DISSERTAÇÃO DE MESTRADO PROFISSIONAL

AVALIAÇÃO DA EFETIVIDADE DE SISTEMAS DE SEGURANÇA DE INSTALAÇÕES NUCLEARES EM CENÁRIOS DE ATAQUES CIBERNÉTICOS E FÍSICOS

Renato Luiz Alves Tavares

Programa de Pós-Graduação Profissional em Engenharia Elétrica

DEPARTAMENTO DE ENGENHARIA
ELÉTRICA FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

AVALIAÇÃO DA EFETIVIDADE DE SISTEMAS DE SEGURANÇA DE INSTALAÇÕES NUCLEARES EM CENÁRIOS DE ATAQUES CIBERNÉTICOS E FÍSICOS

EFFECTIVENESS EVALUATION OF NUCLEAR FACILITIES' SECURITY SYSTEMS UNDER CYBER-PHYSICAL ATTACK SCENARIOS

RENATO LUIZ ALVES TAVARES

ORIENTADOR: WILLIAM FERREIRA GIOZZA, Ph.D.
COORIENTADOR: ROBSON DE OLIVEIRA ALBUQUERQUE, Dr.

DISSERTAÇÃO DE MESTRADO PROFISSIONAL EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: PPEE.MP.035
BRASÍLIA/DF, FEVEREIRO – 2023

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

AVALIAÇÃO DA EFETIVIDADE DE SISTEMAS DE SEGURANÇA DE INSTALAÇÕES NUCLEARES EM CENÁRIOS DE ATAQUES CIBERNÉTICOS E FÍSICOS

Renato Luiz Alves Tavares

Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Engenharia Elétrica

Banca Examinadora

Prof. William Ferreira Giozza, Ph.D, FT/UnB _____
Orientador

Prof. Robson de Oliveira Albuquerque, Dr., FT/UnB _____
Co-orientador

Prof. João José Costa Gondim, Dr., FT/UnB _____
Examinador interno

Prof. Antonio Teixeira e Silva, Dr., IPEN/USP _____
Examinador externo

FICHA CATALOGRÁFICA

TAVARES, RENATO LUIZ ALVES
Avaliação da efetividade de sistemas de segurança de instalações nucleares em cenários de ataques cibernéticos e físicos [Distrito Federal] 2023.
x,72p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2023).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Segurança cibernética	2. Instalações nucleares
3. Infraestruturas Críticas	4. Gerenciamento de riscos
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

TAVARES, R.L.A. (2023). *Avaliação da efetividade de sistemas de segurança de instalações nucleares em cenários de ataques cibernéticos e físicos*. Dissertação de Mestrado Profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF,72p.

CESSÃO DE DIREITOS

Renato Luiz Alves Tavares
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Para minha filha, minha maior alegria e meu maior desafio.

AGRADECIMENTOS

À minha família, por todo o suporte, dedicação e paciência;

Ao meu orientador, pela orientação, pelas sempre interessantes discussões e por acreditar na importância do tema estudado;

Ao meu coorientador, pelas valiosas contribuições para o aperfeiçoamento desse trabalho, desde o princípio;

Aos nobres professores do PPEE/UnB, pela paciência e ensinamentos ao longo das matérias desse curso de mestrado;

A todos os colegas da turma PPEE/ABIN, pela oportunidade de conviver com tantos colegas de incríveis conhecimentos e experiências, tão importantes ao longo das jornadas rumo às aprovações nas disciplinas.

Às servidoras da secretaria do PPEE, pelos inúmeros e valiosos auxílios nas questões administrativas referentes ao curso;

Aos colegas do ESF/DISEN/CNEN, por mantermos, dentro de nossas limitações, um ambiente de trabalho no qual podemos trocar ideias e experiências, tão valiosos na confecção dos cenários deste trabalho;

A todos que de alguma forma passaram por essa caminhada e que, pela minha parca memória, não pude listar nominalmente aqui;

À Agência Brasileira de Inteligência (ABIN) e à Universidade de Brasília (UnB), por formarem uma turma específica de mestrado em segurança cibernética, tema tão importante e necessário no cenário atual;

E por último, e não menos importante, a Nossa Senhora de Nazaré, padroeira de todos os paraenses!

RESUMO

Título: Avaliação da efetividade de sistemas de segurança de instalações nucleares em cenários de ataques cibernéticos e físicos

Autor: Renato Luiz Alves Tavares

Orientador: William Ferreira Giozza, Dr.

Coorientador: Robson de Oliveira Albuquerque, Dr.

Programa de Pós-Graduação Profissional em Engenharia Elétrica – Área de Concentração em Segurança Cibernética

Brasília/DF, 07 de fevereiro de 2023

Este trabalho tem como objetivo avaliar a efetividade probabilística do sistema de segurança física em um modelo de instalação nuclear, sob cenários de ataque envolvendo ameaças híbridas, ou seja, com capacidades cibernéticas e físicas. Em um contexto global propício ao aumento de ataques a infraestruturas críticas, inclusive envolvendo acesso ilícito e sabotagem sobre materiais nucleares, aliado à rápida evolução e diversidade de ataques cibernéticos em diversos setores da sociedade, configura-se notável desafio avaliar a segurança das infraestruturas críticas. Tendo em vista aspectos de confidencialidade sobre o projeto de sistemas de segurança de instalações nucleares reais, foi modelada uma instalação hipotética (Instituto de Ciências Nucleares do Cerrado), considerando o arcabouço legal e regulatório vigente no Brasil e modelos similares em uso pela Agência Internacional de Energia Atômica (AIEA) para o propósito de treinamento. O modelo descreve a caracterização da ameaça, do sistema de segurança e dos cenários de ataque ciberfísicos, sendo utilizados parâmetros probabilísticos de desempenho na literatura para o cálculo da efetividade (P_E) do sistema de segurança, comparando cenários de ataques puramente físicos a outros no qual há o comprometimento de ativos digitais críticos à segurança. Os resultados mostraram um decréscimo significativo na efetividade do sistema, indicando a necessidade de melhorias nas medidas de segurança de instalações nucleares, do ponto de vista regulatório e operacional. Ademais, a metodologia usada no trabalho é geral e aplicável a outros tipos de infraestruturas críticas.

Palavras-chave: segurança cibernética, segurança nuclear, ataque ciberfísico, ameaças híbridas, infraestruturas críticas.

ABSTRACT

Title: Effectiveness Evaluation of nuclear facilities' security systems under cyber-physical attack scenarios

Author: Renato Luiz Alves Tavares

Supervisor: William Ferreira Giozza, Dr.

Co-Supervisor: Robson de Oliveira Albuquerque, Dr.

Programa de Pós-Graduação Profissional em Engenharia Elétrica – Área de Concentração em Segurança Cibernética

Brasília/DF, February 7th 2023

The present work aims to perform an evaluation on the probabilistic effectiveness of the security system for a nuclear facility model, under attack scenarios involving hybrid threats, i.e. with both cyber and physical capabilities. Amid a global context propitious to the increase in attacks over critical infrastructure, including those involving illicit access and sabotage on nuclear materials, combined with the rapid evolution and diversity of cyber attacks in various sectors of society, it is a notable challenge to assess the security of critical infrastructure. Considering aspects of confidentiality on security systems designs for real nuclear facilities, a hypothetical one (Instituto de Ciências Nucleares do Cerrado) was modelled, considering the legal and regulatory framework in force in Brazil and similar models in use by the International Agency of Atomic Energy (IAEA) for training purposes. The model describes the characterization of the threat, the security system and the cyber-physical attack scenarios, using probabilistic performance parameters from the literature to calculate the effectiveness (P_E) of the security system, comparing scenarios of purely physical attacks to others in which security-critical digital assets are compromised. The results showed a significant decrease in the effectiveness of the system, indicating the need for improvements in the safety measures of nuclear installations, from a regulatory and operational point of view. Furthermore, the methodology used in the work is general and applicable to other types of critical infrastructure.

Keywords: Cyber Security, Nuclear Security, Cyberphysical Attack, Hybrid Threats, Critical Infrastructure.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

ABP	Ameaça Base de Projeto
ADC	Ativo Digital Crítico
AIEA	Agência Internacional de Energia Atômica
AP	Área Protegida
APT	*Advanced Persistant Threat*
AV	Área Vigiada
BMS	*Balanced Magnetic Switch*
CDC	Comando do Cerrado
CNEN	Comissão Nacional de Energia Nuclear
CFTV	Circuito Fechado de Televisão
CPPNM	*Convention on the Physical Protection of Nuclear Material*
DDR	Dispositivo de Dispersão Radiológica
DEPO	Design and Evaluation Process Outline
DER	Dispositivo de Exposição Radiológica
DoS	*Denial of Servic*e
DRR	Depósito de Rejeitos Radioativos
DSA	Diagrama de Sequência de Adversário
ECA	Estação Central de Alarmes
ESA	Estação Secundária de Alarmes
ICNC	Instituto de Ciências Nucleares do Cerrado
ICNC-IG	Irradiador Gama do Instituto de Ciências Nucleares do Cerrado
ICNC-R	Reator Nuclear do Instituto de Ciências Nucleares do Cerrado
IEEE	*Institute of Electrical and Electronics Engineers*
INIS	*International Nuclear Information Systems*
IOE	Indivíduo Ocupacionalmente Exposto
LFCN	Laboratório de Fabricação de Combustíveis Nucleares
LGPD	Lei Geral de Proteção de Dados Pessoais
MLC	Movimento de Libertação do Cerrado
NORM	*Naturally Ocurring Radioactive Material*
NTI	*Nuclear Threat Initiative*
ORCRIM	Organização Criminosa

PCD	Ponto Crítico de Detecção
PNB	Programa Nuclear Brasileiro
PD	Probabilidade de Detecção
PTZ	*Pan-Tilt-Zoom*
SisPF	Sistema de Proteção Física
TIC	Tecnologia da Informação e Comunicação
TG	Tempo de Atuação da Força de Resposta
UC	Universidade do Cerrado
VA	Área Vital

1 INTRODUÇÃO

A área da segurança física nuclear é um processo que envolve tecnologias, pessoas, organizações e uma estrutura regulatória que deve refletir os anseios da sociedade na proteção das instalações, pessoas e meio ambiente contra os efeitos potencialmente catastróficos de ações de roubo ou sabotagem envolvendo materiais e instalações nucleares [1]. Para que este processo seja implantado adequadamente, recomendações, normas, diretrizes, acordos, tratados e vários outros instrumentos vêm sendo constantemente desenvolvidos e atualizados para prevenir e mitigar as consequências de incidentes e garantir o uso seguro da tecnologia nuclear para fins pacíficos, que é uma premissa básica prevista na Constituição Federal [2].

Em um cenário de aumento da percepção de ameaças (por exemplo, terrorismo) com o potencial de atingir materiais e instalações nucleares em todo o mundo [3] e o uso cada vez mais disseminado de dispositivos de tecnologia da informação e comunicações (TIC) em sistemas de instrumentação e controle industrial, sistemas de segurança tecnológica, física e de contabilidade e controle de material nuclear [4], torna-se imperativo haver meios pelos quais os Estados procurem garantir a disponibilidade, integridade e confidencialidade das informações que transitam nos sistemas supramencionados, visando o atendimento ao objetivo primordial da segurança nuclear, que é a proteção de indivíduos (sejam ocupacionalmente expostos ou do público) e do meio ambiente contra os riscos oriundos da utilização indevida das radiações ionizantes [5].

No Brasil, foram recentemente publicadas a Lei Geral de Proteção de Dados Pessoais (LGPD) [6] e a Estratégia Nacional de Segurança Cibernética (E-Ciber) [7], que demonstram, de forma inequívoca, a relevância do tema e a preocupação do Estado Brasileiro no sentido de prover proteção aos ativos cibernéticos das infraestruturas críticas e dos serviços públicos nacionais, dos quais a área nuclear faz parte. No entanto, a Comissão Nacional de Energia Nuclear (atualmente a autoridade reguladora nacional em radioproteção e segurança nuclear), embora tenha nos últimos anos realizado a revisão de normas obsoletas [8] e a publicação de novas normas concernentes à segurança física [9] [10], ainda não prevê, na atualidade, requisitos regulatórios que tratem a questão das ameaças com capacidades cibernéticas, em especial considerando ameaças híbridas (envolvendo ativos digitais e físicos) [11].

O cenário brasileiro é refletido em índices como o publicado anualmente pelo Nuclear Threat Initiative (NTI), segundo o qual, para os aspectos de proteção contra sabotagem de instalações nucleares, o Brasil ocupa atualmente o 42º lugar no ranking entre 47 países com instalações nucleares cujas consequências radiológicas seriam relevantes em caso de ataque (por exemplo, reatores de potência e de pesquisa), sendo que, na escala de pontos em relação aos aspectos de segurança cibernética, possui nota zero [12]. O índice do NTI levou em consideração os temas: obrigatoriedade legal/regulatória de se prover segurança cibernética para instalações nucleares; a gestão dos ativos digitais críticos; avaliação de ameaças cibernéticas promovidas pelo Estado; avaliação de vulnerabilidades cibernéticas; planejamento e preparo para resposta a incidentes cibernéticos na área nuclear e programas de conscientização e cultura de segurança cibernética.

No cenário internacional, a Agência Internacional de Energia Atômica, órgão do sistema das

Nações Unidas que é, dentre outras funções, um fórum intergovernamental de desenvolvimento e cooperação técnico-científica em ciência e tecnologia nuclear para fins pacíficos [13], vem publicando ao longo da última década diversas recomendações para tratar, separadamente, os temas da segurança física, cibernética e da informação [14][15][16], enfatizando a necessidade de uma atuação dos Estados membros no fortalecimento das abordagens de segurança de forma local, tendo como premissa básica a soberania da ações dos Estados, os quais têm responsabilidade pela manutenção de regimes próprios de segurança física nuclear.

A Emenda à Convenção de Proteção Física de Material Nuclear (CPPNM/A, na sigla em inglês), instrumento internacional de caráter juridicamente vinculante (obrigatório), recentemente ratificado pelo Congresso Nacional [17] preconiza, como um de seus princípios fundamentais, a proteção das informações cuja manipulação indevida possa acarretar no comprometimento da segurança de materiais e instalações nucleares [18].

O escopo do trabalho de pesquisa, objeto do presente trabalho, voltou-se para a construção de uma base de conhecimentos suficiente para, primeiramente, compreender o problema a ser tratado, ou seja, as ameaças com capacidades cibernéticas e físicas que tenham como alvo instalações nucleares, possíveis modos de operação dessas ameaças, inclusive os ativos de maior vulnerabilidade e que possam resultar em consequências radiológicas indesejáveis do ponto de vista da segurança nuclear.

Em seguida, usaram-se ferramentas já consolidadas, utilizadas na avaliação de vulnerabilidades de instalações nucleares para ataques puramente físicos, porém integrando cenários nos quais ataques cibernéticos compõem as capacidades dos adversários, permitindo gerar, portanto, ataques híbridos (“ciberfísicos”), cujos possíveis impactos nos parâmetros de desempenho do sistema de segurança podem ensejar propostas de ações de melhoria nos referidos sistemas. Ademais, vislumbrou-se comparar os impactos dos ataques ciberfísicos com aqueles oriundos de ataques puramente físicos.

1.1 Justificativa

A relevância e preocupação internacional sobre segurança cibernética e física de instalações nucleares motivaram a publicação de diversos trabalhos acadêmicos na última década, porém as abordagens vêm normalmente sendo realizadas em separado, ou seja, ora tratando de aspectos puramente físicos, ora tratando de aspectos puramente cibernéticos. Especificamente para a área nuclear, é um campo de pesquisa bastante recente, sendo os primeiros trabalhos publicados no início dos anos 2000, tendo um maior volume de pesquisas e publicações a partir de 2010 [19] [20] [21].

No contexto nacional, há uma grande carência de estudos e pesquisas que tratem das questões de segurança física e cibernética envolvendo materiais e instalações nucleares, sejam as abordagens tomadas em separado ou de forma integrada.

Portanto, um trabalho que tenha como objetivo estudar consequências de cenários de ataques envolvendo simultaneamente ativos digitais e físicos da área nuclear, além de trazer uma contribuição para a área com razoável caráter de originalidade acadêmica, pode ser útil como um embasamento para melhorias não apenas na área regulatória, mas também em termos de políticas e procedimentos dos operadores nucleares.

1.2 Objetivos

Este trabalho tem como objetivo geral propor um modelo que permita entender e estimar impactos de ataques combinados cibernéticos e físicos ao sistema de segurança física em uma instalação nuclear, pela aplicação de ferramentas de avaliação de vulnerabilidades.

Para alcançar o objetivo geral, foi necessário realizar as seguintes etapas:

- Modelar uma instalação nuclear e seus sistemas de segurança física, adaptando modelos de instalações existentes na literatura, tendo em vista as questões de sigilo envolvidas nas documentações dos processos e projetos de instalações nucleares reais;
- Avaliar possibilidades de ataques cibernéticos ao sistema de segurança física da instalação nuclear modelada, por exemplo, nos sistemas de monitoramento por circuito fechado de televisão (CFTV), controles de acesso, trancas ou sensores de intrusão;
- Elaborar cenários de ameaças que envolvam adversários com capacidade de realizar ataques híbridos (cibernéticos e físicos), explorando vulnerabilidades cibernéticas documentadas em bases de dados específicas;
- Utilizar ferramentas de avaliação de vulnerabilidades para estimar o efeito dos ataques nos parâmetros clássicos de desempenho dos sistemas de segurança física das instalações nucleares, por exemplo, na efetividade global do sistema, que é função das probabilidades de interrupção e de neutralização;
- Identificar ações no sentido regulatório, técnico e operacional para uma melhoria das ações de segurança de instalações nucleares e propor melhorias para o sistema.

1.3 Hipótese de Pesquisa

O trabalho de pesquisa tem como “hipótese” que a modelagem híbrida e a metodologia propostas permitem uma melhor avaliação da efetividade de cenários de ataque ciberfísicos em termos de compreender esse tipo de ataque, possibilitando o desenvolvimento de ações de resposta com controles cibernéticos e físicos de forma integrada, para diferentes ativos e práticas da área nuclear.

1.4 Metodologia

Na elaboração da introdução histórica, do contexto da área de segurança cibernética do programa nuclear brasileiro e levantamento bibliográfico, foram utilizados dados provenientes de diversas fontes, como livros, teses, dissertações, artigos científicos publicados em periódicos, trabalhos de conferência e publicações na imprensa. As bases de dados utilizadas para a busca foram:

- Google Acadêmico;
- International Nuclear Information System (INIS), da Agência Internacional de Energia Atômica;
- IEEE Xplore; e

- Rede de Bibliotecas do Exército Brasileiro (RedeBIE).

Para atingir o objetivo do trabalho, foi seguida uma metodologia dividida em quatro etapas, podendo ser visualizada de forma esquemática na Fig. 1.1:

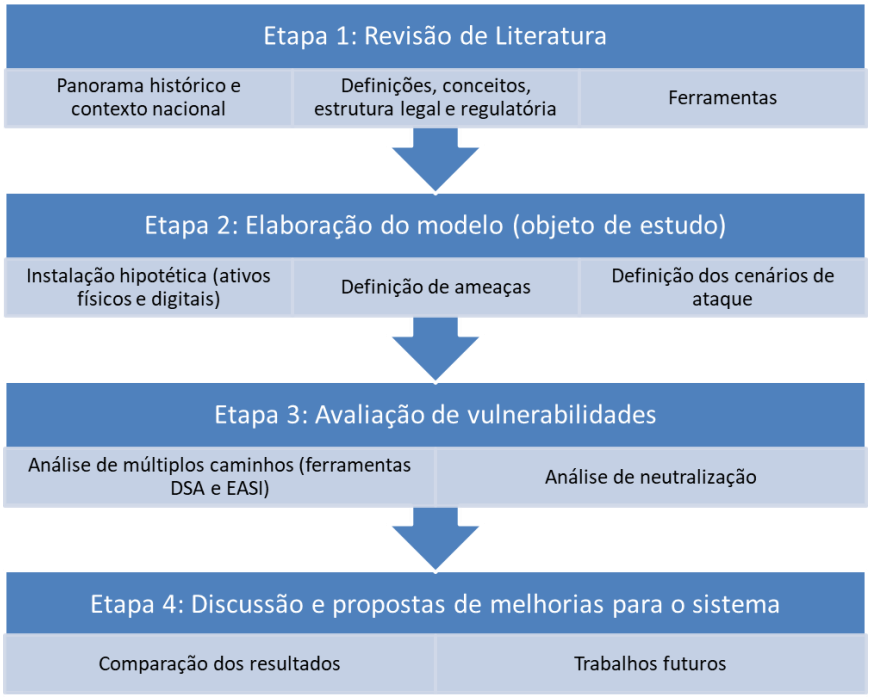


Figura 1.1. Etapas do estudo.

Na primeira etapa, “Revisão de Literatura”, foi realizado um trabalho de pesquisa, tendo como insumos leis, normas, livros, artigos, recomendações internacionais e demais publicações sobre segurança cibernética e física de instalações nucleares, com a intenção de descrever um panorama atualizado sobre os temas e viabilizar a criação de modelos de instalações nucleares adequados à realização do estudo.

Na segunda etapa, “Elaboração do modelo”, tendo como insumo o arcabouço teórico do país elaborado na etapa anterior, e considerando as restrições regulatórias vigentes no para o compartilhamento de informações relativas aos sistemas de segurança de instalações reais [11], criou-se um modelo de instalação nuclear, ou utilizados modelos existentes na literatura, como os modelos de instalação nuclear de [1], [22] e [23], adaptando-os de forma a viabilizar a elaboração de cenários de ataque envolvendo ativos digitais e físicos simultaneamente. O modelo deste trabalho contempla tanto a estrutura de segurança física quanto os equipamentos e as redes de comunicação do sistema de proteção física alvos dos ataques. A necessidade de se criar modelos de instalações deve-se à necessidade da manutenção da confidencialidade das plantas e processos reais.

Nessa fase, ainda, foi postulada uma ameaça-base de projeto (ABP), tendo como base a metodologia adotada internacionalmente [24], que resultou em uma descrição das intenções, motivações e capacidades de possíveis adversários, incluindo as capacidades cibernéticas e os modos de ataque a serem empregados.

Na terceira etapa, destinada a exibir os resultados da avaliação de vulnerabilidades, foram elaborados cenários de ataque ciberfísicos, nos quais os ataques aos ativos digitais críticos exploraram vulnerabilidades conhecidas em equipamentos do sistema de segurança, da seguinte forma:

Cenário 1: Sistema operando normalmente (efetividade base de projeto face à ameaça puramente física de sabotagem no reator nuclear);

Cenário 2: Ataque cibernético ao sistema de câmeras (Circuito Fechado de TV – CFTV) como parte do mesmo ataque físico do cenário 1;

Cenário 3: Ataque cibernético ao sistema de controle de acesso das portas do prédio do Reator, como parte do mesmo ataque físico do cenário 1;

Cenário 4: Ataque cibernético à rede de sensores de intrusão na cerca dupla da área protegida, como parte do mesmo ataque físico dos cenários anteriores;

Na quarta etapa, "Discussão e propostas de melhorias", é realizada uma consolidação e análise dos resultados obtidos, por meio da comparação nos valores da efetividade do sistema de segurança, em particular nos impactos decorrentes dos ataques, e são discutidas possíveis melhorias no sistema de segurança, de forma a se buscar uma melhor resposta tanto em termos físicos quanto lógicos, visando a validação da hipótese do trabalho.

1.5 Contribuições da Pesquisa

O presente trabalho se propõe a contribuir para a área da engenharia elétrica, e mais precisamente para a segurança cibernética com uma abordagem integrada desta com a segurança física nuclear. Nesse contexto, como parte do trabalho de pesquisa, foi publicado um artigo contemplando um dos cenários estudados nessa dissertação [25], especificamente o ataque ciberfísico ao sistema de câmeras usadas na vigilância e monitoramento. No artigo mencionado, os resultados já indicavam um decréscimo significativo da efetividade do sistema de proteção física, motivando a elaboração dos outros cenérios envolvendo diferentes ativos digitais da instalação.

1.6 Organização do Trabalho

Este trabalho consiste das seguintes partes:

Neste Capítulo 1, "Introdução", são apresentadas as bases para o desenvolvimento do trabalho: um panorama histórico das ações de segurança física nuclear e as interfaces com a segurança cibernética e o cenário atual relacionado ao tema. Mostra, ainda, a hipótese de pesquisa, a metodologia e a organização do trabalho.

O Capítulo 2, "Referencial Teórico e Trabalhos Correlatos", tem a finalidade de descrever conceitos, definições, ferramentas e técnicas utilizadas para se obterem os resultados previstos no trabalho, além de trabalhos correlatos.

O Capítulo 3, "Modelo e Framework Proposto", fornece uma descrição detalhada do objeto de estudo (a instalação nuclear), das ameaças postuladas, com suas intenções, motivações e capacidades.

O Capítulo 4, "Avaliação de Desempenho", apresenta os cenários de ataque com as vulnerabilidades cibernéticas exploradas pelos adversários, a avaliação das vulnerabilidades e determinação do parâmetro de desempenho do sistema de segurança (Efetividade) para todos os cenários estudados;

Finalmente, o Capítulo 5, "Conclusões", consolida e compara os resultados obtidos, aponta desafios para a implantação das etapas desse estudo em cenários reais e delineia oportunidades de continuação do tema estudado, a serem exploradas por outros pesquisadores acerca do tema.

2 REFERENCIAL TEÓRICO E TRABALHOS CORRELATOS

O Brasil, sendo um país no qual o caráter pacífico do seu programa nuclear está expresso textualmente na Constituição Federal [2], tem buscado nas últimas décadas a consolidação e expansão de seu já maduro programa nuclear, o qual não apenas é voltado para a produção de energia elétrica limpa, mas também para outras aplicações da tecnologia nuclear, como a propulsão naval, a produção de radiofármacos, diagnósticos médicos e outras aplicações nas áreas médica e industrial [26]. O país conta com instalações de mineração, beneficiamento, conversão e enriquecimento de urânio (Figura 2.1), resultando em um ciclo do combustível nuclear aberto e com total domínio tecnológico autóctone, ao contrário da maioria dos países da América Latina, mesmo que algumas etapas do ciclo ainda não supram em escala industrial todas as necessidades do país [27].

Figura 2.1. O ciclo do Combustível Nuclear - urânio. Fonte:[28]

Nesse contexto, é de fundamental importância prover a segurança dos ativos envolvidos com o programa nuclear, em particular os materiais e as instalações nucleares. Dentre esses ativos, crescem em importância os ativos digitais, entendidos como sistemas e tecnologias que criam, acessam, processam, calculam, comunicam ou armazenam informações no formato digital [15]. Desses ativos, consideram-se ativos digitais críticos (ADC) aqueles cujo comprometimento possa acarretar impactos significativos à segurança nuclear ou à segurança física nuclear, e que necessitam de segurança, em todos os domínios.

2.1 Segurança Nuclear, Segurança Física e Segurança Cibernética

As acepções da palavra "segurança" no contexto da área nuclear englobam uma variedade de disciplinas [5]:

– A Segurança Nuclear ou Segurança Tecnológica ("nuclear safety") consiste na obtenção de condições operacionais, prevenção e controle de acidentes e mitigação apropriada das consequências de acidentes, resultando em proteção de indivíduos ocupacionalmente expostos (IOEs), do público e do meio ambiente contra os riscos da radiação. A Segurança Nuclear é alcançada por meio de um conjunto de medidas de caráter técnico e administrativo, incluídas no projeto, na construção, no comissionamento, na operação, na manutenção e no descomissionamento de uma instalação nuclear [1].

– A Segurança Física Nuclear ("nuclear security") consiste na prevenção, detecção e resposta a eventos de roubo, sabotagem, acesso não autorizado, transferência ilícita ou outros atos maléficos envolvendo material nuclear, materiais radioativos, bem como as instalações que os operam. É um conceito abrangente, que inclui o arcabouço legal e regulatório, procedimentos e práticas dos operadores. Existe, ainda, na terminologia da área, o conceito de "Proteção Física", que consiste nas medidas tomadas pelos operadores, no âmbito das instalações, sob fiscalização e licenciamento do órgão regulador, para materializar os objetivos da Segurança Física Nuclear [1].

Ambas as áreas da "segurança" têm como objetivo sinérgico a proteção de pessoas, sejam ocupacionalmente expostos ou do público, a sociedade, as propriedades e o meio ambiente contra os efeitos possivelmente danosos da radiação ionizante. As medidas promovidas por ambas as áreas devem idealmente ser projetadas de forma integrada [22].

Os atentados terroristas de 11 de setembro de 2001 realizados nos Estados Unidos acarretaram em uma ampla mudança em termos de legislação internacional, por exemplo, na publicação da Resolução 1540 do Conselho de Segurança das Nações Unidas, que requer que os Estados Membros desenvolvam e apliquem medidas contra a proliferação de agentes químicos, biológicos, radiológicos e nucleares e os respectivos vetores, visando deter a aquisição ou construção de armas de destruição em massa por atores não estatais [1]. Tal resolução encontra- se internalizada no direito nacional por meio do Decreto 7722, de 20 de abril de 2012 [29].

Nos anos seguintes, houve um grande desenvolvimento da ciência e da engenharia envolvida com a segurança física de materiais nucleares. Foram desenvolvidas diversas áreas de conhecimentos voltados a características específicas, como (Figura 2.2):

- Proteção Física no Transporte de Materiais Nucleares e Radioativos;
- Proteção Física de Instalações Nucleares e Radiativas;
- Estimativa de Ameaças;
- Contabilidade e Controle de Material Nuclear (em suporte ao atendimento aos tratados internacionais ratificados pelo Brasil, como o Tratado de Não-Proliferação de Armas Nucleares – TNP);
- Medidas de Proteção Física voltadas aos grandes eventos públicos (que envolvem grandes aglomerações de pessoas e podem ser alvos de ações mal-intencionadas com materiais radioativos ou nucleares provenientes de roubo);
- Arquiteturas nacionais de detecção de contrabando de materiais nucleares e radiológicos (nos limites nacionais como fronteiras terrestres, portos ou aeroportos);

- Desenvolvimento de pessoas, treinamento, cultura de segurança.

Figura 2.2. Diferentes domínios da Segurança Física Nuclear ("nuclear security"). Adaptado de [1].

Mais recentemente, a descoberta do *worm* "Stuxnet", que teve como alvo a infraestrutura de ultracentrífugas para enriquecimento de urânio do Irã, trouxe a atenção da comunidade internacional no sentido da possibilidade de um ataque cibernético acarretar em consequências cinéticas, uma vez que houve destruição de parte daqueles ativos físicos essenciais à consecução dos objetivos do programa nuclear iraniano [30]. Em especial, o ataque chamou a atenção pelo fato de impactar sistemas de automação industrial (em inglês conhecidos como "Operational Technology" - OT).

Desde o "Stuxnet", cresceram as preocupações internacionais no sentido de proteger os ativos digitais críticos de instalações nucleares contra atos mal-intencionados de roubo ou sabotagem, não apenas aqueles que podem incorrer em consequências radiológicas, mas também atos que visem o vazamento de informações de caráter sigiloso que transitam em meio digital, tendo em vista os segredos industriais envolvidos nos projetos e operações desse tipo de instalação. Assim, foi desenvolvido um extenso compêndio de recomendações internacionais no sentido de guiar os Estados no sentido de estabelecer medidas legais, regulatórias e técnicas em segurança cibernética [15].

Nesse contexto, a Segurança Cibernética pode ser definida, conforme [15] como um aspecto particular da segurança da informação, que trata da proteção de sistemas computacionais contra ações maléficas. O glossário do setor nuclear e radiológico brasileiro [5], por sua vez, define "segurança computacional" como medidas contra-ataques cibernéticos, prevenindo, detectando, bloqueando e respondendo a tentativas de acesso não autorizado a ativos digitais críticos à segurança nuclear.

A disciplina de Segurança Cibernética, ao longo do tempo, vem evoluindo para muitas áreas do conhecimento [31]. Este trabalho tem foco na área de segurança de infraestruturas críticas, com ênfase na segurança cibernética de sistemas ciber-físicos.

A Figura 2.3 permite visualizar, de forma esquemática, os diferentes aspectos e áreas de conhecimento específicas da Segurança Cibernética, com ênfase no domínio estudado neste trabalho.

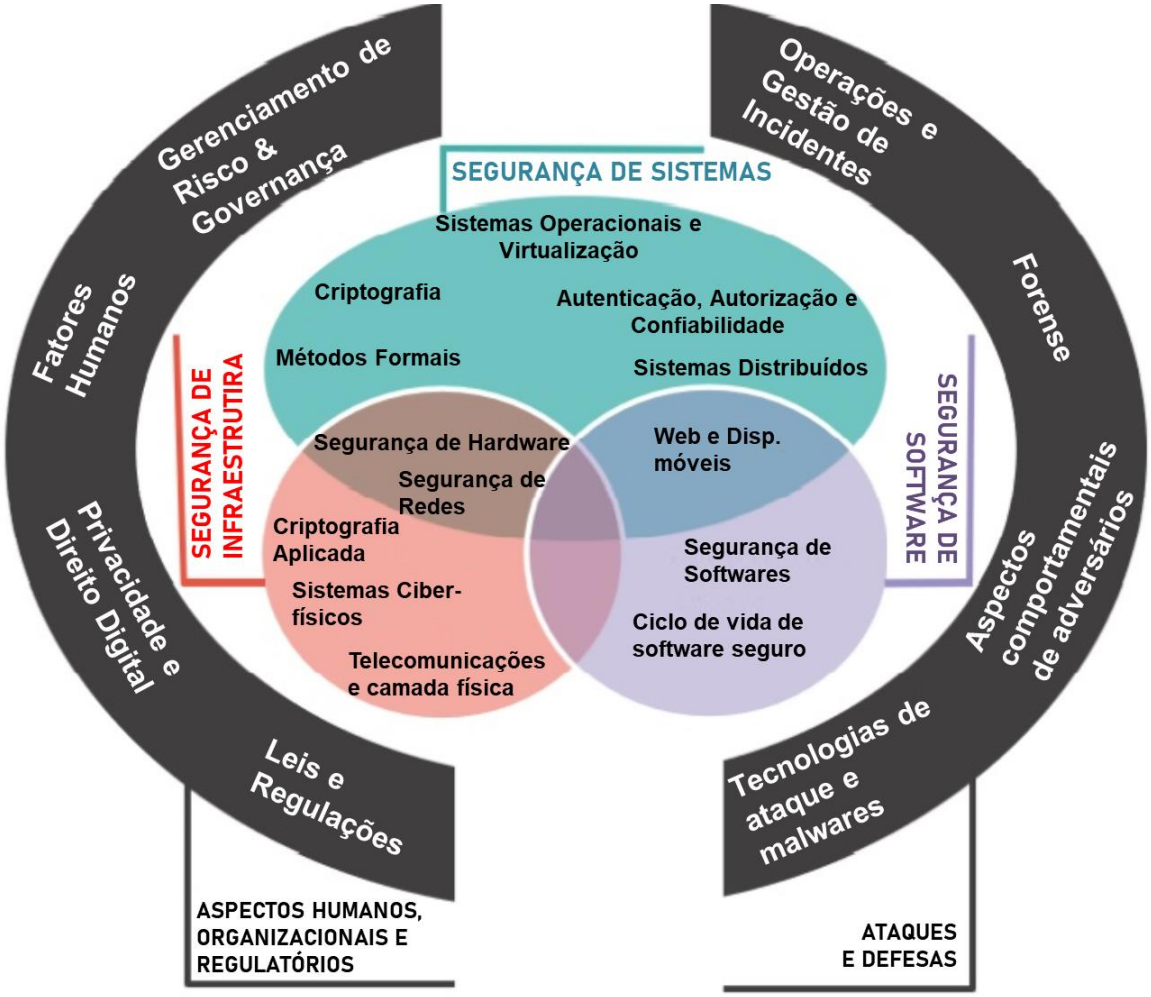


Figura 2.3. Áreas do conhecimento em Segurança Cibernética. Adaptado de [31].

2.2 O *framework* DEPO: Design and Evaluation Process Outline

O *framework* DEPO (*Design and Evaluation Process Outline*) [32] surgiu da necessidade de sistematizar a sequência de ações necessárias à definição de requisitos, objetivos, projeto e avaliação de um sistema de segurança física (na terminologia da área nuclear, denomina-se Sistema de Proteção Física – SisPF).

O processo se inicia com a definição de requisitos e objetivos, que para serem formulados, o projetista deve caracterizar (descrever) a instalação, definir a ameaça e identificar os alvos. Esta fase envolve um levantamento detalhado de informações como operações e condições da planta, e requerimentos de proteção física.

Em seguida, é feita a definição de ameaças, o que envolve a consideração de características como motivação, intenção e capacidades das ameaças; finalmente a definição dos alvos, ou seja, os ativos que o sistema se propõe a proteger.

Com base nos recursos e informações da primeira fase, incluindo os requisitos regulatórios vigentes, o projetista deve elaborar ou revisar um sistema de proteção física que contemple as metas definidas.

A terceira fase, então, consiste na avaliação de vulnerabilidades do sistema projetado, considerando as ameaças definidas na primeira fase, de forma a garantir que o SisPF atenda aos objetivos inicialmente estipulados.

Dada a complexidade envolvida em sistemas de proteção física, tal avaliação comumente envolve modelagem e simulação. Caso essa última fase leve à conclusão da existência de vulnerabilidades no SisPF, o sistema inicial deve ser novamente projetado, até que sejam atendidos os objetivos.

A Figura 2.4 permite visualizar de forma esquemática as fases e etapas do *framework* DEPO:

Figura 2.4. O framework DEPO. Adaptado de [1].

Em particular, a avaliação de vulnerabilidades realizada no escopo deste trabalho será realizada por meio das ferramentas EASI (*Estimation of Adversary Sequency Interruption*) e de Diagramas de Sequência de Adversário (DSA), ambas descritas em [32].

2.3 Segurança Cibernética em Instalações Nucleares

A recomendação da Agência Internacional de Energia Atômica (AIEA) [15] conceitua que, para instalações nucleares, os ativos digitais críticos (ADC) normalmente dão suporte aos sistemas que realizam as funções de segurança nuclear, proteção física e contabilidade/controle de materiais nucleares, ou armazenam e processam informações sensíveis relacionadas às funções mencionadas. Tais ADCs podem estar vulneráveis a ataques cibernéticos e serem atacados de forma específica por adversários, o que pode ter impactos adversos à segurança nuclear e física. O comprometimento de ADCs pode potencialmente contribuir ou resultar, por exemplo, em:

- Sabotagem que pode levar a consequências radiológicas inaceitáveis para o público e meio ambiente, se áreas vitais forem atacadas;

- Remoção não-autorizada (roubo) de materiais nucleares ou radioativos;
- Condições degradadas na prevenção, detecção e resposta a eventos de segurança física;
- Perda, alteração ou negação de acesso à informações sensíveis.

Uma estratégia de segurança cibernética [15] consiste em aplicar uma abordagem gradual baseada em níveis e zonas de segurança. Os níveis de segurança representam o grau de proteção requerido. Cada nível possui diferentes conjuntos de requisitos a satisfazer e medidas de segurança específicas (Figura 2.5):

Figura 2.5. Abordagem gradual dos requisitos de segurança cibernética. Adaptado de [15].

A Tabela 2.1 exemplifica uma correlação entre as funções e sistemas típicos de instalações nucleares, os impactos a serem considerados e a classificação em níveis de segurança.

Tabela 2.1. Sistemas e funções de instalações nucleares e níveis de segurança. Adaptado de [15].

Tipo de sistema / função	**Descrição dos ativos digitais**	**Nível de segurança**
Todos os sistemas da instalação	Todos	Básico
Sistemas de proteção do reator (prevenção de condições de acidente) Sistemas de remoção de calor do reator e do armazenamento de combustíveis	Sistemas vitais para a instalação	1
Instrumentação e Controle do reator Sistemas de gestão de resposta a emergências radiológicas Segurança tecnológica em condições normais de operação Proteção Física Sistemas de Controle de Acesso à Áreas Vitais da instalação	Sistemas que requerem um alto nível de proteção	2
Sistemas de informações de variáveis de processo Sistemas de informações de balanço de planta Sistemas de informação de manutenção	Sistemas em tempo real que não sejam estritamente necessários para a operação	3

Sistemas relacionados à geração elétrica Sistemas de monitoração radiológica		
Sistemas de telecomunicação Sistemas de tecnologia da informação de escritório Sistemas de permissão de trabalho / ordem de serviço Gestão de documentação	Sistemas de gerenciamento de dados técnicos que são usados para gerenciamento de avidades de manutenção ou operação	4
Disposivos móveis pessoais quando presentes nas áreas de segurança	Sistemas que não são diretamente importantes para o controle técnico ou para fins operacionais	5

A partir da Tabela 2.1 observa-se que, de acordo com a recomendação da Agência Internacional de Energia Atômica, os ativos digitais críticos relacionados com o sistema de proteção física requerem um alto nível de proteção, de nível 2, evidenciando a relevência do presente estudo.

2.4 Modelos de Instalações usados para fins acadêmicos e de treinamento

Tendo em vista o caráter de sigilo envolvido na divulgação de detalhes relativos à segurança física de instalações nucleares reais, como planos, desenhos e projetos, normalmente são utilizados modelos de instalações para estudar diversos aspectos relativos ao assunto.

Além da óbvia conveniência em termos de sigilo de informações de caráter sensível, o uso de modelos tem as seguintes vantagens [33]:

- Possibilita a aplicação de diferentes cenários de riscos, ameaças e ataques, orientando as tomadas de decisão na área de segurança física com base em adversários dinâmicos;
- Possibilita utilizar simulação, reduzindo custos;
- Permite avaliar benefícios oriundos de propostas de melhorias, novas estratégias de mitigação e mesmo mudanças regulatórias em potencial; e
- Aprimora as bases técnicas necessárias aos operadores de instalações para reavaliar suas medidas de proteção física, mantendo a conformidade com as regulações vigentes.

Dois dos modelos mais conhecidos nos estudos sobre segurança física são o HARI (*Hypothetical Atomic Research Institute*)[23] e o LPNPP (*Lone Pine Nuclear Power Plant*)[33], ambos desenvolvidos pelo Departamento de Energia (DoE) do governo dos Estados Unidos e utilizados nos programas de treinamento da AIEA.

O HARI é uma instalação que contém um reator nuclear de pesquisa, localizado em uma cidade fictícia (Figura 2.6):

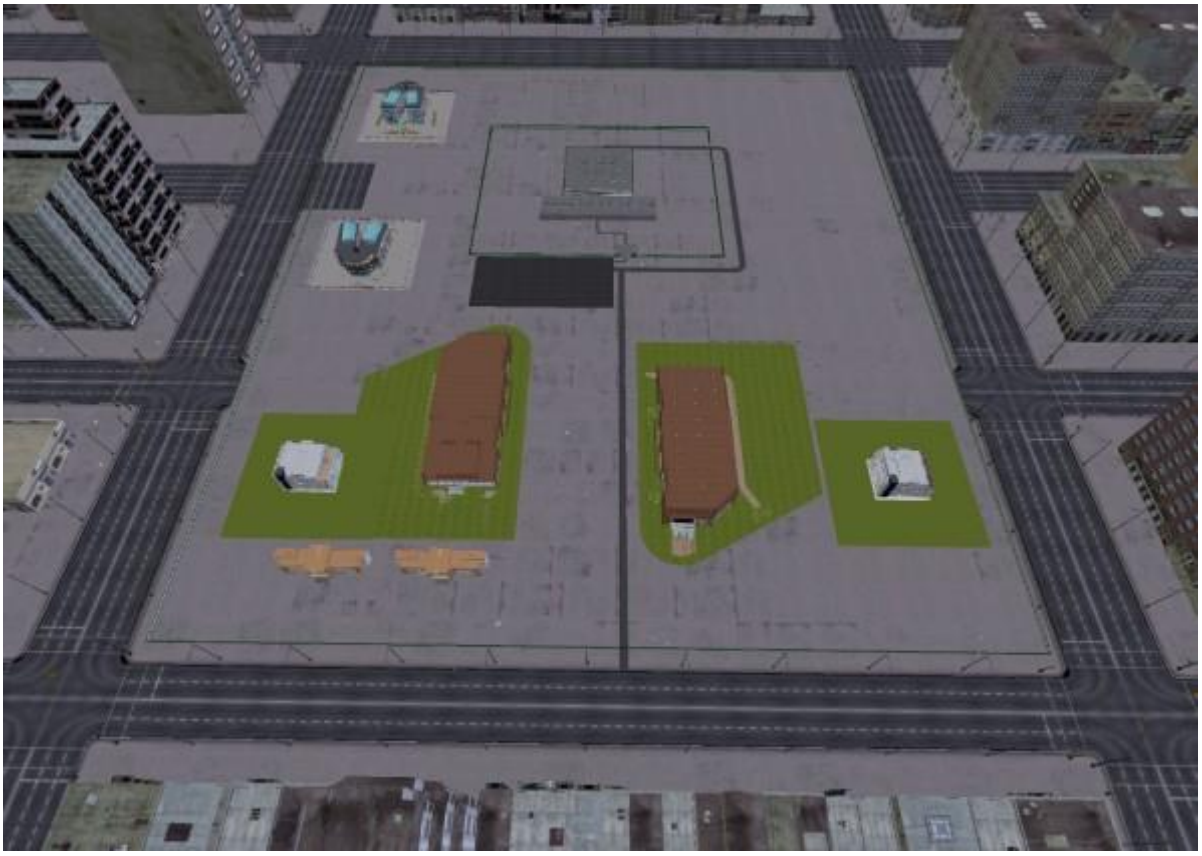


Figura 2.6. A instalação de pesquisa nuclear hipotética HARI. Fonte: [23]

O LPNPP é uma usina nuclear com um reator de potência destinado à produção de energia elétrica (Figuras 2.7 e 2.8):

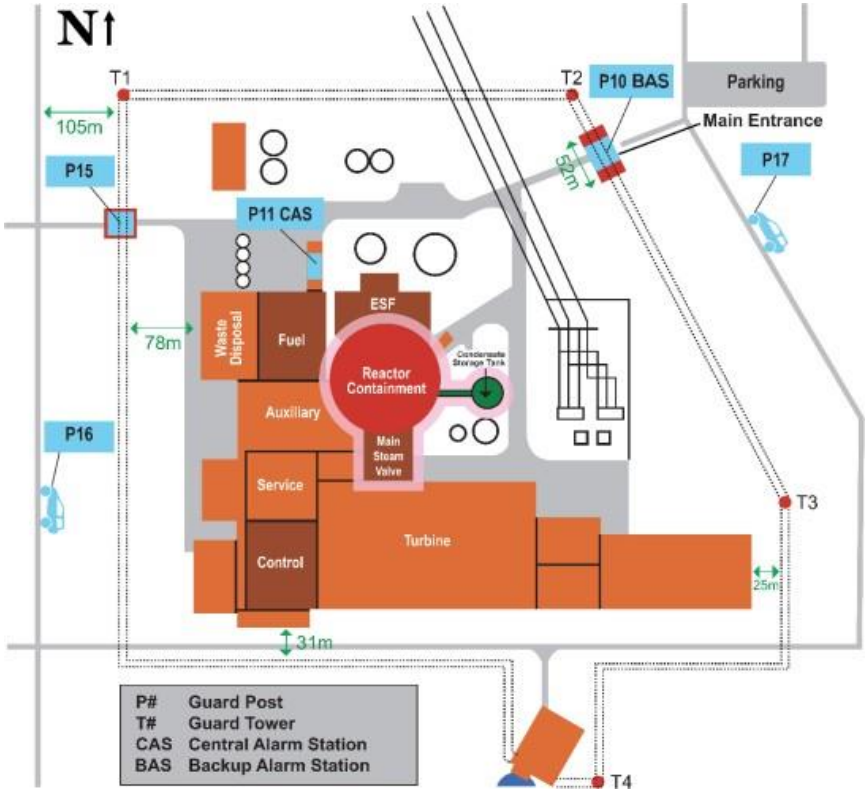


Figura 2.7. Modelo de usina nuclear Lone Pine Nuclear Power Plant. Fonte:[33].

Figura 2.8. A usina nuclear de Lone Pine - visão tridimensional. Fonte: [33].

Para a área de segurança cibernética, o modelo de instalação mais conhecido e consolidado é o Asherah Nuclear Power Simulator (ANS)[34], desenvolvido no âmbito de um projeto de pesquisa coordenado pela AIEA e conduzido pela Universidade de São Paulo (USP).

O ANS consiste de um modelo de reator PWR implantado em Matlab e utiliza elementos de hardware (“hardware-in-the-loop”) para simular uma sala de controle de um reator nuclear, suas redes de comunicação e elementos de controle (controlador lógico programável – PLC). O ANS vem sendo utilizado em treinamentos e exercícios nacionais de segurança cibernética [34].

A Figura 2.9 mostra a interface de controle do sistema:

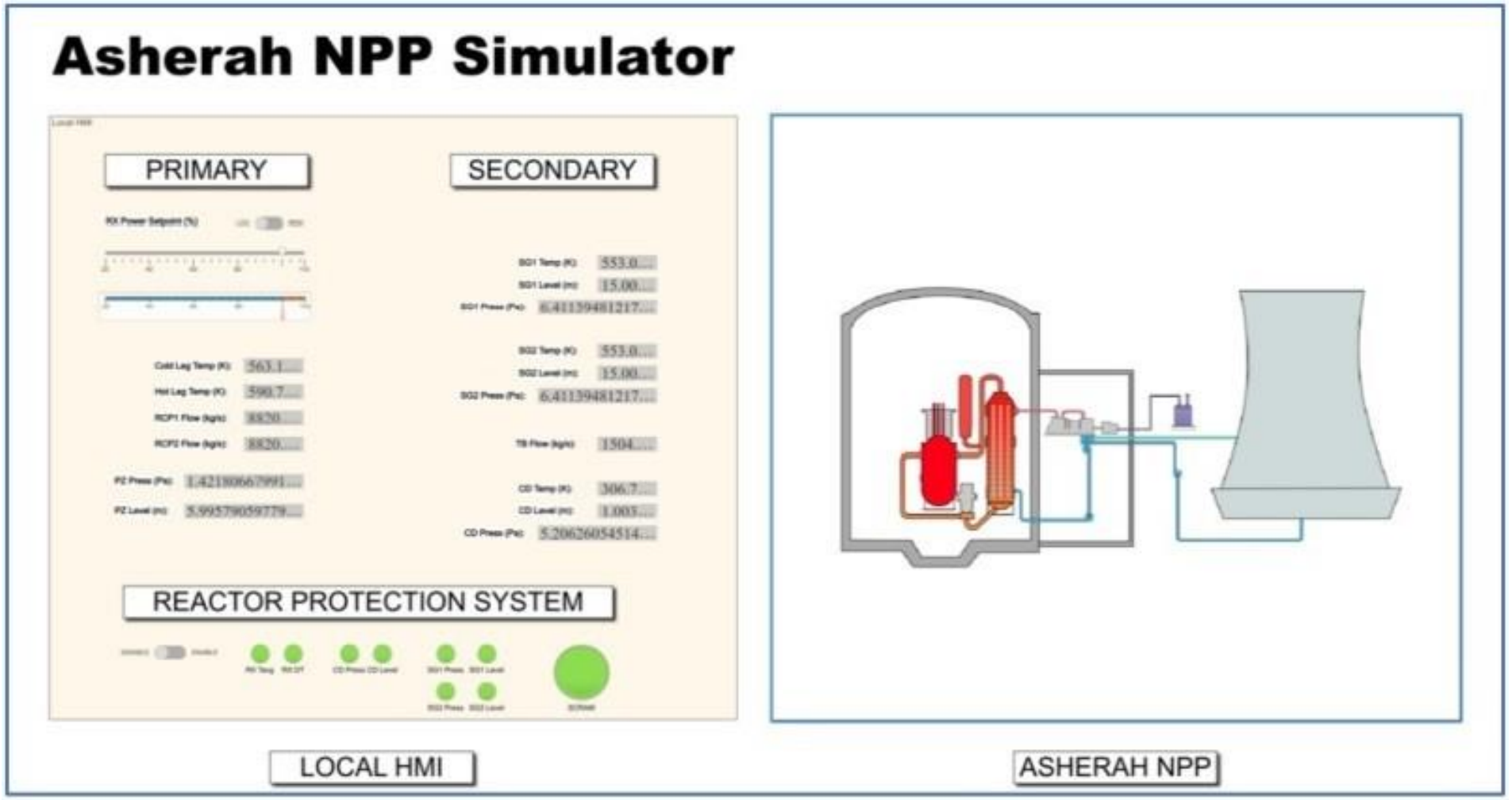


Figura 2.9. Interface local de operação do ANS. Fonte:[34].

Em relação aos modelos apresentados, este trabalho propõe, no Capítulo 3, um modelo que conjuga a possibilidade de se analisarem cenários tanto cibernéticos quanto físicos, uma vez que contempla os ativos digitais e físicos do sistema de proteção física da instalação nuclear simultaneamente.

2.5 Estimativas de Ameaças: Motivação, Intenção e Capacidades

O documento [14] da AIEA e o glossário nacional do setor nuclear brasileiro [5] trazem definições similares para "ameaça", como um indivíduo ou grupo de indivíduos com intenção, motivação e capacidade (recursos técnicos, tecnológicos, financeiros, materiais e humanos) para cometer um ato maléfico envolvendo materiais e instalações nucleares, fontes radioativas ou instalações radiativas. É importante notar que, de acordo com essa definição, as ameaças são pessoas, e não as ações que as mesmas realizam, o que pode diferir do entendimento corriqueiro para a palavra (por exemplo, "ameaça" de incêndio ou "ameaça" de chuva).

A metodologia para definição de ameaças consiste em três passos básicos [32]:

- Listar as informações necessárias para definir a ameaça;
- Coletar informações sobre ameaças potenciais;
- Organizar as informações para que sejam utilizáveis.

No primeiro passo, é importante decidir que tipo de informação é relevante para que se obtenha uma boa estimativa das ameaças a uma instalação. Uma lista mínima de informações necessárias para se caracterizar qualitativamente uma ameaça, ou um conjunto de ameaças, deve incluir motivação, potenciais metas baseadas na identificação de alvos e capacidades.

No segundo passo, devem-se coletar informações sobre as ameaças potenciais, que devem levar em consideração a comunidade no qual a instalação se insere, fatores como a reputação da instalação, condições de trabalho, relações públicas, consciência sobre segurança dos trabalhadores e do público local, bem como a relação entre empregados e empresa operadora. Tais informações podem ser obtidas de agências de inteligência, órgãos de segurança pública ou de fontes abertas.

No terceiro passo, as informações coletadas devem ser colocadas em formato que torne possível a utilização, e devem incluir uma avaliação qualitativa referente às probabilidades de ações, motivações e capacidades (exemplo: muito alta, alta, média, baixa, muito baixa).

No caso de a instalação ter consequências radiológicas muito altas, por exemplo, reatores de potência ou materiais enquadrados na Categoria 1 (Anexo A), uma abordagem qualitativa é preferível, por proporcionar maior detalhamento e possibilitar uma avaliação das ações de segurança por desempenho. Essa avaliação é denominada "Ameaça-Base de Projeto (ABP)". O Nuclear Security Series nº10 [24] provê recomendações para a elaboração, uso e manutenção de uma ABP.

Uma ABP [24] é uma descrição qualitativa e quantitativa de um adversário ao qual o detentor de uma licença de operação de uma instalação nuclear deve proporcionar meios técnicos, operacionais e humanos de se contrapor. Essa descrição, portanto, serve de insumo para o projeto, dimensionamento e avaliação dos sistemas de segurança, pelos critérios de desempenho, sendo a abordagem utilizada neste trabalho.

2.6 Trabalhos Correlatos

As pesquisas sobre potenciais efeitos de ataques cibernéticos em sistemas ciberfísicos normalmente são realizadas ou por uma perspectiva de tecnologia da informação e comunicações (TIC), ou por perspectivas puramente físicas e de engenharia de controle [36]. No domínio da TIC, em [37] foram analisados potenciais ataques cibernéticos em sistemas de controle de subestações elétricas. O enfoque da pesquisa era nas potenciais ameaças dos ataques na infraestrutura de comunicações de rede, não considerando, no entanto, consequências físicas oriundas de tais ataques. Em [38] foi apresentado um primeiro passo no sentido de uma modelagem gráfica do impacto físico de ataques cibernéticos em redes inteligentes (smart grids), mostrando, no ambiente de simulação "Matlab", um ataque cibernético bem-sucedido pode causar um apagão local na rede.

Especificamente na área nuclear, há vários estudos recentes com o objetivo de contribuir para a segurança cibernética e física. A maioria deles trata física e cibernética como diferentes domínios de segurança ou se concentra isoladamente em diferentes sistemas da instalação nuclear. Por exemplo, [39] discute a inter-relação entre ataques cibernéticos e físicos, mas tem um foco maior em sistemas de controle e instrumentação, enquanto [40] trata de ameaças internas em ativos físicos usando a mesma metodologia do presente trabalho, que é usada na análise puramente física de sistemas de segurança (Estimate of Adversary Sequence Interruption
- EASI), mas não considera ataques via ativos cibernéticos.

A segurança cibernética é considerada de forma isolada em estudos como os de [21], que tratou de forma genérica de possíveis problemas de segurança cibernética em reatores nucleares de potência, em [20], que desenvolveram uma proposta de medidas de segurança cibernética para sistemas de segurança tecnológica de instalações nucleares. O estudo de [41] tratou da avaliação de risco de ataques em redes sem fio de instalações nucleares, em [42] foi estudada uma forma de identificação de ativos digitais de interesse em reatores nucleares de potência, [43] tratou do desenvolvimento de uma plataforma para a segurança cibernética de sistemas de controle em centrais nucleares e [44] fez uma descrição cronológica dos malwares voltados para a infraestrutura nuclear.

Em relação aos cenários de ataques físicos, vários trabalhos tratam exclusivamente do assunto, como [45], que fez uma revisão sobre metodologias de análise de risco em instalações nucleares, envolvendo ativos físicos, [46], que tratou da ameaça de veículos aéreos não tripulados à instalações nucleares, [47], que tratou de técnicas de rotas de ataques físicos e [48] estudou a identificação de áreas vitais para a proteção física de reatores nucleares de potência. Ademais, [33] descreve um modelo hipotético de instalação nuclear, modelo este utilizado e adaptado para fins de treinamento e pesquisa pela Agência Internacional de Energia Atômica (AIEA) na área de proteção física.

Finalmente, estudos sobre sistemas ciberfísicos, considerados de forma integrada, foram realizados por [22], já mencionado anteriormente, e [49], que tratou da avaliação de risco em sistemas ciberfísicos considerando aspectos de segurança tecnológica e física, de uma forma geral, não tratando especificamente da área nuclear.

A Figura 2.10 representa graficamente onde se localiza o presente trabalho nos domínios da segurança nuclear (nuclear safety), segurança cibernética (cyber security) e segurança física (nuclear security):

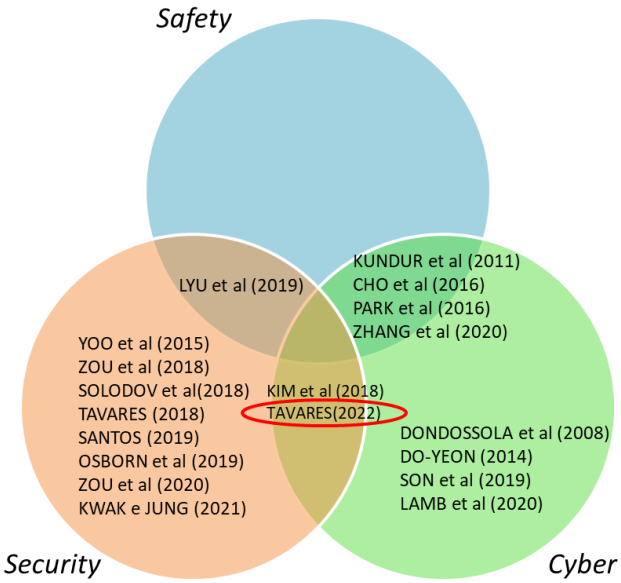


Figura 2.10. Inserção do presente trabalho nos domínios da área de segurança nuclear.

A tabela 2.2 ilustra os diferentes domínios da segurança abordados em cada um dos trabalhos pesquisados, em comparação com presente trabalho:

Tabela 2.2.Comparação entre os domínios de segurança abordados nos trabalhos correlatos.

Trabalho Correlato	**Segurança Física**	**Segurança Cibernética TIC**	**Segurança Cibernética OT**	**Segurança Técnica**
Presente trabalho	✓	✓	✓	
Park *et al* [20]		✓		✓
Do-Yeon [21]		✓	✓	
Santos [22]	✓			
Osborn *et al* [33]	✓			
Friedberg *et al* [36]	✓	✓		✓
Dondossola *et al* [37]			✓	
Kundur *et al* [38]		✓		✓
Cho *et al* [39]			✓	✓
Zou *et al* [40]	✓			
Kim *et al* [41]		✓		
Son *et al* [42]			✓	
Zhang *et al* [43]			✓	
Lamb *et al* [44]		✓	✓	
Yoo *et al* [45]	✓			
Solodov *et al* [46]	✓			
Zou *et al* [47]	✓			
Kwak *et al* [48]	✓			
Lyu *et al* [49]			✓	✓

2.7 Síntese do capítulo

Este capítulo teve o propósito de esclarecer ao leitor acerca dos principais conceitos necessários à continuidade do trabalhos, descrever modelos de instalações já utilizados em trabalhos correlatos, de que forma o presente estudo se insere no contexto da área e no que pretende trazer de contribuição.

3 MODELO E FRAMEWORK PROPOSTO

Este capítulo tem o propósito de apresentar o modelo e o framework propostos no trabalho: a Seção 3.1 descreve o desenvolvimento de um modelo de instalação nuclear (Instituto de Ciências Nucleares do Cerrado), da ameaça-base de projeto para a instalação e os cenários de ataque ciber-físicos, e a Seção 3.2 descreve os métodos e ferramentas de avaliação de vulnerabilidades utilizados para calcular a efetividade do sistema de segurança: o framework DEPO (Design and Evaluation Process Outline) e o método EASI (Estimate of Adversary Sequence Interruption).

3.1 Modelagem da Instalação Nuclear

Devido a restrições regulatórias para o compartilhamento de informações relativas aos sistemas de segurança de instalações reais [11], foi necessário criar um modelo de instalação nuclear com nível de detalhamento suficiente para viabilizar a aplicação das ferramentas de avaliação de vulnerabilidades de forma a considerar os ataques ciberfísicos. O ponto de partida para a elaboração do modelo de instalação foi o objeto de estudo descrito em [1], porém aquele modelo havia sido concebido considerando-se os requisitos regulatórios vigentes à época, de forma que, na concepção da instalação para o presente trabalho, foi necessário compreender os requisitos constantes da norma brasileira de proteção física atualmente vigente [11], que é posterior ao trabalho de [1]. Dessa forma, na análise do primeiro cenário de ataque, que se dá de forma puramente física, é possível inferir se a instalação modelada tem seu sistema de segurança eficaz em face da ameaça e atende aos requisitos normativos em vigor.

3.1.1 Descrição das ativos a serem protegidos e áreas de segurança

O nome escolhido para a instalação foi “Instituto de Ciências Nucleares do Cerrado – ICNC”, e consiste em um terreno de 4km^2, localizado no interior do campus da Universidade do Cerrado (UC), onde operam as seguintes instalações nucleares e radiativas:

- Reator nuclear de pesquisa (ICNC-R1): do tipo piscina aberta, de 20MW de potência térmica, contendo combustível de urânio enriquecido a 19,99% em massa do isótopo ^{235}U (em uma massa total de cerca de 30 kg de urânio), portanto considerado de baixo enriquecimento (Categoria II, conforme Anexo A). Igual quantidade de combustível fresco (não-irradiado) encontra-se armazenado para uso futuro na área controlada do reator. Pelas características desse tipo de instalação, o material nuclear nele armazenado pode ser alvo tanto de roubo (combustível fresco armazenado) quanto de sabotagem (elementos de combustíveis em operação). O reator é utilizado em pesquisa básica e na fabricação de radioisótopos para uso em medicina;

- Laboratório de fabricação de combustíveis nucleares (LFCN): Consiste em uma unidade de pesquisa, desenvolvimento e fabricação de elementos de combustíveis do tipo placa, opera sob demanda com materiais nucleares, nas mesmas proporções, massa e enriquecimento dos utilizados no reator de pesquisas, além de utilizar pequenas fontes de ^{137}Cs usadas na calibração de equipamentos de instrumentação nuclear. A fabricação dos elementos de combustíveis é realizada usando-se de elevado nível de automação do processo. Os materiais nucleares presentes no laboratório podem ser alvos de roubo ou sabotagem, a exemplo daqueles presentes no reator;

- Irradiador gama (ICNC-IG1): Consiste em uma unidade de grande porte, contendo um arranjo de fontes de ^{60}Co, de elevada atividade, cerca de 100.000Ci (categoria 1, de alto risco radiológico, conforme o guia de categorização de fontes da AIEA [50]). O irradiador é usado para esterilização de produtos médicos e farmacêuticos, tratamento de alimentos, modificação ou indução de cores em pedras preciosas, conservação de obras de arte, esterilização de sangue e hemocomponentes, dentre outras aplicações. A operação do irradiador é realizada por meio da sala de controle, com elevado grau de automação, inclusive nos sistemas de intertravamento de segurança radiológica. Dada a dificuldade de se remover fisicamente as fontes, pelo peso e dimensões, considera-se que o modo de ataque físico mais plausível é a sabotagem envolvendo as fontes de Cobalto;

- Depósito de rejeitos radioativos (DRR): Consiste em um local de tratamento e armazenamento seguro para os combustíveis irradiados e os rejeitos radioativos da própria instalação (luvas, roupas e ferramentas contaminadas, fontes de calibração exauridas) e também oriundos de outros locais da região e do país, sendo alguns de baixa atividade (materiais radioativos de ocorrência natural– NORM na sigla em inglês, oriundos da indústria do petróleo) ou de alta atividade (cabeçotes em desuso de equipamentos usados em radioterapia, com fontes de 60Co e 137Cs).

A Figura 3.1 mostra a disposição espacial das instalações do ICNC:

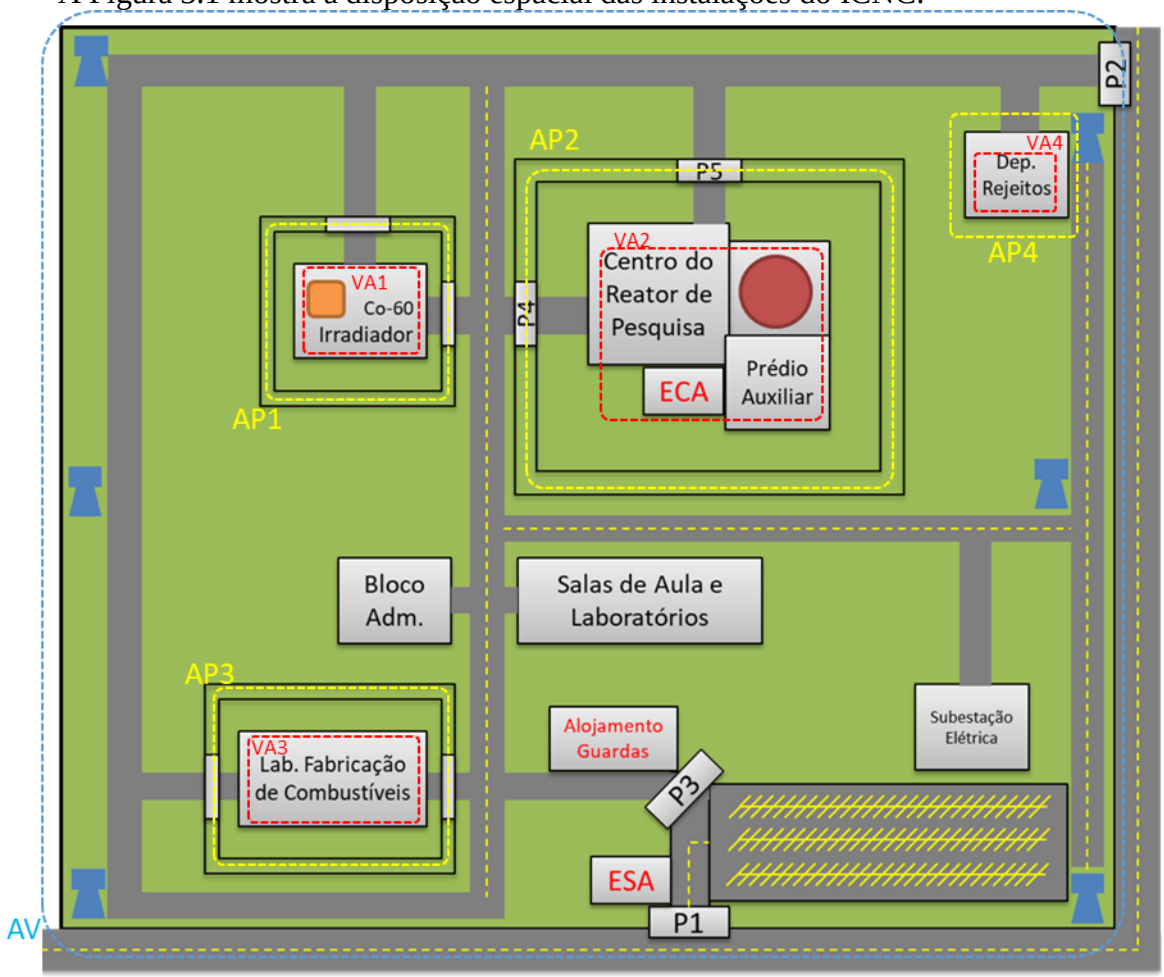


Figura 3.1. A instalação "Instituto de Ciências Nucleares do Cerrado - ICNC".

Na Figura 3.1 pode-se visualizar a delimitação das áreas de segurança da instalação, conforme requerido pela Norma [11]: em azul a área vigiada (AV); em amarelo, as áreas protegidas do

Irradiador Gama (AP1), do reator (AP2), do laboratório de combustíveis (AP3) e do depósito de rejeitos (AP4); e em vermelho as áreas vitais VA1, VA2, VA3 e VA4, seguindo a mesma numeração dos ativos das áreas protegidas, respectivamente.

A área vigiada é delimitada por uma barreira física do tipo cerca simples, sinalizada e dotada de uma zona de isolamento, livre de obstáculos, de forma a permitir a sua inspeção visual durante as ações de patrulhamento motorizado (rondas) realizado pelos vigilantes armados, em duplas. Há, ainda, seis torres de observação (em azul na Figura 3.1) que suplementam as ações de vigilância na AV. Os vigilantes dispõem de meios redundantes de comunicação, um rádio e um "botão de pânico" cujo acionamento enseja o início dos procedimentos de verificação, confirmação via observação eletrônica (dependendo do local do alarme) e resposta ao possível incidente.

A AV pode ser acessada a partir do exterior de duas formas: pela portaria principal P1 (acesso de pedestres e veículos) ou pelo portão de carga P2 (exclusivo para veículos de serviço e de carga). P1 é mantido aberto durante o expediente normal do instituto, sendo mantido trancado em outros horários. P2 é aberto apenas sob demanda, estando as chaves em poder da equipe de segurança e sendo aberto sob prévia notificação.

Os veículos que acessam o instituto pelo portão P1, após confirmação do acesso, devem ser estacionados em local próprio, no interior da AV, porém a área de estacionamento é separada fisicamente dos prédios do instituto por uma cerca simples similar à cerca externa da AV. Os pedestres, então, acessam os prédios do instituto através de outro portão, P3, no qual há o controle de acesso de pedestres por meio de crachás e catracas, e para os visitantes são emitidos crachás temporários, após identificação pela equipe de vigilância.

A área protegida do Reator (AP2), como se pode visualizar na Figura 3.2, é delimitada por uma cerca dupla, sinalizada, com sensores de intrusão do tipo infravermelho instalados entre as cercas e suplementação de vigilância por circuito fechado de televisão (CFTV), possuindo câmeras fixas e do tipo "pan-tilt-zoom" (PTZ), com iluminação noturna de intensidade e uniformidade compatíveis para uma visualização adequada. O acionamento de quaisquer dos alarmes é visualizado na Estação Central de Alarmes (ECA), que se localiza no interior da área protegida, tendo ainda uma redundância na Estação Secundária de Alarmes (ESA), localizada em anexo ao portão P1, próximo à entrada principal do instituto.

No caso de um evento que acione algum alarme, a informação é visualizada pelo operador do CFTV e, caso seja confirmada alguma ação hostil ou comportamento anormal, são notificados por rádio ou ramal telefônico os vigilantes armados (efetivo de dez respondedores por turno, mais os dois rondantes motorizados armados) para o efetivo atendimento ao incidente. O alojamento dos respondedores localiza-se anexo ao portão de pedestres P3. São realizados exercícios anuais para verificar a operacionalidade dos sistemas e a prontidão dos respondedores, medindo-se e registrando-se o tempo necessário para o aprestamento e desdobramento do efetivo até às áreas vitais a serem protegidas, para efeitos de conformidade com o órgão regulador nuclear nacional.

O controle de acesso à área AP2 é realizado por meio de controladores de acesso ligados à rede instalados no acesso à referida área. Para liberar o acesso, é necessário aproximar um crachá previamente cadastrado, ou, em caso de falha de leitura, os pesquisadores ou colaboradores possuem senhas individuais para liberar o acesso.

Figura 3.2. Área protegida AP2 do reator de pesquisas ICNC-R1.

3.1.2 A área vital do Reator ICNC-R1

A área vital do reator (VA2) é delimitada pelo interior do prédio, como se pode visualizar na Figura 3.3. O controle de acesso à área de operação é realizado em uma sala específica para este fim, acessada diretamente pela entrada principal do prédio. Os usuários devem passar por um portal detector de metais, e os pertencem por um equipamento de raios-x. O acesso à área interna do prédio (sala de controle e da piscina do reator, estação central de alarmes e sala de armazenamento de combustível fresco) é realizado por barreiras do tipo “torniquete” e controladores de acesso biométrico (impressão digital) ou acesso por senha para o caso de falha na leitura da biometria. As portas, inclusive a porta de acesso de cargas, são monitoradas por CFTV e possuem sensores magnéticos de abertura e nos ambientes há sensores volumétricos de presença (infravermelhos), ativados manualmente fora do horário de expediente do instituto e que exibem as informações de alarme na ECA e na ESA.

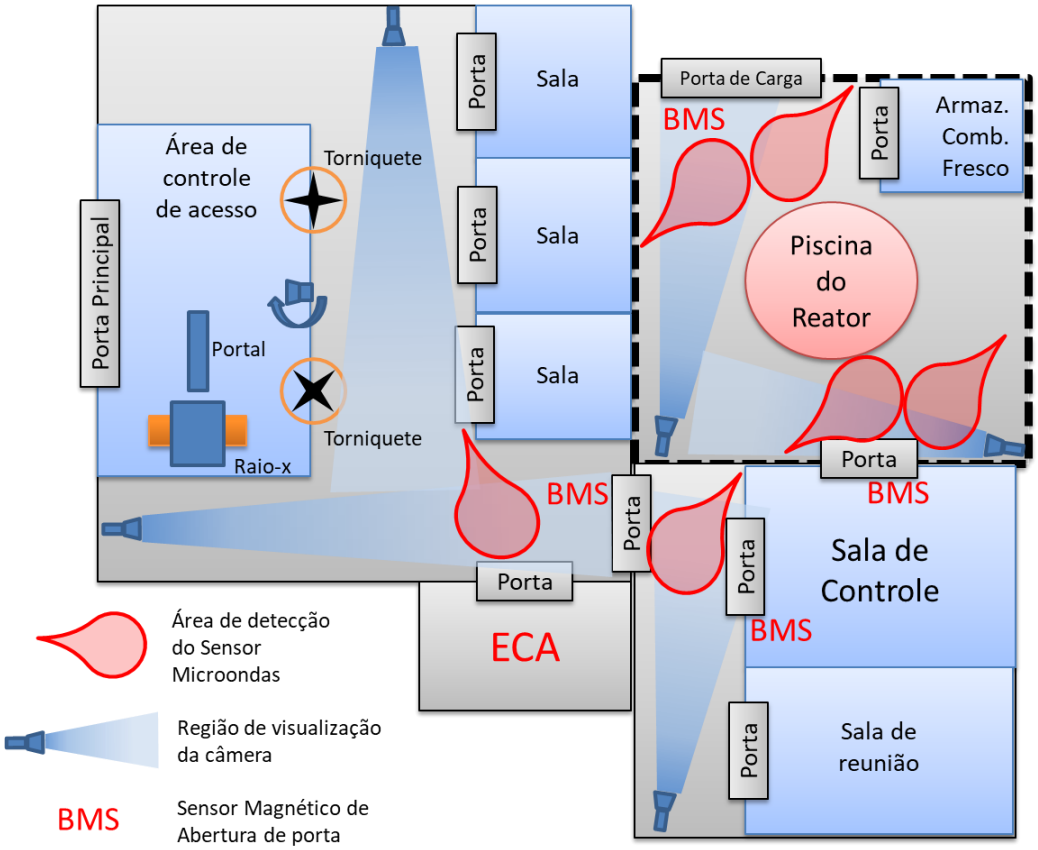


Figura 3.3. Área vital VA2 do reator de pesquisas ICNC-R1.

3.1.3 Equipe de resposta a incidentes de segurança

Em relação à capacidade de resposta a incidentes, a equipe de segurança e vigilância é composta de dez respondedores armados por turno, que se localizam em um alojamento contíguo ao portão P3 (próximo ao estacionamento), dois rondantes armados e motorizados, dois operadores de CFTV e alarmes na ECA e dois na ESA, totalizando dezesseis pessoas, e deste efetivo, doze armados para o engajamento a alguma ameaça que venha a se concretizar. Por restrições legais, os armamentos e equipamentos à disposição da força de vigilância consistem em arma curta, tonfa, lanterna, colete à prova de bala, rádio comunicador e "botão de pânico".

Os rondantes dispõem de motocicletas para a atividade de patrulhamento, e a resposta dedicada dispõe de viatura de prontidão (veículo de passeio com cinco lugares), com rádio instalado para comunicação com a ECA. Caso a capacidade de uma possível ameaça exceda aquela da força local, e haja necessidade de escalar as ações para a esfera externa, a ECA possui ramal externo para contatar as forças policiais locais, que se localizam a cerca de vinte minutos do instituto em condições normais de trânsito.

3.1.4 Parâmetros de desempenho da equipe de resposta

Atendendo aos requisitos regulatórios de [11], a instalação realiza ensaios e exercícios anuais com o intuito de verificar a operacionalidade dos equipamentos, a proficiência dos operadores e determinar os tempos médios para cada uma das etapas da ação de resposta, reproduzidos na Tabela 3.1:

Tabela 3.1: Parâmetros de desempenho estimados da força de resposta. Adaptado de [1].

Etapa da ação de resposta	**Tempo para a AP do Reator**
Tempo de ativação do alarme	<1s
Tempo de avaliação do alarme	5s
Comunicação à equipe de resposta	20s
Tempo de preparação da equipe de resposta	45s
Tempo de deslocamento à área protegida sob ataque	60s
Tempo para avaliação, posicionamento das forças e início do engajamento	20s
Total para um efetivo de 10 homens	**150s**

Os outros parâmetros de desempenho, T_D e P_D (tempo de retardo e probabilidade de detecção, respectivamente), encontram-se no Anexo C e serão utilizados nos cálculos da análise multicaminhos + EASI para os cenários estudados.

3.1.5 Redes de comunicação do sistema de proteção física da ICNC

No tocante às redes de comunicação, a rede do ICNC encontra-se implantada de forma a abranger as seguintes funções:

- Sistema de Segurança (Proteção Física): compreende os controladores de acesso, sistemas de controle e visualização de alarmes e de circuito fechado de televisão (CFTV);
- Rede corporativa: acesso a internet, e-mail corporativo, ferramentas para ensino e pesquisa;
- Resposta a emergências nucleares e radiológicas: sistemas de apoio à decisão para avaliar intensidades e deslocamento de plumas radioativas na atmosfera em cenários de acidentes nucleares;
- Contabilidade e Controle de Material Nuclear: sistemas online que registram e possibilitam o monitoramento de movimentações de materiais nucleares, em atendimento a tratados internacionais;
- Instrumentação e controle de processos: sistemas de controle de variáveis afetas à operação da planta, como reatividade do reator, temperatura, pressão, vazão, atividade radioativa, bem como a interface homem-máquina para exibição do estado da planta.

A figura 3.4 permite a visualização de um diagrama da rede do Sistema de Proteção Física:

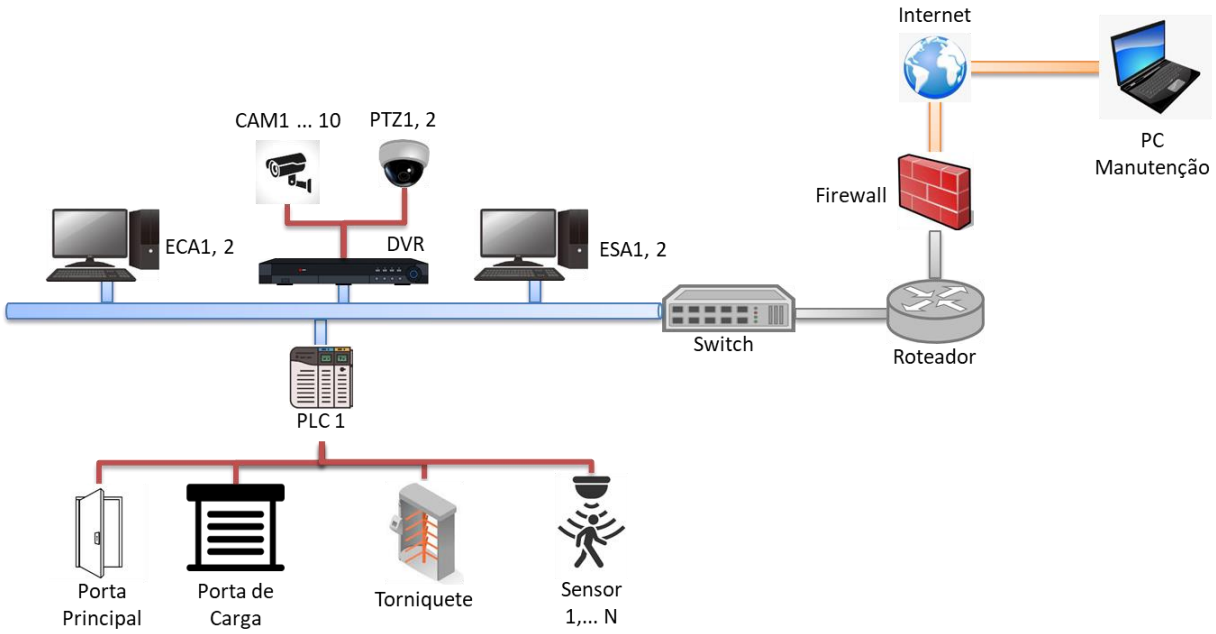


Figura 3.4. Diagrama de rede do sistema de segurança da ICNC.

3.2 Modelos de Ameaças

Sobre o modelo de ameaça desenvolvido para o presente trabalho, analogamente à fase de concepção do modelo de instalação nuclear, as restrições de acesso a dados levaram à opção por postular uma ameaça, tendo como base os trabalhos de [1], [22] e a metodologia recomendada pela Agência Internacional de Energia Atômica [24], de forma coerente e crível considerando-se a realidade brasileira.

No aspecto qualitativo, foram definidas as seguintes ameaças para o ICNC:

- Ameaça 1: Organização ambientalista “Filhos de Gaia”

  Trata-se de uma organização que, dentre outras atividades, possui interesse em desmoralizar a área nuclear como um todo, por considerá-la uma indústria “suja” em termos ambientais e com finalidade bélica e de dominação de potências internacionais. Seu *modus operandi* inclui manifestações em instalações nucleares, bloqueio de vias durante operações de transporte de elementos de combustíveis, e recentemente utilizaram veículos aéreos não- tripulados (*drones*) para sobrevoar instalações nucleares, inclusive chocando-os contra o prédio da contenção de um reator nuclear de potência, com o intuito de mobilizar a opinião pública para a causa antinuclear. Realizam, ainda, a disseminação de informações falsas e mobilização e cooptação de apoiadores usando-se das redes sociais (“hacktivismo”). De uma forma geral, não possuem amplos conhecimentos em técnicas, táticas ou procedimentos para burlar sistemas de segurança, mas podem utilizar-se de informações obtidas por conluio com adversários internos (*insiders*). No cenário local, a organização possui alta probabilidade de

ação, no entanto considera-se baixa a severidade de uma ação em termos de consequências radiológicas.

- Ameaça 2: Organização criminosa “Comando do Cerrado” (CdC)

  A região no entorno da Universidade do Cerrado, onde se localiza o ICNC, experimentou um crescimento acelerado das atividades criminais relacionadas ao tráfico de entorpecentes, roubos de cargas e ações envolvendo caixas eletrônicos em agências bancárias. A ORCRIM “Comando do Cerrado” vem conquistando o domínio territorial dos pontos de venda de drogas na região, tendo em vista o elevado poderio econômico, a grande disponibilidade de armamentos de uso restrito, como fuzis de assalto, o uso de explosivos e a realização de ações pontuais de assassinato de lideranças de ORCRIM rivais. Apesar da grande capacidade em termos de armamentos, táticas e procedimentos, não se considera que a CdC tenha intenção de perpetrar atos maléficos envolvendo materiais nucleares ou fontes radioativas, a menos que, considerando a motivação econômica dessa organização, que suas capacidades sejam utilizadas por outros atores de forma indireta visando lucro com o contrabando de materiais nucleares para outros atores do cenário internacional.
- Ameaça 3: Grupo “Fr33_Hack3rs”

  Recentemente foram detectados indícios de ataques do grupo hacker “Fr33_Hack3rs” cujos alvos foram infraestruturas críticas do país, como abastecimento de água, geração/distribuição de energia elétrica e sistema financeiro. Este grupo tem características comuns a ameaças do tipo Persistente Avançada (APT), como capacidade de desenvolver malwares de forma dedicada, monitorar redes e coletar informações de forma a dificultar a detecção, usar e explorar vulnerabilidades de dia zero (*0-day exploits*). Trata-se de uma ameaça não específica para o programa nuclear, mas ataques direcionados à área nuclear têm o potencial de roubar informações sensíveis do ponto de vista de segredo industrial, bem como facilitar e viabilizar ataques físicos à infraestrutura crítica nuclear, o que tem o potencial de causar prejuízos do ponto de vista de reputação ou mesmo interromper as ações do programa nuclear nacional. Tendo-se em vista o histórico das ações do grupo, considera- se alta a probabilidade de ataque do grupo no país.
- Ameaça 4: Organização terrorista “Movimento de Libertação do Cerrado”

  O Movimento de Libertação do Cerrado (MLC) é um grupo que tem como objetivo a separação da região do Cerrado do restante do país e a formação de um Estado teocrático, de caráter radical e belicoso. Atualmente possui duas células em cidades diferentes, uma próxima à capital e outra nas proximidades das fronteiras. Essas células obtêm receitas por meio do contrabando de armas e produtos de luxo, criação de negócios de fachada, lavagem

de dinheiro e financiamento por grupos terroristas estrangeiros de mesma vertente religiosa. O aumento da repressão a essas atividades ilícitas causou recente recrudescimento nas ações do MLC, que se voltou para outras ações criminosas, aliando-se à ORCRIM "Comando do Cerrado" em assaltos a banco e caixas eletrônicos. Foram, ainda, interceptadas comunicações com grupos terroristas estrangeiros sobre a confecção de dispositivos de exposição radiológica (DER) e de dispersão radiológica (DDR) usando-se fontes radioativas, bem como sabotagens em instalações nucleares com vistas à contaminação radiológica de algumas áreas, que teriam a possibilidade de causar caos social. O MLC é bastante ativo na internet e redes sociais, disseminando a ideologia do grupo e recrutando integrantes para atuarem como "lobos-solitários" em ações pontuais contra instalações governamentais e eventos públicos com grande aglomeração de pessoas. O grupo possui conhecida capacidade cibernética, tendo reivindicado a autoria de ataques de ransomware contra redes de televisão, órgãos governamentais e grandes corporações da área da saúde. Assim, considera- se que o grupo possui elevada probabilidade de ação, e alta severidade das consequências de um ataque bem-sucedido.

Tendo-se a estimativa de ameaças acima elencada, foram tabuladas as capacidades dos diferentes tipos de ameaça, conforme a metodologia da AIEA [24], chegando-se aos dados da Tabela 3.2 para a Ameaça-Base de Projeto (ABP):

Tabela 3.2: Ameaça-Base de Projeto para o ICNC. Adaptado de [1].

Características da Ameaça	**Ameaça Terrorista**	**Ameaça Criminosos**	**Ameaça Protestos**	**Ameaça-Base de Projeto (ABP)**
Número de adversários	5	10-15	<100	**5**
Armamentos	Arma longa automática + pistola	Arma longa automática + pistola	Não	**Arma longa automática + pistola**
Explosivos	Dinamite, TNT, plástico	Dinamite, explosivos caseiros	Não	**Dinamite**
Ferramentas	Mecânicas e Elétricas	Mecânicas e Elétricas	Mecânicas	**Mecânicas e Elétricas**
Transporte	Veículo comum, veículo-bomba, meios marítimos	Veículo comum	Veículo comum	**Veículo comum**
Conhecimento da instalação	Médio	Médio	Médio	**Médio**
Habilidades Técnicas	Alto (Técnicas, Táticas e Procedimentos paramilitares), conhecimentos cibernéticos	Médio	Médio (uso de vetores não convencionais como drones)	**Alto (Técnicas, Táticas e Procedimentos paramilitares, conhecimentos cibernéticos, drones)**
Financiamento	Alto	Alto	Médio	**Alto**

Conluio com *insiders*	Sim	Sim	Não	**Sim**
Estrutura de apoio	Alto	Alto	Médio	**Alto**
Dispostos a matar/morrer	Sim/Sim	Sim/Não	Não/Não	**Sim/Sim**

3.3 Aplicação do framework DEPO no modelo da instalação nuclear

O método EASI [51] vem sendo utilizado há décadas na avaliação de sistemas de proteção física de instalações nucleares, tendo sido desenvolvido originalmente para a proteção de arsenais nucleares e instalações que armazenam materiais nucleares "especiais", como plutônio ou urânio de alto enriquecimento. O método é baseado nas seguintes considerações sobre risco em segurança física.

3.3.1 Abordagem de gerenciamento de risco aplicada à segurança física nuclear

A definição clássica de risco é:

$$R = P * C \qquad \text{(Eq. 3.1)}$$

Onde:
R:= Risco;

P:= Probabilidade de ocorrência de um evento indesejado; e
C:= Consequência do evento indesejado.

Por sua vez, o valor de P depende de dois fatores: a probabilidade de ocorrer um ato maléfico por um adversário (o adversário decidiu tomar a ação de atacar), e a probabilidade de, dado que se tentou um ataque, que ele teve sucesso. Assim, a probabilidade de um ataque bem- sucedido pode ser escrita como:

$$P = P_A * P_S \qquad \text{(Eq. 3.2)}$$

Onde:
P:= Probabilidade de o ataque ter sido bem-sucedido;
P_A:= Probabilidade de ocorrer o ataque; e
P_S:= Probabilidade Condicional que o ataque foi bem-sucedido, ocorrida a tentativa.

Como em um sistema de segurança o objetivo é reduzir a probabilidade de que o adversário complete sua missão com sucesso, no caso da ocorrência de um ataque, ou o sistema é efetivo e o adversário é interrompido ou neutralizado, ou o sistema é derrotado, no caso de um ataque bem sucedido, ou seja, os eventos são excludentes. Em termos de probabilidades:

$$P_E + P_S = 1 \qquad \text{(Eq. 3.3)}$$

Onde:
P_E:= Probabilidade do sucesso do sistema de segurança face ao ataque (Efetividade); e
P_S:= Probabilidade que o ataque tenha sucesso.

Reescrevendo a Equação 3.3 explicitando em termos de P_S:

$$P_S = 1 - P_E \quad \text{(Eq. 3.4)}$$

Finalmente, substituindo o valor de P_S na Equação 3.1, temos, na equação do risco:

$$R = P_A * (1 - P_E) * C \quad \text{(Eq. 3.5)}$$

Da Equação 3.5 depreende-se que:

- O risco depende de forma diretamente proporcional à probabilidade P_A de um ataque (relacionada com a atratividade do material ou instalação), à vulnerabilidade ($1-P_E$) do sistema de proteção física e das consequências (C) oriundas das ações maléficas sobre o material (relacionada diretamente à natureza, quantidade, enriquecimento).
- Por outro lado, um incremento na efetividade do sistema de segurança (maior valor de P_E) reduz o risco.

No entanto, a utilização da Equação 3.5 esbarra na limitação de quantificar o risco R, pois as condições básicas para o cálculo probabilístico puro não são atendidas, isto é, as variáveis não são aleatórias nem independentes, especialmente por conta do parâmetro P_A, que depende do comportamento humano, não podendo ser modelado matematicamente por uma variável aleatória.

Assim, uma simplificação conservadora e que é normalmente adotada nos estudos envolvendo projetos de sistemas de segurança é desconsiderar o efeito da dissuasão, ou seja, assumir que o adversário irá atacar a instalação com 100% de probabilidade (P_A=1). Essa premissa possibilita focar o gerenciamento de risco em duas variáveis: na efetividade do sistema de segurança (P_E) e nas consequências de um ataque bem sucedido (C). Neste trabalho, é considerada apenas a efetividade.

A efetividade do sistema de segurança depende, ainda, de dois fatores probabilísticos:

$$P_E = P_I * P_N \quad \text{(Eq. 3.6)}$$

Onde:

P_I:= Probabilidade de Interrupção; e

P_N:= Probabilidade de Neutralização.

A probabilidade de interrupção P_I é definida como a probabilidade de se efetuar uma abordagem dos adversários pela força de segurança, o que dependerá do desempenho de detecção, alarme, confirmação de intrusão e vigilância. É normalmente considerada como um fator fortemente dependente das tecnologias empregadas no sistema de segurança (detectores, sensores, câmeras, dentre outros aspectos).

A probabilidade de neutralização P_N é definida como, uma vez já tendo ocorrido a abordagem, a probabilidade que o engajamento (combate) propriamente dito entre a equipe de segurança e a força adversária resulte na captura, prisão, fuga ou morte dos adversários. Essa probabilidade é normalmente considerada como fortemente dependente das características do componente humano da segurança (treinamento, armamento, táticas e procedimentos de engajamento), assim como de outras variáveis externas (temperatura, chuva, neve, luz solar, conhecimento do terreno), que podem impactar o desempenho no combate.

No escopo do presente trabalho os valores de P_N são extraídos da literatura [32], tabelados,

considerando iguais condições de armamento, equipamento, táticas e conhecimento para os lados antagônicos. Os dados de neutralização estão elencados no Anexo D.

Para determinar a P_I, é necessário determinar o Ponto Crítico de Detecção (PCD), ou seja, a última oportunidade eficaz de detecção do adversário, a partir do qual, seguindo o caminho, ele completará a missão independente de ser detectado ou não. O PCD é definido em [32] como o ponto no qual há um retardo ao longo do caminho do adversário imediatamente maior ou igual ao tempo da força de resposta, permitindo a ela atuar em tempo hábil na interrupção e neutralização. Na Figura 3.5 é possível visualizar um diagrama temporal que ilustra a determinação do PCD:

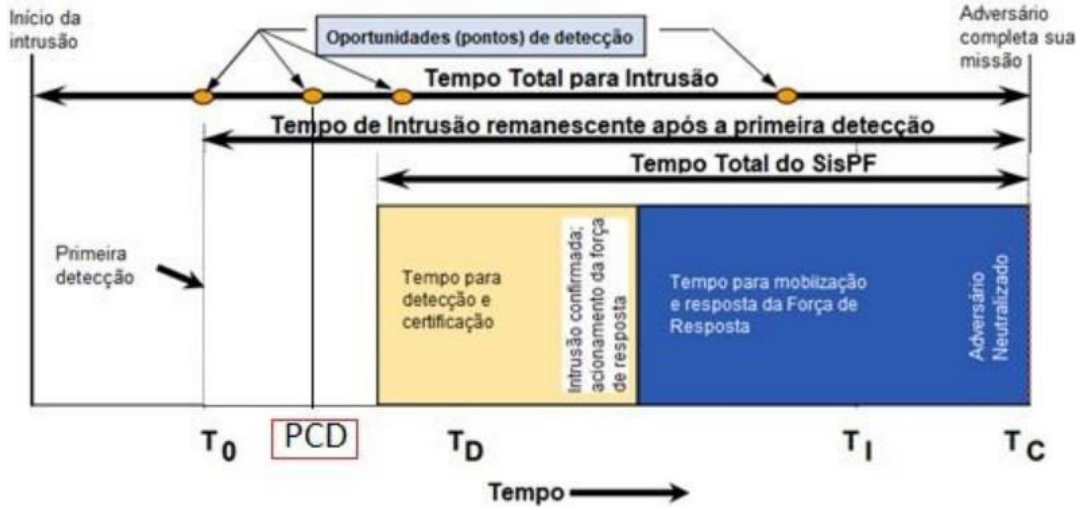


Figura 3.5. O Ponto Crítico de Detecção. Adaptado de [1].

Da Figura 3.5 pode-se depreender que o sistema de segurança (SisPF) da instalação necessita de um tempo total que inclui as etapas de detecção e confirmação de intrusão (T_D), mobilização e deslocamento de forma a neutralizar o adversário (T_I). Esse tempo total deve ser contabilizado, a partir do alvo e comparado com as oportunidades de detecção (rondas, níveis de sensores, posicionamento fixo de postos de vigilância, sendo a primeira oportunidade em T_0 no gráfico). Apenas as oportunidades de detecção anteriores ao ponto do tempo total do SisPF (no gráfico, à esquerda do início do mesmo) representam oportunidades tempestivas de detecção. E a última oportunidade tempestiva de detecção representa o PCD, após do qual as ações de detecção não conseguirão interromper tampouco neutralizar a ação adversa, que tem um tempo total de T_C para o adversário concluir a ação. Na Figura 3.1, é possível visualizar o PCD na segunda oportunidade de detecção (segunda camada de sensores). Se a identificação e certificação se desse na terceira oportunidade, a força de resposta já não poderia atuar em tempo hábil.

Assim, determinado o PCD, a probabilidade de interrupção dependerá do fato do sucesso na detecção, nas oportunidades anteriores ao PCD, incluindo o mesmo. Assim:

$$P_I = 1 - [P_{S1} * P_{S2} * .... * P_{SN}] \quad \text{(Eq. 3.7)}$$

Onde:

P_I:= Probabilidade de interrupção; e

P_{SN}:= Probabilidade de o adversário não ser detectado na n-ésima oportunidade de detecção anterior ao PCD.

Expressando a Equação 3.7 em termos da probabilidade de detecção de cada nível, temos:

$$P_I = 1 - [(1 - P_{D1}) * (1 - P_{D2}) *....* (1 - P_{DN})] \quad \text{(Eq. 3.8)}$$

Onde:

P_I:= Probabilidade de interrupção; e

P_{DN}:= Probabilidade de detecção no n-ésimo nível anterior ao PCD.

Portanto, para se calcular o P_I para um determinado caminho, deve-se primeiramente determinar o tempo de resposta da força de segurança, em seguida, começando-se do alvo, somarem-se todos os tempos de retardo das barreiras físicas até que esta soma seja maior ou igual ao T_G (T_G é o tempo total do SisPF, ou seja, T_D+T_I na Figura 3.1). O ponto crítico dedetecção, assim, localiza-se no nível de sensoriamento imediatamente após o ponto onde o somatório dos tempos de retardo excede o tempo de resposta. Em seguida, os valores das probabilidades de detecção (PD) das camadas de sensores subsequentes são utilizados para calcular o P_I, usando-se a Equação 3.8.

3.3.2 Análise de múltiplos caminhos usando Diagramas de Sequência de Adversário

Para uma instalação que possui diversos caminhos possíveis para se acessar um alvo, a probabilidade de interrupção P_I é calculada usando-se os Diagramas de Sequência de Adversário (DSA). Os DSA são ferramentas gráficas que representam todos os caminhos possíveis em uma instalação, desde o exterior até o alvo do roubo ou sabotagem (Figura 3.6).

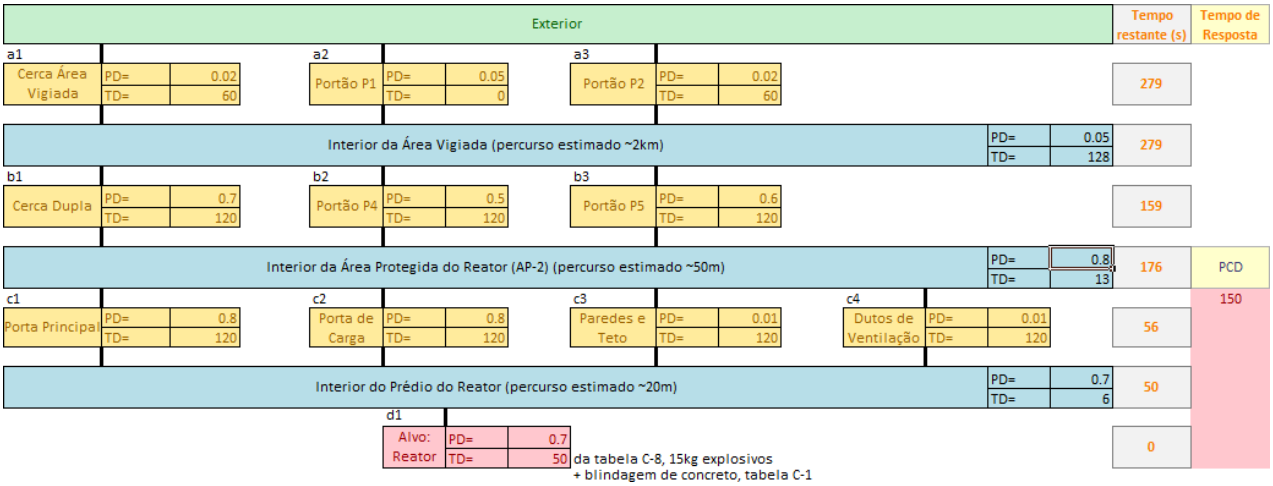


Figura 3.6. Exemplo de Diagrama de Sequência de Adversário.

No DSA são representados os elementos de proteção física (cercas, paredes, janelas, portas, elementos de detecção e controle de acesso), assim como as probabilidades de detecção (P_D) associadas a cada elemento (em amarelo) ou zona (em azul) e os tempos de retardo fornecidos pelas barreiras físicas (T_D). Cada n-upla ordenada {ax, bx, cx, dx}, vista na vertical do diagrama, representa um caminho possível pelo qual, a partir do exterior, um adversário pode acessar o alvo. Assim, o número de caminhos possíveis é dado pelas possíveis n-uplas, ou seja, pelo produto do número de elementos em cada nível. No exemplo da Figura 3.2, o número de caminhos é de 36, tendo em vista que:

$$\text{número de caminhos} = (\#\text{nível a}) * (\#\text{nível b}) * (\#\text{nível c}) = 3 * 3 * 4 = 36 \quad \text{(Eq. 3.9)}$$

Assim, a utilização do DSA proporcionará o cálculo do P_I para cada caminho da instalação até o alvo. Considera-se que o caminho (ou os caminhos) com menor P_I são os mais vulneráveis da instalação, devendo ser tomados como representativos do sistema como um todo [52].

Portanto, a efetividade global do SisPF para a instalação será:

$$P_E = \min (P_I) * P_N \qquad \text{(Eq. 3.10)}$$

Onde:

P_E:= Efetividade do Sistema de segurança da instalação;

min (P_I):= Mínimo P_I dentre todos os caminhos possíveis da instalação; e

P_N:= Probabilidade de Neutralização.

3.4 Síntese do capítulo

Este capítulo teve o propósito de descrever o modelo de instalação nuclear e como será realizada a avaliação das vulnerabilidades do sistema de proteção física modelado, contemplando os elementos físicos e cibernéticos do sistema de segurança, dentro de uma abordagem de gerenciamento de riscos.

4 AVALIAÇÃO DA EFETIVIDADE

Este Capítulo se destina a exibir os resultados obtidos para a eficácia (P_E) do sistema de segurança do ICNC, considerando o modelo de instalação concebido e a ameaça-base de projeto postulada na Seção 3.1. Nas Seções seguintes, foram desenvolvidos quatro cenários de ataques à instalação, o primeiro considerando um ataque inteiramente físico, similar aos ataques estudados por [1] e [22], o segundo e o terceiro adicionando ao mesmo ataque físico ataques cibernéticos em diferentes ativos digitais críticos do sistema de proteção física (sistema de vigilância por CFTV, controles de acesso e sensores de intrusão na cerca dupla da área protegida), que são parte das redes administrativa e da operacional.

Os cenários de ataque desenvolvidos possibilitaram o cálculo de P_E por meio da ferramenta EASI e da análise de múltiplos caminhos, visando a uma posterior comparação para se vislumbrar o impacto em P_E oriundo do comprometimento dos ativos digitais.

4.1 Cenários de Ataques

4.1.1. Cenário 1: Efetividade do Sistema de Segurança em Condições Normais (ataque puramente físico)

4.1.1.1 Etapas do Ataque 1

No primeiro cenário, a ameaça descrita na Tabela 3.2 (Ameaça-Base de Projeto) realiza a seguinte ação planejada de sabotagem no ICNC, nas seguintes etapas:

1. Durante o turno da noite, a força adversa monitora a rotina de rondas na área vigiada do ICNC usando as imagens captadas por um drone, determinando quais os momentos de maior vulnerabilidade dos acessos à instalação;
2. No momento em que os guardas rondantes estão mais distantes da entrada de serviço (portão de carga P2), um grupo de 5 adversários armados acessa a área vigiada da instalação, usando de alicates de corte, inutilizando o portão e P2 e permitindo o acesso ao instituto pela via auxiliar com um veículo comum, carregando explosivos e armamentos;
3. No interior da área vigiada, usam alicates para cortar o portão P5, acessando à pé o interior da área protegida do Reator ICNC-R1, carregando os explosivos a serem utilizados nas ações subsequentes;
4. Um dos adversários monta os explosivos na porta de carga do prédio do reator, inutilizando-a;
5. Sob a cobertura de quatro adversários, um dos elementos do grupo monta os explosivos na estrutura do reator e os detona, causando uma explosão que destrói o reator e espalha material radioativo no ambiente;
6. Um dos elementos do grupo possui uma câmera montada no capacete, para transmissão ao vivo da ação via redes sociais, sendo a transmissão ainda replicada por robôs (bots), com o intuito de causar pânico e caos social na população, aumentar a percepção antinuclear na opinião pública e causar perdas econômicas à região do Cerrado.

A Figura 4.1 permite visualizar a evolução temporal das etapas 1 a 3 do ataque no diagrama da instalação, sendo as etapas 2 e 3 concomitantes à 6 (transmissão ao vivo pela Internet das ações da força adversa):

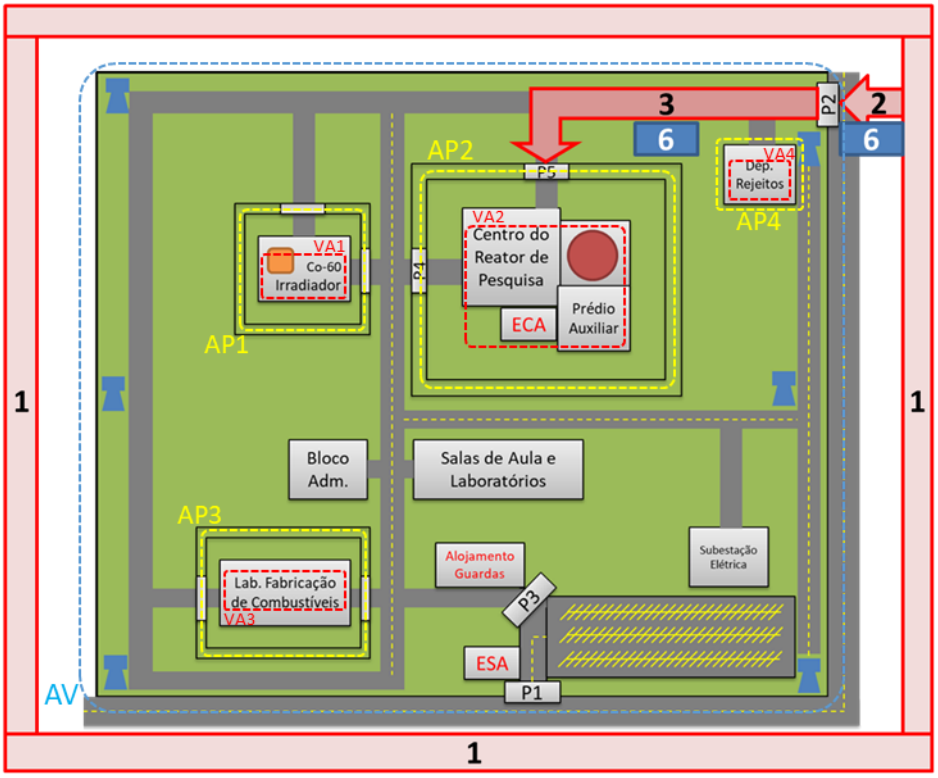


Figura 4.1. Etapas 1, 2 e 3 do ataque do cenário 1 ao reator ICNC-R1.

A Figura 4.2 permite visualizar a evolução temporal das fases 4 e 6, relativas à entrada na área protegida do ICNC:

Figura 4.2. Etapa 4 do ataque do cenário 1- área protegida do Reator ICNC-R1.

A Figura 4.3 possibilita a visualização das etapas finais do ataque de sabotagem ao reator ICNC-R1, concomitantes à transmissão em tempo real:

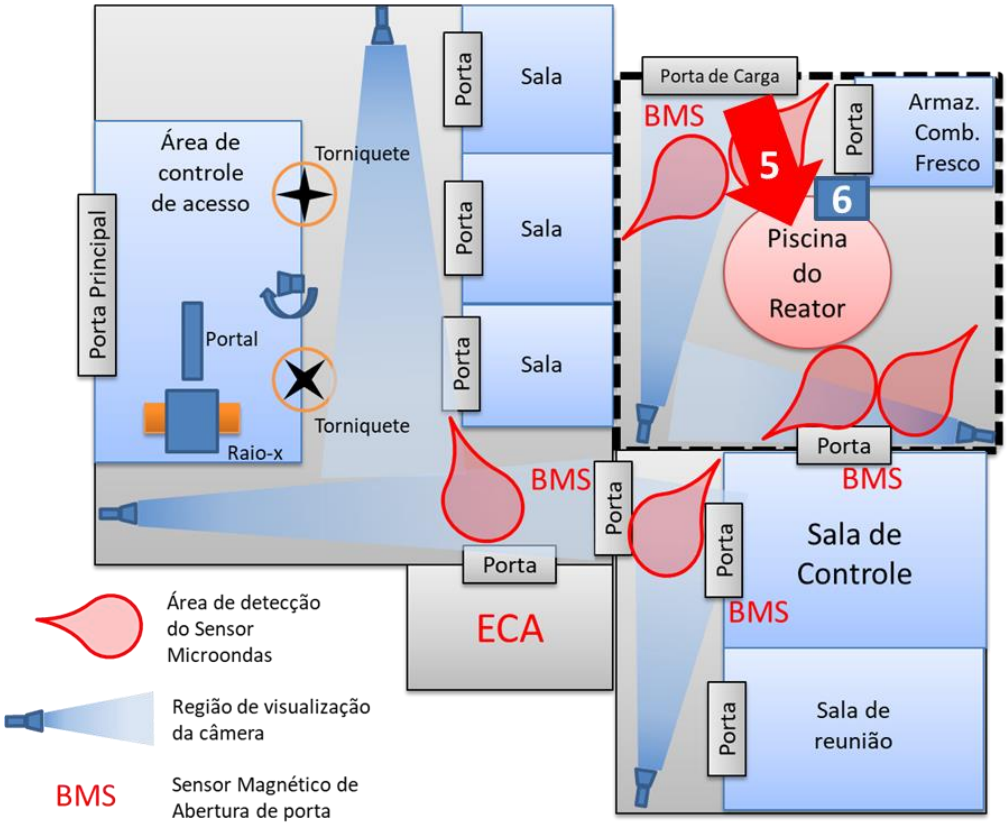


Figura 4.3. Fases 5 e 6 do ataque físico ao Reator ICNC-R1.

4.1.1.2 Modelagem DSA e Cálculo da Efetividade para o Cenário 1

Mapeando as rotas possíveis de intrusão da instalação por meio da ferramenta de Diagrama de Sequência de Adversário (DSA), até a sabotagem no Reator, tem-se (Fig. 4.4):

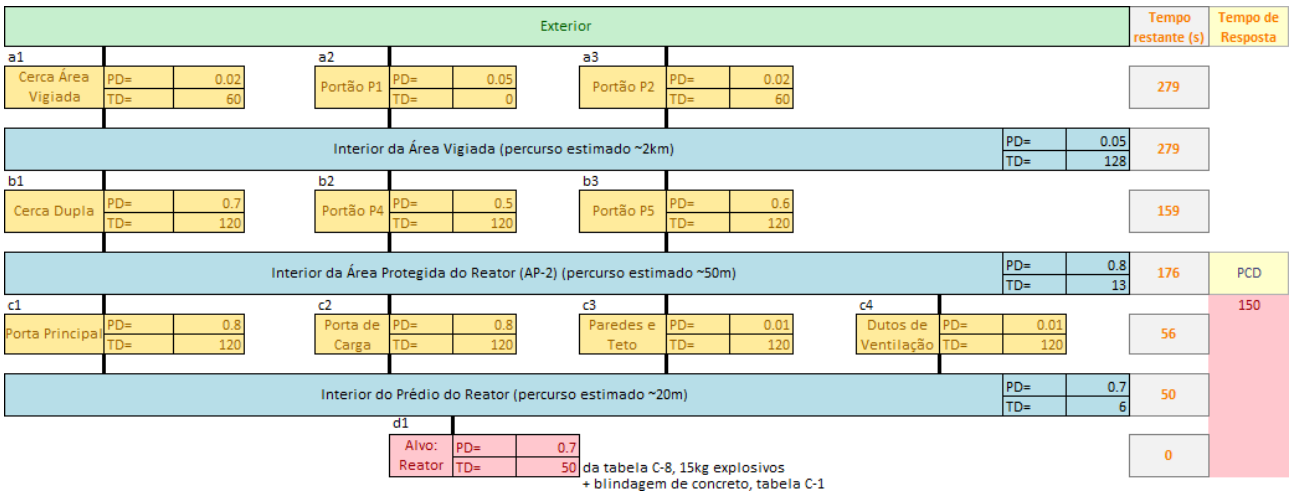


Figura 4.4. Diagrama de Sequência de Adversário para o cenário 1 - ataque puramente físico ao Reator.

Observe-se que o DSA foi preenchido com os valores de Probabilidades de Detecção (PD) e

Tempos de Retardo (TD, do inglês "*Time Delay*") constantes das tabelas constantes dos Anexos B e C, conforme os elementos do modelo da ICNC proposto na Seção 3.1. O Ponto Crítico de Detecção (PCD) foi determinado contabilizando-se os tempos de retardo das barreiras físicas a partir do alvo, sendo, nesse caso, localizado no interior da área protegida do reator, de forma que os termos de PD só são contabilizados na Equação 3.8, que calcula a probabilidade de interrupção (P_I) até AP-2, descartando-se os elementos c1, c2, c3, c4, o interior do prédio do reator e o elemento d1, por não representarem oportunidades tempestivas de detecção.

A partir do DSA da Figura 4.4, ainda, determinou-se o número total de caminhos, pelas combinações {ax,bx,cx,d1} desde o exterior até o alvo, totalizando-se 36 caminhos possíveis. Os cálculos relativos aos valores de P_I encontram-se no Apêndice A.

Para o cálculo da efetividade do sistema (P_E) utiliza-se a Equação 3.10, multiplicando-se o valor de P_I em cada caminho pelo valor da probabilidade de neutralização (P_N) oriunda da tabela do Anexo D. Considera-se, para efeitos práticos, o menor valor obtido de P_E (ou seja, o mais vulnerável) como representativo do sistema.

O gráfico da Figura 4.5 permite visualizar os resultados de P_E para todos os caminhos:

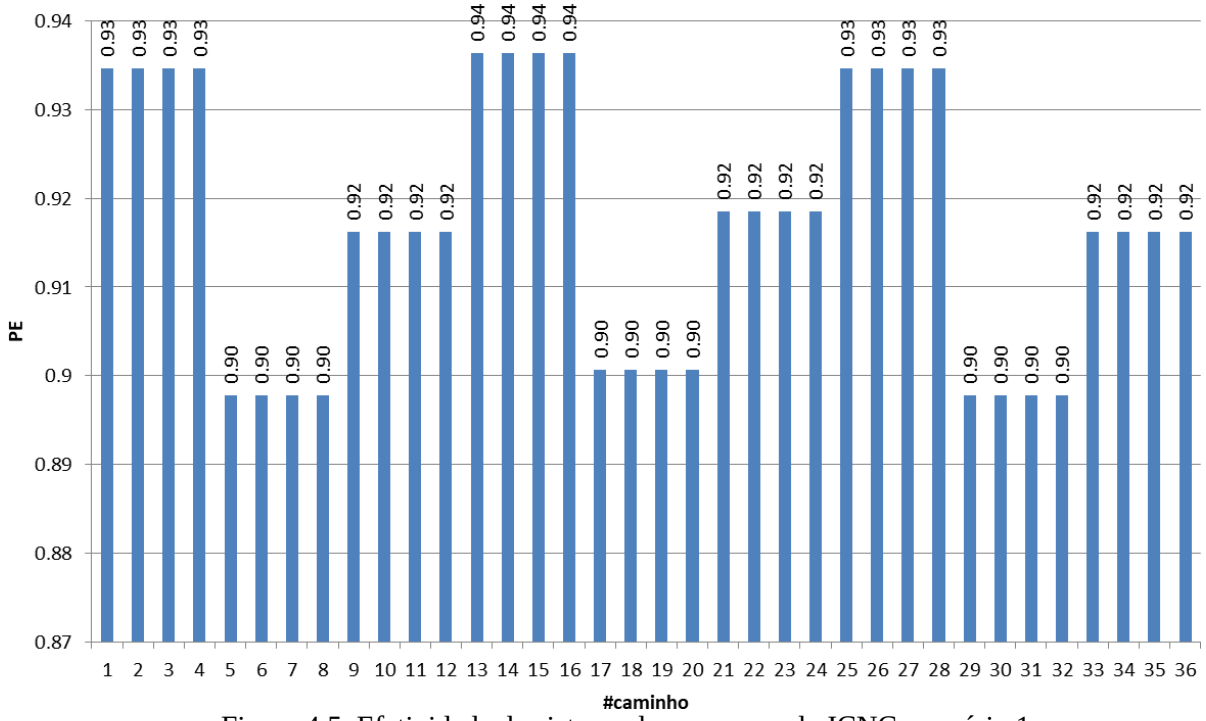


Figura 4.5. Efetividade do sistema de segurança do ICNC - cenário 1.

Da Figura 4.5 depreende-se que, para um ataque puramente físico realizado pela ameaça descrita na Ameaça-Base de Projeto contra o Reator, o sistema de segurança da ICNC possui efetividade de 90%.

4.1.2. Cenário 2: Efetividade do Sistema de Segurança para ataque físico combinado a um ataque cibernético ao sistema de CFTV)

4.1.2.1 Etapas do Ataque 2

O segundo cenário soma ao primeiro um ataque cibernético no sistema de circuito fechado de televisão (CFTV), usado na vigilância dos acessos à área protegida (cerca dupla e portões P4 e P5), o que se considerou um cenário plausível, uma vez que a ameaça-base de projeto possui capacidades cibernéticas (tabela 3.1, Seção 3.1). Assim, a sequência do ataque seguiu as seguintes etapas:

1. Durante o turno da noite, a força adversa monitora a rotina de rondas na área vigiada do ICNC usando as imagens captadas por um drone, determinando quais os momentos de maior vulnerabilidade dos acessos à instalação;
   Como preparação para a entrada da equipe armada, um ataque é realizado sobre as máquinas da ECA (Estação Central de Alarmes), explorando, por exemplo, vulnerabilidades conhecidas em equipamentos de CFTV comuns na área industrial como as CVE-2021-27232[53] e CVE-2021-27197[54], CVE-2022-39861[55] e CVE-2021-1521[56], dos fabricantes Pelco (Digital Sentry Server), Cisco (Video Surveillance 8000 IP Camera) e Samsung (Factory Camera FB), que possibilitam aos atacantes, por exemplo, gravar vídeos de situações normais de operação, e, tendo acesso às máquinas atacadas, manipular as imagens à disposição da força de resposta, ou mesmo provocar uma situação de negação de serviço (*denial of service* - DoS);
2. No momento em que os guardas rondantes estão mais distantes da entrada de serviço (portão de carga P2), e o sistema de CFTV comprometido, um grupo de 5 adversários armados acessa a área vigiada da instalação, usando de alicates de corte, inutilizando o portão e P2 e permitindo o acesso ao instituto pela via auxiliar com um veículo comum, carregando explosivos e armamentos;
3. No interior da área vigiada, usam alicates para cortar o portão P5, acessando à pé o interior da área protegida do Reator ICNC-R1, carregando os explosivos a serem utilizados nas ações subsequentes;
4. Um dos adversários monta os explosivos na porta de carga do prédio do reator, inutilizando-a;
5. Sob a cobertura de quatro adversários, um dos elementos do grupo monta os explosivos na estrutura do reator e os detona, causando uma explosão que destrói o reator e espalha material radioativo no ambiente;
6. Um dos elementos do grupo possui uma câmera montada no capacete, para transmissão ao vivo da ação via redes sociais, sendo a transmissão ainda replicada por robôs (bots), com o intuito de causar pânico e caos social na população, aumentar a percepção antinuclear na opinião pública e causar perdas econômicas à região do Cerrado.

A Figura 4.6 permite visualizar a sequência do ataque cibernético à rede do sistema de segurança do ICNC:

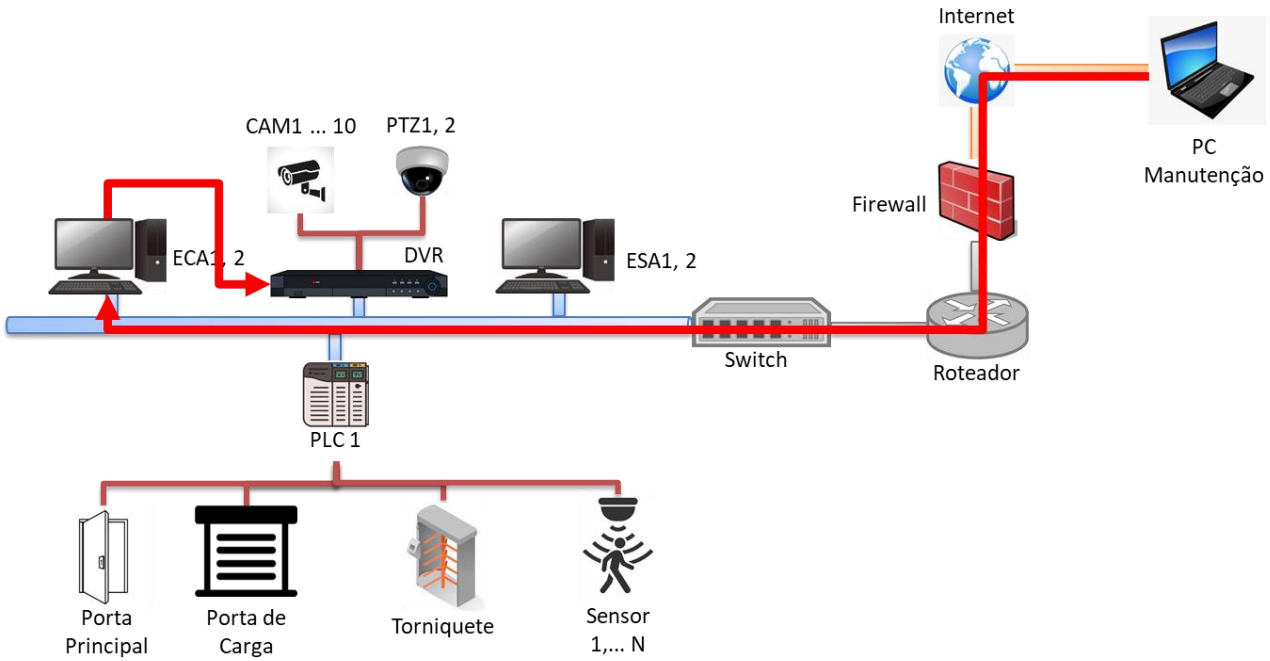


Figura 4.6. Sequência do ataque cibernético ao sistema de CFTV – Cenário 2.

Da Figura 4.6 é possível afirmar que o ataque cibernético partiu de uma estação remota de manutenção, possivelmente viabilizado por um ataque de engenharia social, possibilitando o controle da máquina.

4.1.2.2 Modelagem DSA e Cálculo da Efetividade para o Cenário 2

Na Figura 4.7, pode-se visualizar o DSA para o cenário 2:

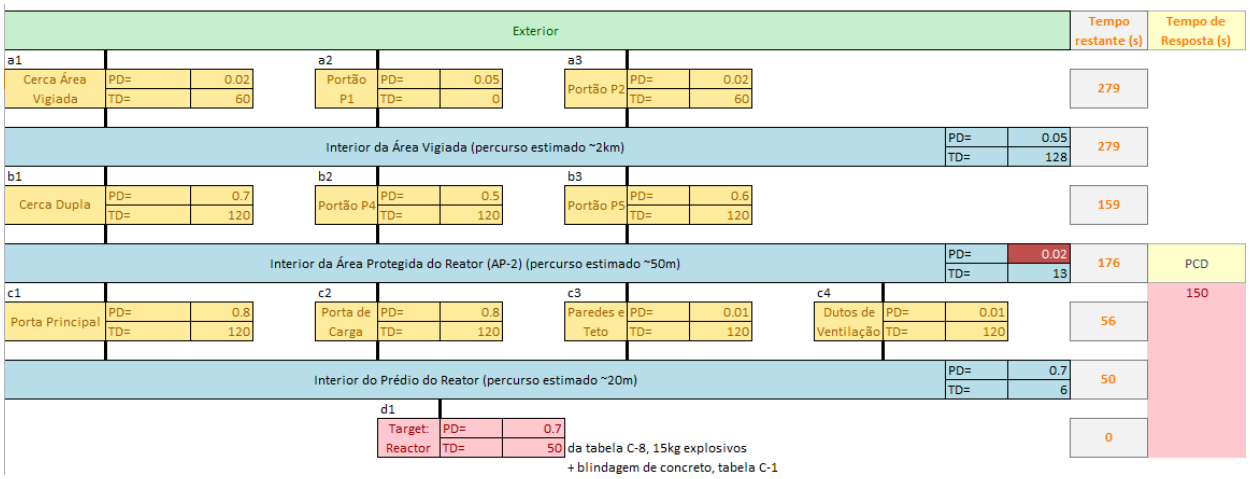


Figura 4.7. Diagrama de Sequência de Adversário para o Cenário 2.

O ataque cibernético sobre o CFTV reduziu a probabilidade de detecção (P_D) no interior da área protegida de 0,8 (conforme a tabela B-1 do Anexo B) para 0,02 (2%), que corresponde à probabilidade residual de a equipe atacante ser detectada de forma visual pelos vigilantes em ronda, conforme a tabela B-3 do Anexo B. Como não houve qualquer mudança nos tempos de retardo associados aos elementos posteriores ao PCD original, o mesmo continua no mesmo ponto, no interior da área protegida do reator. Assim, o valor de P_D modificado no ataque cibernético é levado em consideração nos cálculos de P_I e P_N.

Assim, realizando os cálculos de P_I e P_E para os 36 caminhos possíveis (memórias de cálculo

no Apêndice A), pode-se visualizar na Figura 4.8 os valores de P_E:

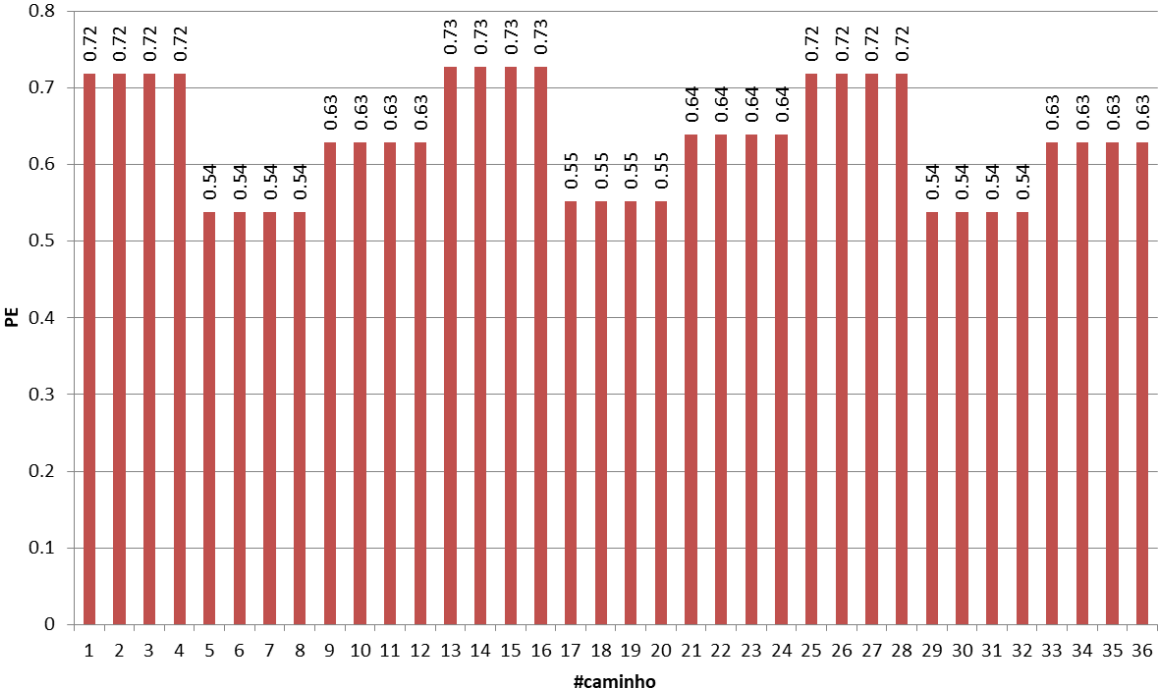


Figura 4.8. Valores de P_E para todos os caminhos - Cenário 2.

Da Figura 4.8 pode-se afirmar que a efetividade do sistema de segurança do ICNC, para o cenário do ataque cibernético ao sistema de CFTV somado ao ataque físico resultou em 0,54 (54%).

4.1.3. Cenário 3: Efetividade do Sistema de Segurança para ataque físico combinado a um ataque cibernético ao sistema de controle de acesso

4.1.3.1 Etapas do Cenário 3

O terceiro cenário inclui, além do ataque físico, um ataque cibernético envolvendo o sistema de controle de acesso, usado para gerenciar a abertura e fechamento das portas do prédio do reator (porta principal e porta de carga), bem como do torniquete do ponto de entrada da área controlada radiológica. A sequência do ataque contempla as seguintes etapas:

1. Durante o turno da noite, a força adversa monitora a rotina de rondas na área vigiada do ICNC usando as imagens captadas por um drone, determinando quais os momentos de maior vulnerabilidade dos acessos à instalação.
2. Aproveitando-se do fato de um dos integrantes da equipe de segurança ter instalado um ponto de acesso sem fio à internet ligado ao switch da rede de segurança, para possibilitar a conexão das máquinas da rede à internet (normalmente bloqueada pelo *firewall*), um atacante externo executou um ataque do tipo *man-in-the-middle*, ganhando acesso remoto à rede, inclusive ao Controlador Lógico Programável (PLC), localizado na Estação Central de Alarmes, explorando, por exemplo, vulnerabilidades conhecidas conhecidas de PLCs usados na área industrial como as CVE-2018-19616[57] (Rockwell Automation Allen-Bradley PowerMonitor 1000), CVE-2022-30318[58] (Honeywell ControlEdge) e CVE-2022-31207[59] (Omron SYSMAC Cx),

que possibilitam aos atacantes, por exemplo, obter privilégios de administrador e mudar os estados das entradas e saídas analógicas e digitais do PLC, abrindo e fechando portas e liberando o acesso pelo torniquete. Assim, no momento planejado do ataque, o atacante remoto acionou a abertura da porta principal e de carga do prédio do reator, bem como liberou o acesso no torniquete na entrada da área controlada (Figura 4.9). Como o ataque ocorreu no período noturno, fora do horário de expediente normal do instituto, não houve a atuação manual de fechamento das portas pelos operadores;

3. As demais etapas do ataque físico são idênticas às do primeiro e segundo cenários.

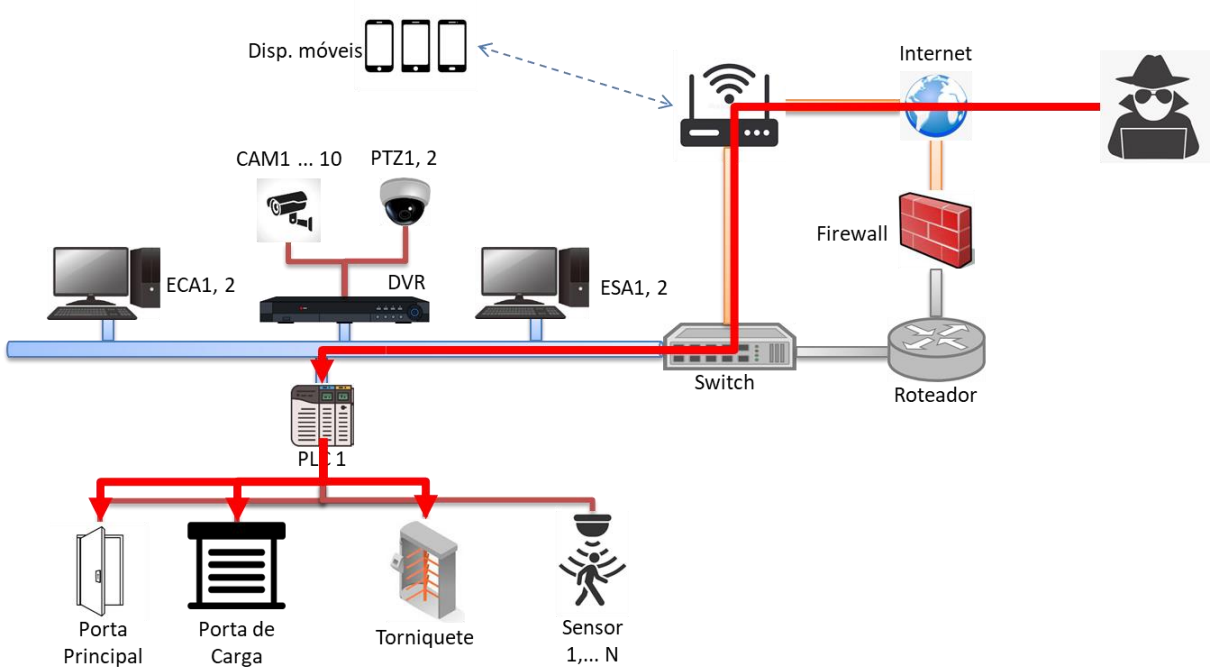


Figura 4.9. Ataque cibernético ao sistema de controle de acesso - Cenário 3.

4.1.3.2 Modelagem DSA e Cálculo da Efetividade para o Cenário 3

O DSA para o esse ataque pode ser visualizado na Figura 4.10:

Exterior													Tempo restante (s)	Tempo de Resposta (s)
a1 Cerca Área Vigiada	PD= 0.02 TD= 60		a2 Portão P1	PD= 0.05 TD= 0		a3 Portão P2	PD= 0.02 TD= 60						317	
Interior da Área Vigiada (percurso estimado ~2km)											PD= 0.05 TD= 128		189	PCD
b1 Cerca Dupla	PD= 0.7 TD= 120		b2 Portão P4	PD= 0.5 TD= 120		b3 Portão P5	PD= 0.6 TD= 120						69	150
Interior da Área Protegida do Reator (AP-2) (percurso estimado ~50m)											PD= 0.8 TD= 13		56	
c1 Porta Principal	PD= 0.8 TD= 0		c2 Porta de Carga	PD= 0.8 TD= 0		c3 Paredes e Teto	PD= 0.01 TD= 120		c4 Dutos de Ventilação	PD= 0.01 TD= 120			56	
Interior do Prédio do Reator (percurso estimado ~20m)											PD= 0.7 TD= 6		50	
d1 Target: Reactor	PD= 0.7 TD= 50	da tabela C-8, 15kg explosivos + blindagem de concreto, tabela C-1											0	

Figura 4.10. Diagrama de Sequência de Adversário para o Cenário 3.

Da figura 4.10 pode-se observar que o ataque sobre o PLC, tendo deixado abertas a porta principal (elemento c1) e de carga (elemento c2) do prédio do reator, não alterou os parâmetros originais de probabilidade de detecção em quaisquer dos elementos, no entanto os tempos de retardo originalmente proporcionados por ambas as portas (barreiras físicas) vai a zero, mudando o posicionamento do PCD e deixando apenas duas oportunidades tempestivas de detecção, no nível "a" (elementos a1, a2, a3) ou no interior da área vigiada. Assim, na Equação 3.10 entrarão apenas os valores respectivos de P_D dos elementos restantes.

Assim, realizando-se os cálculos de P_E para todos os caminhos (Apêndice A), a Figura 4.11 possibilita visualizar os valores da efetividade do sistema de segurança no terceiro cenário:

Figura 4.11. Valores de P_E para todos os caminhos - Cenário 3.

Da Figura 4.11 pode-se afirmar que a efetividade do sistema de segurança do ICNC, para o cenário do ataque cibernético ao sistema de controle de acesso, somado ao ataque físico, resultou no valor de 0,07 (7%).

4.1.4 Cenário 4: Efetividade do Sistema de Segurança para ataque físico combinado a um ataque cibernético à rede de sensores de intrusão na cerca dupla de área protegida

4.1.4.1 Etapas do Cenário 4

O quarto cenário estudado contempla o mesmo modo de ataque físico dos cenários anteriores, desta vez com um ataque cibernético sobre o sistema de detecção (sensores de intrusão instalados nos limites da área protegida). O cenário segue a seguinte sequência:

1. Durante o turno da noite, a força adversa monitora a rotina de rondas na área vigiada do ICNC usando as imagens captadas por um drone, determinando quais os momentos de maior vulnerabilidade dos acessos à instalação.
2. Aproveitando-se do fato de um dos integrantes da equipe de segurança ter instalado um ponto de acesso sem fio à internet ligado ao switch da rede de segurança, para possibilitar a conexão das máquinas da rede à internet (normalmente bloqueada pelo

firewall), um atacante externo executou um ataque do tipo *man-in-the-middle*, ganhando acesso remoto à rede, inclusive ao Controlador Lógico Programável (PLC), localizado na Estação Central de Alarmes, explorando, por exemplo, vulnerabilidades conhecidas de PLCs usados na área industrial como as CVE-2021-33012 [60] (Rockwell Automation MicroLogix 1100), CVE-2021-37204 [61] (família Siemens SIMATIC S7) e CVE-2021-37205 [62] (SIMATIC Drive Controller), que possibilitam aos atacantes, por exemplo, causar condições de negação de serviço (*denial-of-service ou DoS*) no PLC. Assim, no momento planejado do ataque, o atacante remoto causou o DoS no PLC, as portas e o torniquete falharam em modo seguro (fechadas) mas os sensores de intrusão ficaram inoperantes, restando aos operadores da Central de Alarmes contar com a vigilância por câmeras e as rondas realizadas pela equipe de segurança (Figura 4.12);

3. As demais etapas do ataque físico são idênticas às do primeiro e segundo cenários.

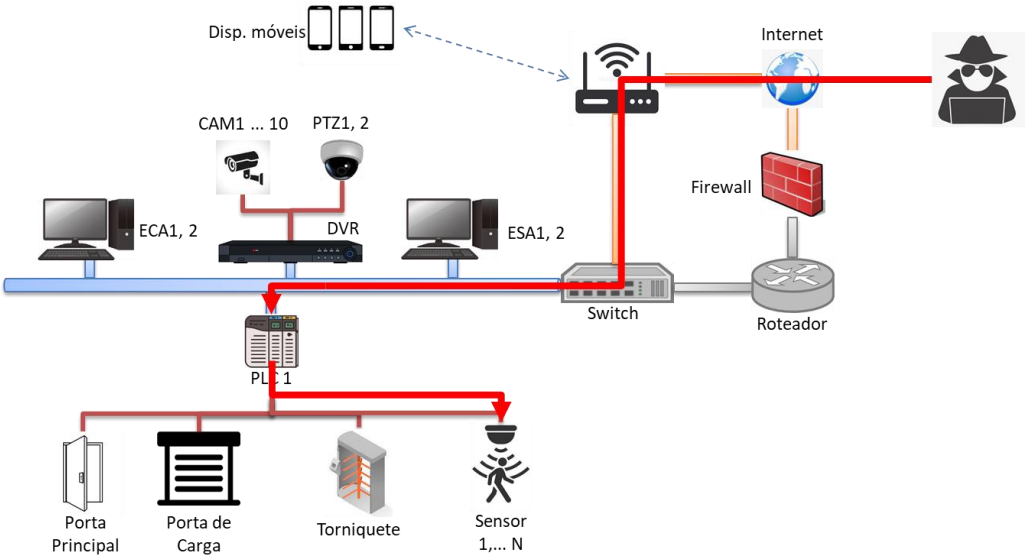


Figura 4.12. Ataque cibernético ao sistema de detecção de intrusão - Cenário 4..

4.1.4.2 Modelagem DSA e Cálculo da Efetividade para o Cenário 4

O DSA para esse cenário de ataque pode ser visualizado na Figura 4.13:

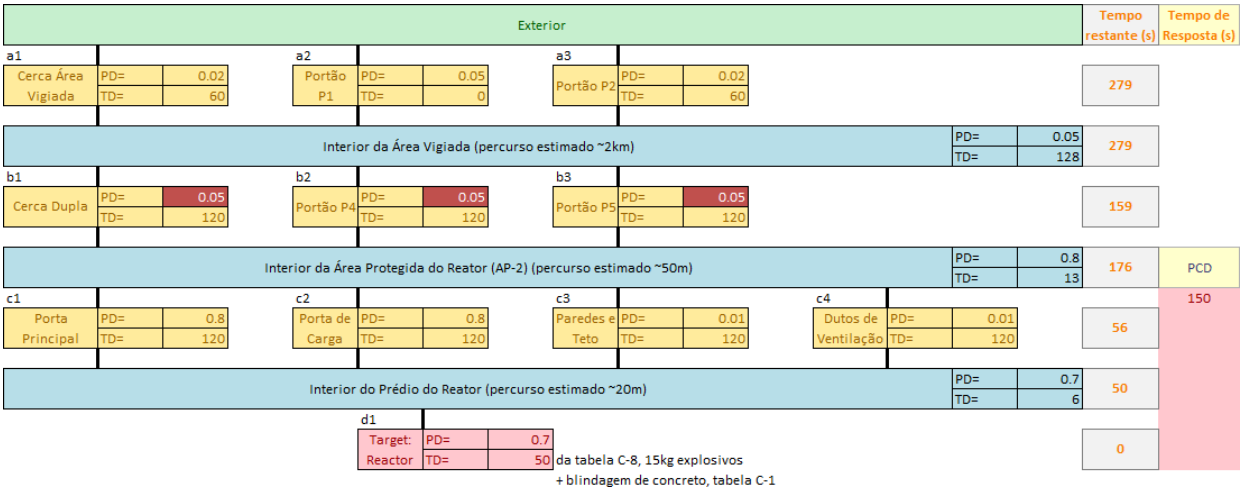


Figura 4.13. Diagrama de Sequência de Adversário - Cenário 4.

Da Figura 4.13 pode-se observar que o ataque sobre o PLC, tendo deixado inoperantes os sensores de intrusão nos limites da área protegida, não representou alteração nos parâmetros originais de tempos de retardo em quaisquer dos elementos, deixando inalterado o posicionamento do PCD dos cenários 1 e 2 e permitindo três oportunidades tempestivas de detecção, no nível "a" (elementos a1, a2, a3), no interior da área vigiada e no nível "b" (elementos b1, b2, b3). No entanto, os valores de P_D para o nível "b" são reduzidos para 0,05, tendo-se em vista a probabilidade de detecção residual das rondas, que pode ou não ser confirmada pela vigilância eletrônica via CFTV.

Assim, realizando-se os cálculos de P_E para todos os caminhos (Apêndice A), a Figura 4.14 possibilita visualizar os valores da efetividade do sistema de segurança no quarto cenário:

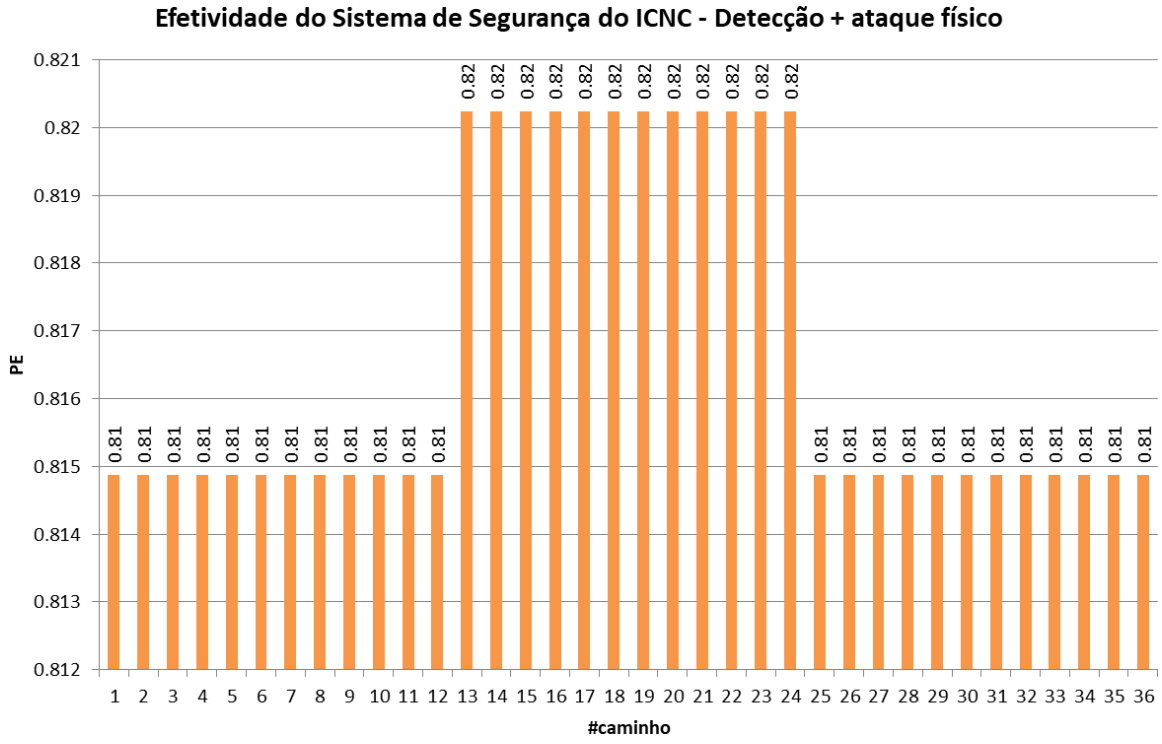


Figura 4.14. Valores de P_E para todos os caminhos - Cenário 4.

Da Figura 4.14 pode-se afirmar que a efetividade do sistema de segurança do ICNC, para o cenário do ataque cibernético ao sistema de detecção, somado ao ataque físico, resultou no valor de 0,81 (81%).

4.2 Análise Comparativa das Efetividades e Discussão sobre os Resultados

A Tabela 4.1 possibilita uma comparação direta entre a efetividade do sistema de segurança do ICNC, tomando como base o P_E do ataque puramente físico (Cenário 1):

Tabela 4.1. Comparação de efetividade do sistema de segurança do ICNC nos diferentes cenários.

	Efetividade (P_E)	**Diferença Relativa (%)**
Cenário 1	0,90 (90%)	
Cenário 2	0,54 (54%)	-40%
Cenário 3	0,07 (7%)	-92%
Cenário 3	0,81 (81%)	-10%

Em que pese não haver requisitos regulatórios nacionais que obriguem os operadores de instalações nucleares a alcançar um valor específico de efetividade, verificou-se que em todos os casos houve significativa redução na efetividade do sistema de segurança.

Especificamente, os resultados do trabalho permitiram elencar as seguintes constatações:

- O ataque cibernético envolvendo os ativos digitais dos sistemas de vigilância por CFTV conjugado ao ataque físico (cenário 2) representou impacto percentual de -40% quando comparado ao cenário 1 (puramente físico) tendo uma efetividade residual de 54%;

- O cenário no qual houve um ataque cibernético ao PLC responsável pelo controle de acesso (cenário 3) teve o maior impacto dentre todos os casos analisados, de -92%, restando uma efetividade residual de apenas 7%, praticamente inviabilizando a atuação da força de resposta;

- O cenário 3 equivale, em termos de efeitos, à ação de uma ameaça interna (*insider* ativo), que propositalmente deixaria portas abertas no fim do expediente visando facilitar a ação adversa de intrusão. Ameaças internas representam um grande objeto de preocupação na literatura da área de segurança nuclear, tendo-se desenvolvido recomendações e publicações internacionais no sentido de mitigar essa ameaça;

- O ataque cibernético envolvendo os ativos digitais da rede de sensores de intrusão conjugados ao ataque físico (cenário 4) representou uma diferença absoluta de -10% quando comparado ao cenário 1, puramente físico, tendo o sistema uma efetividade residual de 81%;

- Os cenários 3 e 4 foram concebidos e viabilizados por meio de uma ligação à internet feita de forma insegura pela própria força de segurança, o que evidencia uma oportunidade de melhoria no que diz respeito à cultura de segurança, e em particular, à cultura de segurança cibernética. Atualmente não há requisitos normativos específicos que obriguem os operadores nucleares a promover ações no sentido de fomentar a cultura de segurança cibernética na força de trabalho, o que pode suscitar ações potencialmente perigosas como as descritas nos cenários estudados;

- A despeito de o projeto inicial do sistema de segurança ter sido concebido considerando-se a regulamentação vigente relativa à segurança física de instalações nucleares (Norma CNEN NN 2.01), observou-se que a mera conformidade com a mesma não garante uma mitigação adequada dos riscos oriundos de cenários de ataque híbridos, pois não foram observados requisitos mais específicos de forma a direcionar a adoção de medidas e controles de segurança cibernética nos ativos digitais relacionados ao sistema de proteção física. É possível, então, afirmar que seria desejável uma revisão do arcabouço regulatório nacional de segurança de instalações nucleares, de forma a abranger os modos de ataques híbridos;

- O modelo proposto no trabalho possui uma limitação no que tange às ações de resposta ao incidente do ponto de vista cibernético, que poderiam, se tempestivas, mitigar o efeito dos ataques, reduzindo os cenários 2, 3 e 4 ao cenário 1, no qual o sistema de segurança possui razoável efetividade em repelir o ataque (90%), uma vez que se daria apenas no aspecto cinético.

5 CONCLUSÕES

Em relação aos objetivos e à hipótese de pesquisa do trabalho, os cenários concebidos, considerando ameaças com capacidades cinéticas e cibernéticas, a execução da avaliação das vulnerabilidades usando as ferramentas do framework DEPO e o método EASI possibilitaram o entendimento de como os cenários de ataque híbridos impactam a efetividade do sistema de segurança; os resultados de -40%, -92% e -10% de diferença percentual na redução de P_E significariam, em um cenário real, uma perda da capacidade de resposta efetiva e tempestiva ao ataque perpetrado, o que é particularmente significativo considerando-se que o sistema de segurança foi dimensionado em conformidade à regulação em vigor.

Confirma-se, portanto, a hipótese descrita na Seção 1.3 de que a análise realizada é melhor no que diz respeito ao entendimento das ameaças híbridas e suas consequências que a abordagem feita separadamente, ora considerando aspectos físicos, ora considerando aspectos cibernéticos, comum nos trabalhos correlatos.

Aplicando-se essas considerações ao caso real, faltam requisitos regulatórios aplicáveis às ações de resposta a incidentes cibernéticos, de forma específica para instalações nucleares, o que seria uma oportunidade de revisão regulatória concernente ao tema, o que poderia, teoricamente, possibilitar a implantação de estratégias de resposta dos pontos de vista cibernético e físico de forma integrada.

Algumas melhorias que poderiam mitigar os riscos de ataques e proporcionar maior resiliência em face das ameaças listadas incluem:

- A revisão do arcabouço regulatório nacional no que diz respeito à inclusão de requisitos relativos à segurança cibernética, avaliação de ameaças com capacidades cibernéticas e cultura de segurança cibernética, tornando-os obrigatórios para os detentores de licenças de operação envolvendo materiais nucleares;
- A adoção de ações de controle, como sistemas de gerenciamento e monitoramento de redes, registro de eventos e resposta a incidentes de rede, bem como o estabelecimento de cadeia de notificações às autoridades com responsabilidades à segurança de materiais nucleares;
- No tocante à segurança física, considerar ameaças com capacidades não convencionais como os vetores aéreos não tripulados (*drones*) na prevenção e resposta a incidentes;

Em relação aos possíveis trabalhos futuros, vislumbram-se diversas oportunidades:

- Realizar análises similares para outros ativos digitais envolvidos na operação de instalações nucleares, como as funções de contabilidade e controle de material nuclear, comunicações, resposta e sistemas de suporte a emergências radiológicas, sistemas de instrumentação e controle de processos, sistemas de segurança de processo e sistemas corporativos, estudando os diferentes tipos de riscos e impactos para cada uma das funções elencadas;
- Estudar os impactos de ataques ciberfísicos em outros tipos de instalações sujeitas a diferentes regulamentações da área nuclear, como depósitos de rejeitos radioativos, instalações de medicina/indústria que operam com fontes radioativas, ou mesmo em operações de transporte de materiais radioativos, nas quais os ativos a proteger encontram-se mais vulneráveis do que na instalação propriamente dita;

- Usar o framework DEPO e as ferramentas de avaliação de vulnerabilidades como a análise multicaminhos e o EASI em outros tipos de indústrias ou infraestruturas críticas, como indústrias químicas/petroquímicas, abastecimento de água, geração/transmissão de energia elétrica, considerando modelos específicos para cada indústria e as respectivas legislações vigentes.

REFERÊNCIAS BIBLIOGRÁFICAS

1 TAVARES, R.L.A. Projeto e avaliação do sistema de proteção física de uma instalação nuclear. 2018. 133p. Dissertação (Mestrado em Engenharia Nuclear) – Instituto Militar de Engenharia – IME, Rio de Janeiro. Disponível em: (https://redebie.decex.eb.mil.br/pergamumweb/vinculos/00005d/00005dfb.pdf).

2 BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>.

3 BUNN, M., ROTH, N., TOBEY, W. *Combating Complacency about Nuclear Terrorism*. Cambridge, MA: Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2019. Disponível em: <https://scholar.harvard.edu/files/matthew_bunn/files/bunn_nuclearsecuritypolicybrief_2 _2019.pdf>.

4 WORLD INSTITUTE FOR NUCLEAR SECURITY. Effectively Integrating Physical and Cyber Security. Ver. 1.1. Vienna, Austria: WINS Best Practice Guide, 2015. Disponível em: <https://wins.org/document/4-11-effectively-integrating-physical-and-cybersecurity/>.

5 COMISSÃO NACIONAL DE ENERGIA NUCLEAR. Glossário do Setor Nuclear e Radiológico Brasileiro. 2.ed. Rio de Janeiro, 2020. Disponível em: <http://appasp.cnen.gov.br/seguranca/normas/pdf/glossario.pdf>.

6 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União. Brasília/DF, 15 de agosto de 2018. Seção 1, p.59. Disponível em: <http://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/36849373/do1-2018-08-15-lei-no-13-709-de-14-de-agosto-de-2018-36849337>.

7 BRASIL. Decreto nº 10.222, de 05 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. Diário Oficial da União. Brasília/DF, 06 de fevereiro de 2020. Seção 1, p. 6. Disponível em: <http://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419>.

8 LIMA, F.P.C., MONTEIRO FILHO, J.S., TAVARES, R. L. A. *Brazilian Nuclear Security Framework*. In: *International Conference on Nuclear Security: Commitments and Actions*. December 5-9, 2016, Vienna, Austria. Proceedings... Disponível em: <https://www.iaea.org/publications/12238/international-conferenceon-nuclear-security-commitments-and-actions>.

9 LIMA, A.R., TAVARES, R.L.A, MONTEIRO FILHO, J.S.M, DA SILVA, F.C.A. Panorama da segurança física de fontes radioativas no Brasil. *Brazilian Journal of Radiation Sciences*, v. 6, n.2B, p. 462, 2018. Disponível em: <https://www.bjrs.org.br/revista/index.php/REVISTA/article/view/462>.

10 TAVARES, R. L. A., LIMA, A.R., MONTEIRO FILHO, J.S. *Strengthening the security on transport of nuclear and other radioactive material: challenges and actions for regulatory improvements in Brazil.* In: *International Conference on Nuclear Security*. February 10-14, 2020, Vienna, Austria. Proceedings... Disponível em: <https://conferences.iaea.org/event/181/contributions/15615/>.

11 COMISSÃO NACIONAL DE ENERGIA NUCLEAR. Resolução nº 253/2019: *Proteção Física de Materiais e Instalações Nucleares*. Rio de Janeiro: CNEN, 2019. (CNEN NN 2.01).

12 NUCLEAR THREAT INITIATIVE. *NTI Nuclear Security Index: Losing Focus in a Disordered World*. Fifth Edition, July 2020. Disponível em: <https://www.ntiindex.org/wpcontent/uploads/2020/07/2020_NTI-Index_Report_Final.pdf >.

13 INTERNATIONAL ATOMIC ENERGY AGENCY. *IAEA Statute*. Disponível em:<https://www.iaea.org/about /statute>.

14 INTERNATIONAL ATOMIC ENERGY AGENCY. *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)*. Vienna, Austria: 2011. Disponível em: <https://wwwpub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf>.

15 INTERNATIONAL ATOMIC ENERGY AGENCY. *Computer Security for Nuclear Security*. Vienna, Austria: 2021. Disponível em: <https://wwwpub.iaea.org/MTCD/Publications/PDF/Pub1918_web.pdf>.

16 INTERNATIONAL ATOMIC ENERGY AGENCY. *Security of Nuclear Information*. Vienna, Austria: 2015. Disponível em: <https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1677web32045715.pdf>.

17 BRASIL. Decreto 11.188, de 5 de setembro de 2022. Promulga a Emenda à Convenção sobre a Proteção Física do Material Nuclear, adotada pela República Federativa do Brasil, em Viena, em 2005. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D11188.htm>.

18 INTERNATIONAL ATOMIC ENERGY AGENCY. *Amendment to the Convention on the Physical Protection of Nuclear Material.* Vienna, Austria, 2016. (INFCIRC/274/Rev.1/Mod.1). Disponível em: <https://www.iaea.org/sites/default/files/infcirc274r1m1.pdf>.

19 WORLD ECONOMIC FORUM. *Cybersecurity of Civil Nuclear Facilities: Assessing the Threat, Mapping the Path Forward.* Moscow – Geneva, 2016. Disponível em:<http://www.pircenter.org/media/content/files/13/14758399064.pdf >.

20 PARK, J., YONGSUK, S., PARK, C. *Implementation of cyber security for safety systems of nuclear facilities*. Progress in Nuclear Energy, v. 88, p. 88-94, 2016. Disponível em: <https://doi.org/10.1016/ j.pnucene.2015.12.009>.

21 DO-YEON, K. *Cyber security issues imposed on nuclear power plants*. Annals of Nuclear Energy, v. 65, p. 141-143, 2014. Disponível em: <https://linkinghub.elsevier.com/retrieve/pii/S0306454913005781>

22 SANTOS, P.M.R. Projeto de Segurança Física em Uma Instalação Nuclear Brasileira. 2019. 197p. Dissertação (Mestrado em Engenharia Nuclear) – Instituto Militar de Engenharia – IME, Rio de Janeiro. Disponível em: <https://bdex.eb.mil.br/jspui/bitstream/123456789/9144/1/Disserta %C3%A7%C3%A3oPedroMaciel_v11.pdf>.

23 SANDIA NATIONAL LABORATORIES. *Hypothetical Atomic Research Institute (HARI) – The*

Hypothetical Facility. Sandia: Albuquerque, 2017. Disponível em: < https://share#ng.sandia.gov/itc/assets/hypo_fac_hari_090117.pdf> .

24 INTERNATIONAL ATOMIC ENERGY AGENCY. *National Nuclear Security Threat Assessment,*

Design Basis Threats and Representative Threat Statements (Nuclear Security Series 10-G Rev. 1).

IAEA: Vienna, 2021. Disponível em: < https://www#pub.iaea.org/MTCD/publications/PDF/P1926_web.pdf>. ISBN 978-92-0-131120-7>.

25 TAVARES, R. L. A., ALBUQUERQUE, R. d. O, GIOZZA, W. F. *Effectiveness evaluation of a nuclear facility security system under a cyber-physical attack scenario*. In: 2022 17th Iberian Conference on Information Systems and Technologies (CISTI), Madrid, Spain, 2022, pp. 1-6, doi: 10.23919/CISTI54924.2022.9820179.

26 KASSENOVA, T., FLORENTINO, L.P., SPEKTOR, M. *Perspectivas para a Governança Nuclear no Brasil.* Fundação Getúlio Vargas: Rio de Janeiro, 2020. Disponível em: <https://ri.fgv.br/noticias/perspectivas-para-governanca-nuclear-no-brasil >.

27 KASSENOVA, T. O Caleidoscópio Nuclear do Brasil: Uma identidade em evolução. Carnegie Endowment for International Peace: Washington, 2014. Disponível em: <https://carnegieendowment.org/files/brazil_nuclear_kaleidoscope_portuguese.pdf >.

28 INDÚSTRIAS NUCLEARES DO BRASIL. Ciclo do Combustível Nuclear. Disponível em: <https://www.inb.gov.br/Nossas-Atividades/Ciclo-do-combustivel-nuclear>.

29 BRASIL. Decreto nº 7.722, de 20 de abril de 2012. Dispõe sobre a execução no Território Nacional das Resoluções nº 1540 (2004), e nº 1977 (2011), adotadas pelo Conselho de Segurança das Nações Unidas em 28 de abril de 2004 e em 20 de abril de 2011, as quais dispõem sobre o combate à proliferação de armas de destruição em massa e sobre a vigência do Comitê 1540. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7722.htm>.

30 LOPES, G. V., OLIVEIRA, C. F. J. "Stuxnet e Defesa Cibernética Estadunidense à Luz da Análise de Política Externa, RBED, vol. 1, nº 1, jul. 2014. DOI: https://doi.org/10.26792/rbed.v1n1.2014.39457

31 BASIN, D. CyBOK - *The cyber security body of knowledge*. University of Bristol, ch. Formal Methods for Security, versão.[Online]. Disponível em: https://www. cybok. org, 2021.

32 GARCIA, M.L. *The Design and Evaluation of Physical Protection Systems – Second Edition.* Elsevier Butterworth-Heinemann: New York, 2008.

33 OSBORN, D., COHN, B., PARKS, M. J., KNUDSEN, R., ROSS, K., FAUCETT, C., HASKIN, T., KITSOS, P., NOEL, T. *Light Water Reactor Sustainability Program - Modeling for Existing Nuclear Power Plant Security Regime*. Technical Report SAND2019-12015. United States Department of Energy, 2019.

34 BUSQUIM E SILVA, R.A, CORREA, D. ANTUNES, F.R., SOUZA, F. C. S., PIQUEIRA, J.R.C., MARQUES, R.P. *The Asherah Nuclear Power Plant Simulator (ANS) As a Training Tool at the Brazilian Cyber Guardian Exercise*. In: International Conference on Nuclear Security (ICONS) 2020. Anais. Vienna, 2020. Disponível em: <https://conferences.iaea.org/event/181/contributions/15641/attachments/8545/11600/cn274_Full_Paper_Rodney_Busquim_e_Silva_EGC_Final.pdf>.

35 BUSQUIM E SILVA, R.A, SHIRVAN, K., PIQUEIRA, J.R.C., MARQUES, R.P. *Development of the Asherah Nuclear Power Plant Simulator for Cyber Security Assessment*. In: International Conference on Nuclear Security (ICONS) 2020. Anais. Vienna, 2020. Disponível em: < https://conferences.iaea.org/event/181/contributions/15642/attachments/8548/11374/cn274_Full_Paper_Rodney_Busquim_e_Silva_ANS_Final.pdf>.

36 FRIEDBERG, I., McLAUGHLIN, K., SMITH, P., LAVERTY, D. SEZER, S. *STPASafeSec: Safety and security analysis for cyber-physical systems*. Journal of Information Security and Applications, volume 34, 2017, pp.183-196.

37 DONDOSSOLA, G., SZANTO, J., MASERA, M., NAI FOVINO, I. *Effects of intentional threats to power substation control systems*. International Journal of Critical Infrastructures, vol.4, 2008, pp. 129-143. doi: 10.1504/IJCIS.2008.016096.

38 KUNDUR, D., FENG, X., MASHAYEKH, S., LIU, S., ZOURNTOS, T., BUTLERPURRY, K.L.

Towards modelling the impact of cyber-attacks on a smart grid. Int. J. Secur. Networks, vol.6 , 2011, pp. 2-13.

39 CHO, C., CHUNG, W., KUO, S. *Cyberphysical Security and Dependability Analysis of Digital Control Systems in Nuclear Power Plants*. IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 46, no. 3, pp. 356-369, March 2016.

40 ZOU, B., YANG, M., GUO, J., WANG, J., BENJAMIN, E., LIU, H., LI, W. *Insider threats of Physical Protection Systems in nuclear power plants: Prevention and evaluation*. Progress in Nuclear Energy, Volume 104, 2018, pp. 8-15, ISSN 0149- 1970.

41 KIM, S., LIM, H., LIM, S. M., SHIN, I. H. *Study on cyber security assessment for wireless network at nuclear facilities*. 6th International Symposium on Digital Forensic and Security (ISDFS), pp. 1-5. 2018. Proceedings…

42 SON, J., CHOI, J., YOON, H. *New Complementary Points of Cyber Security Schemes for Critical Digital Assets at Nuclear Power Plants*. IEEE Access, vol. 7, pp. 78379- 78390, 2019.

43 ZHANG, F., HINES, J. W., COBLE, J. B. *A Robust Cybersecurity Solution Platform Architecture for Digital Instrumentation and Control Systems in Nuclear Power Facilities*. Nuclear Technology, 206:7, pp. 939-950, 2020.

44 LAMB, C.C., FASANO, R.E., ORTIZ, T. *Advanced Malware and Nuclear Power: Past, Present and Future*. In: Annals of the International Conference on Nuclear Security (ICONS 2020). Proceedings… 45 YOO, H., LEE, N., HAM, T., SEO, J. *Methodology for analyzing risk at nuclear facilities*. Annals of Nuclear Energy, Volume 81, 2015, Pages 213-218, ISSN 0306- 4549.

46 SOLODOV, A., WILLIAMS, A., AL-HANAEI, S. *Analyzing the threat of unmanned aerial vehicles (UAV) to nuclear facilities*. Secur J, 31, 2018, pp. 305–324.

47 ZOU, B., LI, M., YANG, M. *Vulnerability learning of adversary paths in Physical Protection Systems using AMC/EASI*. Progress in Nuclear Energy, volume 134, 2021, 103666, ISSN 0149-1970.

48 KWAK, M. W., JUNG, W. S. *Vital area identification for the physical protection of NPPs in low#power and shutdown operations*. Nuclear Engineering and Technology, Volume 53, Issue 9, 2021, pp. 2888-2898, ISSN 1738-5733.

49 LYU, X., DING, Y., YANG, S. *Safety and security risk assessment in cyberphysical systems*. IET Cyber-Physical Systems: Theory & Applications, v. 4, iss. 3, p. 221 – 232, 2019.

50 INTERNATIONAL ATOMIC ENERGY AGENCY. *Categorization of Radioactive Sources (IAEA Safety Standards Series nº RS-G-1.9)*. IAEA: Vienna, 2005. Disponível em: < https://www#pub.iaea.org/MTCD/Publications/PDF/Pub1227_web.pdf>. ISBN 92–0–103905–0.

51 BENNETT, H.A. U*ser´s Guide for Evaluating Physical Security Capabilities of Nuclear Facilities by the EASI Method*. SAND77-0082, Sandia National Laboratories: Albuquerque, 1977. Disponível em: <https://www.nrc.gov/docs/ML1925/ML19253A369.pdf>.

52 GARCIA, M.L. *Vulnerability Assessment of Physical Protection Systems*. Elsevier Butterworth-Heinemann: New York, 2006.

53 NATIONAL VULNERABILITY DATABASE. CVE-2021-27232 Detail. Disponível em: <

https://nvd.nist.gov/vuln/detail/CVE-2021-27232>

54 NATIONAL VULNERABILITY DATABASE. *CVE-2021-27197 Detail*. Disponível em: <

https://nvd.nist.gov/vuln/detail/CVE-2021-27197>

55 NATIONAL VULNERABILITY DATABASE. *CVE-2022-39861 Detail*. Disponível em: <

https://nvd.nist.gov/vuln/detail/CVE-2022-39861>

56 NATIONAL VULNERABILITY DATABASE. *CVE-2021-1521 Detail*. Disponível em: <

https://nvd.nist.gov/vuln/detail/CVE-2021-1521>

57 NATIONAL VULNERABILITY DATABASE. *CVE-2018-19616 Detail*. Disponível em: <

https://nvd.nist.gov/vuln/detail/CVE-2018-19616>

58 NATIONAL VULNERABILITY DATABASE. *CVE-2022-31207 Detail*. Disponível em: <

https://nvd.nist.gov/vuln/detail/CVE-2022-31207>

59 NATIONAL VULNERABILITY DATABASE. *CVE-2022-30318 Detail*. Disponível em: <

https://nvd.nist.gov/vuln/detail/CVE-2022-30318>

60 NATIONAL VULNERABILITY DATABASE. *CVE-2021-33012 Detail*. Disponível em: <

https://nvd.nist.gov/vuln/detail/CVE-2021-33012>.

61 NATIONAL VULNERABILITY DATABASE. *CVE-2021-37204 Detail*. Disponível em: <

https://nvd.nist.gov/vuln/detail/CVE-2021-37204>

62 NATIONAL VULNERABILITY DATABASE. *CVE-2021-37205 Detail*. Disponível em: <

https://nvd.nist.gov/vuln/detail/CVE-2021-37205>

APÊNDICES

Apêndice A: Memórias de Cálculo da Análise Multicaminhos para todos os cenários

Cenário 1: Ataque Puramente Físico

Cálculos da Probabilidade de Interrupção (PI) e da Efetividade para os 36 caminhos:

#Caminho	Caminho	PD nível a	PD Avig PD	Nível b	PD AP-2	PI	PN	PE
1	[a1,b1,c1,d1]	0.02	0.05	0.7	0.8	0.94414	0.99	0.9346986
2	[a1,b1,c2,d1]	0.02	0.05	0.7	0.8	0.94414	0.99	0.9346986
3	[a1,b1,c3,d1]	0.02	0.05	0.7	0.8	0.94414	0.99	0.9346986
4	[a1,b1,c4,d1]	0.02	0.05	0.7	0.8	0.94414	0.99	0.9346986
5	[a1,b2,c1,d1]	0.02	0.05	0.5	0.8	0.9069	0.99	0.897831
6	[a1,b2,c2,d1]	0.02	0.05	0.5	0.8	0.9069	0.99	0.897831
7	[a1,b2,c3,d1]	0.02	0.05	0.5	0.8	0.9069	0.99	0.897831
8	[a1,b2,c4,d1]	0.02	0.05	0.5	0.8	0.9069	0.99	0.897831
9	[a1,b3,c1,d1]	0.02	0.05	0.6	0.8	0.92552	0.99	0.9162648
10	[a1,b3,c2,d1]	0.02	0.05	0.6	0.8	0.92552	0.99	0.9162648
11	[a1,b3,c3,d1]	0.02	0.05	0.6	0.8	0.92552	0.99	0.9162648
12	[a1,b3,c4,d1]	0.02	0.05	0.6	0.8	0.92552	0.99	0.9162648
13	[a2,b1,c1,d1]	0.05	0.05	0.7	0.8	0.94585	0.99	0.9363915
14	[a2,b1,c2,d1]	0.05	0.05	0.7	0.8	0.94585	0.99	0.9363915
15	[a2,b1,c3,d1]	0.05	0.05	0.7	0.8	0.94585	0.99	0.9363915
16	[a2,b1,c4,d1]	0.05	0.05	0.7	0.8	0.94585	0.99	0.9363915
17	[a2,b2,c1,d1]	0.05	0.05	0.5	0.8	0.90975	0.99	0.9006525
18	[a2,b2,c2,d1]	0.05	0.05	0.5	0.8	0.90975	0.99	0.9006525
19	[a2,b2,c3,d1]	0.05	0.05	0.5	0.8	0.90975	0.99	0.9006525
20	[a2,b2,c4,d1]	0.05	0.05	0.5	0.8	0.90975	0.99	0.9006525
21	[a2,b3,c1,d1]	0.05	0.05	0.6	0.8	0.9278	0.99	0.918522
22	[a2,b3,c2,d1]	0.05	0.05	0.6	0.8	0.9278	0.99	0.918522
23	[a2,b3,c3,d1]	0.05	0.05	0.6	0.8	0.9278	0.99	0.918522
24	[a2,b3,c4,d1]	0.05	0.05	0.6	0.8	0.9278	0.99	0.918522
25	[a3,b1,c1,d1]	0.02	0.05	0.7	0.8	0.94414	0.99	0.9346986
26	[a3,b1,c2,d1]	0.02	0.05	0.7	0.8	0.94414	0.99	0.9346986
27	[a3,b1,c3,d1]	0.02	0.05	0.7	0.8	0.94414	0.99	0.9346986
28	[a3,b1,c4,d1]	0.02	0.05	0.7	0.8	0.94414	0.99	0.9346986
29	[a3,b2,c1,d1]	0.02	0.05	0.5	0.8	0.9069	0.99	0.897831
30	[a3,b2,c2,d1]	0.02	0.05	0.5	0.8	0.9069	0.99	0.897831
31	[a3,b2,c3,d1]	0.02	0.05	0.5	0.8	0.9069	0.99	0.897831
32	[a3,b2,c4,d1]	0.02	0.05	0.5	0.8	0.9069	0.99	0.897831
33	[a3,b3,c1,d1]	0.02	0.05	0.6	0.8	0.92552	0.99	0.9162648
34	[a3,b3,c2,d1]	0.02	0.05	0.6	0.8	0.92552	0.99	0.9162648
35	[a3,b3,c3,d1]	0.02	0.05	0.6	0.8	0.92552	0.99	0.9162648
36	[a3,b3,c4,d1]	0.02	0.05	0.6	0.8	0.92552	0.99	0.9162648

Cenário 2: Ataque Físico + Ataque Cibernético ao sistema de CFTV

Cálculos da Probabilidade de Interrupção (PI) e da Efetividade para os 36 caminhos:

#Caminho	Caminho	PD nível a	PD Avig	PD Nível b	PD AP-2	PI	PN	PE
1	[a1,b1,c1,d1]	0.02	0.05	0.7	0.02	0.726286	0.99	0.719023
2	[a1,b1,c2,d1]	0.02	0.05	0.7	0.02	0.726286	0.99	0.719023
3	[a1,b1,c3,d1]	0.02	0.05	0.7	0.02	0.726286	0.99	0.719023
4	[a1,b1,c4,d1]	0.02	0.05	0.7	0.02	0.726286	0.99	0.719023
5	[a1,b2,c1,d1]	0.02	0.05	0.5	0.02	0.54381	0.99	0.538372
6	[a1,b2,c2,d1]	0.02	0.05	0.5	0.02	0.54381	0.99	0.538372
7	[a1,b2,c3,d1]	0.02	0.05	0.5	0.02	0.54381	0.99	0.538372
8	[a1,b2,c4,d1]	0.02	0.05	0.5	0.02	0.54381	0.99	0.538372
9	[a1,b3,c1,d1]	0.02	0.05	0.6	0.02	0.635048	0.99	0.628698
10	[a1,b3,c2,d1]	0.02	0.05	0.6	0.02	0.635048	0.99	0.628698
11	[a1,b3,c3,d1]	0.02	0.05	0.6	0.02	0.635048	0.99	0.628698
12	[a1,b3,c4,d1]	0.02	0.05	0.6	0.02	0.635048	0.99	0.628698
13	[a2,b1,c1,d1]	0.05	0.05	0.7	0.02	0.734665	0.99	0.727318
14	[a2,b1,c2,d1]	0.05	0.05	0.7	0.02	0.734665	0.99	0.727318
15	[a2,b1,c3,d1]	0.05	0.05	0.7	0.02	0.734665	0.99	0.727318
16	[a2,b1,c4,d1]	0.05	0.05	0.7	0.02	0.734665	0.99	0.727318
17	[a2,b2,c1,d1]	0.05	0.05	0.5	0.02	0.557775	0.99	0.552197
18	[a2,b2,c2,d1]	0.05	0.05	0.5	0.02	0.557775	0.99	0.552197
19	[a2,b2,c3,d1]	0.05	0.05	0.5	0.02	0.557775	0.99	0.552197
20	[a2,b2,c4,d1]	0.05	0.05	0.5	0.02	0.557775	0.99	0.552197
21	[a2,b3,c1,d1]	0.05	0.05	0.6	0.02	0.64622	0.99	0.639758
22	[a2,b3,c2,d1]	0.05	0.05	0.6	0.02	0.64622	0.99	0.639758
23	[a2,b3,c3,d1]	0.05	0.05	0.6	0.02	0.64622	0.99	0.639758
24	[a2,b3,c4,d1]	0.05	0.05	0.6	0.02	0.64622	0.99	0.639758
25	[a3,b1,c1,d1]	0.02	0.05	0.7	0.02	0.726286	0.99	0.719023
26	[a3,b1,c2,d1]	0.02	0.05	0.7	0.02	0.726286	0.99	0.719023
27	[a3,b1,c3,d1]	0.02	0.05	0.7	0.02	0.726286	0.99	0.719023
28	[a3,b1,c4,d1]	0.02	0.05	0.7	0.02	0.726286	0.99	0.719023
29	[a3,b2,c1,d1]	0.02	0.05	0.5	0.02	0.54381	0.99	0.538372
30	[a3,b2,c2,d1]	0.02	0.05	0.5	0.02	0.54381	0.99	0.538372
31	[a3,b2,c3,d1]	0.02	0.05	0.5	0.02	0.54381	0.99	0.538372
32	[a3,b2,c4,d1]	0.02	0.05	0.5	0.02	0.54381	0.99	0.538372
33	[a3,b3,c1,d1]	0.02	0.05	0.6	0.02	0.635048	0.99	0.628698
34	[a3,b3,c2,d1]	0.02	0.05	0.6	0.02	0.635048	0.99	0.628698
35	[a3,b3,c3,d1]	0.02	0.05	0.6	0.02	0.635048	0.99	0.628698
36	[a3,b3,c4,d1]	0.02	0.05	0.6	0.02	0.635048	0.99	0.628698

Cenário 3: Ataque Físico + Ataque Cibernético ao sistema de Controle de Acesso

Cálculos da Probabilidade de Interrupção (PI) e da Efetividade para os 36 caminhos:								
#Caminho	Caminho	PD nível a	PD Avig	PD Nível b	PD AP-2	PI	PN	PE
1	[a1,b1,c1,d1]	0.02	0.05	0	0	0.069	0.99	0.06831
2	[a1,b1,c2,d1]	0.02	0.05	0	0	0.069	0.99	0.06831
3	[a1,b1,c3,d1]	0.02	0.05	0	0	0.069	0.99	0.06831
4	[a1,b1,c4,d1]	0.02	0.05	0	0	0.069	0.99	0.06831
5	[a1,b2,c1,d1]	0.02	0.05	0	0	0.069	0.99	0.06831
6	[a1,b2,c2,d1]	0.02	0.05	0	0	0.069	0.99	0.06831
7	[a1,b2,c3,d1]	0.02	0.05	0	0	0.069	0.99	0.06831
8	[a1,b2,c4,d1]	0.02	0.05	0	0	0.069	0.99	0.06831
9	[a1,b3,c1,d1]	0.02	0.05	0	0	0.069	0.99	0.06831
10	[a1,b3,c2,d1]	0.02	0.05	0	0	0.069	0.99	0.06831
11	[a1,b3,c3,d1]	0.02	0.05	0	0	0.069	0.99	0.06831
12	[a1,b3,c4,d1]	0.02	0.05	0	0	0.069	0.99	0.06831
13	[a2,b1,c1,d1]	0.05	0.05	0	0	0.0975	0.99	0.096525
14	[a2,b1,c2,d1]	0.05	0.05	0	0	0.0975	0.99	0.096525
15	[a2,b1,c3,d1]	0.05	0.05	0	0	0.0975	0.99	0.096525
16	[a2,b1,c4,d1]	0.05	0.05	0	0	0.0975	0.99	0.096525
17	[a2,b2,c1,d1]	0.05	0.05	0	0	0.0975	0.99	0.096525
18	[a2,b2,c2,d1]	0.05	0.05	0	0	0.0975	0.99	0.096525
19	[a2,b2,c3,d1]	0.05	0.05	0	0	0.0975	0.99	0.096525
20	[a2,b2,c4,d1]	0.05	0.05	0	0	0.0975	0.99	0.096525
21	[a2,b3,c1,d1]	0.05	0.05	0	0	0.0975	0.99	0.096525
22	[a2,b3,c2,d1]	0.05	0.05	0	0	0.0975	0.99	0.096525
23	[a2,b3,c3,d1]	0.05	0.05	0	0	0.0975	0.99	0.096525
24	[a2,b3,c4,d1]	0.05	0.05	0	0	0.0975	0.99	0.096525
25	[a3,b1,c1,d1]	0.02	0.05	0	0	0.069	0.99	0.06831
26	[a3,b1,c2,d1]	0.02	0.05	0	0	0.069	0.99	0.06831
27	[a3,b1,c3,d1]	0.02	0.05	0	0	0.069	0.99	0.06831
28	[a3,b1,c4,d1]	0.02	0.05	0	0	0.069	0.99	0.06831
29	[a3,b2,c1,d1]	0.02	0.05	0	0	0.069	0.99	0.06831
30	[a3,b2,c2,d1]	0.02	0.05	0	0	0.069	0.99	0.06831
31	[a3,b2,c3,d1]	0.02	0.05	0	0	0.069	0.99	0.06831
32	[a3,b2,c4,d1]	0.02	0.05	0	0	0.069	0.99	0.06831
33	[a3,b3,c1,d1]	0.02	0.05	0	0	0.069	0.99	0.06831
34	[a3,b3,c2,d1]	0.02	0.05	0	0	0.069	0.99	0.06831
35	[a3,b3,c3,d1]	0.02	0.05	0	0	0.069	0.99	0.06831
36	[a3,b3,c4,d1]	0.02	0.05	0	0	0.069	0.99	0.06831

Cenário 4: Ataque Físico + Ataque Cibernético ao sistema de detecção (Sensores)

Cálculos da Probabilidade de Interrupção (PI) e da Efetividade para os 36 caminhos:

#Caminho	Caminho					PD nível a		PD Avig
PD Nível b	PD AP-2	PI				PN	PE	
1	[a1,b1,c1,d1]	0.02	0.05	0.05	0.8	0.82311	0.99	0.814879
2	[a1,b1,c2,d1]	0.02	0.05	0.05	0.8	0.82311	0.99	0.814879
3	[a1,b1,c3,d1]	0.02	0.05	0.05	0.8	0.82311	0.99	0.814879
4	[a1,b1,c4,d1]	0.02	0.05	0.05	0.8	0.82311	0.99	0.814879
5	[a1,b2,c1,d1]	0.02	0.05	0.05	0.8	0.82311	0.99	0.814879
6	[a1,b2,c2,d1]	0.02	0.05	0.05	0.8	0.82311	0.99	0.814879
7	[a1,b2,c3,d1]	0.02	0.05	0.05	0.8	0.82311	0.99	0.814879
8	[a1,b2,c4,d1]	0.02	0.05	0.05	0.8	0.82311	0.99	0.814879
9	[a1,b3,c1,d1]	0.02	0.05	0.05	0.8	0.82311	0.99	0.814879
10	[a1,b3,c2,d1]	0.02	0.05	0.05	0.8	0.82311	0.99	0.814879
11	[a1,b3,c3,d1]	0.02	0.05	0.05	0.8	0.82311	0.99	0.814879
12	[a1,b3,c4,d1]	0.02	0.05	0.05	0.8	0.82311	0.99	0.814879
13	[a2,b1,c1,d1]	0.05	0.05	0.05	0.8	0.828525	0.99	0.82024
14	[a2,b1,c2,d1]	0.05	0.05	0.05	0.8	0.828525	0.99	0.82024
15	[a2,b1,c3,d1]	0.05	0.05	0.05	0.8	0.828525	0.99	0.82024
16	[a2,b1,c4,d1]	0.05	0.05	0.05	0.8	0.828525	0.99	0.82024
17	[a2,b2,c1,d1]	0.05	0.05	0.05	0.8	0.828525	0.99	0.82024
18	[a2,b2,c2,d1]	0.05	0.05	0.05	0.8	0.828525	0.99	0.82024
19	[a2,b2,c3,d1]	0.05	0.05	0.05	0.8	0.828525	0.99	0.82024
20	[a2,b2,c4,d1]	0.05	0.05	0.05	0.8	0.828525	0.99	0.82024
21	[a2,b3,c1,d1]	0.05	0.05	0.05	0.8	0.828525	0.99	0.82024
22	[a2,b3,c2,d1]	0.05	0.05	0.05	0.8	0.828525	0.99	0.82024
23	[a2,b3,c3,d1]	0.05	0.05	0.05	0.8	0.828525	0.99	0.82024
24	[a2,b3,c4,d1]	0.05	0.05	0.05	0.8	0.828525	0.99	0.82024
25	[a3,b1,c1,d1]	0.02	0.05	0.05	0.8	0.82311	0.99	0.814879
26	[a3,b1,c2,d1]	0.02	0.05	0.05	0.8	0.82311	0.99	0.814879
27	[a3,b1,c3,d1]	0.02	0.05	0.05	0.8	0.82311	0.99	0.814879
28	[a3,b1,c4,d1]	0.02	0.05	0.05	0.8	0.82311	0.99	0.814879
29	[a3,b2,c1,d1]	0.02	0.05	0.05	0.8	0.82311	0.99	0.814879
30	[a3,b2,c2,d1]	0.02	0.05	0.05	0.8	0.82311	0.99	0.814879
31	[a3,b2,c3,d1]	0.02	0.05	0.05	0.8	0.82311	0.99	0.814879
32	[a3,b2,c4,d1]	0.02	0.05	0.05	0.8	0.82311	0.99	0.814879
33	[a3,b3,c1,d1]	0.02	0.05	0.05	0.8	0.82311	0.99	0.814879
34	[a3,b3,c2,d1]	0.02	0.05	0.05	0.8	0.82311	0.99	0.814879
35	[a3,b3,c3,d1]	0.02	0.05	0.05	0.8	0.82311	0.99	0.814879
36	[a3,b3,c4,d1]	0.02	0.05	0.05	0.8	0.82311	0.99	0.814879

ANEXOS

Anexo A: Categorização de Material Nuclear

Tabela extraída da norma CNEN NN-2.01 “Proteção Física de Materiais e Instalações Nucleares”

Material	Forma	Categoria (por massa do material)		
		I	II	III [c]
Plutônio[a]	Não irradiado [b]	Maior ou igual a 2kg	Maior que 500g e menor que 2kg	Maior que 15g e menor ou igual a 500g
Urânio-235	Não irradiado [b]			
	Enriquecido a 20% ou mais em ^{235}U	Maior ou igual a 5kg	Maior que 1kg e menor que 5kg	Maior que 15g e menor ou igual a 1kg
	Enriquecimento igual ou superior a 10%, porém inferior a 20% em ^{235}U	X	Maior ou igual a 10kg	Maior que 1kg e menor que 10kg
	Enriquecimento acima do natural, mas abaixo de 10% em ^{235}U	X	X	Maior ou igual a 10kg
Urânio-233	Não irradiado [b]	Maior ou igual a 2kg	Maior que 500 g e menor que 2kg	Maior que 15g e menor ou igual a 500g
Combustível Irradiado	X	X	Urânio natural ou exaurido, tório ou combustível de baixo enriquecimento (menos de 10% de conteúdo físsil)[d][e]	X
Outros materiais protegidos[f]				

(a) Todo plutônio, excetuando-se aquele de concentração isotópica superior a 80% de ^{238}Pu.
(b) Material nuclear não irradiado em reator ou material irradiado em reator com nível de radiação inferior a 1Gy/h (100 rad/h) a 1 metro de distância, sem blindagem.
(c) Quantidades não classificadas como Categoria III e o urânio natural e tório deverão ser protegidas conforme práticas prudentes de gestão e de engenharia.
(d) O material poderá ser reavaliado e reclassificado pela CNEN, sob circunstâncias específicas.
(e) Outros tipos de combustível que, em virtude de seu conteúdo físsil, sejam classificados como Categoria I ou II antes de serem irradiados poderão ter a categoria reduzida em um nível, a critério da CNEN, caso seu nível de radiação exceda 1Gy/h (100 rad/h) a 1 metro de distância, sem blindagem.
(f) Serão categorizados a critério da CNEN, analisando-se cada caso.

Anexo B: Dados de Probabilidades de Detecção

Tabelas extraídas de [1], [22] e [32]

Tabela B-1. Probabilidades de detecção de sensores de intrusão

Component Type	Component Description	No Equipment P(D)	Hand Tools P(D)	Power Tools P(D)	High Explosives P(D)	Land Vehicle P(D)
Exterior Sensors	Seismic Buried Cable	0.5	0.5	0.5	0.5	0.9
	Electric field	0.5	0.3	0.3	0.5	0.9
	Infrared	0.8	0.4	0.4	0.5	0.8
	Microwave	0.8	0.7	0.7	0.7	0.9
	Video motion	0.8	0.6	0.6	0.7	0.9
	Multiple non-complementary	0.9	0.8	0.8	0.8	0.99
	Multiple complementary	0.99	0.95	0.95	0.99	0.99
Interior Sensors	Sonic	0.5	0.5	0.5	0.5	N/A
	Capacitance	0.5	0.5	0.5	0.5	N/A
	Video Motion	0.5	0.5	0.5	0.5	N/A
	Infrared	0.5	0.5	0.5	0.5	N/A
	Ultrasonic	0.5	0.5	0.5	0.5	N/A
	Microwave	0.5	0.5	0.5	0.5	N/A
	Multiple non-complementary	0.75	0.75	0.75	0.75	N/A
	Multiple complementary	0.9	0.9	0.9	0.9	N/A
Position Sensors	Position Switch	0.5	0.2	0.2	0.2	N/A
	Balanced Magnetic Switch	0.8	0.8	0.8	0.8	N/A
Fence Sensors	Taut Wire	0.5	0.25	0.25	0.75	0.85
	Vibration	0.5	0.1	0.1	0.75	0.85
	Strain	0.1	0.1	0.1	0.1	0.9
	Electric Field	0.5	0.4	0.4	0.75	0.9
	Multiple Sensors	0.75	0.5	0.5	0.8	0.9
Barrier Sensors	Vibration	0.9	0.4	0.4	0.9	N/A
	Glass Breakage	0.9	0.6	0.6	0.9	N/A
	Conducting Tape	0.8	0.2	0.2	0.9	N/A
	Grid Mesh	0.9	0.6	0.6	0.95	N/A
	Multiple Sensors	0.99	0.9	0.9	0.99	N/A
Helicopter Detector	Radar	0.1				
	Sonic	0.1				

Tabela B-2. Detecção em controles de acesso.

Component Type	Component Description	Independent P(D)	Land Vehicle P(D)
ID Verification	Casual Recognition	0.02	
	Credential	0.05	
	Credential and PIN	0.35	
	Picture Badge	0.1	
	Picture Badge and PIN	0.6	
	Exchange picture badge	0.5	
	Exchange picture badge and PIN	0.8	
	Retinal scan and PIN	0.99	
	Hand geometry and PIN	0.95	
	Speech pattern and PIN	0.95	
	Signature dynamics and PIN	0.95	
	Fingerprint and PIN	0.95	
Personnel Access Authorization Check	General observation of authorization	0.1	
	Authorization verification each time location is accessed	0.6	
Two Person Rule	Presence in area	0	
	Within sight	0.1	
	Dedicated observation	0.5	
	Dedicated observation with alarm	0.95	
Vehicle Authorization Check	Authorization form check		0.35
	Serial number verification		0.45
	Visual check of insignia/ license plate		0.15

Tabela B-3. Detecção em vigilância humana.

Component Type	Component Description	No Equipment P(D)	Small Arms P(D)	Light Antitank Weapons (LAW) P(D)	Independent of threat attribute P(D)
SO at Post Observation	Duress, LAW protected	0.8	0.8	0.8	
	Duress, small arms protected	0.8	0.8	0.45	
	Duress, small arms protected: LAW protected on alert	0.8	0.8	0.45	
	Duress, unprotected	0.8	0.45	0.45	
	Duress, unprotected: LAW protected position on alert	0.8	0.45	0.45	
	Duress, unprotected: small arms protected position on alert	0.8	0.45	0.45	
	No duress, LAW protected	0.8	0.8	0.45	
	No duress, small arms protected	0.8	0.45	0.45	
	No duress, small arms protected: LAW protected position on alert	0.8	0.45	0.45	
	No duress, unprotected	0.8	0	0	
	No duress, unprotected: LAW protected position on alert	0.8	0	0	
	No duress, unprotected: small arms protected on alert	0.8	0	0	
SO in Tower Observation	LAW resistant tower	0.05	0.05	0.02	
	Small arms resistant	0.05	0.05	0.02	
SO on Patrol	Random				0.02
	Scheduled				0.01
General Observation	Personnel always in vicinity				0.02
	Personnel generally in vicinity				0.01

Tabela B-4. Detecção em medidas e equipamentos contra roubo de material, para diferentes atributos de ameaça.

		Threat Attribute						
Component Type	**Component Description**	**No Equipment P(D)**	**Hand Tools P(D)**	**Power Tools P(D)**	**High Explosives P(D)**	**Metal Contraband P(D)**	**Small Arms P(D)**	**Radioactive Contraband P(D)**
Explosives Detector	Animal Olfaction	0			0.1			
	Handheld vapor collection	0			0.45			
	Thermal Neutron	0			0.25			
	Vapor Collection	0			0.35			
Handheld Metal Detector	Ferrous and solid lead materials	0	0.85	0.75		0.25	0.5	
	Ferrous materials and all forms of lead	0	0.85	0.75		0.25	0.5	
	Ferrous materials only	0	0.85	0.75		0.25	0.5	
Item Search	Cursory	0	0.1	0.1	0.1			0.1
	Rigorous	0	0.75	0.75	0.45			0.65
Personnel Search	Pat down	0	0.9	0.9	0.3			0.9
	Strip inspection	0	0.9	0.9	0.9			0.9
Portal Metal Detector	Ferrous and solid lead materials	0	0.9	0.9		0.8	0.6	
	Ferrous materials and all forms of lead	0	0.9	0.9		0.8	0.6	
	Ferrous materials only	0	0.9	0.9		0.8	0.6	
Vehicle Search	Cursory	0	0.1	0.1	0.1			0.1
	Rigorous including cargo	0	0.5	0.5	0.25			0.4
X-Ray Inspection	Standard	0	0.9	0.9			0.6	0.9
Drive thru	Plastic	0						0.5

Anexo C: Dados de Retardo de Componentes

Tabelas extraídas de [1], [22] e [32]

Tabela C-1. Tempo de retardo conforme as classes de barreiras físicas.

Component Type	Component Description	No Equipment (sec)	Hand Tools (sec)	Power Tools (sec)	Explosives (sec)		Land Vehicle (sec)
					Stage 1	Stage 2	
Walls	60 cm reinforced concrete wall	Infinite	Infinite	900	180	300	Infinite
	30 cm reinforced concrete wall	Infinite	Infinite	840	120	54	N/A
	20 cm reinforced concrete wall	Infinite	Infinite	600	120	0	N/A
	Wood studs and sheetrock	60	30	30	30	0	N/A
Doors	60 cm steel and concrete rolling door	Infinite	Infinite	930	200	300	N/A
	30 cm steel and concrete rolling door	Infinite	Infinite	640	160	54	N/A
	30 cm wood door with metal sheeting	Infinite	Infinite	530	160	30	N/A
	10 cm wood door with metal sheeting	Infinite	300	180	30	0	5 for large vehicle door
	5 cm wood door	Infinite	12	12	12	0	N/A
	5 cm wood door with glass panel	Infinite	12	12	12	0	N/A
	.75 cm steel plate door	Infinite	300	30	30	0	N/A
	Class V or VI vault door	Infinite	480	60	60	0	N/A
	Steel turnstile	Infinite	72	18	18	0	N/A
Miscellaneous Barriers	High security padlock	Infinite	90	60	30	0	N/A
	Concrete Block Vehicle Barrier	0	300	300	30	0	5
	2.5 m chain link mesh fence	10	10	10	10	0	1
	Welded wire fabric fence	10	10	10	10	0	1
	2.5 m concrete panel wall	10	10	10	10	0	N/A
	Tempered glass window	5	5	5	5	5	N/A
	Electromagnetic Strike Lock	15	10	5	5	2	N/A

Tabela C-2. Tempos de retardo ocasionados por agentes de segurança (SO).

Component Type	Component Description	No Equipment (sec)	Small Arms (sec)	Light Antitank Weapons (LAW) (sec)
SO at Post Delay	Unprotected post	30000	0	0
	Small arms protected post	30000	30	0
	Unprotected post normally but moves to small arms protected position on alert	30000	30	0
	LAW protected post	30000	125	125
	Unprotected post normally but moves to LAW protected position on alert	30000	125	125
	Small arms protected post normally, but moves to LAW protected position on alert	30000	125	125
SO in Tower Delay	Small arms resistance	60	30	0
	LAW resistant tower	125	125	60

Tabela C-3. Tempos para penetração em cercas.

Barrier Description	*Penetration Equipment*	*Equipment Weight (kg)*	*Penetration Time (Minutes)* Min.	Mean	Max.	Standard Deviation
2.5-m chain-link mesh with outriggers 4-mm x 50-mm mesh	Ladder	5.0	0.1	0.2	0.3	0.04
	Tarpaulin	2.0	0.1	0.2	0.3	0.04
	Pliers	1.0	1.0	2.0	3.0	0.41
	Manual bolt cutters	3.0	0.5	1.0	1.5	0.20
	Circular saw	10	0.5	1.0	1.5	0.20
	Manual bolt cutters, gloves (more cuts)	3.5	0.75	1.5	2.25	0.31
	Circular saw (more cuts)	11.0	0.75	1.5	2.25	0.31
	Gloves	0.5	0.1	0.2	0.3	0.04
Vinyl-coated 3-mm x 50-mm mesh	Manual bolt cutters	3.0	0.5	1.0	1.5	0.20
	Pliers	1.0	1.0	2.0	3.0	0.41
	Circular Saw	11.0	0.75	1.5	2.25	0.31
2.5-m chain-link mesh without outriggers vinyl-coated, 1.8-mm x 40-mm mesh	Ladder	5.0	0.1	0.2	0.3	0.04
	No equipment	0.0	0.05	0.10	0.15	0.02
	Manual bolt cutters	3.0	0.5	1.0	1.5	0.20
	Pliers	0.5	1.0	2.0	3.0	0.41
	Vise grip pliers	0.5	0.30	0.60	0.90	0.12

Tabela C-4. Tempos para penetração em portões.

Chain-link mesh pipe 2.4-m x 4-m chain-link gate on metal pipe frame, chained and padlocked	Truck	1,500	0.05	0.1	0.15	0.02
	Pliers	1.0	1.0	2.0	3.0	0.41
Chain-link mesh pipe 1.2-m x 2.4-m gate, 11-gauge x 5-cm mesh on 4.8-cm metal pipe frame, chained and padlocked	Sledgehammer	5	0.5	1.0	1.5	0.20
	1.8-m pry bar	10	1.0	2.0	3.0	0.41
	Bolt cutters	3	0.75	1.5	2.25	0.31
	Hacksaw	0.2	1.0	2.0	3.0	0.41

Tabela C-5. Tempos para penetração em paredes.

Barrier Description	*Penetration Equipment*	*Equipment Weight (kg)*	*Penetration Time (Minutes)* *Min.*	*Mean*	*Max.*	*Standard Deviation*
Concrete-10 cm Thick, Reinforced Concrete-210 kg/cm^2 one layer, 6.4-mm dia., 15-cm x 15-cm mesh	Sledgehammer, hand bolt cutters	10	2.0	4.0	6.0	0.82
	Sledgehammer, cutting torch	30	2.5	5.0	7.5	1.02
	Circular saw, sledge-hammer	5	4.3	8.6	12.9	1.76
	Rotohammer, chisel, punch, sledgehammer, hand bolt cutters, generator	50	3.2	6.4	9.6	0.57
	Explosives (1.0), sledgehammer, manual bolt cutters	20	2.3	3.5	5.25	
	Explosives (3.0), hand bolt cutters	10	1.2	2.5	3.7	
	Explosives (5.0), hand bolt cutters	7	1.2	2.3	3.4	
	Explosive (10)	10	1.0	2.0	3.0	
	Sledgehammer, hand hydraulic bolt cutters	20	2.4	4.8	7.2	0.98
Concrete- 210 kg/cm2 one layer No. 5 rebar, 15-cm centers	Sledgehammer, cutting torch	30	2.0	4.0	6.0	0.82
	Rotohammer, chisel, hand hydraulic bolt cutters, generator	50	3.9	7.8	11.7	1.59

Tabela C-5. Tempos para penetração em paredes (cont.)

Concrete- 15cm Thick, Reinforced Concrete-210 kg/cm² one layer, No. 4 rebar, 20-cm centers	Sledgehammer, hand bolt cutters	15	4.0	8.0	12.0	1.63
	Explosives (1.0), sledgehammer, hand bolt cutters	14	2.5	3.7	5.6	
	Explosives (3.0), hand bolt cutters	5	1.9	2.9	4.3	
	Explosives (5.0), hand bolt cutters	7	1.7	2.5	3.8	
Concrete-20 cm Thick, Reinforced Concrete-210 kg/cm² one layer, No. 5 rebar, 15-cm centers	Rotohammer, drill, sledge, chisel, punch, cutting torch, generator	65	7.0	14.0	21.0	2.86
	Explosives (2.0), sledgehammer, hand hydraulic bolt cutters	30	4.3	6.5	9.7	
	Explosives (3.0), hand hydraulic bolt cutters	20	2.5	3.75	5.6	
	Explosives (5.0), hand hydraulic bolt cutters	22	2.5	3.75	5.6	
	Explosives (1.2)	12	1.5	3.0	4.5	
Concrete-30 cm Thick, Reinforced Concrete- 210 kg/cm² one layer, No. 4 rebar, 15-cm centers	Explosives (5.0), hand bolt cutters	8	2.2	3.25	4.9	
	Explosives (7), hand bolt cutters	9	2.3	3.5	5.2	
	Explosives (1.2), hand bolt cutters	14	2.5	3.8	5.6	
	Explosives (16), hand bolt cutters	18	2.5	3.8	5.6	
Concrete-46 cm Thick, Reinforced Concrete-350 kg/cm2 two layers, No. 4 rebar, 15-cm centers	Explosives (16), hand-held power hydraulic bolt-cutters, generator	28.2	5.0	7.5	11.2	1.22
	Explosives (20), hand bolt cutters	22	2.5	5.0	7.5	
Concrete- 60 cm Thick, Reinforced Concrete-350 kg/cm² four layers, No. 6 rebar, 15-cm centers	Explosives (30), gas-powered hydraulic bolt cutters	59	7.3	11.0	16.5	

Tabela C-6. Tempos para penetração em portas.

Barrier Description	*Penetration Equipment*	*Equipment Weight (kg)*	*Penetration Time (Minutes)* Min.	Mean	Max.	*Standard Deviation*
Sheet Metal Standard industrial pedestrian door, 1.6-mm metal, panic hardware, cylinder lock, rim set, butt hinges with removable pins	Explosives (1.0)	1	1.25	1.9	2.8	
	Sledgehammer, cutting torch, burn bar, fire resistant suit	171	1.6	3.2	4.8	0.65
	Cordless drill	2.7	1.5	3.0	4.5	0.61
	Pry bar	7	0.1	0.2	0.3	0.41
	Fire ax	4.5	1.9	3.8	5.7	0.78
	Hammer, suction cups, punch, chisel	4	1.0	2.0	3.0	0.41
	Suction cups, sledge, cutting torch	25	0.5	1.0	1.5	0.20
	Explosives (.5)	2.5	1.2	2.5	3.2	
	Lock picking tools	0.2	0.10	2.5	5.0	1.0
	Pipe wrench	1	0.2	1.2	2.5	
	Explosives (2.0)	2.0	1.2	2.5	3.7	
Standard industrial pedestrian door, hollow steel 1.6-mm narrow glass one side, louvers near bottom.	Hammer	2.0	0.15	0.3	0.45	0.06
	Fire ax	4.5	0.80	1.6	2.40	0.33

Tabela C-6. Tempos para penetração em portas (cont.).

Barrier Description	*Penetration Equipment*	*Equipment Weight (kg)*	*Penetration Time (Minutes)* Min.	Mean	Max.	Standard Deviation
Sheet Metal Standard industrial pedestrian door, 1.3-mm half glass expanded metal 2.8-mm grill	Grappling hook, wire cable, truck	1,520	0.3	0.6	0.9	0.12
	Manual bolt cutters	4.5	0.5	1.0	1.5	0.20
Standard industrial vehicle door, hollow steel panel, 1.6-mm	Explosives (0.5)	0.5	0.75	1.1	1.7	
	Sledgehammer, cutting torch, burn bar, fire-resistant suit, water	385	0.80	1.6	2.4	0.33
	Sledgehammer, cutting torch, fire-resistant gloves, water	275	1.5	3.0	4.5	0.61
	Truck	2,025	0.3	0.6	0.9	0.12
	Pry bar, wooden plank	9	.75	1.5	2.25	0.31
	Fire ax	4.5	1.1	2.2	3.3	0.45
	Explosives (1.0)	1.0	1.25	1.9	2.8	
Standard 10cm wooden vehicle door, with 1.6-mm sheeting	Explosives (1.0)	0.5	0.8	1.3	1.9	
	Sledgehammer, cutting torch, burn bar, fire-resistant suit, water	385	1.0	2.0	3.0	0.41
	Sledgehammer, cutting torch, burn bar, fire-resistant suit	171	0.65	1.3	1.95	0.27

Tabela C-6. Tempos para penetração em portas (cont.).

Barrier Description	*Penetration Equipment*	*Equipment Weight (kg)*	*Penetration Time (Minutes)*			
			Min.	*Mean*	*Max.*	*Standard Deviation*
Sheet Metal	Truck	2,025	0.35	0.7	1.05	0.14
	Pry bar, wooden plank	9	1.0	2.0	3.0	0.41
	Fire ax	4.5	1.1	2.2	3.3	0.45
	Explosives (1.0)	1.0	1.3	1.9	2.8	
Steel Plate Magazine door, 6.4-mm steel plate, one padlock	Explosives, linear shaped charge (0.5)	0.5	1.1	1.7	2.0	
	Sledge hammer, cutting torch, fire-resistant gloves, water	248	2.0	4.0	6.0	0.82
	Circular Saw	16	2.1	4.2	6.3	0.86
	Suction cups, sledge-hammer, chisel	4.5	0.6	1.2	1.8	0.24
	Sledgehammer, cutting torch, burn bar, fire-resistant suit, water	385	1.25	2.5	3.75	0.51
Steel Plate/Void/Steel Plate Heavy door with two large-hinged hasps for padlocking, 19-mm steel, 10-cm air space, 1.3-mm	Explosives (4)	10	1.3	1.9	2.8	
	Sledgehammer, cutting torch, burn bar, fire-resistant suit, water	385	3.1	6.2	9.3	1.27
	Sledgehammer, cutting torch, burn bar, fire-resistant gloves	165	0.3	0.6	0.9	0.12

Tabela C-7. Taxas de corte em barras metálicas de grades com alicate de corte padrão de 1m.

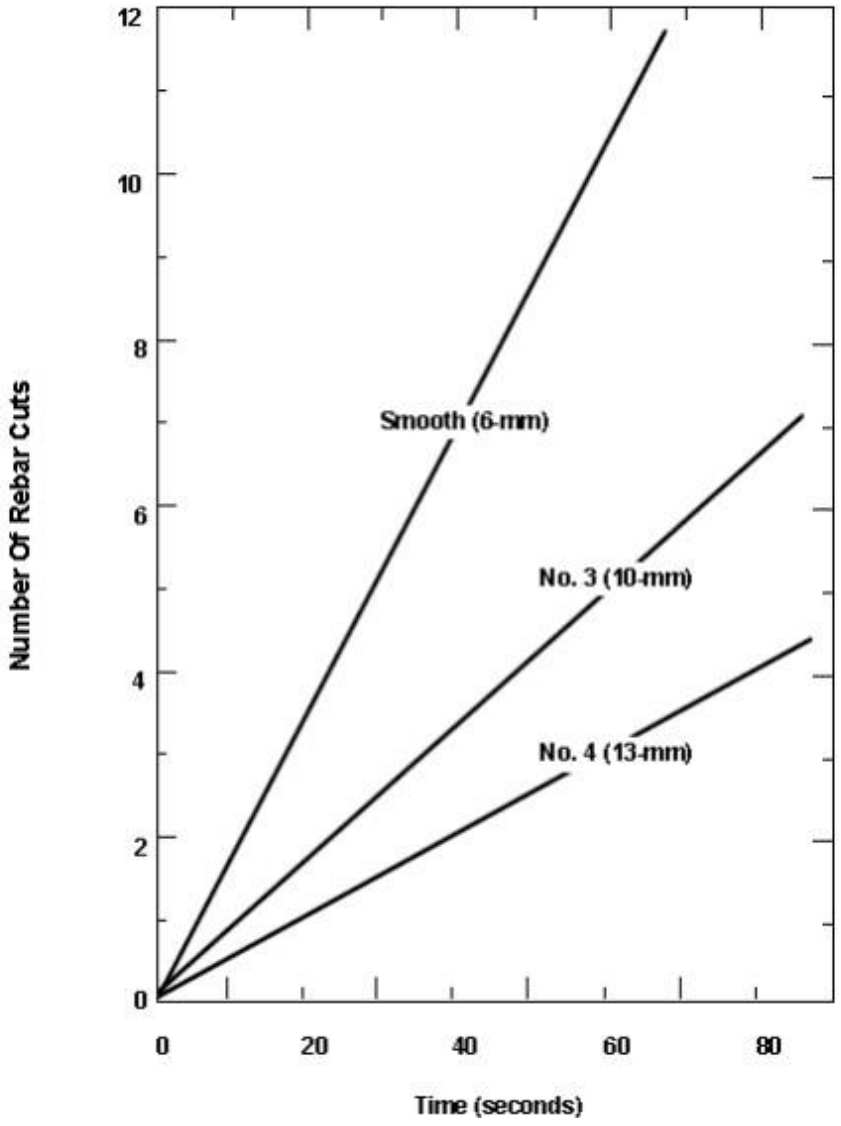


Tabela C-8. Tempo necessário para montar pacotes de explosivos em função da massa do pacote.

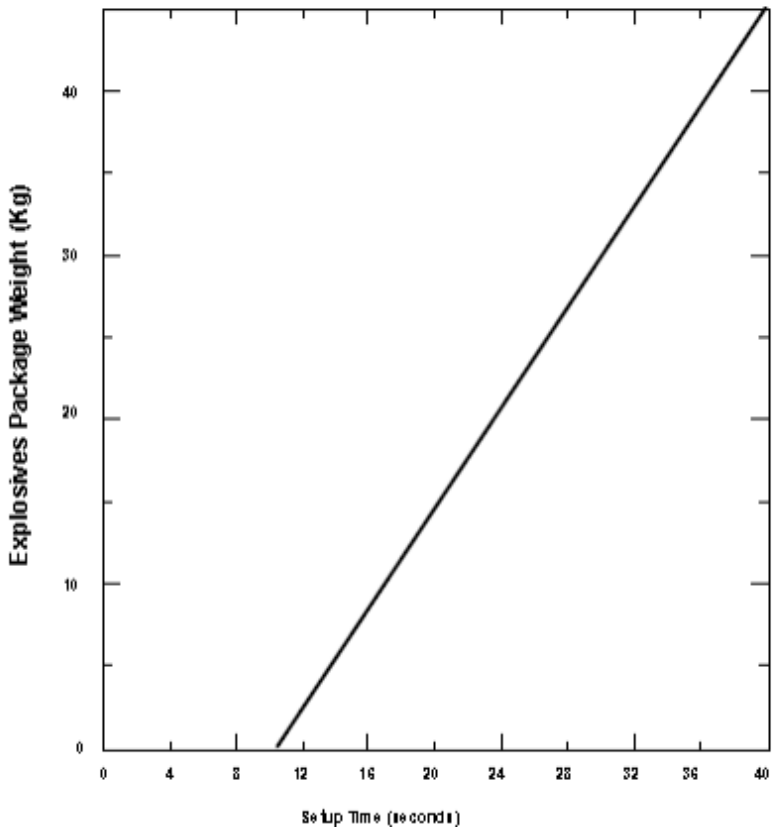


Tabela C-9. Taxas de corrida para diferentes tipos de pisos e diferentes tipos de cargas.

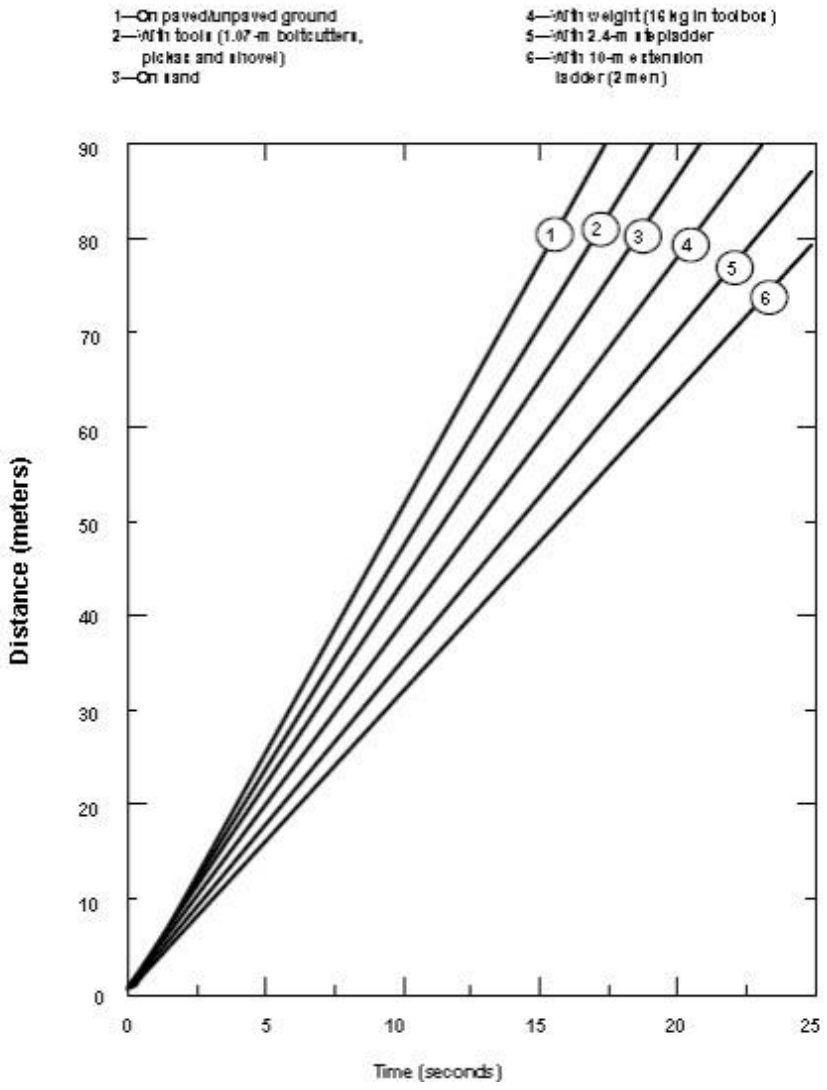
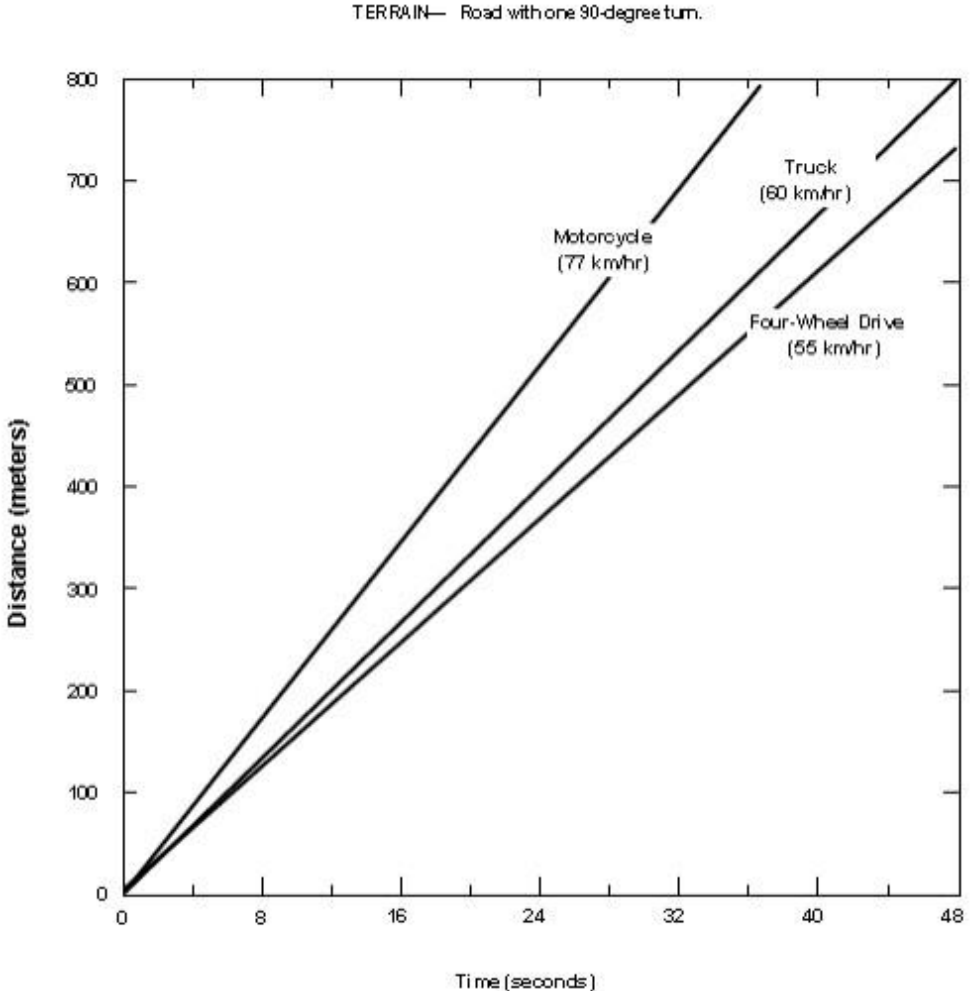


Tabela C-10. Distâncias para diferentes tipos de veículos (motoristas experientes) em estrada com curvas de 90°.



Anexo D: Dados de Neutralização

Tabela D-1. Probabilidade de Neutralização em função do número de adversários e da força de resposta, considerando iguais equipamentos e armamento para ambos.

Probability of Neutralization for Different Numbers of Adversaries and Responders

Number of Adversaries \ Number of Responders	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	0.50	0.83	0.96	0.99	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
2	0.17	0.50	0.78	0.92	0.98	0.99	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
3	0.04	0.23	0.50	0.74	0.89	0.96	0.99	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
4	0.01	0.08	0.26	0.50	0.72	0.86	0.94	0.98	0.99	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
5	0.00	0.02	0.11	0.28	0.50	0.70	0.84	0.92	0.97	0.99	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
6	0.00	0.01	0.04	0.14	0.30	0.50	0.68	0.82	0.91	0.96	0.98	0.99	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
7	0.00	0.00	0.01	0.06	0.16	0.32	0.50	0.67	0.81	0.90	0.95	0.98	0.99	1.00	1.00	1.00	1.00	1.00	1.00	1.00
8	0.00	0.00	0.00	0.02	0.08	0.18	0.33	0.50	0.66	0.79	0.88	0.94	0.97	0.99	0.99	1.00	1.00	1.00	1.00	1.00
9	0.00	0.00	0.00	0.01	0.03	0.09	0.19	0.34	0.50	0.65	0.78	0.87	0.93	0.96	0.98	0.99	1.00	1.00	1.00	1.00
10	0.00	0.00	0.00	0.00	0.01	0.04	0.10	0.21	0.35	0.50	0.65	0.77	0.86	0.92	0.96	0.98	0.99	1.00	1.00	1.00