UNIVERSIDADE FEDERAL FLUMINENSE

ANDREI MANTESSO COIMBRA

IDENTIFICAÇÃO DE CRITICALIDADES DE RAMOS E DE VULNERABILIDADES DA ESTIMAÇÃO DE ESTADO A ERROS GROSSEIROS E ATAQUES CIBERNÉTICOS

NITERÓI

2026

ANDREI MANTESSO COIMBRA

IDENTIFICAÇÃO DE CRITICALIDADES DE RAMOS E DE VULNERABILIDADES DA ESTIMAÇÃO DE ESTADO A ERROS GROSSEIROS E ATAQUES CIBERNÉTICOS

Tese apresentada ao Programa de Pós-Graduação em Computação da Universidade Federal Fluminense como requisito parcial para a obtenção do Grau de Doutor em Computação. Área de concentração: Ciência da Computação

Orientadores:
Prof. Dr. Julio Cesar Stacchini de Souza

Prof. Dr. Milton Brown Do Coutto Filho

NITERÓI

2026

Ficha catalográfica automática - SDC/BCPV
Gerada com informações fornecidas pelo autor

C652i Coimbra, Andrei Mantesso
Identificação de Criticalidades de Ramos e de Vulnerabilidades da Estimação de Estado a Erros Grosseiros e Ataques Cibernéticos / Andrei Mantesso Coimbra. - 2026.
131 f.: il.

Orientador: Julio Cesar Stacchini de Souza.
Coorientador: Milton Brown Do Coutto Filho.
Tese (doutorado)-Universidade Federal Fluminense, Instituto de Computação, Niterói, 2026.

1. Estimação de estado. 2. Análise de observabilidade. 3. Criticalidades. 4. Cibersegurança. 5. Produção intelectual. I. Souza, Julio Cesar Stacchini de, orientador. II. Do Coutto Filho, Milton Brown, coorientador. III. Universidade Federal Fluminense. Instituto de Computação. IV. Título.

CDD - XXX

Bibliotecário responsável: Debora do Nascimento - CRB7/6368

ANDREI MANTESSO COIMBRA

IDENTIFICAÇÃO DE CRITICALIDADES DE RAMOS E DE VULNERABILIDADES DA ESTIMAÇÃO DE ESTADO A ERROS GROSSEIROS E ATAQUES CIBERNÉTICOS

Tese apresentada ao Programa de Pós-Graduação em Computação da Universidade Federal Fluminense como requisito parcial para a obtenção do Grau de Doutor em Computação. Área de concentração: Ciência da Computação

Aprovada em 23 de setembro de 2026.

BANCA EXAMINADORA

Prof. Dr. Julio Cesar Stacchini de Souza - Orientador, UFF

Prof. Dr. Milton Brown Do Coutto Filho - Orientador, UFF

Prof. Dr. José Viterbo Filho, Universidade Federal Fluminense - UFF

Prof. Dr. Vitor Hugo Ferreira, Universidade Federal Fluminense - UFF

Prof. Dr. Edimar José de Oliveira, Universidade Federal de Juiz de Fora - UFJF

Prof. Dr. João Bosco Augusto London Junior, Universidade de São Paulo - USP/SC

Niterói

2026

Considerações Éticas

Declaração de Considerações Éticas

Esta pesquisa é de natureza metodológica e computacional. Não envolveu experimentos com seres humanos, sistemas implantados em operação nem dados pessoais ou sensíveis. As simulações foram realizadas exclusivamente com os sistemas-teste IEEE de 14, 30, 118 e 300 barras, de domínio público, e com planos de medição publicados na literatura ou elaborados pelo autor; não foram utilizados dados operacionais de empresas do setor elétrico.

Declaração de Uso de IA Generativa

Em atendimento à Portaria CNPq nº 2.664, de 6 de março de 2026, e às Diretrizes sobre Ética e Uso de IA Generativa do PGC/IC-UFF, declara-se o uso das seguintes ferramentas de Inteligência Artificial Generativa:

a) **Revisão bibliográfica.** NotebookLM (Google), versão gratuita para *web*, utilizada de 30 de outubro de 2025 a 31 de julho de 2026, e Claude (Anthropic), nas versões indicadas no item b: apoio à leitura, à síntese e à organização dos artigos que compõem a revisão de literatura. As sínteses produzidas não substituíram a leitura das referências citadas.

b) **Preparação do manuscrito.** Claude (Anthropic), plano pago, utilizado a partir de 13 de julho de 2026, sempre na versão mais recente disponível: modelos da família Claude Opus (até o Claude Opus 5.5) e, quando disponível, o Claude Fable. Finalidades: revisão gramatical e ortográfica; padronização terminológica e de notação; sugestões de reescrita para clareza e coesão; tradução inicial do Resumo para o inglês (Abstract); apoio na incorporação das correções solicitadas pela banca examinadora, incluindo sugestões de redação de trechos pontuais a partir das indicações do autor; conferência das referências cruzadas, da correspondência entre as afirmações e as referências citadas e da formatação das referências bibliográficas; e apoio na edição do código LaTeX.

c) **Implementação computacional.** Claude Code (Anthropic), com o modelo Claude Sonnet 5: conversão para a linguagem Python de rotinas originalmente implementadas em MATLAB pelo autor. Os resultados produzidos pelas rotinas convertidas foram verificados por comparação com os obtidos na implementação original.

Todas as sugestões foram avaliadas individualmente pelo autor, a quem coube a decisão sobre sua incorporação e a redação final. O conteúdo intelectual — concepção da pesquisa, formulação do problema, desenvolvimento metodológico, análise dos resultados e conclusões — foi produzido de maneira autoral e submetido a curadoria crítica, sendo o resultado final de inteira responsabilidade do autor.

Dedico este trabalho à minha esposa, Luana, pelo apoio durante estes anos, e ao meu filho Benício, por todas as vezes que ele se esforçou para entender que eu não podia brincar com ele por estar trabalhando na tese. Saiba, filho, que essa troca me custou muito.

Agradecimentos

Depois de alguns anos dedicados a este trabalho, começo agradecendo a Deus pela oportunidade de estudar algo de que tanto gosto. Diante da distância que sempre nos separou dos grandes centros, cursar um mestrado e, agora, um doutorado nessa área um dia pareceu um objetivo distante.

Agradeço aos meus pais, que sempre acreditaram que eu poderia trilhar caminhos que eles próprios não puderam trilhar.

Aos meus orientadores, pelos saberes compartilhados e compreensão ao longo de todo o percurso. Durante o doutorado, atravessei mudanças pessoais que me afastaram temporariamente da pesquisa, e eles souberam compreender esses momentos com generosidade.

Aos colegas do grupo de pesquisa, pelo companheirismo constante; em especial, a Ayres Nishio, cuja contribuição foi fundamental para este trabalho.

Por fim, e de modo muito especial, agradeço à minha família: Luana, minha esposa, e Benício, meu filho, que nasceu durante o doutorado. Foram eles que mais sentiram minha ausência – e, ao mesmo tempo, foram eles minha maior motivação para persistir.

Resumo

A Estimação de Estado (EE) fornece às demais funções dos Centros de Operação do Sistema a estimativa do estado da rede elétrica, essencial para a realização de análises e tomada de decisão sobre ações de controle. A ocorrência de situações adversas pode ameaçar a observabilidade da rede e a capacidade de depuração de Erros Grosseiros pela EE, consequentemente comprometendo a qualidade e a confiabilidade dos resultados obtidos. Tais adversidades estão relacionadas a condições críticas às quais o estimador pode estar submetido, sendo influenciadas pela topologia da rede e plano de medição utilizado. A verificação da condição de observabilidade, quando considerada isoladamente, produz uma resposta binária — o sistema é ou não é observável — e não detalha as vulnerabilidades da EE. Conhecer as criticalidades associadas aos ramos da rede e às medidas é importante para identificar vulnerabilidades para a EE, o que pode subsidiar decisões quanto a reforços no sistema de medição para mitigar os efeitos de eventos como erros grosseiros nas medidas ou ataques cibernéticos. No entanto, a identificação de criticalidades, sobretudo as de maior cardinalidade, requer a solução de um problema combinatório e computacionalmente oneroso. As criticalidades de ramos estão fortemente correlacionadas com as criticalidades de medidas. No entanto, trabalhos voltados para a sua identificação são muito raros na literatura. Nesse sentido, este trabalho desenvolve um método eficiente para a obtenção das criticalidades de ramos e, a partir delas, as criticalidades de medidas e de Unidades de Medição (UM). A contribuição metodológica desta tese é a transformação do problema de identificação de criticalidades de ramos, de natureza topológica e estrutural, em um problema de identificação de criticalidades de medidas em um sistema de medição hipotético, composto por uma medida de fluxo de potência em cada ramo, o que permite a aplicação de métodos numéricos eficientes e paralelizáveis. A partir das criticalidades de ramos, pode-se obter as criticalidades de UMs diretamente, e as criticalidades de medidas, em um número de combinações reduzido. É apresentada também uma metodologia para, a partir do conhecimento das criticalidades de ramos, identificar aqueles que devem ser protegidos para preservar a observabilidade da rede em caso de ataques cibernéticos que comprometam UMs e tornem indisponíveis as suas medidas (ataques à disponibilidade, como os de negação de serviço), além de indicar o que deve

ser reforçado no sistema de medição para atingir tal objetivo. A eficácia e eficiência das metodologias propostas são discutidas a partir de resultados de simulações empregando os sistemas IEEE 14-, 30-, 118- e 300-barras.

Palavras-chave: Estimação de estado; Análise de observabilidade; Criticalidades; Cibersegurança.

Abstract

State Estimation (SE) provides the other functions of System Operation Centers with the estimate of the power network state, which is essential for performing analyses and making decisions on control actions. The occurrence of adverse situations may threaten network observability and the ability of SE to process gross errors, consequently compromising the quality and reliability of the results obtained. Such adversities are related to critical conditions to which the estimator may be subjected, being influenced by the network topology and the metering plan in use. Verifying the observability condition, when considered in isolation, yields a binary answer — the system is either observable or not — and does not detail the vulnerabilities of SE. Knowing the criticalities associated with network branches and measurements is important to identify vulnerabilities of SE, which can support decisions regarding metering system reinforcements to mitigate the effects of events such as gross measurement errors or cyberattacks. However, the identification of criticalities, especially those of higher cardinality, requires solving a combinatorial and computationally expensive problem. Branch criticalities are strongly correlated with measurement criticalities; nevertheless, works devoted to their identification are very rare in the literature. In this context, this work develops an efficient method for obtaining branch criticalities and, from them, the criticalities of measurements and of measurement units. The methodological contribution of this thesis is the transformation of the problem of identifying branch criticalities, of topological and structural nature, into a problem of identifying measurement criticalities in a hypothetical metering system, composed of one power flow measurement on each branch, which allows the application of efficient and parallelizable numerical methods. From the branch criticalities, the criticalities of measurement units can be obtained directly, and the measurement criticalities, through a reduced number of combinations. A methodology is also presented to, based on the knowledge of branch criticalities, identify those branches that must be protected to preserve network observability in the event of cyberattacks that compromise measurement units and make their measurements unavailable (availability attacks, such as denial-of-service attacks), in addition to indicating what should be reinforced in the metering system to achieve this goal. The effectiveness and efficiency of the proposed methodologies are

discussed based on simulation results employing the IEEE 14-, 30-, 118-, and 300-bus systems.

Keywords: State estimation; Observability analysis; Criticalities; Cybersecurity.

Lista de Figuras

2.1 Níveis de segurança 22

2.2 Etapas da EE 24

3.1 Sistema de 6 barras com um ramo irrelevante 40

4.1 Sistema 9 barras exemplo 47

4.2 Sistema 9 barras (Grafo não direcionado com peso unitário nas arestas) . . 47

4.3 Sistema hipotético com uma medida de fluxo em cada ramo 50

4.4 Tempo computacional cumulativo IEEE 14-barras 52

4.5 Tempo computacional cumulativo IEEE 30-barras 53

4.6 Tempo computacional por cardinalidade IEEE 14-barras 53

4.7 Tempo computacional por cardinalidade IEEE 30-barras 54

4.8 Sistema 9 Barras com Plano de Medição 55

4.9 Sistema 9 Barras com Plano de Medição 62

4.10 Sistema hipotético sem medidas nos ramos irrelevantes 63

5.1 Sistema de 9 barras 70

5.2 Sistema de 9 barras 72

6.1 Sistema 9 barras exemplo 95

6.2 IEEE 30 barras com 14 UMs 98

6.3 IEEE 30 barras com 21 UMs 100

6.4 IEEE 30 barras com 28 UMs 102

Lista de Tabelas

4.1 C_k-ramos identificadas *offline* — IEEE 14-barras 52

4.2 C_k-ramos identificadas *offline* — IEEE 30-barras 52

4.3 Criticalidades de ramos (determinadas sem plano de medição) 55

4.4 Criticalidades de ramos com ramos irrelevantes em destaque 57

4.5 Criticalidades de ramos com C_{k-r}-ramos 58

4.6 Criticalidades de ramos atualizadas 60

4.7 Quantidade de C_k-ramos por cardinalidade 60

4.8 IEEE 118 com 68 UMs e 11 ramos irrelevantes 61

4.9 IEEE 118 com 80 UMs e 7 ramos irrelevantes 61

4.10 IEEE 118 com 92 UMs e 4 ramos irrelevantes 62

4.11 C_k-ramos identificadas até $k = 4$ 65

5.1 A_k-UMs associadas às C_k-ramos 70

5.2 C_k-UMs do sistema 9 barras 71

5.3 Quantidade de ramos por A_k-UMs 74

5.4 Definição final dos subconjuntos de busca 75

5.5 C_k-meds encontradas 76

5.6 C_k-meds identificadas até $k = 4$ 78

5.7 Tempo (s) por cardinalidade — IEEE 118 barras 79

5.8 Tempo (s) por cardinalidade — IEEE 300 barras 79

6.1 UMs associadas às C_k-ramos 96

6.2 C_k-ramos após o processamento de duplicidade de UMs 97

6.3 Quantidade de C_k-ramos por cardinalidade (IEEE 30 barras — 14 UMs) . 98

6.4 UMs a serem reforçadas (IEEE 30 barras — 14 UMs) 99

6.5 Quantidade de C_k-ramos por cardinalidade (IEEE 30 barras — 21 UMs) . 100

6.6 UMs a serem reforçadas (IEEE 30 barras — 21 UMs) 101

6.7 Quantidade de C_k-ramos por cardinalidade (IEEE 30 barras — 28 UMs) . 102

6.8 UMs a serem reforçadas (IEEE 30 barras — 28 UMs) 103

6.9 Quantidade de C_k-ramos por cardinalidade (IEEE 118 barras — 68 UMs) . 104

6.10 UMs a serem reforçadas — sistema completo (IEEE 118 barras — 68 UMs) 105

6.11 UMs a serem reforçadas — Área 1 (IEEE 118 barras — 68 UMs) 106

6.12 UMs a serem reforçadas — Área 2 (IEEE 118 barras — 68 UMs) 106

6.13 UMs a serem reforçadas — Área 3 (IEEE 118 barras — 68 UMs) 107

Lista de Abreviaturas e Siglas

AGC *Automatic Generation Control*

AGM Árvore Geradora Mínima

AMI *Advanced Metering Infrastructure*

AOC Análise de Observabilidade e Criticalidade

CCA *Coordinated Cyberattack*

CCPA *Coordinated Cyber-Physical Attack*

CLP Controlador Lógico Programável

COS Centro de Operação do Sistema

CPPS *Cyber-Physical Power System*

CPU *Central Processing Unit*

CTI *Covert Topological Information*

DDoS *Distributed Denial of Service*

DoS *Denial of Service*

DSA *Dominating Set Augmentation*

DTU *Data Transfer Unit*

EE Estimação de Estado

EG Erro Grosseiro

FDIA *False Data Injection Attack*

FTU *Feeder Terminal Unit*

GPU *Graphics Processing Unit*

IECPS *Integrated Energy Cyber-Physical System*

IED *Intelligent Electronic Device*

IES *Integrated Energy System*

IHM Interface Homem-Máquina

LR *Load Redistribution Attack*

MILP *Mixed-Integer Linear Programming*

MINLP *Mixed-Integer Nonlinear Programming*

MITM *Man-in-the-Middle*

MMA *Most Minimal Attacks*

MQP Mínimos Quadrados Ponderados

MSM *Most Shortest Minimal Attacks*

PLI Programação Linear Inteira

PLI-B Programação Linear Inteira Binária

PMCR Proteção Mínima de Criticalidades de Ramos

PMU *Phasor Measurement Unit*

RTU *Remote Terminal Unit*

SCADA *Supervisory Control and Data Acquisition*

SCP *Set Covering Problem*

SEP Sistema Elétrico de Potência

TPH *Tree-Pruning Heuristic*

TSA *Time Synchronization Attack*

UM Unidade de Medição

UMF Unidade de Medição Fasorial

Sumário

1 Introdução **12**

1.1 Da observabilidade à Análise de Criticalidades . . . 13

1.2 Motivação . . . 16

1.3 Objetivos . . . 17

1.4 Contribuições . . . 18

1.5 Organização dos capítulos . . . 19

2 Fundamentos Teóricos da Estimação de Estado **21**

2.1 Operação dos Sistemas Elétricos de Potência . . . 21

2.1.1 Níveis de Operação do Sistema . . . 22

2.2 Visão Geral . . . 23

2.2.1 Base de Dados . . . 23

2.2.2 Etapas do Processo . . . 24

2.3 Formulação Matemática . . . 25

2.3.1 Modelo de medição não linear . . . 25

2.3.2 Método dos Mínimos Quadrados Ponderados . . . 26

2.3.3 Solução Iterativa por Gauss-Newton . . . 27

2.3.4 Modelo Linear Desacoplado . . . 28

2.4 Análise de Observabilidade . . . 30

2.5 Processamento de Erros Grosseiros . . . 31

2.5.1 Vetor de Resíduos e Matriz de Covariância . . . 31

2.5.2 Detecção e Identificação de Erros Grosseiros . . . 32

2.6 Considerações Finais 33

3 Análise de Observabilidade e Criticalidade 34

3.1 Avaliação das Vulnerabilidades da EE 34

3.1.1 Requisitos da EE 35

3.1.2 A limitação informacional da análise binária 35

3.1.3 Implicações do conhecimento das criticalidades 37

3.2 Tuplas Críticas: Definições e Propriedades Gerais 38

3.2.1 Propriedades das Criticalidades de Ramos 39

3.2.2 Propriedades das Criticalidades de Unidade de Medição 41

3.2.3 Propriedades das Criticalidades de Medidas 43

4 Identificação de Criticalidades de Ramos 45

4.1 O problema combinatório da identificação das Criticalidades de Ramos . . 45

4.2 Metodologia Offline 46

4.2.1 Abordagem Topológica: Algoritmo de Kruskal 46

4.2.2 Abordagem Numérica 48

4.2.2.1 O Plano de Medição Hipotético 48

4.2.2.2 Verificação de Criticalidades de Medidas via Matriz de Covariância dos Resíduos 50

4.2.3 Comparação de desempenho entre a abordagem topológica (Kruskal) e numérica (Sistema Hipotético) 51

4.2.4 Atualização das Criticalidades de Ramos 55

4.2.5 Desafios no processo de atualização das criticalidades de ramos . . . 60

4.3 Metodologia Online 62

4.4 Aplicação de GPUs 64

4.5 Considerações Finais 65

5 Identificação de criticalidades no sistema de medição 67

5.1 Visão Geral da Metodologia Integrada . . . 68

5.2 Identificação das Criticalidades de UMs . . . 68

5.3 Identificação das criticalidades de medidas . . . 72

1) Criação dos subconjuntos de medidas. . . . 73

2) Determinação dos limites de busca. . . . 73

3) Busca local. . . . 75

5.4 Aceleração por Computação Paralela em GPU . . . 76

5.5 Resultados e Discussão . . . 77

5.5.1 Identificação das criticalidades de medidas . . . 78

6 Proteção das criticalidades de ramos contra ataques cibernéticos 82

6.1 Seleção de UMs para Reforço . . . 83

6.2 Metodologia de Proteção Baseada em Criticalidades . . . 88

6.2.1 Formulação Matemática . . . 89

6.2.1.1 Formulação geral do Problema de Cobertura de Conjuntos 90

6.2.1.2 Aplicação ao problema de Proteção Mínima de Criticalidades de Ramos . . . 91

6.2.1.3 Estratégias de proteção . . . 93

Situação 1 — Reforço global. . . . 93

Situação 2 — Reforço por área. . . . 93

6.2.1.4 Redução da quantidade de restrições . . . 94

6.3 Testes e Resultados . . . 95

6.3.1 Sistema 9 barras exemplo . . . 95

6.3.2 Sistema IEEE 30 barras . . . 97

6.3.3 Sistema IEEE 118 barras . . . 103

6.4 Considerações Finais . . . 107

7 Conclusões e Trabalhos Futuros **109**

7.1 Trabalhos Futuros 111

Referências **113**

Apêndice A – Ataques Cibernéticos a Sistemas Ciberfísicos de Potência **120**

A.1 Histórico dos Ataques Cibernéticos 121

A.2 Ataques Cibernéticos 123

A.2.1 Ataques de injeção de dados falsos 124

A.2.2 Ataques de negação de serviço 124

A.2.3 Ataques de sincronização temporal 125

A.2.4 Ataques de repetição 125

A.2.5 Ataques *man-in-the-middle* 126

A.2.6 Ataques cibernéticos coordenados 126

A.3 Ataques Físicos 126

A.4 Ataques Ciberfísicos Coordenados 127

A.4.1 Priorização do ataque físico 128

A.4.2 Priorização do ataque cibernético 128

A.5 Estratégias de Defesa em Sistemas Ciberfísicos 129

A.5.1 Prevenção e planejamento antes do ataque 129

A.5.1.1 Proteção do acesso e alocação de recursos em CPPS . . . 129

A.5.1.2 Planejamento resiliente da infraestrutura em IECPS . . . 130

1 Introdução

A operação segura e confiável de Sistemas Elétricos de Potência (SEPs) depende de processos computacionais capazes de lidar com um elevado volume de dados, em tempo quase real, sob condições de incerteza, falhas e mudanças topológicas. Avanços na capacidade de processamento e na infraestrutura computacional permitiram que problemas antes inviáveis, em razão do custo computacional associado, passassem a ser tratados de maneira sistemática nos Centros de Operação do Sistema (COS). Estudos como fluxo de potência, estimação de estado, análise de contingências e despacho ótimo são hoje executados de forma integrada, apoiados por sistemas supervisórios e por algoritmos de maior complexidade.

Dentre essas funcionalidades, a Estimação de Estado (EE) ocupa uma posição central. Introduzida no início da década de 1970 (Schweppe; Wildes, 1970; Schweppe; Rom, 1970; Schweppe, 1970), a EE é responsável por fornecer a melhor estimativa do estado da rede — módulos e ângulos das tensões nas barras — a partir de um conjunto redundante de medidas coletadas pelo sistema *Supervisory Control and Data Acquisition* (SCADA). Essas medidas incluem fluxos e injeções de potência, magnitudes de tensão complementadas por informações sobre os parâmetros e a topologia da rede, considerados conhecidos. A partir do estado estimado, a EE alimenta diversas outras funções do COS que subsidiam a operação do sistema sob supervisão.

Como a EE é uma das fontes primárias de informação, espera-se que os dados por ela fornecidos sejam confiáveis. Entretanto, as medidas recebidas pelo SCADA estão sujeitas a diferentes tipos de incertezas e falhas: erros de calibração, defeitos em equipamentos, falhas de comunicação e, mais recentemente, ataques cibernéticos (He; Yan, 2016; Liu; Ning; Reiter, 2011). Diante desse cenário, os dados operativos devem ser processados e validados antes de serem disponibilizados às funções do COS. Nesse sentido, a EE atua como um filtro que, além de estimar o estado da rede, é responsável por detectar e identificar Erros Grosseiros (EGs) nas medidas, contribuindo para a integridade da base de dados utilizada na operação.

1.1 Da observabilidade à Análise de Criticalidades

Para que a EE estime o estado da rede, o conjunto de medidas disponível deve ser suficiente em quantidade, tipo e localização. A etapa responsável por verificar essa condição é conhecida na literatura como Análise de Observabilidade (Abur; Gomez Exposito, 2004; Monticelli, 1999). Para sistemas observáveis, pode-se obter uma solução única para o problema de estimação; caso contrário, identificam-se as ilhas observáveis e os ramos não observáveis, possibilitando a recuperação da observabilidade por meio de pseudomedidas ou do reforço do sistema de medição.

A verificação da condição de observabilidade, quando considerada isoladamente, fornece uma resposta binária: o sistema é ou não observável. Considerada dessa forma, ela não revela o grau de vulnerabilidade da supervisão diante de eventos que possam comprometer o conjunto de medidas disponíveis. A literatura dispõe de indicadores que caracterizam diferentes níveis dessa vulnerabilidade, como as medidas críticas, os conjuntos críticos e as tuplas críticas (Clements; Davis, 1986; Korres; Contaxis, 1991; Crainic *et al.*, 1990; London; Alberto; Bretas, 2007; Sou; Sandberg; Johansson, 2012). A perda de medidas deve-se a diversos fatores, entre os quais: manutenção programada, falhas de comunicação, falhas em equipamentos, ataques cibernéticos e remoção de medidas portadoras de EGs pelo processo de depuração da EE. Mesmo em sistemas de medição bem projetados, a indisponibilidade de um subconjunto reduzido de elementos pode levar à perda de observabilidade e comprometer a capacidade de detectar e identificar EGs.

A caracterização desse grau de vulnerabilidade é o objeto da Análise de Criticalidades. Nesta tese, o grau de vulnerabilidade da supervisão frente a condições adversas à EE é expresso pela cardinalidade das tuplas críticas — quanto menor a cardinalidade, mais próximo da inobservabilidade o sistema se encontra — e pela quantidade e distribuição dessas tuplas entre ramos, medidas e Unidades de Medição (UMs). Entende-se por criticalidade a condição em que a remoção simultânea de um conjunto mínimo de elementos, medidas, ramos ou UMs, torna o sistema não observável. Tais conjuntos são denominados k-tuplas críticas, denotados por C_k. Conforme a natureza dos elementos envolvidos, distinguem-se três classes: C_k de ramos (C_k-ramos), C_k de medidas (C_k-meds) e C_k de UMs (C_k-UMs). O tratamento integrado dessas três classes, tendo as C_k-ramos como ponto de partida, constitui o eixo metodológico desta tese (Seção 1.4).

A presença de criticalidades impõe limitações ao processo de EE. EGs que afetem medidas críticas (C_1-med) não podem ser detectados; em pares críticos (C_2-med), erros

podem ser detectados, mas não identificados. Em C_k-med de cardinalidade $k > 2$, $(k-1)$ erros simultâneos comprometem a capacidade de identificação (Clements; Davis, 1988). Erros topológicos envolvendo ramos críticos não são detectáveis, e a indisponibilidade simultânea dos elementos de uma C_k-ramo, C_k-med ou C_k-UM leva à inobservabilidade. Em síntese, as criticalidades constituem caminhos mínimos para a perda de observabilidade e para o comprometimento da capacidade de depuração de dados.

Do exposto, a Análise de Observabilidade, tal como tradicionalmente concebida, deve ser ampliada, incorporando, de forma integrada, a análise de criticalidades para a identificação das vulnerabilidades estruturais que afetam o processo de EE.

A identificação de *Cks* é um problema de natureza combinatória e de grande relevância para EE, pois permite delimitar as fronteiras da observabilidade do sistema. Na literatura, vários trabalhos sobre a determinação de *Cks* de baixa cardinalidade (medidas críticas e duplas críticas de medidas) podem ser encontrados (Costa; Piazza; Mandel, 1990; Korres; Contaxis, 1991; London; Alberto; Bretas, 2007; Augusto *et al.*, 2017; Coutto Filho; Souza; Schilling, 2007; Coutto Filho; Souza; Villavicencio Tafur, 2013). Entretanto, são menos numerosos os trabalhos que tratam da identificação de criticalidades de cardinalidades mais elevadas. Um dos primeiros trabalhos que trataram da identificação de criticalidades de medidas foi Clements e Davis (1986), no qual também se encontra um estudo sobre o impacto dessas criticalidades na detecção e na identificação de múltiplos EGs. Em Crainic *et al.* (1990), a capacidade do sistema de medição de preservar a observabilidade é avaliada por índices de segurança frente à perda de k medidas, com a identificação de medidas, pares e triplas críticas de medidas. A observabilidade robusta frente à perda de medidas foi também tratada em Castillo *et al.* (2008). Em Sou, Sandberg e Johansson (2012), o objetivo foi identificar as *Cks* mais esparsas (aquelas de menor cardinalidade) associadas a uma dada medida. Em Coutto Filho, Souza e Augusto (2014), busca-se identificar as criticalidades de UMs a partir das criticalidades de medidas. Em Augusto *et al.* (2016), as criticalidades de medidas são utilizadas para avaliar a capacidade de observação da rede elétrica pela EE. Já em Augusto *et al.* (2019), utilizou-se o algoritmo *Branch & Bound* para identificação de criticalidades de UMs com cardinalidade superior a 3.

As C_k-ramos carregam informações relevantes sobre as vulnerabilidades que podem prejudicar a EE, tanto na ocorrência de eventos físicos quanto na de eventos cibernéticos. A determinação de criticalidades envolvendo ramos da rede, por sua vez, tem sido menos explorada, em razão do custo computacional decorrente de sua natureza combinatória. Os

trabalhos pioneiros nessa direção (Clements; Davis, 1988; Chen; Abur, 2008) abordaram principalmente as repercussões das criticalidades de ramos sobre o processamento de erros topológicos. Crainic *et al.* (1990) também definem ramos críticos e pares críticos de ramos, a partir das árvores geradoras da rede, e os relacionam ao nível de segurança que o sistema de medição pode atingir: em uma rede com um ramo crítico, a perda das, no máximo, quatro medidas associadas a esse ramo (fluxos em suas extremidades e injeções em suas barras terminais) torna a rede não observável. Em Theodoro *et al.* (2012), propôs-se um método algébrico-grafo, baseado na fatoração da matriz de incidência barra-ramo, para identificar os casos de ilhamento decorrentes da perda de um equipamento, bem como as barras que compõem cada ilha.

Esta tese dá continuidade à pesquisa desenvolvida na dissertação de mestrado do autor (Coimbra, 2019). Parte dos resultados da dissertação foram publicados em Coimbra *et al.* (2021), acrescidos de resultados obtidos já durante o doutorado. Nesses trabalhos, propôs-se uma metodologia integrada que, partindo das criticalidades de ramos, obtém as criticalidades de medidas e de UMs por meio de propriedades que as inter-relacionam. Tal abordagem inverte a ordem de análise adotada na maior parte da literatura, que parte das criticalidades de medidas para chegar às demais. Mostrou-se que as C_k-ramos podem ser obtidas *offline*, por meio do algoritmo de Kruskal, para uma topologia básica e, posteriormente, atualizadas em tempo real à medida que ocorrem mudanças na rede ou no sistema de medição. As C_k-UMs são obtidas diretamente a partir das C_k-ramos, e as C_k-meds, por associação às C_k-ramos e por uma busca heurística em subconjuntos de medidas. Na dissertação, a metodologia foi testada nos sistemas IEEE 14 e 30 barras, e foi também avaliada a identificação das C_k-ramos pela verificação do determinante da matriz de ganho de um pseudo-sistema de medição com medidas de injeção em todas as barras, estratégia preterida em favor do algoritmo de Kruskal por seu maior custo computacional.

Entretanto, o processo de atualização das C_k-ramos em tempo real pode conter erros, caso criticalidades de cardinalidade suficientemente elevada não tenham sido previamente determinadas *offline* — tarefa computacionalmente dispendiosa, podendo ser inviável para redes de maior porte. A atualização das características qualitativas de um plano de medição em tempo real é também tratada em London, Alberto e Bretas (2007), em que, a partir de um caso base, a identificação de medidas críticas e de conjuntos críticos é atualizada apenas por meio da refatoração da matriz Jacobiana. Já no doutorado, em (Coimbra; Souza; Coutto Filho, 2025), a etapa de identificação das criticalidades de ramos — anteriormente realizada por meio do algoritmo de Kruskal, em uma abordagem topológica — foi substituída por uma abordagem numérica baseada em um sistema de

medição hipotético, com uma medida de fluxo de potência em cada ramo, que permite verificar a criticalidade de cada tupla localmente, em submatrizes da matriz de covariância dos resíduos, o que reduziu o tempo de processamento. Neste trabalho, as duas etapas foram integradas em uma metodologia unificada, com aceleração por meio de computação paralela em *Graphics Processing Unit* (GPU), demonstrando a viabilidade de aplicação a redes de maior porte (sistemas IEEE 118 e 300 barras). Além disso, o conhecimento das C_k-ramos é empregado na seleção de UMs a reforçar para a proteção da supervisão contra ataques que comprometam a disponibilidade de suas medidas, aplicação não abordada na dissertação.

1.2 Motivação

O desconhecimento das vulnerabilidades do processo de EE impede ações preventivas ou corretivas eficazes em situações que podem colocar em risco não apenas a observabilidade, mas também a capacidade da EE de tratar EGs. A boa capacidade de depuração de EGs pela EE contribui para aumentar a resiliência do processo de supervisão, independentemente de tais erros terem sido provocados por um atacante malicioso ou por falhas no sistema de medição e/ou de comunicação. A presença de EGs compromete a eficácia da análise de resíduos da estimação, colocando em risco a confiabilidade da EE e a qualidade dos valores estimados. A depuração de EGs pode ser um processo demorado, sobretudo quando vários deles ocorrem simultaneamente (Coutto Filho; Souza; Glover, 2019; Clements; Davis, 1986), o que exige a aplicação repetida do método do maior resíduo normalizado para medições suspeitas (Abur; Gomez Exposito, 2004). Além disso, EGs que afetam as C_k-meds (Braga Flor *et al.*, 2023) são difíceis (e, por vezes, impossíveis) de tratar pelas técnicas usuais de depuração de EGs (Clements; Davis, 1988). As criticalidades de ramos se relacionam fortemente com as criticalidades de UMs e de medidas, porém métodos para sua identificação são menos numerosos na literatura do que os voltados às criticalidades de medidas. Além disso, o aproveitamento do conhecimento das criticalidades para a avaliação da resiliência da supervisão — em particular, para o tratamento de cenários envolvendo ataques cibernéticos — permanece pouco explorado. Portanto, torna-se vantajoso conhecer antecipadamente as C_k-ramos, C_k-UMs e C_k-meds presentes no processo de EE.

1.3 Objetivos

O objetivo geral do trabalho é desenvolver uma metodologia eficiente e eficaz para a determinação das criticalidades de ramos e, a partir de tais criticalidades, realizar de forma integrada a identificação de criticalidades de UMs e de medidas, bem como indicar reforços no plano de medição para conter os efeitos de ataques cibernéticos que comprometam UMs, tornando indisponíveis as suas medidas.

Registra-se que a grande maioria dos estimadores de estado em uso nas empresas de energia elétrica processa apenas medidas de *Remote Terminal Unit* (RTU); medidas de *Phasor Measurement Unit* (PMU) podem ser empregadas em estimadores independentes como auxílio ao processo de depuração de erros nos dados (Coutto Filho; Souza; Guimaraens, 2014). Contudo, é importante destacar que no contexto deste trabalho o termo unidades de medição pode se referir tanto a RTUs quanto a PMUs, uma vez que nas análises de criticalidades de natureza estrutural aqui realizadas o efeito da presença de medidas de fluxo de potência e de sincrofasores de corrente é o mesmo. Medidas de ângulo de tensão, embora possam ser também facilmente consideradas nas metodologias propostas, não foram incluídas nas análises realizadas. Tais medidas não se relacionam diretamente com os ramos da rede e sua presença não agrega capacidade crítica sobre ramos que interligam ilhas observáveis, não sendo aqui vistas como suficientes para alterar as vulnerabilidades que as criticalidades formadas pelas demais medidas representam. Mais especificamente, destacam-se os seguintes objetivos:

- Apresentar as propriedades, estabelecidas na dissertação de mestrado do autor (Coimbra, 2019), que relacionam as C_k-ramos às C_k-UMs e C_k-meds;
- Desenvolver um método numérico eficiente para a identificação de C_k-ramos, visto como um problema de identificação de C_k-meds;
- Integrar as etapas de identificação de C_k-ramos e de C_k-meds para obter as C_k-meds de forma eficiente a partir do conhecimento das C_k-ramos;
- Empregar o conhecimento das C_k-ramos para, com foco na proteção preventiva da supervisão da rede contra ataques cibernéticos que comprometam a disponibilidade das medidas, indicar quais UMs devem ser reforçadas.

1.4 Contribuições

As principais contribuições desta tese são:

- Desenvolvimento de um método que transforma a identificação de C_k-ramos em identificação de C_k-meds em um sistema de medição hipotético, com uma medida de fluxo de potência em cada ramo, permitindo o emprego de métodos numéricos e de técnicas computacionais eficientes. Diferentemente das estratégias adotadas na dissertação de mestrado — verificação topológica de ilhamento pelo algoritmo de Kruskal ou do determinante da matriz de ganho de um pseudo-sistema de medição —, a criticalidade de cada tupla é verificada localmente, em submatrizes da matriz de covariância dos resíduos, o que viabiliza o processamento paralelo em GPU;

- Proposição de uma metodologia que integra a obtenção de C_k-ramos e de C_k-meds, sendo estas últimas obtidas por meio da análise de combinações de conjuntos reduzidos de medidas, com aceleração por computação paralela em GPU. Em relação à busca direta no espaço completo de medidas (Nishio *et al.*, 2024), o espaço de busca é restrito aos subconjuntos associados às C_k-ramos; em relação à dissertação, a metodologia dispensa a etapa de atualização das C_k-ramos, adota um novo critério para os limites de busca das C_k-meds e é aplicada a sistemas de maior porte (IEEE 118 e 300 barras);

- Estabelecimento de uma metodologia que emprega programação linear inteira para, a partir de C_k-ramos, determinar o conjunto mínimo de UMs a reforçar, de modo a mitigar o efeito de ataques cibernéticos que comprometam UMs, tornando indisponíveis as suas medidas. Diferentemente das abordagens de seleção de medidas a proteger baseadas em conjuntos básicos de medidas ou no custo mínimo de ataques furtivos (Bobba *et al.*, 2010; Dán; Sandberg, 2010), a seleção é orientada pelas criticalidades de ramos.

As seguintes publicações decorrem da presente pesquisa de tese:

- COIMBRA, Andrei Mantesso *et al.* Network-Based Approach to Identify Criticalities in State Estimation. **IEEE Transactions on Power Systems**, v. 36, n. 4, p. 3394–3405, jul. 2021. ISSN 0885-8950. DOI: 10.1109/TPWRS.2021.3055122

- COIMBRA, Andrei Mantesso; SOUZA, Julio Cesar Stacchini de; COUTTO FILHO, Milton Brown. Identificação de Tuplas Críticas de Ramos na Estimação de Estado.

In: ANAIS do Simpósio Brasileiro de Automação Inteligente. [*S. l.: s. n.*], ago. 2025. Disponível em: https://ojs.sba.org.br/index.php/sbai/article/view/5120

- COIMBRA, Andrei Mantesso *et al.* Identificação de Tuplas de Ramos e de Medidas Críticas para a Estimação de Estado. *In:* ANAIS do XXVI Congresso Brasileiro de Automática. São Paulo: [*s. n.*], out. 2026. v. 1. Disponível em: https://ojs.sba.org.br/index.php/cba/article/view/6378

Adicionalmente, durante o período de doutoramento, o autor participou da seguinte publicação correlata:

- COUTTO FILHO, Milton Brown *et al.* Educational Tool for Power System State Estimation Teaching and Learning. **IEEE Transactions on Power Systems**, v. 38, n. 6, p. 5885–5895, 2022. ISSN 0885-8950. DOI: 10.1109/TPWRS.2022.3229908

1.5 Organização dos capítulos

Esta tese está organizada em sete capítulos, conforme descrito a seguir.

O Capítulo 2 apresenta os fundamentos da EE, incluindo a formulação por Mínimos Quadrados Ponderados (MQP), a modelagem das medidas, o processamento de resíduos e a detecção de EGs.

O Capítulo 3 introduz a análise de observabilidade e criticalidade, as definições formais de criticalidade para os três tipos de elementos (ramos, medidas e UMs) e as propriedades que estabelecem as relações entre eles.

O Capítulo 4 apresenta a abordagem numérica proposta para identificação de criticalidades de ramos, baseada no conceito de sistema de medição hipotético, com comparações em relação à abordagem topológica anteriormente adotada na dissertação de mestrado do autor.

O Capítulo 5 descreve a metodologia integrada para identificação de criticalidades de ramos, medidas e UMs, incluindo a aceleração por computação paralela em GPU, e apresenta os resultados de validação nos sistemas IEEE 14, 30, 118 e 300 barras.

O Capítulo 6 apresenta a aplicação da metodologia ao estudo da resiliência da supervisão, formulando, por meio de programação linear inteira, uma estratégia de proteção

preventiva de UMs contra ataques cibernéticos que comprometam a disponibilidade de suas medidas, fundamentada no conhecimento das C_k-ramos.

O Capítulo 7 reúne as conclusões e propõe diretrizes para trabalhos futuros.

2 Fundamentos Teóricos da Estimação de Estado

Este capítulo apresenta os fundamentos teóricos necessários ao desenvolvimento desta tese. Inicialmente, contextualiza-se a operação dos SEP e o papel da EE nos COS. Em seguida, discutem-se as etapas que compõem o processo de EE, sua modelagem matemática (não linear e linear), os aspectos relacionados à análise de observabilidade clássica e o processamento de resíduos para detecção e identificação de EGs. Esses fundamentos subsidiam a discussão sobre Análise de Observabilidade e Criticalidade (AOC), tema central do Capítulo 3.

2.1 Operação dos Sistemas Elétricos de Potência

A operação dos SEP envolve um equilíbrio permanente entre a geração e o consumo de energia. Durante a operação, exige-se que os limites dos equipamentos envolvidos sejam respeitados, tais como a capacidade de transmissão das linhas, dos transformadores e dos geradores, bem como os limites de tensão estabelecidos por regulação. Tais limites são denominados restrições de operação do sistema.

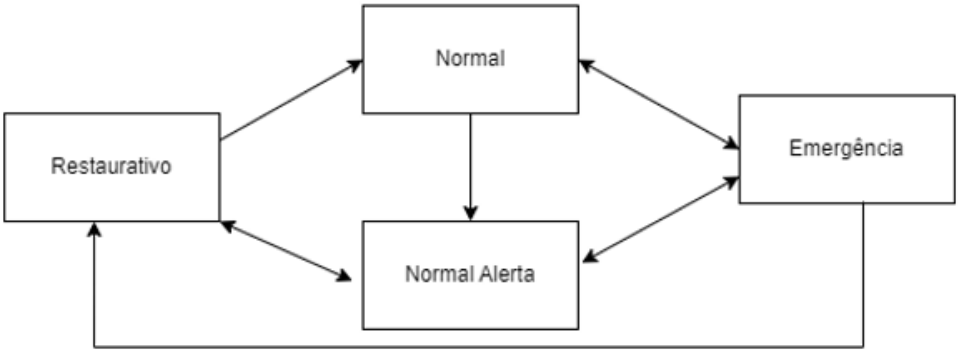
Para a operação do sistema, os COS são responsáveis por duas funções: monitoramento e segurança. O monitoramento é necessário porque a carga do sistema varia ao longo do dia, sendo preciso verificar continuamente se as restrições de operação estão sendo atendidas. A segurança, por sua vez, refere-se à capacidade do sistema de suportar contingências sem entrar em colapso. Entendem-se por contingências eventos como falhas em equipamentos, curtos-circuitos ou alterações na configuração da rede decorrentes de manutenção ou substituição de equipamentos.

2.1.1 Níveis de Operação do Sistema

A literatura apresenta diferentes propostas para classificar os níveis de operação do sistema. Monticelli (1999) classifica a operação em seis níveis: Seguro, Seguro Corretivo, Alerta, Emergência Corretiva, Emergência Não Corretiva e Restaurativo. Abur e Expósito (2004) adotam uma classificação mais sintética, com apenas quatro níveis: Normal Seguro, Normal Inseguro, Emergência e Restaurativo. Observa-se que Monticelli subdivide alguns níveis, por exemplo, Emergência Corretiva e Não Corretiva, enquanto Abur e Expósito os consolidam em um único nível de Emergência. Essas divisões têm um propósito organizacional e não afetam a compreensão do processo.

A Figura 2.1 apresenta um diagrama dos níveis de segurança de um sistema.

Figura 2.1 - Níveis de segurança



Fonte: Elaboração própria (2026).

No nível Normal (1), toda a carga do sistema é atendida, todas as restrições de operação são respeitadas e, mesmo diante de alguma contingência, não há perda de carga nem violação das restrições do sistema. No nível Normal Alerta (2), toda a carga continua sendo atendida e nenhuma restrição é violada, porém, caso ocorra uma contingência, não é possível restabelecer o sistema sem perda de carga. No nível de Emergência (3), toda a carga ainda é atendida, mas algumas restrições do sistema são violadas. Quando, para a restauração do sistema, há perda de carga, o nível passa para o estado Restaurativo (4); quando não há perda de carga, o sistema pode retornar diretamente aos níveis (1) ou (2). As setas no diagrama indicam as transições entre os níveis: o estado (1) pode passar diretamente para (3) ou, primeiro, para (2) e, posteriormente, para (3). Sempre que houver perda de carga para o restabelecimento do sistema, considera-se que o nível é Restaurativo (4).

Em todos os níveis de operação, a EE é a função responsável por fornecer o estado atual

da rede, a tensão complexa (módulo e ângulo) em cada barra, a partir das informações disponíveis no sistema SCADA. Este estado constitui a base sobre a qual as demais funções de análise, controle e operação são executadas. Por essa razão, a confiabilidade da EE condiciona a confiabilidade da operação do sistema.

2.2 Visão Geral

A EE é responsável por fornecer o estado da rede — tensão complexa em cada barra — a partir de um conjunto de medidas recebidas pelo sistema SCADA. Tais medidas são processadas para obter o estado da rede de forma consistente. Como as medidas brutas podem conter erros decorrentes de calibração, defeitos em equipamentos, falhas de comunicação ou ataques cibernéticos, faz-se necessário um processamento que permita filtrar essas imperfeições. Quando uma medida contém um EG, tal medida precisa, sempre que possível, ser retirada do processo de estimação. Para que isso seja viável, é preciso que o sistema possua mais medidas do que estados a serem estimados, condição na qual se diz que o sistema é redundante.

2.2.1 Base de Dados

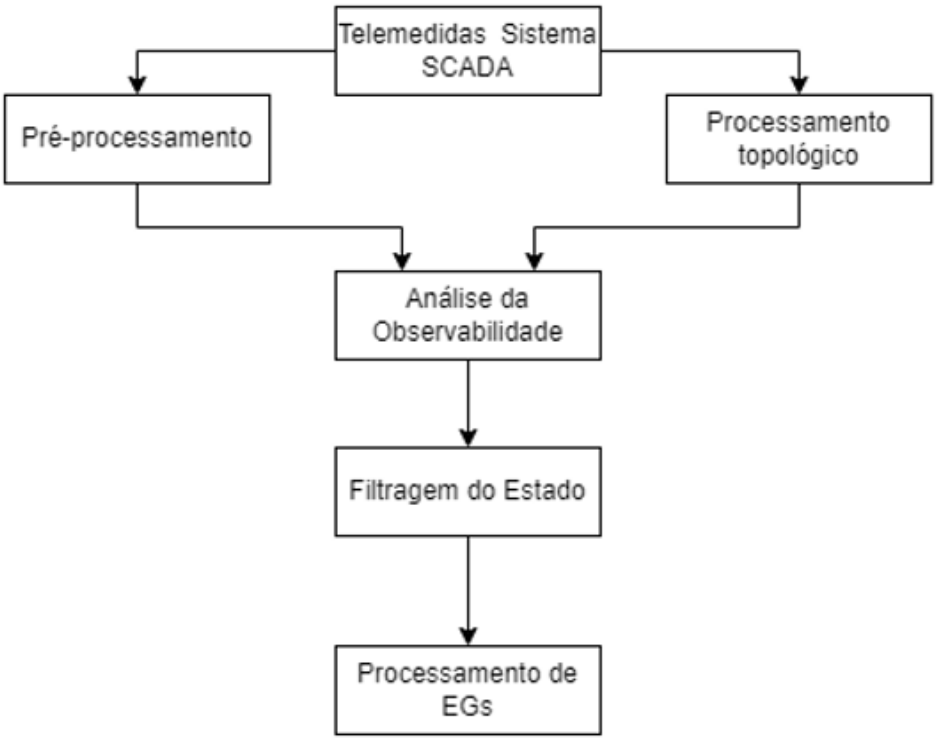
Para o processo de estimação, são necessárias duas bases de dados: a estática e a dinâmica. A primeira é constituída pelos parâmetros da rede: valores de impedância das linhas de transmissão, dos transformadores e dos bancos de capacitores e de indutores. Espera-se que essas informações estejam corretas, pois erros nesses valores comprometem o processo de estimação. A literatura apresenta estudos voltados à detecção de erros de parâmetros (Clements; Davis, 1988), mas esse processamento não é o foco da EE convencional.

A segunda base de dados, dinâmica, é recebida pelo sistema SCADA em tempo real e contém os valores das medidas analógicas — tensões nas barras, medidas de injeção e fluxo de potência, além de medidas de ângulo provenientes de Unidades de Medição Fasorial (UMFs), quando disponíveis — bem como o estado de chaves e disjuntores, que constitui informação binária. A partir dos estados de chaves e disjuntores, é possível determinar a topologia atual da rede.

2.2.2 Etapas do Processo

Partindo dessas duas bases, é possível estimar o estado da rede. A função EE pode ser dividida em cinco etapas: pré-processamento, processamento topológico, análise de observabilidade, filtragem do estado e processamento de erros grosseiros. A Figura 2.2 apresenta o diagrama da sequência das etapas da EE.

Figura 2.2 - Etapas da EE



Fonte: Elaboração própria (2026).

- Pré-processamento: avaliam-se os valores das medidas recebidas com base em uma faixa esperada. O intuito é eliminar medidas com erros evidentes.
- Processamento topológico: nesta etapa, obtêm-se os estados das chaves e dos disjuntores, avaliam-se os valores recebidos e corrigem-se eventuais erros de conexão, para então se obter o modelo barra-ramo da rede.
- Análise de Observabilidade: determina se a quantidade e a posição das medidas recebidas permitem obter o estado da rede. Quando isso não ocorre, recorre-se a pseudomedidas ou determinam-se as ilhas observáveis da rede.
- Filtragem do estado: esta é a etapa principal da função EE. Com base no modelo barra-ramo da rede e no conjunto de medidas, estima-se o estado atual da rede, isto

é, o módulo e o ângulo da tensão em cada barra.

- Processamento de Erros Grosseiros: após a obtenção do estado da rede, calculam-se as medidas com base nesse estado e confrontam-se esses valores com as medidas recebidas, definindo-se, assim, os resíduos da estimação. O objetivo é detectar EGs que não foram identificados na primeira etapa do processo. Quando possível, essas medidas são eliminadas, e o estado é novamente estimado.

Dessa forma, as etapas da EE atuam sequencialmente para transformar os dados brutos recebidos do sistema de supervisão em uma representação da condição operativa da rede. Enquanto o pré-processamento e o processamento topológico tratam e organizam as informações de entrada, a análise de observabilidade verifica se o sistema pode ser estimado com o conjunto de medidas disponível. Em seguida, a filtragem do estado fornece estimativas das grandezas elétricas da rede, e o processamento de EGs avalia a consistência dos resultados obtidos. Ao final do processo, a EE fornece resultados com a maior confiabilidade possível às demais aplicações dos COS.

2.3 Formulação Matemática

2.3.1 Modelo de medição não linear

A função EE é descrita pelo modelo apresentado em Equação (2.1), que relaciona as medidas coletadas às componentes do estado, com os erros de medição adicionados.

$$\mathbf{z} = h(\mathbf{x}) + \mathbf{e} \tag{2.1}$$

Sendo que:

- $\mathbf{z}$ é o vetor das medidas coletadas, de dimensão $(m \times 1)$, em que m é o número de medidas;
- $h(\cdot)$ é o vetor de equações não lineares (as do problema de fluxo de potência), de dimensão $(m \times 1)$;
- $\mathbf{x}$ é o vetor de estado do sistema, de dimensão $(n \times 1)$, em que $n = 2NB - 1$, sendo NB o número de barras do sistema. Quando há medidas de ângulo provenientes de UMFs, tem-se $n = 2NB$, uma vez que a própria medida de ângulo serve como referência angular do sistema;

- **e** é o vetor de dimensão $(m \times 1)$ que contém os erros das medidas. Esses erros refletem as incertezas dos medidores.

Algumas hipóteses são feitas sobre os erros das medidas: assume-se que não são correlacionados, possuem distribuição normal, com média zero e matriz de covariância **R**, conforme Equação (2.2).

$$E(\mathbf{e}) = 0 \qquad \text{Cov}(\mathbf{e}) = E(\mathbf{e}\mathbf{e}^T) = \mathbf{R} \tag{2.2}$$

Como os erros de medição não são correlacionados, a matriz **R** é diagonal, composta pelos valores das variâncias dos erros das medidas (σ^2), com dimensão $(m \times m)$.

$$\mathbf{R} = \begin{bmatrix} \sigma_1^2 & 0 & \cdots & 0 \\ 0 & \sigma_2^2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_m^2 \end{bmatrix} \tag{2.3}$$

2.3.2 Método dos Mínimos Quadrados Ponderados

Com base no modelo apresentado em Equação (2.1), a EE é estruturada como um problema de otimização para estimar o estado da rede. O método mais utilizado para a solução desse problema é o dos MQP. Define-se a função objetivo $J(\mathbf{x})$ da EE como um problema de minimização, conforme Equação (2.4).

$$J(\mathbf{x}) = \sum_{i=1}^{m} \varepsilon_i^2 \, \alpha_i = \sum_{i=1}^{m} \left[z_i - h_i(\mathbf{x}) \right]^2 \alpha_i \tag{2.4}$$

Sendo:

- $J(\mathbf{x})$: função objetivo;
- z_i: i-ésima medida;
- α_i: peso atribuído à i-ésima medida, $\alpha_i = \dfrac{1}{\sigma_i^2}$;
- m: número de medidas;
- ε_i: erro relativo à i-ésima medida.

Na forma matricial, tem-se:

$$\min_{\mathbf{x}} \; J(\mathbf{x}) = [\mathbf{z} - h(\mathbf{x})]^T \, \mathbf{R}^{-1} \, [\mathbf{z} - h(\mathbf{x})] \tag{2.5}$$

A solução por MQP consiste, portanto, em encontrar o vetor $\hat{\mathbf{x}}$, denominado estado estimado, que minimize $J(\mathbf{x})$. Para se determinar o mínimo, impõe-se a condição dada pela Equação (2.6).

$$g(\mathbf{x}) = \frac{\partial J(\mathbf{x})}{\partial \mathbf{x}} = -\mathbf{H}^T(\mathbf{x}) \, \mathbf{R}^{-1} \, [\mathbf{z} - h(\mathbf{x})] = 0 \tag{2.6}$$

onde:

$$\mathbf{H}(\mathbf{x}) = \left[\frac{\partial h(\mathbf{x})}{\partial \mathbf{x}} \right] \tag{2.7}$$

$\mathbf{H}(\mathbf{x})$ é a matriz Jacobiana do processo de estimação, contendo as derivadas das equações das medidas em relação às variáveis de estado.

2.3.3 Solução Iterativa por Gauss-Newton

Expandindo a função não linear $g(\mathbf{x})$ em torno do vetor de estado $\mathbf{x}^k$ por meio da série de Taylor, tem-se:

$$g(\mathbf{x}) = g\left(\mathbf{x}^k\right) + \mathbf{G}\left(\mathbf{x}^k\right) \left(\mathbf{x} - \mathbf{x}^k\right) + \cdots = 0 \tag{2.8}$$

Desprezando as componentes não lineares da expansão da série, chega-se à seguinte expressão:

$$\mathbf{x}^{k+1} = \mathbf{x}^k - \left[\mathbf{G}\left(\mathbf{x}^k\right)\right]^{-1} g\left(\mathbf{x}^k\right) \tag{2.9}$$

onde:

$$\begin{aligned} \mathbf{G}\left(\mathbf{x}^k\right) &= \frac{\partial g(\mathbf{x}^k)}{\partial \mathbf{x}} = \mathbf{H}^T\left(\mathbf{x}^k\right) \mathbf{R}^{-1} \mathbf{H}\left(\mathbf{x}^k\right) \\ g\left(\mathbf{x}^k\right) &= -\mathbf{H}^T\left(\mathbf{x}^k\right) \mathbf{R}^{-1} \left[\mathbf{z} - h\left(\mathbf{x}^k\right)\right] \end{aligned} \tag{2.10}$$

Usando o método iterativo de Gauss-Newton, o problema é resolvido iterativamente

de acordo com a seguinte equação:

$$\mathbf{x}^{k+1} = \mathbf{x}^{k} + \mathbf{G}^{-1}\left(\mathbf{x}^{k}\right) \mathbf{H}^{T}\left(\mathbf{x}^{k}\right) \mathbf{R}^{-1} \left[\mathbf{z} - h\left(\mathbf{x}^{k}\right)\right] \tag{2.11}$$

O processo iterativo encerra-se quando $\Delta\mathbf{x} = \left|\mathbf{x}^{k+1} - \mathbf{x}^{k}\right|$ for menor que uma tolerância preestabelecida.

2.3.4 Modelo Linear Desacoplado

Para a análise de observabilidade estrutural, adota-se usualmente o modelo linear desacoplado, que reduz o esforço computacional em relação ao modelo completo. Em situações particulares — por exemplo, quando as medidas de potência ativa e reativa não são tomadas aos pares, quando o subproblema reativo não dispõe de medidas de magnitude de tensão ou quando há mau condicionamento numérico —, a conclusão obtida com o modelo linear pode não se aplicar ao modelo não linear (Monticelli, 1999). Esse modelo também é conhecido como modelo desacoplado (potência ativa–ângulo de fase). Para tanto, assume-se que: (i) as medidas de injeção e fluxo de potência, ativa e reativa, são tomadas aos pares; (ii) as resistências série dos ramos são desprezadas; (iii) as susceptâncias em derivação são desconsideradas; (iv) as magnitudes das tensões são consideradas unitárias (1 p.u.) e as diferenças angulares entre barras adjacentes, pequenas; e (v) uma barra é adotada como referência angular, não sendo necessária uma medida de ângulo para esse fim. O modelo correspondente é dado em Equação (2.12).

$$\mathbf{z}_a = \mathbf{H}_a\, \boldsymbol{\theta} + \mathbf{v}_a \tag{2.12}$$

onde:

- $\boldsymbol{\theta}$: vetor de ângulos das tensões nodais, excluído o ângulo da barra de referência ($(NB-1)\times 1$);
- $\mathbf{z}_a$: vetor de medidas de injeções e fluxos de potência ativa ($m \times 1$);
- $\mathbf{v}_a$: vetor de erros associados às medidas ($m \times 1$), com média zero e matriz de covariância igual à matriz identidade $\mathbf{I}$;
- $\mathbf{H}_a$: matriz Jacobiana associada às medidas de potência ativa ($m \times (NB-1)$).

Para que o sistema seja observável, a matriz $\mathbf{H}_a$ deve apresentar posto completo. Portanto, a observabilidade da rede é determinada pela topologia e pela organização das medidas — tipo, quantidade e localização — (Gou; Abur, 2000).

Cabe distinguir dois conceitos. A observabilidade algébrica corresponde à condição de posto completo de $\mathbf{H}_a$, propriedade da matriz que decorre da topologia da rede e da localização das medidas; em condições genéricas, ela equivale à observabilidade topológica, verificada sobre o grafo da rede (Wu; Monticelli, 1985). A observabilidade numérica, por sua vez, refere-se à verificação desse posto por meio da fatoração de $\mathbf{H}_a$ ou de $\mathbf{G}_a$ em aritmética de ponto flutuante, sendo sensível ao condicionamento das matrizes e à tolerância adotada para identificar pivôs nulos (Monticelli, 1999). As análises desta tese são de natureza estrutural, isto é, dependem apenas da topologia e da localização das medidas.

A adoção de susceptâncias-série unitárias não é uma condição para a obtenção do modelo desacoplado, mas uma simplificação adicional, adequada à análise estrutural de observabilidade e de criticalidades, cujos resultados dependem apenas da posição dos elementos não nulos de $\mathbf{H}_a$ (Coutto Filho; Souza; Schilling, 2007). Considerando que todas as medidas possuam a mesma relevância no processo de estimação e que os ramos da rede estejam representados apenas pelas susceptâncias-série unitárias, os elementos de $\mathbf{H}_a$ associados a uma medida l são definidos como segue (Coutto Filho; Souza; Schilling, 2007).

- Fluxo de potência ativa no ramo i-k:

$$\mathbf{H}_a(l,i) = 1; \qquad \mathbf{H}_a(l,k) = -1 \tag{2.13}$$

sendo nulos os demais elementos da linha l. O mesmo vale para as Equações (2.14) a (2.16), apresentadas a seguir.

- Injeção de potência ativa na barra i:

$$\mathbf{H}_a(l,i) = nb_i; \qquad \mathbf{H}_a(l,k) = -1, \;\; \forall\, k \in \mathcal{A}_i \tag{2.14}$$

sendo nb_i correspondente ao número de barras conectadas em i e $\mathcal{A}_i$ o conjunto das barras adjacentes à barra i.

Na presença de UMFs, a matriz Jacobiana incluirá medidas de ângulos e correntes, segundo as equações a seguir. No modelo desacoplado, apenas o ângulo da tensão e a parte real do fasor de corrente se relacionam com os ângulos das tensões: assim como o fluxo de potência ativa, a parte real da corrente no ramo é aproximada por uma função linear da diferença angular entre suas barras terminais, enquanto a magnitude da tensão e a parte imaginária da corrente se relacionam com as magnitudes das tensões e pertencem ao subproblema reativo. Na presença de medidas de ângulo, estas fornecem a referência angular, e o vetor $\boldsymbol{\theta}$ passa a incluir os ângulos de todas as barras.

- Medida de ângulo da tensão na barra i:

$$\theta_i \rightarrow \mathbf{H}_a(l,i) = 1 \tag{2.15}$$

- Parte real da corrente entre as barras i-k:

$$I_{ik} \rightarrow \mathbf{H}_a(l,i) = 1; \qquad \mathbf{H}_a(l,k) = -1 \tag{2.16}$$

Assim, de acordo com Equação (2.12) e usando o método MQP, tem-se que:

$$\mathbf{G}_a \, \hat{\boldsymbol{\theta}} = \mathbf{H}_a^T \, \mathbf{z}_a \tag{2.17}$$

em que $\mathbf{G}_a = \mathbf{H}_a^T \mathbf{H}_a$ é a matriz de ganho associada às equações de medidas de potência ativa. Dessa forma, um sistema será considerado observável se a matriz de ganho $\mathbf{G}_a$ for não singular, isto é, se possuir posto completo e, consequentemente, inversa.

2.4 Análise de Observabilidade

A análise de observabilidade é a etapa do processo de EE que verifica se o conjunto de medidas disponível, considerando o tipo, a quantidade e a localização, é suficiente para que o estado da rede possa ser obtido. Quando o sistema é numericamente observável, isto é, quando $\mathbf{G}_a$ é não singular, pode-se obter uma solução única para a Equação (2.17); caso contrário, o sistema é classificado como não observável, e técnicas de recuperação da observabilidade devem ser empregadas, como o uso de pseudomedidas para tratar as ilhas observáveis identificadas.

Os métodos de análise de observabilidade encontrados na literatura podem ser, de forma geral, divididos em duas categorias: numéricos (ou algébricos) e topológicos. Os métodos numéricos avaliam a observabilidade pela fatoração da matriz Jacobiana $\mathbf{H}_a$, da matriz de ganho $\mathbf{G}_a$ ou da matriz de Gram (Gou; Abur, 2000; Korres, 2011); por operarem em aritmética de ponto flutuante, dependem do condicionamento dessas matrizes e da tolerância adotada para identificar pivôs nulos. Os métodos topológicos, por sua vez, baseiam-se em propriedades estruturais da rede, explorando a relação entre medidas e ramos por meio de algoritmos de teoria dos grafos (Monticelli; Wu, 1985; Krumpholz; Clements; Davis, 1980).

2.5 Processamento de Erros Grosseiros

Desde que a retirada não comprometa a observabilidade, as medidas portadoras de EGs são removidas do processo de estimação. Medidas críticas — aquelas cuja retirada compromete a observabilidade do sistema — apresentam resíduo nulo, de modo que EGs que as afetem não podem ser detectados pela análise de resíduos. Se uma medida crítica for considerada suspeita por outros meios, como os testes de pré-processamento descritos a seguir, e descartada, a observabilidade pode ser recuperada com o emprego de uma pseudomedida. Medidas com erros evidentes são identificadas ainda na etapa de pré-processamento (figura 2.2), por meio de testes, tais como a verificação do enquadramento do valor no intervalo esperado e a comparação com outras medidas redundantes e com o último valor recebido.

2.5.1 Vetor de Resíduos e Matriz de Covariância

Para a detecção e identificação dos demais EGs, o método mais utilizado no estimador por MQP é a análise de resíduos normalizados. Há alternativas, como o teste baseado no valor da função objetivo $J(\hat{\mathbf{x}})$ (teste do qui-quadrado), a identificação por teste de hipóteses (*Hypothesis Testing Identification*) e o emprego de estimadores robustos (Abur; Gomez Exposito, 2004; Monticelli, 1999). Assim, após a filtragem do estado, calculam-se os valores das medidas em função do estado estimado, estabelecendo-se a diferença entre os valores medidos e estimados.

$$\mathbf{r} = \mathbf{z} - h(\hat{\mathbf{x}}) \tag{2.18}$$

Linearizando-se o modelo de medição em torno do estado estimado, o vetor de resíduos relaciona-se com o vetor de erros das medidas por meio da matriz de sensibilidade dos resíduos $\mathbf{S}$:

$$\mathbf{r} = \mathbf{S}\,\mathbf{e}, \qquad \mathbf{S} = \mathbf{I} - \mathbf{H}\,\mathbf{G}^{-1}\mathbf{H}^{T}\mathbf{R}^{-1} \tag{2.19}$$

Como, por hipótese, os erros $\mathbf{e}$ têm distribuição normal, com média zero e matriz de covariância $\mathbf{R}$ (Equação (2.2)), o vetor de resíduos também apresenta distribuição normal, com valor esperado igual a zero e matriz de covariância $\mathbf{\Omega} = \mathbf{S}\,\mathbf{R}$, dada por:

$$\mathbf{\Omega} = \mathbf{R} - \mathbf{H}\,\mathbf{G}^{-1}\mathbf{H}^{T} \tag{2.20}$$

em que $\mathbf{G}$ é a matriz de ganho do processo de estimação, sendo dada por:

$$\mathbf{G} = \mathbf{H}^{T}\mathbf{R}^{-1}\mathbf{H} \tag{2.21}$$

A matriz $\mathbf{\Omega}$, denominada covariância dos resíduos, é utilizada tanto no processamento de EGs quanto na análise de criticalidades, pois suas propriedades refletem o grau de interação entre as medidas. Essa característica é explorada nos capítulos subsequentes desta tese.

2.5.2 Detecção e Identificação de Erros Grosseiros

O resíduo normalizado de cada medida é calculado conforme Equação (2.22).

$$r_N(i) = \frac{|z_i - h_i(\hat{\mathbf{x}})|}{\sqrt{\Omega_{(i,i)}}} = \frac{|r(i)|}{\sqrt{\Omega_{(i,i)}}} \tag{2.22}$$

Os valores normalizados são, então, confrontados com um limiar de detecção previamente estabelecido (λ), segundo a regra:

$$\begin{cases} r_N(i) \geq \lambda: & \text{a medida } i \text{ é suspeita de conter EG;} \\ r_N(i) < \lambda: & \text{não há indicação de EG na medida } i. \end{cases} \tag{2.23}$$

As medidas cujo resíduo normalizado, em módulo, iguala ou excede esse limiar são classificadas como portadoras de EG (Abur; Gomez Exposito, 2004; Monticelli, 1999).

Desde que não seja crítica e que o EG seja identificável — isto é, que a medida não pertença a um par crítico —, a medida portadora do maior resíduo normalizado é eliminada, e o processo de estimação é repetido até que todas as medidas remanescentes apresentem resíduos abaixo do limiar.

2.6 Considerações Finais

Este capítulo apresentou os fundamentos teóricos necessários ao desenvolvimento da tese. Foram discutidos o papel da EE na operação dos SEP, as etapas que compõem o processo de estimação, as formulações matemáticas baseadas nos modelos não linear e linear, e os mecanismos clássicos de análise de observabilidade e processamento de erros grosseiros. Destacou-se, ainda, a importância da matriz de covariância dos resíduos $\mathbf{\Omega}$ no processamento de EGs, bem como as limitações que surgem na presença de medidas críticas. Esses elementos fundamentam o desenvolvimento do Capítulo 3.

3 Análise de Observabilidade e Criticalidade

Este capítulo apresenta os aspectos principais da AOC. Inicialmente, abordam-se as razões pelas quais a verificação da observabilidade, considerada isoladamente, não é suficiente para avaliar o sistema de medição destinado à EE. Em seguida, apresentam-se as propriedades das C_k-ramos, C_k-meds e C_k-UMs, bem como as relações entre esses três tipos de criticalidades.

3.1 Avaliação das Vulnerabilidades da EE

A Análise de Observabilidade ocupa, há mais de cinco décadas, uma posição consolidada no processo de EE. Desde os trabalhos seminais de Schweppe e Wildes (1970), passando pela formulação topológica de Krumpholz, Clements e Davis (1980) e pelos fundamentos teóricos estabelecidos por Monticelli e Wu (1985), essa etapa tem sido tratada como antecedente à filtragem do estado: verifica-se, primeiro, se o conjunto de medidas é suficiente para determinar o estado da rede; em seguida, procede-se à estimação propriamente dita. Essa estrutura permanece, em essência, a mesma nos compêndios contemporâneos da área (Abur; Gomez Exposito, 2004; Monticelli, 1999; Ahmad, 2013).

O argumento desenvolvido nesta seção não nega a importância dessa formulação clássica nem desconsidera sua consolidação histórica. Argumenta-se, isto sim, que o escopo atribuído à etapa de Análise de Observabilidade não atende plenamente aos requisitos contemporâneos da supervisão de redes elétricas, sendo necessário o conhecimento das vulnerabilidades dos sistemas. Assim, a identificação das criticalidades tem uma finalidade instrumental: revelar essas vulnerabilidades, levando a uma maior consciência sobre a situação em que a supervisão da rede se encontra.

3.1.1 Requisitos da EE

Para que a EE cumpra adequadamente seu papel, quatro requisitos podem ser identificados:

- **Observabilidade:** existência, no conjunto de medidas disponível, de informação suficiente para determinar o estado de toda a rede. Trata-se de condição necessária, mas, como se argumentará adiante, não suficiente para assegurar os demais requisitos.
- **Confiabilidade:** capacidade do estimador de discriminar entre medidas válidas e espúrias, identificando estas últimas e processando-as conforme os critérios estabelecidos. A confiabilidade está associada à capacidade de depuração por meio da análise de resíduos — no estimador por MQP, usualmente por meio do teste dos resíduos normalizados — (Handschin *et al.*, 1975; Monticelli, 1999).
- **Qualidade:** precisão estatística e coerência interna das grandezas estimadas, refletindo o quanto o estado fornecido pela EE corresponde, dentro das margens estatísticas estabelecidas, ao estado mais provável da rede.
- **Robustez:** capacidade do processo de EE de manter os três requisitos anteriores diante de eventos adversos — perda de medidas, indisponibilidade de UMs, alterações topológicas, falhas de comunicação ou ataques cibernéticos ao sistema.

Esses quatro requisitos não são arbitrários. Cada um deles é tratado de forma autônoma na literatura clássica, como a *observabilidade* em Krumpholz, Clements e Davis (1980) e Monticelli e Wu (1985); a *confiabilidade* em Handschin *et al.* (1975) e Clements e Davis (1986); a *qualidade* nas formulações estatísticas do método MQP (Schweppe; Wildes, 1970); e a *robustez*, nos trabalhos sobre a manutenção da observabilidade diante da perda de medidas (Crainic *et al.*, 1990; Castillo *et al.*, 2008) e, mais recentemente, sobre cibersegurança (Liu; Ning; Reiter, 2011). Tais requisitos, embora teoricamente autônomos, são operacionalmente acoplados, e a análise de observabilidade clássica, ao isolar o primeiro deles, deixa de capturar esse acoplamento.

3.1.2 A limitação informacional da análise binária

A verificação da observabilidade, considerada isoladamente, não distingue entre sistemas de medição estruturalmente distintos, como se comenta a seguir.

Considere os sistemas de medição S_A e S_B, ambos observáveis. Admita que em S_A a perda de qualquer medida mantenha o sistema observável e permita a detecção de EGs via teste dos resíduos normalizados. Por outro lado, em S_B, suponha que haja ao menos uma medida crítica; uma vez removida, tal medida torna o sistema não observável. Pela análise de observabilidade clássica, S_A e S_B são equivalentes, mas, do ponto de vista operativo, são distintos. Em S_B, qualquer EG que afete a medida crítica não é detectável, nem identificável, conforme demonstrado por Clements e Davis (1986) e referenciado em (Monticelli, 1999, cap. 8) e (Abur; Gomez Exposito, 2004, cap. 5).

Esse exemplo ilustra um problema mais geral: a verificação binária da observabilidade não informa sobre a confiabilidade nem sobre a robustez do processo de EE. Um sistema observável pode conter medidas críticas (que comprometem a confiabilidade), pares críticos de medidas (que afetam o tratamento de EGs), tuplas críticas de cardinalidade superior (que prejudicam o processamento de múltiplos EGs) e ramos críticos (que interferem na detecção de erros topológicos).

Cabe ressaltar que a análise qualitativa do sistema de medição já estabelecida na literatura — identificação de medidas críticas, de conjuntos críticos e de UMs críticas — distingue S_A de S_B (Coutto Filho; Souza; Schilling, 2007; Coutto Filho; Souza; Augusto, 2014). Um sistema observável, sem medidas críticas, sem pares críticos de medidas e sem UMs críticas, mantém a observabilidade diante da perda de uma medida ou de uma UM e permite detectar e identificar um EG simples. A limitação aqui discutida refere-se, portanto, à verificação da observabilidade considerada isoladamente; a contribuição desta tese situa-se na identificação, de forma integrada, das criticalidades de cardinalidade mais elevada e das que envolvem ramos e UMs.

A literatura estabelece uma conexão entre a observabilidade da rede e a eficácia do processamento de EGs. Os trabalhos de Clements e Davis (Clements; Davis, 1986, 1988) fundamentaram essa relação ao demonstrar que elementos críticos impõem limites estruturais ao estimador: EGs em medidas críticas são indetectáveis, ao passo que EGs em pares críticos de medidas, embora detectáveis, não são identificados. Essa lógica estende-se ao domínio topológico, no qual ramos críticos inviabilizam a detecção de erros de topologia por meio da análise residual. Chen e Abur (2008) mostram que a capacidade de detectar tais falhas depende do posicionamento estratégico dos medidores. Por fim, Augusto *et al.* (2019) e Coimbra *et al.* (2021) generalizaram essas constatações para criticalidades de cardinalidade superior (C_ks), interpretando a cardinalidade como uma métrica de distância à inobservabilidade, noção relacionada à de observabilidade robusta à perda de medidas

(Crainic *et al.*, 1990; Castillo *et al.*, 2008), contribuindo para a análise de vulnerabilidades frente a múltiplos EGs simultâneos ou ataques à medição.

Em (Monticelli, 1999, cap. 7) e (Abur; Gomez Exposito, 2004, cap. 4), a análise de observabilidade é apresentada como uma etapa autônoma, dedicada à verificação do posto da matriz Jacobiana ou à identificação de ilhas observáveis, sem a incorporação sistemática da identificação de criticalidades.

Essa separação tem consequências práticas. Quando a análise de observabilidade é executada de forma autônoma, e seu resultado binário é encaminhado às demais etapas da EE, perdem-se informações estruturais que poderiam ser exploradas para o planejamento e a operação do sistema de medição. A identificação das criticalidades, que se situa na fronteira entre observabilidade e processamento de EGs, é deslocada para uma etapa posterior, dependente do resultado da filtragem do estado.

Cabe destacar que as análises de observabilidade e de criticalidade compartilham a mesma base: ambas consideram a relação entre as medidas, estabelecida pela configuração da rede e contida nas matrizes $\mathbf{H}_a$, $\mathbf{G}_a$ e $\mathbf{\Omega}_a$, e empregam as mesmas ferramentas de fatoração e análise de dependência linear. A análise de observabilidade verifica se o posto dessas matrizes é completo; a análise de criticalidades indica quão distante o posto dessas matrizes está de deixar de ser completo e por quais caminhos.

3.1.3 Implicações do conhecimento das criticalidades

O conhecimento das criticalidades tem implicações em pelo menos três frentes. Na operação, fornece informações sobre a robustez do sistema de medição, permitindo identificar antecipadamente as configurações de medição, unidades de medição e ramos cuja perda comprometeria a EE. Em termos da constituição do sistema de medição, caracteriza as proximidades à inobservabilidade da rede, expressas pela cardinalidade das tuplas críticas, fornecendo métricas para estudos de expansão e reforço do sistema de medição. Planos de medição com maior incidência de criticalidades de cardinalidade reduzida indicam maior vulnerabilidade estrutural a ser superada.

E, no âmbito da cibersegurança, em cenários de ataques cibernéticos direcionados a medidores (He; Yan, 2016; Liu; Ning; Reiter, 2011) — em particular, ataques que comprometam UMs, tornando indisponíveis as suas medidas —, o conhecimento prévio das criticalidades permite identificar quais UMs devem ser protegidas prioritariamente. Esta aplicação é desenvolvida no Capítulo 6.

A identificação das criticalidades, entretanto, é um problema de natureza combinatória, o que por décadas restringiu sua aplicação às cardinalidades mais baixas (Clements; Davis, 1986; Costa; Piazza; Mandel, 1990). Essa limitação é enfrentada nos Capítulos 4 e 5, nos quais se demonstra que as criticalidades de ramos, medidas e UMs podem ser identificadas e atualizadas em tempos da ordem de segundos.

O aproveitamento desse conhecimento depende, contudo, da compreensão das relações estruturais entre os três tipos de criticalidade. As seções seguintes apresentam as propriedades das criticalidades de ramos, medidas e UMs, que podem ser encontradas em (Coimbra, 2019) e (Coimbra *et al.*, 2021), e que constituem a base das metodologias desenvolvidas nesta tese.

3.2 Tuplas Críticas: Definições e Propriedades Gerais

Uma tupla crítica C_k é definida como um conjunto minimal de k elementos essenciais à observabilidade, sejam eles ramos (C_k-ramos), medidas (C_k-meds) ou unidades de medição (C_k-UMs). Nesta tese, uma UM corresponde à unidade de medição instalada em uma barra — o que engloba a RTU e, quando presente, a PMU —, responsável pelas medidas tomadas nessa barra, conforme o plano de medição: a injeção de potência na barra e os fluxos de potência (ou correntes) nos ramos que dela partem. A UM localizada na barra i é denotada UM_i, e sua indisponibilidade implica a perda simultânea de todas as suas medidas. Assim, uma C_1-UM corresponde ao conceito de unidade de medição (ou RTU) crítica já estabelecido na literatura (Coutto Filho; Souza; Augusto, 2014). Se uma C_k se tornar indisponível, a rede perde a observabilidade. A cardinalidade k pode ser interpretada como uma medida de distanciamento da inobservabilidade: quanto menor a cardinalidade da tupla crítica, mais próximo da inobservabilidade o sistema de medição se encontra. A partir dessa definição, decorrem duas propriedades gerais que se aplicam a qualquer elemento primário considerado crítico.

Propriedade 1: Uma C_k não contém uma C_j, $\forall\, j < k$ ($C_k \not\supset C_j$);

Propriedade 2: Quando r elementos de uma C_k ($r < k$) ficam indisponíveis, esta C_k se torna uma C_{k-r}.

A Propriedade 1 estabelece que, em uma tupla crítica, não pode haver um subconjunto j entre os k elementos que leve à não observabilidade da rede. Em outras palavras, uma C_3 não pode conter uma C_2 ou uma C_1 ($C_3 \not\supset C_2$ e $C_3 \not\supset C_1$), pois caso uma C_2 contenha uma

C_1, e essa, por sua vez, se torne indisponível, o sistema já não seria observável. Entretanto, um elemento de uma C_2 ou de uma C_3 pode fazer parte de outras tuplas críticas. Por exemplo, sendo uma C_3 composta pelos elementos (α, β, γ), qualquer elemento desse trio pode fazer duplas com outros elementos que não pertençam a essa C_3, como: (α, δ), (β, ε), (γ, η), ou trios com outros elementos como: (α, β, δ), $(\alpha, \beta, \varepsilon)$, (α, β, η), já que os elementos δ, ε, η não pertencem à referida C_3.

Como apresentado, uma tupla crítica é um conjunto minimal de elementos que leva o sistema à não observabilidade. A Propriedade 2, então, trata da redução de uma tupla crítica quando um ou mais de seus elementos se torna indisponível. A perda de um elemento de uma tupla crítica não leva o sistema à inobservabilidade, exceto quando se tratar de uma C_1, porém reduzirá a cardinalidade da tupla crítica. Tomando o mesmo exemplo, sendo uma C_3 (α, β, γ), a perda do elemento α altera a cardinalidade da tupla, que passa a ser uma C_2 (β, γ), bem como todas as outras tuplas das quais o elemento α faça parte terão suas cardinalidades reduzidas. Generalizando, a perda de r elementos de uma C_k a tornará uma C_{k-r}.

3.2.1 Propriedades das Criticalidades de Ramos

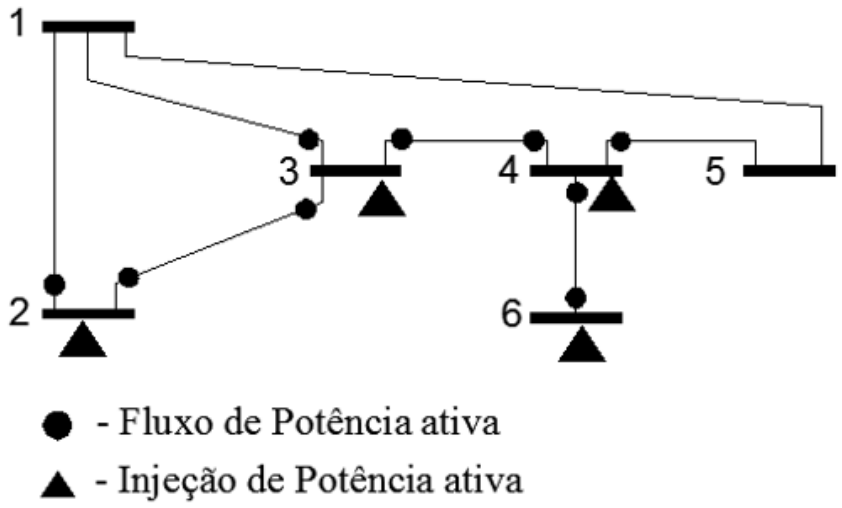
Mudanças na topologia da rede podem comprometer a EE e levar à não observabilidade do sistema. Em Clements e Davis (1988), encontram-se mais detalhes sobre a influência das C_k-ramos no processamento de EGs.

A identificação das C_k-ramos está relacionada à identificação de ilhamentos da rede. Em Theodoro *et al.* (2012), propôs-se um método algébrico-grafo, baseado na fatoração da matriz de incidência barra-ramo, para identificar os casos de ilhamento decorrentes da perda de um equipamento, bem como as barras que compõem cada ilha. A identificação exaustiva de todas as C_k-ramos até uma dada cardinalidade, por sua vez, constitui um problema de natureza combinatória, que requer, para cada alteração topológica, a execução de algoritmos com tempos de processamento compatíveis com os ambientes de planejamento e operação.

As propriedades a seguir podem ser exploradas para tornar mais eficiente a identificação de C_k-ramos. Um conceito utilizado para este fim é o de Ramo Irrelevante, definido como o ramo que não participa do processo de EE. Em outras palavras, trata-se de um ramo no qual não há medidas (fluxos ou correntes), nem incidentes (injeções) em suas barras terminais (Abur; Gomez Exposito, 2004). A Figura 3.1 apresenta, como exemplo, um sistema de 6 barras com um ramo irrelevante, no caso, o ramo $R_{1\text{-}5}$. Observa-se que

há 13 medidas e 5 variáveis de estado (ângulos, considerando o estimador linear) a serem estimadas, sendo possível determinar todas elas a partir das medidas disponíveis; são 5 variáveis, sendo uma das barras adotada como referência angular. O ramo $R_{1\text{-}5}$ é irrelevante, pois não há medidas relacionadas a ele e, portanto, não participa do processo de EE.

Figura 3.1 - Sistema de 6 barras com um ramo irrelevante



Fonte: Elaboração própria (2026).

Propriedade 3: Um conjunto de k ramos forma uma C_k-ramo se a indisponibilidade simultânea de tais ramos resulta em uma rede elétrica ilhada, desde que o mesmo não ocorra se quaisquer j ramos do mesmo conjunto ($j < k$) se tornarem indisponíveis;

Propriedade 4: Em um sistema de medição qualquer, se todos os k ramos que formam uma C_k-ramo (conforme a Propriedade 3) são ramos irrelevantes, ou estiverem indisponíveis, então a rede elétrica não é observável;

Propriedade 5: Quando r ramos ficam indisponíveis ou irrelevantes, todas as C_k-ramos ($k > r$) que contêm os r ramos tornar-se-ão C_{k-r}-ramos.

De acordo com a Propriedade 3, a determinação das criticalidades de ramos pode ser realizada apenas em função da topologia da rede, ou seja, não depende de um sistema de medição específico. Assim, se um conjunto de ramos resultar em uma rede elétrica ilhada, tal conjunto será considerado uma C_k-ramo. Como depende apenas da topologia da rede, a determinação dessas criticalidades de ramos pode ser realizada *offline*. Por outro lado, a atualização das criticalidades com base em um plano de medição específico pode ser realizada *online*, conforme a Propriedade 5.

Do ponto de vista da EE, um ramo não participará do processo de estimação se ele estiver indisponível ou se ele for um ramo irrelevante. Assim, segundo as Propriedades 3 e 4, um ramo quando indisponível ou irrelevante terá o mesmo efeito para a EE e para a atualização das C_k-ramos. Essa equivalência, que fundamenta as Propriedades 4 e 5, é explicada a seguir.

A Propriedade 4 trata conjuntamente duas situações de origens distintas, mas de mesmo efeito sobre a EE. Um ramo indisponível — por exemplo, desligado para manutenção — deixa de fazer parte da topologia da rede. Um ramo irrelevante continua fisicamente presente, mas, como não há medidas incidentes sobre ele (nem fluxo no ramo, nem injeção em suas barras terminais), sua susceptância não aparece em nenhuma linha da matriz $\mathbf{H}_a$ (Equações (2.13), (2.14) e (2.16)). Assim, a matriz $\mathbf{H}_a$ obtida com o ramo irrelevante é idêntica à que se obteria se ele fosse retirado da rede: para a EE, um ramo irrelevante equivale a um ramo indisponível.

Considere, então, uma C_k-ramo. Pela Propriedade 3, a retirada simultânea de seus k ramos ilha a rede. Se esses ramos estiverem indisponíveis, irrelevantes (pela perda das medidas incidentes sobre eles) ou parte indisponíveis e parte irrelevantes, a matriz $\mathbf{H}_a$ será a de uma rede ilhada. Nessa situação, nenhuma medida relaciona os ângulos de barras de ilhas distintas e, na ausência de medidas de ângulo — premissa adotada nesta tese —, a diferença angular entre a ilha que não contém a barra de referência e o restante da rede não pode ser determinada: somar uma mesma constante aos ângulos de todas as barras dessa ilha não altera o valor de nenhuma medida. A matriz $\mathbf{H}_a$ não tem, portanto, posto completo, e o sistema não é observável, como estabelece a Propriedade 4.

Essa equivalência também explica a Propriedade 5. As C_k-ramos definidas pela Propriedade 3 dependem apenas da topologia da rede. Para um plano de medição específico, os ramos irrelevantes devem ser tratados como retirados da rede, e as C_k-ramos de interesse passam a ser as da rede resultante, obtidas das C_k-ramos topológicas pela Propriedade 5, seguida da aplicação da Propriedade 1. É nesse sentido que um ramo irrelevante, embora fisicamente presente, reduz a cardinalidade das C_k-ramos que o contêm.

3.2.2 Propriedades das Criticalidades de Unidade de Medição

Analogamente às demais tuplas críticas, um conjunto de k UMs constitui uma C_k-UM se a indisponibilidade simultânea de todas as suas medidas torna o sistema não observável, o que não ocorre para nenhum subconjunto próprio desse conjunto. As C_k-ramos fornecem um meio de identificar as C_k-UMs, como se descreve a seguir.

Para a definição das propriedades das criticalidades de UMs, observe, primeiramente, que cada UM está associada a um ou mais ramos. Por exemplo, no sistema da Figura 3.1, o ramo $R_{4\text{-}6}$ é crítico, pois sua ausência fará com que a barra 6 fique isolada. Assim, a perda simultânea de UM_4 e UM_6 tornará o ramo $R_{4\text{-}6}$ irrelevante, pois todas as medidas que envolvem esse ramo — os fluxos em $R_{4\text{-}6}$ e as injeções nas barras 4 e 6 — pertencem a essas duas UMs e, pela Propriedade 4, a rede se tornará não observável.

Denomina-se A_k-UM o conjunto de todas as UMs que possuem medidas incidentes nos ramos que compõem uma C_k-ramo. Todas as A_k-UMs que não contiverem A_j-UMs ($\forall\, j < k$) serão consideradas C_k-UMs. Assim, valem as seguintes propriedades:

Propriedade 6: Se uma A_k-UM não contiver uma A_j-UM ($j < k$), então ela será considerada uma C_k-UM;

Propriedade 7: Quando r UMs ficam indisponíveis, todas as C_k-UMs ($k > r$) que contêm as r UMs se tornarão C_{k-r}-UMs.

A Propriedade 7 está relacionada à Propriedade 2 e serve para atualizar as criticalidades de UMs em caso de indisponibilidade.

Observa-se que o índice k de uma A_k-UM e de uma C_k-UM refere-se à cardinalidade do próprio conjunto de UMs, que não coincide necessariamente com a cardinalidade da C_k-ramo que lhe deu origem: uma mesma UM pode ter medidas incidentes em mais de um ramo da tupla, e um mesmo ramo pode ter medidas incidentes de duas UMs.

A identificação das C_k-UMs pela Propriedade 6 é completa quando cada UM permite determinar os fluxos em todos os ramos que partem de sua barra — por exemplo, quando mede os fluxos em todos esses ramos, ou a injeção e os fluxos em todos eles menos um. Nesse caso, após a perda de um conjunto de UMs, as UMs remanescentes determinam a diferença angular em todo ramo com pelo menos uma barra terminal servida por uma delas, e os demais ramos tornam-se irrelevantes. Se os ramos relevantes ainda interligassem todas as barras, o sistema permaneceria observável; logo, a perda de UMs só leva à inobservabilidade quando torna irrelevantes todos os ramos de alguma C_k-ramo, o que exige a perda de toda a A_k-UM correspondente. Assim, toda C_k-UM coincide com a A_k-UM de alguma C_k-ramo, desde que todas as C_k-ramos até a cardinalidade de interesse sejam conhecidas. Quando as UMs não determinam todos os fluxos de suas barras, a perda de UMs pode tornar o sistema não observável sem que todos os ramos de alguma C_k-ramo se tornem irrelevantes, e a identificação pela Propriedade 6 não tem garantia de completude.

3.2.3 Propriedades das Criticalidades de Medidas

Sobre a identificação das criticalidades de medidas, algumas abordagens para identificação de C_1-meds e C_2-meds podem ser encontradas em (London; Alberto; Bretas, 2007) e (Coutto Filho; Souza; Schilling, 2007). Em razão do custo computacional envolvido, são menos numerosas as metodologias para identificação de C_ks para $k > 2$, entre as quais (Sou; Sandberg; Johansson, 2012; Augusto *et al.*, 2019; Coimbra *et al.*, 2021; Nishio *et al.*, 2024).

Na análise residual, o vetor de resíduos (diferença entre os valores das medidas observadas e os valores estimados correspondentes) é normalizado e submetido à validação estatística (r_n-*test*). A matriz de covariância $\mathbf{\Omega}_a$ utilizada nesta validação é dada por:

$$\mathbf{\Omega}_a = \mathbf{I} - \mathbf{H}_a \mathbf{G}_a^{-1} \mathbf{H}_a^T \tag{3.1}$$

A matriz de covariância $\mathbf{\Omega}_a$ representa o grau de interação entre as medidas, o que pode ser explorado na análise de criticalidades. A Propriedade 8 traduz as condições de observabilidade em termos de dependência linear entre as colunas associadas às medidas.

Propriedade 8: As k colunas da matriz $\mathbf{\Omega}_a$ correspondentes às medidas que formam uma C_k-med são linearmente dependentes (Augusto *et al.*, 2017);

Essa relação de dependência também pode ser obtida por meio da fatoração triangular da matriz Jacobiana, que explicita de forma direta a relação entre medidas e estados e se beneficia de técnicas de esparsidade (London; Alberto; Bretas, 2007). Nesta tese, adota-se a verificação por submatrizes de $\mathbf{\Omega}_a$ porque ela é local — a dimensão da submatriz é igual à cardinalidade da tupla testada — e independente entre tuplas, o que permite o processamento paralelo em GPU (Capítulos 4 e 5).

As próximas propriedades valem para C_k-meds de qualquer cardinalidade e estão relacionadas às C_k-ramos.

Propriedade 9: O conjunto de k medidas que, ao ficarem simultaneamente indisponíveis, tornam irrelevantes todos os ramos que constituem uma C_k-ramo forma uma C_k-med. De acordo com a Propriedade 1, isso é verdadeiro desde que não ocorra para nenhum subconjunto do grupo;

Propriedade 10: Quando r medidas ficam indisponíveis, todas as C_k-meds ($k > r$) que contêm as r medidas tornam-se C_{k-r}-meds.

A Propriedade 9 está de acordo com a Propriedade 4 e, assim como nas Propriedades 5 e 7, a Propriedade 10 está relacionada à Propriedade Geral 2.

4 Identificação de Criticalidades de Ramos

As criticalidades de ramos ocupam uma posição estruturalmente fundamental entre os três tipos de criticalidades. Partindo das criticalidades de ramos, é possível obter diretamente as C_k-UMs, sem precisar combiná-las, e encontrar algumas C_k-meds em um espaço de busca reduzido.

Durante a realização deste trabalho de pesquisa, duas metodologias foram desenvolvidas para determinar as criticalidades de ramos, uma aqui denominada Offline e outra denominada Online. Na primeira, as criticalidades de ramos são determinadas unicamente a partir da topologia da rede, podendo posteriormente ser atualizadas para topologias e planos de medição específicos. Na segunda, as criticalidades de ramos são identificadas já considerando a topologia e o sistema de medição de interesse para análise. Para se obter as criticalidades de ramos, foi utilizado o Algoritmo de Kruskal (Cormen *et al.*, 2009) (aqui referido como Abordagem Topológica), ou um método que lança mão de um plano de medição hipotético que permite transformar o problema de identificação de criticalidades de ramos em um problema de identificação de criticalidades de medidas (aqui referido como Abordagem Numérica). Tais abordagens e métodos serão descritos a seguir.

4.1 O problema combinatório da identificação das Criticalidades de Ramos

Pela Propriedade 3 apresentada no Capítulo 3, um conjunto de k ramos forma uma C_k-ramo se sua indisponibilidade simultânea resultar no ilhamento da rede, desde que nenhum subconjunto próprio desse conjunto produza o mesmo efeito. A identificação de todas as C_k-ramos exige, em princípio, apenas a verificação do ilhamento da rede — isto é, da conectividade do grafo — para a indisponibilidade de cada possível combinação de ramos, sem necessidade de análise de observabilidade. A identificação de ilhamentos pode ser realizada, por exemplo, pelo método algébrico-grafo de Theodoro *et al.* (2012),

baseado na fatoração da matriz de incidência barra-ramo.

Considerando uma rede com N_R ramos, o número de combinações possíveis de k ramos é dado pelo coeficiente binomial $\binom{N_R}{k}$. A avaliação exaustiva de todas as criticalidades de cardinalidade até um valor $k_{\max}$ demanda, portanto, a análise de N_C combinações, onde:

$$N_C = \sum_{k=1}^{k_{\max}} \binom{N_R}{k} \tag{4.1}$$

A quantidade de combinações cresce rapidamente com N_R e com $k_{\max}$, caracterizando o problema, quando tratado por enumeração exaustiva, como combinatório e de elevado esforço computacional. Para o sistema IEEE 30-barras, por exemplo, que possui 41 ramos, a avaliação de combinações de 1 até 8 ramos implica analisar mais de 123 milhões de configurações distintas.

Além disso, as criticalidades de ramos podem demandar reavaliação sempre que ocorrerem alterações na topologia da rede ou no plano de medição. Embora a identificação inicial possa ser realizada antecipadamente, a viabilidade do emprego das criticalidades em ambientes de operação depende do tempo de processamento computacional da identificação e da atualização das C_k-ramos. Esses fatores motivaram posteriormente a busca por métodos eficientes para a identificação das C_k-ramos, particularmente para cardinalidades elevadas e redes de maior porte.

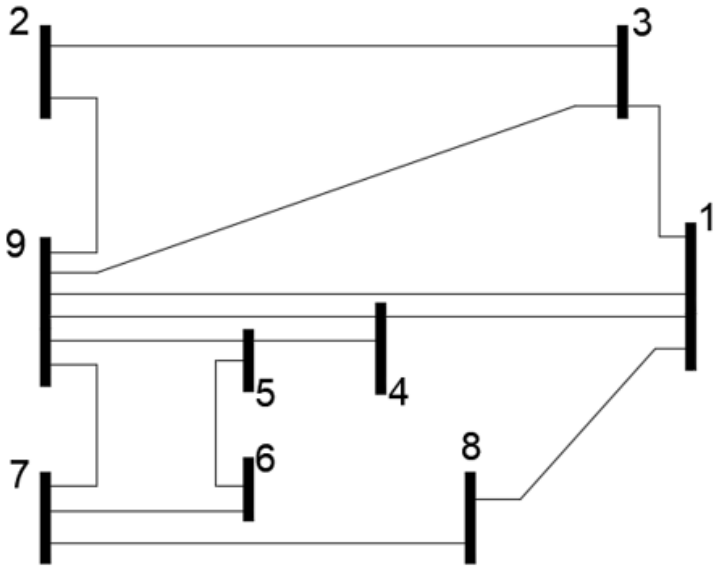
4.2 Metodologia Offline

4.2.1 Abordagem Topológica: Algoritmo de Kruskal

A primeira abordagem desenvolvida para a identificação das criticalidades de ramos, apresentada na dissertação de mestrado do autor (Coimbra, 2019) e em (Coimbra *et al.*, 2021), baseia-se exclusivamente na topologia da rede, em conformidade com a Propriedade 3. A rede elétrica é representada por um grafo não direcionado, no qual cada barra corresponde a um vértice e cada ramo a uma aresta, atribuindo-se peso unitário a todas as arestas. A Figura 4.1 ilustra um sistema de 9 barras e 14 ramos, enquanto a Figura 4.2 mostra o grafo não direcionado equivalente ao sistema 9 barras com peso unitário nas arestas.

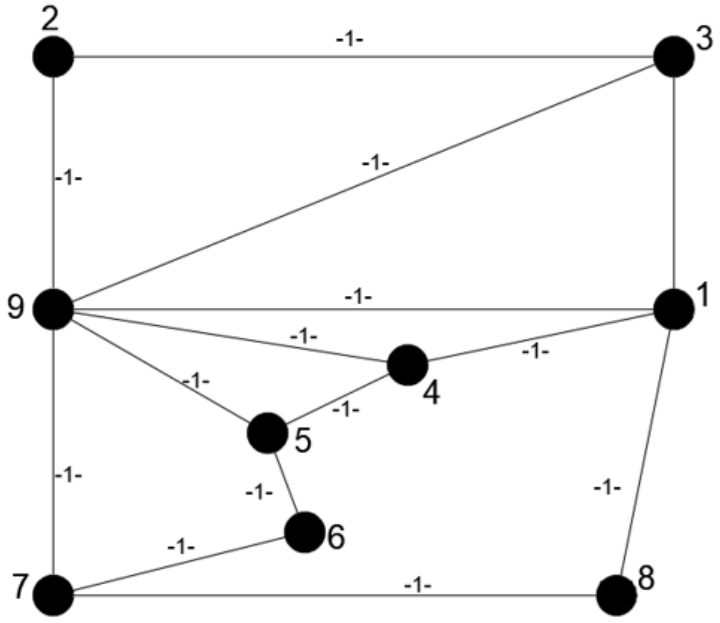
A verificação do ilhamento é realizada por meio do algoritmo de Kruskal, originalmente concebido para a determinação da Árvore Geradora Mínima (AGM) de um grafo ponderado. Uma AGM é um subconjunto de arestas que conecta todos os vértices do

Figura 4.1 - Sistema 9 barras exemplo



Fonte: Elaboração própria (2026).

Figura 4.2 - Sistema 9 barras (Grafo não direcionado com peso unitário nas arestas)



Fonte: Elaboração própria (2026).

grafo, sem formar ciclos, com soma mínima de pesos. Para um grafo conexo com N_B vértices, a AGM contém exatamente $N_B - 1$ arestas; como os pesos são unitários, o custo da AGM de uma rede conexa de N_B barras é igual a $N_B - 1$.

A identificação das criticalidades de ramos explora essa propriedade. Para um dado conjunto de k ramos, removem-se as arestas correspondentes do grafo e obtém-se a AGM do grafo resultante. Se o custo da árvore obtida for inferior a $N_B - 1$, conclui-se que

o grafo deixou de ser conexo — ou seja, a remoção daquele conjunto de ramos resultou no ilhamento da rede, caracterizando-o como uma C_k-ramo, em conformidade com a Propriedade 3. O procedimento é executado para combinações de ramos de cardinalidade crescente: primeiro individualmente, depois em pares, trios, e assim sucessivamente. Cabe observar que a mesma verificação de conectividade pode ser realizada por uma busca em largura ou em profundidade no grafo, de custo linear no número de barras e de ramos (Cormen *et al.*, 2009). O algoritmo de Kruskal foi mantido nesta tese por ser o método empregado na dissertação de mestrado do autor (Coimbra, 2019) e em (Coimbra *et al.*, 2021), servindo como referência para a comparação apresentada na Seção 4.2.3.

A abordagem topológica é conceitualmente simples. Por depender apenas da topologia da rede, é realizada de modo *offline*, considerando um modelo de rede completa (com todos os ramos existentes conectados), sendo a reavaliação necessária apenas em caso de expansão da rede. Com base nas propriedades descritas no Capítulo 3, as criticalidades de ramos identificadas *offline* podem ser facilmente atualizadas para cada configuração da rede e plano de medição específicos (Coimbra *et al.*, 2021). Entretanto, tal atualização pode falhar caso criticalidades de cardinalidade suficientemente alta não sejam obtidas, o que para sistemas de maior porte pode se tornar inviável. Cada combinação de ramos demanda a execução completa do algoritmo de Kruskal sobre o grafo, e o número de combinações cresce exponencialmente. Essa limitação motivou o desenvolvimento da abordagem numérica apresentada a seguir.

4.2.2 Abordagem Numérica

A abordagem numérica proposta (Coimbra; Souza; Coutto Filho, 2025) substitui a verificação topológica de ilhamento por uma verificação algébrica de dependência linear, realizada sobre a matriz de covariância dos resíduos. O elemento central dessa transformação é o emprego de um sistema de medição hipotético.

4.2.2.1 O Plano de Medição Hipotético

A motivação para o plano de medição hipotético decorre de uma equivalência estabelecida nas Propriedades 3 e 4. Para facilitar o entendimento, as propriedades serão novamente apresentadas.

Propriedade 3: Um conjunto de k ramos forma uma C_k-ramo se a indisponibilidade simultânea de tais ramos resulta em uma rede elétrica ilhada, desde que o mesmo não

ocorra se quaisquer j ramos do mesmo conjunto ($j < k$) se tornarem indisponíveis;

Propriedade 4: Em um sistema de medição qualquer, se todos os k ramos que formam uma C_k-ramo (conforme a Propriedade 3) são ramos irrelevantes, ou estiverem indisponíveis, então a rede elétrica não é observável;

Do ponto de vista da observabilidade, um ramo indisponível e um ramo irrelevante produzem o mesmo efeito sobre a rede. Em ambos os casos, o ramo não participa do processo de Estimação de Estado.

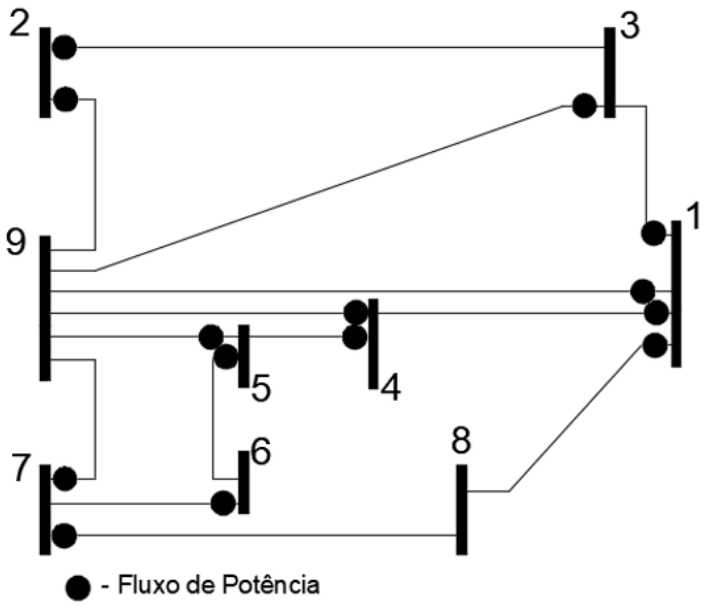
Explora-se essa equivalência considerando-se um sistema de medição hipotético composto por uma única medida de fluxo de potência ativa em cada ramo da rede. Neste sistema hipotético, a indisponibilidade da medida associada a um ramo torna esse ramo irrelevante para a EE. Por conseguinte, o efeito da indisponibilidade de um conjunto de ramos passa a corresponder, de forma exata, ao efeito da indisponibilidade do conjunto de medidas de fluxo associadas a esses ramos, ou seja, o ilhamento físico da rede é o mesmo ilhamento sob a ótica da EE.

De acordo com a Propriedade 4, se a indisponibilidade de um conjunto de k ramos resulta no ilhamento da rede, então a indisponibilidade das k medidas de fluxo nestes ramos no sistema hipotético torna a rede não observável. Em outras palavras, cada C_k-ramo da rede corresponde a uma C_k-med no sistema de medição hipotético formado pelas medidas de fluxo tomadas nos ramos que compõem a tupla crítica. A Figura 4.3 apresenta o sistema de medição hipotético associado ao sistema de 9 barras da Figura 4.1, com uma medida de fluxo de potência por ramo.

Essa correspondência vale nos dois sentidos e não depende de os ramos serem ou não irrelevantes no sistema de medição original. No sistema hipotético, com susceptâncias-série unitárias, a medida de fluxo no ramo i-k corresponde a uma linha de $\mathbf{H}_a$ com $+1$ na coluna da barra i, -1 na coluna da barra k e zeros nas demais (Equação (2.13)). Retirar as medidas de fluxo de um conjunto de ramos produz, portanto, exatamente a matriz $\mathbf{H}_a$ da rede sem esses ramos. Se a rede sem esses ramos permanecer conexa, existe uma árvore geradora formada por ramos cujas medidas de fluxo continuam disponíveis; percorrendo essa árvore a partir da barra de referência, cada medida de fluxo determina a diferença angular entre as barras terminais de seu ramo, e todos os ângulos ficam determinados, ou seja, o sistema hipotético é observável. Se, ao contrário, a rede ficar ilhada, os ângulos da ilha que não contém a barra de referência não podem ser determinados, pois somar uma mesma constante a todos eles não altera nenhum fluxo medido; o sistema hipotético

não é observável. Assim, a retirada de um conjunto de medidas de fluxo torna o sistema hipotético não observável se, e somente se, a retirada dos ramos correspondentes ilha a rede. Como essa equivalência vale para qualquer subconjunto, a condição de minimalidade também se preserva: cada C_k-ramo corresponde a uma C_k-med do sistema hipotético, e cada C_k-med do sistema hipotético corresponde a uma C_k-ramo.

Figura 4.3 - Sistema hipotético com uma medida de fluxo em cada ramo



Fonte: Elaboração própria (2026).

A adição do sistema hipotético, conforme proposto, permite que, em vez de se buscar diretamente as criticalidades de ramos por meio de verificações topológicas, se busquem as criticalidades de medidas do sistema hipotético por meio de operações numéricas, tarefa para a qual existem métodos eficientes, como o descrito a seguir.

4.2.2.2 Verificação de Criticalidades de Medidas via Matriz de Covariância dos Resíduos

A identificação das criticalidades de medidas do sistema hipotético apoia-se na Propriedade 8, que estabelece que as colunas da matriz de covariância dos resíduos $\mathbf{\Omega}_a$ associadas às medidas que formam uma C_k-med são linearmente dependentes. A matriz $\mathbf{\Omega}_a$ é dada por:

$$\mathbf{\Omega}_a = \mathbf{I} - \mathbf{H}_a \mathbf{G}_a^{-1} \mathbf{H}_a^T \tag{4.2}$$

onde $\mathbf{H}_a$ é a matriz Jacobiana associada às medidas de potência ativa e $\mathbf{G}_a = \mathbf{H}_a^T \mathbf{H}_a$

é a matriz de ganho (admitindo-se $\mathbf{R} = \mathbf{I}$ no modelo linear desacoplado).

A verificação de criticalidade de um conjunto candidato de k medidas pode ser realizada de forma localizada, processando-se apenas a submatriz $\widetilde{\mathbf{\Omega}}_a$ de $\mathbf{\Omega}_a$, composta pelas linhas e colunas associadas às medidas em análise (Augusto *et al.*, 2017). Se essas medidas formam uma C_k-med, isto é, se sua indisponibilidade simultânea torna a rede não observável, as colunas de $\widetilde{\mathbf{\Omega}}_a$ são linearmente dependentes. Essa dependência pode ser verificada pelo processo de eliminação de Gauss, aplicado à triangularização de $\widetilde{\mathbf{\Omega}}_a$: a ocorrência de um pivô nulo durante a triangularização indica a dependência linear e, portanto, a criticalidade do conjunto testado.

Os elementos da submatriz $\widetilde{\mathbf{\Omega}}_a$ são obtidos diretamente por:

$$\widetilde{\mathbf{\Omega}}_a(i,j) = -\mathbf{h}_i \, \mathbf{G}_a^{-1} \, \mathbf{h}_j^T \tag{4.3}$$

$$\widetilde{\mathbf{\Omega}}_a(i,i) = 1 - \mathbf{h}_i \, \mathbf{G}_a^{-1} \, \mathbf{h}_i^T \tag{4.4}$$

onde $\mathbf{h}_i$ e $\mathbf{h}_j$ são os vetores-linha da matriz $\mathbf{H}_a$ associados às medidas i e j, respectivamente. A matriz $\mathbf{G}_a$ é esparsa, e sua inversa pode ser calculada pelo método descrito em Monticelli (1999).

A principal vantagem dessa formulação reside no fato de que a dimensão da submatriz $\widetilde{\mathbf{\Omega}}_a$ corresponde apenas ao número de medidas na tupla testada, e não à dimensão total do sistema. Assim, o custo computacional da verificação de uma tupla independe do porte da rede, dependendo apenas da cardinalidade da tupla. Esse aspecto favorece a aplicação do método a redes de grande porte.

4.2.3 Comparação de desempenho entre a abordagem topológica (Kruskal) e numérica (Sistema Hipotético)

Esta seção apresenta os resultados da aplicação da abordagem numérica proposta à identificação das criticalidades de ramos, em comparação com a abordagem topológica baseada no algoritmo de Kruskal. As simulações foram realizadas em um processador Intel® Xeon® E5-2630 v4, 2,2 GHz.

A metodologia foi avaliada nos sistemas IEEE 14 e IEEE 30 barras. Para o sistema IEEE 14 barras, todas as criticalidades de ramos existentes foram identificadas; para o sistema IEEE 30 barras, a busca foi limitada à cardinalidade $k = 8$. As Tabelas 4.1 e 4.2

apresentam o número de C_k-ramos identificadas em cada sistema, por cardinalidade.

Tabela 4.1 - C_k-ramos identificadas *offline* — IEEE 14-barras

Cardinalidade (k)	**Número de C_k-ramos**
1	1
2	8
3	12
4	26
5	44
6	24

Fonte: Elaboração própria (2026).

Tabela 4.2 - C_k-ramos identificadas *offline* — IEEE 30-barras

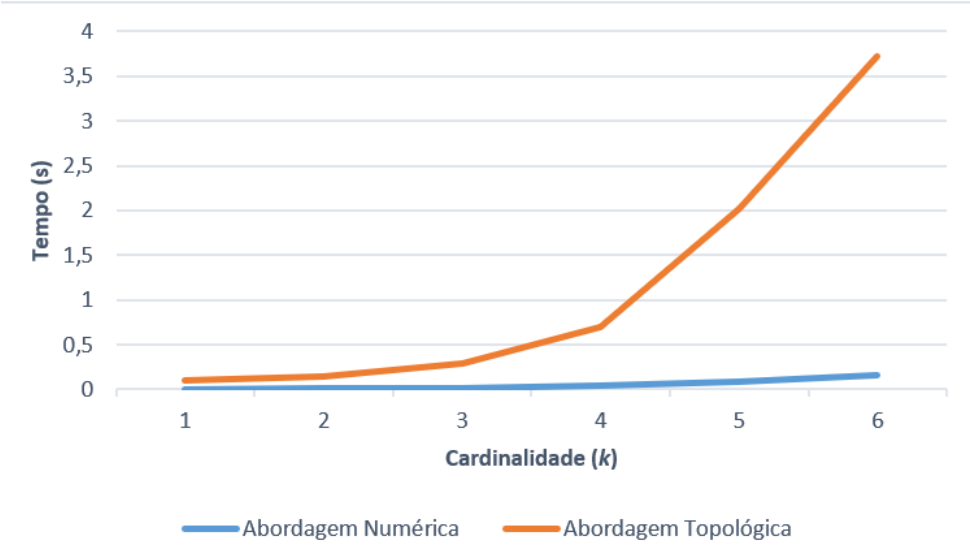
Cardinalidade (k)	**Número de C_k-ramos**
1	3
2	26
3	14
4	83
5	100
6	612
7	504
8	704

Fonte: Elaboração própria (2026).

Os resultados obtidos pela abordagem numérica proposta são idênticos aos obtidos por meio do algoritmo de Kruskal. A coincidência dos resultados nos sistemas e cardinalidades testados fornece evidência empírica da correção da implementação; a correção do método, por sua vez, decorre da correspondência entre as C_k-ramos e as C_k-meds do sistema hipotético, explicada na Seção 4.2.2.1.

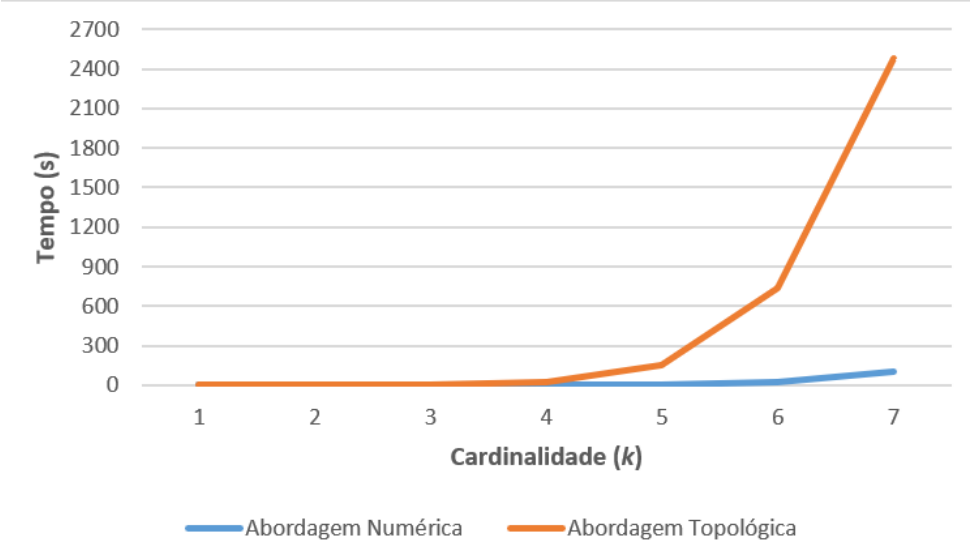
Embora ambas as abordagens conduzam ao mesmo conjunto de criticalidades, o esforço computacional difere entre elas. As Figuras 4.4 e 4.5 apresentam os tempos computacionais cumulativos, isto é, o tempo para identificar todas as C_k-ramos até cada cardinalidade, para os sistemas IEEE 14 e IEEE 30 barras, respectivamente. As Figuras 4.6 e 4.7 apresentam os tempos não cumulativos, correspondentes à identificação das C_k-ramos de cada cardinalidade isoladamente.

Figura 4.4 - Tempo computacional cumulativo IEEE 14-barras



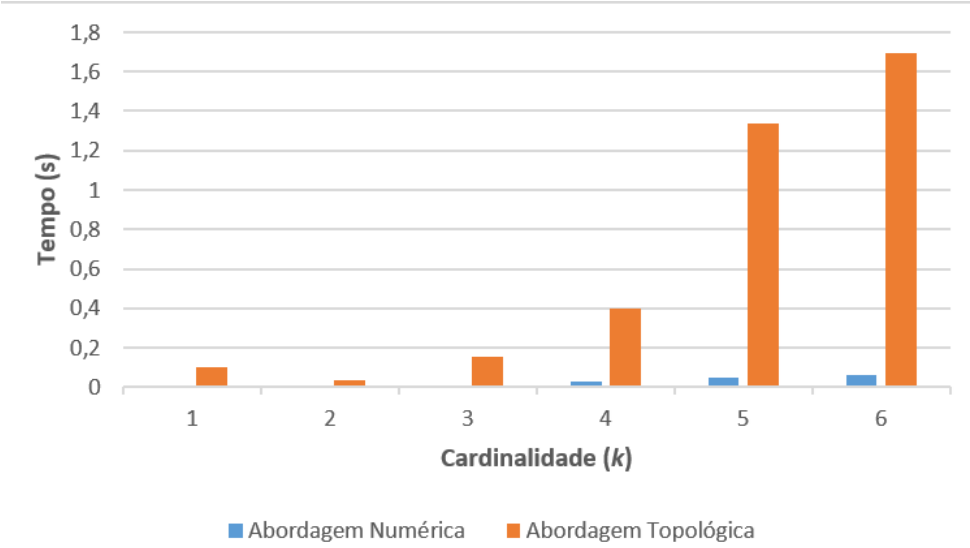
Fonte: Elaboração própria (2026).

Figura 4.5 - Tempo computacional cumulativo IEEE 30-barras



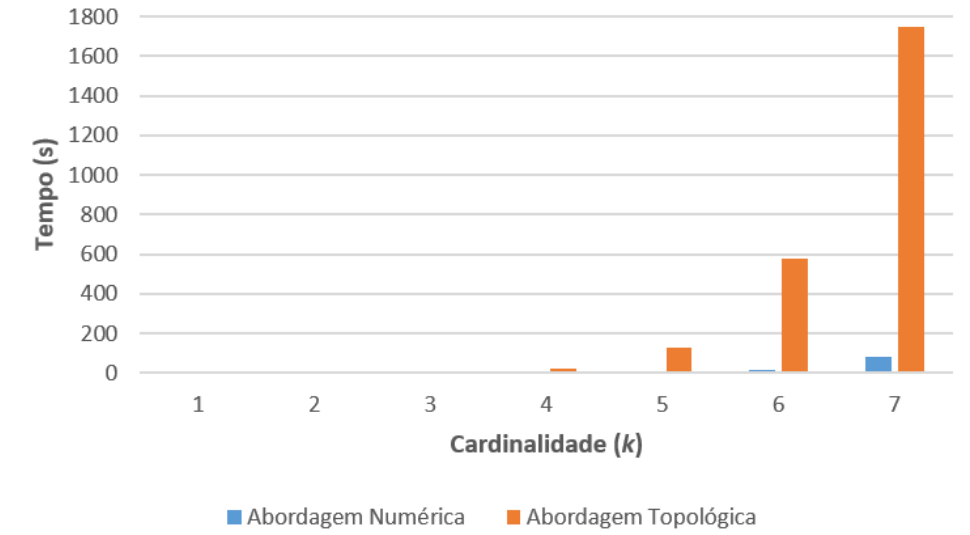
Fonte: Elaboração própria (2026).

Figura 4.6 - Tempo computacional por cardinalidade IEEE 14-barras



Fonte: Elaboração própria (2026).

Figura 4.7 - Tempo computacional por cardinalidade IEEE 30-barras



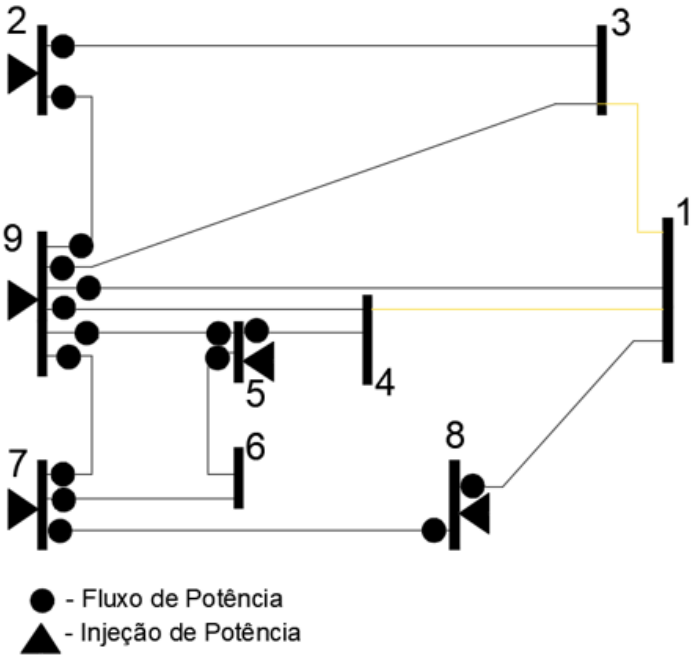
Fonte: Elaboração própria (2026).

Os resultados evidenciam que a abordagem numérica é mais eficiente que a abordagem topológica baseada no algoritmo de Kruskal, particularmente para cardinalidades elevadas. Enquanto o tempo da abordagem baseada em Kruskal cresce acentuadamente com a cardinalidade — refletindo o custo combinatório de executar o algoritmo de árvore geradora mínima para cada combinação de ramos —, a abordagem numérica mantém tempos inferiores ao longo de todas as cardinalidades avaliadas. Tal diferença é maior no sistema IEEE 30-barras, de maior porte, no qual a vantagem da abordagem numérica se acentua nas cardinalidades mais elevadas, uma vez que o número de combinações a testar é maior.

4.2.4 Atualização das Criticalidades de Ramos

Considere o plano de medição da rede de 9 barras apresentada na Figura 4.8. Observa-se que os ramos $R_{1\text{-}3}$ e $R_{1\text{-}4}$ (em destaque) são irrelevantes, ou seja, não possuem medidas incidentes e não participam do processo de estimação de estado.

Figura 4.8 - Sistema 9 Barras com Plano de Medição



Fonte: Elaboração própria (2026).

As criticalidades desse sistema podem ser determinadas de modo *offline* pelo Método Numérico ou utilizando o algoritmo de Kruskal, sem considerar o plano de medição. As criticalidades de ramos do sistema exemplo são apresentadas na Tabela 4.3.

Tabela 4.3 - Criticalidades de ramos (determinadas sem plano de medição)

Cardinalidade (k)	**C_k-ramos**
1	–
2	$(R_{1\text{-}8}, R_{7\text{-}8})$; $(R_{2\text{-}3}, R_{2\text{-}9})$; $(R_{5\text{-}6}, R_{6\text{-}7})$
3	$(R_{1\text{-}3}, R_{2\text{-}3}, R_{3\text{-}9})$; $(R_{1\text{-}3}, R_{2\text{-}9}, R_{3\text{-}9})$; $(R_{1\text{-}4}, R_{4\text{-}5}, R_{4\text{-}9})$; $(R_{1\text{-}8}, R_{5\text{-}6}, R_{7\text{-}9})$; $(R_{1\text{-}8}, R_{6\text{-}7}, R_{7\text{-}9})$; $(R_{4\text{-}5}, R_{5\text{-}6}, R_{5\text{-}9})$; $(R_{4\text{-}5}, R_{5\text{-}9}, R_{6\text{-}7})$; $(R_{5\text{-}6}, R_{7\text{-}8}, R_{7\text{-}9})$; $(R_{6\text{-}7}, R_{7\text{-}8}, R_{7\text{-}9})$

continua na página seguinte

Tabela 4.3 – continuação

Cardinalidade (k)	**C_k-ramos**
4	($R_{1\text{-}3}$, $R_{1\text{-}4}$, $R_{1\text{-}8}$, $R_{1\text{-}9}$); ($R_{1\text{-}3}$, $R_{1\text{-}4}$, $R_{1\text{-}9}$, $R_{7\text{-}8}$); ($R_{1\text{-}4}$, $R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{5\text{-}9}$); ($R_{1\text{-}4}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{6\text{-}7}$); ($R_{1\text{-}8}$, $R_{4\text{-}5}$, $R_{5\text{-}9}$, $R_{7\text{-}9}$); ($R_{4\text{-}5}$, $R_{5\text{-}9}$, $R_{7\text{-}8}$, $R_{7\text{-}9}$)
5	($R_{1\text{-}3}$, $R_{1\text{-}4}$, $R_{1\text{-}9}$, $R_{5\text{-}6}$, $R_{7\text{-}9}$); ($R_{1\text{-}3}$, $R_{1\text{-}4}$, $R_{1\text{-}9}$, $R_{6\text{-}7}$, $R_{7\text{-}9}$); ($R_{1\text{-}3}$, $R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$); ($R_{1\text{-}3}$, $R_{1\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$, $R_{7\text{-}8}$); ($R_{1\text{-}3}$, $R_{1\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{7\text{-}9}$); ($R_{1\text{-}4}$, $R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$); ($R_{1\text{-}4}$, $R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$); ($R_{1\text{-}4}$, $R_{1\text{-}8}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{7\text{-}9}$); ($R_{1\text{-}4}$, $R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{7\text{-}8}$); ($R_{1\text{-}4}$, $R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{7\text{-}8}$); ($R_{1\text{-}4}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{7\text{-}8}$, $R_{7\text{-}9}$)
6	($R_{1\text{-}3}$, $R_{1\text{-}4}$, $R_{1\text{-}9}$, $R_{4\text{-}5}$, $R_{5\text{-}9}$, $R_{7\text{-}9}$); ($R_{1\text{-}3}$, $R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{5\text{-}9}$); ($R_{1\text{-}3}$, $R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{6\text{-}7}$); ($R_{1\text{-}3}$, $R_{1\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{7\text{-}9}$); ($R_{1\text{-}3}$, $R_{1\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$, $R_{6\text{-}7}$, $R_{7\text{-}9}$); ($R_{1\text{-}3}$, $R_{1\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{5\text{-}9}$, $R_{7\text{-}8}$); ($R_{1\text{-}3}$, $R_{1\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{6\text{-}7}$, $R_{7\text{-}8}$); ($R_{1\text{-}4}$, $R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{5\text{-}6}$, $R_{7\text{-}9}$); ($R_{1\text{-}4}$, $R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{6\text{-}7}$, $R_{7\text{-}9}$); ($R_{1\text{-}4}$, $R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{5\text{-}6}$, $R_{7\text{-}9}$); ($R_{1\text{-}4}$, $R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{6\text{-}7}$, $R_{7\text{-}9}$); ($R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$); ($R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$); ($R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$, $R_{7\text{-}8}$); ($R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{7\text{-}9}$); ($R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$, $R_{7\text{-}8}$); ($R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{7\text{-}9}$)
7	($R_{1\text{-}4}$, $R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{5\text{-}9}$, $R_{7\text{-}9}$); ($R_{1\text{-}4}$, $R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{5\text{-}9}$, $R_{7\text{-}9}$); ($R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{5\text{-}9}$); ($R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{6\text{-}7}$); ($R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{5\text{-}9}$); ($R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{6\text{-}7}$); ($R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{7\text{-}9}$); ($R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$, $R_{6\text{-}7}$, $R_{7\text{-}9}$); ($R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{5\text{-}9}$, $R_{7\text{-}8}$); ($R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{6\text{-}7}$, $R_{7\text{-}8}$); ($R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{7\text{-}9}$); ($R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$, $R_{6\text{-}7}$, $R_{7\text{-}9}$); ($R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{5\text{-}9}$, $R_{7\text{-}8}$); ($R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{6\text{-}7}$, $R_{7\text{-}8}$)

Partindo da base de dados de criticalidades de ramos determinada *offline*, aplica-se a Propriedade 5.

Propriedade 5: Quando r ramos ficam indisponíveis ou irrelevantes, todas as C_k-ramos ($\forall\, k > r$) que contêm os r ramos se tornarão C_{k-r}-ramos.

A Tabela 4.4 apresenta as criticalidades de ramos determinadas *offline*, com destaque para os ramos irrelevantes. Todas as C_k-ramos que possuem um ramo irrelevante se tornarão C_{k-r}-ramos.

Tabela 4.4 - Criticalidades de ramos com ramos irrelevantes em destaque

Cardinalidade (k)	**C_k-ramos**
1	–
2	($R_{1\text{-}8}$, $R_{7\text{-}8}$); ($R_{2\text{-}3}$, $R_{2\text{-}9}$); ($R_{5\text{-}6}$, $R_{6\text{-}7}$)
3	($\mathbf{R_{1\text{-}3}}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$); ($\mathbf{R_{1\text{-}3}}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$); ($\mathbf{R_{1\text{-}4}}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$); ($R_{1\text{-}8}$, $R_{5\text{-}6}$, $R_{7\text{-}9}$); ($R_{1\text{-}8}$, $R_{6\text{-}7}$, $R_{7\text{-}9}$); ($R_{4\text{-}5}$, $R_{5\text{-}6}$, $R_{5\text{-}9}$); ($R_{4\text{-}5}$, $R_{5\text{-}9}$, $R_{6\text{-}7}$); ($R_{5\text{-}6}$, $R_{7\text{-}8}$, $R_{7\text{-}9}$); ($R_{6\text{-}7}$, $R_{7\text{-}8}$, $R_{7\text{-}9}$)
4	($\mathbf{R_{1\text{-}3}}$, $\mathbf{R_{1\text{-}4}}$, $R_{1\text{-}8}$, $R_{1\text{-}9}$); ($\mathbf{R_{1\text{-}3}}$, $\mathbf{R_{1\text{-}4}}$, $R_{1\text{-}9}$, $R_{7\text{-}8}$); ($\mathbf{R_{1\text{-}4}}$, $R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{5\text{-}9}$); ($\mathbf{R_{1\text{-}4}}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{6\text{-}7}$); ($R_{1\text{-}8}$, $R_{4\text{-}5}$, $R_{5\text{-}9}$, $R_{7\text{-}9}$); ($R_{4\text{-}5}$, $R_{5\text{-}9}$, $R_{7\text{-}8}$, $R_{7\text{-}9}$)
5	($\mathbf{R_{1\text{-}3}}$, $\mathbf{R_{1\text{-}4}}$, $R_{1\text{-}9}$, $R_{5\text{-}6}$, $R_{7\text{-}9}$); ($\mathbf{R_{1\text{-}3}}$, $\mathbf{R_{1\text{-}4}}$, $R_{1\text{-}9}$, $R_{6\text{-}7}$, $R_{7\text{-}9}$); ($\mathbf{R_{1\text{-}3}}$, $R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$); ($\mathbf{R_{1\text{-}3}}$, $R_{1\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$, $R_{7\text{-}8}$); ($\mathbf{R_{1\text{-}3}}$, $R_{1\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{7\text{-}9}$); ($\mathbf{R_{1\text{-}4}}$, $R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$); ($\mathbf{R_{1\text{-}4}}$, $R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$); ($\mathbf{R_{1\text{-}4}}$, $R_{1\text{-}8}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{7\text{-}9}$); ($\mathbf{R_{1\text{-}4}}$, $R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{7\text{-}8}$); ($\mathbf{R_{1\text{-}4}}$, $R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{7\text{-}8}$); ($\mathbf{R_{1\text{-}4}}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{7\text{-}8}$, $R_{7\text{-}9}$)
6	($\mathbf{R_{1\text{-}3}}$, $\mathbf{R_{1\text{-}4}}$, $R_{1\text{-}9}$, $R_{4\text{-}5}$, $R_{5\text{-}9}$, $R_{7\text{-}9}$); ($\mathbf{R_{1\text{-}3}}$, $R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{5\text{-}9}$); ($\mathbf{R_{1\text{-}3}}$, $R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{6\text{-}7}$); ($\mathbf{R_{1\text{-}3}}$, $R_{1\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{7\text{-}9}$); ($\mathbf{R_{1\text{-}3}}$, $R_{1\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$, $R_{6\text{-}7}$, $R_{7\text{-}9}$); ($\mathbf{R_{1\text{-}3}}$, $R_{1\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{5\text{-}9}$, $R_{7\text{-}8}$); ($\mathbf{R_{1\text{-}3}}$, $R_{1\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{6\text{-}7}$, $R_{7\text{-}8}$); ($\mathbf{R_{1\text{-}4}}$, $R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{5\text{-}6}$, $R_{7\text{-}9}$); ($\mathbf{R_{1\text{-}4}}$, $R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{6\text{-}7}$, $R_{7\text{-}9}$); ($\mathbf{R_{1\text{-}4}}$, $R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{5\text{-}6}$, $R_{7\text{-}9}$); ($\mathbf{R_{1\text{-}4}}$, $R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{6\text{-}7}$, $R_{7\text{-}9}$); ($R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$); ($R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$); ($R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$, $R_{7\text{-}8}$); ($R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{7\text{-}9}$); ($R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$, $R_{7\text{-}8}$); ($R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{7\text{-}9}$)

continua na página seguinte

Tabela 4.4 – continuação

Cardinalidade (k)	**C_k-ramos**
7	($\underline{\mathbf{R_{1\text{-}4}}}$, $R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{5\text{-}9}$, $R_{7\text{-}9}$); ($\underline{\mathbf{R_{1\text{-}4}}}$, $R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{5\text{-}9}$, $R_{7\text{-}9}$); ($R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{5\text{-}9}$); ($R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{6\text{-}7}$); ($R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{5\text{-}9}$); ($R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{6\text{-}7}$); ($R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{7\text{-}9}$); ($R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$, $R_{6\text{-}7}$, $R_{7\text{-}9}$); ($R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{5\text{-}9}$, $R_{7\text{-}8}$); ($R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{6\text{-}7}$, $R_{7\text{-}8}$); ($R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{7\text{-}9}$); ($R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$, $R_{6\text{-}7}$, $R_{7\text{-}9}$); ($R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{5\text{-}9}$, $R_{7\text{-}8}$); ($R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{6\text{-}7}$, $R_{7\text{-}8}$)

A Tabela 4.5 apresenta as novas C_{k-r}-ramos (em destaque) após a retirada dos ramos irrelevantes. Observa-se que a tabela apresenta criticalidades que não respeitam a Propriedade 1.

Propriedade 1: Uma C_k não contém uma C_j, $\forall\, j < k$.

Observa-se, por exemplo, que após a atualização surgiu a dupla $(R_{2\text{-}3}, R_{3\text{-}9})$. Entretanto, a base de criticalidades já continha a sêxtupla $(R_{1\text{-}8}, R_{1\text{-}9}, R_{2\text{-}3}, R_{3\text{-}9}, R_{4\text{-}5}, R_{4\text{-}9})$, que contém a nova dupla. Portanto, essa sêxtupla deve ser removida para que a Propriedade 1 seja respeitada.

Tabela 4.5 - Criticalidades de ramos com C_{k-r}-ramos

Cardinalidade (k)	**C_k-ramos**
1	–
2	($R_{1\text{-}8}$, $R_{7\text{-}8}$); ($R_{2\text{-}3}$, $R_{2\text{-}9}$); ($R_{5\text{-}6}$, $R_{6\text{-}7}$); ($\underline{\mathbf{R_{2\text{-}3}, R_{3\text{-}9}}}$); ($\underline{\mathbf{R_{2\text{-}9}, R_{3\text{-}9}}}$); ($\underline{\mathbf{R_{4\text{-}5}, R_{4\text{-}9}}}$); ($\underline{\mathbf{R_{1\text{-}8}, R_{1\text{-}9}}}$); ($\underline{\mathbf{R_{1\text{-}9}, R_{7\text{-}8}}}$)
3	($R_{1\text{-}8}$, $R_{5\text{-}6}$, $R_{7\text{-}9}$); ($R_{1\text{-}8}$, $R_{6\text{-}7}$, $R_{7\text{-}9}$); ($R_{4\text{-}5}$, $R_{5\text{-}6}$, $R_{5\text{-}9}$); ($R_{4\text{-}5}$, $R_{5\text{-}9}$, $R_{6\text{-}7}$); ($R_{5\text{-}6}$, $R_{7\text{-}8}$, $R_{7\text{-}9}$); ($R_{6\text{-}7}$, $R_{7\text{-}8}$, $R_{7\text{-}9}$); ($\underline{\mathbf{R_{4\text{-}9}, R_{5\text{-}6}, R_{5\text{-}9}}}$); ($\underline{\mathbf{R_{4\text{-}9}, R_{5\text{-}9}, R_{6\text{-}7}}}$); ($\underline{\mathbf{R_{1\text{-}9}, R_{5\text{-}6}, R_{7\text{-}9}}}$); ($\underline{\mathbf{R_{1\text{-}9}, R_{6\text{-}7}, R_{7\text{-}9}}}$)

continua na página seguinte

Tabela 4.5 – continuação

Cardinalidade (k)	**C_k-ramos**
4	($R_{1\text{-}8}$, $R_{4\text{-}5}$, $R_{5\text{-}9}$, $R_{7\text{-}9}$); ($R_{4\text{-}5}$, $R_{5\text{-}9}$, $R_{7\text{-}8}$, $R_{7\text{-}9}$); ($\mathbf{R_{1\text{-}8}}$, $\mathbf{R_{1\text{-}9}}$, $\mathbf{R_{4\text{-}5}}$, $\mathbf{R_{4\text{-}9}}$); ($\mathbf{R_{1\text{-}9}}$, $\mathbf{R_{4\text{-}5}}$, $\mathbf{R_{4\text{-}9}}$, $\mathbf{R_{7\text{-}8}}$); ($\mathbf{R_{1\text{-}9}}$, $\mathbf{R_{4\text{-}9}}$, $\mathbf{R_{5\text{-}9}}$, $\mathbf{R_{7\text{-}9}}$); ($\mathbf{R_{1\text{-}8}}$, $\mathbf{R_{1\text{-}9}}$, $\mathbf{R_{2\text{-}3}}$, $\mathbf{R_{3\text{-}9}}$); ($\mathbf{R_{1\text{-}8}}$, $\mathbf{R_{1\text{-}9}}$, $\mathbf{R_{2\text{-}9}}$, $\mathbf{R_{3\text{-}9}}$); ($\mathbf{R_{1\text{-}8}}$, $\mathbf{R_{4\text{-}9}}$, $\mathbf{R_{5\text{-}9}}$, $\mathbf{R_{7\text{-}9}}$); ($\mathbf{R_{1\text{-}9}}$, $\mathbf{R_{2\text{-}3}}$, $\mathbf{R_{3\text{-}9}}$, $\mathbf{R_{7\text{-}8}}$); ($\mathbf{R_{1\text{-}9}}$, $\mathbf{R_{2\text{-}9}}$, $\mathbf{R_{3\text{-}9}}$, $\mathbf{R_{7\text{-}8}}$); ($\mathbf{R_{4\text{-}9}}$, $\mathbf{R_{5\text{-}9}}$, $\mathbf{R_{7\text{-}8}}$, $\mathbf{R_{7\text{-}9}}$); ($\mathbf{R_{1\text{-}9}}$, $\mathbf{R_{4\text{-}5}}$, $\mathbf{R_{5\text{-}9}}$, $\mathbf{R_{7\text{-}9}}$)
5	($\mathbf{R_{1\text{-}8}}$, $\mathbf{R_{1\text{-}9}}$, $\mathbf{R_{4\text{-}9}}$, $\mathbf{R_{5\text{-}6}}$, $\mathbf{R_{5\text{-}9}}$); ($\mathbf{R_{1\text{-}8}}$, $\mathbf{R_{1\text{-}9}}$, $\mathbf{R_{4\text{-}9}}$, $\mathbf{R_{5\text{-}9}}$, $\mathbf{R_{6\text{-}7}}$); ($\mathbf{R_{1\text{-}9}}$, $\mathbf{R_{4\text{-}5}}$, $\mathbf{R_{4\text{-}9}}$, $\mathbf{R_{5\text{-}6}}$, $\mathbf{R_{7\text{-}9}}$); ($\mathbf{R_{1\text{-}9}}$, $\mathbf{R_{4\text{-}5}}$, $\mathbf{R_{4\text{-}9}}$, $\mathbf{R_{6\text{-}7}}$, $\mathbf{R_{7\text{-}9}}$); ($\mathbf{R_{1\text{-}9}}$, $\mathbf{R_{4\text{-}9}}$, $\mathbf{R_{5\text{-}6}}$, $\mathbf{R_{5\text{-}9}}$, $\mathbf{R_{7\text{-}8}}$); ($\mathbf{R_{1\text{-}9}}$, $\mathbf{R_{4\text{-}9}}$, $\mathbf{R_{5\text{-}9}}$, $\mathbf{R_{6\text{-}7}}$, $\mathbf{R_{7\text{-}8}}$); ($\mathbf{R_{1\text{-}9}}$, $\mathbf{R_{2\text{-}3}}$, $\mathbf{R_{3\text{-}9}}$, $\mathbf{R_{5\text{-}6}}$, $\mathbf{R_{7\text{-}9}}$); ($\mathbf{R_{1\text{-}9}}$, $\mathbf{R_{2\text{-}3}}$, $\mathbf{R_{3\text{-}9}}$, $\mathbf{R_{6\text{-}7}}$, $\mathbf{R_{7\text{-}9}}$); ($\mathbf{R_{1\text{-}9}}$, $\mathbf{R_{2\text{-}9}}$, $\mathbf{R_{3\text{-}9}}$, $\mathbf{R_{5\text{-}6}}$, $\mathbf{R_{7\text{-}9}}$); ($\mathbf{R_{1\text{-}9}}$, $\mathbf{R_{2\text{-}9}}$, $\mathbf{R_{3\text{-}9}}$, $\mathbf{R_{6\text{-}7}}$, $\mathbf{R_{7\text{-}9}}$)
6	($R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$); ($R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$); ($R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$, $R_{7\text{-}8}$); ($R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{7\text{-}9}$); ($R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$, $R_{7\text{-}8}$); ($R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{7\text{-}9}$); ($\mathbf{R_{1\text{-}9}}$, $\mathbf{R_{2\text{-}3}}$, $\mathbf{R_{3\text{-}9}}$, $\mathbf{R_{4\text{-}5}}$, $\mathbf{R_{5\text{-}9}}$, $\mathbf{R_{7\text{-}9}}$); ($\mathbf{R_{1\text{-}9}}$, $\mathbf{R_{2\text{-}9}}$, $\mathbf{R_{3\text{-}9}}$, $\mathbf{R_{4\text{-}5}}$, $\mathbf{R_{5\text{-}9}}$, $\mathbf{R_{7\text{-}9}}$)
7	($R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{5\text{-}9}$); ($R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{6\text{-}7}$); ($R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{5\text{-}9}$); ($R_{1\text{-}8}$, $R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{6\text{-}7}$); ($R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{7\text{-}9}$); ($R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$, $R_{6\text{-}7}$, $R_{7\text{-}9}$); ($R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{5\text{-}9}$, $R_{7\text{-}8}$); ($R_{1\text{-}9}$, $R_{2\text{-}3}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{6\text{-}7}$, $R_{7\text{-}8}$); ($R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{7\text{-}9}$); ($R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}5}$, $R_{4\text{-}9}$, $R_{6\text{-}7}$, $R_{7\text{-}9}$); ($R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{5\text{-}9}$, $R_{7\text{-}8}$); ($R_{1\text{-}9}$, $R_{2\text{-}9}$, $R_{3\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{6\text{-}7}$, $R_{7\text{-}8}$)

A Tabela 4.6 apresenta as criticalidades de ramos após o processo de atualização e refinamento, e a Tabela 4.7 a quantidade de C_k-ramos por cardinalidade.

Tabela 4.6 - Criticalidades de ramos atualizadas

Cardinalidade (k)	**C_k-ramos**
1	–
2	($R_{1\text{-}8}$, $R_{7\text{-}8}$); ($R_{2\text{-}3}$, $R_{2\text{-}9}$); ($R_{5\text{-}6}$, $R_{6\text{-}7}$); ($R_{2\text{-}3}$, $R_{3\text{-}9}$); ($R_{2\text{-}9}$, $R_{3\text{-}9}$); ($R_{4\text{-}5}$, $R_{4\text{-}9}$); ($R_{1\text{-}8}$, $R_{1\text{-}9}$); ($R_{1\text{-}9}$, $R_{7\text{-}8}$)
3	($R_{1\text{-}8}$, $R_{5\text{-}6}$, $R_{7\text{-}9}$); ($R_{1\text{-}8}$, $R_{6\text{-}7}$, $R_{7\text{-}9}$); ($R_{4\text{-}5}$, $R_{5\text{-}6}$, $R_{5\text{-}9}$); ($R_{4\text{-}5}$, $R_{5\text{-}9}$, $R_{6\text{-}7}$); ($R_{5\text{-}6}$, $R_{7\text{-}8}$, $R_{7\text{-}9}$); ($R_{6\text{-}7}$, $R_{7\text{-}8}$, $R_{7\text{-}9}$); ($R_{4\text{-}9}$, $R_{5\text{-}6}$, $R_{5\text{-}9}$); ($R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{6\text{-}7}$); ($R_{1\text{-}9}$, $R_{5\text{-}6}$, $R_{7\text{-}9}$); ($R_{1\text{-}9}$, $R_{6\text{-}7}$, $R_{7\text{-}9}$)
4	($R_{1\text{-}8}$, $R_{4\text{-}5}$, $R_{5\text{-}9}$, $R_{7\text{-}9}$); ($R_{4\text{-}5}$, $R_{5\text{-}9}$, $R_{7\text{-}8}$, $R_{7\text{-}9}$); ($R_{1\text{-}9}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{7\text{-}9}$); ($R_{1\text{-}8}$, $R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{7\text{-}9}$); ($R_{4\text{-}9}$, $R_{5\text{-}9}$, $R_{7\text{-}8}$, $R_{7\text{-}9}$); ($R_{1\text{-}9}$, $R_{4\text{-}5}$, $R_{5\text{-}9}$, $R_{7\text{-}9}$)

Tabela 4.7 - Quantidade de C_k-ramos por cardinalidade

Cardinalidade (k)	**Número de C_k-ramos**
1	0
2	8
3	10
4	6
5	0
6	0
7	0

Fonte: Elaboração própria (2026).

Embora o processo de atualização de C_k-ramos tenha baixo custo computacional, sua taxa de sucesso depende de a etapa *offline* ter encontrado criticalidades de ramos para a rede completa com cardinalidade suficientemente elevada para que todas as criticalidades das cardinalidades de interesse sejam encontradas para configurações de rede e planos de medição específicos. A seção seguinte apresenta resultados que ilustram a dificuldade de se encontrar todas as criticalidades de interesse quando a etapa *offline* não foi adequadamente realizada.

4.2.5 Desafios no processo de atualização das criticalidades de ramos

O processo de atualização da base de criticalidades de ramos tem a vantagem de dispensar nova busca combinatória diante de uma ampliação do plano de medição. Por exemplo,

a inserção de uma medida de fluxo no ramo irrelevante $R_{1\text{-}3}$ do sistema da Figura 4.8, tornando-o relevante, exige apenas que o processo de atualização seja refeito. Entretanto, a determinação de todas as criticalidades de ramos de modo *offline* é inviável para sistemas de grande porte. Dependendo do porte do sistema, mesmo a identificação de todas as criticalidades de cardinalidade ainda bastante inferior à cardinalidade máxima se torna inviável. A pergunta que surge então é: é possível determinar até que cardinalidade se deve avançar de modo *offline* para se encontrar todas as criticalidades até um k de interesse para uma dada configuração de rede e plano de medição específicos?

Não se dispõe, neste trabalho, de uma relação analítica que determine essa cardinalidade. Esta seção apresenta um estudo com o sistema IEEE 118 barras de forma a ilustrar o problema e mostrar o efeito da identificação insuficiente das C_k-ramos na etapa *offline*. Nas simulações realizadas, buscou-se determinar as criticalidades de ramos até $k = 4$ para um plano de medição específico por meio do processo de atualização, partindo de C_k-ramos de diferentes cardinalidades identificadas *offline*, ainda sem levar em consideração o plano de medição, mas apenas a topologia da rede. Os resultados são apresentados nas Tabelas 4.8 a 4.10 considerando sistemas de medição com diferentes níveis de redundância. Observa-se que em sistemas com menor redundância e, por consequência, maior número de ramos irrelevantes, é necessário um esforço maior na determinação das criticalidades *offline* para que todas as criticalidades de ramos até $k = 4$ sejam encontradas quando é feita a atualização para o plano de medição corrente. Para o sistema IEEE 118-barras, para encontrar todas as C_k-ramos *offline* para a cardinalidade $k = 8$ foi necessário analisar 23,4 trilhões de combinações de ramos. Para sistemas de maior porte, isto se tornaria inviável. As colunas (Até $k = n$) representam a cardinalidade máxima utilizada na atualização com objetivo de determinar as C_k-ramos até $k = 4$.

Tabela 4.8 - IEEE 118 com 68 UMs e 11 ramos irrelevantes

Cardinalidade da C_k-ramo (Atualização)	**Identificação *offline* das C_k-ramos** (%)				
	Até $k = 4$	**Até $k = 5$**	**Até $k = 6$**	**Até $k = 7$**	**Até $k = 8$**
1	100,00	100,00	100,00	100,00	100,00
2	98,50	100,00	100,00	100,00	100,00
3	92,10	100,00	100,00	100,00	100,00
4	70,80	88,88	93,80	98,10	100,00

Fonte: Elaboração própria (2026).

Tabela 4.9 - IEEE 118 com 80 UMs e 7 ramos irrelevantes

Cardinalidade da C_k-ramo (Atualização)	**Identificação *offline* das C_k-ramos** (%)				
	Até $k = 4$	**Até $k = 5$**	**Até $k = 6$**	**Até $k = 7$**	**Até $k = 8$**
1	100,00	100,00	100,00	100,00	100,00
2	100,00	100,00	100,00	100,00	100,00
3	86,40	100,00	100,00	100,00	100,00
4	85,90	97,80	100,00	100,00	100,00

Fonte: Elaboração própria (2026).

Tabela 4.10 - IEEE 118 com 92 UMs e 4 ramos irrelevantes

Cardinalidade da C_k-ramo (Atualização)	**Identificação *offline* das C_k-ramos** (%)				
	Até $k = 4$	**Até $k = 5$**	**Até $k = 6$**	**Até $k = 7$**	**Até $k = 8$**
1	100,00	100,00	100,00	100,00	100,00
2	100,00	100,00	100,00	100,00	100,00
3	95,90	100,00	100,00	100,00	100,00
4	87,40	97,80	100,00	100,00	100,00

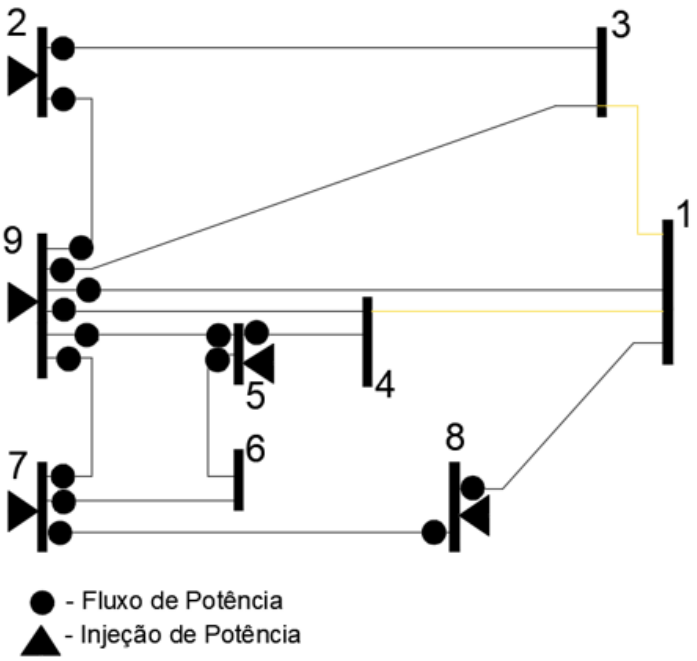
Fonte: Elaboração própria (2026).

4.3 Metodologia Online

Como foi demonstrado na seção anterior, pode ser necessário determinar *offline* criticalidades de ramos de cardinalidade elevada para que o resultado do processo de atualização das C_k-ramos para um dado sistema de medição (principalmente os de menor redundância) seja confiável. A falta de algumas tuplas críticas de ramos, após o processo de atualização, compromete a capacidade da metodologia a ser apresentada no próximo capítulo de encontrar as criticalidades de medidas e de UMs.

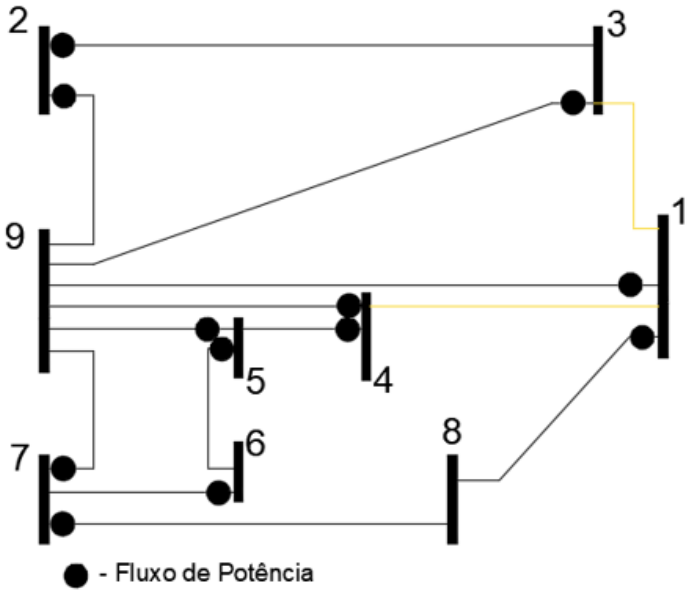
Na Metodologia Online, a abordagem numérica apresentada na Seção 4.2.2 é novamente utilizada. Entretanto, para a identificação das C_k-ramos, o sistema hipotético já não considera medidas de fluxo de potência em ramos irrelevantes, uma vez que tais ramos não participam das C_k-ramos, levando com isso a uma redução na quantidade de ramos (medidas de fluxo) a serem combinados. A Figura 4.9 retoma o sistema exemplo de 9 barras, no qual os ramos irrelevantes $R_{1\text{-}3}$ e $R_{1\text{-}4}$ estão destacados. A Figura 4.10 apresenta o sistema hipotético equivalente, com uma medida de fluxo em cada ramo, exceto nos ramos irrelevantes $R_{1\text{-}3}$ e $R_{1\text{-}4}$.

Figura 4.9 - Sistema 9 Barras com Plano de Medição



Fonte: Elaboração própria (2026).

Figura 4.10 - Sistema hipotético sem medidas nos ramos irrelevantes



Fonte: Elaboração própria (2026).

Aplica-se novamente o método numérico, transformando a busca por criticalidades de ramos em uma busca por criticalidades de medidas. O resultado obtido é o mesmo apresentado na Tabela 4.6, sem a necessidade do processo de atualização.

Em resumo, a vantagem do emprego da Metodologia Online é que a busca pode ser realizada até uma cardinalidade de interesse, sem o risco de não encontrar todas as tuplas

críticas de ramos, o que pode acontecer durante o processo de atualização na Metodologia Offline. No restante dos resultados apresentados neste trabalho, a abordagem numérica é utilizada para determinar o conjunto de criticalidades de ramos.

4.4 Aplicação de GPUs

Mesmo com a aplicação da metodologia descrita na seção anterior, o custo computacional para sistemas de grande porte pode resultar em tempos incompatíveis com o ambiente de operação do sistema elétrico. Como exemplo, na busca de criticalidades até $k = 8$ para o sistema IEEE 300 barras, que possui 409 ramos, é necessário o teste de $1{,}85 \times 10^{16}$ combinações.

Uma possível forma de contornar este problema é o uso de GPUs. Sua aplicação original é o processamento gráfico, mas seu uso em aplicações científicas para aceleração de cálculos tem se disseminado.

Nishio *et al.* (2024) empregaram processamento paralelo em GPUs para estender a análise de criticalidades na EE a tuplas de cardinalidade 3 ou superior. Essa plataforma será utilizada nesta etapa de busca de criticalidade de ramos e, posteriormente, para busca de criticalidade de medidas, como será apresentado no Capítulo 5.

Para avaliar a metodologia com o suporte dessa plataforma, foram simulados os sistemas-teste IEEE de 14, 30 e 118 barras, que podem ser encontrados em (Souza; Coutto Filho; Guimaraens, 2026; Rocha *et al.*, 2018; Coutto Filho; Souza; Villavicencio Tafur, 2013) e o sistema IEEE 300 barras desenvolvido neste trabalho com 225 UMs completas. No sistema IEEE 118 barras, considera-se que todas as medidas associadas às UMs estão presentes. O ambiente computacional utilizado consiste em um processador Intel Core i9-9300H, 32 GB de memória RAM e uma GPU GTX 1650. Buscou-se identificar as k-tuplas críticas de ramos até a cardinalidade $k = 4$ (quadras críticas). A seguir, os resultados são apresentados e discutidos sob dois aspectos: a eficácia, medida pela correta obtenção das criticalidades, e a eficiência, medida pelo tempo computacional.

Tabela 4.11 - C_k-ramos identificadas até $k = 4$

Rede	Nº de C_k-ramos	Tempo sem GPU (s)	Tempo com GPU (s)
IEEE 14	50	0,005	0,002
IEEE 30	296	0,099	0,004
IEEE 118	260	266,772	0,928
IEEE 300	1006	-	38,083

Fonte: Elaboração própria (2026).

No sistema IEEE 14 barras, observa-se uma redução de 60% do tempo computacional, ainda que o tempo sem uso de GPU já fosse reduzido. No sistema IEEE 118 barras, a redução alcança 99% do tempo gasto. Para o sistema IEEE 300 barras, a execução sem GPU não foi realizada, uma vez que o processamento exigiria a avaliação de $1{,}126 \times 10^9$ combinações. Diante desse volume, o custo computacional esperado para a execução exclusivamente em *Central Processing Unit* (CPU) mostrou-se excessivamente elevado em relação aos recursos computacionais disponíveis, inviabilizando a realização do experimento em condições práticas.

Os resultados confirmam a eficácia da metodologia: a busca exaustiva realizada em cada sistema atestou que todas as C_k-ramos procuradas foram corretamente identificadas. No que se refere à eficiência, verifica-se que a abordagem numérica demanda tempos computacionais muito menores que os da abordagem topológica de Coimbra *et al.* (2021), constatação já registrada em Coimbra, Souza e Coutto Filho (2025) ainda sem o uso de GPUs. A esse ganho soma-se o proporcionado pelo processamento paralelo, que reduz de forma expressiva os tempos, sobretudo nos sistemas de maior porte.

4.5 Considerações Finais

Este capítulo apresentou uma abordagem numérica eficiente para a identificação das criticalidades de ramos, baseada no conceito de sistema de medição hipotético. A ideia central consiste em transformar o problema de identificação de criticalidades de ramos, tradicionalmente tratado por meio de verificações topológicas, em um problema de identificação de criticalidades de medidas, resolvido por operações numéricas localizadas sobre a matriz de covariância dos resíduos.

Os resultados demonstraram que a abordagem numérica conduz exatamente às mesmas criticalidades obtidas pela abordagem topológica, porém com esforço computacional

menor que o da implementação baseada no algoritmo de Kruskal, sobretudo para criticalidades de cardinalidade elevada e redes de maior porte.

Além da redução de tempo, a formulação numérica apresenta uma vantagem estrutural: por se basear em operações algébricas independentes entre tuplas, ela é adequada ao emprego de técnicas de processamento paralelo. Essa característica é explorada no Capítulo 5, no qual a abordagem numérica aqui desenvolvida é integrada a uma metodologia unificada para a identificação conjunta de criticalidades de ramos, UMs e medidas, com aceleração por computação paralela em GPU.

5 Identificação de criticalidades no sistema de medição

O Capítulo 4 apresentou uma abordagem numérica eficiente para a identificação das criticalidades de ramos. Este capítulo apresenta uma metodologia que integra a obtenção das criticalidades de ramos, unidades de medição e medidas, tendo as C_k-ramos identificadas como ponto de partida.

A motivação para essa estratégia foi estabelecida no Capítulo 3: as criticalidades de ramos apresentam caráter estrutural, e propriedades específicas, particularmente as Propriedades 6 e 9, permitem que as demais criticalidades sejam obtidas a partir delas, dispensando, em parte, a busca combinatória direta no espaço de medidas. Essa inversão da ordem de análise, em relação à abordagem usual da literatura, constitui o eixo metodológico desta tese.

Nesse eixo metodológico, as C_k-ramos são o ponto de partida comum para a obtenção das demais criticalidades, conforme o esquema

$$C_k\text{-UMs} \Longleftarrow C_k\text{-ramos} \Longrightarrow C_k\text{-meds}.$$

Primeiro, as C_k-ramos são identificadas por meio do sistema de medição hipotético (Capítulo 4). A partir delas, seguem-se dois caminhos. No primeiro, as C_k-UMs são obtidas das A_k-UMs associadas às C_k-ramos, por aplicação da Propriedade 6, sem busca combinatória (Seção 5.2). No segundo, as C_k-meds são identificadas por uma busca heurística restrita às medidas das UMs associadas a cada C_k-ramo, motivada pela Propriedade 9, e cada tupla candidata é verificada pela Propriedade 8 (Seção 5.3). Como as C_k-UMs e as C_k-meds são obtidas a partir das C_k-ramos, a busca combinatória de maior porte fica concentrada na identificação destas.

A metodologia aqui apresentada tem como base: (*i*) as relações entre os três tipos de criticalidade; (*ii*) o uso do sistema hipotético que garante eficiência e eficácia na identificação das criticalidades de ramos; e (*iii*) a introdução de uma busca heurística para iden-

tificação das criticalidades de medidas baseada na sua forte relação com as criticalidades de ramos. Além disso, é mostrado como a aplicação de computação paralela, tanto para a identificação de criticalidades de ramos (conforme visto no Capítulo 4 com o emprego de GPUs) quanto de medidas, viabiliza a aplicação da metodologia para a identificação de criticalidades de cardinalidades mais elevadas em sistemas de maior porte.

5.1 Visão Geral da Metodologia Integrada

A metodologia integrada parte do princípio, discutido no Capítulo 3, de que as criticalidades de ramos podem servir de ponto de partida para a identificação das demais criticalidades. Isso significa que, conhecido o conjunto de C_k-ramos para um dado sistema de medição, é possível obter:

i. as criticalidades de UMs, por aplicação direta da Propriedade 6, sem necessidade de busca combinatória;

ii. as criticalidades de medidas, por aplicação da Propriedade 8 em espaços de busca substancialmente reduzidos, definidos pelos grupos de medidas associadas a cada C_k-ramo.

A eficiência do método decorre de as criticalidades de UMs e de medidas serem obtidas a partir das criticalidades de ramos.

5.2 Identificação das Criticalidades de UMs

A identificação das criticalidades de UMs a partir das criticalidades de ramos baseia-se na Propriedade 6, reproduzida a seguir por conveniência:

Propriedade 6: Se uma A_k-UM não contiver uma A_j-UM ($\forall\, j < k$), então ela será considerada uma C_k-UM.

Conforme estabelecido no Capítulo 3, A_k-UM denota o conjunto de UMs associadas aos ramos que compõem uma C_k-ramo — isto é, contém as UMs localizadas nas barras terminais desses ramos e com ao menos uma medida neles incidente (injeção ou fluxo de potência). A identificação das C_k-UMs envolve, portanto, dois passos. Primeiro, para cada C_k-ramo previamente identificada, monta-se o conjunto A_k-UM correspondente. Em

seguida, aplica-se a Propriedade 6: descartam-se os conjuntos que contenham subconjuntos de cardinalidade inferior já presentes na lista de candidatos, em conformidade com a Propriedade 1.

Observe-se que a cardinalidade de A_k-UM não coincide necessariamente com a da C_k-ramo que lhe deu origem, pois uma mesma UM pode estar associada a mais de um ramo do conjunto. O índice k das C_k-UMs refere-se à cardinalidade do próprio conjunto de UMs.

O Quadro 5.1 apresenta o pseudocódigo para identificação de C_k-UMs. Destaca-se que não é necessário realizar a análise combinatória de UMs.

Quadro 5.1 - Pseudocódigo para identificação de C_k-UMs

Entrada: Lista de ramos da rede
Plano de medição
Lista `L-Ck-ramos` com todas as C_k-ramos identificadas

Saída: Lista `L-Ck-UMs` contendo as C_k-UMs

1: **Para cada** C_k-ramo **em** `L-Ck-ramos`:
2: Construir o conjunto A_k-UM, formado pelas UMs localizadas nas barras terminais dos ramos que compõem a C_k-ramo
3: Adicionar A_k-UM à lista `L-candidatos`
4: **Fim Para**
5: Ordenar `L-candidatos` por cardinalidade crescente
6: **Para cada** candidato A_i **em** `L-candidatos`:
7: **Se** A_i não contém nenhum A_j de `L-candidatos` com $|A_j| < |A_i|$:
8: Declarar A_i como C_k-UM, com $k = |A_i|$
9: Adicionar A_i a `L-Ck-UMs`
10: **Fim Para**
11: **Retornar** `L-Ck-UMs`

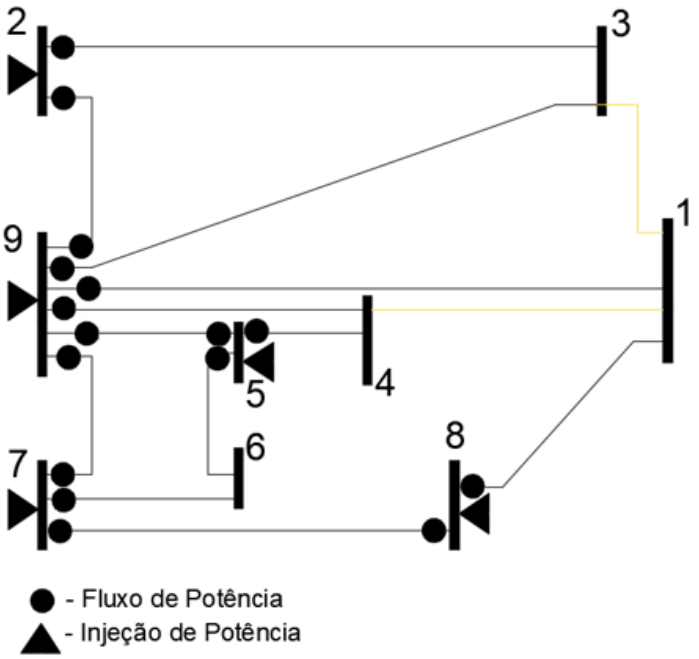
Fonte: Elaboração própria (2026).

Cabe destacar duas características desse procedimento: ele não envolve uma busca combinatória no espaço de UMs — o número de candidatos a serem avaliados é, no máximo, igual ao número de C_k-ramos identificadas —; e a verificação da Propriedade 6 envolve apenas comparações de conjuntos, com custo computacional muito inferior ao custo da identificação das C_k-ramos.

Para ilustrar esse processo, utiliza-se novamente o sistema exemplo de 9 barras apre-

sentado anteriormente, reproduzido por conveniência na Figura 5.1.

Figura 5.1 - Sistema de 9 barras



Fonte: Elaboração própria (2026).

A Tabela 5.1 apresenta as A_k-UMs associadas às C_k-ramos. Após identificadas as A_k-UMs, aplica-se a Propriedade 6 e as A_k-UMs que não contiverem A_j-UMs ($j < k$) serão declaradas como tuplas críticas de UMs. Na Tabela 5.1, os casos em que diferentes C_k-ramos levaram à identificação das mesmas A_k-UMs estão destacados por cores iguais.

Tabela 5.1 - A_k-UMs associadas às C_k-ramos

C_k-ramos	A_k-UMs
$(R_{1\text{-}8}, R_{7\text{-}8})$	UM7, UM8
$(R_{2\text{-}3}, R_{2\text{-}9})$	UM2, UM9
$(R_{5\text{-}6}, R_{6\text{-}7})$	UM5, UM7
$(R_{2\text{-}3}, R_{3\text{-}9})$	UM2, UM9
$(R_{2\text{-}9}, R_{3\text{-}9})$	UM2, UM9
$(R_{4\text{-}5}, R_{4\text{-}9})$	UM5, UM9
$(R_{1\text{-}8}, R_{1\text{-}9})$	UM8, UM9
$(R_{1\text{-}9}, R_{7\text{-}8})$	UM7, UM8, UM9
$(R_{1\text{-}8}, R_{5\text{-}6}, R_{7\text{-}9})$	UM5, UM7, UM8, UM9
$(R_{1\text{-}8}, R_{6\text{-}7}, R_{7\text{-}9})$	UM7, UM8, UM9

continua na página seguinte

Tabela 5.1 – continuação

C_k-ramos	A_k-UMs
$(R_{4\text{-}5}, R_{5\text{-}6}, R_{5\text{-}9})$	UM5, UM9
$(R_{4\text{-}5}, R_{5\text{-}9}, R_{6\text{-}7})$	UM5, UM7, UM9
$(R_{5\text{-}6}, R_{7\text{-}8}, R_{7\text{-}9})$	UM5, UM7, UM8, UM9
$(R_{6\text{-}7}, R_{7\text{-}8}, R_{7\text{-}9})$	UM7, UM8, UM9
$(R_{4\text{-}9}, R_{5\text{-}6}, R_{5\text{-}9})$	UM5, UM9
$(R_{4\text{-}9}, R_{5\text{-}9}, R_{6\text{-}7})$	UM5, UM7, UM9
$(R_{1\text{-}9}, R_{5\text{-}6}, R_{7\text{-}9})$	UM5, UM7, UM9
$(R_{1\text{-}9}, R_{6\text{-}7}, R_{7\text{-}9})$	UM7, UM9
$(R_{1\text{-}8}, R_{4\text{-}5}, R_{5\text{-}9}, R_{7\text{-}9})$	UM5, UM7, UM8, UM9
$(R_{4\text{-}5}, R_{5\text{-}9}, R_{7\text{-}8}, R_{7\text{-}9})$	UM5, UM7, UM8, UM9
$(R_{1\text{-}9}, R_{4\text{-}9}, R_{5\text{-}9}, R_{7\text{-}9})$	UM5, UM7, UM9
$(R_{1\text{-}8}, R_{4\text{-}9}, R_{5\text{-}9}, R_{7\text{-}9})$	UM5, UM7, UM8, UM9
$(R_{4\text{-}9}, R_{5\text{-}9}, R_{7\text{-}8}, R_{7\text{-}9})$	UM5, UM7, UM8, UM9
$(R_{1\text{-}9}, R_{4\text{-}5}, R_{5\text{-}9}, R_{7\text{-}9})$	UM5, UM7, UM9

A Tabela 5.2 apresenta as criticalidades de UMs do sistema exemplo. Ressalta-se novamente que não há necessidade de gerar combinações de UMs: o procedimento se restringe a operações sobre conjuntos. Em sistemas pequenos, este benefício é pouco perceptível, já que o número de combinações de UMs é reduzido. Entretanto, em sistemas de grande porte ele se torna relevante. Por exemplo, a busca exaustiva de C_k-UMs para o sistema IEEE 118 barras com 92 UMs, limitada à cardinalidade $k = 6$, exigiria a avaliação de 765 milhões de combinações.

Tabela 5.2 - C_k-UMs do sistema 9 barras

Cardinalidade (k)	C_k-UMs
1	—
2	(UM2, UM9); (UM5, UM7); (UM5, UM9); (UM7, UM8); (UM7, UM9); (UM8, UM9)

Fonte: Elaboração própria (2026).

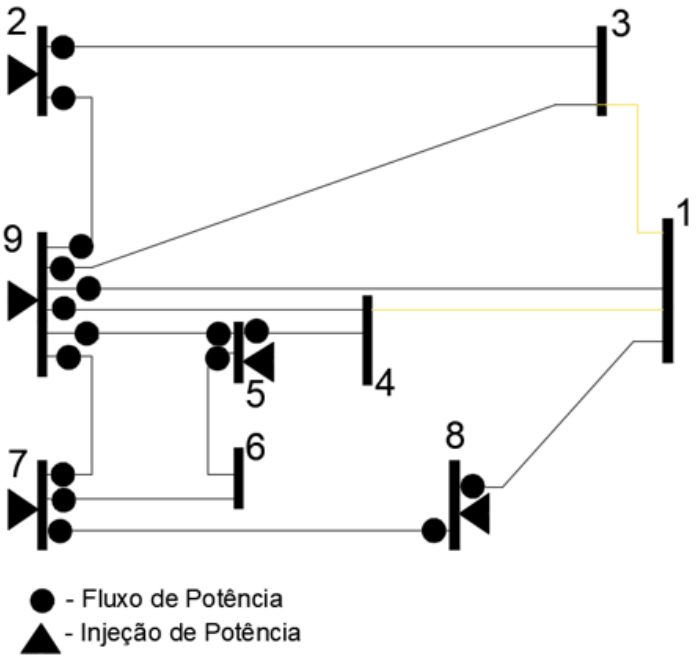
5.3 Identificação das criticalidades de medidas

A identificação das C_k-meds apoia-se na Propriedade 8, segundo a qual as colunas da matriz de covariância dos resíduos $\mathbf{\Omega}_a$ associadas às medidas que compõem uma C_k-med são linearmente dependentes. Essa propriedade fornece o mecanismo numérico de verificação de criticalidade para qualquer tupla candidata.

A aplicação direta da Propriedade 8 a todas as combinações possíveis de medidas, entretanto, esbarra novamente na natureza combinatória do problema. A heurística proposta em Coimbra *et al.* (2021) contorna esse obstáculo restringindo o espaço de busca aos subconjuntos de medidas associadas a cada C_k-ramo previamente identificada. A motivação para tal restrição decorre da Propriedade 9: dada a relação estrutural entre C_k-ramos e C_k-meds, é razoável esperar que as criticalidades remanescentes sejam formadas, predominantemente, por medidas pertencentes às UMs situadas nas vizinhanças das C_k-ramos.

A heurística é organizada em três etapas: (1) criação dos subconjuntos de medidas, (2) determinação dos limites de busca de cada subconjunto e (3) busca local em cada subconjunto. Para exemplificar o procedimento, utiliza-se o sistema exemplo de 9 barras.

Figura 5.2 - Sistema de 9 barras



Fonte: Elaboração própria (2026).

1) Criação dos subconjuntos de medidas. A cada C_k-ramo identificada corresponde um subconjunto formado pela reunião de todas as medidas pertencentes às UMs associadas — isto é, todas as medidas das UMs do conjunto A_k-UM correspondente, localizadas nas barras terminais dos k ramos que compõem a tupla. Tomando a Figura 5.2 como referência, à dupla crítica de ramos $(R_{1\text{-}8}, R_{7\text{-}8})$ corresponde o subconjunto $\{P_7, P_8, F_{7\text{-}6}, F_{7\text{-}8}, F_{7\text{-}9}, F_{8\text{-}1}, F_{8\text{-}7}\}$. Cada subconjunto contém, tipicamente, um número de medidas inferior ao total do plano de medição, o que reduz o espaço de busca em relação à enumeração exaustiva.

2) Determinação dos limites de busca. Para cada subconjunto definem-se uma cardinalidade inferior k_{inf} e uma cardinalidade superior k_{sup}, que delimitam a faixa das tuplas a serem testadas.

O limite inferior é estabelecido a partir da cardinalidade k_{ramo} da C_k-ramo que deu origem ao subconjunto:

$$k_{\text{inf}} = k_{\text{ramo}} \tag{5.1}$$

A justificativa para a Equação (5.1) é a seguinte: para que k ramos deixem simultaneamente de ser relevantes para a EE, é necessário remover no mínimo k medidas. Consequentemente, a uma C_k-ramo só podem estar associadas C_k-meds de cardinalidade igual ou superior a k. Assim, no subconjunto vinculado a um ramo crítico as criticalidades possíveis têm cardinalidade a partir de 1; no vinculado a uma dupla crítica de ramos, a partir de 2; e assim sucessivamente. Esse critério difere do limite arbitrado empiricamente em Coimbra *et al.* (2021), no qual o limite inferior era dado pela quantidade de medidas associadas diretamente à C_k-ramo, menos uma.

O limite superior k_{sup} corresponde, no caso geral, ao número total de medidas do subconjunto, podendo ser reduzido à cardinalidade máxima de interesse k_{max}, quando aplicável:

$$k_{\text{sup}} = k_{\text{max_interesse}} \qquad \text{ou} \qquad k_{\text{sup}} = \text{número de medidas do subconjunto} \tag{5.2}$$

Para exemplificar essa etapa, considere-se a Tabela 5.3. Para cada C_k-ramo há uma coluna com o número de ramos correspondente e uma coluna com as A_k-UMs. Os subconjuntos de medidas são formados por todas as medidas das A_k-UMs. Observa-se que

há algumas redundâncias de subconjuntos: por exemplo, às duplas de ramos $(R_{2\text{-}3}, R_{2\text{-}9})$, $(R_{2\text{-}3}, R_{3\text{-}9})$ e $(R_{2\text{-}9}, R_{3\text{-}9})$ estão associadas as UM2 e UM9. Observa-se também que ao trio de ramos $(R_{1\text{-}8}, R_{5\text{-}6}, R_{7\text{-}9})$ e à quadra de ramos $(R_{1\text{-}8}, R_{4\text{-}5}, R_{5\text{-}9}, R_{7\text{-}9})$ estão associadas as UM5, UM7, UM8 e UM9. Para evitar algumas redundâncias de tuplas visitadas, mantém-se apenas um subconjunto de A_k-UMs e o menor k_{ramo} associado a ele. Voltando ao exemplo anterior, há um trio e uma quadra de ramos associados às UM5, UM7, UM8 e UM9. Nesse caso, mantém-se o menor valor de k_{ramo}, $k = 3$.

Tabela 5.3 - Quantidade de ramos por A_k-UMs

C_k-ramos	Nº de ramos	Todas as medidas das A_k-UMs
$(R_{1\text{-}8}, R_{7\text{-}8})$	2	UM7, UM8
$(R_{2\text{-}3}, R_{2\text{-}9})$	2	UM2, UM9
$(R_{5\text{-}6}, R_{6\text{-}7})$	2	UM5, UM7
$(R_{2\text{-}3}, R_{3\text{-}9})$	2	UM2, UM9
$(R_{2\text{-}9}, R_{3\text{-}9})$	2	UM2, UM9
$(R_{4\text{-}5}, R_{4\text{-}9})$	2	UM5, UM9
$(R_{1\text{-}8}, R_{1\text{-}9})$	2	UM8, UM9
$(R_{1\text{-}9}, R_{7\text{-}8})$	2	UM7, UM8, UM9
$(R_{1\text{-}8}, R_{5\text{-}6}, R_{7\text{-}9})$	3	UM5, UM7, UM8, UM9
$(R_{1\text{-}8}, R_{6\text{-}7}, R_{7\text{-}9})$	3	UM7, UM8, UM9
$(R_{4\text{-}5}, R_{5\text{-}6}, R_{5\text{-}9})$	3	UM5, UM9
$(R_{4\text{-}5}, R_{5\text{-}9}, R_{6\text{-}7})$	3	UM5, UM7, UM9
$(R_{5\text{-}6}, R_{7\text{-}8}, R_{7\text{-}9})$	3	UM5, UM7, UM8, UM9
$(R_{6\text{-}7}, R_{7\text{-}8}, R_{7\text{-}9})$	3	UM7, UM8, UM9
$(R_{4\text{-}9}, R_{5\text{-}6}, R_{5\text{-}9})$	3	UM5, UM9
$(R_{4\text{-}9}, R_{5\text{-}9}, R_{6\text{-}7})$	3	UM5, UM7, UM9
$(R_{1\text{-}9}, R_{5\text{-}6}, R_{7\text{-}9})$	3	UM5, UM7, UM9
$(R_{1\text{-}9}, R_{6\text{-}7}, R_{7\text{-}9})$	3	UM7, UM9
$(R_{1\text{-}8}, R_{4\text{-}5}, R_{5\text{-}9}, R_{7\text{-}9})$	4	UM5, UM7, UM8, UM9
$(R_{4\text{-}5}, R_{5\text{-}9}, R_{7\text{-}8}, R_{7\text{-}9})$	4	UM5, UM7, UM8, UM9
$(R_{1\text{-}9}, R_{4\text{-}9}, R_{5\text{-}9}, R_{7\text{-}9})$	4	UM5, UM7, UM9
$(R_{1\text{-}8}, R_{4\text{-}9}, R_{5\text{-}9}, R_{7\text{-}9})$	4	UM5, UM7, UM8, UM9
$(R_{4\text{-}9}, R_{5\text{-}9}, R_{7\text{-}8}, R_{7\text{-}9})$	4	UM5, UM7, UM8, UM9
$(R_{1\text{-}9}, R_{4\text{-}5}, R_{5\text{-}9}, R_{7\text{-}9})$	4	UM5, UM7, UM9

3) Busca local. Em cada subconjunto, enumeram-se as tuplas de medidas com cardinalidade entre k_{inf} e k_{sup}, aplicando-se a Propriedade 8 a cada uma delas. As tuplas cuja submatriz $\widetilde{\mathbf{\Omega}}_a$ apresenta colunas linearmente dependentes são declaradas C_k-meds.

O número total de tuplas visitadas pela heurística é dado por:

$$\text{tuplas visitadas} = \sum_{s=1}^{NS} \left[\sum_{c=k_{\text{inf}}^{(s)}}^{k_{\text{sup}}^{(s)}} \left(\frac{k_{\text{max}}^{(s)}!}{c! \left(k_{\text{max}}^{(s)} - c \right)!} \right) \right] \tag{5.3}$$

onde NS é o número de subconjuntos, s identifica o s-ésimo subconjunto, $k_{\text{inf}}^{(s)}$ e $k_{\text{sup}}^{(s)}$ são os limites que definem as cardinalidades das tuplas de medidas a serem avaliadas dentro do s-ésimo conjunto de medidas, $k_{\text{max}}^{(s)}$ é o número total de medidas que formam o s-ésimo conjunto, e c representa uma dada cardinalidade dentro da faixa de cardinalidades sob investigação. Tais parâmetros são utilizados para calcular as combinações de $k_{\text{max}}^{(s)}$ elementos distintos, tomados c a c. Observa-se que o custo para encontrar as C_k-meds dependerá do número de conjuntos de medidas, do número de medidas que compõem cada um deles e dos limites que definem as cardinalidades de interesse. No exemplo, adota-se a cardinalidade máxima de interesse $k_{\text{max}} = 6$, de modo que $k_{\text{sup}} = 6$ em todos os subconjuntos. Os limites de cada subconjunto são apresentados na Tabela 5.4.

Tabela 5.4 - Definição final dos subconjuntos de busca

Medidas das A_k-UMs	k_{inf}	k_{sup}
UM7, UM8	2	6
UM2, UM9	2	6
UM5, UM7	2	6
UM5, UM9	2	6
UM8, UM9	2	6
UM7, UM8, UM9	2	6
UM5, UM7, UM8, UM9	3	6
UM5, UM7, UM9	3	6
UM7, UM9	3	6

Fonte: Elaboração própria (2026).

A Tabela 5.5 apresenta a quantidade de tuplas encontradas pela metodologia. A busca exaustiva exige visitar 82.159 tuplas, enquanto a metodologia proposta visita 52.221, o que corresponde a uma redução de 36% do espaço de busca neste exemplo. Observa-se que

90% das tuplas até $k = 6$ foram encontradas; entretanto, todas as tuplas até $k = 5$ foram identificadas, e as cardinalidades mais baixas representam as maiores vulnerabilidades dos sistemas de medição. Em sistemas de maior porte, a redução do espaço de busca é maior, como será demonstrado nos resultados a seguir.

Tabela 5.5 - C_k-meds encontradas

Cardinalidade (k)	**Busca exaustiva**	**Metodologia proposta**
1	—	—
2	—	—
3	—	—
4	4	4
5	5	5
6	11	9

Fonte: Elaboração própria (2026).

5.4 Aceleração por Computação Paralela em GPU

A formulação da metodologia integrada apresentada nas seções anteriores admite uma propriedade computacional explorada nesta seção: as verificações de criticalidade de tuplas distintas são independentes entre si. Para cada tupla candidata, monta-se uma submatriz $\widetilde{\mathbf{\Omega}}_a$ específica e aplica-se a eliminação de Gauss localmente, sem qualquer dependência das demais tuplas. Essa independência torna a metodologia adequada ao emprego de técnicas de processamento paralelo.

O cálculo computacional moderno apoia-se predominantemente em duas arquiteturas: as Unidades Centrais de Processamento (*Central Processing Units* — CPUs), compostas por um número moderado de núcleos projetados para tarefas sequenciais complexas, e as Unidades de Processamento Gráfico (*Graphics Processing Units* — GPUs), que dispõem de milhares de núcleos otimizados para a execução simultânea de tarefas paralelas relativamente simples. Originalmente concebidas para processamento gráfico, as GPUs têm sido cada vez mais empregadas em aplicações científicas e de engenharia, particularmente em problemas com elevado grau de paralelismo intrínseco.

A verificação de criticalidade de uma tupla, conforme formulada no Capítulo 4 e empregada na busca heurística, possui exatamente o perfil adequado à arquitetura de GPUs: trata-se de uma operação relativamente simples — montagem de uma submatriz pequena e eliminação de Gauss localizada —, replicada um grande número de vezes para

diferentes tuplas, sem interdependência entre as execuções. Essa estrutura permite que centenas ou milhares de tuplas sejam avaliadas simultaneamente, com ganhos potenciais de várias ordens de grandeza em relação à execução sequencial.

A integração da metodologia com computação paralela em GPU apoia-se na plataforma desenvolvida por Nishio *et al.* (2024), originalmente concebida para análise extensiva de medidas a partir de busca direta no espaço total. A plataforma fornece a infraestrutura para montagem de submatrizes $\widetilde{\mathbf{\Omega}}_a$ e para aplicação paralela da eliminação de Gauss em GPU, sendo adaptável a diferentes estratégias de enumeração de tuplas.

Na metodologia proposta nesta tese, a plataforma é empregada em duas frentes complementares. A primeira é a identificação numérica das criticalidades de ramos, no contexto do sistema de medição hipotético (Capítulo 4): cada tupla candidata de ramos corresponde a uma submatriz $\widetilde{\mathbf{\Omega}}_a$ que pode ser verificada paralelamente. A segunda é a busca heurística por C_k-meds (Seção 5.3): as tuplas dos subconjuntos definidos para cada C_k-ramo são avaliadas em paralelo. Em ambas as frentes, o número de medidas envolvidas em cada verificação é reduzido — corresponde à cardinalidade da tupla testada —, o que se ajusta de forma natural à arquitetura da GPU.

5.5 Resultados e Discussão

Esta seção apresenta os resultados da aplicação da metodologia integrada aos sistemas IEEE 14, 30, 118 e 300 barras, considerando diferentes níveis de redundância do sistema de medição. Os resultados são organizados em três frentes: (1) validação da metodologia por comparação com busca exaustiva, com foco na completude das criticalidades identificadas; (2) desempenho computacional, incluindo a aceleração obtida com o emprego de GPU; e (3) discussão geral sobre escalabilidade e aplicabilidade.

As simulações foram executadas em um computador com processador Intel Core i9-9300H, 32 GB de memória RAM e GPU NVIDIA GTX 1650. Os planos de medição adotados foram os dos sistemas IEEE 14, 30 e 118 barras, cujos respectivos sistemas de medição podem ser encontrados em (Souza; Coutto Filho; Guimaraens, 2026; Rocha *et al.*, 2018; Coutto Filho; Souza; Villavicencio Tafur, 2013); no caso do IEEE 118 barras, considerou-se a presença de todas as medidas associadas às UMs instaladas. Para o IEEE 300 barras, adotou-se o plano de medição com 225 UMs completas desenvolvido neste trabalho (Capítulo 4). Em todos os experimentos, estabeleceu-se como objetivo a identificação das tuplas críticas de ramos e de medidas até a cardinalidade $k = 4$, de modo

que o parâmetro $k_{\max}$ da segunda etapa da metodologia foi fixado nesse valor.

5.5.1 Identificação das criticalidades de medidas

As C_k-ramos obtidas serviram de ponto de partida para a identificação das tuplas críticas de medidas, restringindo a busca às combinações formadas dentro dos grupos de medidas associados a cada criticalidade de ramos. A Tabela 5.6 apresenta a quantidade de C_k-meds identificadas até $k = 4$ e os respectivos tempos de processamento.

Tabela 5.6 - C_k-meds identificadas até $k = 4$

Rede	**Nº de C_k-meds**	**Tempo (s)**
IEEE 14	94	0,025
IEEE 30	830	0,098
IEEE 118	24	0,117
IEEE 300	232	0,561

Fonte: Elaboração própria (2026).

A validação seguiu o mesmo procedimento adotado para as C_k-ramos no Capítulo 4, com busca exaustiva independente. Nos sistemas IEEE 14, 118 e 300 barras, todas as criticalidades de medidas existentes até $k = 4$ foram encontradas pela metodologia. No IEEE 30 barras, a metodologia identificou a totalidade das C_k-meds até $k = 3$ e cerca de 90% das de cardinalidade $k = 4$. Essa cobertura parcial na maior cardinalidade é consequência esperada da estratégia adotada: como a busca se restringe aos grupos de medidas associados às criticalidades de ramos, tuplas críticas de medidas sem correspondência direta com as C_k-ramos enumeradas podem escapar à identificação. Trata-se do compromisso deliberado da metodologia — abrir mão da garantia formal de completude na segunda etapa em troca de uma redução do espaço de combinações —, e os resultados indicam que a parcela eventualmente não identificada é pequena, concentrada nas cardinalidades mais altas, em consonância com a relação estrutural entre criticalidades de ramos e de medidas.

A distribuição das quantidades identificadas entre os sistemas merece atenção, pois evidencia o papel da redundância do sistema de medição. O IEEE 30 barras, com plano de medição de menor redundância relativa, concentra 830 C_k-meds até $k = 4$ — o maior contingente entre os sistemas testados, apesar de seu porte intermediário. Já o IEEE 118 barras, com sistema de medição altamente redundante, apresenta apenas 24 C_k-meds

nessa faixa de cardinalidade. O contraste confirma o comportamento esperado: quanto maior a redundância, menor a ocorrência de criticalidades de baixa cardinalidade, que migram para ordens superiores. Cabe ressaltar, contudo, que as criticalidades de baixa cardinalidade são precisamente as mais relevantes do ponto de vista operativo, por representarem os caminhos mais curtos para a inobservabilidade. Além disso, quanto maior a redundância, maior o número de combinações e, consequentemente, maior esforço computacional necessário para encontrá-las.

Para dimensionar o ganho proporcionado pela exploração da relação entre criticalidades de ramos e de medidas, as Tabelas 5.7 e 5.8 comparam, respectivamente, por cardinalidade, o tempo necessário para obter as C_k-meds dos sistemas IEEE 118 e 300 barras pela metodologia proposta e pela busca direta no espaço completo de medidas realizada na plataforma de Nishio *et al.* (2024).

Tabela 5.7 - Tempo (s) por cardinalidade — IEEE 118 barras

Cardinalidade (k)	**Metodologia proposta**	**Nishio *et al.* (2024)**
1	0,0025	0,0005
2	0,0177	0,0010
3	0,0251	0,1446
4	0,0722	23,9828
Tempo total	**0,1175**	**24,1289**

Fonte: Elaboração própria (2026).

Tabela 5.8 - Tempo (s) por cardinalidade — IEEE 300 barras

Cardinalidade (k)	**Metodologia proposta**	**Nishio *et al.* (2024)**
1	0,0267	0,0006
2	0,0564	0,0087
3	0,1120	2,6887
4	0,3656	1088,7084
Tempo total	**0,5606**	**1091,4064**

Fonte: Elaboração própria (2026).

Os resultados demonstram o padrão característico dos dois enfoques, que se repete em ambos os sistemas. Nas cardinalidades mais baixas ($k = 1$ e $k = 2$), a busca direta é ligeiramente mais rápida, pois o número de combinações ainda é pequeno e a metodologia

proposta carrega o custo de estruturação dos grupos de medidas. O quadro se inverte a partir de $k = 3$ e torna-se acentuado em $k = 4$. No IEEE 118 barras, enquanto a busca direta demanda 23,9828 s para varrer as combinações de quádruplas do plano de medição completo, a metodologia proposta conclui a mesma cardinalidade em 0,0722 s — mais de 300 vezes mais rápido. No IEEE 300 barras, a diferença é ainda maior: 1088,7084 s, cerca de 18 minutos, contra 0,3656 s, quase 3.000 vezes mais rápido. O contraste ilustra o mecanismo central da proposta: o crescimento combinatório, que domina o custo da busca direta nas cardinalidades altas, é contido pela restrição do espaço de busca aos grupos de medidas associados às C_k-ramos, cujo tamanho é ditado pela cardinalidade da tupla e não pelo porte do plano de medição.

No acumulado das quatro cardinalidades, a segunda etapa da metodologia consome 0,1175 s no IEEE 118 barras, contra 24,1289 s da busca direta, e 0,5606 s no IEEE 300 barras, contra 1091,4064 s. As razões acumuladas — aproximadamente 205 vezes e 1.950 vezes, respectivamente — evidenciam que a vantagem da metodologia cresce com o porte do sistema, precisamente onde a busca direta se torna proibitiva. Incluindo o custo da identificação das criticalidades de ramos em GPU, o tempo total da metodologia para o IEEE 118 barras é de 1,0455 s — aproximadamente 23 vezes inferior ao da busca direta. Há, ainda, um regime de operação em que a vantagem se amplia: quando alterações no plano de medição não fazem surgir novos ramos irrelevantes, as C_k-ramos permanecem válidas e apenas a etapa de identificação de C_k-meds precisa ser reexecutada. Nesse cenário de atualização, o tempo de resposta da metodologia é mais de 200 vezes menor que o da busca direta, o que a habilita para uso recorrente no acompanhamento de mudanças do sistema de medição — condição essencial para a aplicação em ambiente próximo ao tempo real.

Os resultados das três frentes convergem para uma mesma leitura. A eficácia da metodologia foi verificada por comparação exaustiva, com completude integral na identificação das C_k-ramos e cobertura integral ou quase integral na identificação das C_k-meds. A eficiência decorre da combinação de dois mecanismos independentes e complementares: a redução do espaço de busca, obtida pela exploração da relação estrutural entre criticalidades de ramos e de medidas, e a paralelização das verificações de criticalidade, viabilizada pela independência entre as avaliações de tuplas distintas. O primeiro mecanismo atua sobre o número de combinações a testar; o segundo, sobre o custo de testá-las. É a atuação simultânea de ambos que produz os ganhos de duas a três ordens de grandeza observados no IEEE 118 e 300 barras.

Do ponto de vista da escalabilidade, os experimentos indicam que os ganhos crescem com o porte do sistema e com a cardinalidade analisada, as duas dimensões em que o problema se torna intratável para as abordagens convencionais. Esse comportamento indica a aplicabilidade da metodologia a redes de maior dimensão.

Por fim, cabe situar estes resultados no contexto da tese. A identificação das criticalidades não constitui um fim em si mesma: seu propósito é fornecer o conhecimento das vulnerabilidades da rede sobre o qual se apoiam as ações preventivas de reforço do sistema de medição e outras que podem decorrer da consciência que se passa a ter sobre a situação em que a supervisão da rede se encontra (contribuindo para o que em um contexto amplo a literatura trata como *situational awareness*). Nesse sentido, a título de exemplo, os resultados aqui apresentados constituem a base da aplicação desenvolvida no Capítulo 6, em que o conjunto de C_k-ramos identificado passa a constituir o dado de entrada do problema de proteção contra ataques cibernéticos. Dois aspectos dos resultados obtidos são particularmente relevantes para aquela aplicação. O primeiro é a completude: como será visto, a garantia oferecida pelo modelo de proteção é circunscrita ao conjunto de criticalidades previamente identificadas, de modo que a identificação integral das C_k-ramos, verificada por busca exaustiva no Capítulo 4, é condição necessária para a validade prática da proteção obtida. O segundo é o custo computacional: ao reduzir a identificação das criticalidades de minutos para menos de um segundo, a metodologia torna viável a manutenção desse conjunto atualizado frente a alterações topológicas e do plano de medição, o que estende o alcance das ações de reforço de um contexto estritamente de planejamento para um contexto compatível com a operação do sistema.

6 Proteção das criticalidades de ramos contra ataques cibernéticos

Os capítulos anteriores estabeleceram as relações entre os diferentes tipos de criticalidade (Capítulo 3) e apresentaram metodologias computacionalmente eficientes para a identificação das criticalidades de ramos, medidas e unidades de medição (Capítulos 4 e 5), as duas últimas sendo obtidas a partir da primeira. Este capítulo apresenta uma ampliação desse arcabouço, empregando a base de dados de criticalidades de ramos como subsídio para a escolha de UMs a serem reforçadas visando à proteção das criticalidades de ramos (e, consequentemente, do sistema de supervisão) contra ataques cibernéticos.

A digitalização progressiva dos sistemas elétricos de potência, impulsionada pela integração de tecnologias de informação e comunicação à infraestrutura de medição e controle, ampliou a exposição desses sistemas a ameaças cibernéticas (He; Yan, 2016). A função EE, por ocupar posição central na cadeia de decisão, constitui alvo particularmente sensível. Um ataque bem-sucedido ao sistema de medição pode comprometer a qualidade dos dados fornecidos a todas as demais funções do COS, com consequências operativas e econômicas.

Neste contexto, o conhecimento prévio das criticalidades oferece uma vantagem ao defensor. Se as tuplas críticas de ramos, medidas ou UMs são conhecidas, sabe-se quais conjuntos de equipamentos, uma vez comprometidos, levariam a rede à inobservabilidade ou degradariam a capacidade de depuração de erros grosseiros. Esse conhecimento permite formular o problema de proteção de forma dirigida, partindo das vulnerabilidades do sistema, em vez de proteger indistintamente todos os equipamentos, o que é economicamente inviável, ou mesmo escolhê-los segundo outro critério que não seja a própria vulnerabilidade do sistema.

Assim, este capítulo apresenta uma formulação baseada em programação linear inteira para o problema de proteção preventiva de criticalidades de ramos, identificadas conforme a metodologia do Capítulo 4, indicando UMs a serem reforçadas para isso. No Apêndice A é apresentado um histórico dos ataques cibernéticos aos sistemas elétricos de potência, os

diferentes tipos de ataque e as principais propostas para proteção preventiva do SEP.

6.1 Seleção de UMs para Reforço

Esta seção apresenta uma revisão bibliográfica sobre a escolha de UMs a serem protegidas, para depois expor a proposta desta tese para seleção de UMs para proteção das C_k-ramos. Essa proposta se restringe aos Sistemas Ciberfísicos de Potência (*Cyber-Physical Power Systems* — CPPS).

A proteção preventiva busca reduzir a superfície de ataque e aumentar o esforço necessário para que um adversário comprometa o processo de estimação de estado. Entre as medidas tradicionalmente consideradas encontram-se a proteção física dos dispositivos de aquisição, a autenticação dos equipamentos, a criptografia dos canais de comunicação e o controle de acesso à infraestrutura SCADA. Contudo, em sistemas de grande porte, a proteção integral de todos os medidores, canais de comunicação e unidades de aquisição pode ser técnica ou economicamente inviável. Por essa razão, uma parcela da literatura concentra-se no problema de determinar quais medidas ou UMs devem receber proteção prioritária.

Nesse contexto, a proteção pode ser realizada em diferentes níveis. No nível individual, cada medida é considerada um recurso que pode ser protegido separadamente. No nível das unidades de medição, admite-se que o comprometimento de uma UM permita ao atacante manipular simultaneamente todas as medições associadas àquela unidade. Essa distinção é relevante, pois a seleção de medidas individuais não conduz necessariamente à mesma solução obtida quando os dados são agrupados conforme os dispositivos responsáveis por sua aquisição e transmissão.

Bobba *et al.* (2010) apresentam uma das primeiras formulações sistemáticas para a seleção de medições a serem protegidas contra ataques de injeção de dados falsos. Os autores demonstram que, na ausência de variáveis de estado verificáveis de maneira independente, a proteção de um conjunto de medidas básicas constitui condição necessária e suficiente para impedir ataques furtivos. Um conjunto básico é formado pelo número mínimo de medidas que mantém o sistema observável; no modelo linear, sua cardinalidade é igual ao número de variáveis de estado estimadas.

A seleção proposta por Bobba *et al.* (2010) é, portanto, determinada pela observabilidade algébrica. Para identificar um conjunto básico sem realizar uma busca combinatória entre todas as medidas disponíveis, os autores empregam a decomposição LU da matriz

Jacobiana **H**. Mediante uma permutação de suas linhas, as medidas são representadas em um espaço de estados equivalente, no qual as linhas associadas à matriz identidade correspondem às medidas básicas e as demais representam medidas redundantes. O procedimento também permite substituir determinadas medidas básicas por medidas redundantes linearmente independentes, produzindo diferentes conjuntos de proteção capazes de assegurar a mesma condição de posto completo.

A contribuição de Bobba *et al.* (2010) estabelece uma relação direta entre proteção e observabilidade: se as medidas protegidas forem suficientes para tornar o sistema observável, não existirá vetor não nulo **c** capaz de satisfazer simultaneamente a estrutura do ataque e a restrição de não alteração das medidas seguras. A abordagem, entretanto, pressupõe que as medidas selecionadas sejam protegidas contra acesso físico, modificação dos dados e comprometimento dos canais de comunicação. Além disso, a disponibilidade dessas medidas também precisa ser preservada, pois a perda de uma medida pertencente ao conjunto básico pode reduzir o posto da matriz protegida e restabelecer a possibilidade de ataques furtivos.

Dán e Sandberg (2010) ampliam essa discussão ao introduzirem um índice de segurança associado a cada medição. Esse índice quantifica o custo mínimo para realizar um ataque furtivo com um objetivo específico, normalmente expresso pelo menor número de medições que precisam ser comprometidas para alterar determinada grandeza. Quanto menor o índice, mais vulnerável é a medição e menor é o esforço exigido do atacante. A escolha dos dispositivos a serem protegidos passa, assim, a ser orientada pelo aumento do custo dos ataques mínimos, em vez de depender exclusivamente da obtenção de observabilidade a partir do conjunto protegido.

Os autores consideram dois modelos de comprometimento. No primeiro, denominado ataque a medidores, cada medida pode ser atacada individualmente e possui custo próprio. No segundo, as medições são agrupadas conforme as UMs responsáveis por sua aquisição. Nesse caso, o comprometimento de uma UM dá acesso ao conjunto de medidas associado àquela unidade, de modo que o custo do ataque é calculado pelo número de unidades comprometidas, e não pela quantidade total de medições alteradas. Essa modelagem aproxima o problema da arquitetura real dos sistemas SCADA, nos quais diversas medições de uma subestação podem compartilhar o mesmo terminal, canal de comunicação ou mecanismo de autenticação.

Para a proteção no nível das medições individuais, Dán e Sandberg (2010) recuperam a condição de posto completo: devem ser protegidas n medidas cujas linhas correspondentes

na matriz **H** sejam linearmente independentes. No nível das UMs, a condição é distinta, pois uma única unidade pode concentrar várias medições. Os autores demonstram que o conjunto de UMs protegido deve constituir um conjunto dominante no grafo das unidades; embora essa condição seja necessária, não é suficiente para assegurar proteção perfeita. Dessa forma, propõem o algoritmo *Dominating Set Augmentation* (DSA), que acrescenta UMs a um conjunto dominante até eliminar os ataques furtivos remanescentes.

Quando o orçamento disponível não permite a proteção completa, Dán e Sandberg (2010) propõem estratégias gulosas para a implantação incremental dos dispositivos de criptografia. O algoritmo *Most Shortest Minimal Attacks* (MSM) seleciona, a cada iteração, o bloco de medições que aparece no maior número de ataques de menor custo, buscando elevar o menor índice de segurança do sistema. Já o algoritmo *Most Minimal Attacks* (MMA) considera a frequência com que cada bloco aparece no conjunto total de ataques mínimos, procurando elevar o custo médio dos ataques possíveis. Assim, a seleção pode ser direcionada tanto à melhoria da situação do elemento mais vulnerável quanto à elevação global do esforço exigido do adversário.

Bi e Zhang (2014a) reformulam a seleção de medidas protegidas por meio de uma representação gráfica da observabilidade. O objetivo é determinar o menor conjunto de medidas cuja proteção impeça que um ataque furtivo comprometa um conjunto previamente escolhido de variáveis de estado. Os autores mostram que esse problema pode ser representado como uma variante do problema da Árvore de Steiner, na qual as barras correspondentes às variáveis que se deseja proteger são tratadas como vértices terminais, e as medições selecionadas devem formar uma estrutura observável conectada à barra de referência.

A partir dessa equivalência, são desenvolvidos dois métodos exatos. O primeiro realiza a enumeração dos possíveis vértices de Steiner até encontrar a menor sub-rede observável que contenha os estados selecionados. Embora forneça a solução ótima, sua complexidade cresce rapidamente com o tamanho da rede. O segundo método formula o problema como uma programação linear inteira mista — *Mixed-Integer Linear Programming* (MILP) — baseada em um modelo de fluxo em rede. Essa formulação explora a estrutura gráfica do problema e reduz o esforço computacional em comparação com a enumeração direta.

Para sistemas de maior porte, Bi e Zhang (2014a) propõem ainda uma heurística de poda de árvore — *Tree-Pruning Heuristic* (TPH). O procedimento parte de uma árvore observável e remove progressivamente vértices, ramos e medidas que não são indispensáveis à proteção dos estados selecionados. Embora não garanta a solução ótima em todos os

casos, a heurística apresentou resultados próximos aos obtidos pelos métodos exatos, com redução do tempo computacional. Os algoritmos também podem ser utilizados de forma incremental, permitindo que o operador amplie gradualmente o conjunto de estados protegidos à medida que novos recursos de segurança se tornem disponíveis.

Em trabalho complementar, Bi e Zhang (2014b) consideram que a defesa não precisa se limitar à proteção direta das medições. Os autores propõem ocultar do atacante os valores exatos das reatâncias de determinadas linhas de transmissão, estratégia denominada informação topológica encoberta — *Covert Topological Information* (CTI). Como a construção de um *False Data Injection Attack* (FDIA) furtivo depende do conhecimento da matriz Jacobiana, impedir o acesso aos parâmetros de um conjunto estrategicamente escolhido de linhas pode inviabilizar a elaboração do vetor de ataque.

A seleção das linhas cujas informações devem permanecer ocultas também é formulada como um problema de Árvore de Steiner. Além disso, os autores desenvolvem uma estratégia mista que combina a proteção de medições reais com a ocultação de parâmetros de linhas. Para fins de modelagem, uma linha cuja reatância é mantida em sigilo pode ser representada por um medidor virtual seguro, pois o desconhecimento de seu parâmetro restringe as alterações de estado que o atacante consegue introduzir sem gerar inconsistências. O problema conjunto de escolha das medições e das informações topológicas protegidas é formulado como MILP e complementado por uma heurística de poda de árvore.

A abordagem de Bi e Zhang diferencia-se das anteriores por permitir que o operador selecione previamente quais variáveis de estado deseja preservar. Os autores mencionam, por exemplo, a possibilidade de priorizar barras ou subestações com maior importância econômica, social ou operacional. Contudo, uma vez definidos os estados-alvo, o conjunto de medidas é escolhido com base na conectividade gráfica, na observabilidade da sub-rede e na minimização do custo ou da quantidade de recursos protegidos.

Deng, Xiao e Lu (2017) questionam uma hipótese presente em grande parte dos trabalhos anteriores: a de que uma medida selecionada possa ser tornada absolutamente invulnerável. Em sua formulação, a possibilidade de comprometimento de cada medidor depende do orçamento de defesa aplicado a ele. Quanto maior o investimento em determinado dispositivo, maior será o custo imposto ao atacante para violá-lo. A interação entre defensor e adversário é modelada considerando um atacante racional, que procura alcançar seu objetivo com o menor custo possível, enquanto o defensor distribui seus recursos de modo a elevar esse custo acima da capacidade disponível para o ataque.

Inicialmente, os autores determinam a menor quantidade total de recursos que deve ser distribuída entre os medidores para assegurar que qualquer ataque capaz de alterar uma variável de estado apresente custo superior a um limite especificado. Em seguida, analisam o caso no qual apenas um número limitado de medidores pode receber proteção. Nessa extensão, devem ser decididos simultaneamente quais medidores serão selecionados e qual parcela do orçamento será atribuída a cada um.

Esse problema é formulado como uma programação não linear inteira mista — *Mixed-Integer Nonlinear Programming* (MINLP). As variáveis binárias representam a escolha dos medidores, enquanto as variáveis contínuas determinam os recursos aplicados a cada dispositivo. Para viabilizar a solução em redes de maior porte, Deng, Xiao e Lu (2017) empregam a decomposição de Benders, separando as decisões discretas de seleção das decisões contínuas de alocação de orçamento. Os resultados apresentados pelos autores indicam que a decomposição reduz o esforço computacional e permite tratar inclusive o sistema IEEE de 300 barras.

Liu, Li e Li (2017), por sua vez, formulam a seleção das medidas protegidas como um problema MILP binível. No nível superior, o defensor procura minimizar a quantidade de medições de carga e de fluxo que devem ser protegidas. No nível inferior, o atacante determina o menor conjunto de medidas que precisa comprometer para produzir uma alteração mínima especificada em uma carga, respeitando restrições físicas relacionadas ao balanço de potência, aos fluxos nas linhas e aos limites plausíveis de modificação das cargas. A proteção é considerada adequada quando o menor custo de ataque excede a capacidade atribuída ao adversário.

Diferentemente das formulações baseadas apenas na relação algébrica, Liu, Li e Li (2017) incorporam restrições associadas às características físicas da rede e à magnitude das alterações maliciosas. Os autores argumentam que variações excessivas nas medições de carga poderiam ser identificadas por previsões ou por informações históricas disponíveis no centro de controle. Dessa forma, o problema do atacante não consiste somente em produzir um vetor pertencente ao espaço coluna da matriz Jacobiana, mas também em manter as alterações dentro de limites operacionalmente plausíveis.

Como o modelo binível exige a solução sucessiva de diversos subproblemas MILP, os autores propõem um procedimento de decomposição entre problema mestre e subproblemas. O problema mestre determina provisoriamente as medidas protegidas, enquanto os subproblemas procuram encontrar ataques viáveis contra as diferentes barras de carga. Quando um ataque é identificado, uma nova restrição é adicionada ao problema mestre,

obrigando o defensor a proteger ao menos uma das medidas utilizadas naquele ataque. O processo é repetido até que não seja possível encontrar um conjunto de medidas comprometidas dentro da capacidade do adversário.

Para melhorar a escalabilidade, Liu, Li e Li (2017) desenvolvem ainda uma estratégia distribuída. A rede é particionada em sub-redes conectadas por linhas de interligação. Quando as medidas associadas a essas linhas são protegidas, o conjunto mínimo necessário para atacar uma barra de carga fica restrito à sub-rede em que ela se encontra. Consequentemente, os problemas de proteção podem ser resolvidos separadamente para cada região, reduzindo o tamanho das formulações MILP. A própria divisão da rede é determinada por outro modelo MILP, que busca equilibrar o tamanho das sub-redes e, simultaneamente, limitar a quantidade de linhas de interligação cujas medidas precisam ser protegidas.

6.2 Metodologia de Proteção Baseada em Criticalidades

Os trabalhos citados evidenciam uma evolução gradual das estratégias para a escolha dos recursos de medição a serem protegidos. Bobba *et al.* (2010) fundamentam a seleção na observabilidade algébrica e na identificação de conjuntos básicos de medidas. Dán e Sandberg (2010) introduzem o custo mínimo de ataque como indicador de vulnerabilidade e estendem a análise das medidas individuais para conjuntos de medições agrupados por UMs. Bi e Zhang (2014a) utilizam a observabilidade gráfica e estruturas do tipo Árvore de Steiner para minimizar a quantidade de medidas necessárias à proteção de estados previamente escolhidos. Em Bi e Zhang (2014b), a seleção é ampliada para incluir informações topológicas encobertas e estratégias mistas de proteção. Deng, Xiao e Lu (2017) incorporam a limitação orçamentária e a relação entre investimento defensivo e custo de comprometimento. Por fim, Liu, Li e Li (2017) combinam a seleção de medidas com restrições físicas do ataque, formulações biníveis e decomposição territorial da rede.

Apesar das diferenças metodológicas, essas abordagens compartilham uma característica: a seleção é conduzida principalmente por critérios de observabilidade, posto da matriz Jacobiana, custo mínimo do ataque, quantidade ou custo dos dispositivos protegidos, conectividade topológica, proteção de estados previamente escolhidos ou capacidade atribuída ao atacante. No caso específico das unidades de medição, a literatura examinada é mais restrita. Entre os trabalhos analisados, Dán e Sandberg (2010) são os que representam mais explicitamente o comprometimento conjunto das medições pertencentes a uma

UM; os demais concentram-se predominantemente na escolha de medidores individuais, medições de fluxo e injeção, linhas de interligação ou parâmetros topológicos.

Também é necessário distinguir os diferentes sentidos atribuídos ao termo "crítico". Alguns trabalhos denominam críticas as barras ou variáveis de estado consideradas economicamente importantes, enquanto outros utilizam índices de segurança para identificar medições cujo ataque exige menor esforço. Essas definições não correspondem, necessariamente, à análise estrutural das criticalidades do sistema de medição (ramos, medidas e UMs), o que é considerado neste trabalho. Nos trabalhos examinados, não se observa que a identificação e a priorização dos ramos, medidas ou UMs a serem protegidas tenham como critério central uma análise sistemática dessas criticalidades. Mesmo quando a observabilidade é empregada como restrição, ela é utilizada predominantemente para construir um conjunto protegido de posto completo ou uma sub-rede observável, e não para classificar previamente os elementos do plano de medição segundo sua participação nas diferentes estruturas de criticalidade.

Ataques cibernéticos, ainda que aleatórios, sem que o atacante tenha informações detalhadas sobre a configuração da rede e sistema de medição sendo atacado, podem impactar severamente a supervisão do sistema elétrico, bastando para isso que pontos vulneráveis sejam atingidos. Neste contexto, ataques que atingem medidas que, quando tornadas indisponíveis pelo atacante ou por eliminação durante o processamento de EGs pela EE, fazem com que ramos que formam uma certa criticalidade se tornem irrelevantes, causam também a inobservabilidade da rede pela EE. A formulação apresentada neste trabalho busca reforçar um conjunto mínimo de UMs de forma a proteger criticalidades de C_k-ramos de interesse.

6.2.1 Formulação Matemática

A proposta que se segue visa à proteção das criticalidades de ramos, partindo do reforço das UMs incidentes nestas criticalidades. Assim, a metodologia consiste em determinar um conjunto de UMs a serem previamente protegidas usando como dados de entrada as C_k-ramos identificadas segundo a metodologia apresentada no Capítulo 4. Em sistemas elétricos de potência, a EE depende diretamente da disponibilidade das medidas obtidas nas UMs (RTUs ou PMUs). Conforme mencionado, a perda de determinadas medidas ou UMs pode tornar o sistema não observável, especialmente quando essas perdas coincidem com as tuplas de ramos críticos, as C_k-ramos. Para isso, a formulação do problema de Proteção Mínima de Criticalidades de Ramos (PMCR) apresentada baseia-se nos prin-

cípios da Programação Linear Inteira (PLI), conforme definidos por Maculan e Fampa (2022). Segundo os autores, um problema de programação linear consiste em determinar os valores de um conjunto de variáveis de decisão que minimizam (ou maximizam) uma função objetivo linear, sujeita a restrições também lineares. Quando as variáveis de decisão são restritas a valores binários (0 ou 1), o modelo é classificado como um problema de Programação Linear Inteira Binária (PLI-B).

A PMCR foi modelada utilizando a formulação do conhecido Problema de Cobertura de Conjuntos (*Set Covering Problem* — SCP), um dos modelos clássicos da Otimização Combinatória. Sua estrutura responde a uma pergunta recorrente em problemas de decisão: dado um conjunto de exigências que precisam ser integralmente satisfeitas e um conjunto de alternativas capazes de satisfazê-las, quais alternativas devem ser selecionadas de modo que nenhuma exigência fique descoberta e o custo total seja mínimo?

6.2.1.1 Formulação geral do Problema de Cobertura de Conjuntos

Formalmente, o SCP é definido a partir de um conjunto finito de elementos que devem ser cobertos e de uma família de subconjuntos candidatos, cada qual associado a um custo. Sejam $\mathcal{T}$ o conjunto dos elementos a cobrir, $\mathcal{U}$ o conjunto dos candidatos disponíveis, c_u o custo de seleção do candidato $u \in \mathcal{U}$ e $S_t \subseteq \mathcal{U}$ o subconjunto dos candidatos capazes de cobrir o elemento $t \in \mathcal{T}$. Definindo a variável binária x_u, que assume valor 1 quando o candidato u é selecionado e 0 caso contrário, o modelo é escrito como:

$$\begin{aligned} \text{Minimizar} \quad & Z = \sum_{u \in \mathcal{U}} c_u \, x_u \\ \text{sujeito a:} \quad & \sum_{u \in S_t} x_u \geq 1, \quad \forall \, t \in \mathcal{T}, \\ & x_u \in \{0,1\}, \quad \forall \, u \in \mathcal{U}. \end{aligned} \tag{6.1}$$

A função objetivo contabiliza o custo total da configuração escolhida, somando apenas os custos dos candidatos efetivamente selecionados, uma vez que os termos associados a $x_u = 0$ se anulam. O conjunto de restrições constitui o núcleo conceitual do modelo: para cada elemento t a ser coberto, escreve-se uma restrição que exige a seleção de pelo menos um dos candidatos aptos a cobri-lo. Como as variáveis são binárias, a soma $\sum_{u \in S_t} x_u$ corresponde à contagem de candidatos selecionados que cobrem t, de modo que impor essa contagem como maior ou igual a um equivale a proibir que t permaneça descoberto. O modelo resultante possui, portanto, $|\mathcal{T}|$ restrições de cobertura e $|\mathcal{U}|$ variáveis de decisão.

Cabe destacar o significado do operador de desigualdade ($\geq$): ele admite sobreposição. Um mesmo elemento pode ser coberto por dois ou mais candidatos sem que a solução se torne inviável — a redundância é permitida, embora não seja recompensada, já que cada candidato adicional incrementa o valor da função objetivo. Essa característica distingue o problema de cobertura do problema de particionamento, no qual a restrição assume a forma de igualdade e cada elemento deve ser coberto exatamente uma vez (Goldbarg; Luna, 2005).

O SCP é um problema NP-difícil; sua relevância prática é atestada pela diversidade de domínios em que é aplicado, com destaque para a localização de instalações e serviços de emergência, o posicionamento de antenas em redes de telecomunicações e o escalonamento de tripulações em sistemas de transporte. Em todos esses casos, a estrutura subjacente é a mesma: um conjunto de exigências que não podem ficar desatendidas e um conjunto de alternativas, cada uma capaz de atender simultaneamente a um subconjunto dessas exigências.

6.2.1.2 Aplicação ao problema de Proteção Mínima de Criticalidades de Ramos

A adequação do SCP ao problema tratado neste trabalho decorre de uma correspondência direta entre seus elementos constitutivos e as entidades do sistema de medição. As tuplas de ramos críticos identificadas no Capítulo 4 desempenham o papel dos elementos que devem ser cobertos (protegidos), ao passo que as Unidades de Medição instaladas no sistema desempenham o papel dos candidatos à seleção para reforço. A ação de "cobrir" uma tupla crítica corresponde, no contexto do PMCR, a reforçar ao menos uma das UMs que incidem sobre os ramos que a compõem.

Definem-se, assim, os seguintes conjuntos e parâmetros:

- $\mathcal{U} = \{1, 2, \ldots, n\}$: conjunto das UMs existentes no sistema;
- $\mathcal{T}$: conjunto de tuplas críticas de ramos identificadas (C_1, C_2, C_3, C_4, ...);
- $S_t \subseteq \mathcal{U}$: conjunto de UMs incidentes aos ramos que compõem a tupla crítica $t \in \mathcal{T}$;
- c_u: custo associado ao reforço da UM u (no caso simples, $c_u = 1$).

A variável de decisão é definida como

$$x_u = \begin{cases} 1, & \text{se a UM } u \text{ for reforçada,} \\ 0, & \text{caso contrário,} \end{cases} \qquad \forall\, u \in \mathcal{U}. \tag{6.2}$$

A formulação geral do problema é dada por:

$$\begin{aligned} \text{Minimizar} \quad & Z = \sum_{u \in \mathcal{U}} c_u\, x_u \\ \text{sujeito a:} \quad & \sum_{u \in S_t} x_u \geq 1, \quad \forall\, t \in \mathcal{T}, \\ & x_u \in \{0,1\}, \quad \forall\, u \in \mathcal{U}. \end{aligned} \tag{6.3}$$

A função objetivo minimiza o custo total da proteção implantada. No caso simples, em que se adota $c_u = 1$ para toda UM, o problema reduz-se à minimização da quantidade de unidades protegidas — configuração conhecida na literatura como caso unitário (*unicost*) do SCP. A adoção de custos diferenciados permite, quando pertinente, refletir a heterogeneidade das UMs quanto ao tipo (RTU ou PMU), à localização física, à dificuldade de acesso ou ao investimento requerido pelo mecanismo de proteção.

Cada restrição do modelo é gerada a partir de uma tupla crítica de ramos. A exigência de que ao menos uma UM incidente aos ramos da tupla t seja protegida impede que a totalidade das medidas associadas àquela tupla crítica de ramos seja simultaneamente perdida, o que faria com que todos os ramos que formam a tupla crítica se tornassem irrelevantes. Como a criticalidade de uma tupla de ramos reside justamente no fato de que a perda conjunta de seus ramos compromete a observabilidade do sistema, a proteção de um único elemento de S_t é suficiente para desfazer a condição de falha associada a t. Nesse sentido, o operador (≥ 1) traduz com precisão o requisito operacional: não se exige o reforço de todas as UMs incidentes, mas apenas que a tupla não possa ser integralmente comprometida.

O caráter de sobreposição admitido pelo modelo é particularmente conveniente no contexto do PMCR. Uma mesma UM pode incidir sobre ramos pertencentes a diferentes tuplas de ramos e, ao ser protegida, satisfaz simultaneamente todas as restrições correspondentes. A minimização da função objetivo tende a favorecer a seleção dessas UMs de maior incidência, o que confere ao modelo a capacidade de identificar os pontos de reforço de maior alcance do sistema sem que tal critério precise ser explicitado por meio de regras heurísticas.

6.2.1.3 Estratégias de proteção

A dimensão do problema é determinada pelo número de UMs do sistema, que define a quantidade de variáveis, e pelo número de tuplas críticas de ramos identificadas, que define a quantidade de restrições. Em sistemas de grande porte, ambos os valores podem assumir magnitudes elevadas e, como consequência, a solução ótima pode envolver um número expressivo de UMs a serem protegidas — o que pode se mostrar inviável do ponto de vista orçamentário ou operacional. Diante dessa limitação, vislumbram-se duas estratégias de proteção possíveis, descritas a seguir.

Situação 1 — Reforço global. A primeira estratégia corresponde à formulação apresentada anteriormente, aplicada à proteção de todas as criticalidades de ramos. Nela, o conjunto $\mathcal{T}$ reúne todas as tuplas críticas de ramos identificadas e o conjunto $\mathcal{U}$ abrange todas as UMs instaladas, de modo que a solução ótima Z representa o menor custo de proteção capaz de assegurar que nenhuma tupla crítica de ramos possa ser integralmente comprometida. Trata-se da referência de comparação para qualquer estratégia alternativa, uma vez que estabelece o custo mínimo associado à garantia plena de proteção.

Situação 2 — Reforço por área. A segunda estratégia busca considerar uma característica comum aos sistemas elétricos de grande porte: o direcionamento de maiores investimentos a áreas prioritárias e/ou mais sensíveis para a operação do sistema. A motivação é essencialmente prática: quando a proteção global se revela custosa, pode ser conveniente concentrar os recursos disponíveis em uma área específica — seja por sua maior importância operativa ou por integrar um plano de implantação em etapas.

Sejam $\mathcal{A}$ uma área do sistema e $\mathcal{U}_{\mathcal{A}} \subseteq \mathcal{U}$ o conjunto das UMs a ela pertencentes. Define-se o conjunto das tuplas de ramos críticas associadas a uma dada área como

$$\mathcal{T}_{\mathcal{A}} = \{\, t \in \mathcal{T} \;:\; S_t \cap \mathcal{U}_{\mathcal{A}} \neq \varnothing \,\}, \tag{6.4}$$

isto é, o conjunto das tuplas para as quais existe ao menos uma UM interna à área capaz de cobri-las. Essa definição é necessária para assegurar a viabilidade do modelo: uma tupla cujas UMs incidentes se situem inteiramente fora de $\mathcal{A}$ geraria uma restrição impossível de satisfazer com as variáveis disponíveis, tornando o problema inviável.

O problema de proteção restrito à área $\mathcal{A}$ é então formulado como:

$$\begin{aligned} \text{Minimizar} \quad & Z_{\mathcal{A}} = \sum_{u \in \mathcal{U}_{\mathcal{A}}} c_u \, x_u \\ \text{sujeito a:} \quad & \sum_{u \in S_t \cap \mathcal{U}_{\mathcal{A}}} x_u \geq 1, \quad \forall \, t \in \mathcal{T}_{\mathcal{A}}, \\ & x_u \in \{0,1\}, \quad \forall \, u \in \mathcal{U}_{\mathcal{A}}. \end{aligned} \tag{6.5}$$

Estruturalmente, trata-se do mesmo problema de cobertura de conjuntos, aplicado a um subconjunto de elementos e a um subconjunto de candidatos. A redução de porte é imediata: o número de variáveis passa de $|\mathcal{U}|$ para $|\mathcal{U}_{\mathcal{A}}|$ e o número de restrições, de $|\mathcal{T}|$ para $|\mathcal{T}_{\mathcal{A}}|$.

Duas observações são pertinentes quanto ao alcance dessa formulação. A primeira diz respeito ao escopo da garantia obtida: a solução do problema restrito assegura proteção apenas às tuplas críticas de ramos pertencentes a $\mathcal{T}_{\mathcal{A}}$, não garantindo a proteção às demais tuplas críticas de ramos do sistema. A proteção por área constitui, portanto, uma solução parcial deliberada, e não uma aproximação da solução global.

A segunda observação refere-se às tuplas de fronteira. Em razão dos ramos de interligação entre áreas, uma mesma tupla crítica pode possuir UMs incidentes em mais de uma área, figurando simultaneamente em $\mathcal{T}_{\mathcal{A}}$ e $\mathcal{T}_{\mathcal{B}}$. Caso o procedimento seja aplicado de forma independente a todas as áreas e as soluções sejam posteriormente reunidas, obtém-se uma solução viável para o problema global, porém não necessariamente ótima, uma vez que as tuplas de fronteira tendem a ser cobertas mais de uma vez.

6.2.1.4 Redução da quantidade de restrições

Independentemente da situação de proteção adotada, o modelo admite um procedimento de pré-processamento capaz de reduzir seu porte sem alterar o conjunto de soluções ótimas. Convém observar que nem toda tupla crítica de ramos gera uma restrição efetivamente ativa: se existirem duas tuplas t e t' tais que $S_t \subseteq S_{t'}$, a satisfação da restrição associada a t implica automaticamente a satisfação da restrição associada a t', que se torna redundante e pode ser eliminada do modelo. A aplicação sistemática desse critério de dominância entre linhas constitui procedimento usual em problemas de cobertura e contribui para a redução do esforço computacional em sistemas de grande porte. Essa situação pode ser observada na Tabela 6.1, apresentada adiante, na qual se nota que as UMs associadas (A_k-UMs) a diferentes C_k-ramos são as mesmas.

Por fim, registra-se que a garantia oferecida pelo modelo, em qualquer das duas situ-

ações propostas, é circunscrita ao conjunto de tuplas críticas previamente identificadas e para a proteção até uma cardinalidade de interesse.

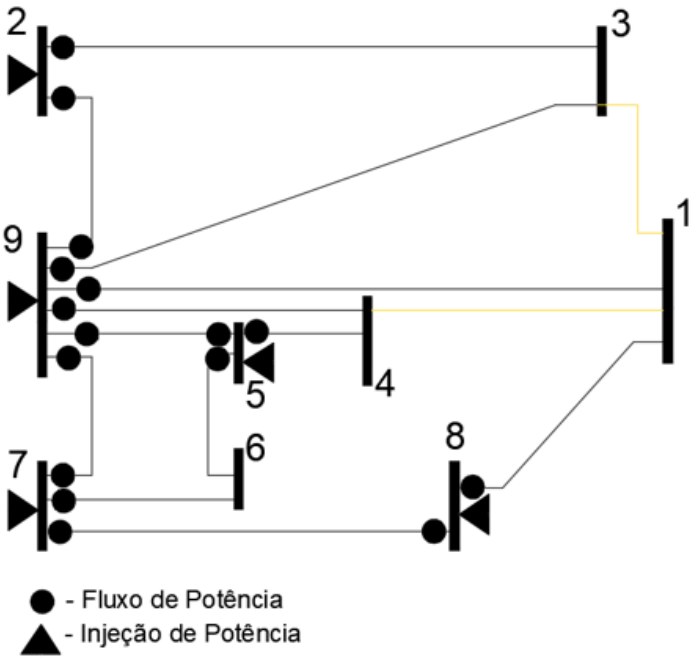
6.3 Testes e Resultados

Com o objetivo de demonstrar o processo de proteção preventiva das C_k-ramos mediante o critério de escolha de UMs, apresentado na seção anterior, apresenta-se com mais detalhes o processo, as tabelas de C_k-ramos e UMs associadas, bem como a tabela final após o processamento de duplicidade de UMs. Utiliza-se o sistema 9 barras exemplo, adotado ao longo desta tese. Em seguida, expõem-se os resultados obtidos para os sistemas IEEE de 30 e 118 barras, para os quais se reportam a quantidade de UMs e de C_k-ramos e os respectivos critérios de proteção, sem o detalhamento tabular das C_k-ramos.

6.3.1 Sistema 9 barras exemplo

Para exemplificar o processo, utiliza-se novamente o sistema exemplo de 9 barras.

Figura 6.1 - Sistema 9 barras exemplo



Fonte: Elaboração própria (2026).

Na Tabela 6.1 são apresentadas as C_k-ramos do sistema e as respectivas UMs associadas.

Tabela 6.1 - UMs associadas às C_k-ramos

C_k-ramos	UMs associadas
$(R_{1\text{-}8}, R_{7\text{-}8})$	UM7, UM8
$(R_{2\text{-}3}, R_{2\text{-}9})$	UM2, UM9
$(R_{5\text{-}6}, R_{6\text{-}7})$	UM5, UM7
$(R_{2\text{-}3}, R_{3\text{-}9})$	UM2, UM9
$(R_{2\text{-}9}, R_{3\text{-}9})$	UM2, UM9
$(R_{4\text{-}5}, R_{4\text{-}9})$	UM5, UM9
$(R_{1\text{-}8}, R_{1\text{-}9})$	UM8, UM9
$(R_{1\text{-}9}, R_{7\text{-}8})$	UM7, UM8, UM9
$(R_{1\text{-}8}, R_{5\text{-}6}, R_{7\text{-}9})$	UM5, UM7, UM8, UM9
$(R_{1\text{-}8}, R_{6\text{-}7}, R_{7\text{-}9})$	UM7, UM8, UM9
$(R_{4\text{-}5}, R_{5\text{-}6}, R_{5\text{-}9})$	UM5, UM9
$(R_{4\text{-}5}, R_{5\text{-}9}, R_{6\text{-}7})$	UM5, UM7, UM9
$(R_{5\text{-}6}, R_{7\text{-}8}, R_{7\text{-}9})$	UM5, UM7, UM8, UM9
$(R_{6\text{-}7}, R_{7\text{-}8}, R_{7\text{-}9})$	UM7, UM8, UM9
$(R_{4\text{-}9}, R_{5\text{-}6}, R_{5\text{-}9})$	UM5, UM9
$(R_{4\text{-}9}, R_{5\text{-}9}, R_{6\text{-}7})$	UM5, UM7, UM9
$(R_{1\text{-}9}, R_{5\text{-}6}, R_{7\text{-}9})$	UM5, UM7, UM9
$(R_{1\text{-}9}, R_{6\text{-}7}, R_{7\text{-}9})$	UM7, UM9
$(R_{1\text{-}8}, R_{4\text{-}5}, R_{5\text{-}9}, R_{7\text{-}9})$	UM5, UM7, UM8, UM9
$(R_{4\text{-}5}, R_{5\text{-}9}, R_{7\text{-}8}, R_{7\text{-}9})$	UM5, UM7, UM8, UM9
$(R_{1\text{-}9}, R_{4\text{-}9}, R_{5\text{-}9}, R_{7\text{-}9})$	UM5, UM7, UM9
$(R_{1\text{-}8}, R_{4\text{-}9}, R_{5\text{-}9}, R_{7\text{-}9})$	UM5, UM7, UM8, UM9
$(R_{4\text{-}9}, R_{5\text{-}9}, R_{7\text{-}8}, R_{7\text{-}9})$	UM5, UM7, UM8, UM9
$(R_{1\text{-}9}, R_{4\text{-}5}, R_{5\text{-}9}, R_{7\text{-}9})$	UM5, UM7, UM9

A primeira etapa, independentemente da metodologia de proteção utilizada (sistema completo ou por área), consiste em reduzir as restrições do modelo, retirando as duplicidades de UMs associadas.

Tabela 6.2 - C_k-ramos após o processamento de duplicidade de UMs

C_k-ramos	UMs associadas
$(R_{1\text{-}8}, R_{7\text{-}8})$	UM7, UM8
$(R_{2\text{-}3}, R_{2\text{-}9})$	UM2, UM9
$(R_{5\text{-}6}, R_{6\text{-}7})$	UM5, UM7
$(R_{4\text{-}5}, R_{4\text{-}9})$	UM5, UM9
$(R_{1\text{-}8}, R_{1\text{-}9})$	UM8, UM9
$(R_{1\text{-}9}, R_{7\text{-}8})$	UM7, UM8, UM9
$(R_{1\text{-}8}, R_{5\text{-}6}, R_{7\text{-}9})$	UM5, UM7, UM8, UM9
$(R_{4\text{-}5}, R_{5\text{-}9}, R_{6\text{-}7})$	UM5, UM7, UM9
$(R_{1\text{-}9}, R_{6\text{-}7}, R_{7\text{-}9})$	UM7, UM9

Fonte: Elaboração própria (2026).

Assim, para o sistema 9 barras tem-se:

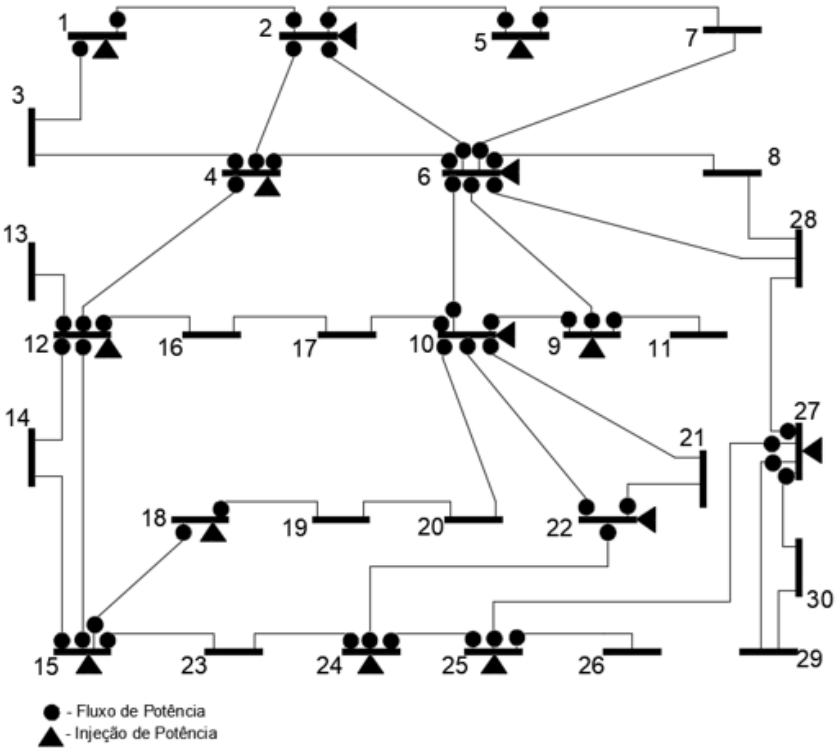
- $\mathcal{U} = \{\text{UM2}, \text{UM5}, \text{UM7}, \text{UM8}, \text{UM9}\}$: conjunto das UMs existentes no sistema;
- $\mathcal{T}$: proteção de todas as tuplas críticas, após o processamento de duplicidade (Tabela 6.2);
- $S_t \subseteq \mathcal{U}$: conjunto de UMs incidentes aos ramos que compõem a tupla crítica $t \in \mathcal{T}$;
- c_u: caso simples, $c_u = 1$ para todas as UMs.

Aplicando o modelo, conclui-se que o reforço das UMs 7 e 9 é suficiente para cobrir todas as C_k-ramos do sistema.

6.3.2 Sistema IEEE 30 barras

Para o sistema IEEE 30 barras, foram definidos três níveis de redundância, com 14, 21 e 28 UMs. Optou-se por fazer a proteção de todo o sistema, não definindo subáreas. No sistema com 14 UMs há 4 ramos irrelevantes, sendo eles: $R_{8\text{-}28}$, $R_{16\text{-}17}$, $R_{19\text{-}20}$ e $R_{29\text{-}30}$. A Figura 6.2 apresenta o sistema com a disposição das UMs e a Tabela 6.3 a quantidade de C_k-ramos do sistema por cardinalidade. A Tabela 6.4 apresenta as UMs a serem reforçadas para proteção das C_k-ramos de acordo com a cardinalidade. Observa-se que a partir de $k = 2$ a quantidade de UMs escolhidas é sempre igual a 10.

Figura 6.2 - IEEE 30 barras com 14 UMs



Fonte: Elaboração própria (2026).

Tabela 6.3 - Quantidade de C_k-ramos por cardinalidade (IEEE 30 barras — 14 UMs)

Cardinalidade (k)	**C_k-ramos**
1	11
2	18
3	22
4	87
5	68

Fonte: Elaboração própria (2026).

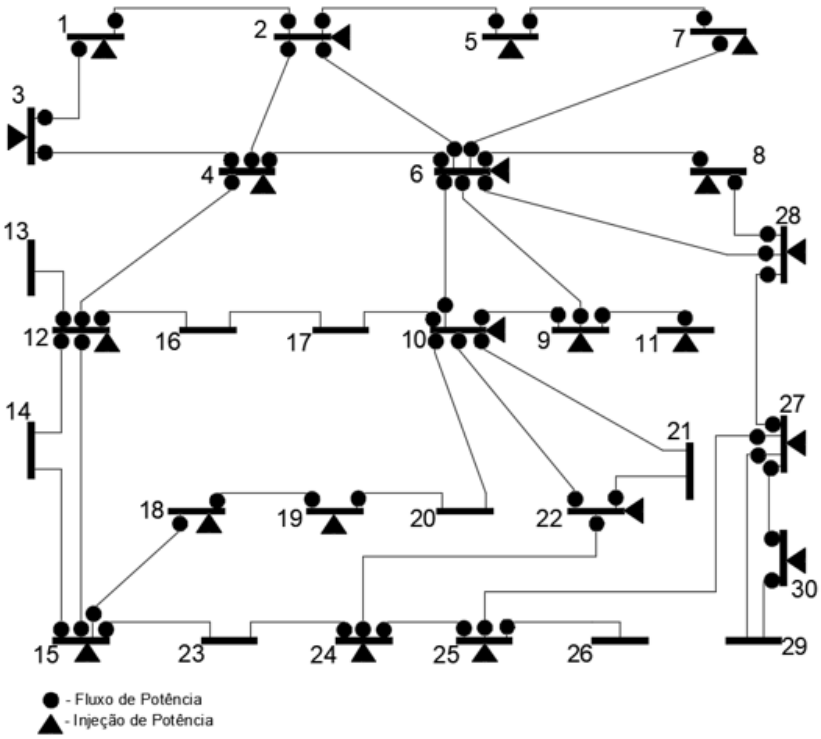
Tabela 6.4 - UMs a serem reforçadas (IEEE 30 barras — 14 UMs)

Cardinalidade – C_k-ramos	**Restrições analisadas**	**Qtd. de UMs**	**UMs reforçadas**
1	7	7	{6, 9, 10, 12, 18, 25, 27}
2	11	10	{1, 2, 6, 9, 10, 12, 18, 24, 25, 27}
3	11	10	{1, 2, 6, 9, 10, 12, 18, 24, 25, 27}
4	11	10	{1, 2, 6, 9, 10, 12, 18, 24, 25, 27}
5	11	10	{1, 2, 6, 9, 10, 12, 18, 24, 25, 27}

Fonte: Elaboração própria (2026).

No sistema com 21 UMs há apenas um ramo irrelevante, sendo ele $R_{16\text{-}17}$. A Figura 6.3 apresenta o sistema com a disposição das UMs e a Tabela 6.5 a quantidade de C_k-ramos do sistema por cardinalidade. A Tabela 6.6 apresenta as UMs escolhidas para proteção das C_k-ramos de acordo com a cardinalidade. Mais uma vez, observa-se que a partir de $k = 2$ a quantidade de UMs escolhidas é sempre igual a 10; entretanto, a quantidade de UMs escolhidas para proteção dos ramos críticos é menor, o que pode ser justificado pela quantidade de ramos críticos no sistema.

Figura 6.3 - IEEE 30 barras com 21 UMs



Fonte: Elaboração própria (2026).

Tabela 6.5 - Quantidade de C_k-ramos por cardinalidade (IEEE 30 barras — 21 UMs)

Cardinalidade (k)	**C_k-ramos**
1	5
2	23
3	24
4	73
5	208

Fonte: Elaboração própria (2026).

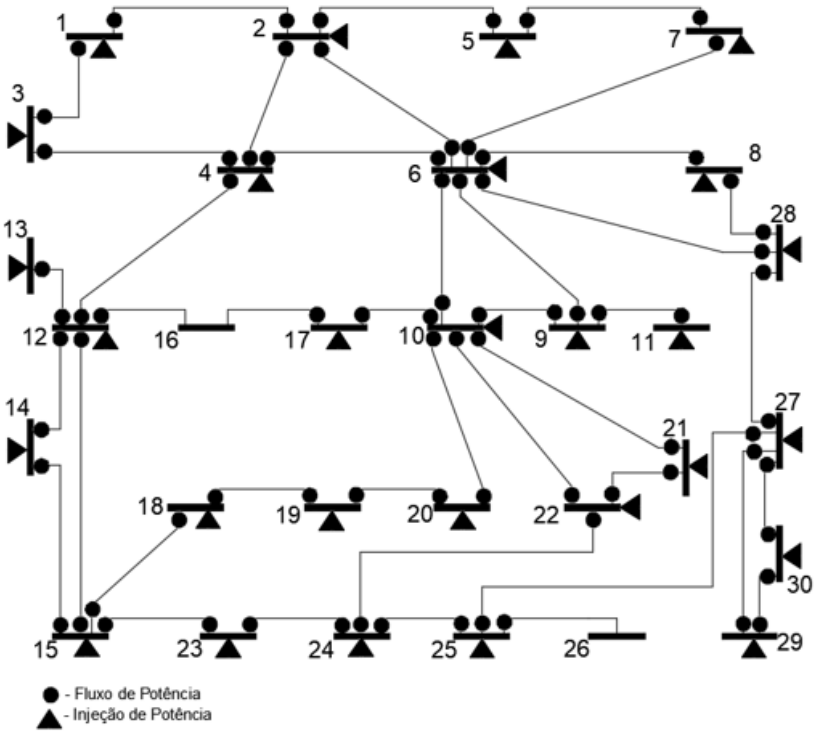
Tabela 6.6 - UMs a serem reforçadas (IEEE 30 barras — 21 UMs)

Cardinalidade – C_k-ramos	**Restrições analisadas**	**Qtd. de UMs**	**UMs reforçadas**
1	4	4	{10, 11, 12, 25}
2	12	10	{3, 6, 7, 10, 11, 12, 19, 24, 25, 30}
3	13	10	{3, 6, 7, 10, 11, 12, 19, 24, 25, 27}
4	17	10	{2, 3, 6, 10, 11, 12, 19, 24, 25, 27}
5	29	10	{2, 3, 6, 10, 11, 12, 19, 24, 25, 27}

Fonte: Elaboração própria (2026).

No sistema com 28 UMs não há ramos irrelevantes. A Figura 6.4 apresenta o sistema com a disposição das UMs e a Tabela 6.7 a quantidade de C_k-ramos do sistema por cardinalidade. A Tabela 6.8 apresenta as UMs escolhidas para proteção das C_k-ramos de acordo com a cardinalidade. A análise para esse caso é similar à do caso com 21 UMs. A partir de $k = 2$, a quantidade de UMs não se altera, apenas as UMs escolhidas. Novamente, a quantidade de UMs escolhidas para proteção das criticalidades de ramos é menor.

Figura 6.4 - IEEE 30 barras com 28 UMs



Fonte: Elaboração própria (2026).

Tabela 6.7 - Quantidade de C_k-ramos por cardinalidade (IEEE 30 barras — 28 UMs)

Cardinalidade (k)	**C_k-ramos**
1	3
2	26
3	14
4	83
5	100

Fonte: Elaboração própria (2026).

Tabela 6.8 - UMs a serem reforçadas (IEEE 30 barras — 28 UMs)

Cardinalidade – C_k-ramos	Restrições analisadas	Qtd. de UMs	UMs reforçadas
1	3	3	{11, 13, 25}
2	19	10	{3, 6, 7, 9, 10, 12, 15, 20, 25, 30}
3	20	10	{3, 6, 7, 9, 10, 12, 15, 20, 25, 27}
4	34	10	{2, 4, 6, 9, 10, 12, 15, 20, 25, 27}
5	38	10	{2, 4, 6, 9, 10, 12, 15, 20, 25, 27}

Fonte: Elaboração própria (2026).

6.3.3 Sistema IEEE 118 barras

Para análise do sistema IEEE 118 barras, optou-se por fazer os dois tipos de proteção: (1) proteção do sistema completo; e (2) proteção por área. Foi avaliado um plano de medição com 68 UMs, que apresenta 11 ramos irrelevantes. Para a proteção por área, adotou-se a divisão apresentada em Rocha (2010), que organiza o sistema em três áreas:

- **Área 1:** barras 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 25, 26, 27, 28, 29, 30, 31, 32, 113, 114, 115, 117.
- **Área 2:** barras 24, 38, 62, 64, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 116, 118.
- **Área 3:** barras 33, 34, 35, 36, 37, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 63, 65.

A divisão em áreas permite avaliar, no mesmo sistema e sob os mesmos dados de entrada, o contraste entre a solução global e as soluções parciais, incluindo o efeito das tuplas de fronteira discutido na formulação.

A Tabela 6.9 apresenta a quantidade de C_k-ramos por cardinalidade. Observa-se, de imediato, o porte do conjunto de criticalidades: são 289 tuplas críticas de ramos no total,

das quais 23 são ramos críticos. A exemplo dos casos anteriores, a primeira etapa consiste no processamento de duplicidade das UMs associadas, que reduz o conjunto de restrições efetivamente submetidas ao modelo; as quantidades de restrições analisadas após essa redução são reportadas nas tabelas de resultados de cada caso.

Tabela 6.9 - Quantidade de C_k-ramos por cardinalidade (IEEE 118 barras — 68 UMs)

Cardinalidade (k)	**C_k-ramos**
1	23
2	67
3	38
4	161

Fonte: Elaboração própria (2026).

A Tabela 6.10 apresenta as UMs escolhidas para a proteção do sistema completo, de acordo com a cardinalidade das C_k-ramos consideradas.

Tabela 6.10 - UMs a serem reforçadas — sistema completo (IEEE 118 barras — 68 UMs)

Cardinalidade – C_k-ramos	**Restrições analisadas**	**Qtd. de UMs**	**UMs reforçadas**
1	18	18	{9, 12, 27, 28, 32, 50, 51, 59, 62, 68, 71, 80, 86, 92, 94, 100, 105, 110}
2	46	34	{3, 5, 9, 12, 15, 19, 22, 27, 28, 30, 32, 35, 40, 44, 49, 50, 51, 54, 59, 62, 65, 68, 71, 75, 77, 80, 85, 86, 89, 92, 94, 100, 105, 110}
3	50	35	{3, 5, 9, 12, 15, 19, 22, 27, 28, 30, 32, 35, 40, 44, 46, 50, 51, 54, 59, 62, 65, 68, 70, 71, 75, 77, 80, 85, 86, 89, 92, 94, 100, 105, 110}
4	63	35	{3, 5, 9, 12, 15, 19, 22, 23, 27, 28, 30, 32, 35, 40, 44, 46, 50, 51, 54, 59, 62, 65, 68, 71, 75, 77, 80, 85, 86, 89, 92, 94, 100, 105, 110}

Fonte: Elaboração própria (2026).

Para as criticalidades de cardinalidade unitária, a quantidade de UMs reforçadas coincide com a quantidade de restrições analisadas (18), como é de se esperar: cada C_1-ramo impõe a proteção de uma UM específica, sem margem de escolha para o modelo. A partir de $k = 2$, repete-se o comportamento observado no IEEE 30 barras: a quantidade de UMs protegidas estabiliza-se — 34 unidades em $k = 2$ e 35 a partir de $k = 3$ —, com alterações apenas pontuais na composição do conjunto (a inclusão da UM46 e da UM70 em $k = 3$, por exemplo, e a substituição da UM70 pela UM23 em $k = 4$). O acréscimo de 17 restrições entre $k = 2$ e $k = 4$ (de 46 para 63) produziu o acréscimo de apenas uma UM na solução, confirmando que as tuplas de ordem superior encontram-se, em sua maioria, cobertas pela proteção definida nas ordens inferiores. Em termos de esforço relativo, a proteção plena do sistema completo requer 35 das 68 UMs, ou seja, cerca de metade do sistema de medição.

Na sequência, o modelo foi aplicado isoladamente a cada uma das três áreas. As

Tabelas 6.11 a 6.13 apresentam os resultados para as Áreas 1, 2 e 3, respectivamente.

Tabela 6.11 - UMs a serem reforçadas — Área 1 (IEEE 118 barras — 68 UMs)

Cardinalidade – C_k-ramos	**Restrições analisadas**	**Qtd. de UMs**	**UMs reforçadas**
1	5	5	{9, 12, 27, 28, 32}
2	16	11	{3, 5, 9, 12, 15, 19, 22, 27, 28, 30, 32}
3	14	12	{3, 5, 9, 12, 15, 19, 21, 23, 27, 28, 30, 32}
4	13	12	{3, 5, 9, 12, 15, 19, 22, 23, 27, 28, 30, 32}

Fonte: Elaboração própria (2026).

Tabela 6.12 - UMs a serem reforçadas — Área 2 (IEEE 118 barras — 68 UMs)

Cardinalidade – C_k-ramos	**Restrições analisadas**	**Qtd. de UMs**	**UMs reforçadas**
1	10	10	{62, 68, 71, 80, 86, 92, 94, 100, 105, 110}
2	17	14	{62, 68, 71, 75, 77, 80, 85, 86, 89, 92, 94, 100, 105, 110}
3	21	17	{38, 62, 68, 69, 70, 71, 76, 77, 80, 85, 86, 89, 92, 94, 100, 105, 110}
4	21	17	{24, 38, 62, 68, 69, 71, 75, 77, 80, 85, 86, 89, 92, 94, 100, 105, 110}

Fonte: Elaboração própria (2026).

Tabela 6.13 - UMs a serem reforçadas — Área 3 (IEEE 118 barras — 68 UMs)

Cardinalidade – C_k-ramos	**Restrições analisadas**	**Qtd. de UMs**	**UMs reforçadas**
1	3	3	{50, 51, 59}
2	13	10	{35, 37, 40, 44, 49, 50, 51, 54, 59, 65}
3	15	11	{34, 37, 40, 44, 46, 50, 51, 54, 59, 61, 65}
4	15	11	{34, 37, 40, 45, 49, 50, 51, 54, 59, 61, 65}

Fonte: Elaboração própria (2026).

Os resultados por área evidenciam a redução de porte proporcionada pela decomposição. Considerando a proteção plena ($k = 4$), as Áreas 1, 2 e 3 demandam, respectivamente, 12, 17 e 11 UMs — valores substancialmente inferiores às 35 UMs da proteção global, o que viabiliza a implantação da proteção em etapas compatíveis com os recursos disponíveis. A Área 2, que concentra o maior número de barras e de criticalidades, é também a que demanda o maior contingente de proteção, indicando que a distribuição das criticalidades entre as áreas pode orientar a ordem de priorização em um plano de implantação gradual.

Nota-se, ainda, a consistência entre as soluções por área e a solução global: nas cardinalidades unitárias, as 18 UMs da proteção global correspondem exatamente à união das UMs das três áreas ($5+10+3$), uma vez que cada C_1-ramo impõe uma UM específica, sem interação entre áreas. Nas cardinalidades superiores, contudo, a soma das soluções por área ($12+17+11 = 40$ UMs, em $k = 4$) supera a solução global (35 UMs). Essa diferença é consequência direta das tuplas de fronteira: criticalidades com UMs incidentes em mais de uma área são cobertas de forma independente em cada subproblema, gerando proteções redundantes que a otimização global evita. A escolha de uma ou outra estratégia de reforço depende, contudo, do critério de planejamento adotado e das restrições financeiras para investimento nos reforços.

6.4 Considerações Finais

Os resultados obtidos mostram que a determinação do conjunto mínimo de UMs a serem reforçadas pode ser guiada pelo conhecimento das criticalidades de ramos, tendo sido

observado que com a proteção de C_k-ramos de cardinalidades inferiores é possível proteger C_k-ramos de maior cardinalidade. O conjunto de UMs a reforçar pode ser diferente caso os custos de reforço associados sejam representados, o que é possível na formulação proposta. A proteção de criticalidades de ramos em partes específicas da rede, onde a supervisão é mais importante, foi também considerada e leva à redução de custos com reforço de UMs, uma vez que uma quantidade menor de UMs deve ser reforçada. Os resultados obtidos mostram que o conhecimento das C_k-ramos é útil para indicar vulnerabilidades a serem protegidas. Tal importância é ainda mais direta caso se considere a possibilidade de ataques físicos a instalações e linhas de transmissão, o que não foi considerado neste trabalho.

7 Conclusões e Trabalhos Futuros

A estimação de estado de sistemas de potência, responsável por fornecer a condição de operação mais provável do sistema elétrico e alimentar de dados as funções avançadas de análise, automação e controle, pode experimentar condições adversas que afetam o seu desempenho e a qualidade de seus resultados. Dentre tais adversidades pode-se destacar, por exemplo, erros grosseiros que acometem as medidas recebidas no centro de operação e, mais recentemente, ataques cibernéticos que buscam comprometer o funcionamento do estimador. Quando isto acontece, a observabilidade da rede ou a capacidade de depurar erros grosseiros são em geral afetadas. A chance de eventos adversos efetivamente prejudicarem o funcionamento do estimador é maior quando envolvem os pontos mais vulneráveis para o processo de estimação de estado. Tais vulnerabilidades, do ponto de vista estrutural, se concentram nas criticalidades de medidas, unidades de medição e ramos da rede, podendo ser constituídas por elementos individuais ou grupos de elementos.

Este trabalho apresenta metodologias para a identificação de criticalidades para a estimação de estado, enfocando não apenas as criticalidades de medidas, mas também as criticalidades de ramos e unidades de medição. A maioria dos trabalhos correlatos encontrados na literatura se dedica à identificação de criticalidades de medidas de baixa cardinalidade, em geral até pares críticos de medidas. Isto se deve, em parte, à dificuldade de prosseguir com a identificação de criticalidades de mais alta cardinalidade, dada a natureza combinatória deste problema. Somado a isso, percebem-se as medidas críticas e os pares críticos de medidas como estando associados a eventos de ocorrência mais provável, envolvendo erro grosseiro ou indisponibilidade de uma única medida. Porém, os erros grosseiros (ou indisponibilidades) podem acometer grupos de medidas correlacionadas, por exemplo, por pertencerem à mesma unidade de medição, compartilharem o mesmo canal de comunicação ou estarem simultaneamente submetidos a um ataque cibernético. Em tais situações, criticalidades de maior cardinalidade podem também estar presentes e comprometer a função estimação de estado. As criticalidades de ramos, por sua vez, podem também ser diretamente associadas a eventos comuns na operação do sistema

elétrico, como o chaveamento de linhas de transmissão e a ocorrência de contingências. Nestes casos, ou mesmo na ocorrência de ataques físicos em instalações, a supervisão da rede pode ser afetada se os eventos atingirem uma criticalidade de ramos.

As metodologias propostas neste trabalho são baseadas, inicialmente, na identificação de criticalidades de ramos, pouco abordadas na literatura e, como visto nos capítulos anteriores, importantes e interessantes para a determinação também das criticalidades de unidades de medição e medidas. Duas metodologias para identificação das criticalidades de ramos foram apresentadas. A primeira se baseia apenas na topologia da rede e, a partir de uma configuração de rede completa, as criticalidades são determinadas *offline* uma única vez. Posteriormente, para configurações de rede e sistemas de medição específicos as criticalidades obtidas *offline* são atualizadas de forma eficiente. A segunda considera tanto a topologia da rede quanto o sistema de medição correntes, por isso denominada *online*. Com base no sistema de medição corrente, um sistema de medição hipotético reduzido, convenientemente escolhido, é empregado e permite que o problema de identificação de criticalidades de ramos seja tratado como um problema de identificação de criticalidades de medidas, com o emprego de um método numérico eficiente para sua solução.

Ambas as metodologias utilizam o conceito de ramo irrelevante para a estimação de estado e propriedades das criticalidades de ramos. Apesar de a primeira metodologia permitir atualizações muito eficientes das criticalidades de ramos, falhas na determinação destas podem ocorrer se a cardinalidade das criticalidades obtidas *offline* não for suficientemente grande, por vezes muito maior que a cardinalidade de interesse quando da atualização. Este problema se manifesta sobretudo nas situações em que a atualização deve ocorrer para sistemas de medição que se encontram com mais baixa redundância. Para sistemas de maior porte, a obtenção de todas as criticalidades de ramos de cardinalidade mais elevada pode ser inviável, mesmo isso sendo realizado *offline*. A segunda metodologia, por sua vez, por considerar simultaneamente a topologia da rede e o sistema de medição, permite a obtenção das criticalidades de ramos de forma eficiente, mesmo para sistemas de maior porte. Neste caso, as criticalidades obtidas devem ser atualizadas sempre que ocorrer uma alteração topológica ou alteração no conjunto de ramos irrelevantes para a EE.

Foi apresentada também uma metodologia para, a partir do conhecimento das criticalidades de ramos, obter também as criticalidades de unidades de medição e de medidas. A obtenção das criticalidades de unidades de medição ocorre de forma muito eficiente e direta, sem a necessidade de se analisar combinações de UMs e sem falhas de identifi-

cação. A obtenção das criticalidades de medidas, por sua vez, requer a análise de uma quantidade bastante reduzida de combinações de medidas, ocorrendo de forma eficiente conforme indicado nos resultados obtidos no Capítulo 5. Isto é possível explorando de forma heurística a relação entre as criticalidades de ramos previamente conhecidas e as criticalidades de medidas.

Finalmente, a informação sobre as criticalidades de ramos foi explorada para a indicação de unidades de medição a serem reforçadas de forma a tornar a supervisão da rede mais resiliente a ataques cibernéticos. Uma metodologia que utiliza programação linear inteira binária é empregada para se obter o reforço de mínimo custo que garante a proteção de criticalidades de ramos até uma certa cardinalidade de interesse. Observou-se que as unidades de medição indicadas para a proteção das criticalidades de ramos de baixa cardinalidade já são suficientes para aumentar significativamente a resiliência da supervisão da rede. Simulações utilizando um sistema exemplo de pequeno porte e também os sistemas IEEE 14-, 30-, 118- e 300-barras foram realizadas para ilustrar as metodologias propostas, com os resultados obtidos apresentados e discutidos.

7.1 Trabalhos Futuros

A pesquisa realizada abre caminho para diversos desenvolvimentos futuros, podendo ser destacados:

Determinação sistemática da cardinalidade *offline* mínima para as criticalidades de ramos — os resultados do Capítulo 4 mostraram que, conhecida a cardinalidade-alvo das criticalidades de UMs e de medidas, é possível limitar a busca *offline* das criticalidades de ramos, com economia computacional expressiva. Permanece em aberto, contudo, a determinação sistemática — idealmente com garantias teóricas — da cardinalidade *offline* mínima necessária para assegurar a identificação completa das criticalidades derivadas, para diferentes cardinalidades-alvo e níveis de redundância de medidas.

Índices de vulnerabilidade da supervisão — a base de dados de criticalidades produzida pela metodologia desenvolvida fornece subsídios para a construção de índices quantitativos que sintetizem o nível de vulnerabilidade de um plano de medição. Tais índices podem considerar não apenas a cardinalidade das tuplas críticas, interpretável como distância para a inobservabilidade, mas também a distribuição das criticalidades de medidas pelas UMs, refletindo a probabilidade de perdas conjuntas. Métricas dessa natureza permitem comparar planos de medição, priorizar reforços e acompanhar a evolução da robustez

da supervisão ao longo do tempo, em linha com esforços de quantificação já presentes na literatura (Coutto Filho; Souza; Villavicencio Tafur, 2013).

Integração com a análise de contingências — as alterações topológicas decorrentes de contingências modificam as criticalidades do sistema, degradando a capacidade de supervisão da rede. A integração da análise de criticalidades à análise de contingências comumente realizada em centros de operação permitiria avaliar, para cada cenário, não apenas os impactos elétricos da contingência, mas também seus efeitos sobre a observabilidade e sobre a capacidade de depuração de erros grosseiros, agregando a dimensão da supervisão aos estudos de segurança operativa.

Ampliação do escopo da aplicação em cibersegurança — a formulação de proteção apresentada no Capítulo 6 contempla ataques dirigidos às UMs, sob a hipótese de que o reforço de uma unidade de medição a torna inacessível ao adversário. Duas extensões se delineiam. A primeira é a consideração de ataques ciberfísicos coordenados, nos quais a proteção deve abranger conjuntamente linhas de transmissão e unidades de medição. A segunda é a parametrização dos custos de proteção com valores efetivamente diferenciados por equipamento — possibilidade já prevista na formulação, por meio dos coeficientes da função objetivo, mas não explorada nos testes, que adotaram o caso unitário.

Referências

ABUR, Ali; GOMEZ EXPOSITO, Antonio. **Power System State Estimation: Theory and Implementation**. New York: Marcel Dekker, 2004. (Power Engineering). ISBN 978-0-8247-5570-6. DOI: 10.1201/9780203913673.

AHMAD, Mukhtar. **Power System State Estimation**. Boston: Artech House, 2013. (Artech House Power Engineering Series). ISBN 978-1-60807-511-9.

AUGUSTO, Andre Abel; COUTTO FILHO, Milton Brown; SOUZA, Julio Cesar Stacchini de; GUIMARAENS, Marcio Andre Ribeiro. Branch-and-Bound Guided Search for Critical Elements in State Estimation. **IEEE Transactions on Power Systems**, v. 34, n. 3, p. 2292–2301, mai. 2019. ISSN 0885-8950. DOI: 10.1109/TPWRS.2018.2881421.

AUGUSTO, Andre Abel; COUTTO FILHO, Milton Brown; SOUZA, Julio Cesar Stacchini de; MIRANDA, Vladimiro. Probabilistic Assessment of State Estimation Capabilities for Grid Observation. **IET Generation, Transmission & Distribution**, v. 10, n. 12, p. 2933–2941, set. 2016. ISSN 1751-8695. DOI: 10.1049/iet-gtd.2015.1406.

AUGUSTO, Andre Abel; GUIMARAENS, Marcio Andre Ribeiro; COUTTO FILHO, Milton Brown; SOUZA, Julio Cesar Stacchini de. Assessing Strengths and Weaknesses of Measurement Sets for State Estimation. *In:* 2017 IEEE Manchester PowerTech. Manchester: IEEE, jun. 2017. p. 1–6. ISBN 978-1-5090-4237-1. DOI: 10.1109/PTC.2017.7980839.

BI, Suzhi; ZHANG, Ying Jun. Graphical Methods for Defense Against False-Data Injection Attacks on Power System State Estimation. **IEEE Transactions on Smart Grid**, v. 5, n. 3, p. 1216–1227, mai. 2014. ISSN 1949-3053. DOI: 10.1109/TSG.2013.2294966.

BI, Suzhi; ZHANG, Ying Jun. Using Covert Topological Information for Defense Against Malicious Attacks on DC State Estimation. **IEEE Journal on Selected Areas in Communications**, v. 32, n. 7, p. 1471–1485, jul. 2014. ISSN 0733-8716. DOI: 10.1109/JSAC.2014.2332051.

BOBBA, Rakesh B.; DAVIS, Katherine R.; WANG, Qiyan; KHURANA, Himanshu; NAHRSTEDT, Klara; OVERBYE, Thomas J. Detecting False Data Injection Attacks

on DC State Estimation. *In:* PREPRINTS of the First Workshop on Secure Control Systems (CPSWEEK). [*S. l.: s. n.*], abr. 2010.

BRAGA FLOR, Vinicius Bernardo; COUTTO FILHO, Milton Brown; SOUZA, Julio Cesar Stacchini de; VERGARA, Pedro Pablo. Critical Data Visualization to Enhance Protection Schemes for State Estimation. **IEEE Transactions on Smart Grid**, v. 14, n. 2, p. 1249–1261, mar. 2023. ISSN 1949-3053. DOI: 10.1109/TSG.2022.3203404.

CASTILLO, Enrique; CONEJO, Antonio J.; PRUNEDA, Rosa E.; SOLARES, Cristina; MENENDEZ, Jose Maria. $m - k$ Robust Observability in State Estimation. **IEEE Transactions on Power Systems**, v. 23, n. 2, p. 296–305, mai. 2008. ISSN 0885-8950. DOI: 10.1109/TPWRS.2008.920707.

CHEN, Jian; ABUR, Ali. Enhanced Topology Error Processing via Optimal Measurement Design. **IEEE Transactions on Power Systems**, v. 23, n. 3, p. 845–852, ago. 2008. ISSN 0885-8950. DOI: 10.1109/TPWRS.2008.926083.

CHEN, Thomas M. Stuxnet, the Real Start of Cyber Warfare? [Editor's Note]. **IEEE Network**, v. 24, n. 6, p. 2–3, nov. 2011. DOI: 10.1109/MNET.2010.5634434.

CLEMENTS, K. A.; DAVIS, P. W. Detection and Identification of Topology Errors in Electric Power Systems. **IEEE Transactions on Power Systems**, v. 3, n. 4, p. 1748–1753, nov. 1988. ISSN 0885-8950. DOI: 10.1109/59.192991.

CLEMENTS, K. A.; DAVIS, P. W. Multiple Bad Data Detectability and Identifiability: A Geometric Approach. **IEEE Transactions on Power Delivery**, v. 1, n. 3, p. 355–360, jul. 1986. ISSN 0885-8977. DOI: 10.1109/TPWRD.1986.4308015.

COIMBRA, Andrei Mantesso. **Identificação de criticalidades de ramos, medidas e unidades de medição na estimação de estado**. Mar. 2019. Dissertação (Mestrado em Computação) – Universidade Federal Fluminense, Niterói.

COIMBRA, Andrei Mantesso; NISHIO, Ayres; SOUZA, Julio Cesar Stacchini de; COUTTO FILHO, Milton Brown. Identificação de Tuplas de Ramos e de Medidas Críticas para a Estimação de Estado. *In:* ANAIS do XXVI Congresso Brasileiro de Automática. São Paulo: [*s. n.*], out. 2026. v. 1. Disponível em: https://ojs.sba.org.br/index.php/cba/article/view/6378.

COIMBRA, Andrei Mantesso; SOUZA, Julio Cesar Stacchini de; COUTTO FILHO, Milton Brown. Identificação de Tuplas Críticas de Ramos na Estimação de Estado. *In:* ANAIS do Simpósio Brasileiro de Automação Inteligente. [*S. l.: s. n.*], ago. 2025. Disponível em: https://ojs.sba.org.br/index.php/sbai/article/view/5120.

COIMBRA, Andrei Mantesso; SOUZA, Julio Cesar Stacchini de; COUTTO FILHO, Milton Brown; AUGUSTO, Andre Abel. Network-Based Approach to Identify Criticalities in State Estimation. **IEEE Transactions on Power Systems**, v. 36, n. 4, p. 3394–3405, jul. 2021. ISSN 0885-8950. DOI: 10.1109/TPWRS.2021.3055122.

CORMEN, Thomas H.; LEISERSON, Charles E.; RIVEST, Ronald L.; STEIN, Clifford. **Introduction to Algorithms**. 3. ed. Cambridge: MIT Press, 2009. ISBN 978-0-262-03384-8.

COSTA, Antonio Simoes; PIAZZA, T. S.; MANDEL, A. Qualitative Methods to Solve Qualitative Problems in Power System State Estimation. **IEEE Transactions on Power Systems**, v. 5, n. 3, p. 941–949, ago. 1990. ISSN 0885-8950. DOI: 10.1109/59.65924.

COUTTO FILHO, Milton Brown; SOUZA, Julio Cesar Stacchini de; AUGUSTO, Andre Abel. Critical Measuring Units for State Estimation. *In:* 2014 Power Systems Computation Conference. Wroclaw: IEEE, ago. 2014. p. 1–7. ISBN 978-83-935801-3-2. DOI: 10.1109/PSCC.2014.7038472.

COUTTO FILHO, Milton Brown; SOUZA, Julio Cesar Stacchini de; GLOVER, John Duncan. Roots, Achievements, and Prospects of Power System State Estimation: A Review on Handling Corrupted Measurements. **International Transactions on Electrical Energy Systems**, v. 29, n. 4, e2779, abr. 2019. ISSN 2050-7038. DOI: 10.1002/etep.2779.

COUTTO FILHO, Milton Brown; SOUZA, Julio Cesar Stacchini de; GLOVER, John Duncan; BRAGA FLOR, Vinicius Bernardo; NISHIO, Ayres; LIMA, Rafael Carlos Soares; DAIBES, Joao Victor; QUINTANILHA, Luiz; COIMBRA, Andrei Mantesso; SOARES, Wellyngton; CARNEIRO, Henrique. Educational Tool for Power System State Estimation Teaching and Learning. **IEEE Transactions on Power Systems**, v. 38, n. 6, p. 5885–5895, 2022. ISSN 0885-8950. DOI: 10.1109/TPWRS.2022.3229908.

COUTTO FILHO, Milton Brown; SOUZA, Julio Cesar Stacchini de; GUIMARAENS, Marcio Andre Ribeiro. Enhanced Bad Data Processing by Phasor-Aided State Estimation. **IEEE Transactions on Power Systems**, v. 29, n. 5, p. 2200–2209, set. 2014. ISSN 0885-8950. DOI: 10.1109/TPWRS.2014.2304620.

COUTTO FILHO, Milton Brown; SOUZA, Julio Cesar Stacchini de; SCHILLING, Marcus Theodor. Handling Critical Data and Observability. **Electric Power Components and Systems**, Taylor & Francis, v. 35, n. 5, p. 553–573, mai. 2007. ISSN 1532-5008. DOI: 10.1080/15325000601078187.

COUTTO FILHO, Milton Brown; SOUZA, Julio Cesar Stacchini de; VILLAVICENCIO TAFUR, Johnny Edward. Quantifying Observability in State Estimation. **IEEE**

Transactions on Power Systems, v. 28, n. 3, p. 2897–2906, ago. 2013. ISSN 0885-8950. DOI: 10.1109/TPWRS.2013.2241459.

CRAINIC, E. D.; HORISBERGER, H. P.; DO, X. D.; MUKHEDKAR, D. Power Network Observability: The Assessment of the Measurement System Strength. **IEEE Transactions on Power Systems**, v. 5, n. 4, p. 1267–1285, nov. 1990. ISSN 0885-8950. DOI: 10.1109/59.99378.

DÁN, György; SANDBERG, Henrik. Stealth Attacks and Protection Schemes for State Estimators in Power Systems. *In:* 2010 First IEEE International Conference on Smart Grid Communications. [*S. l.: s. n.*], out. 2010. p. 214–219. DOI: 10.1109/SMARTGRID.2010.5622046.

DENG, Ruilong; XIAO, Gaoxi; LU, Rongxing. Defending Against False Data Injection Attacks on Power System State Estimation. **IEEE Transactions on Industrial Informatics**, v. 13, n. 1, p. 198–207, fev. 2017. ISSN 1551-3203. DOI: 10.1109/TII.2015.2470218.

GOLDBARG, Marco Cesar; LUNA, Henrique Pacca L. **Otimização combinatória e programação linear: modelos e algoritmos**. 2. ed. Rio de Janeiro: Elsevier, 2005. ISBN 978-85-352-1520-5.

GOU, Bei; ABUR, Ali. A Direct Numerical Method for Observability Analysis. **IEEE Transactions on Power Systems**, v. 15, n. 2, p. 625–630, mai. 2000. ISSN 0885-8950. DOI: 10.1109/59.867151.

HANDSCHIN, E.; SCHWEPPE, Fred C.; KOHLAS, J.; FIECHTER, A. Bad Data Analysis for Power System State Estimation. **IEEE Transactions on Power Apparatus and Systems**, v. 94, n. 2, p. 329–337, mar. 1975. ISSN 0018-9510. DOI: 10.1109/T-PAS.1975.31858.

HE, Haibo; YAN, Jun. Cyber-Physical Attacks and Defences in the Smart Grid: A Survey. **IET Cyber-Physical Systems: Theory & Applications**, v. 1, n. 1, p. 13–27, dez. 2016. ISSN 2398-3396. DOI: 10.1049/iet-cps.2016.0019.

KORRES, George N. A Gram Matrix-Based Method for Observability Restoration. **IEEE Transactions on Power Systems**, v. 26, n. 4, p. 2569–2571, nov. 2011. ISSN 0885-8950. DOI: 10.1109/TPWRS.2011.2126290.

KORRES, George N.; CONTAXIS, G. C. Identification and Updating of Minimally Dependent Sets of Measurements in State Estimation. **IEEE Transactions on Power Systems**, v. 6, n. 3, p. 999–1005, ago. 1991. ISSN 0885-8950. DOI: 10.1109/59.119239.

KRUMPHOLZ, G. R.; CLEMENTS, K. A.; DAVIS, P. W. Power System Observability: A Practical Algorithm Using Network Topology. **IEEE Transactions on Power Apparatus and Systems**, PAS-99, n. 4, p. 1534–1542, jul. 1980. ISSN 0018-9510. DOI: 10.1109/TPAS.1980.319578.

LIANG, Gaoqi; WELLER, Steven R.; ZHAO, Junhua; LUO, Fengji; DONG, Zhao Yang. The 2015 Ukraine Blackout: Implications for False Data Injection Attacks. **IEEE Transactions on Power Systems**, v. 32, n. 4, p. 3317–3318, jul. 2017. ISSN 0885-8950. DOI: 10.1109/TPWRS.2016.2631891.

LIU, Xuan; LI, Zhiyi; LI, Zuyi. Optimal Protection Strategy Against False Data Injection Attacks in Power Systems. **IEEE Transactions on Smart Grid**, v. 8, n. 4, p. 1802–1810, jul. 2017. ISSN 1949-3053. DOI: 10.1109/TSG.2015.2508449.

LIU, Yao; NING, Peng; REITER, Michael K. False Data Injection Attacks Against State Estimation in Electric Power Grids. **ACM Transactions on Information and System Security**, v. 14, n. 1, p. 1–33, mai. 2011. ISSN 1094-9224. DOI: 10.1145/1952982.1952995.

LONDON, Joao Bosco Augusto; ALBERTO, Luis Fernando Costa; BRETAS, Newton Geraldo. Analysis of Measurement-Set Qualitative Characteristics for State-Estimation Purposes. **IET Generation, Transmission & Distribution**, v. 1, n. 1, p. 39–45, jan. 2007. ISSN 1751-8687. DOI: 10.1049/iet-gtd:20050171.

MACULAN, Nelson; FAMPA, Marcia Helena Costa. **Otimização Linear**. Brasília: Editora Universidade de Brasília, jul. 2022. ISBN 978-85-230-0927-4.

MONTICELLI, Alcir. **State Estimation in Electric Power Systems: A Generalized Approach**. Boston: Kluwer Academic Publishers, 1999. (The Kluwer International Series in Engineering and Computer Science). ISBN 978-0-7923-8519-6. DOI: 10.1007/978-1-4615-4999-4.

MONTICELLI, Alcir; WU, Felix F. Network Observability: Identification of Observable Islands and Measurement Placement. **IEEE Transactions on Power Apparatus and Systems**, PAS-104, n. 5, p. 1035–1041, mai. 1985. ISSN 0018-9510. DOI: 10.1109/TPAS.1985.323453.

NISHIO, Ayres; COUTTO FILHO, Milton Brown; SOUZA, Julio Cesar Stacchini de; CLUA, Esteban Walter Gonzalez. GPU Parallel Processing to Enable Extensive Criticality Analysis in State Estimation. **Concurrency and Computation: Practice and Experience**, v. 36, n. 20, e8200, 2024. ISSN 1532-0634. DOI: 10.1002/cpe.8200.

ROCHA, Helder Roberto de Oliveira. **Construção de planos de medição para a estimação de estado em sistemas de potência via metaheurísticas**. 2010. Tese (Doutorado em Computação) – Universidade Federal Fluminense, Niterói.

ROCHA, Helder Roberto de Oliveira; SILVA, Jair Adriano Lima; SOUZA, Julio Cesar Stacchini de; COUTTO FILHO, Milton Brown. Fast and Flexible Design of Optimal Metering Systems for Power Systems Monitoring. **Journal of Control, Automation and Electrical Systems**, v. 29, n. 2, p. 209–218, abr. 2018. ISSN 2195-3899. DOI: 10.1007/s40313-017-0357-4.

SCHWEPPE, Fred C. Power System Static-State Estimation, Part III: Implementation. **IEEE Transactions on Power Apparatus and Systems**, PAS-89, n. 1, p. 130–135, jan. 1970. ISSN 0018-9510. DOI: 10.1109/TPAS.1970.292680.

SCHWEPPE, Fred C.; ROM, Douglas B. Power System Static-State Estimation, Part II: Approximate Model. **IEEE Transactions on Power Apparatus and Systems**, PAS-89, n. 1, p. 125–130, jan. 1970. ISSN 0018-9510. DOI: 10.1109/TPAS.1970.292679.

SCHWEPPE, Fred C.; WILDES, J. Power System Static-State Estimation, Part I: Exact Model. **IEEE Transactions on Power Apparatus and Systems**, PAS-89, n. 1, p. 120–125, jan. 1970. ISSN 0018-9510. DOI: 10.1109/TPAS.1970.292678.

SOU, Kin Cheong; SANDBERG, Henrik; JOHANSSON, Karl Henrik. Computing Critical k-Tuples in Power Networks. **IEEE Transactions on Power Systems**, v. 27, n. 3, p. 1511–1520, ago. 2012. ISSN 0885-8950. DOI: 10.1109/TPWRS.2012.2187685.

SOUZA, Julio Cesar Stacchini de; COUTTO FILHO, Milton Brown; GUIMARAENS, Marcio Andre Ribeiro. Allocating PMUs to Facilitate Processing of Bad Data in SCADA-Based State Estimation. **Journal of Modern Power Systems and Clean Energy**, v. 14, n. 3, p. 896–906, mai. 2026. ISSN 2196-5420. DOI: 10.35833/MPCE.2025.000295.

THEODORO, Edson Aparecido Rozas; BENEDITO, Raphael Augusto de S.; LONDON, Joao Bosco Augusto; ALBERTO, Luis Fernando Costa. Algebraic-Graph Method for Identification of Islanding in Power System Grids. **International Journal of Electrical Power & Energy Systems**, v. 35, n. 1, p. 171–179, fev. 2012. ISSN 0142-0615. DOI: 10.1016/j.ijepes.2011.10.010.

WHITEHEAD, David E.; OWENS, Kevin; GAMMEL, Dennis; SMITH, Jess. Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies. *In:* 2017 70th Annual Conference for Protective Relay Engineers (CPRE). [*S. l.: s. n.*], abr. 2017. p. 1–8. DOI: 10.1109/CPRE.2017.8090056.

WU, Felix F.; MONTICELLI, Alcir. Network Observability: Theory. **IEEE Transactions on Power Apparatus and Systems**, PAS-104, n. 5, p. 1042–1048, mai. 1985. ISSN 0018-9510. DOI: 10.1109/TPAS.1985.323454.

YANG, Ting; LIU, Yuzhe; LI, Wei. Attack and Defence Methods in Cyber-Physical Power System. **IET Energy Systems Integration**, v. 4, n. 2, p. 159–170, 2022. ISSN 2516-8401. DOI: 10.1049/esi2.12068.

ZANG, Tianlei; TONG, Xiaoning; LI, Chuangzhi; GONG, Yahui; SU, Rui; ZHOU, Buxiang. Research and Prospect of Defense for Integrated Energy Cyber-Physical Systems Against Deliberate Attacks. **Energies**, MDPI, v. 18, n. 6, p. 1479, jan. 2025. ISSN 1996-1073. DOI: 10.3390/en18061479.

APÊNDICE A – Ataques Cibernéticos a Sistemas Ciberfísicos de Potência

Antes de apresentar o histórico dos ataques cibernéticos, algumas definições se fazem necessárias. Enquanto Yang, Liu e Li (2022) desenvolvem sua pesquisa com foco em Sistemas Ciberfísicos de Potência (*Cyber-Physical Power Systems* — CPPS), Zang *et al.* (2025) abordam os Sistemas Ciberfísicos Integrados de Energia (*Integrated Energy Cyber-Physical Systems* — IECPS). Segundo o entendimento dos autores, o primeiro resulta da evolução do sistema de potência tradicional, antes organizado em torno do equipamento físico, voltado à transmissão e à conversão de energia, para um sistema heterogêneo e multidimensional que integra controle, computação e comunicação. Nele, os dispositivos físicos de potência conectam-se ao sistema de informação por meio de Dispositivos Eletrônicos Inteligentes (*Intelligent Electronic Devices* — IEDs), viabilizando a aquisição ubíqua de dados, a identificação de estado e a regulação da operação. O acoplamento entre fluxos de energia e de informação visa à controlabilidade e à observabilidade do sistema, e seu escopo permanece no domínio elétrico: geração, transmissão, distribuição e consumo de eletricidade. Os autores destacam que os terminais cibernéticos — RTU, *Data Transfer Unit* (DTU), *Feeder Terminal Unit* (FTU), *Transformer Supervisory Terminal Unit* e PMU instalados nas subestações e no equipamento primário — constituem o ponto de contato entre os domínios físico e cibernético e, por possuírem funções simples e ocuparem espaços publicamente expostos, oferecem oportunidades de comprometimento do sistema.

O IECPS, por sua vez, emprega mecanismos avançados de sensoriamento e controle para coordenar múltiplos sistemas de energia — eletricidade, gás natural e calor —, articulando subsistemas de escalas temporais e distribuições espaciais distintas. A distinção que Zang *et al.* (2025) estabelecem explicitamente não é frente ao CPPS, mas frente aos Sistemas Integrados de Energia (*Integrated Energy Systems* — IES): o IECPS concentra-se nos mecanismos de interação entre as redes cibernética e física, enquanto o IES reduz o papel da camada cibernética e não representa o impacto real de ataques cibernéticos sobre o sistema físico.

A diferença de abrangência é relevante para a leitura do histórico apresentado a seguir: no IECPS, a convergência dos vetores energéticos faz com que mesmo falhas pequenas em um único sistema possam propagar-se aos demais e acumular-se até resultar em falhas em cascata multissistêmicas, ao passo que, no CPPS, a propagação permanece circunscrita à rede elétrica e à sua camada de comunicação. Os vetores de ataque cibernético, contudo, são em larga medida comuns aos dois casos, uma vez que ambos dependem da integridade e da disponibilidade dos dados de medição.

A.1 Histórico dos Ataques Cibernéticos

A transição da segurança da informação tradicional para o campo da guerra cibernética moderna é marcada pelo surgimento do *worm* Stuxnet. Diferentemente de ameaças anteriores, o Stuxnet foi identificado como a primeira verdadeira "arma cibernética" projetada especificamente para controlar e danificar maquinário físico industrial. Chen (2011) descreve que este *malware* era seletivo, utilizando quatro vulnerabilidades de "dia zero"[1] no Windows para buscar Controladores Lógicos Programáveis (CLPs) específicos da Siemens. A sofisticação do código e o uso de certificados digitais roubados sugerem o envolvimento de Estados nacionais em seu desenvolvimento, visando sabotar infraestruturas críticas como a planta nuclear de Bushehr no Irã. Este evento demonstrou que ataques cibernéticos poderiam transpor o domínio digital e causar danos físicos reais.

Com a digitalização dos SEPs, ficou evidente que eles também poderiam sofrer ataques similares. O setor elétrico de um Estado nacional constitui um campo sensível diante de uma guerra cibernética e a má operação do sistema elétrico pode levar um país inteiro a ficar horas ou dias sem energia elétrica. Um trabalho seminal que demonstrou a vulnerabilidade do sistema elétrico diante de um ciberataque coordenado foi apresentado em Liu, Ning e Reiter (2011).

Até o ano de 2011, acreditava-se que a função EE poderia garantir a confiabilidade do estado da rede (módulo e ângulo das tensões nas barras) para operação do SEP por meio do tradicional teste de detecção e identificação de dados espúrios das medidas que chegam pelos sistemas SCADA. Entretanto, com o trabalho de Liu, Ning e Reiter (2011) sobre FDIAs, ficou demonstrado que, se um invasor possuir conhecimento da configuração e da topologia da rede elétrica, ele pode injetar medidas falsas de forma coordenada que burlam as técnicas tradicionais de detecção de erros grosseiros na estimação de estado. O

[1] Ataque de "dia zero" se refere a uma falha de segurança no Windows ou em qualquer outro sistema, desconhecida pelo criador do software.

perigo central reside no fato de que o resíduo da medição permanece abaixo do limiar de detecção, permitindo manipulações arbitrárias nas variáveis de estado. Embora até a data da publicação não houvesse registro de um ataque dessa natureza, o trabalho demonstrou que isso era possível.

Isso mudou em 2015, quando foi registrado na Ucrânia o primeiro apagão publicamente atribuído a um ciberataque contra o SEP. Este ataque foi analisado detalhadamente por Whitehead *et al.* (2017) e Liang *et al.* (2017). O ataque utilizou *spear phishing*[2] para introduzir o *malware* BlackEnergy 3, seguido pela captura de credenciais de VPN e manipulação manual das Interfaces Homem-Máquina (IHMs) para abrir disjuntores em mais de 50 subestações, afetando 225.000 consumidores. Liang *et al.* (2017) enfatizam que este evento validou as suposições teóricas dos FDIAs.

Outros ataques foram relatados com o passar dos anos. Em uma recente publicação, Zang *et al.* (2025) apresentam uma evolução nos ataques contra IECPS. Nesse trabalho, os autores relatam que o ataque à Ucrânia em 2015 atingiu 750.000 residências, não 225.000 como relatado em Whitehead *et al.* (2017), além de acrescentar a informação de que o ataque foi atribuído ao grupo russo "SandWorm". No ano de 2019, um ataque cibernético à hidrelétrica Simón Bolívar na Venezuela paralisou 22 estados; o processo de restauração foi ainda dificultado devido a uma explosão na planta. Ainda em 2019, na Índia, a usina nuclear Kudankulam, a maior do país, sofreu um ataque cibernético. Embora o incidente tenha causado poucos danos, gerou comoção pública no país. A partir de 2020, a extorsão financeira via *ransomware*[3] tornou-se predominante: no Brasil, a Light S.A. foi alvo do *malware Sodinokibi*; em Portugal, a EDP foi atingida pelo *Ragnar Locker*; e nos EUA (2021), o ataque à Colonial Pipeline, maior empresa de oleodutos de combustível do país, forçou a interrupção de todas as operações, causando perdas econômicas elevadas e escassez de combustível em diversos estados. Mais recentemente, em 2022, o grupo "SandWorm" tentou utilizar o *malware Industroyer2* contra subestações de alta tensão na Ucrânia, mas o ataque foi detectado a tempo. Em 2023, a empresa italiana Acea, responsável pelo fornecimento de eletricidade e água em Roma, foi atacada pelo grupo de *ransomware* Black Basta, resultando na queda de seus serviços web.

Com a crescente complexidade das *Smart Grids*, a literatura passou a focar em modelos de defesa sistêmicos e na gestão de incertezas. He e Yan (2016) apresentaram uma

[2] Diferentemente dos ataques cibernéticos generalistas realizados por meio de e-mail, SMS ou chamadas telefônicas (*phishing*), *spear phishing* se refere a ataques direcionados, em que o atacante possui conhecimento do alvo de ataque de modo que o ataque se pareça mais convincente devido à sua personalização.

[3] *Ransomware* é uma modalidade de software malicioso (*malware*) que restringe o acesso a sistemas ou arquivos, geralmente por meio de criptografia, e condiciona sua liberação ao pagamento de um resgate.

pesquisa abrangente classificando as vulnerabilidades sob uma perspectiva de Sistemas Ciberfísicos. Eles destacam que a *Smart Grid* integra tecnologias de informação com a geração, transmissão e distribuição, criando uma superfície de ataque vasta e heterogênea. A pesquisa detalha esquemas de ataque em vários níveis, incluindo o Controle Automático de Geração (*Automatic Generation Control* — AGC), no qual o ataque *Aurora*[4] pode destruir geradores, e ataques em Infraestruturas de Medição Avançada (*Advanced Metering Infrastructure* — AMI) que afetam a privacidade e o faturamento. Os autores enfatizam que a segurança física e a cibersegurança tradicionais não são mais suficientes isoladamente, exigindo uma abordagem integrada de proteção, detecção e mitigação.

Yang, Liu e Li (2022) e Zang *et al.* (2025) apresentaram revisões bibliográficas com o objetivo de sistematizar os tipos de ameaças multidimensionais conhecidas até o momento; ambos convergem na classificação das ameaças em três domínios principais: ataques cibernéticos, ataques físicos e ataques coordenados ciberfísicos. Eles ainda propuseram um modelo de defesas em três níveis: prevenção, detecção durante o ataque e mitigação e resposta pós-ataque. Os tipos de ataques e os níveis de proteção sugeridos são apresentados na próxima seção.

A.2 Ataques Cibernéticos

Os ataques cibernéticos são direcionados aos dispositivos computacionais, aos terminais de aquisição de dados, aos sistemas de controle e às redes de comunicação que integram a infraestrutura energética. Seu objetivo consiste em comprometer propriedades essenciais da informação, como integridade, disponibilidade, confidencialidade e autenticidade. Em sistemas elétricos ciberfísicos, esses ataques podem modificar medidas, interromper canais de comunicação, retransmitir informações antigas ou assumir o controle de dispositivos legítimos. Como consequência, o centro de controle pode receber uma representação incorreta ou incompleta do estado real do sistema e, com base nela, emitir comandos operacionais inadequados.

[4] O ataque *Aurora* é um tipo de ataque ciberfísico direcionado aos sistemas de controle e proteção de geradores elétricos. Seu princípio consiste em comandar a abertura e o fechamento de um disjuntor em momentos estrategicamente escolhidos, fazendo com que o gerador seja reconectado à rede fora de sincronismo. Essa reconexão inadequada provoca esforços elétricos e mecânicos intensos, capazes de causar danos permanentes ao equipamento (He; Yan, 2016).

A.2.1 Ataques de injeção de dados falsos

Os ataques de injeção de dados falsos, FDIAs, estão entre as ameaças mais relevantes para os sistemas elétricos ciberfísicos. Nessa modalidade, o invasor altera deliberadamente valores de medidas, informações operacionais ou resultados do processo de estimação de estado com o propósito de induzir decisões incorretas no centro de controle. Os dados adulterados podem afetar grandezas como tensão, potência injetada, fluxo de potência, frequência, pressão e vazão, dependendo dos subsistemas energéticos envolvidos.

A principal característica dos FDIAs é a possibilidade de construção de vetores de ataque compatíveis com o modelo matemático utilizado pelo sistema. Dessa forma, as alterações introduzidas podem manter os resíduos normalizados do estimador abaixo dos limites empregados pelos mecanismos convencionais de detecção de dados ruins, dificultando a identificação do ataque.

Zang *et al.* (2025) agrupam os FDIAs em três modalidades principais. Os FDIAs gerais buscam modificar medições ou estados estimados sem necessariamente alterar a topologia do sistema. Os ataques de redistribuição de carga, *Load Redistribution Attacks* (LRs), alteram a distribuição espacial das cargas, mas preservam o valor total da demanda, reduzindo a possibilidade de detecção por verificações simples de balanço. Já os ataques de falsa topologia adulteram informações relativas ao estado de linhas, transformadores, válvulas, disjuntores ou dispositivos de proteção, simulando alterações inexistentes na configuração física da rede. Para manter a coerência da falsa topologia, o atacante também precisa modificar as medições associadas aos componentes afetados.

A.2.2 Ataques de negação de serviço

Os ataques de negação de serviço — *Denial of Service* (DoS) — têm como finalidade comprometer a disponibilidade dos serviços de comunicação. Para isso, o atacante pode explorar vulnerabilidades de protocolos, bloquear canais de transmissão ou gerar um volume excessivo de tráfego, impedindo que informações legítimas sejam processadas em tempo adequado. Nos ataques distribuídos de negação de serviço, *Distributed Denial of Service* (DDoS), múltiplos dispositivos comprometidos são utilizados simultaneamente para ampliar a intensidade e a abrangência da ofensiva.

Em sistemas energéticos, a indisponibilidade da comunicação pode impedir o recebimento de telemetria, atrasar a transmissão de alarmes e bloquear o envio de comandos de controle. Como resultado, funções dependentes de comunicação em tempo real, como

a estimação remota de estados, o controle de frequência, a operação de microrredes e a coordenação entre diferentes subsistemas energéticos, podem apresentar desempenho inadequado ou tornar-se completamente indisponíveis. Além disso, ataques DoS podem ser utilizados para ocultar falhas físicas ou impedir que o centro de controle atue durante a evolução de uma contingência.

A.2.3 Ataques de sincronização temporal

Os ataques de sincronização temporal, *Time Synchronization Attacks* (TSAs), exploram a dependência dos sistemas de monitoramento e controle em relação a referências precisas de tempo, geralmente fornecidas por sistemas de navegação por satélite. Muitos dispositivos de sincronização transmitem ou recebem sinais sem mecanismos robustos de autenticação e criptografia, permitindo que o invasor gere sinais falsificados ou interfira na recepção dos sinais legítimos.

A alteração da referência temporal provoca erros na marcação de tempo e no alinhamento das medições obtidas por UMFs. Como as grandezas fasoriais coletadas em diferentes pontos da rede precisam estar sincronizadas, pequenos desvios temporais podem produzir erros significativos nos ângulos de fase estimados. Tais inconsistências podem comprometer os sistemas de medição, prejudicar a avaliação do estado da rede e conduzir à emissão de comandos de controle inadequados, incluindo atuações incorretas de proteção e desligamentos indevidos de unidades geradoras.

A.2.4 Ataques de repetição

Nos ataques de repetição, *replay attacks*, o invasor intercepta dados ou comandos legítimos transmitidos durante a operação normal e os retransmite posteriormente. Como as mensagens reproduzidas foram originalmente válidas, elas podem ser aceitas pelo sistema caso não existam mecanismos adequados de autenticação, marcação temporal ou verificação de sequência.

O atacante pode, por exemplo, retransmitir valores de medidas antigas para ocultar uma condição anormal da rede, fazendo com que o centro de controle continue observando um estado aparentemente normal. Também podem ser repetidos comandos de abertura e fechamento de disjuntores, sinais do Controle Automático de Geração (AGC) ou instruções dirigidas a outros equipamentos. Nesses casos, o ataque não se limita a comprometer a percepção do operador, podendo provocar atuações físicas repetitivas e potencialmente

destrutivas.

A.2.5 Ataques *man-in-the-middle*

Nos ataques *Man-in-the-Middle* (MITM), o invasor posiciona-se de forma oculta entre dois dispositivos ou sistemas que acreditam estar se comunicando diretamente. Mediante a exploração de vulnerabilidades nos protocolos de comunicação, falsificação de endereços, instalação de *malware* ou personificação de dispositivos legítimos, o atacante passa a interceptar as mensagens trocadas.

Uma vez estabelecida a posição intermediária, o invasor pode ler, bloquear, atrasar e modificar tanto os dados enviados ao centro de controle quanto os comandos transmitidos aos dispositivos de campo. Essa atuação bidirecional permite, por exemplo, alterar uma instrução de controle e, posteriormente, modificar as medições de retorno para ocultar seus efeitos. Por ocorrer no interior do canal de comunicação e preservar aparentemente o fluxo normal de mensagens, o MITM apresenta elevado grau de furtividade e pode permanecer ativo por períodos prolongados.

A.2.6 Ataques cibernéticos coordenados

Além das modalidades isoladas, Zang *et al.* (2025) destacam os ataques cibernéticos coordenados, *Coordinated Cyberattacks* (CCAs), nos quais duas ou mais técnicas são empregadas de maneira combinada. Entre os exemplos relatados encontram-se a associação entre FDIA e atraso de comunicação, FDIA e DoS, TSA e DoS, além da alteração simultânea de dados pertencentes a diferentes subsistemas energéticos.

A coordenação permite que uma técnica compense as limitações de outra. Um FDIA pode, por exemplo, modificar os dados utilizados pelo operador, enquanto um ataque DoS impede o recebimento de informações que revelariam a adulteração. De modo semelhante, dados elétricos, térmicos e de gás podem ser modificados simultaneamente, explorando as interdependências existentes entre esses sistemas. Essa combinação aumenta a flexibilidade, a furtividade e o potencial destrutivo da ofensiva.

A.3 Ataques Físicos

Os ataques físicos são caracterizados pela atuação direta sobre equipamentos, instalações e recursos que compõem a infraestrutura energética. Diferentemente dos ataques exclu-

sivamente cibernéticos, essa categoria busca degradar ou eliminar a funcionalidade de componentes físicos, como linhas de transmissão, subestações, transformadores, gasodutos, estações de gás, sensores, dispositivos de medição e sistemas de comunicação.

Yang, Liu e Li (2022) mencionam ataques eletromagnéticos capazes de danificar equipamentos por meio de sobretensões ou pulsos eletromagnéticos. Os autores também destacam os ataques de ressonância, nos quais sinais de carga, referência ou controle são manipulados de forma oscilatória, buscando excitar modos dinâmicos do sistema. Quando a frequência do sinal de ataque se aproxima de uma frequência característica da malha de controle, as oscilações podem ser amplificadas, provocando desvios de frequência, degradação do controle carga-frequência e perda de estabilidade.

Zang *et al.* (2025) descrevem outras formas de ataques físicos, como o emprego de bombas de grafite, ataques realizados por veículos aéreos não tripulados e interferência por laser. Os autores também incluem o furto de energia por conexões clandestinas entre as ações que afetam fisicamente a infraestrutura, embora essa prática produza principalmente perdas não técnicas e não possua, necessariamente, o mesmo potencial de provocar colapsos sistêmicos que os ataques dirigidos a equipamentos críticos. De maneira geral, os efeitos dos ataques físicos podem variar desde a degradação parcial de um componente até sua completa indisponibilidade.

A.4 Ataques Ciberfísicos Coordenados

Os ataques ciberfísicos coordenados, *Coordinated Cyber-Physical Attacks* (CCPAs), combinam ações realizadas nos domínios cibernético e físico, explorando a interdependência entre as redes de informação e a infraestrutura energética. Essa categoria representa uma ameaça especialmente relevante porque o componente cibernético pode ser utilizado para ocultar, intensificar ou prolongar os efeitos da agressão física. Simultaneamente, o dano físico pode ampliar as consequências das alterações produzidas nos sistemas de informação e controle.

A coordenação pode envolver, por exemplo, a destruição de uma linha, tubulação ou unidade de medição associada à adulteração de dados enviados ao centro de controle. Enquanto a infraestrutura física é danificada, um FDIA pode produzir medições aparentemente normais, e um ataque DoS pode impedir a transmissão de alarmes ou informações de falha. Dessa forma, o operador permanece sem conhecimento preciso da condição do sistema e pode emitir comandos que agravam a contingência. Zang *et al.* (2025) orga-

nizam os CCPAs em duas estratégias principais, conforme a ordem em que as ações são realizadas.

A.4.1 Priorização do ataque físico

Na estratégia com priorização do ataque físico, o invasor inicialmente danifica um componente da infraestrutura, como uma linha, tubulação, reator de compensação ou dispositivo de medição. Em seguida, utiliza recursos cibernéticos para ocultar a falha ou retardar sua identificação. A adulteração das medições pode simular condições normais ou produzir uma falsa situação de sobrecarga, induzindo o sistema de despacho a tomar decisões inadequadas. Alternativamente, um ataque DoS pode bloquear ou atrasar o envio das informações sobre o componente danificado.

Essa atuação cria uma janela temporal na qual a falha física permanece sem tratamento adequado. Durante esse intervalo, o atacante pode ampliar a extensão dos danos, atingir novos componentes ou explorar a resposta incorreta do sistema, aumentando a probabilidade de falhas em cascata.

A.4.2 Priorização do ataque cibernético

Na estratégia com priorização do ataque cibernético, o invasor começa comprometendo a capacidade de percepção, comunicação ou controle do sistema. Isso pode ocorrer por meio da interrupção dos canais de comunicação, da adulteração das medições ou da modificação dos dados de carga. Uma vez reduzida a consciência situacional do centro de controle, o atacante executa a ação física contra uma infraestrutura que se encontra, naquele momento, menos protegida ou operando com base em informações incorretas.

Os LRs são frequentemente empregados nessa abordagem. Inicialmente, o invasor modifica os dados de demanda para alterar a percepção dos fluxos e das condições operacionais. Em seguida, realiza o desligamento ou a destruição física de uma linha e continua alterando as medições para ocultar a contingência. A combinação entre preparação cibernética, dano físico e ocultação posterior permite prolongar a permanência do ataque e ampliar seus efeitos.

A.5 Estratégias de Defesa em Sistemas Ciberfísicos

As estratégias de proteção aplicáveis aos CPPS e aos IECPS podem ser organizadas de acordo com a evolução temporal de um incidente. Embora empreguem terminologias distintas, Yang, Liu e Li (2022) e Zang *et al.* (2025) convergem para uma estrutura composta por três etapas: prevenção antes do ataque, detecção e resposta durante sua ocorrência e recuperação e aperfeiçoamento das defesas após o evento.

Apesar dessa convergência estrutural, as duas revisões apresentam enfoques diferentes. Yang, Liu e Li (2022) concentram-se predominantemente no sistema elétrico e nas interações entre redes de comunicação, sistemas de controle e equipamentos de potência. Por essa razão, enfatizam autenticação, criptografia, detecção de intrusões e controle resiliente. Zang *et al.* (2025), por sua vez, ampliam a análise para sistemas que integram eletricidade, gás, calor, transporte e infraestrutura de comunicação. Consequentemente, atribuem maior importância ao planejamento da infraestrutura, à coordenação entre diferentes vetores energéticos, ao isolamento de falhas entre subsistemas e à recuperação conjunta das redes físicas e cibernéticas. Como a contribuição desta tese se concentra na prevenção antes do ataque, nas próximas seções será apresentada uma revisão apenas desta primeira etapa. Quanto às etapas de proteção durante o ataque e recuperação e aperfeiçoamento das defesas após o evento, recomenda-se a leitura das revisões apresentadas em (Yang; Liu; Li, 2022; Zang *et al.*, 2025).

A.5.1 Prevenção e planejamento antes do ataque

A primeira etapa tem por finalidade reduzir a superfície de ataque, identificar vulnerabilidades e preparar o sistema para suportar perturbações antes que uma ação maliciosa seja iniciada. Os autores, contudo, abordam essa preparação por perspectivas distintas e complementares.

A.5.1.1 Proteção do acesso e alocação de recursos em CPPS

Para Yang, Liu e Li (2022), a defesa preventiva começa pelo controle do acesso aos dispositivos e às redes do CPPS. O crescimento do número de dispositivos eletrônicos inteligentes, sensores, unidades de medição e recursos energéticos distribuídos exige mecanismos capazes de verificar a legitimidade dos usuários e equipamentos conectados. Nesse contexto, a autenticação e o acesso confiável constituem a primeira barreira contra intrusões, impedindo que dispositivos não autorizados ingressem na infraestrutura de comunicação ou

assumam a identidade de componentes legítimos.

Os autores também destacam a criptografia dos dados transmitidos entre dispositivos de campo, redes de comunicação e centros de controle. Dependendo da criticidade da informação e da capacidade computacional dos equipamentos, podem ser empregados algoritmos simétricos ou assimétricos. Nesse modelo, a autorização não é concedida permanentemente com base apenas na localização do dispositivo; sua credibilidade deve ser continuamente avaliada durante a interação com o sistema.

A prevenção proposta por Yang, Liu e Li (2022) não se restringe ao bloqueio do acesso. Os autores defendem que diferentes cenários de ataque sejam simulados para identificar antecipadamente os componentes mais vulneráveis e estimar a extensão dos possíveis danos. Árvores de ataque, grafos de ataque e modelos de propagação de falhas permitem representar os caminhos que um invasor pode percorrer até alcançar ativos críticos. A partir dessas análises, recursos limitados de defesa podem ser distribuídos de maneira mais eficiente, priorizando dispositivos, canais de comunicação e áreas cuja perda produziria consequências mais severas.

Métodos baseados em teoria dos jogos, análise probabilística e redes bayesianas são apresentados como instrumentos para equilibrar o custo da proteção e o risco associado a diferentes ataques. As estratégias resultantes podem ser implementadas por meio de *firewalls*, mecanismos de isolamento entre redes e dispositivos de separação dos fluxos de comunicação. Assim, o enfoque preventivo de Yang, Liu e Li (2022) combina proteção de acesso, análise de vulnerabilidades e alocação otimizada dos recursos de cibersegurança.

A.5.1.2 Planejamento resiliente da infraestrutura em IECPS

Zang *et al.* (2025) expandem a prevenção para o planejamento conjunto das infraestruturas física e cibernética. Em vez de se concentrarem apenas na proteção do acesso à informação, os autores procuram garantir que o IECPS continue operando mesmo quando alguns de seus componentes forem comprometidos. Essa abordagem é organizada em três frentes: planejamento de equipamentos redundantes, planejamento do acoplamento entre sistemas e alocação antecipada de recursos emergenciais.

O planejamento de redundância abrange tanto o domínio energético quanto o cibernético. No primeiro, são considerados equipamentos adicionais de geração, microturbinas, unidades solares, dispositivos de armazenamento fixos ou móveis e sistemas combinados de eletricidade, calor e refrigeração. Esses recursos podem substituir componentes indis-

poníveis e reduzir a interrupção do fornecimento após um ataque. No domínio cibernético, a redundância envolve dispositivos de medição, PMUs, *gateways*, controladores e canais de comunicação. O aumento da redundância das medições melhora a observabilidade do sistema e dificulta a execução de ataques de injeção de dados falsos, pois o invasor precisa comprometer um conjunto maior de informações para manter a coerência dos dados adulterados.

Entretanto, Zang *et al.* (2025) ressaltam que a redundância excessiva aumenta os custos de implantação. Portanto, o problema não consiste simplesmente em duplicar todos os equipamentos, mas em determinar quais componentes devem ser reforçados, em que quantidade e em quais localizações. O planejamento deve buscar uma solução de compromisso entre investimento, confiabilidade e resiliência.

Outra contribuição apresentada por Zang *et al.* (2025) é o planejamento do acoplamento entre os sistemas energético e de transporte. Veículos elétricos podem funcionar como recursos móveis de armazenamento e fornecer energia à rede ou a edificações. Em condições normais, a coordenação da recarga contribui para reduzir picos de demanda. Durante uma emergência, veículos de geração móvel, unidades de armazenamento transportáveis e veículos elétricos podem auxiliar o suprimento de áreas isoladas.

O sistema de transporte também pode apoiar a recuperação da infraestrutura cibernética. Quando um ataque interrompe as comunicações, veículos de comunicação emergencial, aeronaves não tripuladas ou outros recursos móveis podem estabelecer redes provisórias entre o centro de controle e a área afetada. Assim, diferentemente da abordagem de Yang, Liu e Li (2022), predominantemente concentrada na proteção do sistema elétrico e de sua rede de dados, Zang *et al.* (2025) tratam outros setores como recursos ativos de defesa.

A terceira frente preventiva consiste no planejamento antecipado de recursos para situações nas quais ataques deliberados coincidam com eventos extremos. Essa estratégia envolve o aprimoramento da percepção do sistema, a previsão de riscos e a distribuição prévia de recursos emergenciais. Entre os exemplos encontram-se o posicionamento de armazenamento móvel, geradores, reservatórios de gás e equipes de manutenção nas regiões com maior probabilidade de falha. Nesse caso, a prevenção deixa de ser exclusivamente cibernética e passa a integrar informações meteorológicas, condições da infraestrutura e riscos de ataques oportunistas.