Universidade Federal
do Rio de Janeiro
Escola Politécnica

Engenharia Nuclear
UFRJ

ANÁLISE DO SISTEMA DE PROTEÇÃO FÍSICA DE UM LABORATÓRIO HIPOTÉTICO DO SETOR NUCLEAR

Luiz Thiago Longo Sardo

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

Orientadores: Paulo Fernando Ferreira Frutuoso e Melo
Ricardo Tadeu Lopes

Rio de Janeiro, RJ – Brasil
Agosto de 2019

ANÁLISE DO SISTEMA DE PROTEÇÃO FÍSICA DE UM LABORATÓRIO HIPOTÉTICO DO SETOR NUCLEAR

Luiz Thiago Longo Sardo

Projeto de Graduação submetido ao Corpo Docente do Departamento de Engenharia Nuclear da Escola Politécnica / UFRJ, como parte dos requisitos necessários para a obtenção do grau de Engenheiro Nuclear.

Examinado por:

_____

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

_____

Prof. Ricardo Tadeu Lopes, D. Sc.

_____

Prof. Andressa dos Santos Nicolau, D. Sc.

Rio de Janeiro, RJ - Brasil

Agosto de 2019

Longo Sardo, Luiz Thiago.
Análise do Sistema de Proteção Física de um Laboratório Hipotético do Setor Nuclear/Luiz Thiago Longo Sardo. - Rio de Janeiro: UFRJ/ Escola Politécnica, 2019.
27 p.: il.; 29,7 cm
Orientadores: Paulo Fernando Ferreira Frutuoso e Melo.
Ricardo Tadeu Lopes
Projeto de Graduação – UFRJ / Escola Politécnica / Engenharia Nuclear, 2019.
Referências Bibliográficas: p. 26-27.
1. Segurança Nuclear. 2. Sistema de Proteção Física. 3. Fontes Radioativas. 4. Risco. I. Paulo Fernando Ferreira Frutuoso e Melo e Ricardo Tadeu Lopes. II. Universidade Federal do Rio de Janeiro, Escola Politécnica, Curso de Engenharia Nuclear. III. Análise do Sistema de Proteção Física de um Laboratório Hipotético do Setor Nuclear

Agradecimentos

Agradeço, primeiramente, a Deus, por ter tornado toda essa caminhada possível, onde conheci pessoas que foram essenciais nesta fase.

Agradeço aos meus pais, Paulo e Glória, por todos os ensinamentos, por toda educação, por todo o apoio e por sempre acreditarem em mim, fazendo o possível para que eu pudesse caminhar sozinho. Vocês serão sempre meus maiores exemplos.

Agradeço à minha namorada, Camila, por estar ao meu lado em todos os momentos, me apoiando em cada projeto. Por ser a pessoa que torna meus finais de semana mais divertidos e por ter tido paciência nos finais de cada período.

Agradeço aos professores e funcionários do Programa de Engenharia Nuclear da Universidade Federal do Rio de Janeiro, por seu excelente trabalho na formação não só de profissionais de engenharia, mas também de cidadãos. Em especial, agradeço aos professores Paulo Fernando Frutuoso e Melo e Ricardo Tadeu Lopes pela orientação nesse trabalho.

Agradeço aos professores e funcionários da *Missouri University of Science and Technology*, e a todos os amigos que conheci durante o intercâmbio, que foram essenciais na minha formação como pessoa e Engenheiro Nuclear.

Agradeço aos funcionários da START, *National Consortium for the Study of Terrorism and Responses to Terrorism*, em especial ao Steve Sin, pelos ensinamentos e auxílio no meu aprendizado em segurança nuclear.

Agradeço à CAPES, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, pela oportunidade do intercâmbio para os Estados Unidos durante a graduação.

Por fim, agradeço aos amigos do curso de Engenharia Nuclear, que tornaram a faculdade um local mais agradável.

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

ANÁLISE DO SISTEMA DE PROTEÇÃO FÍSICA DE UM LABORATÓRIO HIPOTÉTICO DO SETOR NUCLEAR

Luiz Thiago Longo Sardo

Agosto/2019

Orientadores: Paulo Fernando Ferreira Frutuoso e Melo
Ricardo Tadeu Lopes

Curso: Engenharia Nuclear

O uso de materiais radioativos e/ou nucleares é essencial na nossa sociedade, portanto se faz necessário garantir a segurança destes materiais. Neste trabalho foi realizado um estudo de caso, com foco em *security*, de um típico laboratório do setor nuclear, contendo fontes radioativas de diferentes atividades, visando avaliar a vulnerabilidade do sistema de proteção física do laboratório em questão. Foram considerados dois cenários hipotéticos de um evento de furto de uma fonte radioativa deste laboratório, sendo um com a presença de um *insider*, e outro sem a presença do mesmo. A partir disso, calculou-se a frequência de ataque com sucesso, as consequências desses cenários baseado no *International and Nuclear Radiological Event Scale* (INES) e por fim determinou-se o risco a partir das diferentes probabilidades de neutralização e interrupção. A partir dos resultados encontrados, foi verificado que é essencial investir em melhorias no sistema de proteção física dos laboratórios do setor nuclear. É necessário que a cultura de segurança nuclear seja priorizada no Brasil assim como é em outros países. A AIEA enfatiza que a preocupação com segurança nuclear precisa ser mundial, evitando assim, possíveis danos à sociedade.

Palavras-chave: segurança nuclear, sistema de proteção física, fontes radioativas, risco.

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

ANALYSIS OF THE PHYSICAL PROTECTION SYSTEM OF A HYPOTHETICAL LABORATORY OF THE NUCLEAR SECTOR

Luiz Thiago Longo Sardo

August/2019

Advisors: Paulo Fernando Ferreira Frutuoso e Melo
Ricardo Tadeu Lopes

Major: Nuclear Engineering

Radioactive and/or nuclear materials are essentials in our society, therefore it is necessary to ensure the safety of these materials. This work performed a case study, focusing on security, of a typical laboratory in the nuclear sector, in which radioactive sources of different activities are available, aiming to evaluate the vulnerability of the physical protection system for this laboratory. Two hypothetical scenarios were considered of a robbery event of a radioactive source from this lab, one with an insider and another without one. Then, it was calculated the attack frequency with success, the consequences of these scenarios based on the International and Nuclear Radiological Event Scale (INES), and finally it was determined the risk based on different interruption and neutralization probabilities. From the obtained results, it was verified that there should be a main concern to invest in improvements of the physical protection system of the nuclear sector labs. The security culture in nuclear sector must be a main concern in Brazil and other countries. The IAEA emphasizes that the concern with nuclear security needs to be worldwide, avoiding possible damage to society.

Keywords: nuclear security, physical protection system, radioactive sources, risk.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

1. Introdução

O estudo de segurança nuclear pode ser dividido em três áreas, *safety*, *security* e *safeguards*. Tais termos foram expostos em inglês pela impossibilidade da diferenciação dos dois primeiros na língua portuguesa.

Safeguards pode ser facilmente traduzido como salvaguardas, que diz respeito ao acordo de salvaguardas, que tem como objetivo deter a propagação de armas nucleares, detectando previamente o mau uso de tecnologia ou materiais nucleares. A Agência Internacional de Energia Atômica (AIEA) é responsável pela fiscalização dos países que assinaram o acordo.

Safety está relacionado à análise de segurança de uma instalação nuclear e à preocupação da estimativa de dose recebida pelos trabalhadores, pelo público, e pelo meio ambiente.

Já *security* está relacionada à vulnerabilidade do Sistema de Proteção Física (SPF) de qualquer local que possua materiais radioativos e/ou nucleares [1]. O SPF é definido como um conjunto de medidas que têm por objetivo proteger o material nuclear contra roubo, furto ou qualquer outra forma de remoção não autorizada, contribuir para a recuperação do material nuclear que porventura tenha sido removido de forma não autorizada ou esteja desaparecido, proteger as instalações e os materiais nucleares de atos não autorizados, em especial de sabotagem, contribuir para minimizar ou mitigar os efeitos de um ato de sabotagem na instalação nuclear, e contribuir para manter a integridade física do pessoal na instalação nuclear [2].

Apesar do Brasil ter apenas uma pequena parcela da sua matriz energética proveniente da energia nuclear, onde são utilizados materiais nucleares, utilizam-se materiais radioativos para diversos outros procedimentos. Pode-se citar o uso de iodo-131 em medicina nuclear em exames de radiodiagnóstico, o uso de cobalto-60 para tratamentos de câncer com radioterapia, entre outros. Além disso, podemos citar o uso de fontes radioativas para a realização de gamagrafia em asas de aviões, com o intuito de detectar a ocorrência de defeitos ou rachaduras [3], entre outros.

No Brasil, o órgão responsável por regular e fiscalizar o uso da energia nuclear é a Comissão Nacional de Energia Nuclear (CNEN), uma autarquia federal vinculada ao Ministério da Ciência, Tecnologia e Inovação (MCTI). A CNEN se preocupa com a proteção radiológica, visando a segurança do trabalhador, do meio ambiente e do público.

Porém no Brasil, a preocupação com a proteção física destes materiais poderia ser melhorada com novas normas, exceto quando diz respeito ao combustível nuclear utilizado nas usinas de Angra 1 e 2, no qual existem diversas medidas de segurança. Por exemplo, de acordo com a norma NN 3.01 [4] o controle de visitantes visa somente a proteção radiológica do mesmo, não levando em consideração a necessidade de fiscalizar o visitante, para um eventual furto de material nuclear e/ou radioativo. Segundo a norma NE 5.01 [5], o objetivo principal é o de estabelecer exigências mínimas de radioproteção e segurança, visando assegurar um nível adequado de controle da eventual exposição do público, bens e meio ambiente à radiação ionizante.

Após uma revisão de todas as normas em vigência da CNEN, pode-se observar que apenas a norma NN 5.04 [6] visa a proteção física de materiais radioativos em transporte, como pode ser entendido de acordo com o seu art. 1º: "Instituir a obrigatoriedade de instalação de sistemas de rastreamento de sinais de posicionamento em veículos utilizados para o transporte de produtos perigosos Classe 7 (materiais radioativos)".

Tomando como exemplo o acidente radiológico que ocorreu em Goiânia em 1987 [7], que gerou consequências elevadas, um evento terrorista utilizando materiais radioativos teria uma consequência provavelmente maior. Portanto, devemos dar total importância à implantação de uma política de segurança física em torno da área nuclear, levando em consideração os riscos que a falta da mesma pode causar.

A AIEA, órgão central internacional para a cooperação técnica e científica na área nuclear, que trabalha visando a segurança e o uso pacífico da tecnologia e ciência nuclear, possui uma preocupação com a implantação de uma cultura de segurança ao redor do mundo. A mesma estabelece que todas as organizações envolvidas em implantar um sistema de proteção física deveriam dar a devida prioridade à cultura de segurança, para seu desenvolvimento e manutenção necessária, assegurando a sua implantação efetiva em toda a organização [8].

Em vista disso, tem-se a necessidade da implantação de segurança física nos estabelecimentos que utilizam materiais radioativos a fim de evitar um evento de sabotagem, visando a segurança da sociedade. Tendo como exemplo as tensões que os principais países do mundo têm passado no quesito de segurança, esta preocupação se faz extremamente necessária.

Com o que foi exposto, pode-se perceber como o uso de materiais radioativos e/ou nucleares são essenciais na nossa sociedade, portanto se faz necessário garantir a segurança destes materiais.

Este trabalho tem como objetivo um estudo de caso de um laboratório de pesquisa hipotético que utiliza em sua rotina diferentes fontes radioativas. Neste estudo, será realizada uma avaliação da proteção física do laboratório, estimando a probabilidade de um possível roubo e/ou furto de uma fonte radioativa.

Este trabalho desenvolve um estudo preliminar para estimar o efeito do risco total considerando o evento iniciador (EI) de *security* com uma subsequente falha dos sistemas de proteção física que podem levar a um evento maior, como um ataque terrorista utilizando uma bomba suja.

Pode-se associar o risco a um dano, que pode acontecer com determinada probabilidade ou frequência. Para acidentes que são eventos raros, o risco deve ser calculado ou estimado a partir de um modelo teórico, possuindo um determinado grau de incerteza que depende da qualidade dos dados e modelos disponíveis.

No caso de eventos frequentes, o risco pode ser estimado estatisticamente, mas para eventos que ocorrem com baixa frequência, raros, tais riscos precisam ser estimados teoricamente. A estimativa do risco de *security* pode ser realizada utilizando a equação [9]:

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

As variáveis utilizadas na Eq. 1 são definidas da seguinte forma

f_A - frequência de ataque do adversário;
P_I - probabilidade de interrupção do adversário pelo SPF;
P_N - probabilidade de neutralização do adversário pela força de resposta;
C - consequência do ataque;

Vale ressaltar a diferença de definição entre perigo e risco. O perigo é inerente à fonte, representando sua capacidade de produzir um determinado dano, enquanto o risco pode depender do perigo, mas também depende da vulnerabilidade das medidas de segurança e defesa [10]. Portanto, pode-se concluir que uma instalação nuclear pode ser perigosa, mas de baixo risco.

O risco pode ser associado a um dano causado em um determinado acidente, que pode ter uma determinada frequência de ocorrência. Para acidentes raros o risco deve ser

calculado através de uma estimativa deduzida de um modelo teórico. Tal estimativa deve ser associada a um determinado grau de incerteza que varia em função da qualidade dos dados e modelos utilizados. Para eventos frequentes podemos estimar o risco de forma estatística [10].

1.1.Objetivo

Este trabalho tem como principal objetivo realizar um estudo de caso de um típico laboratório do setor nuclear, contendo fontes radioativas de diferentes atividades, com foco em *security*, visando avaliar a vulnerabilidade do sistema de proteção física do laboratório em questão. Propõe-se que sejam realizados dois cenários de um evento de furto de uma fonte radioativa deste laboratório, sendo um com a presença de um *insider*, como um funcionário insatisfeito, por exemplo, e outro sem a presença do mesmo. Vale ressaltar que os cenários serão considerados de forma completamente hipotética. A partir disso, calcular a frequência de ataque com sucesso, as consequências desses cenários baseado no *International and Nuclear Radiological Event Scale* (INES) [11,12] e determinar o risco a partir das diferentes probabilidades de neutralização.

O foco em *security* se dá pelo fato do Brasil ser carente em preocupação com a proteção física de estabelecimentos que utilizam materiais radioativos e/ou nucleares.

1.2.Motivação

No mundo de hoje, a ameaça de um ataque terrorista é prevalente em muitos países. O maior medo é que um destes ataques seja aprimorado pelos efeitos de um material radioativo ou nuclear. Tal medo aumentou após o atentado de 2001, às torres gêmeas nos EUA, criando um estigma e preocupações com o terrorismo.

De acordo com a AIEA, o termo “Nuclear Security”, traduzido livremente como segurança nuclear, pode ser definido como “prevenção e detecção de, e resposta a, roubo, sabotagem, acesso não autorizado, transporte ilegal, ou outros atos maliciosos envolvendo materiais nucleares, outras substâncias radioativas ou suas instalações associadas” (*The International Legal Framework for Nuclear Security* - AIEA) [13].

Apesar da responsabilidade da segurança nuclear de uma determinada nação ser completamente do governo desta própria nação, a necessidade de uma cooperação internacional vem se tornando cada vez mais evidente; por conta disso, a AIEA se tornou

responsável por auxiliar os países em seus sistemas de proteção física e infraestrutura assim como facilitar, regional e internacionalmente, esforços para aprimorar a segurança, incluindo medidas de proteção contra terrorismo nuclear.

De acordo com o *US Department of State*, foi criada uma Iniciativa Global de Combate ao Terrorismo (*The Global Initiative to Combat Nuclear Terrorism* - GICNT), uma parceria voluntária composta por oitenta e oito países e seis organizações internacionais comprometidos em fortalecer a capacidade global de prevenir, detectar e responder ao terrorismo nuclear. Desde a sua criação, em 2006, a GICNT já conduziu mais de cem atividades multilaterais, sempre aberta às nações para compartilhar seus interesses em comum e ativamente comprometida com o combate ao terrorismo nuclear [14,15].

Apesar do uso de fontes radioativas para fins maliciosos ser raro, estes não são inexistentes, portanto, pode-se observar a preocupação mundial com tais eventos, sendo necessária a disseminação de uma cultura de segurança. Em vista disso, este trabalho visa calcular o risco de um evento de furto de fonte radioativa com o intuito de aprimorar o sistema de proteção física de instalações nucleares, aumentando a eficiência de detecção do intruso, mitigando estes eventos.

2. Metodologia e procedimentos

O laboratório selecionado para o estudo é um típico laboratório de pesquisa do setor nuclear, possuindo fontes radioativas seladas utilizadas em projetos de pesquisa, emissores de raios X, irradiadores industriais de fontes gama e fontes de radiação seladas exauridas. Tal laboratório permitirá realizar os cálculos probabilísticos dos cenários de furto que serão desenvolvidos.

Para desenvolver os possíveis cenários se faz necessário avaliar o Sistema de Proteção Física (SPF) do laboratório, onde será utilizado o Diagrama de Sequência do Adversário (DSA). Conforme prevê a norma da CNEN NN 2.01 [2], o projeto da instalação deve atender a requisitos básicos como delimitar, com barreiras físicas, as seguintes áreas de segurança sucessivas, dotadas de grau crescente de proteção física:

a) Área vigiada;
b) Área protegida;
c) Área interna; e
d) Área vital;

Serão analisados os possíveis caminhos a serem percorridos para o evento de furto da fonte radioativa, a fim de analisar a eficácia do SPF, determinando assim os valores de probabilidade de detecção (P_D) e tempo de atraso (T_D). Para este trabalho será estimado o tempo da força resposta assumindo que a mesma viajará a pé [1]. A partir dos valores determinados anteriormente, poderemos então calcular a probabilidade de interrupção (P_I), que é essencial para determinar o quão vulnerável uma instalação nuclear é quando se trata da proteção física da mesma. Tal vulnerabilidade é chamada de Probabilidade de Sucesso do Adversário (P_S), dada pela equação:

$$P_S = 1 - P_I * P_N \tag{2}$$

A partir disso, podemos afirmar que a probabilidade de sucesso do adversário multiplicada pela frequência de ataque por ano, resultará na frequência de um ataque com sucesso, dado pela equação:

$$F_{ataque,s} = P_S * f_{ataque} \tag{3}$$

Tal ataque resultará na violação do sistema de proteção física da instalação em questão. E a frequência calculada acima será utilizada para determinar a frequência de falha de segurança do evento iniciador.

Este trabalho será dividido da seguinte forma:

- Desenvolver a planta do laboratório hipotético;
- Desenvolver uma análise de segurança que permita calcular os parâmetros citados anteriormente, como probabilidade de interrupção, probabilidade de neutralização, frequência de ataque e risco associado;
- Identificar os possíveis eventos iniciadores;
- Calcular o risco associado a cada cenário estudado.

Para realizar a análise de *security* da instalação, faz-se necessário montar o Diagrama de Sequência do Adversário (DSA), que será utilizado para calcular a frequência de falha de um Evento Iniciador (EI). Este evento, posteriormente, servirá para representar os elementos de detecção e atraso de um Sistema de Proteção Física (SPF) [9].

3. Análise de *Security*

Nesta parte do trabalho, será abordada uma análise de *security* que tem por objetivo analisar, através de cálculos e probabilidades, os sistemas que previnem e/ou detectam possíveis ataques adversários. As duas maiores preocupações em *security* são os roubos de materiais radioativos e/ou nucleares e a sabotagem de equipamentos de uma instalação nuclear com o intuito de gerar danos à população.

Como já foi exposto anteriormente, este trabalho abordará o roubo de material radioativo de um laboratório nuclear, com o objetivo futuro de causar dano à população. Como diversos caminhos diferentes podem ser realizados pelo adversário, optamos por escolher o caminho mais fácil para o mesmo, ou seja, o de maior vulnerabilidade para a instalação. Nos outros cenários analisados, o grupo de adversários teriam um tempo de atraso maior para completar suas tarefas, aumentando desta forma as probabilidades de interrupção e neutralização, diminuindo a probabilidade de sucesso do grupo.

Para realizar a análise a partir das equações (1,2,3) que foram expostas anteriormente, no item 2, se faz necessário calcular a probabilidade de interrupção, de neutralização, a frequência de ataque, o valor de consequência relacionado ao nível do acidente e a estimativa do valor de risco. Esses últimos dois parâmetros podem ser determinados através do INES [11,12], mostrado na Figura 1.

Figura 1: Escala INES de acidentes e incidentes [11].

O INES é uma ferramenta para levar ao público a significância da segurança em eventos nucleares e radiológicos. É utilizado para avaliar quantitativamente eventos que resultaram na liberação de material radioativo ao meio ambiente e a exposição à radiação de trabalhadores e o público. Também pode ser utilizado para eventos sem consequências, mas em que as medidas de prevenção antes utilizadas não funcionaram como previsto [11,12].

INES:

Os eventos são divididos em 7 níveis numa escala logarítmica, onde a severidade de um evento é de dez vezes maior que a de um evento da escala imediatamente anterior.

Os eventos são considerados da seguinte forma:

- impacto nas pessoas e no meio ambiente;
- impacto nas barreiras radiológicas e controle;
- impacto na defesa em profundidade, que pode ser definido como um projeto com múltiplas barreiras de equipamentos e procedimentos, com o objetivo de limitar as consequências e a evolução para condições graves [16].

Eventos sem significância são classificados como abaixo da escala/nível 0.

Os eventos 1-3 são chamados de incidentes e 4-7 de acidentes:

- Incidente: "Episódio repentino que reduz significativamente as margens de segurança sem, contudo, as anular, apresentando por isso apenas potenciais consequências para a segurança.";
- Acidente: "Acontecimentos imprevistos e repentinos provocados pela ação do homem ou da natureza, com danos significativos e efeitos muito limitados no tempo e no espaço, suscetíveis de atingirem pessoas, os bens ou o meio ambiente." [17].

O valor da consequência [12] é determinado pela seguinte equação:

$$C = 0{,}8 * 10^{N-7} \tag{4}$$

onde N é o nível do evento de acordo com o INES.

Neste caso, o evento é classificado como nível 2, resultando em um valor de consequência relativa associado $C = 8.0\ x\ 10^{-6}$.

Alguns termos chave utilizados em *security* são necessários para um melhor entendimento da análise feita nesta parte do trabalho e serão apresentados abaixo, conforme foi anteriormente definido [1,18]:

- Segurança ou Prevenção de Perdas
  - Identificação e eliminação de perigos em uma instalação de processos antes da ocorrência de um acidente, utilizando as devidas tecnologias.
- Acidente:
  - Evento ou sequência de eventos de ocorrência anormal, podendo resultar em consequências indesejadas, como por exemplo, perda, dano ou prejuízo, seja pessoal, ambiental ou patrimonial.
- Incidente:
  - Perda de contenção de material.
- Cenário
  - Conjunto formado pela identificação do perigo, suas causas e seus respectivos efeitos.
- Evento Iniciador de Acidente
  - Todo e qualquer evento para o qual se faz necessária a utilização de um ou mais sistemas de proteção, para que seja evitado um possível acidente em uma instalação industrial.
- Evento Indesejado
  - Evento iniciador de um cenário acidental.
- Cenário Acidental
  - Sequência de eventos que se iniciou em um evento indesejado, conduzindo o sistema da instalação a um estado de perigo.
- Perigo
  - Pode ser definido como perigo potencial, visto que é uma condição física ou química com o potencial de causar danos às pessoas, à instalação ou ao meio ambiente.
- Risco
  - Potencial perda ou dano devido à probabilidade de um evento indesejado e suas consequências adversas.

Em *security* a definição de risco é baseada na análise e no conjunto de três fatores bem conhecidos, que são *ameaça*, *vulnerabilidade* e *consequência* [19,20], definidos abaixo.

- Ameaça
    - Qualquer indicação, circunstância, ou evento, com o potencial de causar perda ou dano a uma instalação ou à população.
- Vulnerabilidade
    - Qualquer fraqueza no projeto de uma instalação ou em sua infraestrutura, implantação ou operação, podendo ser explorado por um adversário. Tal fraqueza pode ser identificada nas características da construção, propriedades dos equipamentos utilizados, comportamento dos trabalhadores, localização das pessoas, ou práticas pessoais e operacionais.
- Consequência
    - Resultados de um evento, incluindo perdas diretas ou indiretas imediatamente, no curto e longo prazo. As perdas podem estar relacionadas aos seres humanos, meio ambiente, à economia, à política, e a outros impactos. O valor de C utilizado neste estudo pode variar de 0 a 1, representando a severidade do evento [12].

3.1. Cálculo de P_I e P_N

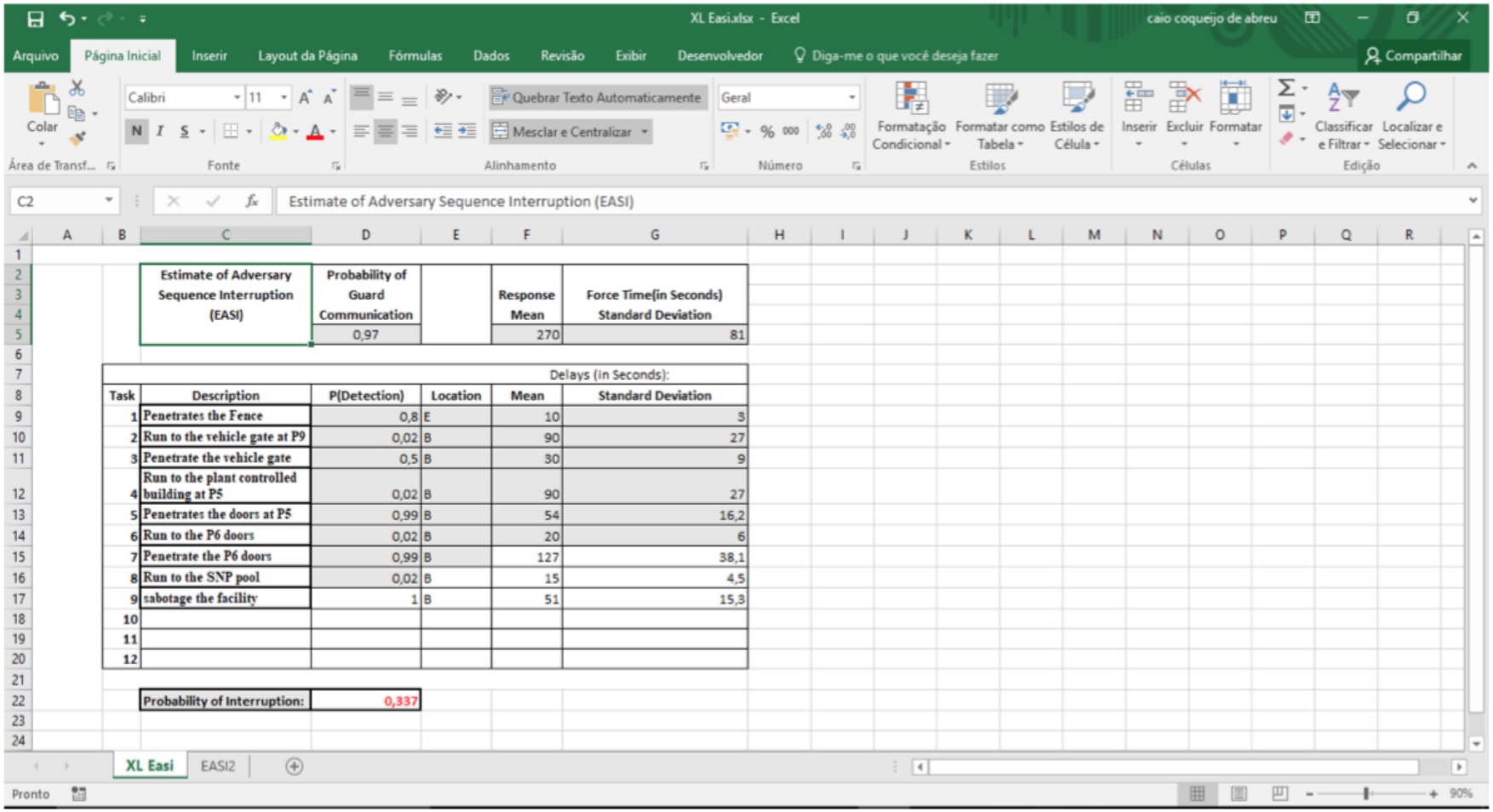
A análise realizada é para calcular os parâmetros de vulnerabilidade do caminho percorrido pelo adversário, que são as probabilidades de interrupção e probabilidade de neutralização, $\boldsymbol{P_I}$ e $\boldsymbol{P_N}$, respectivamente. O cálculo da probabilidade de interrupção é dado pelo modelo feito em Excel EASI, *Estimate of Adversary Sequence Interruption* [9]. E a probabilidade de neutralização será calculada através de uma macro em Excel.

O EASI é um modelo que permite calcular a probabilidade de interrupção, $\boldsymbol{P_I}$, de um determinado roubo ou ação de sabotagem, baseado na probabilidade de detecção, P_D, de cada sensor que o adversário precisará ultrapassar, a probabilidade de comunicação com a força de resposta antes do adversário completar a tarefa, e o tempo de resposta. Pode ser definido como uma ferramenta que ilustra quantitativamente as consequências de

alterar parâmetros de proteção física em um determinado caminho, como pode ser visto na Figura 2.

Os parâmetros de entrada que permitem calcular a probabilidade de interrupção são dados pelas funções de detecção de proteção física, atraso, resposta e probabilidade de comunicação dos alarmes. Os parâmetros de detecção e comunicação são apresentados como as probabilidades de que cada um desses sistemas irá funcionar perfeitamente, enquanto os parâmetros de atraso e resposta devem ser dados em tempo. Vale ressaltar que cada parâmetro de entrada se refere a um caminho específico traçado pelo adversário.

O parâmetro de entrada conhecido como probabilidade de detecção deve ser dado para cada sensor que o adversário irá encontrar em seu caminho. A comunicação entre um alarme e a força de resposta é conhecida como probabilidade de comunicação entre os guardas, P_C. Na maioria dos SPF a probabilidade de comunicação com sucesso com a força de resposta, aumenta com o tempo. Uma avaliação realizada pelo Sandia National Laboratories [SNL] indicou que a maioria dos sistemas trabalha com $P_C \geq 0{,}95$[9], tal suposição pode ser utilizada em um trabalho analisando uma determinada instalação, a não ser que tenha motivos para acreditar que esta não é válida.



Estimate of Adversary Sequence Interruption (EASI)	Probability of Guard Communication		Response Mean	Force Time(in Seconds) Standard Deviation
	0,97		270	81

				Delays (in Seconds):	
Task	Description	P(Detection)	Location	Mean	Standard Deviation
1	Penetrates the Fence	0,8	E	10	3
2	Run to the vehicle gate at P9	0,02	B	90	27
3	Penetrate the vehicle gate	0,5	B	30	9
4	Run to the plant controlled building at P5	0,02	B	90	27
5	Penetrates the doors at P5	0,99	B	54	16,2
6	Run to the P6 doors	0,02	B	20	6
7	Penetrate the P6 doors	0,99	B	127	38,1
8	Run to the SNP pool	0,02	B	15	4,5
9	sabotage the facility	1	B	51	15,3
10					
11					
12					

Probability of Interruption:	0,337

Figura 2: Exemplo do programa EASI Model [9]

Para o cálculo da probabilidade de neutralização, P_N, será utilizado um programa [21] feito através de uma macro, VBA, em Excel® conforme a Figura 3.

Este programa foi desenvolvido baseado no modelo de Markov [22], no qual o valor final da probabilidade de neutralização varia de acordo com o número de guardas, número de pessoas que realizará o roubo ou sabotagem e armamentos utilizados pelos mesmos.

Neste programa, precisaremos selecionar o tipo de ameaça, podendo ser ativista, criminoso ou terrorista, a quantidade de pessoas e as armas utilizadas. Também se faz necessário selecionar os mecanismos de defesa como vigia, patrulha, posto, posto fortificado, torre, torre fortificada, entre outros, incluindo o número de cada mecanismo de defesa e as armas disponíveis para a defesa da instalação. O programa utiliza uma função de decaimento exponencial para calcular os efeitos na probabilidade de neutralização quando grupos de resposta sucessivos na ordem de batalha têm tempos de chegada variáveis. O objetivo é enfatizar os três fatores mais importantes para a resposta, que são o número de pessoas (grupo de ameaça e resposta), armas utilizadas (nenhuma, bastão, revólver ou rifle) e o tempo de chegada (tempo do caminho do adversário e tempo de resposta) [21].

A macro utiliza algumas hipóteses para chegar a um valor final para P_N:

(i) Armas superiores aumentam P_N quando se fixa um número de guardas e adversários;

(ii) Quantidade de guardas superiores relativa ao número de adversários, aumentam P_N para uma quantidade fixa de armas;

(iii) O efeito de armas superiores é a multiplicação da força

   a. $P_N = f\ (E_{guardas} * M_{guardas}, E_{adversários} * M_{adversários})$
   b. M = número de combatentes
   c. E = multiplicador de força da eficácia da arma

(iv) A regra para efetividade de duas armas é utilizada para $P_N = 0{,}5$

   a. 1 bastão = 2 pessoas sem armas
   b. 1 arma = 2 pessoas com bastão
   c. 1 rifle automático = 2 pessoas com armas

(v) As forças de resposta apenas são levadas em consideração na batalha se estas conseguirem chegar a tempo de interromper a detecção dada no ponto de detecção crítico, definido como a última oportunidade na qual o tempo de

resposta do SPF é menor do que o tempo restante para o adversário completar a sua tarefa.

(vi) A probabilidade de neutralização aumenta quanto menor for o tempo que o grupo de resposta leva para chegar ao local dos adversários.

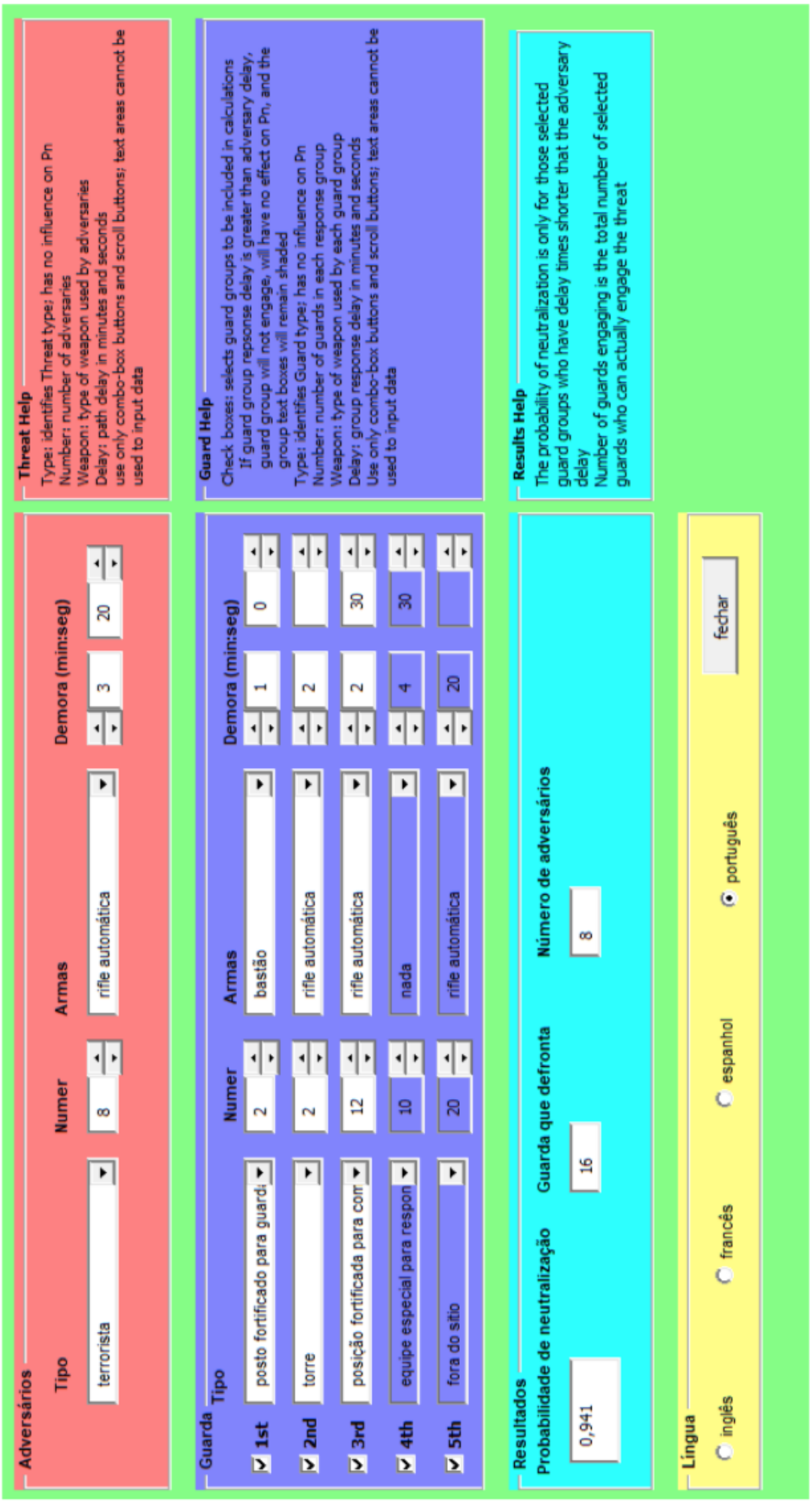


Figura 3: Exemplo da macro de neutralização

Para realizar a análise do SPF, foi necessário criar uma planta hipotética de um laboratório, tornando possível traçar os possíveis caminhos a serem percorridos pelo grupo adversário. Na Figura 4 podemos ver a planta do laboratório, no qual se apresenta uma legenda para o mesmo:

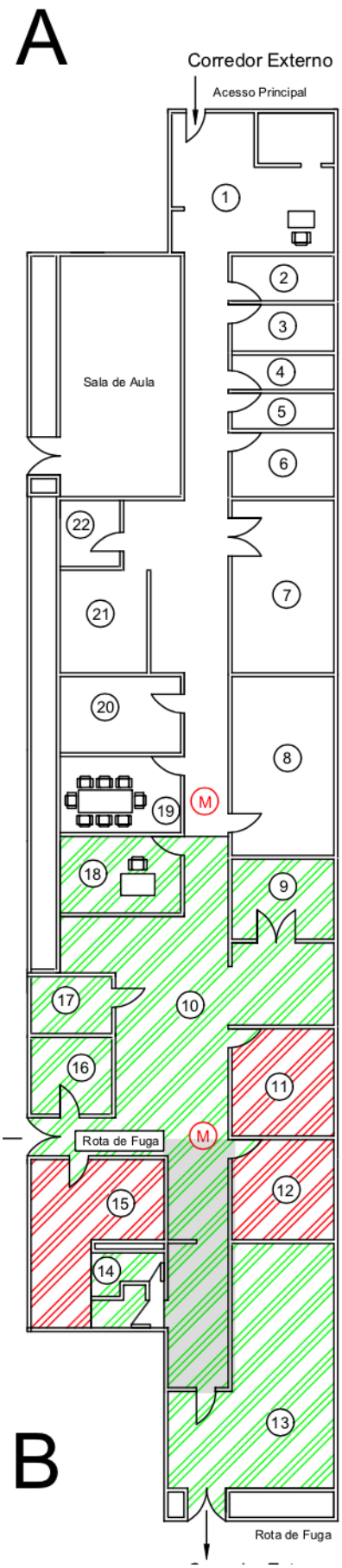


Figura 4: Planta do laboratório hipotético.

A. Posto de guarda
    1. Sala de arquivos
    2. Sala de arquivos
    3. Sala de arquivos
    4. Sala de arquivos
    5. Sala de arquivos
    6. Sala de arquivos
    7. Laboratório de informática
    8. Biblioteca
    9. Eletrônica
    10. Área de protótipos
    11. Laboratório de raios-x
    12. Câmara escura
    13. Laboratório de ensaios experimentais
    14. Banheiro
    15. Irradiador

B. Posto de guarda
    16. Laboratório de fluorescência
    17. Laboratório de espectroscopia gama
    18. Laboratório de tomografia
    19. Sala de reunião
    20. Laboratório de controle de qualidade
    21. Copa
    22. Lavabo

    Área não hachurada = área livre
    Área hachurada verde = área supervisionada
    Área hachurada vermelha = área controlada
    M = Monitor Geiger Muller

O laboratório está situado em um instituto de pesquisa, onde o mesmo atua em diferentes áreas, como dosimetria, fluorescência, imagem por radiações ionizantes, como tomografia, entre outros. Por ser um laboratório do setor nuclear, com diversos laboratórios em seu interior e diferentes áreas de atuação, o mesmo detém algumas fontes radioativas utilizadas para pesquisa, no qual o grupo de adversários está interessado.

3.2. Diagrama de sequência do adversário

Como exposto anteriormente, para analisar a eficácia do SPF da instalação a ser estudada, se faz necessário montar o DSA, contendo a probabilidade de detecção (P_D) e tempo de atraso (T_D) para cada tarefa a ser realizada pelo grupo de adversários. Como existem diferentes possibilidades de caminhos a serem percorridos dentro da instalação, consequentemente existem diferentes possibilidades de ataques maliciosos. Alguns

mecanismos são úteis para dificultar o grupo de adversários, como a implantação de sensores, controle de acesso monitorado, paredes de maior espessura, limitação de acesso em determinadas áreas, entre outros. A combinação dos fatores citados acima dificulta o ataque malicioso com sucesso.

Os valores da probabilidade de interrupção (P_I) e probabilidade de neutralização (P_N) estão diretamente ligados à eficácia do sistema de proteção, como pode ser visto na Eq. 5:

$$E = P_I * P_N \tag{5}$$

O cálculo de P_I é dado pelo EASI Model [9] como consequência dos valores de P_D dos elementos encontrados no caminho traçado pelo grupo de adversários [23]. Para tal, se faz necessário traçar o DSA com P_D e T_D [9]. Vale ressaltar que a instalação possui outras áreas não explicitadas na Figura 4, que os invasores precisarão percorrer para chegar ao laboratório; após a chegada, os invasores tentarão romper a parede da biblioteca, para então acessar o mesmo. Na Tabela 1 apresenta-se o DSA para o cenário 1, sem a presença de um *insider*, enquanto na Tabela 2, teremos o DSA para o cenário 2, considerando a presença de um *insider*, que estará esperando o grupo de invasores, dentro da biblioteca do laboratório.

Os valores de P_D e T_D para as Tabelas 1 e 2 foram determinados através de uma consulta às tabelas disponibilizadas pelo *Sandia National Lab.* em um *handbook* de pesquisas de situações hipotéticas denominado *HARI - Hypothetical Atomic Research Institute* [23]. Nessas tabelas podemos consultar as probabilidades de detecção e tempo de atraso para cada situação, considerando os tipos de sensores de cada cenário, como câmeras de segurança, infravermelho, postos de guarda, entre outros.

Tabela 1: Diagrama de Sequência do Adversário para o Cenário 1 [23]

Sequência	Barreira	Sensores	P_D	T_D (seg)
1	Portão de veículo	Múltiplos sensores	0,99	10
2	Correr p/ portão de acesso	Reconhecimento casual	0,02	20
3	Portão de acesso	Pesquisa pessoal	0,9	30
4	Correr até o laboratório	Reconhecimento casual	0,02	10
5	Parede 20 cm de concreto reforçado (com uso de ferramentas)	Câmeras de vídeo	0,5	600
6	Correr até a porta de controle	Reconhecimento casual	0,02	3
7	Porta de controle de acesso	Impressão digital e PIN	0,95	12
8	Correr até a porta da sala das fontes radioativas	Reconhecimento casual	0,02	3
9	Porta de acesso à sala com fontes radioativas (10 cm de metal)	Múltiplos sensores	0,99	180
10	Sair da instalação correndo	Reconhecimento casual	0,02	60

A Tabela 2 difere da Tabela 1 por não precisar conter as probabilidades de detecção e tempo de atraso para a porta de controle de acesso e porta de acesso à sala com fontes radioativas, itens 7 e 9 na sequência, respectivamente, por contar com a ajuda de um *insider*.

Tabela 2: Diagrama de Sequência do Adversário para o Cenário 2 [23]

Sequência	Barreira	Sensores	P_D	T_D (seg)
1	Portão de veículo	Múltiplos sensores	0,99	10
2	Correr p/ portão de acesso	Reconhecimento casual	0,02	20
3	Portão de acesso	Pesquisa pessoal	0,9	30
4	Correr até o laboratório	Reconhecimento casual	0,02	10
5	Parede 20 cm de concreto reforçado (com uso de ferramentas)	Câmeras de vídeo	0,5	600
6	Correr até a porta de controle	Reconhecimento casual	0,02	3
7	Correr p/ a sala contendo fontes radioativas	Reconhecimento casual	0,02	3
8	Sair da instalação correndo	Reconhecimento casual	0,02	60

3.3. P_I - Probabilidade de Interrupção

Para ambos os cenários, 1 e 2, através do DSA apresentado nas Tabelas 1 e 2, podemos calcular as respectivas probabilidades de interrupção através do EASI Model [9], como pode ser visto nas Figuras 5 e 6.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds)	Standard Deviation
	0,95		300	75

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Portão de veículo	0,99	B	10	2,5
2	Correr p/ portão de acesso	0,02	B	20	5
3	Portão de acesso	0,9	M	30	7,5
4	Correr p/ laboratório	0,02	B	10	2,5
5	Parede 20 cm de concreto reforçado	0,5	E	600	150
6	Correr p/ porta de controle	0,02	B	3	0,75
7	Porta de controle de acesso	0,95	E	12	3
8	Correr p/ a sala contendo fontes	0,02	B	3	0,75
9	Porta da sala com fontes	0,99	M	180	45
10	Sair da instalaçao correndo com a fonte	0,02	B	60	15
11					
12					

Probability of Interruption:	0,95

Figura 5: Probabilidade de interrupção para o cenário 1, considerando o grupo sem *insider*.

Estimate of Adversary Sequence Interruption	Probability of Guard Communication		Response Force Time (in Seconds)	Standard Deviation
	0,95		300	75

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Portão de veículo	0,99	B	10	2,5
2	Correr p/ portão de acesso	0,02	B	20	5
3	Portão de acesso	0,9	M	30	7,5
4	Correr p/ laboratório	0,02	B	10	2,5
5	Parede 20 cm de concreto reforçado	0,5	E	600	150
6	Correr p/ porta de controle	0,02	B	3	0,75
7	Correr p/ a sala contendo fontes	0,02	B	3	0,75
8	Sair da instalaçao correndo com a fonte	0,02	B	60	15
9					
10					
11					
12					

Probability of Interruption:	0,94

Figura 6: Probabilidade de interrupção para o cenário 2, considerando o grupo com *insider*.

3.4. P_N - Probabilidade de Neutralização

Por definição, a probabilidade de neutralização, é o resultado do conjunto de fatores de eficiência da força resposta, relacionada à capacidade tática, força do adversário, instrumentos utilizados para neutralização, como armas, entre outros. Diferentes cenários podem ser analisados para determinar a probabilidade de neutralização de um

determinado evento, portanto para simplificar, será utilizado o método numérico a partir do programa de neutralização [1]. Outros métodos podem ser utilizados para determinar a probabilidade de neutralização, como a opinião de especialistas, complexas simulações computacionais, ou simulações físicas de invasão.

No cenário 1, o grupo de adversários será composto por 4 indivíduos, todos portando pistolas, enquanto que no cenário 2, o grupo será composto por 5 indivíduos, por contar com a presença adicional do *insider*, também portando uma pistola cada um. A força resposta será integrada por duas equipes com três guardas cada uma, todos portando armamentos com o mesmo poder bélico do grupo adversário.

O tempo de demora assumido para os grupos de força resposta foi o mesmo utilizado para os cálculos de probabilidade de interrupção, 300 segundos, 5 minutos, considerando que o grupo viajará a pé e a velocidade da marcha é de 3m/s. Uma diminuição neste tempo não causa diferença significativa na probabilidade de neutralização, pois para esta, o número de guardas é mais relevante. Para os adversários, o tempo de demora se dá pela soma de todas as tarefas para que a missão seja bem sucedida. Além de somar o tempo de todas as tarefas, assume-se que em 5 minutos o grupo consegue sair do laboratório, chegar até o carro e sair da instalação ou seja, para o cenário 1, 20 minutos e 28 segundos, e para o cenário 2, 17 minutos e 16 segundos.

As Figuras 7 e 8, constam as informações contidas acima para determinar as respectivas probabilidades de neutralização do grupo de adversários, para cada um dos cenários.

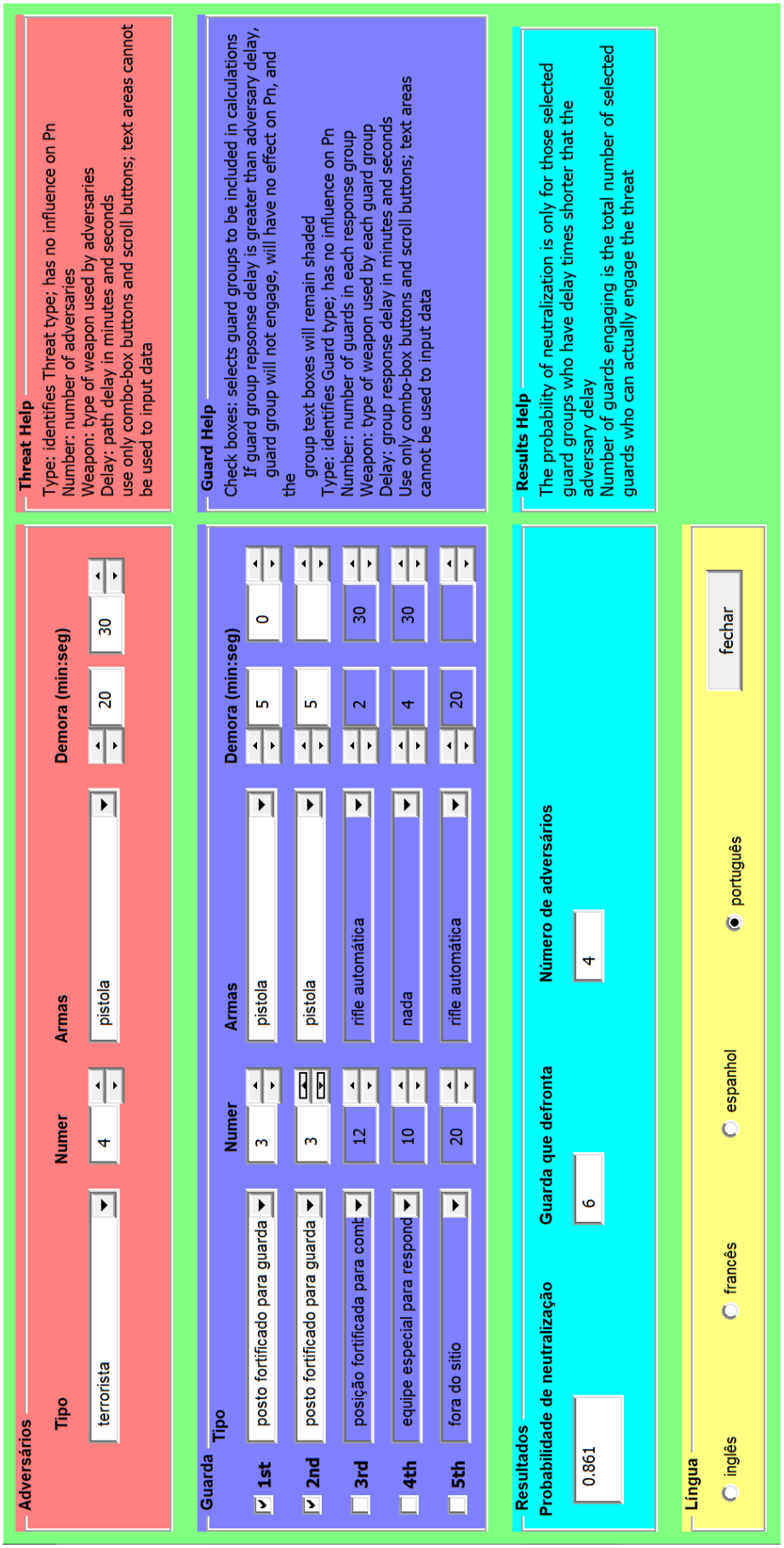


Figura 7: Probabilidade de Neutralização para o cenário 1.

Figura 8: Probabilidade de Neutralização para o cenário 2.

4. Resultados

A frequência de ataque (f_{ataque}) é assumida com o valor de 1,0E-03 por ano [1]. A partir das probabilidades de interrupção e neutralização determinadas para os dois cenários, pode-se determinar os valores de Risco (Eq. 1), Probabilidade de Sucesso do Adversário (Eq. 2), Frequência de Ataque com Sucesso (Eq. 3) e Eficácia do Sistema de Proteção (Eq. 5), como pode-se verificar na tabela 3.

Tabela 3: Resultados

	Cenário 1 (s/ insider)	Cenário 2 (c/ insider)
P_I	0,95	0,94
P_N	0,86	0,70
Risco	1,46E-09	2,74E-09
$P_{sucesso}$	0,18	0,34
$F_{ataque,s}$	1,83E-04	3,42E-04
Eficácia	0,82	0,66

Pode-se perceber que a probabilidade de sucesso para o cenário 1 é de cerca de 18%, enquanto que a probabilidade de sucesso para o cenário 2, onde se considera a presença de um *insider*, é quase o dobro, cerca de 34%. Porém, vale ressaltar que a frequência de ataque com sucesso é relativamente baixa, mesmo considerando a presença de um *insider*, isto se deve ao fato da instalação contar com mecanismos de defesa que dificultam um possível ataque.

5. Conclusões e Recomendações

Este estudo teve como objetivo expor a importância da cultura da segurança no setor nuclear e analisar com ênfase em *security* um cenário de terrorismo em um laboratório hipotético contendo fontes radioativas. A metodologia utilizada para tal análise é recente, desenvolvida nos anos 2000, e vem sendo cada vez mais utilizada pelos Estados Unidos, por sua preocupação com segurança, por este motivo a maior parte das referências são autores e laboratórios americanos. O trabalho enfrentou algumas limitações por seu caráter sigiloso e pela escassez de trabalhos na literatura.

O objetivo foi de analisar os cenários hipotéticos, determinando assim suas probabilidades de neutralização e interrupção, para então determinar o risco associado à instalação e podemos verificar que mesmo com a presença do *insider*, que facilita o trabalho do grupo de adversários, caso o sistema de proteção seja eficaz, com diversas barreiras, o risco permanece pequeno, dificultando a missão do grupo terrorista.

Pode-se pensar em melhorias para o laboratório em questão, como o aumento de mecanismos de defesa, utilizando câmeras de monitoramento, acessos controlados, policiamento da instituição, entre outros. Este trabalho poderia se estender para os laboratórios brasileiros do setor nuclear, que muitas vezes estão mais preocupados com a proteção radiológica que com a proteção física.

Portanto, é necessário que a cultura de segurança nuclear seja priorizada no Brasil assim como é em outros países. A AIEA enfatiza que a preocupação com segurança nuclear precisa ser mundial, evitando assim, possíveis danos à sociedade.

Além disso, recomenda-se futuramente avaliar a frequência de ataque utilizada neste trabalho, se a mesma se aplica a cenários hipotéticos como estes e em realizar a mesma análise para laboratórios brasileiros do setor nuclear.

Referências

1. HAWILA, Mohammad. **Combined Safety and Security Risk Evaluation Considering Safety and Security- Type Initiating Events**. Texas A&M University, 2016.

2. COMISSÃO NACIONAL DE ENERGIA NUCLEAR. *CNEN NN 2.01 - Proteção física de unidades operacionais da área nuclear*. Resolução CNEN 110/11, nov. 2011. Disponível em: http://appasp.cnen.gov.br/seguranca/normas/pdf/Nrm201.pdf. Acesso em 10 jun. 2019.

3. CARDOSO, Eliezer de Moura. **Aplicações da Energia Nuclear**. CNEN. Disponível em: http://www.cnen.gov.br/images/cnen/documentos/educativo/aplicacoes-da-energia-nuclear.pdf. Acesso em 13 jun. 2019.

4. COMISSÃO NACIONAL DE ENERGIA NUCLEAR. *CNEN NN 3.01 – Diretrizes Básicas De Proteção Radiológica*. Resolução 164/14, mar. 2014. Disponível em: http://appasp.cnen.gov.br/seguranca/normas/pdf/Nrm301.pdf. Acesso em 10 jun. 2019.

5. COMISSÃO NACIONAL DE ENERGIA NUCLEAR. *CNEN NE 5.01 – Transporte De Materiais Radioativos*. Resolução CNEN 013/88, ago. 1988. Disponível em: http://appasp.cnen.gov.br/seguranca/normas/pdf/Nrm501.pdf. Acesso em 10 jun. 2019.

6. COMISSÃO NACIONAL DE ENERGIA NUCLEAR. *CNEN NN 5.04 - Rastreamento De Veículos De Transporte De Materiais Radioativos*. Resolução CNEN 148/13, mar 2013. Disponível em: http://appasp.cnen.gov.br/seguranca/normas/pdf/Nrm504.pdf. Acesso em 13 jun. 2019.

7. BRASIL. Relatório do Acidente Radiológico em Goiânia. apresentado por Rex Nazaré Alves, à Comissão Parlamentar de Inquérito do Senado Federal, mar. 1988. Disponível em:http://www.iaea.org/inis/collection/NCLCollectionStore/_Public/19/076/19076677.pdf. Acesso em 13 jun.2019.

8. IAEA. **Nuclear Security Culture: Implementing Guide.**Viena: [s.n.], 2008. p. 48.

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

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

11. INTERNATIONAL ATOMIC ENERGY AGENCY. International Nuclear and Radiological Event Scale (INES). Vienna, 2013. Disponível em: https://www.iaea.org/topics/emergency-preparedness-and-response-epr/international-nuclear-radiological-event-scale-ines. Acesso em 14 jun. 2019.

12. INTERNATIONAL ATOMIC ENERGY AGENCY. INES The International Nuclear And Radiological Event Scale User's Manual. 2008 Edition. Vienna, 2013. Disponível

em: https://www-pub.iaea.org/MTCD/Publications/PDF/INES2013web.pdf. Acesso em 14 jun. 2019.

13. INTERNATIONAL ATOMIC ENERGY AGENCY. The International Legal Framework for Nuclear Security. IAEA International Law Series n. 4. Vienna, 2011. Disponível em: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1486_web.pdf. Acesso em 13 jun. 2019.

14. GICNT. Disponível em: https://www.state.gov/t/isn/c18406.htm. Acesso em 13 jun. 2019.

15. GICNT. Disponível em: http://www.gicnt.org/index.html. Acesso em 13 jun. 2019.

16. IAEA. **Defense in Depth in Nuclear Safety.** Viena, 1996.

17. ENB. **Revista Técnica e Formativa da Escola Nacional de Bombeiros,** nº 17, Sintra, 2001, p.48.

18. ABREU, Caio Coqueijo de. **Análise de risco considerando a segurança nuclear e proteção física de uma instalação nuclear hipotética**. 2018. Dissertação, Programa de Engenharia Nuclear, COPPE, Universidade Federal do Rio de Janeiro, Rio de Janeiro, RJ, 2018

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

20. COX, JR; ANTHONY L. **Some limitations of 'Risk = Threat x Vulnerability x Consequence' for Risk Analysis of Terrorist Attacks**. Risk Anal. 28(6):1749-61, dec. 2008.

21. 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.

22. E. E. Lewis. **Introduction to Reliability Engineering**. Wiley, New York, 1994.

23. HARI. **Hypothetical Facility Exercise Data Handbook**. The Twenty-Seventh International Training Course, United States Government, Department of Energy, Washington, DC, 2017.