização prévia de incertezas por meio de dados operacionais e das observações provenientes de diferentes sistemas.

PINTO (2010) apresenta uma aplicação da metodologia DFM (*Dynamic Flowgraph Methodology*) em um sistema digital de controle proposto para o pressurizador (PZR) das usinas nucleares atuais. O estudo consiste na modelagem DFM desse sistema de controle e de suas interações com o processo a ser controlado. Três preocupações existentes na literatura foram consideradas na análise: a modelagem do sistema, levando-se em consideração uma visão holística, a incorporação dos resultados da análise de falhas a uma APS (Análise Probabilística de Segurança) já existente e a identificação de falhas de *software*, principal componente de um sistema digital. Os resultados obtidos demonstram que a metodologia possibilita uma análise de falhas eficiente do sistema digital, levando em conta todas as possíveis interações existentes entre seus componentes. Além disso, a DFM identifica falhas estritamente ligadas ao *software*, contribuindo para a confiabilidade destes elementos.

A revisão bibliográfica acima reúne um conjunto de temas aplicados à atualização do sistema analógico para o sistema digital, bem como a utilização da I & C digitais em sistemas relacionados com a segurança e não relacionados com a segurança em usinas nucleares, mostrando que existe espaço para a proposição de métodos que possam complementar o licenciamento desses sistemas,

Assim, a abordagem proposta nesta tese de doutorado, busca de forma realista e inovadora, a utilização da informação do risco na análise de segurança de sistemas de I & C digitais aplicados a centrais nucleares através do estudo de eventos operacionais em conjunto com a avaliação de defesa em profundidade e diversidade (D3) de sistema de I & C digital.

3 VISÃO GERAL DA ESTRUTURA DA INSTRUMENTAÇÃO E CONTROLE (I & C)

3.1 INTRODUÇÃO

Um sistema de controle de processo em uma usina nuclear tem que executar uma variedade de tarefas: atuação automática, comunicação, monitoração, atuação manual do operador, gerenciamento de alarmes, funções, manutenção, etc.

Os sistemas de I & C em uma usina nuclear são cuidadosa e formalmente estruturados, permitindo que cada função da I & C possa ser identificada com seus objetivos de segurança ou operacionais, ajudando a organizar e garantir separação apropriada, como por exemplo: entre as funções de controle e de proteção. A Figura 3.1 mostra os sistemas de I & C relacionados com a segurança e os sistemas de I & C não relacionados com a segurança da usina.

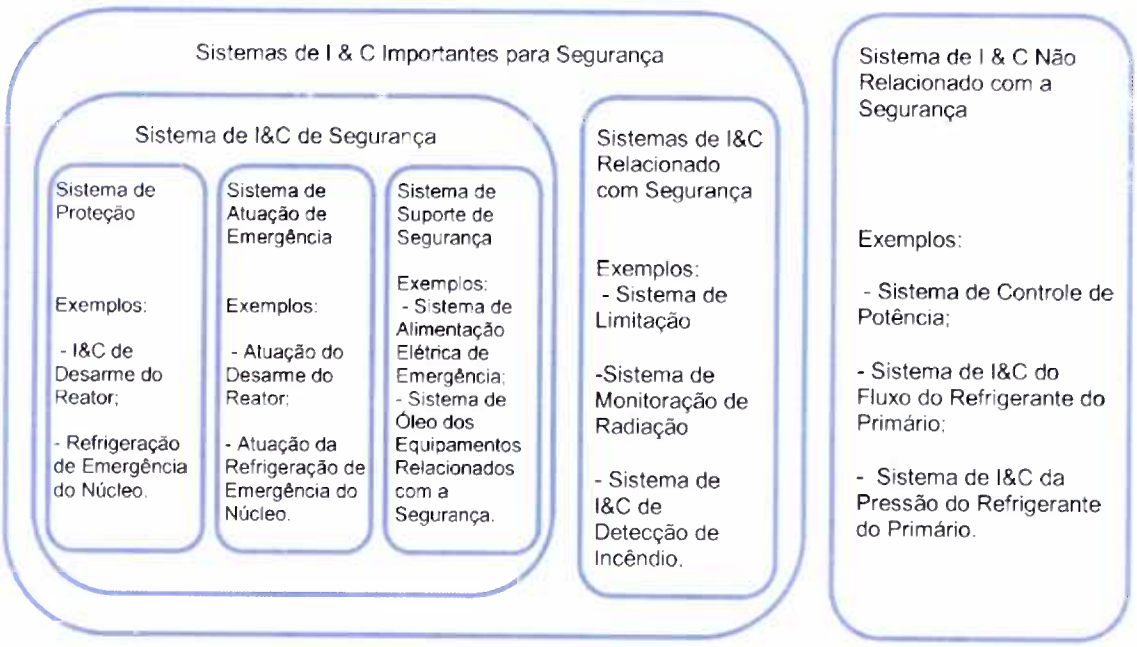


Figura 3.1 – Sistemas de I & C relacionados com a segurança e os sistemas não relacionados com a segurança (IEC, 1993).

3.1.1 ESTRUTURAS PRINCIPAIS

Os processos mostrados na Figura 3.2 podem ser implantados usando uma grande variedade de estruturas e hierarquias e existem muitos sistemas diferentes.

Na Figura 3.2 é mostrado, de uma forma resumida, como as informações medidas através dos sensores chegam aos níveis de controle do sistema de instrumentação e controle da usina. Do lado direito, a figura mostra como essas informações e ações, com prioridades diferentes, como controle manual, sistema proteção e de limitação, são transmitidas para a usina. Sinais de processo podem, em alguns casos simples, ser usados para iniciar os intertravamentos e atuações, não sendo, porém, mostrados na figura.

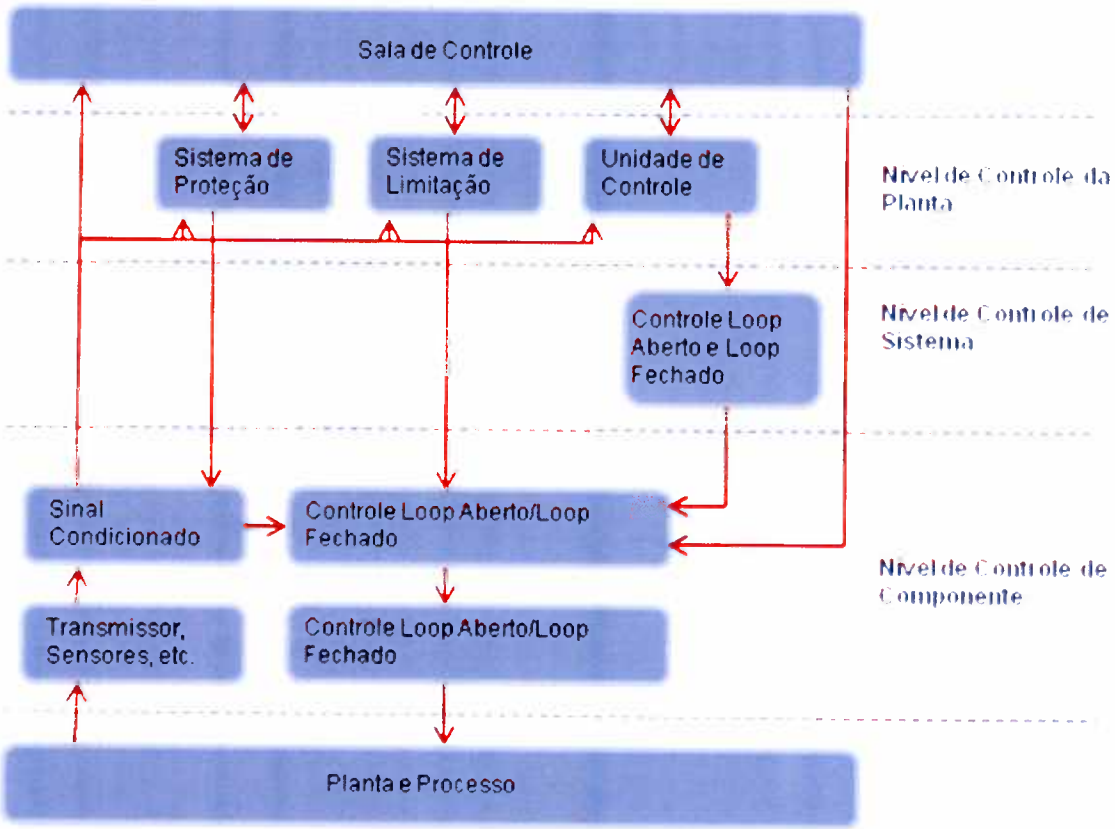


Figura 3.2 – Estrutura da I & C em uma usina nuclear (IAEA, 1988b e IAEA, 1980).

Os níveis hierárquicos nas seções horizontais são divididos em funções diferentes, conforme mostrado a seguir:

- Nível de controle de componente (ou dispositivo). Este é o mais baixo nível com lógicas simples e intertravamentos, normalmente em conexão com atuações em componentes como: partir e desligar bombas, motores e ventiladores, fechamento de válvulas, etc.
- Nível de controle sistema (ou grupo). Vários sistemas de controle (*open* ou *closed loop*) são usados para manter todas as variáveis de processo dentro de valores operacionais normais. Estes sistemas estarão sujeitos à intervenção do sistema de proteção ou de limitação se as margens de segurança forem excedidas.
- Nível de controle da usina. Esta é a seção de posição mais alta do I & C, normalmente situada dentro da sala de controle. Funções que interessam ao desempenho e modo de operação da usina são controladas e monitoradas neste nível. Por exemplo, o sistema de controle principal identifica uma demanda externa de energia e coordena e distribui sinais para sistemas e subsistemas, fazendo com que a usina responda.

3.1.2 ESTRUTURAS DE UNIDADES SUBSIDIÁRIAS

Valores medidos, gerados por variáveis de processo, são convertidos em sinais elétricos ou pneumáticos que são transmitidos então a unidades subsidiárias usadas para indicação, controle e funções de proteção. Como foi descrito anteriormente, há uma tendência crescente para unidades locais fazerem mais processamento de sinais e conteram mais lógicas de processamento. Esta tendência introduz sistemas especialistas locais, orientando os operadores de painéis locais e o pessoal de manutenção.

Antes da transmissão, os sinais dos sensores são normalmente convertidos para um nível de sinal padronizado, por exemplo: 4–20 miliampere (mA) ou 0–10 volt. Para transmissão remota de sinais, o 4–20 mA, sinal corrente, é o mais comum por ser

mais imune a ruídos. Sinais de voltagem (como 0–10 V) são geralmente usados dentro da sala de controle para registradores e indicadores.

3.2 SISTEMAS ANALÓGICOS

Muitas usinas nucleares ainda usam dispositivos analógicos para prover informação ao operador, processos de controle e para atuação do sistema de proteção, conforme mostrado na Figura 3.3. Existem diferentes versões, mas um sistema analógico típico pode incluir o seguinte:

- Unidades de desarme principais (ou mestre). Interface das unidades de desarme principais com transmissor de 4–20 mA. Uma unidade de desarme principal, contendo circuitos necessários para receber os inputs dos transmissores e prover as funções de chaveamento e os sinais de saídas analógicas para energizar um relé de desarme em qualquer nível dentro do 4–20 mA ou uma faixa de resistência de um sinal de entrada.
- Unidades de desarme escravas são usadas em conjunto com as unidades de desarme principais quando é desejável ter diferentes *setpoints* de um transmissor comum. Os escravos obtêm seus sinais de entrada de um sinal de saída analógico da unidade de desarme principal ou mestre. Sete unidades escravas podem ser controladas por uma única unidade de desarme do reator principal, permitindo assim até oito *setpoints* diferentes para um único parâmetro medido. Ao contrário da unidade principal, não há nenhuma conexão direta de um transmissor com uma unidade escrava, nem com qualquer sinal analógico gerado pela unidade escrava. Porém, cada escravo tem sua própria função chave lógica de saída para desarme de alta ou baixa, que é independente de seu mestre ou de qualquer outro escravo paralelo.

- Relé de desarme. Cada unidade mestre ou escrava é capaz de suprir cada relé de desarme com cargas de até 1 A em 24 VDC nominal. Contatos destes relés proveem a função lógica necessária para as variáveis de entrada do processo. As unidades de desarme são projetadas com diodo de isolamento de saída, que permite conexão de saída paralela de várias unidades de desarme em um relé.
- Suprimento de energia. As unidades de desarme são projetadas com circuitos de regulação de energia individuais de forma que a voltagem do suprimento de energia principal não precisa ser regulada precisamente.

Figura 3.3 – Exemplo de sala de controle que utiliza I & C analógica.

3.3 SISTEMAS DIGITAIS

Os sistemas analógicos e digitais monitoram, controlam e protegem equipamentos e processos críticos para assegurar que a usina opere com segurança e confiabilidade. Porém, sistemas analógicos e digitais executam tarefas diferentemente para realizar estas funções. Sistemas analógicos executam instruções de hardware,

enquanto que os sistemas digitais realizam suas funções por meio de software armazenado na memória, usando processamento e equipamento de transmissão de dados (hardware). O uso de hardware e software dá flexibilidade aos sistemas digitais, mas também aumenta a vulnerabilidade para falhas de software e para novas falhas de hardware (NRC, 1995 & NRC, 1994a).

3.3.1 SISTEMA DE I & C DIGITAL TELEPERM XS/XP - SIEMENS

A Siemens desenvolveu dois sistemas de I & C complementares, Teleperm XP e Teleperm XS, cujas características principais incluem: uma arquitetura com redundância adaptável; a aplicação consequente de padronização para interfaces e comunicação e uma Interface Homem-Sistema (IHS) altamente ergonômica (Figura 3.4).

Figura 3.4 – Futura sala de controle digital.

O sistema de engenharia no Teleperm XP é denominado ES 680, enquanto no Teleperm XS é denominado SPACE.

A Figura 3.5 mostra a arquitetura simplificada do sistema de I & C digital da Siemens Teleperm XS/XP.

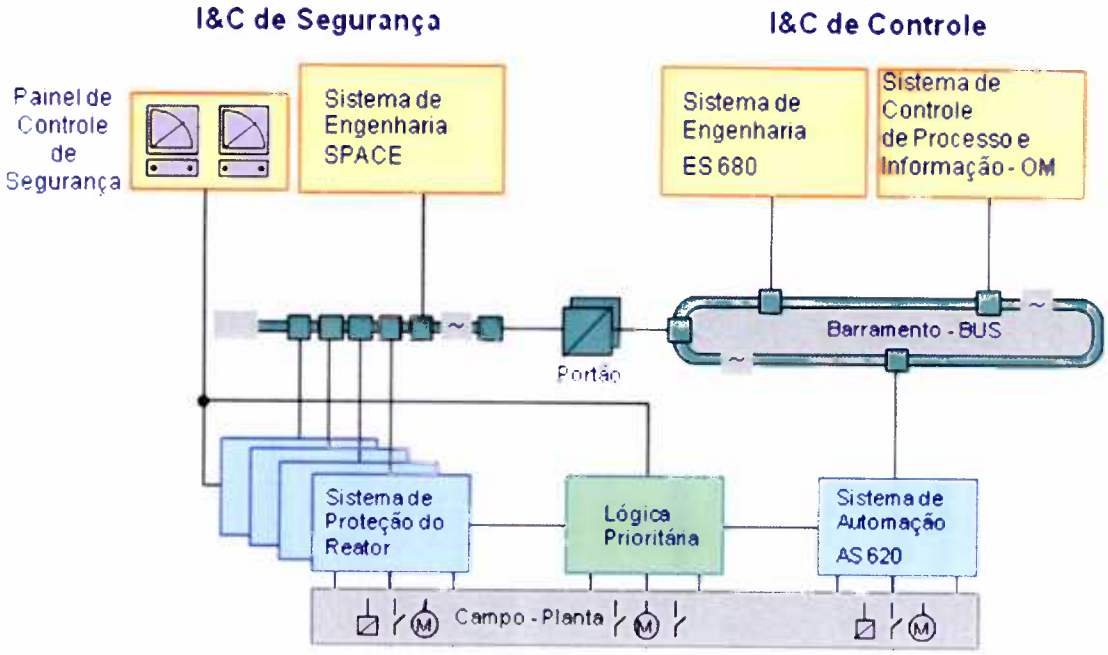


Figura 3.5 – Configuração simplificada do sistema Teleperm XS/XP

O Teleperm XP é planejado para executar funções automáticas para as quais nenhuma qualificação específica para aplicações nucleares é requerida. Este é o caso para o controle de parâmetros de processo essenciais, para quase todo o sistema de interface de homem-sistema. Isto significa que o sistema de controle Teleperm XP pode ser usado para uma usina térmica (termoelétrica), como a termoelétrica da Siemens na Companhia Siderúrgica Nacional (CSN) em Volta Redonda, no estado do Rio de Janeiro, como também para todas as aplicações de controle para usinas nucleares.

Por outro lado, o sistema Teleperm XS é planejado para os sistemas de segurança, I & C exclusiva para uma usina nuclear, especialmente para as tarefas requeridas para um desligamento seguro do reator, por exemplo, que ative sistemas de segurança e limitação de potência do reator e funções de controle do circuito primário.

O sistema de engenharia provê a interface central entre o equipamento para funções automáticas, controle de operador e monitoração. É uma parte integrante do

sistema de I & C e apóia não só criando funções/tarefas, mas também manutenção e diagnóstico de todos os componentes de I & C (Figuras 3.6 e 3.7).

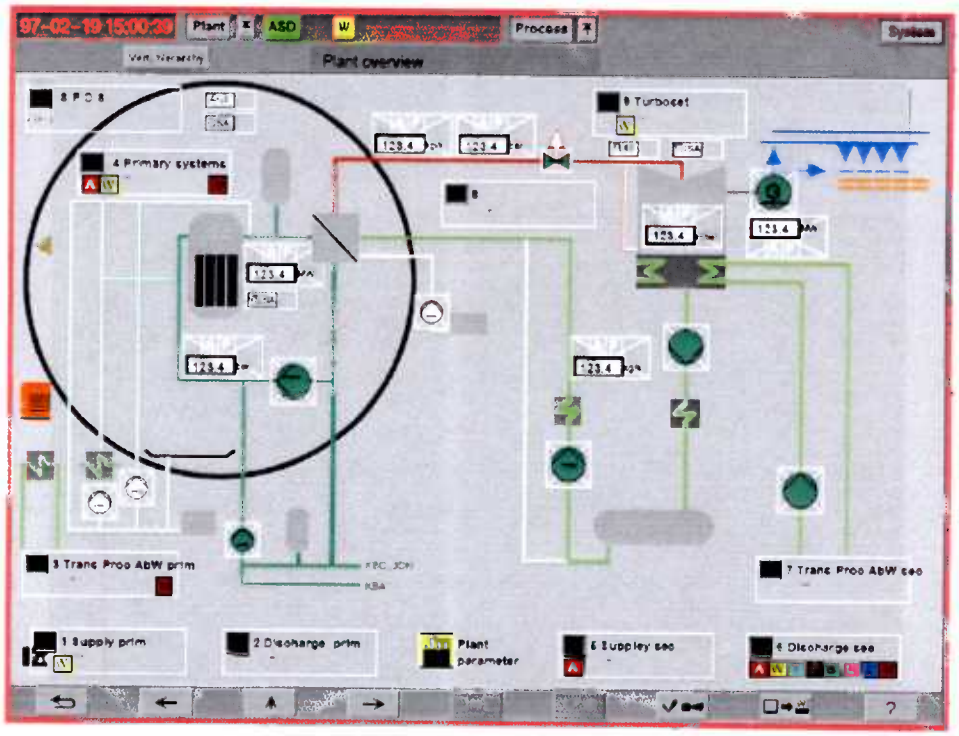


Figura 3.6 – Tela do Sistema de Refrigeração do Reator - SRR.

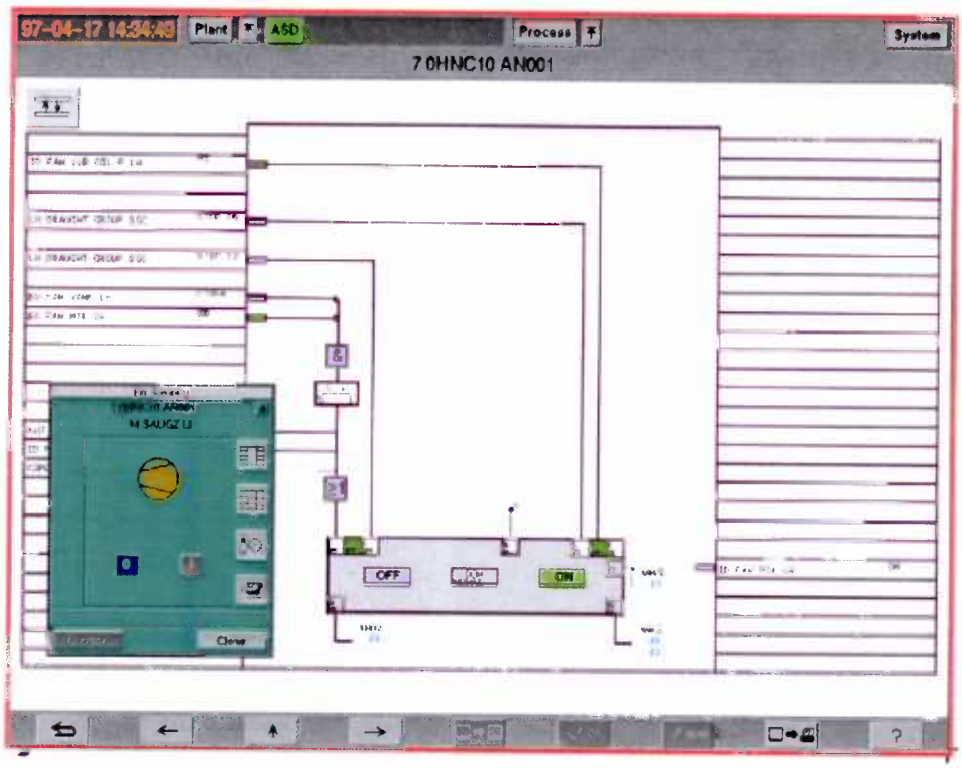


Figura 3.7 – Tela de lógica de acionamento de equipamento/alarme.

As usinas nucleares que já utilizam o sistema de I & C digital da Siemens (Teleperm XS/XP) são mostradas na Figura 3.8.

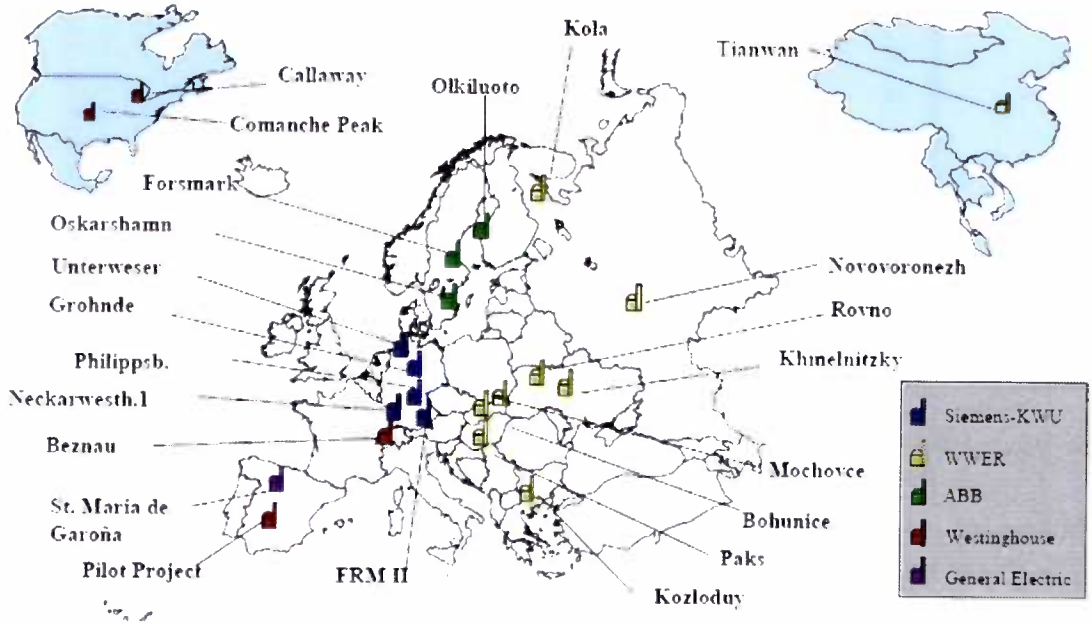


Figura 3.8 – Usinas que já Utilizam o sistema Teleperm XS/XP

Exemplos de salas de controle digital mostradas na Figura 3.9.

Figura 3.9 – Exemplos de salas de controle que utilizam I & C Digital.

3.4 SISTEMA DE PROTEÇÃO DO REATOR (SPR)

O Sistema de Proteção de Reator (SPR) de uma usina nuclear tem a função de desligar o reator e colocar em funcionamento os sistemas de segurança, para evitar acidentes que levem ao superaquecimento e à deterioração do núcleo, mantendo o reator operando dentro de uma faixa segura. Se um ou mais parâmetros físicos entram em uma faixa inaceitável de valores, um sinal de desarme do reator será gerado e com isso causará a inserção das barras de controle no núcleo do reator, assegurando a paralisação da reação nuclear em cadeia (IAEA, 1999c).

3.4.1 SISTEMA DE PROTEÇÃO DO REATOR (SPR) - FILOSOFIA DO PROJETO ALEMÃO

Sete das doze usinas nucleares alemãs (PWR), que compreendem toda a quarta geração de I & C de usinas nucleares mais a central nuclear de Biblis B, conforme mostrado na Tabela 3.1 (IAEA, 1999c), possuem um sistema de I & C com equipamentos e sistemas usados para transmissão e conversão de sinais, indicação, armazenamento de dados e atuação para as funções de proteção, limitação, controle e monitoração.

Tabela 3.1 – Gerações da instrumentação e controle das usinas PWR alemãs.

Geração	Usina	Início da Operação Comercial	MWe
1	Obrigheim	1969	357
2	Stade	1972	672
3	Biblis A	1974	1204
	Neckarwestheim 1	1976	840
	Biblis B	1977	1300
	Unterweser	1979	1320
4 Konvoi	Grafenrheinfeld	1982	1345
	Grohnde	1985	1430
	Philippsburg	1985	1402
	Isar	1986	1410
	Emsland	1988	1363
	Neckarwestheim 2	1989	1365

A terminologia alemã SPR inclui o sistema de atuação de proteção e de segurança (chamado em alguns países de sistema de segurança). O SPR é projetado de acordo com exigências reguladoras, particularmente a norma KTA 3501 (KTA, 1985) e também com a análise de segurança da usina.

O SPR alemão se distingue do SPR de outros países, tendo como principais características:

- Uma exigência para dois critérios diversos de iniciação para cada evento iniciador postulado;
- Um critério de falha determinístico (Figura 3.10) que conduz ao projeto dois de três (2D3) como um mínimo para redundância e diversidade funcional;
- Automatização tal que nenhuma intervenção manual seja necessária durante os primeiros 30 minutos, de acordo com o evento iniciador postulado. Isto significa uma extensão significativa de automatização de

funções e recursos necessários. São permitidas intervenções manuais, mas só dentro de certos limites;

- Separação física de canais de I & C redundantes e de equipamentos relevantes;
- Edifício de emergência, protegido contra eventos externos, projetado de modo semelhante à contenção do reator. Este edifício de emergência possui uma sala de controle de emergência, e se houver uma indisponibilidade da sala de controle principal, o pessoal de operação tem recursos para 10 h de operação (por exemplo: armazenamento de água e unidades de bombeamento e o segundo grupo de geradores diesel de emergência com quatro geradores diesel pequenos).

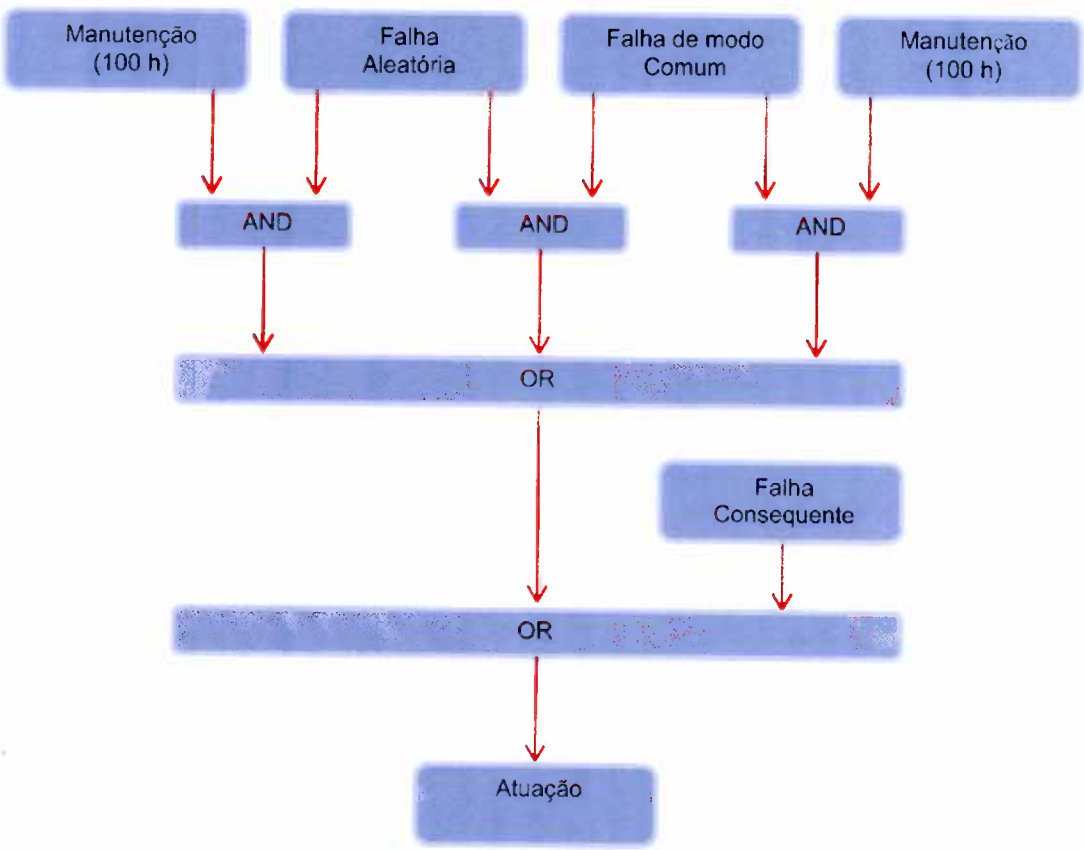


Figura 3.10 – Combinações de falhas de acordo com a norma KTA 3501 (KTA, 1985).

3.4.1.1 ESTRUTURA DO SPR ALEMÃO

Na estrutura do SPR alemão, os desligamentos do reator e da turbina ficam situados nas áreas menos protegidas por causa de suas características de falha-segura. Seções para adquirir dados medidos, processo analógico, formação de valores limites e portas lógicas são três vezes ou até mesmo quatro vezes redundantes. Os sinais de saída para todas as ações de proteção são gerados pelas portas lógicas que priorizam os sinais de atuação do SPR, depois os sinais do Sistema de Limitação e finalmente as funções manuais e de controle.

3.4.1.1.1 EVENTOS INICIADORES POSTULADOS

São postulados 15 eventos iniciadores, os quais:

- Distúrbio durante a partida da unidade, falhas na movimentação das barras de controle e na diluição de boro;
- Vazamento no Sistema de Refrigeração do Reator (SRR) de tamanhos diferentes e também rupturas em tubos dos Geradores de Vapor (GV);
- Ruptura na linha de vapor em locais diferentes e falhas na abertura das válvulas de desvio;
- Falha no fechamento das válvulas de isolamento do vapor principal e no Sistema de Água de Alimentação dos Geradores de Vapor;
- Desligamento das Bombas de Refrigeração do Reator (BRR) ou das Bombas de Água de Alimentação dos Geradores de Vapor, falha no suprimento de energia e possíveis conseqüências de eventos externos.

3.4.1.1.2 AÇÕES DE PROTEÇÃO

Ações de proteção incluem:

- Desligamento do reator e da turbina, mais isolamento da contenção;

- Controle da pressão alta e baixa do refrigerante do reator nos tanques de armazenamento de refrigerante ou do poço da contenção;
- Boração extra do sistema de boração de emergência;
- Operação do sistema de água de alimentação principal de fluxo mínimo como também das válvulas de alívio;
- Operação do sistema de água de alimentação de emergência e dos geradores diesel de emergência.

3.4.1.1.3 MEDIÇÕES NECESSÁRIAS

As informações necessárias para a operação da usina são adquiridas através de medidas como:

- Fluxo de nêutrons / potência do reator:
  - Fluxo neutrônico (sistema de instrumentação externa do núcleo);
  - Elevação de temperatura do refrigerante do reator
- Pressão e temperatura média do refrigerante na saída do reator (perna quente);
- Velocidade das bombas de refrigerante do reator e consequentemente o fluxo do refrigerante do reator;
- Nível no pressurizador e dos geradores de vapor;
- Atividade nas linhas de vapor principais;
- Pressão nos geradores de vapor e presença de condensado no vapor principal (gotas);
- Pressão na contenção do reator;
- Monitoração de voltagens e frequências.

3.4.2 SISTEMA DE PROTEÇÃO DO REATOR - FILOSOFIA DO PROJETO AMERICANO

O objetivo do SPR é prevenir a liberação de material radioativo para o meio ambiente. O SPR pode desarmar o reator para prevenir operações inseguras que poderiam conduzir a condições de acidente. Se um acidente acontece, o SPR atuará os DTS (Dispositivo Técnico de Segurança) que são projetados para mitigar as conseqüências de um acidente. Os parâmetros operacionais do reator são monitorados através dos sensores locais para descobrir qualquer condição que requeira um desarme do reator ou atuação dos DTS. Processos selecionados são medidos através de circuitos analógicos ou digitais que comparam *setpoints* para iniciar a ação de desarme do reator (IAEA, 1999c).

3.4.2.1 PROJETO DO SISTEMA

O sistema de instrumentação e controle da usina envia sinais de desarme para dois trens de lógicas nos gabinetes do SPR. Quando uma condição insegura é sentida, um sinal é enviado aos gabinetes de proteção e o desarme do reator é requerido, os gabinetes de proteção enviam um sinal para abrir os disjuntores de desarme do reator, os quais removem a energia do mecanismo de inserção de barras de controle, permitindo que elas caiam no núcleo do reator por gravidade. Se a atuação dos DTS é requerida, os gabinetes de proteção atuam o equipamento de segurança apropriado. Sinais também são providos pelos trens de lógica para permitir, automatica ou manualmente, o inicio de intertravamentos e bypasses.

3.4.2.1.1 CRITÉRIO DE FALHA ÚNICA

O SPR é projetado com redundância um de dois, dois de três ou dois de quatro canais de instrumentação para cada função de proteção e um de dois circuitos de trens de lógicas. Estes canais redundantes e trens de lógicas estão eletricamente

isolados e fisicamente separados. Então, qualquer falha única em um canal ou trem não evitará a ação de proteção quando exigida. Perda de energia para um canal ou trem de lógica resulta em um sinal de desarme do reator.

3.4.2.1.2 TESTABILIDADE

O SPR é testado em quaisquer condições de operação da usina. Isto assegura disponibilidade e precisão dos sensores do sistema até os dispositivos finais (disjuntores de desarme do reator, equipamentos de DTS, etc.).

3.4.2.1.3 QUALIFICAÇÃO DE EQUIPAMENTO

Uma gama de testes de qualificação ambiental, testes de desempenho, etc., é empregada para assegurar o funcionamento dos equipamentos em condições de acidente com perda de refrigerante.

3.4.2.1.4 INDEPENDÊNCIA

Cada instrumento de processo é destinado para um dos quatro canais de proteção. A independência de canal é levada ao longo de todo o sistema e se estende do sensor até os dispositivos que atuam nas funções de proteção. Separação física é usada para separar transmissores redundantes e a separação do cabeamento é alcançada através da separação dos cabos, bandejas de cabos, condutos e penetrações na contenção do prédio do reator para cada canal redundante. Equipamentos analógicos redundantes estão separados, localizados em módulos e prateleiras de proteções diferentes. Cada canal redundante tem sua fonte de energia elétrica e os dois disjuntores de desarme do reator são atuados por duas lógicas matrizes separadas. Os disjuntores de desarme do reator estão conectados em série com o suprimento de energia, quando eles abrem e interrompem a alimentação elétrica para o mecanismo de acionamento das barras de controle. Com isso as barras de controle caem no núcleo do reator por gravidade.

3.4.2.1.5 DIVERSIDADE

Para assegurar uma operação segura, protegendo principalmente o Sistema de Refrigeração do Reator (SRR), o SPR continuamente monitora diversas variáveis através de diferentes tipos de sensores. Ao garantir esta diversidade de monitoração, permite que o SPR tenha uma confiabilidade maior no enfrentamento de acidentes postulados.

3.4.2.1.6 INTERAÇÃO ENTRE O SISTEMA DE PROTEÇÃO E O DE CONTROLE

O sistema de proteção é projetado para ser independente do sistema de controle, mas, em certas aplicações, sinais de controle e outras funções que não são de segurança são derivados de canais de proteção individuais através de amplificadores de isolamento. Os amplificadores de isolamento são classificados como parte do sistema de proteção e ficam situados dentro das prateleiras analógicas da proteção do reator. Funções que não são de proteção incluem esses sinais usados para controle, monitoração de processo remota e computador de processo. Os amplificadores de isolamento são projetados de forma que um circuito pequeno, um circuito aberto ou a aplicação de CA ou voltagem de DC no lado de saída isolada do circuito não afetará o lado das entradas. Os sinais obtidos pelos amplificadores de isolamento nunca retornam às prateleiras da proteção do reator.

3.4.2.2 TIPOS DE PROJETO DE SISTEMA DE PROTEÇÃO

O projeto do sistema de proteção americano pode ser de dois tipos diferentes:

- Sistema de Relé de Proteção;
- Sistema de Proteção Estatal Sólido (SPES).

O dois sistemas executam as mesmas funções, sendo o SPES um projeto posterior ao Sistema de Relé de Proteção.

Para cumprir as funções de desligamento do reator e atuação dos dispositivos de segurança, vários parâmetros dos sistemas primário e secundário são monitorados e enviados para o sistema de proteção do reator, como exemplo:

- Potência nuclear (INE);
- Pressão do pressurizador;
- Nível do pressurizador;
- Temperatura do refrigerante do reator;
- Fluxo de refrigerante do reator;
- Fluxo de água de alimentação principal;
- Fluxo de vapor principal;
- Nível dos geradores de vapor;
- Pressão do vapor principal;
- Potência da turbina;
- Tensão e frequência nos barramentos de serviço.

Para que haja o desligamento do reator, é necessário que ocorra a abertura de um ou ambos os disjuntores de desligamento do reator, que cortará o fornecimento de energia elétrica para os mecanismos de acionamento das barras de controle e com isto, as barras de controle cairão por gravidade, desarmando o reator. Para provocar a abertura dos disjuntores de desligamento do reator, é necessário que haja a desenergização de suas bobinas de subvoltagem UV TRIP COIL e/ou SHUNT TRIP COIL, que são alimentadas diretamente da lógica do Sistema de Proteção do Reator (DES SPR 01).

Um disjuntor de desvio (BYA e BYB), em paralelo com cada disjuntor de desligamento do reator (RTA e RTB), permite efetuar um teste com os disjuntores de desligamento do reator com a unidade em operação. Os disjuntores de desvio (BYA e BYB) são intertravados de maneira que, caso um já esteja fechado e tentar-se fechar o

outro, o primeiro abrirá automaticamente. Isto previne que se desviem os dois disjuntores de desligamento simultaneamente.

3.4.2.3 SINAIS DE DESARME DO REATOR

- Manual;
- Alto fluxo de nêutrons na faixa da fonte;
- Alto fluxo de nêutrons na faixa intermediária;
- Alto fluxo nêutrons na faixa de potência;
- Alta taxa positiva de fluxo de nêutrons na faixa de potência;
- Alta taxa negativa de fluxo de nêutrons na faixa de potência;
- Afastamento da ebulição nucleada (DNB);
- Sobrepotência do reator;
- Baixo fluxo no sistema de refrigeração do reator;
- Subfrequência nos barramentos elétricos de serviços;
- Subtensão nos barramentos elétricos de serviços;
- Abertura do disjuntor das bombas de refrigeração do reator;
- Baixa pressão no pressurizador;
- Alto nível no pressurizador;
- Alta pressão no pressurizador;
- Nível muito baixo no gerador de vapor;
- Desarme da turbina;
- Injeção de segurança no sistema primário;

4 LICENCIAMENTO DA I & C DIGITAL

4.1 INTRODUÇÃO AO LICENCIAMENTO DE REATORES NUCLEARES

O processo de licenciamento de reatores nucleares no Brasil decorre do exercício de atribuição estatutária legal da Comissão Nacional de Energia Nuclear (CNEN). Este processo é regulado por norma, que prevê a emissão de atos como aprovações, licenças e autorizações, bem como emendas ou cancelamentos desses atos. Este processo de tomada de decisão é feito a partir da verificação do atendimento a requisitos e padrões de segurança. Esta conformidade garantirá, com base no conhecimento vigente da tecnologia nuclear, que a operação dessas instalações não implique em risco indevido à saúde e à segurança dos trabalhadores e da população, bem como ao meio ambiente.

A norma CNEN-NE-1.04 (CNEN, 1984a), regula o processo de licenciamento de instalações nucleares, está em vigor, desde 1984 e se aplica às atividades relacionadas com a localização, a construção e a operação de instalações nucleares, abrangendo as seguintes etapas:

- Aprovação do Local;
- Licença de Construção;
- Autorização para Utilização de Materiais Nucleares;
- Autorização para Operação Inicial;
- Autorização para Operação Permanente.

Para que a CNEN emita essas licenças e autorizações, é necessário que o proprietário dessas instalações faça solicitações formais através de requerimentos, anexando informações, dados, planos e relatórios de análise de segurança (RAS),

cujos requisitos de conteúdo mínimo estão estabelecidos na norma CNEN-NE-1.04 (CNEN, 1984a).

A avaliação de segurança é realizada com base na documentação de suporte ao requerimento de licença visando subsidiar a tomada de decisão sobre a aceitabilidade da instalação proposta, conhecendo o risco associado à operação da mesma.

De acordo com a norma CNEN-NE-1.04 (CNEN, 1984a), ao descrever e analisar a instalação, os relatórios devem dar atenção especial às principais considerações de segurança, apresentando os "critérios principais" utilizados na execução do projeto, as bases de projeto e sua relação com estes critérios, bem como informações relativas ao arranjo, dimensões e materiais empregados num nível suficiente para garantir que o projeto final esteja conforme as bases de projeto, com adequada margem de segurança.

Já a caracterização, pelo órgão regulador, de um nível de risco indevido determina os chamados objetivos de segurança que, em última instância, especificam metas ou níveis de desempenho a ser atingidos pela instalação, tanto em condições normais de operação quanto em circunstâncias associadas aos acidentes postulados na sua base de projeto. O cumprimento dos objetivos de segurança caracteriza os critérios fundamentais para o processo de tomada de decisão no processo de licenciamento.

4.1.1 CONCEITO DE ESTRATÉGIA REGULADORA

A forma como o órgão regulador se assegura que os objetivos de segurança são cumpridos pelos licenciados define o que se chama de estratégia reguladora. Em termos internacionais, há uma grande diversidade de abordagens ou estratégias reguladoras para garantir a segurança das instalações nucleares (BÁRBARA, NANCY, 2002).

A estratégia prescritiva é aquela que adota um nível bem detalhado para os requisitos de projeto ou para a condução da operação. O órgão regulador se assegurará do alcance dos objetivos de segurança pela extensiva verificação da conformidade com seus requisitos.

A estratégia da instalação de referência é aquela que considerará o princípio da adoção exclusiva de tecnologias comprovadas e considerará satisfatório o desempenho da instalação se for comparável àquele de uma instalação de referência já licenciada (IAEA, 1993).

A estratégia baseada em risco é aquela que julgará as soluções de projeto e o desempenho da operação com base explícita em avaliações quantitativas de risco. Outras possíveis estratégias são baseadas em desempenho (orientada para resultados), a estratégia orientada para os processos ou, ainda, a estratégia baseada na auto-avaliação, entre outras.

Entretanto, é reconhecido que cada estratégia possui suas vantagens e desvantagens e que, em geral, os órgãos reguladores utilizam uma combinação delas como forma de se assegurar que os objetivos de segurança sejam cumpridos. As normas da CNEN para o licenciamento de reatores nucleares revelam, claramente, essa combinação de estratégias regulatórias (CNEN, 1984a & IAEA, 1993).

4.1.2 PRINCIPAIS CRITÉRIOS ADOTADOS NO LICENCIAMENTO NO BRASIL

Com a decisão do governo brasileiro, na década de 60, de construir e operar uma usina nuclear para geração termoelétrica, e a posterior opção pela tecnologia americana da empresa *Westinghouse*, a regulamentação nuclear brasileira foi fortemente influenciada pelo modelo utilizado nos Estados Unidos da América, particularmente no que se refere às etapas estabelecidas para o processo de licenciamento.

A lei básica para regular a utilização da energia nuclear naquele país é o chamado *Atomic Energy Act*, de 1954, que estabeleceu o arcabouço legal para toda a regulamentação nuclear subseqüente. Em 1974, através do chamado *Energy Reorganization Act*, foi criado um órgão exclusivamente regulador do uso da energia nuclear e independente de quaisquer outras atividades de promoção desta forma de energia, a *US Nuclear Regulatory Commission* (NRC).

A coletânea de regulamentos técnicos federais americanos, conhecida como *Code of Federal Regulations* (CFR) possui vários títulos, sendo o Título 10 aquele que trata do tema energia. Cada título é dividido em diversas partes. Toda a regulamentação da NRC está no Título 10, entre as Partes 0 e 199, que apresentam os requisitos para todas as pessoas e organizações que recebem uma licença da NRC para o uso de materiais nucleares ou para a operação de instalações nucleares.

Muitas das normas da CNEN foram desenvolvidas a partir de textos de referência baseados na versão vigente à época desta regulamentação da NRC.

As partes mais relevantes para o licenciamento e controle de reatores nucleares e as correspondentes normas da CNEN são mostradas na Tabela 4.1.

Tabela 4.1 – Comparação da entre o 10 CFR e as normas da CNEN.

10 CFR	Norma da CNEN correspondente
20 *Standards for Protection Against Radiation*	NE-3.01 "Diretrizes Básicas de Radioproteção"
50 *Licensing of Production and Utilization Facilities*	NE-1.04 "Licenciamento de Instalações Nucleares"
50.46 *Acceptance Criteria for Emergency Core Cooling Systems for LWR*	NE-1.20 "Aceitação de Sistemas de Resfriamento de Emergência do Núcleo de Reatores a Água Leve"
50.73 *Licensee Event Report System*	NN-1.14 "Relatórios de Operação de Usinas Nucleoelétricas"
50 *Appendix B Quality Assurance Criteria for NPP and Fuel Reprocessing Plants*	NN-1.16 "Garantia da Qualidade para a Segurança de Usinas Nucleoelétricas e Outras Instalações"
50 *Appendix. K – ECCS Evaluation Model*	NE-1.19 "Qualificação de Programas de Cálculo para a Análise de Acidentes de Perda de Refrigerante em Reatores a Água Pressurizada"
55 *Operator's licenses*	NE-1.01 "Licenciamento de Operadores de Reatores Nucleares"
100 *Reactor Site Criteria*	Resolução 09/69 – "Normas para Escolha de Local para a Instalação de Reatores de Potência"

Como país importador da tecnologia nuclear e com as reduzidas dimensões do programa nuclear brasileiro, ressalvas nas normas da CNEN reconhecem a possibilidade de inexistência de normalização nacional sobre determinado assunto, remetendo a solução para padrões reconhecidos internacionalmente.

Embora identificados como merecedores de especial atenção, e requeridosno item 6.4.4 da norma NE-1.04 (CNEN, 1984a), adotando uma estratégia regulatória não prescritiva, não estão estabelecidos requisitos mínimos para os chamados critérios principais de projeto. Já a regulamentação americana apresenta, no Apêndice A do

10CFR-Parte 50 (NRC, 2009c), os chamados Critérios Gerais de Projeto para Usinas Nucleares de Potência, que estabelecem os requisitos necessários ao projeto, à fabricação, à construção, aos testes e ao desempenho de sistemas estruturas e componentes. A legislação americana reconhece que o atendimento a esses requisitos fornece garantia razoável de que a operação da instalação não implicará em risco indevido ao público e ao meio ambiente.

Um total de 45 critérios gerais de projeto está dividido em 6 categorias, embora sejam feitas ressalvas que reconhecem esses critérios como ainda incompletos e, em alguns casos, não aplicáveis:

I Requisitos gerais (1 a 5);

II Proteção por múltiplas barreiras contra a liberação de produtos de fissão (10 a 19);

III Sistemas de proteção e controle de reatividade (20 a 29);

IV Sistemas que contêm fluídos (30 a 46);

V Contenção do reator (50 a 57);

VI Controle de combustível e de radioatividade (60 a 64).

O Critério Geral de Projeto nº 1 (Normas e Registros da Qualidade) requer que estruturas, sistemas e componentes sejam projetados, fabricados, construídos, montados e testados de acordo com padrões de qualidade compatíveis com a importância da função de segurança a ser executada. Sempre que códigos e padrões reconhecidos sejam empregados, esses devem ser identificados e avaliados para determinar sua aplicabilidade, adequação e suficiência, sendo suplementados ou modificados para garantir a qualidade do produto necessária ao desempenho da função de segurança. Um Programa de Garantia da Qualidade deve ser desenvolvido e implantado para fornecer adequada confiança de que esse item terá o desempenho

como esperado. Convém ressaltar que os requisitos ao programa de garantia da qualidade estão estabelecidos no Apêndice B do 10CFR Parte 50 (NRC, 2009d), que corresponde à norma CNEN-NN-1.16 (CNEN, 1999), na regulamentação da CNEN.

O conteúdo dos relatórios de análise de segurança deve atender aos requisitos estabelecidos no 10CFR Parte 50.34 (NRC, 2009e), corresponde aos itens 6.4 e 8.4 da norma NE-1.04 (CNEN, 1984a), respectivamente para o Relatório Preliminar de Análise de Segurança (RPAS) e para o Relatório Final de Análise de Segurança (RFAS).

Dentro do modelo regulador americano, a NRC publica os chamados guias regulatórios que, embora não sejam obrigatórios, descrevem formas consideradas aceitáveis pela NRC para o atendimento dos requisitos do 10CFR, promovendo assim uma maior eficiência no processo de licenciamento e nas avaliações que sua equipe técnica elabora como suporte ao processo de tomada de decisão. Os guias regulatórios estão agrupados em dez divisões, sendo os que se aplicam às atividades da CNEN:

- Divisão 1 - reatores de potência
- Divisão 2 - reatores de pesquisa e de teste.

Os Relatórios de Análise de Segurança (RAS) deverão documentar a forma como o projeto da instalação atende aos Critérios Gerais de Projeto, incluindo a identificação e a caracterização da aplicabilidade de códigos e padrões empregados. O guia regulador que estabelece o conteúdo e o formato para os relatórios de análise de segurança de usinas nucleares é o Regulatory Guide 1.70 – "*Standard Format and Content of Safety Analysis Reports for NPP*" (NRC, 1994b). Com amparo no item 6.2.1 da norma CNEN-NE-1.04 (CNEN, 1984a), a CNEN tem adotado esta referência como modelo padrão para relatórios de análise de segurança de usinas nucleares.

Assim o Relatório Final de Análise de Segurança (RFAS) atualmente está organizado em 19 capítulos, com o seguinte conteúdo:

- Capítulo 1 – Introdução e Descrição Geral da Planta.
- Capítulo 2 – Característica do Sítio.
- Capítulo 3 – Projeto das Estruturas, Componentes, Equipamentos e Sistemas.
- Capítulo 4 – Reator.
- Capítulo 5 – Sistema de refrigeração do Reator e Sistemas Conectados.
- Capítulo 6 – Engenharia de Segurança.
- Capítulo 7 – Instrumentação e Controle.
- Capítulo 8 – Sistemas Elétricos.
- Capítulo 9 – Sistemas Auxiliares.
- Capítulo 10 – Sistema Secundário Água-Vapor.
- Capítulo 11 – Gerenciamento de Rejeitos Radioativos.
- Capítulo 12 – Proteção Radiológica.
- Capítulo 13 – Condução da Operação.
- Capítulo 14 – Operação de Testes iniciais.
- Capítulo 15 – Análise de Acidente.
- Capítulo 16 – Especificação Técnica.
- Capítulo 17 – Programa da Garantia da Qualidade.
- Capítulo 18 – Engenharia de Fatores Humanos.
- Capítulo 19 – Avaliação Probabilística de Segurança.

As normas e padrões industriais codificam as boas práticas de engenharia e constituem o primeiro nível na cadeia de requisitos reguladores. Em geral, os guias reguladores são códigos e padrões industriais que a NRC reconhece como práticas seguras de engenharia. Alguns códigos são considerados obrigatórios e são explicitamente referidos no artigo 50.55a do 10 CFR Parte 50 (NRC, 2009a), por

exemplo, as normas IEEE Std 279 "*Criteria for Protection Systems for Nuclear Power Plant*" (IEEE,1971) e a IEEE Std 603 "*Criteria for Safety Systems for Nuclear Power Plant*" (IEEE, 1980b).

Essas normas industriais, em geral, são preparadas por instituições com grande experiência e tradição na elaboração de padrões e que passaram a produzir normas especiais para aplicação na área nuclear. Este conjunto de códigos e normas passou a ser designado como "ANSI Nuclear Standards" (BARROSO, 1982). As principais instituições participantes são:

- *American Society of Mechanical Engineers (ASME);*
- *Institute of Electrical and Electronics Engineers (IEEE);*
- *American Society for Testing Materials (ASTM);*
- *American Nuclear Society (ANS);*
- *Health Physics Society (HPS);*
- *American Institute of Chemical Engineers (AIChE);*
- *Institute of Nuclear Materials Management (INMM).*

Outra categoria de documentos utilizados pela NRC como apoio à sua atividade reguladora são os denominados NUREG, que são relatórios técnicos sobre temas diversos e com uma grande variedade de aplicações. Destacam-se, entre estes, o adotado pela CNEN como orientação para o seu processo de avaliação de Relatórios de Análise de Segurança (RAS), submetidos dentro do processo de licenciamento, o NUREG 0800 "*Standard Review Plan for Review of Safety Analysis Reports for Nuclear Power Plants*" (NRC, 1997b).

A partir de 1983, como mais uma decorrência do acidente na usina nuclear *Three Mile Island*, a NRC decidiu incorporar mais dois capítulos no seu Plano de

Revisão (NUREG 0800), abrangendo a área da Engenharia de Fatores Humanos e a área de Avaliação Probabilística de Segurança (APS).

4.2 HISTÓRICO DA REGULAÇÃO DOS SISTEMAS DE I & C DIGITAL EM USINAS NUCLEARES

A IEEE Std 279 (IEEE, 1971) foi a primeira norma industrial dirigida para sistemas relacionados com a segurança em usinas nucleares. Descreve critérios para Sistemas de I & C de Classe IE (relacionado com a segurança) em usinas nucleares, que permanecem relevantes até hoje como, por exemplo: critério de falha única, separação entre sistemas de segurança e de controle e independência de canais. A norma foi preparada por muitos pesquisadores, engenheiros e pessoas de órgãos reguladores que foram instrumentistas no projeto e na aprovação dos sistemas de I & C originais nas primeiras usinas nucleares operadas nos Estados Unidos. A maioria dos sistemas de I & C das usinas operadas atualmente foi licenciada com base na IEEE Std 279 (IEEE, 1971). Esta norma também é o único padrão industrial incorporado no Code of Federal Regulations - 10CFR50.55a(h) (NRC, 2009a).

A seguir são mostrados os tópicos discutidos na IEEE Std 279 (IEEE, 1971). O esquema numerado é o mesmo usado na IEEE Std 279 (IEEE, 1971):

- *4.1 General Functional Requirement.*
- *4.2 Single Failure Criterion: "Any single failure within the protection system shall not prevent proper protective action at the system level when required".*
- *4.3 Quality of Components and Modules.*
- *4.4 Equipment Qualification.*
- *4.5 Channel Integrity.*
- *4.6 Channel Independence.*
- *4.7 Control and Protection System Interaction.*

- *4.8 Derivation of System Inputs.*
- *4.9 Capability for Sensor Checks.*
- *4.10 Capability for Test and Calibration.*
- *4.11 Channel Bypass or Removal from Operation.*
- *4.12 Operating Bypasses.*
- *4.13 Indication of Bypasses.*
- *4.14 Access to Means for Bypassing.*
- *4.15 Multiple Set Points.*
- *4.16 Completion of Protective Action Once It Is Initiated.*
- *4.17 Manual Initiation.*
- *4.18 Access to Set Points Adjustments, Calibration, and Test Points.*
- *4.19 Identification of protective Actions.*
- *4.20 Information Read-Out.*
- *4.21 Systems Repair.*
- *4.22 Identification.*

Algumas normas da indústria foram desenvolvidas no período de 1971-1980 para esclarecer a IEEE Std 279 (IEEE, 1971) e alguns tópicos não considerados na IEEE Std 279 (IEEE, 1971). Todas estas normas sofreram uma ou mais revisões para cada um de seus tópicos inicias. Porém, a IEEE Std 279 (IEEE, 1971) permanece como foi originalmente aprovada.

- A norma IEEE Std 603–1980 (IEEE, 1980b), é efetivamente uma atualização da IEEE Std 279-1971 (IEEE, 1971). Ela foi revisada várias vezes e em 1995 a norma IEEE Std 603 –1991 (IEEE, 1980b) foi endossada através do guia regulador RG-1.153 (NRC, 1981b).
- As normas IEEE Std 323 (IEEE, 1999) e IEEE Std 344 (IEEE, 1998a) esclarecem a qualificação ambiental (temperatura, pressão e radiação) e

condições sísmicas como sistemas de Classe 1E descritos na norma IEEE Std 279 (IEEE, 1971).

- A norma IEEE Std 338 (IEEE, 1980a) provê orientação detalhada para a implantação das seções 4.9, 4.10 e partes de 4.19 e 4.20 na IEEE Std 279 (IEEE, 1971).
- A norma IEEE Std 379 (IEEE, 1987) esclarece os critérios de falha única da seção 4.2 na IEEE Std 279 (IEEE, 1971).

Depois do acidente em Three Mile Island em 1979 a NRC desenvolveu um guia regulador RG-1.97 (NRC, 1981a) e a IEEE e a ANS desenvolveram uma norma, IEEE Std 497 (IEEE, 1981), que é consistente com o RG 1.97 (NRC, 1981a).

Como já existiam usinas nucleares licenciadas e operacionais, houve a necessidade de criar um mecanismo para expedir a aprovação de mudanças secundárias significativas em equipamentos da usina que não são de segurança. Foi emitida uma seção nova do *Code of Federal Regulations* (CFR), 10CFR50.59 (NRC, 2009b) que permitem licenças de modificações de projeto, desde que seja comprovado que não há mudança na base do licenciamento ou não requer modificações nas especificações técnicas. O CFR, junto com o EPRI, publicou NSAC 125 (NRC, 1998b), que é um guia para as usinas nucleares, para implantar modificações, referenciado como modificações 10CFR50.59 (NRC, 2009b).

Em 1992 a NRC negou um pedido de atualização da I & C digital de um Sistema de Proteção do Reator (SPR) de uma usina nuclear, que efetivamente requeria que toda a atualização digital fosse revisada pelo pessoal da NRC, e conseqüentemente, desaprovou uma modificação com base no 10CFR50.59 (NRC, 2009b). As operadoras de usinas nucleares solicitaram ao EPRI o desenvolvimento de um guia para prover orientações para implantar atualizações na I & C analógica para digital usando o processo 10CFR50.59 (NRC, 2009b). O EPRI modificou o processo do NSAC 125 (NRC, 1998b) ajustando as exigências para uma atualização digital. Foi

criado um comitê representado pelos engenheiros de I & C das usinas e depois de numerosas reuniões e revisões, a aprovação do consenso foi adquirida em 1993. O EPRI emitiu um documento (EPRI, 1995), usando o processo 10 CFR 50.59 (NRC, 2009b). Em maio de 1995, a NRC endossou um documento a respeito (EPRI, 1995). Em 2001, o guia foi revisado para refletir mudanças no processo do 10 CFR 50.59 (NRC, 2009b) e foi publicado como EPRI TR-102348 Revisão 1 (NEI 01-01) (EPRI, 2002).

O guia do EPRI para licenciamento das atualizações da I & C digitais descreve um procedimento aceitável de como a I & C digital e os tópicos de licenciamento associados podem ser encaminhados no processo de modificação de projeto de acordo com as avaliações do 10 CFR 50.59 (NRC, 2009b). Também provê orientação em relação às falhas de causa comuns em uma I & C digital, especificamente através da avaliação da defesa em profundidade e diversidade e o uso do conhecimento do risco (*risk insight*) em avaliações D3.

4.3 GUIAS REGULADORES, NORMAS E DIRETRIZES MAIS RELEVANTES NA INCORPORAÇÃO DOS SISTEMAS DE I & C DIGITAIS NA AVALIAÇÃO PROBABILÍSTICA DE SEGURANÇA (APS)

As duas normas que são mais relevantes em relação à incorporação dos sistemas de I & C digitais em uma APS de usinas nucleares, são a IEEE Std 603-1998 (IEEE, 1998b) e a IEEE Std 7-4.3.2-2003 (IEEE, 2003). O guia regulador da NRC RG 1.153 (NRC, 1981b) e o RG 1.152 (NRC, 1997a) endossam, respectivamente, as versões mais novas destas duas normas. Estes dois guias reguladores mais o Capitulo 7 do *Standard Review Plan - NUREG-0800* (NRC, 1997b) proveem as orientações mais relevantes do projeto e licenciamento dos sistemas de I & C digitais em usinas nucleares. Conseqüentemente, qualquer metodologia proposta para

sistemas de I & C digitais a ser incorporada em uma APS tem que estar de acordo com esta estrutura reguladora.

4.3.1 RG 1.153 (NRC, 1981b) E IEEE Std 603-1998 (IEEE, 1998b).

A norma IEEE Std 603 "*Standard Criteria for Safety Systems in Nuclear Generating Stations*" (IEEE, 1998b) é uma atualização e expansão da maioria das seções da IEEE Std 279 (IEEE, 1971). Os sistemas de I & C digitais da maioria das usinas operacionais atuais encontram quase todas as orientações para base de licenciamento na IEEE Std 603 (IEEE, 1998b); as orientações que não estão descrita nelas são encontradas na IEEE Std 279 (IEEE, 1971).

De acordo com a posição reguladora da NRC, para estar em conformidade com os requisitos da norma IEEE Std 603-1998 (IEEE, 1998b), provê um método aceitável para satisfazer os requisitos reguladores do projeto, confiabilidade, qualificação, e testabilidade da instrumentação e controle dos sistemas de segurança da usinas nucleares.

4.3.2 RG 1.152 (NRC, 1997a) E IEEE Std 7.4.3.2-2003 (IEEE, 2003).

O guia regulador RG 1.152 (NRC, 1997a) e a norma IEEE Std 7.4.3.2 (IEEE, 2003), esclarecem tópicos relacionados com os sistemas digitais no RG 1.153 (NRC, 1981b) e na norma IEEE Std 603-1998 (IEEE, 1998b). As duas normas devem ser aplicadas simultaneamente a sistemas digitais.

IEEE Std 7-4.3.2 (IEEE, 2003) foi preparada pelo comitê de engenharia de usinas nucleares do *Institute of Electrical and Electronics Engineers* (IEEE) e o comitê de normas de usinas nucleares da *American Nuclear Society* (ANS). A NRC trabalhou com o IEEE e a ANS desenvolvendo a IEEE Std 7-4.3.2 (IEEE, 2003) para assegurar que a orientação provida pela norma tivesse consenso e fosse consistente com os

requisitos reguladores. A IEEE Std 7-4.3.2 (IEEE, 2003) evoluiu de duas versões anteriores: a de 1993 e a de 1982. Esta norma identifica diretrizes para computadores digitais (inclusive *hardware, software, firmware*, e interfaces) completando a IEEE Std 603-1998 (IEEE, 1998b). A NRC reconhece que o processo de desenvolvimento para sistemas de computador continua evoluindo.

Sistemas de I & C digitais compartilham transmissões de dados, funções, e equipamento de processo mais que os sistemas analógicos. Embora estes compartilhamentos sejam bases para muitas das vantagens dos sistemas digitais, também existe a preocupação com respeito a sua vulnerabilidade para um tipo diferente de falha. A preocupação é que um projeto que usa software, bancos de dados e equipamento de processos compartilhados tem o potencial para propagar uma falha de causa comum (FCC) em equipamento redundante. Outra preocupação é o erro programado no software que pode derrotar a redundância alcançada pela estrutura de hardware. Por causa destas preocupações, a NRC colocou ênfase no estudo da defesa em profundidade contra a propagação de FCC.

O princípio da defesa em profundidade é prover vários níveis ou escalões de defesa para assegurar a segurança da usina, tal que as falhas em equipamentos e erro humano não resultem em uma ameaça à segurança do público.

A NRC não endossa, até o momento, o conceito de metas de confiabilidade quantitativas como meio de determinar a confiabilidade dos computadores digitais usados em sistemas de segurança. Conforme discutido na Seção 5.15 da IEEE Std 7-4.3.2 (IEEE, 2003) a aceitação pela NRC da confiabilidade do sistema de computador está baseada em critérios determinísticos tanto para o hardware como para o software.

Falhas de software que não são conseqüências de falhas de hardware são causadas por erros de projeto e não seguem o comportamento de falhas aleatórias usadas em confiabilidade de hardware. Acredita-se que a determinação da confiabilidade quantitativa, usando uma combinação de análise, testabilidade e

experiência operacional, provê informações importantes da segurança do sistema de computadores e também um nível adicional de confiabilidade em seu desempenho seguro. A NRC reconhece que os sistemas digitais comercialmente disponíveis em aplicações nucleares confiam muito em métodos quantitativos por causa dos dados de experiências operacionais (como número de horas de operação com sucesso) acumuladas durante os anos de funcionamento. A NRC não pretende impedir que os dados de experiência operacionais sejam usados como justificativa de um desempenho com sucesso.

A norma IEEE Std 7-4.3.2 (IEEE, 2003) possui oito anexos. Esta norma declara que esses anexos são informativos e não fazem parte de IEEE 7-4.3.2 (IEEE, 2003). A NRC acredita que estes anexos contêm informações que podem ser úteis, porém, não devem ser vistos como a única forma ou método possível de solução. Como não foi alcançado um consenso na indústria nuclear, a NRC não endossou estes anexos.

A posição reguladora da NRC considera que ter conformidade com as exigências da IEEE Std 7-4.3.2 (IEEE, 2003), com a exceção somente das metas de confiabilidade quantitativas (Seção 5.15), é um método aceitável para satisfazer os requisitos reguladores com respeito à alta confiabilidade funcional e exigências de qualidade de projeto para computadores usados como componentes de um sistema de segurança.

A norma IEEE Std 7-4.3.2 (IEEE, 2003) especifica exigências adicionais de sistemas digitais para os critérios e exigências da IEEE Std 603-1998 (IEEE, 1998b). Os critérios contidos nesta norma quando usados junto com os critérios e exigências da IEEE Std 603 (IEEE, 1998b) estabelecem o mínimo de requisitos funcionais e exigências de projeto para computadores usados em componentes de sistemas de segurança em usinas nucleares, conforme mostra na Tabela 4.2.

Tabela 4.2: Relação entre a norma IEEE Std 603-1998 (IEEE, 1998b) e a IEEE Std 7-4.3.2 (IEEE, 2003).

Critérios da IEE Std 603-1998	**Exigências Adicionais da IEEE Std 7-4.3.2-2003**	**Anexos**
4. *Safety System Design Basis*	4. *Safety System Design Basis*	Anexo B
5. *Safety System Criteria*	-	Anexo B
5.1 *Single Failure Criterion*	-	-
5.2 *Completion of Protection Action*	-	-
5.3 *Quality*	5.3.1 *Software Development* 5.3.2 *Software Tools* 5.3.3 *Verification and validation (V&V)* 5.3.4 *Independent Verification and Validation (IV&V)* 5.3.5 *Software Configuration Management* 5.3.6 *Software Project Risk Management*	Anexos D e F
5.4 *Equipment Qualification*	5.4.1 *Testing Software and Diagnostics* 5.4.2 *Qualification of existing Compilers*	Anexo C
5.5 *System integrity*	5.5.1 *Design for Computer Integrity* 5.5.2 *Design for Test and Calibration*	Anexos B e C
5.6 *Independence*	5.6 *Independence*	Anexo E
5.7 *Capability for Test and Calibration*	-	-
5.8 *Information Displays*	-	-
5.9 *Control of Access*	-	-
5.10 *Repair*	-	-
5.11 *Identification*	5.11 *Identification*	-
5.12 *Auxiliary Features*	-	-
5.13 *Multi-Unit Stations*	-	-
5.14 *Human Factor Considerations*	-	-
5.15 *Reliability*	5.15 *Reliability*	Anexo F
6. *Sense and Command Features Functional Design Requirements*	-	-
7. *Execute Feature Functional Design Requirements*	-	-
8. *Power Source Requirements*	-	-

4.3.3 CAPÍTULO 7 DO *STANDARD REVIEW PLAN* (NRC, 1997b)

A atualização do Capitulo 7 (I & C) do *Standard Review Plan* (NRC, 1997b) tem como objetivo primário incorporar as orientações de revisão para os sistemas I & C digitais em usinas nucleares relacionados com a segurança e de sistemas não relacionados com a segurança. As novas diretrizes primárias pertinentes a atualizações digitais são encontradas na *Branch Technical Positions* (BTP):

- BTP 14, "*Guidance on Software Reviews for Digital Computer-Based I & C Systems*" (NRC, 1997c), descreve a posição da NRC em um método de desenvolvimento aceitável e critérios de aceitação especificos para software critico de segurança. A metodologia é prescrita em termos de desenvolvimento de processo e critérios de aceitação. O processo de desenvolvimento aceitável focaliza em desenvolvimento de alta qualidade e os critérios de aceitação focalizam os testes para satisfazer as exigências de projeto e de subsistema individuais. O método é difícil e não necessariamente requer teste para todas as condições operacionais esperadas.
- BTP 18, "*Guidance on the Use of Programmable Logical Controllers in Digital Computer-Based I & C Systems*" (NRC, 1997d).
- BTP 19 "*Guidance for Evaluation of Defense-in-Depth and Diversity (D3) in Digital Computer-Based Instrumentation and Control Systems*" (NRC, 1997e), descreve a posição da NRC em relação a D3, descreve um método aceitável para avaliação do desempenho do D3 e critérios de aceitação especifico.
- BTP 21, "*Guidance on Digital Computer Real-Time Performance*" (NRC, 1997f).

4.3.4 RG 1.174 (NRC, 1998a) Informação do Risco

Este não é um guia regulador especifico para I & C, mas um guia regulador para qualquer mudança na base de licenciamento da usina. Pode ser aplicado para avaliar o risco que uma mudança proposta no sistema de I & C introduzirá.

A abordagem com informação do risco, para o processo de tomada de decisão reguladora, representa uma filosofia pela qual os resultados e decisões advindas da avaliação do risco são considerados em conjunto com outros fatores. A abordagem da informação do risco amplia e melhora o tratamento determinístico, pois:

a) Permite considerações explícitas de um amplo conjunto de mudanças para a segurança;

b) Provê argumentos lógicos para priorizar estas mudanças baseadas no risco, experiência operacional e/ou julgamento de engenharia;

c) Facilita as considerações de um amplo conjunto de recursos para defender estas mudanças;

d) Identifica e qualifica fontes de incertezas na análise;

e) Leva a uma tomada de decisão adequada, provendo um mecanismo para testar sensibilidade de resultados para um conjunto de suposições.

Uma abordagem reguladora com informação do risco pode ser usada para reduzir o conservadorismo desnecessário em um tratamento determinístico, ou pode ser usado para identificar áreas com conservadorismo insuficiente na análise determinística e providenciar as bases e requisitos adicionais ou ações reguladoras.

A abordagem informação do risco situa-se entre as abordagens com base no risco e o tratamento puramente determinístico. Os detalhes da emissão reguladora em consideração determinarão aonde a decisão da informação do risco se situará neste espectro.

O conceito de defesa em profundidade continua a ser o princípio da prática reguladora. Os resultados e decisões advindas da avaliação do risco podem tornar os

elementos da defesa em profundidade mais claros, pelo alcance prático de quantificações.

A regulamentação pode ser tanto prescritiva quanto baseada no desempenho. Os requisitos prescritivos especificam aspectos particulares, ações ou elementos programáticos para serem incluídos no projeto ou processo, como um meio de alcançar o objetivo desejado. Um requisito baseado no desempenho depende de resultados (medidos ou calculados, isto é resultados de desempenho) a serem encontrados. Contudo, provê maior flexibilidade ao licenciado para atingir estes resultados.

4.3.5 EPRI TR1002835 (EPRI, 2004)

Este guia mostra uma abordagem alternativa ao BTP 19 (NRC, 1997e). Recomenda uma integração de métodos determinísticos, como prescrito no BTP 19 (NRC, 1997e), e métodos de informação do risco com o uso de APS para determinar o risco potencial de uma mudança na base do licenciamento, representado por uma atualização digital proposta no RG 1.174 (NRC, 1998a) para critérios de aceitação da mudança. Este guia não foi endossada pela NRC.

4.3.6 NUREG/CR-6303 (NRC, 1994c)

Descreve o método para a avaliação do desempenho da Defesa em Profundidade e Diversidade que são referenciados no BTP-19 (NRC, 1997e). Também inclui orientações para determinar se há diversidade suficiente entre partes diferentes de um sistema de I & C digital, de modo que eles não estejam sujeitos à mesma falha de causa comum. Este relatório apresenta uma abordagem dirigida a características do projeto digital que possuem potencial para FCC e incorporam o uso de informação do risco.

5 METODOLOGIAS APLICADAS À AVALIAÇÃO DE DEFESA EM PROFUNDIDADE E DIVERSIDADE DE I & C DIGITAL

5.1 INTRODUÇÃO

O objetivo deste capítulo é apresentar as duas principais metodologias que utilizam a avaliação de defesa em profundidade e diversidade em sistemas de I & C digital. A primeira metodologia, apresentada no item 5.2, é a da NRC, que mostra uma abordagem determinística da avaliação D3 (NRC, 1997e & NRC, 1994c). A segunda, apresentada no item 5.3, é a do EPRI, que mostra uma abordagem utilizando Avaliação Probabilística de Segurança (APS), aplicando informação do risco (EPRI, 2004).

5.1.1 DEFESA EM PROFUNDIDADE

Defesa em profundidade é um princípio fundamental no projeto e operação de uma usina nuclear, sendo base para uma tecnologia essencial de segurança. Toda a atividade de segurança, quer sejam organizacional, comportamental ou relacionada a equipamento, está sujeita a camadas ou níveis de segurança sobrepostos, a fim de que, se uma falha acontecer, esta será compensada ou corrigida sem que haja dano para os trabalhadores ou indivíduos do público. Esta ideia de níveis múltiplos (ou escalões) de proteção é a característica central da defesa em profundidade e é repetidamente usada nos princípios de segurança aplicados em usinas nucleares (IAEA, 1984 & IAEA, 1988a).

O conceito de defesa em profundidade provê uma estratégia geral para medidas de segurança e características da usina nuclear. Quando corretamente aplicada, assegura que nenhuma falha única humana ou mecânica poderia conduzir ao dano ao público e as combinações de falhas conduziriam a um dano pequeno.

A defesa em profundidade ajuda a estabelecer que as três funções básicas de segurança de uma central nuclear estejam preservadas (controle da potência, resfriamento do combustível e confinamento dos materiais radioativos) e com isso garante-se que materiais radioativos não alcancem as pessoas ou o ambiente.

5.1.1.1 NÍVEIS DE PROTEÇÃO

A defesa em profundidade é implantada por meio de uma série de barreiras físicas e níveis de proteção, por exemplo: barreiras físicas podem ser a matriz do combustível, o encamisamento do combustível, o reator, o sistema primário de refrigeração, a contenção e o prédio do reator, conforme mostrado na Figura 5.1.

Níveis de proteção são:

- Uma combinação de projetos conservativos, garantia da qualidade e cultura de segurança;
- Controle da operação normal e anormal e detecção de falhas;
- Sistemas de segurança e sistemas de proteção;
- Gerenciamento de acidentes;
- Resposta à emergência.

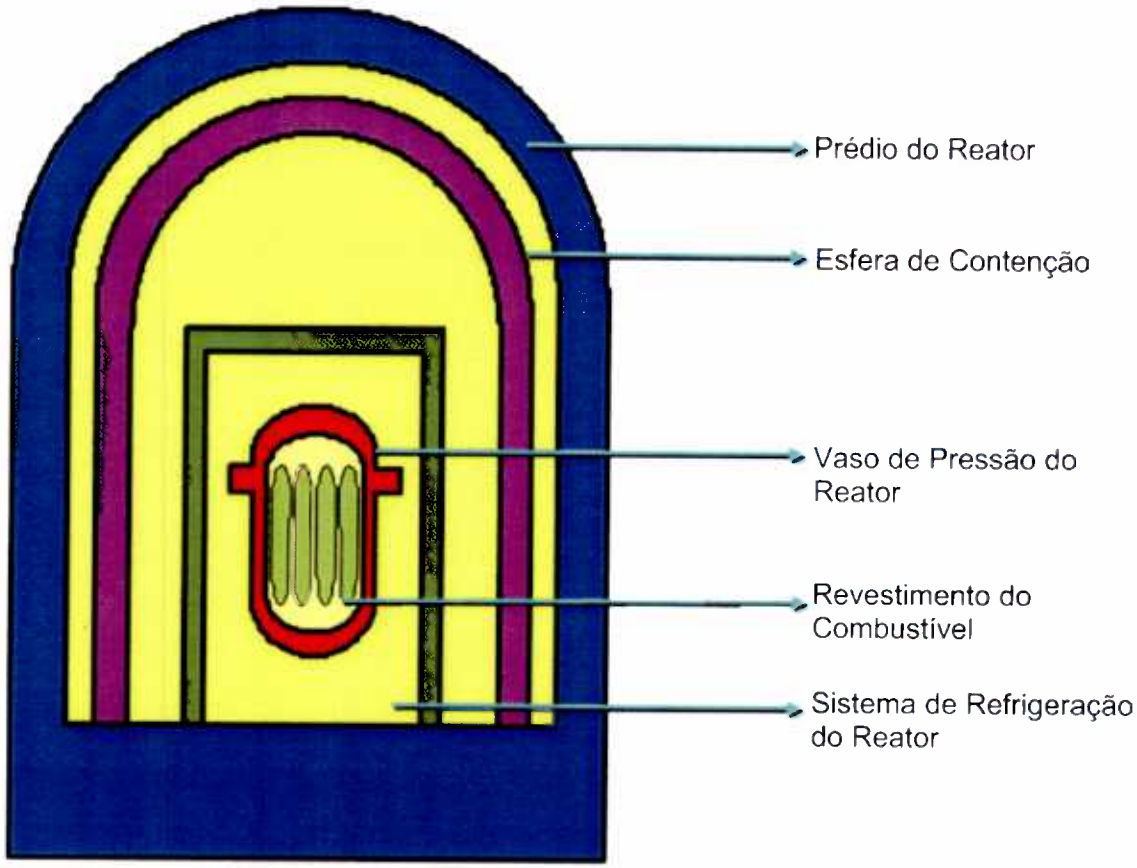


Figura 5.1 – Defesa em profundidade: barreiras e níveis de proteção (CNEN, 2003).

Dentro das funções de segurança da I & C, a defesa em profundidade é alcançada com uma hierarquia de sistemas que proveem níveis progressivos de proteção. Na maioria dos reatores, o sistema de controle é categorizado como o primeiro nível de proteção e o sistema proteção (ou segurança) provê o nível final. Em algumas usinas nucleares, sistemas de limitação proveem um nível intermediário de segurança entre o controle e sistemas de proteção (IAEA, 1999c).

A defesa em profundidade não é possível para todas as falhas postuladas concebíveis do sistema de I & C. Para algumas contingências, a defesa em profundidade confia em barreiras físicas e/ou outros níveis de proteção fora dos sistemas de I & C.

5.1.1.2 CATEGORIZAÇÃO DAS FUNÇÕES DA I & C

Funções diferentes da I & C, sistemas associados e equipamentos, conectados com vários níveis da filosofia da defesa em profundidade, são classificados de acordo com a sua importância para a segurança. Requisitos de funcionalidade, confiabilidade, desempenho e qualificação ambiental destas funções, sistemas e equipamentos têm de forma crescente se tornado uma exigência nas últimas décadas. A categorização baseada no guia de segurança da Agência Internacional de Energia Atômica (IAEA, 1984) e a norma IEC-1226 (IEC, 1993) são mostradas na Tabela 5.1. Esta classificação é semelhante à da NRC (NRC, 1983).

Tabela 5.1 – Categoria da IEC das funções da I & C (IEC, 1993).

Categoria	Descrição	Sistema
A	Funções, sistemas associados e equipamento (Dispositivo Técnico de Segurança - DTS) que têm o principal papel na realização ou manutenção da segurança da Central Nuclear. Os DTS previnem eventos iniciadores postulados ou mitigam as suas conseqüências.	Sistema de Proteção do Reator, Sistema de Atuação de Segurança e Sistema de Suporte à Segurança.
B	São os DTS que fazem um papel complementar aos DTS categoria A na realização ou manutenção da segurança da central nuclear. A operação dos DTS categoria B pode evitar a necessidade de iniciar a operação dos DTS da categoria A. Os DTS da categoria B podem melhorar ou complementar a execução dos DTS da categoria A na mitigação eventos iniciadores postulados, de forma a evitar ou minimizar danos que a usina ou equipamentos possam sofrer ou que haja liberação de radioatividade.	Sistema automático de Controle, Sistema de Limitação e Sistema de processamento de dados da sala de controle principal.
C	São os DTS que fazem um papel auxiliar ou indireto na realização ou manutenção da segurança da central nuclear.	Sistema de Comunicação de Emergência e Sistema de Monitoração de Radiação.

5.1.2 DIVERSIDADE

Diversidade é o uso de dois ou mais meios físicos ou funcionalmente diferentes para executar a mesma função, protegendo contra certos tipos de falhas de causa comum que ocorrem devido ao projeto ou de erros de manutenção. A diversidade pode ser provida pelo uso de hardware e software de projetos ou origens diferentes que desempenham a mesma função (por exemplo: computadores de fabricantes diferentes em dois sistemas de segurança). Falhas devido a erros no projeto de um sistema não afetariam assim o desempenho do outro.

Outro modo de assegurar a diversidade é usando parâmetros físicos diferentes (sinais de processo e de neutrônica para iniciar uma ação) ou usando mecanismos físicos diferentes (um sistema de desligamento poderia usar as barras de controle ou injeção a alta pressão de ácido bórico para desligar o reator).

5.2 ABORDAGEM D3 DA NRC

A NRC tem manifestado a preocupação de que os erros no projeto de software devido aos programas fontes e a FCC (NRC, 1997e, NRC, 1991 & NRC, 1993), poderiam degradar a atual defesa em profundidade fornecida pelos quatro escalões de defesa: os sistemas de controle, Sistema de Desarme do Reator, Dispositivos Técnicos de Segurança (DTS) e o Sistema de Monitoramento e Indicações. Sua posição para resolver esta questão é firmada em quatro pontos no BTP-19 (NRC, 1997e & NRC, 1994c):

1. O requerente à licença deverá avaliar a defesa em profundidade e diversidade do Sistema de I & C proposta, para demonstrar que as vulnerabilidades a FCC foram tratadas adequadamente.
2. Ao realizar a avaliação, o requerente deverá analisar cada FCC postulada para cada evento que é avaliado na análise do acidente no Relatório de Análise de Segurança (RAS), utilizando os melhores métodos de estimativa. O

requerente deverá demonstrar uma adequada diversidade no projeto para cada um destes eventos.

3. Se uma FCC postulada conseguir desabilitar uma função de segurança, então os diversos meios de defesa devem ser requeridos para realizar a mesma função ou uma função diferente, tendo uma base documentada de que esses meios não estejam sujeitos as mesmas FCC. As diversas funções poderão ser executadas por um sistema que não seja de segurança, se o sistema for de qualidade suficiente para desempenhar as funções necessárias no âmbito das condições associadas ao evento.

4. Um conjunto de displays e controles localizados na sala de controle principal deve ser previsto para atuação manual em nível de sistema para as funções críticas de segurança e monitoramento de parâmetros que dão suporte às funções de segurança. Os displays e controles devem ser independentes e diferentes do sistema de computadores de segurança.

Todos os quatro pontos são aplicáveis aos reatores avançados. Os pontos 1, 2 e 3 aplicam-se a usinas em operação que vão substituir a atual I & C analógica do Sistema de Desarme do Reator e dos Dispositivos Técnicos de Segurança por uma I & C digital. O NUREG/CR-6303 (NRC, 1994c) estabelece orientações detalhadas para a realização de uma avaliação D3, utilizando um método de avaliação (chamado Método Determinístico BTP-19) que a NRC reconhece como aceitável.

5.2.1 RELAÇÃO COM A AVALIAÇÃO DO 10 CFR 50.59 (NRC, 2009b)

A regulamentação 10 CFR 50.59 (NRC, 2009b) especifica os critérios para determinar uma alteração da licença necessária antes de implantar a modificação na usina. Conforme discutido no EPRI TR-102348 (EPRI, 2002) e NEI 96-07 Revisão 1 (NEI 96-07, 2000) as únicas falhas que necessitam de uma consideração especial e uma revisão da NRC com base em uma avaliação no 10 CFR 50.59 (NRC, 2009b),

são aquelas estimativas de falhas já consideradas na base do licenciamento da usina, como descrito no Relatório Análise de Segurança (RAS).

Para os equipamentos que são avaliados para aplicações de segurança, a probabilidade de FCC digital deve ser bem inferior à probabilidade de falhas simples, assumida na base do licenciamento. Assim, embora o potencial de FCC digitais deva ser considerado na avaliação, em geral não necessariamente leva por si só a uma alteração na licença pelo 10 CFR 50.59 (NRC, 2009b).

As FCC Digitais e suas potenciais questões D3 devem ser abordadas no projeto de atualização da I & C (independente da avaliação do 10 CFR 50.59). Informações sobre o projeto do equipamento digital, qualificação e aplicação, devem ser avaliadas para garantir que a probabilidade das FCC digitais seja mais baixa que a probabilidade de falhas simples aleatórias, assumida na base do licenciamento.

5.2.2 QUANDO UMA AVALIAÇÃO D3 É NECESSÁRIA (COM PERSPECTIVAS DA REGULAMENTAÇÃO DA NRC)

As avaliações D3 não são exigidas para todas as atualizações digitais, com base na orientação reguladora existente. Segundo o *Standard Review Plan* Capítulo 7, Seção 7.0a SRP-NUREG-0800 (NRC, 1997b), a NRC espera uma avaliação D3 a ser realizada para atualizações digitais que envolva o Sistema de Desarme do Reator e ou Dispositivos Técnicos de Segurança (DTS). O SRP-NUREG 0800 (NRC, 1997b) ainda diz que a avaliação D3 deve ser realizada especificamente para o sistema I & C de segurança incorporado à tecnologia de computadores digitais.

A posição da NRC foi reiterada no capítulo 5.2.1 do EPRI TR-102348 (EPRI, 2002), que afirma que um processo formal de análise de defesa em profundidade e diversidade pelo BTP-19 (NRC, 1997e) é esperado somente para atualizações substanciais de I & C digital para o Sistema de Desarme do Reator e os Dispositivos Técnicos de Segurança. EPRI TR-102348 (EPRI, 2002) recomenda em caso de

dúvida, a revisão do Relatório de Avaliação de Segurança (RAS). O documento EPRI-TR-102348 (EPRI, 2002) determina se uma avaliação D3 deve ser realizada, quando uma série de pequenas atualizações ou modificações feitas na I & C.

5.3 ABORDAGEM D3 DO EPRI

O documento EPRI-TR1002835 (EPRI, 2004) traz orientações para dar suporte à utilização da avaliação de defesa em profundidade e diversidade (D3) em atualizações digitais que afetam o sistema de instrumentação e controle (I & C) de usinas nucleares. Para algumas atualizações digitais, uma avaliação de D3 é executada analisando o potencial de vulnerabilidade para falhas de causa comum do software ou outros sistemas digitais que possam simultaneamente afetar múltiplos trens ou sistemas.

O foco da avaliação D3 do EPRI (EPRI, 2004) está nas FCC em sistemas digitais que poderiam degradar a segurança da usina. As FCC digitais postuladas poderiam comprometer a redundância construída em sistemas de segurança, ou impactar na defesa em profundidade, controle e os sistemas monitoração.

Os métodos apresentados pelo EPRI combinam técnicas determinísticas e de informação do risco. O uso do conhecimento do risco pode ajudar a focalizar o esforço do D3 em áreas que potencialmente trariam maior benefício em termos de segurança da usina. Também permite dar garantia, em termos de confiabilidade e segurança, a um equipamento digital.

O EPRI apresenta 3 metodologias para a execução da avaliação D3 que são recomendados como alternativas à abordagem da avaliação determinística BTP-19 (NRC, 1997e):

- Método Determinístico Estendido, baseado na BTP-19 (NRC, 1997e), mas com *risk insights* aplicados.

- Método Padrão com informação do risco, baseado na utilização da PRA modificada de modo a refletir a atualização digital.
- Método Simplificado com informação do risco, que utilizam dados a partir da APS já existente (não modificada).

Os três métodos são composições de abordagens determinísticas e da informação do risco.

6 METODOLOGIA

6.1 INTRODUÇÃO

A abordagem proposta nessa tese tem por base a informação do risco e consiste em avaliar os eventos operacionais utilizando o relacionamento entre os seguintes critérios de confiabilidade: falha, tipo de falha, taxa de falha, níveis de defesa em profundidade e diversidade (Apêndice A e Apêndice B). O objetivo dessa abordagem é possibilitar a identificação dos principais modos de falha dos sistemas digitais, com potencial para as falhas de causa comum (FCC) no software, possíveis vulnerabilidades do sistema de I & C digital, como também a avaliação das causas dominantes destes modos de falha. Desta forma, complementa a atual abordagem determinística e serve de base para a tomada de decisão ao licenciamento dessa nova tecnologia digital.

6.2 DEFINIÇÃO DOS CRITÉRIOS DE CONFIABILIDADE

O primeiro passo para fazer a avaliação dos eventos operacionais é definir os critérios de confiabilidade falha, tipo de falha, taxa de falha, nível de defesa em profundidade e diversidade.

6.2.1 CRITÉRIO FALHA

Para o critério 'falha' são consideradas duas categorias possíveis:

- Falha de causa comum (FCC);
- Falha simples (FS).

Foram dadas importâncias diferentes, em relação à confiabilidade, para as duas categorias de critério de falha. A FCC tem uma importância maior do que a FS. A

justificativa para essa afirmação é que a FCC pode quebrar o projeto de redundância e diversidade, como por exemplo, falha de causa comum nos quatro canais de I & C devido à falha de software, ou em diferentes placas de memórias de sistemas redundantes e diversos que, apesar de terem fabricantes diferentes, possuem componentes na grande maioria iguais (NRC, 1997e, NRC, 1991 & NRC, 1993). Por esse motivo os eventos operacionais que forem classificados como FCC terão resultados de nível de confiabilidade mais restritivos que os eventos operacionais que tiverem FS (Apêndices A e B).

6.2.2 CRITÉRIO TIPO DE FALHA

Para o critério 'tipo de falha' são consideradas três categorias possíveis de tipos de falha:

- Falha de Software (FSOFT);
- Falha de Hardware (FH);
- Falha da Interface Homem-Sistema (FIHS).

Para o critério 'tipo de falha' também foram dadas importâncias diferentes em relação à confiabilidade: a falha de software tem uma importância maior que os dois outros tipos de falha, a falha de hardware e a falha da interface homem-sistema, que possuem importâncias iguais. A principal justificativa para essa distinção importância é que os mecanismos de falha do software ainda não estão totalmente definidos, sendo classificados em sua grande maioria como FCC, podendo assim causar maior vulnerabilidade ao sistema de I & C digital do que os outros tipos de falha (KANG e SUNG, 2002). Por esse motivo, os relacionamentos que tiverem eventos operacionais classificados como FSOFT terão seus resultados mais restritivos do que os eventos que forem classificados como FH e FIHS (Apêndices A e B).

6.2.3 CRITÉRIO TAXA DE FALHA

Para o critério 'taxa de falha' foram criados intervalos respeitando a importância da FCC em relação à FS, conforme já definido no critério de 'falha' (Tabela 6.1).

Para as FCC foram definidos quatro intervalos de taxa de falha e para as FS foram definidos três, baseados na experiência operacional e no julgamento de especialista em avaliação de segurança de sistema de I & C digital (MODARRES, 2006), que entende que os quatro intervalos da FCC são mais restritivos que os três intervalos da FS e com isso os eventos operacionais que tiverem relacionamentos que se enquadrarem nesta condição terão resultados mais rigorosos (Apêndices A e B).

Tabela 6.1 – Intervalos da taxa de falha (λ) para FCC e para FS.

Intervalos (λ) para FCC	Intervalos (λ) para FS
$\lambda > 10^{-2}$	$\lambda > 10^{-2}$
$10^{-2} \geq \lambda > 10^{-4}$	$10^{-2} \geq \lambda > 10^{-5}$
$10^{-4} \geq \lambda > 10^{-6}$	$\lambda \leq 10^{-5}$
$\lambda \leq 10^{-6}$	-

6.2.4 CRITÉRIO NÍVEL DE DEFESA EM PROFUNDIDADE

Para o critério 'nível de defesa em profundidade' foram definidos quatro escalões de defesa baseados na estrutura e resposta do sistema de instrumentação e controle (Figura 6.1):

- Escalão nível 1: monitoração e indicação (M&I) - é um conjunto de sensores, *display* de parâmetro de segurança, controles manuais independentes requeridos para resposta humana a eventos.
- Escalão nível 2: controle (CTR) - são os equipamentos não de segurança que rotineiramente impedem excursões do reator em direção a regimes inseguros de funcionamento e são usados para o funcionamento normal do reator.

- Escalão nível 3: limitação (LIM) – sistema que monitora os desvios inadmissíveis de uma grande quantidade de variáveis de processo, e com ações escalonadas para levar a usina a condições operacionais normais. Uma parte dessas limitações não é de importância somente em operação de potência, mas também durante a partida e parada da usina, além dos casos de acidentes.
- Escalão nível 4: sistema de proteção do reator (SPR) - sistema de segurança da usina nuclear que reconhece as condições iniciais para a ocorrência de determinados acidentes e a ativação das medidas defensivas necessárias para evitá-los ou manter suas conseqüências dentro de limites pré-estabelecidos.

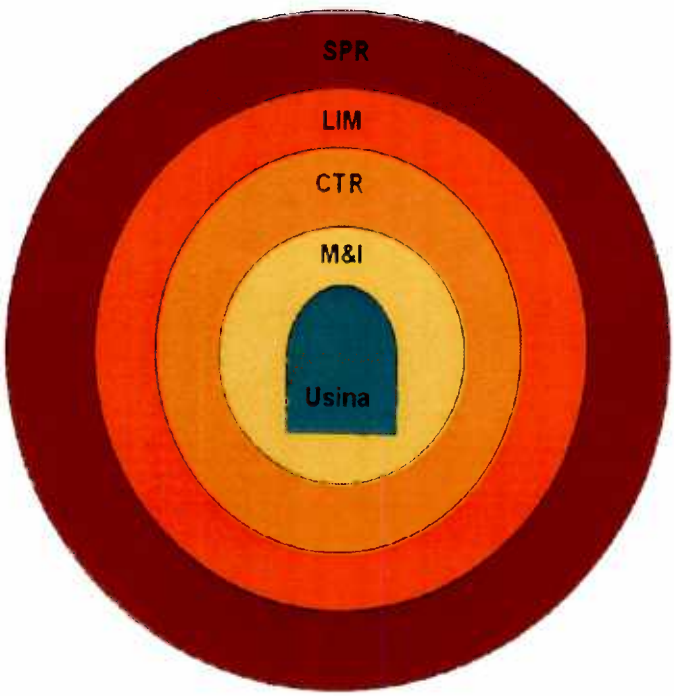


Figura 6.1 – Níveis de defesa em profundidade da I & C digital.

O nível de defesa em profundidade mais importante é o mais externo (SPR), conforme mostrado na Figura 6.1. Essa importância vai diminuindo até chegar no nível mais interno (M&I). Os eventos operacionais irão ser avaliados em relação ao nível de

defesa em profundiade que foi violado e o resultado dos relacionamentos irá ser mais restritivo ou não, observando também a importância desse nível de defesa em profundidade mostrado na avaliação (Apêndices A e B).

6.2.5 CRITÉRIO DIVERSIDADE

Para o critério 'diversidade' foram definidos cinco tipos de diversidade:

- de Projeto;
- de Equipamento
- Humana;
- de Sinal;
- de Software.

A diversidade de projeto consiste em:

- Diferentes tecnologias;
- Diferentes abordagens dentro de uma tecnologia (por exemplo, instrumentação com transformador acoplado à corrente alternada (AC) versus instrumentação com transformador acoplado à corrente contínua (DC);
- Arquitetura diferente (ou seja, arranjo e ligação de componentes diferentes).

A diversidade de equipamento consiste em:

- Diferentes fabricantes de projetos fundamentalmente distintos;
- O mesmo fabricante de projetos fundamentalmente diferentes;
- Diferentes fabricantes fazendo o mesmo projeto;
- Diferentes versões do mesmo projeto.

Em equipamentos de informática, há detalhes adicionais que ajudam no sentido de avaliar o grau de diversidade:

- Diferentes arquiteturas de computador;
- Diferentes versões de *chip*;
- Diferentes projetos de placas de circuito impresso (placa do processador, placas de memória ou placas de controle de periféricos);
- Diferentes estruturas de barramentos elétricos.

A diversidade humana consiste em:

- Diferentes organizações desenvolvendo etapas do projeto (especificação, desenvolvimento do sistema e V&V);
- Diferentes equipes de gerenciamento de engenharia dentro da mesma empresa;
- Diferentes projetistas, engenheiros ou programadores;
- Diferentes testadores, instaladores, ou o pessoal de certificação.

A diversidade de sinal consiste em:

- O mesmo parâmetro do reator ou de processo detectado por um conjunto redundante de diferentes sensores.

A diversidade de software consiste em:

- Diferentes algoritmos, lógica, e arquitetura de programa;
- Diferentes temporizações e ordens de execução;
- Diferentes linguagens de programação;
- Diferentes sistemas operacionais.

Os eventos operacionais que tiverem uma ou mais diversidade requerida irá ter resultados mais restritivos do que eventos que não requerem diversidade alguma (Apêndices A e B).

6.2.6 NÍVEIS DE CONFIABILIDADE

Após definir todos os critérios de confiabilidade, faz-se a avaliação do evento respeitando o relacionamento entre eles, conforme mostrados na Tabela A.1 do Apêndice A e no fluxograma de blocos do Apêndice B. O resultado gerado será enquadrado em cinco níveis de confiabilidade para os sistemas de I & C digitais, conforme mostrado na Tabela 6.2.

Tabela 6.2 – Níveis de confiabilidade (NC) dos sistemas de I & C digitais.

Nível	Cor	Descrição
Crítico	Preta	Nível crítico de confiabilidade - é o pior nível que um sistema de I & C digital pode alcançar. Usinas nucleares que apresentam sistemas de I & C digital com este nível de confiabilidade não garantem que os mesmos irão responder corretamente, principalmente em caso de acidentes severos. É necessário refazer toda a análise de segurança do projeto, procurando identificar problemas na especificação, desenvolvimento e verificação e validação do sistema.
Perigoso	Vermelha	Nível Perigoso de confiabilidade - Usinas nucleares que apresentam sistemas de I & C digital com este nível de confiabilidade precisam rever imediatamente a análise de segurança do projeto em conjunto com a avaliação D3 e os modos de falhas que resultaram neste nível de confiabilidade.
Alerta	Laranja	Nível de alerta de confiabilidade - demonstra a necessidade que a usina tem de atacar as vulnerabilidades do sistema de I & C digital, observando os modos de falhas encontradas nas suas avaliações e analisando que ações irão minimizar suas ocorrências e melhorando as barreiras de defesas em profundidade e diversidades.
Atenção	Amarelo	Nível de atenção de confiabilidade – mostra que o sistema de I & C digital ainda pode melhorar sua confiabilidade, devendo também observar os modos de falhas presentes em suas avaliações e estudando medidas para evitá-las ou reduzir assim a chance de ocorrência.

Satisfatório	Verde	Nível satisfatório de confiabilidade – é um nível aceitável de operação do sistema de I & C digital. Usinas que apresentam este nível de confiabilidade demonstram que todos os objetivos de segurança foram alcançados, mas precisam trabalhar para garantir que este nível de confiabilidade permaneça.

6.3 ESTUDO DE EVENTOS OPERACIONAIS

O estudo de eventos operacionais na área de I & C digital considera eventos ocorridos em usinas nucleares que sejam significativos para a segurança da usina, a fim de prover informações necessárias para gerar os resultados dos níveis de confiabilidade, estudos de anomalias operacionais, tendências, análise de padrões de ocorrências operacionais e vulnerabilidade dos sistemas de I & C digitais. A experiência operacional no mundo sobre sistemas de I & C digitais em usinas nucleares vem crescendo nos últimos anos e pode agregar conhecimento que permite uma avaliação do ponto de vista da informação do risco.

Como ponto de partida de nosso estudo sobre experiência operacional de sistemas de I & C digital, utilizamos como fonte de pesquisa para a aquisição dos dados operacionais alguns institutos e empresas que possuem em suas páginas na internet acesso às informações sobre eventos operacionais, conforme mostrado a seguir:

- *Westinghouse;*
- *Areva Framatome (ANP);*
- Agência Internacional de Energia Atômica (AIEA);
- *Electric Power Research Institute (EPRI);*
- *Vereinigung der Grosskraftwerksbeatrieber (VGB);*
- *Nuclear Regulatory Commission (NRC);*
- *Institute of Nuclear Power Operations (INPO);*
- *World Assocation of Nuclear Operators (WANO).*

As duas principais fontes de pesquisa utilizadas para a construção do banco de dados para o estudo foram os relatórios de incidentes da AIEA (*Incident Reporting System - IRS*) e os relatórios de eventos da NRC (*Licensee Event Report - LER*).

Foram incluidos no banco de dados 169 eventos operacionais na área de I & C digital de sete usinas nucleares no periodo de 1980 a 2006, com o objetivo de validar a metodologia (Apêndice C).

6.4 CONSTRUÇÃO DO BANCO DE DADOS DE EVENTOS OPERACIONAIS NA ÁREA DE I & C DIGITAL DE USINAS NUCLEARES

Com o objetivo de armazenar os dados coletados sobre eventos operacionais, foi construido um banco de dados para receber essas informações. Como primeiro passo para a construção desse banco de dados, foram definidas as informações a serem controladas por ele, divididas em dados de entrada e de saída, conforme a Tabela 6.3.

Tabela 6.3 - Entradas e saídas de dados

Categoria	Descrição	Dados
Entradas	Informações da Usina Nuclear	País
		Usina
		Potência (MWe)
		Operadora
		Projeto
		Data da construção
		Data da operação inicial
	Informações do Evento Operacional	Data do cadastro
		Data do evento
		Título do evento
		Resumo do evento
		Status da usina no dia do evento
		Sistemas afetados pelo evento
		Falha
		Tipo de falha
		Modo de falha
		Defesa em profundidade desafiada
		Diversidade requerida
Saídas	Cálculos	Tempo de operação da usina em horas.
		Número de eventos cadastrados
		Taxa de falha
		Avaliação do nível de confiabilidade

6.4.1 DADOS DE ENTRADA

As informações das usinas nucleares foram previamente armazenadas em um banco de dados auxiliar, a fim de facilitar o preenchimento dessas entradas no banco de dados principal. No total, foram cadastradas 430 usinas (IAEA, 2006).

As informações dos eventos operacionais foram adquiridas através dos relatórios da AIEA (*Incident Reporting System - IRS*) e dos relatórios de eventos da NRC (*Licensee Event Report - LER*).

A classificação do evento foi dividida em três etapas, denominadas no banco de dados de Falha, Tipo de Falha e Modo de Falha.

A primeira etapa de classificação do evento é de acordo com a falha: FCC ou FS.

A segunda etapa, o evento operacional é classificado de acordo com o tipo de falha: falha de hardware (FH), falha de software (FSOFT) e falha de interface homem-sistema (FIHS).

Na terceira e última etapa, o evento operacional é classificado quanto ao modo de falha, conforme a experiência operacional dos eventos cadastrados, como por exemplo: canal de instrumentação inoperante e falha de comunicação de dados (Tabela 7.1).

Após o cadastro do evento, é necessário avaliar qual escalão de defesa em profundidade, entre os quatros já definidos, o evento desafiou e quais diversidades são requeridas para evitá-lo ou minimizá-lo.

6.4.2 DADOS DE SAÍDA

Os dados de saída utilizados na avaliação são:

- Tempo de operação da usina em horas;
- Número de eventos cadastrados;
- Taxa de falha;
- Nível de confiabilidade.

6.4.2.1 TEMPO DE OPERAÇÃO DA USINA

O tempo de operação da usina foi calculado a partir da sua data da operação inicial (dado de entrada) e contado até a data que em foi gerado o cálculo da taxa de falha e depois convertido em horas de operação. Essa variável é sempre atualizada. No caso de uma atualização da instrumentação e controle, a data a ser considerada será a data da operação inicial do sistema de I & C digital.

6.4.2.2 NÚMERO DE EVENTOS CADASTRADOS

O número de eventos é a contagem dos eventos cadastrados no banco de dados que possuem em comum as seguintes informações de entrada:

- Usina;
- Falha;
- Tipo de falha;
- Modo de falha

Os eventos cadastrados que tiverem essas informações serão contabilizados em conjunto, gerando a informação de saída 'número de eventos cadastrados'.

6.4.2.3 TAXA DE FALHA

Para fazer a estimativa de taxa de falha foi utilizada a abordagem apresentada por SIU e KELLY (1998), que possibilita estimar a taxa de falha mesmo quando nenhum evento de falha for encontrado, permitindo assim obter o resultado do 'nível de confiabilidade' para todos os modos de falha cadastrados, após realizar os relacionamentos entre os critérios de confiabilidade.

As taxas de falha utilizadas foram assim estimadas usando o cálculo padrão bayesiano que envolve uma distribuição a priori não-informativa de Jeffrey da função densidade de probabilidade

$$f(\lambda) = \frac{1}{\sqrt{\lambda}} \qquad (6.1)$$

A distribuição a priori do nosso estado de conhecimento acerca de λ, $f(\lambda)$, e a função verossimilhança de "r" eventos no tempo "t" $L(E_1 / \lambda)$ é.

$$f(\lambda / E_1) = \frac{L(E_1 / \lambda) f(\lambda)}{\int_0^\infty L(E_1 / \lambda) f(\lambda) d\lambda} \quad \text{Teorema de Bayes} \qquad (6.2)$$

onde a nossa evidência empírica de "r" eventos de falha no tempo "t", dada uma taxa de falha assumida de "λ" é:

$$L(E_1 / \lambda) = \frac{(\lambda t)^r . e^{-\lambda t}}{r!} \quad \text{Probabilidade de Poisson} \quad (6.3)$$

Transformando a função densidade de probabilidade na distribuição a posteriori do nosso estado de conhecimento, após incorporação da evidência empírica através da equação 6.2:

$$f(\lambda / r, t) = \sqrt{\frac{t\ (\lambda t)^r \exp(-\lambda t)}{\lambda \quad \Gamma(r + 1/2)}} \qquad (6.4)$$

Com isso, a taxa de falha estimada média $\langle \lambda \rangle$, na condição observada de "r" eventos de falhas no tempo "t", é simplesmente

$$\langle \lambda \rangle = \int_0^\infty \lambda f(\lambda / r, t) d\lambda \qquad (6.5)$$

$$\langle \lambda \rangle = \frac{(r + 1/2)\ eventos}{t \qquad h} \qquad (6.6)$$

Como realimentação dinâmica, teremos a distribuição a priori do nosso estado de conhecimento acerca de λ, a equação 6.2, transformando a função densidade de probabilidade na distribuição a posteriori do nosso estado de conhecimento em:

$$f(\lambda / E_2) = \frac{L(E_2 / \lambda) f(\lambda / E_1)}{\int_0^\infty L(E_2 / \lambda) f(\lambda / E_1) d\lambda} \qquad (6.7)$$

6.4.2.4 AVALIAÇÃO DO NÍVEL DE CONFIABILIDADE

Esta avaliação é o resultado final gerado pela metodologia proposta nesta tese e registrada no banco de dados principal, podendo ser um dos cinco níveis de confiabilidade (PRETO, VERMELHO, LARANJA, AMARELO ou VERDE), conforme já mostrado na Tabela 6.2.

6.5 FERRAMENTA PARA A COLETA E ANÁLISE DE DADOS DOS EVENTOS OPERACIONAIS DE SISTEMAS DE I & C DIGITAL

Foi desenvolvida uma ferramenta para auxiliar a análise e coleta de dados. Essa ferramenta é um software desenvolvido com a linguagem Visual Basic versão 6.0, na forma de um banco de dados, chamado MAFIC-D (Figura 6.2), que possibilita uma interface de fácil uso para inserir, classificar e processar os eventos operacionais.

Figura 6.2 – Tela principal do programa MAFIC-D.

A ferramenta utiliza como plataforma de dados o programa Microsoft Access, para armazenar os registros de entradas e saídas. Para gerar gráficos a partir dessa ferramenta, usaremos o programa Microsoft Excel. Para gerar futuros relatórios, será usado o programa Microsoft Word. O programa executável desenvolvido a partir do programa Visual Basic faz o gerenciamento da interface com os programas Microsoft Access, Microsoft Excel e Microsoft Word (Figura 6.3).

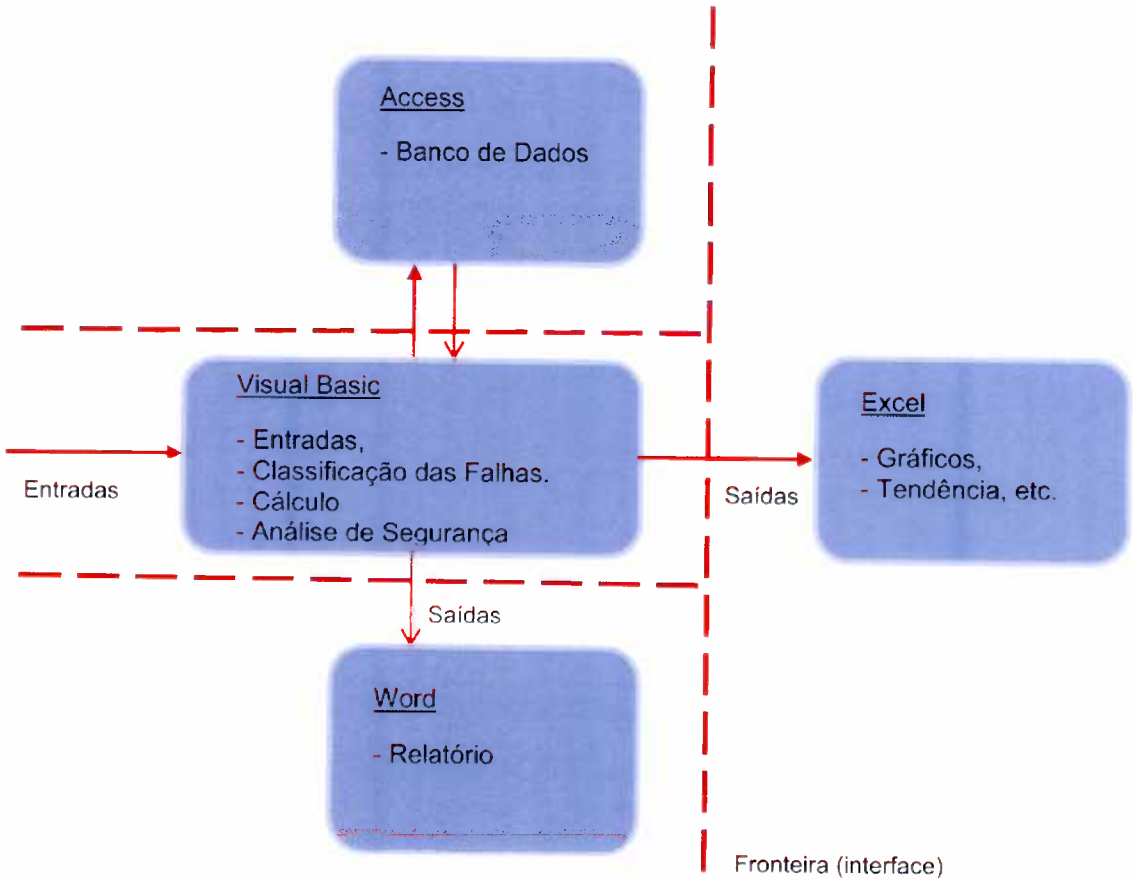


Figura 6.3 – Estrutura básica do sistema de coleta e análise de eventos.

6.5.1 UTILIZAÇÃO DO PROGRAMA MAFIC-D

Antes de fazer a avaliação do evento operacional e a aplicação da metodologia, o analista precisa cadastrar os eventos no programa MAFIC-D, com as seguintes informações (Figura 6.4):

- O número de registro é criado automaticamente;

- Seleciona-se a usina que apresentou o evento operacional;
- Data do evento;
- Título do evento operacional;
- Modo de operação da usina no dia do evento;
- Resumo do evento operacional.

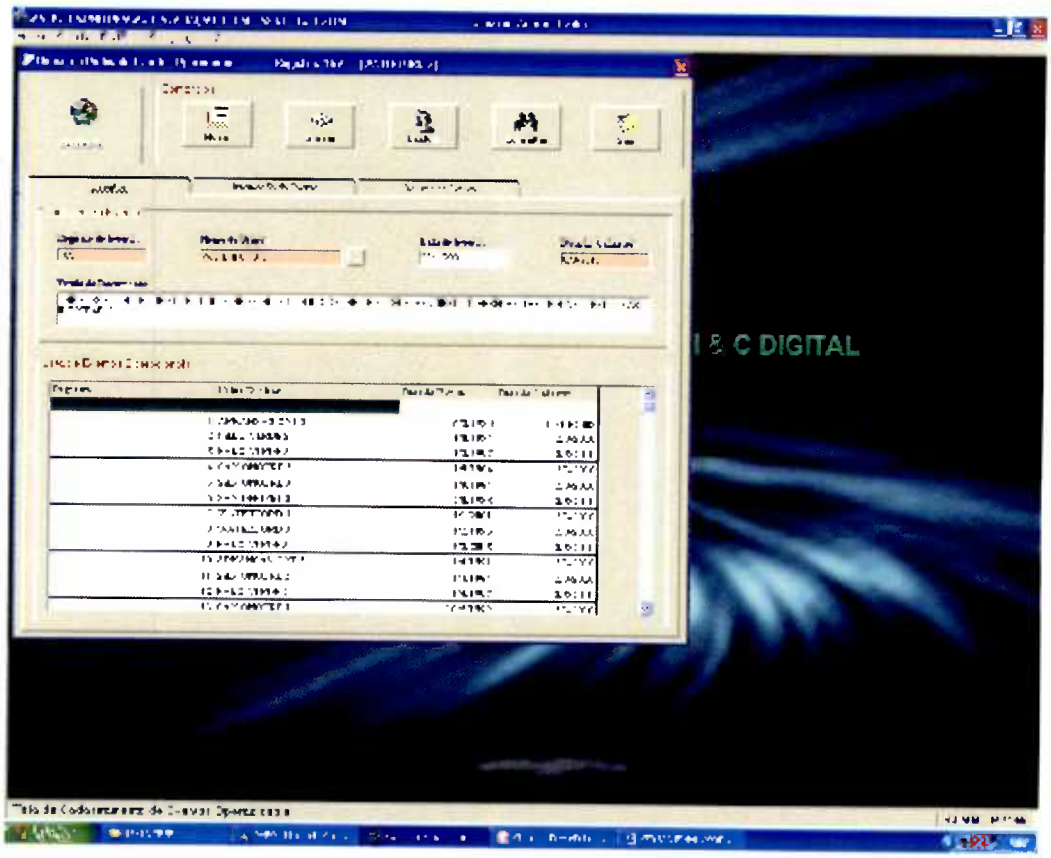


Figura 6.4 – Tela de cadastro dos eventos operacionais.

Após cadastrar todas as informações dos eventos operacionais, o analista de segurança terá de classificar os eventos quanto à falha, ao tipo de falha e ao modo de falha. Essa classificação é baseada na interpretação e no julgamento do especialista em segurança das informações do relatório do evento (MODARRES, 2006).

O próximo passo é fazer a avaliação de defesa em profundidade e diversidade. Para isso, o analista precisa abrir a tela de avaliação de eventos operacionais de I & C digital, no menu de arquivo do programa, selecionar a usina e o evento que será

analisado (Figuras 6.5 e 6.6). Em seguida, é preciso analisar qual foi o último nível de defesa em profundidade desafiado pelo evento e que diversidades são requeridas para minimizar ou evitar esse evento (Figura 6.6). Essa avaliação também é baseada na interpretação e no julgamento do especialista em segurança das informações do relatório do evento (MODARRES, 2006).

O programa MAFIC-D irá calcular a taxa de falha, baseado nas informações que foram registradas no banco de dados, e irá gerar o resultado do nível de confiabilidade da I & C digital, baseado nos relacionamentos dos critérios de confiabilidade (Figura 6.6).

A tela de avaliação dos eventos operacionais possui as seguintes informações de entrada e saída:

- Na primeira janela, são mostradas as principais informações da usina, seu nível de confiabilidade geral, por tipo de falha e modo de falha, com suas respectivas quantidades de eventos operacionais cadastrados (Figura 6.5);
- Na segunda janela, é mostrada a lista de eventos operacionais que possuem a mesma falha, tipo de falha e modo de falha (Figura 6.6);
- Na terceira janela, são mostradas as informações da avaliação D3, o valor da taxa de falha calculada, o tempo de operação da usina em horas e o resultado do nível de confiabilidade específico do modo de falha selecionado (Figura 6.7).

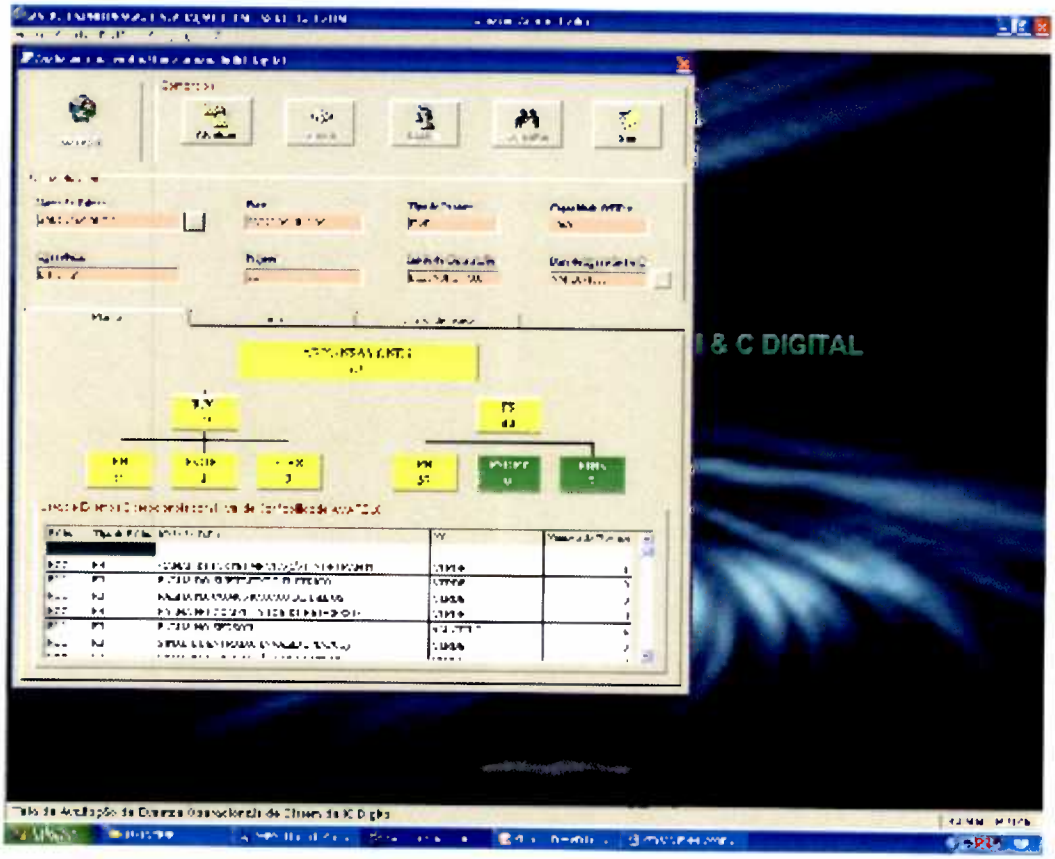


Figura 6.5 – Tela de avaliação dos eventos operacionais - Principal.

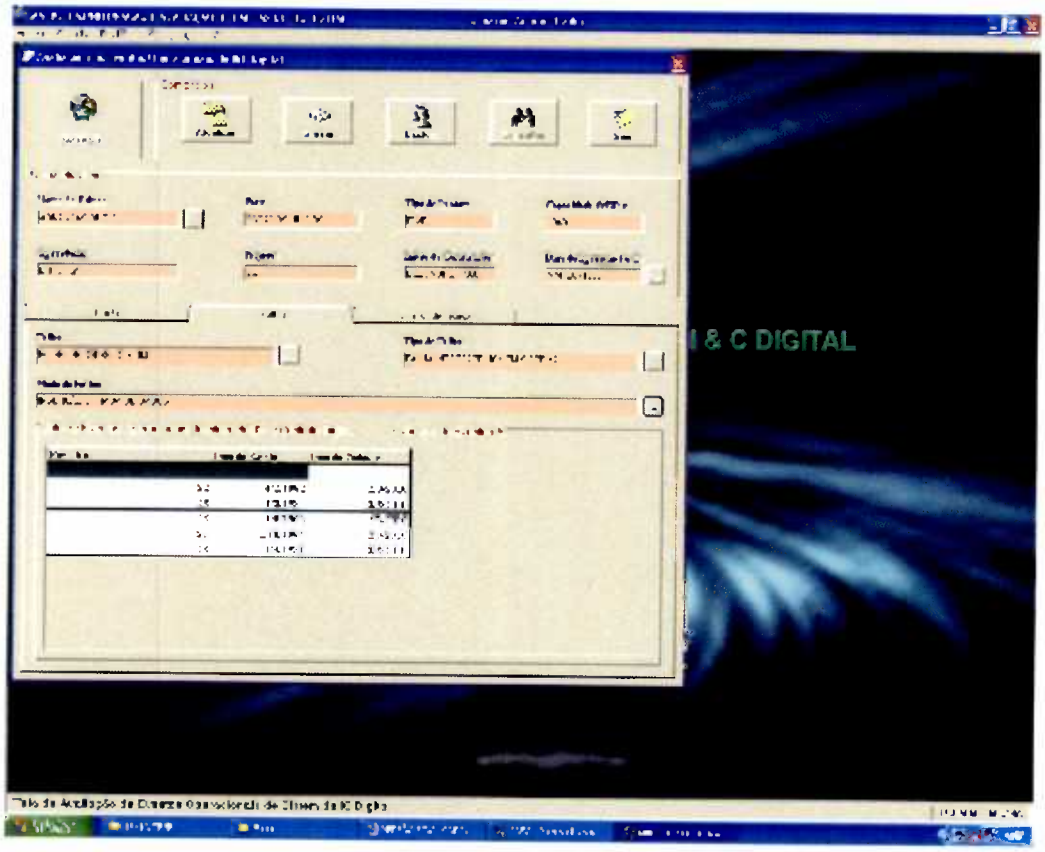


Figura 6.6 – Tela de avaliação dos eventos operacionais - Eventos Semelhantes

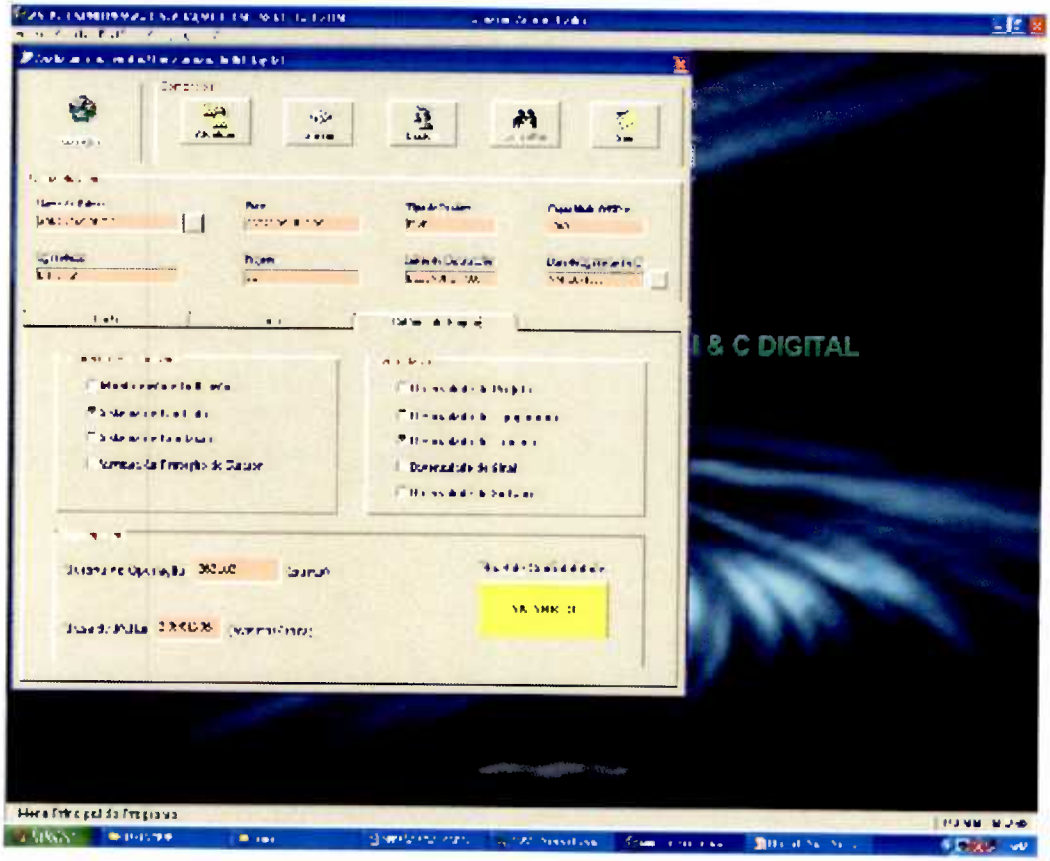


Figura 6.7 – Tela de avaliação dos eventos operacionais – Avaliação D3.

O Programa MAFIC-D possui ainda bancos de dados auxiliares que facilitam o preenchimento das informações para o banco de dados principais (Figura 6.8):

- Banco de dados de países;
- Banco de dados de sistemas de usinas;
- Banco de dados de usinas no mundo (Figura 6.9);
- Banco de dados de tipos de falhas;
- Banco de dados de modos de falhas;

Figura 6.8 – Tela de entrada dos bancos de dados auxiliares.

O banco de dados auxiliar de usinas, mostrado na Figura 6.9 (IAEA, 2006), possui as seguintes informações:

- País de origem;
- Projeto da usina;
- Operadora;
- Tipo de reator;
- Potência da usina;
- Data do início da construção;
- Data do início da operação.

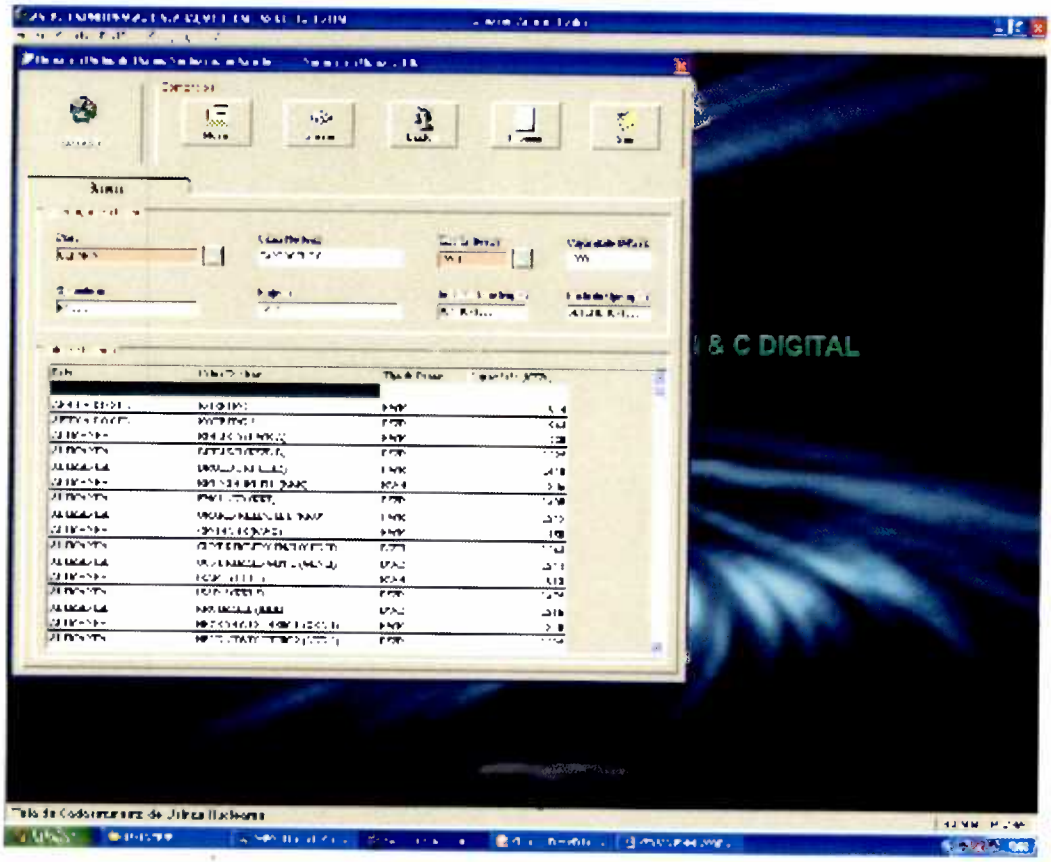


Figura 6.9 – Tela de cadastro de usinas.

7 RESULTADOS

7.1 INTRODUÇÃO

Com o objetivo de validar a metodologia proposta neste trabalho, foram analisados 169 eventos operacionais de sistemas de I & C digital de sete usinas nucleares americanas da *Combustion Engineering Inc.* (CE), no periodo de 1980 a 2006. Estes eventos foram reportados à NRC e registrados como LER, significativos para a segurança da usina (Apêndice C). As sete usinas são:

- Arkansas One 2;
- Palo Verde 1;
- Palo Verde 2;
- Palo Verde 3;
- San Onofre 2;
- San Onofre 3;
- Waterford 3.

No final da década de 1970, e depois da revisão reguladora feita pela NRC, com base nas abordagens deterministicas comumente usadas na época, a *Combustion Engineering Inc.* (CE) licenciou o primeiro sistema de proteção do reator digital (SPR-Digital) baseado em computador em uma usina nuclear nos Estados Unidos. O SPR-Digital foi chamado de *Core Protection Calculation System* (CPCS).

O sistema utiliza computadores redundantes digitais rodando o software e com o hardware construído para satisfazer os critérios reguladores da NRC, guias reguladores e normas IEEE nucleares existentes para sistemas de instrumentação e controle digital (Capítulo 4.0). A primeira usina nuclear americana que usou esse sistema foi a Arkansas Nuclear One, unidade 2.

As sete usinas da *Combustion Engineering* possuem a mesma I & C e o mesmo sistema de proteção do reator (CPCS), permitindo, além da avaliação individual da usina, comparações de desempenho entre elas.

Os 169 eventos foram contabilizados de acordo com a falha, tipo de falha e modo de falha. De acordo com a falha:

- 123 eventos foram de falhas simples (FS) e
- 46 eventos foram de falha de causa comum (FCC).

De acordo com o estudo, 73 % dos eventos são falhas simples e 27 % são falhas de causa comum (Figura 7.1),

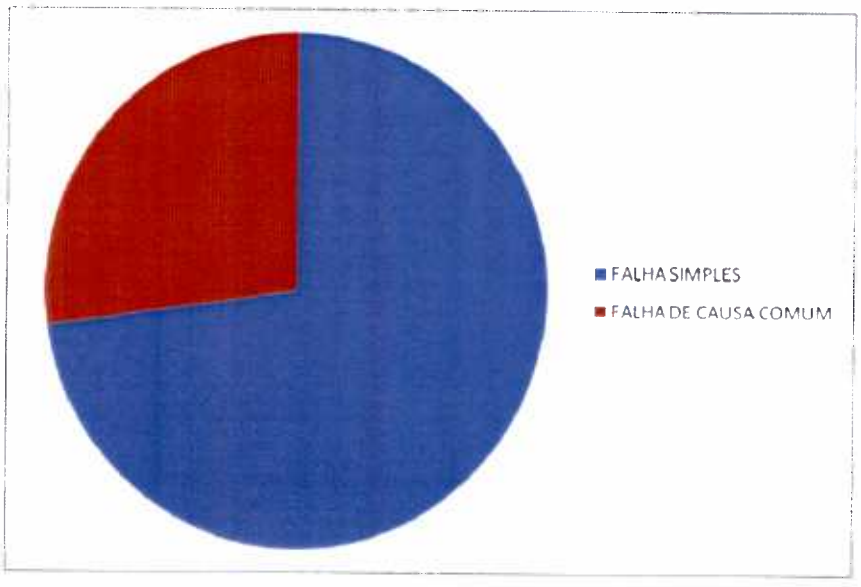


Figura 7.1 – Gráfico de falhas.

De acordo com o tipo de falha, os eventos foram contabilizados, sendo:

- 126 falhas de hardware (FH);
- 40 falhas de interface homem-sistema (FIHS);
- 3 falhas de software (FSOFT).

Desses, 74 % são falhas de hardware, 24 % são falhas de interface homem-sistema e somente 2 % são falhas de software (Figura 7.2).

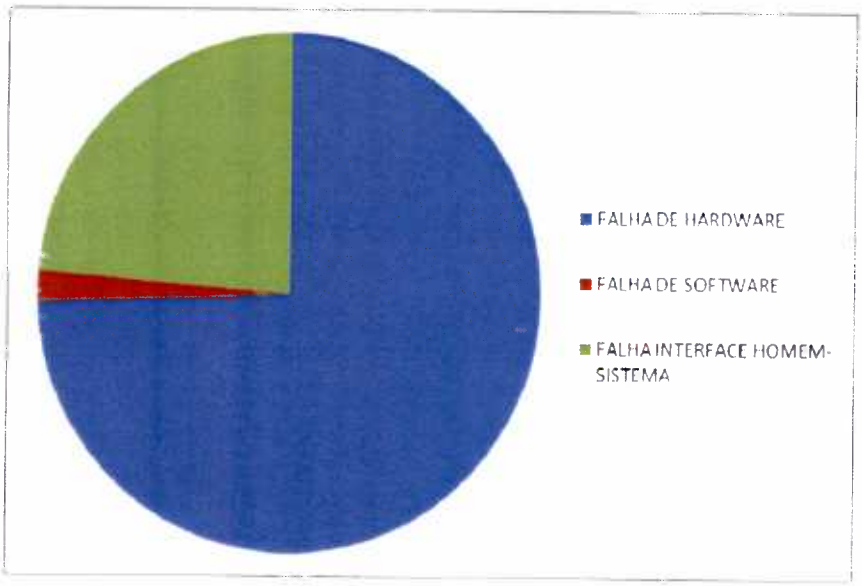


Figura 7.2 – Gráfico de tipos de falha

Com base nestes eventos foram definidos e contabilizados treze modos de falha, mostrados nas Tabelas 7.1.

Tabela 7.1 Modos de falha.

TIPO DE FALHA	MODO DE FALHA	FS	FCC
FH	CANAL DE INSTRUMENTAÇÃO INOPERANTE	17	2
FH	FALHA DO SUPRIMENTO ELÉTRICO	21	1
FH	FALHA NA COMUNICAÇÃO DE DADOS	4	-
FH	FALHA NO COMPUTADOR DE PROCESSO	16	1
FH	FALHA NO SENSOR	15	4
FH	SINAL DE ENTRADA INVÁLIDO (INPUT)	24	4
FH	SINAL DE SAÍDA INVÁLIDO (OUTPUT)	15	-
FH	TEMPERATURA ALTA	1	1
FSOFT	ERRO NO CÓDIGO FONTE	-	2
FSOFT	FALHA NO SISTEMA DE AQUISIÇÃO DE DADOS	1	-
FIHS	FALHA DE CALIBRAÇÃO	4	22

TIPO DE FALHA	MODO DE FALHA	FS	FCC
FIHS	FALHA NA EXECUÇÃO DE TESTES PERIÓDICOS	5	1
FIHS	INSERÇÃO ERRADA DE DADOS	-	8
TOTAL		123	46
TOTAL GERAL		169	

Esta avaliação identificou que os principais modos de falha para os sistemas de I & C digital são as falhas simples de hardware: a falha do suprimento elétrico e a falha de sinal de entrada inválido. No caso das falhas de causa comum a falha de interface homem-sistema/falha de calibração é o principal modo de falha.

Os resultados apresentados pelo método demonstraram que nenhuma das sete usinas nucleares apresentou nível de confiabilidade menor que o AMARELO (nível de Alerta) e só a Central Nuclear de Palo Verde 1 teve nível de confiabilidade VERDE (nível satisfatório) conforme mostrado na Tabela 7.2 (Figura D5).

Tabela 7.2 – Níveis de confiabilidade das usinas.

USINA	NÍVEL DE CONFIABILIDADE	FALHAS
Arkansas One 2	AMARELO	FCC/FSOFT FCC/FIHS FCC/FH FS/FH
Palo Verde 1	VERDE	-
Palo Verde 2	AMARELO	FCC/FSOFT
Palo Verde 3	AMARELO	FCC/FIHS
San Onofre 2	AMARELO	FCC/FH FCC/FIHS
San Onofre 3	AMARELO	CC/FH FCC/FIHS
Waterford 3	AMARELO	FCC/FIHS

Esses eventos estão contabilizados por ano na Tabela 7.3 e mostrados graficamente na Figura 7.3.

Tabela 7.3 – Eventos mostrados por ano

USINAS	EVENTOS POR 5 ANO				
	1980-84	1985-89	1990-94	1995-99	2000-06
ARKANSAS ONE 2	43	11	3	6	1
PALO VERDE 1	2	5	0	1	3
PALO VERDE 2	0	0	2	2	5
PALO VERDE 3	0	0	0	2	5
SAN ONOFRE 2	25	9	0	1	0
SAN ONOFRE 3	3	5	2	0	0
WATERFORD 3	0	14	3	6	4
MÉDIA	10	6	1	3	3

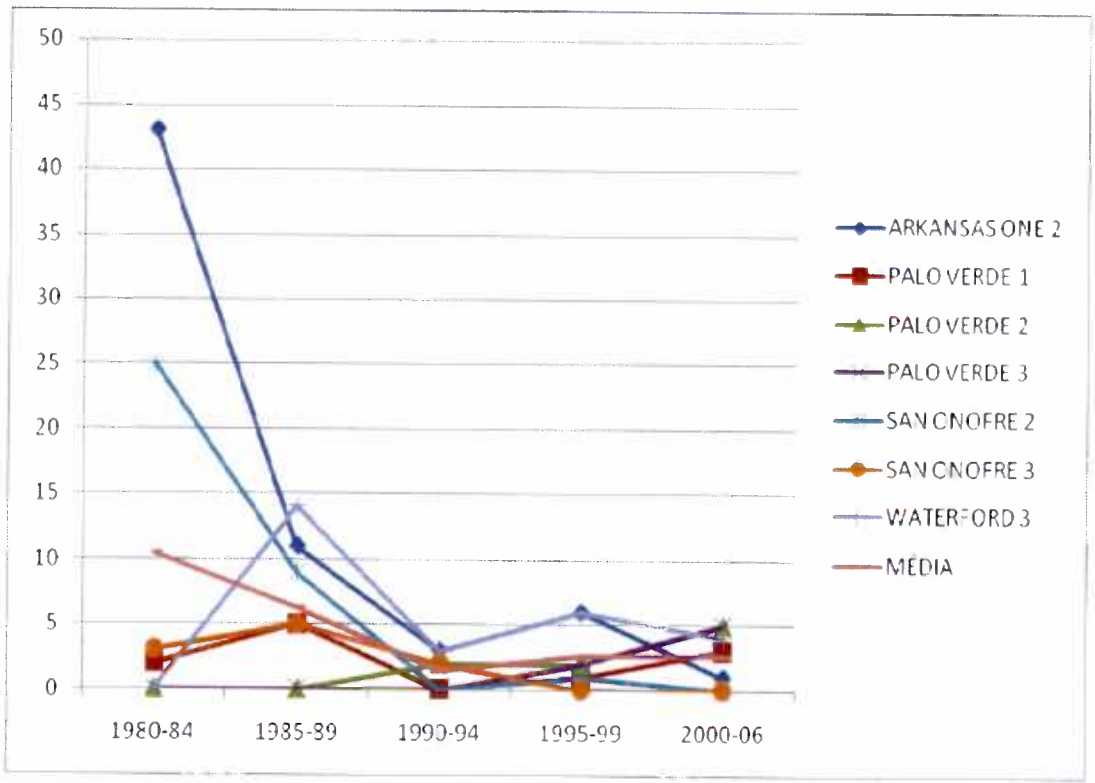


Figura 7.3 – Gráfico de eventos operacionais por ano.

7.2 COMPARAÇÃO COM OUTROS ESTUDOS

A NRC apresenta um método determinístico do BTP-19 (NRC, 1997e) para avaliação D3 de sistema de I & C digital, conforme já apresentado no Capítulo 5.

A metodologia proposta nesta tese traz alternativas para solucionar algumas lacunas do método da NRC:

- O método da NRC trata apenas dos eventos iniciadores analisados no Relatório de Análise de Segurança (RAS) da usina. Consequentemente, o método pode não considerar contribuições significativas para o risco da usina oriundos da experiência operacional, que são avaliados nesta tese.
- O método da NRC só considera as falhas do sistema de segurança e não as falhas dos sistemas relacionados com a segurança e os sistemas não relacionados com a segurança (Sistema de Monitoração e Indicação e o Sistema de Controle Automático); esta tese considera as falhas de todos os sistemas de segurança, os relacionados com a segurança e os não relacionados com a segurança.

A metodologia proposta nesta tese complementa a avaliação determinística da NRC, incluindo uma abordagem com informação do risco.

BRILL (2000) estudou eventos operacionais na base de dados da NRC (*Licensee Event Report - LER*) no período de 1994 a 1999, avaliando a freqüência dos eventos iniciadores relatados por falhas de sistemas instrumentação e controle. Seu trabalho considerou LER de todos os sistemas da usina, incluindo o sistema de I & C digital. O estudo mostrou que cerca de 8% de todos os eventos relatados eram referentes a falhas da I & C digital, sendo que:

- 34,22% foram falhas de interface homem-sistema (FIHS);
- 34,00% foram falhas de hardware (FH);
- 31,78% foram falhas de software (FSOFT).

Ainda, 9% dos eventos operacionais de I & C digital provocaram desarme no reator.

BRILL (2000) neste período de 5 anos, não avaliou e também não estimou as taxas de falha dos modos de falha que provocaram as três categorias de tipos de falha (FIHS, FH e FSOFT). Além disso, o trabalho não avaliou a confiabilidade do sistema digital observando as defesas e profundidade e diversidade requeridas para minimizar ou evitar as falhas observadas. A metodologia proposta nesta tese lista e avalia os modos de falha dos sistemas de I & C digitais e as implicações destas falhas sobre confiabilidade do sistema, além de aumentar o conjunto de dados de experiências operacionais de sistemas digitais.

8 CONCLUSÕES E RECOMENDAÇÕES

Decisões reguladoras relativas ao projeto de sistema I & C digital têm sido baseadas em critérios determinísticos de projeto, como o critério de falha única, separação física, isolamento elétrico de canais redundantes e programas de testes (seção 4.2). Todas estas abordagens, de um modo ou de outro tratam de preocupações básicas de confiabilidade, embora de um modo qualitativo e sem considerar a importância de se conhecer os modos de falha específicos dessa nova tecnologia digital. Hoje, no mundo, não existe um consenso sobre uma metodologia que considere o papel quantitativo da confiabilidade digital.

A metodologia proposta neste trabalho traz informações que visam complementar o processo regulador, utilizando a abordagem da informação do risco, requerendo níveis de confiabilidade necessários para a decisão a respeito da aceitabilidade do sistema de I & C digital em usinas nucleares.

Foi constatado que para a aplicação da metodologia, é necessário que o analista tenha um bom conhecimento do projeto da usina e pleno conhecimento da I & C digital. Os relatórios de eventos operacionais devem apresentar todas as informações necessárias para a aplicação do método. Os relatórios de eventos operacionais enviados para os órgãos reguladores, geralmente, possuem requisitos mínimos (Apêndice D) que atendem à metodologia proposta nesta tese de doutorado, como os 169 relatórios de eventos operacionais utilizados para validar o método (Apêndice C).

O estudo de validação da metodologia manteve-se fiel à realidade, utilizando uma base de dados de eventos operacionais ocorridos em sete usinas nucleares americanas da *Combustion Engineering Inc.* (CE), reportados à NRC, no período de 1980 a 2006. Este fato permitiu utilizar eventos operacionais ocorridos com o mesmo sistema de I & C digital, possibilitando testar os relacionamentos entre os critérios de

confiabilidade (falha, tipo de falha, taxa de falha, níveis de defesa em profundidade e diversidade) e fazer comparações de desempenho da I & C digital entre as usinas.

O estudo dos eventos operacionais mostrou que o número de FS é maior que o número de FCC, mas o resultado da metodologia demonstrou que as FCC, mesmo sendo em número menor, possuem uma importância maior na hora de se calcular o nível de confiabilidade e que o cuidado maior ainda deve ser com a FCC de software.

A aplicação da metodologia possibilitou levantar alguns questionamentos sobre o processo de licenciamento dos sistemas de instrumentação e controle digital, como por exemplo:

- O cuidado com a calibração dos sensores e canais;
- A qualidade dos processos de desenvolvimento de software;
- O processo de verificação e validação de software;
- Testes de hardware e software;
- Qualificação ambiental do hardware digital.

Outro ponto importante deste trabalho foi o levantamento de onze modos de falha, que foram identificados no estudo da base de dados dos 169 eventos operacionais:

- Canal de instrumentação inoperante;
- Falha do suprimento elétrico;
- Falha na comunicação de dados;
- Falha no computador de processo;
- Falha no sensor;
- Sinal de entrada inválido (INPUT);
- Sinal de saída inválido (OUTPUT);
- Temperatura alta;
- Erro no código fonte;

- Falha no sistema de aquisição de dados;
- Falha de calibração.

Ficou evidenciado que o método desenvolvido é de fácil aplicação e permite identificar, de um modo geral, o nível de confiabilidade do sistema de I & C da usina, mostrando suas principais vulnerabilidades, possibilitando traçar ações reguladoras a fim de minimizá-las ou evitá-las. Pode ainda servir de parâmetro de comparação de desempenho com outras usinas, principalmente quando essas usinas pertencerem ao mesmo projeto e possuírem sistemas de I & C digital iguais.

A ferramenta desenvolvida para executar a metodologia, o programa MAFIC-D, facilita e auxilia a aplicação dos relacionamento entre os critérios de confiabilidade, a análise dos relacionamentos e a coleta de dados. Os resultados obtidos, através desta ferramenta, demonstraram ser satisfatórios e complementam o processo de tomada de decisão reguladora do licenciamento da I & C digital de usinas nucleares e ainda podem ser usados para fazer o acompanhamento do desempenho da I & C digital, pós licenciamento, durante toda a vida útil do sistema, servindo de base para elaboração de listas de verificação de inspeções reguladoras.

Como sugestões e recomendações resultantes deste estudo, apresentamos as seguintes considerações:

- Identificar novos modos de falha, através do estudo de outros eventos operacionais, complementando o conjunto existente da experiência operacional;
- Utilizar esta metodologia com eventos operacionais de centrais alemãs, a fim de levantar a experiência operacional das usinas que utilizam o sistema de I & C digital Telepem XS/XP da Siemens, objetivando complementar a tomada de decisão para o processo de licenciamento deste sistema I & C digital para a Central Nuclear de Angra 2 e 3.

- Utilizar a metodologia para avaliar a I & C digital de reatores de pesquisa, já que os mesmos não possuem APS específica, mas possuem experiência operacional que podem ser aplicada ao método proposto nesta tese de doutorado.
- Utilizar as informações dos níveis de confiabilidade e dos modos de falha em uma APS especifica e aprovada da usina, auxiliando nas atualizações dos dados de falhas especificos da I & C digital da instalação, bem como dados de falhas obtidos da experiência operacional de outras usinas nucleares.

REFERÊNCIAS BIBLIOGRÁFICAS

BARBARA M., NANCY E. D., 2002, *Regulatory Strategies and Safety Culture in Nuclear Power Installations*, Paper based on work performed for Swedish Nuclear Power Inspectorate (SKI), Vienna.

BARROSO, A. C. O., COSTA, J. R., 1982. *Leis, Guias Regulatórios e Normas Utilizados no Processo de Licenciamento de Centrais Nucleares nos EUA e na Alemanha*, Relatório DR-Nº 111/82, CNEN, Rio de Janeiro.

BASTL, W., BOCK, H. W., 1998, *German Qualification and Assessment of Digital I & C Systems Important to Safety*, Reliability Engineering and System Safety 59, pp 163-170.

BICKEL, J. H., 2008, *Risk Implications of Digital Reactor Protection System Operating Experience*, Reliability Engineering and System Safety 93, pp 107-124.

BRILL, R. W., 2000, *Instrumentation And Control System Failures In Nuclear Power Plants*, International Symposium on Software Reliability Engineering, San Jose, California. Disponível em:
http://www.chillarege.com/fastabstracts/issre2000/home.html.
Acesso em: 26 jan. 2010, 22:07:00.

CHUANG, C. F., CHOU, H. P., CHEN, Y. B., SHIAO, H., 2008, *Regulatory Overview of Digital I & C System in Taiwan Lungmen Project*, Annals of Nuclear Energy 35, pp 877-889.

CNEN, 1984a, *CNEN-NE-1.04: Licenciamento de Instalações Nucleares*, Norma Experimental, Comissão Nacional de Energia Nuclear, Rio de Janeiro.

CNEN, 1999, *CNEN-NN-1.16: Garantia da Qualidade para a Segurança de Usinas Nucleoelétricas e Outras Instalações*, Comissão Nacional de Energia Nuclear, Rio de Janeiro.

CNEN, 2000, *CNEN-NN-1.14: Relatórios de Operação de Usinas Nucleoelétricas*, Comissão Nacional de Energia Nuclear, Rio de Janeiro.

CNEN, 2003, *Fundamentos da Ação Regulatória sobre Reatores Nucleares*, Comissão Nacional de Energia Nuclear, Rio de Janeiro.

EPRI, 1995, *TR-102348: Guideline on Licensing Digital Upgrades*, Electric Power Research Institute, Palo Alto.

EPRI, 2002, *TR-102348 (NEI 01-01): Guideline on Licensing Digital Upgrades*, Electric Power Research Institute, Palo Alto.

EPRI, 2004, *TR1002835: Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital I & C Upgrades Applying Risk-Informed and Deterministic Methods*, Electric Power Research Institute, Palo Alto.

FISCHER, H. D., PIEL, L., 1999, *Diversity in Computerized Reactor Protection Systems*, Reliability Engineering and System Safety 63, pp 91-97.

FLEMING, N. K., SILADY, F. A., 2002, *A Risk Informed Defese-in-Depth Framework for Existing and Advanced Reactors*, Reliability Engineering and System Safety 78, pp 205-225.

GARRETT, C. J., APOSTOLAKIS, G. E., 2002, *Automated hazard analysis of digital control systems*, Reliability Engineering and System Safety, 77, pp. 1-17.

HUANG, Hui-Wen, SHIN, C., YIH S., CHEN Ming-Hueil, 2007, *Software Failure Events Derivation and Analysis by Fram-Based tecnique*, Annals of Nuclear Energy 34, pp 307-318.

IAEA, 1980, *Protection Systems and Related Features in Nuclear Power Plants: A Safety*, Safety Series 50-SG, International Atomic Energy Agency, Vienna.

IAEA, 1984, *Safety Related Instrumentation and Control Systems for Nuclear Power Plants*, Safety Series 50-SG-D8, International Atomic Energy Agency, Vienna.

IAEA, 1988a, *Basic Safety Principles for Nuclear Power Plants*, International Nuclear Safety Advisor Group (INSAG-3), International Atomic Energy Agency, Vienna.

IAEA, 1988b, *Code on the Safety of Nuclear Power Plants*: Design, Safety Series S 50-C-D, International Atomic Energy Agency, Vienna.

IAEA, 1993, *The Safety of Nuclear Installations*, Safety Series No. 110, International Atomic Energy Agency, Vienna.

IAEA, 1998, *Modernization of instrumentation and control in nuclear power plants*, Technical Document 1016, International Atomic Energy Agency, Vienna.

IAEA, 1999a, *Specification of requirements for upgrades using digital instrument and control systems*, Technical Document 1066, International Atomic Energy Agency, Vienna.

IAEA, 1999b, *Verification and Validation of Software Related to Nuclear Power Plant Instrumentation and Control*, Technical Reports Series No. 384, International Atomic Energy Agency, Vienna.

IAEA, 1999c, *Modern Instrumentation and control for nuclear power plants*, Technical Reports Series No. 387, International Atomic Energy Agency, Vienna.

IAEA, 2000, *Software for Computer Based Systems Important to Safety in Nuclear Power Plants*, Safety Guide NS-G 1.1, International Atomic Energy Agency, Vienna.

IAEA, 2002a, *Instrumentation and Control Systems Important to Safety in Nuclear Power Plants*, Safety Guide NS-G 1.3, International Atomic Energy Agency, Vienna.

IAEA, 2002b, *Harmonization of the licensing process for digital instrumentation and control systems in nuclear power plants*, Technical Document 1327, International Atomic Energy Agency, Vienna.

IAEA, 2004a, *Managing modernization of nuclear power plant instrumentation and control systems*, Technical Document 1389, International Atomic Energy Agency, Vienna.

IAEA, 2004b, *Management of life cycle and ageing at nuclear power plants: Improved I & C maintenance*, Technical Document 1402, International Atomic Energy Agency, Vienna.

IAEA, 2006, *Nuclear Power Reactors in the World*, Reference Data Series N° 2, International Atomic Energy Agency, Vienna.

IEC, 1993, *Nuclear Power Plants — Instrumentation Systems Important to Safety — Classification*, International Electrotechnical Commission IEC-1226, Geneva.

IEEE, 1971, *Standard IEEE 279: Criteria for Protection Systems in Nuclear Generating Stations*, Institute of Electrical and Electronics Engineers, New York.

IEEE, 1980a, *Standard IEEE 338: Criteria for Periodic Surveillance Testing In Nuclear Power Generating Station Safety Systems*, Institute of Electrical and Electronics Engineers, New York.

IEEE, 1980b, *Standard IEEE 603: Criteria for Safety Systems for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers*, New York.

IEEE, 1981, *Standard IEEE 497: Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations*, Institute of Electrical and Electronics Engineers, New York.

IEEE, 1987, *Standard IEEE 379: Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety System*, Institute of Electrical and Electronics Engineers, New York.

IEEE, 1998a, *Standard IEEE 344: Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations*, Institute of Electrical and Electronics Engineers, New York.

IEEE, 1998b, *Standard IEEE 603: Criteria for Safety Systems for Nuclear Power Generating Stations*, New York.

IEEE, 1999, *Standard IEEE 323: Recommended Practice for Environmental (Temperature, pressure and radiation) Qualification of Class 1E Equipment for Nuclear Power Generating Station*, Institute of Electrical and Electronics Engineers, New York.

IEEE, 2003, *Standard IEEE 7-4.3.2: Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations*, New York.

KANG, H. G., SUNG, T., 2002, *An Analysis of Safety Critical Digital Systems for risk Informed*, Reliability Engineering and System Safety 78, pp 307-314.

KANG, H. G., JANG, Seung-Cheol, 2007, *Plant Risk Effect Analysis Focusing on Digital I & C Equipment Failures*, Journal of Nuclear Science and Technology 44, pp 509-596.

KTA, 1985, *KTA-3501: Reactor Protection System and Surveillance of Safety Equipment*, Kerntechnische Ausschuss (KTA), German Committee for Nuclear Technologies, Bonn.

LI, F., YANG, Z., AN, Z., ZHANG, L., 2002, *The first Digital Reactor Protection System in China*, Nuclear Engineering and Design, Vol. 218, pp 215-225.

LU, L., JIANG, J., 2004, *Probabilistic Safety Assessment for Instrumentation and Control Systems in Nuclear Power Plants: An Overview*, Journal of Nuclear Science and Technology, Vol. 41, pp 323-330.

MODARRES, M., 2006, *Risk Analysis in Engineering: Techniques, Tools and Trends*, Taylor & Francis Group, Florida.

MODARRES, M., 2009, *Advanced nuclear power plant regulation using risk-informed and performance-based methods*, Reliability Engineering and System Safety 94, pp 211-217.

NAP, 1997 *Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues*, National Academy Press, Washington, DC.

NEI 96-07, 2000, *Revision 1, Guidelines for 10 CFR 50.59*, Nuclear Energy Institute, Washington, DC.

NRC, 1981a, *Instrumentation for Light-Water-Cooled Nuclear Power Plant to Assess Plant and Environmental Conditions During and Following an Accident*, Regulatory Guide 1.97, Nuclear Regulatory Commission, Washington, DC.

NRC, 1981b, *Standard Criteria for Safety Systems in Nuclear Generating Stations*, Regulatory Guide 1.153, Nuclear Regulatory Commission, Washington, DC.

NRC, 1983, *Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident*, Regulatory Guide 1.97, Rev. 3, Nuclear Regulatory Commission, Washington, DC.

NRC, 1991, *Digital Computer Systems for Advanced Light Water Reactors*, Safety Requirements Memorandum SECY-91-292, Nuclear Regulatory Commission, Washington, DC.

NRC, 1993, *Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs*, Safety Requirements Memorandum SECY-93-087, Nuclear Regulatory Commission, Washington, DC.

NRC, 1994a, *Final Safety Evaluation Report Related to the Certification of the Advanced Boiling Water Reactor Design*, Main Report, Nuclear Regulatory Commission, Washington, DC.

NRC, 1994b, *Standard Format and Content of Safety Analysis Reports for NPP*, Regulatory Guide 1.70, Nuclear Regulatory Commission, Washington, DC.

NRC, 1994c, *Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems*, NUREG CR-6303, Nuclear Regulatory Commission, Washington, DC.

NRC, 1995, *Guideline on Licensing Digital Upgrades*, Generic Letter 95-02 TR-102348, Nuclear Regulatory Commission, Washington, DC.

NRC, 1997a, *Standard Criteria for Digital Computers in Nuclear Generating Stations*, Regulatory Guide 1.152, Nuclear Regulatory Commission, Washington, DC.

NRC, 1997b, *Standard Review Plan Capítulo 7 (I & C)*, NUREG-0800, Nuclear Regulatory Commission, Washington, DC.

NRC, 1997c, *Guidance on Software Reviews for Digital Computer-Based I & C Systems*, Branch Technical Position HICB-14, Nuclear Regulatory Commission, Washington, DC.

NRC, 1997d, *Guidance on the Use of Programmable Logical Controllers in Digital Computer-Based I & C Systems*, Branch Technical Position HICB-18, Nuclear Regulatory Commission, Washington, DC.

NRC, 1997e, *Guidance for Evaluation of Defense-in-Depth and Diversity (D3) in Digital Computer-Based Instrumentation and Control Systems*, Branch Technical Position HICB-19, Nuclear Regulatory Commission, Washington, DC.

NRC, 1997f, *Guidance on Digital Computer Real-Time Performance*, Branch Technical Position HICB-21, Nuclear Regulatory Commission, Washington, DC.

NRC, 1998a, *An Approach for Using Probabilistic Risk Assessment in Risk-informed Decisions on Plant-Specific Changes to the Licensing Basis*, Regulatory Guide 1.174, Nuclear Regulatory Commission, Washington, DC.

NRC, 1998b, *Guidelines for 10CFR50.59 Safety Evaluations, Nuclear Safety Analysis Center*, NSAC-125, Nuclear Regulatory Commission, Washington, DC.

NRC, 2005, *Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments*, NUREG CR-6901, Nuclear Regulatory Commission, Washington, DC.

NRC, 2009a, *Code and Standards*, 10CFR-Part 50.55a, Nuclear Regulatory Commission, Washington, DC.

NRC, 2009b, *Changes, Test and Experiments*, 10CFR-Part 50.59, Nuclear Regulatory Commission, Washington, DC.

NRC, 2009c, *Changes, General Design Criteria – GDC*, 10CFR-Part 50 Appendix A, Nuclear Regulatory Commission, Washington, DC.

NRC, 2009d, *Changes, Quality Assurance Criteria for NPP and Fuel Reprocessing Plants*, 10CFR-Part 50 Appendix B, Nuclear Regulatory Commission, Washington, DC.

NRC, 2009e, *Changes, Contents of Applications; Technical Information*, 10CFR Part 50.34B, Nuclear Regulatory Commission, Washington, DC.

PINTO, J. M. O., 2010, *Análise de um Sistema Simplificado de Controle Digital Proposto para o Pressurizador de uma Usina Nuclear Através de um Modelo de Simulação Dinâmica*, Dissertação de Mestrado, Universidade Federal do Rio de Janeiro, Rio de Janeiro.

SHIN, L. C., PARK, C. E., JIN, C. C., TAE, S. J., 2001, *Defense-in Depth and Diversity Evaluation to Cope With Design Bases Events Concurrent With Common Cause Failure in Digital Plant Protection System for KNGR*, Nuclear Engineering and Design 207, pp 95-104.

SIU N. O., KELLY D. L., 1998, *Bayesian Parameter Estimation in Probabilistic Risk Assessment*, Reliability Engineering and System Safety, 62, pp. 89-116.

SMIDTS, C., KNUDSEN, J., KVARFORDT, K., WOOD, T., 2008, *Key Attributes of the SAPHIRE Risk and Reliability Analysis Software for Risk-Informed Probabilistic Applications*, Reliability Engineering and System Safety 93, pp 1151-1164.

XING, L., MESHKAT, L., DONOHUE, S. K., 2007, *Reliability Analysis of Hierarchical Computer-Based Systems Subject to Common-Cause Failures*, Reliability Engineering and System Safety, 92, pp. 351-359.

ZITROU, A., BEDFORD, T., WALLS, L., 2010, *Bayes Geometric Model Common Cause Failure Rates*, Reliability Engineering and System Safety, 95, pp. 70-76.

APÊNDICE

APÊNDICE A – RELACIONAMENTO DOS CRITÉRIOS DE CONFIABILIDADE

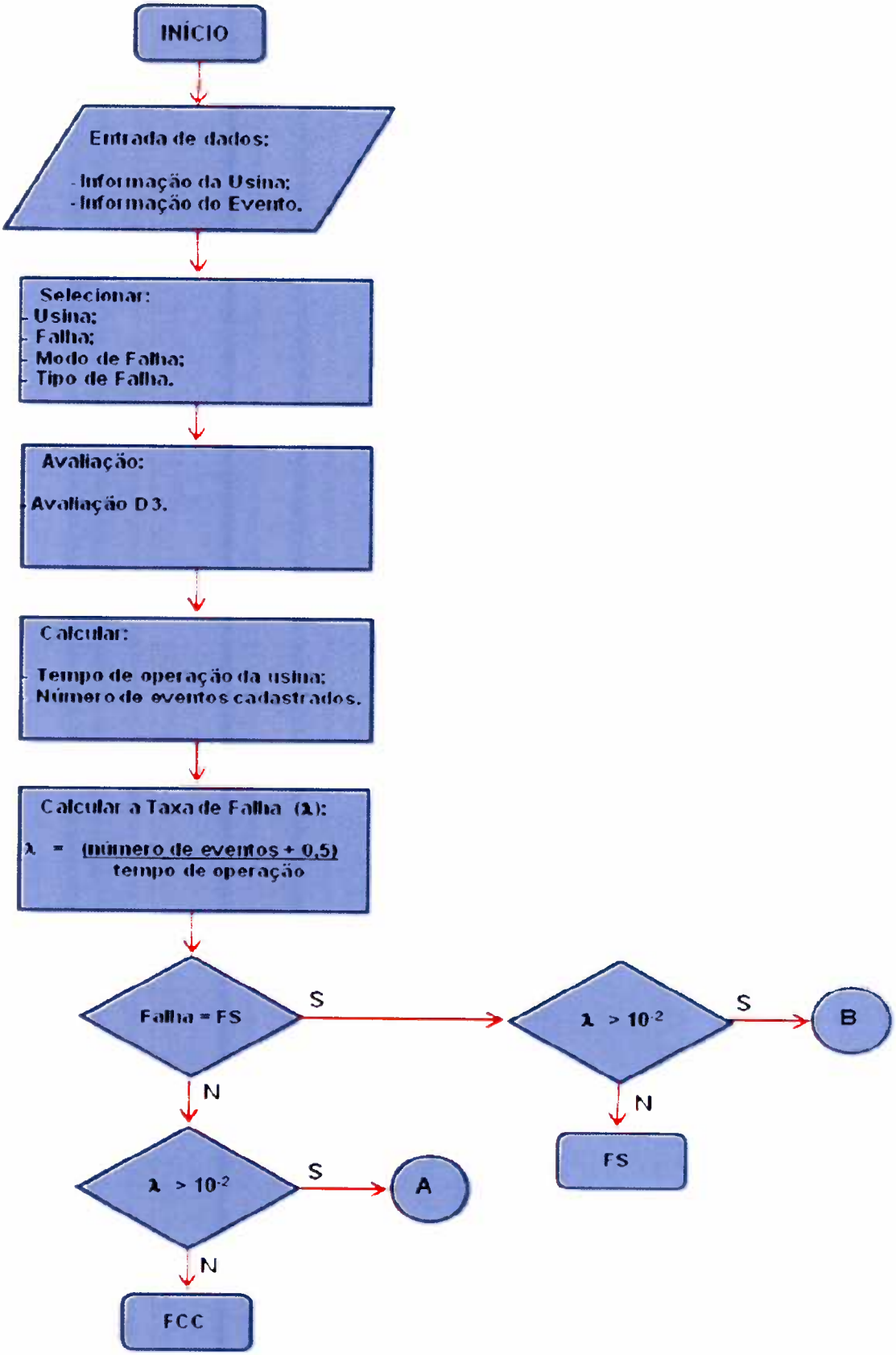
Tabela A – Relacionamentos dos critérios de confiabilidade

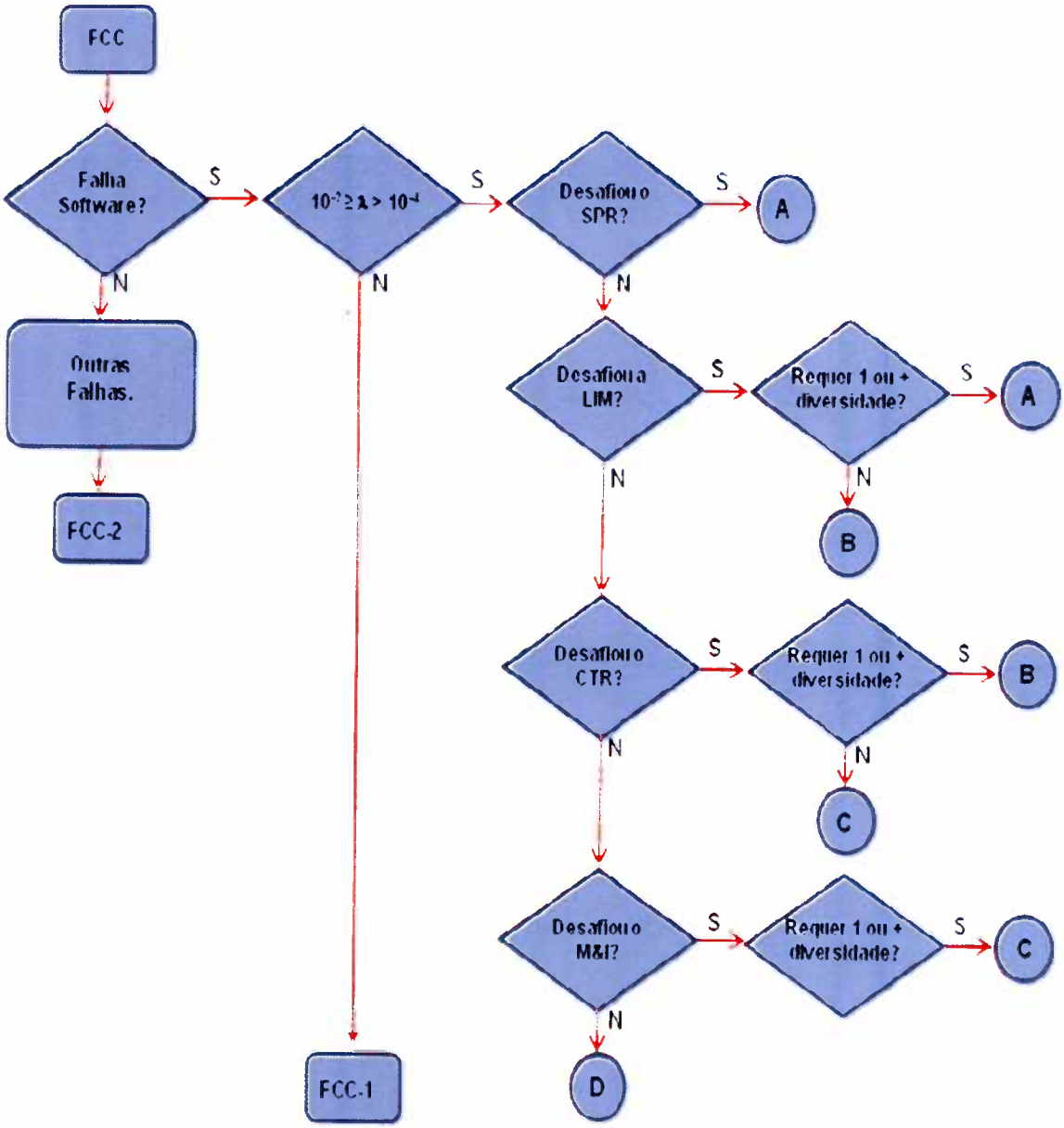
Falha	Tipo de Falha	λ	D3	Nível de Confiabilidade
FS		$\lambda > 10^{-2}$		VERMELHO
FCC		$\lambda > 10^{-2}$		PRETO
FCC	Falha de Software	$10^{-2} \geq \lambda > 10^{-4}$	Desafiou o SPR	PRETO
FCC	Falha de Software	$10^{-2} \geq \lambda > 10^{-4}$	Desafiou o LIM Requer 1 ou+ diversidade	PRETO
FCC	Falha de Software	$10^{-2} \geq \lambda > 10^{-4}$	Desafiou o LIM Não requer diversidade	VERMELHO
FCC	Falha de Software	$10^{-2} \geq \lambda > 10^{-4}$	Desafiou o CTR Requer 1 ou+ diversidade	VERMELHO
FCC	Falha de Software	$10^{-2} \geq \lambda > 10^{-4}$	Desafiou o CTR Não requer diversidade	LARANJA
FCC	Falha de Software	$10^{-2} \geq \lambda > 10^{-4}$	Desafiou o M&I Requer 1 ou+ diversidade	LARANJA
FCC	Falha de Software	$10^{-2} \geq \lambda > 10^{-4}$	Desafiou o M&I Não requer diversidade	AMARELO
FCC	Falha de Software	$10^{-4} \geq \lambda > 10^{-6}$	Desafiou o SPR Requer 1 ou+ diversidade	VERMELHO
FCC	Falha de Software	$10^{-4} \geq \lambda > 10^{-6}$	Desafiou o SPR Não requer diversidade	LARANJA
FCC	Falha de Software	$10^{-4} \geq \lambda > 10^{-6}$	Desafiou o LIM Requer 1 ou+ diversidade	LARANJA
FCC	Falha de Software	$10^{-4} \geq \lambda > 10^{-6}$	Desafiou o LIM Não requer diversidade	AMARELO
FCC	Falha de Software	$10^{-4} \geq \lambda > 10^{-6}$	Desafiou o CTR Requer 1 ou+ diversidade	AMARELO
FCC	Falha de Software	$10^{-4} \geq \lambda > 10^{-6}$	Desafiou o CTR Não requer diversidade	VERDE
FCC	Falha de Software	$\lambda \leq 10^{-6}$	Desafiou o SPR	LARANJA

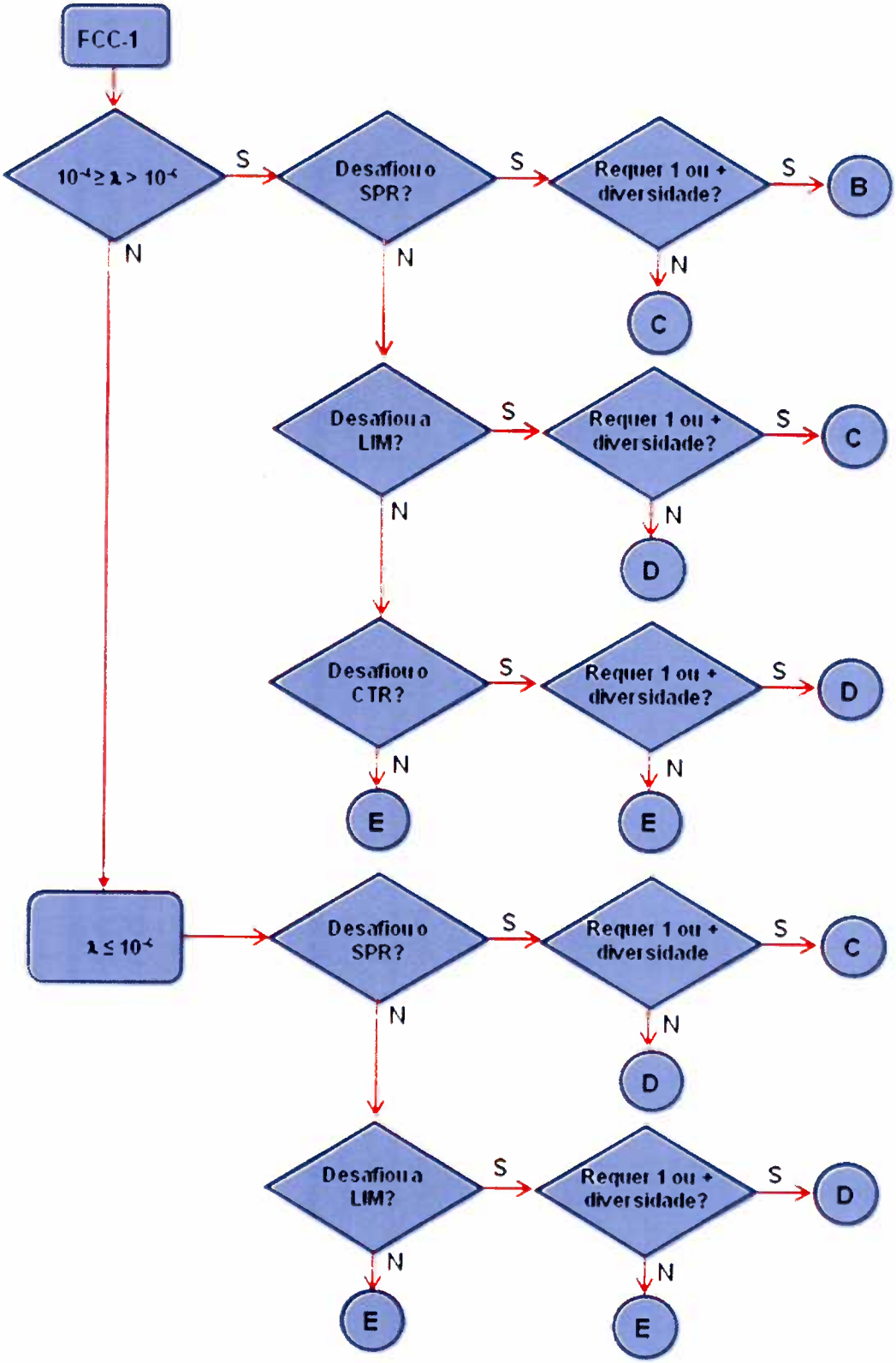
			Requer 1 ou+ diversidade	
FCC	Falha de Software	$\lambda \leq 10^{-6}$	Desafiou o SPR Não requer diversidade	AMARELO
FCC	Falha de Software	$\lambda \leq 10^{-6}$	Desafiou o LIM Requer 1 ou+ diversidade	AMARELO
FCC	Falha de Software	$\lambda \leq 10^{-6}$	Desafiou o LIM Não requer diversidade	VERDE
FCC	Falha de Hardware Falha IH-S	$10^{-2} \geq \lambda > 10^{-4}$	Desafiou o SPR	VERMELHO
FCC	Falha de Hardware Falha IH-S	$10^{-2} \geq \lambda > 10^{-4}$	Desafiou o LIM Requer 1 ou+ diversidade	VERMELHO
FCC	Falha de Hardware Falha IH-S	$10^{-2} \geq \lambda > 10^{-4}$	Desafiou o LIM Não requer diversidade	LARANJA
FCC	Falha de Hardware Falha IH-S	$10^{-2} \geq \lambda > 10^{-4}$	Desafiou o CTR Requer 1 ou+ diversidade	LARANJA
FCC	Falha de Hardware Falha IH-S	$10^{-2} \geq \lambda > 10^{-4}$	Desafiou o CTR Não requer diversidade	AMARELO
FCC	Falha de Hardware Falha IH-S	$10^{-2} \geq \lambda > 10^{-4}$	Desafiou o M&I Requer 1 ou+ diversidade	AMARELO
FCC	Falha de Hardware Falha IH-S	$10^{-2} \geq \lambda > 10^{-4}$	Desafiou o M&I Não requer diversidade	VERDE
FCC	Falha de Hardware Falha IH-S	$10^{-4} \geq \lambda > 10^{-6}$	Desafiou o SPR Requer 1 ou+ diversidade	VERMELHO
FCC	Falha de Hardware Falha IH-S	$10^{-4} \geq \lambda > 10^{-6}$	Desafiou o SPR Não requer diversidade	LARANJA
FCC	Falha de Hardware Falha IH-S	$10^{-4} \geq \lambda > 10^{-6}$	Desafiou o LIM Requer 1 ou+ diversidade	LARANJA
FCC	Falha de Hardware Falha IH-S	$10^{-4} \geq \lambda > 10^{-6}$	Desafiou o LIM Não requer diversidade	AMARELO
FCC	Falha de Hardware Falha IH-S	$10^{-4} \geq \lambda > 10^{-6}$	Desafiou o CTR Requer 1 ou+ diversidade	AMARELO
FCC	Falha de Hardware Falha IH-S	$10^{-4} \geq \lambda > 10^{-6}$	Desafiou o CTR Não requer diversidade	VERDE
FCC	Falha de Hardware Falha IH-S	$\lambda \leq 10^{-6}$	Desafiou o SPR Requer 1 ou+ diversidade	LARANJA
FCC	Falha de Hardware Falha IH-S	$\lambda \leq 10^{-6}$	Desafiou o SPR Não requer diversidade	AMARELO
FCC	Falha de Hardware Falha IH-S	$\lambda \leq 10^{-6}$	Desafiou o LIM Requer 1 ou+ diversidade	AMARELO

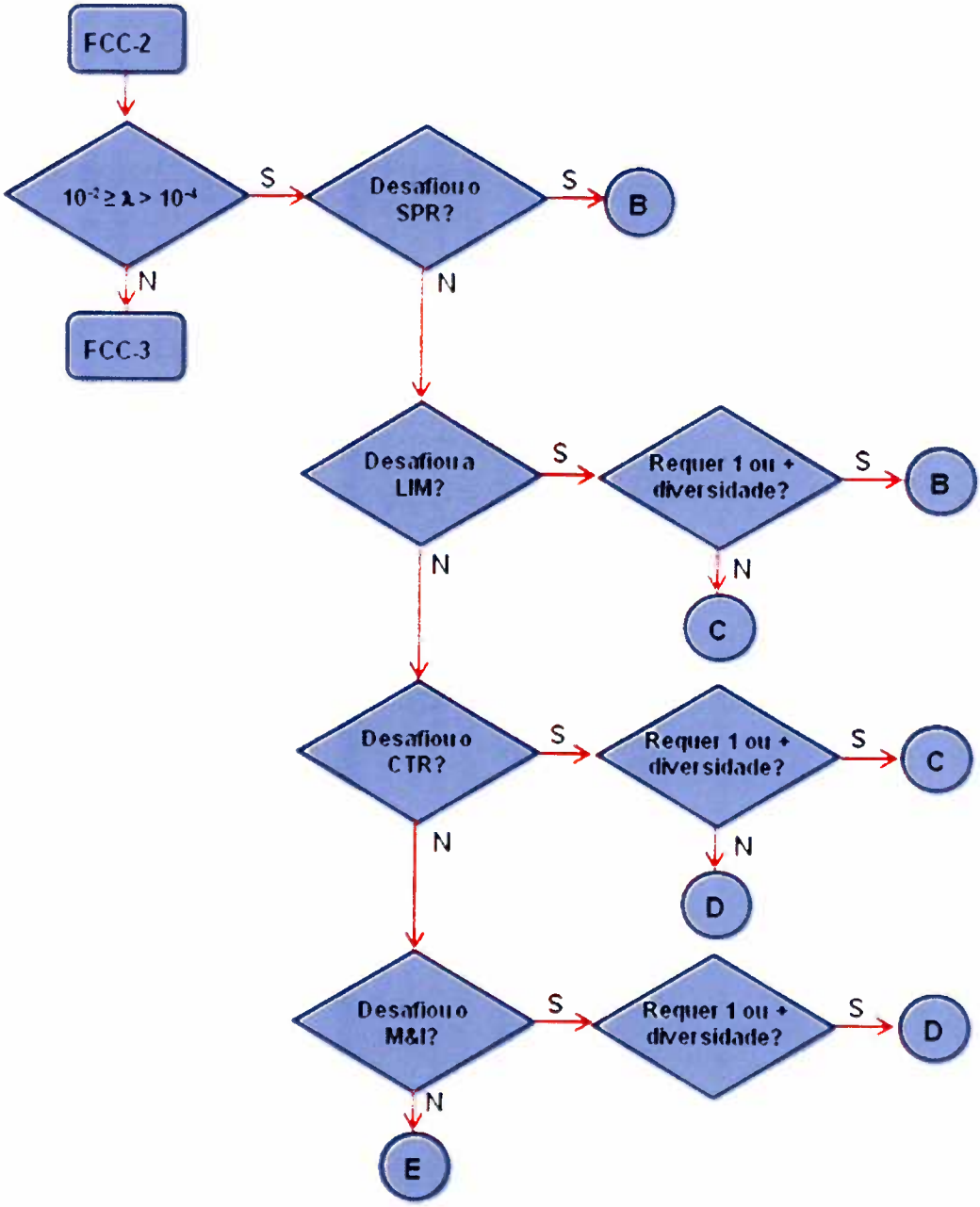
FCC	Falha de Hardware Falha IH-S	$\lambda \leq 10^{-6}$	Desafiou o LIM Não requer diversidade	VERDE
FS	Falha de Software	$10^{-2} \geq \lambda > 10^{-5}$	Desafiou o SPR	VERMELHO
FS	Falha de Software	$10^{-2} \geq \lambda > 10^{-5}$	Desafiou o LIM Requer 1 ou+ diversidade	VERMELHO
FS	Falha de Software	$10^{-2} \geq \lambda > 10^{-5}$	Desafiou o LIM Não requer diversidade	LARANJA
FS	Falha de Software	$10^{-2} \geq \lambda > 10^{-5}$	Desafiou o CTR Requer 1 ou+ diversidade	LARANJA
FS	Falha de Software	$10^{-2} \geq \lambda > 10^{-5}$	Desafiou o CTR Não requer diversidade	AMARELO
FS	Falha de Software	$10^{-2} \geq \lambda > 10^{-5}$	Desafiou o M&I Requer 1 ou+ diversidade	AMARELO
FS	Falha de Software	$10^{-2} \geq \lambda > 10^{-5}$	Desafiou o M&I Não requer diversidade	VERDE
FS	Falha de Hardware Falha IH-S	$\lambda \leq 10^{-5}$	Desafiou o SPR Requer 1 ou+ diversidade	LARANJA
FS	Falha de Hardware Falha IH-S	$\lambda \leq 10^{-5}$	Desafiou o SPR Não requer diversidade	AMARELO
FS	Falha de Hardware Falha IH-S	$\lambda \leq 10^{-5}$	Desafiou o LIM Requer 1 ou+ diversidade	AMARELO
FS	Falha de Hardware Falha IH-S	$\lambda \leq 10^{-5}$	Desafiou o LIM Não requer diversidade	VERDE

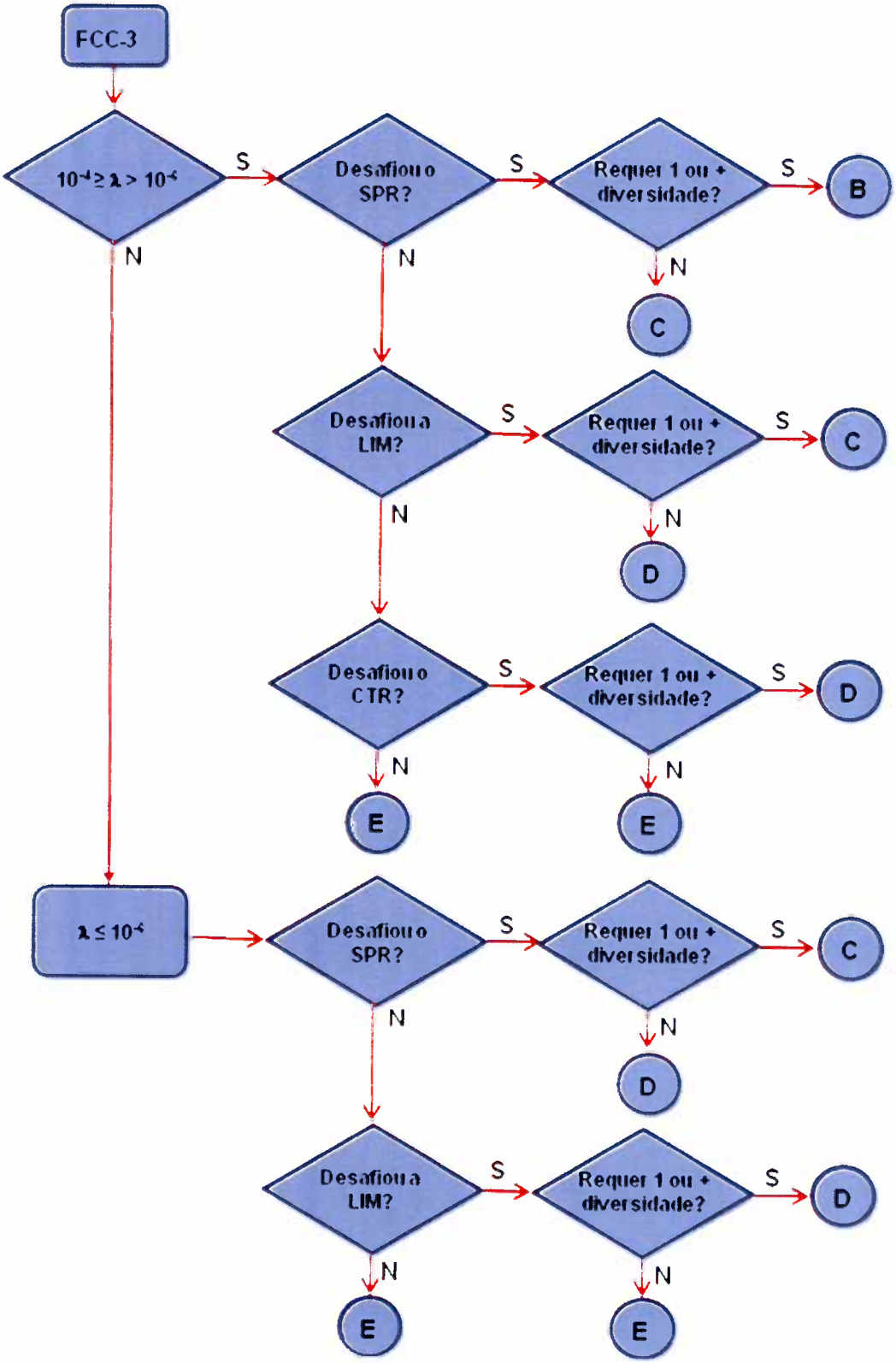
APÊNDICE B – FLUXOGRAMA DE BLOCOS DA LÓGICA DOS RELACIONAMENTOS APLICADOS NO PROGRAMA MAFIC-D

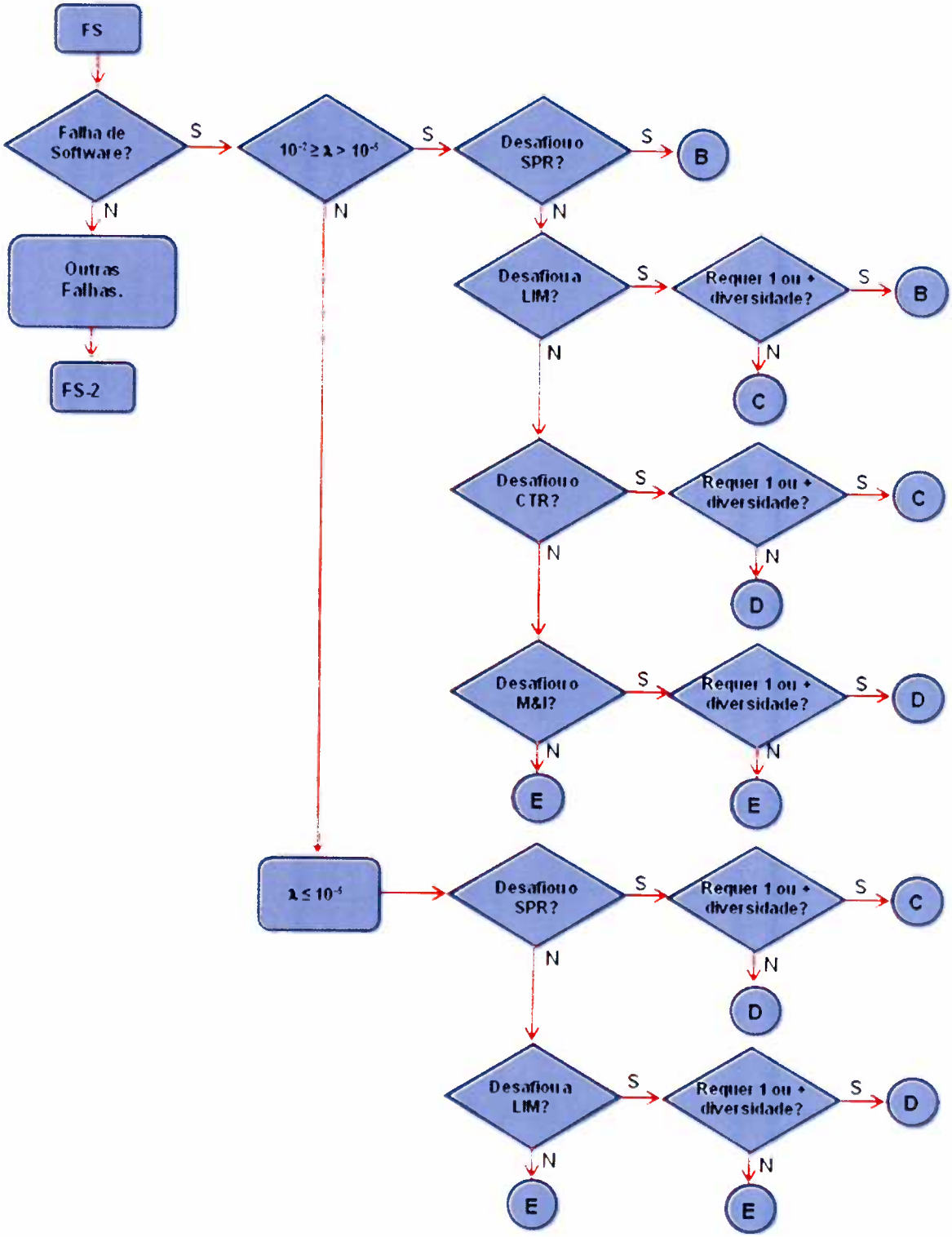


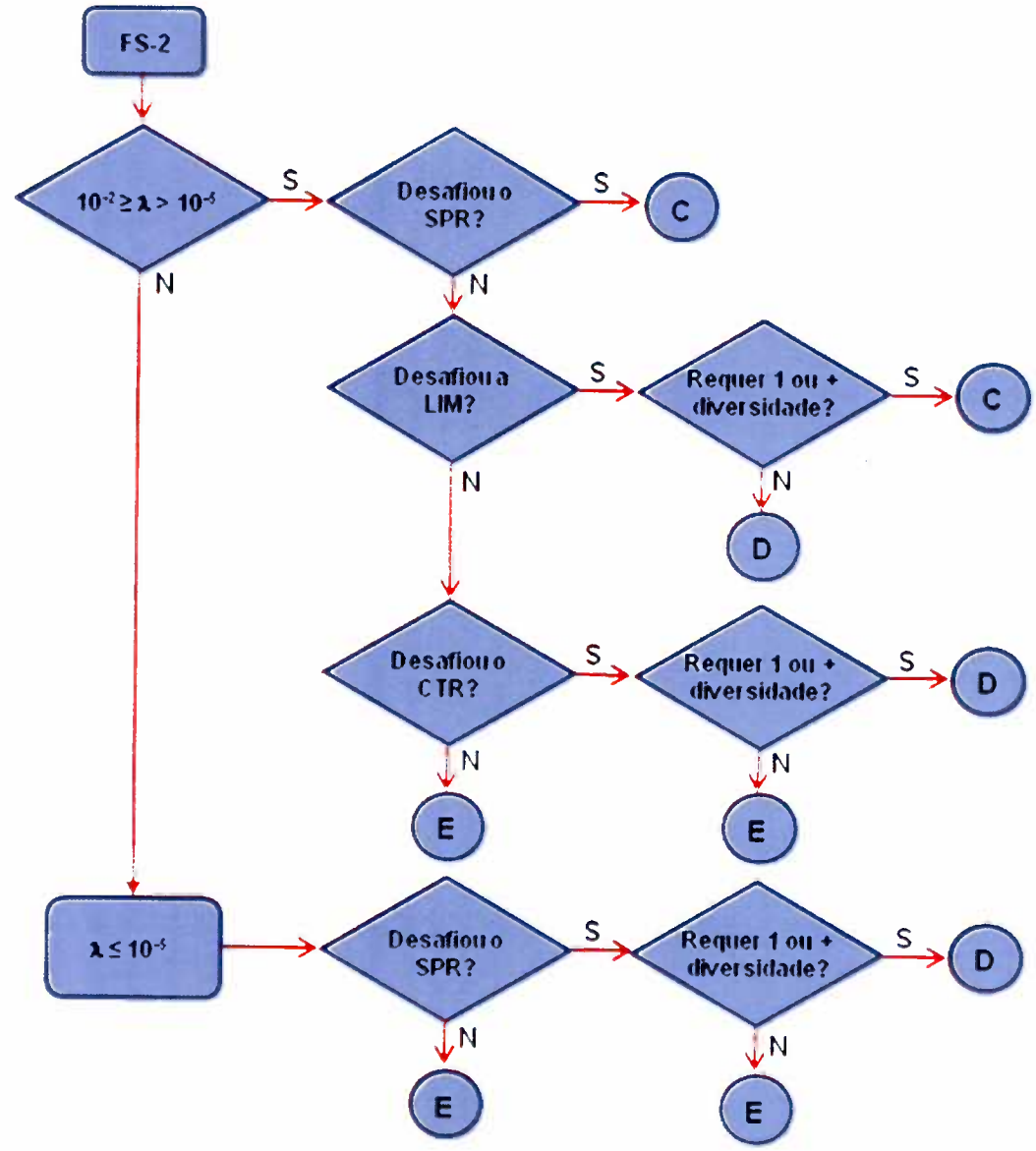

FCC
Falha Software?
S
N
$10^{-2} \geq \lambda > 10^{-4}$
S
N
Desafiou o SPR?
S
A
N
Outras Falhas.
FCC-2
Desafiou a LIM?
S
Requer 1 ou + diversidade?
S
A
N
B
N
Desafiou o CTR?
S
Requer 1 ou + diversidade?
S
B
N
C
N
Desafiou o M&I?
S
Requer 1 ou + diversidade?
S
C
N
D
FCC-1

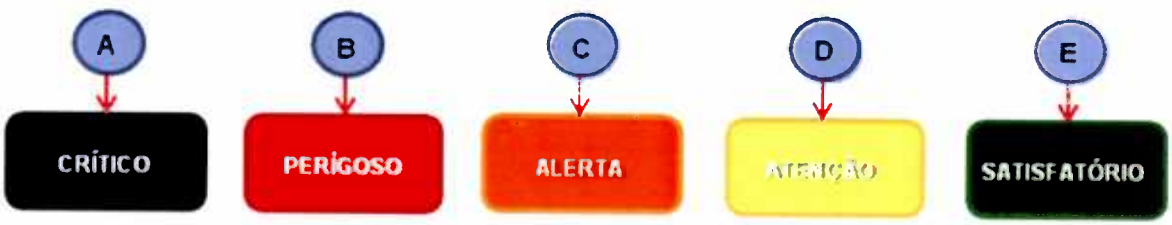

FCC-1
$10^{-4} \geq \lambda > 10^{-5}$
S
Desafiou o SPR?
S
Requer 1 ou + diversidade?
S
B
N
N
N
C
Desafiou a LIM?
S
Requer 1 ou + diversidade?
S
C
N
N
D
Desafiou o CTR?
S
Requer 1 ou + diversidade?
S
D
N
N
E
E
$\lambda \leq 10^{-5}$
Desafiou o SPR?
S
Requer 1 ou + diversidade
S
C
N
N
D
Desafiou a LIM?
S
Requer 1 ou + diversidade?
S
D
N
N
E
E


FCC-2
$10^{-3} \geq \lambda > 10^{-4}$
S
Desafiou o SPR?
S
B
N
FCC-3
N
Desafiou a LIM?
S
Requer 1 ou + diversidade?
S
B
N
N
C
Desafiou o CTR?
S
Requer 1 ou + diversidade?
S
C
N
N
D
Desafiou o M&I?
S
Requer 1 ou + diversidade?
S
D
N
E


FCC-3
$10^{-4} \geq \lambda > 10^{-6}$
S
Desafiou o SPR?
S
Requer 1 ou + diversidade?
S
B
N
N
C
Desafiou a LIM?
S
Requer 1 ou + diversidade?
S
C
N
N
D
Desafiou o CTR?
S
Requer 1 ou + diversidade?
S
D
N
N
E
E
$\lambda \leq 10^{-6}$
Desafiou o SPR?
S
Requer 1 ou + diversidade?
S
C
N
N
D
Desafiou a LIM?
S
Requer 1 ou + diversidade?
S
D
N
N
E
E


FS
Falha de Software?
S
N
$10^{-2} \geq \lambda > 10^{-5}$
S
N
Desafiou o SPR?
S
B
N
Outras Falhas.
FS-2
Desafiou a LIM?
S
Requer 1 ou + diversidade?
S
B
N
N
C
Desafiou o CTR?
S
Requer 1 ou + diversidade?
S
C
N
N
D
Desafiou o M&I?
S
Requer 1 ou + diversidade?
S
D
N
N
E
E
$\lambda \leq 10^{-5}$
Desafiou o SPR?
S
Requer 1 ou + diversidade?
S
C
N
N
D
Desafiou a LIM?
S
Requer 1 ou + diversidade?
S
D
N
N
E
E


FS-2
$10^{-2} \geq \lambda > 10^{-5}$
S
Desafiou o SPR?
S
C
N
N
Desafiou a LIM?
S
Requer 1 ou + diversidade?
S
C
N
N
D
Desafiou o CTR?
S
Requer 1 ou + diversidade?
S
D
N
N
E
E
$\lambda \leq 10^{-5}$
Desafiou o SPR?
S
Requer 1 ou + diversidade?
S
D
N
N
E
E


A
CRÍTICO
B
PERIGOSO
C
ALERTA
D
ATENÇÃO
E
SATISFATÓRIO

APÊNDICE C – LISTA DE EVENTOS OPERACIONAS DE USINAS NUCLEARES UTILIZADOS NO PROGRAMA. MAFIC-D

Tabela C – Lista de eventos operacionais.

Usina	Falha	Título
ARKANSAS ONE 2	FS	DROPPED CEA CAUSED CEAC PEN. FACTOR AND SENSED LOW DNBR
ARKANSAS ONE 2	FS	SINGLE CHANNEL EXCORE DETECTOR DATA SET INVALID
ARKANSAS ONE 2	FS	LOSS OF 120V INVERTER FAILS CEAC(N) AND CPC CHANNEL "X"
ARKANSAS ONE 2	FS	SINGLE RTD TIME CONSTANTS OOT
ARKANSAS ONE 2	FS	SINGLE RTD TIME CONSTANTS OOT
ARKANSAS ONE 2	FS	OPERATORS FAIL TO PERFORM MONTHLY CEAC FUNCTIONAL SURVEILLANCE
ARKANSAS ONE 2	FS	SINGLE CPCS CHANNEL DNBR/LPD TIME CONSTANT DATA SET INVALID
ARKANSAS ONE 2	FS	TEMP INPUT FROM FAILED RTD CAUSES D CHANNEL CPC TO FAIL
ARKANSAS ONE 2	FCC	INACCURATE CROSS CALIBRATION OF EXCORE VS. CALORIMETRIC ?T POWER TO ALL 4 CPC CHANNELS
ARKANSAS ONE 2	FCC	MAINT. ON CEAC DISPLAY REQUIRED DISABLING CEAC #1 INPUTS
ARKANSAS ONE 2	FCC	DURING POWER ESCALATION TESTING A SOFTWARE ERROR WAS FOUND
ARKANSAS ONE 2	FS	LIGHTNING STORM IN AREA CAUSED POWER SURGE IN POWER SUPPLY TO CEAC 2 AND CPC C
ARKANSAS ONE 2	FS	DATA COMMUNICATION FAILURE CAUSES CPC WATCHDOG TIMER TIMEOUT REQUIRING CPC CHANNEL REBOOT
ARKANSAS ONE 2	FS	DURING CONTROLLED SHUTDOWN CEA BANK INSERTION GENERATED CPCS LOW DNBR BASED ON CEA POSITION
ARKANSAS ONE 2	FS	DATA COMMUNICATION FAILURE CAUSES CPC WATCHDOG TIMER TIMEOUT REQUIRING CPC CHANNEL REBOOT
ARKANSAS ONE 2	FS	DROPPED CEA CAUSED CEAC PEN. FACTOR AND SENSED LOW DNBR
ARKANSAS ONE 2	FS	DROPPED CEA CAUSED CEAC PEN. FACTOR AND SENSED LOW DNBR
ARKANSAS ONE 2	FCC	RCP "D" TRIP CAUSES LOW DNBR IN 2/4 CPC CHANNELS
ARKANSAS ONE 2	FS	HIGH ASI DURING SHUTDOWN RESULTED IN SENSED LOW DNBR/ HIGH LDP
ARKANSAS ONE 2	FS	FAILURE TO PERFORM "D" CHANNEL CPC CALIBRATION
ARKANSAS ONE 2	FS	PROCEDURAL ERROR DURING CPC RESPONSE TIME TESTING WITHOUT CPC BYPASSES IN PLACE CAUSED CPCS TRIPS.
ARKANSAS ONE 2	FS	HIGH ASI DURING STARTUP RESULTED IN SENSED LOW DNBR

Usina	Falha	Titulo
ARKANSAS ONE 2	FS	MISPOSITIONED CEA CAUSED CEAC PEN. FACTOR AND SENSED LOW DNBR
ARKANSAS ONE 2	FS	SINGLE RTD INPUT INVALID
ARKANSAS ONE 2	FS	SINGLE CHANNEL EXCORE DETECTOR DATA SET INVALID
ARKANSAS ONE 2	FS	SINGLE CHANNEL EXCORE DETECTOR DATA SET INVALID
ARKANSAS ONE 2	FS	FAILURE TO BYPASS CPCS DURING LOW POWER PHYSICS TESTS INVOLVING CEA MOTION
ARKANSAS ONE 2	FS	CPC COMPUTER PROCESSOR LOCKS UP REQUIRING CPC CHANNEL REBOOT
ARKANSAS ONE 2	FCC	INACCURATE CROSS CALIBRATION OF RCS FLOW DATA SETS
ARKANSAS ONE 2	FCC	COMMUNICATION DATA LINK FAILURE MISSED SURVEILLANCES ON BOTH CEAC CHANNELS
ARKANSAS ONE 2	FCC	HIGH LOG POWER BYPASS REMOVAL SETPOINTS (1E-4) INCORRECT
ARKANSAS ONE 2	FCC	TECHNICIANS INSERT WRONG DATA SETS IN ALL 4 CPC CHANNELS
ARKANSAS ONE 2	FCC	TECHNICIANS INSERT WRONG DATA SETS IN ALL 4 CPC CHANNELS
ARKANSAS ONE 2	FCC	TECHNICIANS INSERT WRONG DATA SETS IN 2 OF 4 CPC CHANNELS
ARKANSAS ONE 2	FCC	VENDOR SUPPLIES ERRONEOUS DATA INPUT TO ALL 4 CPC CHANNELS
ARKANSAS ONE 2	FCC	VENDOR SUPPLIES ERRONEOUS DATA INPUT TO ALL 4 CPC CHANNELS
ARKANSAS ONE 2	FCC	2 OF 2 CEACS FEEDING 4/4 CPCS INOPERABLE
ARKANSAS ONE 2	FCC	MULTIPLE RTD SENSORS FAIL TO MEET RESPONSE TIME REQUIREMENTS, FAILING 4 OF 4 CPC CHANNELS
ARKANSAS ONE 2	FCC	MULTIPLE RTD SENSORS FAIL TO MEET RESPONSE TIME REQUIREMENTS, FAILING 4 OF 4 CPC CHANNELS
ARKANSAS ONE 2	FS	DATA COMMUNICATION FAILURE CAUSES CPC WATCHDOG TIMER TIMEOUT REQUIRING CPC CHANNEL REBOOT
ARKANSAS ONE 2	FCC	MULTIPLE RTD SENSORS FAIL TO MEET RESPONSE TIME REQUIREMENTS, FAILING 2 OF 4 CPC CHANNELS
ARKANSAS ONE 2	FS	2 A LOOP RCS (DP) FLOW INDICATORS INOPERABLE.
ARKANSAS ONE 2	FS	CPC COMPUTER PROCESSOR LOCKS UP REQUIRING CPC CHANNEL REBOOT
ARKANSAS ONE 2	FS	CPC COMPUTER PROCESSOR LOCKS UP REQUIRING CPC CHANNEL REBOOT
ARKANSAS ONE 2	FS	CPC COMPUTER PROCESSOR LOCKS UP REQUIRING CPC CHANNEL REBOOT
ARKANSAS ONE 2	FS	CPC COMPUTER PROCESSOR LOCKS UP REQUIRING CPC CHANNEL REBOOT
ARKANSAS ONE 2	FS	CPC COMPUTER PROCESSOR LOCKS UP REQUIRING CPC CHANNEL REBOOT
ARKANSAS ONE 2	FS	CEAC COMPUTER PROCESSOR LOCKS UP REQUIRING CEAC CHANNEL REBOOT
ARKANSAS ONE 2	FS	CEAC COMPUTER PROCESSOR LOCKS UP REQUIRING

Usina	Falha	Título
		CEAC CHANNEL REBOOT
ARKANSAS ONE 2	FS	CEAC MICROPROCESSOR BOARD FAILURE CAUSES CEA DATA SET ERROR - CPC CHANNEL "X" AND CEAC(N) TRIPS
ARKANSAS ONE 2	FS	MUX FAILURE CAUSES CEA DATA SET ERROR - CPC CHANNEL "X" AND CEAC(N) TRIPS
ARKANSAS ONE 2	FS	MUX FAILURE CAUSES CEA DATA SET ERROR - CPC CHANNEL "X" AND CEAC(N) TRIPS
ARKANSAS ONE 2	FS	MUX FAILURE CAUSES CEA DATA SET ERROR - CPC CHANNEL "X" AND CEAC(N) TRIPS
ARKANSAS ONE 2	FCC	MULTIPLE RTD SENSORS FAIL TO MEET RESPONSE TIME REQUIREMENTS, FAILING 2 OF 4 CPC CHANNELS
ARKANSAS ONE 2	FS	LOSS OF CONDENSER VACUUM RESULTS IN TURBINE TRIP, HIGH PZR PRESSURE AUXILIARY CPCS TRIP
ARKANSAS ONE 2	FCC	RCP "D" TRIP CAUSES LOW DNBR IN 2/4 CPC CHANNELS
ARKANSAS ONE 2	FS	PROCEDURAL ERROR IN COORDINATING CPCS AND HIGH LOG POWER BYPASSES DURING TESTING RESULTED IN REACTOR TRIP
ARKANSAS ONE 2	FCC	ELEVATED TEMPERATURES IN CPC ROOM
ARKANSAS ONE 2	FS	HIGH ASI DURING STARTUP RESULTED IN SENSED LOW DNBR
ARKANSAS ONE 2	FS	TESTING IN OTHER CHANNELS CAUSED CPCS TRIPS
ARKANSAS ONE 2	FS	PCS CHANNEL RESULTED IN ERRONEOUS CEA POSITION TO CEAC WHICH GENERATED CEAC PEN
ARKANSAS ONE 2	FS	HIGH ASI DURING STARTUP RESULTED IN SENSED LOW DNBR/ HIGH LDP
ARKANSAS ONE 2	FS	SINGLE CHANNEL EXCORE DETECTOR DATA SET INVALID
PALO VERDE 1	FS	CEAC MEMORY BOARD FAILURE CAUSES CEA DATA SET ERROR - CPC CHANNEL "X" AND CEAC(N) TRIPS
PALO VERDE 1	FCC	2 OF 2 CEACS FEEDING 4/4 CPCS INOPERABLE
PALO VERDE 1	FS	CEAC MICROPROCESSOR BOARD FAILURE CAUSES CEA DATA SET ERROR - CPC CHANNEL "X" AND CEAC(N) TRIPS
PALO VERDE 1	FS	SINGLE RTD TIME CONSTANTS OOT
PALO VERDE 1	FS	ELECTRICAL FAULT CAUSES CEA DATA SET ERROR - CPC CHANNEL "X" AND CEAC(N) TRIPS
PALO VERDE 1	FS	LOSS OF OFFSITE POWER CAUSES CPC TRIPS ON UNIT 1,2 AND VARIABLE OVERPOWER TRIP ON UNIT 3
PALO VERDE 1	FS	EXCESSIVE CEA DEVIATION FROM GROUP POSITION CAUSED CEAC PEN. FACTOR AND SENSED LOW DNBR
PALO VERDE 1	FS	ELECTRICAL GRID DISTURBANCE CAUSED VARIABLE OVERPOWER TRIPS ON ALL CPCS CHANNELS
PALO VERDE 1	FS	DROPPED CEA SUBGROUP CAUSED CEAC PEN. FACTOR AND SENSED LOW DNBR
PALO VERDE 1	FS	LOAD REJECTION TEST CAUSED RCP SPEED REDUCTION CAUSING LOW DNBR CPCS TRIPS
PALO VERDE 1	FCC	BOTH CEACS INOPERABLE FOR SURVEILLANCE TESTS FOLLOWED BY INDIVIDUAL CEAS "SLIPPING" OUT OF GROUP POSITIONS.
PALO VERDE 2	FS	LOW DNBR TRIP AS A RESULT OF RCP 1B TRIPPING ON A

Usina	Falha	Título
		PHASE-TO-PHASE ELECTRICAL FAULT.
PALO VERDE 2	FCC	REACTOR VENDOR SUPPLIES SOFTWARE UPDATE CONTAINING LATENT SOFTWARE ERROR
PALO VERDE 2	FS	CPC CHANNEL "X" DATA LINK FAILURE TO PLANT COMPUTER (INABILITY TO AUTOMATICALLY CONFIRM CEA POSITIONS)
PALO VERDE 2	FS	CEAC MEMORY BOARD FAILURE CAUSES CEA DATA SET ERROR - CPC CHANNEL "X" AND CEAC(N) TRIPS
PALO VERDE 2	FCC	TECHNICIANS INSERT WRONG DATA SETS IN ALL 4 CPC CHANNELS
PALO VERDE 2	FCC	INCORRECT ACCEPTANCE CRITERIA FOR EXCORE CALIBRATION >80%
PALO VERDE 2	FS	CEAC MICROPROCESSOR BOARD FAILURE CAUSES CEA DATA SET ERROR - CPC CHANNEL "X" AND CEAC(N) TRIPS
PALO VERDE 2	FS	LOSS OF OFFSITE POWER CAUSES CPC TRIPS ON UNIT 1,2 AND VARIABLE OVERPOWER TRIP ON UNIT 3
PALO VERDE 2	FS	LOW DNBR CAUSED BY AN ERRONEOUS POWER LEVEL INPUT FROM THE MIDDLE EXCORE DETECTOR TO THE CHANNEL "B" CORE PROTECTION CALCULATOR.
PALO VERDE 2	FCC	2/4 RCPS TRIPPED RESULTING IN LOW DNBR CPCS TRIPS
PALO VERDE 2	FS	HIGH ASI DURING STARTUP RESULTED IN SENSED LOW DNBR
PALO VERDE 2	FS	DUE TO EQUIPMENT PROBLEMS WITH TEMPERATURE
PALO VERDE 2	FS	FAST BUS TRANSFER CAUSED RCP SPEED DROP AND LOW DNBR CPCS TRIPS
PALO VERDE 2	FS	CEAC MICROPROCESSOR BOARD FAILURE CAUSES CEA DATA SET ERROR - CPC CHANNEL "X" AND CEAC(N) TRIPS
PALO VERDE 3	FS	LOSS OF 120V INVERTER FAILS CEAC(N) AND CPC CHANNEL "X"
PALO VERDE 3	FS	ELECTRICAL FAULT CAUSES CEA DATA SET ERROR - CPC CHANNEL "X" AND CEAC(N) TRIPS
PALO VERDE 3	FCC	INACCURATE CROSS CALIBRATION OF EXCORE VS. CALORIMETRIC ?T POWER TO 2 OF 4 CPC CHANNELS
PALO VERDE 3	FCC	3 OF 4 CPC NEUTRON FLUX CROSS CHANNEL CALIBRATIONS OOT
PALO VERDE 3	FS	LOSS OF 120V INVERTER FAILS CEAC(N) AND CPC CHANNEL "X"
PALO VERDE 3	FS	LOSS OF OFFSITE POWER CAUSES CPC TRIPS ON UNIT 1,2 AND VARIABLE OVERPOWER TRIP ON UNIT 3
PALO VERDE 3	FCC	INACCURATE CROSS CALIBRATION OF EXCORE VS. CALORIMETRIC ?T POWER TO ALL 4 CPC CHANNELS
PALO VERDE 3	FS	ELECTRICAL GRID DISTURBANCE CAUSED VARIABLE OVERPOWER TRIPS ON ALL CPCS CHANNELS
PALO VERDE 3	FCC	INACCURATE CROSS CALIBRATION OF EXCORE VS. CALORIMETRIC ?T POWER TO ALL 4 CPC CHANNELS
SAN ONOFRE 2	FS	CEAC FAILURE RESULTED IN CPCS TRIP
SAN ONOFRE 2	FS	CEAC 1 DECLARED INOPERABLE DUE TO ERRONEOUS CEA #20 POSITION INDICATION. MOST LIKELY SOURCE OF FAILURE WAS RSPT

Usina	Falha	Titulo
SAN ONOFRE 2	FCC	INACCURATE CROSS CALIBRATION OF EXCORE VS. CALORIMETRIC ?T POWER TO ALL 4 CPC CHANNELS
SAN ONOFRE 2	FS	DROPPED CEAS CAUSED CEAC PEN. FACTOR AND SENSED LOW DNBR
SAN ONOFRE 2	FS	OPERATORS PERCEIVED ALL FOUR CPCS TO BE INOPERABLE BASED UPON MISUNDERSTANDING OF THE FUNCTION OF CPC ALARM AND ANNUNCIATOR LIGHTS.
SAN ONOFRE 2	FCC	INACCURATE CROSS CALIBRATION OF RCS FLOW DATA SETS
SAN ONOFRE 2	FCC	INACCURATE CROSS CALIBRATION OF EXCORE VS. CALORIMETRIC ?T POWER TO ALL 4 CPC CHANNELS
SAN ONOFRE 2	FCC	TECHNICIANS INSERT WRONG DATA SETS IN ALL 4 CPC CHANNELS
SAN ONOFRE 2	FS	CEAC MICROPROCESSOR BOARD FAILURE CAUSES CEA DATA SET ERROR - CPC CHANNEL "X" AND CEAC(N) TRIPS
SAN ONOFRE 2	FS	A SPURIOUS CPC CHANNEL C TRIP OCCURRED REQUIRING PLACING CPC C INOP FOR TROUBLESHOOTING.
SAN ONOFRE 2	FS	HIGH ASI DURING SHUTDOWN RESULTED IN SENSED LOW DNBR/ HIGH LDP
SAN ONOFRE 2	FS	FAILURE TO PERFORM 4 HOUR CEA POSITION VERFICATION WHILE CPCS CHANNEL B INOPERABLE AND CEAC(1) INOP FLAGS SET IN ALL FOUR CPCS CHANNELS.
SAN ONOFRE 2	FS	CEA POSITION TRANSMITTER OR CABLE FAILURE CAUSES CEA DATA SET ERROR - CPCS CHANNEL "X" AND CEAC(N) TRIPS
SAN ONOFRE 2	FS	MALFUNCTION OF DATA ACQUISITION SYSTEM ADC RESULTS IN FAILURE OF CPC CHANNEL B
SAN ONOFRE 2	FS	DURING POST-CORE HOT FUNCTIONAL TESTING CALIBRATION PROBLEM IMPACTING RTD SIGNALS USED BY CPCS IDENTIFIED
SAN ONOFRE 2	FS	REACTOR TRIPPED WHEN 120 VAC VITAL BUS 3 WAS DE-ENERGIZED DUE TO FAILURE OF INVERTER Y003
SAN ONOFRE 2	FS	CPC CHANNEL D FAILED FOR NO APPARENT REASON.
SAN ONOFRE 2	FS	CPC CHANNEL A FAILED DUE TO POWER SUPPLY MALFUNCTION.
SAN ONOFRE 2	FS	FAULTY RSPT RESULTED IN ERRONEOUS INDICATIONS OF CEA #79 TO CEAC 1
SAN ONOFRE 2	FS	DROPPED CEA 12 DROPPED FROM 148" TO 120" CAUSING CEAC PFS AND LOW DNBR CPCS TRIPS.
SAN ONOFRE 2	FS	DRIFT IN LINEAR GAIN OF EXCORE AMPLIFIER USED AS INPUT TO CPC CHANNEL B RESULTED IN CHANNEL BEING DECLARED INOP
SAN ONOFRE 2	FS	DROPPED CEAS 68, 87 CAUSE CEAC PFS AND LOW DNBR CPCS TRIPS.
SAN ONOFRE 2	FS	FAULTY CPIA CARD RESULTS IN INACCURATE CEA #28 POSITION INDICATION TO CEAC 1
SAN ONOFRE 2	FS	MORE THAN 3 AUTORESTARTS IN 12 HRS IN CPC CHANNEL C DUE TO POWER SUPPLY FLUCTUATIONS
SAN ONOFRE 2	FS	LOOSE CEA POSITION CABLE CAUSED CEAC DEVIATION

Usina	Falha	Titulo
		ALARMS ON CEAC 2 AND CPC CHANNEL D
SAN ONOFRE 2	FS	CPC CHANNEL C DECLARED INOP DUE TO OUT OF TOLERANCE CALIBRATION FACTOR FOR COLD LEG RTD CONVERTER CIRCUIT DRIFT
SAN ONOFRE 2	FCC	ADDRESSIBLE CONSTANTS IN CPC CHANNELS B AND D WERE FOUND TO BE INCORRECT.
SAN ONOFRE 2	FS	CPC D CHANNEL EXPERIENCED 3 SPURIOUS TRIPS DUE TO FAILED DATA CARD (MUX)
SAN ONOFRE 2	FS	FAULTY RSPT RESULTED IN ERRONEOUS INDICATIONS OF CEA #20 TO CEAC 1
SAN ONOFRE 2	FS	LOCAL POWER SUPPLY FAILURE CAUSES CPC CHANNEL D TO FAIL
SAN ONOFRE 2	FS	POWER SUPPLY FLUCTUATION
SAN ONOFRE 2	FS	LOSS OF 120V INVERTER FAILS CEAC(N) AND CPC CHANNEL "X"
SAN ONOFRE 2	FS	CEA POSITION TRANSMITTER OR CABLE FAILURE CAUSES CEA DATA SET ERROR - CPCS CHANNEL "X" AND CEAC(N) TRIPS
SAN ONOFRE 2	FCC	LOCAL POWER SUPPLY FAILURE CAUSES CPC WATCHDOG TIMER FAILURE
SAN ONOFRE 2	FS	CPC D CHANNEL POWER SUPPLY TRIPPED REQUIRING BYPASSING CPC D
SAN ONOFRE 3	FCC	OPERATORS FAIL TO PERFORM 12HR AUTO-RESTART SURVEILLANCE ON ALL CPC CHANNELS
SAN ONOFRE 3	FCC	INACCURATE CROSS CALIBRATION OF EXCORE VS. CALORIMETRIC ?T POWER TO ALL 4 CPC CHANNELS
SAN ONOFRE 3	FCC	WITH COLSS OUT OF SERVICE FOR MAINT., AND COLSS BACKUP COMPUTER SYSTEM SUBSEQUENTLY FAILED
SAN ONOFRE 3	FS	WITH CPC CHANNEL 'A' IN BYPASS, CPC 'D' WAS DECLARED INOPERABLE
SAN ONOFRE 3	FS	CPC CHANNEL 'A' REMOVED FROM SERVICE FOR INVESTIGATION AND REPAIR OF INTERMITTENT SENSOR FAILURE
SAN ONOFRE 3	FS	COLSS MONITORED AZIMUTHAL POWER TILT NOT CONSISTENT WITH TECH. SPEC. REQUIRED MEASUREMENTS.
SAN ONOFRE 3	FS	DROPPED CEA DURING CONTROLLED SHUTDOWN CAUSED CEAC PEN. FACTOR AND SENSED LOW DNBR
SAN ONOFRE 3	FS	CEAC MICROPROCESSOR BOARD FAILURE CAUSES CEA DATA SET ERROR - CPC CHANNEL "X" AND CEAC(N) TRIPS
SAN ONOFRE 3	FS	DROPPED CEA DURING FULL POWER OPERATION CAUSED CEAC PEN. FACTOR AND SENSED LOW DNBR
SAN ONOFRE 3	FCC	VENDOR SUPPLIES ERRONEOUS DATA INPUT TO ALL 4 CPC CHANNELS
WATERFORD 3	FCC	INACCURATE CROSS CALIBRATION OF EXCORE VS. CALORIMETRIC ?T POWER TO ALL 4 CPC CHANNELS
WATERFORD 3	FCC	OPERATORS FAIL TO PERFORM REFUELING INTERVAL SURVEILLANCE ON ALL CPC CHANNELS
WATERFORD 3	FS	REACTOR TRIP OCCURRED WHEN RCS PRESSURE WAS OUT OF RANGE ALLOWED BY CPCS. CAUSED BY AUTOMATIC TRUBINE RUNBACK.

Usina	Falha	Título
WATERFORD 3	FS	THE SURVEILLANCE LOG ENTRY CONTAINED A NOTATION INDICATING THAT CPCS, REQUIRED TO PERFORM THE CHANNEL CHECK, WAS INOPERABLE.
WATERFORD 3	FS	CPCS "D" CHANNEL INOP DUE TO FAILED RTD AND SET TO TRIP. CEAC(1) WAS UNDER TEST AND OPERATOR INSERTED PF=3.0, INSTEAD OF 1.0 CAUSING TRIP TO CPCS "A".
WATERFORD 3	FS	ELECTRICAL FAULT TRIPPED RCPS 1A, 2A THIS GENERATED LOW DNBR CPCS TRIPS.
WATERFORD 3	FCC	INACCURATE CROSS CALIBRATION OF EXCORE VS. CALORIMETRIC ?T POWER TO ALL 4 CPC CHANNELS
WATERFORD 3	FCC	HIGH LOG POWER BYPASS REMOVAL SETPOINTS (1E-4) INCORRECT
WATERFORD 3	FS	CEA POSITION TRANSMITTER OR CABLE FAILURE CAUSES CEA DATA SET ERROR - CPCS CHANNEL "X" AND CEAC(N) TRIPS
WATERFORD 3	FS	CEA POSITION TRANSMITTER OR CABLE FAILURE CAUSES CEA DATA SET ERROR - CPCS CHANNEL "X" AND CEAC(N) TRIPS
WATERFORD 3	FS	SINGLE RTD TIME CONSTANTS OOT
WATERFORD 3	FS	SINGLE RTD TIME CONSTANTS OOT
WATERFORD 3	FS	HIGH ASI DURING START-UP RESULTED IN SENSED LOW DNBR/ HIGH LDP
WATERFORD 3	FS	LOW DNBR CPCS TRIPS.
WATERFORD 3	FCC	HIGH LOG POWER BYPASS REMOVAL SETPOINTS (1E-4) INCORRECT
WATERFORD 3	FCC	OPERATORS FAIL TO CONFIRM ASI IN ALL 4 CPC CHANNELS WHEN REACTOR POWER > 20%
WATERFORD 3	FCC	OPERATORS FAIL TO CONFIRM ASI IN ALL 4 CPC CHANNELS WHEN REACTOR POWER > 20%
WATERFORD 3	FS	DROPPED CEA CAUSED CEAC PEN. FACTOR AND SENSED LOW DNBR TRIP.
WATERFORD 3	FS	REACTOR POWER CUTBACK AND TURBINE SETBACK TO ~50% CAUSED LOW RCS PRESSURE AND LOW DNBR CPCS TRIPS.
WATERFORD 3	FS	HIGH ASI DURING POWER REDUCTION TO RECOVER DROPPED CEA RESULTED IN SENSED LOW DNBR/ HIGH LDP
WATERFORD 3	FS	DROPPED CEA CAUSED CEAC PEN. FACTOR AND SENSED LOW DNBR TRIP.
WATERFORD 3	FS	DROPPED CEA CAUSED CEAC PEN. FACTOR
WATERFORD 3	FS	PLANT MONITORING COMPUTER DOWN OPERATORS HAD TO MANUALLY ADJUST CEA POSITIONS
WATERFORD 3	FS	ELECTRICAL NOISE WITHIN EXCORE NUCLEAR INSTRUMENTATION CAUSED CPCS CHANNELS C AND D TO MOMENTARILY SPIKE ABOVE 1.0E-4 PERCENT POWER
WATERFORD 3	FS	HIGH ASI DURING STARTUP RESULTED IN SENSED LOW DNBR/ HIGH LDP
WATERFORD 3	FS	HIGH ASI DURING STARTUP RESULTED INSENSED LOW DNBR/ HIGH LDP
WATERFORD 3	FS	TURBINE TRIP CAUSED CPCS TRIP

APÊNDICE D – REQUISITOS MÍNIMOS DE UM RELATÓRIO DE EVENTO OPERACIONAL.

Conforme a norma CNEN-NN 1.14 (CNEN, 2000) seção 6.3, o relatório de evento operacional deverá conter os seguintes requisitos:

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*;

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;

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) o 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*.

APÊNDICE E – CÓDIGO FONTE DOS RELACIONAMENTOS FEITOS NO PROGRAMA MAFIC-D

A seguir, é mostrada a sub-rotina do código fonte dos relacionamentos entre os critérios de confiabilidade:

```
'*************************************************************************
' Subrotina que Calcula o Nível de Confiabilidade                        *
'*************************************************************************
'*
On Error GoTo ERRO
Dim ref1, ref3, ref4 As String
Dim ref2 As Double
Dim ref5, ref6, ref7, ref13 As Boolean
Dim ref8, ref9, ref10, ref11, ref12 As Boolean

'***CARREGAMENTO DE VARIÁVEL
   ref1 = txtFalha.Text
   ref3 = txtCausa.Text
   ref4 = txtTFalha.Text

   ref2 = txtTaxaFalha.Text
   'ref2 = Format(txtTaxaFalha.Text, "#0.0################")
   ref2 = txtTaxaFalha.Text
   ref5 = chkSPR.Value
   ref6 = chkLIM.Value
   ref7 = chkCRT.Value
   ref13 = ChkMEI.Value
```

```
    ref8 = chkDP.Value
    ref9 = chkDE.Value
    ref10 = chkHU.Value
    ref11 = chkS.Value
    ref12 = chkSOF.Value


'***RELACIONAMENTO ENTRE AS VARIÁVEIS

'****************************************FALHA SIMPLES

   If (ref1 = "FALHA SIMPLES") Then                    '***FALHA SIMPLES

     If (ref2 > 0.01) Then
      txtDesempenho.Text = "VERMELHO"
     Else

     If (ref4 = "FALHA DE SOFTWARE") Then              '***FALHA DE SOFTWARE

       If ((ref2 <= 0.01) And (ref2 > 0.00001)) Then

         If (ref5 = True) Then                         '***DESAFIO O SPR
          txtDesempenho.Text = "VERMELHO"
         ElseIf (ref6 = True) Then                     '***DESAFIO O LIM
          If ((ref8 = True) Or (ref9 = True) Or (ref10 = True) Or (ref11 = True) Or (ref12 = True))
Then
           txtDesempenho.Text = "VERMELHO"
          Else
           txtDesempenho.Text = "LARANJA"
          End If
```

```
        ElseIf (ref7 = True) Then                    '***DESAFIO O CTR
         If ((ref8 = True) Or (ref9 = True) Or (ref10 = True) Or (ref11 = True) Or (ref12 = True))
Then
          txtDesempenho.Text = "LARANJA"
         Else
          txtDesempenho.Text = "AMARELO"
         End If
        ElseIf (ref13 = True) Then                   '***DESAFIO O M&I
         If ((ref8 = True) Or (ref9 = True) Or (ref10 = True) Or (ref11 = True) Or (ref12 = True))
Then
          txtDesempenho.Text = "AMARELO"
         Else
          txtDesempenho.Text = "VERDE"
         End If
        Else
         txtDesempenho.Text = "VERDE"
        End If


      ElseIf (ref2 <= 0.00001) Then


        If (ref5 = True) Then                        '***DESAFIO O SPR
         If ((ref8 = True) Or (ref9 = True) Or (ref10 = True) Or (ref11 = True) Or (ref12 = True))
Then
          txtDesempenho.Text = "LARANJA"
         Else
          txtDesempenho.Text = "AMARELO"
         End If
        ElseIf (ref6 = True) Then                    '***DESAFIO O LIM
```

```
        If ((ref8 = True) Or (ref9 = True) Or (ref10 = True) Or (ref11 = True) Or (ref12 = True))
Then
          txtDesempenho.Text = "AMARELO"
        Else
          txtDesempenho.Text = "VERDE"
        End If
      Else
        txtDesempenho.Text = "VERDE"
      End If

    End If

  Else                                '***OUTROS MODOS DE FALHAS

    If ((ref2 <= 0.01) And (ref2 > 0.00001)) Then

      If (ref5 = True) Then                    '***DESAFIO O SPR
        txtDesempenho.Text = "LARANJA"
      ElseIf (ref6 = True) Then                '***DESAFIO O LIM
        If ((ref8 = True) Or (ref9 = True) Or (ref10 = True) Or (ref11 = True) Or (ref12 = True))
Then
          txtDesempenho.Text = "LARANJA"
        Else
          txtDesempenho.Text = "AMARELO"
        End If
      ElseIf (ref7 = True) Then                '***DESAFIO O CTR

        If ((ref8 = True) Or (ref9 = True) Or (ref10 = True) Or (ref11 = True) Or (ref12 = True))
Then
          txtDesempenho.Text = "AMARELO"
```

```
            Else
              txtDesempenho.Text = "VERDE"
            End If
          Else
            txtDesempenho.Text = "VERDE"
          End If


        ElseIf (ref2 <= 0.00001) Then


        If (ref5 = True) Then                    '***DESAFIO O SPR
          If ((ref8 = True) Or (ref9 = True) Or (ref10 = True) Or (ref11 = True) Or (ref12 = True))
Then
            txtDesempenho.Text = "AMARELO"
          Else
            txtDesempenho.Text = "VERDE"
          End If
        Else
          txtDesempenho.Text = "VERDE"
        End If


      End If


    End If


  End If

'*****************************************FALHA DE CAUSA COMUM

  ElseIf (ref1 = "FALHA DE CAUSA COMUM") Then        '***FALHA DE CAUSA COMUM
```

```
If (ref2 > 0.01) Then
 txtDesempenho.Text = "PRETO"
Else

 If (ref4 = "FALHA DE SOFTWARE") Then          '***FALHA DE SOFTWARE

  If ((ref2 <= 0.01) And (ref2 > 0.0001)) Then

   If (ref5 = True) Then                    '***DESAFIO O SPR
    txtDesempenho.Text = "PRETO"
   ElseIf (ref6 = True) Then                '***DESAFIO O LIM
    If ((ref8 = True) Or (ref9 = True) Or (ref10 = True) Or (ref11 = True) Or (ref12 = True))
Then
     txtDesempenho.Text = "PRETO"
    Else
     txtDesempenho.Text = "VERMELHO"
    End If
   ElseIf (ref7 = True) Then                '***DESAFIO O CTR
    If ((ref8 = True) Or (ref9 = True) Or (ref10 = True) Or (ref11 = True) Or (ref12 = True))
Then
     txtDesempenho.Text = "VERMELHO"
    Else
     txtDesempenho.Text = "LARANJA"
    End If
   ElseIf (ref13 = True) Then               '***DESAFIO O M&I
    If ((ref8 = True) Or (ref9 = True) Or (ref10 = True) Or (ref11 = True) Or (ref12 = True))
Then
     txtDesempenho.Text = "LARANJA"
    Else
```

```
            txtDesempenho.Text = "AMARELO"
          End If
        Else
          txtDesempenho.Text = "AMARELO"
        End If


      ElseIf ((ref2 <= 0.0001) And (ref2 > 0.000001)) Then


        If (ref5 = True) Then                    '***DESAFIO O SPR
          If ((ref8 = True) Or (ref9 = True) Or (ref10 = True) Or (ref11 = True) Or (ref12 = True))
Then
            txtDesempenho.Text = "VERMELHO"
          Else
            txtDesempenho.Text = "LARANJA"
          End If
        ElseIf (ref6 = True) Then                '***DESAFIO O LIM
          If ((ref8 = True) Or (ref9 = True) Or (ref10 = True) Or (ref11 = True) Or (ref12 = True))
Then
            txtDesempenho.Text = "LARANJA"
          Else
            txtDesempenho.Text = "AMARELO"
          End If
        ElseIf (ref7 = True) Then                '***DESAFIO O CTR
          If ((ref8 = True) Or (ref9 = True) Or (ref10 = True) Or (ref11 = True) Or (ref12 = True))
Then
            txtDesempenho.Text = "AMARELO"
          Else
            txtDesempenho.Text = "VERDE"
          End If
```

```
        Else
          txtDesempenho.Text = "VERDE"
        End If

      ElseIf (ref2 <= 0.000001) Then

        If (ref5 = True) Then                    '***DESAFIO O SPR
          If ((ref8 = True) Or (ref9 = True) Or (ref10 = True) Or (ref11 = True) Or (ref12 = True))
Then
            txtDesempenho.Text = "LARANJA"
          Else
            txtDesempenho.Text = "AMARELO"
          End If
        ElseIf (ref6 = True) Then                '***DESAFIO O LIM
          If ((ref8 = True) Or (ref9 = True) Or (ref10 = True) Or (ref11 = True) Or (ref12 = True))
Then
            txtDesempenho.Text = "AMARELO"
          Else
            txtDesempenho.Text = "VERDE"
          End If
        Else
          txtDesempenho.Text = "VERDE"
        End If

      End If

    Else                                         '***OUTROS MODOS DE FALHAS

      If ((ref2 <= 0.01) And (ref2 > 0.0001)) Then
```

```
        If (ref5 = True) Then                    '***DESAFIO O SPR
          txtDesempenho.Text = "VERMELHO"
        ElseIf (ref6 = True) Then                '***DESAFIO O LIM
          If ((ref8 = True) Or (ref9 = True) Or (ref10 = True) Or (ref11 = True) Or (ref12 = True))
Then
            txtDesempenho.Text = "VERMELHO"
          Else
            txtDesempenho.Text = "LARANJA"
          End If
        ElseIf (ref7 = True) Then                '***DESAFIO O CTR
          If ((ref8 = True) Or (ref9 = True) Or (ref10 = True) Or (ref11 = True) Or (ref12 = True))
Then
            txtDesempenho.Text = "LARANJA"
          Else
            txtDesempenho.Text = "AMARELO"
          End If
        ElseIf (ref13 = True) Then               '***DESAFIO O M&I
          If ((ref8 = True) Or (ref9 = True) Or (ref10 = True) Or (ref11 = True) Or (ref12 = True))
Then
            txtDesempenho.Text = "AMARELO"
          Else
            txtDesempenho.Text = "VERDE"
          End If
        Else
          txtDesempenho.Text = "VERDE"
        End If


      ElseIf ((ref2 <= 0.0001) And (ref2 > 0.000001)) Then
```

```
        If (ref5 = True) Then                    '***DESAFIO O SPR
          If ((ref8 = True) Or (ref9 = True) Or (ref10 = True) Or (ref11 = True) Or (ref12 = True))
Then
            txtDesempenho.Text = "VERMELHO"
          Else
            txtDesempenho.Text = "LARANJA"
          End If
        ElseIf (ref6 = True) Then                '***DESAFIO O LIM
          If ((ref8 = True) Or (ref9 = True) Or (ref10 = True) Or (ref11 = True) Or (ref12 = True))
Then
            txtDesempenho.Text = "LARANJA"
          Else
            txtDesempenho.Text = "AMARELO"
          End If
        ElseIf (ref7 = True) Then                '***DESAFIO O CTR
          If ((ref8 = True) Or (ref9 = True) Or (ref10 = True) Or (ref11 = True) Or (ref12 = True))
Then
            txtDesempenho.Text = "AMARELO"
          Else
            txtDesempenho.Text = "VERDE"
          End If
        Else
          txtDesempenho.Text = "VERDE"
        End If

      ElseIf (ref2 <= 0.000001) Then

        If (ref5 = True) Then                    '***DESAFIO O SPR
          If ((ref8 = True) Or (ref9 = True) Or (ref10 = True) Or (ref11 = True) Or (ref12 = True))
Then
```

```
            txtDesempenho.Text = "LARANJA"
          Else
            txtDesempenho.Text = "AMARELO"
          End If
        ElseIf (ref6 = True) Then                    '***DESAFIO O LIM
          If ((ref8 = True) Or (ref9 = True) Or (ref10 = True) Or (ref11 = True) Or (ref12 = True))
Then
            txtDesempenho.Text = "AMARELO"
          Else
            txtDesempenho.Text = "VERDE"
          End If
        Else
            txtDesempenho.Text = "VERDE"
        End If

      End If

    End If

   End If

  End If

  VDesempenho = txtDesempenho.Text

Exit Sub

ERRO:
MsgBox Err15, vbCritical, "ERRO"
```