ANÁLISE DE RISCO CONSIDERANDO A SEGURANÇA NUCLEAR E PROTEÇÃO FÍSICA DE UMA INSTALAÇÃO NUCLEAR HIPOTÉTICA

Caio Coqueijo de Abreu

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Engenharia Nuclear, COPPE, da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Engenharia Nuclear.

Orientador: Paulo Fernando Ferreira Frutuoso e Melo

Rio de Janeiro

Março 2018

ANÁLISE DE RISCO CONSIDERANDO A SEGURANÇA NUCLEAR E PROTEÇÃO FÍSICA DE UMA INSTALAÇÃO NUCLEAR HIPOTÉTICA

Caio Coqueijo de Abreu

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

Examinada por:

_____

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

_____

Prof. Antônio Carlos Marques Alvim, Ph D.

_____

Prof. Celso Marcelo Franklin Lapa, D.Sc.

RIO DE JANEIRO, RJ – BRASIL

MARÇO DE 2018

Abreu, Caio Coqueijo de

Análise de risco considerando a segurança nuclear e proteção física de uma instalação nuclear hipotética/Caio Coqueijo de Abreu. – Rio de Janeiro: UFRJ/COPPE, 2018.

X, 92 p.: il.; 29,7 cm.

Orientador: Paulo Fernando Ferreira Frutuoso e Melo

Dissertação (mestrado) – UFRJ/ COPPE/ Programa de Engenharia Nuclear, 2018.

Referências Bibliográficas: p. 80-82.

1. Análise de Segurança. 2. Proteção Física. 3. Sabotagem. I. Melo, Paulo Fernando Ferreira Frutuoso e. II. Universidade Federal do Rio de Janeiro, COPPE, Programa de Engenharia Nuclear. III. Título.

Dedico este trabalho aos meus familiares, em especial aos meus Pais e Irmão.

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

ANÁLISE DE RISCO CONSIDERANDO A SEGURANÇA NUCLEAR E PROTEÇÃO FÍSICA DE UMA INSTALAÇÃO NUCLEAR HIPOTÉTICA

Caio Coqueijo de Abreu

Março/2018

Orientador: Paulo Fernando Ferreira Frutuoso e Melo
Programa: Engenharia Nuclear

Após os ataques de 11 de setembro feitos às torres gêmeas dos EUA, diversos países do continente europeu se tornaram alvos de inúmeros ataques terroristas. Após estes incidentes recorrentes, a grande preocupação com eventos que possam ter uma grande consequência à vida e à segurança tornaram-se um enfoque principal na política. Devido à evolução de ameaças do terrorismo às potencias mundiais, viu-se necessário o investimento em segurança, principalmente em instalações que utilizam materiais nucleares. Este trabalho terá enfoque na análise de importância de componentes de um sistema de emergência e a vulnerabilidade dos sistemas de proteção física da instalação nuclear. O grau de importância será analisado através das probabilidades de falha e indisponibilidade dos componentes. A vulnerabilidade do sistema de proteção física é feita através do cálculo das probabilidades de interrupção e neutralização. A metodologia utilizada para a combinação de *Safety* e *Security* será através de árvores de falha com frequência de eventos.

Os resultados irão evidenciar o grau de ameaça e o risco de sabotagem da instalação nuclear, a importância da combinação da análise da proteção física quando a sua eficiência em dissuadir um adversário e da análise probabilística dos sistemas. A alocação de recursos para os sistemas de proteção física será resultado de uma eficiente análise probabilística dos sistemas.

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

RISK ANALYSIS CONSIDERING NUCLEAR SAFETY AND PHYSICAL PROTECTION OF A HYPOTHETICAL NUCLEAR INSTALLATION

Caio Coqueijo de Abreu

March/2018

Advisors: Paulo Fernando Ferreira Frutuoso e Melo
Department: Nuclear Engineering

Following the September 11 attacks on US twin towers, several countries on the European continent have become targets of numerous terrorist attacks. Following these recurring incidents, a major concern with events that are a major consequence of life and security have become a major focus in politics. Due to the evolution of threats of terrorism to the world powers, it has been necessary to acquire safely, especially in facilities that use nuclear materials. This work focuses on the analysis of components of an emergency system and a vulnerability of the physical protection systems of the nuclear installation. The degree of analysis will be analyzed through the probabilities of failure and unavailability of the components. A vulnerability of the physical protection system by controlling the probability of interruption and neutralization. A methodology used for the combination of safety and security is through fault trees with frequency of events.

The results will evidence the degree of threat and risk of sabotage of the nuclear facility, the importance of combining physical protection analysis when its efficiency in deterring an adversary and probabilistic analysis of systems. The allocation of resources to the physical protection systems will be the result of an efficient probabilistic analysis of the systems.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABP	Acidentes de Base de Projeto
AE	Árvores de evento
AF	Árvores de falha
ASD	Análise de segurança determinística
APS	Análise probabilística de segurança
CNEN	Comissão Nacional de Energia Nuclear
CNPq	Conselho Nacional de Desenvolvimento Científico e Tecnológico
DBT	*Desing Basis Threat*
DSA	Diagrama de sequência do adversário
EASI	Estimate of Adversary Sequence Interruption
EI	Evento iniciador
EIP	Evento Inicial Postulado
FV	*Fussell-Vesely*
INES	*International Nuclear and Radiological Event Scale*
LOCA	*Loss of coolant accident*
LBLOCA	*Large Break Loss-of-Coolant-Accident*
LOFA	*Loss of flow accident*
NRC	*Nuclear Regulatory Commission*
PDC	Ponto de Detecção Crítico
PWR	*Pressurized Water Reactor*
PRA	*Probabilistic Risk Assessment*
RAW	*Risk-Achievement Worth*
RIDM	*Risk-Informed decision making*
RRW	*Risk-Reduction Worth*
SBLOCA	*Small Break Loss-of-Coolant-Accident*
SPF	Sistema de Proteção Física
SAPHIRE	*System Analysis Programs for Hand-On Integrated Reliability Evaluations*

1. Introdução

As questões de segurança nuclear podem ser definidas de duas maneiras: *Security*, que está relacionada com a prevenção, detecção e resposta a um furto, sabotagem, acesso não autorizado e transferência ilegal de materiais ou outros atos maliciosos envolvendo materiais nucleares e outras substâncias radioativas e suas instalações associadas. *Safety*, que está relacionada aos sistemas de limitação e realização de condições de funcionamento adequadas, à prevenção de acidentes ou à atenuação das consequências de acidentes, que resultem na proteção dos trabalhadores, do público e do ambiente contra os riscos de radiação indevida.

A obrigatoriedade da inclusão de projetos de *Safety* ou Segurança e *Security* ou Proteção Física em instalações que possua um ciclo do combustível nuclear é de responsabilidade da agência reguladora, no Brasil, Comissão Nacional de Energia Nuclear (CNEN). A agência cria normas que devem ser respeitadas a fim de estabelecer princípios e requisitos gerais básicos exigidos em uma instalação nuclear e minimizar a probabilidade de incidentes ou acidentes nucleares ou radiológicos e, portanto, de manter o risco para o público e o ambiente abaixo do limite aceitável. Essas normas abrangem instalações de produção, manuseio, utilização, processamento, reprocessamento, transporte ou estocagem de materiais do interesse do Programa Nuclear Brasileiro (CNEN, 2011).

Este trabalho tem como objetivo mostrar a diferença de conceitos e cálculos relacionados a *Safety* e *Security* em uma instalação nuclear hipotética. O cálculo de risco será baseado em um evento de grande perda de refrigerante ou *Large Break Loss Of*

Coolant Accident (LBLOCA) como um evento iniciador proposital, ou seja, sabotagem. Ao final, o objetivo é entender como um projeto de uma instalação juntando dois fatores, *Safety* e *Security*, pode gerar benefícios a fim de minimizar a probabilidade de acidentes ou mitigar e prevenir ações maliciosas.

> "Em uma análise de segurança de um projeto de instalação nuclear, deverão ser aplicados métodos determinísticos e probabilísticos. " (IAEA, 2000)

No Brasil, a palavra "Segurança" possui uma definição ampla. Diferente dos termos *Safety* e *Security* em inglês, uma única palavra, "Segurança", remete à ideia de sistemas de proteção física e sistemas de mitigação de acidentes.

Em geral, 98% dos produtos radioativos de uma instalação nuclear de geração elétrica são retidos no elemento combustível ou *fuel assembly* como mostra a Figura 1. Portanto, o objetivo primordial de um sistema de mitigação e controle do reator é providenciar além de uma troca de calor eficiente, controlar a energia liberada decorrente da reação de fissão do combustível evitando o superaquecimento ou o derretimento do núcleo. A prevenção relativa à liberação desses produtos radioativos para o ambiente é a base de criação para o projeto de múltiplas barreiras, chamados de Defesa em Profundidade ou *defense-in-depth.* São elas:

- Pastilha de combustível;
- Revestimento metálico;
- Vaso e tubulação;
- Contenção;
- Plano de emergência externo;

No caso de ocorrência de acidente, as barreiras devem limitar as consequências e a evolução para condições graves.

O estudo de segurança começa com a prevenção contínua de anormalidades operacionais e falhas de equipamentos ou humanas. Caso ocorra uma operação anormal ou um transiente, o conjunto de sistemas de segurança e sensores deve ser capaz de alertar operadores e, por conseguinte, seguir os procedimentos de segurança para normalizar e controlar o evento. Por isso, existem diversos dispositivos de detecção, além de sistemas de controle, limitação e proteção (ETN, 2017).

Caso não haja o controle da situação e consequentemente o evento evolua para Acidentes de Base de Projeto (ABP), o controle da situação se fará através da limitação do progresso do evento e da mitigação de suas consequências através de ações complementares na gestão do acidente. Dentre as limitações, a zona de exclusão que é associada e definida pela potência do reator (ETN, 1998).

A zona de exclusão pela norma CNEN 09/69 (CNEN, 1969) é definida pela área pertencente ao patrimônio da concessionária que circunda o reator. Nesta área ela tem autoridade para determinar todas as atividades, inclusive remoção de pessoal. Portanto, a concessionária responsável, a Eletronuclear, possui exigência quanto à zona de exclusão relacionada à dose equivalente a indivíduos localizados em qualquer ponto de seu contorno. Em um período de 2h após a liberação de produtos de fissão, o indivíduo não deverá receber uma dose corporal limite de 25 REM (dose externa) ou 0,25 Sv ou uma dose na tireoide equivalente a 300 REM (dose interna) ou 3 Sv devido à inalação de I-131 situado em um ponto sobre a linha limítrofe externa (CNEN, 1969).

Para isso, a gestão do acidente deve incluir as ações complementares. Se houver uma liberação significativa de material radioativo, as consequências radiológicas devem ser mitigadas através das ações do plano de emergência externo.

O termo *Safety* é utilizado para análises de segurança que abordam a variedade de fontes de energia relacionadas com o reator e seus papéis em transientes operacionais e em acidentes de projeto. O resultado das análises também define requisitos para os sistemas de segurança (Knief, 1992).

Figura 1 – Exemplo de Elemento combustível

Fonte: Nuclear Power.

A análise de segurança determinística (ASD) é a base do licenciamento de instalações nucleares no mundo. Ela consiste na simulação numérica da operação da usina, avaliando o seu comportamento frente a um espectro abrangente de eventos acidentais, denominados Acidentes de Base de Projeto (ABP). As ASD são ferramentas

essenciais na definição e verificação do atendimento dos critérios de segurança dos sistemas e das especificações técnicas (IAEA, 2010).

Os ABP são definidos por acidentes postulados ou escolhidos de maneira determinística ou considerações probabilísticas, utilizados para base de construção e projeto de uma usina nuclear (Petrangeli, 2006).

Tais acidentes são divididos em:

- Sobrerresfriamento;
- Sub-resfriamento;
- Sobre-enchimento;
- Acidente de perda de vazão;
- Acidente de perda de refrigerante;
- Transiente de reatividade;
- Transiente antecipado com falha do desarme;
- Eventos Externos;

Os objetivos de uma análise de segurança probabilística são determinar todos os fatores contribuintes significativos para os riscos de liberação de radiação decorrente de uma instalação ou atividade e avaliar até que ponto o projeto global está bem equilibrado e atende aos critérios probabilísticos de segurança quando estes foram definidos.

A análise probabilística de segurança (APS) envolve uma série de métodos analíticos. Estes incluem o desenvolvimento de modelos de lógica de árvore de eventos e de árvore de falhas. Utilizam para análise de sequências de acidentes, métodos de solução dos modelos lógicos, modelos de fenômenos que poderiam ocorrer, como por exemplo, dentro da contenção de uma usina nuclear, e os modelos de transporte de radionuclídeos no meio ambiente para determinar seus efeitos na saúde e na economia (IAEA, 2010).

Uma análise de segurança probabilística da instalação deve ser realizada com o objetivo de:

(1). Fornecer uma análise sistemática que cumpra os objetivos gerais de segurança;

(2). Demonstrar que um projeto equilibrado foi alcançado de tal forma que nenhuma característica particular ou EIP (Evento Inicial Postulado) faça uma contribuição desproporcionalmente grande ou significativamente incerta para o risco global e que os dois primeiros níveis de defesa em profundidade do primário sejam capazes de garantir a segurança;

(3). Garantir que sejam evitados pequenos desvios nos parâmetros das plantas que possam dar origem a um comportamento severamente anormal;

(4). Fornecer avaliações das probabilidades de ocorrência de danos severos ao núcleo e avaliações dos riscos de grandes liberações fora da zona de exclusão, necessitando de uma resposta a curto prazo, particularmente para liberações associadas com falha precoce na contenção;

(5). Fornecer avaliações das probabilidades de ocorrência e das consequências de perigos externos, em particular aqueles que são exclusivos do local da usina (IAEA, 2000).

Na análise de segurança, uma abordagem amplamente utilizada é a combinação de Árvores de falha (AF) e Árvores de evento (AE). As árvores de eventos delineiam as características gerais das sequências de acidentes que se iniciam a partir do evento iniciador (EI) e, dependendo do sucesso ou falha dos sistemas de mitigação de segurança, levam a um resultado bem-sucedido ou a danos ao sistema.

As árvores de evento são criadas a partir dos sistemas de mitigação que são incluídas no projeto. A Figura 2 mostra um exemplo de AE com 4 sistemas de proteção. AE é dividida e, para cada sistema de proteção, existe uma ramificação com probabilidade de sucesso ou falha.

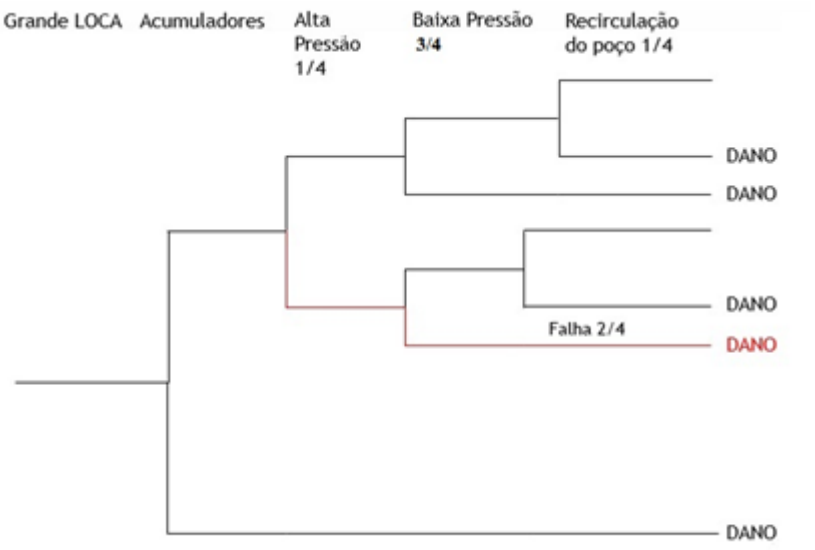

Figura 2 – Exemplo de Árvore de Evento do Sistema de injeção de Água de um reator PWR

As árvores de falha são utilizadas para modelar a falha dos sistemas de segurança e dos sistemas de suporte. As AF são detalhadas em componentes básicos do sistema de segurança, como por exemplo, válvulas e bombas. Para cada componente, existe um cálculo de probabilidade de falha ou de indisponibilidade que pode ser baseado em opinião de especialista, como por exemplo a estimativa de taxa de falha (λ).

Para o cálculo de frequência do acidente ou evento topo, cada componente, incluindo suas dependências e linha de falha serão adicionados nas AF com portões lógicos e eventos básicos. Com o intuito de simplificar as contas, será considerado como evento topo o LBLOCA, pois, possui a maior probabilidade de causar evento severo no reator. O evento topo e sua frequência serão levantados da literatura.

Alguns cálculos como *Risk-Achievement Worth* (RAW), *Risk-Reduction Worth* RRW e *Fussell-Vesely* (FV) são utilizados para análise de importância de componentes de uma instalação nuclear. Elas servem, através do Diagrama de Pareto, de análise dos componentes críticos do sistema que levam mais facilmente ao evento topo (MODARRES, 2006).

O Princípio de Pareto consiste em identificar e tomar decisões sobre os componentes deixando-os para depois ou desconsiderando. Ou seja, o grau de importância do componente será definido pela participação da falha de um sistema. O componente de maior importância será aquele capaz de gerar maior probabilidade de dano ao sistema.

O RRW pode ser chamado de fator de diminuição de risco. Ele apresenta a máxima diminuição do risco provocado pelo aumento da confiabilidade de um componente. O RAW pode ser chamado de fator de aumento de risco. Ele mede o aumento da probabilidade de falha do sistema resultante do pior caso de falha de um componente. O FV descreve como um componente não crítico contribui para a falha do sistema.

A análise de *Security* se refere aos sistemas utilizados para prevenir ou detectar ataques de adversários ou ameaças. Uma abordagem diferente de *Safety,* o Diagrama de Sequência do Adversário (DSA) é usado para a frequência de falha de um EI de *Security*, ou seja, serve como uma ferramenta de representação de todos os elementos de detecção e atraso em um Sistema de Proteção Física (SPF) (GARCIA, 2008).

Em uma instalação que possua preocupação com a segurança física, as múltiplas barreiras de proteção física servem para evitar que um adversário tenha acesso à instalação ou, caso falhe, aumentar o tempo de detecção do intruso ao adentrar a instalação e sabotá-la. No entanto, estas barreiras podem ser ultrapassadas de diversas

maneiras. Portanto, devido ao grande número de possibilidades de o adversário atacar uma barreira física, o número de caminhos possíveis torna-se grande. Logo, o DSA usa o método de gravar diversos caminhos que são representados por gráficos. O gráfico mostra caminhos possíveis que o adversário possa seguir e completar a missão de sabotar (GARCIA, 2008).

Existem 3 etapas para a criação de um DSA para uma instalação:

1. Modelando a instalação separando-a em áreas físicas adjacentes;
2. Definindo camadas de proteção e elementos de caminho entre as áreas adjacentes;
3. Gravar detecção e valores de atraso para cada elemento;

A abordagem do Sistema de Proteção Física deve ser realizada independente da análise de segurança.

A estimativa do risco de *Security* pode ser feita utilizando a Equação (1): (GARCIA, 2008).

$$R = P_A * (1 - P_I * P_N) * C \quad (1)$$

Onde:

P_A: É a frequência do ataque do adversário;

P_I: É a probabilidade de interrupção do adversário;

P_N: É a probabilidade de neutralizar o adversário pela força de resposta;

C: É a consequência do ataque;

Já a estimativa do risco de *Safety*:

$$R = F * C \quad (2)$$

Onde:

F: É a frequência de falha do sistema de segurança dado em anos;

C: É a consequência do ataque;

O risco está associado a um dano, derivado de um acidente, que poderia acontecer com uma determinada probabilidade. Quando os acidentes são eventos raros, o risco é resultado de um cálculo ou estimativa mediante um modelo teórico. O risco se estima com determinado grau de incerteza que depende da qualidade dos dados e modelos.

O risco pode ser classificado em dois tipos (TWEEDDALE, 2003):

1. Altos riscos precisam de uma pesquisa para determinar as causas (alta probabilidade, altas consequências) e realizar ações para reduzi-los.
2. Baixos riscos devidos a eventos de baixa probabilidade e grandes consequências (severidade) precisam de Gestão de Riscos para garantir que a probabilidade é realmente pequena e continue sendo pequena. Uma ação é conhecida como *Risk Informed decision making* (RIDM).

Essas classificações podem ser aplicadas tanto em *Security* quanto em *Safety*. Porém, possuem cálculos distintos.

Pode-se perceber que F na Equação (2) descreve um evento iniciador aleatório probabilístico e independente. Diferente da parcela da Equação (1), a probabilidade do evento está associada aos sistemas de proteção e ao ataque do adversário. O Valor C de consequência remete à mesma ideia na Equação (1) e (2), uma vez que a falha na segurança afeta de forma semelhante os indivíduos do público.

1.1. Objetivo

O objetivo principal deste estudo é criar uma ligação entre *Safety* e *Security*. No Brasil, atualmente existem estudos apenas relacionados a *Safety*. No entanto, é primordial fomentar a cultura de segurança e o estudo sobre a segurança física em instalações com material nuclear.

> "Os princípios fundamentais da segurança nuclear incluem a incorporação de uma cultura de segurança nuclear em todas as organizações envolvidas. Com a implantação coerente de uma cultura de segurança nuclear, o pessoal permanece atento à necessidade de manter um elevado nível de segurança ...Todas as organizações envolvidas na implantação de proteção física devem dar a devida prioridade à cultura de segurança; ao seu desenvolvimento e manutenção necessários para assegurar sua efetiva implantação em toda a organização ". (IAEA, 2008)

Os cálculos feitos neste trabalho terão enfoque nas considerações e diferenças de risco em *Safety* e em *Security* determinando a frequência de falha de segurança tanto combinada quanto isoladas. A combinação dos tipos de segurança pode permitir uma melhor alocação de recursos do estado. No entanto, a importância do trabalho é mostrar que diferentes cenários dentro de uma instalação nuclear podem gerar complicações e criar falta de segurança ao público. Além de evidenciar que a proteção de materiais nucleares e outros materiais radioativos incluindo instalações associadas contra atos maliciosos de agentes não estatais afetam a segurança mundial como um todo.

1.2. Proposta

1.2.1 Metodologia

Para este trabalho, será utilizada uma instalação nuclear de geração de energia hipotética do tipo *Pressurized Water Reactor* (PWR), mesmo tipo de usinas utilizadas no Brasil. Esta instalação irá permitir calcular e analisar probabilisticamente o evento iniciador decorrente de uma sabotagem de forma que o adversário, caso tenha sucesso na missão, irá resultar no acionamento de emergência da usina.

As instalações e proteções físicas, assim como a localização de componentes básicos de um reator que serão apresentadas são hipotéticas.

O circuito primário será o enfoque na sabotagem do adversário. Por considerar um evento iniciador LBLOCA, além de iniciar o evento, o adversário terá a missão de interromper sistemas de proteção passivos ou não, para que evolua para um acidente severo.

Através do programa *System Analysis Programs for Hand-On Integrated reliability Evaluations* (SAPHIRE) (NRC, 2017), o componente de maior importância do sistema de segurança será selecionado pelo adversário através do estudo do RAW, RRW e LV. (FULLWOOD, 2000)

A motivação ao utilizar este programa é mostrar que um evento iniciador em um componente com grau de importância elevado pode progredir à falha geral dos sistemas de emergência do reator e levar ao evento topo. Assim como usinas convencionais licenciadas do tipo PWR, o circuito primário terá redundâncias e serão separadas fisicamente. Dentre diversos outros programas de análise probabilística, o SAPHIRE foi

escolhido pela facilidade, por ser acessível e satisfatório no trabalho (FULLWOOD, 2000).

Não será o objetivo deste trabalho mostrar ações de operadores para mitigar e acionar sistemas de segurança, ou qualquer ação de erro humano. O sistema primário será simplificado, no entanto, serão calculados a probabilidade/indisponibilidade do sistema em árvores de falha reduzidas.

Para a ação de sabotagem, será utilizado o DSA com a finalidade de avaliar a eficiência do Sistema de Proteção Física. O SPF da instalação hipotética terá áreas de divisão e adjacências como a CNEN 2.01 define (CNEN, 2017):

I. Área Vigiada
II. Área Protegida
III. Área Vital

Dentre diversos caminhos criados na planta, os mais vulneráveis serão analisados a fim de "facilitar" a missão do adversário e focar em fragilidades do sistema de segurança física. Diversos elementos de detecção serão considerados na planta com o intuito de obter a maior eficiência, incluído o atraso do SPF com seus respectivos valores de probabilidade de detecção (P_D) e tempo de atraso (T_d). O tempo da força resposta será postulado. Estes elementos de detecção e força resposta estão vinculados à Equação (1) na probabilidade de interrupção do adversário (P_I).

A vulnerabilidade de um caminho de segurança é chamada de probabilidade de sucesso do adversário (P_s), que é igual à Equação (3)

$$P_s = (1 - P_I * P_N). \quad (3)$$

A probabilidade de sucesso do adversário vezes a frequência de ataque (f_{ataque}) por ano dá a frequência de um ataque bem-sucedido ($F_{ataque,S}$) como mostra a Equação (4).

$$F_{ataque,S} = P_s * f_{ataque} \quad (4)$$

Esta frequência é usada na análise de segurança combinada com a frequência de falha do Evento Iniciador (Hawila, 2016).

1.2.2 Procedimentos

O trabalho irá se basear na Análise Probabilística de Safety e a junção em *Safety-Security* para calcular a frequência combinada das falhas do SPF e Sistemas de Emergência.

A análise de *Safety* é representada pela falha progressiva de sistemas de emergência do reator e componentes do circuito primário, alvo do adversário. Já a análise em *Security*, as sucessivas quebras de barreiras físicas são representadas pelo Diagrama de Sequência Adversa.

As árvores de evento e falha são criadas usando o software SAPHIRE para auxiliar o processo de avaliação de risco dos cenários de falha de sistema escolhidos a partir de Eventos Iniciadores tanto em *Safety* quanto em *Security* (FULLWOOD, 2000).

Por possuir diversas plantas e componentes hipotéticos, a formulação do layout e de componentes de segurança serão listados a seguir:

I. Desenvolver uma planta hipotética para o circuito primário de uma instalação nuclear PWR;
II. Criar uma Planta do sítio da usina nuclear em questão com divisões em áreas definidas pela CNEN;

III. A partir da criação do circuito primário e do sítio, detalhar:
    a. *Security*: Equipamentos de segurança, dimensões, sistema de resposta ao adversário;
    b. *Safety*: Sistemas de Emergência do Reator e Defesas em profundidade.
IV. Análise de *Security* para o layout do circuito primário, com o intuito de calcular os parâmetros de segurança, tais como a probabilidade de interrupção (P_I), a probabilidade de neutralização (P_N), a frequência de ataque (f_{ataque}) e o risco (R) associado;
V. Fazer a AE e AF para o circuito primário e sistemas de emergência.
VI. Identificar componentes de maior grau de importância que causam maior probabilidade de dano ao reator e que tenham maior acessibilidade pelo adversário;
VII. Identificar alvo e traçar caminhos possíveis para a missão do adversário;
VIII. Conduzir análise de segurança combinada para os componentes do sistema do circuito primário, considerando o ataque do adversário como um EI;
IX. Crie AE e AF usando o software SAPHIRE incluído a análise combinada de *Safety* e *Security;*
X. Calcular a frequência individual e combinada em *Safety* e *Security;*
XI. Calcular o valor de risco associado para cada caso de EI;

1.3. Problemática e Importância

Em 2001 o mundo se deparou com o maior ataque terrorista a uma potência mundial. Criou-se uma estigma e preocupações com o terrorismo.

O programa da agência de segurança nuclear dos Estados Unidos é influenciado por uma avaliação das intenções, motivações e capacidades de comunicação entre terroristas e criminosos. As avaliações emitidas pelas autoridades nacionais continuam a concluir que os grupos terroristas têm a ambição de adquirir, e possivelmente usar, armas não convencionais, tais como dispositivos explosivos nucleares improvisados e dispositivos de dispersão radiológica - as chamadas "bombas sujas" (IAEA, 2017).

Historicamente, alguns eventos podem ser vistos como indicadores de que futuras ameaças e atos maliciosos envolvendo materiais radioativos podem ser realizados por grupos extremistas.

O uso de fontes radioativas para fins maliciosos tem sido raro, mas não desconhecidas. Sabotagem de ataques ou ameaças de ataques contra instalações nucleares também ocorreram no passado, mas nenhum desses eventos relatados ainda resultou em dispersão de radioatividade.

No entanto, a preocupação com eventos deste tipo às instalações com materiais nucleares tornou-se o enfoque principal na política. Devido à evolução de ameaças do terrorismo às potencias mundiais, países alvo de terrorismo e agências reguladoras decidiram investir e disseminar a Cultura de Segurança.

Esta é definida, pela norma 1.26 da CNEN, como um conjunto de características e atitudes de organizações e de indivíduos que estabelece como prioridade maior que as questões de segurança da instalação e receberão atenção proporcional à sua importância (CNEN, 1988).

A avaliação combinada do risco de uma instalação nuclear hipotética relacionados aos sistemas de proteção do reator e proteções físicas da usina nunca foi feita.

Ao final do trabalho, o cálculo deve servir para aprimorar meios e direcionar recursos a fim de aumentar a eficiência de detecção do intruso e, consequentemente, aumentar a segurança das instalações nucleares.

Este trabalho demonstra métodos e meios para que possam ser aplicados as outras instalações nucleares. O cálculo das probabilidades para demais instalações seguem exatamente as mesmas diretrizes deste trabalho.

1.4. Acidente

Dentre os acidentes listados na base de projetos, os que geram maiores consequências e limitam o projeto de reator são aqueles associados à perda da capacidade do refrigerante de remover calor. O acidente que causa o maior dano e mais grave em relação à consequência gerada é a perda completa do refrigerante. No entanto, pequenas perdas de fluido e / ou perda de fluxo de refrigerante também podem ter consequências importantes, como é o caso do *small breake loss of coolant accident* (SBLOCA) e *loss of flow accident* (LOFA), respectivamente.

O LOCA é mais provável nos reatores refrigerados a água, onde o conteúdo de energia armazenada do refrigerante em alta pressão e alta temperatura pode ser liberado para a contenção por ruptura de um tubo exposto. O acidente de perda de refrigerante pode ser classificado de pequenas rupturas na tubulação até grandes rupturas do tipo guilhotina, considerado o pior caso (Knief, 1992).

Dentro do grupo de LBLOCA incluem-se as rupturas no sistema primário de refrigeração do reator com perda de refrigerante na contenção com tamanho de ruptura com diâmetro equivalente de 23 cm até uma quebra em guilhotina de um circuito de refrigeração do primário.

Em consequência da perda rápida de refrigerante no sistema primário, os sistemas de emergência, passivo e ativo, de um PWR entram em ação.A ocorrência do LOCA gera o seguinte cenário:

- Uma quebra dupla de tubo do tipo guilhotina na extremidade da linha de refrigerante do primário para permitir o livre fluxo de refrigerante em ambas as extremidades.
- O refrigerante vira vapor sob a influência da energia armazenada e é descarregado rapidamente no prédio de contenção.
- Embora a perda de líquido de refrigeração interrompa a cadeia de fissão, o desligamento do reator é iniciado por uma leitura de pressão inferior ao *set point* de proteção para assegurar a sub-criticalidade.
- Os sistemas de resfriamento de núcleo de emergência ou *Emergency Core Cooling System* (ECCS) funcionam para esfriar o núcleo e evitam danos excessivos causados por calor de decaimento.
- A radioatividade liberada com o refrigerante primário é retida dentro da estrutura de contenção.
- O sistema de remoção de calor residual mantém a eficácia do ECCS e reduz a pressão de contenção.
- Quando as características de segurança funcionam com eficácia, o núcleo é resfriado com uma quantidade mínima de falha de combustível local.

Portanto, para que ocorra o acidente severo, ou seja, o derretimento do núcleo, os sistemas de segurança devem falhar em inundar e resfriar o núcleo instantânea e continuamente.

A Tabela 1 mostra a evolução resumida após a tubulação do sistema primário sofrer guilhotina. Os tempos de entrada dos sistemas foram postulados.

Pela Tabela 1, vemos que a evolução do acidente gera um aumento de pressão na contenção do reator e, consequentemente, a pressão na linha do sistema primário chega ao limite de projeto de 132 bars. O limite de pressão em 1,4 segundos gera um sinal que aciona o sistema de recuperação do reator. Em 300 segundos após o acidente de ruptura, o primeiro sistema passivo entra em ação para inundar e evitar o derretimento do núcleo. 80 segundos após os acumuladores despejarem água borada no reator, o sistema de baixa pressão é acionado a fim de remover o calor residual e manter o núcleo resfriado até atingir a quantidade mínima de falha do combustível.

Tabela 1- Sequência de entrada dos sistemas de segurança a partir do evento de ruptura de tubulação do tipo guilhotina localizada na perna quente do reator hipotético do tipo PWR

Sequência LOCA Grande	
Evento	Tempo (s)
Quebra da tubulação- Guilhotina	0
Trip do Reator a baixa pressão <132 bar. 1.Trip da Turbina 2.Trip da bomba	1.40
Perda de eficiência de Remoção de calor pelo Secundário. 1.P_{rcs}<132 bar 2.$P_{contenção}$>1,03bar	1.40
ECCS 1. P_{rcs}<110 bar 2. $P_{contenção}$>1,03bar	7.56
Nível do Pressurizador <2,28 m	12.10
Acumuladores	300
Pico de pressão na contenção (1,72 bar)	350
Núcleo recuperado	370

Bombas do Sistema de Baixa pressão	380
Linha recuperada	420
Perna quente recuperada	470
Acumuladores na Perna fria isolado	510

1.5. Sistemas de Segurança

Um sistema de proteção é um conjunto de componentes de segurança nuclear em uma usina projetada para “desligar” com segurança o reator e evitar a liberação de materiais radioativos. Uma vez que ocorra um grave acidente de combustível e haja liberação de radionuclídeos para atmosfera da contenção e do prédio, as consequências estarão além do controle. Sendo assim, os elementos de proteção e mitigação da defesa em profundidade são focados em limitar a liberação e evitar danos ao reator (KNIEF, 1992).

Os sistemas de proteção são redundantes e possuem 3 principais características:

1. Mecanismos inerentes do reator, como por exemplo efeito Doppler e circulação natural do refrigerante, que dependem apenas das leis da natureza.
2. A função de segurança passiva, como por exemplo, controle de desligamento, barras de controle inseridas por gravidade, injeção de refrigerante em uma situação de emergência, como é o caso dos acumuladores, e fornecimento de barreiras à liberação de radioatividade.
3. Sistemas ativos são sistemas que necessitam de uma ação humana ou equipamentos para serem acionados usando por exemplo bombas, motores e fontes de energia, fornecem o elemento restante da segurança do reator.

Em uma situação de perda de refrigerante, os sistemas ativo e passivo entram em ação. Os ativos, sistema de emergência de baixa pressão acionado pela leitura de baixa pressão e nível de refrigerante no sistema primário, acionam bombas e, após injetar refrigerante, servem para a contínua refrigeração do reator. Os passivos, que precedem o sistema de baixa pressão, são sistemas independentes de bombas. Neles atuam somente sensores de leitura de pressão que, ao sentir a baixa pressão do sistema primário, abrem as válvulas. Exemplo de um sistema passivo são os acumuladores.

Estes sistemas são comuns em uma instalação nuclear com reator do tipo PWR e a eficácia do sistema é estudada para que uma usina seja licenciada. A Tabela 2 mostra a árvore de eventos dos sistemas de segurança da instalação hipotética utilizada neste trabalho.

Tabela 2 – Árvore de eventos dos sistemas de segurança de uma instalação hipotética, tipo PWR, após um acidente de perda de refrigerante do tipo guilhotina

LARGE BREAK LOCA	DESCARREGAMENTO EFETIVO DOS ACUMULADORES 4/8	INJEÇÃO DE ÁGUA DO SISTEMA DE BAIXA PRESSÃO 3/4	SISTEMA DE RECIRCULAÇÃO DO POÇO 1/4	CLASSIFICAÇÃO	RAMO
A	B	C	D		
			P3	OK	L1
		P2		DANO	L2
	P1				
				DANO	L3
				DANO	L4

Para que não haja dano, o sistema passivo de descarregamento efetivo dos acumuladores 4/8, sistemas ativos de injeção de água do sistema de baixa pressão e recirculação do poço 1/4 devem obter sucesso, como mostra o ramo L1.

Os ramos L2, L3 e L4 correspondem à falha de um dos sistemas e que, por conseguinte, causam danos ao núcleo.

P1: Descarga para o sistema primário de quatro acumuladores, sendo efetiva a descarga na perna quente ou fria de um loop intacto.

P2: Injeção no sistema primário de um trem do sistema de injeção de emergência de baixa pressão nas pernas frias e quentes de um loop intacto.

P3: Recirculação desde o poço da contenção mediante um trem, com sua bomba de baixa pressão e trocador de calor efetivo, injetando nas duas pernas de um loop intacto.

Neste trabalho será calculada a falha do sistema de segurança de baixa pressão que cause danos ao núcleo pelo ramo L3.

O sistema será composto de 4 trens de redundância e componentes básicos como bomba, válvulas e tanques de armazenamento.

Os dados retirados da IAEA (1988) servirão para o cálculo da indisponibilidade e probabilidade dos componentes em questão. Os cálculos de corte mínimo e probabilidade de sucesso na árvore de eventos decorrente do acidente foram efetuados a partir do programa SAPHIRE. Aproximações serão feitas devido à complexidade do evento.

2. SAFETY

O sistema de emergência explicado na Subseção 1.5 será o enfoque desta seção. A APS de falha dos componentes básicos de um sistema de injeção de baixa pressão foi conduzida usando o Nível 1 de abordagem.

> "A Análise Probabilística de Segurança (APS) é uma avaliação aprofundada e integrada da segurança de uma instalação nuclear que, a partir de um estado inicial e considerando as probabilidades de progressão de determinadas falhas de equipamentos e erros do operador, produz estimativas numéricas do nível de segurança da instalação. A APS complementa a abordagem determinística de avaliação de segurança de uma instalação nuclear, que consiste em analisar de modo conservador um conjunto de acidentes críveis tomados como base de projeto" (IPEN, 2017)

Deste modo, a APS pode ser desenvolvida em três níveis como mostra a Figura 3 (IPEN, 2017):

- APS Nível 1 - Tem como objetivo avaliar a probabilidade de ocorrerem danos ao núcleo do reator. Tal avaliação mapeia e identifica pontos fortes e deficiências do sistema de segurança. Ao fim de uma APS de Nível 1, é possível propor procedimentos que previnem ou mitigam acidentes. A fim de melhorar a confiabilidade do sistema, podem ser implantados procedimentos como:
    1. Uso de componentes de fabricantes diferentes;
    2. Redundâncias;
    3. Localização distinta na planta.

- APS Nível 2 – Tem como objetivo avaliar, a partir dos resultados obtidos na APS Nível 1, e quantificar o material radioativo que poderá ser liberado a partir de um acidente e estimar a probabilidade de que seja liberado para fora da atmosfera de contenção. Esta análise resulta em um conhecimento adicional sobre a importância da defesa em profundidade de uma instalação nuclear.
- APS Nível 3 – Tem como objetivo avaliar, a partir dos resultados obtidos na APS Nível 2, as consequências do acidente nuclear em termos de danos ao público e danos ao meio ambiente (NRC, 2017).

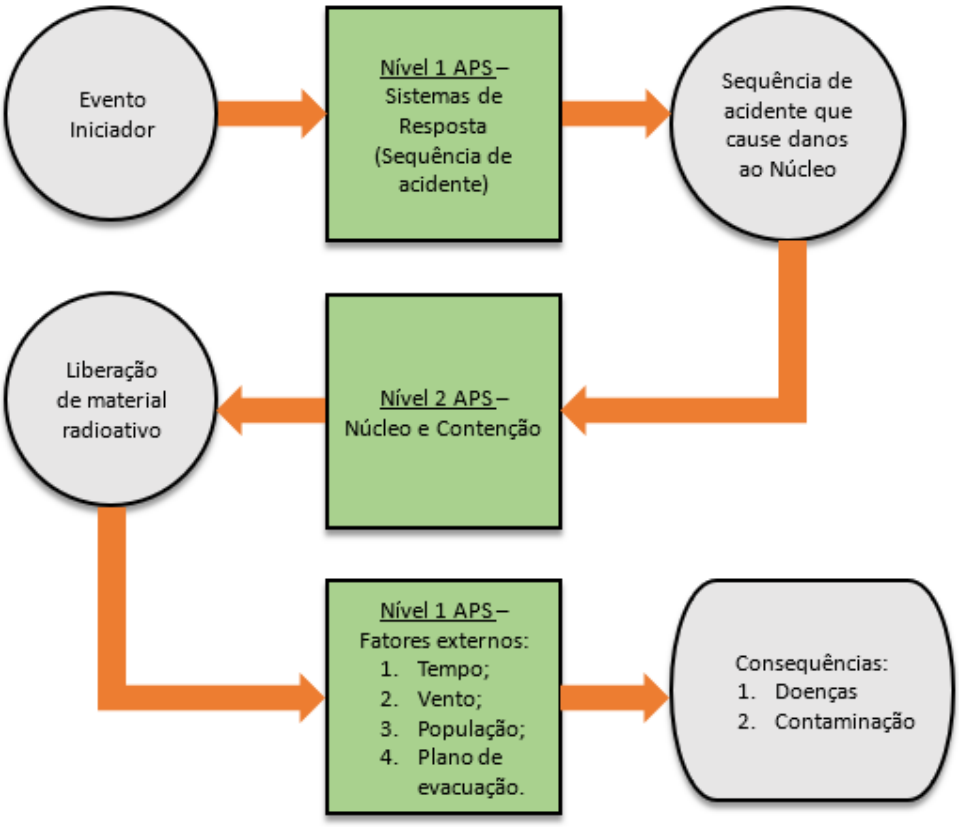

Figura 3 – Desenvolvimento e dependências dos três níveis de APS

Fonte: NRC, 2017

Neste capítulo, as frequências de falha dos componentes do sistema de injeção de emergência de baixa pressão (como válvulas, trocadores de calor e bombas) foram consideradas para calcular a frequência de falha a partir do EI básico para todo o evento de falha do sistema de resfriamento. O objetivo desta seção é fornecer cenário e priorizar o componente de maior importância para que haja falha do sistema de resfriamento.

O primeiro passo em uma APS é a identificação do evento topo e diferentes eventos iniciadores que levem ao evento. Eles fornecem a base para uma APS e, caso sejam inseridos erradamente ou omitidos nas árvores de falha, pode haver um comprometimento quando à análise de perfil de risco do sistema. Logo, os principais ganhos ao usar uma análise por árvores de falhas são a identificação e quantificação de possíveis falhas do sistema. (IAEA, 2006)

Os principais objetivos da análise de eventos iniciais são:

i. Identificar um conjunto de eventos que comprometam a operação normal da planta e que exijam mitigação bem-sucedida para evitar danos no núcleo;
ii. Agrupar os eventos iniciadores para facilitar a modelagem eficiente da resposta da planta e iniciar a avaliação de frequência de eventos, fornecendo resolução suficiente em relação à modelagem de sequências de acidentes;
iii. Fornecer estimativas para as frequências dos grupos de eventos iniciadores usando informações disponíveis e técnicas de estimação de frequência.

Nos eventos iniciadores, são introduzidos códigos de falha para cada componente do sistema e sua respectiva frequência de falha. A frequência utilizada é um valor que representa quantas vezes um evento provavelmente ocorrerá durante um período de tempo (ex. 10^{-4} / ano). Esta frequência pode ser construída por opinião de especialistas

ou dados de falha médio dos componentes que é determinada pelo número de incidentes pelo tempo observado.

Para calcular a frequência de evento topo da falha, cada frequência de falha de componente individual deve ser encontrada primeiro.

Na Figura 4, vimos que os componentes A, B e C são adicionados como eventos iniciadores e ligados por uma lógica booleana de portões OU e. Esta lógica será explicada na Seção 3.2. Serão adicionados, nos eventos iniciadores, a frequência de falha de cada componente e seu respectivo código.

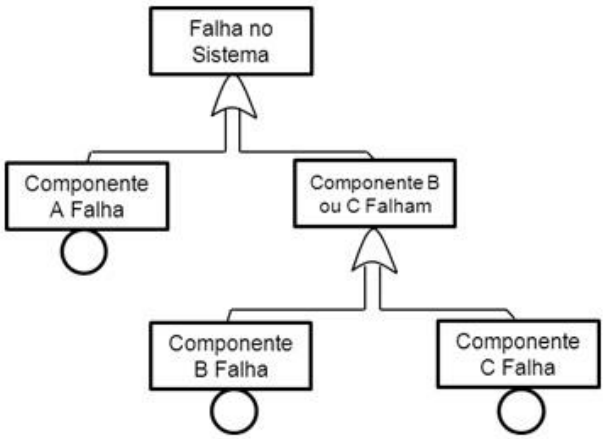

Figura 4 - Exemplo de árvore de falha

Por ser um sistema de emergência de uma usina nuclear e as falhas dos componentes resultarem em eventos perigosos e danosos, existe uma dificuldade na estimativa de frequência destes eventos. Por isso, foram utilizados dados de frequência média retirados do documento técnico de confiabilidade de componente para uso na avaliação probabilística de segurança, uma vez que a planta e os componentes dos sistemas são hipotéticas. (IAEA, 1988)

2.1. Sistema de Injeção de Baixa Pressão

A árvore de falha do sistema de injeção de baixa pressão foi simplificada para o cálculo de cortes mínimos e probabilidade de sucesso.

A Figura 5 mostra os trens do sistema de injeção de baixa pressão tanto na perna quente quanto na perna fria e os acumuladores.

O sistema possui 4 trens de redundância, sendo que para cada par, um tanque de água borada é compartilhada. Os dois tanques são interligados e, portanto, podem ser considerados como um único tanque com capacidade de 500 m^3. Os tanques estão localizados em quatro compartimentos separados no mesmo nível das bombas de remoção de calor residual.

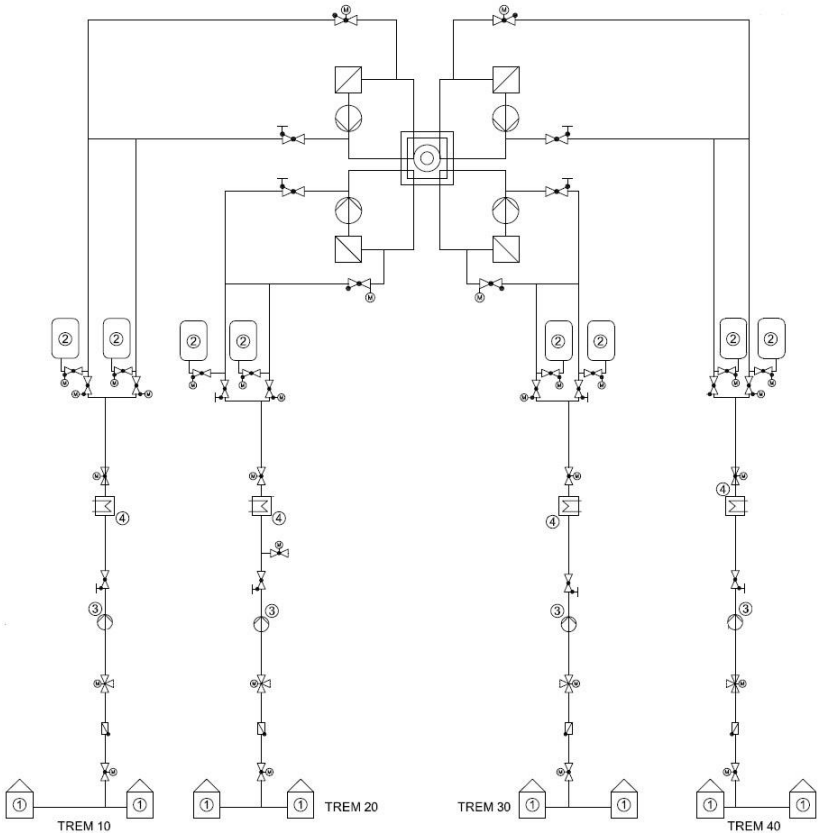

Figura 5 – Planta hipotética dos 4 trens de injeção de baixa pressão e acumuladores de um reator PWR

Considerações e simplificações:

i. Foi desconsiderada a indisponibilidade para cada trem devido à Manutenção;
ii. A falha de causa comum foi considerada para bomba (operação), 2 válvulas de retenção e válvula de bloqueio;

Para que uma planta seja licenciada, diversos cálculos devem ser feitos para que seja comprovada a segurança da usina nuclear. O projeto dos sistemas deve ser efetivo e viável (real) mesmo em caso de falha de algum dos componentes. Portanto, para que a segurança seja garantida e atenda aos padrões internacionais de licenciamento, algumas técnicas já citadas no Capítulo 3 devem ser implantadas. A segurança de independência, diversidade e redundância devem ser geridas a fim de aumentar a confiabilidade dos sistemas.

A Figura 5 mostra um exemplo de redundância, diversidade e independência dos sistemas de injeção de baixa pressão e seus respectivos componentes. Quatro trens de segurança sendo que, para que haja sucesso (inundar o reator), apenas 3/4 dos trens deve funcionar (redundância). As bombas dos respectivos trens são independentes das demais. E por fim, a diversidade pode ser vista pela utilização de componentes de mesma função (exemplo: Bombas), porem de fabricantes diferentes, para reduzir a chance de ocorrência de falha de causa comum.

De acordo com a severidade de um acidente e a frequência de um evento topo, a relação pode ser dita proporcional, ou seja, à medida que a frequência aumenta, a severidade ou gravidade do acidente aumenta. E um dos principais meios de tomada de decisão é o *Risk Informed decision making* (RIDM) (TWEEDDALE, 2003).

RIDM é um método de avaliação de segurança dos sistemas de defesa e emergência. Ele usa as taxas de falha para estimar o risco de uma instalação. Esta estimativa de risco é utilizada juntamente com análises baseadas em padrões para decidir se os investimentos em segurança são justificados e bem alocados. Esta abordagem tem muitos benefícios incluindo uma compreensão bem melhorada da segurança e a identificação de vulnerabilidades.

A Figura 6 mostra a relação entre a probabilidade de ocorrência de um evento e sua consequência. Para estimar a gravidade de um evento, as fontes de risco devem ser identificadas e contabilizadas. Uma vez identificada, a probabilidade e a consequência de cada risco deve ser definida e classificada. Um exemplo de classificação de risco mostrado na Figura 6 é a classificação por cor.

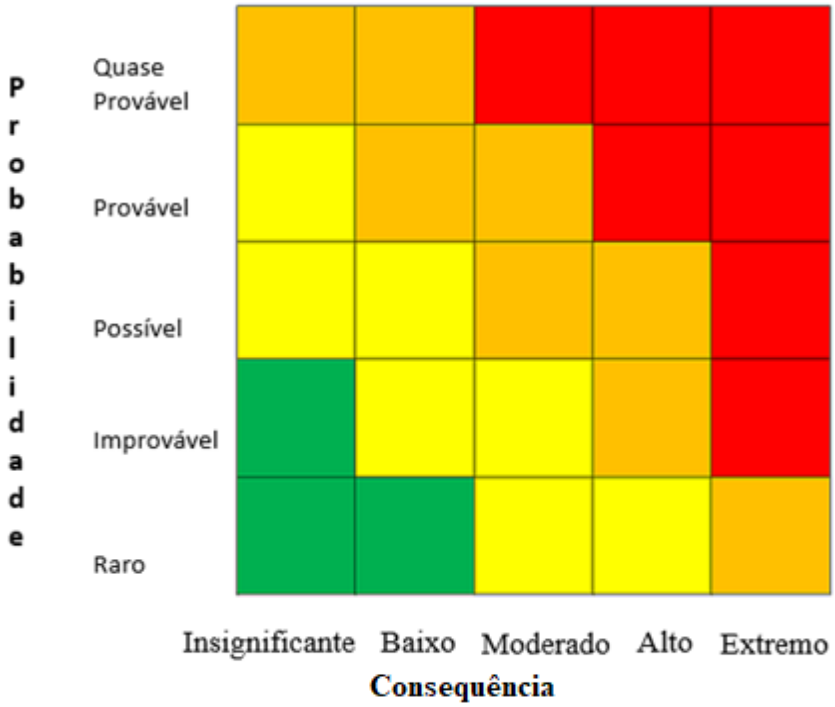

Figura 6 – Probabilidade x Consequência

No quadro das probabilidades, "quase provável" significa que o risco deverá ocorrer na maioria das circunstâncias, "provável" significa que provavelmente ocorreria na

maioria das circunstâncias, "possível" significa que poderia ocorrer em algum momento, "improvável" significa que não se espera que ocorra e "raro" significa que pode ocorrer apenas em circunstâncias excepcionais.

Para as consequências, "extremo" significa que tem um impacto significativo na consecução de metas / objetivos, "alto" ou "moderado" implica impactos altos ou moderados, "baixo" implica impacto apenas em um aspecto limitado de uma atividade e "insignificante" implica que as consequências são tratadas pelas operações de rotina (IAEA, 2016).

2.2. Análise Booleana

Nesta seção, será explicado como a álgebra booleana pode ser aplicada para as árvores de falha.

2.2.1 Álgebra Booleana

A álgebra booleana é comumente utilizada em situações que se ramificam, como por exemplo, uma chave tem a função de abrir ou fechar, as válvulas têm a função de se manter aberta ou fechar, bombas em partir ou não, ou seja, os eventos podem ocorrer ou não. A árvore de falha, como vimos na Figura 4, é um exemplo em que os eventos são ligados a um portão lógico que determina se a falha “passa” ou não para ocasionar o evento topo. Esta relação entre eventos utiliza a álgebra booleana. Por ser uma teoria extensa, a explicação da álgebra será básica e os portões lógicos utilizados neste trabalho serão apenas “OU” e “E”. A Tabela 3 mostra as regras básicas utilizadas na álgebra booleana (NRC, 1981).

Tabela 3 – Regras básicas da álgebra booleana

	Matemático	Simbolismo	Denominação
A	$X \cap Y = Y \cap X$	$X.Y = Y.X$	Comutativa
B	$X \cup Y = Y \cup X$	$X + Y = Y + X$	
C	$X \cap (Y \cap Z) = (X \cap Y) \cap Z$	$X.(Y.Z) = (X.Y).Z$	Associativa
D	$X \cup (Y \cup Z) = (X \cup Y) \cup Z$	$X + (Y + Z) = (X + Y) + Z$	
E	$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$	$X.(Y.Z) = (X.Y) + (X.Z)$	Distributiva
F	$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$	$X + (Y.Z) = (X + Y).(X + Z)$	

De acordo com os itens A e B da Tabela 3, as operações de união e interseção, respectivamente, são comutativas. Em outras palavras, uma operação é comutativa se uma alteração na ordem dos números não altera os resultados. Portanto, as ordens dos números podem ser trocadas.

As relações C e D são semelhantes às leis associativas da álgebra comum, como nas Equações (5) e (6):

$$a.(b.c) = (a.b).c \quad (5)$$

OU

$$a + (b + c) = (a + b) + c \quad (6)$$

Se tivermos uma série de operações "OU" ou uma série de operações "E", as leis associativas nos permitem agrupar os eventos da maneira que quisermos. Em outras palavras, uma operação é associativa se uma alteração no agrupamento não alterar os resultados. Isso significa que o parêntese pode ser movido das Equações (5) e (6).

As relações E F são denominadas distributivas em que expressões podem ser manuseadas sempre que houver uma combinação de operação “E” e “OU”. A propriedade distributiva permite que se remova o parêntese em uma expressão. Para fazer isso, basta multiplicar o valor externo aos parênteses com cada um dos termos entre parênteses.

2.2.2. Árvore de Falhas

Como vimos anteriormente, uma árvore de falhas é um diagrama que utiliza lógica booleana e que possui regras básicas de cálculo. Elas descrevem certos eventos, os chamados eventos iniciadores, que devem ocorrer para que o evento de falha “maior” aconteça, ou seja, relaciona falha em falha. Esta relação é conectada pelos chamados operadores. O operador básico é o "portão" e cada portão possui entradas e uma saída.

A saída do portão é o evento de falha "maior" e as entradas do portão são os eventos de falha mais básicos ("menores”) relacionados à saída. Ao desenhar uma árvore de falha, deve-se pensar na lógica de falhas e ordená-las conforme a atuação do sistema, ou seja, não é um processo padronizado e único (NRC, 1981).

As duas categorias de portas básicas são o portão OU e E. Como esses portões relacionam os eventos exatamente da mesma maneira que a lógica booleana, há uma correspondência biunívoca entre a representação algébrica e a árvore de falhas.

A Figura 7 mostra duas árvores de falha com dois eventos cada, A e B, que são conectados (1a) pelo portão OU e (2a) pelo portão E que ocasionam o evento topo Q.

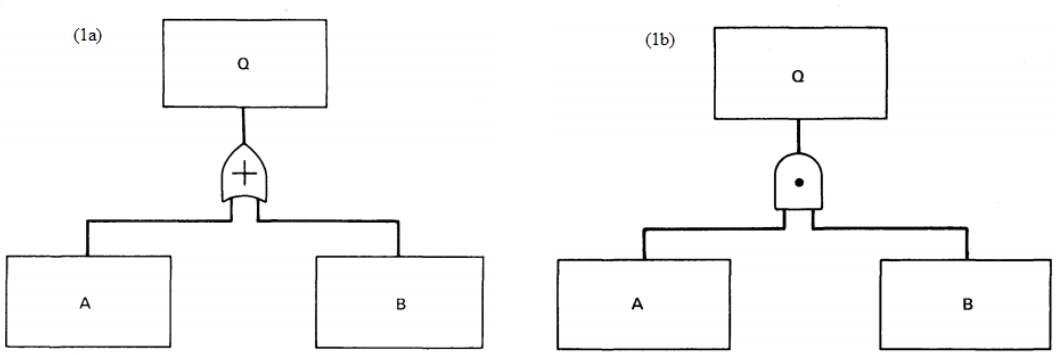

Figura 7 – Exemplo de árvores de falha com operadores “Ou” e “E”

A Figura 8 exemplifica uma situação de árvore de falha com 4 eventos iniciadores independentes (A, B, C e D) para uma representação do evento topo T. O cálculo a seguir mostra como os eventos iniciadores contribuem para o evento topo. De acordo com a lógica, as combinações de eventos são:

I. A;

II. B;

III. C;

IV. AB, AC e AD.

Estes eventos únicos (A, B e C) são eventos de maior contribuição para que ocorra o evento topo T e são chamados de cortes mínimos. Ou seja, basta a falha de um deles para que ocorra o T. Isto se dá pelo fato de a lógica seguir com portão “E” ligados aos Eventos 1 e 2, mas coexistir nas ramificações os eventos únicos (A, B e C) e portões “OU”.

Por outro lado, o evento iniciador D só será o causador do evento topo T combinando com os demais eventos, como visto no item IV.

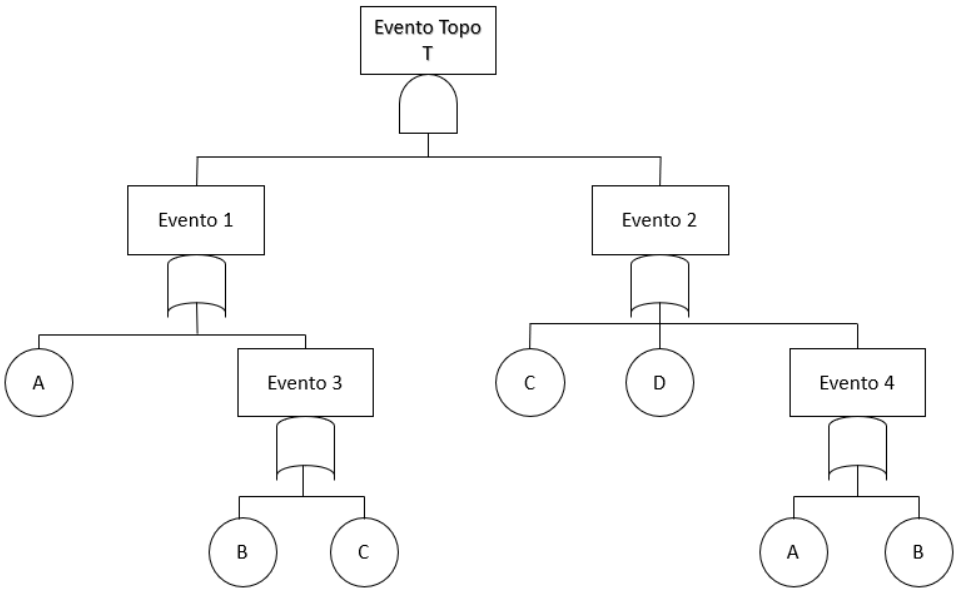

Figura 8 – Exemplo de árvore de falha com 4 eventos iniciadores.

T= [Evento 1] * [Evento 2]

[Evento 1]= A + [Evento 3] [Evento 2]= C + D + [Evento 4]

[Evento 3]= B + C [Evento 4]= A + B

Substituindo os valores de [Evento 1], [Evento 2], [Evento 3] e [Evento 4] em T, temos:

T={A+[Evento 3]} * {C+D+[Evento 4]}

T=A*C+A*D+A*[Evento 4]+C*[Evento 3]+D*[Evento 3]+ [Evento 3]*[Evento 4]

T={A*C+C*(A+B)+C*[Evento 4]}+A*D+A*[Evento 4]+D*[Evento 3]+B*[Evento 4]

T=C+A*D+A*[Evento 4]+D*[Evento 3]+B*[Evento 4]

T=C+A*D+A*(A+B)+D(B+C)+B*(A+B), sabendo que A*(A+B)=A e B*(A+B)=B

T=C+A+B+AD+BD+CD.

2.2.3. Árvore de Eventos

Após ser calculada a frequência topo, a próxima etapa é avaliar a consequência da estimativa do valor do risco. Para este trabalho foram utilizadas árvores de eventos. Elas

consistem na representação gráfica de vários cenários de acidentes que possam ocorrer em decorrência de um evento iniciador. Uma árvore de eventos é gerada ao combinar, a partir de um evento iniciador, uma sequência de cenários decorrentes do sucesso ou falha dos sistemas de emergência da planta (KUMAMOTO, 2007).

A árvore do evento leva em conta os sistemas que estão relacionados ao evento e que, por critérios de sucesso ou falha dos respectivos sistemas, a sequência termine em recuperação ou dano ao núcleo. A Figura 9 mostra um exemplo de árvore de eventos com os sistemas de segurança a partir de um evento iniciador de ruptura e tubulação. Os sistemas são representados como blocos e com setas de sucesso ou falha da função para cima ou para baixo, respectivamente.

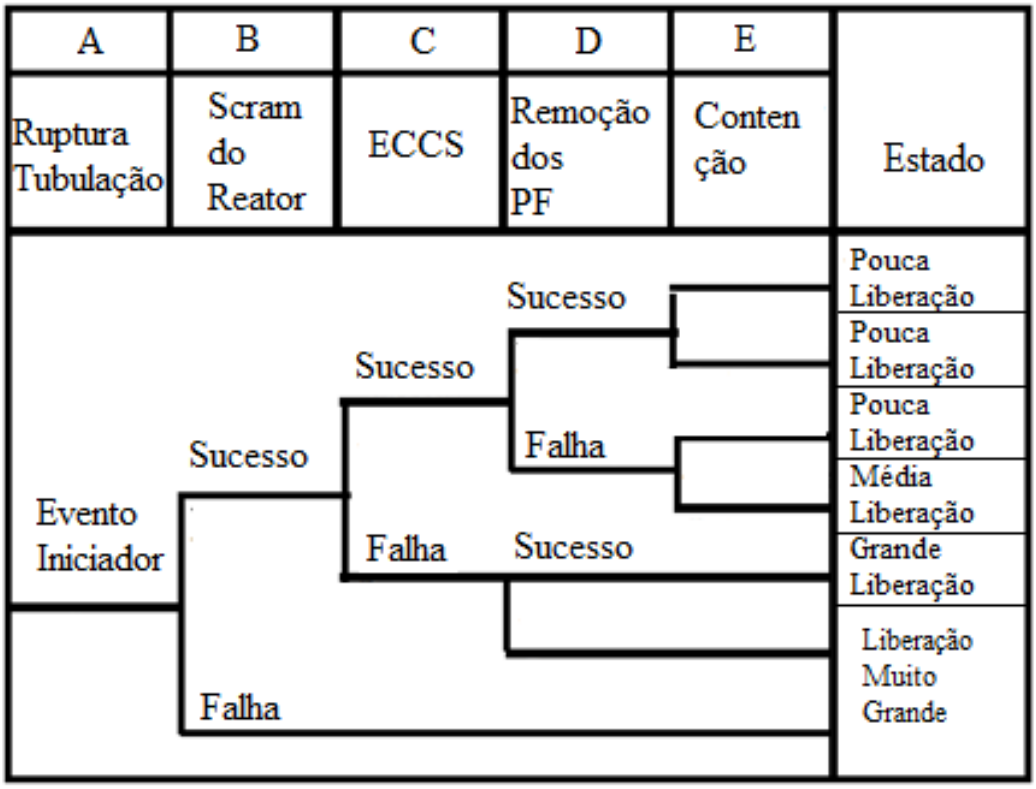

Figura 9 – Exemplo de árvore de evento para um evento iniciador de ruptura de tubulação

Fonte: Kumamoto, 2007

2.3. Componentes

Esta seção relata a análise que foi realizada no sistema de injeção de baixa pressão para encontrar a frequência de falha combinada dos 4 trens de emergência., como visto na Figura 5, e a construção das árvores de falhas usando o software SAPHIRE.

Foram considerados, para cada trem:

I. 1 bomba;
II. 1 válvulas retenção do sistema;
III. 7 válvulas de bloqueio;
IV. 1 trocador de calor;
V. 1 válvula tripla.

Existem várias classificações de falha de um componente. Elas podem ser:

i. Missão;
ii. Demanda;
iii. Espera.

Todos esses casos diferem na percepção de falha do sistema. A falha de um componente em missão considera o ponto de vista de seu funcionamento por um período de tempo especificado, como é o caso da bomba do sistema primário que deve operar continuamente no período em que o reator estiver frio a potência zero até a remoção de calor residual no desligamento.

A falha em demanda ocorre em um instante de tempo, ou seja, o funcionamento de um gerador diesel só ocorre depois que o mesmo é ligado. Ao tentar ligar o gerador, ele pode falhar, ocorrendo uma falha na demanda. Isto pode ocorrer em bombas dos sistemas de emergência. Por exemplo, um dos cenários já discutidos é o LOCA. O sistema

requerido para ajudar na refrigeração e evitar o dano severo é objeto de estudo deste trabalho, e, a falha da bomba em ligar é um exemplo de falha em demanda. Em geral, a frequência de falha na demanda de um componente é baixa (IAEA, 1988).

Ao modelar os componentes em espera, as falhas durante o modo de espera devem ser contabilizadas. As falhas que ocorrem durante o modo de espera não são reveladas até um teste ou uma demanda de componente real, portanto, geralmente estão incluídas no modelo como uma falha relacionada à demanda. Nesses casos, a falha relacionada à demanda deve compreender as falhas cujo mecanismo está puramente relacionado à demanda e também falhas relacionadas ao tempo que o componente gastou em uma condição de espera. Para componentes em espera, se a taxa de falha for determinada com base na experiência operacional, ela é baseada em operação registrada durante o desempenho do teste, o que geralmente é uma ou várias horas. No caso real, componentes específicos são necessários para operar por momentos que diferem substancialmente daquele que foi a base para a determinação da taxa de falha.

Tabela 4 – Siglas de modos de falha

Modos de Falha	
O	Falha em abrir
E	Falha em Fechar
D	Falha em Manter a Posição
T	Quebra
F	Falha em Funcionar
Q	Obstrução
R	Falha em Operar

Tabela 5 – Siglas da lógica inserida no programa SAPHIRE

Lógica da Árvore	
FLB	Falha Local por Bloqueio
FPE	Falha Prévia de Entrada
LF	Falha Local de Apenas um Componente
F	Falha do Trecho ou Componente

A Tabela 4 mostra siglas de modos de falhas que serão atribuídos a cada componente do sistema em questão. A Tabela 5 mostra a lógica utilizada para a montagem da árvore de falha no programa SAPHIRE. O sistema foi divido em nós e trechos. A Tabela 6 mostra uma planilha com os modos de falha e a frequência de cada componente do Trem 1.

Tabela 6 – Componentes do Trem 1, modos de falha e taxa de falha por ano

Componente	Sigla	Descrição do Modulo de Falha	Módulo	Taxa de Falha (por ano)
Tanque	T-TREM1	Ruptura no Tanque	-	2,28E-04
Válvula retenção	VC2-TREM1	Válvula retenção Falha em Abrir	Demanda	6,22E-03
Válvula tripla	VT2-TREM1	Falha da Válvula Tripla em Manter a Posição	Espera	5,30E-08
Bomba	B2-TREM1	Falha da bomba em funcionar	Missão	1,60E-05
Válvula de Bloqueio	VB5-TREM1	Válvula Motora Falha em Abrir	Missão	1,63E-04
Trocador de Calor	TC1-TREM1	Ruptura no Trocador de Calor	-	3,00E-06
Válvula de Bloqueio	VB6-TREM1	Válvula Motora Falha em Abrir	Demanda	1,63E-04
Válvula de Bloqueio	VB7-TREM1	Válvula Motora Falha em Abrir	Demanda	1,63E-04
Válvula de Bloqueio	VB8-TREM1	Válvula Motora Falha em Abrir	Demanda	1,63E-04
Válvula de Bloqueio	VB9-TREM1	Válvula Motora Falha em Abrir	Demanda	1,63E-04
Válvula de Bloqueio	VB10-TREM1	Válvula Motora Falha em Abrir	Demanda	1,63E-04
Válvula de Bloqueio	VB11-TREM1	Válvula Motora Falha em Abrir	Demanda	1,63E-04

A Figura 10 mostra os componentes do Trem 1 que serão utilizados na criação da árvore de falha no programa SAPHIRE. Para cada Trem, os componentes serão diferenciados por um código (ex: VB7-TREM1 e VB7-TREM2).

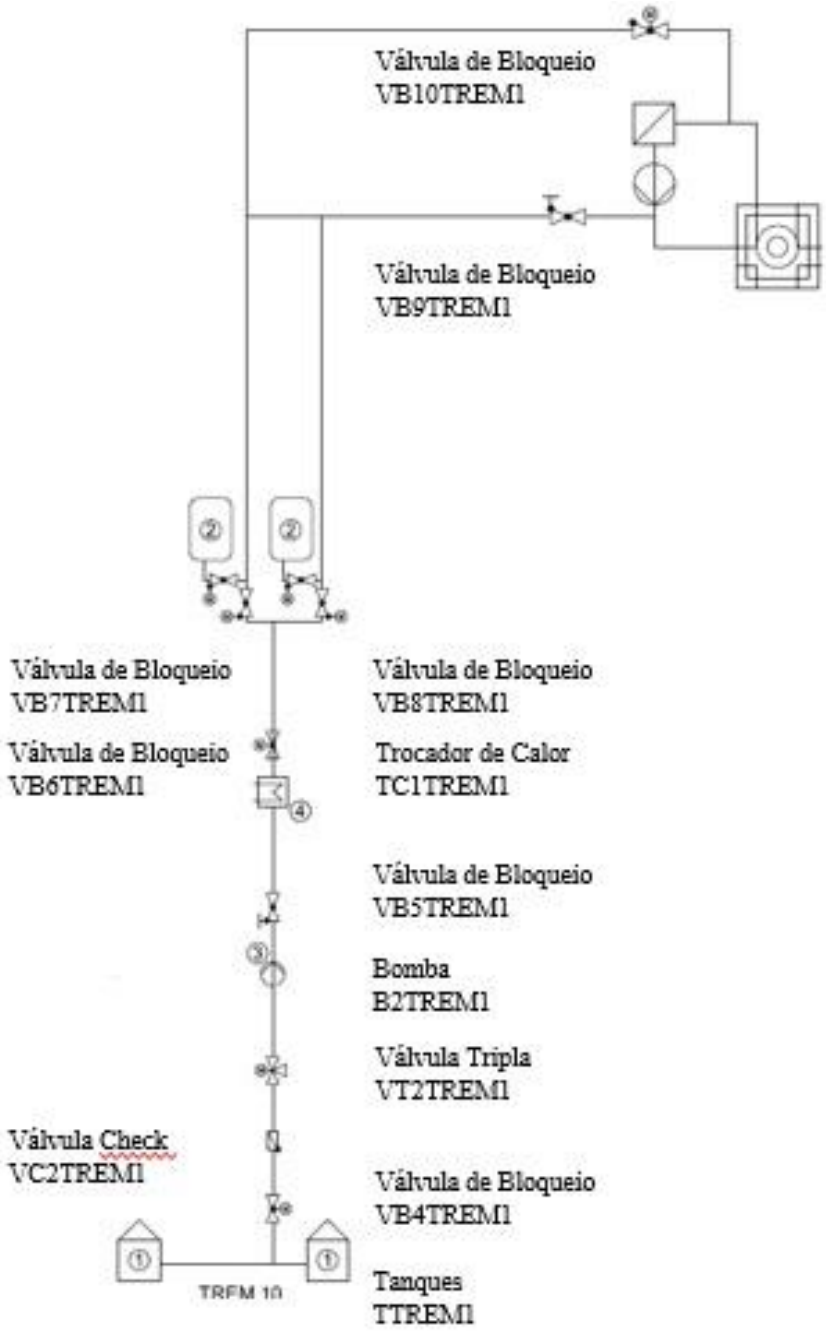

Figura 10 – Trem de falha 1 e nomenclatura dos componentes

2.4. Importância dos componentes

Vimos na subseção anterior que os componentes podem ser classificados de acordo com a sua função em missão, demanda ou espera. Esta subseção irá mostrar, a partir de um olhar qualitativo, a importância dos componentes e qual componente causará maior dano ao sistema, caso ele não funcione. Para isto teremos que definir o tempo de missão para cada componente. Voltando à Tabela 4, vemos que os únicos componentes com módulo de missão são a bomba B1 e a válvula de bloqueio VB5. Para que o reator consiga sair de um acidente severo LBLOCA e reduza os efeitos de derretimento do núcleo, os sistemas de emergência devem funcionar até que o calor residual caia a um nível aceitável. PETRANGELI (1988) diz que as bombas dos sistemas de emergência conseguem manter o núcleo coberto e resfriado até 20 horas após o acionamento do sistema. Portanto, para o cálculo de importância, os valores de frequência de falha e missão foram adicionados na Tabela 7.

Tabela 7 - Cálculo de importância para os componentes do trem 1

Componente	Descrição do Modulo de Falha	Módulo	Tx falha ou Prob	Missão (Horas)	Indisp
Tanque	Ruptura no Tanque	-	2,60E-08	-	2,60E-08
Válvula de retenção	Válvula retenção Falha em Abrir	Demanda	7,10E-07	-	7,10E-07
Válvula tripla	Falha da Válvula Tripla em Manter a Posição	Espera	6,05E-12	-	6,05E-12
Bomba	Falha da bomba em funcionar	Missão	1,83E-09	20	3,66E-08
Válvula de Bloqueio	Válvula Motora Falha em Abrir	Missão	1,86E-08	20	3,72E-07
Trocador de Calor	Ruptura no Trocador de Calor	-	3,42E-10	-	3,42E-10
Válvula de Bloqueio	Válvula Motora Falha em Abrir	Demanda	1,86E-08	-	1,86E-08
Válvula de Bloqueio	Válvula Motora Falha em Abrir	Demanda	1,86E-08	-	1,86E-08
Válvula de Bloqueio	Válvula Motora Falha em Abrir	Demanda	1,86E-08	-	1,86E-08
Válvula de Bloqueio	Válvula Motora Falha em Abrir	Demanda	1,86E-08	-	1,86E-08
Válvula de Bloqueio	Válvula Motora Falha em Abrir	Demanda	1,86E-08	-	1,86E-08
Válvula de Bloqueio	Válvula Motora Falha em Abrir	Demanda	1,86E-08	-	1,86E-08

A Tabela 8 mostra os valores retirados do programa SAPHIRE para o cálculo de importância. A Figura 11 mostra o diagrama de Pareto para RRW acumulado.

Tabela 8 – Resultado do programa Saphire para a análise de importância

Componentes	FV	RRW	RRW acumulado	%	RRW acumulado %	RAW
VC2-TREM1	6,10E-01	2,565	2,565	20%	20%	8,59E+05
VB5-TREM1	3,97E-01	1,47	4,035	11%	31%	8,59E+05
B2-TREM1	3,15E-02	1,032	5,067	8%	39%	8,59E+05
T-TREM1	2,24E-02	1,023	6,09	8%	46%	8,59E+05
VB6-TREM1	1,60E-02	1,016	7,106	8%	54%	8,59E+05
TC1-TREM1	2,94E-04	1	8,106	8%	62%	8,59E+05
VT2-TREM1	5,20E-06	1	9,106	8%	69%	8,59E+05
VB8-TREM1	5,73E-10	1	10,106	8%	77%	1,03E+00
VB7-TREM1	5,73E-10	1	11,106	8%	85%	1,03E+00
VB9-TREM1	5,73E-10	1	12,106	8%	92%	1,03E+00
VB10-TREM1	5,73E-10	1	13,106	8%	100%	1,03E+00

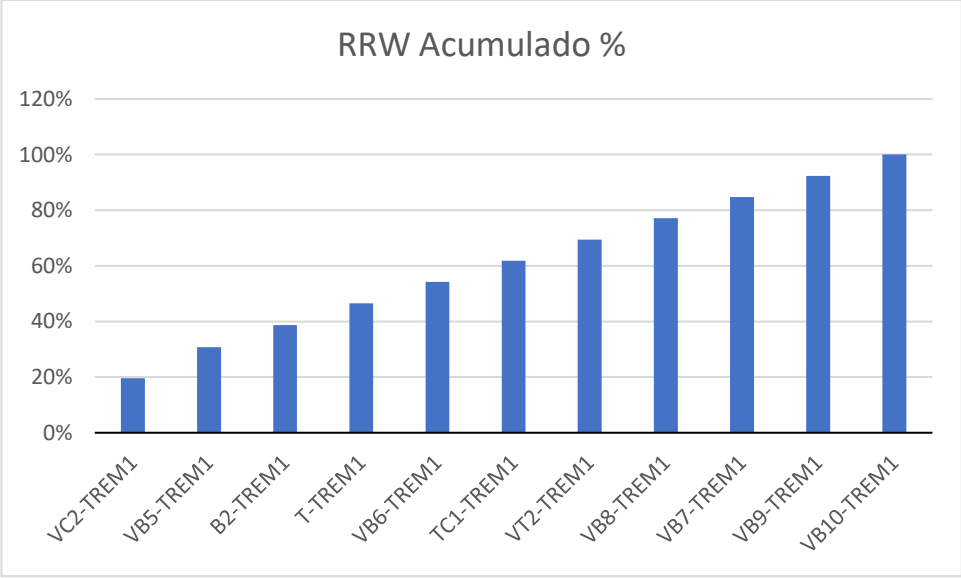

Figura 11 - RRW Acumulado para componentes do trem 1.

A Figura 11 mostra que os componentes válvula de retenção 2 e válvula de bloqueio 5 são os mais propensos em falhar. Este resultado condiz com os valores de taxa de falha de **7,10E -07** e **3,72E-07** da Tabela 7.

Portanto, para o cálculo da árvore de falha combinada de *safety* e *security*, será adicionado, além das probabilidades de sabotagem dos adversários, o valor da taxa de falha apenas do componente da válvula de retenção 2. Este valor é justificado pelo gráfico 1 e pela Tabela 8.

2.5. Análise de falha de segurança dos sistemas de baixa pressão

Vimos nas subseções anteriores que os componentes são redundantes e independentes para cara trem do sistema de emergência. Para que haja dano ao núcleo, como vimos na Tabela 2, o sistema de 4 redundâncias deve falhar com o portão de votação 2/4 para que ocasione o ramo L3 de dano ao núcleo. Portanto, na árvore de eventos criada no programa SAPHIRE, como mostra na Figura 12, deverá existir um portão 2/4 que ligue os trens de 1 a 4.

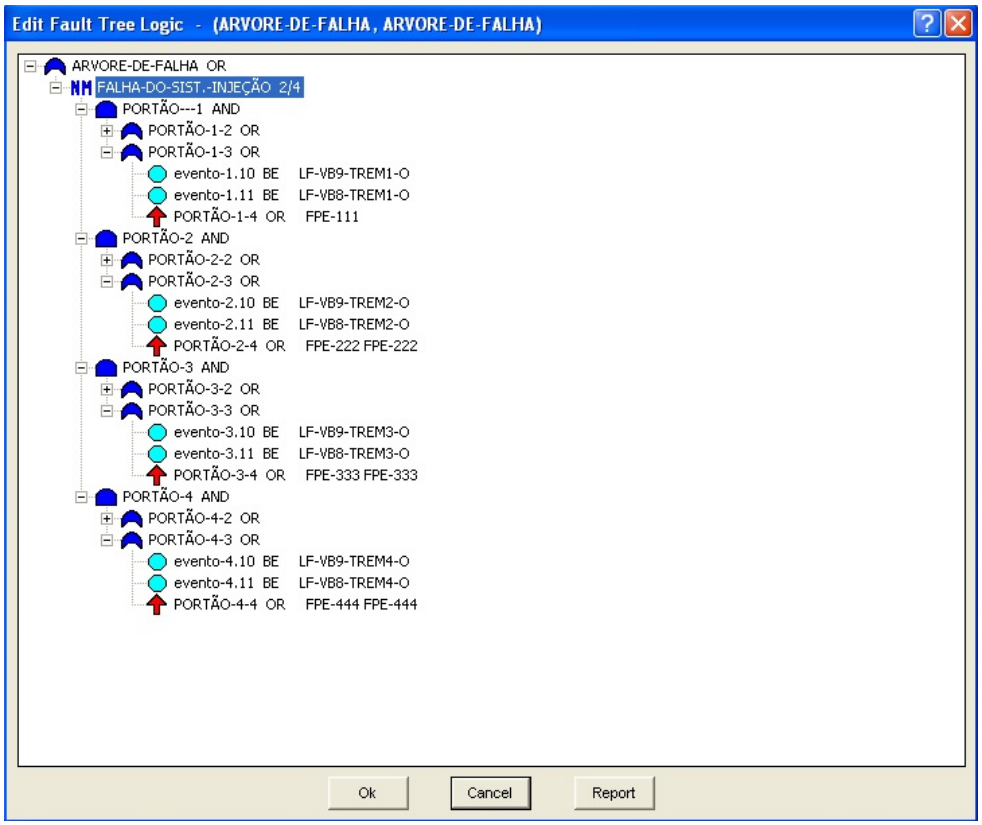

Figura 12 – Lógica da árvore de falha para o sistema de injeção a baixa pressão de 4 trens redundantes

A Figura 13 mostra a árvore apenas do Trem 1. Nela podemos ver a lógica com portões “Ou” e “E”.

O portão 1-4 é duplicado e inserido nos portões 1-2 e 1-3 por existir uma ramificação na injeção de água na perna quente e fria do sistema primário (rever a Figura 10). Os componentes tanque, válvula de retenção 2, válvula tripla 2, bomba, trocador de calor e válvulas de bloqueio 5 e 6 são compartilhadas (rever a Figura 10).

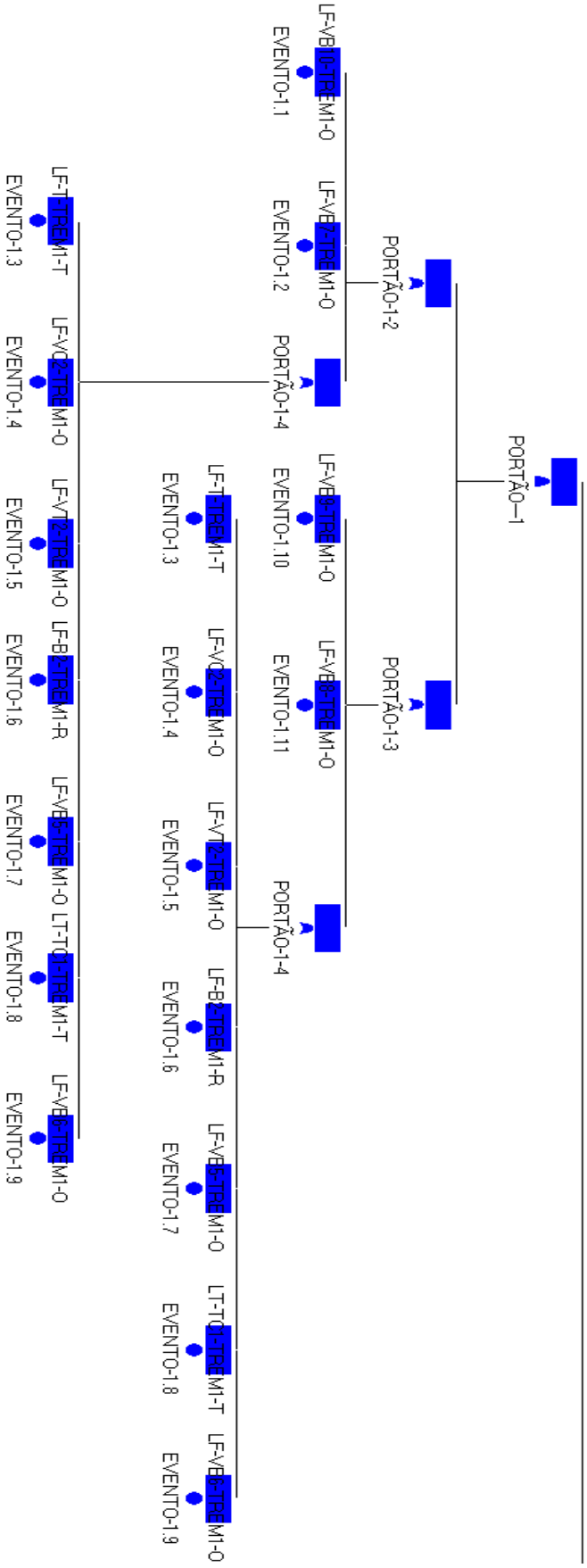

Figura 13 – Árvore de falha do trem 1.

De acordo com a lógica implantada no programa SAPHIRE, o valor de frequência de falha por ano do sistema de injeção de baixa pressão com portão de votação 2/4 é de **2,769E-04** por ano.

2.6. Cálculo do Risco para o sistema de baixa pressão

Para que seja feita e estimativa do risco, deve ser calculado o valor da consequência do evento. De acordo com o *International Nuclear and Radiological Event Scale* (INES), os eventos podem ser classificados em uma escala de 0 a 7, sendo 7 o mais severo. Os níveis de 1-3 são classificados de "incidentes", enquanto os níveis de "4-7" são chamados de "acidentes" (IAEA, 2013).

Os acidentes são definidos como qualquer evento, incluindo erros de operação, falhas de equipamentos, cujas consequências potenciais não sejam desprezíveis do ponto de vista da proteção ou segurança. O termo incidente descreve eventos que são, de fato, acidentes menores, ou seja, que se distinguem dos acidentes apenas em termos de serem menos severos. A Figura 14 mostra a INES.

Figura 14 – Escala de acidentes e incidentes

Fonte: INES, 2013.

O valor de consequência pode ser calculado através da Equação (7) (INES, 2013):

$$C = 0{,}8 * 10^{N-7} \quad (7)$$

Onde:

N = Nível do evento que resultou após a falha dos componentes do sistema.

Neste trabalho, a sabotagem do sistema de injeção de baixa pressão é classificada como nível 5 com um médio lançamento de materiais radioativos para fora da contenção. O valor de consequência relativa associado C é **8,0E-02**.

Aplicando o valor da consequência para o cálculo do risco, o valor de risco associado a cada cenário de falha é estimado pela multiplicação do valor da consequência, calculada pelo INES, com a frequência de falha, calculada na subseção anterior, como mostra na equação (2). O resultado do risco é de **2,22E-05** por ano.

3.SECURITY

A análise de *Security* é baseada em sistemas que previnem ou detectam ataques de adversários. A detecção e a prevenção remetem à ideia de mitigar e se antecipar perante uma ação de uma ameaça humana e exige que reconheçamos a capacidade do adversário humano para se adaptar e, portanto, eventualmente derrotar o sistema de proteção física.

Esta seção tem o objetivo de analisar, através de cálculos e probabilidades, caminhos que possam ser feitos por um adversário para que a missão seja bem-sucedida. O caminho será completo, ou seja, o adversário terá que passar por todas as barreiras físicas de proteção da instalação, desde o ponto mais externo da instalação, denominada área vigiada, até o seu alvo, localizada na área vital, sem que seja interrompido até o ponto de detecção crítica.

Existem duas preocupações quanto à segurança nuclear, que são o roubo de materiais nucleares ou radioativos e sabotagem de equipamentos da instalação com o intuito de gerar consequências e risco para a população. Para este trabalho, o enfoque será a sabotagem do sistema primário que resulta em um acidente severo LBLOCA e os sistema de injeção de água a baixa pressão.

No capítulo anterior, vimos que 2/4 do sistema de emergência deve falhar para que cause danos ao núcleo no ramo L3. No entanto, está sessão irá demonstrar através de probabilidades de detecção de sensores, os caminhos que os adversários deveram fazer para que completem a missão. A instalação é hipotética e baseada em sistemas e *layout* de um reator do tipo PWR.

Para que seja simplificada, o caminho escolhido pelo adversário será o de maior vulnerabilidade, ou seja, o caminho com o maior risco associado. Esta simplificação é primordial, pois inúmeros caminhos podem ser feitos pelo adversário, no entanto, poucos caminhos são tão efetivos para que a missão seja bem-sucedida.

Pelas equações (1), (2), (3) e (4), devem ser calculados os parâmetros de segurança como probabilidade de interrupção, probabilidade de neutralização, a frequência de ataque de segurança, o valor de consequência relacionado ao nível de acidente (baseada no INES) e a estimativa do valor do risco de caminho associados.

Para que seja bem entendido, alguns termos utilizados em *security* que aparecem para o cálculo e aplicação da metodologia devem ser definidos (HAWILA, 2016):

- **Segurança ou Prevenção de Perdas**

Emprego de tecnologias apropriadas para a identificação de perigos de uma instalação de processos e a eliminação dos mesmos antes da ocorrência de um acidente.

- **Incidente**

Perda de contenção de material ou energia

- **Acidente**

Evento ou sequência de eventos de ocorrência anormal, que resulta em consequências indesejadas ou em perda, dano ou prejuízo pessoal, ambiental ou patrimonial.

- **Evento Indesejado**

Evento iniciador de um cenário acidental.

- **Evento Iniciador de Acidente**

É qualquer evento cuja ocorrência demande a operação de um ou mais sistemas de proteção para que não ocorra um acidente em uma instalação industrial.

- **Cenário**

Conjunto formado pelo perigo identificado, suas causas e cada um dos seus efeitos.

- **Cenário Acidental**

Sequência lógica de eventos que, a partir de um evento indesejado, conduz o sistema industrial a um estado de perigo.

- **Perigo**

Condição física ou química que possui o potencial de causar danos às pessoas, à propriedade ou ao meio-ambiente.

- **Risco**

Medida de ferimentos humanos, danos ambientais, ou perdas econômicas em termos tanto da chance de ocorrência de incidentes como da magnitude das perdas ou ferimentos.

Em *security*, o risco é baseado na análise e agregação de três fatores amplamente reconhecidos: **ameaça**, **vulnerabilidade** e **consequência**.

- **Ameaça**

Utilizada para se referir a um adversário postulado contra o qual as medidas de segurança foram concebidas, enquanto que adversário geralmente se refere a alguém que realmente tenta realizar um ato malicioso (IAEA, 2015).

- **Vulnerabilidade**

1. Uma característica física ou atributo operacional que torna uma entidade, um recurso, um sistema, uma rede, uma instalação, uma atividade ou uma área geográfica aberta para exploração ou suscetível a uma determinada ameaça (IAEA, 2015).
2. Fraqueza de um bem ou controle que pode ser explorado por uma ameaça (IAEA, 2015).

- **Consequência**

Definida pelo resultado de um evento que pode incluir perda de longo a curto prazo, diretas ou indiretas e imediatas ou não. Tal resultado inclui impactos em diversas camadas como impacto econômico, humano, ambiental e etc. A consequência é calculada a partir da Equação (7). O valor de C usado neste estudo é escalado de 0 a 1 representando a gravidade do evento e projetado para que a gravidade de um evento seja aproximadamente dez vezes maior para cada aumento de nível na escala.

3.1. Programas para o cálculo de P_i e P_n

A análise do caminho do adversário deve ser realizada de maneira sistemática. Os sistemas de segurança e proteção física, como barreiras ou sensores, possuem probabilidade de detecção e atraso. Portanto, a vulnerabilidade consiste em calcular através dos parâmetros, a probabilidade de interrupção (P_i) e probabilidade de neutralização (P_n), vista na Equação (1).

3.1.1. EASI

O programa *Estimate of Adversary Sequence Interruption* (EASI) será utilizado para o cálculo da probabilidade de interrupção em uma análise de interação de detecção, atraso, resposta e comunicação. Ele consiste em um programa Excel em que as entradas

do programa são as probabilidades de detecção de cada sensor que o adversário deverá ultrapassar sem que seja detectado ou que, caso seja detectado, não exista tempo hábil para força de contrarresposta. (GARCIA, 2008)

A Figura 15 mostra um exemplo do programa EASI.

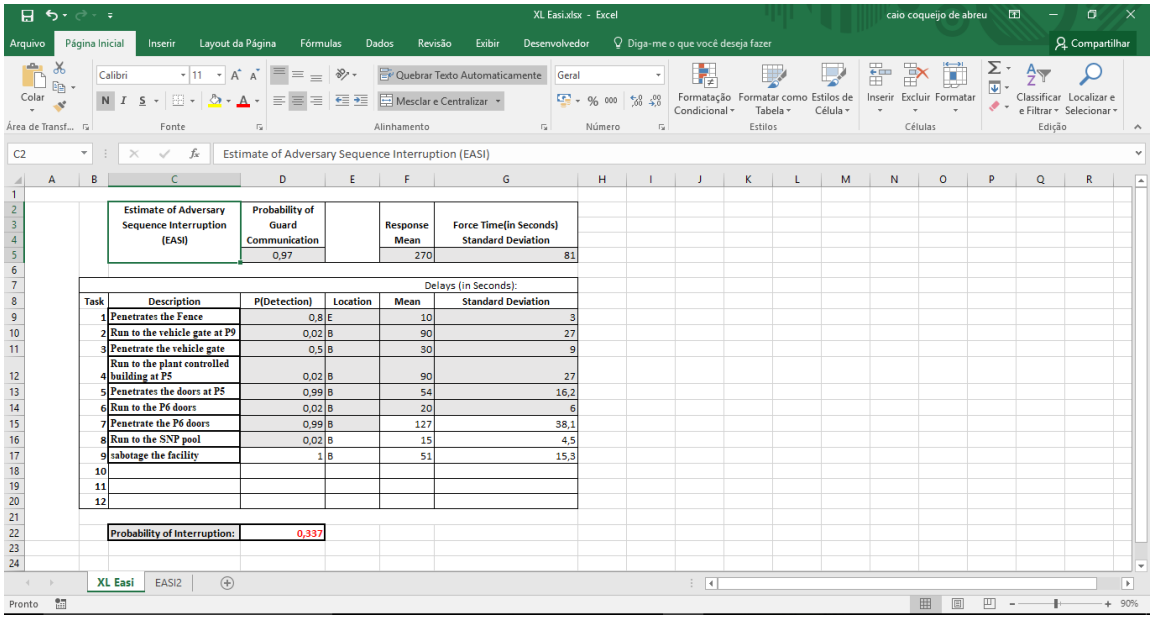

Figura 15 – Exemplo do programa EASI

Existem diversos programas que analisam a interação e avaliam o desempenho do SPF ao longo de um caminho específico e sob condições específicas de ameaça e operação do sistema (GARCIA, 2008). São eles:

I. FESEM (Forcible Entry Safeguards Effectiveness Model)

II. ISEM (Insider Safeguards Effectiveness Model)

III. SAFE (Safeguards Automated Facility Evaluation)

No entanto, alguns deles utilizam modelos antigos e outros estão em desenvolvimento. Portanto, o EASI, por ser fácil e acessível, é um programa satisfatório para este trabalho por atender todas as demandas (GARCIA, 2008).

No programa EASI, os parâmetros de entrada representam as funções de proteção física de detecção, atraso e resposta. Os parâmetros de atraso e respostas são inseridos no programa em forma de tempo médio e desvio padrão, como pode ser visto na Figura 15, colunas “F” e “G”. O tempo de resposta, o desvio padrão e a probabilidade de comunicação dos guardas são parâmetros necessários para o cálculo de P_i.

Por fim, o valor de P_d de cada sensor deve ser inserido no modelo de forma ordenada com o caminho do adversário. O P_d é calculado através da Equação (8):

$$P_d = P_S \; x \; P_T \; x \; P_A$$

onde:

P_S= Probabilidade de que o detector detecte atividades anormais ou não autorizadas por adversários;

P_T= Probabilidade de uma indicação de alarme ser transmitida para um ponto de avaliação;

P_A= Probabilidade de uma avaliação precisa do alarme.

Os valores de P_d utilizados para o cálculo de interrupção serão retirados do vigésimo sétimo curso de Treinamento Internacional - *Hypothetical Facility Exercise Data Handbook* (HARI, 2017).

3.1.2. Excel Macro

Para o cálculo da P_N, será utilizado um programa de neutralização feita por macro do Excel. A Figura 16 mostra o exemplo da macro.

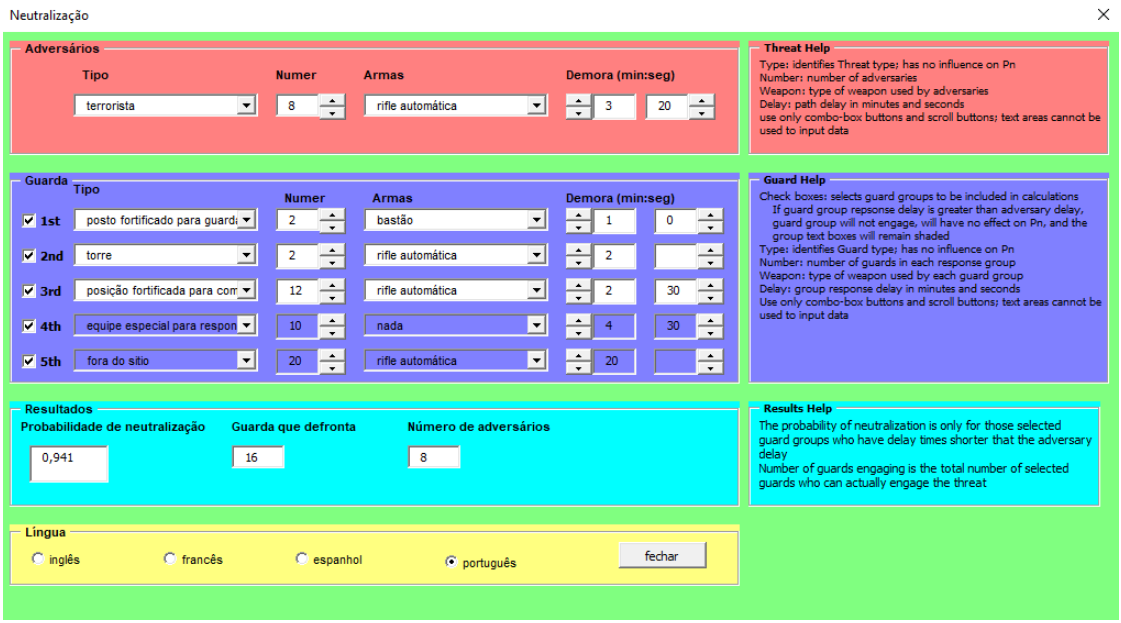

Figura 16 – Exemplo da macro feita no programa Excel para o cálculo do Pn

Este programa usa um conceito derivado de um modelo de Markov, na qual os valores da tabela de dados variam de acordo com o número de guardas, número de terroristas e parâmetros de armamento. O programa possui vários tipos de armamentos e cada um deles possui um coeficiente que serve para definir o grau de força das armas e sua letalidade. Uma função de decaimento exponencial é usada para calcular os efeitos na P_N causada quando grupos de resposta sucessivos na ordem de batalha têm tempos de chegada variáveis. O objetivo desta técnica básica é enfatizar os três fatores mais importantes para a resposta (Snell, 2013):

• Números (um grupo de ameaças, até cinco grupos de resposta);

• Armas (nenhum, bastão, revólveres, rifles);

• Tempos de chegada (atraso do caminho do adversário e tempos de resposta).

O método da planilha é baseado em uma série de hipóteses:

I. As armas superiores aumentam P_N para números iguais de guardas e adversários;

II. Números de guardas relativos ao adversário superiores aumentam P_N para armas iguais;

III. O efeito líquido das armas superiores é a multiplicação da força, onde:

$$P_N = \mathrm{f}\,(E_{guardas} * \mathrm{M}_{guardas}, E_{adversários} * \mathrm{M}_{adversários})$$

M = número de combatentes

E = multiplicador de força de eficácia da arma

IV. A eficácia das armas da regra é usada para $P_N = 0{,}5$;

1 bastão = 2 sem armas

1 arma de mão = 2 bastões

1 rifle automático = 2 armas de mão

V. As forças de resposta são contadas somente na batalha se puderem chegar a tempo de interromper a detecção dada no ponto de detecção crítico;

VI. A probabilidade de neutralização aumenta quando os grupos de resposta chegam mais perto do ponto em que o sensor alarmou.

3.2. Detecção, atraso e resposta

O sistema de proteção física tem como objetivo evitar que o adversário complete a missão em uma ação malevolente ou persuadi-lo de não atacar a instalação devido à dificuldade da missão. Existem meios para que isso possa ocorrer, o primeiro deles é a detecção. A detecção é a capacidade de descobrir a ação do adversário em um tempo hábil. O atraso é a segunda função e tem a capacidade de aumentar o caminho médio e

dificultar o acesso do adversário a sistemas importantes. Por fim, o terceiro é a resposta de guardas e/ou equipes de apoio. A Figura 17 mostra os pilares do SPF (GARCIA, 2008).

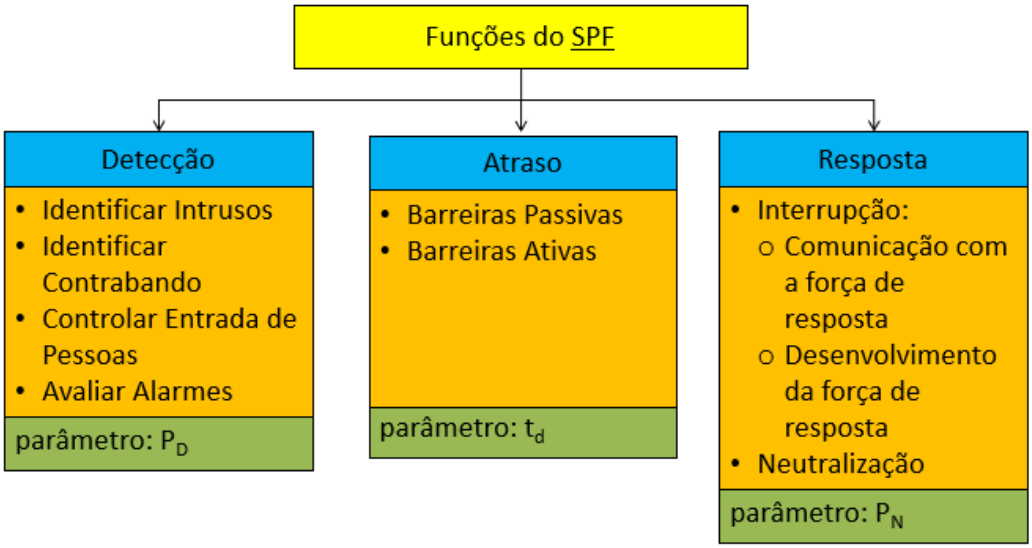

Figura 17 - Pilares do sistema de proteção física

As Figuras 18, 19, 21 e 22 mostram a relação do tempo de tarefa do adversário em completar sua missão versus o tempo de detecção e resposta da força tarefa.

A Figura 18 mostra o tempo de tarefa do adversário, onde:

T_o= Tempo inicial em que o detector alarma;

T_A= Tempo de avaliação do alarme;

T_I= Tempo em que o adversário é interrompido;

T_C= Tempo em que a tarefa está completa;

Como parte das medidas de barreiras de proteção como detectores, paredes e sensores, existe um ponto crítico para que o último elemento de proteção detecte o adversário a tempo de que a força resposta consiga neutralizar. Este ponto é chamado de Ponto de Detecção Crítico (PDC).

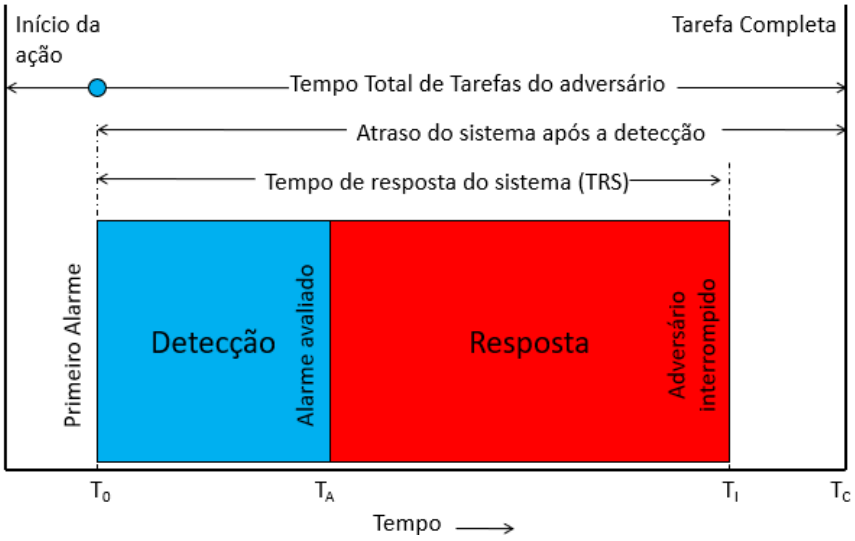

Figura 18 – Exemplo de linha do tempo para uma ação do adversário

A Figura 19 mostra a ineficiência das barreiras e sensores do sistema de proteção física em barrar o adversário. O adversário não possuía quantidade de barreiras mínimas para que seja detectado e seja neutralizado pela força resposta antes de completar sua tarefa.

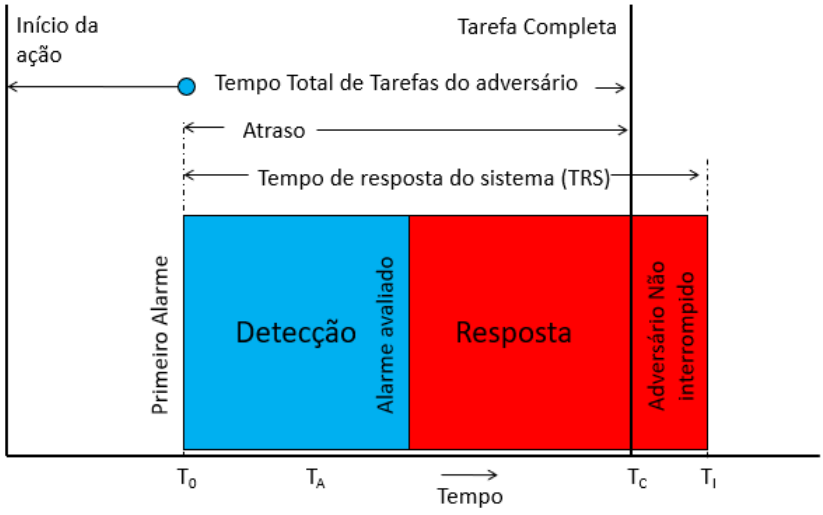

Figura 19 – Exemplo de linha do tempo com deficiência em barreiras de proteção

A Figura 20 exemplifica a quantidade de barreiras para o aumento do tempo de caminho médio do adversário.

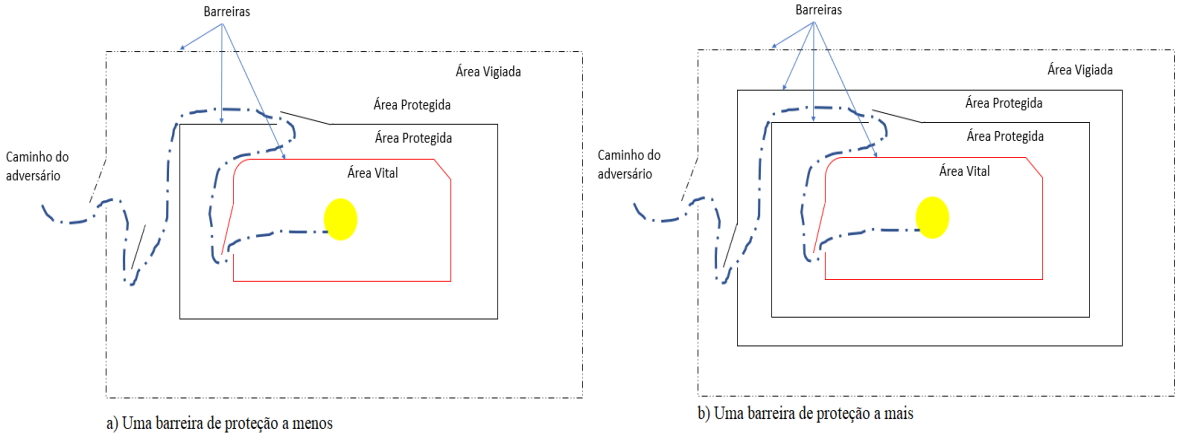

Figura 20 - Exemplo de caminho do adversário com a) mais barreiras e b) menos barreiras

A Figura 21 mostra o atraso do primeiro sensor alarmar, ou seja, o T_o é deslocado para a direita do gráfico da linha do tempo. Existem várias causas para o atraso do alarme, desde detectar um intruso até o tempo de comunicação.

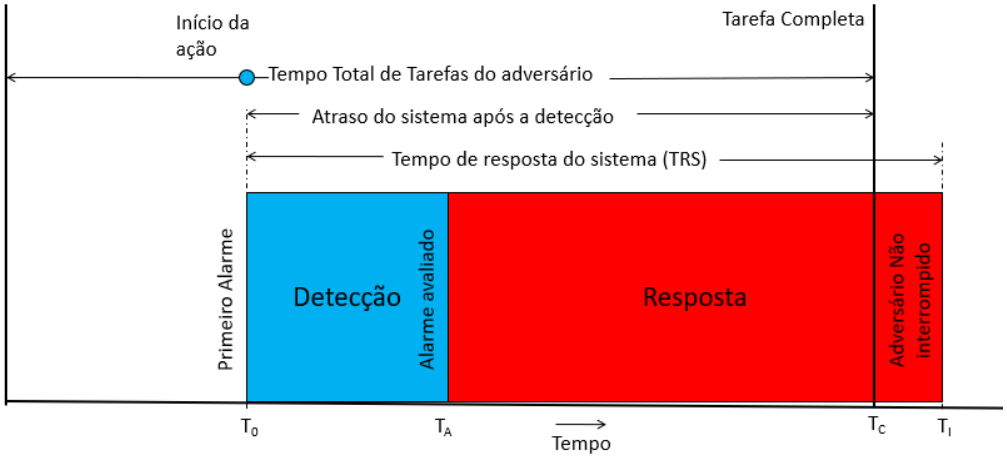

Figura 21 – Exemplo de linha do tempo com o atraso na detecção

E por fim, a Figura 22 mostra o atraso na força resposta após a detecção e comunicação. O tempo de resposta é crucial para o cálculo do PDC, uma vez que o T_I deve ser menor que o tempo total de tarefa do adversário. Caso o ultimo sensor não dê margem de tempo para a resposta dos guardas, a tarefa será completada antes de ser interrompida.

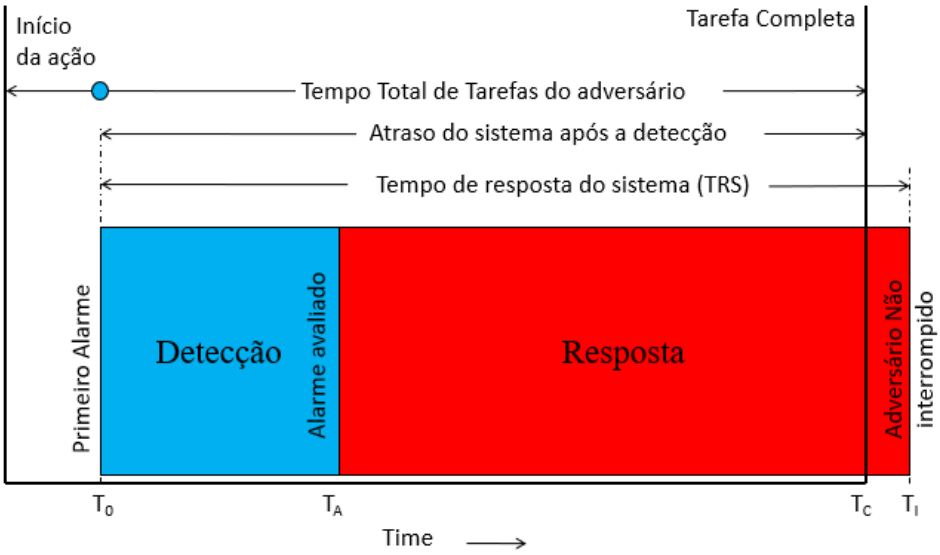

Figura 22 – Exemplo de linha de tempo com atraso na resposta

3.3. Proteção física

De acordo com a norma da CNEN 2.01 de Proteção Física (CNEN, 2017) cada instalação nuclear no Brasil deve submeter um Plano de Proteção Física e requisitos básicos de segurança. Alguns aspectos são levados em consideração quanto à proteção física, são eles:

i. Localização geográfica;

ii. Avaliação de ameaças potenciais;

iii. Controle do acesso à instalação ou ao material nuclear.

A fim de classificar pontos principais de uma instalação nuclear, o projeto deve, a priori, delimitar e projetar áreas de maior risco que são atraentes para sabotagem devido à grande gravidade de consequência radiológica. Existem 3 áreas de segurança consecutivas e adjacentes. São elas, em sequência de grau crescente de proteção, a área vigiada, a protegida e a vital.

A área vigiada é definida como uma delimitação adjacente e exterior às demais áreas que, mantida sob vigilância, é cercada e sinalizada com avisos e sinais que alertam que o acesso àquela determinada área é controlado.

> "O acesso à área vigiada deve ser projetado levando em consideração fatores tais como: compatibilidade com planos para situações de emergência, avaliação de ameaças à segurança e outros casos fortuitos ou de força maior. As áreas para estacionamento de veículos devem ser localizadas, em princípio, no exterior da área vigiada." (CNEN, 2017)

A área protegida é definida como uma área interna à vigiada e envoltória de uma ou mais áreas vitais sob constante proteção e delimitada por barreiras físicas com número reduzido de acesso.

> "A barreira física que circunscreve a área protegida deve ser projetada de modo que seus locais de acesso sejam protegidos e que sua eficácia não seja prejudicada por acidentes geográficos e por estruturas." (CNEN, 2017)

Por fim, a área vital é a parte mais interna das delimitadas. Nela, são localizados equipamentos vitais e/ou material de categoria I no interior de uma estrutura cujas paredes, teto e piso, constituem barreira física. A Tabela 9 mostra as categorias I, II e III que o órgão regulador classifica. As barreiras físicas das áreas vitais devem ser capazes de deter a intrusão de pessoas não autorizadas, a fim de resistir à penetração de objetos

que causem dano ou passíveis de prejudicar o funcionamento dos equipamentos ditos vitais.

> "As áreas vitais devem ser localizadas de modo a que o acesso possa ser limitado a um número reduzido de pessoas autorizadas, evitando-se, sempre que possível, a proximidade de edificações com equipamentos não vitais." (CNEN, 2017)

Tabela 9 – Categorias de matérias nucleares definidas pela CNEN

MATERIAL	**FORMA**	**CATEGORIA I**	**CATEGORIA II**	**CATEGORIA III**
PLUTÔNIO	-	2kg ou mais	Entre 2kg e 500g	500g ou menos
URÂNIO	U-235 contido em urânio enriquecido 20% ou maior Entre 20% e 10% 10% ou menor	5 kg ou mais - -	Entre 5 kg e 1 kg 10 kg ou mais -	1 kg ou menos Menos de 10 kg 10 kg ou mais

Para este trabalho, foi considerado um reator tipo PWR com *layout* hipotético e delimitado de acordo com a norma da CNEN 2.01 como mostra a Figura 23 (CNEN, 2017).

O desenho possui as áreas delimitadas em cores vermelhas de área vital, cor amarela como área protegida e cor verde como área vigiada. Os escritórios estão localizados na área vigiada de controle, assim como o estacionamento particular dos funcionários. O estacionamento para as demais pessoas está localizado externo à área vigiada. O acesso tanto para a área vigiada quando para a área protegida é restrito e identificado com os nomes de "Posto de Acesso 1" e "Posto de Acesso 2". Por fim, a área vital é composta por todos os prédios que são circundados pela área protegida (linha amarela) e identificadas pela linha vermelha. São eles:

i. Sistemas de Segurança de injeção de água a baixa pressão - Trem 1,2,3 e 4;

ii. Prédio das Turbinas;

iii. Prédio do reator composto por sala de controle e laboratórios;

iv. Prédio de rejeitos e laboratórios secundários.

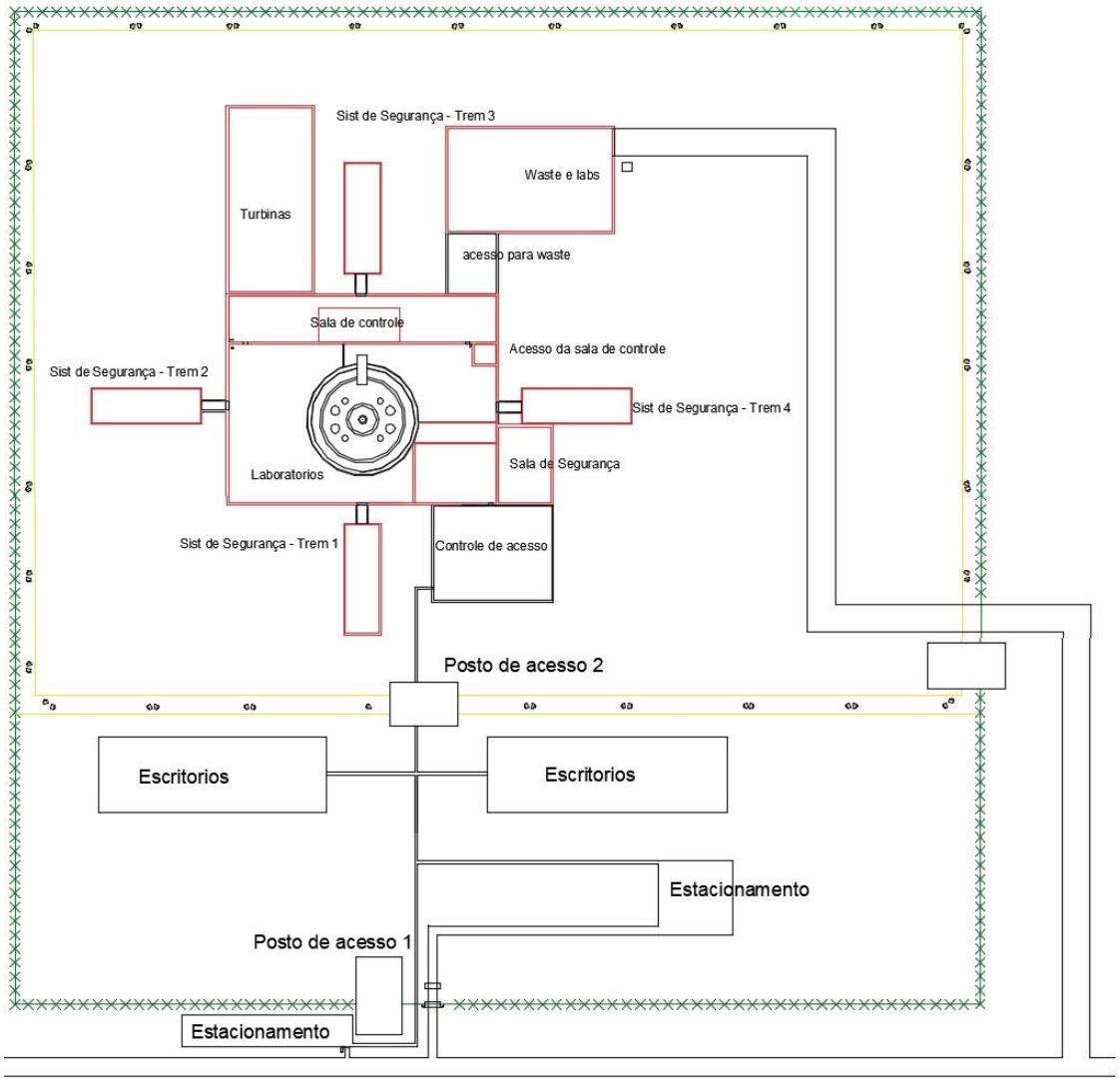

Figura 23 – Layout do reator do tipo PWR

Os sistemas de segurança redundantes respeitam o critério de afastamento. Outro critério de segurança imposto pela CNEN é que todos os prédios devem conter uma porta de emergência apenas com abertura pela parte interna e devem ser providas de dispositivos de alarme contra intrusão (CNEN, 2017).

3.4. Diagrama de Sequência do Adversário

Existem diversas maneiras de projetar um sistema de proteção física. A avaliação da segurança, segundo o órgão regulador, possibilita que sejam aceitos ou não os planos de emergência e mecanismos implantados. No entanto, diferentes caminhos geram inúmeras possibilidades de ataques maliciosos. Alguns mecanismos de segurança como implantação de sensores, controle de acesso por monitoramento, parede de maior espessura, limitação do acesso em áreas vitais, etc., são alguns exemplos de proteção de detecção e atraso. A combinação destes fatores, onde cada elemento de proteção possui sua própria probabilidade de detecção (P_D) e tempo de atraso (T_D), gera dificuldade quanto ao ataque malicioso.

Como visto anteriormente, o Ponto de Detecção Crítico (PDC) é o último componente de detecção que, ao alarmar, proporciona tempo hábil à força de resposta para interromper os adversários antes de completar a missão. Este ponto está diretamente ligado à sequência de componentes de segurança que levam ao atraso do adversário.

Do ponto de vista do projetista, o caminho de maior interesse é o que gera mais combinações das probabilidades mínimas de interromper e neutralizar o adversário e, por conseguinte, o que gera maior risco e tem a maior probabilidade de sucesso da missão.

A eficácia do sistema de proteção está ligada à probabilidade de interrupção (P_I) e à probabilidade de neutralização (P_N) como mostra a Eq (9):

$$E = P_I * P_N$$

Pela Eq (9), percebe-se que nem sempre o pior caminho do sistema, ou seja, o caminho que leva a um menor valor de P_I, gera o caminho menos eficaz do ponto de vista da segurança, pois a probabilidade de neutralização também interfere na escolha do

caminho pelo adversário. O P_I é o acúmulo das probabilidades de detecção (P_D) dos elementos implantadas ao longo do caminho escolhido pelo adversário. (HARI, 2017)

A fim de calcular a probabilidade de interrupção associada ao caminho escolhido pelo adversário, neste trabalho será usado o modelo gráfico Diagrama de sequência do adversário (DSA) (GARCIA, 2008). O cenário de ataque será criado e simplificado no gráfico com os elementos de detecção e atraso do sistema. A Figura 24 mostra um exemplo de diagrama.

Figura 24 – Exemplo de diagrama de sequência do adversário

Na Figura 24, existem as delimitações das áreas já explicadas na subseção anterior em área vigiada, protegida e vital. Os quadrados verdes servem de ligação para as áreas adjacentes e representam os elementos de detecção e atraso para o adversário. Existem 3 blocos verdes para cada elemento, no bloco verde superior é escrito o nome com os detalhes do elemento, como por exemplo 2,5m de parede de concreto entre a área vigiada

e a protegida. Os dois blocos verdes abaixo do nome são, o da esquerda mostra a probabilidade de detecção (P_D) do elemento de proteção, como por exemplo 0,8 na cerca de 2,5m localizada fora do site e área vigiada, e o bloco verde da direta mostra o tempo de atraso (t_d) que este elemento proporciona ao adversário.

3.5. P_I

O intuito do adversário é trazer consequências radiológicas severas através de um acidente LBLOCA. A Figura 25 mostra o layout ampliado para os possíveis caminhos dos adversários de conduzir uma missão de explodir a tubulação do sistema primário e as 2 válvulas (VC2 – TREM 1 e VC2 – TREM 2) dos sistemas de segurança de injeção de água.

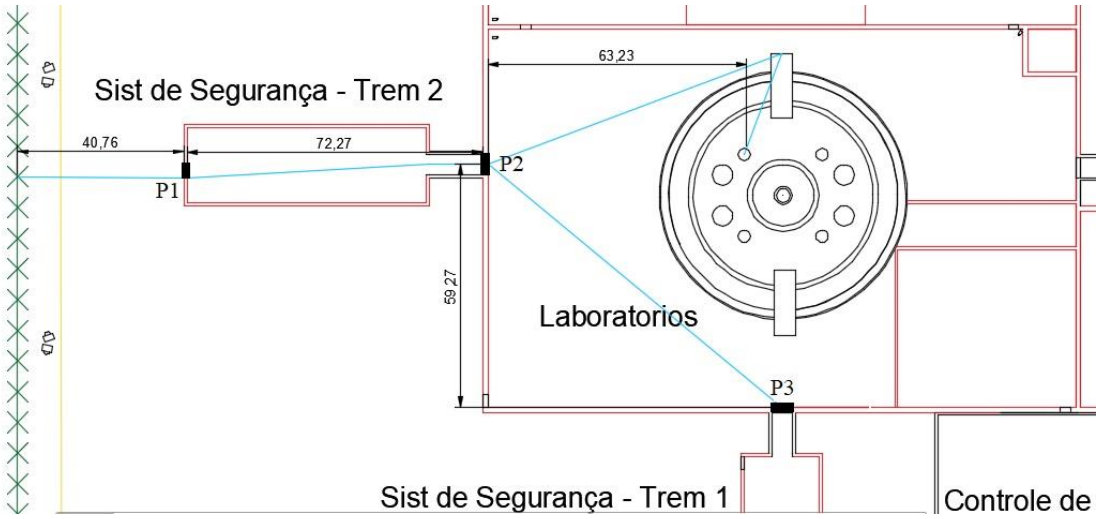

Figura 25 – Caminho de ataque do adversário

O adversário estará munido de ferramentas e explosivos. Para completar a missão, o grupo 1 precisará cortar a cerca→ quebrar a parede de 20 cm de concreto→ correr para a porta P1→ penetrar P1 com explosivos→ correr para a porta P2→ adentrar na P2 com ajuda de *insider* → correr para P3→ destruir a tubulação. O grupo 2 precisará, após

adentrar na porta P2→ correr para P3→ penetrar P3 com ajuda de explosivos→ destruir a válvula.

Seguindo o caminho escolhido, o adversário enfrentará várias camadas de proteção com elementos de proteção. O tempo de força de resposta foi calculado para 300 segundos com a suposição de que a força de resposta viajará a pé e a velocidade de marcha é de 3m/s.

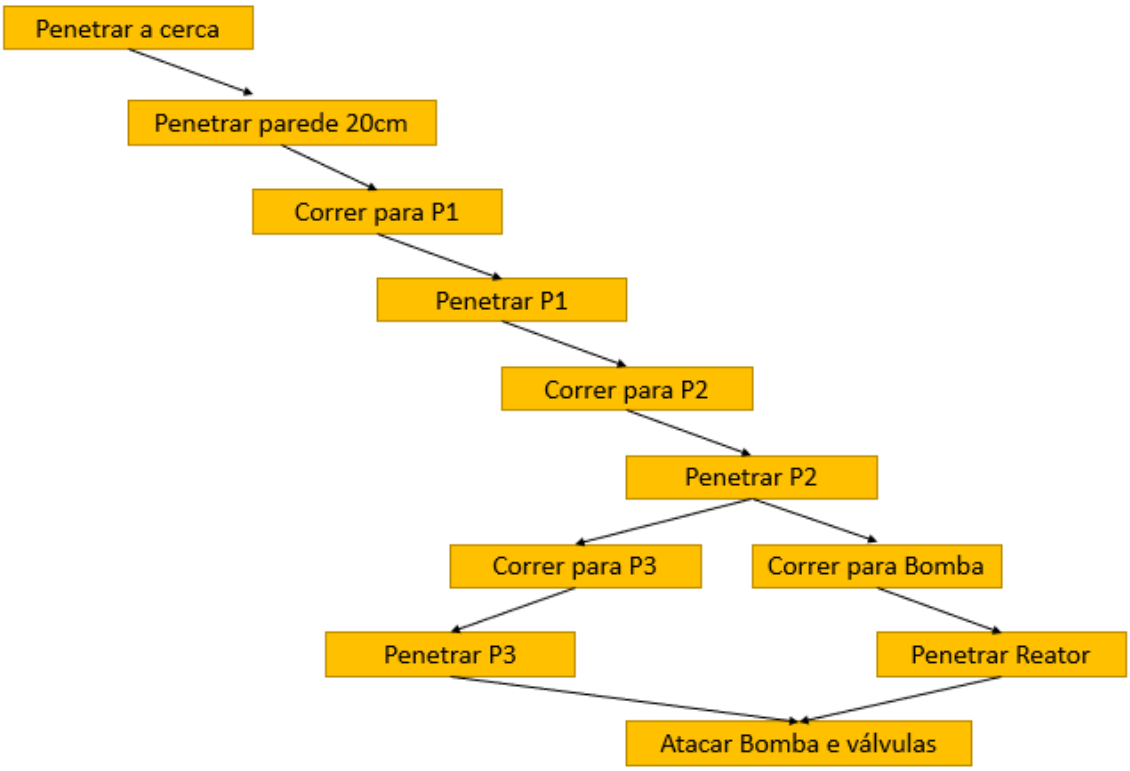

Figura 26 - Caminho dos adversários

A Tabela 10 mostra os valores utilizados para o cálculo do P_I.

Tabela 10 - Lista de sensores e barreiras para o cálculo de Pi

Barreiras	Sensores	Pd	Td (segundos)
Cerca 2,5m	Micro-ondas exterior	0,8	18
Portão de Veículo	Múltiplos Sensores	0,99	10
Portão principal	Pesquisa pessoal	0,9	30
Parede 60 cm Concreto reforçado - com auxílio e ferramenta	Câmera de vídeo	0,5	900
Parede 60 cm Concreto reforçado - com auxílio de explosivo	Múltiplos Sensores	0,99	480
Parede de Concreto 20 cm - com auxílio e ferramenta	Câmera de vídeo	0,5	600
Parede de Concreto 20 cm - com auxílio de explosivo	Múltiplos Sensores	0,99	0
Parede de Madeira - com auxílio e ferramenta	Câmera de vídeo	0,5	30
Porta de Emergência P1 – 30 cm reforçada com metal	Múltiplos Sensores	0,99	214
Porta do controle de acesso	Múltiplos Sensores	0,99	5
Portas de acesso Rejeitos	Impressão digital e PIN	0,95	15
Porta P3 – com auxílio de explosivo	Múltiplos Sensores	0,99	54
Porta de acesso ao reator	Escaneamento por Retina e PIN	0,99	5

As Figuras 27 e 28 mostram, respectivamente, o DSA dos possíveis caminhos do adversário e o tempo de tarefa e detecção. O PDC foi calculado a partir do tempo de resposta de 300 segundos.

Figura 27 – Diagrama de sequência do adversário

Com base na Figura 28, o PDC está localizado onde os adversários tentam penetrar pela porta P1, ou seja, caso tenham sucesso em completar esta tarefa, a força resposta não terá tempo para interromper a missão.

Tarefa do Adversário		Tempo
Penetrar cerca		18
Penetrar concreto 20 cm		600
Correr para P1		10
Penetrar P1		214
Correr para P2		18
Penetrar P2		5
Correr para P3	Correr para Bomba	15
Penetrar P3	Penetrar reator	108
Destruir Válvula	Destruir Tubulação	20

Maximizar detecção

PDC

Maximizar atraso

Figura 28 – Tempo de detecção

A partir do modelo EASI, o valor de P_I é calculado através da inserção das probabilidades de detecção e atraso dos elementos de proteção (GARCIA, 2008). O valor de comunicação estipulado entre guardas e força resposta é de 95% e o desvio padrão para atrasos é de 25%.

Para o grupo 2, o valor de probabilidade de interrupção calculado é de **0,943**, como mostra a Tabela 11. Este valor de interrupção é considerado extremamente alto e geralmente resulta em uma vulnerabilidade suficientemente baixa no sistema de segurança.

Tabela 11 - Resultados do modelo EASI do cálculo de ataque do grupo 2

	Probability of Interruption:		**0.943**
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication	**System Response** Time **(in seconds)** Mean	Standard Deviation
	0,95	30	75

Task	Description	P(Detection)	Locatio	Delays (in seconds): Mea	Standard Deviatio
1	**Penetrar Cerca**	0,8	b	18	4,5
2	**Penetrar parede concreto 20**	0,5	e	600	150
3	**Correr para P1**	0,02	b	10	2,5
	Penetrar P1	0,99	m	214	53,5
5	**Correr para P2**	0,02	b	18	4,5
6	**Penetrar P2**	0,99	e	5	1,25
7	**Correr para P3**	0,02	b	18	4,5
8	**Penetrar P3**	0,99	m	108	27
9	**Destruir Válvula**	1	e	20	5

Para o grupo 1, o valor de probabilidade de interrupção calculado é **0,786,** como mostra a Tabela 12. Este valor ainda é considerado alto, no entanto, ele é menor que o grupo 2 porque possui uma tarefa a menos, por não ser necessário passar por nenhuma porta.

Tabela 12 - Resultados do modelo EASI do cálculo de ataque do grupo 1

	Probability of Interruption:			**0.786**
Estimate of Adversary Sequence Interruption	Probability of Alarm Communication		**System Response** Time **(in seconds)** Mean	Standard Deviation
	0,95		30	75

Task	Description	P(Detection)	Location	Delays (in seconds): Mean	Standard Deviation
1	**Penetrar Cerca**	0,8	b	18	4,5
2	**Penetrar parede concreto 20**	0,5	e	600	150
3	**Correr para P1**	0,02	b	10	2,5
	Penetrar P1	0,99	m	214	53,5
5	**Correr para P2**	0,02	b	18	4,5
6	**Penetrar P2**	0,99	e	5	1,25
7	**Correr para P3**	0,02	b	18	4,5
8	**Destruir Tubulação**	1	e	20	5

A coluna “Location” está relacionada ao tipo de sensor e ao atraso que ele causa. A detecção do sensor pode ser considerada de 3 formas:

I. B: detecta antes do atraso; o atraso é calculado usando a média dos tempos para o elemento; ex: sensores volumétricos que alarmam no momento antes do intruso executar uma tarefa;

II. M: detecta durante o atraso; 0,5 do valor do atraso; ex: uso de explosivo só alarma quando o adversário já tiver completado a tarefa;

III. E: detecta após o atraso; usa 0 para o tempo de atraso da tarefa; ex: porta com sensor magnético que só irá alarmar após a entrada.

3.6. P_N e Frequência de ataque

Para que o P_N seja calculado, algumas definições e ameaças devem ser listadas pelo estado ou órgão regulador a fim de definir e caracterizar o tipo de ameaça que a instalação possa sofrer. GARCIA (2008) menciona que o estudo dos casos é necessário para que sejam conhecidas a capacidade e as intenções de um potencial crime, especulativo ou não, que possa gerar uma situação de emergência como sabotagem, roubo de materiais ou informações. Uma vez que o tipo de adversário seja identificado, os sistemas de proteção física da instalação poderão ser projetados para de maximizar a segurança e minimizar os riscos, como mostra a Figura 28.

O conceito do *Desing basis threat* (DBT) ou Ameaça a uma base de projetos é usado como ferramenta de gerenciamento e projeto que ajuda a facilitar a tomada de decisões ou RIDM pelos executivos e estabelece requisitos técnicos para os especialistas em projetar o SPF. Ele contém informações e serve como base para teste e estudo de projetos (IAEA, 2017).

A probabilidade de neutralização é resultado do conjunto de fatores de eficiência da força resposta relacionada a capacidade, tática, força do adversário, instrumentos de neutralização (armas, bombas). etc. A análise é dividida em dois segmentos, dados sobre o adversário como motivação, inteligência e capacidade de armamento, e dados sobre os equipamentos da força resposta perante a ação maliciosa, como, por exemplo, armas de serviço básico, armas de serviço especial, rifles, pistola, etc.

Inúmeros cenários podem ser analisados, portanto, para minimizar os cálculos, o método utilizado será o numérico simples a partir do programa de neutralização (Hawila, 2016).

Foram presumidos para os adversários o alto treinamento com armas e ações furtivas. O ataque é realizado à noite com 2 grupos de 4 pessoas cada, com o mesmo poder bélico das forças de resposta. São rifles automáticos e pistolas para cada integrante. A força resposta é integrada por 4 equipes que são 4 guardas armados com pistola no interior do prédio vital e localizados no controle de acesso, 4 guardas com rifles no posto fortificado, 4 atiradores de elite na torre fortificada e 10 homens de resposta externa. Com estes dados, o valor de P_N obtido usando o programa de neutralização é de **0,895**. A Figura 29 mostra a macro e os dados utilizados. O tempo de demora para cada grupo de guardas foram presumidos, diferente do grupo 4 de força resposta em que foi utilizado o mesmo valor no cálculo de probabilidade de interrupção no programa EASI, 300 segundos ou 5 minutos. O tempo de demora do adversário, 16 minutos e 40 segundos, é decorrente da soma de todas as tarefas necessárias para que a missão seja bem-sucedida (Figura 27).

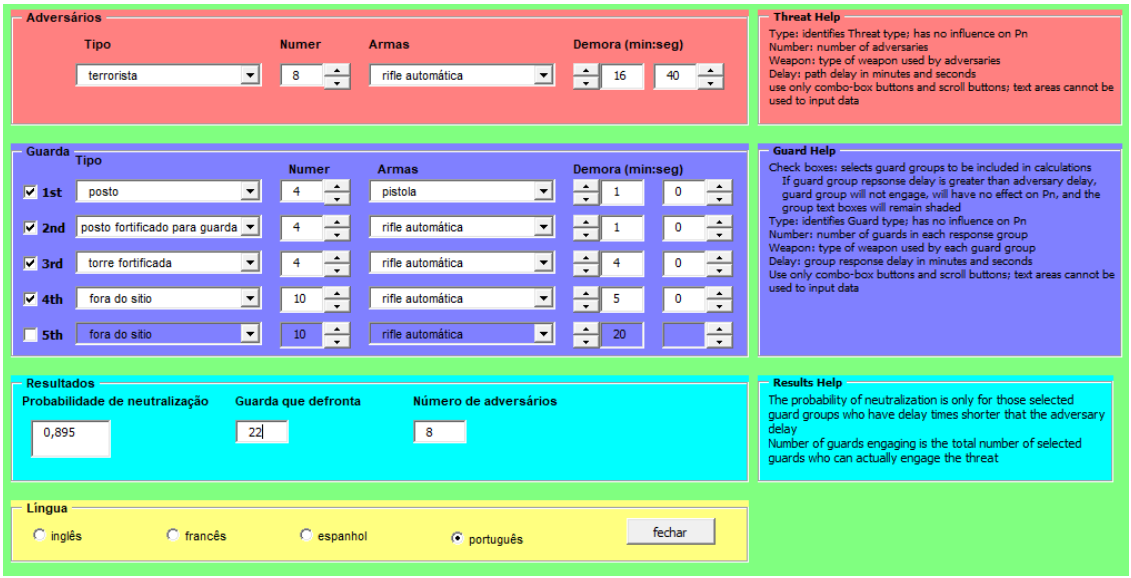

Figura 29 - Macro utilizada para o cálculo da probabilidade de neutralização

A Tabela 13 resume a DBT para um grupo terrorista que é considerado para o cálculo da P_N.

Tabela 13 – Tabela de DBT

		Adversário: Terrorista
Motivação	Ideológico	Baixo
	Econômico	Alto
	Político	Alto
	Pessoal	Baixo
Intenções	Alvos	Sabotagem em uma instalação nuclear
	Objetivo do Ataque	Causar exposição radiológica ao público
	Disposição para morrer	Sim
Capacidades	Número de adversários	8
	Tática	Furtividade, Enganar, Rapidez no ataque, Uso da Força
	Meios de acesso	Vigilância de Fora, Insider Passivo
	Armas	rifles semi-automaticos, 9 mm pistola, facas.
	Explosivos	Explosivos avançados, Bombas caseiras
	Equipamentos e Ferramentas	Ferramentas manuais e ferramentas elétricas comercialmente disponíveis
	Fundo	R$ 60.000
	Transporte	Caminhões leves, incluindo 4x4, carros leves
	Habilidades	Química básica, eletrônica básica
	Habilidades de Cyber	Não
	Outro conhecimento	Sim
	Suporte Estrutural	Baixo
	Assistencia de Insider	Sim, passivo

A partir dos valores de probabilidade de interrupção e de neutralização, pode-se calcular a frequência de ataque com sucesso pela Eq (10). A probabilidade de ataque (P_A) é assumida com o valor de **1,0E-03** por ano (Hawila, 2016).

$$F_{sucesso} = P_A * (1 - P_I * P_N) \quad (10)$$

Inserindo os valores previamente calculados na Eq (10) resulta em $\boldsymbol{F_{sucesso}}$ **= 1,56 E-4** ataque bem-sucedido por ano para o grupo 2, e **2,94 E-4** por ano para o grupo 1.

3.7. Estimativa de Risco

A partir dos valores calculados de frequência de sucesso, o parâmetro final para a estimativa de risco, segunda a Eq (2), é a consequência.

$$R = F * C$$

Visto anteriormente na seção de *safety*, a consequência é estimada do mesmo modo através da equação (7) do INES de categorias de acidente. Neste trabalho, foi definida a categoria 5 de médio lançamento de materiais radioativos para fora da contenção.

$$C = 0.8 * 10^{N-7}$$

O valor de consequência relativa associado C é **8,0E-02** e o valor da estimativa de risco, aplicando a Eq (2) apenas para o grupo de maior frequência de sucesso (grupo 1), é de **2,35E-06**.

4. SAFETY - SECURITY

Este capítulo irá apresentar a árvore de falha para que ocorra o evento LBLOCA a partir de dois eventos iniciais, o evento de sabotagem dos adversários e a falha mecânica no componente mais crítico (subseção 2.4). O evento de sabotagem é divido em duas tarefas, a falha da válvula VC2 dos trens 1 e 2 e a ruptura da tubulação do sistema primário. Os resultados de uma combinação de falhas de componentes com base em um cenário específico foram analisados para determinar a frequência de falha do sistema principal.

Para calcular a frequência total de falhas, será utilizado o programa SAPHIRE. As frequências de falhas calculadas nas seções anteriores serão adicionadas à arvore de falha com uma lógica de eventos. Serão 3 eventos principais:

i. Frequência natural de falha da válvula VC2 de 6,22E-03 por ano;
ii. Frequência do ataque às válvulas VC2 do trem 1 e 2 de 1,56 E-4 por ano;
iii. Frequência do ataque à tubulação do primário de 2,94 E-4 por ano.

Como dito em seções anteriores, o adversário terá a tarefa de destruir o componente de maior importância, portanto, pela subseção 2.4, a válvula será o único componente que irá sofrer danos no sistema de emergência. No entanto, muitos cenários podem ser analisados, como por exemplo, após completar a tarefa de entrar no prédio do sistema de emergência, qualquer componente pode sofrer o ataque, isto mudaria completamente o cálculo e o valor de frequência total da árvore de falha. Para cada ação feita pelo adversário, seria adicionado um evento iniciador à arvore de falha.

A Figura 30 mostra a árvore com os ataques e a respectiva lógica.

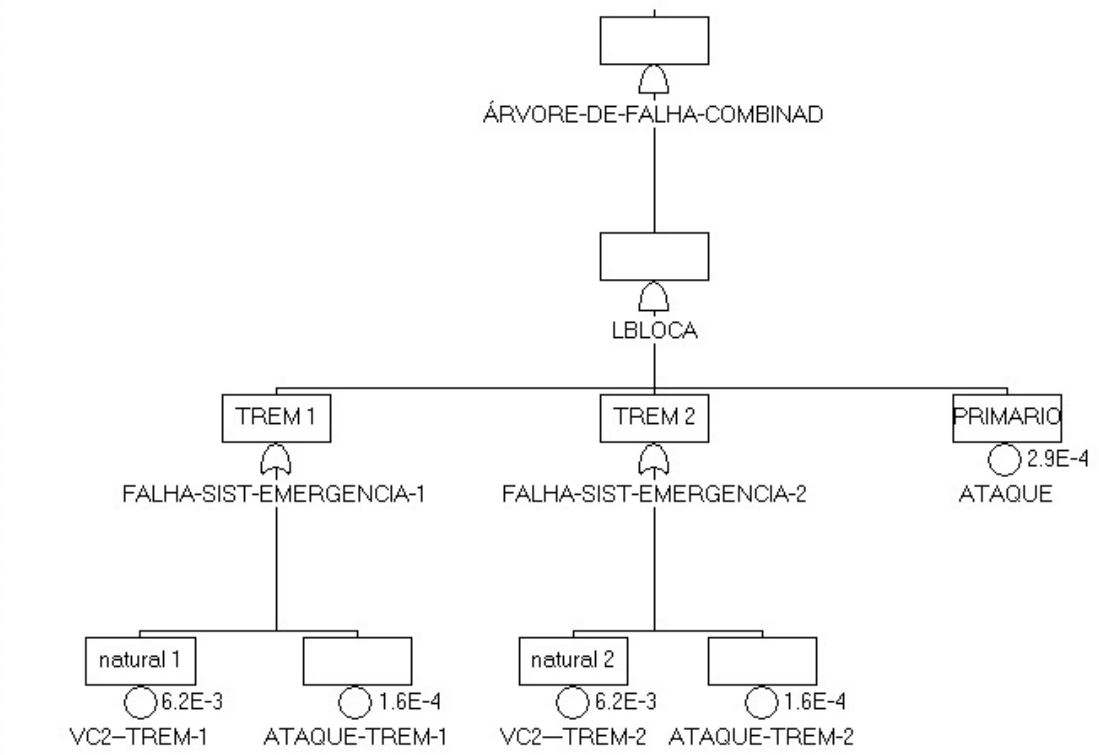

Figura 30 - Árvore de falha combinada

Pela Figura 30 vemos os 5 eventos com os respectivos valores de frequência de falha. Para esta árvore, foram considerados eventos diferentes para o ataque do trem 1 e trem 2, no entanto, os valores de frequência assim como o a falha natural das válvulas são os mesmos. O valor da frequência total é de **1,195E-8** por ano.

O valor de risco associado, utilizando o valor de consequência de **8,0E-2**, é de **9,56E-10**.

5. Conclusões e Recomendações

Este trabalho teve o objetivo de mostrar uma nova metodologia para o estudo de *safety* e *security*. O método vem sendo utilizado e aprimorado pelo programa nuclear dos Estados Unidos e a fonte majoritária de referências são de autores e laboratórios americanos. Portanto, para este trabalho existiram certas limitações quanto à literatura e por ser de caráter sigiloso.

A seção de *safety* tinha o objetivo de calcular, a partir de métodos já conhecidos de árvore de falha e eventos, o tipo de acidente e dano que poderia causar caso a tubulação do sistema primário e os sistemas de injeção de água a baixa pressão falhassem. Foi analisado um circuito hipotético de reator PWR e calculada a frequência de falha do sistema para um portão de votação 2/4. Por fim, a análise de importância dos componentes, seguindo o método de Pareto, mostrou que o componente de maior grau de importância para o referido sistema era a válvula de retenção. Esta análise serviu para selecionar e adicionar o componente na análise conjunta de *safety* e *security*.

A Seção de *security* tinha o objetivo de demonstrar um novo método de análise que não é comumente utilizado na análise de segurança de reatores. O método consiste em definir as probabilidades de segurança necessárias para estimar o valor de risco da instalação nuclear. Os parâmetros para o cálculo da probabilidade de interrupção foram analisados através dos possíveis caminhos dos adversários, a montagem dos sistemas de proteção física que inclui sensores com seus respectivos valores de probabilidade de detecção e atraso, barreiras e comunicação, separação das áreas vigiada, protegida e vital. Os parâmetros para o cálculo de probabilidade de neutralização foram analisados através

da montagem do DBT e da definição da força resposta quando ao tempo de resposta e poderio bélico.

Após os cálculos destas probabilidades, foi definido um valor de frequência de ataque anual de **1,0E-03**. A Tabela 14 mostra todas as probabilidades utilizadas para análise de *security*, frequências de ataque e riscos de *safety* e *security*.

Tabela 14 - Sumário dos valores de probabilidade, frequência e risco

Parâmetros de Security	**Valores**
Frequência de ataque para grupo 1 por ano	2,94E-4
Frequência de ataque para grupo 2 por ano	1,56E-4
Probabilidade de Interrupção para o grupo 1	0,783
Probabilidade de Interrupção para o grupo 2	0,943
Probabilidade de Neutralização	0,895
Consequência	8,0E-2
Frequência de Ataque por ano	1,195E-8
Risco em Security por ano	**2,35E-06**
Risco em Safety para o Sistema de Emergência por ano	**2,22E-05**
Risco de Safety - Security por ano	**9,56E-10**

A Tabela 14 mostra a diferença de valores de risco associados a uma análise separada e combinada de *safety* e *security*. Vemos que a análise associada gera um menor risco que as demais. A análise de *safety* possui um maior risco, no entanto, não foi analisada a frequência de ruptura do tipo guilhotina na tubulação do sistema primário.

O valor desta metodologia após os atentados de 11 de setembro de 2001 é colocar em evidencia o grau de ameaças e quantificar um sistema de proteção quanto à sua eficiência em evitar e dissuadir um adversário. Pretendeu-se criar uma ponte ou uma linha de raciocínio para a segurança nuclear e física, evidenciar a locação de recursos e promover a cultura de segurança. Com isso, os resultados decorrentes da combinação de eventos iniciadores de *safety* e *security*, devido à criação da interface de segurança, mostram a importância em definir a frequência de falha de um sistema não apenas com falhas sistemáticas ou naturais, mas sim com ataques e sabotagens. No Brasil, a preocupação quando a ataques ou sabotagens em instalações nucleares é pequena, no entanto, a IAEA enfatiza que a segurança nuclear é mundial, ou seja, um roubo de material em uma usina que não se compromete com a proteção física pode gerar riscos para toda a sociedade.

A Figura 31 mostra a comparação dos cortes mínimos. Os eventos que contribuem para a frequência de falha total com porcentagem de 95% são os eventos de falha natural mútua das válvulas e ataque ao sistema primário.

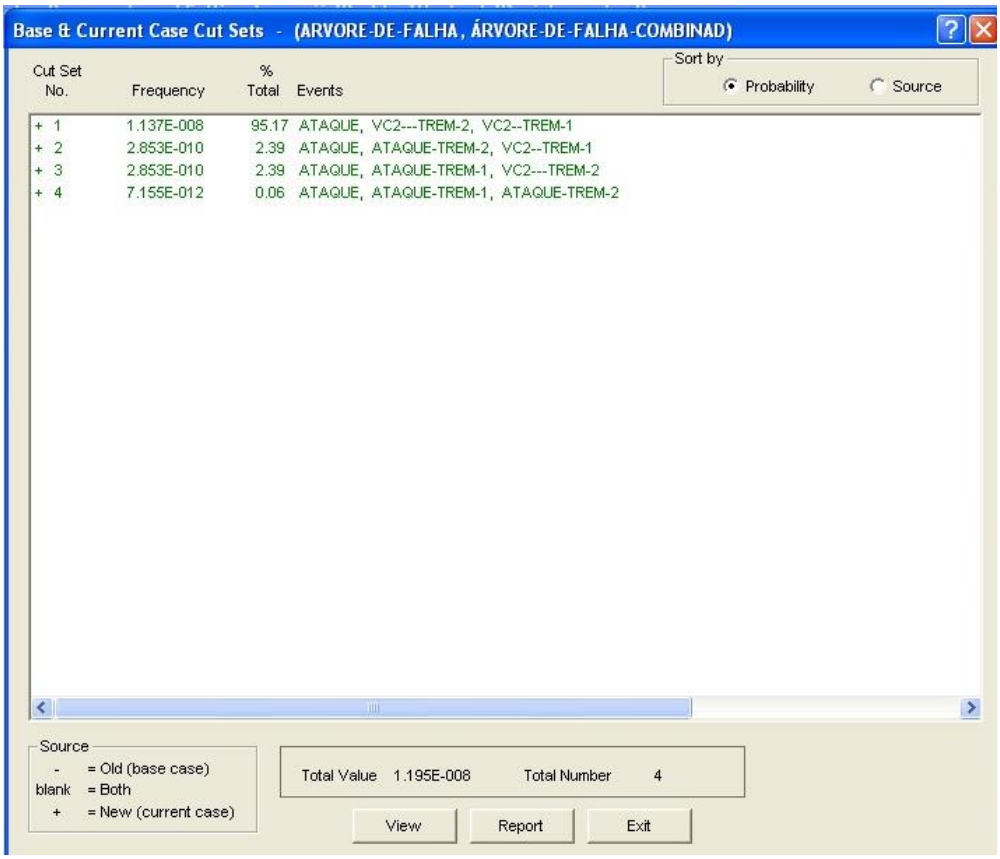

Figura 31 – Importância dos eventos para a frequência total

O enfoque deste trabalho não foi gerar uma situação de sabotagem por *insider* ou roubo de material radioativo. No entanto, cabe enfatizar que, devido à dificuldade e à baixa probabilidade de ocorrência dos eventos de sabotagem que geram um evento de categoria 5 do INES, existe uma maior probabilidade de roubo de material por intermédio de funcionários ou pessoas que tenham acesso à área vital. Existem diversas preocupações quanto à estabilidade do funcionário e a satisfação perante o trabalho. Fatores como esses devem ser analisados a fim de minimizar o acesso às pessoas instáveis ou com objetivos maliciosos. Trabalhos futuros podem ser fundamentados em questões psicológicas e utilizar metodologias de investigação para o cálculo de um ataque/sabotagem ou roubo de material a partir de um *insider*.

REFERÊNCIAS

CNEN, **Normas para Escolha de Locais para Reatores de Potência**, Resolução 09/69, Rio de Janeiro, Brasil, 1969.

CNEN. **Biblioteca digital memória da CNEN**. Disponível em: <http://memoria.cnen.gov.br/memoria/cronologia.asp?unidade=brasil>. Acesso em: 08 mai. 2017.

CNEN. **Proteção física de unidades operacionais da área nuclear (resolução cnen 110/11)**. Disponível em: <http://appasp.cnen.gov.br/seguranca/normas/pdf/nrm201.pdf>. Acesso em: 16 mai. 2017.

CNEN. **Segurança na operação de usinas nucleoelétricas**, Resolução 04/97, Rio de Janeiro, Brasil, 1988.

TN, Angra 2, **Relatório de Impacto Ambiental**, exemplar 61, 1998.

ETN. **Defesa em Profundidade**. Disponível em: http://www.eletronuclear.gov.br/Saibamais/Seguranccedila/Defesaemprofundidade.aspx Acesso em: 02 jun. 2017.

ETN. **Segurança Nuclear**. Disponível em: <http://www.eletronuclear.gov.br/saibamais/seguranccedila/seguran%c3%a7anuclear.aspx>. Acesso em: 07 fev. 2017.

FGV. **Plano nacional de desenvolvimento.** Disponível em: <http://www.fgv.br/cpdoc/acervo/dicionarios/verbete-tematico/plano-nacional-de-desenvolvimento-pnd>. Acesso em: 13 fev. 2017.

FULLWOOD, **Probabilistic safety assessment in the chemical and nuclear industries**. 1ª ed. USA, Butterworth-Heinemann, 2000.

GARCIA M. L., **The Design and Evaluation of Physical Protection Systems**, 2ª ed. Boston, Butterworth Heinemann, 2008.

HAWILA, *Combined Safety and Security Risk Evaluation Considering Safety and Security- Type Initiating Events*. Tese de D.Sc, Texas A&M University, USA, 2016.

HARI, "*Hypothetical Facility Exercise Data Handbook", The Twenty-Seventh International Training Course*, United States Government, Department of energy, 2017.

IAEA, *Nuclear Security Series*. Disponível em: <http://www-ns.iaea.org/security/nuclear_security_series.asp?s=5&l=35>. Acesso em: 16 maio. 2017.

IAEA, **Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. NS-R-1**, Vienna, VIC, 2000.

IAEA, **Component Reliability Data for Use in Probabilistic Safety Assessment, IAEA TECDOC-478**, Vienna, IAEA, 1988.

IAEA, **Determining the Quality of Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants IAEA-TECDOC-1511**, Vienna, IAEA, 2006.

IAEA, **Nuclear security culture: IMPLEMENTING GUIDE**. Viena: [s.n.],. 48 p., IAEA, 2008

IAEA, **Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants. Specific Safety Guide No. SSG-**3, Vienna, IAEA, 2010.

IAEA, **International Nuclear and radiological event scale (INES)**, Vienna, IAEA, 2013.

IAEA, **Nuclear Security Series Glossary- Version 1.3**. Viena, IAEA, 2015.

IAEA, **Procurement Engineering and Supply Chain Guidelines in Support of Operation and Maintenance of Nuclear Facilities,** Vienna, IAEA Nuclear Energy Series, No. NP-T-3.21, 2016.

IAEA. **Nuclear terrorism: threats, risks and vulnerabilities**. Disponível em: <http://www-ns.iaea.org/security/threats.asp?s=4>. Acesso em: 24 mai. 2017.

IPEN, **Análise Probabilística de Segurança e Análise de Confiabilidade.** Disponível em:< https://www.ipen.br/portal_por/portal/interna.php?secao_id=35&campo=684>. Acesso em: 17 out. 2017.

KASSENOVA, O caleidoscópio nuclear do Brasil: Uma identidade em evolução. Brasil, Carnegia, 2014.

KNIEF, **Nuclear Engineering, Theory and Technology of Commercial Nuclear Power**, Second Edition, USA, Taylor & Francis, 1992.

KUMAMOTO, H., **Satisfying safety goals by probabilistic risk assessment.** Japão, Springer, 2007.

MODARRES, **Risk Analysis in Engineering: Techniques, Tools and Trends**, CRC Press, 2006.

NRC, **Systems Analysis Programs for Hands-on Integrated Reliability Evaluation (SAPHIRE) Vol 1**. USA, https://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6952/v1/. Acesso em: 20 dez. 2017

NRC, **PRA-Probabilistic Risk Assessment**. USA, < Disponível em: https://www.nrc.gov/about-nrc/regulatory/risk-informed/pra.html>. Acesso em: 17 out. 2017.

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

Nuclear Power. **PWR Nuclear Fuel Assembly**. Disponível em: https://www.nuclear-power.net/nuclear-power-plant/nuclear-fuel/. Acesso em: 7 dez 2017.

PETRANGELI, Gianni, **Nuclear Safety**, 1 ed., UK, Elsevier, 2006

PLANALTO. **Promulga o tratado sobre a não-proliferação de armas nucleares, assinado em londres, moscou e washington, em 1º de julho de 1968**. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/d2864.htm>. Acesso em: 11 mai. 2017.

SNELL M. K., "**Report on Project Action Sheet PP05 Task 3 between the U.S. Department of Energy and the Republic of Korea Ministry of Education, Science, and Technology (MEST),"**, SANDIA Report SAND2013-0039, 2013.

TWEEDDALE, M. **Managing Risk and Reliability of Process Plants**. Elsevier, 2003