AVALIAÇÃO DA EXTENSÃO DE TEMPOS PERMITIDOS DE INDISPONIBILIDADE E DE INTERVALOS DE TESTES DE ESPECIFICAÇÕES TÉCNICAS DE CENTRAIS NUCLEARES COM BASE EM RISCO

Sonia Maria Orlando Gibelli

TESE SUBMETIDA AO CORPO DOCENTE DA COORDENAÇÃO DOS PROGRAMAS DE PÓS-GRADUAÇÃO DE ENGENHARIA DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE DOUTOR EM CIÊNCIAS EM ENGENHARIA NUCLEAR.

Aprovada por:

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

_____
Prof. Antonio Carlos Marques Alvim, Ph.D.

_____
Prof. Fernando Carvalho da Silva, D.Sc.

_____
Prof. Marcio Nele de Souza, D.Sc.

_____
Dr. Sergio de Queiroz Bogado Leite, Ph.D.

RIO DE JANEIRO, RJ - BRASIL
MARÇO DE 2008

GIBELLI, SONIA MARIA ORLANDO
Avaliação da Extensão de Tempos Permitidos de Indisponibilidades e de Intervalos de Testes de Especificações Técnicas de Centrais Nucleares com Base em Risco
[Rio de Janeiro] 2008
XV, 120 p. 29,7 cm (COPPE/UFRJ, D.Sc., Engenharia Nuclear, 2008)
Tese - Universidade Federal do Rio de Janeiro, COPPE
1. Especificações Técnicas
2. Análise Probabilística de Segurança
3. Medidas Compensatórias de Risco
I. COPPE/UFRJ II. Título (série)

À memória de meus pais,
Sonia Maia Forte Orlando e
Hygino Geraldo Orlando,
e de meus avós,
Maria Guedes Maia Forte e
Nelson Guanabarino Maia Forte

Agradecimentos

Ao meu orientador, Prof. Paulo Fernando Frutuoso e Melo, pela inestimável amizade e segura assistência acadêmica.

Ao Prof. Antonio Carlos Marques Alvim, pelas excelentes aulas e conselhos.

Ao colega Sergio de Queiroz Bogado Leite pela amizade e sábias sugestões.

Aos colegas de sala da CNEN, Júlio Cezar Rausch, Marco Antonio Bayout Alvarenga, Marcos Eduardo Costa Nunes e Renato Alves da Fonseca pela colaboração e apoio em diversas questões técnicas.

Ao colega Auro Correia Pontedeiro, pelo constante incentivo e apoio.

Ao colega Luiz Carlos Pereira Martins, por sua indispensável ajuda na correta formatação do trabalho.

À Maria Emília Frade de Mello por sua presteza na busca de referências bibliográficas.

Aos colegas da ELETRONUCLEAR Luiz Eurípedes Massière de Castro Silva e José Onusic Jr., por suas prontas informações sobre detalhes da APS de Angra 1.

À CNEN, por ter me permitido percorrer o caminho que me conduziu à conclusão desta tese.

Aos meus padrinhos, Vera Maria Guedes Veneu e Antonio Luiz da Rocha Veneu, que me estenderam as mãos nos momentos mais difíceis.

Expresso, ainda, meus sinceros agradecimentos a todos que fizeram deste trabalho, além de uma enriquecedora experiência profissional, uma oportunidade única de voltar ao ambiente acadêmico e fazer tão boas amizades.

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

AVALIAÇÃO DA EXTENSÃO DE TEMPOS PERMITIDOS DE INDISPONIBILIDADE E DE INTERVALOS DE TESTES DE ESPECIFICAÇÕES TÉCNICAS DE CENTRAIS NUCLEARES COM BASE EM RISCO

Sonia Maria Orlando Gibelli

Março/2008

Orientador: Paulo Fernando Ferreira Frutuoso e Melo

Programa: Engenharia Nuclear

O objetivo deste trabalho é, através do uso da Análise Probabilística de Segurança (APS), apresentar um estudo de extensão de Tempos Permitidos de Indisponibilidade (TPI) e de Intervalos de Teste (IT) de Especificações Técnicas (ET) para a Central Nuclear de Angra 1, com base em análise de risco. A medida de risco utilizada para os cálculos é a Freqüência de Dano ao Núcleo (FDN), obtida de uma APS Nível 1. Extensões de TPI e de IT são calculadas através do código SAPHIRE, para os sistemas de Injeção de Segurança (SIS), Água de Serviço (SAS) e Água Auxiliar de Alimentação (SAAA). Para compensar os incrementos de risco das extensões de TPI e de IT, as medidas compensatórias: (1) Teste adicional do trem redundante e (2) Modificação da estratégia de teste, são incorporados nos cálculos de risco. Os resultados mostram que as extensões de TPI propostas são aceitáveis para o SIS e o SAS com as medidas compensatórias. A extensão de TPI proposta não é aceitável para o SAAA. As extensões de IT propostas são aceitáveis para os três sistemas sem a implementação de medidas compensatórias.

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

RISK-BASED EVALUATION OF ALLOWED OUTAGE TIME AND SURVEILLANCE TEST INTERVAL EXTENSIONS FOR NUCLEAR POWER PLANTS

Sonia Maria Orlando Gibelli

March/2008

Advisor: Paulo Fernando Ferreira Frutuoso e Melo

Department: Nuclear Engineering

The main goal of this work is, through the use of Probabilistic Safety Analysis (PSA), to evaluate Technical Specification (TS) Allowed Outage Times (AOT) and Surveillance Test Intervals (STI) extensions for Angra 1 nuclear power plant. PSA has been incorporated as an additional tool, required as part of NPP licensing process. The risk measure used in this work is the Core Damage Frequency (CDF), obtained from the Angra 1 PSA Level 1. AOT and STI extensions are calculated for the Safety Injection System (SIS), Service water System (SAS) and Auxiliary Feedwater System (AFS) through the use of SAPHIRE code. In order to compensate for the risk increase caused by the extensions, compensatory measures as (1) Test of redundant train prior to entering maintenance and (2) Staggered test strategy are proposed. Results have shown that the proposed AOT extensions are acceptable for the SIS and SAS with the implementation of compensatory measures. The proposed AOT extension is not acceptable for the AFS. The STI extensions are acceptable for all three systems.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

LISTA DE SÍMBOLOS

Letras Latinas

d - Duração da indisponibilidade

d_{TPI} - Duração do TPI estendido

f - Freqüência anual média de ocorrências do TPI

FDN_1 - Freqüência de dano ao núcleo, calculada com o componente indisponível

FDN_B - Freqüência de dano ao núcleo calculada originalmente na APS *(baseline)*

FDN_{EIT} - Valor da FDN calculado com a extensão de intervalo de teste

k - Número de componentes de um grupo de causa comum

m - Número total de componentes de um grupo de causa comum

Q - Indisponibilidade média

Q_{CC} - Probabilidade de causa comum

Q_{CCO} - Probabilidade de falha de causa comum na operação

Q_{CCP} - Probabilidade de falha de causa comum na partida

Q'_{CCP} - Probabilidade de causa comum na partida com IT estendido

Q_{FP} - Probabilidade de falha na partida

Q'_{FP} - Probabilidade de falha na partida com IT estendido

Q_{FO} - Probabilidade de falha na operação

Q_k^{Esc} - Probabilidade de k falhas específicas de componentes devido às falhas de causa comum com estratégia de teste escalonado

$Q_k^{(m)}$ - Probabilidade de um evento básico de causa comum envolvendo k componentes específicos em um grupo de causa comum de m componentes, $(1 \leq k \leq m)$

Q_k^{Seq} - Probabilidade de k falhas específicas de componentes devido às falhas de causa comum com estratégia de teste seqüencial

Q_{MX} - Indisponibilidade do componente x devido à manutenção

Q_S - Probabilidade de falha do sistema

Q_T - Probabilidade de falha total de cada componente devido a todas as falhas independentes e às falhas de causa comum

r - Risco associado ao TPI de evento simples

R - Contribuição de risco anual médio

R_1 - Aumento do nível de risco, quando o componente está indisponível

R_B - Risco incondicional de base *(baseline)*

R(t) - Risco condicional

r_c - Critério de risco de evento simples

R_c - Critério de risco anual médio

R_D - Contribuição de risco limitado por teste

R_0 - Freqüência de dano ao núcleo, avaliada com o componente disponível

t - Tempo

T - Intervalo de teste

T_E - Intervalo de teste da extensão

LISTA DE SÍMBOLOS (cont.)

Letras Gregas

α_k - Fração da freqüência total de falha dos eventos que ocorrem em um sistema e envolvem a falha de k componentes devido a causas comuns

α_k^e - Fração da freqüência total de falha dos eventos que ocorrem em um sistema e envolvem a falha de k componentes devido a causas comuns, para a estratégia de teste escalonado

β - Probabilidade condicional de que a causa da falha de um componente seja compartilhada por um ou mais componentes adicionais, dado que um componente falhou

β_e - Fator beta para estratégia de teste escalonado

β_P - Fator beta para as falhas de causa comum na partida

β_O - Fator beta para as falhas de causa comum na operação

γ - Probabilidade condicional de que a causa da falha de um componente que é compartilhada por um ou mais componentes seja compartilhada por dois ou mais componentes adicionais, dado que dois componentes falharam

δ - Probabilidade condicional de que a causa da falha de um componente que é compartilhada por dois ou mais componentes seja compartilhada por três ou mais componentes adicionais, dado que três componentes falharam

ΔFDN - Incremento condicional da FDN, unidade reator-ano

ΔR - Incremento condicional de risco

λ - Taxa de falha por unidade de tempo

LISTA DE SIGLAS

AIEA - Agencia Internacional de Energia Atômica

APS – Análise Probabilística de Segurança

CLO – Condição Limite de Operação

CNEN – Comissão Nacional de Energia Nuclear

ET – Especificação Técnica

FCC – Falhas de Causa Comum

FDN – Freqüência de Dano ao Núcleo

FGLA – Freqüência de Grande Liberação Antecipada

MLG – Múltiplas Letras Gregas

IT – Intervalo de Teste

LOCA – *Loss of Coolant Accident*

MC – Manutenção Corretiva

MP – Manutenção Preventiva

NRC – *Nuclear Regulatory Commission*

RFAS – Relatório Final de Análise de Segurança

RAW – *Risk Achievement Worth*

RRW– *Risk Reduction Worth*

SAAA – Sistema de Água de Alimentação Auxiliar

SAS – Sistema de Água de Serviço

SIS – Sistema de Injeção de Segurança

TPI – Tempo permitido de Indisponibilidade

1. INTRODUÇÃO

O objetivo deste trabalho é, através do uso de técnicas baseadas em análise de risco, apresentar um estudo de extensão de Tempos Permitidos de Indisponibilidades e de Intervalos de Testes de Especificações Técnicas (ET) para centrais nucleares de potência apresentando aplicação específica para a central nuclear de Angra 1 [1]. As Especificações Técnicas são compostas por um conjunto de itens, que estabelecem limites e condições seguras de operação, como parte de exigências regulatórias para a autorização de operação de uma central nuclear.

Tradicionalmente, itens contidos nas Especificações Técnicas, tais como exigências de Condição Limite de Operação (CLO), que incluem os Tempos Permitidos de Indisponibilidade (TPI) para equipamentos e Intervalos de testes (IT), têm sido elaborados baseados em análises determinísticas ou mesmo provenientes de práticas operacionais convencionais e julgamentos de engenharia.

Através da experiência operacional, foram surgindo indícios de que tais práticas poderiam ser desnecessariamente restritivas [2], o que resultou na necessidade crescente, tanto da parte das concessionárias operadoras de centrais nucleares, como dos órgãos regulatórios, de que fossem estabelecidos os riscos associados às especificações técnicas vigentes.

Assim como as exigências para as Especificações Técnicas, a análise de segurança, como parte integrante do processo de licenciamento inicial e de operação de uma central nuclear, também era tradicionalmente desenvolvida através de métodos puramente determinísticos. Entretanto, o desenvolvimento e aprimoramento constante de métodos probabilísticos de análise de risco, ou seja, da Análise Probabilística de Segurança (APS) como ferramenta adicional da análise deteminística para a avaliação das questões de segurança da planta, resultaram em sua incorporação, como requisito do processo de licenciamento de centrais nucleares.

De fato, ao longo dos últimos dez anos, estudos de APS vêem sendo produzidos para a maioria das centrais nucleares no mundo e, em geral, essas APS apresentam um nível de qualidade aceitável para serem usadas rotineiramente tanto pelas operadoras, como pelos órgãos regulatórios, constituindo um conjunto de informações de entrada

para o processo de decisão regulatória nas questões de segurança nuclear. Tais práticas são denominadas regulamentação baseada em risco [3].

A abordagem moderna consta da aplicação de um processo integrado de decisão regulatória, onde são combinadas avaliações com bases determinísticas e probabilísticas.

A Análise Probabilística de Segurança consta de um método sistemático de avaliação quantitativa do comportamento e resposta da planta a eventos iniciadores, tendo como parte dos resultados possíveis, seqüências de acidentes, bem como os riscos associados às mesmas [4]. Ao longo de décadas de experiência operacional foram surgindo várias possíveis aplicações de resultados de APS, sendo uma delas a avaliação das Especificações Técnicas. Os métodos baseados em risco usados para a melhoria de exigências de Especificações Técnicas podem: (1) avaliar o impacto no risco e justificar modificações baseadas em argumentos objetivos de risco (2) fornecer uma base para o processo de decisão regulatória baseada em risco para a avaliação de tais modificações.

A análise baseada em APS fornece uma avaliação quantitativa do impacto no risco da modificação de ET proposta, de tal forma que a justificativa para a mudança seja baseada em argumentos objetivos. Além disso, várias exigências de modificações podem ser avaliadas quantitativamente, através do uso de medidas de risco, podendo-se garantir que são mantidas as margens de segurança da planta, tanto em condições de operação normal como em acidentes.

Este trabalho apresenta proposta de extensão de TPI e de IT para a central de Angra 1, através do uso da APS de Angra 1 como ferramenta de cálculo [5]. A APS de Angra 1 foi desenvolvida pela ELETRONUCLEAR como parte dos requisitos regulatórios exigidos pela CNEN para a concessão da Autorização para a Operação Permanente da Central [6].

A medida de risco utilizada para os cálculos deste trabalho, é a Freqüência de Dano ao Núcleo (FDN), obtida como resultado do estudo de APS Nível 1 [4]. Algumas modificações propostas incorrem em pequenos incrementos de risco, ou seja, menores que 1,0E-06 por reator-ano e são consideradas aceitáveis [7]. Entretanto, quando mudanças propostas de ET resultam em incrementos na FDN maiores do que 1,0E-06 por reator-ano, a aceitação das mesmas é sujeita a um processo de avaliação de acordo

com os critérios de risco adotados. Para alguns desses casos, medidas compensatórias podem ser adotadas como parte integrante da avaliação das propostas. Tais medidas têm a função de balancear ou compensar o aumento de risco calculado associado à mudança proposta.

Este trabalho apresenta a análise da extensão de TPI e de IT para três sistemas de segurança de Angra 1:

1) Sistema de Injeção de Segurança (SIS);

2) Sistema de Água de Serviço (SAS);

3) Sistema de Água Auxiliar de Alimentação (SAAA).

Para compensar aumentos de risco introduzidos através de extensões de TPI propostas para os sistemas SIS, SAS e SAAA, são implementadas as seguintes medidas compensatórias: (1) o teste adicional dos trens redundantes de cada sistema em análise, imediatamente antes do início de uma atividade de manutenção corretiva no trem falho; (2) a modificação da estratégia de teste do tipo seqüencial para o escalonado. Por sua vez, para compensar a extensão de IT, também é implementada, quando pertinente, a estratégia de teste escalonado.

O Capítulo 2 apresenta a caracterização do problema proposto nessa tese detalhando o significado de TPI e de IT e como são tratadas as extensões propostas dos mesmos.

O Capítulo 3 contém a revisão bibliográfica que apresenta um sumário dos trabalhos desenvolvidos internacionalmente ao longo dos últimos 15 anos, na área específica de busca de melhorias e otimização de especificações técnicas, que servem de base para demonstrar a originalidade do presente trabalho.

O Capítulo 4 apresenta as considerações regulatórias ao longo do desenvolvimento de todas as etapas desta tese, culminando na apresentação dos critérios de risco que são utilizados na avaliação quantitativa das extensões de TPI e de IT.

No Capítulo 5 é apresentada e desenvolvida toda a metodologia necessária para a execução deste trabalho. Nele são definidas as medidas de risco utilizadas, os impactos de risco associados ao TPI e ao IT, o tratamento das falhas de causa comum e das medidas compensatórias. O capítulo 5 ainda contém uma descrição das

características necessárias de uma APS para que sejam possíveis os cálculos relativos às extensões de TPI e de IT e, finaliza com as considerações relevantes ao processo de avaliação do risco associado às modificações de especificações técnicas.

O Capítulo 6 desenvolve a modelagem para as simulações a serem executadas, através do código SAPHIRE [8], especificando as particularidades do tratamento de falhas de causa comum de cada tipo de simulação como, manutenção corretiva, extensão de IT, teste do trem redundante e modificação de estratégia de teste. O capítulo 6 é absolutamente necessário como embasamento dos cálculos que são apresentados no capítulo 7.

O Capítulo 7 apresenta os resultados, por meio de tabelas, especificando cada tipo de simulação, dos cálculos efetuados através do SAPHIRE para os três sistemas de segurança de Angra 1, SIS, SAS e SAAA, cujos TPI e IT foram estendidos. Os cálculos para a inclusão das medidas compensatórias, sempre que pertinentes, também são apresentados através de tabelas contendo as modificações dos dados de entrada do SAPHIRE. A comparação dos resultados obtidos com os critérios de aceitação apresentados no Capítulo 4 é comentada ao final de cada simulação. Em seguida, são apontados os TPI e IT dos sistemas supracitados que, segundo essas avaliações de risco, são candidatos à modificação, ou seja, cujos TPI e IT possam ser estendidos sem incorrer em aumento de risco.

Na Seção 7.5 são apresentados os cálculos de combinações de extensões de TPI e de IT simultâneas. Estes cálculos representam os primeiros passos para um estudo de controle de configuração da planta ou dar subsídios para o gerenciamento de risco da planta [2].

A Seção 7.5.1 apresenta as extensões simultâneas de TPI para o SIS e o SAS e a Seção 7.5.2, as extensões simultâneas de IT para os mesmos sistemas. Na Seção 7.5.3 são mostrados os cálculos para as extensões combinadas de TPI e de IT para o SIS.

No Capítulo 8 são apresentadas as conclusões gerais sobre o presente trabalho, visando indicar suas vantagens e limitações, bem como são elaboradas recomendações que indicam o escopo de futuros trabalhos nessa área específica, a fim de possibilitar a continuidade do mesmo.

2. CARACTERIZAÇÃO DO PROBLEMA

2.1 Definição de Especificações Técnicas

As Especificações Técnicas (ET) de Centrais Nucleares de Potência [9] definem limites e condições que garantem que a planta seja operada de maneira consistente com as análises determinísticas e avaliações contidas no Relatório Final de Análise de Segurança (RFAS) [1] da central. As Especificações Técnicas são exigidas como parte do RFAS [1] para a licença de operação da instalação e incorporadas na autorização para a operação.

As especificações técnicas podem ser entendidas como um conjunto de regras de segurança e critérios que definem os limites de operação permitidos à central nuclear, do ponto de vista da segurança [10]. Tais regras, originalmente, são formuladas de forma conservativa em relação à segurança, baseadas, principalmente, em análise determinística e em julgamentos efetuados com base em engenharia.

Exigências de Especificações Técnicas para uma central nuclear constam de [11]: (1) Condições Limites de Operação (CLO) que incluem os Tempos Permitidos de Indisponibilidade (TPI) para equipamentos, (2) Exigências de testes de equipamentos, (3) Limites de segurança, (4) *set points* para sistemas de segurança, (5) Características de projeto, e (6) Controles administrativos.

As exigências de interesse para este estudo são as Condições Limites de Operação (CLO) que incluem os Tempos Permitidos de Indisponibilidade (TPI) para equipamentos e as exigências de testes de equipamentos, que incluem os Intervalos de teste (IT).

As CLO têm o objetivo de garantir que os sistemas de segurança estejam prontos para uso sob demanda. Em caso de falha de sistemas, as ET contêm ações que exigem que a planta seja conduzida a um estado de operação segura, caso o equipamento falho não possa ser restaurado dentro do Tempo Permitido de Indisponibilidade (TPI).

As exigências de vigilância prescrevem testes periódicos para a detecção de falhas e verificação da operabilidade dos equipamentos de segurança, tais como, por

exemplo, bombas. O intervalo de tempo entre dois testes consecutivos é denominado Intervalo de Teste (IT).

As ET estão relacionadas diretamente com a segurança e, portanto, também, com a confiabilidade dos componentes, sistemas e estruturas da planta. Um estudo de APS apresenta uma análise sistemática das possíveis falhas de componentes, sistemas, funções de segurança, bem como as combinações dessas falhas que conduzem a configurações indesejadas da planta ou dano ao núcleo.

Portanto, a APS pode ser considerada uma ferramenta importante para ser usada na avaliação de risco da central. Várias aplicações da APS já são utilizadas para fins regulatórios no processo de decisão baseado em risco, dentre elas a avaliação das ET [12].

2.2 Papel da Análise Probabilística de Segurança (APS)

Ao longo dos anos, a experiência operacional indicou que algumas das exigências das ET poderiam não ser as mais afinadas com a segurança quanto às suas restrições, não apresentando um "balanço da planta" correto, nem em relação à segurança nem, tão pouco, em relação ao melhor desempenho da planta. A partir desta constatação, tornou-se desejável a reavaliação das ET agregando-se cálculos do risco associado, com vistas à implementação de modificações nas mesmas.

A Análise Probabilística de Segurança (APS) de uma central nuclear utiliza uma abordagem estruturada e sistemática para identificar cenários de falhas, consistindo em uma ferramenta tanto conceitual quanto matemática para a análise quantitativa de risco associado à operação de centrais nucleares. Desta forma, a APS pode ser usada para o cálculo das contribuições do risco associadas às propostas de modificações de ET, ou seja, o impacto do risco dessas mudanças. Tal avaliação é denominada "Análise de Especificações Técnicas Baseada em Risco" ou "Análise de Especificações Técnicas Baseada em APS", uma vez que métodos e modelos de APS são utilizados como ferramenta de análise. A avaliação do impacto no risco causado pela mudança pode ser útil para analisar, revisar ou aceitar a mudança proposta. Para isto é necessário que a APS seja específica da planta, ou seja, a modelagem e o banco de dados utilizados para a elaboração da APS devem ser os mais específicos possíveis.

Tipicamente, as propostas de melhorias nas ET envolvem o relaxamento de um ou mais Tempos Permitidos de Indisponibilidade (TPI) ou de Intervalos de Teste (IT). Para isso são necessárias avaliações baseadas em risco desenvolvidas através do uso de métodos e modelos probabilísticos, bem como de resultados e conclusões obtidos de uma APS desenvolvida especificamente para a planta.

O estudo da APS pode ser dividido em três etapas [12]:

1) APS Nível 1, avaliação das falhas com foco na determinação da Freqüência de Dano ao Núcleo (FDN);

2) APS Nível 2, avaliação da resposta da contenção visando, conjuntamente com a APS nível 1, a determinação da - Freqüência de Grande Liberação Antecipada (FGLA);

3) APS Nível 3, avaliação das conseqüências fora do sítio da central, conjuntamente com os resultados da APS nível 2, com a finalidade de estimar o risco à população.

Uma APS Nível 1 identifica seqüências de eventos que podem conduzir ao dano ao núcleo. Desta forma, apresenta resultados que fornecem informações sobre pontos fracos do projeto e modos de prevenção de ocorrência de dano ao núcleo. Em muitos casos, o dano ao núcleo é o precursor de acidentes que induzem liberações de material radioativo com potencial de conseqüências para o público e o meio ambiente.

Uma APS Nível 2 fornece informações adicionais sobre as possíveis formas de liberação de material radioativo da contenção, bem como suas magnitudes e freqüências de ocorrência. Uma APS Nível 2 fornece, também, a importância relativa das seqüências de acidentes que conduzem ao dano ao núcleo, em termos da severidade das liberações radioativas que podem ocorrer após o derretimento do núcleo. Desta forma, resultados de uma APS Nível 2 apontam modos de melhoria no gerenciamento de acidentes, incluindo a mitigação de seus efeitos.

Finalmente, uma APS Nível 3 fornece informações importantes para a adoção de medidas de prevenção e mitigação de acidentes expressas em termos das conseqüências adversas tanto para a saúde dos operadores como da população e a contaminação do meio ambiente. Além disso, a APS Nível 3 fornece subsídios para a efetividade do gerenciamento de acidentes com relação à elaboração do plano de emergência.

Neste trabalho, a APS de Nível 1 será adotada como ferramenta básica para a avaliação de Especificações Técnicas de sistemas de segurança de centrais nucleares. Isso pode ser justificado pelo fato da APS Nível 1 ter como objetivo o cálculo da FDN através de uma metodologia sistemática de avaliação dos atributos de confiabilidade dos sistemas de segurança da central e da determinação das seqüências de acidentes. Portanto, as seqüências de acidentes são diretamente sensíveis às variações de taxas de falhas dos componentes/sistemas de segurança. O escopo da APS Nível 1 se limita à avaliação dos danos materiais que podem ocorrer dentro do núcleo.

Uma APS Nível 2 utiliza como dados de entrada os resultados da APS Nível 1 com o objetivo principal de calcular os níveis de liberação de material radioativo. No caso de se dispor apenas de uma APS de Nível 1, a FDN é usada como única medida de risco [7].

De forma similar, a APS Nível 3 utiliza os resultados da APS Nível 2 como dados de entrada para o cálculo do risco à população.

Como justificado acima, as ET estão relacionadas diretamente com a segurança e, portanto, também, com a confiabilidade dos sistemas e da planta. Nesse sentido, modelos de APS Nível 1 são ferramentas adequadas para serem usadas na avaliação de TPI e de IT em termos dos seus efeitos no nível de risco da planta. A tarefa de avaliação de ET com métodos probabilísticos gira em torno de dois parâmetros: (1) O risco incondicional da planta (*baseline risk*), e (2) os incrementos temporários de risco [13].

O risco incondicional ou de base da planta pode ser definido como o risco total para operação tal como calculado na APS. No caso de uma APS Nível 1, o risco de base total da planta se traduz pelo parâmetro definido como Freqüência de Dano ao Núcleo (FDN). Risco incondicional é, então, por definição, o nível de risco associado à operação da planta presumindo-se que não ocorreram falhas e que nenhum sistema tenha sido isolado para teste e/ou manutenção.

Por outro lado, o risco condicional está associado às indisponibilidades de componentes de sistemas de segurança, causadas por falhas, testes ou manutenções, programadas ou não. O risco condicional, neste caso representa um acréscimo de risco ao risco incondicional (risco de base). Além disso, também pode ser chamado de risco condicional o risco calculado quando alguns componentes estão garantidamente

operáveis, ou seja, suas probabilidades de falhas, para fins de cálculo, são consideradas nulas.

Resumindo, risco condicional está associado a modificações nas probabilidades de falhas dos componentes para quaisquer valores diferentes das taxas de falhas consideradas na APS de base, em geral, modificados para o valor um (1) quando o componente é declarado inoperante ou para zero (0) quando o componente acabou de ser testado.

2.3 Tempos Permitidos de Indisponibilidade (TPI)

Tempos Permitidos de Indisponibilidade (TPI) são definidos como parte das Condições Limites de Operação (CLO) nas ET das centrais nucleares. Os TPI são limites impostos para períodos de indisponibilidade de sistemas ou componentes, seja devido à Manutenção Preventiva (MP) ou à Manutenção Corretiva (MC). O limite imposto para o tempo de indisponibilidade é uma medida de segurança necessária, uma vez que várias dessas manutenções são executadas durante o modo de operação do reator, causando um aumento no risco total associado à operação da planta por perda temporária de redundâncias (trens ou componentes) [14].

A intenção do TPI é fornecer tempo adequado para o reparo de um componente falho sem incorrer em risco indevido associado à perda temporária da função ou componente. Um TPI longo implica em um maior aumento do risco associado, mas um TPI curto pode resultar em um reparo inadequado ou desligamento desnecessário do reator, ambos com implicações no risco total da planta. A experiência operacional em centrais nucleares aponta que mudanças nos TPI são, muitas vezes, necessárias.

Um aumento dos TPI pode ser desejável para fornecer o tempo adequado para reparo ou manutenção, evitando desligamento desnecessário, ou para obter flexibilidade operacional, embora uma maior atenção deva ser focada nos aspectos relacionados com a significância em relação ao risco. Em certos casos, um encurtamento do TPI pode ser exigido devido à grande contribuição para o risco. A APS fornece uma ferramenta de análise sistemática para a avaliação das contribuições de risco associadas aos TPI, bem como para a avaliação do impacto da mudança proposta.

2.4 Intervalos de Teste (IT)

O intervalo de teste é definido como o tempo transcorrido entre dois testes consecutivos em um componente de um sistema.

As ET requerem, entre outros itens, testes de sistemas e componentes de segurança para assegurar a disponibilidade e, portanto, o funcionamento adequado na demanda dos mesmos. Os testes estabelecidos nas ET devem ser executados periodicamente (por exemplo, mensalmente ou a cada três meses). Os períodos de teste estabelecidos pelas ET são denominados Intervalos de Teste [15]. Um pedido de relaxamento de IT constitui, então, um aumento do intervalo de teste ou mesmo uma exceção ao mesmo.

O principal objetivo dos testes é assegurar a operabilidade dos componentes do tipo "em reserva", que operam sob demanda e que são necessários em condições de acidentes. Através dos testes destes sistemas e/ou componentes, falhas que ocorreram no período a partir do último teste ou a partir da última operação destes sistemas e/ou componentes podem ser detectadas, de forma que os mesmos operem adequadamente sob demanda.

O número de testes requeridos pelas ET é grande, exigindo da operadora da planta e do órgão regulatório um esforço substancial no sentido de planejar, conduzir e verificar os testes. Alguns testes podem até causar impacto na segurança quando provocam efeitos adversos, tais como, transientes causados por erros humanos ou desgaste do equipamento devido ao teste.

Em geral, esses efeitos indesejados podem ser reduzidos quando os intervalos de testes são aumentados, uma vez que o número de testes diminui nesses casos. Uma extensão do intervalo de teste, também, é obtida na forma de poupança de recursos a serem despendidos em testes. Entretanto, uma desvantagem importante é o aumento do período no qual o sistema ou componente fica sujeito a falhas, ou seja, o aumento do período de reserva.

Cabe ressaltar que, nas centrais nucleares, são empregados dois tipos de estratégias de testes: (1) seqüencial ou (2) escalonada. Detalhes sobre características dessas estratégias de teste são apresentados na Seção 5.5.2.

2.5 Extensão de TPI e de IT das Especificações Técnicas

O objetivo deste trabalho é aplicar métodos baseados em risco que possibilitem estender os Tempos Permitidos de Indisponibilidade e Intervalos de Testes para bombas de sistemas de segurança da central, utilizando, como exemplos, o Sistema de Injeção de Segurança (SIS), o Sistema de Água de Serviço (SAS) e o Sistema de Água de Alimentação Auxiliar (SAAA**).** Esses três sistemas foram escolhidos porque possuem características distintas, que também podem ser atribuídas a outros sistemas similares e, portanto, representam uma amostragem dos tipos de sistemas de segurança da central no que diz respeito às redundâncias, diversificação, e estratégias de testes vigentes aos quais os mesmos são submetidos. Apesar do escopo deste trabalho ser limitado à análise da proposta de modificação das ET desses três sistemas de segurança, a metodologia apresentada poderá ser aplicada a quaisquer outros sistemas. Além disso, a escolha de dois ou mais sistemas a serem avaliados, em vez de um só, é para permitir tanto uma avaliação individual de cada um deles, como uma avaliação da contribuição simultânea de pelo menos dois ou três sistemas, quanto ao impacto das modificações de ET propostas no risco associado à planta.

O ponto importante deste trabalho é a apresentação da abordagem metodológica, através de cálculos que utilizam a APS como ferramenta de análise de risco, que possibilitam uma futura avaliação global das ET. Em outras palavras, a abordagem metodológica proposta, aplicada aos três sistemas, poderá ser estendida futuramente a uma aplicação a todos os sistemas de segurança da central contemplados nas ET vigentes para que possam ser avaliados conjuntamente.

Métodos e técnicas baseadas em risco são aplicados para estender os TPI e melhorar a eficiência das estratégias de testes, ao mesmo tempo mantendo ou mesmo aumentando os níveis de segurança requeridos para a operação da central.

Intervalos de Tempos Permitidos de Indisponibilidade típicos para a central de Angra 1, por exemplo, são de 48 horas, o que se aplica para ao SAS e ao SAAA. Intervalos de Teste típicos são de um mês [16]. A proposta deste trabalho é considerar, para fins de cálculo para extensão do TPI e do IT do SIS, do SAS e do SAAA, os valores apresentados na Tabela 2.1.

Tabela 2.1 - Extensões propostas para TPI e IT

Sistema	Tempo Permitido de Indisponibilidade (TPI)	Intervalo de Teste (IT)
Sistema de Injeção de Segurança (SIS)	24 horas → 168 horas	1 mês → 3 meses
Sistema de Água de Serviço (SAS)	48 horas → 168 horas	1 mês → 3 meses
Sistema de Água de Alimentação Auxiliar (SAAA)	48 horas → 168 horas	1 mês → 3 meses

Para a realização desta proposta, os seguintes passos devem ser seguidos:

a) Consideração das ET atuais para o SIS, o SAS e o SAAA:

Consta de uma avaliação dos parâmetros das ET correntes dos sistemas a serem analisados no trabalho quanto aos respectivos TIP, IT e política de testes (seqüencial ou escalonado).

b) Consideração da proposta de modificação da ET:

Consta das análises das modificações propostas das ET para o SIS, o SAS e o SAAA, quanto à extensão dos TIP e IT, conforme a Tabela 2.1, utilizando a APS como ferramenta de cálculo.

c) Modelagem de parâmetros tais como indisponibilidade devido à falha na partida, falha na operação, falhas de causa comum, testes de vigilância, manutenção preventiva e corretiva e tempos permitidos de indisponibilidades:

Consta da verificação e revisão da modelagem desses parâmetros na APS para que a metodologia proposta para a modificação das ET seja refletida nos cálculos.

d) Cálculo da proposta de modificação da ET:

Consta dos cálculos realizados através da APS, com a modelagem da modificação proposta para as ET do SIS, do SAS e do SAAA.

e) Consideração do Critério de Aceitação para a Freqüência de Dano ao Núcleo (FDN) tendo como ferramenta a APS Nível 1:

Consta da avaliação dos resultados obtidos na APS para a modificação proposta da ET. Caso seja constatado um incremento no risco, a variação correspondente obtida na FDN deve ser analisada e confrontada com o critério de aceitação para variações de FDN, ou seja, critério de aceitação para resultados de APS Nível 1.

f) Considerações de engenharia:

Os sistemas analisados devem ser submetidos a considerações de engenharia. Em particular, a avaliação de engenharia deve levar em conta o projeto e a função dos sistemas quanto à operabilidade e segurança da planta. Além disso, é primordial que os aspectos de segurança de defesa em profundidade sejam considerados.

g) Discussão e interpretação dos resultados:

O resultado do cálculo do risco correspondente à modificação proposta pode não corresponder a um valor aceitável para a FDN. Neste caso, medidas compensatórias podem ser propostas.

h) Introdução de Medidas Compensatórias:

Este item diz respeito à introdução de medidas compensatórias tais como (1) modificação das estratégias de teste seqüencial para teste escalonado (2) teste do trem redundante antes de executar a MC ou MP. Como discutido nas seções anteriores, as medidas compensatórias têm a função de reduzir ou "compensar" um aumento inaceitável da FDN relativo à modificação de ET proposta.

i) Recomendação para implementação da extensão do TIP e do IT:

Com base nos resultados obtidos, recomendação para a modificação das ET com relação ao relaxamento de TPI e IT do SIS, do SAS e do SAAA.

j) Recomendações para revisões de ET:

Com base nos resultados obtidos para a proposta de modificação das ET do SIS, do SAS e do SAAA, elaboração de recomendação para uma avaliação completa das ET abrangente a todos os sistemas de segurança contemplados nas ET vigentes.

3. REVISÃO BIBLIOGRÁFICA

A partir da pesquisa bibliográfica realizada através do CIN (Centro de Informação Nuclear), da busca de artigos publicados em periódicos como "Reliability Engineering and System Safety", "Risk Analysis", "Nuclear Energy", "Progress in Nuclear Energy" e nas bibliotecas da NRC e da AIEA, foram selecionados trabalhos, publicados nos últimos vinte anos, bastante específicos quanto ao uso da APS para avaliações e otimizações de Especificações Técnicas.

A referência [13] apresenta resultados de estudo de interações entre TPI e IT. A quantificação das interações é desenvolvida em termos de risco, através do uso de métodos de APS como ferramenta. Para tal, é utilizada uma abordagem para modificações de TPI e IT e seus efeitos no risco, incluindo as condições de interações entre os dois parâmetros. O trabalho é dividido em vários passos e tem a intenção de apresentar abordagens que possam abranger desde medidas de risco em nível de componente até nível de FDN. Entretanto, o conteúdo do artigo se concentra somente no estudo em nível de componentes. Segundo o artigo, para que possam ser viabilizadas as inclusões de estratégias de testes e de falhas de causas comuns, seria necessária uma abordagem em nível de sistemas ou acima (FDN). Para tal, é citado um algoritmo que o autor desenvolveu para tratar das interações de pares de TPI com IT.

A abordagem metodológica apresentada na referência [17] inclui o cálculo do impacto no risco da modificação da ET proposta, através do uso de APS. Os cálculos foram desenvolvidos para as centrais Seabrook e South Texas. As medidas de risco utilizadas são indisponibilidades de sistemas e a FDN. O critério de aceitação adotado aprova mudanças cujas alterações no risco não ultrapassem 10%. A diferença entre esta abordagem e a proposta no presente trabalho se encontra, principalmente, na adoção de medidas compensatórias que possam neutralizar o aumento no impacto do risco devido à modificação proposta.

A referência [18] trata da comparação dos incrementos de risco entre um aumento do TPI, ou seja, extensão do tempo de reparo, versus o risco associado ao desligamento da planta. Exemplos são mostrados para os Sistemas de Remoção de Calor Residual e de Água de Serviço, para um reator do tipo BWR. O estudo sugere a utilização de medida compensatória de teste do trem redundante para a decisão

operacional entre operação continuada, com extensão de TPI, e o desligamento da planta.

A referência [15] propõe a otimização de IT baseada em métodos de APS. A abordagem é dividida em três níveis: componente, sistema e planta. O trabalho se concentra na aplicação em nível de sistema que, segundo os autores, induz às mais significativas alterações de ET. São utilizadas estratégias de testes escalonados e seqüenciais. Diferentes estratégias de testes são introduzidas através do desenvolvimento de árvores de falhas que incluem várias variáveis de tempos relativos não só ao intervalo de teste como, também, ao tempo de reparo e duração do teste, além de outras variáveis. Cabe lembrar que essa metodologia só pode ser aplicada em nível de sistemas, o que limita aplicações diretas da maioria das APS, onde a medida de risco mais abrangente é a FDN. O trabalho citado usa métodos de APS, especificamente, processos de Markov [19] para modelar dependências em nível de componentes e de sistemas.

A referência [20] apresenta uma seção dedicada às Especificações Técnicas no que diz respeito às Condições Limite de Operação, exigências de testes e o uso da APS para apresentar os conceitos para a avaliação do que seria o "ótimo", em termos de TPI e IT, em relação a risco. O trabalho cita o uso da APS quanto ao tratamento das falhas de causa comum e enfatiza a importância da distinção entre os TPI associados a eventos simples e TPI acumulado (por exemplo: anual). O artigo também aborda o risco associado às variações de IT e o risco limite de teste. O trabalho apresenta tabelas de cálculo com propostas de extensão de TPI confrontadas com os critérios de aceitação de risco. Não está incluída no trabalho a adoção de medidas compensatórias para compensar possíveis aumentos de risco.

A referência [21] apresenta uma proposta de otimização simultânea de parâmetros relacionados a teste e manutenção baseados em risco (ou indisponibilidade) e funções de custo, modelados através de algoritmo genético em nível de sistemas. O trabalho apresenta um exemplo de aplicação da metodologia para o Sistema de Injeção de Alta Pressão. Os resultados apresentam valores de custos e indisponibilidades de bombas e válvulas, estabelecendo correspondência com intervalos de testes e períodos de manutenção preventiva para as mesmas bombas e válvulas.

A referência [22] utiliza o método para a avaliação do risco associado ao TPI de diversas configurações da planta, através das medidas de risco apresentadas na Seção 5.1 do presente trabalho. Os riscos associados às várias configurações da planta consideradas no trabalho são comparados com um critério de risco adotado, assim como os resultados obtidos para as diversas configurações propostas são confrontados entre si. Entretanto, não é utilizada a metodologia de introdução de medidas compensatórias para configurações que incluam extensões de TPI, quando os riscos associados ultrapassam os riscos aceitáveis, segundo o critério.

A referência [23] apresenta a proposta de gerenciamento de risco de manutenção através do desenvolvimento de um estudo piloto que avalia o risco da planta durante as atividades de manutenção usando métodos de APS. O artigo aborda a modelagem de falhas de causa comum, sem, contudo, apresentar uma aplicação para extensões de TPI e de IT. O escopo do artigo está dentro de um contexto de discussões relativas a monitor de risco, modelo específico de APS, medidas de risco e critério de aceitação e o papel dos órgãos regulatórios.

3.1 Originalidade

Com base na pesquisa bibliográfica apresentada acima se pôde verificar a originalidade da proposta do presente trabalho. Vários esforços foram executados, em âmbito internacional, no sentido de se calcular, através de uma APS, os impactos de risco causados por testes e manutenções (IT e TPI). Foram encontrados na literatura trabalhos que realizaram avaliações em nível de componente, de sistema e, ainda, uns poucos que elegeram a FDN como medida de risco. Alguns dos trabalhos deram ênfase à avaliação das interações entre as contribuições de testes e de manutenções. Outros estudos apresentaram foco na comparação do risco de desligamento da planta com o risco associado à continuação da operação depois de expirados os limites para IT e TPI. Tais trabalhos apresentaram em suas conclusões como sugestão o uso de medidas compensatórias de risco, como por exemplo, o teste do trem redundante antes do início de atividades de manutenção. Além disso, foram ainda encontrados na literatura trabalhos que utilizam algoritmos genéticos para a otimização das ET, onde são considerados parâmetros relacionados a custos.

A originalidade do presente trabalho pode, então, ser justificada pela proposta de modelagem na APS do uso de medidas compensatórias para os casos onde ocorrem aumentos de risco causados pela extensão de IT e de TPI.

Para compensar o aumento do risco associado às extensões de IT e de TPI é proposta neste trabalho a introdução de medidas compensatórias que possam manter ou mesmo reduzir os valores do risco associados às configurações dos sistemas anteriores às modificações propostas. As medidas compensatórias a serem modeladas neste trabalho se referem ao teste do trem redundante imediatamente antes do início do período de TPI e às modificações de estratégias de testes, ou seja, a modelagem e avaliação de testes do tipo escalonado para compensar tanto a extensão do TPI quanto do IT.

Para isso foi desenvolvida neste trabalho uma metodologia específica para se adequar à simulação de falhas (ou MC) de trens de sistemas de segurança, cujas redundâncias são afetadas quanto ao cálculo de falhas de causa comum. Essa metodologia inclui a simulação do teste do trem redundante, também, no que diz respeito ao tratamento de falhas de causa comum, que devem ser modificadas para retratar a condição trem recém testado. Além disso, também é modelada a simulação da extensão do intervalo de teste. Os cálculos foram efetuados através do código de computação SAPHIRE [8], tendo como entrada os dados da APS de Angra 1. O código SAPHIRE, utilizado pela NRC, foi adotado pela ELETRONUCLEAR como ferramenta de cálculo para a APS de Angra 1, bem como pela CNEN, resultando em uma ferramenta adequada para aplicações de APS, o que justifica sua escolha para a utilização neste trabalho.

4. CONSIDERAÇÕES REGULATÓRIAS

Neste trabalho são usados como referências regulatórias os Guias Regulatórios da NRC que abordam as questões do processo de decisão quanto às propostas de modificações de ET [7], [24] e [25].

Segundo a referência [24], a implementação do processo de decisão baseado em risco, no tocante às modificações de ET, deve respeitar um conjunto de regras ou princípios de segurança previamente estabelecidos. Esses princípios estabelecem que a proposta de modificação não deve ferir as regras vigentes, bem como ser consistente com a filosofia de defesa em profundidade [26]. Além disso, as modificações propostas devem manter margens de segurança aceitáveis. No caso de modificações que resultem em um incremento no risco, este deve ser pequeno e consistente com a "Avaliação de Impacto de Risco" [24]. Finalmente, o impacto no risco decorrente da modificação deve ser monitorado através do uso de estratégias de medidas de desempenho.

Para obter consistência com os princípios de segurança no processo de decisão baseado em risco, é proposta uma abordagem de quatro elementos [7, 24, 25] para a avaliação de modificações de ET, conforme descrito a seguir.

4.1 Elemento 1: Definição da Modificação Proposta

A proposta de modificação deve indicar explicitamente a ET afetada, bem como estudos de engenharia disponíveis, métodos, códigos e APS relativos à mesma. A proposta deve, também, determinar como os sistemas, componentes ou parâmetros afetados estão modelados na APS e identificar todos os elementos da APS impactados pela modificação.

4.2 Elemento 2: Análise de Engenharia

Nesta etapa deve ser verificado se a proposta de modificação de ET cumpre as regras vigentes. Além disso, deve ser demonstrado como a mudança afeta os aspectos de defesa em profundidade do projeto e operação da planta, bem como determinar a adequação das margens de segurança relativas à modificação proposta. Em seguida deve-se, também, realizar uma avaliação, baseada em risco da modificação proposta

para determinar o impacto associado. A avaliação deve considerar explicitamente os equipamentos específicos da planta afetados pela modificação, com respeito à funcionalidade, confiabilidade e disponibilidade dos mesmos. Portanto, deve-se fornecer suporte racional para a aceitação das mudanças propostas através da integração de conhecimentos probabilísticos com os tradicionais determinísticos para se chegar a uma determinação final do risco.

Cabe ressaltar que, os aspectos dos sistemas de segurança envolvidos neste trabalho, tais como funções, descrição do funcionamento, condições limite de operação e exigências de testes, relevantes para a análise de engenharia, estão descritos no Apêndice A.

4.3 Elemento 3: Definição da Implementação do Programa de Monitoração

Nesta etapa devem ser considerados a implementação e o desempenho de estratégias formuladas para que: (1) nenhuma degradação ocorra como conseqüência da modificação de ET e (2) a avaliação de engenharia para o impacto da ET proposta continue a refletir as confiabilidades e disponibilidades reais dos equipamentos envolvidos.

4.4 Elemento 4: Documentação das Avaliações e Submissão da Proposta

Este elemento final envolve a documentação de todas as análises relativas à mudança proposta e o requerimento a ser submetido ao Órgão Regulatório para aprovação.

4.5 Critérios de Aceitação

Uma APS fornece uma abordagem estruturada e sistemática de forma a identificar os possíveis cenários de falhas. Portanto, a APS se constitui em uma ferramenta conceitual e matemática, que além de permitir uma avaliação qualitativa, tem a característica de apresentar resultados quantitativos para a avaliação do risco. Normalmente, como já discutido anteriormente, as APS para centrais nucleares podem

ser desenvolvidas para os níveis 1, 2 e 3. Para cada nível deve haver um critério correspondente para que os resultados quantitativos da APS possam ser avaliados, ou seja, confrontados com tais critérios [27]. Entretanto, segundo a NRC [7, 25], existem dois grupos de critérios de aceitação: (1) FDN – Freqüência de Dano ao Núcleo e (2) FGLA - Freqüência de Grande Liberação Antecipada. O critério da FDN corresponde a uma APS de nível 1, enquanto o FGLA está associado a uma APS nível 2. Portanto, para fins de aceitação da APS, os respectivos resultados de uma APS nível 1 e nível 2 devem ser confrontados com a FDN e a FGLA, respectivamente. Cabe ressaltar que a APS nível 3 avalia riscos relativos à saúde do público ou outros riscos à sociedade, o que torna extremamente complexa a elaboração de critérios quantitativos para tais fins.

Considerando-se que neste trabalho a ferramenta de avaliação de modificações de ET baseada em risco é a APS de nível 1, que apresenta como resultado de cálculo a FDN, este será o parâmetro relacionado com os critérios de aceitação apresentados adiante.

O dano ao núcleo representa um evento indesejado de grande importância não somente por poder ser o precursor de grandes liberações para fora da contenção com potencial de conseqüência para a saúde e o meio ambiente, mas, também, por causar grandes prejuízos econômicos.

Neste trabalho, são adotados os critérios de aceitação de risco da NRC [7, 24, 25] para a avaliação e processo de decisão de modificações de Especificações Técnicas. Segundo a Norma da CNEN [28], que rege a segurança de Centrais Nucleares no Brasil, na ausência de guias, critérios e normas, esses podem ser adotados de instituições internacionalmente reconhecidas, tais como a NRC e AIEA. A escolha de critérios da NRC dá-se pelo fato de que, além de ser reconhecida internacionalmente pela alta qualidade dos projetos e documentos emitidos, a NRC regula mais de cem centrais nucleares americanas, muitas delas, com projeto Westinghouse e, portanto, semelhantes ao da primeira central brasileira, Angra 1.

Os critérios de aceitação de risco apresentados no guia regulatório da NRC [7, 25] são fundamentados em princípios e expectativas para a regulamentação baseada em risco. Portanto, tais critérios de aceitação, são funções de resultados de análise de risco em termos da FDN calculada através de uma APS.

A variação da FDN causada por uma modificação proposta deve ser calculada e confrontada com os valores limites que fazem parte dos critérios de aceitação da NRC.

A Figura 1 mostra as três regiões correspondentes a valores de FDN no eixo **x**, versus valores de variações de FDN no eixo **y**, que são usadas como critério de aceitação de variações no risco.

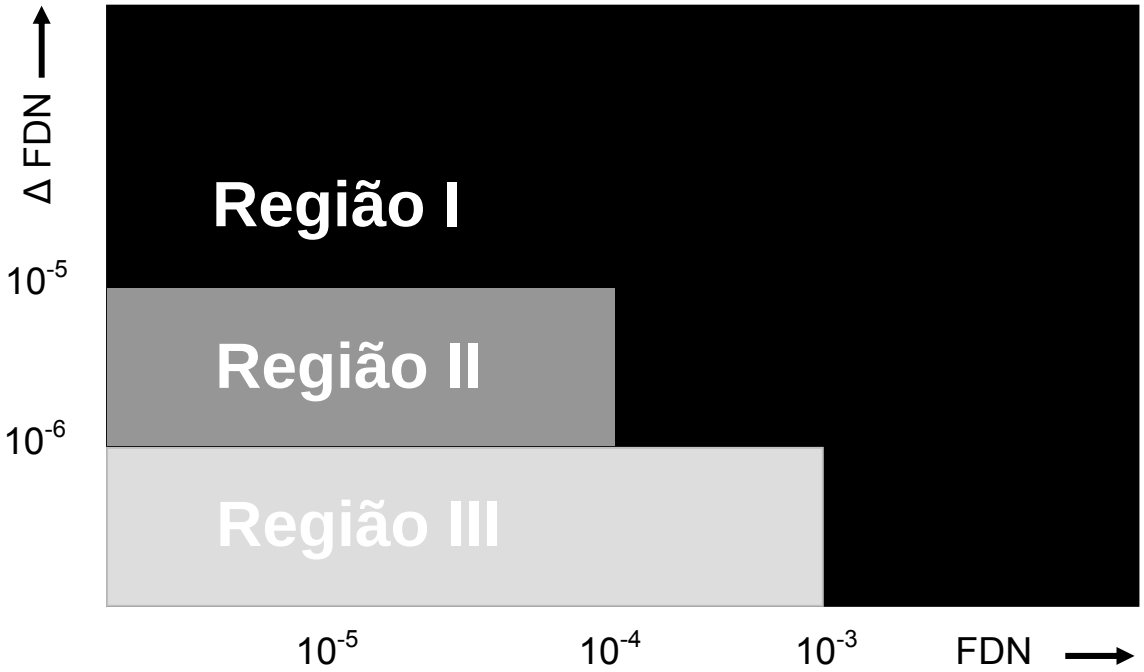

Figura 4.1 – Critério de Aceitação para a Freqüência de Dano ao Núcleo (FDN)

Segundo os documentos da NRC [7, 25], existem quatro tipos de situações onde a variação na FDN deve ser avaliada:

- Caso a aplicação possa mostrar claramente um decréscimo na FDN, a mudança é considerada satisfatória de acordo com o princípio de regulamentação baseada em risco;

- Quando o aumento na FDN é bastante pequeno, ou seja, menor que 1,0E-06 por reator-ano, a modificação é levada em consideração, independentemente do cálculo total da FDN (Região III);

- Quando o incremento na FDN se situa entre 1,0E-06 e 1,0E-05 por reator-ano, deve ser demonstrado que a FDN total é menor do que 1,0E-04 por reator-ano (Região II);

- Normalmente, não são aceitáveis as aplicações que resultam em incrementos na FDN maiores do que 1,0E-05 por reator-ano (Região I).

Os riscos associados às modificações de ET cujas medidas de risco são a FDN, devem ser calculados e comparados com os critérios apresentados na Figura 4.1. Entretanto, existem considerações adicionais de engenharia a serem observadas quando as variações no risco são resultados de modificações de Especificações Técnicas [7, 25].

Cabe ressaltar que as regras citadas nos dois documentos supracitados são aplicáveis às modificações de ET permanentes (opostas às modificações denominadas temporárias). Entretanto, considerando-se a baixa freqüência de ocorrência de entrada de componentes em TPI, sendo os mesmos de natureza temporária, devem ser observados critérios adicionais de aceitação.

O impacto no risco causado pela modificação de TPI deve ser expresso não somente pela variação da FDN, como também, pelo incremento condicional de probabilidade de dano ao núcleo, que é função da variação da FDN e da duração da indisponibilidade do componente. O incremento condicional de probabilidade de dano ao núcleo devido a um evento simples não deve ser maior do que 5,0E-07 [25]. A Seção 5.2 contém mais detalhes sobre o risco condicional de evento simples.

A contribuição anual média dos TPI, apresentada na Seção 5.2, é função, também, da freqüência de ocorrência das manutenções, podendo ser, maior do que um (1) no caso de MP e, geralmente, menor do que um (1) no caso de MC ou falha, quando se espera que esse número fique próximo ao valor da taxa de falha do componente λ. Outros detalhes sobre a avaliação de contribuição anual média de TPI são discutidos na Seção 5.2.

Cabe ressaltar que a NRC não estabeleceu, até o presente, nenhum critério específico para a avaliação da contribuição anual média de risco.

5. ABORDAGEM METODOLÓGICA

A avaliação de uma proposta de extensão de TPI ou de IT deve ser focada em dois ganhos: possibilidade de redução de atividades de manutenção e de testes operacionais desnecessários, com um impacto positivo na confiabilidade e segurança da planta e, no mínimo, a garantia da permanência dos mesmos níveis de segurança anteriores à modificação.

Com relação à extensão dos TPI, uma das justificativas está relacionada com a redução do estresse e de erros provenientes da equipe de manutenção, possibilitando maior flexibilidade para as atividades de manutenção, aumentando a qualidade do trabalho. Além disso, uma extensão de TPI deve também diminuir a freqüência de desligamento da planta, uma vez permitido um período mais longo para o cumprimento das tarefas de manutenção e reparo. Em muitos casos, o risco associado ao desligamento do reator pode ser significativamente maior do que o acréscimo de risco causado pela extensão do TPI. Como é desejável que se evitem desligamentos desnecessários, o que poderia aumentar o risco associado às falhas de sistemas e componentes que são demandados durante a fase de desligamento da planta, a avaliação da extensão de TPI nesses casos é muito importante.

As exigências de testes têm o propósito de garantir que os componentes em reserva estejam operáveis quando forem demandados em condições de incidentes/acidentes. As falhas que possam ter ocorrido no período entre um teste e outro ou desde quando o componente em reserva foi demandado a operar pela última vez podem ser detectadas através de testes dos componentes dos sistemas de segurança. Alguns testes podem até causar um efeito adverso na segurança, como, por exemplo, erros de testes que causam transientes na planta ou testes que provocam desgastes dos equipamentos testados. Em geral, os possíveis efeitos negativos dos testes são reduzidos quando o IT é estendido, dado que o número de testes diminui neste caso. Além disso, a extensão do intervalo de testes adiciona o benefício da redução dos recursos gastos com os testes, tanto para a indústria nuclear como para o órgão regulatório, em planejamento, execução e verificação.

Resumindo, a proposta desse trabalho visa à obtenção da extensão do IT e do TPI, com a garantia da manutenção dos níveis de segurança, tendo como base de

avaliação uma APS, mas, também, garantindo os critérios estabelecidos pelo RFAS [1] e pelo principio de defesa em profundidade.

5.1 Medidas de Risco

Quando se deseja avaliar os riscos associados às ET com base em análise de risco, deve ser tomada uma decisão em relação à escolha tanto das medidas de risco a serem utilizadas, quanto ao nível da análise a ser desenvolvida. As medidas de risco podem ser várias [2], tendo sido adotada neste trabalho, a FDN. A medida de risco selecionada deve ser consistente com a função dos componentes envolvidos nas ET a serem avaliadas. Quando são avaliados componentes cujas funções estão relacionadas com a prevenção de acidentes, as medidas de risco indicadas são aquelas associadas à freqüência de acidentes. Além disso, a FDN é uma boa escolha para medida de risco quando existem interações funcionais entre componentes e sistemas. Por exemplo, a interação entre os sistemas de segurança em geral e aqueles denominados de suporte, como o sistema elétrico.

Geralmente, durante o período de indisponibilidade de componentes, o nível de risco aumenta devido à perda da função dos mesmos. Sempre que um componente se torna indisponível, existe um risco, relativo a este período, que deve ser controlado. A contribuição do risco associada ao tempo de indisponibilidade depende da medida de risco adotada.

Embora as indisponibilidades de sistemas ou funções de segurança possam ser avaliadas, desde que os componentes estejam contidos nos sistemas e funções, a adoção da medida de risco em nível da planta (FDN) é uma boa estratégia, garantindo a inclusão de todas as interações entre os componentes ou mesmo entre sistemas.

O nível da análise desenvolvida está diretamente relacionado com a profundidade de detalhamento da modelagem. A análise pode ser desenvolvida para o nível de sistemas, subsistemas (ou trens) ou de componentes. Para as ET que se referem às exigências para componentes como, por exemplo, as bombas de sistemas de segurança, uma análise até o nível de componentes é necessária. Portanto, neste trabalho a modelagem adotada detalha e identifica os componentes do tipo bombas incluídas nas ET, bem como suas contribuições de risco correspondentes.

5.2 Impacto de Risco Associado aos TPI

A indisponibilidade do componente associada à perda de sua função pode ser devido à indisponibilidade por Manutenção Preventiva (MP) ou à Manutenção Corretiva (MC). A manutenção corretiva ocorre porque o componente falhou. Já a MP é, geralmente, programada e o componente se torna intencionalmente indisponível. Neste trabalho é abordada somente a MC ou falha, não sendo tratados os aspectos metodológicos relativos à MP.

Para o caso de falha do componente, ou seja, MC, o TPI é o período de tempo durante o qual o componente deve ser reparado e se tornar novamente operante. Existem três aspectos relativos à indisponibilidade do componente, controlados pelo TPI:

- Aumento de risco;

- Duração;

- Freqüência de ocorrência.

Baseados nesses três aspectos relativos à indisponibilidade de um componente existem dois tipos de impacto de risco associado ao TPI: (1) o relativo à indisponibilidade individual ou simples do componente durante um dado período de tempo, denominado impacto de risco de TPI de evento simples e (2) o impacto de risco de TPI associado à contribuição anual média dos TPI relativos ao dado componente.

O risco associado ao TPI de evento simples é a contribuição condicional de risco, dada a ocorrência da indisponibilidade do componente. A contribuição anual média de TPI tem caráter incondicional, uma vez que a mesma representa uma média de ocorrências de falhas durante o período de um ano.

A representação para a contribuição de evento simples para o risco está mostrada na Figura 5.1.

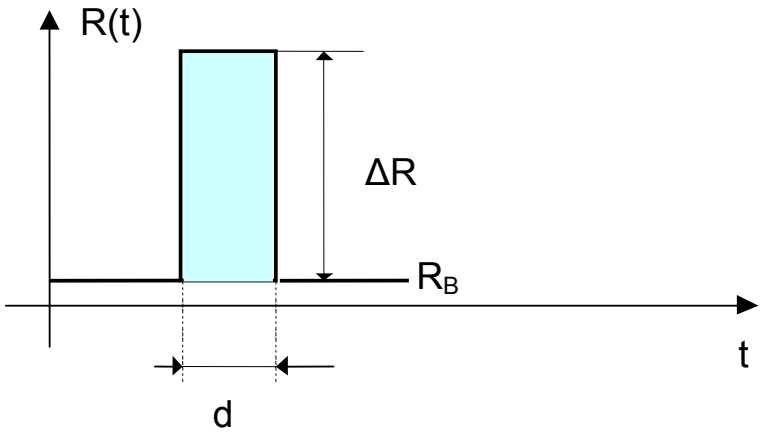

Figura 5.1: Contribuição de risco de evento simples

onde,

R(t) = risco condicional e

t = tempo.

O impacto de risco de TPI de evento simples pode ser expresso pela equação:

$$r = \Delta R \cdot d = (R_1 - R_B) \cdot d \qquad (5.1)$$

onde,

r = risco de evento simples associado ao TPI;

ΔR = incremento condicional de risco;

d = duração da indisponibilidade;

R_1 = aumento no nível de risco, quando o componente está indisponível;

R_B = risco incondicional *(baseline).*

A contribuição anual média para o risco é relativa às várias contribuições de TPI ocorridos ao longo do período de um ano, como mostra a Figura 5.2.

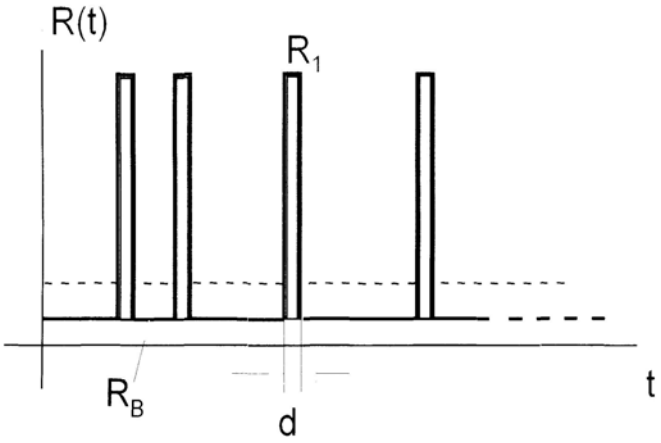

Figura 5.2 - Exemplo de contribuição anual média para o risco

Cabe ressaltar que, para fins deste estudo, d é considerado constante e assume valores do TPI, o que torna a contribuição anual média conservativa, uma vez que, na prática operacional, muitas manutenções são realizadas com duração inferior ao TPI.

A contribuição de risco anual médio dos TPI é o produto do risco do TPI de evento simples pela freqüência de ocorrência do TPI, e pode ser descrita pela expressão:

$$R = f \cdot \Delta R \cdot d \tag{5.2}$$

onde,

f = freqüência anual média de ocorrências do TPI ou freqüência de indisponibilidade.

Considerando-se que R(t) é risco condicional e, no caso desse trabalho, R(t) = FDN, então, o risco de TPI de evento simples pode ser expresso por:

$$r = \Delta FDN \cdot d = (FDN_1 - FDN_B) \cdot d \tag{5.3}$$

onde,

ΔFDN = incremento condicional da FDN durante o intervalo de tempo d

FDN_1 = freqüência de dano ao núcleo, calculada com o componente indisponível, ou seja, com o valor para a indisponibilidade do componente alterado para 1 (um);

e,

FDN_B = freqüência de dano ao núcleo como calculada originalmente na APS, considerando-se que não ocorreram falhas, e que nenhum sistema tenha sido isolado para teste e/ou manutenção.

A contribuição de risco anual média dos TPI é descrita, então, pela expressão:

$$R = f \cdot (FDN_1 - FDN_B) \cdot d \tag{5.4}$$

Como pode ser observado, o risco de evento simples e o risco anual têm características e unidades diferentes. Em termos de FDN, o risco de evento simples é a probabilidade de ocorrência de fusão do núcleo durante o período em que o componente se encontra indisponível. A contribuição anual média de risco é a freqüência de fusão do núcleo por ano devido a um valor médio de ocorrências de indisponibilidades durante o período de um ano.

No momento que ocorre uma indisponibilidade e o componente entra no TPI, o risco de evento simples deve ser controlado no sentido de controlar-se o risco associado a um episódio de indisponibilidade do componente. Por outro lado, a contribuição de risco anual também deve ser controlada pelo fato da mesma ter caráter cumulativo. Portanto, ambos os tipos de contribuições de risco devem ser avaliadas quando é feita a avaliação específica de um TPI bem como quando são propostas modificações de TPI.

De acordo com a Seção 4.5, são estabelecidos critérios para a variação da FDN e para o risco associado à contribuição de evento simples, que denominamos r_c .

A literatura referente à análise de risco [29] apresenta o tratamento dos cálculos relativos às contribuições de TPI de evento simples e média anual quando confrontadas com os respectivos critérios de aceitação:

$$\begin{cases} r \le r_c \quad d \le \dfrac{r_c}{\Delta R} \\ \\ R \le R_c \quad d \le \dfrac{R_c}{\Delta R \cdot f} \end{cases} \quad \text{Critério } d \le \min\left[\frac{r_c}{\Delta R};\ \frac{R_c}{\Delta R \cdot f}\right] \tag{5.5}$$

onde,

r_c = critério de risco de evento simples e

R_c = critério de risco médio anual.

Se a freqüência anual (f) for maior do que 1 (um), então o valor numérico da contribuição anual do TPI é maior do que a contribuição do evento simples. Caso contrário, o valor numérico da contribuição anual do TPI é menor do que a contribuição de evento simples.

Cabe ressaltar que o risco em função da freqüência de ocorrência de manutenções, R, torna-se mais relevante quando se trata de MP, para as quais é preparado um programa para a execução das manutenções, cujas freqüências são conhecidas e, geralmente, possuem valores iguais ou maiores do que um (1).

Ao contrário disso, quando se trata de MC ou falha, o valor esperado para o número de falhas de um componente, em um dado intervalo de tempo, deve ser próximo ao valor da taxa de falhas (λ) do componente [30].

De acordo com a Seção 4.5, o critério para evento simples, r_c , estabelecido pela NRC [7, 24, 25] possui valor de 5,0E-07. Entretanto, conforme comentado na Seção 4.5, não existe valor estabelecido para o critério de contribuição de risco anual médio, R_c.

5.3 Impacto de Risco Associado ao IT

A contribuição de risco associada ao intervalo entre testes, ou seja, a contribuição do IT é devida, principalmente, à possibilidade de que o componente falhe durante o período entre dois testes consecutivos. Após o teste, a probabilidade de falha do componente aumenta com o tempo e, portanto, a contribuição para o risco também aumenta em função do tempo decorrido a partir do último teste.

A probabilidade de que o componente esteja falho cai praticamente a zero logo após o teste, desde que o teste detecte e corrija efetivamente as possíveis falhas. Através de testes podemos limitar o risco associado com possíveis falhas não detectadas. Por esta razão, a contribuição do IT para o risco pode ser denominada de "risco limitado por teste".

Como neste estudo não são considerados os efeitos negativos dos testes, a contribuição de risco de interesse é, então, o risco do componente falhar entre testes.

A relação da indisponibilidade média Q de um componente em reserva, com a sua taxa de falhas em relação ao tempo é determinada pela fórmula [2]:

$$Q = \frac{\int_0^T (1 - e^{-\lambda t})dt}{T} \tag{5.6}$$

$$Q = 1 - \frac{1}{\lambda T}(1 - e^{-\lambda T}) \tag{5.7}$$

onde,

T = intervalo de teste para o componente;

λ = a taxa de falha do componente por unidade de tempo.

Se $\lambda T << 1$, então a equação para Q pode ser aproximada para:

$$Q \cong \frac{1}{2}\lambda T \tag{5.8}$$

Quando o componente é testado, podemos definir o risco limitado por teste da seguinte forma [31,32]:

R_D = contribuição de risco limitado por teste, e

$\Delta R = R_1 - R_0$ = aumento no risco associado à indisponibilidade do componente

onde,

R_1 = freqüência de dano ao núcleo, avaliada com o componente indisponível (indisponibilidade do componente =1, ou *true*) e,

R_0 = freqüência de dano ao núcleo, avaliada com o componente disponível (indisponibilidade = 0, ou *false*).

Então, o risco limitado por teste pode ser determinado através da fórmula:

$$R_D = Q \cdot \Delta R = \frac{1}{2}\lambda T \cdot (R_1 - R_0) \tag{5.9}$$

onde, Q representa a indisponibilidade média do componente entre testes.

Entretanto, quando se deseja uma modificação de IT, no caso desse trabalho, extensão de IT, é fundamental que se calcule a variação da medida de risco adotada, a FDN, causada pela extensão de tempo do intervalo de teste.

Nesse caso, o cálculo deve ser efetuado através da expressão:

$$\Delta FDN = FDN_{EIT} - FDN_{B} \tag{5.10}$$

onde,

FDN_{EIT} = valor da FDN calculado com o valor da extensão do IT

FDN_{B} = valor da FDN *(baseline)*

O cálculo da FDN_{EIT}, para as bombas testadas de cada sistema, SIS, SAS e SAAA, é realizado através do código SAPHIRE considerando-se a alteração do IT para o novo valor da extensão desejada.

O cálculo de FDN_{EIT} inclui a modificação das indisponibilidades de falha na partida e de causa comum na partida do componente para refletir a extensão de IT, que são expressas, para um sistema de dois trens, respectivamente, por:

$$Q'_{FP} = \frac{1}{2}\lambda T_{E} \tag{5.11}$$

$$Q'_{CCP} = \frac{1}{2}\beta\lambda T_{E} \tag{5.12}$$

onde,

Q'_{FP} - probabilidade de falha na partida com IT estendido

Q'_{CCP} - probabilidade de causa comum na partida com IT estendido

T_{E} - intervalo de teste da extensão do IT e,

β, representa o fator de causa comum do Modelo do Fator Beta que é apresentado na Seção 5.4.2.

O critério de aceitação de risco para variações da FDN oriundas de quaisquer variações na configuração da planta, válido também para modificações de IT, está apresentado na Seção 4.5.

5.4 Tratamento de Falhas de Causa Comum

Falhas de causa comum podem ser definidas como aquelas que, quando ocorrem, afetam mais de um componente. Portanto, quando um componente falha devido à uma falha de causa comum, outro ou vários componentes podem também falhar [29].

Para modelar falhas de causa comum que afetam bombas redundantes do mesmo sistema e que pertencem ao mesmo grupo de causa comum, o modelo de Múltiplas Letras Gregas (MLG) pode ser aplicado. Cabe ressaltar que o Modelo do Fator Beta é um caso especial do modelo MLG, quando temos dois componentes no mesmo grupo de causa comum. Esses modelos são apresentados nas seções seguintes [29].

5.4.1 Múltiplas Letras Gregas (MLG)

O modelo de Múltiplas Letras Gregas é considerado o mais geral dentre as várias extensões do Modelo do Fator Beta [33, 34]. O modelo MLG apresenta um método onde outros parâmetros são adicionados ao Modelo do Fator Beta para distinguir falhas de causa comum que atingem diferentes números de componentes, em um sistema que possua um número maior de redundâncias.

Os parâmetros do modelo MLG consistem em uma probabilidade total de falha do componente que inclui os efeitos de todas as contribuições independentes e de causa comum para a falha desse componente, bem como um conjunto de frações de falhas que são usadas para quantificar as probabilidades condicionais de todos os possíveis modos pelos quais uma falha de causa comum de um componente possa ser compartilhada com outros componentes do mesmo grupo, dada a ocorrência de falha do componente. Por exemplo, os quatro primeiros parâmetros do modelo MLG são:

Q_T = probabilidade total de falha de cada componente devido a todas as falhas independentes e de causa comum;

β = probabilidade condicional de que a causa da falha de um componente seja compartilhada por um ou mais componentes adicionais, dado que um componente falhou;

γ = probabilidade condicional de que a causa da falha de um componente que é compartilhada por um ou mais componentes seja compartilhada por dois ou mais componentes adicionais, dado que dois componentes falharam;

δ = probabilidade condicional de que a causa da falha de um componente que é compartilhada por dois ou mais componentes seja compartilhada por três ou mais componentes adicionais, dado que três componentes falharam.

De acordo com as definições acima, a equação geral que expressa, em termos de parâmetros de MLG, "Q_k", a probabilidade das falhas de causa comum entre "k" componentes específicos de um grupo de causa comum com "m"componentes, tal que $1 \le k \le m$, é:

$$Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \prod_{i=1}^{k} \rho_i \left(1-\rho_{k+1}\right) Q_T \qquad (5.13)$$

onde: $\rho_1 = 1,\ \rho_2 = \beta,\ \rho_3 = \gamma,\ \rho_4 = \delta, ..., \rho_{m+1} = 0$

Por exemplo, para um sistema de três componentes (m=3), os parâmetros que contribuem são β e γ. Os demais parâmetros, δ para o caso de m=3, são nulos.

Para o exemplo de causa comum compartilhada por três componentes, γ é a probabilidade de que a falha de causa comum do componente seja compartilhada por exatamente mais dois componentes. Nesse caso, δ = 0 e Q_T é expresso em termos de Q_1, Q_2 e Q_3 da seguinte forma:

$$Q_1^{(3)} = (1-\beta)\cdot Q_T$$

$$Q_2^{(3)} = (1/2)\cdot\beta\cdot(1-\gamma)\cdot Q_T \qquad (5.14\text{ a-c})$$

$$Q_3^{(3)} = \beta\cdot\gamma\cdot Q_T$$

5.4.2 Modelo do Fator Beta

O Modelo do Fator Beta é um dos modelos de parâmetro simples mais utilizados na análise de causa comum. Modelos de parâmetro simples são aqueles que usam um parâmetro além da probabilidade de falha total do componente para o cálculo das falhas de causa comum [29].

O Modelo do Fator Beta é dado pela expressão:

$$Q_k = \begin{cases} (1\text{-}\beta)\cdot Q_T & k = 1 \\ 0 & 1 \prec k \prec m \\ \beta\cdot Q_T & k = m \end{cases} \qquad (5.15\text{ a-c})$$

Pode-se notar que o Modelo do Fator Beta é um caso especial do modelo de MLG, quando $\gamma = 1$ [34].

No Modelo do Fator Beta, uma fração (β) da taxa de falha do componente pode ser associada aos eventos de causa comum compartilhados pelo outro componente do mesmo grupo. De acordo com este modelo, sempre que uma falha de causa comum ocorre, todos os componentes do grupo (dentro do grupo de causa comum) falham.

Então, a expressão em função do modelo de MLG para dois trens fica da seguinte maneira:

$$Q_1 = (1-\beta)\cdot Q_T \qquad (5.16\ a\text{-}b)$$

$$Q_2 = \beta \cdot Q_T$$

e

$$Q_T = Q_1 + Q_2 \qquad (5.17)$$

onde,

Q_1 = probabilidade de todas as falhas independentes

Q_2 = probabilidade de todas as falhas de causa comum

então,

$$\beta = \frac{Q_2}{Q_1 + Q_2} \qquad (5.18)$$

Quando existe mais de um tipo de falha de causa comum como, por exemplo, na modelagem da APS de Angra1, as falhas de causa comum das bombas são divididas em dois tipos:

- falha de causa comum na partida (Q_{CCP});

- falha de causa comum em continuar operando (Q_{CCO}).

Nesse caso:

$$Q_2 = Q_{CCP} + Q_{CCO} = \beta_P \cdot Q_T + \beta_O \cdot Q_T = (\beta_P + \beta_O)\cdot Q_T \qquad (5.19)$$

e,

$$\beta = \beta_P + \beta_O \tag{5.20}$$

onde,

β_P = fator beta para as falhas de causa comum na partida, e

β_O = fator beta para as falhas de causa comum na operação

5.4.3 Grupo de Causa Comum com dois Componentes

Para a avaliação de um sistema de dois componentes pertencentes ao mesmo grupo de causa comum é necessária a representação do modelo de falha de cada componente:

$$A_T = A_I \cup C_{AB} \tag{5.21 a-b}$$

$$B_T = B_I \cup C_{AB}$$

O subscrito T denota a falha total do componente devido a todas as causas. O subscrito I denota as falhas devido a causas independentes e C_{XY} denota as falhas de causa comum. A probabilidade de falha total de A ou de B é dada pela equação (5.14), onde:

$$Q_1 = P[A_I] = P[B_I] \tag{5.22 a-b}$$

$$Q_2 = P[C_{AB}]$$

Um sistema de dois componentes redundantes é dito do tipo “um de dois”, quando basta que apenas um componente funcione para que ocorra o sucesso do sistema. Analogamente, todos os componentes devem falhar para que o sistema seja

considerado falho. O sistema do tipo “um de dois” tem os seguintes cortes mínimos: $[A_I, B_I]$ e $[C_{AB}]$.

Para a quantificação da árvore de falhas expandida é definida a probabilidade:

$Q_k^{(m)}$ = probabilidade de um evento básico de causa comum envolvendo k componentes específicos em um grupo de causa comum de m componentes, ($1 \le k \le m$).

O modelo que usa $Q_k^{(m)}$ para calcular as probabilidades de falha do sistema é denominado Modelo de Parâmetro Básico [34].

Então, a probabilidade de falha do sistema, $S = A_T \cap B_T$, denotada por Q_S é dada em termos do Modelo de Parâmetro Básico, por:

$$Q_S = Q_I^2 + Q_2 \tag{5.23}$$

Se o componente A se encontra falho, a probabilidade de falha condicional de S dado A_T é expressa por (sistema um de dois):

$$P[S/A_T] = \frac{P[A_T \cap B_T]}{P[A_T]} = \frac{Q_S}{Q_T} \tag{5.24}$$

Essa expressão pode ser obtida através da soma dos cortes mínimos. Para isso vamos desenvolver as probabilidades condicionais para cada corte mínimo.

$$P[A_I \cap B_I / A_T] = \frac{P[A_I \cap B_I]}{P[A_T]} = \frac{Q_I^2}{Q_T} \tag{5.25}$$

$$P[C_{AB}/A_T] = \frac{P[C_{AB}]}{P[A_T]} = \frac{Q_2}{Q_T} \tag{5.26}$$

$$\frac{Q_S}{Q_T} = \frac{Q_1^2}{Q_T} + \frac{Q_2}{Q_T} \tag{5.27}$$

Conforme já mostrado, um sistema de dois componentes redundantes pode ser representado através das probabilidades devido a causas independentes e de causa comum, separadamente, expressas em função da probabilidade de falha total do sistema (5-16 a-b) e (5.17).

Para fins de facilidade de cálculos, algumas considerações práticas são adotadas [34]:

$$Q_1 \approx Q_T \text{, uma vez que } (1-\beta) \approx 1 \tag{5.28}$$

Utilizando-se a aproximação (5.28) na equação (5.27) obtém-se:

$$\frac{Q_S}{Q_T} \approx Q_1 + \beta \tag{5.29}$$

A equação (5.29) expressa a probabilidade de falha de um sistema de dois componentes quando um deles está falho. Q_1 representa a probabilidade de falha do componente B devido às causas independentes e β representa as falhas de causa comum.

5.4.4 Grupo de Causa Comum com três Componentes

Na avaliação de um sistema de três componentes, as falhas de causa comum devem ser tratadas de forma mais complexa quanto aos possíveis acoplamentos das bombas. Para isso é necessária a apresentação de alguns conceitos relativos à

representação paramétrica de probabilidades de eventos básicos para um grupo de três componentes [33, 34]:

Um grupo de causa comum composto de três componentes similares A, B e C pode ser expresso pelo seguinte modelo de falha:

$$A_T = A_I \cup C_{AB} \cup C_{AC} \cup C_{ABC}$$

$$B_T = B_I \cup C_{AB} \cup C_{BC} \cup C_{ABC} \qquad (5.30\text{ a-c})$$

$$C_T = C_I \cup C_{AC} \cup C_{BC} \cup C_{ABC}$$

O subscrito T denota a falha total devido a todas as causas, o subscrito I denota as falhas independentes e C_{XY} denota as falhas de causa comum entre os componentes X e Y. Para fins de obtenção do Modelo de Parâmetro Básico para a análise de causa comum, a probabilidade de falha de A_T, B_T ou de C_T é dada pela equação:

$$Q_T = Q_1 + 2Q_2 + Q_3 \qquad (5.31)$$

onde,

Q_T representa a probabilidade total de falha de um trem, e

$$Q_1 = P[A_I] = P[B_I] = P[C_I]$$

$$Q_2 = P[C_{AB}] = P[C_{AC}] = P[C_{BC}] \qquad (5.32\text{ a-c})$$

$$Q_3 = P[C_{ABC}]$$

As equações (5.32 a-c) se referem ao Modelo de Parâmetro Básico para falhas de causa comum [34].

Um sistema de três componentes é do tipo “um de três” quando possui três trens redundantes e basta que um deles funcione para que haja sucesso do sistema. Este é exatamente o caso do SAS, que possui três bombas, cujo critério de sucesso é o funcionamento de apenas uma delas, tanto em condições de operação normal, como em condições de acidente. Portanto, um sistema do tipo “um de três” só é considerado falho quando os seus três componentes falham. A probabilidade de falha do evento indesejado ($S = A_T \cap B_T \cap C_T$), denotada por Q_S, é expressa, em termos do Modelo de Parâmetro Básico por [34]:

$$Q_S = Q_1^3 + 3\,Q_1 \cdot Q_2 + Q_3 \tag{5.33}$$

Similarmente ao modo como foi expressa a probabilidade de falha condicional para um sistema de dois trens, quando um deles se encontra falho, pode-se obter a expressão algébrica em função de Q_1, Q_2 e Q_3, para a representação da falha de um sistema de três componentes, quando desejamos simular a falha de um deles, ou seja, por exemplo, quando a bomba “A” está falha ou se encontra em manutenção corretiva (MC) [34].

Nesse caso, a probabilidade de falha condicional do sistema S, dado que o componente A falhou é:

$$P[S / A_T] = \frac{P[A_T \cap B_T \cap C_T]}{P[A_T]} = \frac{Q_S}{Q_T} \tag{5.34}$$

onde,

Q_S = probabilidade de falha do sistema;

Q_T = probabilidade de falha total de um componente.

Através do desenvolvimento das probabilidades condicionais para os cortes mínimos, obtém-se:

Para $[A_I, B_I, C_I]$:

$$P[(A_I \cap B_I \cap C_I) / A_T] = \frac{P[A_I \cap B_I \cap C_I]}{P[A_T]} = Q_I^2 \frac{Q_1}{Q_T} \qquad (5.35\ a\text{-}e)$$

Para $[A_I, C_{BC}]$:

$$P[A_I \cap C_{BC} / A_T] = \frac{P[A_I \cap C_{BC}]}{P[A_T]} = Q_1 \frac{Q_2}{Q_T}$$

Para $[B_I, C_{AC}]$:

$$P[B_I \cap C_{AC} / A_T] = \frac{P[B_I \cap C_{AC}]}{P[A_T]} = Q_2 \frac{Q_1}{Q_T}$$

Para $[C_I, C_{AB}]$:

$$P[C_I \cap C_{AB} / A_T] = \frac{P[C_I \cap C_{AB}]}{P[A_T]} = Q_2 \frac{Q_1}{Q_T}$$

Para $[C_{ABC}]$:

$$P[C_{ABC} / A_T] = \frac{P[C_{ABC}]}{P[A_T]} = \frac{Q_3}{Q_T}$$

Somando-se todos os termos das equações (5.35 a-e), obtém-se;

$$\frac{Q_S}{Q_T} = Q_1^2 \frac{Q_1}{Q_T} + 2Q_1 \frac{Q_2}{Q_T} + Q_2 \frac{Q_1}{Q_T} + \frac{Q_3}{Q_T} \tag{5.36}$$

Como já citado na Seção 5.4.3, o Modelo de Parâmetro Básico utiliza $Q_k^{(m)}$ para calcular as probabilidades de falha de causa comum. Por motivos práticos, para a análise de grupo de componentes igual ou maior do que três é conveniente que $Q_k^{(m)}$ seja reescrito em termos de outros parâmetros que facilitem os cálculos. Para esse propósito, é recomendado o uso do Modelo do Fator Alfa, cujos parâmetros são:

Q_T = Probabilidade de falha total de cada componente devido a todas as falhas independentes e às falhas de causa comum.

α_k = Fração da freqüência total de falha dos eventos que ocorrem em um sistema e envolvem a falha de k componentes devido a causas comuns.

Usando esses parâmetros, as probabilidades de causa comum envolvendo a falha de k componentes de um sistema de m componentes são expressas de duas maneiras distintas, conforme a estratégia de teste adotada.

5.4.4.1 Sistemas com Estratégia de Teste Seqüencial

Para sistemas submetidos a testes do tipo seqüencial, o Modelo de Parâmetro Básico, que utiliza $Q_k^{(m)}$ para a representação das probabilidades de falhas do sistema é expresso, em termos do Modelo do Fator Alfa, por [29]:

$$Q_k^{(m)} = \frac{k}{\binom{m-1}{k-1}} \frac{\alpha_k}{\alpha_t} Q_T \tag{5.37}$$

onde,

$$k = 1,\ 2, ..., m$$

e

$$\alpha_t = \sum_{k=1}^{m} k\alpha_k$$

Para os testes seqüenciais, a modelagem das probabilidades dos eventos básicos, utilizando-se o Modelo do Fator Alfa, para um sistema de três componentes, é dada por:

$$Q_1 = \left(\frac{\alpha_1}{\alpha_1 + 2\alpha_2 + 3\alpha_3} \right) \cdot Q_T$$

$$Q_2 = \left(\frac{\alpha_2}{\alpha_1 + 2\alpha_2 + 3\alpha_3} \right) \cdot Q_T \tag{5.38 a-c}$$

$$Q_3 = 3 \cdot \left(\frac{\alpha_3}{\alpha_1 + 2\alpha_2 + 3\alpha_3} \right) \cdot Q_T$$

Utilizando-se as equações (5.14 a-c) e (5.38.a-c), obtemos a conversão do Modelo do Fator Alfa em função dos parâmetros das MLG para o teste seqüencial [34]:

$$\alpha_1 = \frac{6(1-\beta)}{6-\beta(3+\gamma)}$$

$$\alpha_2 = \frac{3\beta(1-\gamma)}{6-\beta(3+\gamma)} \qquad \text{(5.39 a-c)}$$

$$\alpha_3 = \frac{2\beta\gamma}{6-\beta(3+\gamma)}$$

Para fins de facilidade de cálculos, torna-se útil o uso de algumas aproximações. Considerando-se $\beta << 1$ e $\gamma \approx 1$ obtém-se:

$$\alpha_1 \approx 1$$

$$\alpha_2 \approx 0 \qquad \text{(5.40 a-c)}$$

$$\alpha_3 \approx \frac{1}{3}\beta\gamma$$

Valores típicos de β e γ para sistemas de segurança de centrais nucleares americanas podem ser encontrados na referência [35].

Substituindo-se os valores aproximados de α_1, α_2 e α_3 (5-40 a-c), nas equações (5.38 a-c), são obtidas as seguintes expressões para Q_1, Q_2 e Q_3, para teste seqüencial:

$$Q_1 \approx \frac{1}{1+\beta\gamma} \cdot Q_T \approx Q_T$$

$$Q_2 \approx 0 \qquad \text{(5.41 a-c)}$$

$$Q_3 \approx \beta\gamma \cdot Q_T$$

Utilizando-se as aproximações para as probabilidades Q_1, Q_2 e Q_3 (5.41 a-c) pode-se aproximar a equação (5.36) para testes do tipo seqüencial:

$$\frac{Q_S}{Q_T} \approx Q_1^2 + \beta\gamma \qquad (5.42)$$

Mas $\frac{Q_S}{Q_T}$ representa a falha do sistema, dada a falha de um trem, onde o termo relativo às falhas independentes dos demais trens é representado por Q_1^2, e o produto $\beta\gamma$ representa as falhas de causa comum.

Para o teste do tipo seqüencial, em termos de cálculos, a equivalência (5.42) indica que para o caso de um sistema de três componentes, a simulação da falha de um deles, como por exemplo, do trem A, pode ser feita substituindo-se o valor das falhas independentes de A por *true* $(P[A_I] = 1)$ e substituindo-se as falhas de causa comum do grupo de três componentes por:

$$Q_{CCABC} \approx \beta\gamma \qquad (5.43)$$

onde, Q_{CCABC} se refere à probabilidade de causa comum dos componentes A, B e C.

Entretanto, as falhas de causa comum duas as duas devem ser substituídas por zero ou *false*. Isso se deve à aproximação considerada para $Q_2 \approx 0$ (5.41 b), onde Q_2 representa as probabilidades de falha dos componentes dois a dois.

5.4.4.2 Sistemas com Estratégia de Teste Escalonado

Para sistemas submetidos a testes do tipo escalonado, o Modelo de Parâmetro Básico, que utiliza $Q_k^{(m)}$ para a representação das probabilidades de falhas do sistema é expresso, em termos do Modelo do Fator Alfa, por [34]:

$$Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \alpha_k^e Q_T \tag{5.44}$$

A partir dessa modelagem, as probabilidades dos eventos básicos de um sistema de três componentes, cuja estratégia de teste é escalonada, podem ser expressas por:

$$Q_1^{(3)} = \alpha_1^e Q_T$$

$$Q_2^{(3)} = \frac{1}{2} \alpha_2^e Q_T \tag{5.45 a-c}$$

$$Q_3^{(3)} = \alpha_3^e Q_T$$

Conforme já mostrado na Seção 5.4.1, através da utilização do modelo MLG, Q_T é expresso em termos de Q_1, Q_2 e Q_3 pelas equações (5.14 a-c). Utilizando-se as equações (5.14 a-c) e (5.45 a-c), podemos exprimir α em função de β e γ para o teste do tipo escalonado:

$$\alpha_1^e = 1 - \beta_e$$

$$\alpha_2^e = \beta_e \cdot (1 - \gamma) \qquad \text{(5.46 a-c)}$$

$$\alpha_3^e = \beta_e \gamma$$

onde β_e se refere ao Fator Beta para a estratégia de teste escalonado.

Utilizando-se a equivalência (5.28) e substituindo-se as equações (5.45 a-c) na equação (5.36), obtemos:

$$\frac{Q_s}{Q_T} \approx Q_1^2 \alpha_1^e + 2Q_1 \alpha_2^e + Q_2 \alpha_1^e + \alpha_3^e \approx$$

$$\approx Q_1^2 + 2Q_1 \alpha_2^e + Q_2 + \alpha_3^e \approx Q_1^2 + \alpha_3^e \qquad (5.47)$$

Deve ser observado que $\alpha_1^e \approx 1, \alpha_2^e \approx 0$ e $Q_2 \approx 0$.

Contudo, $\frac{Q_S}{Q_T}$ representa a falha do sistema, dada a falha de um trem, onde o termo relativo às falhas independentes dos demais trens é representado por Q_1^2, e as falhas de causa comum são representadas por α_3^e, onde $\alpha_3^e = \beta_e \gamma$ (5.46 c).

Em termos de cálculos, a equivalência (5.47) indica que para o caso de um sistema de três componentes, a simulação da falha de um deles, como, por exemplo, do trem A, pode ser feita substituindo-se o valor das falhas independentes de A por *true* $(P[A_1] = 1)$, enquanto as falhas de causa comum dos três componentes devem ser substituídas por:

$$Q_{CCABC} \approx \beta_e \gamma \tag{5.48}$$

onde, Q_{CCABC} se refere à probabilidade de causa comum dos componentes A, B e C.

Cabe ressaltar que usando a aproximações $\alpha_1^e \approx 1$ e $\alpha_2^e \approx 0$ e $Q_2 \approx 0$, para a simulação de um trem falho de um sistema de três componentes, as falhas de causa comum duas a duas devem ser substituídas por zero ou *false.*

5.5 Medidas Compensatórias

Em certos casos, quando mudanças propostas de ET resultam em apenas pequenos incrementos na FDN [7], medidas compensatórias podem ser adotadas como parte da avaliação das propostas. Tais medidas, discutidas a seguir, têm a função de balancear ou compensar o aumento do risco calculado (FDN) associado à mudança proposta, de forma que o risco final se mantenha igual ou inferior ao risco da configuração original.

Quando é desejada uma redução do incremento de risco resultante da modificação de ET proposta, ou mesmo quando a proposta apresentada tenha sido aceita de acordo com os critérios de aceitação, podem ser adotadas medidas compensatórias, tais como as sugeridas abaixo. Medidas compensatórias podem ser consideradas parte integrante da análise da modificação proposta, mas não devem ser sugeridas e/ou implementadas para compensar possíveis deficiências de projeto detectadas ao longo da operação da planta.

Exemplo de medidas compensatórias [25]:

1) Teste adicional do trem redundante logo antes do inicio de uma atividade de manutenção programada, como parte de uma proposta de extensão de TPI;

2) Incorporação de estratégias de teste escalonado como parte de proposta de extensão de IT;

3) Melhoria de procedimentos de teste e de manutenção no sentido de reduzir erros relacionados com atividades de teste e de manutenção;

4) Limitação de testes e manutenções simultâneas de sistemas redundantes ou diversos como parte de uma proposta de extensão de TPI;

5) Melhoria de procedimentos operacionais e treinamento de operadores no sentido de reduzir o impacto de erros humanos;

6) Melhoria de projetos de sistemas, a qual reduziria a indisponibilidade total de sistemas e risco associado à planta.

Quando são sugeridas medidas compensatórias como parte da avaliação de proposta de modificação de ET, o impacto no risco associado a essas medidas deve ser considerado e apresentado, tanto qualitativa quanto quantitativamente.

Segundo o guia da NRC [25], quando avaliações quantitativas são utilizadas, o impacto total das modificações propostas deve ser avaliado por comparação, o que inclui:

1) Avaliação da modificação de ET proposta sem as medidas compensatórias;

2) Avaliação da modificação de ET proposta com as medidas compensatórias;

3) Discussão específica sobre como cada medida compensatória é creditada quantitativamente no modelo da APS ou durante o processo de avaliação.

Dentre as medidas compensatórias citadas acima, nem todas são passíveis de avaliação baseada em estudos de risco. As duas últimas dependem do gerenciamento da planta, treinamento de operadores e de modificação de projeto. A quarta medida compensatória exige cálculos que envolvem o controle de configuração da planta.

Consistindo em uma das aplicações mais complexas da APS, o controle de configuração da planta não se encontra dentro do escopo deste trabalho. Configurações da planta podem ser definidas através das condições dos sistemas e das funções de segurança que, por sua vez, dependem das condições de seus componentes. O controle de configuração da planta requer o gerenciamento das condições operacionais dos componentes, sistemas e funções de segurança, e deve ser executado de acordo com critérios estabelecidos [36].

Neste trabalho, para as propostas de extensão do IT, a compensação será feita através da incorporação de estratégias de testes escalonados. Quanto às propostas de

extensão dos TPI, será implementada a estratégia de teste adicional do trem redundante logo antes do inicio de uma atividade de manutenção programada para compensar possíveis incrementos de risco.

Portanto, dentro do escopo deste trabalho, as medidas compensatórias consideradas para a avaliação de propostas de modificações de ET, são:

1) Teste adicional da bomba do trem redundante logo antes do inicio de uma atividade de manutenção, bem como mudança da estratégia de teste, caso esta já não seja a estratégia de teste vigente, ambos para compensar a extensão de TPI;

2) Implementação da estratégia de teste escalonado, caso esta já não seja a estratégia de teste vigente, para compensar a extensão de IT.

5.5.1 Medida Compensatória: Teste do Trem Redundante

A primeira medida compensatória a ser adotada neste trabalho para balancear ou compensar um pequeno incremento de risco associado à proposta de modificação de ET é a recomendação de que, por exemplo, seja testada a bomba do outro trem logo antes do início do período de indisponibilidade devido à manutenção preventiva ou corretiva do trem em questão.

Conforme mostrado na Seção 5.2 o impacto de risco de TPI de evento simples é expresso pela equação (5.1) e o impacto de risco da TPI média anual, expresso pela equação (5.2).

Ambos esses riscos podem ser reduzidos para um dado período de indisponibilidade d, se R_1 puder ser reduzido, portanto diminuindo o impacto de risco provocado pela indisponibilidade do componente.

Para reduzir o aumento no nível de risco $R_{1,}$ deve ser reduzida a indisponibilidade de um ou mais componentes que contribuem para os cortes mínimos correspondentes [37].

Uma das maneiras de se obter essa redução é através do teste do componente do trem redundante para que seja confirmada a sua operabilidade. Se o teste pode ser

considerado efetivo, então, o valor para a indisponibilidade do componente é reduzido, bem como a contribuição dos cortes mínimos que contêm esse componente.

A partir do teste, a indisponibilidade do componente testado vai começar a crescer de acordo com a expressão (5.8).

Se o período de manutenção, ou TPI, é pequeno, ou seja, com duração de até uma semana, o valor da contribuição da indisponibilidade descrita pela expressão (5.8), é pequeno podendo ser desprezado. Entretanto, o valor dessa indisponibilidade pode ser calculado para um sistema de dois componentes, através da expressão:

$$Q_{FP} \approx \frac{1}{2}\lambda \cdot d_{TPI} \tag{5.49}$$

onde,

d_{TPI} = duração do TPI estendido.

Os cálculos das probabilidades de falhas de causa comum na partida das bombas testadas, também são modificados através das expressões:

$$Q_{CCP}^{(2)} \approx \frac{1}{2}\beta_P \cdot \lambda \cdot d_{TPI}$$

$$Q_{CCPAB}^{(3)} \approx \frac{1}{4}\lambda \cdot \beta \cdot (1-\gamma) \cdot d_{TPI} \tag{5.50 a-c}$$

$$Q_{CCPABC}^{(3)} \approx \frac{1}{2}\lambda \cdot \beta \cdot \gamma \cdot d_{TPI}$$

onde,

$Q_{CCP}^{(2)}$ = probabilidade de causa comum na partida das bombas de sistemas de dois trens;

$Q_{CCPAB}^{(3)}$ = probabilidade de causa comum na partida das bombas de sistemas de três trens acopladas duas a duas;

$Q^{(3)}_{CCPABC}$ = probabilidade de causa comum na partida das bombas de sistemas de três trens acopladas três a três.

5.5.2 Medida Compensatória: Teste Escalonado

O intervalo de teste é definido como o tempo transcorrido entre dois testes consecutivos em um componente de um sistema.

A experiência operacional internacional de centrais nucleares indica que existem dois tipos de estratégias de testes: seqüencial e escalonada [38]. Embora as especificações técnicas regulem a duração dos intervalos de testes para os sistemas de segurança, o tipo de estratégia de teste não é especificado, ficando a critério da operadora a escolha do mais apropriado.

Para uma melhor compreensão das principais diferenças entre as duas estratégias de teste, seja um sistema de dois trens, cujas bombas A e B são parte do trem A e do trem B, respectivamente, sendo as bombas testadas de maneira seqüencial. A representação gráfica da estratégia de teste seqüencial das bombas está apresentada na Figura 5.3. Por exemplo, se os testes das bombas forem mensais, a cada 30 dias as bombas são testadas em seqüência, primeiramente a bomba A e, logo em seguida, a bomba B.

A e B	**A e B**	**A e B**
Teste das Bombas A e B	Teste das Bombas A e B	
Intervalo de Teste	**Intervalo de Teste**	

Figura 5.3 – Teste seqüencial para um sistema de dois trens

No caso do procedimento de teste escalonado, o intervalo de teste é o mesmo para as duas bombas individualmente. Entretanto, as bombas não são testadas ao mesmo tempo, mas de maneira escalonada. A Figura 5.4 contém a representação gráfica do procedimento de teste escalonado para o sistema de dois trens. Por exemplo, se os testes

das bombas forem mensais, cada bomba será testada, no mínimo, de trinta em trinta dias, mas os testes de cada bomba serão defasados de 15 dias em relação aos outros.

Além disso, na estratégia escalonada, quando, por exemplo, o teste da bomba A detecta que a bomba está falha, a bomba B é testada imediatamente, apesar do teste desta última estar programado para 15 dias após. Isso explica o uso do termo "no mínimo", para o intervalo de teste de 30 dias de cada bomba [33]. Portanto, a estratégia de teste escalonado inclui um número maior ou igual de testes de cada bomba em relação à seqüencial.

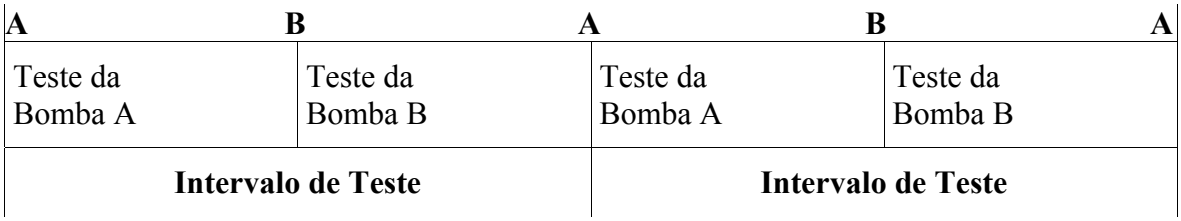

Figura 5.4 – Teste escalonado para um sistema de dois trens

A grande vantagem do teste escalonado é reduzir a incidência de falhas de causa comum introduzida por erros humanos. Em outras palavras, quando duas bombas são testadas seqüencialmente pela mesma equipe, caso seja cometido um erro de procedimento ou de execução do teste, a probabilidade de que esse erro seja repetido no segundo trem não é desprezível. Essa probabilidade de falha humana no teste da segunda bomba condicionada à falha humana durante o teste da primeira é a probabilidade de falha de causa comum. Portanto, a aplicação de procedimento de testes do tipo escalonado reduz a contribuição de falha de causa comum na partida de componentes em reserva.

A expressão que descreve a relação entre os estimadores probabilísticos de eventos básicos, segundo a estratégia de teste adotada, pode ser obtida pela divisão das equações (5.44) e (5.37) [33]:

$$\frac{Q_k^{Esc}}{Q_k^{Seq}} = \frac{1}{k} \tag{5.51}$$

onde:

Q_k^{Esc} = probabilidade de k falhas específicas de componentes devido às falhas de causa comum quando a estratégia de teste é do tipo escalonado;

Q_k^{Seq} = probabilidade de k falhas específicas de componentes devido às falhas de causa comum quando a estratégia de teste é do tipo seqüencial;

k = grupo de k componentes envolvidos no mesmo grupo de causa comum de um total de m componentes ($m \geq k$).

A equação 5.51 pressupõe que $\alpha_k^e = \frac{\alpha_k}{\alpha_t}$ e, portanto, usando as equações (5.39) e (5.46) conclui-se que $\beta = k\beta_e$.

Para um sistema de dois componentes:

$$\frac{Q_2^{2,Esc}}{Q_2^{2,Seq}} = \frac{1}{2} \tag{5.52}$$

Portanto, para um sistema de dois trens, quando a estratégia de teste é modificada de seqüencial para escalonada, a falha de causa comum relativa à falha na partida é reduzida por um fator de dois. Essa relação pode ser explicada através do fato do teste escalonado aumentar o número de testes "contra" as falhas de causa comum.

Para um sistema de três componentes, devem ser considerados os acoplamentos de falha comum dois a dois e três a três separadamente:

1) Acoplamento de componentes dois a dois:

$$\frac{Q_2^{3,Esc}}{Q_2^{3,Seq}} = \frac{1}{2} \tag{5.53}$$

2) Acoplamento de componentes três a três:

$$\frac{Q_3^{3,Esc}}{Q_3^{3,Seq}} = \frac{1}{3} \tag{5.54}$$

5.6 Características da Modelagem da APS

Para a avaliação de modificações de ET, os sistemas e componentes envolvidos devem estar modelados na APS. O modelo da APS deve ser capaz de tratar o alinhamento dos componentes durante os períodos de execução de testes e de manutenção. Tipicamente, Condições Limites de Operação (CLO) e exigências de testes remetem aos sistemas por trens e/ou componentes que são modelados nas árvores de falhas de sistemas de uma APS.

As árvores de falhas devem ser suficientemente detalhadas para incluir, especificamente, componentes para os quais existam exigências de testes e manutenção, de forma que possam ser avaliados.

- Para a avaliação de TPI, os modelos com detalhamento de sistemas por trens são adequados desde que os componentes pertencentes ao trem sejam claramente identificados (ou seja, todos os componentes que possam causar falha do trem);

- Para a avaliação de IT, é necessária a modelagem individual em nível de componentes.

Considerando-se que as APS são tipicamente detalhadas até o nível de componentes, as mesmas podem ser utilizadas para analisar tanto o TPI, como o IT.

Os modelos de indisponibilidade devem incluir contribuições de falhas aleatórias, falhas de causa comum, tempo de indisponibilidade de teste e indisponibilidade devido à manutenção.

As modificações no modelo de indisponibilidade de componentes para teste e manutenção devem ser baseadas em uma estimativa realista das práticas esperadas de teste e manutenção após a aprovação e implementação da modificação de ET. Em outras palavras, devem ser estimadas as freqüências de entrada em TPI para manutenção e testes programados.

O modelo de confiabilidade de componentes para tratar da indisponibilidade devido a teste e manutenção deve ser baseado em dados específicos da planta ou em experiência operacional comprovada da indústria, ou em ambos, conforme apropriado.

O modelo de indisponibilidade de componentes deve ter a flexibilidade de separar as contribuições de teste e de manutenção. Para a avaliação de TPI, a contribuição individual devido à indisponibilidade por manutenção pode ser igualada a zero, para caracterizar a ausência de atividades de manutenção. Para a avaliação de IT, a contribuição de indisponibilidade de teste determina a contribuição do risco associado à execução do teste.

Detalhes adicionais em termos de separação das taxas de falhas das contribuições do tipo falhas relacionadas à demanda e às falhas do tipo em reserva podem ser incorporadas, quando justificáveis, para a avaliação de exigências de teste.

As contribuições de falhas de causa comum devem ser modeladas de tal forma que possam ser modificadas para refletir uma condição na qual um ou mais componentes estejam indisponíveis. Entretanto, deve ser notado que a modelagem de falhas de causa comum não é dependente somente do número de componentes em operação, mas também das razões pelas quais os componentes se tornaram inoperantes, se para manutenção preventiva ou corretiva. Para o gerenciamento do risco e controle apropriado da configuração, as atividades de manutenção preventiva e corretiva devem ser cuidadosamente tratadas para expressar a diferença entre as mesmas.

Para se levar em consideração os efeitos dos tipos de testes efetuados em componentes redundantes (escalonados ou seqüenciais), podem ser usados modelos

dependentes do tempo e avaliações adicionais usando códigos de computação especiais, quando disponíveis.

5.7 Considerações sobre as Avaliações de Risco nas Modificações de ET

O uso da APS para a avaliação de modificações de ET requer um número considerável de hipóteses feitas na elaboração da APS que podem exercer influência significativa na aceitabilidade das modificações propostas.

Segundo o guia da NRC [25], as seguintes suposições devem ser consideradas na avaliação de modificação de TPI de Especificações Técnicas:

1. Avaliações de risco associadas ao TPI que são desenvolvidas com base somente em uma APS elaborada para operação em potência não levam em consideração o risco associado ao desligamento da planta devido a violações de ET.

2. No cálculo de impacto no risco (por exemplo: variação da FDN causada pela mudança do TPI), a variação da FDN média deve ser estimada usando-se a média dos tempos de indisponibilidades atuais e propostos.

3. Quando é avaliado o impacto no risco associado à modificação de TPI, o impacto anual no risco calculado leva em consideração a freqüência dos tempos de indisponibilidade. Portanto, uma extensão de tempo de indisponibilidade pode viabilizar uma melhoria na manutenção do componente, o que pode reduzir a taxa de falha do componente e, conseqüentemente, reduzir o tempo necessário de retirada de componentes para corrigir degradações ou falhas.

4. São freqüentemente solicitados pedidos de extensão de tempos de indisponibilidades de componentes para facilitar a manutenção preventiva de componentes de sistemas de segurança durante a operação em potência. A freqüência e duração da extensão podem ser estimadas, bem como o impacto no risco resultante da indisponibilidade de tais componentes.

5. Quando são estendidos tempos de indisponibilidade de trens de múltiplos sistemas de segurança, a probabilidade devido à contribuição das indisponibilidades de múltiplos componentes aumenta como resultado de combinação de falhas, testes e manutenções. Portanto, a sobreposição de atividades rotineiras programadas e a

ocorrência de falhas aleatórias se tornam mais prováveis. Os riscos condicionais, relativos a tais ocorrências podem ser significativos.

As seguintes hipóteses devem ser consideradas na avaliação de modificações de IT de Especificações Técnicas:

1. Normalmente, os testes têm a finalidade de detectar falhas que possam ter ocorrido durante o período de reserva. A taxa de falhas do componente, λ, representa as falhas na formulação da indisponibilidade do componente. Portanto, presume-se que o teste do componente detecte as falhas, de tal modo que, após o teste, a indisponibilidade do componente se torne igual a zero (0) representada como *false* na expressão booleana [34]. Cabe ressaltar que as APS possuem árvores de falhas que permitem o cálculo da indisponibilidade de sistemas, ou evento indesejado, cuja avaliação é feita através de funções booleanas, que apresentam combinações de falhas dos componentes por meios de portões lógicos do tipo "ou" ou "e".

2. Testes regulares efetuados em componentes de sistemas de segurança podem influenciar o desempenho dos mesmos. Geralmente, para a maioria dos componentes, o aumento do intervalo de teste além de um determinado período pode reduzir o desempenho do componente (ou seja, aumentar a taxa de falhas). Entretanto, não existem dados experimentais disponíveis que avaliem valores de IT além dos quais a taxa de falhas do componente, λ, aumente. Portanto, deve–se ter cuidado na avaliação de extensão de IT quando se utiliza somente a análise baseada em risco.

3. Em relação a testes de componentes redundantes, a estratégia de teste adotada causa um impacto nas medidas de risco avaliadas. As estratégias mais comumente usadas são de testes seqüenciais ou escalonados. Os impactos de risco associados à adoção de diferentes tipos de estratégia devem ser avaliados. Portanto, quando uma modificação de estratégia de teste é proposta, o impacto no risco deve ser avaliado.

6. MODELAGEM PARA AS SIMULAÇÕES

As análises de contribuição de risco associadas aos TPI, bem como algumas avaliações de IT, envolvem o cálculo das Freqüências de Dano ao Núcleo (FDN) através de uma APS da planta. Geralmente, a FDN condicional é calculada para estimar a FDN quando um ou mais componentes se encontram indisponíveis devido a falhas e subseqüentes Manutenções Corretivas (MC). Neste trabalho os cálculos são feitos através da utilização do código de computação SAPHIRE [8] para a análise quantitativa de APS e envolvem modificações de parâmetros de entrada (ou dados) de forma a representar as condições de indisponibilidade da planta [39]. Cabe ressaltar que o código SAPHIRE utilizado neste trabalho possui dados de entrada específicos para a central de Angra 1.

Para que se possa realizar a simulação das extensões de TPI e de IT para os sistemas SIS, SAS e SAAA são necessários os detalhamentos de modelagens de sistemas de dois e de três componentes.

6.1 Modelagem para a Simulação de Manutenção Corretiva

A simulação de MC ou de falha utiliza os resultados obtidos nas seções anteriores para grupo de causa comum de dois ou de três componentes.

O SIS possui duas bombas que pertencem a um mesmo grupo de causa comum. As duas bombas motorizadas do SAAA também pertencem a um mesmo grupo de causa comum. Entretanto, apesar do SAAA possuir uma terceira bomba turbinada, a mesma não faz parte do mesmo grupo de causa comum das motorizadas por possuir características de manufatura, funcionamento e procedimento de teste e manutenção bastante diversos dos aplicados às bombas motorizadas. Portanto, tanto o SIS como o SAAA têm bombas que pertencem a grupos de causa comum de dois componentes, apesar de o SAAA possuir três bombas. A modelagem de causa comum desses tipos de sistemas, na APS de Angra 1, utiliza o Modelo do Fator Beta.

O SAS possui três bombas idênticas, submetidas a testes do tipo seqüencial. Na APS de Angra 1 o SAS está modelado através do modelo de Múltiplas Letras Gregas

(MLG), já que as três bombas pertencem a um mesmo grupo de causa comum de três componentes.

A Tabela 6.1 mostra como devem ser substituídos os valores dos eventos básicos de falha na partida, na operação, e falhas de causa comum para o SIS, o SAS e o SAAA para simular a manutenção corretiva ou falha de um componente pertencente a um mesmo grupo de causa comum de cada tipo de sistema, com base nos detalhes apresentados no Capítulo5. Para tal são utilizadas as expressões (5.29) e (5.43).

Tabela 6.1 - Modificações das probabilidades das bombas para simular MC

Sistema/Bomba	Modificação das falhas na partida e na operação	Modificação das falhas de causa comum e de manutenção
SIS - Bomba A	$Q_{FP} \rightarrow 1$ *(true)* $Q_{FO} \rightarrow 1$ *(true)*	$Q_{CC} \rightarrow \beta$ $Q_{MA} \rightarrow 1$ *(true)*
SAS - Bomba A	$Q_{FO} \rightarrow 1$ *(true)*	$Q_{CCABC} \rightarrow \beta\gamma$ $Q_{CCAB} \rightarrow 0$ $Q_{CCAC} \rightarrow 0$ $Q_{CCBC} \rightarrow 0$
SAAA - Bomba motorizada do trem A	$Q_{FP} \rightarrow 1$*(true)* $Q_{FO} \rightarrow 1$*(true)*	$Q_{CC} \rightarrow \beta$ $Q_{MA} \rightarrow 1$ (*true*)

onde:

Q_{FP} = probabilidade de falha do componente na partida;

Q_{FO} = probabilidade de falha do componente na operação;

Q_{CC} = probabilidade de falha de causa comum da partida das bombas e

Q_{MA} = indisponibilidade do componente A devido à MC.

Conforme apresentado na Seção 5.4.3, os valores das falhas de causa comum para grupos de dois componentes foram substituídos por β de acordo com a expressão (5.29).

Cabe ressaltar que, como já mostrado na Seção 5.4.4.1, no caso do SAS, que é um sistema de três trens redundantes pertencentes ao mesmo grupo de causa comum, submetidos a teste seqüencial, para a simulação de falha de um trem, as falhas de causa comum (relativas às três bombas) devem ser substituídas pelo valor do produto $\beta \cdot \gamma$, (5.43), enquanto que as falhas de causa comum do acoplamento das bombas duas a duas devem ser substituídas por *false* (probabilidade = 0) (5.41b).

É importante enfatizar que, como na modelagem do SAS considera-se que a bomba A opera continuamente durante a operação normal da planta, a contribuição de falha de causa comum das três bombas na partida não foi considerada na modificação de dados para refletir a simulação da MC da bomba A.

6.2 Modelagem para a Simulação da Extensão de IT

As expressões (5.11) e (5.12), apresentadas na Seção 5.3, mostram como são expressas as probabilidades de falha na partida e de causa comum na partida do componente em função da extensão do IT.

Extensões de intervalos de teste podem ser simuladas através da multiplicação da probabilidade de falha na partida da bomba e a probabilidade de causa comum por um fator x, que representa a razão entre o intervalo de teste estendido e o intervalo de teste vigente.

A extensão de IT é simulada, então, multiplicando-se T (intervalo de teste vigente) pelo fator de multiplicação "x" para expressar a extensão proposta.

Então,

$$T_E = x \cdot T \tag{6.1}$$

onde,

T_E = extensão do intervalo de teste

x = fator de multiplicação

T = intervalo de teste vigente

No caso dos sistemas em análise neste trabalho, SIS, SAS e SAAA, os intervalos de teste vigentes são de um (1) mês. Portanto, como se deseja estendê-los para três meses, o fator de multiplicação assume o valor de três (3).

Portanto, ambas as indisponibilidades de falhas na partida e de causa comum devem ser multiplicadas pelo fator x para refletirem a extensão do IT.

$$Q'_{FP} = x \cdot Q_{FP} \tag{6.2}$$

$$Q'_{CCP} = x \cdot Q_{CCP} \tag{6.3}$$

É importante ressaltar que, a taxa de falha na partida, λ, não é modificada pela extensão, ou seja, significa que é assumido que a taxa de falha na partida é constante e, portanto, não é afetada quando se estende o IT.

A Tabela 6.2 mostra como os parâmetros de probabilidade de falha na partida e de causa comum são afetados pela extensão do IT.

Tabela 6.2 - Modificações das probabilidades das bombas para simular a extensão do IT

Sistema/Bombas	Probabilidades
SIS	$Q'_{FP} \rightarrow 3 \cdot Q_{FP}$ $Q'_{CCP} \rightarrow 3 \cdot Q_{CCP}$
SAS	$Q'_{FP} \rightarrow 3 \cdot Q_{FP}$ $Q'_{CCP} \rightarrow 3 \cdot Q_{CCP}$
SAAA	$Q'_{FP} \rightarrow 3 \cdot Q_{FP}$ $Q'_{CCP} \rightarrow 3 \cdot Q_{CCP}$

6.3 Simulação de Medidas Compensatórias

Depois de obtidos os valores para a nova FDN (com os valores propostos de modificações calculados), os mesmos devem ser comparados com os critérios apresentados na Seção 4.5, considerando-se as seguintes condições de contorno:

Para uma planta com a FDN menor que 1.0E-04 por reator ano (caso de Angra1, FDN_B = 4,01E-05 [5]), as modificações propostas devem ser consideradas, conforme apresentado na Seção 4.5, quando:

- Resultam em um decréscimo ou nenhuma alteração na FDN;

- Resultam em acréscimos bem pequenos na FDN, ou seja, menores do que 1.0E-06 por reator/ano;

- Quando o incremento na FDN se situa entre 1,0E-06 e 1,0E-05 por reator-ano, deve ser demonstrado que a FDN total é menor do que 1,0E-04 por reator-ano.

Quando os critérios não são atendidos ou quando a FDN se situa entre 1,0E-06 e 1,0E-05 e se deseja uma redução do risco total, as medidas compensatórias devem ser aplicadas:

1) Para compensar a extensão de TPI – teste do trem redundante e implementação, quando possível, da estratégia de teste escalonado;

2) Para compensar a extensão de IT – modificação de estratégia de teste (de teste seqüencial para teste escalonado), quando possível.

6.3.1 Simulação do Teste da Bomba do Trem Redundante

Conforme discutido na Seção 5.5.1, o teste da bomba do trem redundante é simulado através da modificação das expressões para as probabilidades de falha na partida e falha de causa comum na partida das bombas testadas. Os valores dessas probabilidades podem ser calculados através das expressões (5.49) e (5.50 a-c), onde:

Q_{FP} = representa as probabilidades de falha na partida das bombas;

Q_{CCP} = representa as probabilidades de falha de causa comum na partida das bombas;

Na APS de Angra1, os valores para as probabilidades de falha de causa comum na partida refletem as práticas correntes de duração dos intervalos de testes. Para o caso do SIS, SAS e SAAA os intervalos de testes vigentes são de um (1) mês. Portanto, as probabilidades de causa comum na partida para as bombas do trem redundante testadas desses sistemas devem ser, então, divididas por um fator de quatro para refletir a simulação do teste representado por um "novo" intervalo de teste de 168 horas (T = 1 mês → d_{TPI} = 1 semana).

As tabelas apresentadas a seguir mostram como as probabilidades de falha na partida e de modo comum das bombas devem ser modificadas para refletir, na APS de Angra1, o teste da bomba redundante para os sistemas SIS, SAS e SAAA, antes de entrar no Tempo Permitido de Indisponibilidade (TPI) para MC.

Outra modificação que deve ser feita para similar o teste da bomba do trem redundante é a redução da contribuição de manutenção da bomba testada, para cada um dos sistemas, para o valor zero (0), durante o TPI.

A Tabela 6.3 mostra, para um sistema de dois ou três componentes, como são simulados os testes das bombas redundantes, quando a bomba A falha, e, antes de entrar no TPI para a MC.

Tabela 6.3 - Simulação do teste da bomba do trem redundante para um sistema de dois ou três componentes

Teste das bombas dos componentes redundantes	**Bomba A: início do TPI**	**Bomba B: Teste é realizado imediatamente antes da bomba A entrar no TPI**	**Bomba C: Teste é realizado imediatamente antes da bomba A entrar no TPI**	**Modificação das falhas de causa comum na partida**
Sistema de dois ou três componentes	$Q_{FP} \rightarrow 1$ (*true*) $Q_{FO} \rightarrow 1$ *(true)* $Q_{MA} \rightarrow 1$*(true)*	$Q'_{FP} = Q_{FP}/4$ $Q_{MB} \rightarrow 0$ (*false*)	$Q'_{FP} = Q_{FP}/4$ $Q_{MC} \rightarrow 0$ (*false*)	$Q'_{CCP} = Q_{CCP}/4$

6.3.2 Simulação da Estratégia de Teste Escalonado

Essa segunda medida compensatória pode ser usada para contrabalançar os impactos no risco, decorrentes tanto de extensão de TPI como do IT. A modelagem utilizada para essa simulação está mostrada na Seção 5.5.2. A Tabela 6.4 mostra como devem ser modificadas as falhas de causa comum para refletir a modificação da estratégia de teste de seqüencial para escalonado. As equações (5.53) e (5.54) foram utilizadas para substituir às falhas de causa comum de acoplamento dois a dois e de três, respectivamente.

Tabela 6.4 - Modificação das probabilidades das bombas para refletir a estratégia de teste escalonado

Sistema	Modificação das falhas de causa comum na partida para teste escalonado
SIS - Bombas A e B	$Q'_{CC} \rightarrow \frac{1}{2} \cdot Q_{CC}$
SAS - Bombas A e B ou B e C ou A e C	$Q'_{CC} \rightarrow \frac{1}{2} \cdot Q_{CC}$
SAS - Bombas A e B e C	$Q'_{CC} \rightarrow \frac{1}{3} \cdot Q_{CC}$
SAAA - Bombas motorizadas A e B	$Q'_{CC} \rightarrow \frac{1}{2} \cdot Q_{CC}$

Na Seção 7 são apresentados os cálculos relativos às simulações de manutenção corretiva, teste do trem redundante, extensão de intervalo de teste e mudança de estratégia de teste para o SIS, SAS e SAAA.

7. CÁLCULOS PARA OS SISTEMAS DE SEGURANÇA

Nessa Seção são apresentados os cálculos realizados com o código SAPHIRE [8] para as simulações de extensões de TPI e de IT para o SIS, SAS e SAAA. A análise dos resultados obtidos para as extensões, através de confrontação com os critérios de aceitação apresentados na Seção 4.5, indica, na maioria das vezes, a necessidade da introdução de medidas compensatórias. Portanto, quando indicados, são apresentados, também, os cálculos pertinentes às simulações de teste do trem redundante e de modificação da estratégia de teste do tipo seqüencial para o escalonado.

Os cálculos efetuados para a obtenção do risco de evento simples e do risco anual médio são apresentados para cada sistema e suas respectivas extensões de TPI, considerando, também, a introdução das medidas compensatórias quando pertinentes.

Os riscos de evento simples de cada extensão de TPI e de introdução de medidas compensatórias são comparados e confrontados com os critérios apresentados na Seção 4.5, conforme a metodologia apresentada na Seção 5.2.

Cabe ressaltar que, dada a dificuldade de obtenção de dados específicos de Angra 1 que façam distinção entre as indisponibilidades devido à MP ou MC das bombas dos sistemas em questão, as taxas de falhas (λ) das mesmas foram adotadas como freqüências para os cálculos do risco médio anual associado às extensões de TPI [30].

Considerando-se que neste trabalho são avaliadas, somente, as contribuições de TPI relativas à MC, e que as taxas de falhas, λ, das bombas em questão são muito menores do que um (1), conclui-se que o TPI de evento simples é preponderante para a decisão baseada em risco sobre a aceitação das extensões de TPI ora em análise. Outros detalhes sobre os critérios de aceitação de risco e avaliações de impacto de risco são descritos nas Seções 4.5 e 5.2, respectivamente.

No que diz respeito às avaliações das extensões de IT, o incremento de risco causado pela extensão do IT é confrontado com o permitido pelo critério de risco de aumento de FDN. Quando pertinente, é introduzida a medida compensatória relativa à modificação da estratégia de teste do tipo seqüencial para o escalonado.

Para que sejam refletidas neste trabalho as estratégias de teste e manutenção em prática na central de Angra1, é apresentado, a seguir, um resumo das especificações técnicas vigentes.

7.1 Especificações Técnicas Vigentes

As ET vigentes datam de março de 2005 e fazem parte do capitulo 16 do RFAS [1]. Para o SIS, o tempo permitido de indisponibilidade (TPI) é de 24 horas. Para o SAS e o SAAA, o tempo permitido de indisponibilidade (TPI) é de 48 horas. O intervalo de teste (IT) para as bombas do SIS, SAS e SAAA é de um mês [1].

As práticas operacionais vigentes em Angra 1 adotam estratégias de testes para o SIS e o SAAA do tipo escalonada ao passo que, os testes do SAS são realizados de forma seqüencial.

Considerando-se que somente as bombas do SAS são sujeitas, atualmente, à estratégia de teste seqüencial, essas serão as únicas candidatas, caso necessário, à utilização da medida compensatória de mudança de estratégia de teste para o tipo escalonado.

Cabe ressaltar que, os testes das bombas que operam em reserva do SIS, SAS e SAAA são realizados de maneira *on-line*, ou seja, uma vez demandados a operar, esses sistemas estão sempre prontos para cumprir suas funções, mesmo que os mesmos se encontrem em fase de teste. Portanto, os eventos básicos referentes às contribuições de teste e manutenção para o SIS, SAS e SAAA, se referem exclusivamente aos eventos de manutenção, uma vez que os testes desses sistemas, que normalmente operam em modo de espera, não tornam os equipamentos indisponíveis.

Pelo mesmo motivo, a extensão do intervalo de teste não acarreta qualquer diminuição da contribuição devido a teste para as indisponibilidades das bombas em questão.

A Tabela 7.1 apresenta um panorama dos tipos de estratégias de testes aos quais os sistemas são submetidos atualmente, o tipo de modelagem de falhas de causa comum e as medidas compensatórias candidatas à aplicação, caso necessária.

Tabela 7.1 - Possibilidade de extensão de TPI ou de IT para o SIS, SAS e SAAA

Sistema	Estratégia de teste é escalonada	Múltiplas Letras Gregas (MLG)	Medida Compensatória: Teste do trem redundante	Medida Compensatória: Estratégia de teste escalonado
SIS	SIM	β	SIM	NÃO
SAS	NÃO	β e γ	SIM	SIM
SAAA	SIM	β	SIM	NÃO

7.2 Cálculos para Sistema de Injeção de Segurança (SIS)

O Apêndice A contém, em detalhes, as Funções, Descrição, Condições Limite de Operação, Exigências de Testes bem como, as Considerações de Engenharia relativas ao SIS.

7.2.1 SIS - Cálculos para a Simulação de Manutenção Corretiva

O primeiro passo para a simulação da extensão de TPI consta da elaboração de uma tabela com os cálculos a serem efetuados para o SIS para a simulação de Manutenção Corretiva (MC) no Trem A, como apresentado na Tabela 7.3.

Podemos obter os valores de β_P e de β_O para o SIS na Seção 4.2 da APS de Angra 1 [5]:

- Para a falha de causa comum na partida: $\beta_P = 0,1$

- Para a falha de causa comum na operação: $\beta_O = 0,1$

Entretanto, cabe ressaltar que, na APS de Angra 1, os cálculos dos fatores β_P (partida) e β_O (operação) para o SIS não consideraram a estratégia de teste escalonado, atualmente vigente na operação da central. Portanto, a correção desses valores diminui o valor final da FDN, enquanto que a simulação da MC aumenta a FDN. De fato, os

valores de β_P e β_O devem ser divididos por um fator de dois (2) para refletir a estratégia de teste escalonado, conforme mostrado através da equação (5.52) que expressa a relação entre as estratégias escalonada e seqüencial. O documento da NRC [35] apresenta tabelas com valores típicos de β para as bombas do SIS, o que comprova que, se o teste é do tipo escalonado, os valores de β para o SIS são de aproximadamente 0,05.

A Tabela 7.2 mostra os eventos básicos do SIS modificados para refletir a correção dos valores de β_P e β_O.

Tabela 7.2 - SIS – Correção dos valores das falhas de causa comum utilizados na APS

SIS Eventos Básicos[1] (Código Saphire)	**Descrição**	**Valores utilizados na APS**	**Valores para refletir o teste escalonado**
HPPP12CS	Falha de causa comum na partida das bombas A e B	1,2E-04	6,0E-05
HRPP12CR	Falha de causa comum na operação das bombas A e B	3,0E-06	1,5E-06

Para refletir a MC da bomba A do SIS, os dados de entrada devem ser modificados de acordo com a expressão (5.29), e com a Tabela 6.1

A Tabela 7.3 mostra, então, os eventos básicos que devem ser modificados no SAPHIRE para refletir a MC de uma bomba já com a correção dos valores de β_P e β_O.

[1]A primeira coluna nesta tabela e nas subseqüentes similares, se refere à codificação para os dados de entrada do código SAPHIRE [8] dos diversos modos de falha das bombas dos respectivos sistemas em análise.

Tabela 7.3 - SIS - Simulação da falha da bomba A (MC)

SIS Eventos Básicos (Código Saphire)	**Descrição**	**Valores Modificados para a simulação de MC**
HPPP1FS	Bomba A falha na partida	$Q_{AP} = 1$ *(true)*
HPPP2FS	Bomba B falha na partida	Não modifica
HPPP12CS	Falha de causa comum na partida das bombas A e B	$Q_{CCP} = \beta_P = 0{,}05$
HRPP1FR	Bomba A falha na operação	$Q_{AO} = 1$ (*true)*
HRPP2FR	Bomba B falha na operação	Não modifica
HRPP12CR	Falha de causa comum na operação das bombas A e B	$Q_{CCO} = \beta_O = 0{,}05$
HPTRAINATM	Trem A em manutenção	$Q_{ATM} = 1$ (*true)*
HPTRAINBTM	Trem B em manutenção	$Q_{BTM} = 0$ (*false*)

Conforme descrito na Seção 5.2, o risco de evento simples, r, e o risco anual médio, R, são expressos, respectivamente, pelas equações (5.3) e (5.4):

$$r = (FDN_1 - FDN_B) \cdot d$$

$$R = f \cdot (FDN_1 - FDN_B) \cdot d$$

onde,

f = freqüência anual de o componente entrar no TPI, ou de se encontrar indisponível para manutenção;

FDN_1 = freqüência de dano ao núcleo, calculada com o componente indisponível, ou seja, com o valor para a indisponibilidade do componente alterado para o valor 1 (um ou *true*);

FDN_B = freqüência de dano ao núcleo como calculada originalmente na APS, considerando-se que não ocorreram falhas, e que nenhum sistema tenha sido isolado para teste e/ou manutenção;

d = período ou tempo em que o componente se encontra indisponível

O valor esperado para o número de falhas e, conseqüentemente, número de ocorrências de MC, pode ser estimado através do processo de Poisson [30]. O número de eventos em um intervalo de tempo t, obedece à distribuição com média λt , onde λ é a taxa de falha do componente.

Portanto, os valores para as variáveis citadas acima, necessários para o cálculo do risco associado à falha de uma bomba do SIS são, então, conhecidos ou podem ser calculados.

Procedendo a simulação no SAPHIRE dos dados apresentados na Tabela 7.3, obtemos o valor para FDN_1, como mostra a Tabela 7.4.

Tabela 7.4 - SIS – Valores de riscos e da variação da FDN para a simulação de extensão de TPI

r	R (ano^{-1})	ΔFDN (ano^{-1})	FDN_1(ano^{-1})	f (ano^{-1})	d (ano)
5,0 E-07	1,28E-07	2,6E-05	6,6E-05	0,26	1,9E-02

Algumas observações são relevantes para uma melhor compreensão da análise em questão:

1) Taxa de falha da bomba A do SIS, conforme utilizada para os cálculos na APS de Angra 1, revisão 2f: λ=3,0E-05/h;

2) Freqüência de dano ao núcleo calculada na APS de Angra 1, revisão 2f: FDN_B = 4,015E-05/ ano

O valor obtido para **Δ**FDN, 2,6E-05, é maior do que o critério para aceitação.

A contribuição de evento simples, 5,0E-07, causada pela extensão do TPI do SIS para 168 h, tem valor igual ao critério r_c .

Considerando-se que os dois critérios, incremento de FDN e contribuição de evento simples, devem ser satisfeitos para que a extensão seja permitida, com base em análise de risco, pode-se concluir que a extensão de TPI para o período de 168 horas para o SIS não é aceitável sem a introdução de medidas compensatórias.

A medida compensatória para o caso da extensão do TPI do SIS é o teste do trem redundante (trem B), antes do trem A entrar no período de manutenção, cujos cálculos são apresentados na Seção 7.2.2.

7.2.2 SIS - Cálculos para a Simulação do Teste do Trem Redundante

O teste do trem redundante tem o efeito de simular a introdução de um novo intervalo de teste, menor do que o vigente, que, conseqüentemente, reduz as contribuições de falha na partida e de causa comum na partida da bomba testada, conforme mostrado na Tabela 6.3. Esse valor para o novo intervalo de teste é de 168 horas, justamente o período de duração proposto para o novo TPI. Isso acarreta uma redução para um quarto do valor original na contribuição de falha de causa comum na partida das bombas do SIS (de um mês para uma semana). A Tabela 7.5 mostra os valores a serem modificados para a simulação no SAPHIRE. Cabe ressaltar que os valores das falhas de causa comum na partida e na operação já se encontram corrigidos, dada a correção para os valores de β_P e β_O, conforme mostrado na Seção 5.5.2, através da expressão (5.52).

Tabela 7.5 - SIS - Simulação do teste do trem redundante

SIS Eventos Básicos (Código Saphire)	**Descrição**	**Valores modificados para a simulação do teste do trem redundante**
HPPP1FS	Bomba A falha na partida	$Q_{AP} = 1(true)$
HRPP1FR	Bomba A falha na operação	$Q_{AO} = 1(true)$
HPPP2FS	Bomba B falha na partida	$Q'_{BP} = Q_{BP}/4 = 1,2E-03/4 = 3,0E-04$
HPPP12CS	Falha de causa comum na partida das bombas A e B	$Q'_{CCP} = Q_{CCP}/4 = 6,0E\text{-}05/4 = 1,5E-05$
HRPP2FR	Bomba B falha na operação	Não modifica
HPTRAINATM	Trem A em manutenção	$Q_{ATM} = 1$ *(true)*
HPTRAINBTM	Trem B em manutenção	$Q_{BTM} = 0$ *(false)*

A Tabela 7.6 mostra os resultados da simulação do teste do trem redundante para o SIS.

Tabela 7.6 - SIS - Resultados da simulação do teste do trem redundante

r	**R (ano^{-1})**	**ΔFDN (ano^{-1})**	**FDN$_1$(ano^{-1})**	**f (ano^{-1})**	**d (ano)**
2,0E-07	5,1E-08	1,0E-05	5,05E-05	0,26	1,9E-02

Com a simulação do teste do trem redundante, tanto o valor do incremento de FDN, como o de evento simples, diminuem, sendo que o valor de incremento da FDN se encontra no limite superior do critério de aceitação. Isso significa que apesar da implementação da medida compensatória “teste do trem B”, imediatamente antes da

entrada no período de TPI, outras medidas devem ser consideradas no processo de decisão regulatória baseado em risco, tais como disponibilidades de redundâncias de trens de outros sistemas de segurança para compensar esse aumento de risco.

7.2.3 Cálculos para a Simulação da Estratégia de Teste Escalonado

A introdução da estratégia de teste escalonado para compensar a extensão do intervalo de teste, como já discutido anteriormente, não é aplicável como medida compensatória para o caso do SIS, uma vez que os testes das bombas do SIS já são executados, na prática, de maneira escalonada.

7.2.4 SIS - Cálculos para a Simulação da Extensão do Intervalo de Teste

Conforme mostrado nas Seções 5.3 e 6.2, a extensão do intervalo de teste acarreta um aumento das indisponibilidades de falha na partida das bombas bem como da contribuição de falha de causa comum na partida.

Considerando-se que a proposta de extensão do IT é de três (3) meses, e que o intervalo de teste vigente para o SIS é de um (1) mês, as indisponibilidades das bombas sofrerão aumento de um fator de três, como está mostrado na Tabela 7.7. Cabe ressaltar que os valores das falhas de causa comum já se encontram corrigidos em função da divisão dos valores de β_P e β_O por um fator de dois, conforme mostrado na Tabela 7.2.

A Seção 6.2 mostra, utilizando as equações (6.1), (6.2) e (6.3) como devem ser substituídos os dados de entrada para refletir a extensão do IT.

Tabela 7.7 – SIS - Simulação de extensão de IT

SIS Eventos Básicos (Código Saphire)	Descrição	Valores Vigentes, IT = 1 mês	Valores para simular a extensão do IT para 3 meses
HPPP1FS	Bomba A falha na partida	Q_{AFP} =1,2E-03	$Q'_{AFP} = 3 \cdot Q_{AFP}$ =3,6E-03
HPPP2FS	Bomba B falha na partida	Q_{BFP} =1,2E-03	$Q'_{BFP} = 3 \cdot Q_{BFP}$ =3,6E-03
HPPP12CS	Falha de causa comum na partida das bombas A e B	Q_{CCP} = 6,0E-04	$Q'_{CCP} = 3 \cdot Q_{CCP}$ =1,8E-04

Com esses novos valores para as indisponibilidades das bombas do SIS, pode ser calculado o novo valor para a FDN, denominado FDN_1 e o valor da diferença em relação à FDN_B , denominado ΔFDN .

O resultado apresentado na Tabela 7.8 mostra que, do ponto de vista da análise de risco, a extensão do IT do SIS para três meses é aceitável sem a introdução de medidas compensatórias.

Tabela 7.8 - SIS – Variação da FDN devido à extensão do IT

SIS	ΔFDN (ano^{-1})	FDN_1 (ano^{-1})	FDN_B (ano^{-1})
Extensão de IT	2.0E-08 < 1,0E-06	4,017E-05	4,015E-05

7.3 Cálculos para Sistema de Água de Serviço (SAS)

O Apêndice A contém, em detalhes, as Funções, Descrição, Condições Limite de Operação, Exigências de Testes bem como, Considerações de Engenharia relativas ao SAS.

7.3.1 SAS - Cálculos para a Simulação de Manutenção Corretiva

A APS de Angra 1 adota para a modelagem de falhas de causa comum o modelo de MLG, e o SAS é um sistema de três bombas pertencentes ao mesmo grupo de causa comum com estratégia de teste vigente do tipo seqüencial. Uma bomba do SAS é suficiente para garantir a operação do sistema, ou seja, o SAS é um sistema do tipo "um de três". Para fins de cálculo, neste trabalho é adotada a aproximação descrita na Seção 5.4.4.1.

A modelagem do SAS na APS de Angra 1 considera a bomba A operando continuamente (em operação normal ou em condições de acidente), ou seja, não são consideradas as falhas do tipo "bomba A falha na partida". Portanto, como apresentado na Seção 5.4.4.1, para a simulação de falha de uma das bombas, por exemplo, a bomba do trem A, as falhas independentes devem ser substituídas por *true* $(P[A_I] = 1)$, as falhas de causa comum na operação das bombas A, B e C, duas a duas, devem ser substituídas por *false* e as falhas de causa comum das três bombas na operação devem ser substituídas por $\beta\gamma$ conforme mostrado nas equações (5.41), (5.42) e (5.43).

Os valores de β e γ utilizados na APS de Angra 1 são:

$\beta_P = 0{,}032$

$\beta_O = 0{,}032$

$\gamma = 0{,}63$

$\beta \cdot \gamma = 0{,}02$

Tabela 7.9 - SAS - Simulação da falha da bomba A (MC)

SAS Eventos Básicos (Código Saphire)	**Descrição**	**Valores Modificados para a simulação de MC**
SWPP1AFR	Bomba A falha na operação	*true*
SWPP1BFS	Bomba B falha na partida	Não modifica
SWPP1CFS	Bomba C falha na partida	Não modifica
SWPP1BFR	Bomba B falha na operação	Não modifica
SWPP1CFR	Bomba C falha na operação	Não modifica
SWPP1A1BCS	Falha de causa comum na partida das bombas A e B	*false*
SWPP1A1BCR	Falha de causa comum na operação das bombas A e B	*false*
SWPP1B1CCS	Falha de causa comum na partida das bombas B e C	*false*
SWPP1B1CCR	Falha de causa comum na operação das bombas B e C	*false*
SWPP1A1CCS	Falha de causa comum na partida das bombas A e C	*false*
SWPP1A1CCR	Falha de causa comum na operação das bombas A e C	*false*
SWPP1A1B1CCR	Falha de causa comum na operação das bombas A, B e C	$Q_3 \approx \beta\gamma = 2,0E-02$
SWPP1BTM	Trem B em manutenção	Não modifica
SWPP1CTM	Trem C em manutenção	Não modifica

O resultado obtido para o valor do impacto no risco para as modificações apresentadas na Tabela 7.9 está mostrado na Tabela 7.10.

Tabela 7.10 - SAS - Valores de riscos e da variação da FDN para a simulação de extensão de TPI

r	R (ano^{-1})	ΔFDN (ano^{-1})	FDN_1(ano^{-1})	f (ano^{-1})	d (ano)
2,9E-05	7,3E-06	1,54E-03	1,58E-03	0,25	1,9E-02

Algumas observações são relevantes para uma melhor compreensão da análise em questão:

1) Taxa de falha da bomba da bomba A do SAS, conforme utilizada para os cálculos na APS de Angra 1, revisão 2f: λ = 2,9E-05 / h;

2) Freqüência de dano ao núcleo calculada na APS de Angra 1, revisão 2f: FDN_B = 4,015E-05 / ano

O valor obtido para ΔFDN, 1,54E-03, é maior do que o critério de aceitação para incremento de FDN.

A contribuição de evento simples, 2,9E-05, causada pela extensão do TPI do SAS para 168 h, é maior do que o critério, r_c = 5,0E-07.

Considerando-se que os dois critérios, incremento de FDN e contribuição de evento simples devem ser satisfeitos para que a extensão seja permitida, com base em análise de risco, pode-se concluir que a extensão de TPI para o período de 168 horas para o SAS não é aceitável sem a introdução de medidas compensatórias.

7.3.2 SAS - Cálculos para a Simulação do Teste dos Trens Redundantes

Conforme já citado na Seção 7.2.2, que trata do SIS, o teste do trem redundante tem o efeito de simular a introdução de um novo intervalo de teste, menor do que o vigente, que, conseqüentemente, reduz as contribuições de falha na partida e de causa comum na partida. Esse valor para o novo intervalo de teste é de 168 horas, justamente o período de duração proposto para o novo TPI. Isso acarreta uma redução para um quarto do valor original na contribuição de falha de causa comum na partida das bombas

do SAS (de um mês para uma semana). As equações (5.49) e (5.50) mostram como devem ser modificados os dados de entrada para refletir o teste dos trens redundantes.

Portanto, no caso do SAS, a simulação dos testes dos trens redundantes consta da modificação dos valores de falha na partida e de falha de causa comum na partida dos trens B e C, além de algumas modificações nas contribuições devido à manutenção das bombas B e C. Para tal, a Tabela 7.11 mostra os eventos básicos que devem ser modificados e seus novos valores correspondentes.

Tabela 7.11 - SAS – Simulação do teste das bombas redundantes

SAS Eventos Básicos (Código Saphire)	**Descrição**	**Valores modificados para a simulação do teste dos trens redundantes**
SWPP1AFR	Bomba A falha na operação	*true*
SWPP1BFS	Bomba B falha na partida	$Q'_{BP} = Q_{BP}/4 = 3,6E-04/4 = 9,0E-05$
SWPP1CFS	Bomba C falha na partida	$Q'_{CP} = Q_{CP}/4 = 3,6E-04/4 = 9,0E-05$
SWPP1A1BCS	Falha de causa comum na partida das bombas A e B	$Q'_{CCABP} = Q_{CCABP}/4 = 2,1E-06/4 = 5,3E-07$
SWPP1B1CCS	Falha de causa comum na partida das bombas B e C	$Q'_{CCBCP} = Q_{CCBCP}/4 = 2,1E-06/4 = 5,3E-07$
SWPP1A1CCS	Falha de causa comum na partida das bombas A e C	$Q'_{CCACP} = Q_{CCACP}/4 = 2,1E-06/4 = 5,3E-07$
SWPP1A1B1CCS	Falha de causa comum na partida das bombas A, B e C	$Q'_{CCABCP} = Q_{CCABCP}/4 = 7,3E-06/4 = 1,82E-06$
SWPP1BTM	Trem B em manutenção	*false*
SWPP1CTM	Trem C em manutenção	*false*

O valor da FDN_1 = 3,82E-05 obtido como resultado para as modificações apresentadas na Tabela 7.11 é menor do que o valor da FDN_B = 4,01E-05 *(baseline).*

Com base em um dos itens dos critérios de aceitação de risco, apresentados na Seção 4.5, que diz, "Caso a aplicação possa mostrar, claramente, um decréscimo na FDN, a mudança é considerada satisfatória de acordo com o princípio de regulamentação baseada em risco", pode-se concluir que a medida compensatória, teste das bombas redundantes do SAS, é suficiente para permitir, com base em análise de risco, a extensão de TPI para 168 horas (uma semana).

Considerando-se que os testes dos trens redundantes do SAS já são suficientes como medidas compensatórias para o aumento do TPI, na análise individual do SAS, não é necessária a introdução da outra medida, ou seja, estratégia de teste do tipo escalonado para compensar o aumento do risco causado pela extensão do TPI. Entretanto, essa medida compensatória pode ser usada para compensar a extensão de IT como será mostrado na Seção 7.3.3.

7.3.3 SAS - Cálculos para a Simulação da Extensão do Intervalo de Teste

O teste das três bombas do SAS é realizado mensalmente. As modificações necessárias nos eventos básicos para simular a extensão do intervalo de teste do SAS para três meses são mostradas na Tabela 7.12.

A Seção 6.2 mostra, utilizando as equações (6.1), (6.2) e (6.3) como devem ser substituídos os dados de entrada para refletir a extensão do IT.

Tabela 7.12 - SAS – Simulação da extensão do IT

SAS Eventos Básicos (Código Saphire)	Descrição	Probabilidades de falhas das bombas	Probabilidades de falhas das bombas com extensão de IT
SWPP1BFS	Bomba B falha na partida	$Q_{BFP} = 3,6E-04$	$Q'_{BFP} = 3.Q_{BFP} = = 1,1E-03$
SWPP1CFS	Bomba C falha na partida	$Q_{CFP} = 3,6E-04$	$Q'_{CFP} = 3.Q_{CFP} = = 1,1E-03$
SWPP1A1BCS	Falha de causa comum na partida das bombas A e B	$Q_{CCABP} = 2,1E-06$	$Q'_{CCABP} = 3.Q_{CCABP} = = 6,3E-06$
SWPP1A1CCS	Falha de causa comum na partida das bombas A e C	$Q_{CCACP} = 2,1E-06$	$Q'_{CCACP} = 3.Q_{CCACP} = = 6,3E-06$
SWPP1B1CCS	Falha de causa comum na partida das bombas B e C	$Q_{CCBCP} = 2,1E-06$	$Q'_{CCBCP} = 3.Q_{CCBCP} = = 6,3E-06$
SWPP1A1B1CCS	Falha de causa comum na partida das bombas A, B e C	$Q_{CCABCP} = 7,3E-06$	$Q'_{CCABCP} = 3.Q_{CCABCP} = = 2,2E-05$

Os resultados obtidos para a simulação da extensão do intervalo de teste para o SAS estão mostrados na Tabela 7.13

Tabela 7.13 - SAS – Variação da FDN devido à extensão do IT

SAS	ΔFDN (ano^{-1})	FDN_1 (ano^{-1})	FDN_B (ano^{-1})
Extensão de IT	1,0E-06 < 2,6E-06 < 1,0E-05	4,27E-05	4,01E-05

O valor do risco obtido para a simulação de extensão do IT é maior do que o critério de aceitação sem restrições, ou seja, quando o incremento de FDN é menor do que 1,0E-06. Contudo, como o valor da FDN para a APS de Angra 1 é menor do que 1,0E-04, incrementos de FDN entre os valores de 1,0E-06 e 1,0E-05, conforme apresentado na Seção 4.5, são permitidos.

Entretanto, para que a aceitação do incremento de FDN seja sem restrição, pode-se fazer uso da medida compensatória da mudança de tipo de estratégia de teste de seqüencial para escalonado que será mostrado a seguir.

7.3.4 SAS - Cálculos para a Simulação da Estratégia de Teste Escalonado

A simulação da estratégia de teste escalonado consta da aplicação da modificação das probabilidades de eventos básicos relativos às falhas de causa comum de acordo com a abordagem de metodologia e de simulação dos cálculos, conforme apresentados nas Seções 5.5.2 e 6.3.2, respectivamente. As equações (5.53) e (5.54) são utilizadas para a simulação da modificação de estratégia de teste.

A Tabela 7.14 mostra as modificações necessárias nos eventos básicos para refletir a introdução da estratégia de teste escalonado.

Tabela 7.14 – SAS - Estratégia de teste escalonado

SAS Eventos Básicos (Código Saphire)	Descrição	Probabilidades de falhas das bombas	Probabilidades de falhas com extensão de IT e teste escalonado
SWPP1BFS	Bomba B falha na partida	$Q_{BFP} = 3,6E-04$	$Q'_{BFP} = 3.Q_{BFP} = = 1,1E-03$
SWPP1CFS	Bomba C falha na partida	$Q_{CFP} = 3,6E-04$	$Q'_{CFP} = 3.Q_{CFP} = = 1,1E-03$
SWPP1A1BCS	Falha de causa comum na partida das bombas A e B	$Q_{CCABP} = 2,1E-06$	$Q'_{CCABP} = {3.Q_{CCABP}}/{2} = = 3,2E-06$
SWPP1A1CCS	Falha de causa comum na partida das bombas A e C	$Q_{CCACP} = 2,1E-06$	$Q'_{CCACP} = {3.Q_{CCACP}}/{2} = = 3,2E-06$
SWPP1B1CCS	Falha de causa comum na partida das bombas B e C	$Q_{CCBCP} = 2,1E-06$	$Q'_{CCBCP} = {3.Q_{CCBCP}}/{2} = = 3,2E-06$
SWPP1A1B1CCS	Falha de causa comum na partida das bombas A, B e C	$Q_{CCABCP} = 7,3E-06$	$Q'_{CCABP} = {3.Q_{CCABP}}/{3} = = 7,3E-06$

Os resultados para a introdução da estratégia de teste escalonado, como medida compensatória para a extensão de intervalo de teste para o SAS, estão apresentados na Tabela 7.15.

Tabela 7.15 – SAS – Variação da FDN com a introdução do teste escalonado

SAS	ΔFDN (ano^{-1})	FDN_1 (ano^{-1})	FDN_B (ano^{-1})
Estratégia de Teste escalonado	2,0E-07 < 1,0E-06	4,03E-05	4,01E-05

O valor 2,0E-07, obtido para a ΔFDN para refletir a introdução do teste escalonado com a extensão do IT é menor do que o critério 1,0E-06. Com isso, pode-se concluir que a estratégia de teste escalonado para o SAS compensa o risco acrescido pela extensão do intervalo de teste. Desta forma, a extensão de IT para o SAS é permitida dentro dos critérios de aceitação, com base em risco.

7.4 Cálculos para o Sistema Auxiliar de Água de Alimentação (SAAA)

O Apêndice A contém, em detalhes, as Funções, Descrição, Condições Limite de Operação, Exigências de Testes bem como, as Considerações de Engenharia relativas ao SAAA.

Conforme descrito no Apêndice A, o SAAA é composto de duas bombas motorizadas e uma bomba turbinada. Entretanto, somente as bombas motorizadas podem ser incluídas em um mesmo grupo de causa comum, uma vez que a bomba turbinada não possui redundância similar sendo incluída no projeto para assegurar a diversificação tanto de projeto, como de alimentação elétrica (para possibilitar o funcionamento do SAAA durante a condição de *blackout* [1].

7.4.1 SAAA - Cálculos para a Simulação da Manutenção Corretiva

O primeiro passo para a simulação da extensão de TPI consta dos cálculos a serem efetuados para o SAAA para a simulação de Manutenção Corretiva (MC) no Trem A das bombas motorizadas, como está mostrado na Tabela 7.16. A expressão (5.29) é utilizada para refletir a falha da bomba A e a modificação da falha de causa comum das duas bombas. A Tabela 6.1 mostra a modificação dos dados de entrada para o cálculo da MC.

Pode-se obter os valores de β_P e de β_O para as bombas motorizadas do SAAA na Seção 4.2 da APS de Angra 1 [5]:

- Falha de causa comum na partida: $\beta_P = 0{,}021$

- Falha de causa comum na operação: $\beta_O = 0{,}021$

Entretanto, como já citado anteriormente para o caso do SIS, na APS de Angra-1, os cálculos dos fatores β_P (partida) e β_O (operação) para o SAAA não consideraram a estratégia de teste escalonado, já implementada na operação da central. A correção desses valores diminui o valor final da FDN, enquanto que a simulação da MC aumenta a FDN. Para refletir a estratégia de teste escalonado vigente, os valores de β_P e β_O devem ser divididos por um fator de dois, conforme mostrado na Seção 5.5.2, equação (5.52).

A Tabela 7.16 mostra os eventos básicos do SAAA modificados para refletir a correção dos valores de β_P e β_O, que devem ser divididos por um fator de dois.

Tabela 7.16 - SAAA – Correção dos valores das falhas de causa comum utilizados na APS

SAAA Eventos Básicos (Código Saphire)	**Descrição**	**Valores utilizados na APS**	**Valores para refletir o teste escalonado**
AFPP1A1BCS	Falha de causa comum na partida das bombas motorizadas A e B	1,0E-05	5,0E-06
AFPP1A1BCR	Falha de causa comum na operação das bombas motorizadas A e B	2,1E-06	1,05E-06

A Tabela 7.17 mostra, então, os eventos básicos que devem ser modificados no SAPHIRE para refletir a MC de um trem já com a correção dos valores de β_P e β_O.

Tabela 7.17 - SAAA - Simulação da falha da Bomba A motorizada (MC)

SAAA Eventos Básicos (Código Saphire)	**Descrição**	**Valores modificados para a simulação de MC**
AFPP1AFS	Bomba A falha na partida	$Q_{AP} = 1(true)$
AFPP1BFS	Bomba B falha na partida	Não modifica
AFPP1A1BCS	Falha de causa comum na partida das bombas A e B	$Q_{CCP} = \beta_P = 0{,}01$
AFPP1AFR	Bomba A falha na operação	$Q_{AO} = 1(true)$
AFPP1BFR	Bomba B falha na operação	Não modifica
AFPP1A1BCR	Falha de causa comum na operação das bombas A e B	$Q_{CCO} = \beta_O = 0{,}01$
AFPP1ATM	Trem A em manutenção	$Q_{ATM} = 1(true)$
AFPP1BTM	Trem B em manutenção	$Q_{BTM} = 0$ *(false)*

Os resultados obtidos para os valores dos impactos no risco para as modificações apresentadas na Tabela 7.17 estão mostrados na Tabela 7.18.

Tabela 7.18 - SAAA - Valores de riscos e da variação da FDN para a simulação de extensão de TPI

r	**R (ano^{-1})**	**ΔFDN (ano^{-1})**	**FDN$_1$(ano^{-1})**	**f (ano^{-1})**	**d (ano)**
5,7E-06	5,0E-06	3,0E-04	3,4E-04	0.88	1,9E-02

Algumas observações são relevantes para melhor compreensão da análise em questão:

1) Taxa de falha da bomba A do SAAA, conforme utilizada para os cálculos na APS de Angra 1, revisão 2f: λ = 1,0E-04 / h;

2) Freqüência de dano ao núcleo calculada na APS de Angra 1, revisão 2f: FDN_B = 4,015E-05 / ano.

O incremento de FDN, 3,0E-04, não é aceitável sem a introdução de medidas compensatórias.

O valor de risco de evento simples obtido, 5,7E-06, é maior do que o valor do critério de aceitação, r_c = 5,0E-07.

A introdução da medida compensatória teste do trem redundante é recomendada, e a redução do impacto no risco deve ser avaliada para se verificar se o mesmo é suficiente para compensar o incremento causado pela extensão do TPI.

7.4.2 SAAA - Cálculos para a Simulação do Teste do Trem Redundante

O teste do trem redundante tem o efeito de simular a introdução de um novo intervalo de teste, menor do que o vigente, que, conseqüentemente, reduz as contribuições de falha na partida e de causa comum na partida. Esse valor para o novo intervalo de teste é de 168 horas, justamente o período de duração proposto para o novo TPI. Isso acarreta uma redução para um quarto do valor original na contribuição de falha na partida das bombas e de falhas de causa comum na partida das bombas motorizadas do SAAA (de um mês para uma semana). A Tabela 6.3 mostra como os dados de entrada devem ser modificados para refletir o teste do trem redundante.

A Tabela 7.19 mostra os valores a serem modificados para a simulação no SAPHIRE do teste do trem redundante da bomba motorizada. A Tabela 7.19 incorpora as correções dos valores de β_P e β_O, conforme mostrado na Tabela 7.16.

Tabela 7.19 - SAAA - Simulação do teste do trem redundante da bomba motorizada

SAAA Eventos Básicos (Código Saphire)	Descrição	Valores modificados para a simulação do teste do trem redundante
AFPP1AFS	Bomba A falha na partida	$Q_{AP} = 1 (true)$
AFPP1AFR	Bomba A falha na operação	$Q_{AO} = 1 (true)$
AFPP1BFS	Bomba B falha na partida	$Q'_{BP} = Q_{BP}/4 = 4,9E-04/4 = 1,22E-04$
AFPP1A1BCS	Falha de causa comum na partida das bombas A e B	$Q'_{CCP} = Q_{CCP}/4 = 5,0E-06/4 = 1,25E-06$
AFPP1BFR	Bomba B falha na operação	Não modifica
AFPP1ATM	Trem A em manutenção	$Q_{ATM} = 1$ *(true)*
AFPP1BTM	Trem B em manutenção	$Q_{BTM} = 0$ *(false)*

A Tabela 7.20 mostra os resultados da simulação do teste do trem redundante da bomba motorizada do SAAA.

Tabela 7.20 - SAAA - Resultados da simulação do teste do trem redundante da bomba motorizada

r	R (ano^{-1})	ΔFDN (ano^{-1})	FDN_1(ano^{-1})	f (ano^{-1})	d (ano)
5,0E-06	4,4E-06	2,63E-04	3,03E-04	0,88	1,9E-02

Os valores calculados para os riscos associados à configuração do teste do trem redundante B indicaram que essa medida compensatória não é suficiente para compensar o aumento do TPI, uma vez que tanto o incremento de FDN como o valor para o risco de evento simples não atendem aos critérios estabelecidos, conforme apresentado na Seção 5.2. Entretanto, pode-se, ainda, simular o teste da bomba turbinada AF-2, antes do início do TPI como uma medida compensatória adicional. Apesar da bomba turbinada não pertencer ao grupo de falhas de causa comum, o teste adicional da mesma contribui para uma redução do risco total.

De maneira similar aos testes de trens redundantes apresentados anteriormente, o teste da AF-2 tem o efeito de simular a introdução de um novo intervalo de teste na mesma, menor do que o vigente, que, conseqüentemente, reduz a sua contribuição de falha na partida. Deve ser enfatizado que, diferentemente do teste do trem redundante da bomba motorizada, o teste da AF-2 não promove redução em falhas de causa comum na partida, pelo fato da mesma não pertencer a grupos de causa comum. Esse valor para o novo intervalo de teste é de 168 horas, justamente o período de duração proposto para o novo TPI. Isso acarreta uma redução para um quarto do valor original na contribuição de falha na partida da AF-2 (de um mês para uma semana).

A Tabela 7.21 apresenta os valores de eventos básicos modificados para a simulação do teste adicional da bomba turbinada AF-2 através do SAPHIRE.

Tabela 7.21 - SAAA- Teste do trem redundante B e da bomba turbinada AF-2

SAAA Eventos Básicos (Código Saphire)	**Descrição**	**Valores modificados para a simulação do teste do trem B e da AF-2**
AFPP1AFS	Bomba A falha na partida	$Q_{AP} = 1(true)$
AFPP1AFR	Bomba A falha na operação	$Q_{AO} = 1(true)$
AFPP1BFS	Bomba B falha na partida	$Q'_{BP} = Q_{BP}/4 = 4,9E-04/4 = 1,22E-04$
AFPP1A1BCS	Falha de causa comum na partida das bombas A e B	$Q'_{CCP} = Q_{CCP}/4 = 5,0E\text{-}06/4 = 1,25E-06$
AFPP1BFR	Bomba B falha na operação	Não modifica
AFPP1ATM	Trem A em manutenção	$Q_{ATM} = 1$ (*true)*
AFPP1BTM	Trem B em manutenção	$Q_{BTM} = 0$ *(false)*
AFPP2FS	Bomba turbinada AF-2 falha na partida	$Q'_{AFP} = Q_{AFP}/4 = 7,2E-03/4 = 1,8E-03$
AFPP2TM	Bomba turbinada AF-2 em manutenção	$Q_{AF2TM} = 0$ (*false*)

O resultado da simulação da Tabela 7.21 é o novo valor de FDN_1, como mostra a Tabela 7.22.

Tabela 7.22 - SAAA - Resultados da simulação do teste do trem redundante incluindo o teste da bomba turbinada AF-2

r	R	ΔFDN (ano^{-1})	FDN_1(ano^{-1})	f (ano^{-1})	d (ano)
4,6E-06	4,0E-06	2,42E-04	2,82E-04	0,88	1,9E-02

Os valores calculados para os riscos associados à configuração que inclui os testes do trem redundante B e da AF-2 indicaram que essa medida compensatória não é suficiente para compensar o aumento do TPI, uma vez que tanto o incremento de FDN como o valor para o risco de evento simples, r, não atendem aos critérios estabelecidos, conforme apresentados na Seção 5.2. Portanto, dentro do escopo deste trabalho, a extensão do TPI para o SAAA não deve ser permitida.

7.4.3 SAAA - Cálculos para a Simulação da Estratégia de Teste Escalonado

A introdução da estratégia de teste escalonado para compensar a extensão do intervalo de teste, como já discutido anteriormente, não é aplicável para o caso do SAAA, uma vez que os testes das bombas motorizadas deste sistema, assim como para as bombas do SIS, também, já são executados, na prática, de maneira escalonada.

7.4.4 SAAA - Cálculos para a Simulação da Extensão do Intervalo de Teste

A extensão do intervalo de teste para o SAAA acarreta um aumento das indisponibilidades de falha na partida e falha de causa comum na partida das bombas motorizadas, bem como um aumento na falha na partida da bomba turbinada.

Considerando-se que a proposta de extensão do IT é de três meses, e que o intervalo de teste vigente para o SAAA é de um (1) mês, as indisponibilidades de falha na partida e de causa comum na partida das bombas sofrerão aumento de um fator de três, como está mostrado na Tabela 7.23.

A Tabela 6.2 mostra através da utilização das equações (6.1), (6.2) e (6.3), como devem ser substituídos os dados de entrada para refletir a extensão do IT.

Tabela 7.23 - SAAA - Simulação de extensão de IT

SAAA Eventos Básicos (Código Saphire)	**Descrição**	**Valores Vigentes, IT=1 mês**	**Valores para simular extensão do IT = 3 meses**
AFPP1AFS	Bomba A falha na partida	$Q_{AFP} = 4,9E-04$	$Q'_{AFP} = 3 \cdot Q_{AFP} = 1,47E-03$
AFPP1BFS	Bomba B falha na partida	$Q_{BFP} = 4,9E-04$	$Q'_{BFP} = 3 \cdot Q_{BFP} = 1,47E-03$
AFPP1A1BCS	Falha de causa comum na partida das bombas A e B	$Q_{CCP} = 1,0E-05$	$Q'_{CCP} = 3 \cdot Q_{CCP} = 3,0E-05$
AFPP2FS	Bomba Turbinada AF-2 falha na partida	$Q_{AF2P} = 7,2E-03$	$Q'_{AF2P} = 3.Q_{AF2P} = 2,16E-02$

Os valores calculados para o incremento de FDN e os valores de risco simples e anual estão apresentados na Tabela 7.24.

Tabela 7.24 - SAAA – Variação da FDN devido à extensão do IT

SAAA	**ΔFDN (ano^{-1})**	**FDN$_1$ (ano^{-1})**	**FDN$_B$ (ano^{-1})**
Extensão de IT	1,0E-06 < 1,4E06 < 1,0E-05	4,15E-05	4,015E-05

Observando-se os resultados apresentados na Tabela 7.24 pode-se concluir que a extensão do intervalo de teste do SAAA para três meses pode ser permitida, pois a variação da FDN encontra-se no intervalo entre 1,0E-06 e 1,0E-05 e a FDN$_B$ < 1,0E-04.

Cabe ressaltar que a medida compensatória para este incremento no risco seria o estabelecimento da estratégia de teste escalonado o que, de fato, já é prática da operação do SAAA em Angra 1.

7.5 Combinações de extensões de TPI e de IT simultâneas

As seções 7.2, 7.3 e 7.4 apresentam os cálculos e os resultados para as extensões de TPI e de IT para os sistemas SIS, SAS e SAAA, respectivamente. Como pode ser facilmente observado, as extensões foram calculadas de forma individual e independente umas das outras entre sistemas. Entretanto, a realidade operacional de uma usina nuclear vivencia uma variação constante em sua configuração, onde componentes de trens de sistemas de segurança que se encontravam indisponíveis voltam à condição de operáveis ao mesmo tempo em que outros que estavam operáveis entram em TPI, por MP, MC ou por testes que durante sua execução o tornem indisponíveis.

A configuração da planta pode ser definida através das condições dos sistemas e das funções de segurança que, por sua vez, dependem das condições de seus componentes [36].

Dessa forma, quando múltiplas modificações de ET se fazem necessárias, deve ser avaliado.o impacto de risco coletivo que abranja todas as modificações

Apesar de um estudo de controle de configuração da planta não fazer parte do escopo deste trabalho, é interessante analisar o comportamento do risco quando se propõe a extensão de TPI ou de IT para dois sistemas simultaneamente.

A partir dos resultados obtidos nas Seções 7.2, 7.3 e 7.4 pode-se montar a Tabela 7.25.

Tabela 7.25 – Resultados das extensões de TPI e de IT

Sistema	Extensão de TPI para 168h sem Medida Compensatória	Extensão de TPI para 168h com Medida Compensatória	Extensão de IT para 3 meses sem Medida Compensatória	Extensão de IT para 3 meses com Medida Compensatória
SIS	NÃO	SIM (c/ restrição)	SIM (s/ restrição)	Não Aplicável
SAS	NÃO	SIM (s/ restrição)	SIM (c/ restrição)	SIM (s/restrição)
SAAA	NÃO	NÃO	SIM (c/ restrição)	Não Aplicável

Na Tabela 7.25, o termo "sem restrição" é aplicado quando o valor calculado para o incremento da FDN introduzido pelas extensões de TPI e de IT para os sistemas em questão é menor do que 1,0E-06. Caso o incremento da FDN se situe entre 1,0E-06 e 1,0E-05 é empregado o termo "com restrição", uma vez que, nesse caso, a condição de aceitação do risco depende do valor total da FDN (para Angra 1, FDN_B = 4,01E-05).

Com base nos resultados apresentados na Tabela 7.25, conclui-se que a combinação de extensões simultâneas de TPI e de IT para o SIS e o SAS pode ser simulada.

7.5.1 Extensões simultâneas de TPI para o SIS e o SAS

A primeira simulação a ser feita é a combinação das extensões de TPI para o SIS e o SAS. Como pode ser constatado nas Seções 7.2 e 7.3, as extensões de TPI tanto para o SIS, como para o SAS só são aceitáveis com a introdução de medidas compensatórias, no caso desses sistemas, o teste dos trens redundantes. Portanto, para a obtenção dos riscos de evento simples, anual e o incremento de FDN para o SIS e o SAS simultaneamente, o cálculo com o código SAPHIRE deve ser feito através da simulação dos dados de entrada das Tabelas 7.5 e 7.11, em conjunto. Os resultados dessa simulação estão mostrados na Tabela 7.26.

Cabe ressaltar que o valor da freqüência, na Tabela 7.26, representa a freqüência anual de ocorrência da configuração específica da planta, onde uma bomba do SIS e do SAS se encontram indisponíveis pelo período de uma semana. Tal configuração, sugerida para fins de aplicação de metodologia, é hipotética e não possui dados específicos para a planta quanto a sua freqüência de ocorrência. Por esse motivo, vamos adotar para a freqüência da configuração o maior valor entre as taxas de falhas das bombas do SIS e do SAS (utilizadas como freqüências para a avaliação dos TPI individuais). Nesse caso, $\lambda = 3,0\mathrm{E}-05/\mathrm{h}$.

Tabela 7.26 – Resultados das extensões simultâneas de TPI para o SIS e o SAS

r	R	ΔFDN (ano^{-1})	FDN_1(ano^{-1})	f (ano^{-1})	d (ano)
1,6E-07	4,2E-08	8,5E-06	4,86E-05	0,26	1,9E-02

O risco de evento simples, r, de valor 1,6E-07 é menor do que o critério r_c, de valor 5,0E-07, o que torna esta configuração aceitável.

Na Tabela 7.26, o valor do incremento de FDN se encontra entre 1,0E-05 e 1,0E-06. Considerando-se que a FDN total de Angra 1 é menor do que 1,0E-04, segundo o critério de aceitação da Seção 4.5, as extensões simultâneas de TPI do SIS e do SAS para 168h são aceitáveis com base em análise de risco.

7.5.2 Extensões simultâneas de IT para o SIS e o SAS

Com base nos resultados da Tabela 7.25, pode-se simular, também, as extensões simultâneas de IT, individualmente aceitas sem restrição para o SIS e com restrição para o SAS sem medida compensatória, porém sem restrição para o SAS com medida compensatória. Para tal são usados os dados de entrada para o SAPHIRE, modificados de acordo com as Tabelas 7.7 e 7.14. Cabe ressaltar que os dados contidos na Tabela 7.14 já incorporam a medida compensatória "teste escalonado" para o SAS.

Tabela 7.27 – Resultados das extensões simultâneas de IT para o SIS e o SAS

SIS e SAS	ΔFDN (ano^{-1})	FDN_1(ano^{-1})	FDN_B (ano^{-1})
Extensões de IT	2,0E-07	4,03E-05	4,01E-05

O valor do incremento da FDN, 2,0E-07, apresentado na Tabela 7.27 indica que, com base em análise de risco, são aceitáveis as extensões de IT para o SIS e o SAS simultaneamente. Os valores calculados individualmente para o incremento de FDN para as extensões de IT para o SIS e o SAS, conforme apresentados nas Tabelas 7.8 e 7.15, são respectivamente, 5,0E-08 e 2,0E-07. Observando-se os resultados apresentados nessa tabelas, conclui-se que a contribuição do incremento de risco atribuído à extensão de IT para o SIS é desprezível em relação à do SAS. Cabe ressaltar que, sem a introdução do teste escalonado para o SAS, as extensões de IT simultâneas para o SIS e o SAS não seriam aceitáveis.

7.5.3 Extensões simultâneas de TPI e de IT para o SIS

Outro cálculo importante a ser efetuado é o das extensões simultâneas de TPI e de IT para um mesmo sistema. Para o caso do SIS, a simulação é feita através da combinação dos dados das Tabelas 7.5 e 7.7. Entretanto, é importante que seja observado que essa simulação exige uma combinação de dados de entrada das Tabelas 7.5 e 7.7 modificados, onde o teste do trem redundante e a extensão do intervalo de teste sejam contemplados simultaneamente. A Tabela 7.28 apresenta como devem ser combinados esses dados de entrada.

Tabela 7.28 – SIS - Extensões simultâneas de TPI e de IT

SIS Eventos Básicos (Código Saphire)	**Descrição**	**Valores Modificados para extensão de IT e teste do trem B**
HPPP1FS	Bomba A falha na partida	$Q_{AP} = 1 (true)$
HRPP1FR	Bomba A falha na operação	$Q_{AO} = 1 (true)$
HPPP2FS	Bomba B falha na partida	$Q'_{BP} = \frac{3}{4} Q_{BP} = 9,0E-04$
HPPP12CS	Falha de causa comum na partida das bombas A e B	$Q'_{CCP} = \frac{3}{4} Q_{CCP} = 4,5E-05$
HRPP2FR	Bomba B falha na operação	Não modifica
HPTRAINATM	Trem A em manutenção	$Q_{ATM} = 1$ *(true)*
HPTRAINBTM	Trem B em manutenção	$Q_{BTM} = 0$ *(false)*

Os resultados obtidos para a simulação dos dados da Tabela 7.28 estão apresentados na Tabela 7.29.

Cabe ressaltar que, para a simulação da falha da extensão do TPI, é necessária a simulação da falha na partida do trem A com o valor *true* (indisponibilidade de falha da partida da bomba A = 1). Entretanto, a simulação da extensão de IT implica na modificação das falhas na partida das bombas para um valor três vezes maior (no caso de IT ser estendido de um mês para três meses). Deve ser observado que não importando o valor da extensão proposta de IT, quando combinada com extensão de TPI, o valor *true* para falha na partida da bomba A sobrepuja quaisquer valores possíveis para refletir a extensão do teste da bomba A.

Tabela 7.29 – SIS – Resultados para as extensões simultâneas de TPI e de IT

r	R	ΔFDN (ano^{-1})	FDN_1(ano^{-1})	f (ano^{-1})	d (ano)
2,0E-07	5,1E-08	1,0E-05	5.05E-05	0,26	1,9E-02

Na Tabela 7.29, o risco de evento simples, r, de valor 2,0E-07 é menor do que o critério r_c , de valor 5,0E-07, o que torna esta configuração, por esse aspecto, aceitável.

O valor do incremento de FDN calculado é o valor limite entre aceitação ou não, segundo os critérios estabelecidos na Seção 4.5, para centrais cujas FDN sejam menores que 1,0E-04. Em casos como esse, deve ainda ser acrescentada uma avaliação em relação às configurações dos demais sistemas de segurança quanto ao número de trens disponíveis.

8. CONCLUSÕES E RECOMENDAÇÕES

Os resultados obtidos nos cálculos deste trabalho mostram que, através do uso da APS como ferramenta e de métodos de aplicação de análise de risco, extensões de TPI e de IT de Especificações Técnicas são viáveis, sem incorrer em um aumento inaceitável do risco total da planta, com a implementação de medidas compensatórias.

A análise conjunta dos resultados obtidos neste trabalho, mostra como as extensões de TPI e de IT têm impactos distintos no risco total da planta. A partir da observação da Tabela 7.25 pode-se concluir que as extensões de TPI só são possíveis, dentro dos critérios de risco apresentados na Seção 4.5, quando medidas compensatórias, como o teste dos trens redundantes e/ou a modificação do tipo de estratégia de teste de seqüencial para escalonado, são implementadas. Ao contrário do TPI, o IT pode ser estendido sem a inclusão de medidas compensatórias, tanto para o SIS como para o SAS, como está mostrado na Tabela 7.25.

Outra observação importante diz respeito às diferenças entre os sistemas analisados quanto às suas respectivas contribuições para o impacto no risco total da planta, quando são simulados os mesmos valores de TPI e de IT. Enquanto o SIS e o SAS apresentam um impacto de risco aceitável para essas modificações de ET, a simulação da extensão de TPI para o SAAA resulta em incrementos de risco inaceitáveis, mesmo com a introdução de medidas compensatórias, conforme está mostrado na Tabela 7.25.

Deve ser enfatizado que decisões de modificações de ET, com base em risco, devem ser avaliadas conjuntamente com outras considerações tradicionais como, experiência operacional, lições aprendidas de modificações previamente realizadas, considerações práticas relativas a testes e manutenções [3, 31], ou seja, avaliações tradicionais de engenharia. A aceitação final de mudanças de ET propostas deve ser baseada em todas essas considerações e não somente no uso de resultados obtidos de APS e simplesmente comparados com critérios numéricos.

Apesar de um estudo completo de controle de configuração da planta [36] não fazer parte do escopo deste trabalho, a Seção 7.5 apresenta os cálculos relativos a ocorrências simultâneas de TPI e de IT para o SIS e o SAS. Além disso, foi simulado um exemplo de extensão simultânea de TPI e de IT para um mesmo sistema, no caso o

SIS. Essas simulações com modificações simultâneas em mais de um sistema ou mais de um item de ET no mesmo sistema, representam os primeiros passos na direção de um estudo de controle de configuração da planta.

Um Controle de Configuração da Planta baseado em risco deve ter a capacidade de desempenhar uma avaliação do impacto total no risco oriundo de configurações que reflitam as condições de manutenção ou indisponibilidade dos componentes. Além de permitir um planejamento, baseado em risco, das atividades de manutenção, tal controle visa coibir a ocorrência de configurações de risco inaceitável.

Conforme descritos na Seção 4.5, os critérios de risco utilizados neste trabalho são os adotados pela NRC [7, 24, 25]. Para a avaliação de ET foram estabelecidos dois tipos de critérios, o de incremento de FDN e o de risco simples.

A referência [36], bem como os próprios guias regulatórios da NRC, citam a necessidade do cálculo do risco médio anual, função da freqüência de ocorrência do TPI. O risco anual médio se torna mais relevante do que o risco de evento simples quando a freqüência anual de ocorrência do TPI é maior do que um.

Pelo fato do risco anual médio ser diretamente proporcional à freqüência de ocorrência do TPI, o mesmo pode assumir valores bastante distintos para MC e MP. A freqüência esperada de ocorrência de MC para um dado componente ou bomba, como já comentado no Capítulo 7, tem valor cuja ordem de grandeza varia, geralmente, entre 10^{-3} e 10^{-5}, enquanto que, para a MP, tal freqüência pode ser até algumas vezes maior do que um (1) [2]. Esses fatos explicam o não estabelecimento de um critério para o risco anual médio, até o presente. Em se tratando de um limite para o risco anual médio, a solução poderia estar no estabelecimento de dois critérios distintos para MC e MP respectivamente. Cabe ressaltar que, para fins deste trabalho, cujo escopo aborda apenas a MC, resultando em contribuições de risco de evento simples que sobrepujam, em todos os casos analisados, as contribuições para o risco anual médio, a inexistência de tal critério torna-se irrelevante.

Cabe, ainda, comentar que, segundo a NRC, os critérios estabelecidos para modificação de ET aplicam-se, somente, às modificações permanentes. Apesar disso, no guia regulatório da NRC [25] é mencionado que a freqüência de ocorrência de entrada de componentes em TPI é, normalmente, baixa e que um TPI tem caráter temporário por

natureza. Em vista disso, cabe a interpretação de que o critério de evento simples é, também, adequado à análise de modificação de ET temporária *(one-time)*. Entretanto, para pedidos de modificações temporárias de ET, o processo de decisão regulatória deve incluir informações complementares ao risco de evento simples, tais como, histórico de freqüência de ocorrência do componente, motivos que causaram o pedido de extensão, medidas compensatórias factíveis para diminuir o risco total**.** O risco anual médio deve ser controlado, no sentido de coibir um aumento da freqüência de ocorrência de pedidos de modificações temporárias de ET. Muitos pedidos de modificações temporárias de ET indicam a necessidade de modificações permanentes, avaliação detalhada das condições dos componentes dos sistemas de segurança e, possivelmente, de uma revisão geral da segurança da planta.

Como mostram os resultados deste trabalho, podem ser efetuadas extensões de TPI e de IT de componentes de sistemas de segurança importantes resultando em pequenos ou mesmo desprezíveis incrementos de risco. Extensões de TPI permitem um serviço adequado de manutenção e reparo de componentes, que por sua vez reduzem tanto a freqüência de ocorrência de TPI, como de desligamentos não planejados. Extensões de IT, em particular, podem ser implementadas com praticamente nenhuma contribuição significativa para a FDN, reduzindo substancialmente um fardo desnecessário da equipe de operação da planta na realização de um grande número de testes desnecessários, de tal modo que sua atenção possa ser concentrada em atividades mais relevantes em relação à segurança. A redução do número de testes também reduz o número de ocorrências de desligamentos não planejados, que resultam de transientes causados por testes.

Cabe ressaltar que os dados de falhas dos componentes que compõem o banco de dados de entrada da APS de Angra 1 utilizam valores pontuais médios para as indisponibilidades e taxas de falhas, obtendo como resultado para a FDN um valor também pontual, não contendo a elaboração de uma analise de incertezas. Entretanto, assim como em qualquer estudo baseado em risco, uma análise de modificação de ET pode ser afetada por vários tipos de incertezas relacionadas às hipóteses assumidas ao longo do desenvolvimento da modelagem da APS, bem como em suas aplicações. Incertezas relacionadas a parâmetros como taxas de falhas, envolvem dados oriundos de informações limitadas ou erros aleatórios na análise de sensibilidade.

A elaboração deste trabalho constitui um passo importante para as aplicações de métodos e cálculos de APS para a avaliação de ET de Angra1, incluindo a metodologia de cálculo para a introdução de medidas compensatórias de risco, o que consiste em um passo importante para a implementação de um controle de configuração da planta com base em risco [36]. Entretanto, o presente trabalho apresenta limitações de escopo que são indicações para o desenvolvimento de futuros estudos que enriqueçam e dêem continuidade ao mesmo.

A primeira recomendação para dar prosseguimento a este trabalho, consta da revisão geral das ET de Angra 1, para que as mesmas possam refletir as condições limites de operação e de vigilância balanceadas em relação ao risco total da planta. Para tal, a metodologia apresentada nesse trabalho pode ser utilizada para proceder às avaliações de TPI e de IT de todos os sistemas de segurança, calculando a contribuição de risco de cada sistema individualmente e conjuntamente, com vistas a sugerir modificações adequadas em relação ao risco. Isso resultaria na indicação de algumas modificações permanentes de TPI e de IT, tanto no sentido de estendê-los como no de restringí-los, em casos de TPI com valores de risco associado maiores do que os aceitáveis, de acordo com os critérios estabelecidos.

Entretanto, a experiência operacional indica a necessidade de avaliações temporárias de ET, seja para estender o TPI ou o IT, ou mesmo para o processo de decisão entre a continuação da operação ou o desligamento da planta, este último para que as ET não sejam violadas. Quando se tratam de avaliações temporárias de TPI e de ET, além das medidas compensatórias utilizadas neste trabalho, outras medidas podem ser incorporadas à análise, tais como ações abrangentes a todos os sistemas de segurança como, por exemplo, trazer de volta à operação um trem que se encontrava em manutenção para dar prioridade a outro trem de outro sistema que já se encontrava no TPI (extensão de TPI). Além disso, testes adicionais de trens de quaisquer sistemas de segurança contribuem para a redução de incrementos de risco, oriundos de indisponibilidades de componentes dos demais sistemas.

Quando se trata de modificação de ET, análises de sensibilidade podem ser necessárias para abordar a precisão das hipóteses importantes adotadas ao longo da elaboração do estudo, que funcionam como adjuntas às analises de incertezas. Entretanto, a experiência de análises de sensibilidades desenvolvidas para modificações

de ET com base em risco, mostra que os riscos associados às mesmas são relativamente insensíveis às incertezas, quando comparados com o efeito do risco de incertezas de hipóteses relativas às modificações de projeto ou de procedimentos de operação [25].

Apesar disso, consta das recomendações de aprimoramento deste trabalho a inclusão de uma análise de sensibilidade dos riscos associados aos componentes em questão. Tal análise pode ser feita através de medidas de importância de risco que podem ser relativas ou absolutas e que têm a finalidade de classificar a significância do componente ou sistema em relação ao risco em termos de suas contribuições para o risco total. As medidas de importância têm aplicação direta para o controle de configuração da planta para medir a significância do efeito da indisponibilidade do componente isolado para manutenção.

As medidas de importância mais utilizadas para avaliações de componentes de centrais nucleares e suas principais aplicações são [29]:

1) *Birnbaum* – Mede a taxa de variação do risco em função da variação da probabilidade do evento básico. É sensível à posição do componente na estrutura da árvore de falhas;

2) *Fussel-Vesely* – Indica a importância relativa do desempenho médio do componente no longo termo;

3) RRW *(Risk Reduction Worth)* – Expressa a variação no risco quando é garantido que o componente está disponível.

4) RAW *(Risk Achievement Worth)* - Expressa o aumento do risco quando o componente se encontra indisponível, por manutenção ou falho;

No que diz respeito às modificações de ET avaliadas neste trabalho, as medidas de importância mais adequadas para a realização de análises de sensibilidade são o RAW e *Birnbaum*, para as extensões de TPI e de IT, respectivamente.

Conforme mencionado anteriormente, este trabalho representa um passo importante na direção do controle de configuração da planta, que tem o objetivo de operar de maneira eficiente e efetiva a utilização dos recursos da planta, ou seja, os sistemas de segurança. Portanto, é desejável e recomendável o desenvolvimento de um

programa de controle de configuração em que os seguintes objetivos devam ser alcançados [36]:

- Gerenciamento da configuração dos componentes que estão simultaneamente indisponíveis;

- Gerenciamento dos componentes em reserva que estão operáveis;

- Gerenciamento do tempo de duração da existência da configuração (TPI);

- Gerenciamento da freqüência com a qual a configuração ocorre.

A metodologia de cálculo apresentada nesse trabalho incluindo medidas compensatórias e confrontação com os critérios de risco mostrados na Seção 4.5 constitui a ferramenta básica de cálculo para o gerenciamento dos objetivos apresentados acima. Além disso, as estratégias de controle de configuração envolvem o controle de níveis de risco e de contribuições de risco similares às definidas na Seção 4.5 e abordadas ao longo do desenvolvimento do presente estudo.

Mais uma recomendação para a continuidade deste trabalho é a inclusão de MP na análise de avaliação de TPI. Nesse caso é fundamental que exista um banco de dados específicos da experiência operacional da planta que faça a distinção precisa entre as indisponibilidades ocorridas devido à MP ou à MC para que se possa estimar a freqüência de ocorrência de MP, parâmetro indispensável ao cálculo da contribuição anual média para o risco total da planta. Para tal, é necessário que a coleta de dados operacionais da planta seja direcionada para fins de utilização em estudos de APS [40].

Por último, devem ser enfatizadas a preservação dos conceitos de defesa em profundidade e a observação das limitações de engenharia. De acordo com a Seção 4.5, os guias regulatórios de critérios numéricos [24, 25] são utilizados para garantir que quaisquer incrementos de risco estejam dentro dos limites aceitáveis. Entretanto, isso não exclui as considerações tradicionais, para o processo de decisão, que garantam que modificações satisfaçam as regras e os regulamentos vigentes. As considerações práticas julgam a aceitabilidade da implementação da modificação e as lições aprendidas da experiência operacional evitam a recorrência dos erros.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] ELETROBRÁS TERMONUCLEAR S. A. - ELETRONUCLEAR, **Relatório Final de Análise de Segurança (RFAS),** CNAAA, Angra 1, 1998.

[2] SAMANTA, P.K., KIM**,** I.S., MANKAMO, T., et al., **Handbook of Methods for risk based Analyses of Technical Specifications,** NUREG/CR-6141, 1994.

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, **Risk Informed Regulation of Nuclear Facilities: Overview of the Current Status,** IAEA-TECDOC-1436, Vienna, February, 2005.

[4] U. S. NRC, **Probabilistic Safety Analysis: Procedures Guide,** NUREG/CR – 2815, BNL-NUREG-51559, Washington, D. C., 1985.

[5] ELETROBRÁS TERMONUCLEAR S. A. - ELETRONUCLEAR, **Usina Nuclear de Angra 1: Análise Probabilística de Segurança (APS),** CNAAA, Rev. 2f, Novembro, 2006.

[6] CNEN, **Segurança na Operação de Usinas Nucleoelétricas,** CNEN -NE-1.26, Outubro, 1997.

[7] U. S. NRC, REGULATORY GUIDE 1.174, **An Approach for Using PSA in Risk-Informed Decisions on Plant-specific Changes to the Licensing Basis**, Rev .1, 2002.

[8] RUSSEL, K., D., et al, **Systems Analysis Programs for Hands-On Integrated Reliability Evaluations (SAPHIRE)**, U. S. Nuclear Regulatory Commission, NUREG/CR-6116, Washington D.C., 1998.

[9] U. S. NRC, 10CFR 50.36**, Technical Specifications**, Federal Register, 60 FR 36953, 1995.

[10] MARTORELL, S., SERRADELL, V., SAMANTA, P., **"**Improving Allowed Outage Time and Surveillance Test Interval Requirements: A Study of their Interactions using Probabilistic Methods"**, Reliability Engineering and System Safety**, v. 47, pp.119-129, 1995.

[11] VESELY, W. E., et al, **Risk–based Evaluation Technical Specifications**, EPRI NP-4317, Prepared by Battelle Columbus Division, Columbus, Ohio, December, 1985.

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, **Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1),** Safety Series No. 50-P-4, Vienna, 1992.

[13] MARTORELL, S., SERRADELL, G., SAMANTA, P., **Probabilistic Analysis of the Interaction Between Allowed Outage time and Surveillance Test Interval Requirements,** IAEA-TECDOC-737, "Technical Committee Meeting Report, Budapest, 1993.

[14] U. S. NRC**, Evaluation of Allowed Outage Times (AOTs) from a Risk and Reliability Standpoint,** NUREG/CR-5425, BNL, 1989.

[15] CEPIN, M., Mavko, B., **"**Probabilistic Safety Assessment Improves Surveillance Requirements in Technical Specifications**", Reliability Engineering and System Safety** v.56, pp.69-77, 1997.

[16] U. S. NRC, **Standard Technical Specifications,** Westinghouse Plants, NUREG-1431, Rev. 2, June, 2001.

[17] FLEMING, K.N., MURPHY, R. P., **Lessons Learned in Applying PSA Methods to Technical Specifications Optimization,** IAEA-TECDOC-737, Relatório do TCM ('Technical Committee Meeting), Budapest, 1993.

[18] MANKAMO, T., SAMANTA, P., **Risk-Based Evaluation of allowed Outage Times (AOTs): Considering Risk of Shutdown,** IAEA-TECDOC-737, Relatório do TCM ("Technical Committee Meeting"), Budapest, 1993.

[19] SHOOMAN, M. L., **Probabilistic Reliability: an engineering approach.** 2 ed., Malabar, Florida, Robert E. Krieger Publishing Company, 1990.

[20] WALL, I., HAUGH, J., WORLEGE, D., " Recent applications of PSA for managing nuclear power plants", **Progress in Nuclear Energy**, v. 39, No. 3-4, pp.367-425, 2001.

[21] MARTORELL, S., "Simultaneous and Multi-criteria Optimization of TS Requirements and Maintenance at NPPs"**,** Annals of **Nuclear Energy,** v. 29, pp. 147-168, 2001.

[22] CEPIN, M., MARTORELL, S., "Evaluation of allowed outage time considering a set of plant configurations", **Reliability Engineering and System Safety**, v. 78, pp. 259-266, 2002.

[23] HE, X., TONG, J., CHEN, J., "Maintenance risk management in Daya Bay nuclear power plant: PSA model, tools and applications", **Progress in Nuclear Energy**, v. 49, pp. 103-112, 2007.

[24] U. S. NRC**, Risk-Informed Decision-making: Technical Specifications** NUREG-0800, Standard Review Plan, Chapter 16.1, Revision 1, March, 2007.

[25] U. S. NRC, REG. GUIDE 1.177**, An Approach for Plant-Specific, Risk-Informed Decision-making: Technical Specifications**, 1998.

[26] INTERNATIONAL ATOMIC ENERGY AGENCY, **Basic Safety principles for Nuclear Power Plants**, 75-INSAG-3, Vienna, 1988.

[27] INTERNATIONAL ATOMIC ENERGY AGENCY, **The Role of Probabilistic Safety Assessment and Probabilistic Safety Criteria in Nuclear Power Plant Safety**, Safety Series No. 106, Vienna, 1992.

[28] CNEN, **Licenciamento de Instalações Nucleares,** CNEN -NE-1.04, Outubro, 1984.

[29] MODARRES, M., **Risk Analysis in Engineering,** Techniques, Tools, and Trends, Taylor & Francis Group, Boca Raton, Florida, 2006.

[30] ROSS, M., SHELDON, **Introduction to Probability Models,** Academic Press, Inc., San Diego, California, 1993.

[31] U. S. NRC**, Evaluations of Risks Associated with AOT and STI Requirements at the ANO-1 Nuclear Power Plant**, NUREG/CR-5200, 1998.

[32] VESELY, W. E., **Measures of the Risk Impacts of Testing and Maintenance Activities**, NUREG/CR-3541, Battelle's Columbus Laboratories, November, 1983.

[33] U. S. NRC, **Procedures for Treating Common Cause Failures in Safety and Reliability Studies,** NUREG/CR-4780, vols. 1 and 2, 1987 and 1989.

[34] U. S. NRC, **Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment** NUREG/CR-5485, June, 1998.

[35] U. S. NRC, **Common-Cause Failure Parameter Estimations,** NUREG/CR-5497, October, 1998.

[36] U. S. NRC, **Study of Operational Risk-Based Configuration Control,** NUREG/CR-5641, BNL-NUREG-52261, June, 1991.

[37] U. S. NRC, **Fault Tree Handbook**, NUREG-0492, 1981.

[38] Lewis, E., E., **Introduction to Reliability Engineering**, John Wiley & sons, Inc., New York, 1996.

[39] SMITH, C., L., "Calculating Conditional Core Damage Probabilities for Nuclear Power Plant Operations", **Reliability Engineering Safety**, pp. 299-307, 1998.

[40] U. S. NRC, **Handbook of Parameter Estimation for Probabilistic Risk Assessment**, NUREG/CR- 6823, SAND2003-3348P, September, 2003.

APÊNDICE A - Aspectos Relevantes dos Sistemas para a Análise de Engenharia

Nesta seção são apresentadas as avaliações de engenharia necessárias aos sistemas a serem analisados, no caso desse trabalho, os Sistemas de Injeção de Segurança (SIS), o Sistema de Água de Serviço (SAS) e o Sistema de Água de Alimentação Auxiliar. As principais funções desses sistemas, com ênfase à operação das bombas, as Condições Limite de Operação e as políticas de teste (intervalo de teste exigido) e de manutenção (tempo máximo de indisponibilidade permitido), são descritas a seguir.

1) Sistema de Injeção de Segurança (SIS):

- Funções do SIS

O SIS, é projetado para prover água de refrigeração de emergência para o núcleo do reator no caso de acidente de perda de refrigerante tanto no primário como no secundário. Água contendo alta concentração de boro é, então, injetada no sistema de refrigeração do núcleo com o objetivo de compensar qualquer aumento de reatividade resultante da ruptura. A Figura A.1 apresenta o diagrama do SIS.

- Descrição do SIS

O SIS consiste de dois trens redundantes, cada qual com uma bomba de injeção de segurança, cujo abastecimento de potência elétrica é proveniente de dois barramentos redundantes e separados. O SIS recebe sinal de atuação de um de dois trens redundantes de atuação. As bombas do SIS são horizontais centrífugas e provêem água borada ao Sistema de Refrigeração do Reator.

- Condições Limite de Operação

O reator só poderá se tornar crítico com as duas bombas de injeção de segurança, válvulas e tubulação associadas operáveis.

Uma bomba de injeção de segurança pode se encontrar indisponível, devendo a mesma ser recuperada para a condição de operável dentro do período de 24 horas, tendo sido demonstrado que a bomba redundante se encontra operável.

- Exigências de Testes

As bombas do SIS devem ser testadas em intervalos não superiores a um mês.

- Considerações de Engenharia

A indisponibilidade de uma das bombas de injeção de segurança não causa a perda da função do sistema, pois cada trem é projetado com 100% de capacidade. Portanto, a indisponibilidade de uma das bombas devido à manutenção corretiva ou preventiva é permitida, desde que atendidas as condições limite de operação, sem que seja necessário conduzir a planta ao desligamento. O princípio de defesa em profundidade é preservado desde que a função de segurança seja garantida.

O impacto da indisponibilidade de uma bomba de injeção de segurança na FDN é avaliado quantitativamente através da APS. Essa avaliação deve determinar se uma revisão das ET em relação à extensão de TPI ou IT é possível sem a violação dos critérios de aceitação de risco.

2) Sistema de Água de Serviço (SAS):

- Funções do SAS

O SAS tem a função de prover água para a tubulação dos trocadores de calor do Sistema de Água de Refrigeração de Componentes (SARC) e para a refrigeração dos geradores diesel de emergência. O suprimento de água é vital durante todas as fases de operação da planta, sendo o SAS projetado para prover água em operação normal, em

condições de acidente, para garantir a operação segura e o desligamento da planta. A Figura A.2 apresenta o diagrama do SAS.

- Descrição do SAS

O SAS é composto por dois (2) trens, cada qual alimentado por um barramento elétrico de segurança, e possui três (3) bombas, sendo uma do tipo "*swing*" (C), que pode ser redundância do trem A ou do trem B. Como a bomba A ou B encontra-se ativa durante operação normal da planta, em geral, a bomba *"swing"* "C" fica alinhada ao mesmo trem da bomba em operação. O critério de sucesso do SAS é uma (1) bomba operando.

- Condições Limite de Operação

O reator só poderá se tornar crítico com duas das três bombas operáveis, estas com alimentação elétrica proveniente de barramentos distintos. Válvulas e tubulações associadas devem estar operáveis.

Durante a operação normal da planta, os requerimentos acima podem ser modificados para permitir que quaisquer dos componentes se encontrem inoperáveis. Entretanto, se tal componente não for recuperado dentro de 48 horas, o reator deve ser conduzido à condição de desligado frio dentro das próximas 36 horas.

- Exigências de Testes

O SAS opera continuamente durante a operação normal da planta, o que faz com que sua disponibilidade seja aparente para os operadores da planta. Os componentes redundantes são intercalados periodicamente para permitir inspeção e teste.

As bombas do SAS devem ser testadas em intervalos de tempo não superiores a um (1) mês.

- Considerações de Engenharia

A indisponibilidade de uma bomba do SAS não causa perda da função do sistema, pois cada trem é projetado com 100% de capacidade. Portanto, a indisponibilidade de uma bomba devido à manutenção corretiva ou preventiva não provoca a perda de função do sistema. O princípio de defesa em profundidade é preservado desde que a função de segurança seja garantida.

O impacto da indisponibilidade de uma bomba de água de serviço na FDN é avaliado quantitativamente através da APS. Essa avaliação deve determinar se uma revisão das ET em relação à extensão de TPI ou IT é possível sem a violação dos critérios de aceitação de risco.

3) Sistema de Água de Alimentação Auxiliar (SAAA)

- Funções do SAAA

Como principal função, o SAAA fornece água de alimentação para a remoção de calor residual e para a refrigeração do sistema primário em caso de indisponibilidade do sistema principal de água de alimentação. O SAAA provê uma fonte de refrigeração de emergência em caso de Acidente de Perda de Refrigerante (*Loss of Coolant Accident* – "LOCA") para pequenas rupturas. Como função secundária, o SAAA provê água de alimentação requerida pelos geradores de vapor durante períodos de manutenção em modo de prontidão quente. A Figura A.3 apresenta o diagrama do SAAA.

O SAAA é um sistema de segurança que é requerido em situações de emergência, portanto, o SAAA não atua durante operação normal da planta. A operabilidade do SAAA deve ser garantida através de testes do sistema, normalmente, efetuados durante as paradas para a recarga, e, teste de componentes, como bombas, que são realizados mais freqüentemente durante a operação do reator.

- Descrição do SAAA

O SAAA consiste de três (3) bombas, sendo duas motorizadas e uma turbinada, além de tubulações, válvulas, e instrumentação e controle necessários para o cumprimento de suas funções. Cada bomba motorizada tem a capacidade de suprir um gerador de vapor separadamente, enquanto a bomba turbinada tem a capacidade de suprir os dois geradores de vapor ao mesmo tempo. Cada bomba é parte de um trem de classe de segurança independente. Uma interconexão, normalmente fechada, entre as linhas de descarga das bombas motorizadas, permite que o fluxo de cada bomba possa abastecer as linhas de quaisquer geradores de vapor.

- Condições Limite de Operação

Dentre outras condições, o reator só poderá se tornar crítico se a bomba turbinada e uma das duas bombas motorizadas do SAAA estiverem operáveis, incluindo válvulas e tubulação associadas ao suprimento de água do tanque do SAAA para os geradores de vapor. Caso isso não possa ser cumprido, o reator deve ser conduzido à condição de desligado frio dentro de 48 horas.

- Exigências de Testes

As bombas do SAAA, tanto as motorizadas como a turbinada, devem ser testadas em intervalos não superiores há um mês.

- Avaliação de Engenharia

Considerando-se que o SAAA é composto por duas bombas motorizadas com capacidade de 50% cada uma, e de uma bomba turbinada, com 100% de capacidade, a indisponibilidade de uma bomba motorizada ou da bomba turbinada sozinhas não causam a perda de função do sistema. Portanto, a indisponibilidade de uma bomba devido à manutenção corretiva ou preventiva é permitida sem a exigência de desligamento do reator. O princípio de defesa em profundidade é preservado desde que a função de segurança seja garantida.

O impacto na FDN da indisponibilidade de uma bomba é avaliado quantitativamente através da APS. Essa avaliação deve determinar se uma revisão das ET, com vistas a extensões de TPI e de IT, é possível sem a violação dos critérios de aceitação de risco.

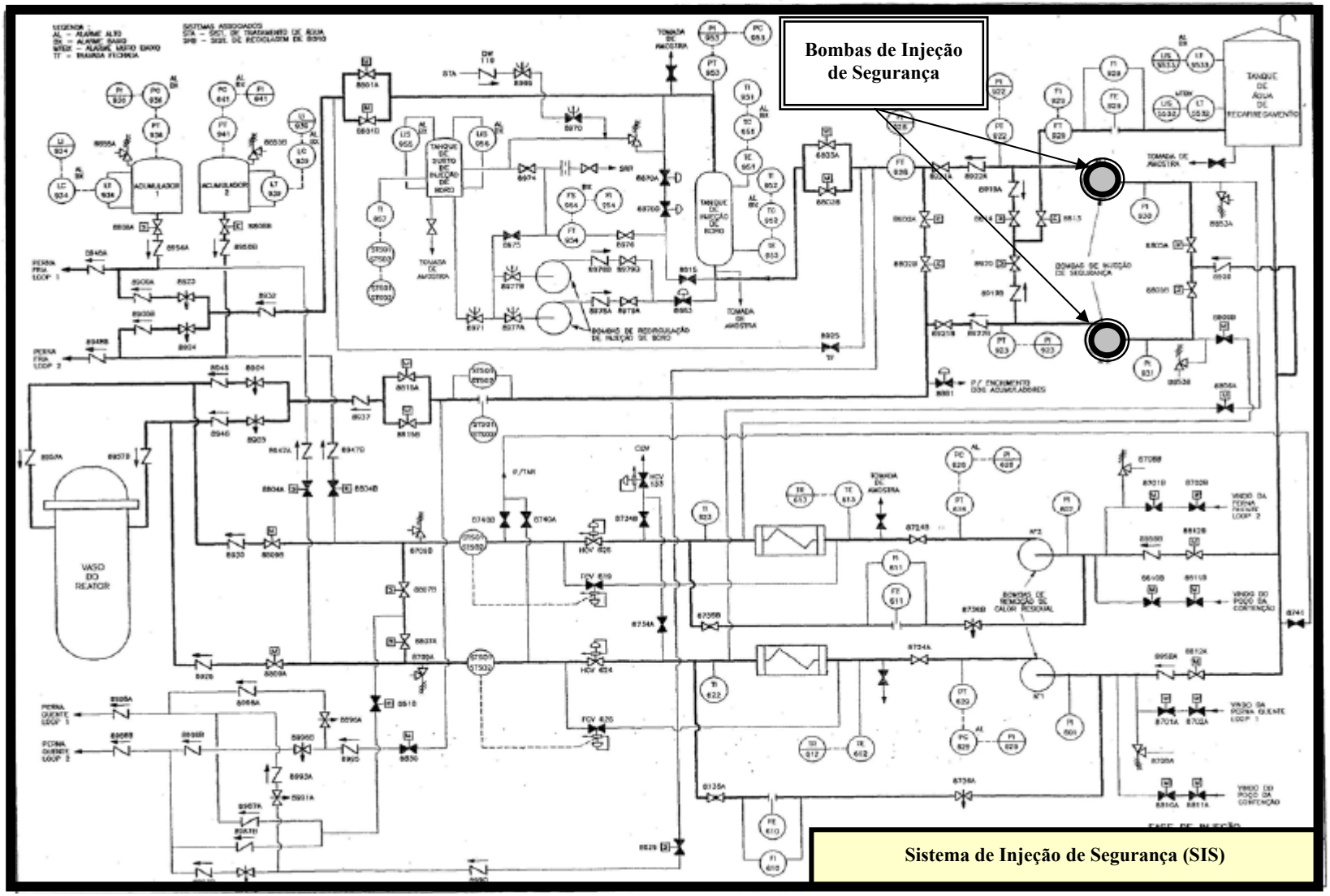

Figura A.1 – Sistema de Injeção de Segurança (SIS)

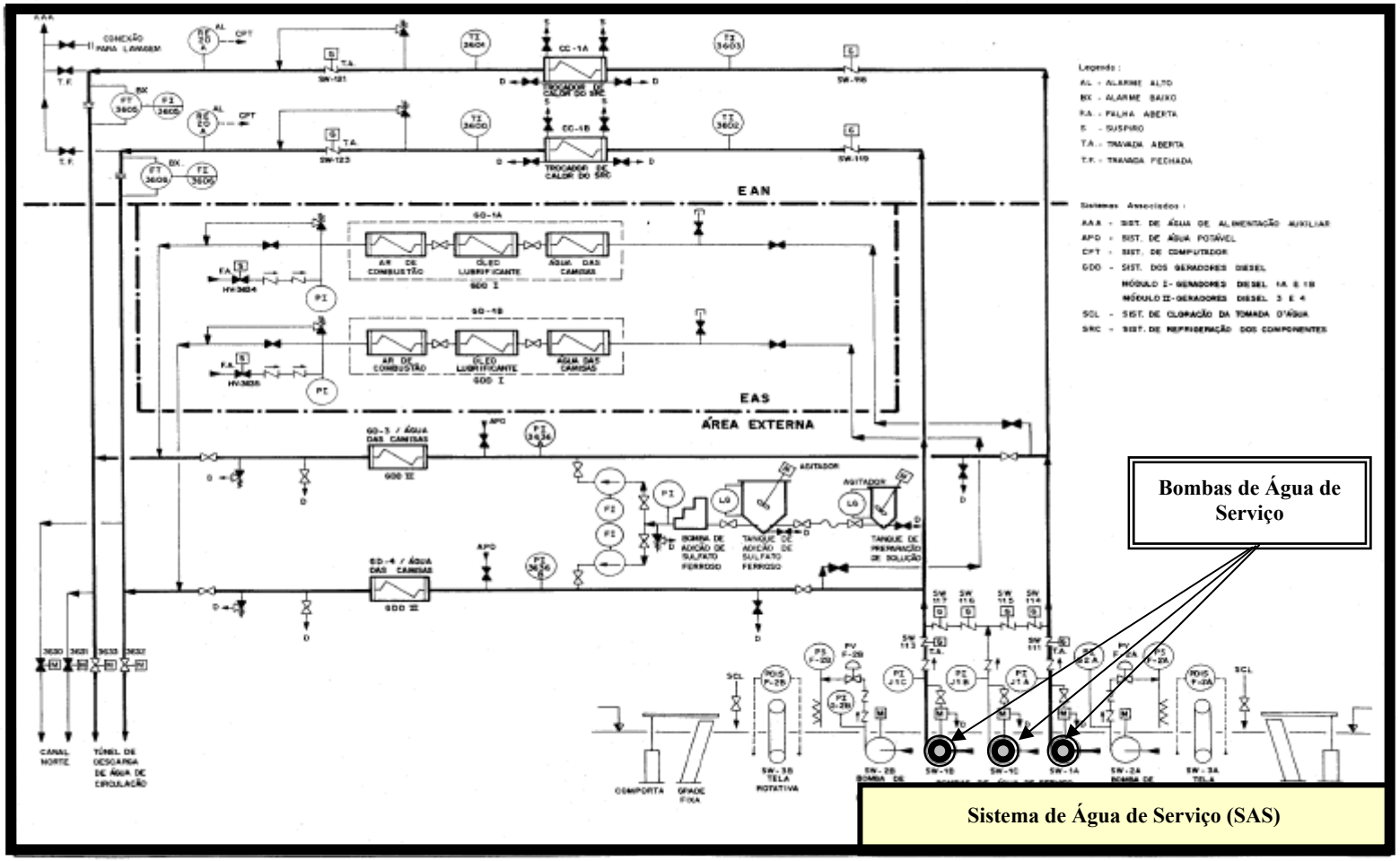

Figura A.2 – Sistema de Água de Serviço (SAS)

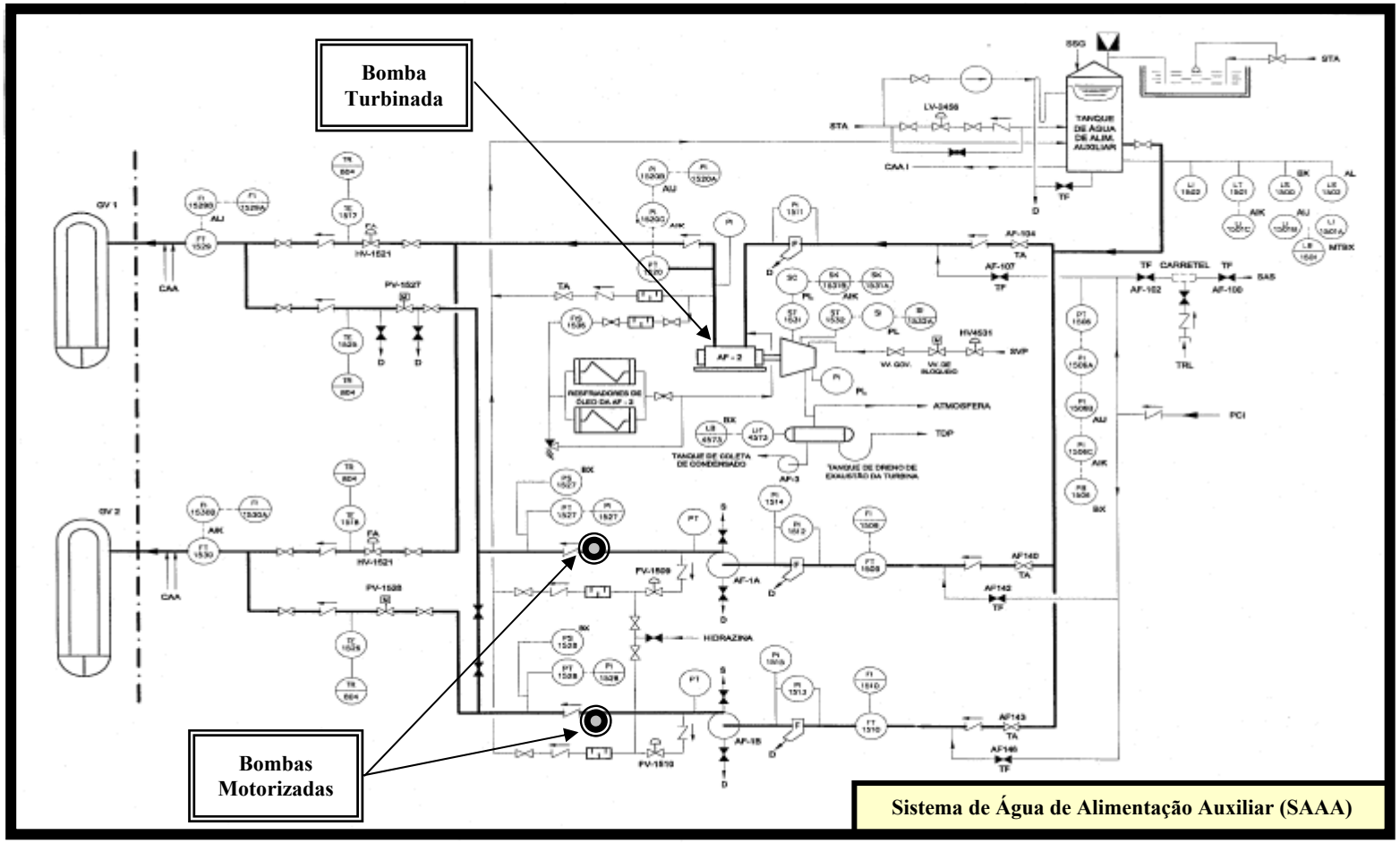

Figura A.3 – Sistema de Água de Alimentação Auxiliar (SAAA)